SBC Documentation



SBC 1000/2000 Series

For the latest documentation, please visit **https://support.sonus.net**

Sonus Technical Publications
http://www.sonus.net

Document Version: 1.0
Software Version: 4.1.0

Copyright © 2015 Sonus Networks. All rights reserved.

Disclaimer

This document presents information for users of the products of Sonus Networks, Inc. (“Sonus”), its affiliates and its subsidiaries (collectively, the “Sonus Group”). Network Equipment Technologies, Inc. is part of the Sonus Group. The Sonus Group does not assume any liability arising out of the application or use of any product or circuit described herein. No part of this document may be copied or reproduced in any form or by any means without the prior written permission of Sonus. For the most current user documentation, please contact your Sonus customer support representative

Copyright

Copyright © 1999 - 2015 Sonus Networks, Inc. All rights reserved. Printed in the U.S.A. This item and the information contained herein are the property of the Sonus Group. This publication may be used, copied, or distributed only in accordance with the terms of the license agreement. Any other use, reproduction, or distribution may occur only upon Sonus’ prior written consent. .

Third-Party Copyrights

Open BSD Copyright (c) 1982, 1986, 1990, 1991, 1993. The Regents of the University of California. All rights reserved. THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the above disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the above disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Disclaimer and Restrictions

on the part of the Sonus Group. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, the Sonus Group assumes no liability resulting from technical or editorial errors or omissions, or for any damages whatsoever resulting from the furnishing, performance, or use of the information contained herein. The Sonus Group reserves the right to revise this publication, and to make changes on the content hereof without notice.

The information in this document may be used by customers solely for the use and understanding of the Sonus Group’s products and solutions. This document is not meant to define an interface between products of the Sonus Group and any third party hardware or software. The Sonus Group reserves the right to change the design and implementation used for any of the tables, screens, field names, etc. to enhance its products as it sees fit.

Warranties

THIS INFORMATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING,BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. REFERENCES TO CORPORATIONS, THEIR SERVICES AND PRODUCTS, ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL THE SONUS GROUP BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS INFORMATION.

Descriptions of, or references to, products, services or publications within the Sonus Group's documentation do not imply endorsement of that product, service or publication. Sonus Networks makes no warranty of any kind with respect to the subject matter included herein, the products listed herein, or the completeness or accuracy of the information. Sonus Networks specifically disclaims all warranties, express, implied or otherwise, including without limitation, all warranties of merchantability and fitness for a particular purpose.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES MAY BE PERIODICALLY MADE TO THE INFORMATION HEREIN.

Trademarks

Sonus Networks, the Sonus Networks logo, Open Services Architecture, Insignus, SMARRT, Sonus Networks Insight, IMX, GSX9000, GSX4000, GSX4010, SBC 5100TM, SBC 5200TM, IMX, SBC9000, the Atreus logo, the Performance Technology, Inc. logo, Insight xAuthority, Monterey 8000, NexusWare, SEGway and SIP Xpress are either registered trademarks or trademarks of

Sonus Networks, Inc. Open Services Partner Alliance and Sonus Networks CARE are service marks of Sonus Networks, Inc. The Sonus Group trademarks may not be used in connection with any product or service that is not the Sonus Group's in any manner that is likely to cause confusion among customers or in any manner that disparages or discredits the Sonus Group. All other product names mentioned herein are trademarks, service marks, registered trademarks, or registered service marks of their respective owners. .

Embedded Sofware

Oracle Enterprise Edition is an embedded part of the Sonus Group product line. The programs included herein are subject to a restricted use license and can only be used in conjunction with this application. You are not allowed to navigate or modify the underlying database schema unless explicitly authorized in writing by Sonus.

Export Laws

Sonus Group product documentation includes technical information developed in the United States that may be subject to limitations on export imposed by the U.S. Department of State and the U.S. Department of Commerce. All use, distribution, and transfer of any technical information shall be in compliance with U.S. export laws and regulations.

Copyright © 2015 Sonus Networks. All rights reserved.

1. Sonus SBC 1000-2000 Documentation 6
1.1 Sonus SBC 1000-2000 User's Guide 6
1.1.1 Getting to Know the Sonus SBC 1000-2000 11
1.1.2 Troubleshooting Sonus SBC 1000-2000 47
1.1.3 Checking your System Information 97
1.1.4 Working with Licenses 106
1.1.5 Working with Certificates 111
1.1.6 Integrating with Active Directory 128
1.1.7 Integrating with RADIUS 143
1.1.8 Working with Physical Ports 153
1.1.9 Working with SIP 188
1.1.10 Working with Telephony Routing 253
1.1.11 Working with Users and Groups 301
1.1.12 Working with Telephony Mapping Tables 313
1.1.13 Working with CAS 352
1.1.14 Working with System Settings 380
1.1.15 Working with Microsoft Unified Communications 404
1.1.16 Working with the ASM and SBA 425
1.1.17 Working with Media 486
1.1.18 Working with Tones 507
1.1.19 Working with SNMP and Alarms 510
1.1.20 Working with Logging 520
1.1.21 Working with Ethernet Interfaces and IP 532
1.1.22 Working with System Software 555
1.1.23 Working with Call Detail Records 567
1.1.24 Working with the Web Interface 583
1.1.25 Working with ISDN 594
1.1.26 Working with SCOM 608
1.1.27 Working with Enhanced 911 Devices 615
1.1.28 Working with Dynamic Routing 618
1.1.29 Working with Access Control Lists and Session Control 622
1.1.30 Working with Network Services 633
1.1.31 SIP Message Manipulation 649
1.1.32 Miscellaneous Topics 677
1.1.33 Working with IPsec 680
1.1.34 Working with NAT and Port Forwarding 707
1.1.35 Working with Branch Survivability 713
1.1.36 Working with Historical Data and TCA Thresholds 723
1.1.37 Working with Multiple Spanning Trees 727
1.1.38 About Signaling Groups 731
1.1.39 Working with RTP Proxies 731
1.1.40 Working With Security 732
1.2 Sonus SBC 1000-2000 API User's Guide 733
1.2.1 Sonus SBC 1000-2000 API - Requirements 737
1.2.2 Sonus SBC 1000-2000 API - Resource Design 738
1.2.3 Sonus SBC 1000-2000 API - Authentication 748
1.2.4 Sonus SBC 1000-2000 API - REST Samples 752
1.2.5 Sonus SBC 1000-2000 API - Deployment Workflow 776
1.3 SBC 1000-2000 Installation and Upgrade Guide 781
1.3.1 SBC 1000-2000 Requirements 782
1.3.2 Installing the Sonus SBC 1000-2000 Hardware 787
1.3.3 Running Initial Setup 796
1.3.4 Upgrading Sonus SBC 1000-2000 805

Copyright © 2015 Sonus Networks. All rights reserved.

1.3.5 Supported Platforms 812
1.4 SBC 1000-2000 FAQ and Best Practices 816
1.4.1 Administration FAQ 819
1.4.2 Best Practices 820
1.4.3 How Incoming Calls are Handled when Server is Unreachable 1443
1.5 SBC 1000-2000 Releases 1449
1.5.1 Production Releases 1450
1.5.2 Service Advisories 1572
1.6 Sonus SBC 1000-2000 Resources 1587
1.6.1 Sonus SBC 1000-2000 Download Center 1588
1.6.2 SBC 1000-2000 Solution Base 1589
1.6.3 Terms and Conditions 1590
1.6.4 Copyright and Trademarks 1590
1.6.5 Contacting Sonus 1595
1.6.6 Sonus SBC 1000-2000 Interface Card Shipping Policy 1595

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000-2000 Documentation

Unified Exchange - Sonus SBC 1000/2000 4.1.x

User's Guide

The Sonus SBC 1000/2000 User's Guide is for system administrators, developers, testers - anyone who uses Sonus SBC 1000/2000. New to Sonus SBC 1000/2000? Start by exploring the User Interface. You may also find the Sonus SBC 1000/2000 Solution Base articles, FAQ & Best Practices articles, and Topic Index useful.

Installation Guide

The Sonus SBC 1000/2000 Installation Guide is for people who are installing Sonus SBC 1000/2000 for the first time. Check the requirements and supported platforms, then download and install Sonus SBC 1000/2000.

Upgrade Guide

The Upgrading Sonus SBC 1000-2000 is for people who are upgrading their version of Sonus SBC 1000/2000. Start by reading the latest Release Notes and version-specific Upgrade Guide for the version to which you are upgrading, then download Sonus SBC 1000/2000 and follow the main Upgrade Guide.

Developer Resources

These resources are for software developers who want to integrate, control, and maintain the Sonus SBC 1000/2000 through the REST Web Service. Take a look at the Sonus SBC 1000-2000 API User's Guide and the API Reference Documentation.

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000-2000 User's Guide

The Sonus SBC 1000/2000 User's Guide is for System Administrators and Operators. It contains detailed task-based instructions for using all the features and functionality of the Sonus SBC 1000/2000 Series gateways.

Getting to Know the Sonus SBC 1000-2000

- Sonus SBC 1000-2000 Status LEDs
- Sonus SBC 1000-2000 System Hardware
- Notes and Limitations
- Sonus SBC 1000-2000 System Performance and Capacity

Troubleshooting Sonus SBC 1000-2000

- Rebooting Sonus SBC 1000-2000
- Resetting the Sonus SBC 1000-2000 to Factory Defaults
- Common Troubleshooting Issues
- Common Troubleshooting Issues with Certificates in Sonus SBC 1000-2000
- Alarms and Events Reference
- Working with the Debug Facility
- Testing a Call
- Testing Network Connections
- Viewing Mounted File Systems
- Viewing Active Processes
- Viewing The SIP Connections Table
- Viewing The Disk Partition Table

Checking your System Information

- Viewing the Software Version and Hardware ID
- Viewing ASM System Details
- Viewing and Clearing Global Call Counters
- Checking Port Status
- Checking Cards and Modules Status
- Checking System Fan Status
- Checking Power Supply Status
- Viewing Installed Modules, Power Supplies, and Ports
- Viewing DSP Module Statistics
- Status Panel States and Actions

Working with Licenses

- Decoding License Keys
- Installing Licenses
- Viewing Licenses

Working with Certificates

- Managing Server Certificates
- Managing Trusted CA Certificates
- Requesting a Signed Certificate using a Standalone Windows CA
- Downloading a CA Certificate using a Standalone Windows CA

Integrating with Active Directory

- Configuring the Sonus SBC 1000-2000 for Active Directory

Copyright © 2015 Sonus Networks. All rights reserved.

- Configuring the Sonus SBC 1000-2000 for Active Directory User Domain Access
- Managing Domain Controllers
- Managing Active Directory Groups to Access Level Mapping
- Querying the Active Directory Cache

Integrating with RADIUS

- Configuring the Sonus SBC 1000-2000 for RADIUS
- Managing RADIUS Servers
- Managing RADIUS User Class Access Level Mapping
- RADIUS User Authentication Tips Using FreeRADIUS

Working with Physical Ports

- Managing Ethernet Ports
- Managing Telephony Ports

Working with SIP

- Managing SIP Signaling Groups
- Managing SIP Profiles
- Managing TLS Profiles
- Managing SIP Server Tables
- Managing Local Registrars
- Managing Contact Registrant Tables
- Managing Remote Authorization Tables
- Managing Local Pass-through Authorization Tables
- Managing SIP Trunk Groups
- Miscellaneous SIP Information

Working with Telephony Routing

- Managing Signaling Groups
- Managing Call Routing Tables
- Managing Transformation Tables
- Managing Action Configurations
- Managing Action Sets
- Routing Usage Examples

Working with Users and Groups

- How User Authentication Works
- Permissions Overview
- Monitoring User Activity
- Changing The Current User's Password
- Managing Remote Authentication
- Managing Local Users
- Managing Global Security Options
- Recovering Admin Passwords

Working with Telephony Mapping Tables

- Managing Cause Code Reroute Tables
- Managing Message Translations
- Managing Q.850 to SIP Override Tables
- Managing SIP to Q.850 Override Tables
- Q850 Cause Codes

Copyright © 2015 Sonus Networks. All rights reserved.

- SIP Response Codes

Working with CAS

- Managing CAS Signaling Groups
- Managing CAS Profiles
- Managing Supplementary Service Profiles

Working with System Settings

- Backing Up Data
- Restoring Data
- Using the Custom Passphrase
- Configuring Host Information and DNS
- Configuring the System Clock Source
- Configuring an NTP Time Source
- Configuring the System Companding Law
- Configuring the System Date and Time
- Configuring Quality of Experience (QoE) Settings
- Partial Configuration Imports
- Importing and Exporting Transformation Tables

Working with Microsoft Unified Communications

- OCS 2007 Setup
- Lync Setup

Working with the ASM and SBA

- Managing the ASM
- Applying an SBA Security Template
- Managing the Lync SBA
- Managing the SBC Communication Service

Working with Media

- Configuring the Media System
- Managing Media Profiles
- Managing Media Crypto Profiles
- Managing Media Lists

Working with Tones

- Creating and Modifying Tone Tables

Working with SNMP and Alarms

- Configuring Alarms and Events
- Managing SNMP Management Addresses
- Configuring Sonus SBC 1000-2000 for SNMP Management
- SNMP MIBs Reference

Working with Logging

- Managing Remote Log Servers
- Managing Subsystems Logging
- Managing Local Logs
- Supported Logging Levels

Copyright © 2015 Sonus Networks. All rights reserved.

- Working with Port Mirroring

Working with Ethernet Interfaces and IP

- Managing Logical Interfaces
- Managing Static IP Route Tables
- Managing Static ARP Tables
- Modifying the Sonus SBC 1000-2000 IP Address
- How the Sonus SBC 1000-2000 Routes IP Traffic to a NIC
- Managing the Hosts Table
- Managing VLANs

Working with System Software

- One-Step Upgrade
- Managing Application Partitions
- Managing the Boot Partition

Working with Call Detail Records

- Call Detail Records Primer
- Configuring the Sonus SBC 1000-2000 for CDR
- Retreiving Call Detail Records From a RADIUS Server
- Vendor Specific Attributes Reference
- Viewing Call Detail Record Statistics

Working with the Web Interface

- Logging in to Sonus SBC 1000-2000
- Managing Login Messages
- Monitoring Real Time Status
- Viewing Alarms and Events

Working with ISDN

- Managing ISDN Signaling Groups

Working with SCOM

- SBC SCOM Object Model and Health Monitoring

Working with Enhanced 911 Devices

- Configuring Emergency Services
- Managing Callback Number Pools
- Viewing Emergency Calls

Working with Dynamic Routing

- Managing Router Instances

Working with Access Control Lists and Session Control

- Managing Access Control Lists

Working with Network Services

- Managing the DHCP Server
- Managing the DHCP Client

Copyright © 2015 Sonus Networks. All rights reserved.

SIP Message Manipulation

- Managing Condition Rule Tables
- Managing Message Rule Tables
- Using the Condition Expression Builder
- Managing Call Admission Control Profile
- Export/Import SIP Message Rule
- Exporting and Importing SIP Message Rules

Miscellaneous Topics

- Resequencing Tables
- The Multiselect Widget

Working with IPsec

- Managing IPsec Tunnels
- Configuring a Site to Site IPsec between the SBC Gateways
- Viewing IPsec Statistics

Working with NAT and Port Forwarding

- Managing NAT Interface Tables
- Managing Port Forwarding Tables

Working with Branch Survivability

- Configuring 3G4G Failover
- Managing Link Monitor Configuration Tables
- Managing Lync CAC Profiles

Working with Historical Data and TCA Thresholds

- Managing TCA Thresholds

Working with Multiple Spanning Trees

- Managing MST Instances
- Modifying Region Settings

About Signaling Groups

Working with RTP Proxies

- Video

Working With Security

Getting to Know the Sonus SBC 1000-2000

This section describes covers hardware related topics of the Sonus SBC 1000/2000 platform including the controls and status indicators.

Sonus SBC 1000-2000 Status LEDs

Sonus SBC 1000-2000 System Hardware

- Sonus SBC 2000 Hardware Specifications
    - Sonus SBC 2000 Front Panel

Copyright © 2015 Sonus Networks. All rights reserved.

    - Sonus SBC 2000 Rear Panel
    - Sonus SBC 2000 Interface Cards
- Sonus SBC 1000 Hardware Specifications
    - Sonus SBC 1000 Front Panel
    - Sonus SBC 1000 Rear Panel
- Safety Precautions
    - Electrostatic Discharge (ESD) Precautions
- Compliance and Regulatory Information
    - Electromagnetic Compatibility Information
    - Product Disposal
    - Sonus SBC 1000 and NET UX1000 Declaration of Conformity
    - Sonus SBC 2000 and NET UX2000 Declaration of Conformity
    - Sonus SBC 1000 FCC and Industry Canada Compliance Statements
    - Sonus SBC 2000 FCC and Industry Canada Compliance Statements
- Hardware Expansion Modules
    - Digital Signal Processing (DSP) Modules
    - Sonus SBC 1000 BRI Card
    - Sonus SBC 1000 FXO Cards
    - Sonus SBC 1000 FXS Cards
- Sonus SBC 1000-2000 System Power Supplies
- Reconfiguring Sonus SBC 1000-2000 Ports

Notes and Limitations

Sonus SBC 1000-2000 System Performance and Capacity

Sonus SBC 1000-2000 Status LEDs

- Status Panel LEDs
- Ethernet Port Status LEDs

Status Panel LEDs

This section describes the Status LEDs located on the front panel of the Sonus SBC 1000/2000 chassis. Overall, when all four Status LEDs are lit green, the system is powered up and is in good operating condition. See below for individual LED ranges. For more information about the error states of these LEDs, see Status Panel States and Actions.



1. Power Status LED

Copyright © 2015 Sonus Networks. All rights reserved.

This status LED indicates the power conditions of the Sonus SBC 1000/2000 system. The normal state of this LED is on and green.

Color	Status
Green	System is connected to proper power source.
Off	System is not connected to power source.

2. Alarms Status LED

This status LED indicates the alarm state of the Sonus SBC 1000/2000 system. The normal state of this LED is green, indicating there is no alarm.

For detailed information about alarm types, see Alarms and Events Reference.

Color	Status
Green	No alarm.
Off	Warning (indicates the lowest severity level of an alarm has occurred).
Amber	Minor alarm.
Red	Major alarm.
Red Blinking	Critical alarm.

3. Peer Node Status LED (Locator LED)

> ☑ The **Peer Node Status** LED is also recognized as the Locator LED when configuring this option in the WEB GUI.

This status LED is green when the Sonus SBC 1000/2000 system is fully powered up. It is also used as a system locator LED for the SBC unit (the green blinking light helps network personnel easily locate the SBC in a rack with other equipment). Through the WEBUI, this LED can be turned off or made to blink once per second. See Configuring Host Information and DNS.

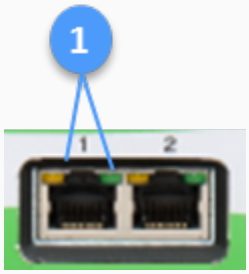
Color	Status
Green	System is fully powered up.
Off	**User Enabled option.** LED is turned off through the LED Locator configuration option. See Configuring Host Information and DNS.
Blinking Green	**User Enabled option.** LED is turned to blinking green through the LED Locator configuration option. Light will blink once per second. See Configuring Host Information and DNS.

4. Ready Status LED

Copyright © 2015 Sonus Networks. All rights reserved.

This status LED indicates if the Sonus SBC 1000/2000 system is properly initialized. The normal state of this LED is on and green.

Color	Status
Green	System is properly initialized.
Off	System is not properly initialized.



Ethernet Port Status LEDs

This section describes the Ethernet Port Status LEDs located in the right and left corners of the Ethernet ports. See below for LED ranges.

Copyright © 2015 Sonus Networks. All rights reserved.

1. Ethernet Port Status LED

> ✅ The Ethernet LEDs displayed represent a Sonus SBC 1000; the Ethernet LEDs function the same for the Sonus SBC 2000.

This Ethernet Port Status LEDs indicate the status conditions of the Ethernet ports on the Sonus SBC 1000/2000 system.

Left-Side LED

Color	Status
Amber	Indicates Ethernet port speed at 10/100Mbps.
Off	Indicates Ethernet port speed at 1000Mbps.

Right-Side LED

Color	Status
Green	Ethernet link is established.
Flashing Green	Ethernet link is active. Data is being sent/received.
Off	Ethernet link is down.

Right/Left LED Combinations

Left-Side Color	Right-Side Color	Result
Amber	Off	Port speed is 10Mbpbs. Ethernet link is down.
Amber	Green	Port speed is 100Mbps. Ethernet link is established.
Off	Green	Port speed is 1000Mbps. Ethernet link is established.

Sonus SBC 1000-2000 System Hardware

This section contains physical and electrical specifications for the chassis and expansion modules, safety information, and compliance and regulatory information.

Sonus SBC 2000 Hardware Specifications

- Sonus SBC 2000 Front Panel
- Sonus SBC 2000 Rear Panel
- Sonus SBC 2000 Interface Cards
  - Inserting and Removing Interface Cards
  - Sonus SBC 2000 FXS Card
  - T1-E1 PSTN Interface Cards

Sonus SBC 1000 Hardware Specifications

- Sonus SBC 1000 Front Panel
- Sonus SBC 1000 Rear Panel

Safety Precautions

- Electrostatic Discharge (ESD) Precautions

Copyright © 2015 Sonus Networks. All rights reserved.

Compliance and Regulatory Information

- Electromagnetic Compatibility Information
- Product Disposal
- Sonus SBC 1000 and NET UX1000 Declaration of Conformity
- Sonus SBC 2000 and NET UX2000 Declaration of Conformity
- Sonus SBC 1000 FCC and Industry Canada Compliance Statements
- Sonus SBC 2000 FCC and Industry Canada Compliance Statements

Hardware Expansion Modules

- Digital Signal Processing (DSP) Modules
- Sonus SBC 1000 BRI Card
- Sonus SBC 1000 FXO Cards
- Sonus SBC 1000 FXS Cards

Sonus SBC 1000-2000 System Power Supplies

Reconfiguring Sonus SBC 1000-2000 Ports

Sonus SBC 2000 Hardware Specifications

This section describes the dimensional, environmental, power, and network specifications and requirements for the Sonus SBC 2000 System.

Dimensions and Weight

Equipment	Height mm/in.	Width mm/in.	Depth mm/in.	Weight lb./kg
Chassis with no interface cards or expansion modules	(1RU) - 44 mm / 1.75 in.	444 mm / 17.5 in.	534 mm / 21 in.	16.5 lbs / 7.48 kgs
Maximum supported configuration	(1RU) - 44 mm / 1.75 in.	444 mm / 17.5 in.	534 mm / 21 in.	23 lbs / 10.43 kgs

Environmental Ranges (Operation and Storage)

Environmental Parameter	Specification
Operating Environmental Conditions	Temperature: 5º to 40º Celsius Humidity: 5% to 85% RH non-condensing Altitude: 60 meters below sea level to 1800 meters above sea level
Storage Environmental Condition	Temperature: -40º to 70º Celsius
Cooling System	Internal forced convection

Power Supply

The Sonus SBC 2000 system comes equipped with either a single power supply, or dual redundant power supplies which comply with the following specifications:

Copyright © 2015 Sonus Networks. All rights reserved.

Item	Specification
Input Voltage	AC: 100-240 VAC Nominal, Auto-switching, 47-63 Hz
AC Maximum Input Current	5A at 115VAC and 2.5A at 230VAC
AC Input Voltage Range (nominal)	100-127VAC and 200-240VAC
Output	300 W-AC: +5V/20A, +12V/24A, -12V/0.6A, +3.3V/20A, +5VSB/3A
Max Power Consumption	300 watts

Sonus SBC 1000/2000 power supplies are tested and certified to meet UL / cUL / IEC 60950-1 safety requirements.

The Sonus SBC 1000/2000 power supplies must be replaced with Sonus-provided units only.

The SBC 2000 power supplies, if equipped with dual supplies, are hot swappable. Note that this only applies to the SBC 2000 and only when two power supplies are installed in the redundant mode.

For more information about the Sonus SBC 1000/2000 power supply units, see Sonus SBC 1000-2000 System Power Supplies.

Networking Interfaces

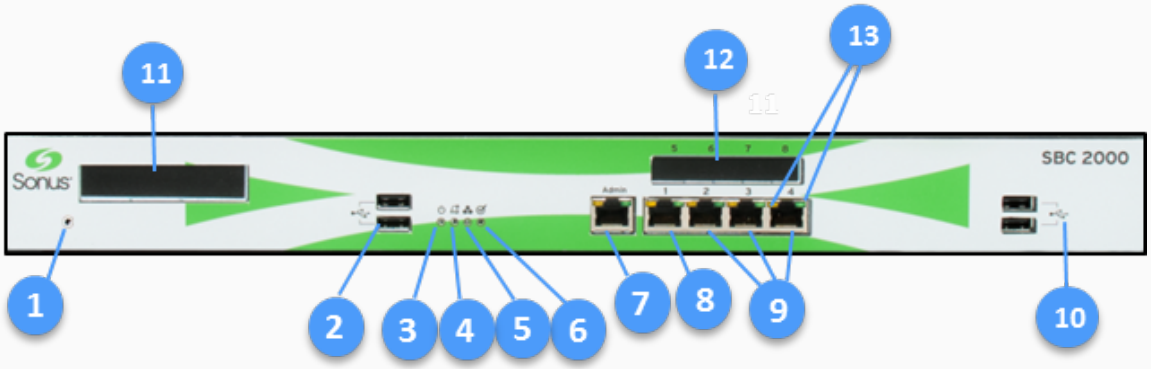
The Sonus SBC 2000 base configuration includes 5 Ethernet ports on the front panel of the unit.

- 1 x 10/100/1000 Base-T administration port (used for initial setup)
- 4 x 10/100/1000 Base-T ports

- Sonus SBC 2000 Front Panel
- Sonus SBC 2000 Rear Panel
- Sonus SBC 2000 Interface Cards

Sonus SBC 2000 Front Panel

Copyright © 2015 Sonus Networks. All rights reserved.



#	Name	Description
1	**Reset**	System reset button. For more information, see Resetting the Sonus SBC 1000-2000 to Factory Defaults.
2	**USB Ports**	USB ports for Sonus SBC 1000/2000 main board
3	**Power**	Power Status LED
4	**Alarm**	Alarm Status LED
5	**Peer Node**	Peer Node Status LED (also recognized as the Locator LED)
6	**Ready**	Ready Status LED
7	**Admin Port**	System Administration Ethernet Port – **do not connect to your live network - see warning below**
8	**Port 1**	Primary Application Ethernet Port 1
9	**Ports 2 - 4**	Ethernet Ports 2 - 4
10	**USB Ports**	USB ports for the Application Service Module (ASM) (when installed)
11	**Expansion Bay**	Future expansion bay
12	**Expansion Bay**	Networking expansion bay
13	**Ethernet Port Status**	Ethernet Status LED

Warnings

Admin Port

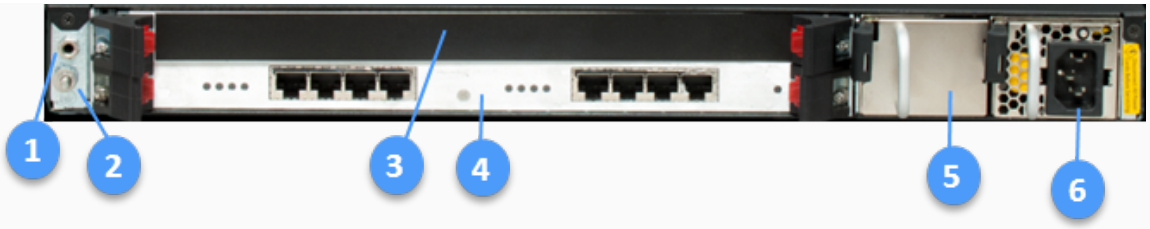
Copyright © 2015 Sonus Networks. All rights reserved.

The Administrative IP port should only be used for Running Initial Setup and disconnected when not in use (especially to avoid conflicts with your network). This interface **cannot be used for VOIP media or protocols**.

Application Ethernet Ports

When two or more LAN Ethernet ports are on the same Bridge (as in the factory-default Sonus SBC 1000/2000 configuration), **they must not be connected to the same Ethernet switch or Ethernet network**. Doing so creates a broadcast loop in the Ethernet network, rendering the network unusable. You may work around this issue by connecting the Ethernet ports directly to an intelligent switch or router running a *spanning tree* protocol.

Sonus SBC 2000 Rear Panel



#	Name	Description / Notes
1	**ESD Plug**	Grounding plug for Electro Static Discharge (ESD) protection wrist strap
2	**Ground Bolt**	Grounding bolt for chassis grounding
3	**Slot 2**	Slot 2 for Sonus SBC 2000 Interface Cards
4	**Slot 1**	Slot 1 for Sonus SBC 2000 Interface Cards
5	**Left Power Supply Bay**	Slot for hot-swappable power supply
6	**Right Power Supply Bay**	Slot for hot-swappable power supply

Sonus SBC 2000 Interface Cards

The Sonus SBC 2000 system allows for the use of interface cards – sometimes referred to as a line card or carrier card – for connecting to specific call equipment or carrier lines. This section describes the available interface cards for the Sonus SBC 2000 system.

- Inserting and Removing Interface Cards
- Sonus SBC 2000 FXS Card
- T1-E1 PSTN Interface Cards

Inserting and Removing Interface Cards

This section describes the steps for inserting and removing Interface Cards from the rear of the Sonus SBC 1000/2000 chassis.

Copyright © 2015 Sonus Networks. All rights reserved.

Review and follow the Sonus SBC 1000/2000 Safety Precautions before performing any service on the Sonus SBC 1000/2000 system.

- Removing an Interface Card
- Inserting an Interface Card

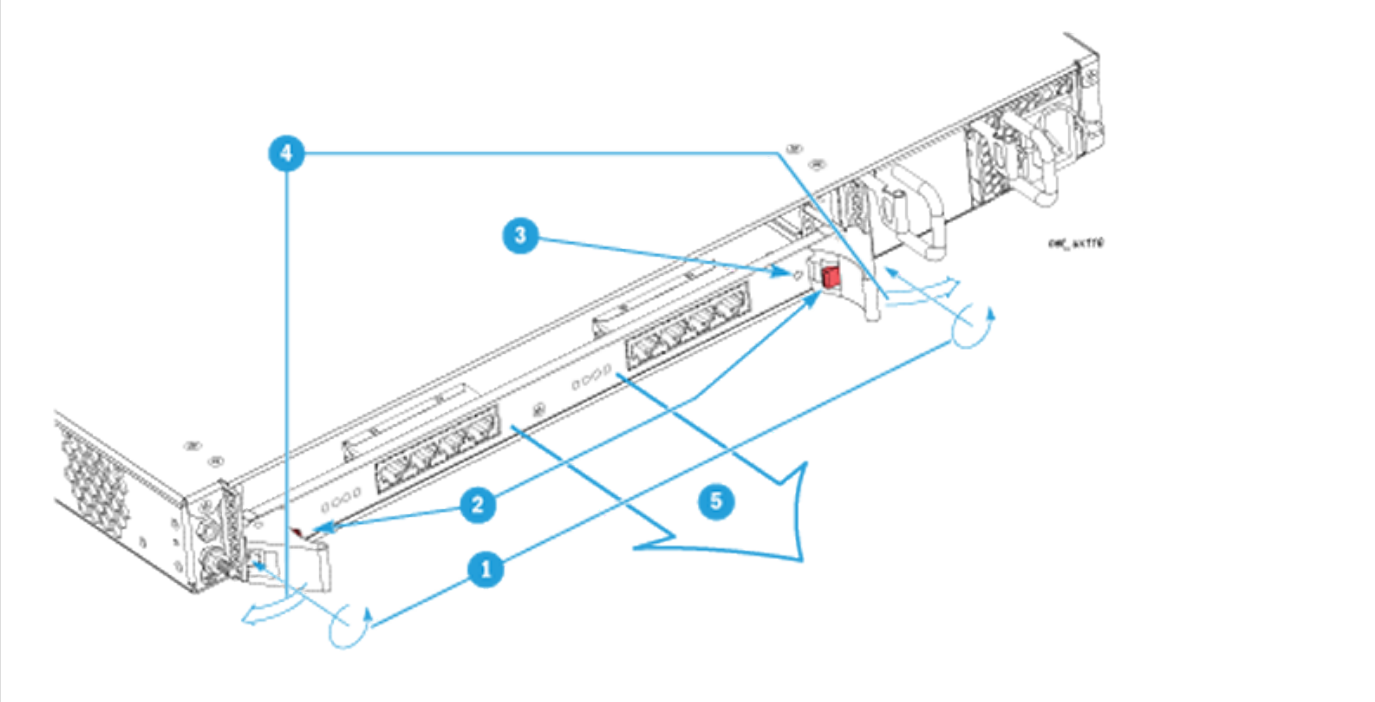
Removing an Interface Card

To Remove an Interface Card

1. Power down the Sonus SBC 1000/2000.

   You must power down the Sonus SBC 1000/2000 system before installing or removing Interface Cards. Hot swapping of Interface Cards is not supported in **Sonus SBC 1000/2000 4.1.x** .

2. Loosen the screws on the right and left side of the interface card until they spin freely.
3. Depress the red buttons on the inside of the attachment levers until they click and lock into place. The Hot Swap status LED should now be lit.
4. Grip the inside of the attachment levers and push toward the outside edges of the card.
5. Carefully pull the card free of the chassis.



Inserting an Interface Card

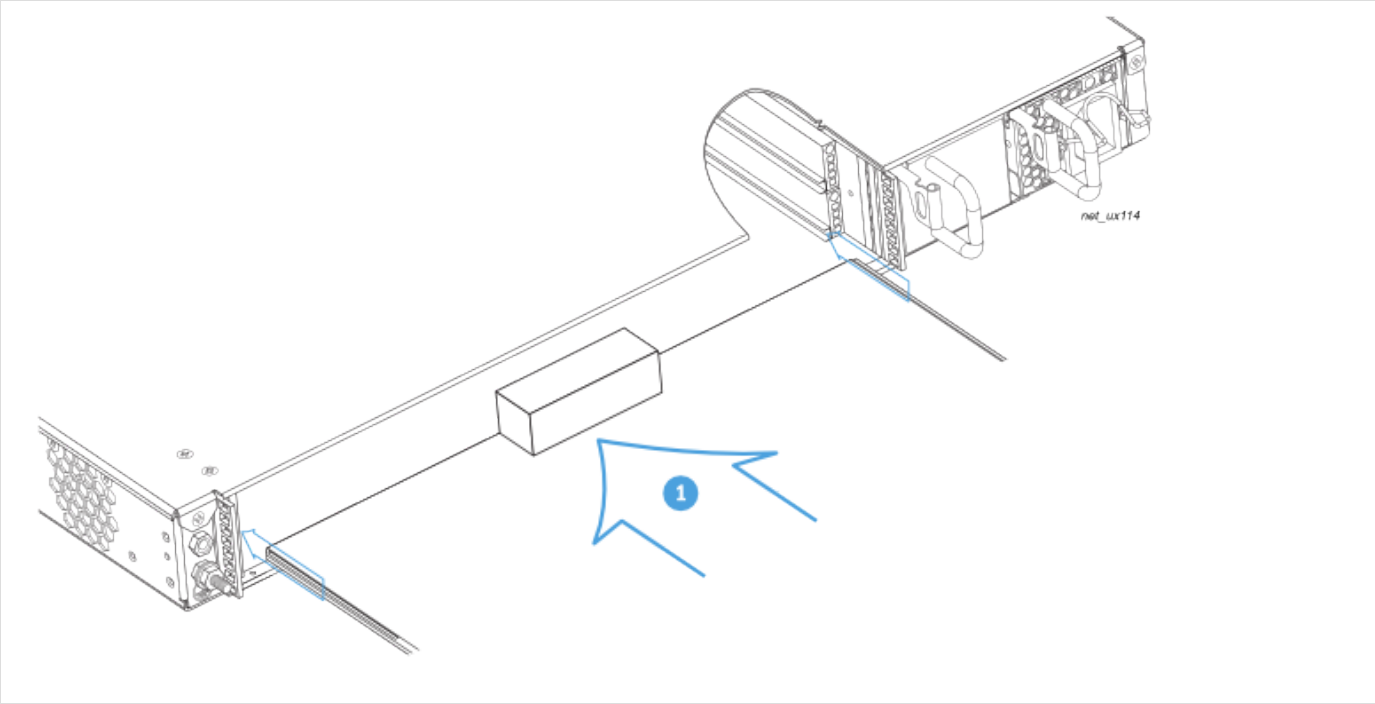
You must power down the Sonus SBC 1000/2000 system before installing or removing Interface Cards. Hot swapping of Interface Cards is not supported in **Sonus SBC 1000/2000 4.1.x** .

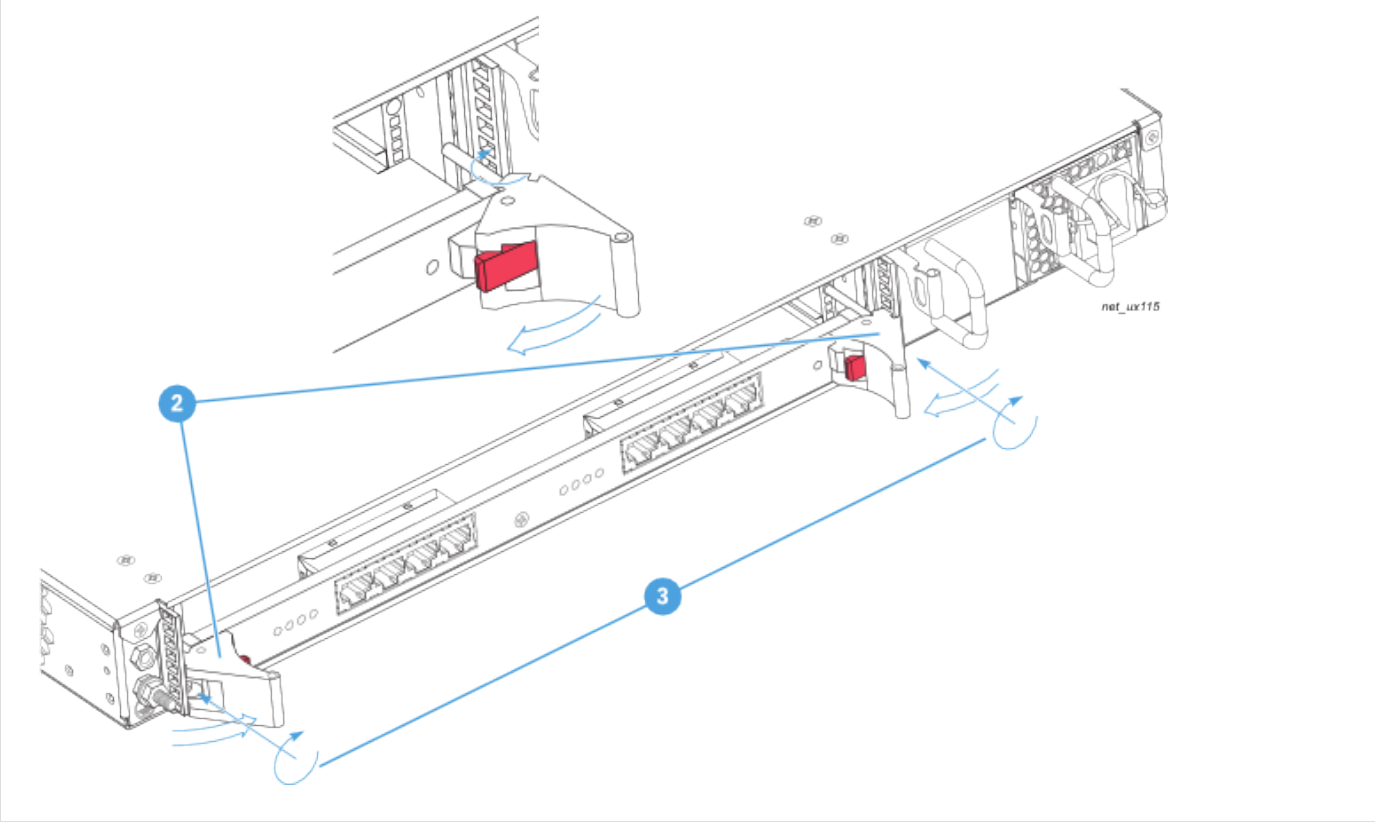
To Insert an Interface Card

1. Carefully insert the card so that the left and right edges slide into the mounting slots.
2. Grip the outside of the attachment levers and push toward the inside of the card until the card locks into place.

   The red buttons click and pop out when the card is properly locked into place.
3. Tighten the screws on the right and left side of the interface card.

Copyright © 2015 Sonus Networks. All rights reserved.





Sonus SBC 2000 FXS Card

Copyright © 2015 Sonus Networks. All rights reserved.



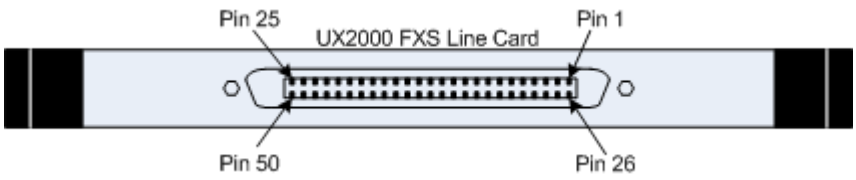
Overview

The Sonus SBC 2000 FXS Interface Card comprises 24 FXS interfaces on a single RJ-21 connector. The Sonus SBC 2000 supports up to a maximum of 48 FXS ports using two FXS Interface Cards.

Interface Specifications and Limitations

Item	Value/Dimension
Maximum external Off-Hook resistance	600 ohms (This includes the resistance of the cable and the DC resistance of the termination device)
Typical Loop Current Limit	23 ma/port
Typical FXS Port Ringing Voltage	45V RMS with 3 REN load
Max. Loop Length	1000m

RJ-21 Connector Pinouts



RJ-21 connector pinout:

Copyright © 2015 Sonus Networks. All rights reserved.

Port Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	2
TIP	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	2
RING	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	4

The last pair of the RJ-21 connector (pins 25 and 50) are routed to an isolated contact to be used for a future feature.

Installation and Service

The Sonus SBC 2000 FXS Interface card have no user serviceable components. Installation and removal of of the Sonus SBC 2000 FXS Interface Card from the chassis should only be performed by qualified service personnel.

T1-E1 PSTN Interface Cards

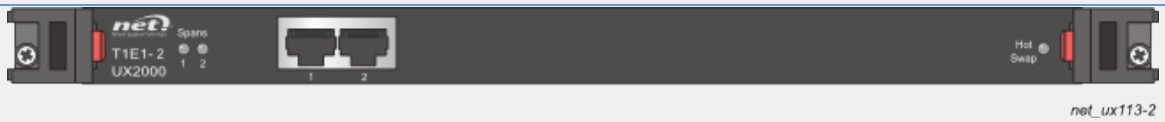
The T1/E1 PSTN Interface card is a TNV1 compliant digital interface card with integrated Channel Service Unit (CSU) function for direct connection to outside plant wiring. This card has board-mounted protection circuits for electrical isolation and protection against power crossing, lightning surges and hazardous voltages.

- Card Port Versions
- Port Status LEDs
- Hot Swap Status LED
- T1/E1 Port Pinouts

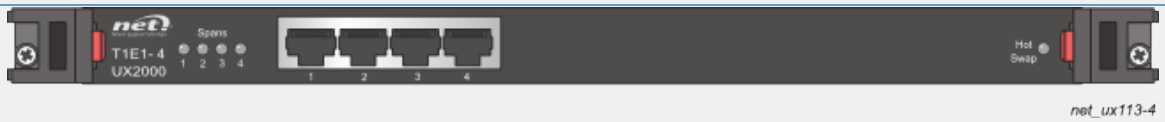
Card Port Versions

The T1/E1 PSTN Interface card comes in 2, 4 or 8 T1/E1 ports. All T1/E1 ports on the card have identical electrical circuit design.

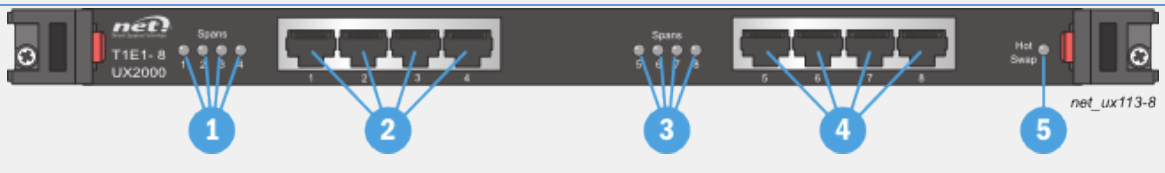
T1/E1 2-Port Card



T1/E1 4-Port Card



T1/E1 8-Port Card



Copyright © 2015 Sonus Networks. All rights reserved.

#	Name	Description
1	Port 1-4 Status	Displays the #status of ports 1 through 4.
2	Ports 1-4	Physical ISDN ports 1 through 4.
3	Port 5-8 Status	Displays the #status of ports 5 through 8.
4	Ports 5-8	Physical ISDN ports 5 through 8.
5	Hot Swap	Displays Hot Swap status of the interface card. **You must power down the Sonus SBC 1000/2000 system before installing or removing Interface Cards.** Hot swapping of Interface Cards is not supported in **Sonus SBC 1000/2000 4.1.x** . For more information on inserting and removing interface cards, see Inserting and Removing Interface Cards.

Port Status LEDs

Each T1/E1 port on the T1/E1 PSTN Interface card has an LED to indicate its operational status. The status states are described below:

Color	Status	Description
Off	No Signal	Indicates the port is not connected or connected cable is not providing a signal. Connect a cable or check the far-end connection.
Green	Link Up	Indicates the port is operating normally.
Red	LOF	Indicates the port has a Loss Of Framing (LOF) error. A cable is connected, but Sonus SBC 1000/2000 can not detect a correct T1 or E1 frame.
Amber	Yellow	Indicates there is a problem with the far-end connection. This status is usually communicated from remote side and indicates the Sonus SBC 1000/2000 receiver is synced up, but there is a problem at the remote side receiver.

Hot Swap Status LED

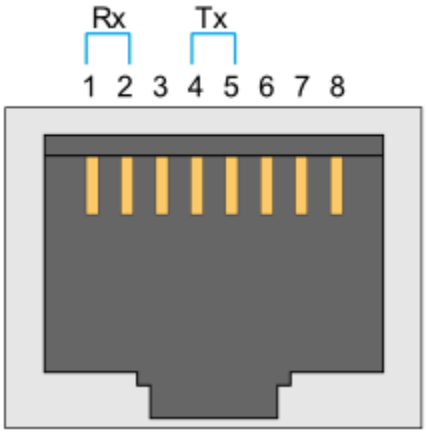
You must power down the Sonus SBC 1000/2000 system before installing or removing Interface Cards. Hot swapping of Interface Cards is not supported in **Sonus SBC 1000/2000 4.1.x** .

For more information about properly removing an Interface Card, see Inserting and Removing Interface Cards.

Copyright © 2015 Sonus Networks. All rights reserved.

T1/E1 Port Pinouts

The T1/E1 ports are connected to the public network using 4-wire shielded 26 AWG or larger twisted pair telecommunication line cords with RJ-48 connectors.



Sonus SBC 1000 Hardware Specifications

This section describes the dimensional, environmental, power, and network specifications and requirements for the Sonus SBC 2000 System.

Dimensions and Weight

Equipment	Height mm/in.	Width mm/in.	Depth mm/in.	Weight lb./kg
Chassis with no interface cards or expansion modules	42.00 / 1.65	441.60 / 17.38	299.00 / 11.77	8.50 / 3.85
Maximum supported configuration	(1RU) - 44 mm / 1.75 in	444 mm / 17.5 in.	305 mm / 12 in.	5.67 kgs / 12.5 lbs

Environmental Ranges (Operation and Storage)

Environmental Parameter	Specification
Operating Environmental Conditions	Temperature: 5º to 40º Celsius Humidity: 5% to 85% RH non-condensing Altitude: 60 meters below sea level to 1800 meters above sea level
Storage Environmental Condition	Temperature: -40º to 70º Celsius
Cooling System	Internal forced convection

Power Supply

For more information about the Sonus SBC 1000/2000 power supply units, see Sonus SBC 1000-2000 System Power Supplies.

Copyright © 2015 Sonus Networks. All rights reserved.

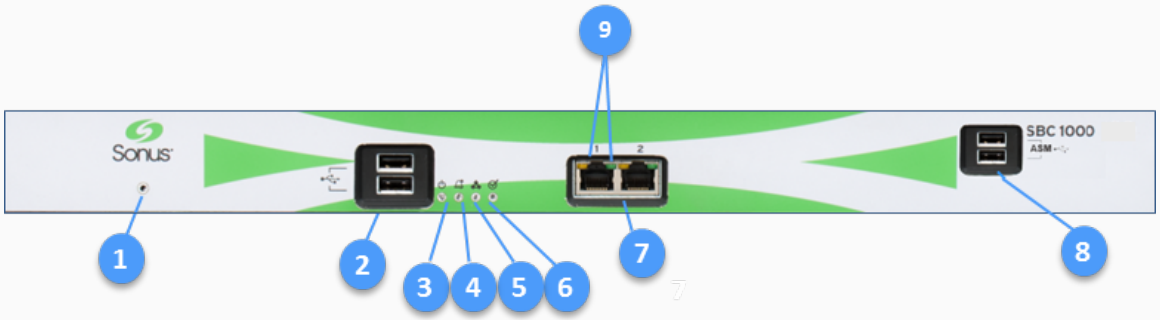
Networking Interfaces

The Sonus SBC 1000 base configuration includes 2 Ethernet ports on the front panel of the unit, or 4 Ethernet ports if the ASM is installed.

- 2 X 10/100/1000 Base-T ports (max).

- Sonus SBC 1000 Front Panel
- Sonus SBC 1000 Rear Panel

Sonus SBC 1000 Front Panel



#	Name	Description
1	**Reset**	System reset button. For more information, see Resetting the Sonus SBC 1000-2000 to Factory Defaults.
2	**USB Ports**	USB ports for Sonus SBC 1000/2000 main board — see USB Ports detail section below
3	**Power**	Power Status LED
4	**Alarm**	Alarm Status LED
5	**Peer Node**	Peer Node Status LED (also recognized as the Locator LED)
6	**Ready**	Ready Status LED
7	**Port 1 - 2**	Ethernet Ports 1 and 2
8	**USB Ports**	USB ports for the Application Service Module (ASM) (when installed)
9	**Ethernet Port Status**	Ethernet Status LED

USB Ports

Usage

Copyright © 2015 Sonus Networks. All rights reserved.

The Sonus SBC 1000 sports two pairs of USB ports (as illustrated above) — each pair serves a particular purpose:

Location	USB Port Intent and Usage Detail
2	These ports are optionally used to attach an external USB drive to store core dumps for troubleshooting (in the event they occur), and as a survivability mechanism for Active Directory Caching (when configured). See Support section below for proper usage.
8	If your Sonus SBC 1000 has a built-in Application Service Module (ASM), this USB port is primarily used for Updating the ASM Recovery Partition, and to (optionally) transfer files between a USB drive and the ASM.

Support

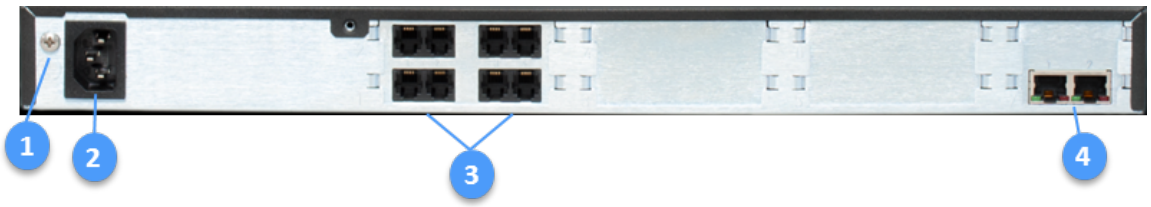
⚠ The following section is applicable only to the USB ports on **location #2** on the Sonus SBC 1000's front panel.

For the Sonus SBC 1000/2000 system to properly recognize the USB thumb drive, you must ensure the following prerequisites are satisfied:

- The USB storage must be of **FAT32 file format**.
- The storage must be at least 1GB (or more) in size.
- The SBC does not require a reboot after the USB drive is installed.

Sonus SBC 1000 Rear Panel

This page describes the rear panel and connectors on the Sonus SBC 1000



#	Name	Description/Notes
1	**Grounding Screw**	Grounding screw Electrostatic Discharge (ESD) protection and Chassis Ground
2	**AC Input**	Connector for the power supply
3	**Analog Telephony Ports**	FXS, FXO, or BRI in various combinations. (FXO only supported in version 2.0) ℹ Depending on your specific Sonus SBC 1000/2000 configuration, some of the ports shown here may not be in your system
4	**DS1 Ports**	T1/E1 Ports

Safety Precautions

Copyright © 2015 Sonus Networks. All rights reserved.

This section provides Sonus SBC 1000/2000 safety precautions and information on how to avoid potentially hazardous electrical situations, in the following topics:

- AC Power
- Electrical
  - Electrostatic Discharge (ESD) Precautions

AC Power

The following information provides safety precautions to follow when using this equipment.

Always disconnect the power source to the system when work is done on or around the power supplies. Be sure you have a full understanding of high powered electronics components before servicing these components. Failure to follow this guideline could result in personal injury, death, or damage to the equipment, or loss of data.

Sonus SBC 1000/2000 equipment must be installed and maintained by qualified service personnel only.

Ensure that all breakers are off before performing service on this equipment.

Sonus SBC 1000/2000 equipment must be grounded. 

To protect against fire hazard replace fuses with the same type and rating as originally installed.

Electrical

Make sure that the correct power supply switch setting is selected. Failure to properly provide the correct power supply switch set may result in damage to the equipment when power is applied.

Multi Power Sources Disconnect Warning Instruction

Disconnect all power supply cords before servicing.

Lithium Battery Warning Instruction

There is a risk of explosion if the battery is replaced by a battery of an incorrect type. Dispose of used batteries according to the instructions.

Electrostatic Discharge (ESD) Precautions

Electrostatic Discharge (ESD) Precautions

To reduce the risk of equipment damage, the Sonus SBC 1000/2000 system should be kept in an electrostatic discharge (ESD) protected environment. The unit should be properly grounded at all times. The Sonus SBC 1000/2000 chassis should be plugged in and its grounding lug should be connected. When performing routine maintenance on the unit, a wrist strap should be plugged into the ESD jack located on the rear of the chassis.

Prevention of ESD Damage

Copyright © 2015 Sonus Networks. All rights reserved.

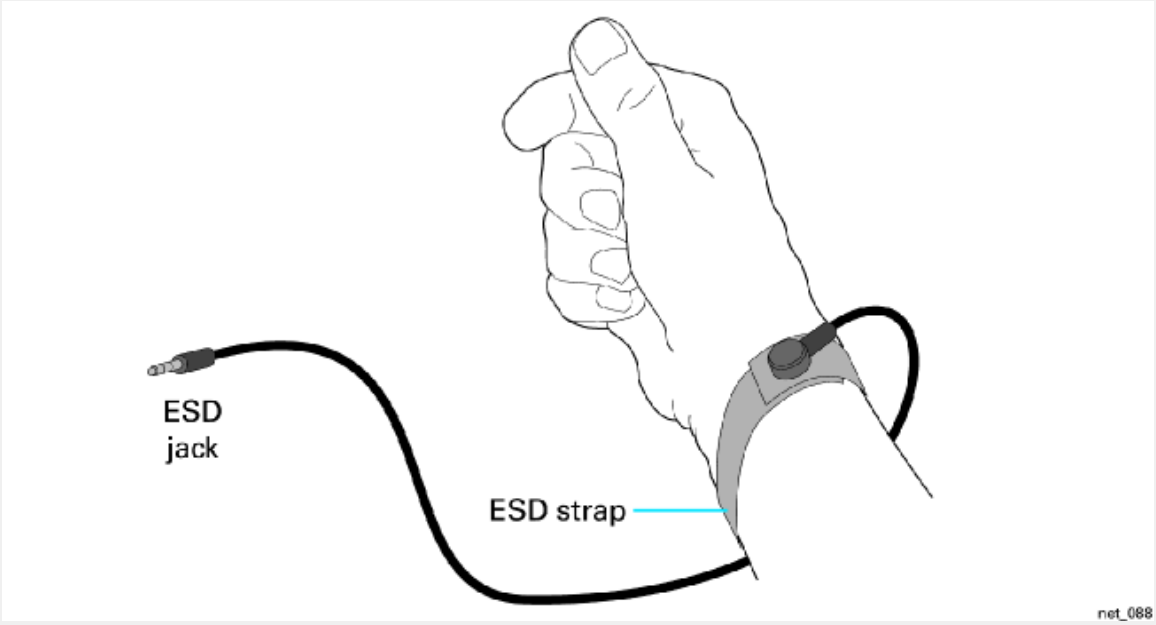
To prevent ESD damage observe the following precautions:

- Wear an ESD grounding strap connected to a proper ground when handling modules.
- Keep boards in their antistatic protection bags until you are ready to install them.
- Do not touch pins, leads, or solder connections on the boards.
- Handle modules only by their edges, ejector handles, or stiffener rails.
- Store and ship modules in antistatic protection packaging.

ESD Ground Connection

Sonus SBC 1000/2000 Series equipment provide an ESD ground connection in the form of a grounding plug for installation and removal of user-serviceable components. Use an ESD wrist strap attached to the grounding plug located on the rear of your Sonus SBC 1000/2000 unit.

ESD Ground Connection Wrist Strap



Sonus SBC 2000 ESD Connection

For information about where to plug in the ESD grounding device at the chassis, see Sonus SBC 2000 Hardware Specifications.

The ESD wrist strap must be attached to the grounding plug located on the rear of your Sonus SBC 1000/2000 unit. The figure below illustrates the location of the ESD grounding plug.

Location of the ESD Plug on the Sonus SBC 2000 Chassis Rear Panel



Sonus SBC 1000 ESD Connection

Copyright © 2015 Sonus Networks. All rights reserved.

The Sonus SBC 1000 does not have a dedicated receptacle for grounding straps, you must connect the strap to the grounding post.

Location of the Grounding Screw on the Sonus SBC 1000 Chassis Rear Panel



Compliance and Regulatory Information

This section provides various compliance and regulatory information related to the safety and operation of the Sonus SBC 1000/2000 product.

- Electromagnetic Compatibility Information
- Product Disposal
- Sonus SBC 1000 and NET UX1000 Declaration of Conformity
- Sonus SBC 2000 and NET UX2000 Declaration of Conformity
- Sonus SBC 1000 FCC and Industry Canada Compliance Statements
- Sonus SBC 2000 FCC and Industry Canada Compliance Statements

Electromagnetic Compatibility Information

Product Emission Class

> The Sonus SBC 1000/2000 system is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Emission Class Levels

Various national agencies (in the United States, the Federal Communications Commission (FCC)) govern the levels of electromagnetic emissions from digital devices. Electromagnetic emissions can interfere with radio and television transmission. To reduce the risk of harmful interference these agencies have established requirements for manufacturers of digital devices.

The manufacturer of a digital device must test and label a product to inform an end-user of the maximum emission level from the product when used in accordance with its instructions. The emissions levels encountered are classified as Class A or Class B. A system that meets the Class A requirements can be marketed for use in an industrial or commercial area. A system that meets the more stringent Class B requirement can be marketed for use in a residential area in addition to an industrial or a commercial area.

The end user is generally held responsible for ensuring that the system is suitable for its environment as stated in the above paragraph, and bears the financial responsibility for correcting any harmful interference.

Modifications

Modifications or changes made to this device, and not approved by Sonus Networks, may void the authority granted by the FCC, or other such agency, to operate this equipment.

Federal Communications Commission Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15

Copyright © 2015 Sonus Networks. All rights reserved.

of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.This equipment generates, uses, and can create radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area can cause harmful interference in which case the user will be required to correct the interference at the user's expense.

Canadian Notice

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of Industry Canada.

Avis Canadien

Cet appareil numérique n'émet pas de bruits radioélectriques depassant les limites applicables aux appareils numériques de la Classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Product Disposal

Ensure that you use proper methods for disposal of any Sonus SBC 1000/2000 equipment. Your disposal methods should be conducted in accordance with all national laws and regulations.

- Ultimate disposal of this product should be handled according to all national laws and regulations.
- Dit produkt dient volgens alle landelijke wetten en voorschriften te worden afgedankt.
- Tämän tuotteen lopullisesta hävittämisestä tulee huolehtia kaikkia valtakunnallisia lakeja ja säännöksiä noudattaen.
- La mise au rebut définitive de ce produit doit être effectuée conformément à toutes les lois et réglementations en vigueur.
- Dieses Produkt muß den geltenden Gesetzen und Vorschriften entsprechend entsorgt werden.
- L'eliminazione finale di questo prodotto deve essere eseguita osservando le normative italiane vigenti in materia.
- Endelig disponering av dette produktet må skje i henhold til nasjonlae lover og forskrifter.
- A descartagem final deste produto deverá ser efectuada de acordo com os regulamentos e a legislacão nacional.
- El desecho final de este producto debe realizarse según todas las leyes y regulaciones nacionales.
- Slutlig kassering av denna produkt bör skötas i enlighet med landets alla lagar och föreskrifter.

Sonus SBC 1000 and NET UX1000 Declaration of Conformity

A Declaration of Conformity for this Sonus SBC 1000 (NET UX1000) product has been prepared and is on file at Sonus.

Copyright © 2015 Sonus Networks. All rights reserved.

Network Equipment Technologies
(A Subsidiary of Sonus Networks, Inc.)
6900 Paseo Padre Parkway
Fremont, CA 94555
U.S.A.
Tel. 510-713-7300

December 17, 2012

Declaration of Conformity

We,
Network Equipment Technologies, Inc.
(A subsidiary of Sonus Networks, Inc.)
6900 Paseo Padre Parkway
Fremont, CA94555
USA

Declare under our sole responsibility that the products
NET - UX1000 Unified Exchange.
Sonus - SBC 1000 Unified Exchange.

Where appropriate, are in conformity with the following harmonized standards.

Emissions: EN55022
EN61000–3-2
EN61000–3-3

Immunity: EN55024
EN61000–4-2
EN61000–4-3
EN61000–4-4
EN61000–4-5
EN61000–4-6
EN61000–4-11

Safety: IEC60950-1, 2nd Edition / Amendment 1.

Telecom: TBR3, TBR4, TBR21 and ETSI ES203021-2.

RoHS 2: EN50581:2012.

Following the provision of the EC Directives:

72/23/EEC and 2006/95/EC	–	**Low Voltage Directive**
89/336/EEC and 2004/108/EC	–	**EMC Directive**
1999/5/EC	–	**Radio Equipment & Telecom Terminal Equipment Directive**
2011/65/EU	–	**RoHS 2 Directive**

Authorized signatory



Lawrence J. Miller
Assistant General Counsel

Sonus SBC 2000 and NET UX2000 Declaration of Conformity

A Declaration of Conformity for this Sonus SBC 2000 (NET UX1000) product has been prepared and is on file at

Copyright © 2015 Sonus Networks. All rights reserved.

Network Equipment Technologies
(A Subsidiary of Sonus Networks, Inc.)
6900 Paseo Padre Parkway
Fremont, CA 94555
U.S.A.
Tel. 510-713-7300

December 10, 2012

Declaration of Conformity

We,
Network Equipment Technologies, Inc.
(A subsidiary of Sonus Networks, Inc.)
6900 Paseo Padre Parkway
Fremont, CA94555
USA

Declare under our sole responsibility that the products
NET – UX2000 Unified Exchange.
Sonus - SBC 2000 Unified Exchange.

Where appropriate, are in conformity with the following harmonized standards.

Emissions: EN55022
EN61000–3-2
EN61000–3-3

Immunity: EN55024
EN61000–4-2
EN61000–4-3
EN61000–4-4
EN61000–4-5
EN61000–4-6
EN61000–4-11

Safety: IEC60950-1, 2nd Edition / Amendment 1.

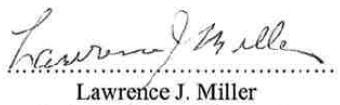
Telecom: TBR4, TBR12 and TBR13.

RoHS 2: EN50581:2012.

Following the provision of the EC Directives:

72/23/EEC and 2006/95/EC	–	**Low Voltage Directive**
89/336/EEC and 2004/108/EC	–	**EMC Directive**
1999/5/EC	–	**Radio Equipment & Telecom Terminal Equipment Directive**
2011/65/EU	–	**RoHS 2 Directive**

Authorized signatory



Lawrence J. Miller
Assistant General Counsel

Sonus.

Sonus SBC 1000 FCC and Industry Canada Compliance Statements

This section describes the requirements for compliance with Federal Communications Commission (FCC) Rules and Industry Canada CS-03 standard.

- FCC Registration and Requirements
  - Service
  - FCC Rules, Part 15
  - FCC Rules, Part 68

Copyright © 2015 Sonus Networks. All rights reserved.

- Industry Canada - Equipment Attachment Limitations
  - Statement of Compliance
  - Ringer Equivalence Number (REN)
  - EMC Compliance Statement

FCC Registration and Requirements

The following paragraphs describe the requirements and information based on FCC rules.

Service

If you experience problem with the Sonus - Sonus SBC 1000 Unified Exchange products, contact Sonus Technical Support Center at 1-800-800-4638 for information on service or repairs. The telephone company can ask you to disconnect the equipment from the network until the problem is corrected or until you are sure that the equipment is not malfunctioning.

FCC Rules, Part 15

The Sonus - Sonus SBC 1000 Unified Exchange has been tested and complies with the limits for a class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference in the user's expense.

FCC Rules, Part 68

1. **FCC Part 68 Registration**
   The Sonus SBC 1000 Unified Exchange complies with Part 68 of the FCC Rules and the requirements adopted by the Administrative Council of Terminal Attachments (ACTA). On the back of this equipment is a label that contains, among other information, the ACTA labeling identification numbers US:1BHISNANSonus SBC 1000 or US:1BHIS04BSonus SBC 1000. If requested, this information must be given to the telephone company.
2. **Ringer Equivalence Number (REN)**
   The ringer equivalence number (REN) is used to determine the quantity of devices which may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.
3. **Facility Interface Information**

   In order to connect registered terminal equipment to the telephone company lines, the terminal equipment must utilize FCC registered jacks. Standardized jacks are used for this equipment.
   The following tables list facility interfaces, manufacturer's network interface port designations, RENs or service order codes, and network jacks.
   This table lists the network trunk interfaces for digital services.

Manufacturer Port Identifier	Digital Interface Code (FIC)	Service Order Code (SOC)	Network Jack
T1/E1 PSTN	04DU9-BN	6.0P & 6.0Y	RJ48

Copyright © 2015 Sonus Networks. All rights reserved.

T1/E1 PSTN	04DU9-DN	6.0P & 6.0Y	RJ48
T1/E1 PSTN	04DU9-1KN	6.0P & 6.0Y	RJ48
T1/E1 PSTN	04DU9-1SN	6.0P & 6.0Y	RJ48

This table lists the network trunk interfaces for loop-start services.

Manufacturer Port Identifier	Digital Interface Code (FIC)	REN	Network Jack
FXO	02LS2	0.4B	RJ11

1. **Disruption of the Network**
   If the Sonus SBC 1000 Unified Exchange disrupts the telephone network, the telephone company can discontinue your service temporarily. If possible, the telephone company will notify you in advance. If advance notice is not practical, they will notify you as soon as possible. You are also informed of your right to file a complaint with the FCC.
2. **Telephone Company Facility Changes**
   The telephone company can make changes in its facilities, equipment, operations, or procedures that can affect the operation of your equipment. If they do, you should be notified in advance so you have an opportunity to maintain uninterrupted telephone service.
3. **Non-live Voice Equipment**
   Non-live voice equipment such as music-on-hold devices and recorded announcers for systems must be approved by and registered in accordance with the ACTA adapted ANSI/TIA-968-B standard, or it must be connected through protective circuitry that is approved by N.E.T. and registered in accordance with the ACTA adapted ANSI/TIA-968-B standard.
4. **Newly Established Network Area and Exchange Codes**
   The routing software features allowing user access to the network must recognize newly established network area codes and exchange codes as they are placed in service.

   Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established restricts the customers and the customer's employees from gaining access to the network and to these codes.
5. **Equipment with Direct Inward Dialing (DID)**
   Allowing the equipment to be operated in such a manner as to not provide for proper answer supervision is a violation of Part 68 of the FCC rules.
   Proper answer supervision is when:
   a. This equipment returns answer supervision to the PSTN when DID calls are:
      - Answered by the called station.
      - Answered by the attendant.
      - Routed to a recorded announcement that can be administered by the CPE user.
      - Routed to a dial prompt.
   b. This equipment returns answer supervision on all DID calls forwarded to the PSTN. Permissible exception are:
      - A call is unanswered.
      - A busy tone is received.
      - A reorder tone is received.

Copyright © 2015 Sonus Networks. All rights reserved.

6. **Hearing-Aid Compatibility**
   Telephones for emergency use and telephones installed in common areas such as lobbies, hospital rooms, elevators, and hotel rooms must have handsets that are compatible with magnetically coupled hearing aids. Persons who are not in common areas must also be provided with hearing-aid compatible handsets, if needed.

   FCC required hearing-aid compatible analog and digital telephones comply with the FCC Rules, Part 68, Section 68.316 and 68.317 for used with the Sonus SBC 1000 Unified Exchange.

1. **Programmed Dialer Features**
   When you program emergency numbers or make test calls to emergency numbers using N.E.T. products with programmed dialer features, stay on the line and briefly explain to the dispatcher the reason for the call before hanging up. Perform these activities in off-peak hours, such as early morning or late evening.
2. **Connecting Off-premises Station Facilities**
   Customers who intend to connect off-premises station (OPS) facilities must inform the telephone company of the OPS class for which the equipment is registered and the connection desired.
3. **Equal Access Requirements**
   Call aggregators such as hotels, hospitals, airports, and so on must provide the end-user equal access codes to the carriers of the user's choice. The most common equal access codes are 800, 888 or 950.

   The Sonus SBC 1000 Unified Exchange is capable of providing user access to interstate providers of operator services through the use of equal access codes. Modification by aggregators to alter these capabilities is a violation of the Telephone Operator Consumer Services Improvement Act of 1990 and Part 68 of the FCC Rules.
4. **Electrical Safety Advisory**
   While the Sonus SBC 1000 Unified Communications Exchange is fully compliant with the FCC rules and regulations, it is recommended that an alternating current (ac) surge arrestor of the form and capability suitable for the model purchased be installed in the ac outlet to which the Sonus SBC 1000 Unified Communications Exchange is connected. Consult with you distributor as to the surge protector requirements for your equipment.

Industry Canada - Equipment Attachment Limitations

The following notices are required by Industry Canada Terminal Attachment Program Procedure DC-01(E), Procedure for Declaration of Conformity and Registration of Terminal Equipment, Section 6.4 and ICES-003, Interference-Causing Equipment Standard for Digital Apparatus, Section 6.2.

Statement of Compliance

This product meets the applicable Industry Canada technical specifications.

Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

Ringer Equivalence Number (REN)

The Ringer Equivalence Number is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

Copyright © 2015 Sonus Networks. All rights reserved.

EMC Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Sonus SBC 2000 FCC and Industry Canada Compliance Statements

This section describes the requirements for compliance with Federal Communications Commission (FCC) Rules and Industry Canada CS-03 standard.

- FCC Registration and Requirements
  - Service
  - FCC Rules, Part 15
  - FCC Rules, Part 68
- Industry Canada - Equipment Attachment Limitations
  - Statement of Compliance
  - Ringer Equivalence Number (REN)
  - EMC Compliance Statement

FCC Registration and Requirements

The following paragraphs describe the requirements and information based on FCC rules.

Service

If you experience problem with the Sonus - Sonus SBC 2000 Unified Communications Exchange products, contact Sonus Technical Support Center at 1-800-800-4638 for information on service or repairs. The telephone company can ask you to disconnect the equipment from the network until the problem is corrected or until you are sure that the equipment is not malfunctioning.

FCC Rules, Part 15

The Sonus - Sonus SBC 2000 Unified Communications Exchange has been tested and complies with the limits for a class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference in the user's expense.

FCC Rules, Part 68

1. **FCC Part 68 Registration**
   The Sonus SBC 2000 Unified Communications Exchange complies with Part 68 of the FCC Rules and the requirements adopted by the Administrative Council of Terminal Attachments (ACTA). On the back of this equipment is a label that contains, among other information, the ACTA labeling identification number US:1BHISNANSonus SBC 2000 If requested, this information must be given to the telephone company.
2. **Ringer Equivalence Number (REN)**
   The ringer equivalence number (REN) is used to determine the quantity of devices which may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

Copyright © 2015 Sonus Networks. All rights reserved.

3. **Facility Interface Information**

   In order to connect registered terminal equipment to the telephone company lines, the terminal equipment must utilize FCC registered jacks. Standardized jacks are used for this equipment.

   The following tables list facility interfaces, manufacturer's network interface port designations, RENs or service codes, and network jacks.

   This table lists the network digital trunk interfaces for digital services.

Manufacturer Port Identifier	Digital Interface Code (FIC)	Service Order Code (SOC)	Network Jack
T1/E1 PSTN	04DU9-BN	6.0P & 6.0Y	RJ48
T1/E1 PSTN	04DU9-DN	6.0P & 6.0Y	RJ48
T1/E1 PSTN	04DU9-1KN	6.0P & 6.0Y	RJ48
T1/E1 PSTN	04DU9-1SN	6.0P & 6.0Y	RJ48

4. **Disruption of the Network**
   If the Sonus SBC 2000 Unified Communications Exchange disrupts the telephone network, the telephone company can discontinue your service temporarily. If possible, the telephone company will notify you in advance. If advance notice is not practical, they will notify you as soon as possible. You are also informed of your right to file a complaint with the FCC.
5. **Telephone Company Facility Changes**
   The telephone company can make changes in its facilities, equipment, operations, or procedures that can affect the operation of your equipment. If they do, you should be notified in advance so you have an opportunity to maintain uninterrupted telephone service.
6. **Non-live Voice Equipment**
   Non-live voice equipment such as music-on-hold devices and recorded announcers for systems must be approved by and registered in accordance with the ACTA adapted ANSI/TIA-968-B standard, or it must be connected through protective circuitry that is approved by N.E.T. and registered in accordance with the ACTA adapted ANSI/TIA-968-B standard.
7. **Newly Established Network Area and Exchange Codes**
   The routing software features allowing user access to the network must recognize newly established network area codes and exchange codes as they are placed in service.

   Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established restricts the customers and the customer's employees from gaining access to the network and to these codes.
8. **Equipment with Direct Inward Dialing (DID)**
   Allowing the equipment to be operated in such a manner as to not provide for proper answer supervision is a violation of Part 68 of the FCC rules.
   Proper answer supervision is when:
   a. This equipment returns answer supervision to the PSTN when DID calls are:
      - Answered by the called station.
      - Answered by the attendant.
      - Routed to a recorded announcement that can be administered by the CPE user.
      - Routed to a dial prompt.
   b. This equipment returns answer supervision on all DID calls forwarded to the PSTN. Permissible

Copyright © 2015 Sonus Networks. All rights reserved.

exception are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

9. **Hearing-Aid Compatibility**
   Telephones for emergency use and telephones installed in common areas such as lobbies, hospital rooms, elevators, and hotel rooms must have handsets that are compatible with magnetically coupled hearing aids. Persons who are not in common areas must also be provided with hearing-aid compatible handsets, if needed.

   FCC required hearing-aid compatible digital telephones comply with the FCC Rules, Part 68, Section 68.316 and 68.317 for used with the Sonus SBC 2000 Unified Communications Exchange.
10. **Programmed Dialer Features**
    When you program emergency numbers or make test calls to emergency numbers using N.E.T. products with programmed dialer features, stay on the line and briefly explain to the dispatcher the reason for the call before hanging up. Perform these activities in off-peak hours, such as early morning or late evening.
11. **Connecting Off-premises Station Facilities**
    Customers who intend to connect off-premises station (OPS) facilities must inform the telephone company of the OPS class for which the equipment is registered and the connection desired.
12. **Equal Access Requirements**
    Call aggregators such as hotels, hospitals, airports, and so on must provide the end-user equal access codes to the carriers of the user's choice. The current equal access codes are 10XXX, 800, 888 or 950.

    The Sonus SBC 2000 Unified Communications Exchange is capable of providing user access to interstate providers of operator services through the use of equal access codes. Modification by aggregators to alter these capabilities is a violation of the Telephone Operator Consumer Services Improvement Act of 1990 and Part 68 of the FCC Rules.
13. **Electrical Safety Advisory**
    While the Sonus SBC 2000 Unified Communications Exchange is fully compliant with the FCC rules and regulations, it is recommended that an alternating current (ac) surge arrestor of the form and capability suitable for the model purchased be installed in the ac outlet to which the Sonus SBC 2000 Unified Communications Exchange is connected. Consult with you distributor as to the surge protector requirements for your equipment.

Industry Canada - Equipment Attachment Limitations

The following notices are required by Industry Canada Terminal Attachment Program Procedure DC-01(E), Procedure for Declaration of Conformity and Registration of Terminal Equipment, Section 6.4 and ICES-003, Interference-Causing Equipment Standard for Digital Apparatus, Section 6.2.

Statement of Compliance

This product meets the applicable Industry Canada technical specifications.

Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

Ringer Equivalence Number (REN)

The Ringer Equivalence Number is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison

Copyright © 2015 Sonus Networks. All rights reserved.

quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

EMC Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Hardware Expansion Modules

Sonus SBC 1000/2000 systems may contain factory-installed hardware modules depending on the system type and configuration you purchased.

> These modules are not user-serviceable and may only be installed or repaired by Sonus-trained service personnel.

> **Do not remove the top panel of the Sonus SBC 1000/2000 chassis.** Operating the Sonus SBC 1000/2000 system with the top panel removed will cause hardware components to overheat and fail. Unauthorized removal of the top panel will void your product warranty and service agreement.

Hardware Expansion Modules

- Digital Signal Processing (DSP) Modules
- Application Solution Module (ASM)

Digital Signal Processing (DSP) Modules

DSP modules are hardware modules installed in the Sonus SBC 1000/2000 chassis that provide the call processing horsepower for the Sonus SBC 1000/2000 system.

For information see Sonus SBC 1000-2000 System Performance and Capacity.

Sonus SBC 1000 DSP Modules

The Sonus SBC 1000 accommodates up to 3 DSPs; one is integrated in the Main Board and two optional factory installed.

Sonus SBC 2000 DSP Modules

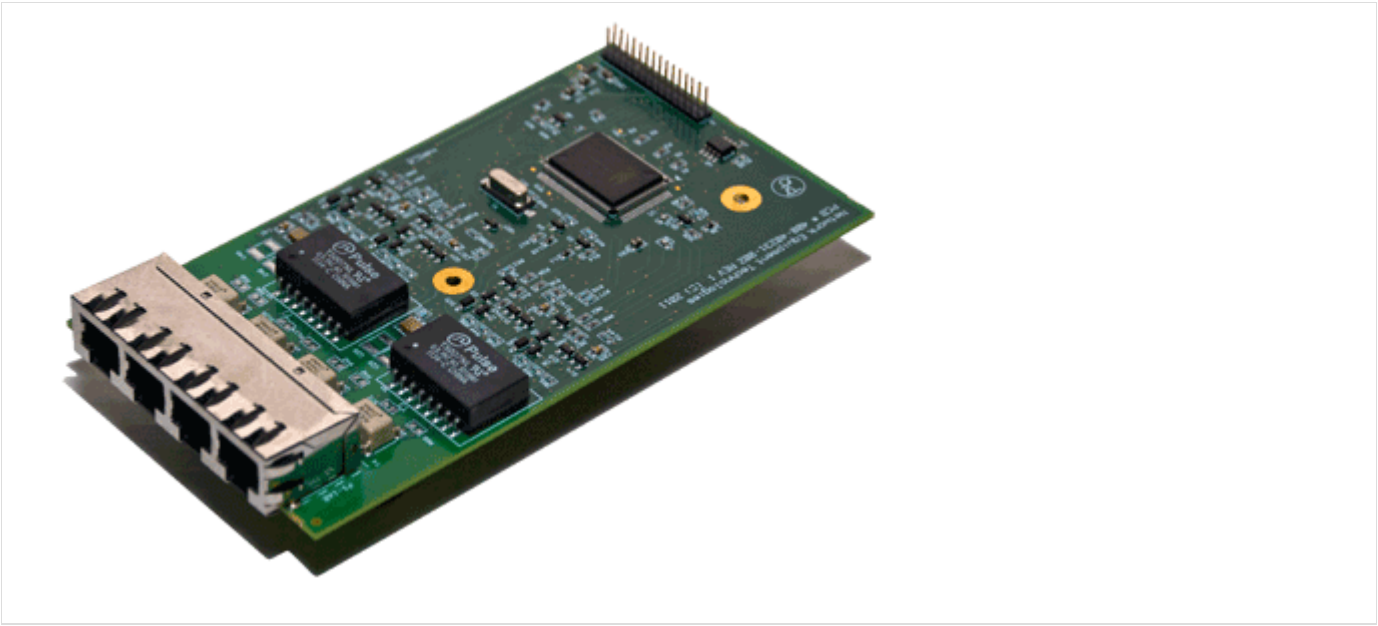
The Sonus SBC 2000 accommodates up to 6 DSP modules.

> **Do not remove the top panel of the Sonus SBC 1000/2000 chassis.** Operating the Sonus SBC 1000/2000 system with the top panel removed will cause hardware components to overheat and fail. Unauthorized removal of the top panel will void your product warranty and service agreement.

> DSP modules are factory installed and can only be upgraded by Sonus-trained service personnel.

Sonus SBC 1000 BRI Card

Copyright © 2015 Sonus Networks. All rights reserved.



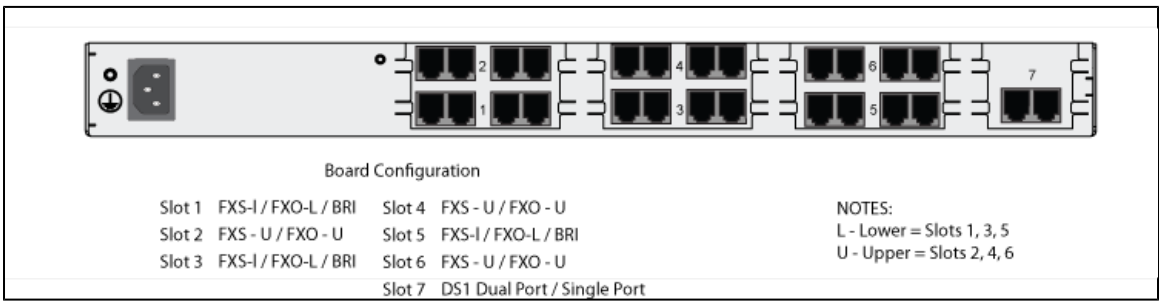
Overview

The Sonus SBC 1000 BRI cards comprise four standard BRI ports with shielded RJ-45 connectors. BRI cards, unlike the FXS/FXO cards are not stackable, and they are installed in the lower three daughter card positions. The Sonus SBC 1000 supports a maximum of three BRI cards, providing a maximum of 12 BRI ports.

Installation and Service

Sonus SBC 1000 daughter cards are not user serviceable components.

Sonus SBC 1000 Daughter Board Configuration



Configuration Examples

EXAMPLE A	SLOT 1 & 2	SLOT 3 & 4	SLOT 5 & 6	SLOT 7
Upper Module	FXO-U	FXS-U	*empty*	*empty*
Lower Module	FXS-L	FXS-L	FXS-L	PRI

EXAMPLE B	SLOT 1 & 2	SLOT 3 & 4	SLOT 5 & 6	SLOT 7

Copyright © 2015 Sonus Networks. All rights reserved.

Upper Module	FXO-U	*empty*	*empty*	*empty*
Lower Module	FXS-L	FXS-L	BRI	PRI

EXAMPLE C	**SLOT 1 & 2**	**SLOT 3 & 4**	**SLOT 5 & 6**	**SLOT 7**
Upper Module	*empty*	*empty*	*empty*	*empty*
Lower Module	FXS-L	*empty*	BRI	PRI

Sonus SBC 1000 FXO Cards



Overview

The Sonus SBC 1000 FXO cards, both upper and lower, comprise four standard FXO ports with RJ-11 connectors. The RJ-11 connectors on the FXO card are Grey in color so that they can be easily distinguished from the Sonus SBC 1000 FXS cards when installed in the chassis.

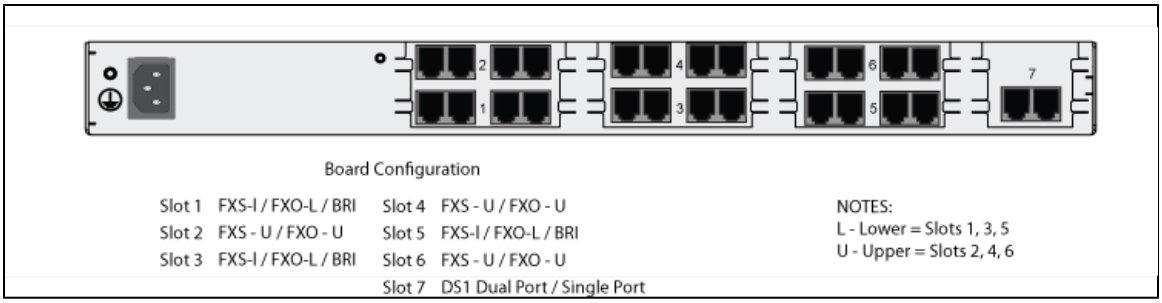
The Sonus SBC 1000 supports a maximum of six FXO cards, providing a maximum of 24 FXO ports. The number of FXO cards installed depends on the specific configuration and limited by the number of other daughter cards (FXS and BRI) installed as part of the specific configuration.

Installation and Service

Sonus SBC 1000 daughter cards are not user serviceable components.

Sonus SBC 1000 Daughter Board Configuration

Copyright © 2015 Sonus Networks. All rights reserved.



Configuration Examples

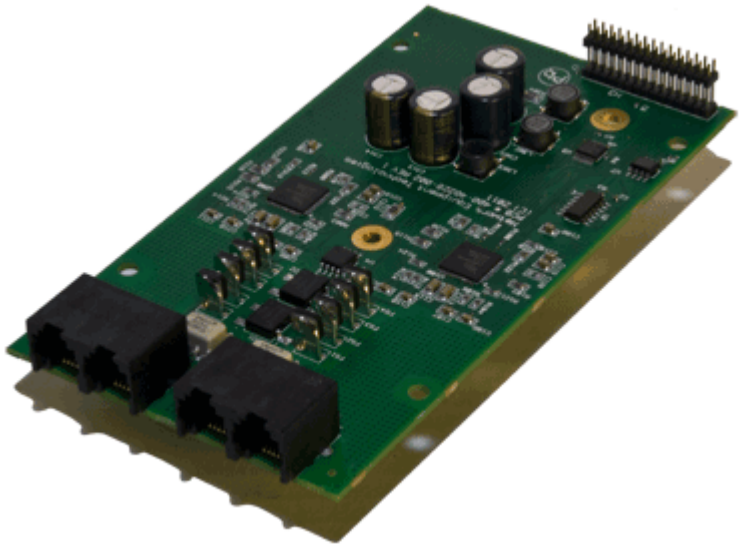
EXAMPLE A	SLOT 1 & 2	SLOT 3 & 4	SLOT 5 & 6	SLOT 7
Upper Module	FXO-U	FXS-U	*empty*	*empty*
Lower Module	FXS-L	FXS-L	FXS-L	PRI

EXAMPLE B	SLOT 1 & 2	SLOT 3 & 4	SLOT 5 & 6	SLOT 7
Upper Module	FXO-U	*empty*	*empty*	*empty*
Lower Module	FXS-L	FXS-L	BRI	PRI

EXAMPLE C	SLOT 1 & 2	SLOT 3 & 4	SLOT 5 & 6	SLOT 7
Upper Module	*empty*	*empty*	*empty*	*empty*
Lower Module	FXS-L	*empty*	BRI	PRI

Sonus SBC 1000 FXS Cards

Copyright © 2015 Sonus Networks. All rights reserved.



(FXS Lower Only Shown)

Overview

The Sonus SBC 1000 FXS cards, both upper and lower, comprise four standard FXS ports with RJ-11 connectors. The RJ-11 connectors on the FXS card are Black in color so that they can be easily distinguished from the Sonus SBC 1000 FXO cards (grey connectors) when installed in the chassis.

The Sonus SBC 1000 supports a maximum of six FXS cards, providing a maximum of 24 FXS ports. The number of FXS cards installed depends on the specific configuration and limited by the number of other daughter cards (FXO and BRI) installed as part of the specific configuration.

Interface Specifications and Limitations

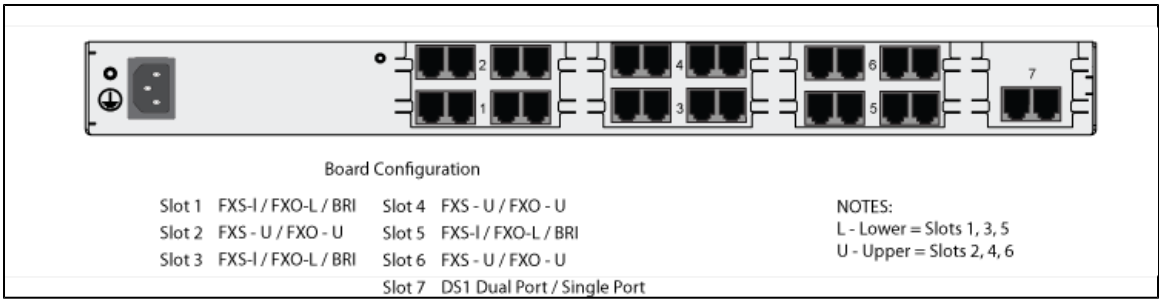
Item	Value/Dimension
Maximum external Off-Hook resistance	600 ohms (This includes the resistance of the cable and the DC resistance of the termination device)
Typical Loop Current Limit	23 ma/port
Typical FXS Port Ringing Voltage	45V RMS with 3 REN load
Max. Loop Length	1000m

Installation and Service

Sonus SBC 1000 daughter cards are not user serviceable components.

Sonus SBC 1000 Daughter Board Configuration

Copyright © 2015 Sonus Networks. All rights reserved.



Configuration Examples

EXAMPLE A	SLOT 1 & 2	SLOT 3 & 4	SLOT 5 & 6	SLOT 7
Upper Module	FXO-U	FXS-U	*empty*	*empty*
Lower Module	FXS-L	FXS-L	FXS-L	PRI

EXAMPLE B	SLOT 1 & 2	SLOT 3 & 4	SLOT 5 & 6	SLOT 7
Upper Module	FXO-U	*empty*	*empty*	*empty*
Lower Module	FXS-L	FXS-L	BRI	PRI

EXAMPLE C	SLOT 1 & 2	SLOT 3 & 4	SLOT 5 & 6	SLOT 7
Upper Module	*empty*	*empty*	*empty*	*empty*
Lower Module	FXS-L	*empty*	BRI	PRI

Sonus SBC 1000-2000 System Power Supplies

> For information on power connection requirements for the Sonus SBC 1000/2000 system, see Power Connection Requirements.

Sonus SBC 1000 Power Supply

Specifications

The Sonus SBC 1000 system comes equipped with a single power supply which complies with the following specifications:

Item	Specification
Input Voltage	AC: 100-240 VAC Nominal, Auto-switching, 47-63 Hz
AC Maximum Input Current	1.25A at 115VAC and 0.63A at 230VAC

Copyright © 2015 Sonus Networks. All rights reserved.

AC Input Voltage Range (nominal)	100-127VAC and 200-240VAC
Output	+12V/10A
Max Power Consumption	144

LED Status Indicator

⚠ There are no visible Power Supply LEDs on the Sonus SBC 1000.

Sonus SBC 2000 Power Supply

Specifications

The Sonus SBC 2000 system comes equipped with either a single power supply, or dual redundant power supplies which comply with the following specifications:

Item	Specification
Input Voltage	AC: 100-240 VAC Nominal, Auto-switching, 47-63 Hz
AC Maximum Input Current	5A at 115VAC and 2.5A at 230VAC
AC Input Voltage Range (nominal)	100-127VAC and 200-240VAC
Output	300 W-AC: +5V/20A, +12V/24A, -12V/0.6A, +3.3V/20A, +5VSB/3A
Max Power Consumption	300 watts

Sonus SBC 1000/2000 power supplies are tested and certified to meet UL / cUL / IEC 60950-1 safety requirements.

⛔ The Sonus SBC 1000/2000 power supplies must be replaced with Sonus-provided units only.

ℹ The SBC 2000 power supplies, if equipped with dual supplies, are hot swappable. Note that this only applies to the SBC 2000 and only when two power supplies are installed in the redundant mode.

LED Status Indicator

The Sonus SBC 1000/2000 power supplies include a LED status indicator on the back of the unit. The following table explains the meaning of the various LED Status states.

LED Status	Power Supply Status Description
Solid Green	Normal (AC on, DC power on)
Blinking Green	Standby (AC on, DC standby on, DC power off) power to the Sonus SBC 1000/2000 main board is ***off***
Solid Red	Alarm Condition
Blinking Red	Fan Failure

Copyright © 2015 Sonus Networks. All rights reserved.

Off	AC Failure

Reconfiguring Sonus SBC 1000-2000 Ports

Overview

When reconfiguring the Sonus SBC 1000/2000 by replacing an interface card with another type of interface card (e.g., replacing an E1/T1 card with an FSX card), references to the old card must be deleted from various portions of the Sonus SBC 1000/2000 configuration.

Applicability

Sonus SBC 1000

Replacement of the following cards in slots 1 through 6:

- Sonus SBC 1000 BRI Card
- Sonus SBC 1000 FXO Card
- Sonus SBC 1000 FXS Card

Sonus SBC 2000

Replacement of the following interface cards in slots 1 and 2:

- T1/E1 PSTN Interface Card
- Sonus SBC 2000 FXS Card

Procedure

The procedure for replacing a line card comprises the following steps:

1. Replace the interface cards using the procedure described in Inserting and Removing Interface Cards.
2. Remove any dependencies Signaling Groups and Routing Tables.
    a. In the WebUI, click the **Settings** tab.
    b. In the left navigation pane, go to **Signaling Groups > [*ISDN or CAS Signaling Group*]**
    c. Delete the ***old*** ports from any ISDN or CAS Signaling Groups. For more information see, Creating and Modifying CAS Signaling Groups and Creating and Modifying ISDN Signaling Groups for more information
3. Delete the ***old*** ports from the Port Table.
    a. In the WebUI, click the **Settings** tab.
    b. In the left navigation pane, go to **Node Interfaces > Ports**.
    c. Delete the ***old*** ports (those with a service status of ***Unknown()***. For more information see, Managing Telephony Ports

    > **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

4. Reboot the Sonus SBC 1000/2000.

After a successful reboot of the Sonus SBC 1000/2000, the ***new*** ports and port types should be displayed in the **Port Table View** page.

Troubleshooting Sonus SBC 1000-2000

Copyright © 2015 Sonus Networks. All rights reserved.

This section will help you troubleshoot problems on your Sonus SBC 1000/2000.

Rebooting Sonus SBC 1000-2000

- Restart Reports

Resetting the Sonus SBC 1000-2000 to Factory Defaults

Common Troubleshooting Issues

Common Troubleshooting Issues with Certificates in Sonus SBC 1000-2000

Alarms and Events Reference

Working with the Debug Facility

Testing a Call

Testing Network Connections

Viewing Mounted File Systems

Viewing Active Processes

Viewing The SIP Connections Table

Viewing The Disk Partition Table

Rebooting Sonus SBC 1000-2000

ASM Behavior on Sonus SBC 1000/2000 Reboot Operation

Depending on your Sonus SBC 1000/2000 model, users with a built-in Working with the ASM and SBA may be impacted by this operation:

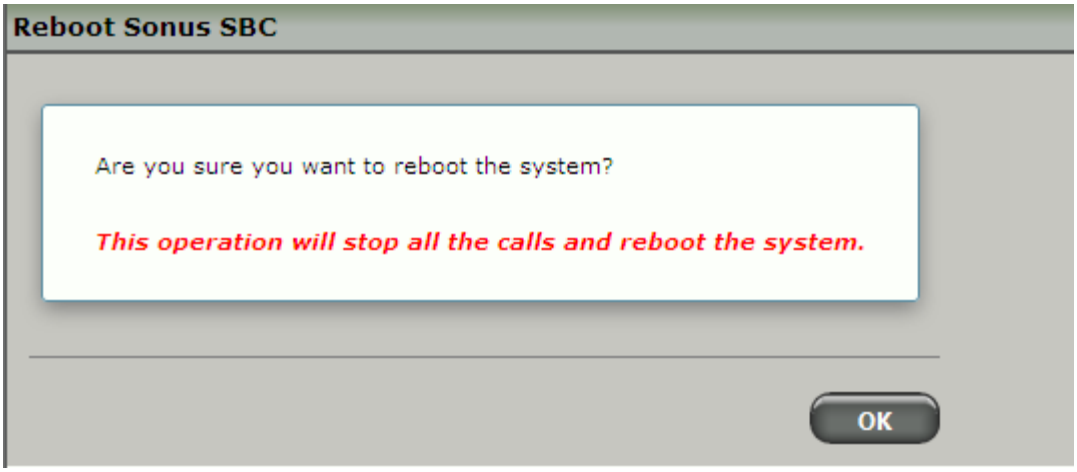
- **Sonus SBC 2000**
  - If the ASM is running, rebooting the Sonus SBC 1000/2000 **will cause the ASM to also reboot.**
  - If the ASM is shut down, rebooting the Sonus SBC 1000/2000 **will not restart the ASM**.
    - *To bring the ASM back into operation, you must physically power off and power back on the Sonus SBC 1000/2000*.
- **Sonus SBC 1000** --- rebooting the Sonus SBC 1000/2000 **will not have an effect on the ASM**.

Rebooting the Sonus SBC 1000/2000

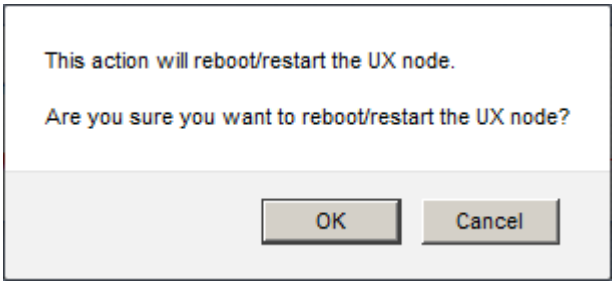
To reboot the Sonus SBC 1000/2000 system:

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **System**, click **Reboot Sonus SBC**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Click **OK**.The following popup will be displayed to confirm the action:



4. Click **OK** to reboot Sonus SBC 1000/2000
5. The web interface will dispatch the following status message throughout the reboot cycle.



On average, the **Sonus SBC 1000/2000 system takes between 3 to 4 minutes to fully reboot** and become reachable again through the web interface.

Upon completion, you will be automatically redirected to the Login Screen

Restart Reports

The Restart Reports feature provide access to the Power On System Test (POST) results. The Restart Reports feature comprises three sets of data presented in three different pages:

- Restart History
- H/W Post Results
- Core Files

Copyright © 2015 Sonus Networks. All rights reserved.

If the SBC 1000/2000 was operating on software versions 3.2 or older, the version and build information may be unavailable.

Restart History

The restart history is persistent and can not be deleted. However, the Restart History is cleared during a factory default. The Restart History contains on the last 20 reports.



Restart History | H/W POST Results | Core Files

Total **19 Restart History Table** Rows — July 22, 2014 06:34:46

Reboot Reason	Start Time	Version	Build
active partition changed from 172.16.110.112	Sat Jul 19 01:56:30 UTC 2014	4.0.0	324
command line reboot	Wed Jul 16 08:59:09 UTC 2014	4.0.0	323
reboot request from 172.16.110.112	Tue Jul 15 21:14:17 PDT 2014	4.0.0	323
active partition changed from 172.16.110.112	Tue Jul 15 20:58:39 PDT 2014	4.0.0	323
autoreboot - password changed	Tue Jul 15 20:15:24 PDT 2014	Unavailable	Unavailable
active partition changed from 172.16.110.112	Thu Jul 10 17:54:44 PDT 2014	Unavailable	Unavailable
active partition changed from 172.16.110.112	Mon Jun 9 23:05:20 PDT 2014	Unavailable	Unavailable
active partition changed from 172.16.110.112	Thu May 29 22:45:50 PDT 2014	Unavailable	Unavailable
active partition changed from 172.16.110.112	Wed May 28 19:48:56 PDT 2014	Unavailable	Unavailable
active partition changed from 172.16.110.112	Tue May 20 19:59:36 PDT 2014	Unavailable	Unavailable
active partition changed from 172.16.110.112	Thu May 15 23:45:45 PDT 2014	Unavailable	Unavailable
active partition changed from 172.16.110.112	Wed May 14 18:25:31 PDT 2014	Unavailable	Unavailable
active partition changed from 172.16.110.112	Mon May 12 20:39:27 PDT 2014	Unavailable	Unavailable
active partition changed from 172.16.110.112	Thu May 8 17:15:50 PDT 2014	Unavailable	Unavailable
autoreboot - password changed	Fri Apr 25 19:50:54 PDT 2014	Unavailable	Unavailable
autoreboot - password changed	Sat Jan 18 00:29:42 PST 2014	Unavailable	Unavailable
autoreboot - password changed	Tue Jan 14 22:45:04 PST 2014	Unavailable	Unavailable
autoreboot - password changed	Fri Jan 10 23:50:26 PST 2014	Unavailable	Unavailable
autoreboot - password changed	Fri Jan 10 20:27:01 PST 2014	Unavailable	Unavailable

Viewing the Restart History

To view the Restart History:

1. Click the **Diagnostics** tab at the top of the WebUI.
2. In the left navigation pane, click **Restart Report**.
3. Click the **Restart History** tab.

Refreshing Restart History

To refresh the Restart History table:

- Click the **refresh** ( ) icon located in upper right-hand corner of the Restart History table.

H/W POST Results

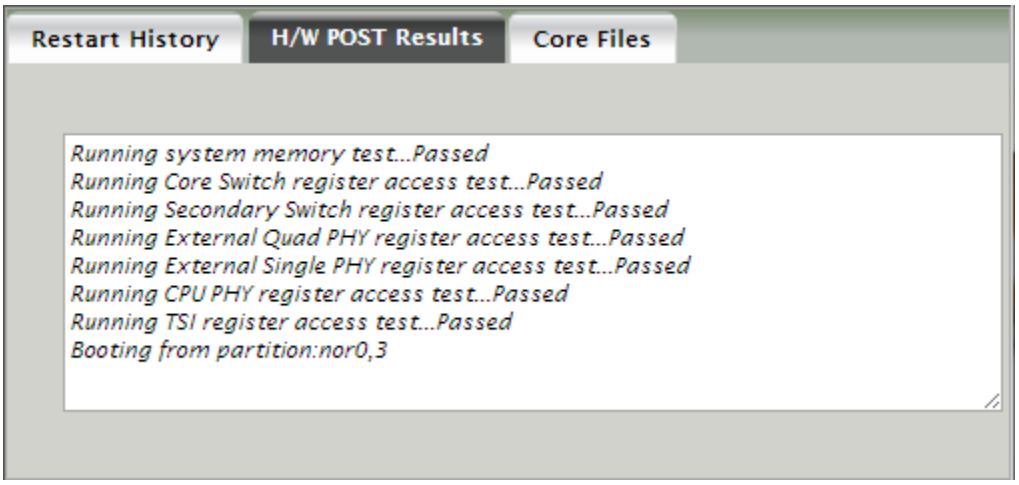
Viewing POST Results

To view the Restart History:

1. Click the **Diagnostics** tab at the top of the WebUI.

Copyright © 2015 Sonus Networks. All rights reserved.

2. In the left navigation pane, click **Restart Report**.
3. Click the **H/W POST Results** tab.

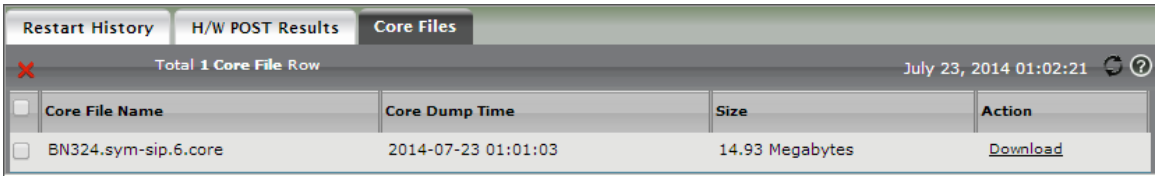


Core Files

Downloading Core Files

To download core files:

1. **Click the Diagnostics tab at the top of the WebUI.**
2. In the left navigation pane, click **Restart Report**.
3. Click the **Core Files** tab.
4. Click the **Download** link next to the core file you wish to view.
5. Save the core file in a convenient location.



Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Caution

Core files should only be downloaded or deleted at the direction of Sonus Global Services.

Resetting the Sonus SBC 1000-2000 to Factory Defaults

This procedure lets you reset the Sonus SBC 1000/2000 to factory defaults. You might want to use this procedure in certain recovery scenarios like lost admin password or lost IP address etc.

Resetting Sonus SBC 1000/2000 to factory defaults removes all user-configured data. This including user names, passwords, customized IP addresses, etc..

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000/2000 Systems with Built-in ASM

If your ASM is already initialized and Lync SBA is deployed, resetting Sonus SBC 1000/2000 to factory defaults **does not reset the ASM/SBA** configuration settings. If you wish to reset the ASM to factory defaults, then you must Re-initialize the ASM.

Manual Reset

To Reset Configuration to Factory Defaults

There are three methods for resetting the Sonus SBC 1000/2000 to a factory default state:

1. If the Sonus SBC 1000/2000 is running, press and **hold** the Reset button for approximately **20 seconds**.
2. Shutdown the Sonus SBC 1000/2000, press and hold the reset button while the unit is powered on. Hold the reset button until the Alarm Status LED first turns yellow and then goes out.
   - Click here to see where the Sonus SBC 1000 Reset button is located



   - Click here to see where the Sonus SBC 2000 Reset button is located



3. Reset the Sonus SBC 1000/2000 from the user interface.

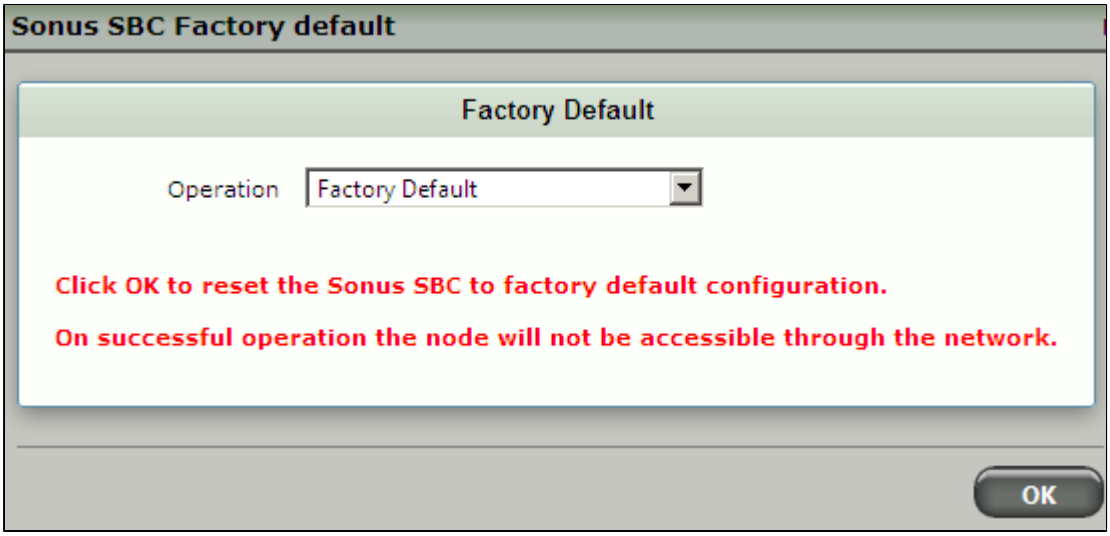
After the Sonus SBC 1000/2000 system has booted, it can be re-initialized by Running Initial Setup.

Resetting Factory Defaults from the UI

To reset the Sonus SBC 1000/2000 to factory defaults from the UI:

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, go to **System > Sonus SBC Factory Default.**

Copyright © 2015 Sonus Networks. All rights reserved.



Operation Selections

Factory Default

This selection performs a total factory reset. After the operation is complete, the Sonus SBC 1000/2000 can be re-initialized by Running Initial Setup.

Partial Reset

This selection removes all configuration information from the Sonus SBC 1000/2000 with the exception of the Logical Interfaces, Ethernet ports, VLANs, ACLs, Static Routes, ASM Networking, Node-Level Settings and Certificate configurations. With this option the Sonus SBC 1000/2000 can still be reached through a browser pointed at its application IP Address.

Common Troubleshooting Issues

- Initial Configuration
  - I set the network configuration in the initial configuration page, but I still cannot see Sonus SBC 1000/2000 on the network.
  - After Initial Configuration, I am importing an old backup from a different Sonus SBC 1000/2000, but my T1/E1 ports do not match the configuration.
- ISDN related issues
  - ISDN port stuck in Yellow alarm state
  - MOC conference participants get static when PSTN caller joins the conference
- SIP related issues
  - Tenor signaling group in Sonus SBC 1000/2000 will be up and then will go down for no apparent reason
- Faxing
  - Where can I find a guide to configure a fax solution for Lync?
  - When do I use G.711 VS T.38?
  - The faxes have quality issues.
  - Faxes from PSTN via Sonus SBC 1000/2000 to FACSys fax server do not complete
- Audio Quality
- Call Completion issues
  - Call rejected from PSTN with ISUP cause code 16, Sonus SBC 1000/2000 sends 500 Internal Server

Copyright © 2015 Sonus Networks. All rights reserved.

Error to Lync
    - Forked PSTN call to Lync and PBX gets disconnected by Sonus SBC 1000/2000 upon receiving STATUS message from PSTN
- Call Presentation
    - Calling Name for PSTN to Lync calls is not displayed correctly
    - Calling Name is not present on outbound calls over ISDN port with NI2 or Euro-ISDN switch variants
- Certificate Related
    - Common Troubleshooting Issues with Certificates in Sonus SBC 1000-2000
- Lync Deployment
    - Config Replication step in the Setup SBA task fails with "A network-related or instance-specific error occurred while establishing a connection to SQL Server"
    - The Config Replication Step of Setup SBA Task Fails with Failed to run configuration replication script
- Lync Operational
    - Calls to PSTN numbers fail. Lync declares the gateway unavailable with Event ID 46046
    - Lync clients at Branch Site cannot establish MTLS connection with the Central Pool
    - Lync Server 2010 Archiving Agent fails to create local queue on the SBA
    - Monitor application does not load. Monitor displays - Failed to connect to the Server. Please try again.
    - When querying Active Directory cache, attributes are missing in the search result
    - Workaround for no ring back in PSTN to Lync calls

Initial Configuration

I set the network configuration in the initial configuration page, but I still cannot see Sonus SBC 1000/2000 on the network.

- Check the Ethernet port's speed and duplexity and match that to the Ethernet port configuration in Sonus SBC 1000/2000.

After Initial Configuration, I am importing an old backup from a different Sonus SBC 1000/2000, but my T1/E1 ports do not match the configuration.

- Try inserting the card into the other slot. Also, you will have to reset the configuration to factory defaults in order to remove the auto populated ports and restore the old configuration again.

ISDN related issues

ISDN port stuck in Yellow alarm state

MOC conference participants get static when PSTN caller joins the conference

SIP related issues

Tenor signaling group in Sonus SBC 1000/2000 will be up and then will go down for no apparent reason

Faxing

Where can I find a guide to configure a fax solution for Lync?

Using a Tenor as an Analog Device in a Lync Sonus SBC 1000/2000 SBA Deployment

When do I use G.711 VS T.38?

Copyright © 2015 Sonus Networks. All rights reserved.

It is recommended to use G.711 when implementing a fax solution where Sonus SBC 1000/2000 and the fax server are on the same LAN. T.38 should be used when there are many hops.

The faxes have quality issues.

Check clock source setting.

Faxes from PSTN via Sonus SBC 1000/2000 to FACSys fax server do not complete

Audio Quality

Call Completion issues

Call rejected from PSTN with ISUP cause code 16, Sonus SBC 1000/2000 sends 500 Internal Server Error to Lync

Forked PSTN call to Lync and PBX gets disconnected by Sonus SBC 1000/2000 upon receiving STATUS message from PSTN

Call Presentation

Calling Name for PSTN to Lync calls is not displayed correctly

Calling Name is not present on outbound calls over ISDN port with NI2 or Euro-ISDN switch variants

Certificate Related

Common Troubleshooting Issues with Certificates in Sonus SBC 1000-2000

Lync Deployment

Config Replication step in the Setup SBA task fails with "A network-related or instance-specific error occurred while establishing a connection to SQL Server"

The Config Replication Step of Setup SBA Task Fails with Failed to run configuration replication script

Lync Operational

Calls to PSTN numbers fail. Lync declares the gateway unavailable with Event ID 46046

Lync clients at Branch Site cannot establish MTLS connection with the Central Pool

Lync Server 2010 Archiving Agent fails to create local queue on the SBA

Monitor application does not load. Monitor displays - Failed to connect to the Server.

Copyright © 2015 Sonus Networks. All rights reserved.

Please try again.

When querying Active Directory cache, attributes are missing in the search result

Workaround for no ring back in PSTN to Lync calls

Common Troubleshooting Issues with Certificates in Sonus SBC 1000-2000

In this troubleshooting article, we present various issues, difficulties, and nuances of employing certificates on the Sonus SBC 1000/2000. Each of the instances is accompanied by an investigation path to assist in remedying the issue.

- Certificate Errors from the Sonus SBC 1000/2000 Log
  - Certificate Not Trusted
  - Certificate and Private Key Do Not Match
  - Failed to authenticate (Server) certificate due to bad encoding format, certificate contents or signature mis-match
  - Connection Refused for Invites or Sonus SBC 1000/2000 does not transmit Options (TG down)
  - Error Opening My Certificate File
  - Certificate Is Not Yet Valid
  - Unable To Get Local Issuer Certificate
  - Configured and Expected host FQDN does not match peer certificate Common Name
  - SSL Hello Fails
  - Server Disconnects TLS negotiation
  - Possible incompatible Wave14 Releases (SBA=7306, Sonus SBC 1000/2000=v140/7457)
  - Failure to automatically import the single base64 encoded file containing bundled certificates
- Reference
  - Exchange Log Error: Target name in the certificate is incorrect
  - X509 Certificate Error Messages

Related Articles

- Working with Sonus SBC 1000/2000 Certificates

Certificate Errors from the Sonus SBC 1000/2000 Log

Copyright © 2015 Sonus Networks. All rights reserved.

Certificate Not Trusted

```
[2010-07-01 23:28:47,440] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:2127) - Verify peer certificate depth=1, issuer:
/DC=net/DC=vx/CN=vx-DEMO5-CA, subject: /DC=net/DC=vx/CN=vx-DEMO5-CA,
status: 0(ok)
[2010-07-01 23:28:47,451] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:2127) - Verify peer certificate depth=0, issuer:
/DC=net/DC=vx/CN=vx-DEMO5-CA, subject:
/C=US/ST=California/L=Fremont/OU=Sonus SBC 1000/2000/CN=sba1.vx.net,
status: 0(ok)
[2010-07-01 23:28:47,453] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:2025) - Received peer server certificate common
name: sba1.vx.net for conn_id: 1
[2010-07-01 23:28:47,454] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:2395) - Configured host FQDN: sba.net.com does not
match peer certificate Common Name: sba1.vx.net for conn_id: 1
[2010-07-01 23:28:47,455] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:2459) - Configured host FQDN: sba.net.com does not
match peer certificate SAN for conn_id: 1
[2010-07-01 23:28:47,459] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:2056) - Peer certificate verify and authentication
failed with error: 27(certificate not trusted)
```

Investigation Path:

- Reboot the Sonus SBC 1000/2000.
- The FQDN programmed as a destination SIP Serverdoes not match the Common or Subject Alternative Name within the received certificate.
    - Change the SIP Server configuration to match the FQDN names within the certificate.
- The SIP Server is programmed with the IP instead of the certificate's matching FQDN for the destination host.

Copyright © 2015 Sonus Networks. All rights reserved.

Certificate and Private Key Do Not Match

Failed to authenticate (Server) certificate due to bad encoding format, certificate contents or signature mis-match

```
[2011-03-15 13:58:31,910] com.net.ux.csm DEBUG (CertManager.cpp:617) -
Received Import Config Data Approve Request
[2011-03-15 13:58:31,910] com.net.ux.csm TRACE (CertManager.cpp:977) -
Approving the Certificate Contents for File:
CertImport20110315135831-000000.pem in holding path
[2011-03-15 13:58:31,912] com.net.ux.csm ERROR (CertManager.cpp:4055) -
Unable to load Server certificate file
[2011-03-15 13:58:31,915] com.net.ux.csm TRACE (CertManager.cpp:3841) -
Successfully loaded Server PKCS7 chain file
[2011-03-15 13:58:31,915] com.net.ux.csm DEBUG (CertManager.cpp:3959) -
Writing certificate chain num: 0
[2011-03-15 13:58:31,916] com.net.ux.csm DEBUG (CertManager.cpp:3959) -
Writing certificate chain num: 1
[2011-03-15 13:58:31,916] com.net.ux.csm DEBUG (CertManager.cpp:3959) -
Writing certificate chain num: 2
[2011-03-15 13:58:31,917] com.net.ux.csm DEBUG (CertManager.cpp:3959) -
Writing certificate chain num: 3
[2011-03-15 13:58:31,919] com.net.ux.csm TRACE (CertManager.cpp:4060) -
Successfully loaded Stack of X509 Certificate
[2011-03-15 13:58:31,959] com.net.ux.csm TRACE (CertManager.cpp:3680) -
Certificate to be imported was successfully validated
[2011-03-15 13:58:31,960] com.net.ux.csm TRACE (CertManager.cpp:4108) -
Successfully loaded Server private key
[2011-03-15 13:58:31,960] com.net.ux.csm ERROR (CertManager.cpp:3754) -
Local Certificate and Private Key do not match, error: 0
[2011-03-15 13:58:31,961] com.net.ux.csm ERROR (CertManager.cpp:662) -
Import certificate validation request failed: host name: 192.168.128.2
status: 3
```

Investigation Path:

- Generate, sign and import a new Sonus SBC 1000-2000 certificate.
- Ensure that the OK on the CSR Generation form is only pressed once before importing the signed certificate.

Connection Refused for Invites or Sonus SBC 1000/2000 does not transmit Options (TG down)

Copyright © 2015 Sonus Networks. All rights reserved.

Connection Refused

```
[2011-03-16 15:43:33,471] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:92) - TransportTlsSocket: connect object 0x2ced58
contructor: memory block used count: 1120
[2011-03-16 15:43:33,472] com.net.ux.sip INFO (CallSession.cpp:5040) -
{SG(5):132 0x2cfb28 0x2a67d0 [1:0:5:1]} HandleCCSetup: Next hop is
mediation.vx.net [10.1.1.7]:5070 CR=0
[2011-03-16 15:43:33,473] com.net.ux.sip INFO (CallSession.cpp:5094) -
{SG(5):132 0x2cfb28 0x2a67d0 [1:0:5:1]} HandleCCSetup: Received
IE_GENERIC_NAME
[2011-03-16 15:43:33,473] com.net.ux.sip INFO (CallSession.cpp:5129) -
{SG(5):132 0x2cfb28 0x2a67d0 [1:0:5:1]} HandleCCSetup: Handling SETUP from
"" '5103644064' National pres=0 to '+15105743571' Unknown.
[2011-03-16 15:43:33,475] com.net.ux.sip INFO (CallSession.cpp:5991) -
{SG(5):132 0x2cfb28 0x2a67d0 [1:0:5:1]} ManageLicense: Outbound sent
MSG_LM_ACQREL to LM. Acquire
[2011-03-16 15:43:33,480] com.net.ux.sip.libctl ERROR (Socket.cpp:698) -
Socket::HandleFDEvent: EPOLLERR fd=30, handle: 0x2ced5c, iSoError = 111
"Connection refused", Local Port: 24586, Remote IP:Port(10.1.1.7:5070),
fd=30
[2011-03-16 15:43:33,480] com.net.ux.sip INFO (ClientTransaction.cpp:615) -
ProcessSocketError: 2b86f8 ClientTransaction::ProcessSocketError=() called
[2011-03-16 15:43:33,481] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:92) - TransportTlsSocket: connect object 0x2b5128
contructor: memory block used count: 1120
[2011-03-16 15:43:33,482] com.net.ux.sip INFO (CallSession.cpp:4441) -
{SG(5):132 0x2cfb28 0x2a67d0 [1:0:5:1]} HandleSocketError: Clean up call
due to Socket Error
```

OR

Copyright © 2015 Sonus Networks. All rights reserved.

Socket::Close and Deletion for OptionServerSession.cpp

```
2011-06-13 13:51:31,044] com.net.ux.sip DEBUG (OptionsServerSession.cpp:88)
- ~OptionsServerSession: 286798
OptionsServerSession::~OptionsServerSession() called
[2011-06-13 13:51:31,044] com.net.ux.sip DEBUG (Session.cpp:175) -
~Session: dtor 286798 id=41
[2011-06-13 13:51:31,044] com.net.ux.sip DEBUG (TransportLayer.cpp:191) -
Close: 0TLS1297-5067 0x2863e8 fd=16 force=0.
[2011-06-13 13:51:31,044] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:188) - TLS connection no shutdown deletion for
conn_id: 423 on handle: 0x288c50, Local Port: 5067, Remote
IP:Port(10.80.61.61:54999), fd=16, current active sockets: 1
[2011-06-13 13:51:31,045] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:242) - Sent alert close notify in object deletion,
server fd=-1, client fd=16 for conn_id: 423
[2011-06-13 13:51:31,047] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:334) - TransportTlsSocket: object 0x288c50
destructor: memory block used count: 570
[2011-06-13 13:51:31,047] com.net.ux.sip.libctl INFO (Socket.cpp:205) -
Socket::Close and Deletion: fd=16
[2011-06-13 13:51:31,047] com.net.ux.sip DEBUG (Session.cpp:71) - ~Dialog:
dtor called 2869e0
[2011-06-13 13:51:31,047] com.net.ux.sip DEBUG (TransportLayer.cpp:162) -
~TransportConnection: 0TLS1297-5067 0x2863e8.
[2011-06-13 13:51:31,047] com.net.ux.sip DEBUG (Session.cpp:316) -
deleteAllDialogs: Session:: remaining dialogs : 0
```

Investigation Path:

- Verify configuration and that services are started on the TLS target system.
- Verify Lync topology configuration for IPs and ports
- Reboot the Lync server (full reboot)

Copyright © 2015 Sonus Networks. All rights reserved.

Error Opening My Certificate File

```
[2010-06-28 06:47:18,279] com.net.ux.sip.libctl DEBUG
(TrustedCertMemStore.cpp:161) - get memory store cert, len: 0, format: 1,
entry: 0
[2010-06-28 06:47:18,281] com.net.ux.sip.libctl FATAL
(TransportTlsSocket.cpp:871) - Error opening My server certificate file,
format: 1
[2010-06-28 06:47:18,320] com.net.ux.sip.libctl ERROR
(TransportTlsSocket.cpp:389) - TLS Client Handshake Setup failed for
conn_id: 2 on handle: 0x3166e0
[2010-06-28 06:47:18,322] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:2698) - TLS Handshake Failed send alert: -1,
recvalert: -1 for conn_id: 2 on handle: 0x3166e0
[2010-06-28 06:47:18,323] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:2482) - Clean up with abort flag: 1, persist close
flag: 1, state: Client Method State, event: Load Server Certificate Event
for conn_id: 2
[2010-06-28 06:47:18,325] com.net.ux.sip ERROR (TransportLayer.cpp:390) -
AbortCB: Connection aborted 0TLS3-24578 0x312100. Err=2 No such file or
directory.
```

Investigation Path:

- Sonus SBC 1000/2000's certificate is missing. Verify a certificate has been imported and is present

Copyright © 2015 Sonus Networks. All rights reserved.

Certificate Is Not Yet Valid

```
et.ux.sba INFO (syslogd.cpp:191) - SymComms.GetDomainName: System is part
of domain 'vx.net'
[2010-06-28 06:55:54,424] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:277) - Received Client TLS handshake message for
conn_id: 3 on handle: 0x31d018, sd=25
[2010-06-28 06:55:54,426] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:1578) - SSL_connect before: socket fd: 25 for
conn_id: 3 in state: SSLv3 read server hello A,
[2010-06-28 06:55:54,438] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:2127) - Verify peer certificate depth=1, issuer:
/DC=net/DC=vx/CN=vx-DEMO5-CA, subject: /DC=net/DC=vx/CN=vx-DEMO5-CA,
status: 0(ok)
[2010-06-28 06:55:54,448] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:2122) - Verify peer certificate depth=0, issuer:
/DC=net/DC=vx/CN=vx-DEMO5-CA, subject:
/C=US/ST=California/L=Fremont/OU=Sonus SBC 1000/2000/CN=sba1.vx.net error:
9(certificate is not yet valid)
[2010-06-28 06:55:54,450] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:2056) - Peer certificate verify and authentication
failed with error: 9(certificate is not yet valid)
```

Investigation Path:

- Verify the Valid From: date and time on the Sonus SBC 1000/2000 certificate is before the current time of the Sonus SBC 1000/2000.
- Set the Sonus SBC 1000/2000 time forward to a time past the Valid From: date/time.

Copyright © 2015 Sonus Networks. All rights reserved.

Unable To Get Local Issuer Certificate

```
DEBUG (TransportTlsSocket.cpp:1578) - SSL_connect before: socket fd: 26 for
conn_id: 3 in state: before/connect initialization,
[2010-06-28 01:14:26,570] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:1583) - SSL_connect after: socket fd: 26 for
conn_id: 3 in state: SSLv3 read server hello A,
[2010-06-28 01:14:26,588] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:277) - Received Client TLS handshake message for
conn_id: 3 on handle: 0x31d650, sd=26
[2010-06-28 01:14:26,590] com.net.ux.sip.libctl DEBUG
(TransportTlsSocket.cpp:1578) - SSL_connect before: socket fd: 26 for
conn_id: 3 in state: SSLv3 read server hello A,
[2010-06-28 01:14:26,595] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:2122) - Verify peer certificate depth=0, issuer:
/DC=net/DC=vx/CN=vx-DEMO5-CA, subject:
/C=US/ST=California/L=Fremont/OU=Sonus SBC 1000/2000/CN=sba1.vx.net error:
20(unable to get local issuer certificate)
[2010-06-28 01:14:26,598] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:2056) - Peer certificate verify and authentication
failed with error: 20(unable to get local issuer certificate)
```

Investigation Path:

- The certificate that signed the peer's certificate is not within Sonus SBC 1000/2000's Trusted (root) store.
    - Delete the current root certificate and import/re-import the root certificate that signed the peer's certificate. See Managing Trusted CA Certificates for further information.
- Reboot the Sonus SBC 1000/2000 and check to see if the problems is resolved.

Configured and Expected host FQDN does not match peer certificate Common Name

```
2011-09-28 11:15:28,272] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:2880) - Configured and Expected host FQDN:
,lync-admin.net.com does not match peer certificate Common Name:
fmt-lyncpool01.net.com for conn_id: 14
```

Investigation Path:

- In the corresponding TLS Profile, set the Validate Client FQDN to Disabled.

Cause

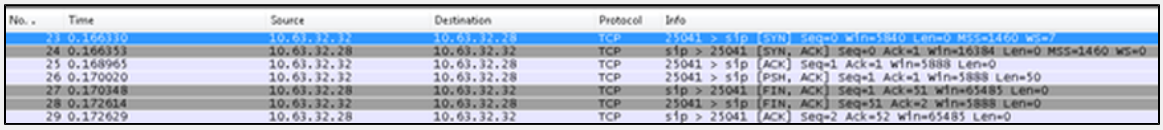
This error occurs when the reverse DNS lookup for the FE returns an FQDN that does not match the Sonus SBC 1000/2000 Federated FQDN configuration. It so happens that in many Lync installations, the FE and the cscp management interface share an IP address, but have two different FQDNs. The reverse lookup, in somes cases, returns the cscp FQDN (which does not match the pool FQDN configured as the Federated FQDN).

Copyright © 2015 Sonus Networks. All rights reserved.

SSL Hello Fails

```
1-03-14 17:21:15,251] com.net.ux.sip.libcommon TRACE (AFEventLoop.cpp:92) -
AFEventLoop::Monitor: Adding fd=18 for events=0x1.
[2011-03-14 17:21:15,251] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:1926) - SSL_connect before: socket fd=16 for
conn_id: 2 in state: before/connect initialization,
[2011-03-14 17:21:15,252] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:1931) - SSL_connect after: socket fd=16 for
conn_id: 2 in state: SSLv3 read server hello A,
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl INFO (Socket.cpp:647) -
Socket::HandleFDEvent: Connection peer shutdown: handle: 0x2556e4, Local
Port: 24578, Remote IP:Port(10.63.32.28:5060), fd=16
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2326) - Received OnSocketClose for conn_id: 2 on
handle: 0x2556e0
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:3047) - TLS Client clean up with abort flag: 1,
persist close flag: 0, state: Handshake State, event: Socket Close Event
for conn_id: 2
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:4450) - FindTLSConnAlmStEntry: Client Entry Key:
(1c203f0a)10.63.32.28 alert code mis-match for conn_id: 2, Count: 1
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:4475) - AddTLSConnAlmStEntry: Client
Entry=0x2562a0, Key: 1c203f0a was added conn_id: 2 with AlertSent: -1,
AlertRecv: -1, Count: 2
[2011-03-14 17:21:15,255] com.net.ux.sip ERROR (TransportLayer.cpp:581) -
AbortCB: Connection aborted 0TLS3-24578 0x2556e4. Err=11 Resource
temporarily unavailable.
[2011-03-14 17:21:15,255] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:3350) - alarmDescStr: TLSv1 Client Handshake
failure: conn_id: 2, port: 5060, AlertSent: -1, AlertRecv: -1. Action: Look
up TLS Alert Code definition to fix the problem., len: 147
```

The following is a sniffer trace of the issue:



No.	Time	Source	Destination	Protocol	Info
23	0.166330	10.63.32.32	10.63.32.28	TCP	25041 > sip [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=7
24	0.166353	10.63.32.28	10.63.32.32	TCP	sip > 25041 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0
25	0.168965	10.63.32.32	10.63.32.28	TCP	25041 > sip [ACK] Seq=1 Ack=1 Win=5888 Len=0
26	0.170020	10.63.32.32	10.63.32.28	TCP	25041 > sip [PSH, ACK] Seq=1 Ack=1 Win=5888 Len=50
27	0.170348	10.63.32.28	10.63.32.32	TCP	sip > 25041 [FIN, ACK] Seq=1 Ack=51 Win=65485 Len=0
28	0.172614	10.63.32.32	10.63.32.28	TCP	25041 > sip [FIN, ACK] Seq=51 Ack=2 Win=5888 Len=0
29	0.172629	10.63.32.28	10.63.32.32	TCP	sip > 25041 [ACK] Seq=2 Ack=52 Win=65485 Len=0

Notice that there is a 50B packet following the TCP handshake and then the other side closes the TCP connection.
The mediation server log indicates a Token failure.

Investigation Path:

- Verify the port numbers are correct in both Sonus SBC 1000/2000 and the target TLS system
- Verify that the FQDNs for the systems are in the DNS server and correct.
- Check the certs and configuration of the peer system. Make sure that the certs are valid and the Sonus SBC 1000/2000 FQDN is configured properly in Exchange or Mediation gateway configurations.

Copyright © 2015 Sonus Networks. All rights reserved.

Server Disconnects TLS negotiation

```
[2011-03-15 19:05:32,084] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:1589) - TLS Client Verify Peer Certificate set for
conn_id: 4337
[2011-03-15 19:05:32,085] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:1649) - Set TLS Server Socket fd=18, sbio: 0x28cd98
for conn_id: 4337
[2011-03-15 19:05:32,085] com.net.ux.sip.libcommon TRACE
(AFEventLoop.cpp:92) - AFEventLoop::Monitor: Adding fd=20 for events=0x1.
[2011-03-15 19:05:32,085] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:1926) - SSL_connect before: socket fd=18 for
conn_id: 4337 in state: before/connect initialization,
[2011-03-15 19:05:32,086] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:1931) - SSL_connect after: socket fd=18 for
conn_id: 4337 in state: SSLv3 read server hello A,
[2011-03-15 19:05:32,088] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:532) - RX Client TLS handshake message for conn_id:
4337 on handle: 0x269a78, fd=18
[2011-03-15 19:05:32,088] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:1926) - SSL_connect before: socket fd=18 for
conn_id: 4337 in state: SSLv3 read server hello A,
[2011-03-15 19:05:32,088] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:1931) - SSL_connect after: socket fd=18 for
conn_id: 4337 in state: SSLv3 read server hello A,
[2011-03-15 19:05:32,090] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:532) - RX Client TLS handshake message for conn_id:
4337 on handle: 0x269a78, fd=18
[2011-03-15 19:05:32,090] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:1926) - SSL_connect before: socket fd=18 for
conn_id: 4337 in state: SSLv3 read server hello A,
[2011-03-15 19:05:32,099] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2594) - Verify peer certificate depth=3, issuer:
/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust
Global Root, subject: /C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions,
Inc./CN=GTE CyberTrust Global Root, status: 0(ok)
[2011-03-15 19:05:32,112] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2594) - Verify peer certificate depth=2, issuer:
/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust
Global Root, subject: /O=Cybertrust, Inc/CN=Cybertrust Global Root, status:
0(ok)
[2011-03-15 19:05:32,119] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2594) - Verify peer certificate depth=1, issuer:
/O=Cybertrust, Inc/CN=Cybertrust Global Root, subject: /O=Cybertrust
Inc/CN=Cybertrust SureServer EV CA, status: 0(ok)
[2011-03-15 19:05:32,138] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2594) - Verify peer certificate depth=0, issuer:
/O=Cybertrust Inc/CN=Cybertrust SureServer EV CA, subject:
/C=US/ST=IL/L=Chicago/streetAddress=161 N Clark
St/1.3.6.1.4.1.311.60.2.1.3=US/1.3.6.1.4.1.311.60.2.1.2=IL/O=Accenture
LLP/2.5.4.15=V1.0, Clause 5.(b)/OU=CIO/serialNumber=00622, status: 0(ok)
[2011-03-15 19:05:32,139] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2490) - TLS Client received peer certificate common
name: AMROM3205.dir.svc.accenture.com for conn_id: 4337
[2011-03-15 19:05:32,139] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2874) - Matched configured host FQDN:
amrom3205.dir.svc.accenture.com with peer certificate Common Name:
AMROM3205.dir.svc.accenture.com for conn_id: 4337
[2011-03-15 19:05:32,139] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:2532) - TLS Client peer certificate verified and
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
authenticated for conn_id: 4337
[2011-03-15 19:05:32,233] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:1931) - SSL_connect after: socket fd=18 for
conn_id: 4337 in state: SSLv3 read finished A,
[2011-03-15 19:05:32,243] com.net.ux.sip.libctl INFO (Socket.cpp:647) -
Socket::HandleFDEvent: Connection peer shutdown: handle: 0x269a7c, Local
Port: 24821, Remote IP:Port(10.63.32.28:5060), fd=18
[2011-03-15 19:05:32,243] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2326) - Received OnSocketClose for conn_id: 4337 on
handle: 0x269a78
[2011-03-15 19:05:32,243] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:3047) - TLS Client clean up with abort flag: 1,
persist close flag: 0, state: Handshake State, event: Socket Close Event
for conn_id: 4337
[2011-03-15 19:05:32,243] com.net.ux.sip.libctl WARN
(TransportTlsSocket.cpp:4441) - FindTLSConnAlmStEntry: Client Entry Key:
1c203f0a(10.63.32.28) found for conn_id: 1 with AlertSent: -1, AlertRecv:
-1, Count: 3
[2011-03-15 19:05:32,243] com.net.ux.sip ERROR (TransportLayer.cpp:581) -
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
AbortCB: Connection aborted 0TLS247-24821 0x269a7c. Err=11 Resource
temporarily unavailable.
```

Investigation Path:

- Check the opposing TLS system's logs for indications as to why it closed the session.

Possible incompatible Wave14 Releases (SBA=7306, Sonus SBC 1000/2000=v140/7457)

```
2010-09-09 16:44:20,450] com.net.ux.sip DEBUG (TransportLayer.cpp:408) -
ClientConnectedCB: 0TLS10-24585 ssl_id: 9, sd: -1, handle=0x29205c, fd=11,
Peer=[172.20.250.133]:5067
[2010-09-09 16:44:20,452] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:1902) - Send application data_len: 1001 for
conn_id: 9 on handle: 0x292058, retry: 0, retry_cnt: 0
[2010-09-09 16:44:20,452] com.net.ux.sip.libctl ERROR (Socket.cpp:590) -
Socket::HandleFDEvent: EPOLLERR fd=11, handle: 0x29205c, iSoError = 32
"Broken pipe", Local Port: 24585, Remote IP:Port(172.20.250.133:5067),
fd=11
[2010-09-09 16:44:20,452] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2034) - Received OnSocketClose for conn_id: 9 on
handle: 0x292058
[2010-09-09 16:44:20,453] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2730) - Clean up with abort flag: 0, persist close
flag: 0, state: Application Data State, event: Socket Close Event for
conn_id: 9
[2010-09-09 16:44:20,453] com.net.ux.sip.libctl INFO
(TransportTlsSocket.cpp:2776) - TLS Client connection closed for conn_id: 9
on handle: 0x292058, Local Port: 24585, Remote
IP:Port(172.20.250.133:5067), fd=11, current active sockets: 0
[2010-09-09 16:44:20,454] com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2062) - Tls Close CBO=0x28cf30 notified to
application
[2010-09-09 16:44:20,454] com.net.ux.sip DEBUG (TransportLayer.cpp:507) -
CloseCB: Connection closed 0TLS10-24585 socket=0x29205c
connection=0x28cf30.
[2010-09-09 16:44:23,601] com.net.ux.sba WARN (syslogd.cpp:205) -
SymComms.SpawnActionThread: Spawning new thread for action: barSetTime
```

Investigation Path:

- Verify the release level on the Front End server is the same as the SBA release level. All version levels should be 4.0.7577.X

Copyright © 2015 Sonus Networks. All rights reserved.

Failure to automatically import the single base64 encoded file containing bundled certificates

The SBC is not able to import base64-encoded bundled certificates. Follow the steps below to import bundled certificates.

- Open the single file provided by the CA vendor as Read-Only.
- Check to see if the file is readable as base64 or PEM encoded format and that it contains bundled certificates.
    - To verify, this file should contain multiple 'Begin Certificate' and 'End Certificate* header lines.
- Copy the first bundled certificate text including the Begin/End header lines
- Paste the first text to *Copy and Paste* option on the Web UI SBC Certificates page(s) based on few criteria listed below.
    - If the bundled file contains the Sonus SBC Certificate, then paste the first text to the Sonus Certificate page via Import X.509 Signed Certificate action and selection of Copy and Paste mode.
    - If the bundled file contains only the Root Chain certificates, then paste the first text to the Trusted CA Certificates page via Import Trusted CA Certificate action and selection of Copy and Paste mode.
- Copy the next bundled certificate text including the Begin/End header lines. Paste the text to the Trusted CA Certificates page.
- Repeat the last step until all the bundled certificates are successfully imported to the Web UI SBC Certificates page(s) one at a time.

Reference

Exchange Log Error: Target name in the certificate is incorrect

> *The Unified Messaging server was unable to exchange the required certificates to enable Transport Layer Security (TLS) with an IP gateway. More information: "A TLS failure occurred because the target name that was specified in the certificate is incorrect. The error code was "1" and the message was "Incorrect function".*

This is caused by some type of FQDN issue on Exchange:

- Ping the Sonus SBC 1000/2000 from Exchange using the Sonus SBC 1000/2000's FQDN
- Verify the Exchange GW configuration is set for FDQN, not IP.
- Reboot the Exchange Server

X509 Certificate Error Messages

An exhaustive list of the error codes and messages is shown below, this also includes the name of the error code as defined in the header file x509_vfy.h Some of the error codes are defined but never returned: these are described as ``unused''.0 X509_V_OK: okthe operation was successful.

```
2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT: unable to get issuer certificatethe issuer
```

Copyright © 2015 Sonus Networks. All rights reserved.

certificate of a looked up certificate could not be found. This normally means the list of trusted certificates is not complete.
3 X509_V_ERR_UNABLE_TO_GET_CRL: unable to get certificate CRLthe CRL of a certificate could not be found.
4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE: unable to decrypt certificate's signaturethe certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys.
5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE: unable to decrypt CRL's signaturethe CRL signature could not be decrypted: this means that the actual signature value could not be determined rather than it not matching the expected value. Unused.
6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY: unable to decode issuer public keythe public key in the certificate SubjectPublicKeyInfo could not be read.
7 X509_V_ERR_CERT_SIGNATURE_FAILURE: certificate signature failurethe signature of the certificate is invalid.
8 X509_V_ERR_CRL_SIGNATURE_FAILURE: CRL signature failurethe signature of the certificate is invalid.
9 X509_V_ERR_CERT_NOT_YET_VALID: certificate is not yet validthe certificate is not yet valid: the notBefore date is after the current time.
10 X509_V_ERR_CERT_HAS_EXPIRED: certificate has expiredthe certificate has expired: that is the notAfter date is before the current time.
11 X509_V_ERR_CRL_NOT_YET_VALID: CRL is not yet validthe CRL is not yet valid.
12 X509_V_ERR_CRL_HAS_EXPIRED: CRL has expiredthe CRL has expired.
13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD: format error in certificate's notBefore fieldthe certificate notBefore field contains an invalid time.
14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD: format error in certificate's notAfter fieldthe certificate notAfter field contains an invalid time.
15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD: format error in CRL's lastUpdate fieldthe CRL lastUpdate field contains an invalid time.
16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD: format error in CRL's nextUpdate fieldthe CRL nextUpdate field contains an invalid time.
17 X509_V_ERR_OUT_OF_MEM: out of memoryan error occurred trying to allocate memory. This should never happen.
18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT: self signed certificatethe passed certificate is self signed and the same certificate cannot be found in the list of trusted certificates.
19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN: self signed certificate in certificate chainthe certificate chain could be built up using the untrusted certificates but the root could not be found locally.
20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY: unable to get local issuer certificatethe issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.
21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE: unable to verify the first certificateno signatures could be verified because the chain contains only one certificate and it is not self signed.
22 X509_V_ERR_CERT_CHAIN_TOO_LONG: certificate chain too longthe certificate chain length is greater than the supplied maximum depth. Unused.
23 X509_V_ERR_CERT_REVOKED: certificate revokedthe certificate has been revoked.
24 X509_V_ERR_INVALID_CA: invalid CA certificatea CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.
25 X509_V_ERR_PATH_LENGTH_EXCEEDED: path length constraint exceededthe basicConstraints pathlength parameter has been exceeded.
26 X509_V_ERR_INVALID_PURPOSE: unsupported certificate purposethe supplied certificate cannot be used for the specified purpose.
27 X509_V_ERR_CERT_UNTRUSTED: certificate not trustedthe root CA is not marked as trusted for the specified purpose.
28 X509_V_ERR_CERT_REJECTED: certificate rejectedthe root CA is marked to reject the specified purpose.
29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH: subject issuer mismatchthe current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the-issuer_checksoption is set.
30 X509_V_ERR_AKID_SKID_MISMATCH: authority and subject key identifier mismatchthe current candidate issuer certificate was rejected because its subject key identifier

Copyright © 2015 Sonus Networks. All rights reserved.

```
was present and did not match the authority key identifier current certificate. Only
displayed when the-issuer_checksoption is set.
31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH: authority and issuer serial number
mismatchthe current candidate issuer certificate was rejected because its issuer
name and serial number was present and did not match the authority key identifier of
the current certificate. Only displayed when the-issuer_checksoption is set.
32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN:key usage does not include certificate signingthe
current candidate issuer certificate was rejected because its keyUsage extension
does not permit certificate signing.
50 X509_V_ERR_APPLICATION_VERIFICATION: application verification failurean
application specific error. Unused.
```

Alarms and Events Reference

This section details all Sonus SBC 1000/2000 alarms and events. The Sonus SBC 1000/2000 system displays these alarms in the Viewing Alarms and Events and are configured in the Configuring Alarms and Events page.

- Alarm and Event Subsystems
  - User Authentication and Directory Services
  - Resource Manager
  - Licensing
  - Microsoft Survivable Branch Appliance Support
  - Call Routing
  - Common Call Control
  - SIP
  - ISDN
  - Telco Interface Process
  - Media Stream Controller
  - Certificate Security Manager
  - BMP
  - Network Services
  - System Health Monitor
  - CAS
  - Configuration
  - TCA Thresholds
  - FQDN
  - Decode Key Table

Alarm and Event Subsystems

Following list provides the alarms and events defined in various Sonus SBC 1000/2000 subsystems.

User Authentication and Directory Services

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description

Copyright © 2015 Sonus Networks. All rights reserved.

1	1	alarm	AD caching failed	communication	System;Service;IPAddress	minor	✅	• Failed to cache attributes from AD in memory. • Suggested action - try again later. • This alarm will be cleared by event AD caching successful.
1	2	event	Online AD query failed	communication	System;Service			• Failed to execute AD query. • Suggested action - confirm that AD is network reachable, check the AD configuration as well as AD access credentials.
1	4	event	User logged in	security	Username;IPAddress			• New user [username] logged in from [ip address] at [time].
1	5	alarm	User login failed	security	Username;IPAddress	major	✅	• User [username] login failed from [ip address] at [time]. • This alarm will be cleared by event User logged in.
1	6	alarm	AD Unreachable	communication	System:Service;IPAddress; DCType	major	✅	• Either AD is network unreachable, or the AD credentials are invalid. • DCType will be either Authentication or Call Route • This alarm will be cleared by 'AD Reachable' event.
1	7	event	AD Reachable	communication	System:Service;IPAddress; DCType			• Active directory is now reachable. • DCType will be either Authentication or Call Route
1	8	event	AD caching successful	communication	System:Service;IPAddress			• AD caching was successful.
1	9	alarm	AD backup failed	equipment	System:Service;IPAddress	minor	✅	• Failed to backup cached values from AD to storage device. • Either the storage device is not present, or it is full. • Contact Sonus TAC for further assistance.
1	10	event	AD successfully backed up	equipment	System:Service;IPAddress			• Successful backup of cached values from AD to storage device.
1	11	alarm	AD cache truncated	equipment	System:Service	minor		• AD Cache is truncated, AD cache results have exceeded the maximum cache size. • Consider caching only the required attributes. • If the query is not found in cache, Online query will be performed, while affecting performance.
1	12	alarm	RADIUS Server Unreachable	communication	System:Service;IPAddress	major	✅	• Either the RADIUS server is network unreachable, or the configuration is incorrect. • Suggested action - check shared secret, listening port, RADIUS server IP. • This alarm will be cleared by 'RADIUS Reachable' event.
1	13	event	RADIUS Reachable	communication	System:Service;IPAddress			• RADIUS server is online.
1	14	alarm	CDR logging failed	communication	System:Service;IPAddress	major		• Sonus SBC 1000/2000 failed to send CDR to RADIUS based accounting server. • Either the RADIUS server is network unreachable, or the configuration is incorrect. • Suggested action - check shared secret, listening port, RADIUS server IP.
1	15	alarm	CDR backup failed	communication	System:Service;IPAddress	major		• Sonus SBC 1000/2000 failed to backup CDR in local file. • Either running with low disk space or CDR backup maximum limit is crossed. • Suggested action - Free up the disk space or save the CDR Queued file for future reference.
1	17	event	User password changed successfully	Security	Username			• Logged any time password is changed by specified user or an administrator. • Event Text: User 'username' password changed successfully by 'username' from 'IP address'. ℹ If not preceded by a password expired event, this was a voluntary password change.

Copyright © 2015 Sonus Networks. All rights reserved.

1	18	alarm	User password change failed	Security	Username	warning	✅	• Logged any time an attempted password change failed by specified user or an administrator. • Event Text: User 'username' password change attempted by 'username' from 'IP address" failed. • Cleared by event 1.17 - User password changed successfully. ℹ If not preceded by a password expired event, this was a voluntary password change.
1	19	event	User account disabled	Security	Username			• Event Text: User 'username' account has been disabled by 'username' from 'IP address'.
1	20	event	User account activated	Security	Username			• Event Text: User 'username' account has been activated by 'username' from 'IP address'.
1	21	event	Global Security Options Changed	Security	Username;IPAddress			• Event Text: Global security options changed by 'username' from 'IP address'.
1	22	alarm	User login blocked	Security	Username	major	✅	• Event Text: User 'username' blocked from login due to excessive incorrect login attempts. • Cleared by event 1.23 - User login unblocked.
1	23	event	User login unblocked	Security	Username			• Event Text: User 'username' unblocked.
1	24	event	User password expired	Security	Username;IPAddress			• Password has expired.
1	25	alarm	AD: Maximum Threads Exceeded	Processing	System;Service	major		• AD has reached maximum threads. Please inform your service representative.

Resource Manager

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
2	1	alarm	Invalid Card ID EEPROM Data	equipment	System;Card	critical		• A Card was detected with invalid Card ID EEPROM contents (failed CRC-CCITT check). • Suggested action - provide the entire alarm message including the numbers at the end to Sonus TAC for further assistance.
2	2	alarm	Card Health Check Failed	equipment	System;Card	critical		• During Line Card activation, a Card Fault was detected after power was applied to the card. • The Card will remain out-of-service. • Suggested action - reboot system. • If issue persists, contact Sonus TAC with the alarm information.
2	3	alarm	Card not Supported	equipment	System;Card	major		• A Card was detected which can be identified, but the Sonus SBC 1000/2000 system software is unable to support. • The Card will remain out-of-service. • Suggested action - reboot system. • If issue persists, contact Sonus TAC with the alarm information.
2	4	alarm	Power Supply input failure	equipment	System;PSU	major	✅	• A Power supply module has indicated a failure of input power. • The Sonus SBC 1000/2000 System has lost Power Supply redundancy. • Suggested action - Verify that the power cable is connected and that the PS is functioning properly.
2	5	event	Power Supply input restored	equipment	System;PSU			• A Power Supply module has indicated that input power has been restored. • This event clears the "Power Supply Input Failure" Alarm.
2	6	alarm	Power Supply output failure	equipment	System;PSU	major		• A Power Supply module has indicated a failure of output power. • The Sonus SBC 1000/2000 System has lost Power Supply redundancy. • Suggested action - Verify that the PS is functioning properly.

Copyright © 2015 Sonus Networks. All rights reserved.

2	7	alarm	Single Fan failure	equipment	System;Fan	major		• Check the System tab to find the Fan ID of the failed fan. • Contact Sonus TAC with this information.
2	8	alarm	Multiple Fan Failures	equipment	System;Fans	critical		• Check the System tab to find the Fan ID's of the failed fans. • Contact Sonus TAC with this information.
2	9	alarm	System Temperature Warm	equipment	System	minor	✅	• The temperature sensors have indicated that the system is running warm (65°C threshold).
2	10	event	System Temperature Warm Cleared	equipment	System			• The temperature sensors have indicated that the system is NO LONGER running warm (55°C threshold). • This event clears the "System Temperature Warm" Alarm.
2	11	alarm	System Temperature Hot	equipment	System	critical	✅	• The temperature sensors have indicated that system is running hot.
2	12	event	System Temperature Hot Cleared	equipment	System			• The temperature sensors have indicated that the system is NO LONGER running hot (65°C threshold). • This event clears the "System Temperature Hot" Alarm.

Licensing

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
3	1	alarm	Licenses expired.	general	System;Service	critical	✅	• License of the node has expired, all the licensed features would fail to work. • Contact Sonus Sales.
3	2	alarm	License expires in 2 weeks.	general	System;Service	major	✅	• License of the node will expire in 2 weeks.
3	3	event	New License applied.	general	System;Service			• New License is applied on the node.
3	4	alarm	Failed to Apply License.	general	System;Service	critical		• Either an invalid key is used, or the license key applies to a different node, or the license key expiry is past the present date. • Contact Sonus Sales to obtain a new license.
3	5	alarm	Failed to acquire license.	general	System;Service	critical		• The alarm is generated when the required license is not available. • Check the number of licensed SIP or TDM channels, the number of SIP registrations, SBA, Transcoding or AD. • Suggested action - obtain license for missing functionality.
3	6	alarm	Licensed DS1 ports exceed installed ports.	general	System;Service	critical		• This alarm is generated when the license key applied has more TDM ports licensed than are installed in the system. As a fix, obtain license with correct number of TDM ports.
3	7	alarm	Licensed BRI ports exceeds installed ports.	general	System;Service	minor		• The alarm is generated when the license key applied has more BRI ports licensed than are installed in the system. The number of BRI ports installed will get activated. As a fix, obtain a license with the correct number of BRI ports.
3	8	alarm	Licensed FXS ports exceeds installed ports.	general	System;Service	minor		• The alarm is generated when the license key applied has more FXS ports licensed than are installed in the system. The number of FXS ports installed will get activated. As a fix, obtain a license with the correct number of FXS ports.
3	9	alarm	Licensed FXO ports exceeds installed ports.	general	System;Service	minor		• The alarm is generated when the license key applied has more FXO ports licensed than are installed in the system. the number of FXO ports installed will get activated. As a fix, obtain a license with the correct number of FXO ports.

Microsoft Survivable Branch Appliance Support

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description

Copyright © 2015 Sonus Networks. All rights reserved.

5	1	alarm	ASM Unreachable	communication	SBA Instance	critical	✅	• ASM system can not be reached, system is down. • Check whether the ASM is rebooting.
5	2	event	Clear ASM Unreachable	communication	SBA Instance			• Clears alarm 'ASM Unreachable'.
5	3	alarm	ASM Failure Recovered	equipment	SBA Instance	minor		• ASM system was previously unreachable, but has come up. • This alarm doesn't autoclear so the user can investigate the cause, but the system should be working correctly now.
5	4	alarm	ASM Services Not Running	processing	SBA Instance	critical	✅	• ASM services are not running, calls through the ASM cannot be placed.
5	5	event	Clear ASM Services Not Running	processing	SBA Instance			• Clears alarm 'ASM Services Not Running'.
5	6	alarm	ASM Services Restarted	processing	SBA Instance	minor		• ASM Services was previously stopped, but has started. This alarm doesn't autoclear so the user can investigate the cause, but ASM Services should be working correctly now.
5	7	alarm	ASM Service Restart Failed	processing	SBA Instance	critical		• The system attempted to restart a failed service on the ASM, service did not start successfully. • User interaction is required.
5	8	event	ASM System Started	processing	SBA Instance			• This event is set when the SBA communication system is first established, and usually indicates that the Application Solution Module (ASM) has finished booting. • It should come up at system startup, it may come again if the ASM hardware is rebooted.
5	9	event	ASM System Shutting down	processing	SBA Instance			• A planned or deliberate shut down is taking place on the Application Solution Module (ASM).
5	10	alarm	Ethernet Link Down	equipment	SBA Instance;Port	major	✅	• Ethernet port specified has lost link. • Source Instance: Eth0/Eth1 via SBA Monitor.
5	11	event	Ethernet Link Up	equipment	SBA Instance			• Ethernet port specific has recovered link.
5	12	alarm	ASM-SBC IP Subnet Mismatch	equipment	SBA Instance	critical	✅	• The ASM and Sonus SBC IP interfaces are in different subnets and cannot communicate.
5	13	event	ASM-SBC IP Subnet Match	equipment	SBA Instance			• The ASM and Sonus SBC IP interfaces are in the same subnet and can now communicate.
5	14	alarm	ASM-QoE SQL database is unreachable	communication	SBA Instance	major	✅	• The QoE database is unreachable from ASM, make sure the Lync Server 2013 is deployed and Monitoring database is running.
5	15	event	Clear ASM-QoE SQL database is unreachable	equipment	SBA Instance			• The QoE database is now reachable from ASM.
5	16	alarm	ASM-failed to store QoE information	equipment	SBA Instance	critical		• Failed to store the QoE information from ASM.
5	17	alarm	ASM-SBC CAC Update Failed	equipment	SBA Instance	major	✅	• The ASM hasn't been able to apply the CAC update.
5	18	event	Clear ASM-SBC CAC Update Failed	equipment	SBA Instance			• Clear alarm "The ASM hasn't been able to apply the CAC Update".

Call Routing

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description

Copyright © 2015 Sonus Networks. All rights reserved.

7	1	event	Configuration change occurred on Action Set	general	ActSetTble			• There is an action set table number/name that should be printed with this event.
7	2	event	Configuration change occurred on Normalization Table	general	NormTble			• There is a normalization table number/name that should be printed with this event.
7	3	event	Configuration change occurred on Route Table	general	RtTble			• There is a route table number/name that should be printed with this event.
7	4	event	Configuration change occurred on Transformation Tables	general	TransTble			• There is a transformation table number/name that should be printed with this event.
7	5	alarm	Route temporarily disabled	communication	RtTble	warning	✅	• This alarm is set if a link is down or some other event has occured to take a route entry out of service.
7	6	event	Route enabled	communication	RtTble			• Route came up.
7	7	alarm	A Call exceeded the limit for number of destinations	communication	CallDest	warning		• A call with destination of X tried to be forked more than the limit allows (currently 8).
7	8	alarm	Call forking used with no forking license	communication	CallDest	warning		• A call with a destination of X was forked with no forking license available.
7	9	alarm	Invocation of InvokeActionSet exceeded the maximum nesting limit	communication	CallDest	warning		• A call with with destination of X tried to execute InvokeActionSet more the the limit allows (currently 10).
7	10	event	Configuration change occurred on Callback Tables	general	CallbackTble			• There is a PSAP Callback table number/name that should be printed with this event.

Common Call Control

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
8	1	event	Channel is in service	communication	Card;Port;Channel			• Channel is up and is in service. • This clears the 'Channel out of service' alarm.
8	2	alarm	Channel is out of service	communication	Card;Port;Channel	minor	✅	• Channel Out Of Service Alarm. • This alarm is automatically cleared when Channel is in service.
8	3	alarm	Emergency Call Attempted	communication	Number;Extension;IPAddress	minor	✅	• Emergency Call is Attempted from Calling Number, Calling Extension, Caller IP address.
8	4	event	Emergency Call Attempted	communication	Number;Extension;IPAddress			• Emergency Call Alarm will be cleared after expiry time in emergency status table.
8	5	alarm	QoE report not sent due to RTCP Media List	communication	SG	minor		• Generated when the Media List does not have RTCP-XR configuration enabled.
8	6	event	Call Transfer failed due to call not being in RTP mode	communication	Card;Port;Channel			• The call is not in RTP mode hence the call transfer could not be honored.
8	7	event	Call Attempt failed due to Media Mode mismatch	communication	Card;Port;Channel			• The call failed due to Media Mode mismatch across SG and Call Route configuration.
8	8	alarm	All calls have been drained on this Signaling Group	communication	SG	Warning		

SIP

Copyright © 2015 Sonus Networks. All rights reserved.

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
9	1	alarm	SIP Server not responding	communication	SIPCluster;ServID;Protocol;IPAddress;Port	major	✅	• SIP server has failed to respond and has been taken out of service. • This alarm will be cleared by the event 'SIP server became responsive'.
9	2	alarm	Signaling Group taken out of service	communication	SG	critical	✅	• All servers in SG have failed. • This alarm will be cleared by 'SIP Signaling group enabled' event.
9	3	event	Signaling Group disabled	communication	SG			• Configuration action has changed this Signaling Group from Enabled to Disabled.
9	4	alarm	SIP-TLS Server Handshake Failure	security	TLSProfile;IPAddress	minor		• TLS server handshake failed with alert code. Action: Refer to Error Alerts in RFC 5246 for the problem.
9	5	alarm	SIP-TLS Handshake Inactivity Timeout Failure	security	TLSProfile;IPAddress	minor		
9	6	alarm	Configured port number mismatch	processing	SG;IPAddress;Port	minor		• Discrepancy of an FQDN/Port configured in the SipServer object that is different than the DNS SRV lookup. • A DNS SRV record can return the port number for the selected protocol. • The DNS SRV port value will take priority over the configured port.
9	7	event	SIP Server became responsive	communication	SIPCluster;ServID;Protocol;IPAddress;Port			• SIP server came up.
9	8	alarm	SIP cluster went down	communication	SIPCluster	major	✅	• SIP cluster went down. • This is due to all the servers in the clusters are not responsive. • This alarm will be cleared by the event 'Sip cluster enabled'.
9	9	event	SIP Cluster enabled	communication	SIPCluster			• SIP cluster enabled.
9	10	event	SIP Signaling group enabled	communication	SG			• SIP Signaling group enabled.
9	11	alarm	SIP Signaling group: DNS failure	communication	SG	major	✅	• Failed to resolve the FQDN entries in the SIP Signaling Group. Suggested action - confirm the FQDNs, and confirm DNS access.
9	12	event	SIP Signaling Group; FQDN resolved	communication	SG			• Successfully resolved the FQDN of the SIP Signaling group.
9	13	alarm	SIP Server; DNS failure.	communication	SIPCluster;ServID	major	✅	• Failed to resolve the SIP server FQDN entries in the SIP Server table. • Suggested action - check the FQDN syntax.
9	14	event	SIP Server; FQDN resolved	communication	SIPCluster;ServID			• SIP Server config FQDN resolved.
9	15	alarm	SIP call session DNS failure	communication	SG	major		• Failed to resolve an FQDN with DNS server during a SIP call session.

Copyright © 2015 Sonus Networks. All rights reserved.

9	16	alarm	Acquiring license for Register failed	communication	SG	major		• Failed to acquire license from License Manager.
9	17	alarm	Session leak or some other resource leak	communication	SG	major		• SIP performs self-check for leaks. Please enable logging for sip and issue "show resources" command.
9	18	alarm	Failed to bind to network interface	communication	SG	minor	✅	• Failed to bind to network interface due to dynamic IP address not available.
9	19	event	Successfully bound to network interface	communication	SG			• Successfully bound to network interface. DHCP lease renewed.
9	20	alarm	SIP Register Server not responding	communication	SIPCluster;ServID;Protocol;IPAddress;Port	major	✅	• SIP Register server has failed to respond. This alarm will be cleared by the event "SIP Regular server became responsive".
9	21	event	SIP Register Server became unresponsive	communication	SIPCluster;ServID;Protocol;IPAddress;Port			• SIP Register server came up.
9	22	alarm	Registration not valid; received stale=false	communication	SIPCluster;ServID;Protocol;IPAddress;Port	major	✅	• Server has sent stale=false. Contact is not Registered.
9	23	event	Config change for SIP endpoint that received stale=false	communication	SG;AorName			• Endpoint which had Stale is False has config change.
9	24	alarm	QoE Notify Message was not successful	communication	SIPCluster;ServID;Protocol;IPAddress;Port	minor	✅	• QoE Notify Message Response was not successful"/" QoE Notify Message received a no response or a failed response. This alarm is cleared by the event 'QoE Notify Message received a successful response'."
9	25	event	QoE Notify Message Response was successful	communication	SG		✅	• QOE Notify Message received a successful response.
9	26	alarm	SIP overload detected	communication	System;Service	minor	✅	• SIP application session processing is overloaded.
9	27	event	SIP overload cleared	communication	System;Service			• SIP application session processing resumes to normal operation, overload cleared.
9	28	alarm	SIP maximum sessions per SG reached	communication	SG	minor	✅	• The maximum number of SIP sessions (calls/register/subscribe) has been reached on the signaling group. Increase the number of SIP Channels for the signaling group.

Copyright © 2015 Sonus Networks. All rights reserved.

9	29	event	Maximum Number of SIP Sessions Alarm Cleared	communication	SG			• SIP sessions per signaling group is under the maximum limit.
9	30	alarm	Error resolving SRV record	communication	SIPCluster;ServID	major	✅	• Failed to execute SRV record query. Suggested action - confirm that DNS server network is reachable, check SRV and DNS server configuration.
9	31	event	SRV record resolved	communication	SIPCluster;ServID	none		• DNS server returned valid SRV record(s).
9	32	alarm	SIP-TLS Handshake Negotiation Start Failure	security	TLSProfile;IPAddress	critical	✅	• Handshake failed due to start with invalid certificate. Action: Import a valid signed Sonus SBC Certificate on local and/or remote gateway.
9	33	event	SIP-TLS Handshake Negotiation Start Successful	security	TLSProfile;IPAddress	none	✅	• Handshake response was started with valid certificate on local and remote gateway. This event clears the 'SIP-TLS Handshake Negotiation Start Failure' alarm.
9	34	event	Maximum supported SIP SGs reached	General	System;Service	warning	✅	• SIP signaling group count reached maximum supported limit.
9	35	event	Maximum supported SIP SGs cleared	General	System;Service	none		• SIP signaling group count is under the maximum supported
9	36	alarm	Maximum non-SIP call sessions reached	General	System; Service	warning	✅	• Number of SIP non-call sessions is over the system capacity
9	37	event	Maximum non-SIP call Sessions cleared	General	System:Service	none		• Number of SIP non-call sessions is under the system capacity
9	38	alarm	Maximum SIP call sessions reached	General	System;Service	warning	✅	• Number of SIP call sessions is over the system capacity
9	39	event	Maximum SIP call sessions cleared	General	System.Service	none		• Number of SIP call sessions is under the system capacity
9	40	Alarm	Broadsoft SIP call re-routed	General	SG	warning	✅	• Broadsoft SIP call re-routed
9	41	event	Broadsoft SIP Call Re-routed cleared	General	SG	none		• Number of SIP Call Sessions is under the system capacity.
9	42	alarm	SIP SG Listen Protocol and SIP Server Host Protocol mismatch	Processing	SIPCluster;ServerID	minor		• Verify that the listen ports and protocols for the SG match those in the server table.
9	43	alarm	Configuration Error: SIP SG and Server Protocol Mismatch	Processing	SIPCluster;ServerID	major		• Verify that the listen ports and protocols for the SG match those in the server table.
9	44	alarm	SIP-TLS Client Handshake Failure	Security	TLSProfile;IPAddress	minor	✅	• TLS client handshake failed with alert code. Action: Refer to Error Alerts in RFC 5246 for the problem.
9	45	event	SIP-TLS Handshake Inactivity Timeout Closed	Security	TLSProfile;IPAddress			• Handshake response was received within specified timeout. This event clears the 'SIP-TLS Handshake Inactivity Timeout Failure' alarm.

Copyright © 2015 Sonus Networks. All rights reserved.

9	46	event	SIP-TLS Server Handshake Failure Cleared	Security	TLSProfile;IPAddress			• Handshake failure error alert condition was cleared. This event clears the 'SIP-TLS Server Handshake Failure' alarm.
9	47	event	SIP-TLS Client Handshake Failure Cleared	Security	TLSProfile;IPAddress			• Handshake failure error alert condition was cleared. This event clears the 'SIP-TLS Client Handshake Failure' alarm.

ISDN

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
10	1	alarm	D-Channel down	communication	Card;Port	critical	✅	• The data link layer of the port has come down.
10	2	event	D-Channel up	communication	Card;Port			• The data link layer of the port has come back up.
10	3	alarm	Call released due to channel restart by far end	communication	Card;Port;Channel	minor		• Call released as the ISDN channel has been restarted by far end.

Telco Interface Process

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
11	1	alarm	Port disabled by operator	communication	Card;Port	major	✅	• The physical layer of the port has been brought down by the operator.
11	2	event	Port enabled by operator	communication	Card;Port			• The physical layer of the port has been brought back up by the operator.
11	3	alarm	DS1 Loopback Enter	communication	Card;Port	critical	✅	• The DS1 has been put into a loopback state by the operator.
11	4	event	DS1 Loopback Exit	communication	Card;Port			• The DS1 has been taken out of the loopback state by the operator.
11	5	alarm	Red Alarm - Loss of Signal	communication	Card;Port	critical	✅	• The physical layer has detected a Red (LOS) alarm.
11	6	event	Red Alarm - Loss of Signal cleared	communication	Card;Port			• The physical layer has detected a Red (LOS) alarm clearing.
11	7	alarm	Red Alarm - Loss of Frame	communication	Card;Port	critical	✅	• The physical layer has detected a Red (LOF) alarm.
11	8	event	Red Alarm - Loss of Frame cleared	communication	Card;Port			• The physical layer has detected a Red (LOF) alarm clearing.
11	9	alarm	Blue Alarm	communication	Card;Port	critical	✅	• The physical layer has detected a blue alarm.
11	10	event	Blue Alarm Cleared	communication	Card;Port			• The physical layer has detected an alarm clearing.
11	11	alarm	Yellow Alarm	communication	Card;Port	critical	✅	• The physical layer has detected an yellow alarm. • This can be originated because of an alarm assert issued by operator or a detection of alarm condition from far end.
11	12	event	Yellow Alarm Cleared	communication	Card;Port			• The physical layer has detected an yellow alarm clear.

Copyright © 2015 Sonus Networks. All rights reserved.

11	13	alarm	Port disabled as port not found on DS1	communication	Card;Port	critical		• This alarm is generated to indicate that a port which was present in the UI is now marked as disabled because the corresponding port was not present on the DS1 physical hardware.
11	14	alarm	Clock recovery switched to port configured as secondary	communication	System	critical	✅	• This alarm is generated to indicate that the primary port from which clock was being recovered has gone down and so clock recovery is now being performed on the secondary port.
11	15	event	Clock recovery switchover to secondary port cleared	communication	System			• This event is generated to indicate that the primary port from which clock was being recovered is back in operation and so clock recovery is now being performed on the primary port.
11	16	alarm	Clock recovery switched to freerun clock	communication	System	critical	✅	• This alarm is generated to indicate that the primary and secondary ports from which clock was being recovered have gone down and so clock recovery is now being performed internally from oscillator holdover clock.
11	17	event	Clock recovery switchover to freerun clock cleared	communication	System			• This event is generated to indicate that either the primary or secondary port from which clock was being recovered is back in-service, so clock will be recovered from the in-service port instead of the oscillator holdover clock.
11	18	alarm	Line card not detected	communication	Card	warning	✅	• Line card not detected.
11	19	event	Line card detected	communication	Card			• Line card detected.
11	20	alarm	Port disabled for relay passthrough state activation	communication	Card;Port	warning	✅	• Port disabled because the corresponding port is activated for relay passthrough state.
11	21	event	Port enabled for relay online state activation	communication	Card;Port			• Port enabled because the corresponding port is re-activated for relay online state.
11	22	alarm	Layer 1 down	communication	Card;Port	critical	✅	• The physical layer has detected layer 1 down due to state conditions that results in non-operational state of the BRI port. • The physical layer state as per I. • 430 specification can be found in the UI Port View for troubleshooting.
11	23	event	Layer 1 up	communication	Card;Port			• The physical layer 1 down alarm is cleared with operational state of the BRI port.
11	24	alarm	Port disabled as port not found on analog card	communication	Card;Port	critical		• Port is now marked as disabled because the corresponding port was not present on the analog physical hardware.
11	25	alarm	Ports disabled for relay pass through state change on analog relay card pairs	communication	System;Card;Card	warning	✅	• Ports are now marked as disabled for activated relay passthrough state on analog FXS/FXO card pair.
11	26	event	Ports enabled for relay online state change on analog relay card pairs	communication	System;Card;Card			• Ports are now marked as enabled for activated relay passthrough state on analog FXS/FXO card pair.
11	27	alarm	Port status down detected	communication	Card;Port	warning	✅	• Line down condition detected.
11	28	event	Port status up	communication	Card;Port			• Line down condition cleared.
11	29	alarm	Port disabled as port not found on BRI	communication	Card;Port	critical		• This alarm is generated to indicate that a port which was present in the UI is now marked as disabled because the corresponding port was not present on the BRI physical hardware.
11	30	alarm	System not operational	communication	System	critical		• System not operational because DSP cannot be initialized. • Contact Sonus TAC with the information in this alarm.

Copyright © 2015 Sonus Networks. All rights reserved.

11	31	alarm	DS1 sync failure	communication	Card;Port	critical	✅	DS1 sync failure could be due to mismatching line configuration. Suggested Action: Disable "Admin State" of unused ports to avoid performance impact.
11	32	event	DS1 sync failure cleared	communication	Card;Port			DS1 sync failure cleared.

Media Stream Controller

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
12	1	alarm	DSP not coming up	equipment	DSP	critical	✅	• This alarm will be generated if a DSP cannot be initialized. • If the DSP does not come up, contact Sonus TAC with the information in this alarm.
12	2	alarm	DSP reset	equipment	DSP	major	✅	• This alarm will be generated if a DSP encounters a fatal error condition and has to be reinitialized.
12	3	event	DSP Card is UP	equipment	Card			• This event will clear the 'DSP not coming up' and 'DSP reset' alarms.
12	4	event	DSP Channel Failure	processing	Card;Port;Channel			• This event will be generated if a DSP channel encounters a fatal error condition and has to be closed.
12	5	alarm	RTP/RTCP Port Range Invalid	equipment	System	critical	✅	• This alarm is generated if a RTP/RTCP port is found to be invalid. The conflicting port is skipped, however, this condition should be resolved by reconfiguring the RTP/RTCP Port Range under Media System Configuration.
12	6	event	RTP/RTCP Port Range Invalid Cleared	equipment	System			• This event will clear the "RTP/RTCP Port Range Invalid" alarm.

Certificate Security Manager

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
13	1	alarm	TLS Own Server Certificate will Expire	security	CertificateCommonName	major	✅	• The Server certificate will expire in a window time. • Suggested Action: Generate, Export CSR and Import a new signed certificate.
13	2	alarm	TLS Own Server Certificate has Expired	security	CertificateCommonName	critical	✅	• The Server certificate has expired. • Suggested Action. • Generate, Export CSR and Import a new signed certificate.
13	4	alarm	TLS Self Sign Certificate Generation Failed	security	CertificateCommonName	critical		• Failed to create a default self signed certificate on the system.
13	5	event	New and Valid TLS Own Server Certificate Detected	security	CertificateCommonName			• The Server certificate was uploaded, validated, and good to use in successfully establishing a TLS connection.
13	6	alarm	TLS Trusted Certificate Authority will Expire	security	CertificateCommonName	major	✅	• The Trusted CA Certificate will expire in a window time. Suggested Action: Import a new trusted CA certificate.
13	7	alarm	TLS Trusted Certificate Authority has Expired	security	CertificateCommonName	critical	✅	• The Trusted CA Certificate has expired. Import a new trusted CA certificate.
13	8	event	TLS Trusted Certificate Authority was Deleted	security	CertificateCommonName			• The Trusted Certificate Authority is successfully deleted due to the expired or expiring soon validity status.
13	9	alarm	TLS Own Server Certificate Expiry Notice	security	CertificateCommonName	minor	✅	• The Server certificate will expire in a window time. Suggestion Action: Generate, Export CSR and Import a new signed certificate.

Copyright © 2015 Sonus Networks. All rights reserved.

13	10	alarm	TLS Trusted Certificate Authority Expiry Notice	security	CertificateCommonName	minor	✅	• The Trusted CA certificate will expire in a window time. Suggestion Action: Import a new trusted CA certificate.

BMP

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
14	1	alarm	Invalid Session for attempted realtime connection	security	IPAddress			• Invalid Session for attempted realtime connection.
14	2	alarm	BMP-TLS Handshake Alert Failure	security	IPAddress	minor		• This alarm will be generated if TLS Connection failed with an Alert. • The connection associated with a TLS Connection ID is aborted.
14	3	alarm	BMP-TLS Handshake Inactivity Timeout Failure	security	IPAddress	minor		• This alarm will be generated if there was long period of inactivity during exchange of handshake messages for an associated TLS Connection ID.

Network Services

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
15	1	alarm	Interface oper down	communication	Port	major	✅	• Occurs when an Ethernet port (of ports 1, 2, 3 and 4) is operationally down (e.g. cable unplugged, mismatched speed/duplexity settings) and if admin-status is ADMIN_UP. • The alarm is automatically cleared when the interface returns to working condition or when the admin-status is configured to be ADMIN-DOWN. • Is generated only on Sonus SBC 2000 platform. • This alarm is not generated on the Sonus SBC 1000 platform (See ID: 15, Sub-ID: 7 in this table). • The operator should check the physical cabling of the port that has this condition and verify the speed and duplexity settings on Sonus SBC 1000/2000 and on the device connected to the other end of the Ethernet cable. • If the alarm is reported on an unused port, the admin-status of the unused port should be configured as "ADMIN-DOWN".
15	2	event	Interface oper up	communication	Port			• Is generated when an Ethernet port (of ports 1, 2, 3 and 4) becomes operationally up. • This event automatically clears the "Interface oper down" alarm.
15	3	event	Interface admin up	communication	LogicalInterface			• Is generated when the admin-status of the Port or Logical Interface is configured to be ADMIN-UP. • Is applicable to Sonus SBC 2000 platform only.
15	4	event	Interface admin down	communication	LogicalInterface			• Is generated when the admin-status of the Port or Logical Interface is configured to be ADMIN-DOWN. • Is applicable to Sonus SBC 2000 platform only.
15	5	event	Admin Port oper down	communication	Port			• Is generated when the Admin Port is operationally down (e.g. cable unplugged, mismatched duplex/speed settings). • Is applicable to Sonus SBC 2000 platform only. • The operator should check the physical cabling of the port that has this condition and verify the speed and duplexity settings on Sonus SBC 1000/2000 and on the device connected to the other end of the Ethernet cable. • It is very common and typical for Sonus SBC 2000 to leave the ADMIN-PORT unconnected and hence this condition is reported as an event and not an alarm.
15	6	event	Admin Port oper up	communication	Port			• Is generated with the port becomes operational after being in an *Admin port oper down* state. • Is applicable to Sonus SBC 2000 platform only.

Copyright © 2015 Sonus Networks. All rights reserved.

15	7	event	Port oper down	communication	Port			• Occurs when an Ethernet port (of ports 1 and 2) is operationally down (e.g. cable unplugged, mismatched speed/duplexity settings). • Is generated only on Sonus SBC 1000 platform. • The same conditions are reported as alarm (ID: 15, Sub-ID: 1) on Sonus SBC 2000 platform. • When this event occurs (noticed as a trap), operator should check the physical cabling of the port that has this condition and verify the speed and duplexity settings on Sonus SBC 1000/2000 and on the device connected to the other end of the Ethernet cable.
15	8	event	RIP license not enabled	communication	System			• RIP feature license is not enabled.
15	9	event	OSPF license not enabled	communication	System			• OSPF feature license is not enabled.
15	10	alarm	Link Monitor Peer down	communication	IPAddress	major	✅	• Generated when a Gateway or host is declared down.
15	11	event	Link Monitor Peer ready	communication	IPAddress	event	✅	• Is generated when a gateway or host is ceclared to be ready for service. It clears the Peer Down alarm.
15	12	event	Tunnel connection disabled by operator	communication	NetworkName			• Tunnel connection is placed Out of Service by operator.
15	13	event	Tunnel connection enabled by operator	communication	NetworkName			• Tunnel connection is placed Back in Service by operator.
15	14	alarm	Tunnel Link Lost	communication	NetworkName	critical	✅	• Tunnel lost communication with the peer. This alarm will be cleared by the "Tunnel link restored" event.
15	15	event	Tunnel Link Restored	communication	NetworkName			• Tunnel is successfully re-established with the peer.
15	16	event	IPsec license not enabled	communication	System			• IPsec license is not enabled.
15	17	alarm	Negotiated Duplexity Half	communication	Port	warning	✅	• Port negotiated duplexity is half. This degrades the performance.
15	18	event	Negotiated Duplexity Full	communication	Port			• Port negotiation duplexity is back to full.
15	19	alarm	Preferred Link down	communication	IP address	critical	✅	• Is generated when the preferred Link is down.
15	20	event	Preferred Link Ready	communication	IP address	event		• Is generated when the preferred link is ready for service. This clears the Preferred Link down alarm.
15	21	alarm	Tunnel Notification failure	communication	NetworkName	critical		• Is generated when Tunnel negotiation failed.
15	22	event	Tunnel local subnet(s) are non-negotiable	communication	NetworkName	event		• Is generated when one or more local subnet(s) failed negotiation as a result of peer config mismatch.
15	23	event	Tunnel remote subnet(s) are non-negotiable	communication	NetworkName	event		• Is generated when one or more remote subnet(s) failed negotiation as a result of peer config mismatch.
15	24	event	Port State Learning	communication	MSTPInstance;Port	event		• Is generated when a Port State is Learning in a Multiple Spanning Tree Instance.

Copyright © 2015 Sonus Networks. All rights reserved.

15	25	event	Port State Forwarding	communication	MSTPInstance;Port	event		• Is generated when a Port State is Forwarding in a Mulitple Spanning Tree Instance.
15	26	event	Port State Discarding	communication	MSTPinstance;Port	event		• Is generated when a Port State is Discarding in a Multiple Spanning Tree Instance.

System Health Monitor

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
16	1	alarm	Application Service restarted	processing	Service	major		• A Sonus SBC 1000/2000 Application service was restarted.
16	2	alarm	Active partition switched	processing	Partition	major		• System detected a problem during previous boot cycle, active partition has switched automatically. • Suggested action - backup the configuration and re-apply the upgrade to the currently inactive partition.
16	3	alarm	Failed to mount partition	processing	Partition	major		• While booting, one of the partition could not be mounted. • Likely a eUSB corruption. • Contact Sonus TAC with the information in this alarm.
16	4	alarm	Failed to set active partition	processing	Partition	major		• Failed to set active partition. • Contact Sonus TAC with the information in this alarm.
16	5	alarm	Attempt to repair boot parameter mismatch failed.	processing	Partition	major		• Attempt to auto repair boot parmeters failed. • Contact Sonus TAC with the information in this alarm.
16	6	alarm	Failed to mount partition	processing	Partition	major		• Boot parameter mismatch was detected. • Attempting to auto repair.
16	7	alarm	Failed Power-on memory self test	equipment	Partition	critical		• Power-on self test failure.
16	8	alarm	Failed Power-on Core Switch test	equipment	Partition	critical		• Power-on self test failure.
16	9	alarm	Failed Power-on Secondary Switch test	equipment	Partition	critical		• Power-on self test failure.
16	10	alarm	Failed Power-on external Quad PHY test	equipment	Partition	critical		• Power-on self test failure.
16	11	alarm	Failed Power-on external Single PHY test	equipment	Partition	critical		• Power-on self test failure.
16	12	alarm	Failed Power-on CPU PHY test	equipment	Partition	critical		• Power-on self test failure.
16	13	alarm	Failed Power-on TSI test	equipment	Partition	critical		• Power-on self test failure.
16	14	alarm	Failed Power-on internal 5-Port PHY test	equipment	Partition	critical		• Power-on self test failure.
16	15	event	System Up After Planned Restart	equipment	System			• System up after planned restart

Copyright © 2015 Sonus Networks. All rights reserved.

16	16	alarm	System Up After Unplanned Restart	equipment	System	major		• System up after unplanned restart.
16	17	alarm	Entered password recovery mode	security	System	major		• SBC has entered password recovery mode.
16	18	event	Exited password recovery mode	security	system			• SBC has exited password recovery mode.
16	19	alarm	Failed to mount USB storage device	equipment	System;Service	major		• SBC discovered USB storage. SBC can mount flash drives formatted with FAT32 file system only.
16	20	event	USB storage device connected	equipment	System;Service			• USB storge device is connected.
16	21	Alarm	USB storage device disconnected	equipment	System;Service	warning		• USB storge device is disconnected. This alarm is cleared when USB drive is connected.
16	22	Alarm	Critical application crash	almProcessing	Service	critical		• A Critical Sonus SBC application has crashed, system will be restarted. Contact Sonus TAC with the information in this alarm and all core files present on the system. Core files can be found in Diagnostics->Restart Report under the 'Core Files' tab.

CAS

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
17	1	alarm	No response	communication	Card;Port;Channel	major	✅	• No response to seizure.
17	2	alarm	Remote end did not back off in glare	communication	Card;Port;Channel	minor		• Remote end did not back off in glare.
17	3	alarm	Wink expected, did not arrive	communication	Card;Port;Channel	major	✅	• Wink expected, did not arrive.
17	4	alarm	No dial tone	communication	Card;Port;Channel	major	✅	• Event of off-hook did not produce dial tone as expected.
17	5	event	CAS signaling group disabled	communication	SG		✅	• CAS signaling group disabled.
17	6	alarm	CAS license not enabled	general	System;Service	major	✅	• Call attempted but CAS feature is not enabled. • This alarm is cleared by CAS license enabled event.
17	7	event	CAS license enabled	general	System;Service			• License manager notify CAS that license is enabled.
17	8	event	Wink Received	communication	Card;Port;Channel			• Wink failure had occurred, but wink is received now.
17	9	event	Dial Tone Received	communication	Card;Port;Channel			• No Dial Tone was received, but Dial Tone is received now.
17	10	event	Response Received	communication	Card;Port;Channel			• No Response to seizure was received, but Response is received now.
17	11	alarm	Invalid character(s) in calling number	communication	Calling	warning		• Invalid character(s) removed, correct issue and delete warning.
17	12	alarm	Invalid character(s) in called number	communication	Called	warning		• Invalid character(s) removed, correct issue and delete warning.
17	13	event	CAS signaling group enabled	communication	SG			• CAS signaling group enabled.
17	14	alarm	CAS-R2 CD Bit error	communication	Card;Port	minor	✅	• CAS-R2 CD Bits are mismatched.

Copyright © 2015 Sonus Networks. All rights reserved.

17	15	event	CAS-R2 CD Bit error clear	communication	Card;Port			• CAS-R2 CD Bits are now matching.
17	16	alarm	Network Glare occured	communication	Card;Port;Channel	minor		• Network glare occured on this interface.

Configuration

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
18	1	event	Config validation failure	general	System;Service	warning		• Config validation failure during startup. • Please check the configuration.
18	2	alarm	Newer Config loaded	general	System;Service	warning		• Configuration loaded from newer release than currently running release.
18	3	event	Password decryption failed	general	System;Service	event		• Password decryption failed on configuration import operation.

TCA Thresholds

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
19	1	alarm	SG Channel Usage exceeded TCA threshold	communication	SG	major	✅	• Signaling Group channel usage exceeded configured TCA threshold.
19	2	event	SG Channel Usage below TCA threshold	communication	SG			• Signaling Group channel usage fell below configured TCA threshold.
19	3	alarm	SIP Call License Usage exceeded TCA threshold	communication	System;Service	major	✅	• SIP Call license usage exceeded configured TCA threshold.
19	4	event	SIP Call License Usage below TCA threshold	communication	System;Service			• SIP Call license usage fell below configured TCA threshold.
19	5	alarm	SIP Registration Usage exceeded TCA threshold	communication	SIPRegistrarTable	major	✅	• SIP Registration usage exceeded configured TCA threshold.
19	6	event	SIP Registration Usage below TCA threshold	communication	SIPRegistrarTable			• SIP Registration usage fell below configured TCA threshold.
19	7	alarm	DSP Usage exceeded TCA threshold	communication	System	major	✅	• DSP usage exceeded configured TCA threshold.
19	8	event	DSP Usage below TCA threshold	communication	System			• DSP usage fell below configured TCA threshold.
19	9	alarm	CPU Usage exceeded TCA threshold	communication	System	major	✅	• CPU usage exceeded configured TCA threshold.
19	10	event	CPU Usage below TCA threshold	communication	System			• CPU usage fell below configured TCA threshold.
19	11	alarm	Memory Usage exceeded TCA threshold	communication	System	major	✅	• Memory usage exceeded configured TCA threshold.
19	12	event	Memory Usage below TCA threshold	communication	System			• Memory usage fell below configured TCA threshold.
19	13	alarm	File Descriptor Usage exceeded TCA threshold	communication	System	major	✅	• File Descriptor Usage exceeded TCA threshold.

Copyright © 2015 Sonus Networks. All rights reserved.

19	14	event	File Descriptor Usage below TCA threshold	communication	System			• File Descriptor Usage fell below TCA threshold.
19	15	alarm	CPU load average in past 1 minute exceeded TCA threshold	communication	System	major	✅	
19	16	event	CPU load average in past 1 minute fell below TCA threshold	communication	System			
19	17	alarm	CPU load average in past 5 minutes exceeded TCA threshold	communication	System	major	✅	
19	18	event	CPU load average in past 5 minutes fell belowTCA threshold	communication	System			
19	19	alarm	CPU load average in past 15 minutes exceeded TCA threshold	communication	System	major	✅	
19	20	event	CPU load average in past 15 minutes fell belowTCA threshold	communication	System			
19	21	alarm	Temporary partition usage exceeded TCA threshold	communication	System	major	✅	
19	22	event	Temporary partition usage fell below TCA threshold	communication	System			
19	23	alarm	Logging partition usage exceeded TCA threshold	communication	System	major	✅	
19	24	event	Logging partition usage fell below TCA threshold	communication	System			

FQDN

ID	Sub-ID	Type	Default Condition	Category	Decode Key	Default Severity	Auto Clear	Notes/Description
20	1	alarm	Failed to resolve FQDN	communication	SNMP;IPAddress	minor	✅	• Failed to resolve IP Address. Ensure that FQDN and DNS server is configured properly.
20	2	event	FQDN resolved	communication	SNMP;IPAddress			• IP Address successfully resolved.

Decode Key Table

Following tables defines the decode key types used through out the system Alarms and Events system in Sonus SBC 1000/2000.

Decode Key	Description
System	By default it will be the Sonus SBC 1000/2000 system
Service	Service in which this alarm/event belongs to, for ex. ISDN, SIP etc..
Username	Username responsible for the generation of the alarm/event, mostly related to the User Authentication Service
IP address	IP address of the system responsible for generation of this alarm/even.
Frame	Frame responsible, at which the data transmission has failed/generated an error
Card/Slot	Card /Slot involved in generating the alarm For ex. TI DSP etc..
ActSetTble	Action set table number responsible for the alarm/event
NormTble	Normalization table number responsible for this alarm
RtTble	Route table number responsible for this alarm/event

Copyright © 2015 Sonus Networks. All rights reserved.

TLSProfile	TLS Profile (ID of the TLS Profile)
TransTble	Translation table number responsible for this alarm/event
Call Dest	Call destination (address) responsible for this alarm/event
Conference ID	Conference ID involved in the alarm generation. It will be an integer starting from 1 to FFFFFFFF
Codec	Media codec like G711, used when this alarm is generated
SG/Signaling Group	Signaling Group on which this alarm occurred
Channel	Channel number that involved in generating this alarm
CallID	Call ID of the call failed/is responsible for generating this alarm
Port	Port number on which this alarm is generated
Interface	Name/Number of the interface involved in generating this alarm. For ex. ETH1, T1 etc..
Server	Server responsible for this alarm. for Ex. SIP server which is not responding
CertificateCommonName	Server certificate common name for ex:"VeriSign Trial Secure Server CA - G2 "
SBAInstance	Its the SBA monitor involved in generating the alarm
Interface	By default it will be the Ethernet interface card
SIPCluster	Name of the SIP cluster associated with a set of SIP servers
ServID	ID of the SIP server
Protocol	Protocol involved in generating this alarm/event
Fan_No	Fan number

Working with the Debug Facility

Usage Warning

This interface should only be used by service personnel or as directed by service personnel

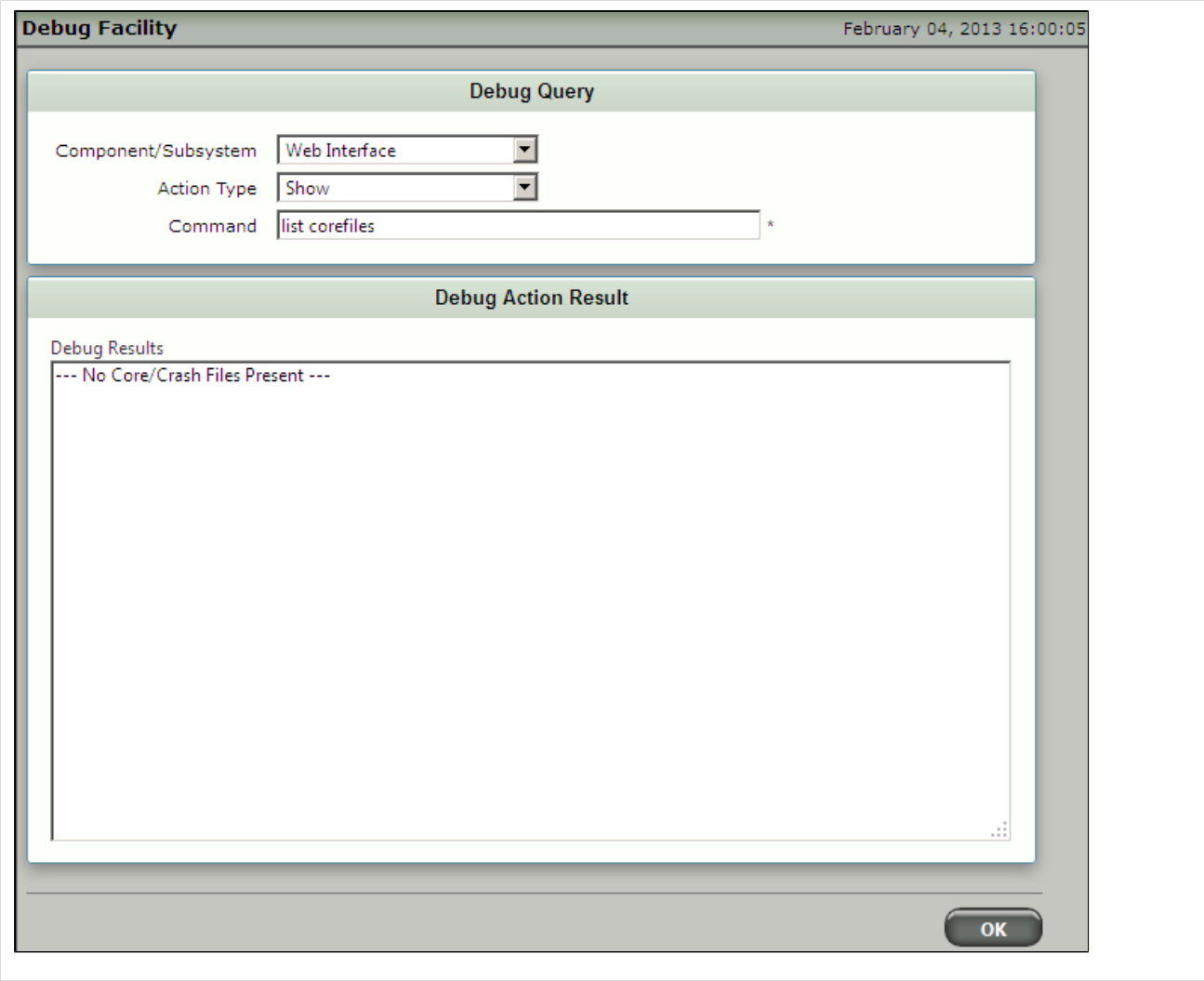
The Sonus SBC 1000/2000's Debug Facility allows end-users to send troubleshooting and maintenance-related commands directly to the system, and view their responses. For example, some of these commands allow for:

- The retrieval of core dumps found on the system
- The ability to safely remove USB flash drive from the front panel

Accessing the Debug facility:

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation pane, go to **Sonus TAC Troubleshooting> Debug Facility**.
3. For each Component/Subsystem, enter the command `help` for a list of the applicable commands.

Copyright © 2015 Sonus Networks. All rights reserved.



Testing a Call

This task allows you to initiate a simple test call from within the Sonus SBC 1000/2000. The test call goes through the gateway's call routing setup using the configured Call Routing Tables, Translation tables, and Music on Hold configuration. You can test a call for a SIP phone or Analog phone. Unlike the Testing a Lync Call operation, this functionality initiates the call from within the Sonus SBC/2000 itself, and not from the Lync SBA.

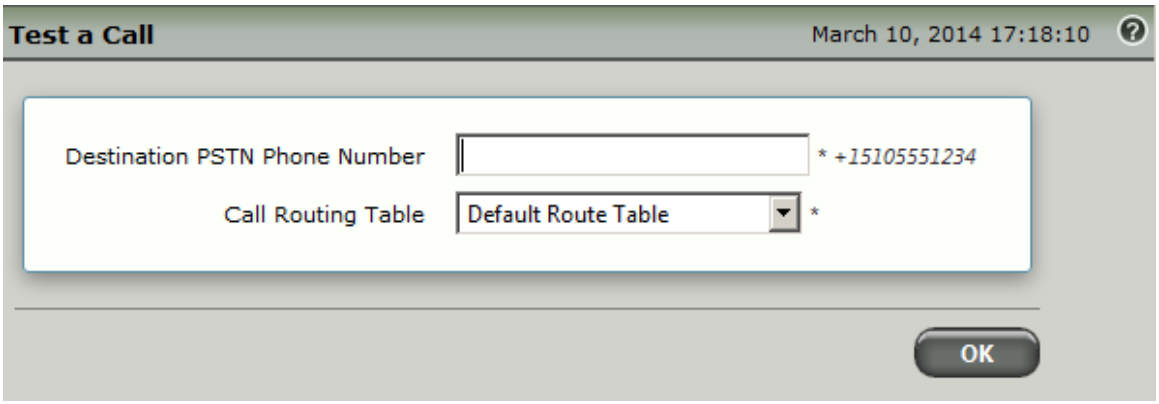
Testing a Call

Before you begin, it is assumed the SBC 1000/2000 is deployed.

To test a call

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation pane, under **Tools**, click **Test a Call**
   .

Copyright © 2015 Sonus Networks. All rights reserved.



3. Enter **Destination Phone Number** (through the **Destination PSTN Phone Number** field). This is the phone number for the SIP phone or Analog phone in which you are testing a call.
4. From the **Call Routing Table** drop down list, select a call routing table. Ensure the Call Routing Table you select is configured properly. For information about Call Routing tables, see Managing Call Routing Tables.
5. Click **OK.**

Expected Outcome

Once the call is made, the call goes through the selected Call Route. After the SIP phone or Analog phone accepts the call, the user will hear music for about 15 seconds.

For an unsuccessful call, check the following:

- Verify the Call Routing Table entry selected. Also check the Translation table for configuration. These tables determine how a call is routed and translated.
- Review Local Log files. Log files record internal and external action on the SBC 2000 (these log files are not available on the SBC1000), including user visible actions (such as placing calls).
- Verify Music On Hold configuration. If configured to use a music file, but there is no music file, no music is played. If configured to use radio (live source), but there is no valid FXS port, no music is played.

Testing Network Connections

The Sonus SBC 1000/2000 provides functionality for using and Ping and Traceroute.

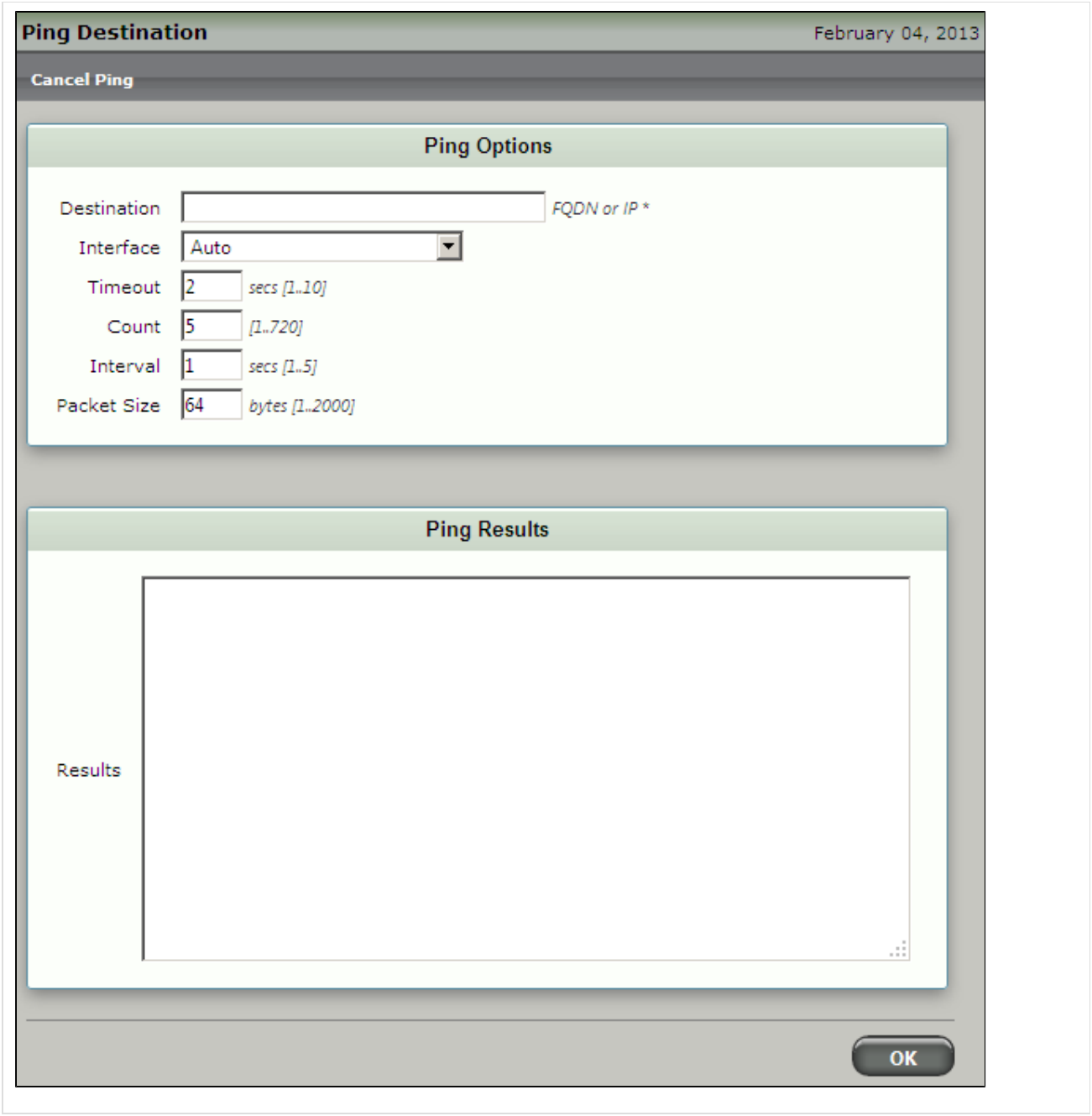
- Ping
- Traceroute to Destination

Ping

To ping a device:

1. In the WebUI, click the **Diagnostics** tab.
2. in the left navigation pane, go to **Tools > Ping Destination**.

Copyright © 2015 Sonus Networks. All rights reserved.



Ping Options - Field Definitions

Destination

The IP address or Fully Qualified Domain Name of the destination machine.

Interface

Specifies the physical interface on the Sonus SBC 1000/2000 over which the ping traffic is sent.

Timeout

Specifies the maximum time, in seconds, that the Sonus SBC 1000/2000 waits for a response to a ping.

Copyright © 2015 Sonus Networks. All rights reserved.

Count

Specifies the number of times to a ping.

Interval

Specifies the interval, in seconds, between pings.

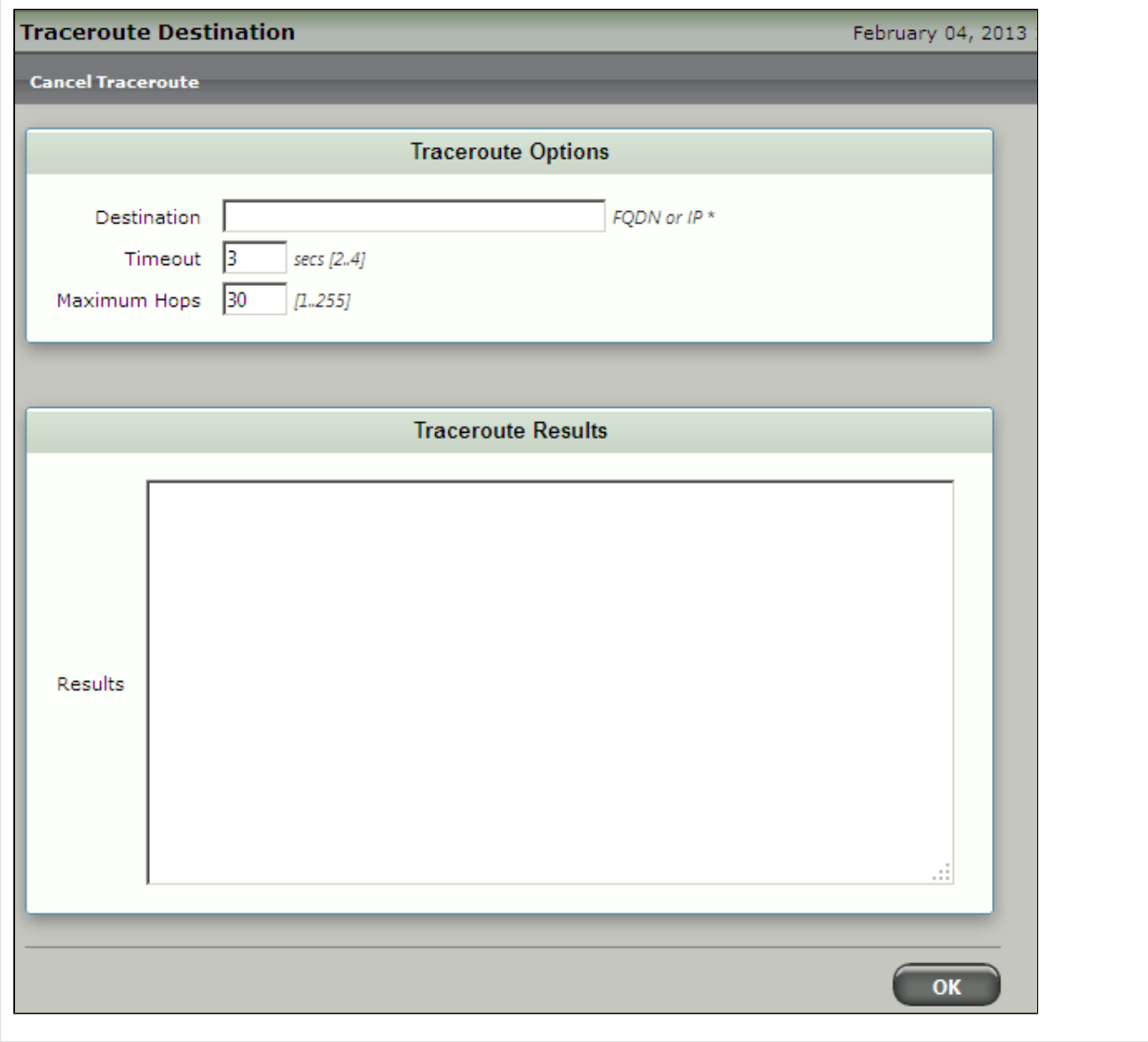
Packet Size

Specifies the payload size of the packet sent. Total packet size is the specified value plus 8 bytes.

Traceroute to Destination

To trace the hops to a destination:

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation pane, go to **Tools > Traceroute to Destination**.



Copyright © 2015 Sonus Networks. All rights reserved.

Traceroute to Destination Options - Field Definitions

Destination

Specifies the IP address or Fully Qualified Domain Name of the machine to which a route is traced.

Timeout

Specifies the maximum time, in seconds, that the Sonus SBC 1000/2000 waits for a response for each hop.

Maximum Hops

Specifies the maximum number of hops before terminating.

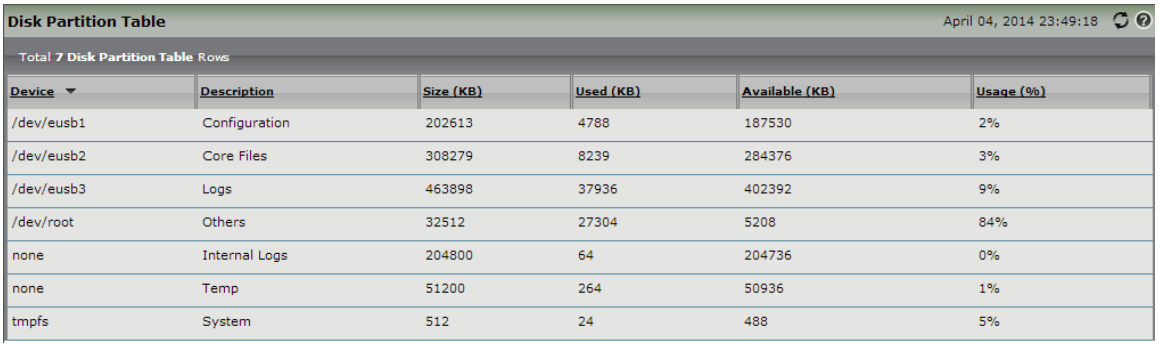
Viewing Mounted File Systems

The Disk Partition facility contains a list of all mounted file systems.

Viewing the Partition Table

To view the table:

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation pane, in the Tools group, click **Disk Partitions**.



Device	Description	Size (KB)	Used (KB)	Available (KB)	Usage (%)
/dev/eusb1	Configuration	202613	4788	187530	2%
/dev/eusb2	Core Files	308279	8239	284376	3%
/dev/eusb3	Logs	463898	37936	402392	9%
/dev/root	Others	32512	27304	5208	84%
none	Internal Logs	204800	64	204736	0%
none	Temp	51200	264	50936	1%
tmpfs	System	512	24	488	5%

Viewing Active Processes

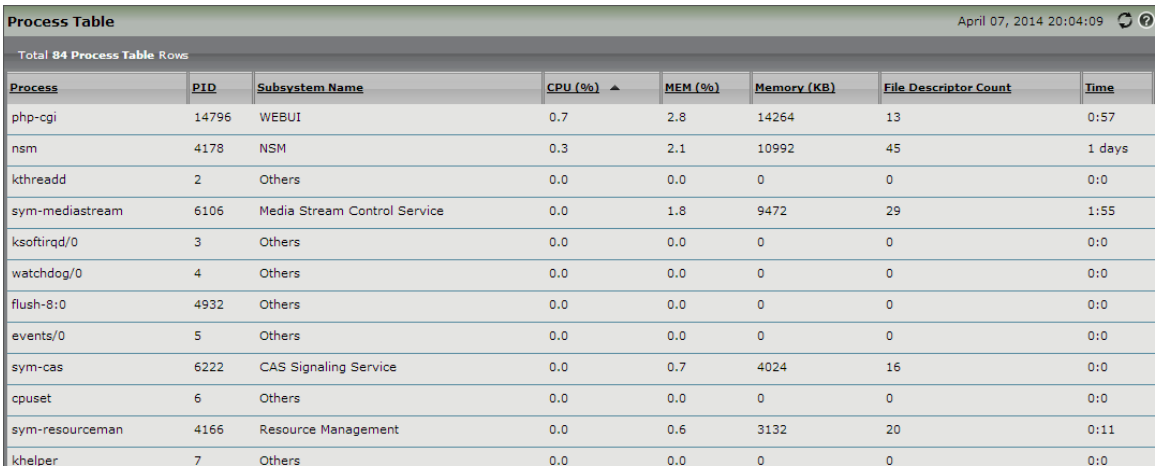
The Process Table facility displays all currently running processes on the SBC1000/2000.

Viewing The Active Processes

To view the Process Table:

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation pane, under Tools, click **Process Table**.

Copyright © 2015 Sonus Networks. All rights reserved.



Process Table — April 07, 2014 20:04:09

Total 84 Process Table Rows

Process	PID	Subsystem Name	CPU (%)	MEM (%)	Memory (KB)	File Descriptor Count	Time
php-cgi	14796	WEBUI	0.7	2.8	14264	13	0:57
nsm	4178	NSM	0.3	2.1	10992	45	1 days
kthreadd	2	Others	0.0	0.0	0	0	0:0
sym-mediastream	6106	Media Stream Control Service	0.0	1.8	9472	29	1:55
ksoftirqd/0	3	Others	0.0	0.0	0	0	0:0
watchdog/0	4	Others	0.0	0.0	0	0	0:0
flush-8:0	4932	Others	0.0	0.0	0	0	0:0
events/0	5	Others	0.0	0.0	0	0	0:0
sym-cas	6222	CAS Signaling Service	0.0	0.7	4024	16	0:0
cpuset	6	Others	0.0	0.0	0	0	0:0
sym-resourceman	4166	Resource Management	0.0	0.6	3132	20	0:11
khelper	7	Others	0.0	0.0	0	0	0:0

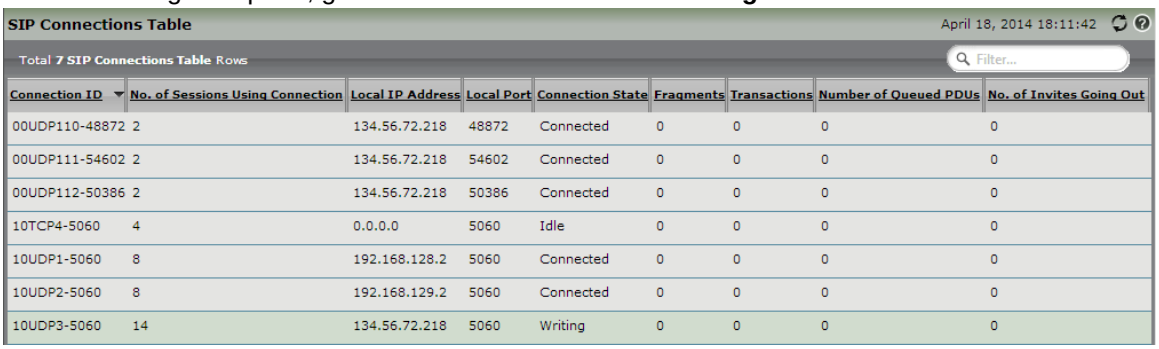
Viewing The SIP Connections Table

The SIP Connections Table displays all the current SIP connections on the SBC1000/2000 and includes information about the connection state, IP addresses, ports, sessions, and more.

Viewing SIP Connections

To view the SIP Connections Table:

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation pane, go to: **Sonus TAC Troubleshooting > SIP Connections Table**.



SIP Connections Table — April 18, 2014 18:11:42

Total 7 SIP Connections Table Rows — Filter...

Connection ID	No. of Sessions Using Connection	Local IP Address	Local Port	Connection State	Fragments	Transactions	Number of Queued PDUs	No. of Invites Going Out
00UDP110-48872	2	134.56.72.218	48872	Connected	0	0	0	0
00UDP111-54602	2	134.56.72.218	54602	Connected	0	0	0	0
00UDP112-50386	2	134.56.72.218	50386	Connected	0	0	0	0
10TCP4-5060	4	0.0.0.0	5060	Idle	0	0	0	0
10UDP1-5060	8	192.168.128.2	5060	Connected	0	0	0	0
10UDP2-5060	8	192.168.129.2	5060	Connected	0	0	0	0
10UDP3-5060	14	134.56.72.218	5060	Writing	0	0	0	0

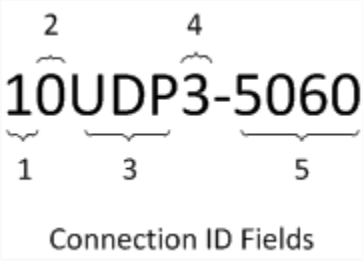
SIP Connections Table - Column Definitions

Connection ID

Copyright © 2015 Sonus Networks. All rights reserved.

Displays the Transport Connection ID, which is a unique identifer of a SIP connection.

The field is composed of five parameters:



Connection ID Fields

1. Listener/Connected to Peer: 0 = connected to peer, 1 = listener
2. Persistent connection: 0= not persistent, 1 = persistent
3. Transport type: UDP, TCP, or TLS
4. Index: Number of sessions for this connection.
5. Port: Local port for this connection.

No of Sessions Using Connection

The total number of sessions using the existing transport connection

Local IP Address

The local IP address of the connection

Local Port

The local port number through which the connection is established.

Connection State

Copyright © 2015 Sonus Networks. All rights reserved.

The current state of the connection.

States (default = Idle):

- Idle
- Error Occurred
- Pending Deletion
- Closing
- Closed
- Removed
- Aborted
- Accepted
- Connecting
- Connected
- Reading
- Writing

Fragments

The total number of message fragments sent from the peer to the current connection.

Transactions

Total number of transactions waiting for the connection to be established.

No of Queued PDUs

The number of PDUs queued for the connection.

No of Invites Going Out

The total number of outbound INVITEs sent via this connection.

Viewing The Disk Partition Table

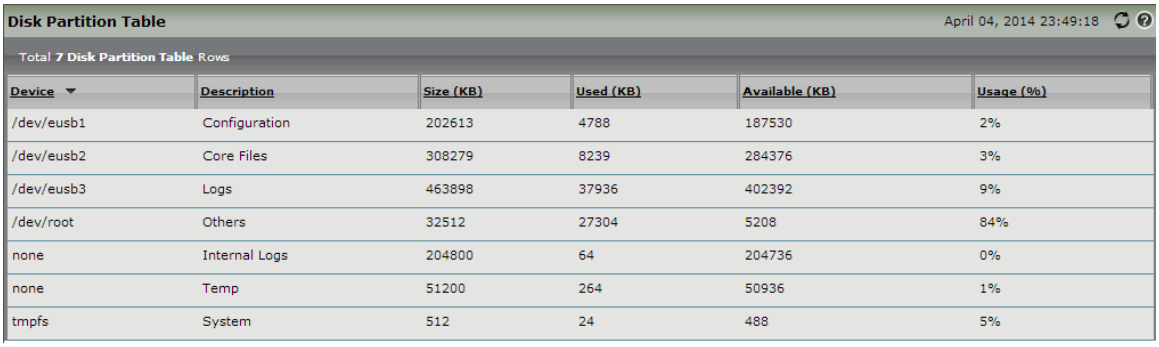
The Disk Partition Table provides a list of all currently mounted file systems on the node.

Viewing Disk Partitions

To view the Disk Partition Table:

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the Diagnostics tab.
2. In the left navigation pane, go to: Tools > Disk Partitions.



Disk Partition Table April 04, 2014 23:49:18

Total **7 Disk Partition Table** Rows

Device	Description	Size (KB)	Used (KB)	Available (KB)	Usage (%)
/dev/eusb1	Configuration	202613	4788	187530	2%
/dev/eusb2	Core Files	308279	8239	284376	3%
/dev/eusb3	Logs	463898	37936	402392	9%
/dev/root	Others	32512	27304	5208	84%
none	Internal Logs	204800	64	204736	0%
none	Temp	51200	264	50936	1%
tmpfs	System	512	24	488	5%

Checking your System Information

This section provides information about how to determine the status of your Sonus SBC 1000/2000, what modules are installed, the status of ports and interfaces, counters and more.

- Viewing the Software Version and Hardware ID
- Viewing ASM System Details
- Viewing and Clearing Global Call Counters
- Checking Port Status
- Checking Cards and Modules Status
- Checking System Fan Status
- Checking Power Supply Status
- Viewing Installed Modules, Power Supplies, and Ports
- Viewing DSP Module Statistics
- Status Panel States and Actions

See Also:

- Is there a compiled list of doc pages for viewing all Sonus SBC 1000-2000 related software versions?

Viewing the Software Version and Hardware ID

The Sonus SBC 1000/2000 system uses a 3 digit software versioning scheme `Major.Minor.Maintenance (patch)`:

- **Major** - updated every major development.
- **Minor** - updated for unplanned minor feature development in between major development cycles.
- **Maintenance** - updated for hot fixes, and service packs.
- **Patch** - present only when used, deliver custom features or bug fixes not covered by the base software.

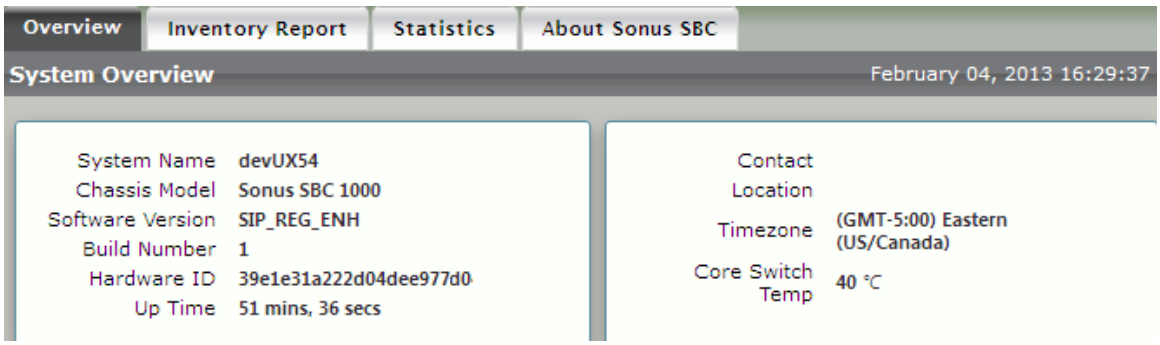
In addition to the software version, a **Build Number** is always associated with the base software version and represents the exact build machine, time, and date. Upgrades to these builds are provided to all customers and partners who have maintenance contracts.

Viewing the Software Version

The Sonus SBC 1000/2000 software version and build number shown is the based on the firmware running on the active partition:

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the **System** tab.
2. In the System page, click the **Overview**tab.



Reporting a Bug?

If you are about to report a defect, ensure you provide the Sonus SBC 1000/2000's **software version** along with the **build number**. You may also be asked to provide the **Chassis Model** - Sonus SBC 1000 or Sonus SBC 2000

Viewing ASM System Details

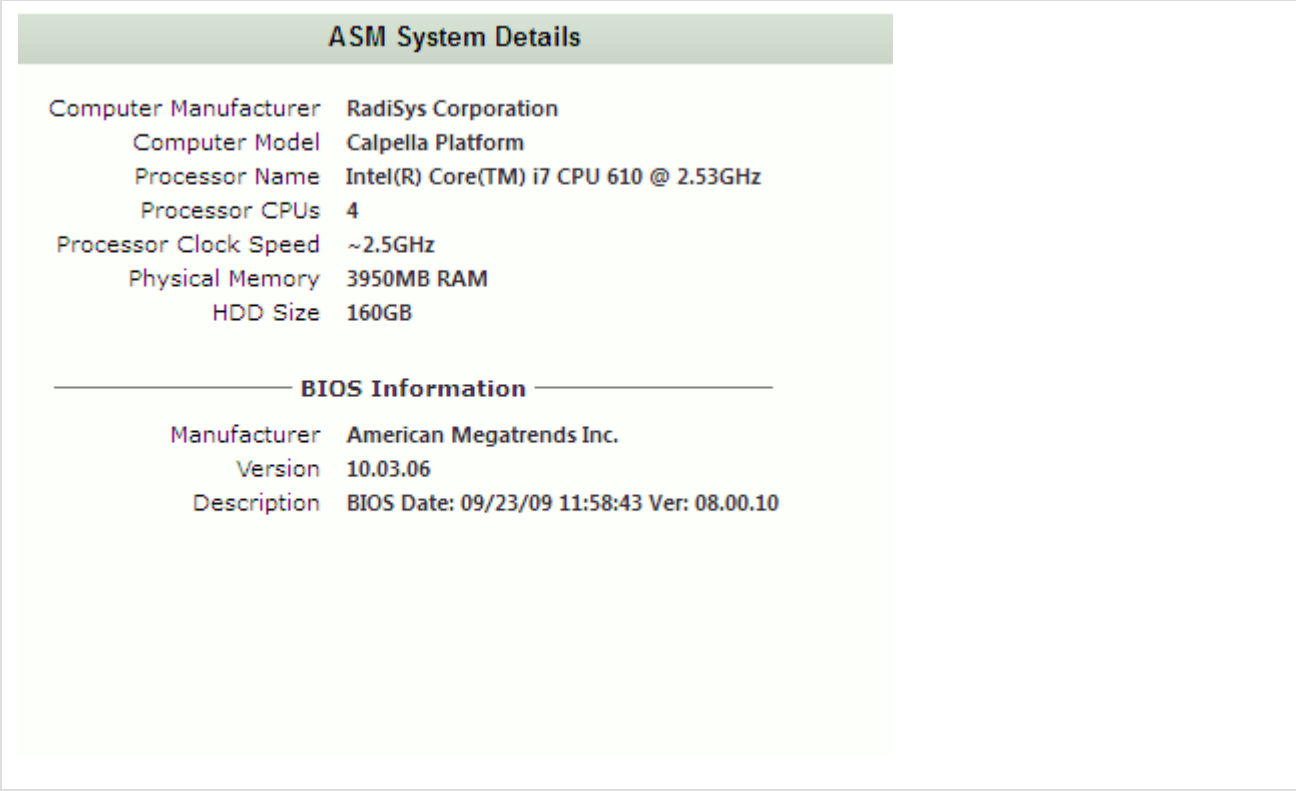
The Application Solution Module (ASM) System Details Panel (available only if your Sonus SBC 1000/2000 system has a built-in ASM) lists the relevant hardware specifications for the ASM.

Viewing ASM System Details

To view the ASM's system details:

1. In the Sonus SBC 1000/2000 WebUI, click the **System** tab.
2. On the System page, click the **Overview** tab.

Copyright © 2015 Sonus Networks. All rights reserved.



Located in Overview Tab

When viewed in the WebUI, the ASM System Details panel view is **located towards the bottom of the web page (on the left)**.

Viewing and Clearing Global Call Counters

The Global Call Counters panel displays three types of counters:

- **Current calls**-
  - Calls Currently Up: the number of calls that are connected
  - Calls Currently Transient: the number of calls that are in the process of either connecting (set up) or disconnecting (torn down).
- **Call counters**- displays statistics about calls attempted and abandoned by the Sonus SBC 1000/2000:
  - Calls Attempted: the total number of calls, successful or not, attempted by the Sonus SBC 1000/2000.
  - Calls Succeeded: the total number of calls successfully attempted by the Sonus SBC 1000/2000.
  - Calls Failed: the total number of calls attempted by the Sonus SBC 1000/2000 that failed.
- **Error counters**- displays statistics about failed calls:
  - Internal Glares: the total number of errors related to SIP INVITE messages transmitted while a request is pending.
  - External Glares: the total number of errors related to SIP INVITE messages received while a request is pending.
  - Due to No Signaling Group: the total number of times the Sonus SBC 1000/2000 failed to find a TDM or IP trunk while attempting to setup a call.

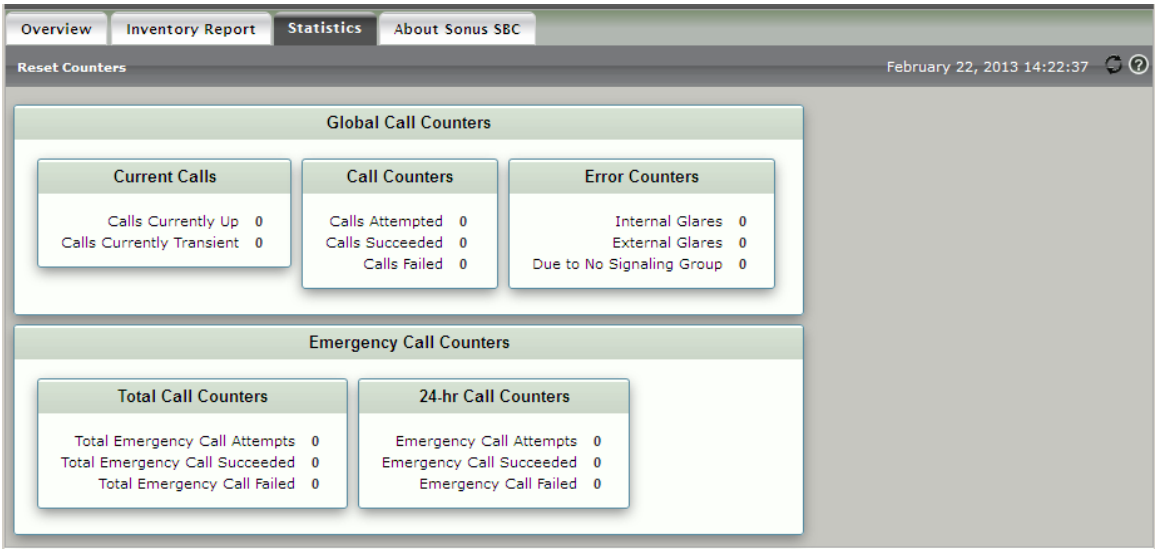
Note: The Sonus SBC 1000/2000 automatically resets the global counters every hour.

How to View Global Call Counters

Copyright © 2015 Sonus Networks. All rights reserved.

To view the call counters :

1. In the WebUI, click the **System** tab.
2. On the System page, click the **Statistics** tab.



Clearing the Global Call Counters

To clear the call counters:

- Click the **Reset Counters** link at the top left-hand side of the page.

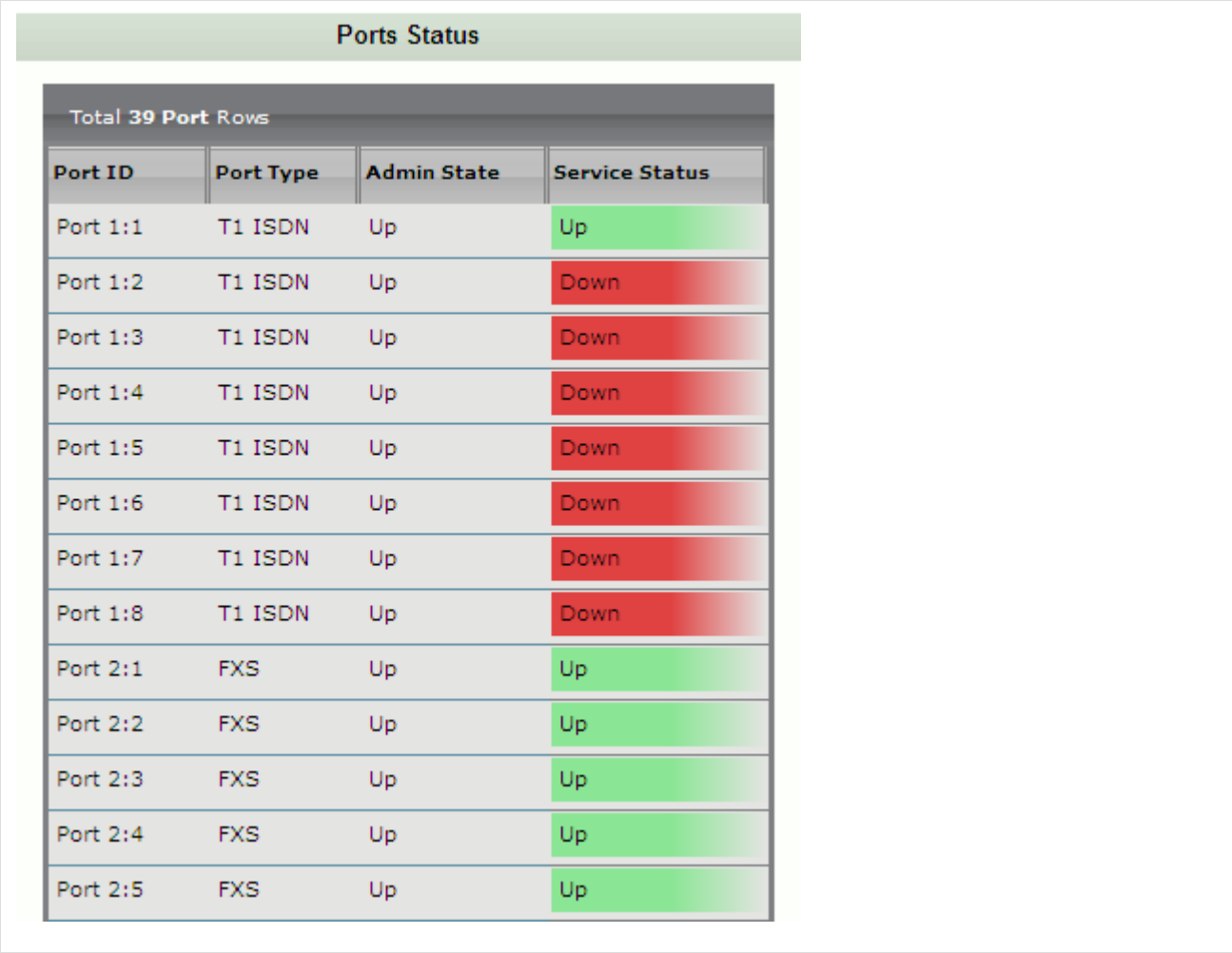
Checking Port Status

Checking Port Status

To view the status of your Sonus SBC 1000/2000 system's physical ports:

1. In the Sonus SBC 1000/2000 WebUI, click the **System** tab.
2. On the System page, click the **Overview** tab.

Copyright © 2015 Sonus Networks. All rights reserved.



Located in Overview Tab

When viewed in the WebUI, the Port Status panel view is **located in the middle of the web page (on the right)**.

Sonus SBC 1000 System Port Configurations

The Sonus SBC 1000 has a maximum of 29 physical ports:

- 2 T1/E1 Port
- 24 Analog (FXS/FXO) ports or 12 ISDN BRI ports
- 1 WAN Port
- 2 Ethernet LAN ports

Sonus SBC 2000 System Port Configurations

The Sonus SBC 2000 has a maximum of 22 physical ports:

- 16 Line Card ports (8 on each of 2 cards)
- 4 Ethernet LAN ports
- 1 Ethernet Admin port
- 1 ASM port (if ASM installed)

Checking Cards and Modules Status

Copyright © 2015 Sonus Networks. All rights reserved.

The **Cards/Modules Status** panel provides the following information:

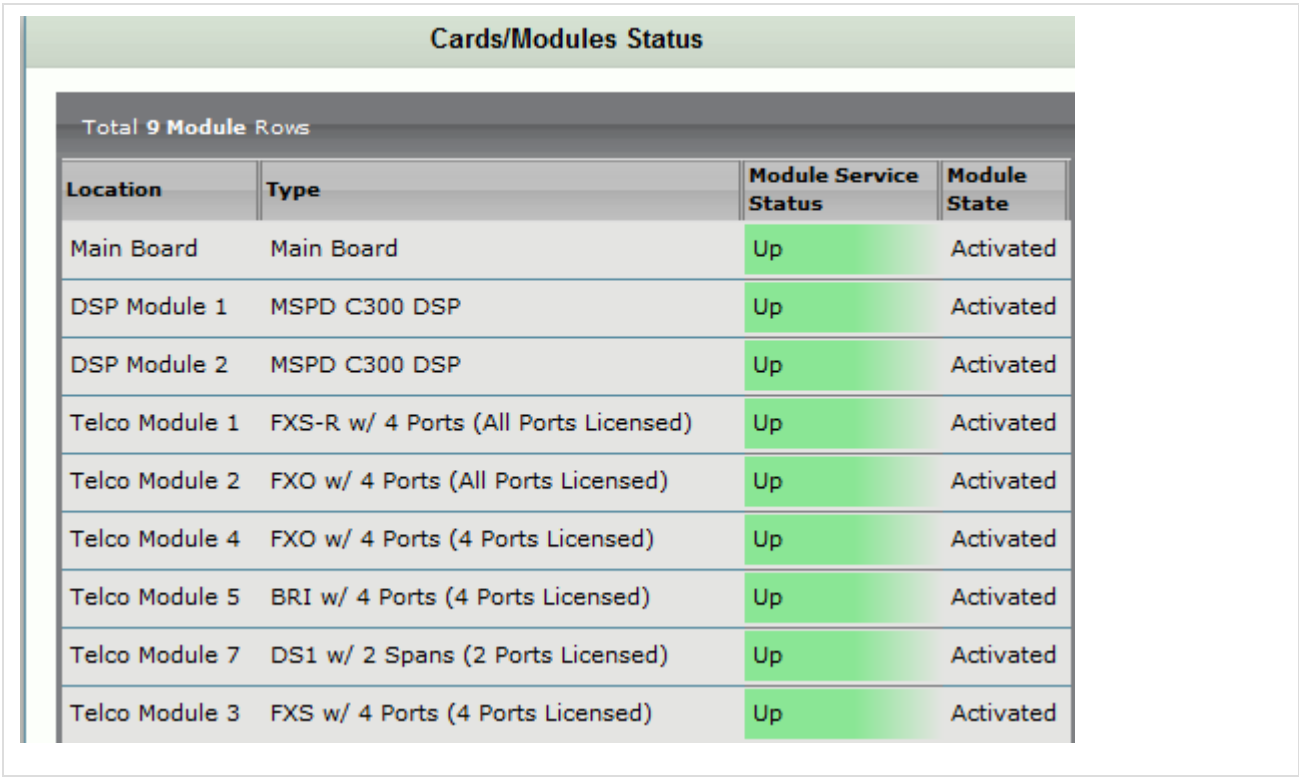
- **Location**. Indicates the location of the module installed.
- **Type**. Indicates the physical type of hardware installed (DSP, FXS, FXO, etc., including number of licensed ports).
- **Module Service Status**. Indicates the service status of the module: **Up** (module is running) or **Down** (module is not running).
- **Module State.** Indicates the activation state of the module: **Activated** (module is activated), **Failed** (module's service is down) or **Unknown** (module's service is down or status is unknown).

Checking Cards and Modules Status

> The information in the **Cards/Modules** status is in sync with the physical cards/module status in the node's Inventory Report.

To view any Card/Module's status:

1. In the Sonus SBC 1000/2000 WebUI, click the **System** tab.
2. On the System page, click the **Overview** tab.



Cards/Modules Status

Total **9 Module** Rows

Location	Type	Module Service Status	Module State
Main Board	Main Board	Up	Activated
DSP Module 1	MSPD C300 DSP	Up	Activated
DSP Module 2	MSPD C300 DSP	Up	Activated
Telco Module 1	FXS-R w/ 4 Ports (All Ports Licensed)	Up	Activated
Telco Module 2	FXO w/ 4 Ports (All Ports Licensed)	Up	Activated
Telco Module 4	FXO w/ 4 Ports (4 Ports Licensed)	Up	Activated
Telco Module 5	BRI w/ 4 Ports (4 Ports Licensed)	Up	Activated
Telco Module 7	DS1 w/ 2 Spans (2 Ports Licensed)	Up	Activated
Telco Module 3	FXS w/ 4 Ports (4 Ports Licensed)	Up	Activated

> **Located in Overview Tab**
>
> When viewed in the WebUI, the Cards and Modules Status panel view is **located approximately half way down the web page**.

Checking System Fan Status

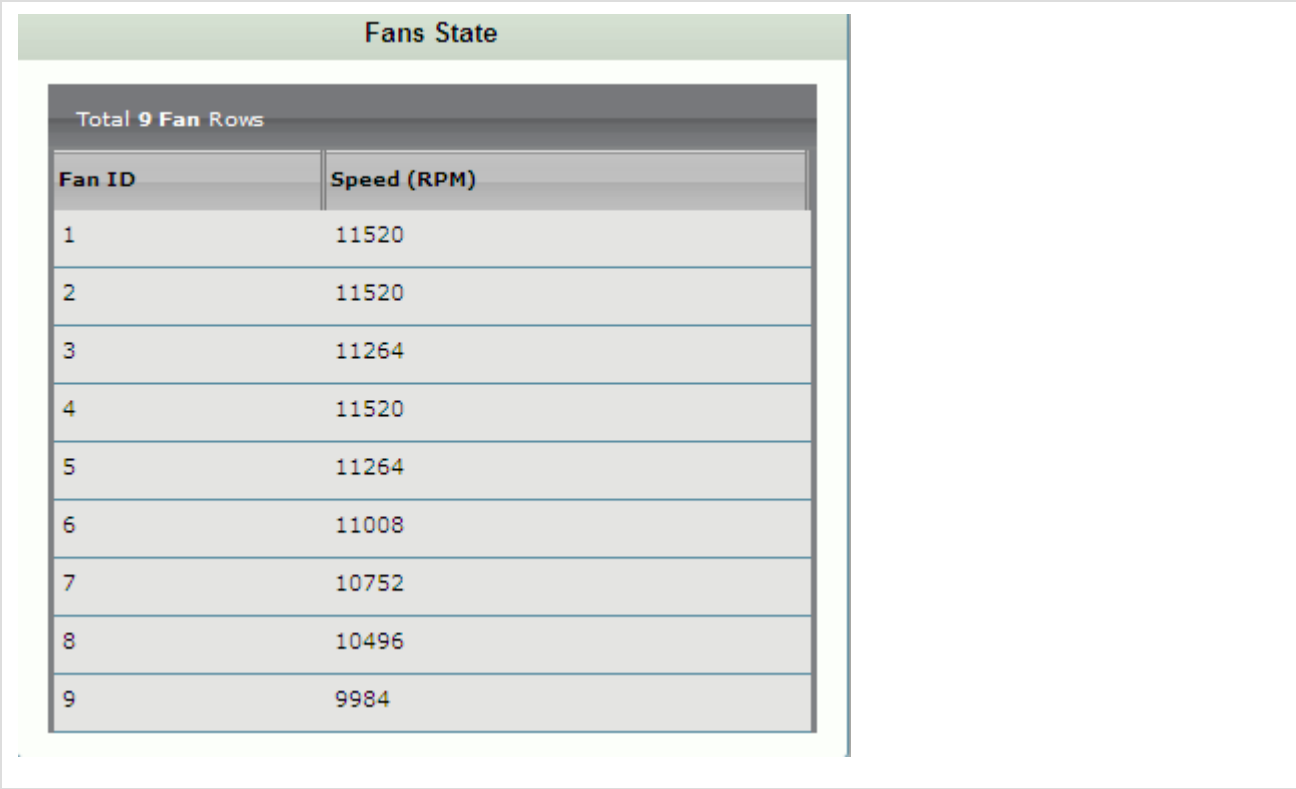
The Fans State Panel (available only on the Sonus SBC 2000 chassis model) lists the current running speed for each of the Sonus SBC 1000/2000 chassis fans.

Checking System Fan Status

Copyright © 2015 Sonus Networks. All rights reserved.

To view fan spin rates:

1. In the Sonus SBC 1000/2000 WebUI, click the **System** tab.
2. On the System page, click the **Overview** tab.



Fans State

Total 9 Fan Rows

Fan ID	Speed (RPM)
1	11520
2	11520
3	11264
4	11520
5	11264
6	11008
7	10752
8	10496
9	9984

Located in Overview Tab

When viewed in the WebUI, the Fans State panel view is **located towards the bottom of the web page (on the right)**.

Checking Power Supply Status

The Power Supplies panel (available only on the Sonus SBC 2000 chassis model) provides detailed power supply operational status, including:

- input and output power(W)
- Input and output voltages
- Input and output currents(A)
- Operating temperature
- Fan speeds

Checking Power Supply Status

To view the status of the power supplies:

1. In the Sonus SBC 1000/2000 WebUI, click the **System** tab.
2. On the System page, click the **Overview** tab.

Copyright © 2015 Sonus Networks. All rights reserved.

Power Supplies

Total **2 PSU** Rows

PSU ID	Is Present	AC Input Good	Power In (W)	Power Out (W)	Voltage In (Nominal-AC)	Voltage Out (DC)	Current In (A)	Current Out (A)	Temp (°C)	Fan 1 Speed (RPM)	Fan 2 Speed (RPM)
PSU Left	✓	✓	73	53	115	12.000	0.634	4.438	42	6706	6725
PSU Right	✓		0	0	0	0.000	0.000	0.000	24	0	0

Located in Overview Tab

When viewed in the WebUI, the Power Supplies panel view is **located approximately half way down the web page**.

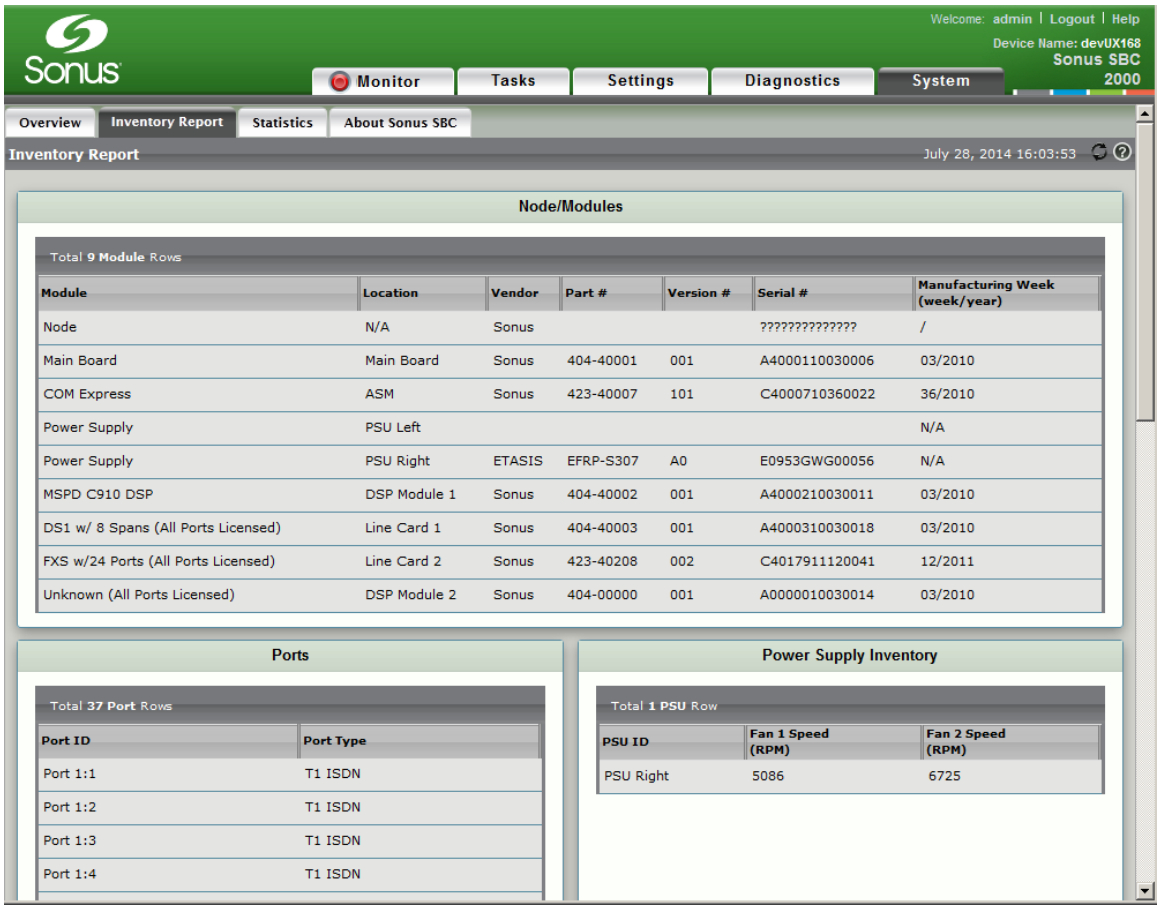
Viewing Installed Modules, Power Supplies, and Ports

This page explains how to determine what physical assets are installed in your Sonus SBC 1000/2000.

Viewing Your Sonus SBC 1000/2000 System Inventories

To view your Sonus SBC 1000/2000 System's assets:

1. Click the **System** tab at the top of the Sonus SBC 1000/2000 WebUI browser page.
2. Click the **Inventory Report** tab.



The **Inventory Report** page comprises three panels: **Node/Module Inventory**, **Ports Inventory**, and **Power Supply Inventory.** The contents of these panels are explained below.

Copyright © 2015 Sonus Networks. All rights reserved.

Node/Module Inventory

The **Node/Module Inventory** panel lists the major modules installed in your Sonus SBC 1000/2000 along with their locations, manufacturing, and identification information.

- **Module.** Module type (i.e., node, main board, power supply, FXS, etc.). This includes module type and number of licensed ports per module.
- **Location**. Physical location of the module in the SBC.
- **Vendor**. Vendor from whom the module was purchased.
- **Part #**. Part number of the module.
- **Version #**. Version number of the module.
- **Serial #**. Serial number of the module.
- **Manufacturing Week.** The week/year the module was manufactured.

Ports Inventory

The **Ports Inventory** panel lists all the licensed ports on the Sonus SBC 1000/2000 and their types (e.g., T1, E1, Ethernet, etc.).

- **Port ID.** Number of port/slot.
- **Port Type.** Identifies port type.

Power Supply Inventory

> Power Supply Inventory is available for SBC2000 only.

The **Power Supply Inventory** panel lists the installed power supplies and their fan speeds. The Sonus SBC 2000 can have either one or two power supplies.

- **PSU ID**. Indicates the location of the power supply.
- **Fan 1 Speed (RPM)**. Speed of fan.
- **Fan 2 Speed (RPM)**. Speed of fan.

Viewing DSP Module Statistics

The DSP Module Table lists information about how many DSPs are installed on your Sonus SBC 1000/2000, their availability and service status. It also displays statistics about how many channels are in use at the time of viewing, along with its CPU usage information.

To view DSP Module Statistics:

1. In the WebUI, click the **Settings** tab at the top of the page.
2. Go to **System > DSPs**.

Copyright © 2015 Sonus Networks. All rights reserved.

DSP Module Table February 22, 2013 14:38:11

Total **6 DSP Module** Rows

Filter...

DSP Slot	Module Type	Available	Channels In Use	CPU Usage (%)	Last CPU Usage Update	Service Status	Last Music on Hold File Update	Music on Hold File Status
1	MSPD C910 DSP	✓	0	0.7	02/22/13 14:38:09	Up	02/20/13 15:29:15	Not Loaded
2	N/A		-	-	-	N/A	-	-
3	N/A		-	-	-	N/A	-	-
4	N/A		-	-	-	N/A	-	-
5	N/A		-	-	-	N/A	-	-
6	N/A		-	-	-	N/A	-	-

Status Panel States and Actions

This section describes the various states indicated by the status panel lights on the front of the Sonus SBC 1000/2000 system chassis.

Front Panel LEDs	Status Description	Actions
 **Power** and **Ready** status is green, **Alarm** is off	Normal status.	The Sonus SBC 1000/2000 is functioning normally. No action is required.
 **Power** status is green, **Ready** i s off	The Ready indicator is off. System is not fully initialized and not ready to process calls.	System did not start up properly or may be incorrectly configured. Use the Working with the Web Interface to check the current configuration.
 **Alarm** status is amber	A minor alarm is active	See Working with the Web Interface and Viewing Alarms and Events for more information about current alarms.
 **Power** and **Ready** status is green, **Peer Node** is off	Normal status. The Peer Node (Locator) LED has been turned off through configuration.	To configure a Peer Node LED to be turned on/off/blinking, see Configuring Host Information and DNS.

Copyright © 2015 Sonus Networks. All rights reserved.

Working with Licenses

This section describes the two types of licenses you will find on your Sonus SBC 1000/2000 system, and provides procedures for installing, decoding, and viewing licenses.

License Types

The Sonus SBC 1000/2000 system uses two types of licenses to enable functions and features of the platform.

Base license

This type of license enables version-specific features in a new Sonus SBC 1000/2000 software version. The new features in new software versions are disabled by default and are only enabled after installing a new base license. For example: New version B of Sonus SBC 1000/2000 software is available with support for feature X. Customers with a software subscription (support contract) are able to download the upgraded software and the new base license from the Sonus SBC 1000-2000 Download Center. If their Sonus SBC 1000/2000 is upgraded to version B, new feature X and all other new features of version B are disabled until a new base license is installed.

Node License

This type of license enables features which are not available as standard functions of the Sonus SBC 1000/2000 system and must be specifically purchased. The Node License also enables physical ports on the FXS, FXO, BRI and DS1 hardware modules/line cards. An SBC 1000 Module or SBC 2000 line card requires a license to enable ports for use on the node. Contact Sonus Sales for more information about licensed features and hardware modules.

Related Topics

- Decoding License Keys
- Installing Licenses
- Viewing Licenses

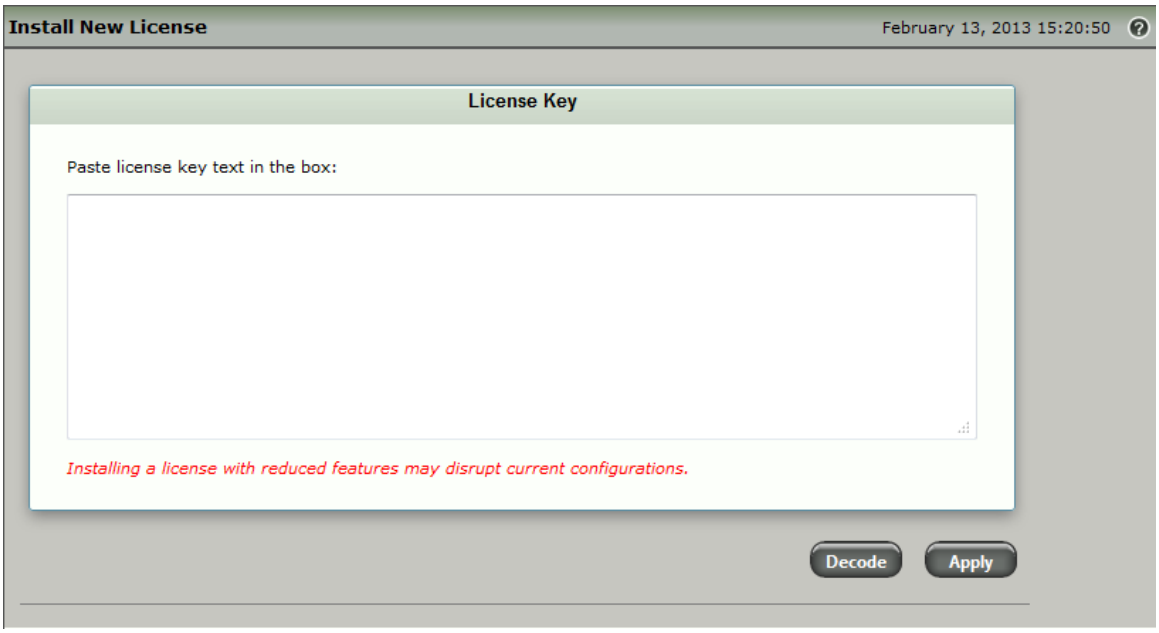
Decoding License Keys

This page describes the procedure for decoding a Sonus SBC 1000/2000 license key. This is useful for displaying the list of Feature Licenses contained in the license.

To decode a license key:

1. In the WebUI, Click the **Settings** tab.
2. In the left navigation pane, go to **System > Licensing > Install New License**.

Copyright © 2015 Sonus Networks. All rights reserved.



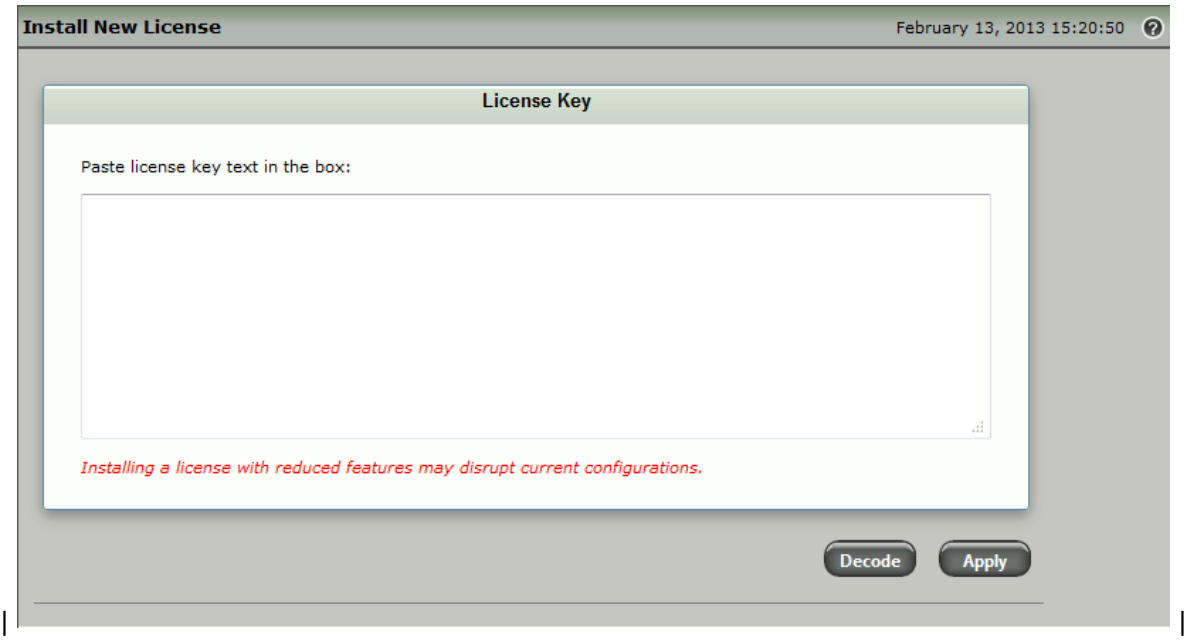
3. Copy the license key you've received from Sonus.
4. Paste the license key into the text box.
5. Click **Decode License Key**.

Installing Licenses

This page describes the procedure for installing new or additional Base/Node license keys.

To Install a License Key:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Licensing > Install New License**.



3. Copy the license key from the email you received from Sonus.
4. Paste the license key into the text box.
5. Click **Apply**.

Copyright © 2015 Sonus Networks. All rights reserved.

Sample License Key

WARNING

Do not attempt to use the sample key in your Sonus SBC 1000/2000!

The license must contain the correct number of TDM ports in the system. An alarm is generated when the license key applied has more TDM ports licensed than are installed in the system, and the license key is rejected.

```
-----BEGIN LICENSE KEY-----
MIICNAYJKoZIhvcNAQcCoIICJTCCAiECAQMxCzAJBgUrDgMCGgUAMIIBqgYJKoZIhvcNAQcBoIIB
mwSCAZftvQdgHEmWJSYvbcp7f0r1StfgdKEIgGATJNiQQBDswYjN5pLsHWlHIymrKoHKZVZlXWYW
QMztnbz33nvvvffee++997o7nU4n99//P1xmZAFs9s5K2smeIYCqyB8/fnwfPyL+x7/3H3z8e7xb
lOllXjdFtfzso93xzkdpvpxWs2J53dlH6/Z8++Cj3+PoN04ePy+m+bLJU2q+bB69a4rPPpq37erR
3btXV1fjq3vjqr64u7ezs3v39/i+evsPF9k28WyabPlNP/IvjW7+a2PqLc0ffwsz9p1nTf8l/tb
/3QfnM2OXp+9PHl81/3dbfKTWbnOj7568fzMtpKPFLT58BZdvXn6xQ+rq6evf2ijIgK++iF1dfz0
7IfV1esnx89+SF09+/LV7/VD6urNq5Muv8GuNnX16vT1mx9SVyfHr7+5ubJ/ifJ4TC2LWdFem8an
y1l6V1sG3z3+dlbPrjLGID+fHOTn2cF0dp7Ppvcm2c5k8viu14BfeJ3XRVa+WC8meX20u3dv//6n
j+8GH5LqvKu68+j/ATFhMF8CAQOAFK0YUHbAsbybUa5JoBuvIu2DZToaMAkGBSsOAwIaBQAwCQYH
KoZIzjgEAwQuMCwCFB6xm9pSeduuyqc9frLxAri8Us00jAhQNOsBnYC9+y2wVk4R6kn/DcqA3sQB
/VeTw=
-----END LICENSE KEY-----
```

Note:

When copying the license text, be sure to copy the entire text shown above including the markers (e.g. *---BEGIN LICENSE KEY---*).

Viewing Licenses

This page describes how you can view the status of each port/feature license along with a copy of the license keys installed on your Sonus SBC 1000/2000. The **Port Licenses** panel enables you to verify if a port is licensed and the number of available licensed ports. The **Feature Licenses** panel enables you to verify whether a feature is licensed, along with the number of remaining licenses available for a given feature at run-time.

The **Port Licenses** panel provides the following information:

- **Feature**. Indicates licensed TDM ports (DS1, BRI, FXS, FXO).
- **Licensed**. Indicates whether the port is licensed.
- **Number of Licensed Ports**. The total number of licensed ports in the node (this includes DSI, BRI, FXS, FXO).

The **Feature License** panel provides the following information:

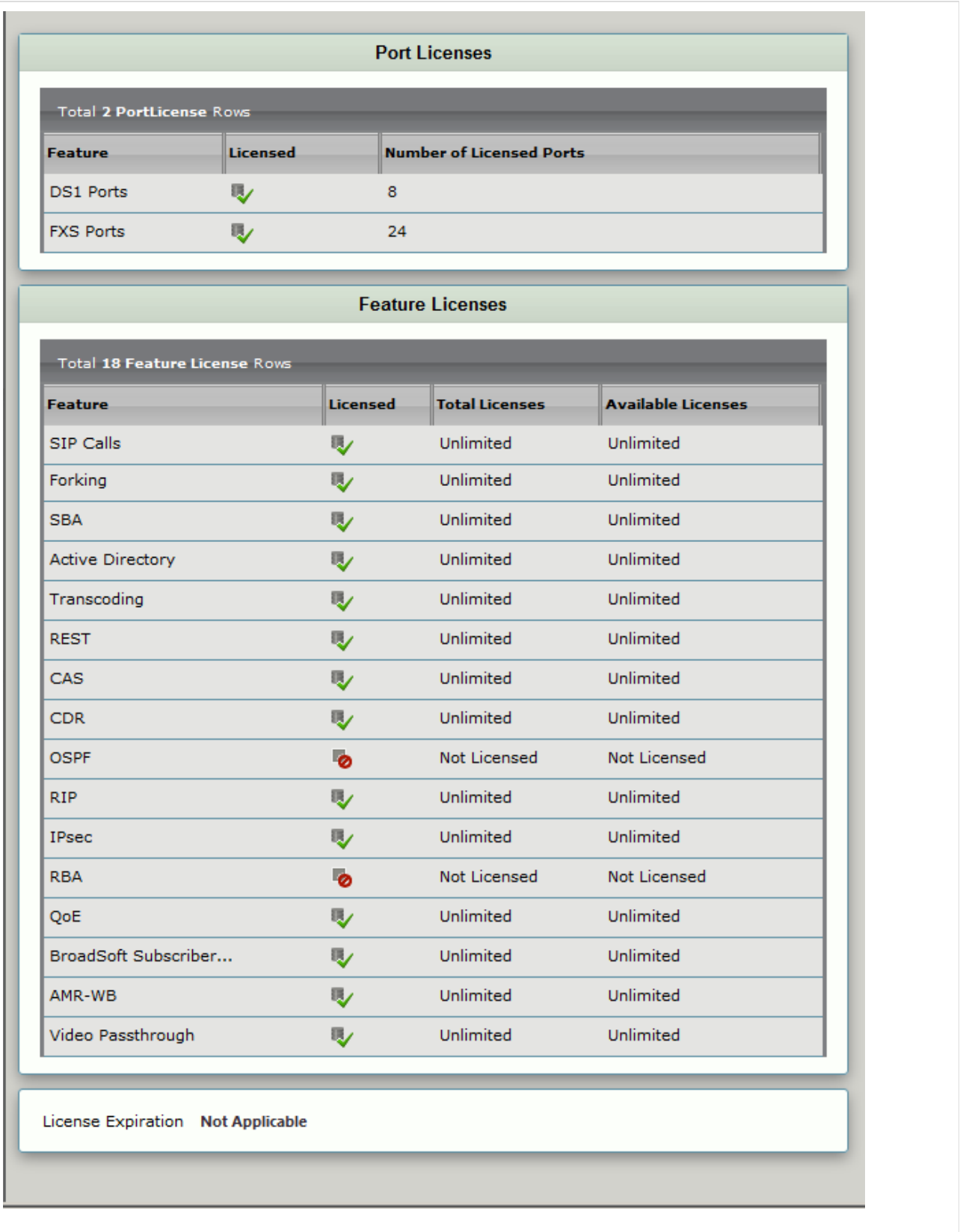
- **Feature**. Indicates licensed features.
- **Licensed**. Indicates whether the feature is licensed.
- **Total Licenses.** The total number of licenses in the node for the specified feature.
- **Available Licenses.** The number of unactivated licenses in the node for the specified feature.

To view your licenses:

1. In the WebUI, click the **Settings** tab.

Copyright © 2015 Sonus Networks. All rights reserved.

2. In the left navigation pane, go to **System> Licensing > Current Licenses**.



Port Licenses

Total **2 PortLicense** Rows

Feature	Licensed	Number of Licensed Ports
DS1 Ports	✓	8
FXS Ports	✓	24

Feature Licenses

Total **18 Feature License** Rows

Feature	Licensed	Total Licenses	Available Licenses
SIP Calls	✓	Unlimited	Unlimited
Forking	✓	Unlimited	Unlimited
SBA	✓	Unlimited	Unlimited
Active Directory	✓	Unlimited	Unlimited
Transcoding	✓	Unlimited	Unlimited
REST	✓	Unlimited	Unlimited
CAS	✓	Unlimited	Unlimited
CDR	✓	Unlimited	Unlimited
OSPF	⊘	Not Licensed	Not Licensed
RIP	✓	Unlimited	Unlimited
IPsec	✓	Unlimited	Unlimited
RBA	⊘	Not Licensed	Not Licensed
QoE	✓	Unlimited	Unlimited
BroadSoft Subscriber...	✓	Unlimited	Unlimited
AMR-WB	✓	Unlimited	Unlimited
Video Passthrough	✓	Unlimited	Unlimited

License Expiration **Not Applicable**

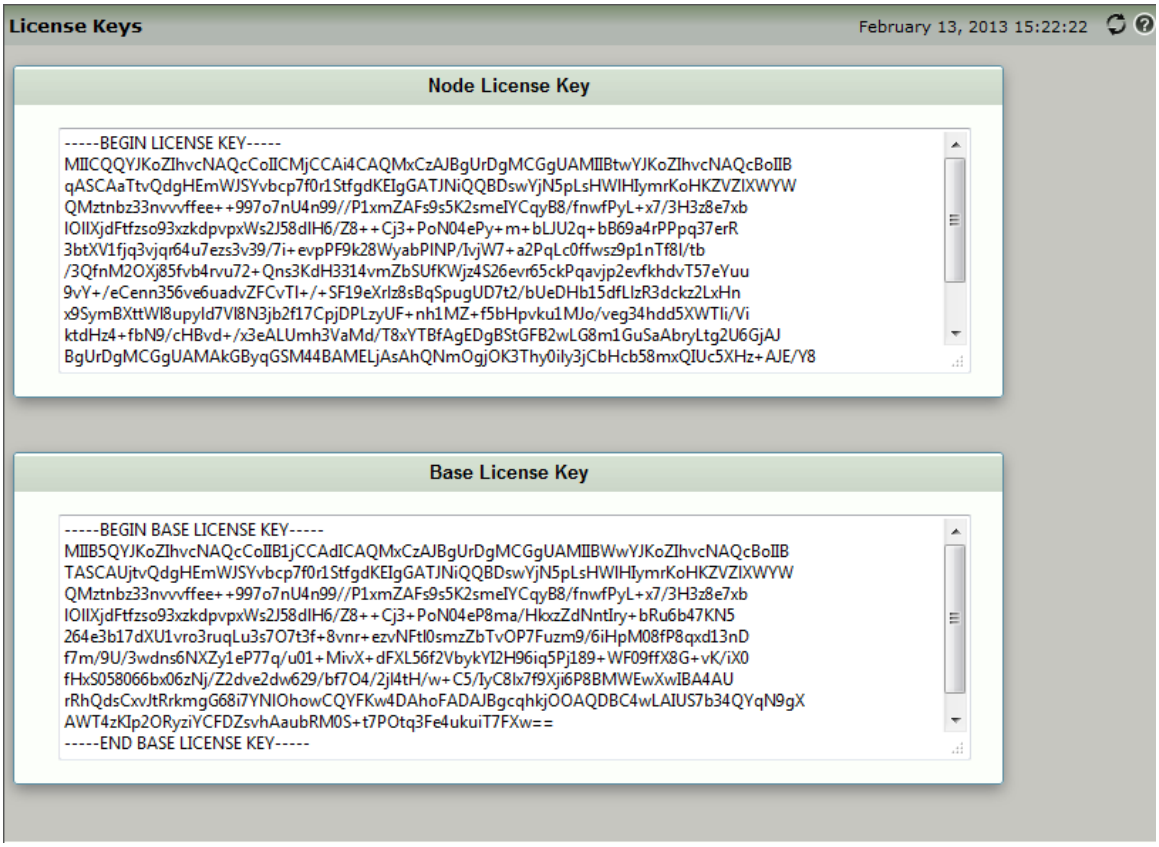
To View License Keys on Sonus SBC 1000/2000

The installed license key view is typically useful for record keeping or when asked to send the key during a

Copyright © 2015 Sonus Networks. All rights reserved.

troubleshooting case with an Sonus representative.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Licensing > License Keys**.



Working with Certificates

This section covers configuration and how-to related topics for certificates on the Sonus SBC 1000/2000 system.

Managing Server Certificates

- Generating Certificate Signing Requests
- Importing a Sonus SBC 1000-2000 Server Certificate
- Exporting Sonus SBC 1000-2000 Server Certificates

Managing Trusted CA Certificates

- Importing Trusted Root CA Certificates
- Exporting Trusted Root CA Certificates
- Viewing Trusted Root Certificate Chains

Requesting a Signed Certificate using a Standalone Windows CA

Downloading a CA Certificate using a Standalone Windows CA

Managing Server Certificates

By default, after having initialized the Sonus SBC 1000/2000 system for the first time, or after a factory reset, the Sonus SBC 1000/2000 system is pre-configured with a **Self-signed Server Certificate**.

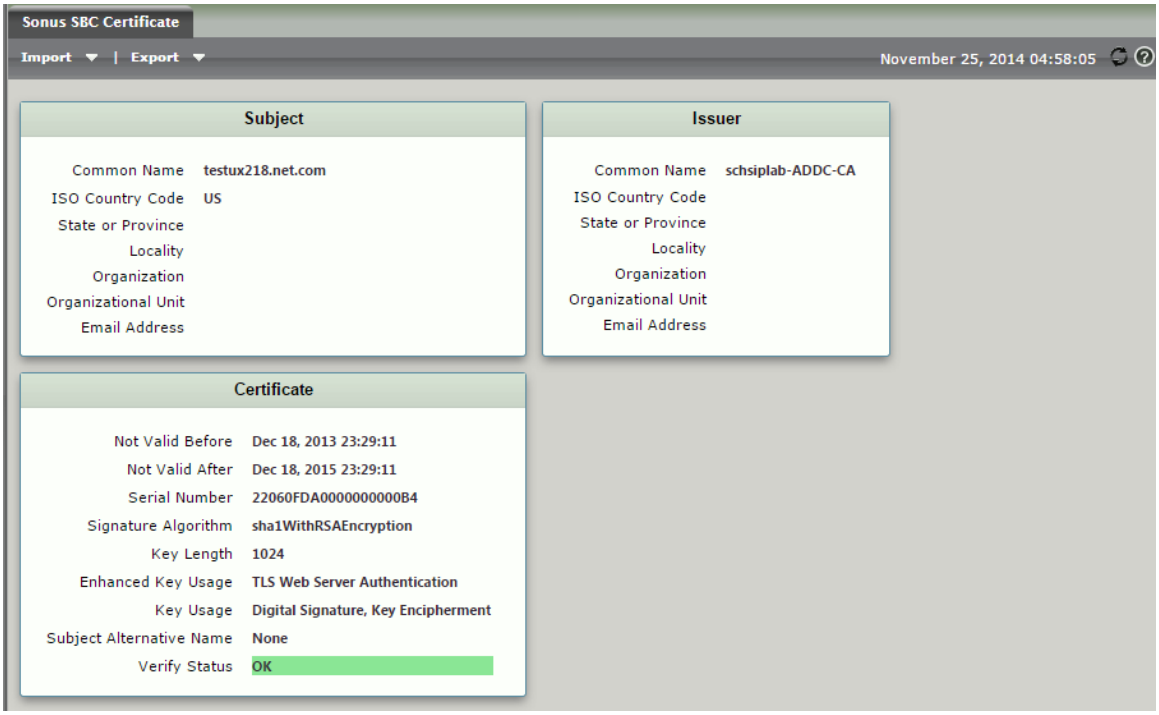
Copyright © 2015 Sonus Networks. All rights reserved.

The process of installing a new Signed Certificate on the Sonus SBC 1000/2000 comprises three general steps which must be followed in this specific order:

1. Generate a Certificate Signing Request (CSR)
2. Obtain and Import a Trusted Root CA Certificate
3. Obtain and Import the Signed Server Certificate

Viewing the Installed Sonus SBC 1000/2000 Server Certificate

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > SBC Certificates > Sonus Certificate**.



Related Topics

Generating Certificate Signing Requests

Importing a Sonus SBC 1000-2000 Server Certificate

Exporting Sonus SBC 1000-2000 Server Certificates

Generating Certificate Signing Requests

You can generate Certificate Signing Request (CSR) to be sent to a trusted Certificate Authority (CA) for signing and later importing on the Sonus SBC 1000/2000. This is typically done when requesting a new security certificate from the CA or when renewing an existing certificate.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > SBC Certificates > Generate Sonus SBC CSR**.

Copyright © 2015 Sonus Networks. All rights reserved.



Under the **Subject Distinguished Name panel**, fill in the fields pertaining to your environment.

The **Common Name** field should be of the form `Host.Domain` specified as specified while Running Initial Setup .

Important Note: the **Subject Alternative Name DNS** field should not be entered unless required by your environment/topology.

Once you have filled in the form, click **OK**. The CSR will be generated and displayed in the result text box.

Importing a Sonus SBC 1000-2000 Server Certificate

You can change the certificate installed on the Sonus SBC 1000/2000 system by obtaining the signed certificate from a Trusted CA or from a local Stand-Alone Windows Certificate Authority, and importing it as outlined in the instructions on this page.

Importing a Server Certificate

Before you begin

Before importing a new Signed Server Certificate, you must first import a valid Trusted CA Certificate.

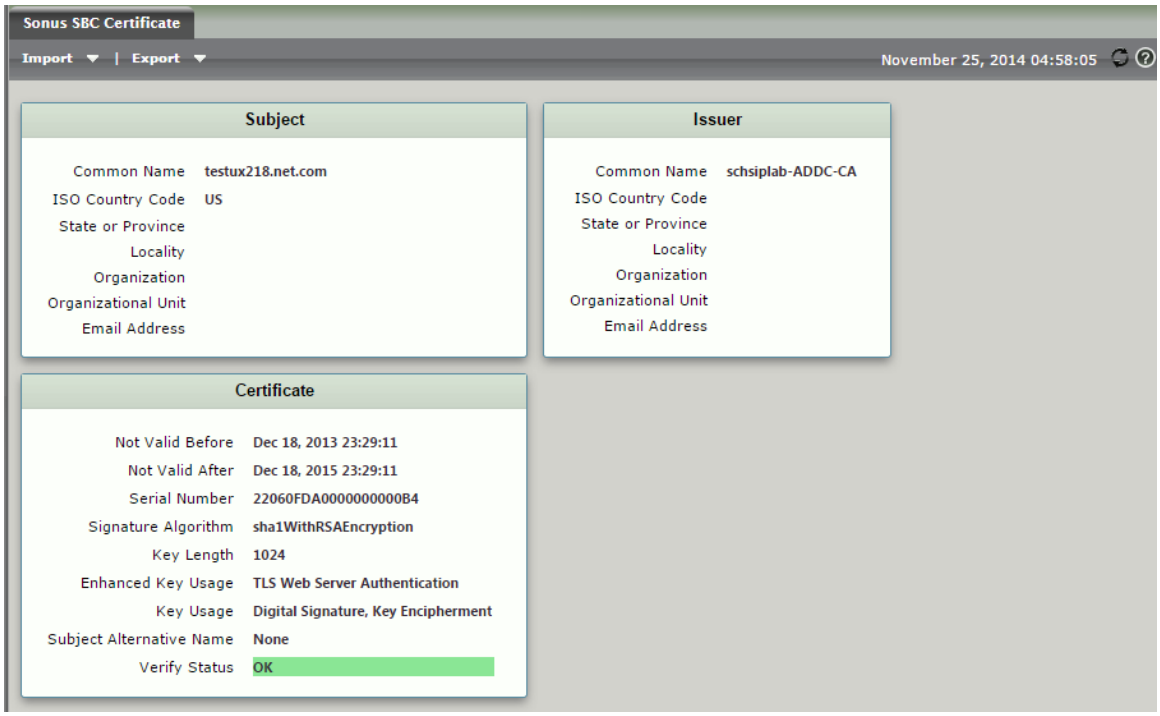
If your node has a SHA-2 256 signed server certificate, the SBC will not interoperate with Lync 2010 or earlier OCS/Lync versions. The signature algorithm (sha256WithRSAEncryption) is shown in the Certificate panel of the Sonus SBC Certificate page in the UI.

SHA2-256 Certificate Compatibility

SHA2-256 CA Certificates may be used for the SBA, SBC, and Lync 2013 Servers. Lync 2010 requires that all devices employ ALL SHA1 Certificates. For more information see the Microsoft SHA1 Deprecation Policy .

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > SBC Certificates > Sonus Certificate**.



Key Usage Field Descriptions

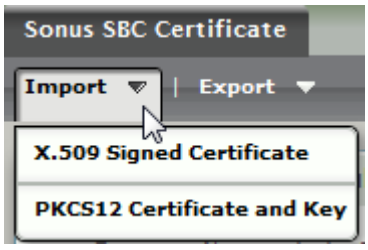
Enhanced Key Usage

This field displays the enhanced key usage regarding the purposes for which the subject's public key may be used.
TLS Web Server Authentication usage purpose is required in order to be compatible with some browsers.

Key Usage

Displays the key usage for defining the purposes of the key contained in the certificate.
Non-repudiation service purpose is disallowed in order to be compatible with some browsers.

To import an X.509 signed certificate:



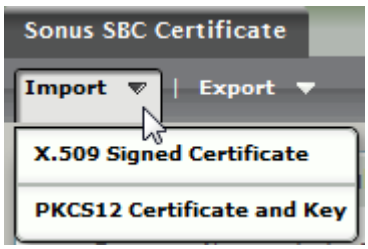
Copyright © 2015 Sonus Networks. All rights reserved.

1. Select **X.509 Signed Certificate** from the **Import** menu at the top of the page.
2. Chose the import mode(**Copy and Paste** or **File Upload**) from the **Mode** pull-down menu.



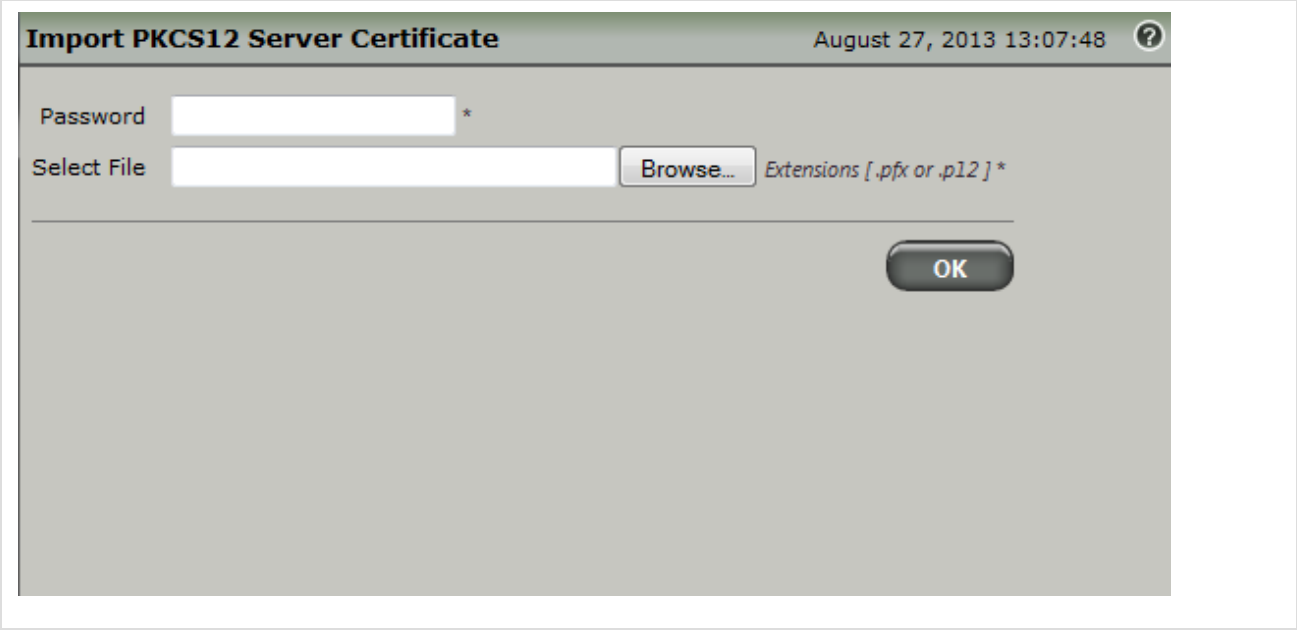
3. If you chose **File Upload**:
    a. Use the **Browse** button to find the file
    b. Click **OK**.
4. If you choose **Copy and Paste**:
    a. Open the file in a text editor.
    b. Paste the contents into the **Paste Base64 Certificate** text field.
5. Click **OK**.

To import a PKCS12 Certificate and Key:



1. Select **PKCS12 Certificate and Key** from the **Import**menu at the top of the page.

Copyright © 2015 Sonus Networks. All rights reserved.



2. Enter the password used to export the certificate in the **Password** field.
3. Browse for the PKCS certificate and key file.

> You must use the same password as was used when exporting the certificate and key.

4. Click **OK**

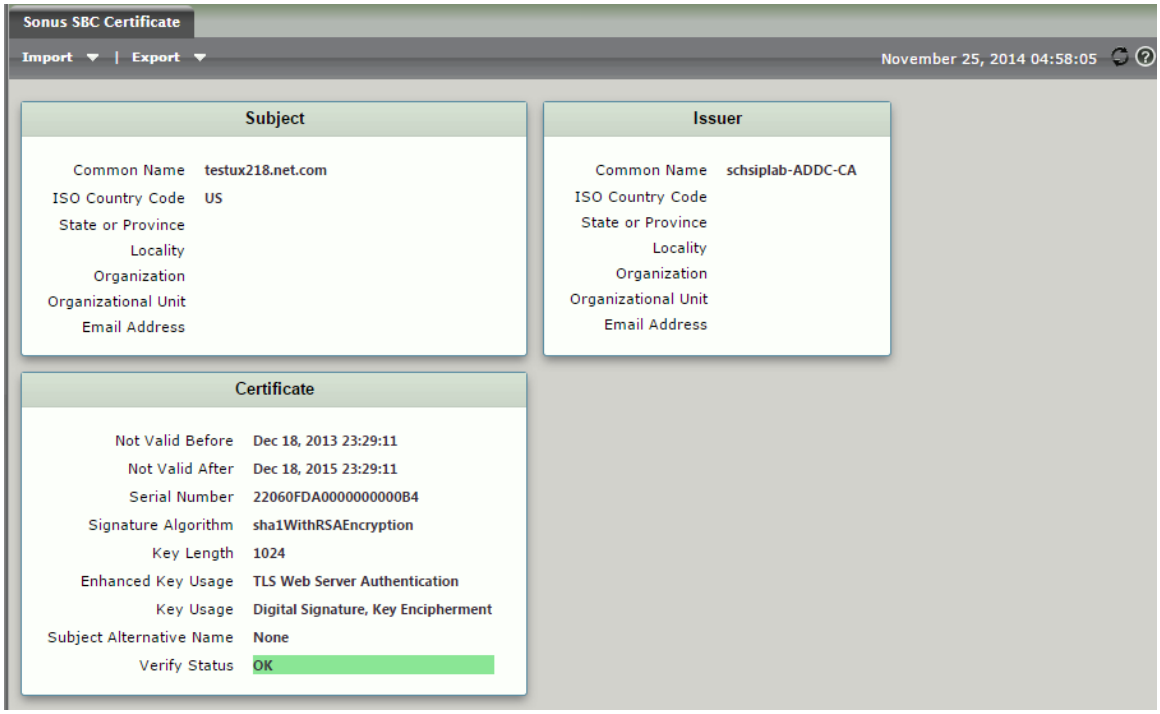
Verifying the Signed Server Certificate

Once you have imported the Signed Server Certificate:

1. In the **Issuer panel**, ensure the **Common Name** field has changed from **Self-Signed** to the issuer's Common Name.
2. In the **Certificate panel**,
   a. Ensure that the **Enhanced Key Usage** field indicates **TLS Web Server Authentication**.
   b. Ensure that the **Verify Status** field indicates **OK**.
   If the Verify Status field does not indicate OK, repeat the steps aboveto obtain a valid certificate.

> According to RFC3280, the **Netscape CertType** field is obsolete and has been replaced by the **X 509v3 Key Usage** field.
> Most modern browsers require the **Enhanced Key Usage** field for certificate acceptance based on use purpose.

Copyright © 2015 Sonus Networks. All rights reserved.



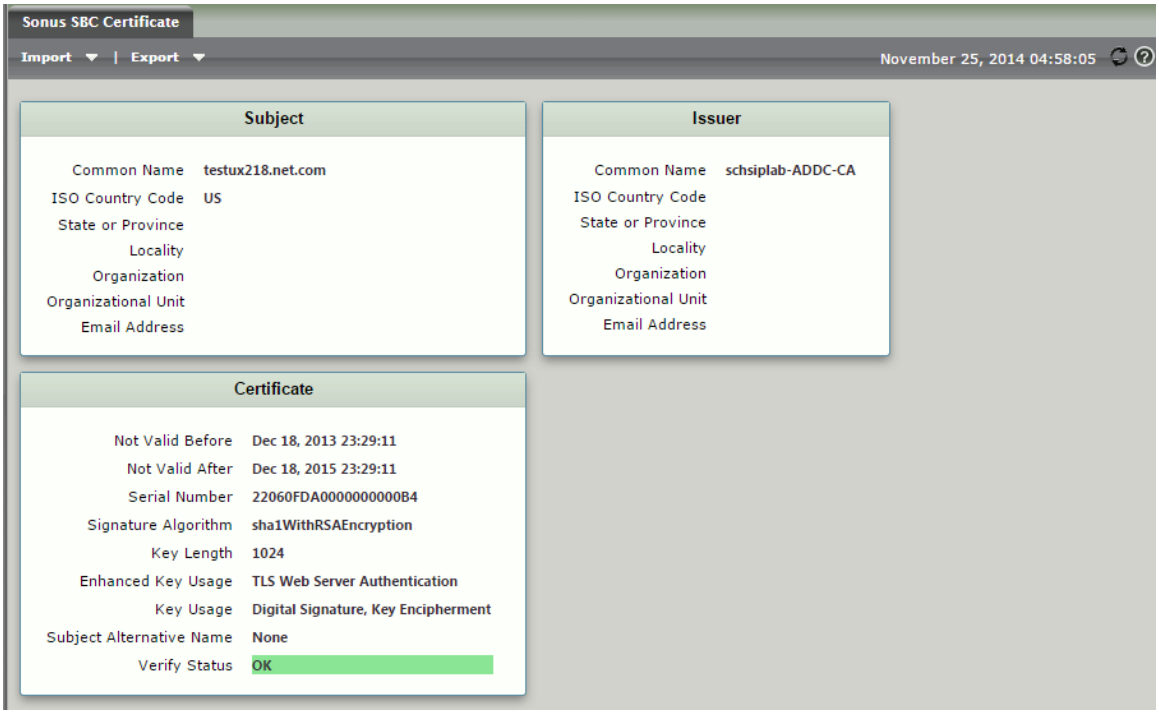
- Server (Sonus SBC 1000/2000) certificates with a 4096 RSA Key are **not** supported due to the amount of time required to generate a key and process calls.
- Trusted Root CA certificates with a 4096 RSA Key are supported, but have not been thoroughly tested.

Exporting Sonus SBC 1000-2000 Server Certificates

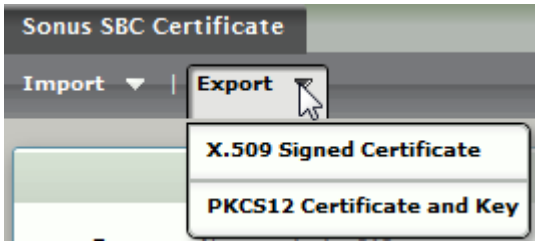
You can export the existing certificate installed on the Sonus SBC 1000/2000 at anytime by following these simple steps:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > SBC Certificates > Sonus Certificate**.

Copyright © 2015 Sonus Networks. All rights reserved.

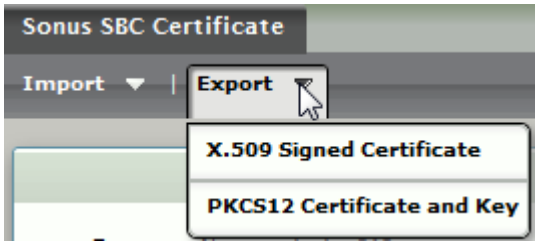


To export an X.509 Signed Certificate:



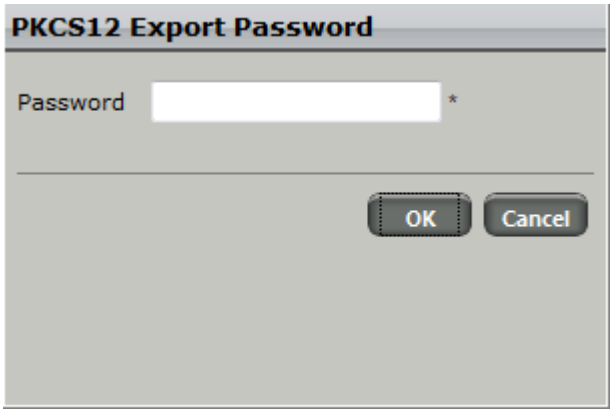
1. Select **X.509 Signed Certificate** from the **Export** menu at the top of the page.
2. Save the file in a convenient location.

To export a PKCS12 Certificate and Key:



1. Select **PKCS12 Certificate and Key** from the **Export**menu at the top of the page.

Copyright © 2015 Sonus Networks. All rights reserved.



2. Enter an export password in the **Password**field.

> **Note:**
>
> The password is user generated/supplied. It will be required in the import process for this certificate on another node.

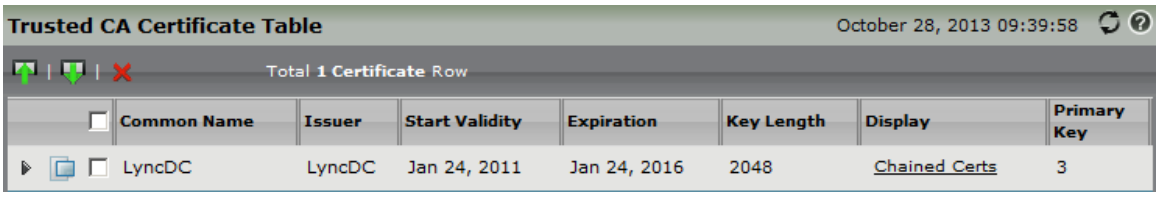
3. Click **OK**.

Managing Trusted CA Certificates

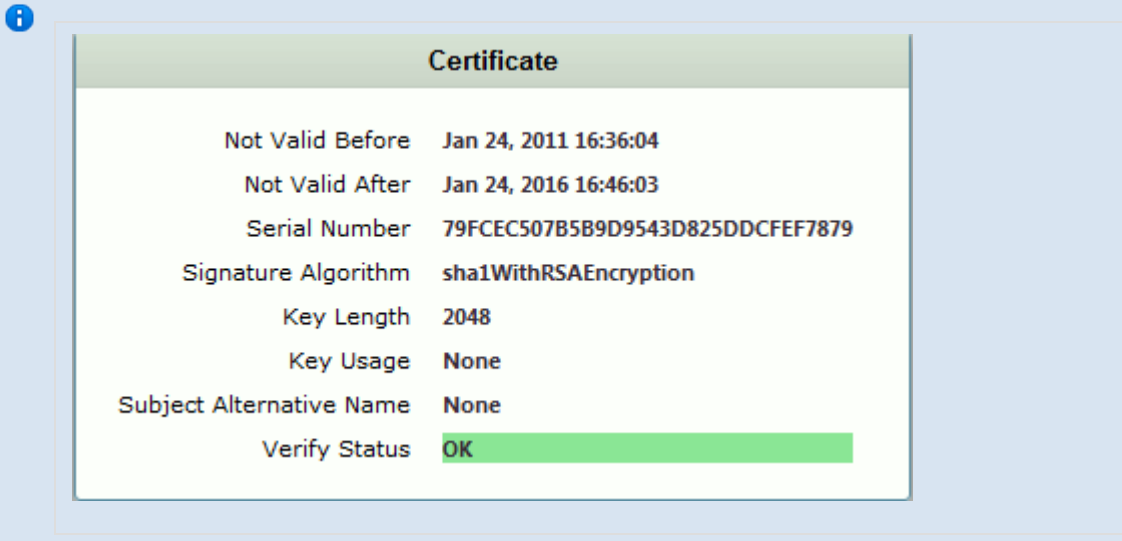
A Trusted CA Certificate is a certificate issued by a trusted certificate authority. Trusted CA Certificates are imported to the Sonus SBC 1000/2000 to establish its authenticity on the network.

Viewing the Installed Trusted CA Certificates

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > SBC Certificates > Trusted CA Certificates**.



Copyright © 2015 Sonus Networks. All rights reserved.



When the **Verify Status** field in the Certificate panel indicates Expired or Expiring Soon, the Trusted CA Certificate must be replaced. The old certificate must be *deleted before a new certificate can be successfully imported*.

To view a Trusted CA Certificate's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Importing Trusted Root CA Certificates

Exporting Trusted Root CA Certificates

Viewing Trusted Root Certificate Chains

Importing Trusted Root CA Certificates

This page describes the process of importing Trusted Root CA Certificates, using either the **File Upload** or **Copy and Paste** methods.

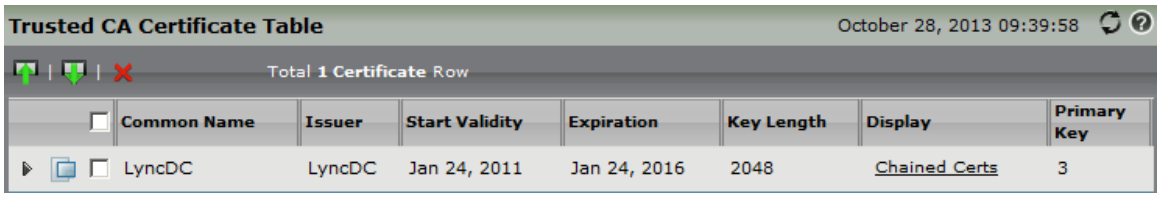
Importing a Trusted Root CA Certificate

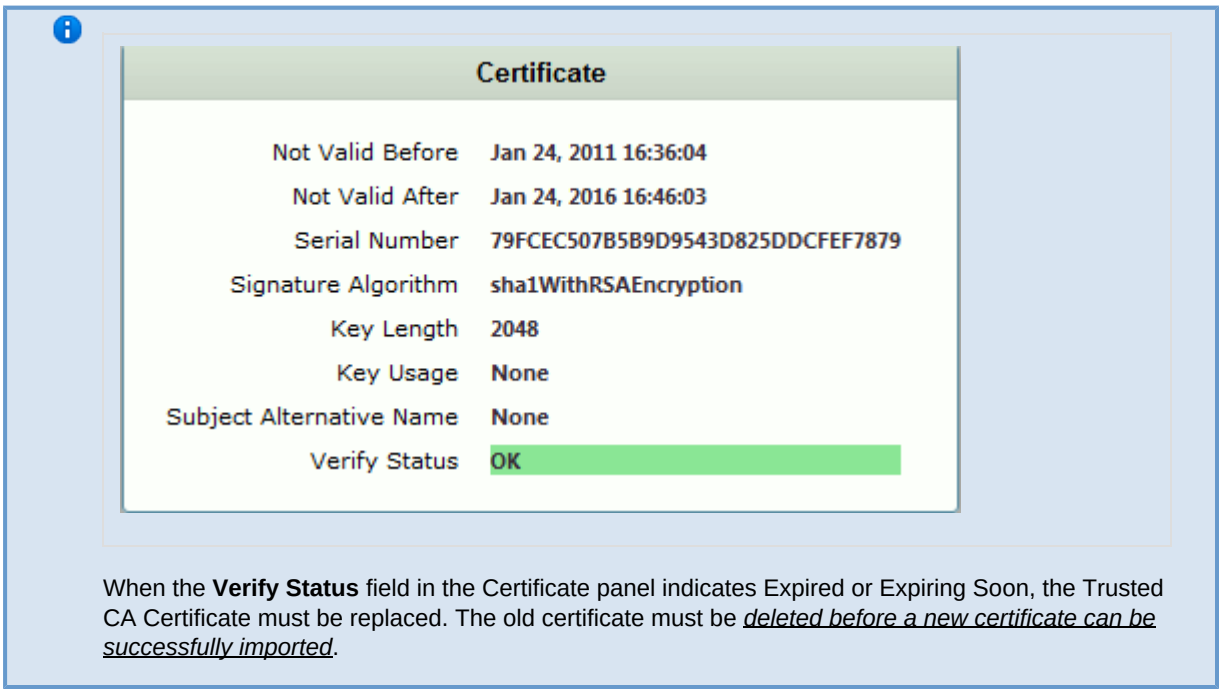
Before you begin: you must obtain a Trusted Root CA Certificate before you can proceed - your options are:

- Contacting your System Administrator or Certificate Vendor (e.g., Verisign), or
- Obtaining the Trusted CA certificate from your local Standalone Windows Certificate Authority

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > SBC Certificates > Trusted CA Certificates**.

Copyright © 2015 Sonus Networks. All rights reserved.

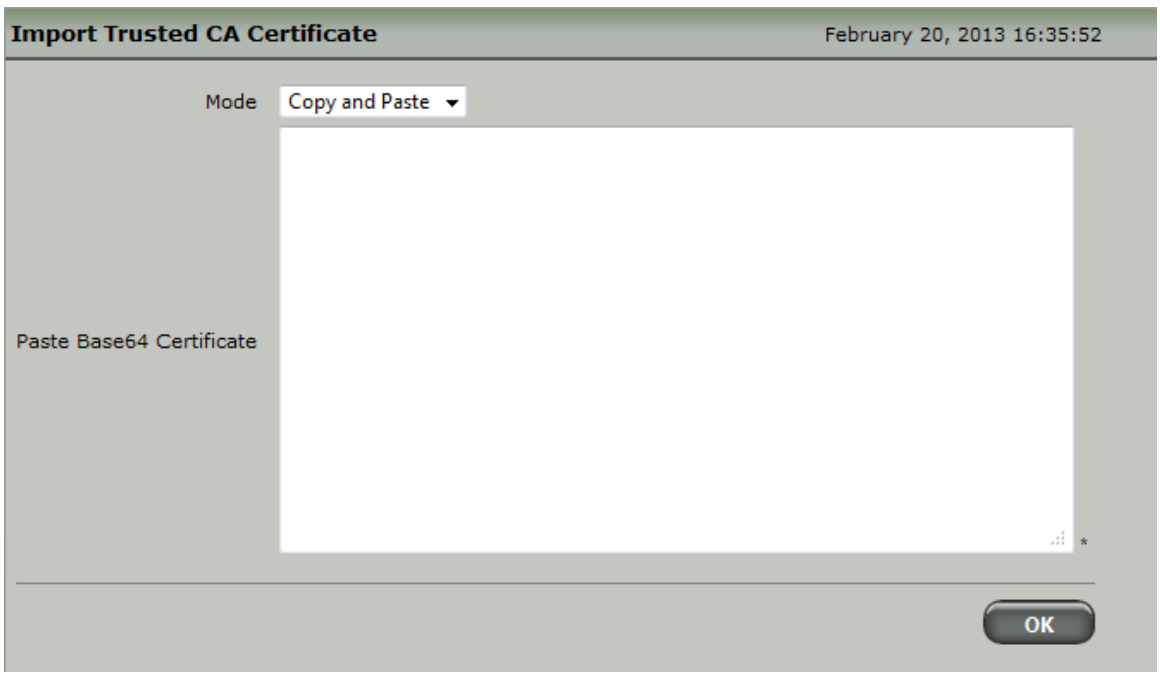




When the **Verify Status** field in the Certificate panel indicates Expired or Expiring Soon, the Trusted CA Certificate must be replaced. The old certificate must be *deleted before a new certificate can be successfully imported*.

To import a Trusted CA Certificate:

1. Click the Import Trusted CA Certificate ( ) Icon.



2. Select either **Copy and Paste** or **File Upload** from the **Mode**menu.

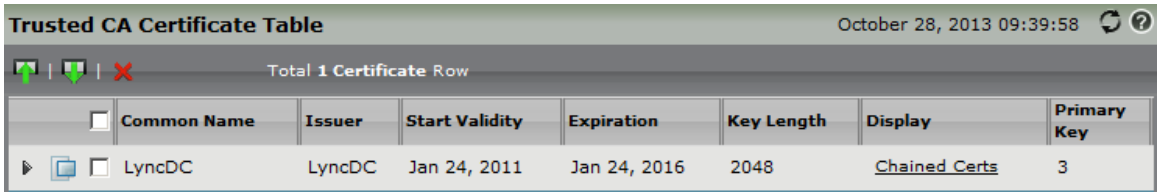
Copyright © 2015 Sonus Networks. All rights reserved.

a. If you choose **File Upload**, use the **Browse** button to find the file.

3. Click **OK**.

Verifying the Trusted Root CA Certificate

In the **Trusted CA Certificate Table** page:



1. View the certificate's details by clicking the popup( ) icon next to the entry you want to view.
2. Under the the **Certificate panel**, ensure that the **Verify Status** field indicates **OK**.
   If the **Verify Status** field does not indicate **OK**, repeat the import steps again to obtain a valid certificate.

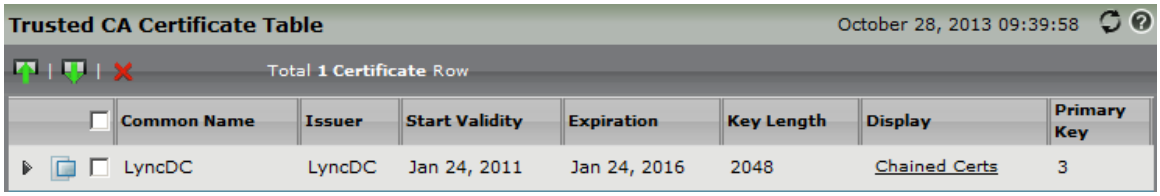
- Trusted Root CA certificates with a 4096 RSA Key are supported, but have not been thoroughly tested.
- Server (Sonus SBC 1000/2000) certificates with a 4096 RSA Key are **not** supported due to the amount of time required to generate a key and process calls.

Exporting Trusted Root CA Certificates

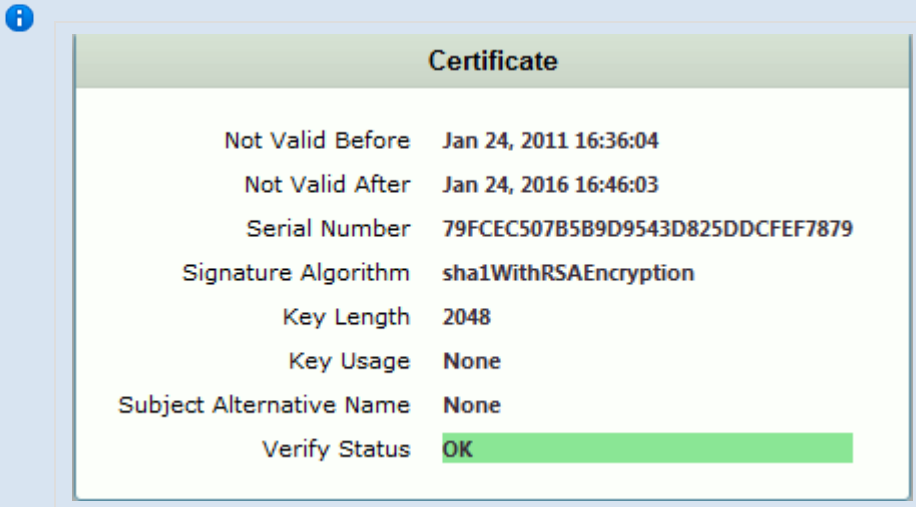
You can export all Trusted Root CA Certificates currently installed on the Sonus SBC 1000/2000 system via the WebUI.

Exporting a Trusted Root CA Certificate

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > SBC Certificates > Trusted CA Certificates**.



Copyright © 2015 Sonus Networks. All rights reserved.



When the **Verify Status** field in the Certificate panel indicates Expired or Expiring Soon, the Trusted CA Certificate must be replaced. The old certificate must be *deleted before a new certificate can be successfully imported*.

To export a Trusted CA Certificate:

1. Select the check box next to the certificate in the **Trusted CA Certificate Table** you wish to export.
2. Click the **Export Trusted CA Certificate** ( ) icon at the top of the Trusted CA Certificate Table.
3. Click **OK** in the confirmation dialog box.
4. Save the file in a convenient location.

Viewing Trusted Root Certificate Chains

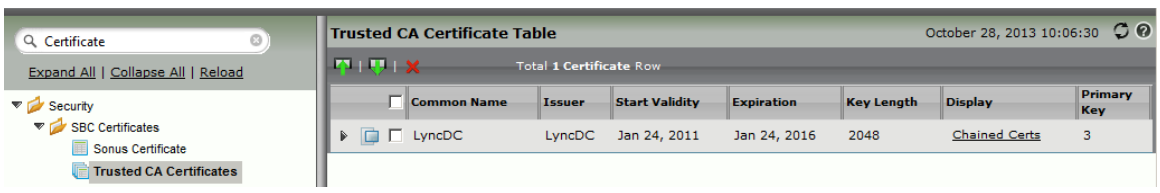
Sonus SBC 1000/2000 supports the display of a **Trusted Root's Certificate Chain** that allows you to see the chained certificate along with its associated details. This article describes how to view chained certificates on the Sonus SBC 1000/2000.

Trusted CA certificates

There are two different types Trusted CA Certificates that can be uploaded to the Sonus SBC 1000/2000 using the Web User Interface:

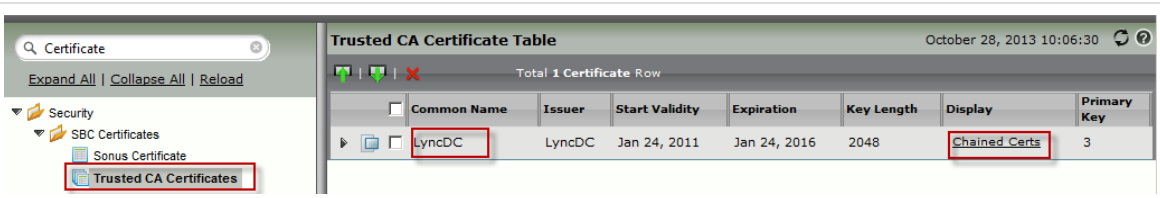
1. Trusted Root Certificate **Chain**
2. Trusted Root Certificate

In earlier system releases versions of Sonus SBC 1000/2000 (1.2.x and earlier), although a **Trusted Root Certificate Chain** could be imported to **Trusted CA Certificates**, the Web UI would not distinguish whether the certificate is **Chained** or not:



Copyright © 2015 Sonus Networks. All rights reserved.

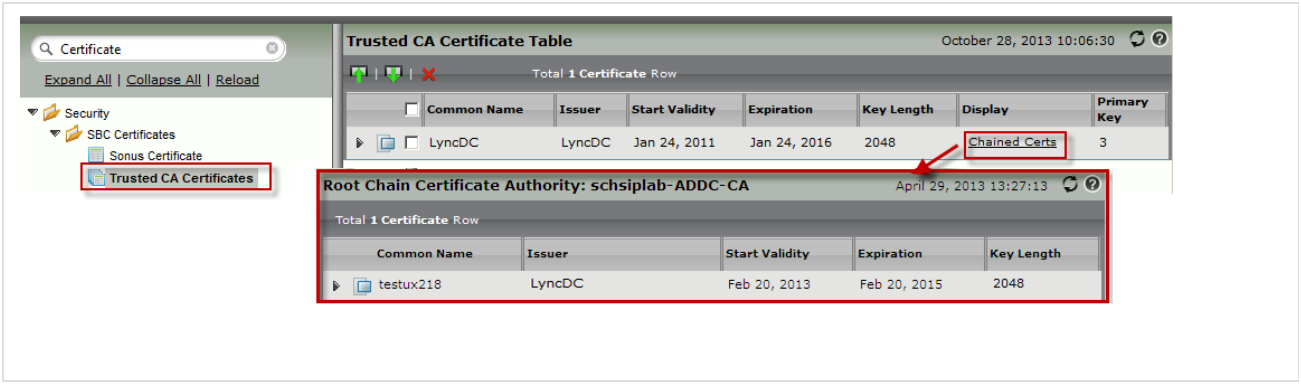
Starting with system release version 1.3.0, there is a new **Display** column on the user interface to distinguish one from another as shown below:



If you click the **Chained Certs** link, a window pop up will dispatch with details of the **Root Chain CA** as shown below:

To view the Chained Certificates:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > SBC Certificates > Trusted CA Certificates**.



Requesting a Signed Certificate using a Standalone Windows CA

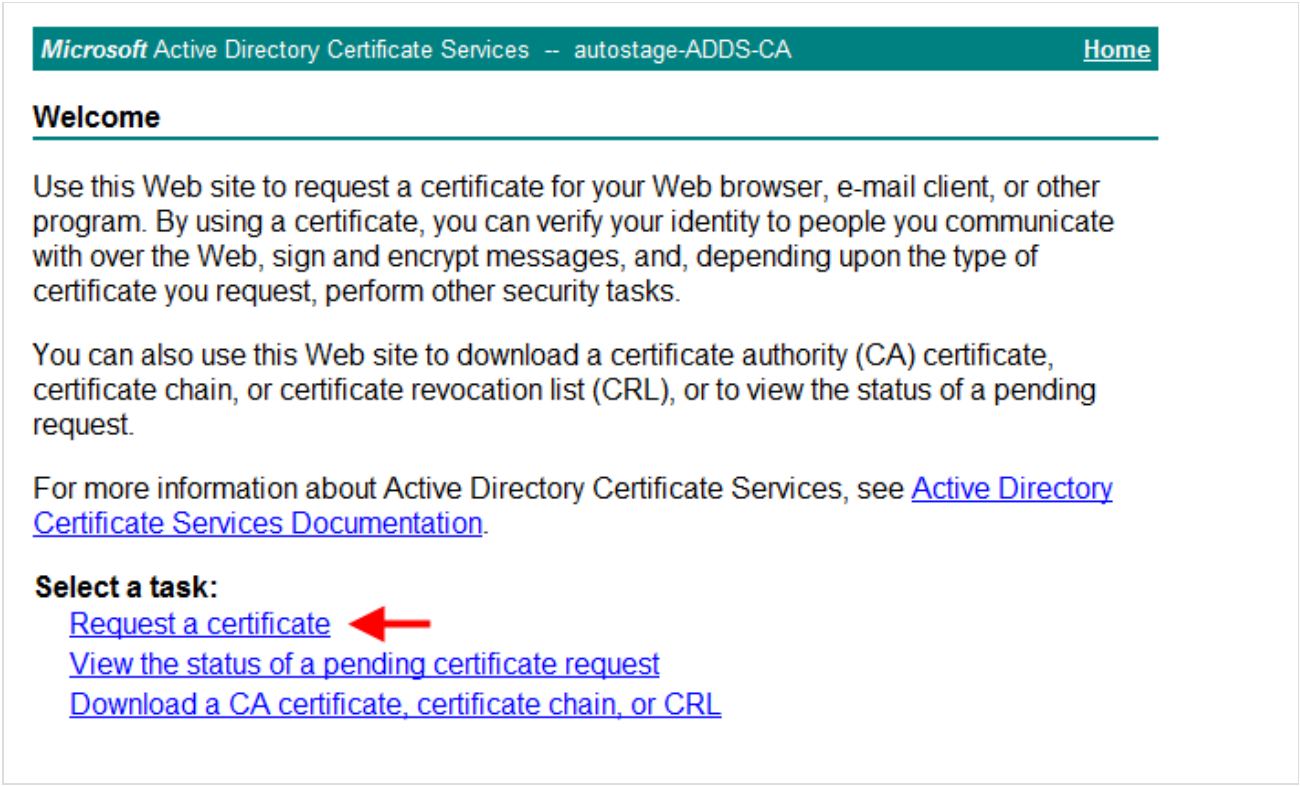
If your environment has Windows Server (2008) with Active Directory Certificate Services (AD CS) installed, you can use it to request a signed certificate.

Requesting a Signed Certificate using a Windows AD CS

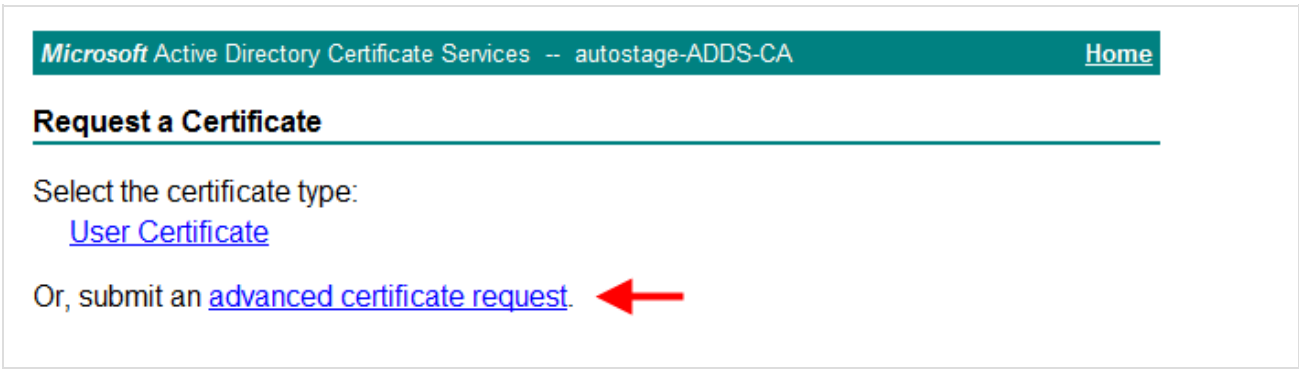
> **Before you begin:** You will need to generate a certificate signing requests.

1. Using a Web Browser, go to your Windows AD CS hosted site — typically `http://<ip.or.fqdn.of.windows.ca.server>/certsrv`
2. Click the **Request a certificate** link:

Copyright © 2015 Sonus Networks. All rights reserved.

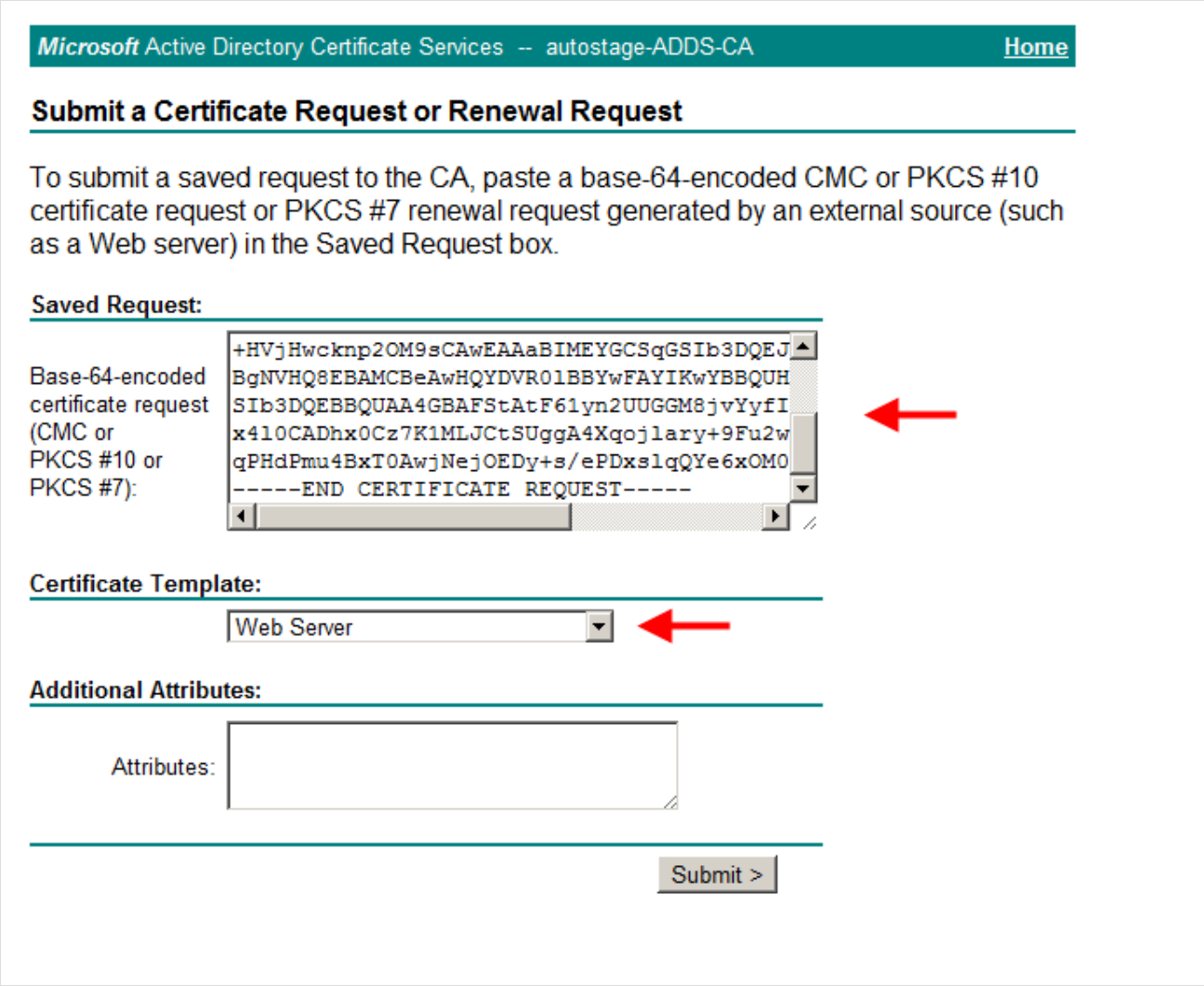


3. Click **advanced certificate request**

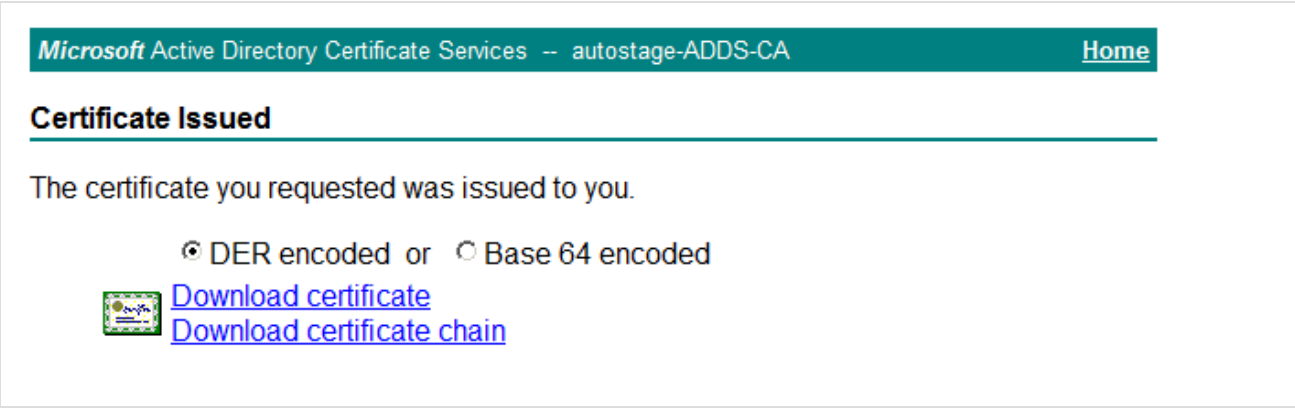


4. Paste the **Certificate Signing Request** in the **Saved Request** text field
5. Select **Web Server** from the Certificate Template drop-down menu.

Copyright © 2015 Sonus Networks. All rights reserved.



6. Click **Submit**. You will be presented with a screen to download the signed certificate:



7. Select either **DER encoded** or **Base 64 encoded** - each option will the determine how the certificate will be imported on the Sonus SBC 1000/2000
    a. If you select the DER option, use the File Upload mode when importing.
    b. if you select the Base 4 option, use the Copy and Paste mode when importing.
8. Click the **Download certificate chain** link.
9. Save the file to your desktop or other convenient location.

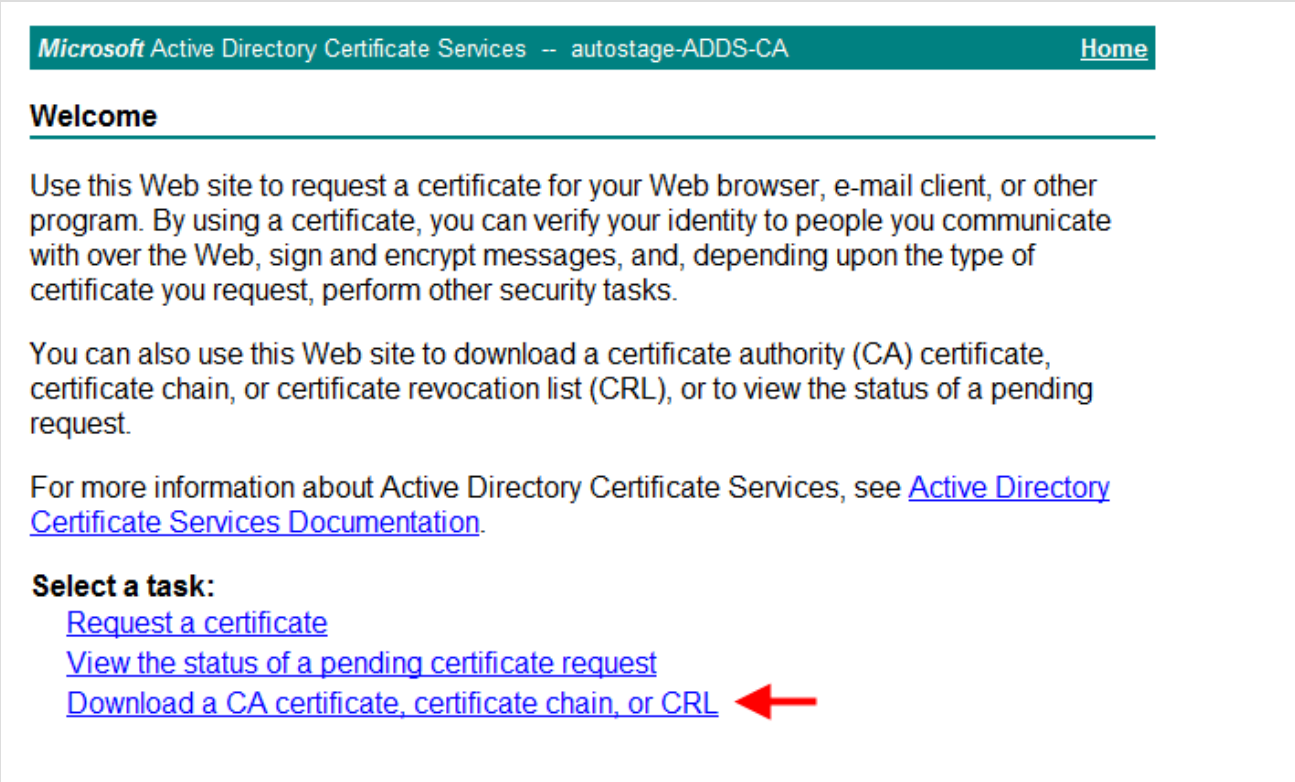
Downloading a CA Certificate using a Standalone Windows CA

Copyright © 2015 Sonus Networks. All rights reserved.

If your environment has Windows Server (2008) with Active Directory Certificate Services (AD CS) installed, you can use it to download its CA certificate chain and later importing it into the Sonus SBC 1000/2000.

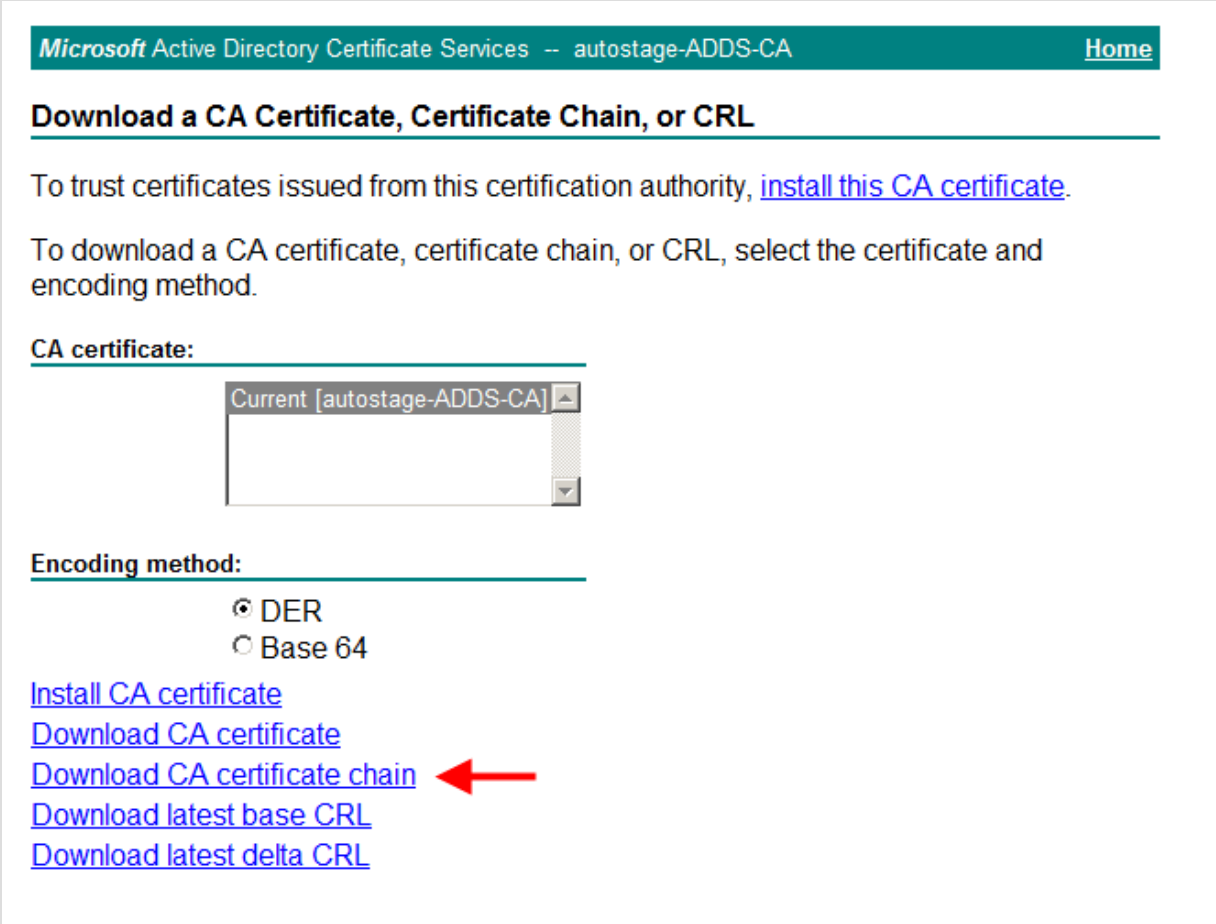
Downloading a CA Certificate Chain using a Windows AD CS

1. Using a Web Browser, go to your Windows AD CS hosted site — typically `http://<ip.or.fqdn.of.windows.ca.server>/certsrv`
2. Click on the **Downolad a CA certificate, certificate chain, or CRL**link.



3. Select either **DER encoded** or **Base 64 encoded** - each option will the determine how the certificate will be imported on the Sonus SBC 1000/2000
    a. If you select the DER option, use the File Upload mode when importing.
    b. if you select the Base 64 option, use the Copy and Paste mode when importing.

Copyright © 2015 Sonus Networks. All rights reserved.



4. Click the **Download CA Certificate chain** link.
5. Save the file to your desktop or other convenient location

Integrating with Active Directory

The Sonus SBC 1000/2000 system acts as an Active Directory client. By default, the Sonus SBC 1000/2000 is able to obtain any readable field in the Active Directory.

Accessing Active Directory

Accessing AD values requires that we have an account with credentials on the particular domain to be queried. Anonymous binds to AD are typically not supported by the domain controller. Administrators are required to create a new user in their system (following standard Active Directory add user practices), preferably one whose credentials never expire, and configure these credentials in Sonus SBC 1000/2000. Sonus SBC 1000/2000 will use these configured credentials when communicating with AD.

> If for some reason the Active Directory server is unreachable, access to Sonus SBC 1000/2000 will fall back to local-only.

Active Directory Queries and Domain Membership Requirements

Domain membership is not required for the Sonus SBC 1000/2000 to query Active Directory. It is important to note that Global Catalog binds are not supported. Only LDAP binds are used to query and collect Active Directory data.

Copyright © 2015 Sonus Networks. All rights reserved.

The configuration requires the domain controller's IP address to be specified. Multiple domain controllers can be configured. The list will be traversed in order if any of the former entries fail to bind. If all the IPs are unreachable or fail to bind, the Sonus SBC 1000/2000 will retry the bind at one minute intervals.

The Sonus SBC 1000/2000 supports multiple domains within the same AD forest. That way the domains have internal trust and hence, the Sonus SBC 1000/2000 can access them with the same user. If mapping to a domain group in a specific domain is required, you need to create a group with a unique group name in that specific domain, so that you can map to that group. If the group name is not unique, the Sonus SBC 1000/2000 is going to query each domain controller for the same group.

Global Catalog binds are not supported. Only LDAP binds are used to query and collect Active Directory data.

In case a user group is configured under multiple authorization modes, the highest authorization level is used. For example, if a user belongs to multiple groups with authorization levels Administrator and Read Only, the user will be authorized as an Administrator.

Related Topics

Configuring the Sonus SBC 1000-2000 for Active Directory

- Managing Active Directory Caching and Statistics

Configuring the Sonus SBC 1000-2000 for Active Directory User Domain Access

Managing Domain Controllers

- Adding and Modifying Domain Controllers

Managing Active Directory Groups to Access Level Mapping

- Creating and Modifying Active Directory Groups Access Level Mapping

Querying the Active Directory Cache

Configuring the Sonus SBC 1000-2000 for Active Directory

This page explains how to configure the Sonus SBC 1000/2000 to use Active Directory services.

This process comprises three parts:

- Active Directory Configuration
- Cache Settings
- User Authentication Settings

The Active Directory configuration part is where you turn on Active Directory (AD), set the way the Sonus SBC 1000/2000 will communicate with the AD server.

The Cache Setting part is where you set up AD attribute caching.

The User Authentication Settings section is where you determine which domain controllers to use.

For additional information about Active Directory, see Call Routing Based on Active Directory User Attributes and Basic AD-based Call Routing for Dummies.

Before You Begin

Copyright © 2015 Sonus Networks. All rights reserved.

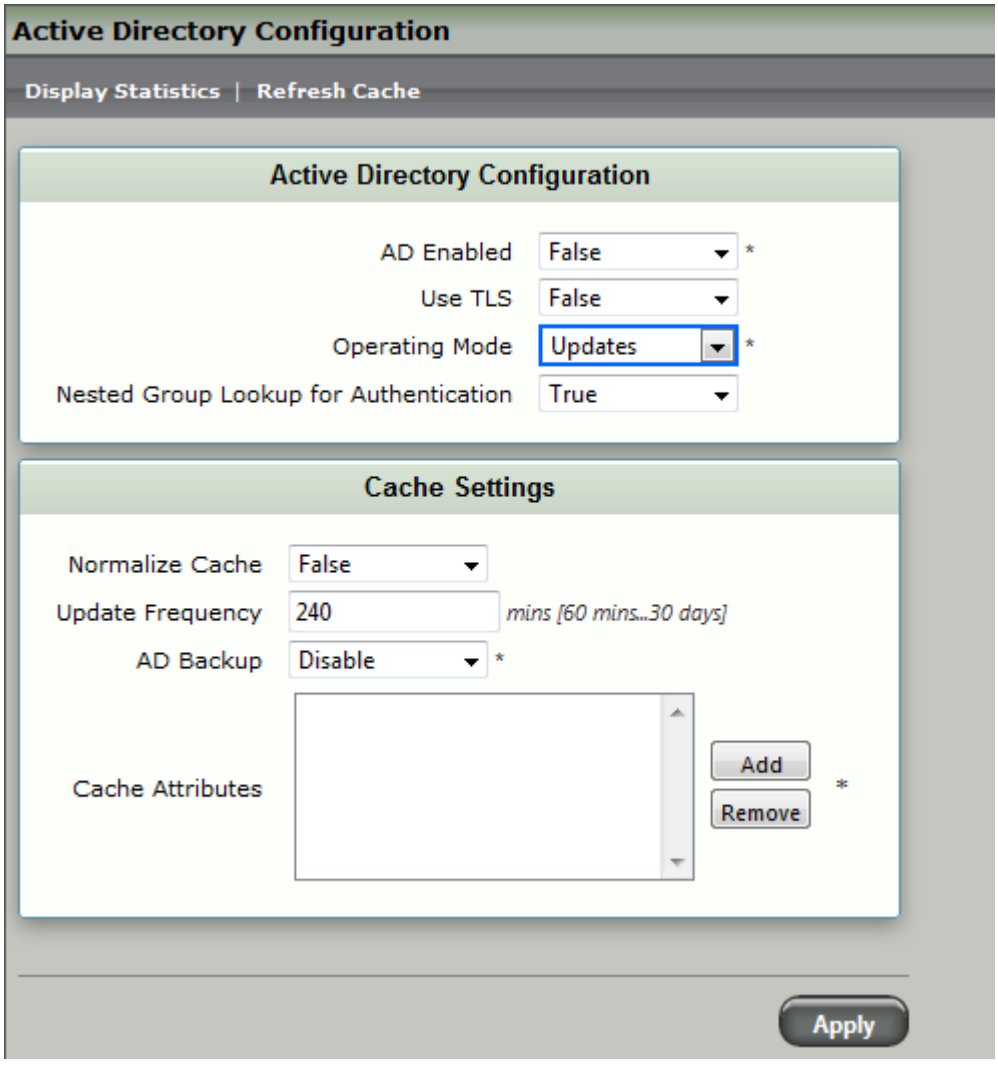
Before you begin, there some things you need to decide:

- Whether or not you are going to use TLS.
- What operating mode you intend to use.
  - Updates - a local cache is built and used to look up AD searchable fields. User authentication is enabled in this mode.
  - Online - Communication with Active Directory is done with queries and no information is cached.
  - Auth-only - This mode allows user authentication using Active Directory, and no queries are allowed.
  - Cache Lookup Only - When selected the SBC examines only the local AD Cache for the requested attribute, if none is found the call fails.

You must have already defined and added at least one domain controller to the Domain Controllers Table.

Configuring Active Directory Services on Your Sonus SBC 1000/2000

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Auth and Directory Services > Active Directory > Configuration**.



Active Directory Configuration - Field Definitions

The fields in the Active Directory Configuration panel determine the manner in which Sonus SBC 1000/2000

Copyright © 2015 Sonus Networks. All rights reserved.

communicates with the Active Directory server.

AD Enabled

Specifies the administrative state of the Active Directory resource.

Use TLS

Specifies whether or not Transport Layer Security (TLS) is used while communicating with Active Directory.

- TLS = FALSE: MD5 Digest is used to secure the AD password over the wire.

> Since **DCs do not support referral chasing or nested group lookups with MD5 Digest**, you can't log in to Sonus SBC 1000/2000 using AD credentials if those credentials require referral chasing or nested group lookup by the DC. Instead, you can individually configure each DC you wish to query when someone attempts to log into the Sonus SBC 1000/2000.

- TLS = TRUE: TLS will be used to secure all communcation for requests to the DC.

> Referral chasing and nested group lookups are supported with TLS enabled. Again, this applies only to authenticating users attempting to log into the Sonus SBC 1000/2000.

> AD lookups for **call routing** are executed the same regardless of the AD TLS configuration. **DC s do not support referral chasing for call route lookups**, therefore you must individually configure each DC that you wish to search for AD call routing queries.

Operating Mode

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the method used by the Sonus SBC 1000/2000 to communicate with Active Directory in order to achieve a balance between performance and accuracy.

- **Online:** All AD queries are sent directly to the DC - no information is cached. User authentication using Active Directory is also enabled in this mode. Online mode can result in a heavy DC load, thus using Online mode is not recommended.
- **Updates:** In this mode, a local cache is built and used to lookup Active Directory searchable fields. If the SBC's cache is filled to capacity, first the cache, then the DC will be queried in attempts to find a match. User authentication using Active Directory is also enabled in this mode; however, sensitive information (including passwords) is not cached.
- **Auth-Only:** Allows user authentication using Active Directory, but no Active Directory queries are allowed.
- **Cache Lookup Only:** When selected, the SBC examines **only** the local AD Cache for the requested attribute. Even if the cache is filled to capacity, the DC will not be queried. The call fails if no match is found in the local cache.

SBC 1000 Note:

Sonus recommends the use of an external flash drive for AD Cache backup on the SBC 1000 when either the **Updates** or **Cache Only** mode is the selected operating mode.

An SNMP alarm will be generated if the local AD cache reaches capacity.

If your cache reaches capacity when in Update Mode, the SBC will automatically query the DC for any entries that are not cached. Queries to the DC are never normalized. Routing may intermittently fail if your transformations rely on normalized cache entries.

Be aware that Cache Normalization is not performed on queries to the DC, even in Update Mode with *Normalize Cache* set to *True*. Therefore, transformations that rely on normalization (e.g. msRTCSIP-Line transformations that do not include tel:) will fail for queries that resort to a DC lookup. If you're cache reaches capacity:

- Reduce the number of cached attributes so that the cache is no longer at capacity
- Set *Normalize Cache* to *False* and modify any transformation that relies on the cache being normalized. (suggested)
- Add transformations to route both normalized and non-normalized AD call route queries. (avoid)

Nested Group Lookup for Authentication

Specifies whether or not nested group lookups are performed to authorize users. Applies only to authentication domain controllers.

Cache Settings - Field Definitions

The fields in the Cache Settings panel determine how Active Directory attributes are cached locally and the frequency at which the local cache is updated. The Sonus SBC 1000/2000 maintains a local cache of Active Directory user attributes. AD caching enhances system performance and survivability.

- **Performance:** Performance is enhanced by eliminating the need to communicate with and query the Active Directory server for each and every call. This improves the performance of the AD server, and has the added

Copyright © 2015 Sonus Networks. All rights reserved.

benefit of increasing call speeds and relieving load on the network.

- **Survivability:** In the event of a loss of communication with the Active Directory, whether through a loss of network connectivity or an AD server error, the Sonus SBC 1000/2000 is still able to perform authentication and authorization tasks based on the Local AD Cache.

Normalize Cache

Specifies whether or not to strip special characters such as dashes "-", parenthesis "(", ")", spaces " ", "tel:" and "sip:" from the values while building a local active directory cache. However, normalization does not apply to name and email fields.

Update Frequency

Specifies the interval, in minutes, between local Active Directory cache updates.

> The Local AD Cache can be updated manually at any time by clicking the **Refresh Cache** text at the top of the Active Directory Configuration page.

Configure Initial Update Time

Specifies when the AD Cache is updated upon initial SBC power up or after an AD Configuration has been edited and applied. If set to **True**, the system waits until the time specified in the **First Update Time** field before updating the AD Cache. If set to **False** the AD Cache is updated immediately upon start up or when a new/edited configuration is applied.

First Update Time

Specifies the time (system time) at which the first AD Cache update occurs after initial SBC power up or after an AD Configuration has been edited and applied. This field is visible only when the **Configure Initial Update Time** field is set to **True**.

> The last saved AD Cache is used until the first update specified by this field occurs.

AD Backup

When **Enabled**, the SBC will raise an alarm and send an SNMP Trap if the AD Cache backup fails. This parameter controls the alarm and trap generation only. It does not control the AD Cache backup function.

Cache Attributes

Specifies which attributes are cached from Active Directory. The attribute names specified must be consistent with attribute names in Active Directory.

> Be careful! Attribute names are case sensitive.

Managing Active Directory Caching and Statistics

Managing Active Directory Caching and Statistics

Manual AD Cache Refresh and Statistics

Copyright © 2015 Sonus Networks. All rights reserved.

This page explains how to configure the Sonus SBC 1000/2000 to use Active Directory services.

Active Directory Caching

Sonus SBC 1000/2000 employs a Local AD Cache in an effort to enhance system performance and survivability.

Performance

Performance is enhanced by eliminating the need to communicate with and query the Active Directory server for each and every call. This improves the performance of the AD server, and has the added benefit of increasing call speeds and relieving load on the network.

Survivability

In the event of a loss of communication with the Active Directory, whether through a loss of network connectivity or an AD server error, the Sonus SBC 1000/2000 is still able to perform authentication and authorization tasks based on the Local AD Cache.

Sonus SBC 1000/2000 Model Differences

If the Sonus SBC 1000/2000 system is rebooted during an Active Directory Server outage, the Sonus SBC 1000/2000 will use its local AD cache for authentication (post power up) if:

- **Sonus SBC 1000**: an external USB storage drive is attached to the Sonus SBC 1000 main board. Without it, the local AD cache is purged between system reboots (and upgrades). In order to achieve a high level of resiliency, **we recommend attaching an external USB drive to your Sonus SBC 1000 unit**.
- **Sonus SBC 2000**: Unlike the Sonus SBC 1000, the Sonus SBC 2000 model has built-in storage with reserved space for the Local AD cache to overcome this situation. No external storage is necessary.

Manual AD Cache Refresh

In addition to scheduled periodic AD Cache updates, the Sonus SBC 1000/2000 allows you to refresh (update) the AD Cache manually. Subsequent updates are automatically performed at the interval specified in the **Update Frequency** field or the time specified in the **First Update Time** field, whichever occurs first.

Typically this feature is used to make user information available immediately after they are added to Active Directory, rather than wait for the automatic update, which might take as long as 30 days.

To Refresh the AD Cache:

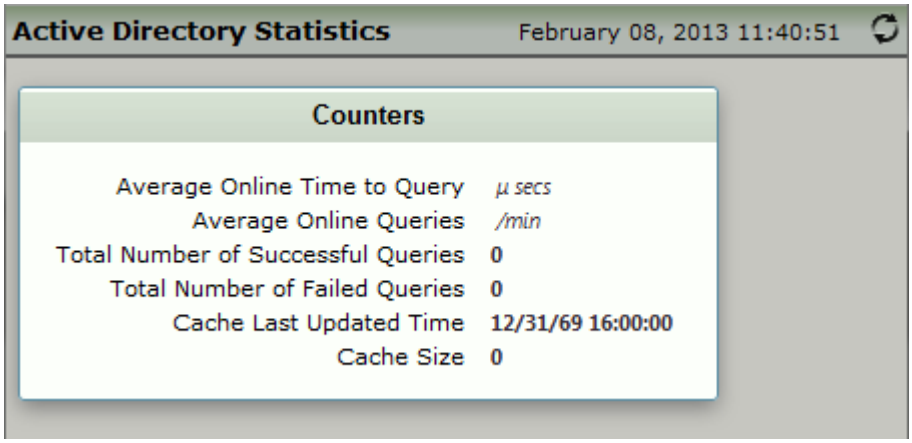
- Click the Refresh Cache text at the top of the Active Directory Configuration page.

Viewing Active Directory Statistics

To view Active Directory Query Statistics:

Click the Display Statistics text at the top of the Active Directory Configuration page.

Copyright © 2015 Sonus Networks. All rights reserved.



Tips on Active Directory Cache Size

The total size for the Active Directory cache is 20MB. Here's a quick calculation showing how the cache memory is utilized:

Number of Records to cache	100,000
Number of Attributes per record	4
Number of bytes per attribute	50
Total cache size	**100,000 * 4 * 50 = 20MB (approx)**

Note: The maximum cache size is 25MB
The database pointer information consumes a small portion of the memory, thus the cache capacity will be slightly less than calculation above.

Configuring the Sonus SBC 1000-2000 for Active Directory User Domain Access

This page describes how to configure Sonus SBC 1000/2000 for Active Directory User Group Access:

- Step 1 - Configure the Domain Controllers
- Step 2 - Configure Sonus SBC 1000/2000 for Active Directory Access
- Step 3 - Configure AD User Group to Access Level Mapping
- Step 4 - Login with an Active Directory Domain User

Step 1 - Configure the Domain Controllers

This step allows you to specify the Domain Controller(s) which will be used in the Sonus SBC 1000/2000 system. The information from the same domain controller(s) will be used for AD-based telephony routing and for Logging in to Sonus SBC 1000-2000 using an AD domain user.

To add a Domain Controller, follow the instructions outlined in Adding and Modifying Domain Controllers with the following settings:

Copyright © 2015 Sonus Networks. All rights reserved.

- **Description**: The name you wish to use for referencing this domain controller - used in the next step
- **IP Address/FQDN**: IP address or FQDN of the Domain Controller
- **Search Scope**: for example `dc=uxdemo,dc=net`
- **LDAP Query**: for example `userPrincipalName=*`



Step 2 - Configure Sonus SBC 1000/2000 for Active Directory Access

In this step, we configure the Active Directory settings on Sonus SBC 1000/2000 such that we can authenticate users through the Domain Controller created earlier. Configuring the Sonus SBC 1000-2000 for Active Directory with the following settings:

In the **Active Directory Configuration** settings group:

- **AD Enabled**: True
- **User Name**: (for example, uxacc@uxdemo.net)
- **Password**: (the password for the AD user)
- **Use TLS**: False
- **Operating Mode**: Updates

In the **Cache Settings** group:

- **Normalize Cache**: False
- **Update Frequency**: 60 (minutes)
- **Cache Attributes**: for example `telephoneNumber, msRTCSIP-Line, mobile, displayName, userPrincipalName`

In the **User Authentication Settings**

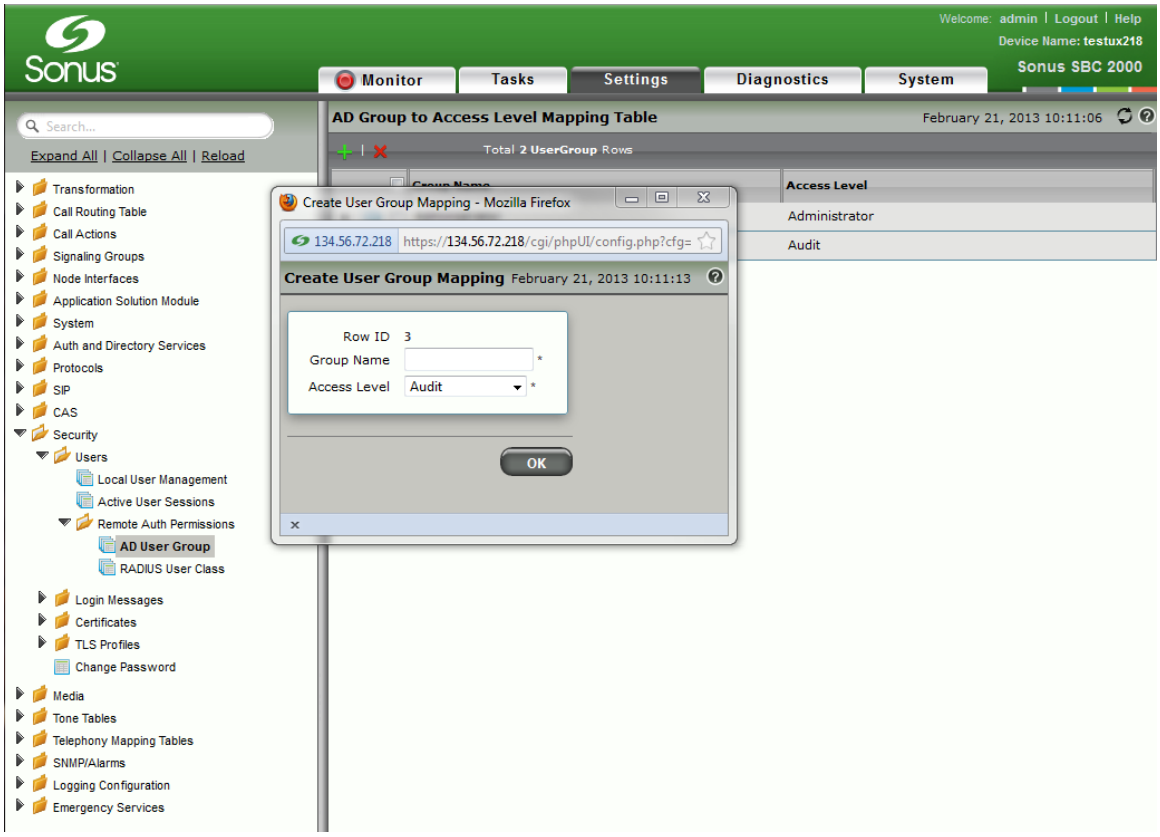
- Select the **Domain Controller** - created in Step 1

Copyright © 2015 Sonus Networks. All rights reserved.

Step 3 - Configure AD User Group to Access Level Mapping

In this step, we map the Active Directory (AD) group with the Sonus SBC 1000/2000 access level for the AD user we wish to grant access on the Sonus SBC 1000/2000:

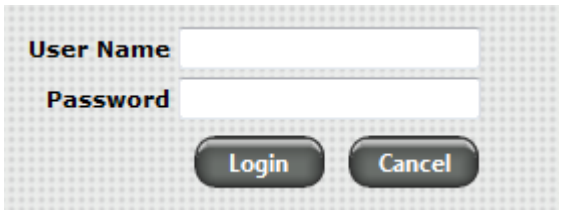
- **Group Name**: enter the name of the AD group
- **Access level**: select the access level for the group



Step 4 - Login with an Active Directory Domain User

To verify the AD domain user can access the Sonus SBC 1000/2000, the AD username must be supplied in the format `USERNAME@DOMAIN` - see How User Authentication Works. Enter the following in the login screen

- **User Name**: enter the AD user name in the format `USERNAME@DOMAIN`; for example `readonlyuser1@uxdemo.net`
- **Password**: enter the password of the AD user

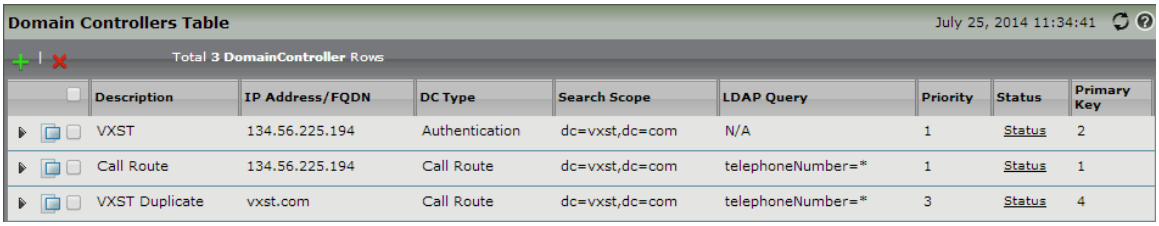


Managing Domain Controllers

Working with Domain Controllers

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Auth and Directory Services > Active Directory > Domain Controllers**.



Description	IP Address/FQDN	DC Type	Search Scope	LDAP Query	Priority	Status	Primary Key
VXST	134.56.225.194	Authentication	dc=vxst,dc=com	N/A	1	Status	2
Call Route	134.56.225.194	Call Route	dc=vxst,dc=com	telephoneNumber=*	1	Status	1
VXST Duplicate	vxst.com	Call Route	dc=vxst,dc=com	telephoneNumber=*	3	Status	4

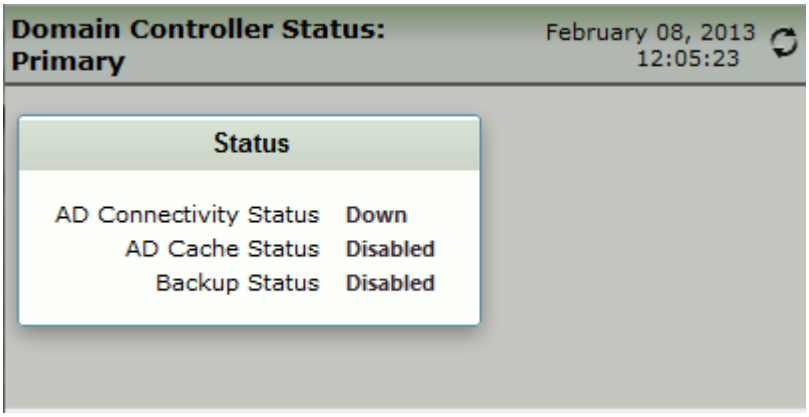
To view a Domain Controller's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

To view a Domain Controller's Status:

- Click the **Status** text next to the Domain Controller for which you want to check status.



Adding and Modifying Domain Controllers

Adding and Modifying Domain Controllers

Before You Begin

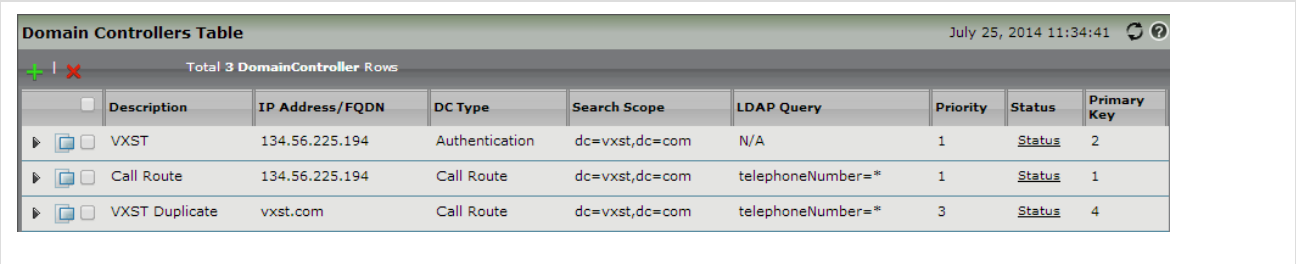
Gather the following information:

- A description (name) of the domain controller
- The IP Address of Fully Qualified Domain Name of the domain controller
- The search scope
- The LDAP query

To add or modify a Domain Controller:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Auth and Directory Services > Active Directory > Domain Controllers**.

Copyright © 2015 Sonus Networks. All rights reserved.

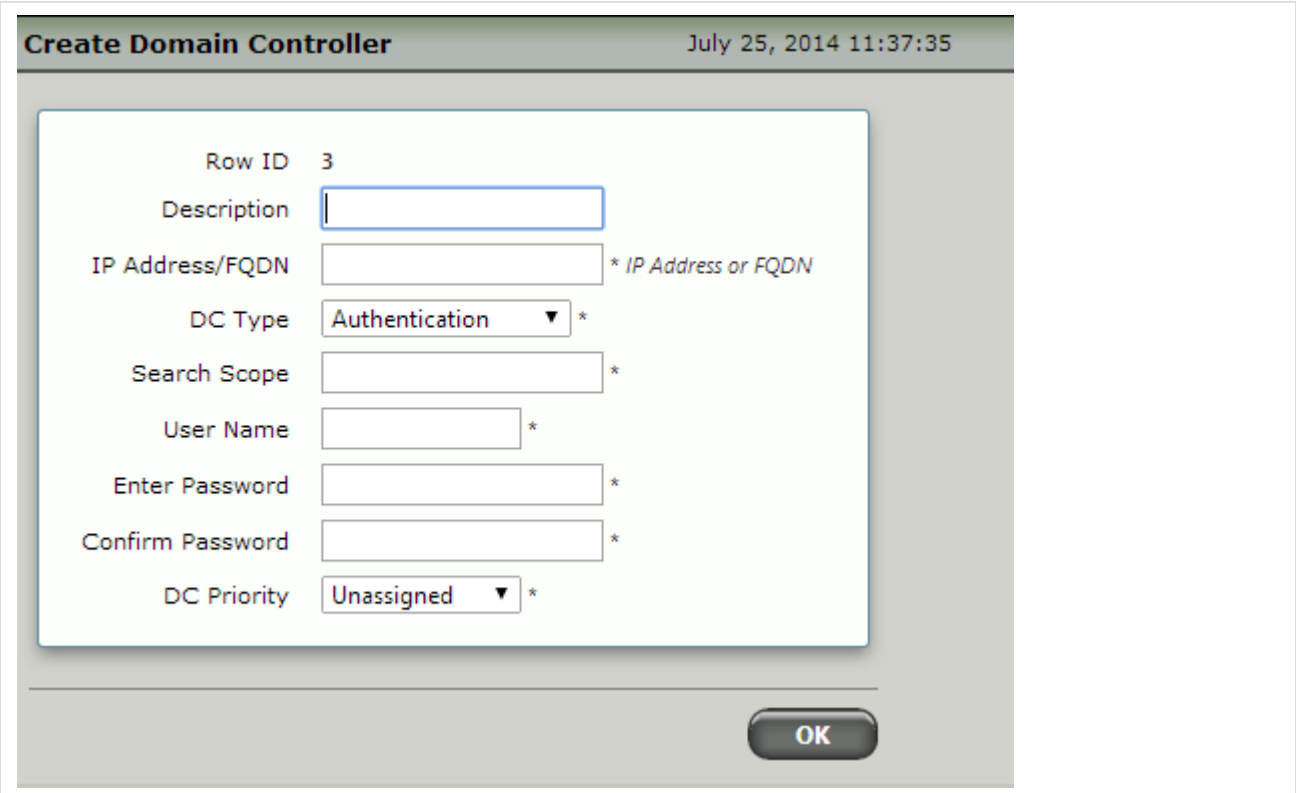


Modifying Domain Controller Properties

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Adding a Domain Controller

1. Click the **Add Domain Controller**( ) icon at the top of the **Domain Controllers Table**page.



Domain Controller - Field Definitions

IP Address/FQDN

Specifies an IP address or Fully Qualified Domain Name (FQDN) of the Domain Controller.

DC Type

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the type of domain controller, either Authentication or Call Route.

- **Authentication:** used for authenticating user log-ins.
- **Call Route:** a Call Route domain controller supplies call routing information.

Search Scope

Specifies the tree location in Active Directory to use as the starting point for search queries or authentication requests.

LDAP Query

Applies a filter to the Search Scope to limit the number of active directory users included in the cache.

User Name

Specifies username (BindDN) to use for querying the Active Directory. The user name must be either the *sAMAccountName* or the *UPN*.

Enter/Confirm Password

Specifies a new password (BindPW) to use for querying the Active Directory.

DC Priority

Specifies the priority ranking of the domain controller for Active Directory queries and is based on domain controller type.
Specifies the order in which the AD queries the domain controllers. Both authentication and call routing domain controllers start at priority 1 (highest) and both may have priority 1.

Managing Active Directory Groups to Access Level Mapping

The Sonus SBC 1000/2000 does not manage individual Active Directory user's Sonus SBC 1000/2000 permissions directly, instead they are managed by mapping their Sonus SBC 1000/2000 access level to the Acive Directory (AD) Group(s) to which the user belongs.

When Active Directory users are authenticated, their permissions on the Sonus SBC 1000/2000, will depend on the configured **mapping between their existing Active Directory Group and the Sonus SBC 1000/2000 Access Level**.

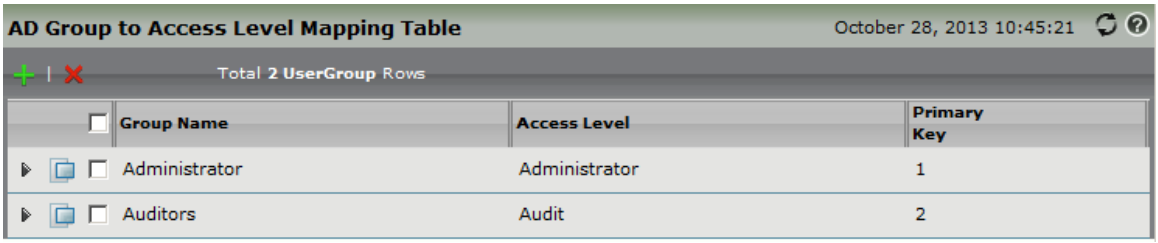
Missing AD Group to Sonus SBC 1000/2000 Access Level Mapping

If an AD user belongs to a Group which is not mapped to a Sonus SBC 1000/2000 access level, this user's access will be denied on the Sonus SBC 1000/2000.

Working with Active Directory Groups to Access Level Mapping

1. In the WebUI, click **Settings**.
2. In the left navigation pane, go to **Security > Remote Auth Permissions > AD User Group.**

Copyright © 2015 Sonus Networks. All rights reserved.



To view an Active Directory Groups to Access Level Mapping's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

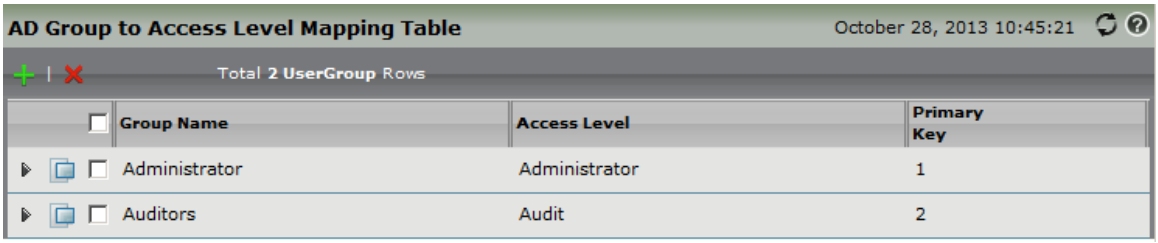
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Active Directory Groups Access Level Mapping

Creating and Modifying Active Directory Groups Access Level Mapping

To create or modify an Active Directory Group to the Access Level Mapping:

1. In the WebUI, click **Settings**.
2. In the left navigation pane, go to **Security > Remote Auth Permissions > AD User Group.**



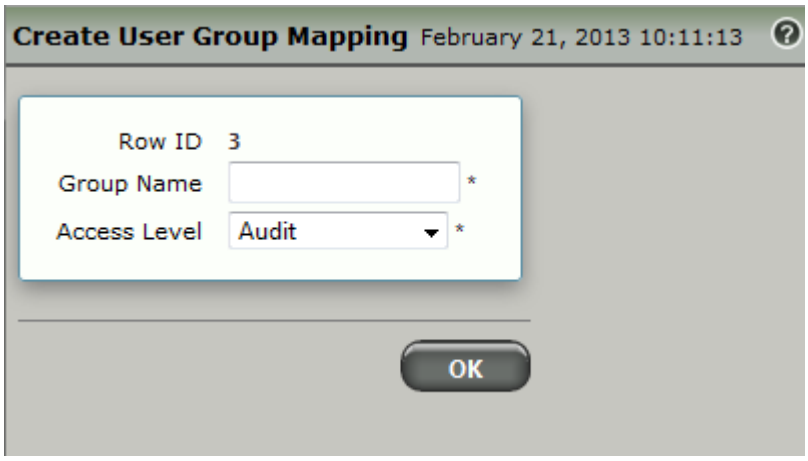
Modifying an Active Directory Group to the Access Level Mapping

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating an Active Directory Group to the Access Level Mapping

1. Click **Create AD User Group** ( )icon.

Copyright © 2015 Sonus Networks. All rights reserved.



Active Directory Groups - Field Definitions

Group Name

Specifies the name of a valid Active Directory user group to which a Sonus SBC 1000/2000 access level is assigned.

Access Level

Specifies the Access Level assigned to the AD User Group specified above. For more information about Access Levels, see Permissions Overview.

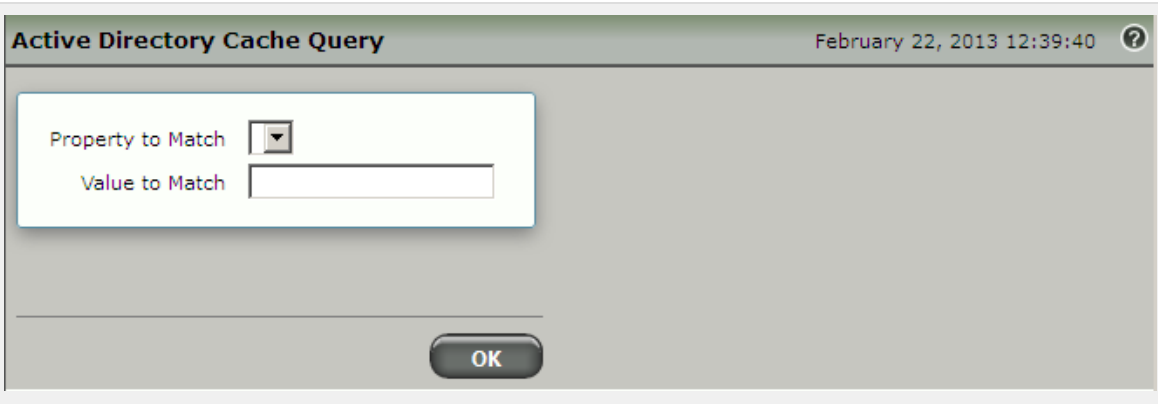
Querying the Active Directory Cache

The Active Directory Cache Query tool allows you to query the local AD Cache for records that match a selected property/value pair. The query returns the records associated with the first match it finds. This tool is useful in determining if the Cache has been updated after a record has been added on the Domain Controller.

⚠ Before you can use this tool, you must have successfully integrated with Active Directory.

To query the cache:

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation pane, go to **Tools > Query AD Cache.**



3. Select a property to match (e.g., **userPrincipalName**).

Copyright © 2015 Sonus Networks. All rights reserved.

4. Enter a value (e.g., **rmushu**).

In this example, if the query finds a userPrincipalName attribute with the value rmushu, the query will return all the attribute/value pairs associates with that record.

Integrating with RADIUS

The Sonus SBC 1000/2000 system fully integrates with RADIUS servers for both authentication and for Call Detail Records (CDR)

Configuring the Sonus SBC 1000-2000 for RADIUS

Managing RADIUS Servers

- Creating and Modifying RADIUS Servers

Managing RADIUS User Class Access Level Mapping

- Creating and Modifying RADIUS User Class Access Level Mapping
- Setting Missing RADIUS User Class Access Level

RADIUS User Authentication Tips Using FreeRADIUS

Configuring the Sonus SBC 1000-2000 for RADIUS

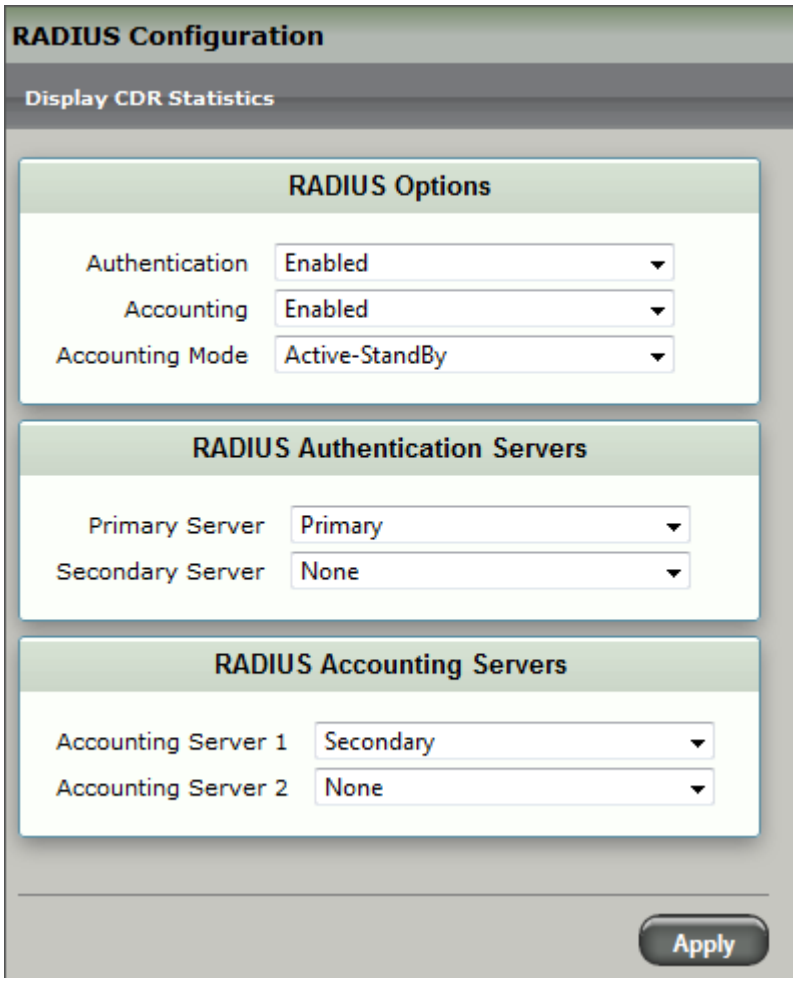
Before You Begin

If you wish to configure the Sonus SBC 1000/2000 for either RADIUS Authentication or Accounting, you must first add one or more RADIUS Server(s) for the Sonus SBC 1000/2000 to use.

Configuring RADIUS Services on Sonus SBC 1000/2000

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Auth and Directory Services > RADIUS > Configuration**.

Copyright © 2015 Sonus Networks. All rights reserved.



Did you know?

It is possible to configure a single RADIUS server to be used for both RADIUS-based authentication and CDR accounting at the same time. To do this, simply create **two** RADIUS server entries pointing to the same RADIUS server IP address/FQDN — enter port 1812 to be used as the authentication server entry, and port 1813 for the accounting server entry.

RADIUS Options - Field Definitions

Authentication

You can configure Sonus SBC 1000/2000 to authenticate users via RADIUS Authentication Server(s). If enabled, you must specify the RADIUS user permissions on Sonus SBC 1000/2000 by configuring the necessary RADIUS User Class Access Level Mapping.

Accounting

You can configure Sonus SBC 1000/2000 for RADIUS accounting using the Sonus SBC 1000/2000 Call Detail Records (CDR) feature. If enabled, the Sonus SBC 1000/2000 must have a valid CDR license before it can log call details.

Accounting Mode Options

Copyright © 2015 Sonus Networks. All rights reserved.

If you wish to record call details to RADIUS Accounting Server(s), you must choose an **Accounting Mode** (i.e., the way you want Sonus SBC 1000/2000 to send those call record details):

- **Active-Standby Mode**
  In the Active-StandBy mode, all accounting related requests are sent to the first accounting server (A-Server One) when it is UP. That is when it is pingable and active. In the event Server One becomes unreachable, accounting requests are then sent to the second accounting server (A-Server Two).
  If A-Server One and A-Server Two become unreachable CDR information is backed up and queued for retry on the Sonus SBC 2000 hard drive. On the Sonus SBC 1000, if an eUSB device is present, the Call Detail Records (CDRs) will be queued on the eUSB device up to a limit of 1,500 records.
- **Active-Active Mode**
  In the Active-Active mode, all accounting requests are sent to both A-Servers. If one of the servers becomes unreachable, a retry procedure is executed. If the retry procedure fails, an alarm is raised every five minutes until the server becomes reachable again.
  If any or both servers become unreachable, the records are queued as described for the Active-StandBy Mode.
- **Round Robin Mode**
  In the Round Robin Mode, accounting requests are alternated between A-Server One and A-Server Two. The first, third, fifth, etc., (odd numbered) requests are sent to A-Server One and the second, fourth, sixth, etc. (even numbered) are sent to A-Server Two. All the call-legs belonging to the same call will go to the same server. These legs will be linked with a unique Acct-Multi-Session-Id per call. When only one server is reachable, all the accounting packets will go to same server. If both servers become unreachable, the records are queued as described for the Active-StandBy Mode.

RADIUS Authentication Servers - Field Definitions

Primary Server/Secondary Servers

Specifies the RADIUS server to use as either Primary or Secondary for RADIUS Authentication. Servers selected for authentication must be configured for authentication and assigned to the correct UDP (Default 1812) Port for RADIUS authentication

RADIUS Accounting Servers - Field Definitions

Accounting Server 1/Accounting Server 2

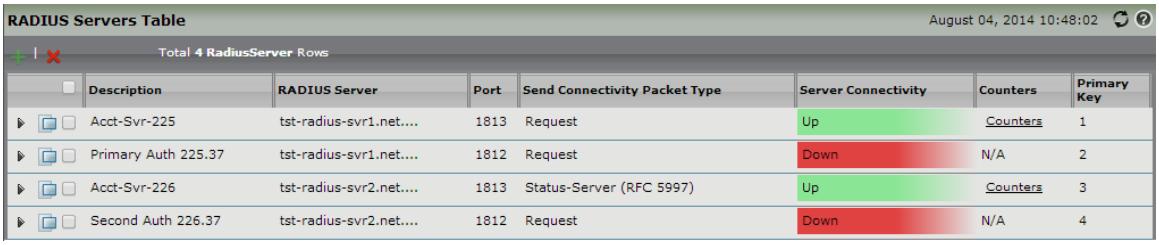
Specifies the RADIUS server to use as either Primary or Secondary for RADIUS Authentication. Servers selected for accounting must be configured for accounting and assigned to the correct UDP Port (Normally, Port 1813) for RADIUS accounting. Although you must specify at least one RADIUS Accounting server, Sonus recommends you use two.

Managing RADIUS Servers

Working with RADIUS Servers

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Auth and Directory Services > RADIUS > RADIUS Servers**.

Copyright © 2015 Sonus Networks. All rights reserved.



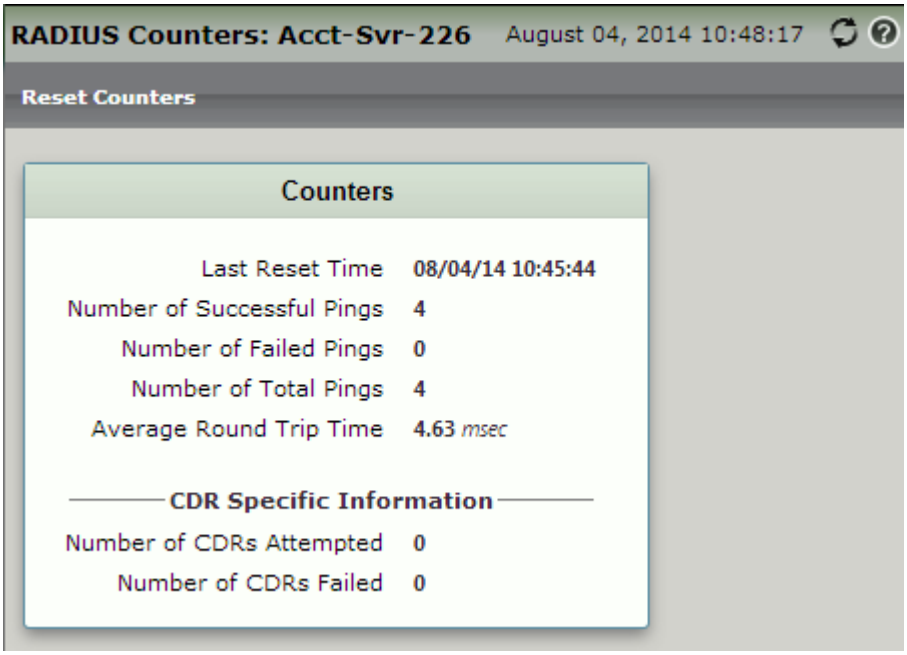
To view a RADIUS Server's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

To view a RADIUS Server's counters:

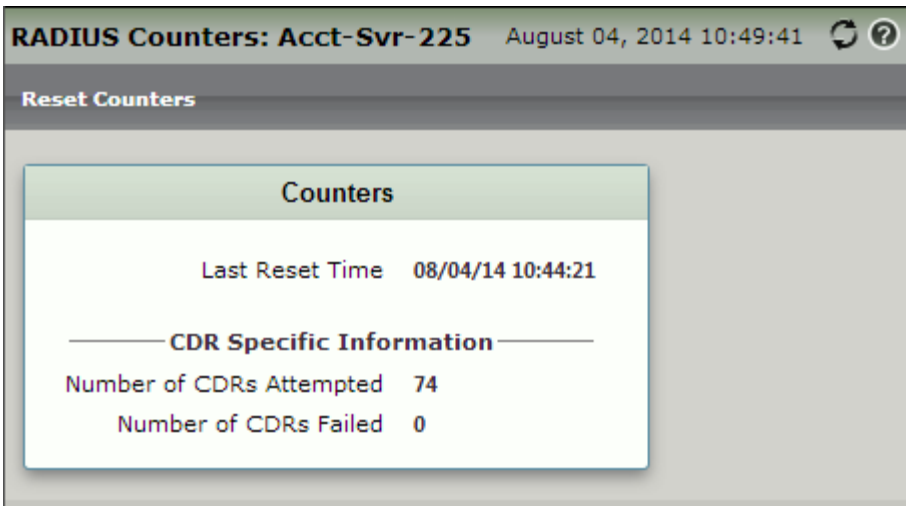
- Click the **Counters** text next to the RADIUS server entry in the table.

RADIUS Server Counters



RADIUS Accounting Server Counters

Copyright © 2015 Sonus Networks. All rights reserved.



Accounting Server Counter Display Behaviour

If any server has the Send Connectivity Packet Type parameter set to Request, Ping counters are irrelevant (if the secondary server is set to NONE, even though the ping counters appear, they will not increment.).

To reset a RADIUS Server's counters:

- Click the **Reset Counters** text at the top of the **RADIUS Counters** panel.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

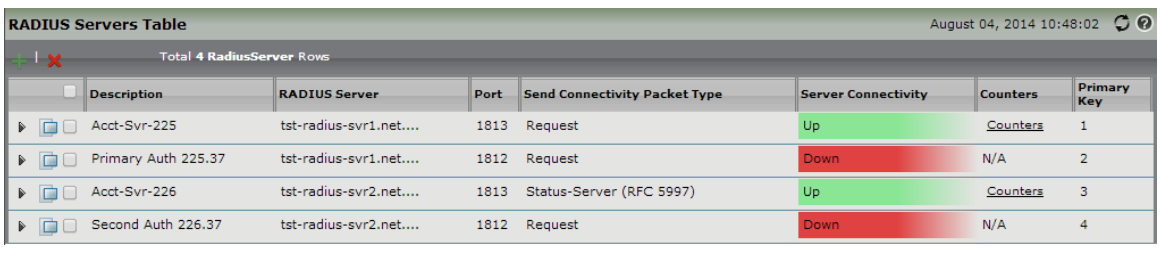
Creating and Modifying RADIUS Servers

Creating and Modifying RADIUS Servers

How to Add a RADIUS Server

To add or modify a RADIUS Server:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Auth and Directory Services > RADIUS > RADIUS Servers**.



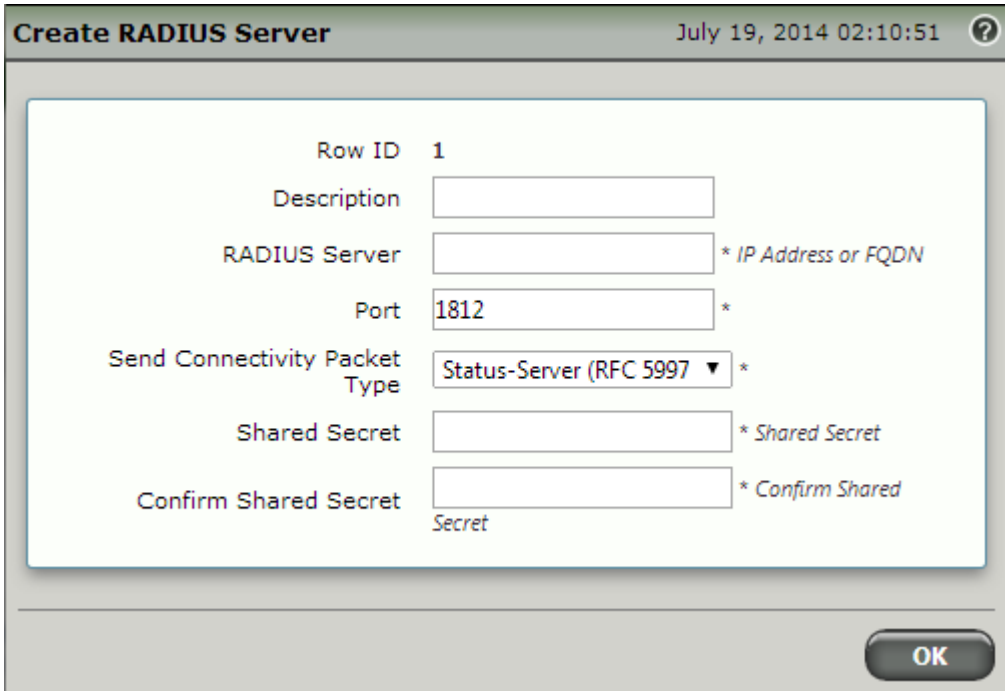
Modifying RADIUS Server Properties

Copyright © 2015 Sonus Networks. All rights reserved.

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a RADIUS Server

1. Click the **Create RADIUS Server**( ) icon at the top of the **RADIUS Servers Table**page.



Server Status Notes

When Status-Server (RFC 5997) is selected in the Send Connectivity Packet Type list box:

- A RADIUS server will appear as **Down** in the **Server Connectivity** column of the RADIUS Servers Table until the Sonus SBC 1000/2000 has successfully pinged the RADIUS server three consecutive times. This process requires approximately one minute for accounting servers. For authentication servers, the process requires approximately three minutes with pings one minute apart. You can check on the progress by clicking the **Counters** text in the row of the server about which you are concerned.

When Request is selected in the Send Connectivity Packet type list box:

- A RADIUS server will appear as **Down** in the **Server Connectivity** column of the RADIUS Servers Table until the Sonus SBC 1000/2000 has successfully received a response from the RADIUS server.

Create RADIUS Servers - Field Definitions

Description

A human readable name for the RADIUS server.

RADIUS Server

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the IP Address or Fully Qualified Domain Name (FQDN) of the RADIUS server.

Port

Specifies the port over which the Sonus SBC 1000/2000 will communicate with the RADIUS server for authentication or accounting.

- **Authentication Servers**: use port 1812 (default)
- **Accounting Servers**: use port 1813 by default, however you may use any valid non-reserved port.

Send Connectivity Packet Type

Status-Server (RFC 5997): Sends a Status-Server packet once each minute to verify network connectivity. Connectivity status is declared as ***Up*** when a response to the packet is successfully received, or declared as ***Down*** if no response is received.

Request: Sends an Access-Request or Accounting-Request packet, on demand, to verify the connectivity status. Connectivity status is declared as ***Up*** when a response to the packet is successfully received, or declared as ***Down*** if no response is received.

- **Access-Request Packet:** Sent to the authentication server to verify connectivity when a RADIUS based user attempts to login.
- **Accounting-Request Packet:** Sent to the Accounting server to verify connectivity when a call occurs.

Shared Secret

Specifies a text string used for authenticating with the RADIUS server.

Managing RADIUS User Class Access Level Mapping

The Sonus SBC 1000/2000 does not manage individual RADIUS user's Sonus SBC 1000/2000 permissions directly, instead they are managed by mapping their Sonus SBC 1000/2000 access level to the RADIUS Class to which the user belongs. The **User Class** is defined by the Class attribute in the RADIUS server. This attribute is retrieved upon successful authentication and matched with mapped user access level in Sonus SBC 1000/2000.

When RADIUS users are authenticated, their permissions on the Sonus SBC 1000/2000, will depend on the configured **mapping between their existing RADIUS Class and the Sonus SBC 1000/2000 Access Level**.

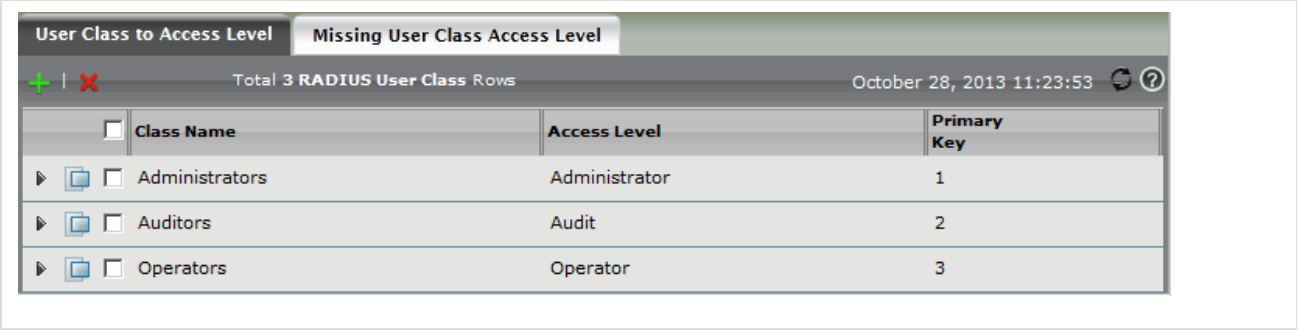
Configure Sonus SBC 1000/2000 Authentication for Non-mapped RADIUS User Classes

If a RADIUS user belongs to a Class which is not mapped to a Sonus SBC 1000/2000 access level, then a default access will be used from the Missing User Class Access Level tab.

Working with RADIUS User Class Access Level Mapping

1. Go to **Security > Users > Remote Auth Permissions > RADIUS User Class**.
2. Click the **User Class to Access Level**tab.

Copyright © 2015 Sonus Networks. All rights reserved.



To view a RADIUS User Class Access Level's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

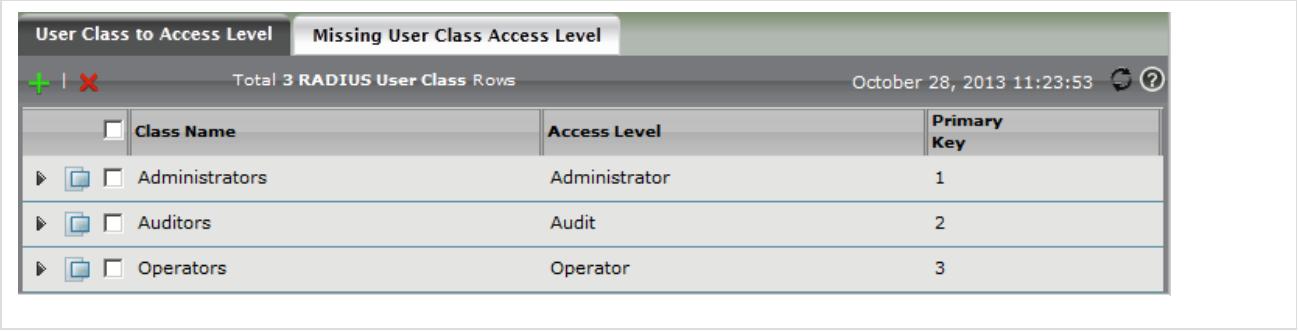
Creating and Modifying RADIUS User Class Access Level Mapping

Setting Missing RADIUS User Class Access Level

Creating and Modifying RADIUS User Class Access Level Mapping

To create or modify a RADIUS User Class Access Level Mapping:

1. Go to **Security > Users > Remote Auth Permissions > RADIUS User Class**.
2. Click the **User Class to Access Level**tab.



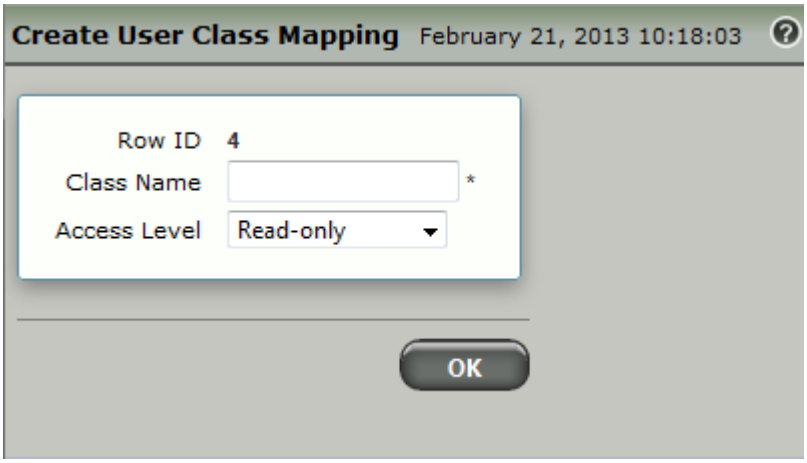
Modifying a RADIUS User Class Access Level Mapping

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a RADIUS User Class Access Level Mapping

1. Click the **Create User Class**( ) icon.

Copyright © 2015 Sonus Networks. All rights reserved.



2. Enter the name of the class to which you are granting access in the Class Name text field.
3. Select an access level from the **Access Level** drop-down box.
4. Click **OK**.

> **Important**
>
> The **Class Name** field is case sensitive and must match the RADIUS class exactly.

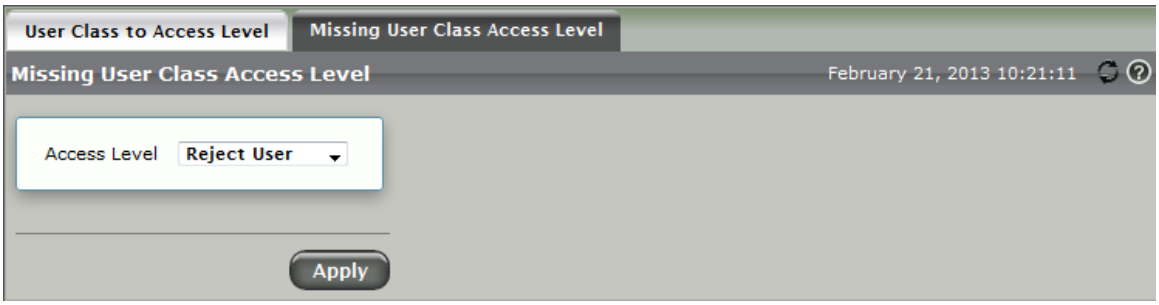
Setting Missing RADIUS User Class Access Level

In addition to the existing access levels, the **Reject User** access level is only applicable to RADIUS users. It behaves as a "disabled mode" for RADIUS users whose Class membership does not map to one of the other Sonus SBC 1000/2000 access levels.

How to Set the Missing Class Group Access Level

To set the Missing User Class Access Level:

1. Go to **Security > Users > Remote Auth Permissions > RADIUS User Class**.
2. Click the **Missing User Class Access Level**tab.



3. Select the access level you want to map to a user with no RADIUS class in the **Access Level** drop-down box.
4. Click **Apply**.

RADIUS User Authentication Tips Using FreeRADIUS

This page contains some high-level technical tips when authenticating a RADIUS user between the Sonus SBC 1000/2000 to a FreeRADIUS Server provider:

Copyright © 2015 Sonus Networks. All rights reserved.

- FreeRADIUS Sample Configuration
- RADIUS Server Authentication Message Exchange
  - If the request is authenticated
  - If the request is not authenticated

FreeRADIUS Sample Configuration

In this section, we provide sample FreeRADIUS configuration bits relevant to RADIUS user authentication on Sonus SBC 1000/2000.

Users

We configure a RADIUS user called **raduser** who's User Class is **ReadOnlyClass**. This class name needs to be configured on the Sonus SBC 1000/2000 - see Managing RADIUS User Class Access Level Mapping.

```
raduser User-Password == "Passw0rd"
        Class == "ReadOnlyClass"
```

radiusd.conf

This is used for the RADIUS server healthcheck:

```
status_server = yes
```

clients.conf

This defines the RADIUS client information with the RADIUS Server settings configured on Sonus SBC 1000/2000

```
client 172.16.250.246/32 {
       secret          = Passw0rd
       shortname       = Sonus SBC 1000/2000246
}
```

RADIUS Server Authentication Message Exchange

When a RADIUS user attempts to authenticate on the Sonus SBC 1000/2000 system, the Sonus SBC 1000/2000 behaves as a RADIUS authentication client and sends an Access-Request to the RADIUS server:

```
rad_recv: Access-Request packet from host 172.16.250.246:38525, id=170, length=65
        Service-Type = Login-User
        User-Name = "raduser"
        User-Password = "Passw0rd"
        NAS-Port = 0
        NAS-IP-Address = 172.16.250.246
```

Copyright © 2015 Sonus Networks. All rights reserved.

If the request is authenticated

The RADIUS server responds with Access-Accept and it returns the Class attribute attribute:

```
Sending Access-Accept of id 170 to 172.16.250.246 port 38525
        Class == 0x41646d696e6973747261746f72436c617373
```

After Sonus SBC 1000/2000 receives the Access-Accept, Sonus SBC 1000/2000 uses the Class attribute returned by RADIUS to map the appropriate access level.

If the request is not authenticated

The RADIUS server responds with Access-Reject:

```
Sending Access-Reject of id 215 to 172.16.250.246 port 5412
```

Working with Physical Ports

This section contains information about configuring and managing Ethernet and telephony ports on the Sonus SBC 1000/2000. Information includes, but is not limited to, configuring ports, setting port types, and viewing counters and channel details.

Managing Ethernet Ports

- Configuring Ethernet Ports on the Sonus SBC 1000
- Configuring Ethernet Ports on the Sonus SBC 2000
- Viewing Ethernet Port Counters

Managing Telephony Ports

- Setting the DS1 Port Types
- Configuring T1 Ports
- Configuring E1 Ports
- Configuring FXS Ports
- Configuring Powerdown Telephony Passthrough
- Viewing Port Counters and Channel Details
- Configuring BRI Ports
- Configuring FXO Ports
- Calibrating FXO Ports

Managing Ethernet Ports

Sonus SBC 1000

The Sonus SBC 1000 has two Ethernet ports used for communicating with the IP network. All SIP traffic is carried on these two ports. Unlike the Sonus SBC 2000, this model has no dedicated Management Port.

Sonus SBC 2000

The Sonus SBC 2000 has four Ethernet ports and one Ethernet Management port. By default, each of the four non-management ports are in their own system created VLAN, and are isolated from one another.

Copyright © 2015 Sonus Networks. All rights reserved.

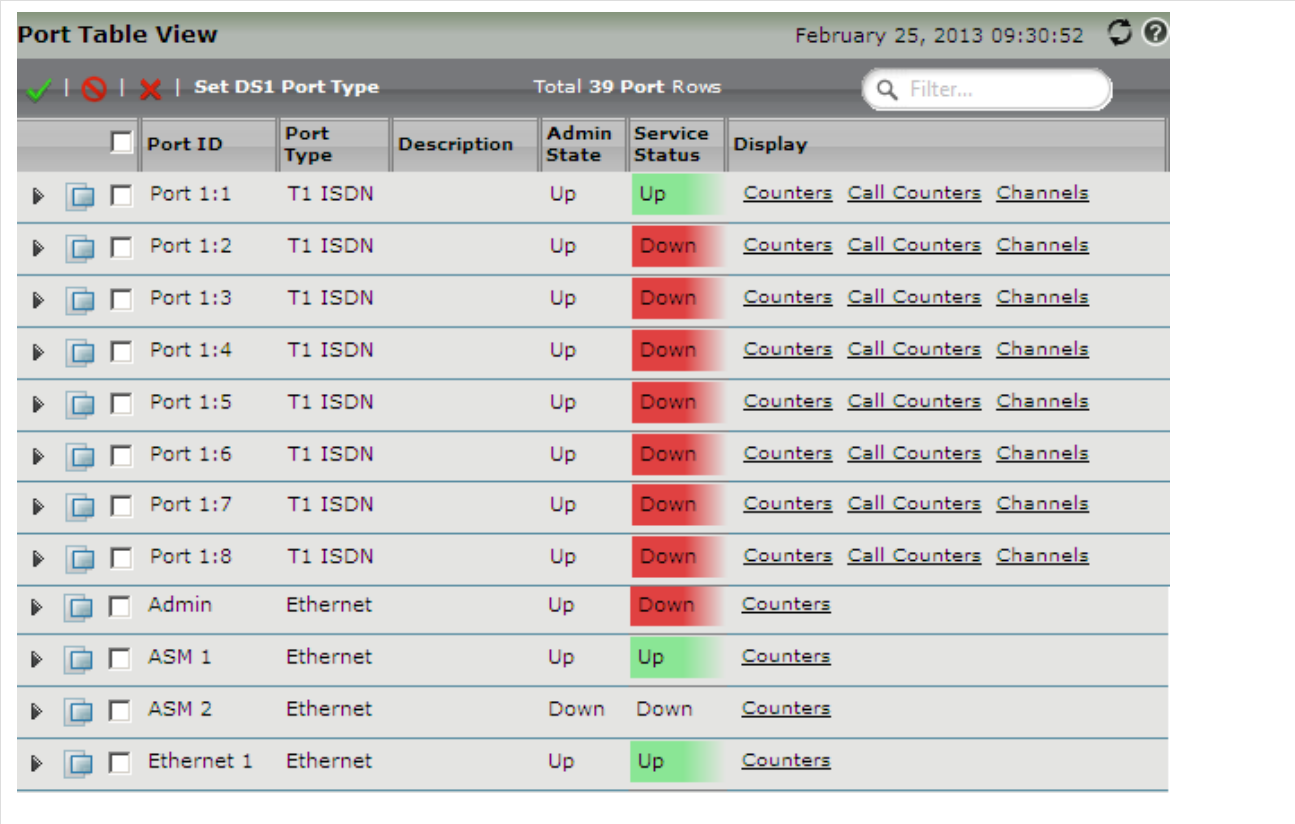
ASM

If the unit is equipped with a built-in ASM, then all ASM traffic is carried uniquely through this Ethernet port.

> For communication between the Sonus SBC 1000/2000 and the ASM to work properly, the ASM port's **Default Untagged VLAN** must be set to a VLAN whose logical IP address is in the same subnet as the ASM's IP address. For example, if the ASM port's default VLAN is set to **Ethernet 1 VLAN**, then the logical interface **Ethernet 1 IP** must have its IP address in the same subnet as the ASM IP.

Working with Ethernet Ports

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.



To view a Ethernet Port's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

> **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

See also, Viewing Port Counters and Channel Details,

Configuring Ethernet Ports on the Sonus SBC 1000

Configuring Ethernet Ports on the Sonus SBC 2000

Copyright © 2015 Sonus Networks. All rights reserved.

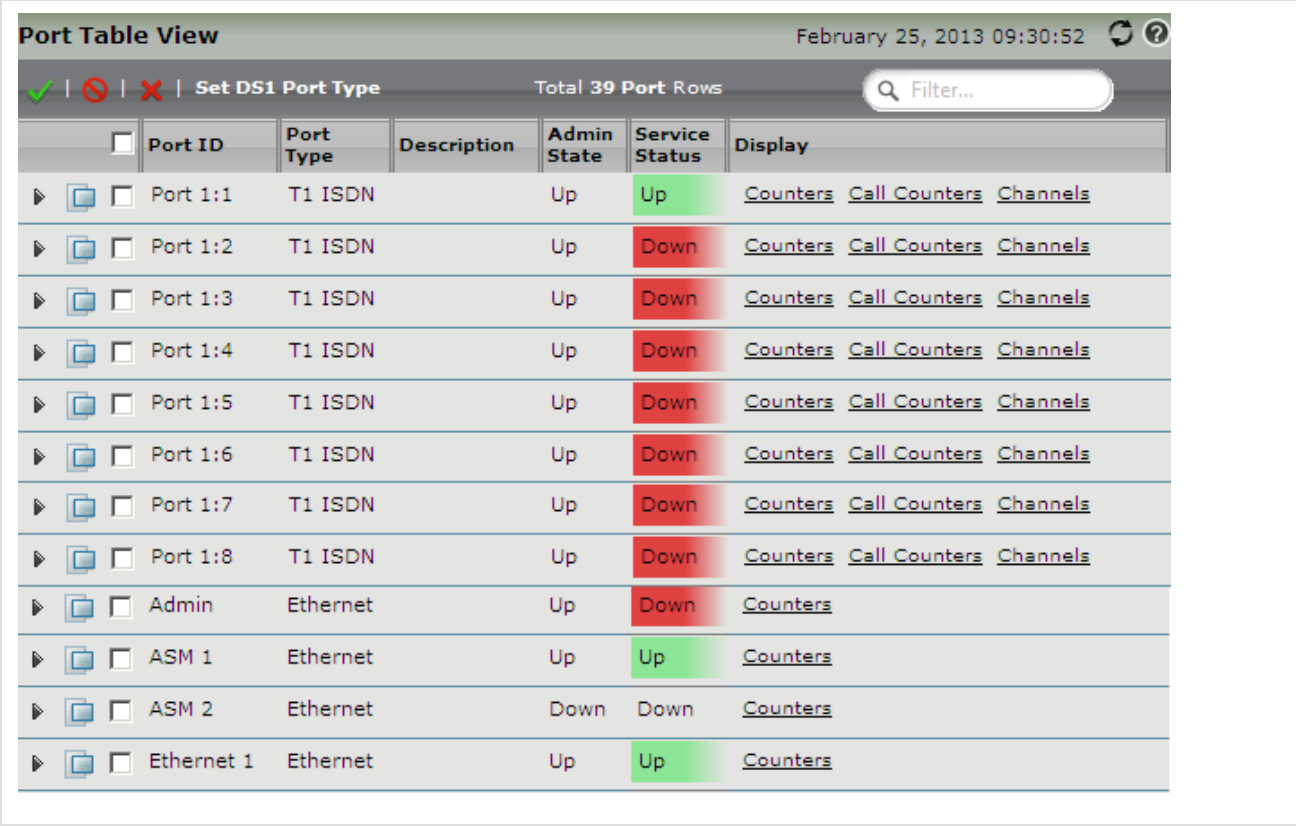
Viewing Ethernet Port Counters

Configuring Ethernet Ports on the Sonus SBC 1000

The Sonus SBC 1000 allows you to configure the Identification information, Physical Data Layer, and Networking Layer for the Ethernet ports. If you want to change the IP Address, you must configure the associated Logical Interface or use the Modify Ethernet IP task found under the Tasks tab.

To access the Ethernet Ports on the Sonus SBC 1000:

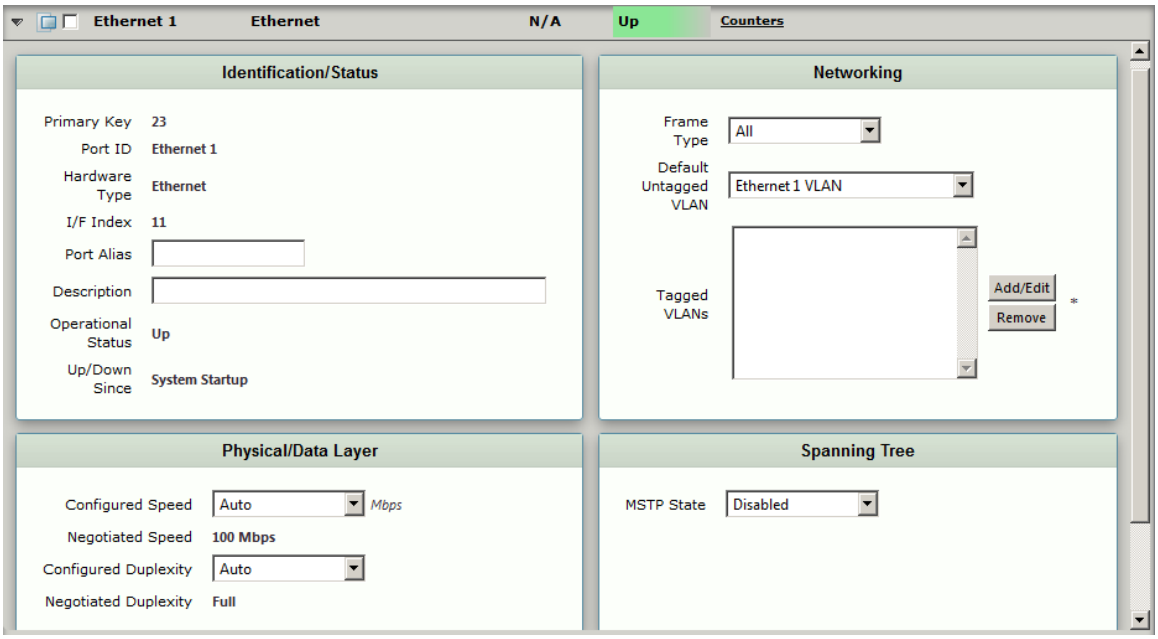
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.



Configuring the Ethernet Ports on the Sonus SBC 1000

1. Click the expand (▸) icon next to the port you wish to configure

Copyright © 2015 Sonus Networks. All rights reserved.



Identification/Status - Field Definitions

Port Alias

Specifies an alternative name for the interface; typically configured by the SNMP-based Network Manager.
This parameter is unique among all the interfaces known to the SNMP Network Manager. The value cannot have whitespace characters.

Description

Description for the port or interface. Maximum entry: 64 characters.

Physical/Data Layer - Field Definitions

Configured Speed

Configures auto-negotiation or a specific speed for the Ethernet port. The default value should be changed only when necessary.

- **Auto:** When **Auto** is selected the port speed is automatically negotiated by the Ethernet port and reported in the **Negotiated Speed** field.
- **1000/100/10:** The specified port speed 1000 Mbps, 100 Mbps, or 10 Mbps is reported in the **Negotiated Speed** field.

Configured Duplexity

Specifies auto-negotiation or a specific value for the duplexity of the Ethernet port. Valid entries: **Auto**, **Full** or **Half**. Default value: **Auto**. The default value should be changed only when necessary.

Networking - Field Definitions

Frame Type

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the type of Ethernet frames that can be received on this port.

- **All**: When selected, both untagged and tagged Ethernet frames are accepted on this port.
- **Untagged**: When selected, only untagged frames are accepted on this port.
- **Tagged**: When selected, only tagged frames are accepted on this port, and no default VLAN will be configured.

The **ASM 1** Ethernet port is limited to **Untagged** mode only.

Default Untagged VLAN

Specifies the default VLAN to which untagged frames will be assigned when they are received on this port. Visible only when **Untagged** or **All** is selected from the **Frame Type** list box. For more information about VLANs, see Creating and Modifying VLANs.

Tagged VLANs

Specifies the tagged VLAN(s) of which this Ethernet port is a member. Only user created VLANs can be selected. Visible only when **Tagged** or **All** is selected from the **Frame Type** list box. Since the **ASM 1** Ethernet port is limited to **Untagged** mode only, the **Tagged VLAN** selection is not be present for this port.

Spanning Tree

MSTP State

Determines whether MSTP is enabled/disabled on the port(s). Valid options: **Enabled** (MSTP is enabled) or **Disabled** (default; MSTP is disabled and does not transmit/receive BPDU packets).

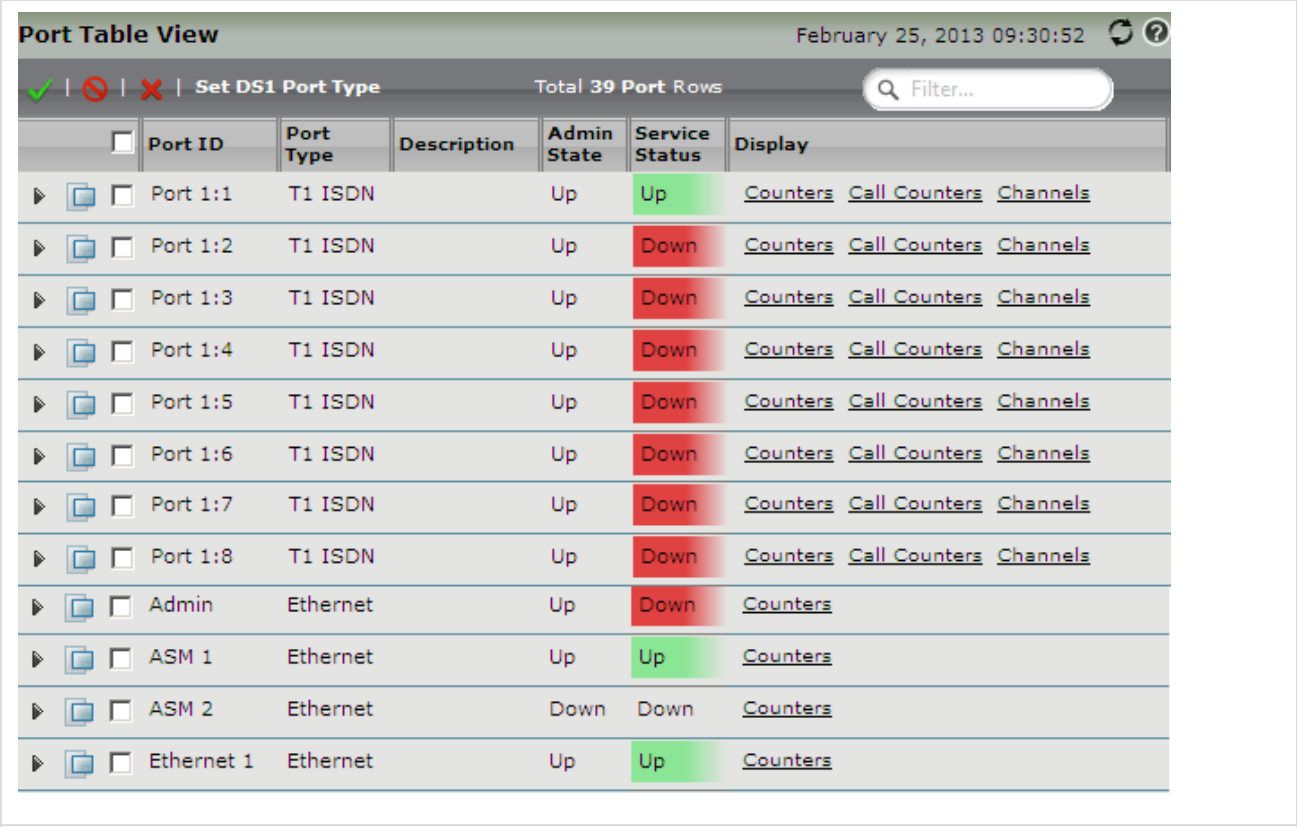
Configuring Ethernet Ports on the Sonus SBC 2000

The Sonus SBC 2000 allows you to configure the Identification/Status information, Physical Data Layer, and Networking Layer for the Ethernet ports. If you want to change the IP Address, you must configure the associated Logical Interface or use the Modify Ethernet IP task found under the Tasks tab.

To access the Ethernet Ports on the Sonus SBC 2000:

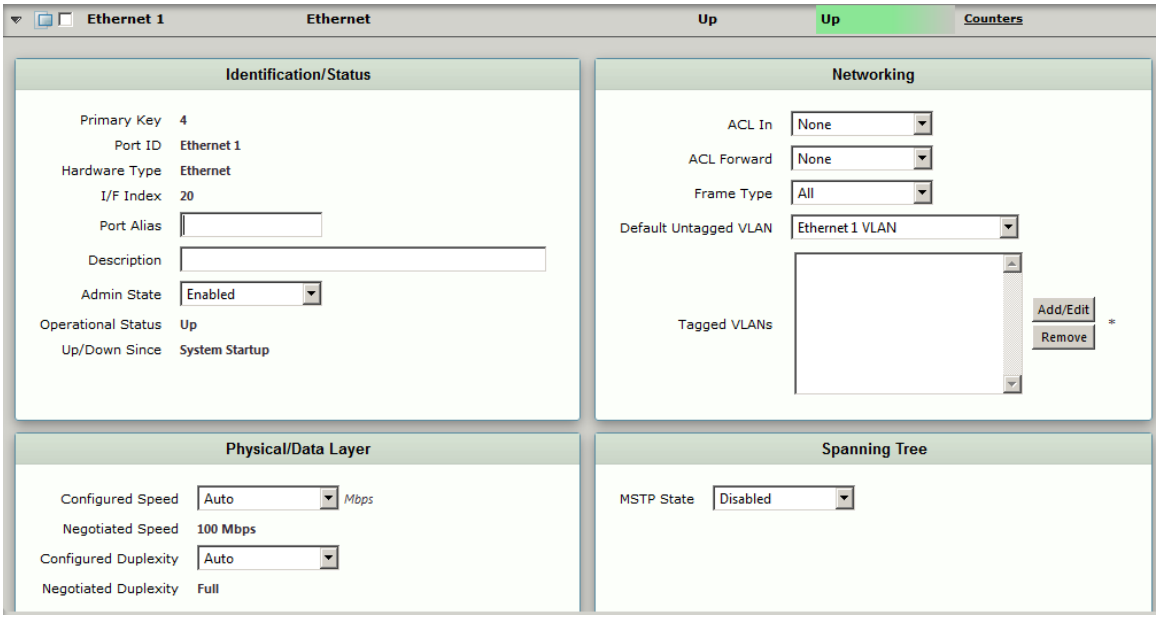
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.

Copyright © 2015 Sonus Networks. All rights reserved.



Configuring the Ethernet Ports on the Sonus SBC 2000

1. Click the expand (▸) icon next to the port you wish to configure



> The **ASM 2** Ethernet port is for special applications, and cannot be used for VOIP-gateway or SBC functionalities.

Identification/Status - Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

Port Alias

Specifies an alternative name for the interface; typically configured by the SNMP-based Network Manager.
This parameter is unique among all the interfaces known to the SNMP Network Manager. The value cannot have whitespace characters.

Description

Description for the port or interface. Maximum entry: 64 characters.

Admin State

Specifies the administrative state of the port.

Physical Data Layer - Field Definitions

Configured Speed

Configures auto-negotiation or a specific speed for the Ethernet port. The default value should be changed only when necessary.

- **Auto:** When **Auto** is selected the port speed is automatically negotiated by the Ethernet port and reported in the **Negotiated Speed** field.
- **1000/100/10:** The specified port speed 1000 Mbps, 100 Mbps, or 10 Mbps is reported in the **Negotiated Speed** field.

Configured Duplexity

Specifies auto-negotiation or a specific value for the duplexity of the Ethernet port. Valid entries: **Auto**, **Full** or **Half**. Default value: **Auto**. The default value should be changed only when necessary.

Networking - Field Definitions

ACL In

Determines the Access Control List (ACL) to be used on this port when filtering incoming packets. For more information about Access Control Lists, see Managing Access Control Lists.

ACL Forward

Determines the Access Control List (ACL) to be used when filtering forwarded (i.e. routed) packets received on this port. For more information about Access Control Lists, see Managing Access Control Lists.

Frame Type

Copyright © 2015 Sonus Networks. All rights reserved.

Determines the type of Ethernet frames that can be received on this port.

- **All**: When selected, both untagged and tagged Ethernet frames are accepted on this port.
- **Untagged**: When selected, only untagged frames are accepted on this port.
- **Tagged**: When selected, only tagged frames are accepted on this port, and no default VLAN will be configured.

> The **ASM 1** Ethernet port is limited to **Untagged** mode only.

Default Untagged VLAN

Determines the default VLAN that untagged frames will be assigned to when being received on this port. You can select from both user created VLANs and the system created port specific VLANs (e.g. **Ethernet 1 VLAN**). Visible only when **Untagged** or **All** is selected from the **Frame Type** list box.

> By default, each Ethernet port will be assigned to their own port specific system created VLAN (e.g. **Ethernet 1 VLAN**). When the port specific VLAN is selected, IP layer communication takes place with its default Logical Interface (e.g. **Ethernet 1 IP**).

Tagged VLANs

Determines the tagged VLAN(s) which this Ethernet port is a member. Only user created VLANs can be selected. Visible only when **Tagged** or **All** is selected from the **Frame Type** list box. Since the **ASM 1** and **ASM 2** Ethernet ports are limited to **Untagged** mode only, **Tagged VLAN** selection will not be present for this port.

Spanning Tree

MSTP State

Determines whether MSTP is enabled/disabled on the port(s). Valid options: **Enabled** (MSTP is enabled) or **Disabled** (default; MSTP is disabled and does not transmit/receive BPDU packets).

Viewing Ethernet Port Counters

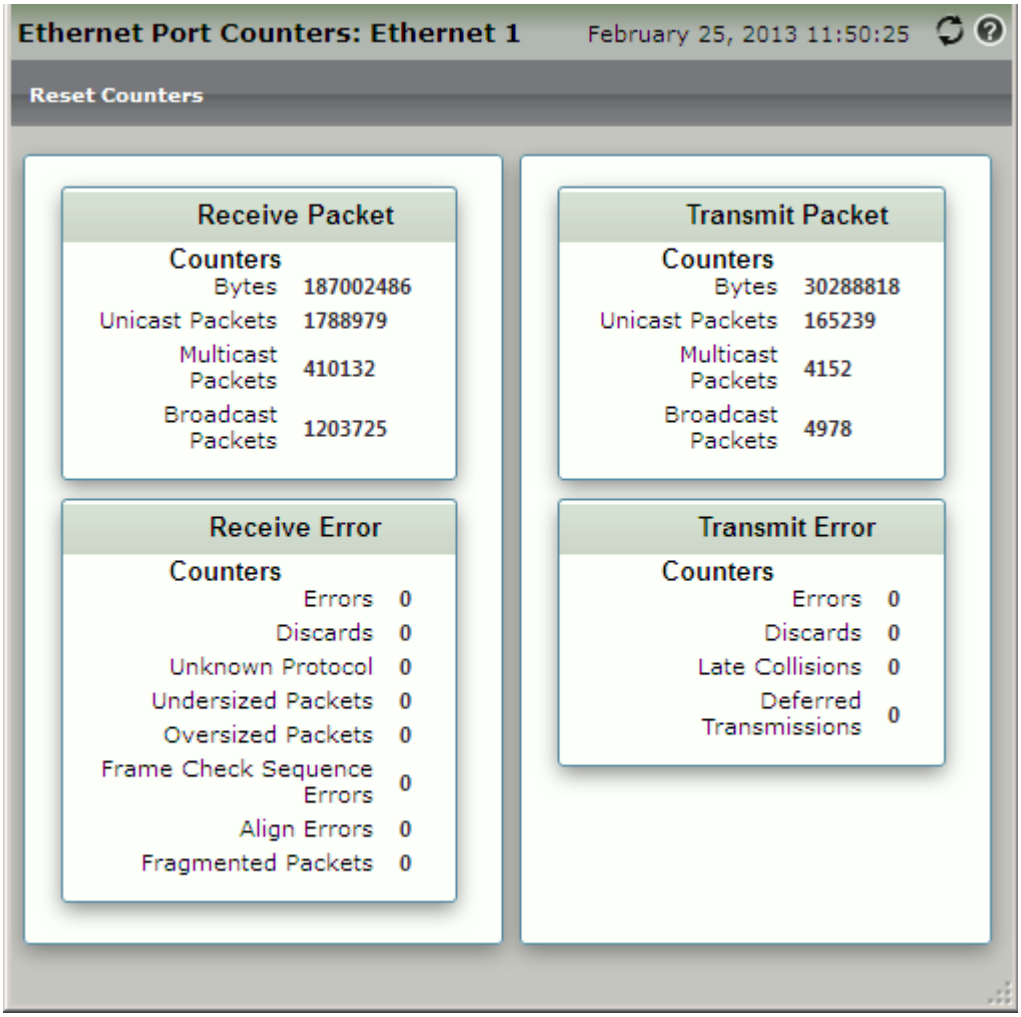
This page describes the procedure to view Ethernet port counters.

How to View Ethernet Port Counters

To View the Ethernet Port Counters:

1. In the WebUI, click the **Settings** tab at the top of the page.
2. Go to **Node Interfaces > Ports**.
3. Click the **Counters**link in the row of the Ethernet port for which you want to view the counters.

Copyright © 2015 Sonus Networks. All rights reserved.



Managing Telephony Ports

The Telephony Port settings allow you to configure the physical properties of the telephony trunks (T1/E1) and analog ports (FXS). Digital trunk type selection (T1 or E1, ISDN or CAS) and analog line profile selection are done here. To configure the protocol layer settings, see the respective signaling group settings for ISDN and CAS.

> If the expected port type is not listed in the **Port Table View,** check the node's Inventory Report to verify that the physical ports (FXS, FXO, BRI, and DSI hardware modules/line cards) are licensed. The physical hardware must be present and licensed for it to be displayed.

Partial T1/E1 Support

Sonus SBC 1000/2000 supports full 23B+1D channels on T1 port and 30B+1D channels on E1 port, as well as fractional T1/E1 (limited numbers of channels). Typically, branch offices do not lease full T1/E1 resources and therefore are limited to the number of channels through which they can connect to their carrier. Partial T1/E1 support on the Sonus SBC 1000/2000 allows the user to configure the number of B-channels on a port to match the number of leased channels. The D-channels for T1 and E1 remain numbers 24 and 16 respectively.

The effect of not using partial T1/E1 support when limited numbers of leased channels are available is that some calls (those exceeding the provisioned channel capacity of the T1/E1 line) will not be successful. For example, if a

Copyright © 2015 Sonus Networks. All rights reserved.

branch office has lease only four channels, and the Sonus SBC 1000/2000 is not configured for partial T1/E1, if there are already four channels in use and the Sonus SBC 1000/2000 attempts to place a call on the fifth or any succeeding channel, the carrier will simple reject the attempt and return a response code.

Channel Configuration on T1 Ports
The number of channels for a T1 port can vary from 1 to 23, with channel 16 reserved as the D-channel.

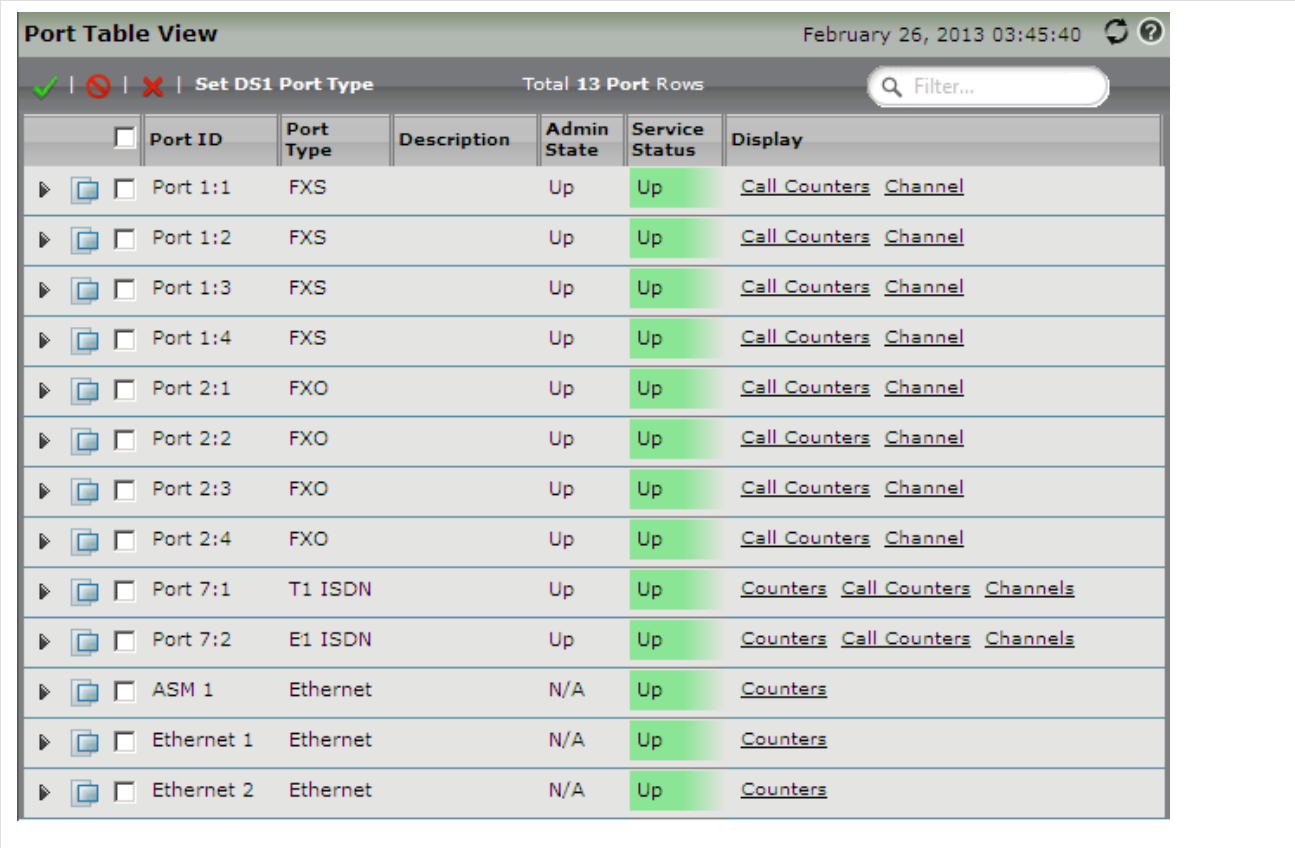
Channel Configuration on E1 Ports
The number of channels for an E1 port can vary from 1 to 30, with a start channel in the range 1 o 30, excluding channel 16 (D-channel).

The Sonus SBC 1000/2000 does not support NFAS like configuration, wherein multiple T1/E1 ports may have a primary and backup D-channel and not all T1/E1 ports need to have 24th/16th channel reserved for D-Channel.

The number of channels on a port are configurable in the **Port and Protocol** panel of the **Signaling Group** when the Fractional option is selected.

Working with Telephony Ports

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.



To view a Telephony Port's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Deleting Telephony Ports Overview

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 2000 T1/E1 Line Card ports are automatically discovered and populated in the **Ports Page** area of the configuration as shown in the **System** tab and when Checking Port Status in the **Settings** tab of the WebUI. **Physical T1/E1 Ports associated with hardware in the Sonus SBC 1000/2000 System cannot be deleted**.

When a line card is physically removed, its configuration is maintained but its ports will not be present when Monitoring Real Time Status. This is done for the case where you are replacing or servicing a line card.

If you have permanently removed or changed the type of line card (e.g., from an 8-port to a 2-port card), then the ports listed in the Sonus SBC 1000/2000 configuration are no longer associated with present hardware and hence can be deleted via the WebUI. Take the following common scenario:

1. Initially 8 port E1/T1 line card are installed. When the Sonus SBC 1000/2000 system comes up, the configuration auto discovers 8 ports.
2. The Sonus SBC 1000/2000 system admininstrator powers off the Sonus SBC 1000/2000 and replaces the 8 ports card with a 2 ports card.
3. When the Sonus SBC 1000/2000 is powered back on, the Webui will still display 8 ports in **Settings** tab. However, only two ports will be displayed in the Monitor view.
4. At this point, the Sonus SBC 1000/2000 system administrator can go ahead and delete ports 3 through 8.

To delete unused ports, simply select the checkbox next to the port(s) you wish delete, then click the Delete ( ) icon located at the top of the window.

> **Sonus SBC 1000** Telephony Ports cannot be deleted via the WebUI.

Related Topics

Setting the DS1 Port Types

Configuring T1 Ports

Configuring E1 Ports

Configuring FXS Ports

Configuring Powerdown Telephony Passthrough

Viewing Port Counters and Channel Details

Configuring BRI Ports

Configuring FXO Ports

Calibrating FXO Ports

Setting the DS1 Port Types

This section describes how to configure the DS1 port types (T1/E1) on the Sonus SBC 1000/2000 system. Using this feature sets all the DS1 ports on the SBC 1000/2000 to either T1 or E1. In most geographical area only T1 or E1 is available. However, in some countries both are available and the SBC may be required to support both simultaneously. When this is the case, ports can be set individually. To set an individual port to T1 see: Configuring T1 Ports. To set an individual port to E1 see: Configuring E1 Ports.

Sonus SBC 2000 T1/E1 Ports

Copyright © 2015 Sonus Networks. All rights reserved.

T1/E1 ports on the Sonus SBC 2000 are provided via removable T1/E1 PSTN Interface cards. The Sonus SBC 2000 supports up to two T1/E1 PSTN Interface cards with a maximum of 16 physical T1/E1 ports. The T1/E1 PSTN Interface cards are available in 2, 4 and 8 port versions. Each Sonus SBC 2000 T1/E1 PSTN Interface Card provides two four-port spans, each span is individually configurable as either T1 or E1.

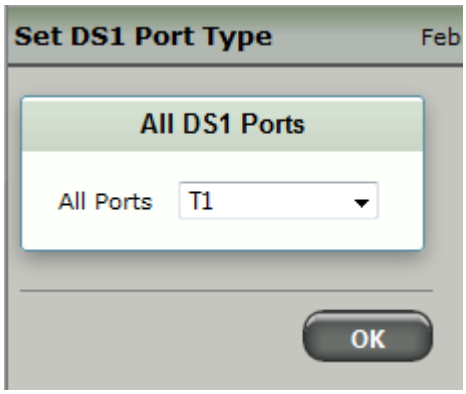
Sonus SBC 1000 T1/E1 Ports

T1/E1 ports on the Sonus SBC 1000 are provided via a non-removable internal card in either one port or two port versions.

Setting the Port Type

To set the port type:

1. Click the **Set DS1 Port Type** text at the top of the **Port Table View**page.



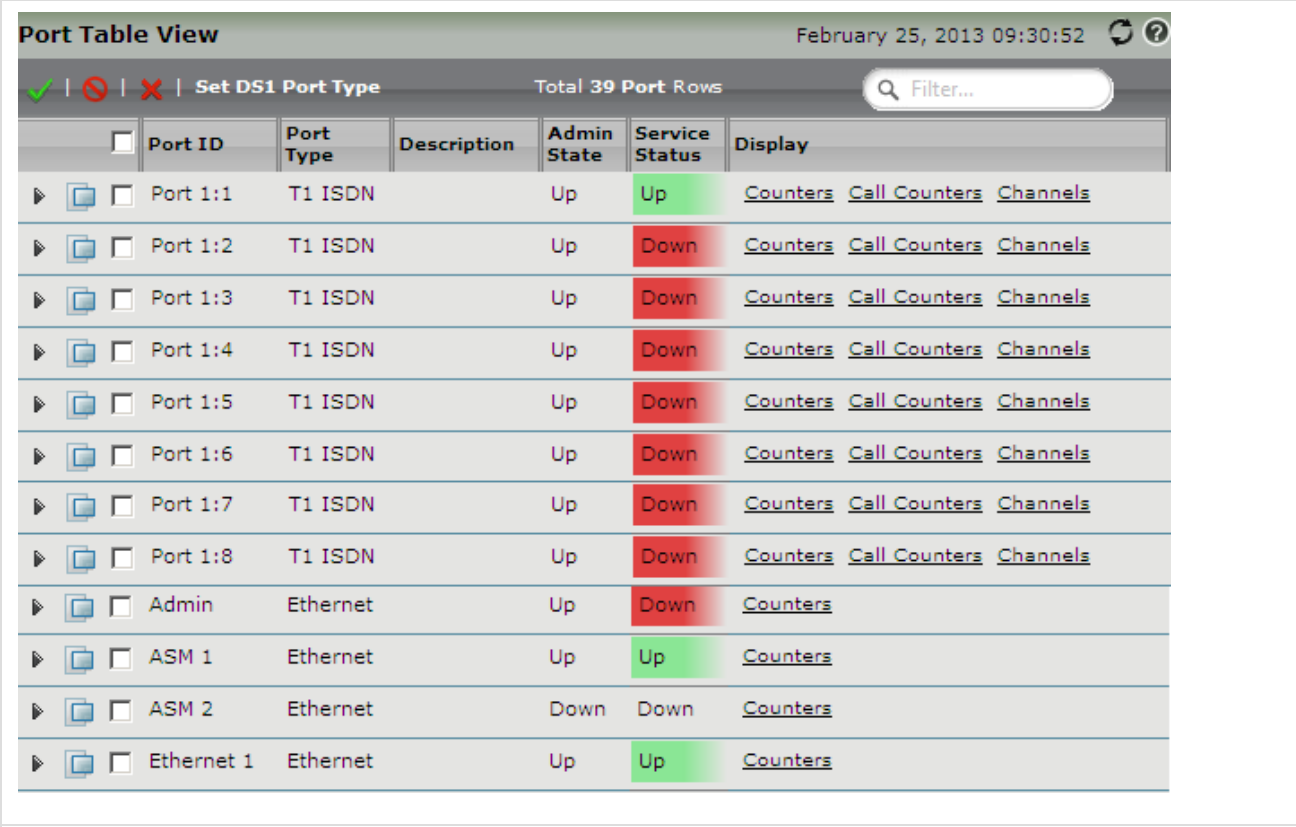
2. Select either **T1** or **E1** from the ports menu(s).
3. Click **OK**.

Configuring T1 Ports

Modifying, Enabling, and Disabling a Port

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.

Copyright © 2015 Sonus Networks. All rights reserved.

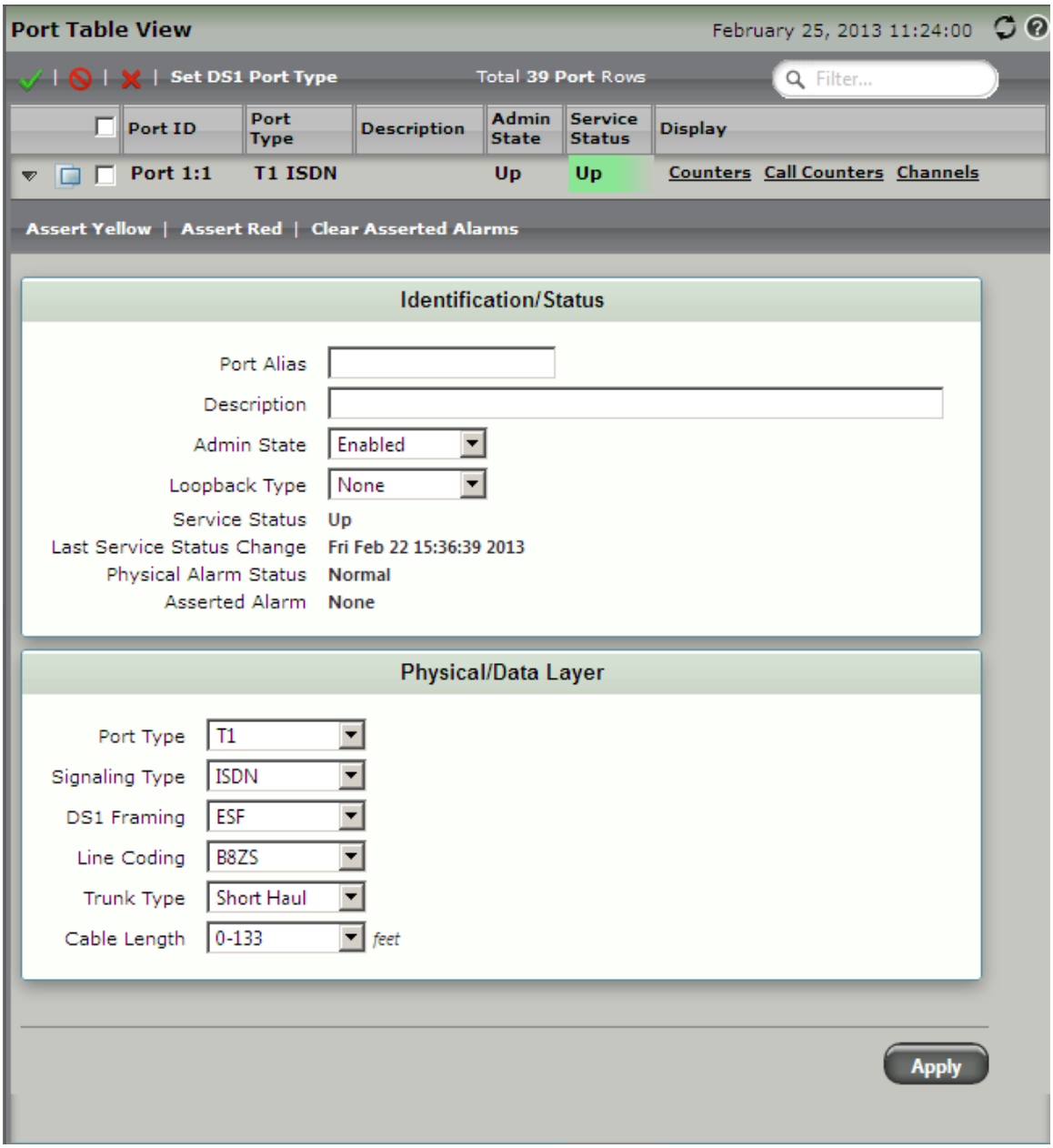


Port ID	Port Type	Description	Admin State	Service Status	Display
Port 1:1	T1 ISDN		Up	Up	Counters Call Counters Channels
Port 1:2	T1 ISDN		Up	Down	Counters Call Counters Channels
Port 1:3	T1 ISDN		Up	Down	Counters Call Counters Channels
Port 1:4	T1 ISDN		Up	Down	Counters Call Counters Channels
Port 1:5	T1 ISDN		Up	Down	Counters Call Counters Channels
Port 1:6	T1 ISDN		Up	Down	Counters Call Counters Channels
Port 1:7	T1 ISDN		Up	Down	Counters Call Counters Channels
Port 1:8	T1 ISDN		Up	Down	Counters Call Counters Channels
Admin	Ethernet		Up	Down	Counters
ASM 1	Ethernet		Up	Up	Counters
ASM 2	Ethernet		Down	Down	Counters
Ethernet 1	Ethernet		Up	Up	Counters

To modify a Port:

Click the **expand** (▸) Icon next to the entry you wish to modify.

Copyright © 2015 Sonus Networks. All rights reserved.



T1 Ports - Field Definitions

Port Alias

Specifies a human readable name for the port, maximum 128 characters.

Identification/Status - Field Definitions

The Identification/Status Panel controls the network identity of the port and its administrative state (Up or Down). It also provides the port's current service status and when that status last changed.

Port Alias

Specifies an alias for the port. This text is configured by the operator for exclusive use by SNMP-based element and network management systems to assign a key to the port or interface, that is unique across the managed network. Examples would be "Node10Port5" and "VerizonPort5"

Copyright © 2015 Sonus Networks. All rights reserved.

Admin State

Specifies the administrative state of the port.

Lookback Type

Specifies the loop back status of the port.

Loopback is used when testing the line so that any potential fault can be isolated to a particular section of the line. The various loop types control the point at which the loop happens and helps narrow down the faulty section of the line. The **Line** type is the only loopback type available for E1.

Loopback disrupts normal traffic on the line. Consequently, the loopback type option should be set to **None** when not actively performing troubleshooting activities related to the associated port.

Physical/Date Layer

Used to specify the Layer 1 and Layer two properties of the port.

Signaling Type

Specifies the signaling type for the port. ISDN or CAS.

DS1 Framing

Specifies the framing type used on a T1 Port. The Choices available for T1 are ESF and D4. DS1 Framing options must match at each end of the line.

D4 or Super Frame (SF)
A Super Frame consists of twelve consecutive 193-bit frames. Due to the unique bit sequences exchanged, the framing schemes are not compatible with each other. These two types of framing (SF, and ESF) use their 8 kbit/s framing channel in different ways.

ESF or Extended Super Frame
whereas an Extended Super Frame consists of twenty-four consecutive 193-bit frames of data.

Compatibility
Due to the unique bit sequences exchanged, the framing schemes are not compatible with each other. These two types of framing (SF, and ESF) use their 8 kbit/s framing channel in different ways.

Line Coding

Specifies the line coding for the port.
In telecommunication, a line code (also called digital baseband modulation, also called digital baseband transmission method) is a code chosen for use within a communications system for baseband transmission purposes. Line coding is often used for digital data transport.

Line coding consists of representing the digital signal to be transported by an amplitude- and time-discrete signal that is optimally tuned for the specific properties of the physical channel (and of the receiving equipment). The waveform pattern of voltage or current used to represent the 1s and 0s of a digital data on a transmission link is called line encoding. The common types of line encoding are unipolar, polar, bipolar, and Manchester encoding.

Copyright © 2015 Sonus Networks. All rights reserved.

Trunk Type

Specifies the trunk type for T1 Ports. Choices are Short Haul and Long Haul

Cable Length

Specifies a range of length in feet for Short Haul trunk types.

Line Buildout

Specifies the attenuation used for a Long Haul type T1 port, in decibels.

Enabling and Disabling Logical Interfaces

To enable a Logical Interface:

1. Select the check box next to the entry you wish to enable.
2. Click the **Enable** ( ) icon at the top of the table.

To disable a Logical Interface:

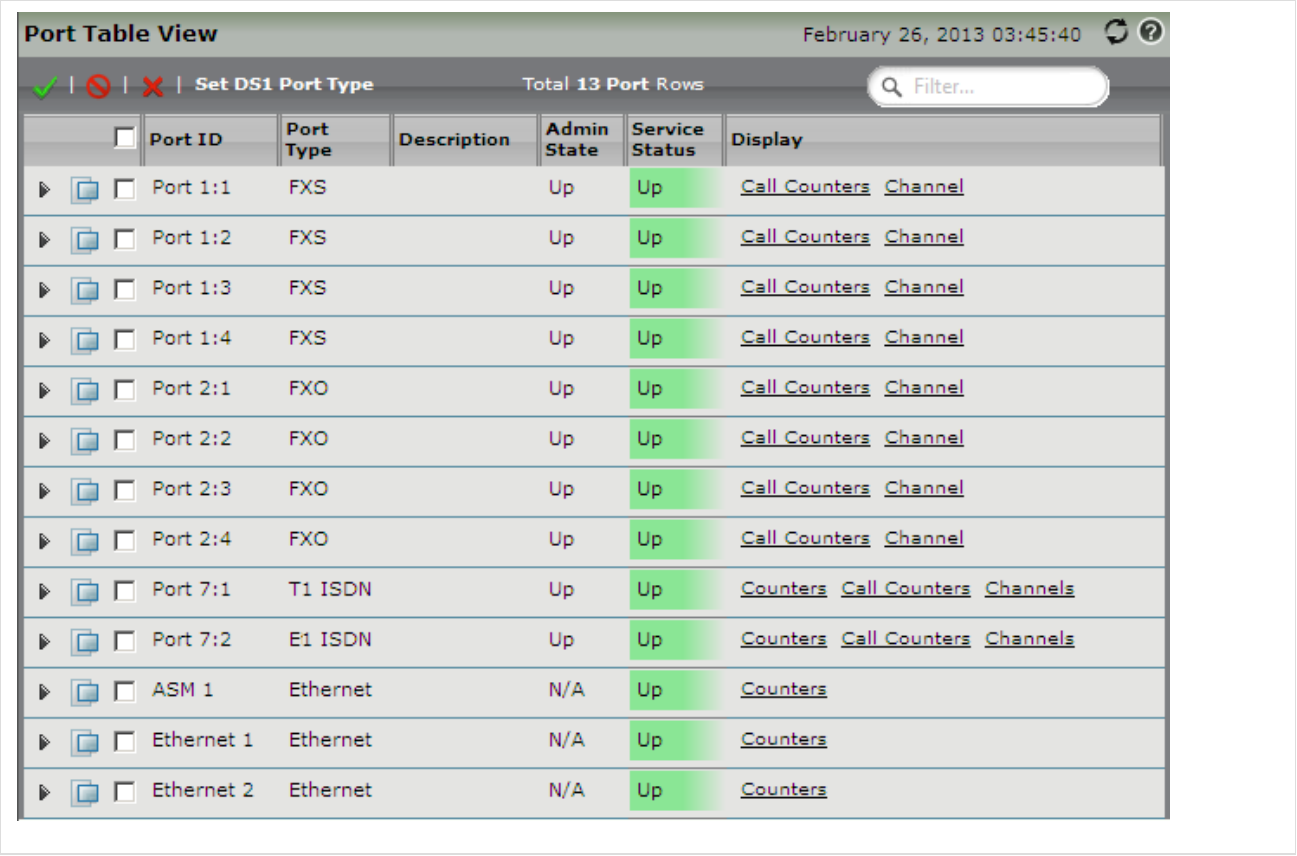
1. Select the check box next to the entry you wish to disable.
2. Click the **Disable** ( ) icon at the top of the table.

Configuring E1 Ports

Modifying, Enabling, and Disabling a Port

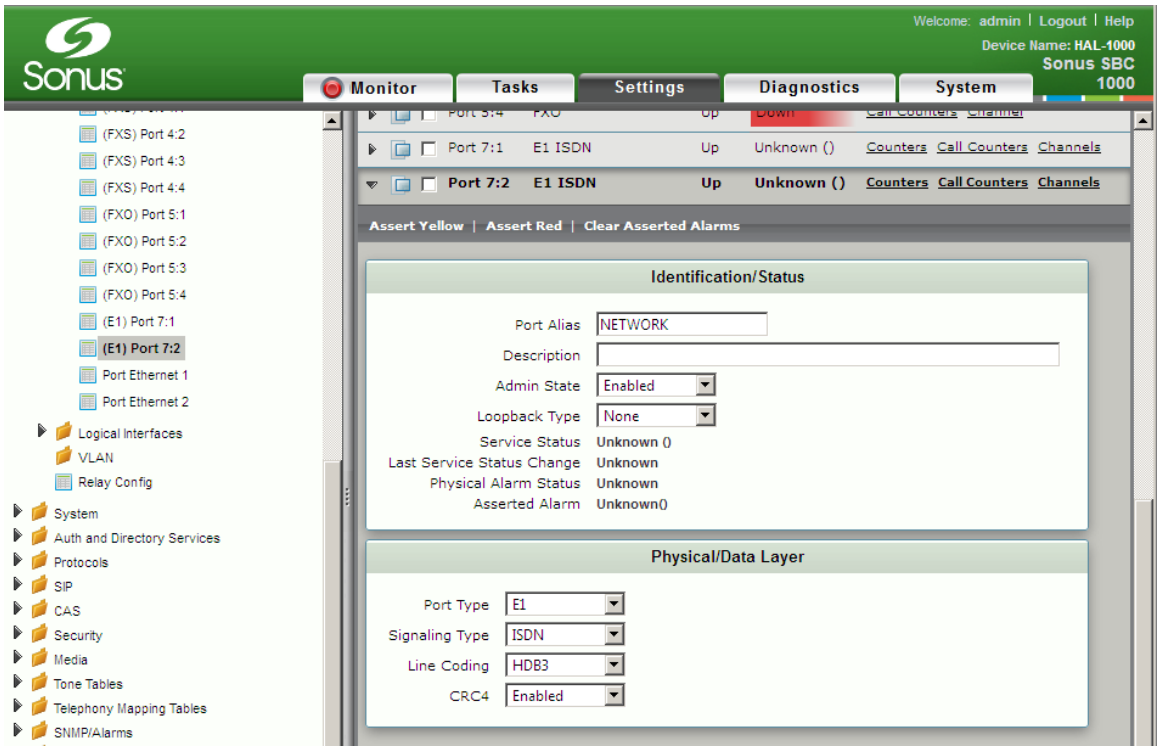
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.

Copyright © 2015 Sonus Networks. All rights reserved.



To modify a Port:

Click the **expand** (▸) Icon next to the entry you wish to modify.



Copyright © 2015 Sonus Networks. All rights reserved.

Identification/Status - Field Definitions

The Identification/Status Panel controls the network identity of the port and its administrative state (Up or Down). It also provides the port's current service status and when that status last changed.

Port Alias

Specifies an alias for the port. This text is configured by the operator for exclusive use by SNMP-based element and network management systems to assign a key to the port or interface, that is unique across the managed network. Examples would be "Node10Port5" and "VerizonPort5"

Admin State

Specifies the administrative state of the port.

Lookback Type

Specifies the loop back status of the port.

Loopback is used when testing the line so that any potential fault can be isolated to a particular section of the line. The various loop types control the point at which the loop happens and helps narrow down the faulty section of the line. The **Line** type is the only loopback type available for E1.

Loopback disrupts normal traffic on the line. Consequently, the loopback type option should be set to **None** when not actively performing troubleshooting activities related to the associated port.

Physical/Date Layer

Used to specify the Layer 1 and Layer two properties of the port.

Signaling Type

Specifies the signaling type for the port. ISDN or CAS.

Line Coding

Specifies the line coding for the port.

CRC4

Specifies whether or not to use CRC4 checking.

Note: If CRC is not configured the same way at each end of the line, an E1 line may not come up. Be sure that the CRC4 configurations at each end match.

To enable a Port:

1. Select the check box next to the entry you wish to enable.
2. Click the **Enable** (✔) icon at the top of the table.

To disable a Port:

1. Select the check box next to the entry you wish to disable.

Copyright © 2015 Sonus Networks. All rights reserved.

2. Click the **Disable** ( ) icon at the top of the table.

Configuring FXS Ports

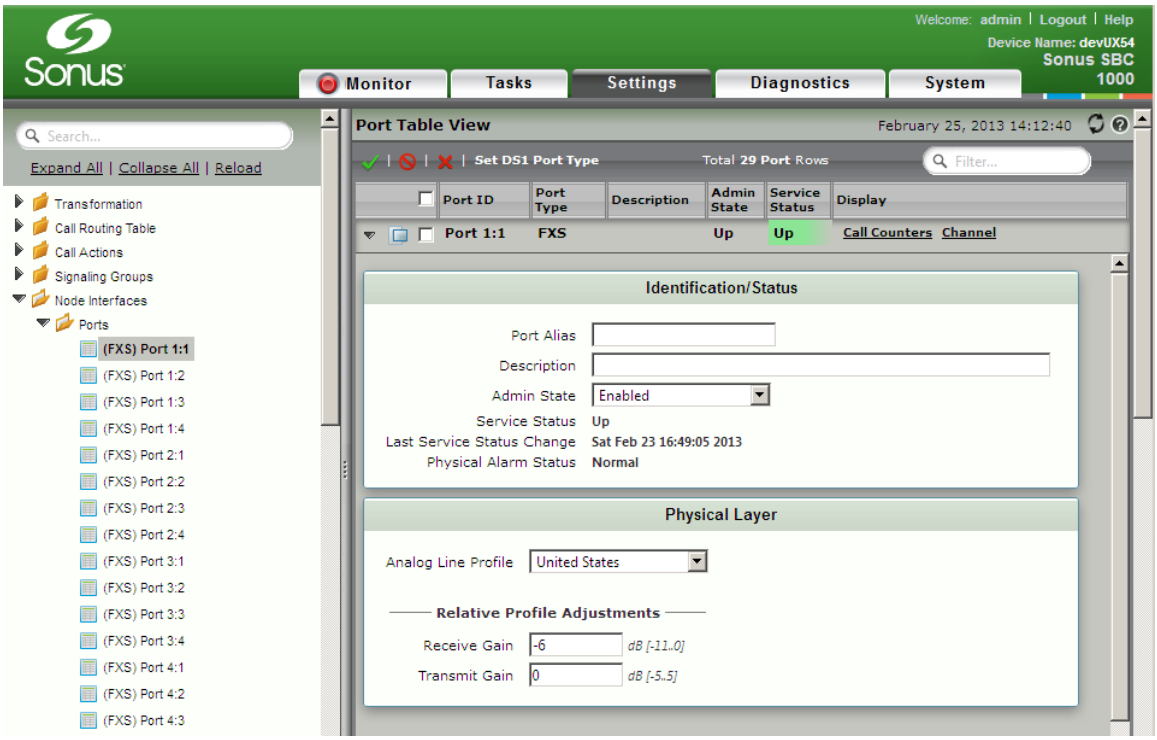
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.



To modify a Port:

Click the **expand** ( ) Icon next to the entry you wish to modify.

Copyright © 2015 Sonus Networks. All rights reserved.



Identification/Status - Field Definitions

The Identification/Status Panel controls the network identity of the port and its administrative state (Up or Down). It also provides the port's current service status and when that status last changed.

Port Alias

Specifies an alias for the port. This text is configured by the operator for exclusive use by SNMP-based element and network management systems to assign a key to the port or interface, that is unique across the managed network. Examples would be "Node10Port5" and "VerizonPort5"

Admin State

Specifies the administrative state of the port.

Physical Layer - Field Definitions

Analog Line Profile

Analog line profiles allow users to change the impedance presented by the Sonus SBC 1000/2000 FXS ports. It should match the impedance of the specified country's Telco. Some countries use resistive impedance and some use complex impedance. For example, telephone companies in the United States use 600 ohm resistive impedance where as Australia uses 220 ohms in series with the parallel combination of 820 ohms and 120 nF.

Relative Profile Adjustments

- Negative values represent signal attenuation (lower volume).
- Positive values represent signal amplification (higher volume).

Receive Gain

Copyright © 2015 Sonus Networks. All rights reserved.

Allows you to control the gain or loss (in decibels) to the received voice levels.

Transmit Gain

Specifies the gain or loss in decibels to apply to the transmitted voice levels.

⚠ Receive and Transmit Gain affect FAX functionality. Use/Modify with care.

Configuring Powerdown Telephony Passthrough

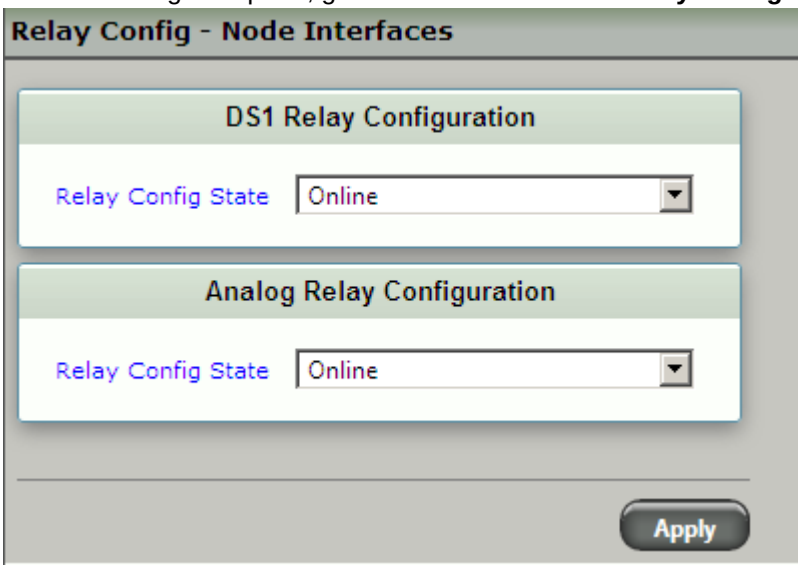
This feature enhances system reliability by providing the ability to physically and electrically connect the two DS1 ports (T1/E1) in the event of a loss of electrical power to the Sonus SBC 1000. It also allows you to maintain connectivity between the PSTN or other T1/E1 connection and the PBX or other gateway on the enterprise side while the Sonus SBC 1000 is being configured. You can physically install the Sonus SBC 1000, select the Passthrough mode, and continue configuring the Sonus SBC 1000 with no interruption to network/phone services. When the Sonus SBC 1000 is ready to be placed into service, simply *"flip the switch"*, (i.e., select either **Online** or **Powerdown Passthrough** mode) and the Sonus SBC 1000 will be online and fully functioning as a gateway between the external (i.e., ISDN side) and the internal side of the connection.

ℹ This feature is available on the Sonus SBC 1000 only.

Configuring the Relay State

To configure the relay state:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Relay Config**.



3. Select the appropriate option in the **Relay Config State** field.

DS1 Relay Configuration - Field Definitions

DS1 Relay Config State

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the Powerdown Telephony Passthrough mode for DS1 ports.

Online Mode Operation
In the Online Mode the Sonus SBC 1000 operates as a gateway between the two DS1 (T1/E1) ports, if power is lost, then connectivity between the two ports is also lost.

Passthrough Mode Operation
In the Passthrough Mode the two DS1 (T1/E1) ports are physically and electrically connected by a relay.

Powerdown Passthrough Mode Operation
In the Powerdown Passthrough Mode, the two DS1 (T1/E1) ports operate normally, using the Sonus SBC 1000 as a gateway unless the Sonus SBC 1000 loses power. If the Sonus SBC 1000 loses power the DS1 (T1/E1) ports are physically and electrically connected by a relay.

Analog Relay Configuration - Field Definitions

This panel is not visible when no FXS/FXO cards with relays are installed.
The Analog Relay Configuration panel is only visible when the following conditions are true:

- FXS cards with relays are installed in the lower slots (1,3, and 5).
- FXO cards are installed in the upper slots directly above the corresponding FXS cards.

Relay Config State

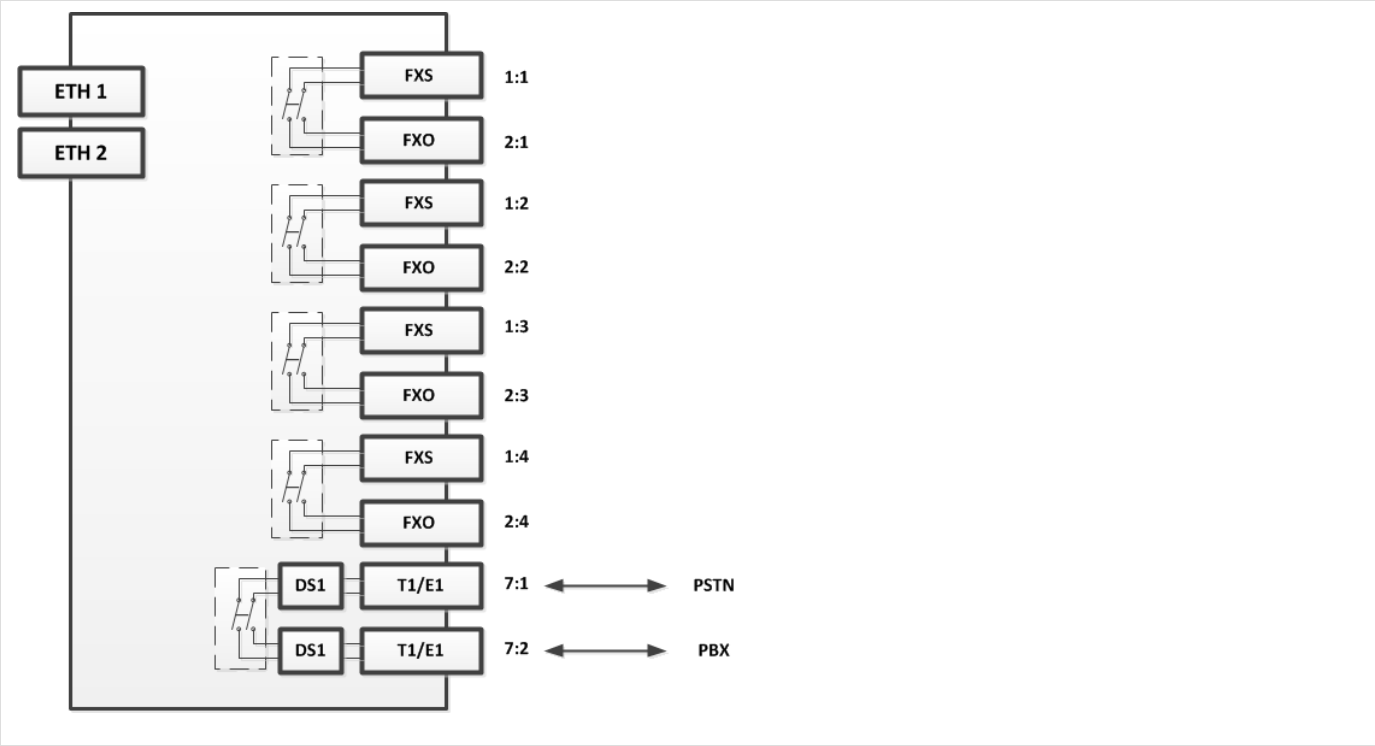
Specifies the Powerdown Telephony Passthrough mode for FAX/FXO ports.

Online Operation
In the online mode, the analog (FXS/FXO) ports are controlled and routed by the SBC.

> If the SBC is powered down, the FXS and FXO ports are physically and electrically connected in the same manner as they are in the passthrough mode.

Passthrough Operation
In the passthrough mode, the FXO and FXS ports are physically connected via relays. In this mode, there is a 1:1 correspondence between FXS and FXO ports. FXS port 1:1 is physically/electrically connected directly to FXO port 2:1, FXS port 1:2 connects to FXO port 2:2, etc.

Copyright © 2015 Sonus Networks. All rights reserved.



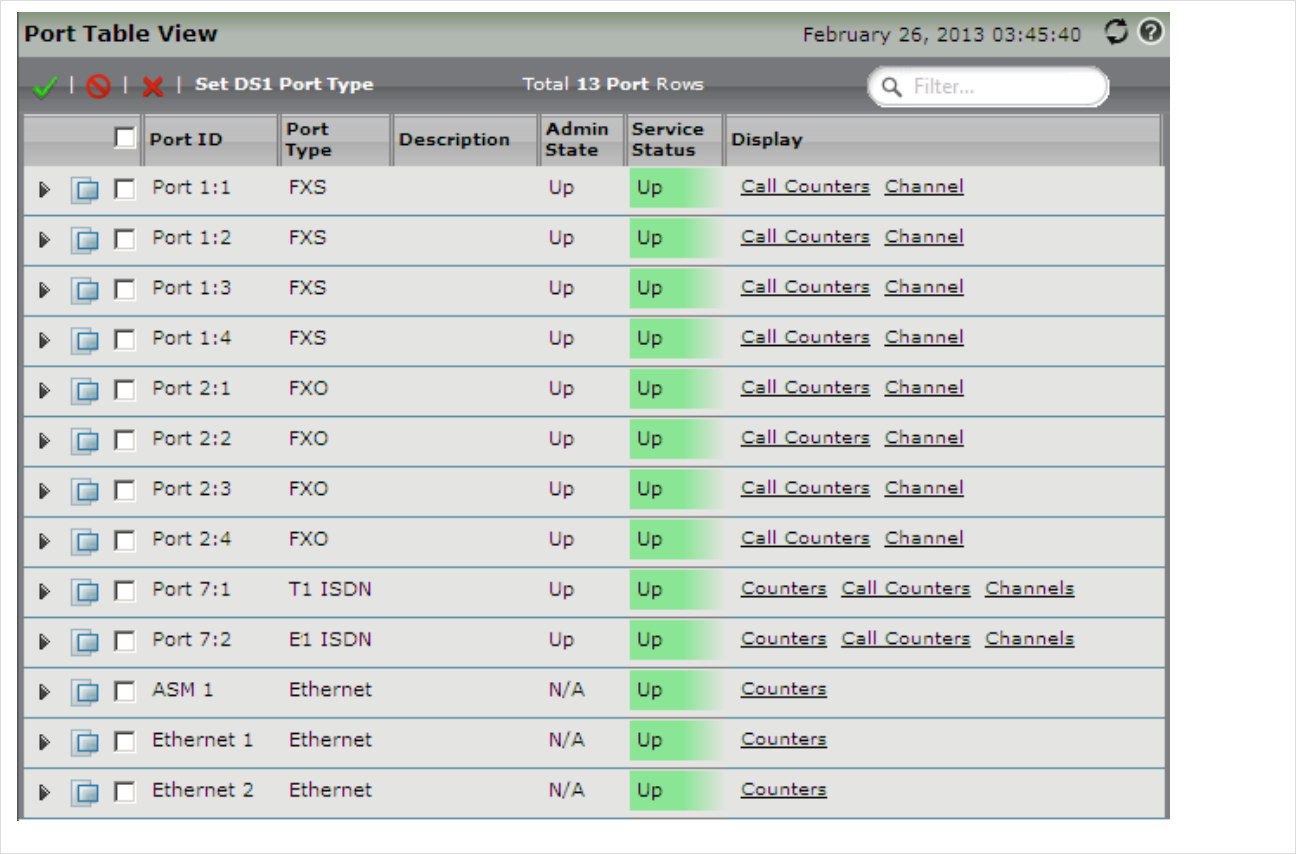
Viewing Port Counters and Channel Details

This page describes how to read and reset the counters associated with ISDN and Ethernet ports

- ISDN Ports
  - DS1 Port Counters
  - Port Call Counters
  - Channel Detail Information Pages
    - Channel Table Page
    - Detailed Call Information
    - Outbound Channel Details

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.

Copyright © 2015 Sonus Networks. All rights reserved.



ISDN Ports

Each ISDN port has three informational displays associated with it; DS1 Port Counters, Port Call Counters, and a Channel Table. This section will describe each of those displays and their contents.

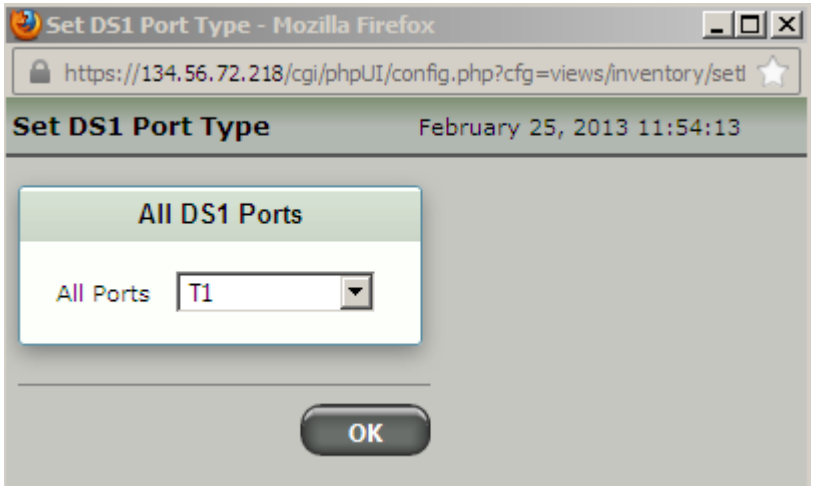
DS1 Port Counters

The DS1 Port Counters page provides you with information about transmission and receive errors, transmit and receive frames and bytes, and other port traffic metrics.

To view the DS1 Port Counters page:

- Click the **Counters**text in the row corresponding to the port who's counters you want to view.

Copyright © 2015 Sonus Networks. All rights reserved.



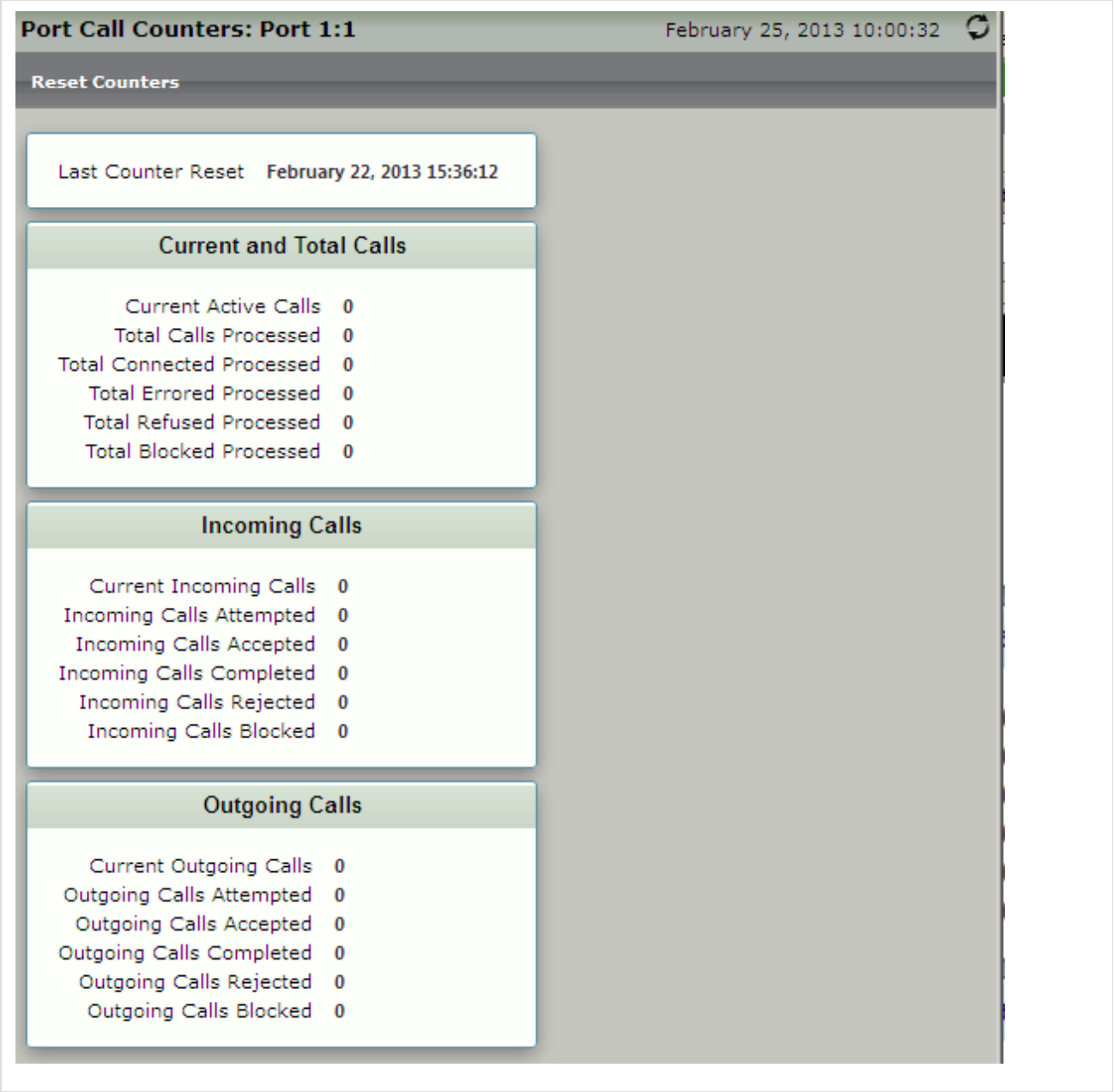
Port Call Counters

The Port Call Counters page provides you with information about incoming, outgoing, and current calls on the selected port.

To view the Port Call Counters page:

- Click the **Call Counters**text in the row corresponding to the port who's Port Call Counters you want to view.

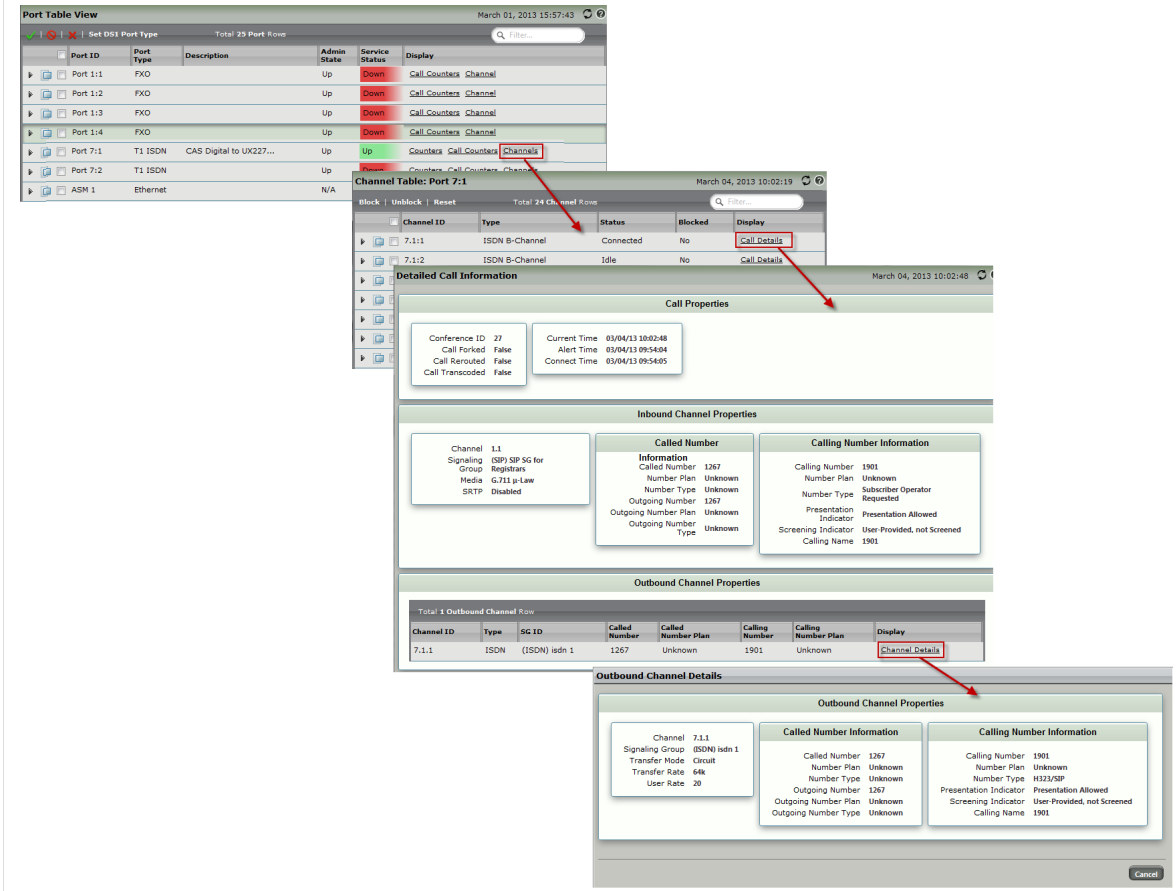
Copyright © 2015 Sonus Networks. All rights reserved.



Channel Detail Information Pages

The Sonus SBC 1000/2000 provides a fine level of granularity of port/channel information, with nested dialogs.

Copyright © 2015 Sonus Networks. All rights reserved.



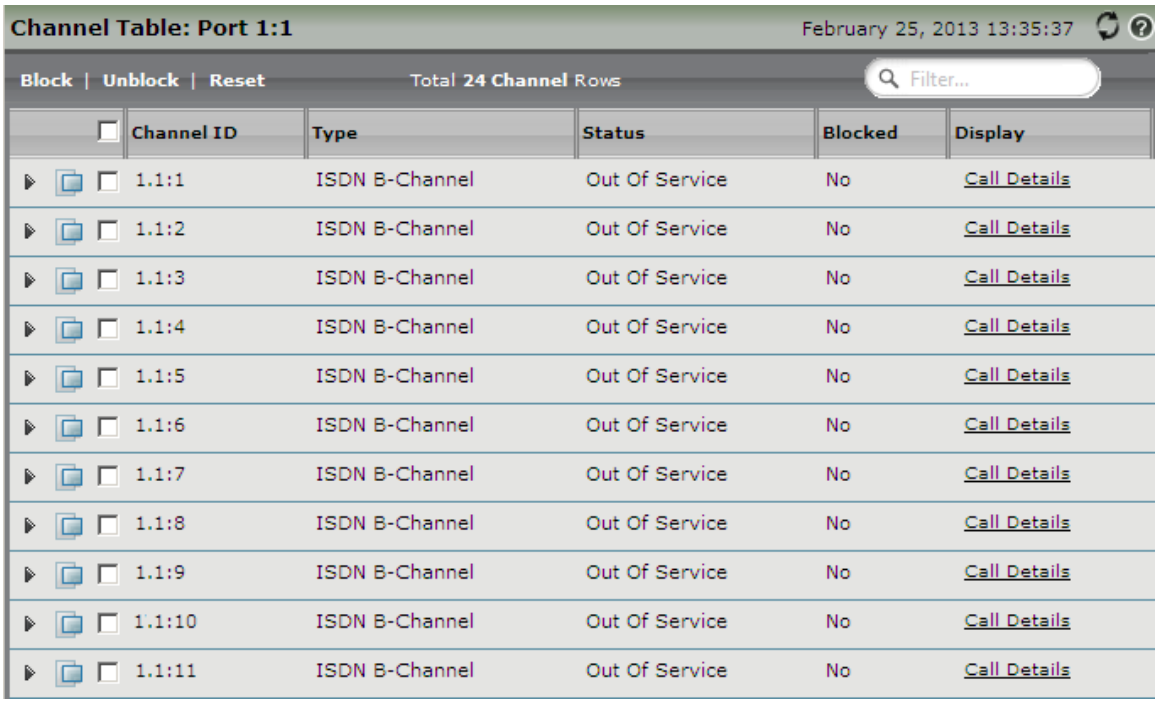
Channel Table Page

The Channel Table allows you to see details about a call in progress on a selected channel.

To view the Channel Table:

- Click the **Channels** text in the row corresponding to the port who's Channel Table you want to view.

Copyright © 2015 Sonus Networks. All rights reserved.

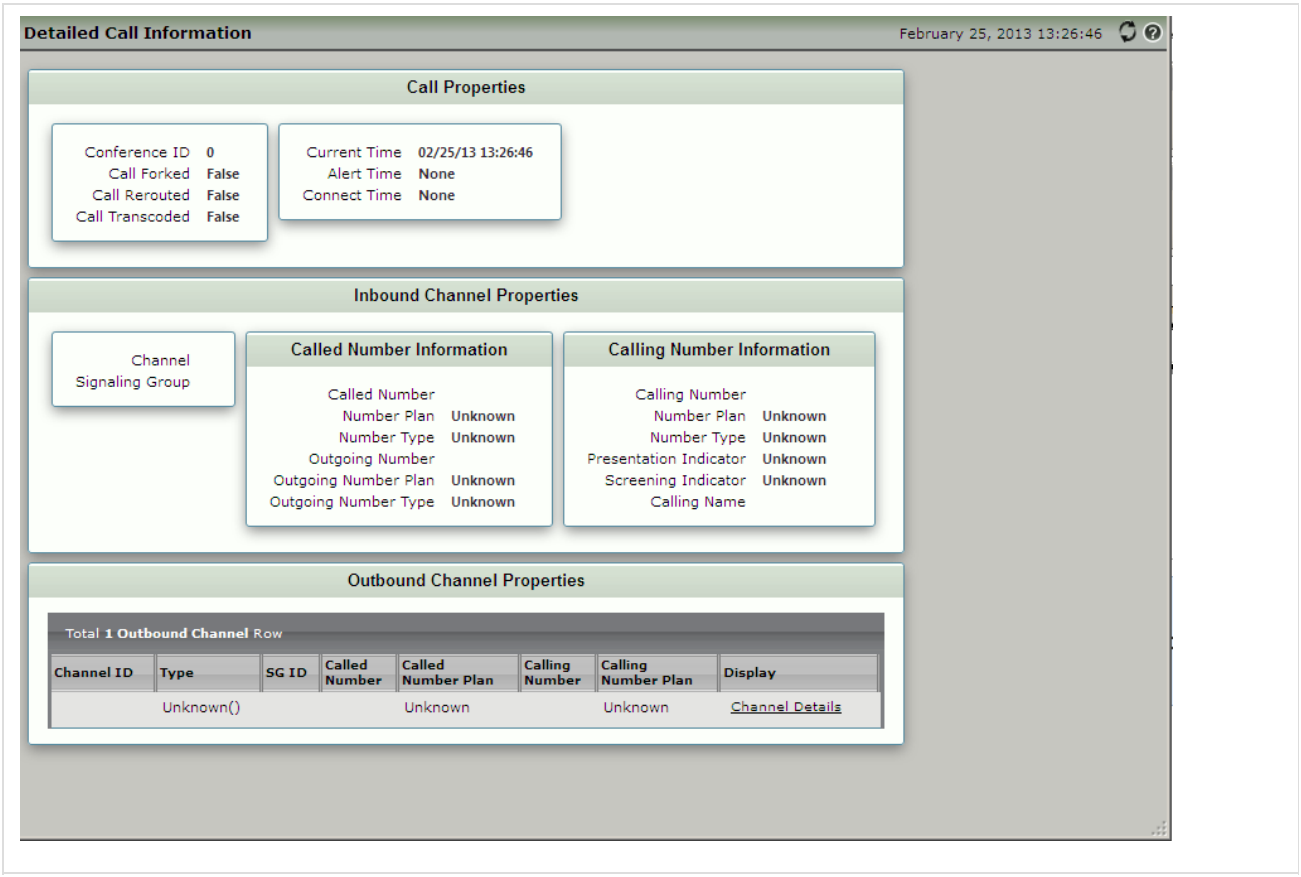


Detailed Call Information

This page provides you with a detailed list of information about a call which is currently up on the channel selected in the Channel Table.

To view the details of an active call in the Channel Table:

- Click the **Call Details** text in the row corresponding to the channel in the Channel Table panel.



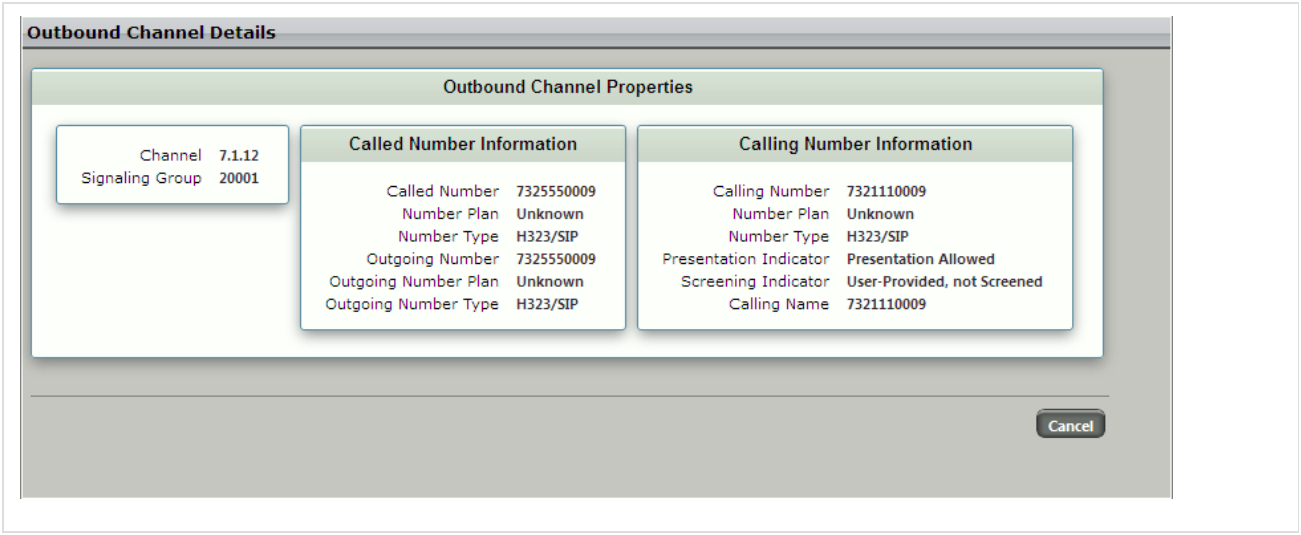
Copyright © 2015 Sonus Networks. All rights reserved.

Outbound Channel Details

This page provides you with the finest granularity of detail, with information about the current call on the outbound channel.

To view information about a call on an outbound channel

- Click the **Channel Details** text in the Outbound Channel Properties pane of the Detailed Call Information panel:*

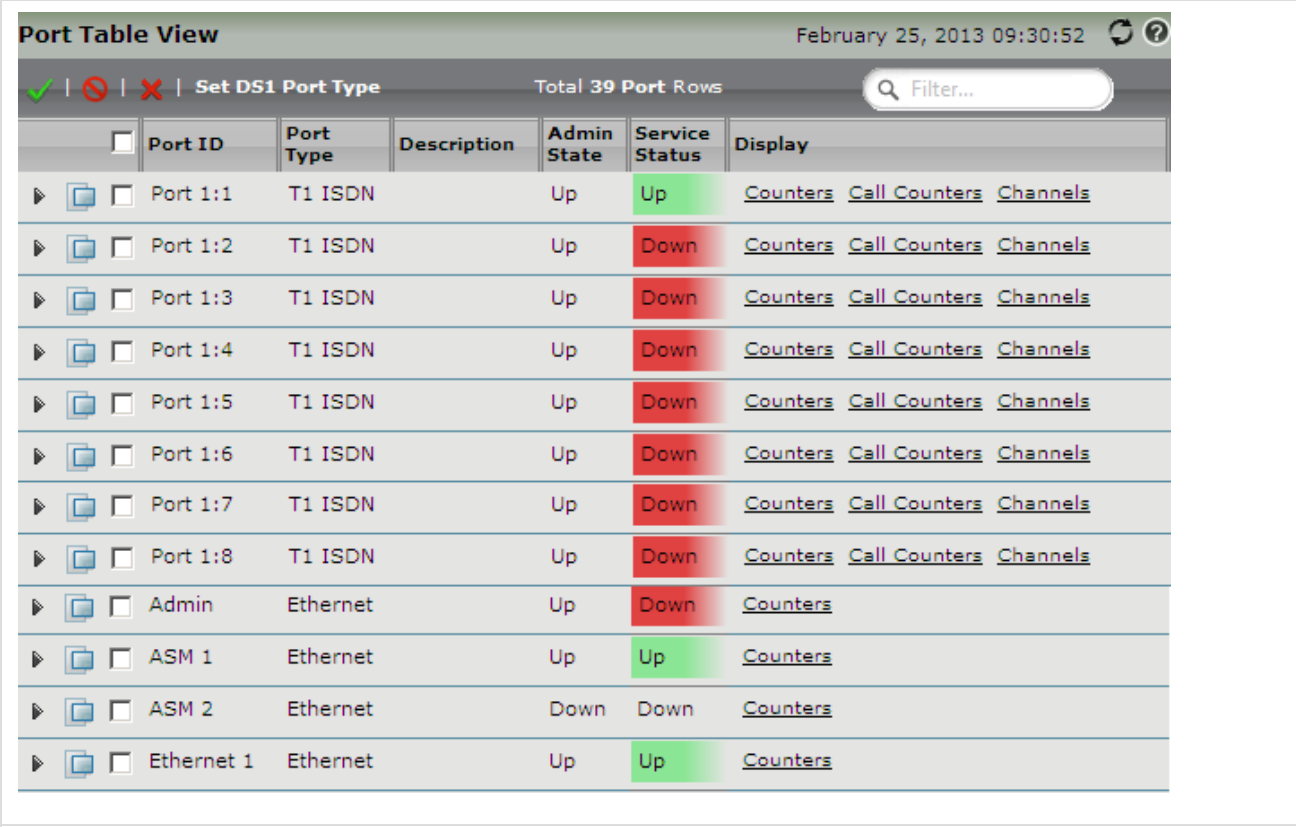


Configuring BRI Ports

Modifying, Enabling and Disabling a Port

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.

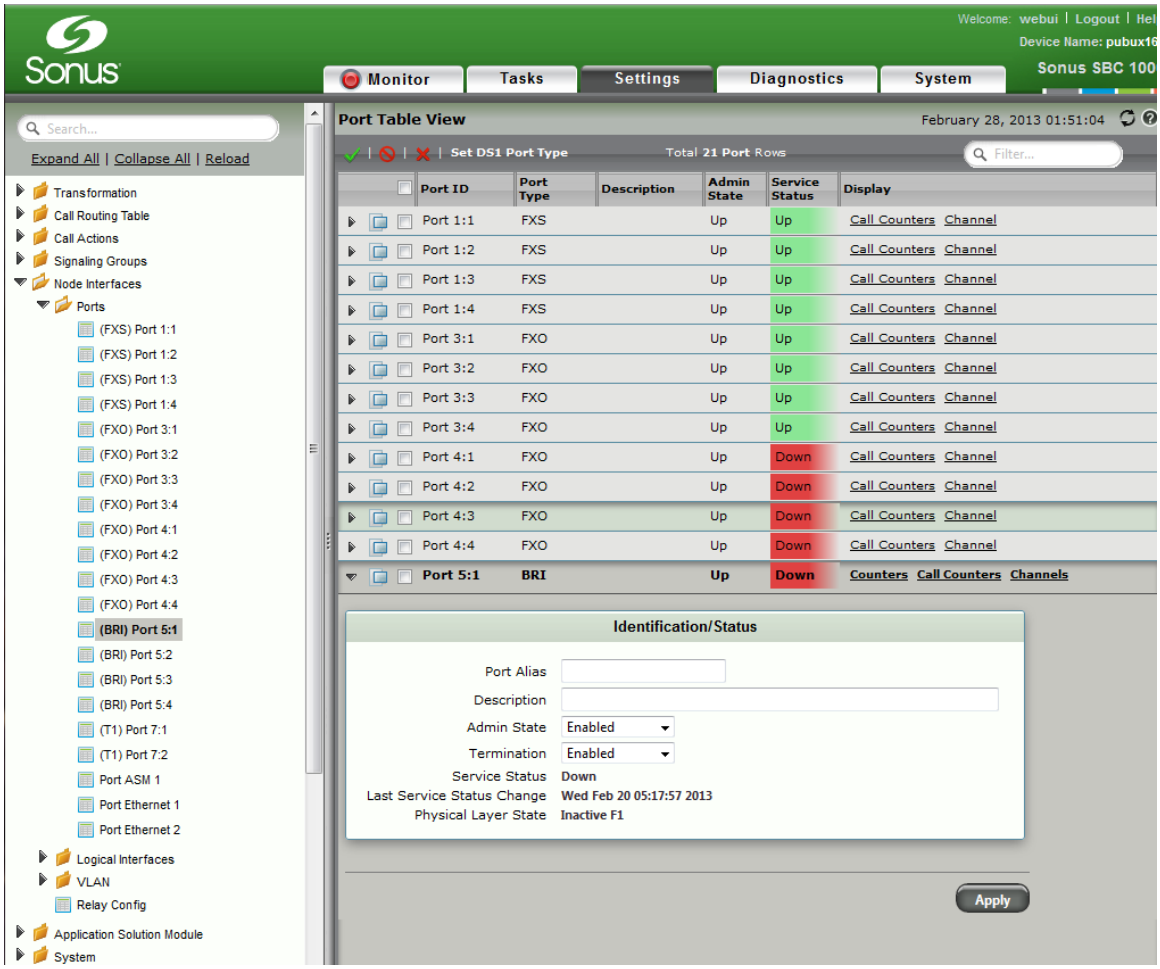
Copyright © 2015 Sonus Networks. All rights reserved.



To modify a port:

Click the **expand** (▸) Icon next to the entry you wish to modify.

Copyright © 2015 Sonus Networks. All rights reserved.



Identification/Status - Field Definitions

The Identification/Status Panel controls the network identity of the port and its administrative state (Up or Down). It also provides the port's current service status and when that status last changed.

Port Alias

Specifies an alias for the port. This text is configured by the operator for exclusive use by SNMP-based element and network management systems to assign a key to the port or interface, that is unique across the managed network. Examples would be "Node10Port5" and "VerizonPort5"

Admin State

Specifies the administrative state of the port.

Termination

Copyright © 2015 Sonus Networks. All rights reserved.

This option determines whether or not the ISDN S/T interface is terminated on this port.

The BRI physical interface comprises two parts:

- in-house cabling (S/T bus) from the ISDN terminal to the Network Termination (NT).
- transmission from the NT to the Central Office (U-reference point).

An S/T bus must be terminated at both ends. One end of which is the Network Termination device and the other end is the Terminal Equipment (TE) end.

Common Connection and Termination Scenarios

Connection Scheme	Termination
No other devices on the same S-Bus.	Enabled
Other devices on the same S-Bus ***and*** the SBC is ***not the last*** device on the bus.	Disabled
SBC is connected to a PBX.	Enabled

Important Note

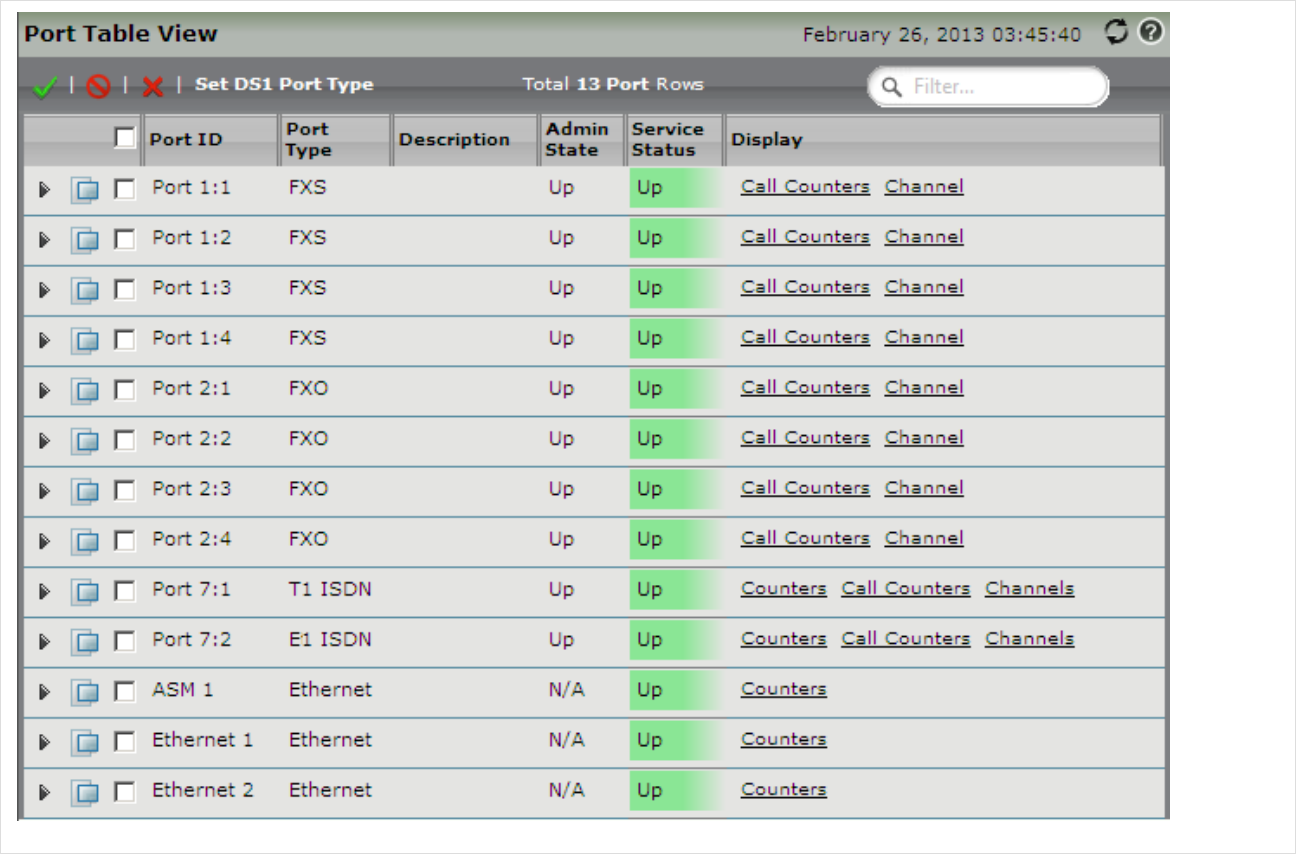
The BRI port on the SBC does not supply power.

See Also:*Adding and Modifying ISDN Signaling Groups*

Configuring FXO Ports

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces> Ports**.

Copyright © 2015 Sonus Networks. All rights reserved.

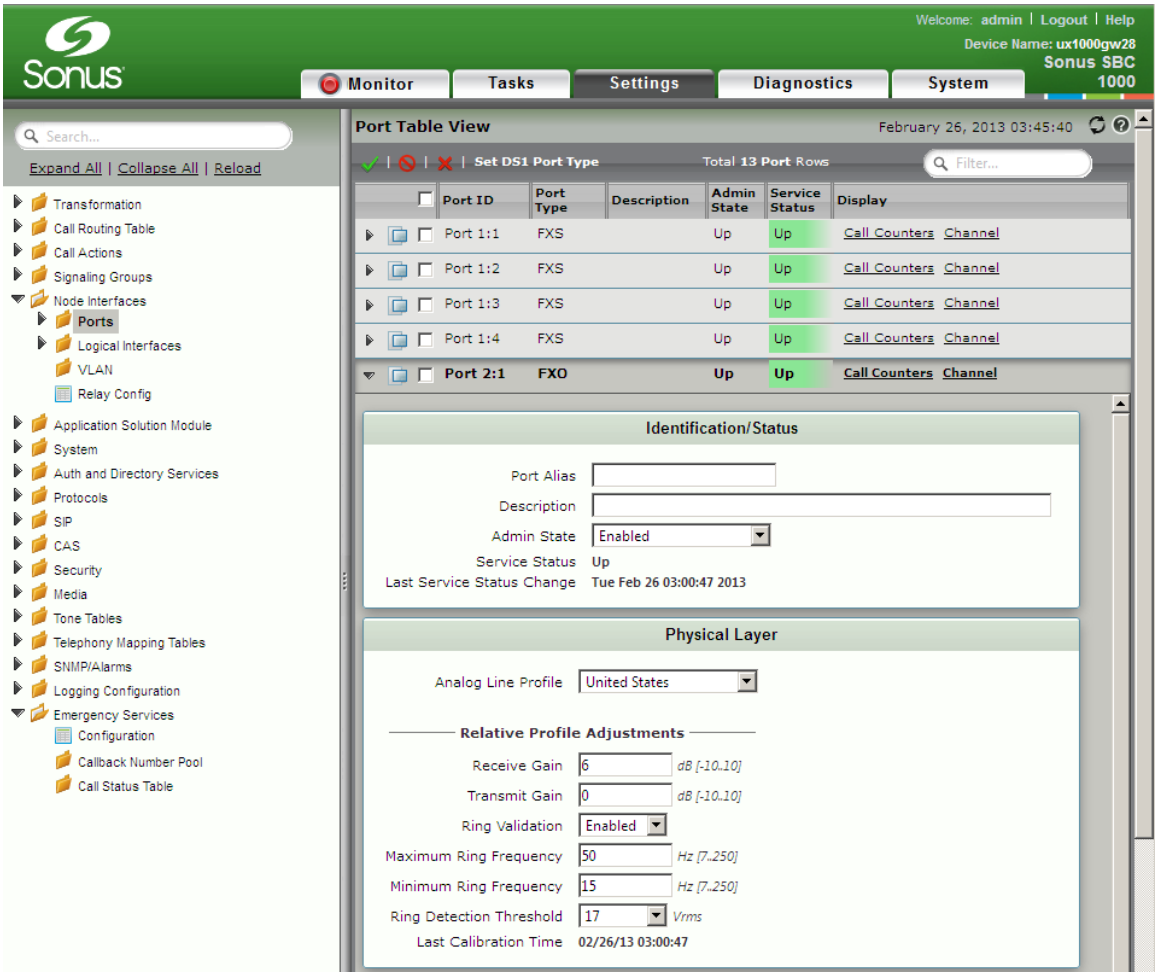


Port ID	Port Type	Description	Admin State	Service Status	Display
Port 1:1	FXS		Up	Up	Call Counters Channel
Port 1:2	FXS		Up	Up	Call Counters Channel
Port 1:3	FXS		Up	Up	Call Counters Channel
Port 1:4	FXS		Up	Up	Call Counters Channel
Port 2:1	FXO		Up	Up	Call Counters Channel
Port 2:2	FXO		Up	Up	Call Counters Channel
Port 2:3	FXO		Up	Up	Call Counters Channel
Port 2:4	FXO		Up	Up	Call Counters Channel
Port 7:1	T1 ISDN		Up	Up	Counters Call Counters Channels
Port 7:2	E1 ISDN		Up	Up	Counters Call Counters Channels
ASM 1	Ethernet		N/A	Up	Counters
Ethernet 1	Ethernet		N/A	Up	Counters
Ethernet 2	Ethernet		N/A	Up	Counters

To modify a Port:

Click the **expand** (▸) Icon next to the entry you wish to modify.

Copyright © 2015 Sonus Networks. All rights reserved.



Identification/Status - Field Definitions

The Identification/Status Panel controls the network identity of the port and its administrative state (Up or Down). It also provides the port's current service status and when that status last changed.

Port Alias

Specifies an alias for the port. This text is configured by the operator for exclusive use by SNMP-based element and network management systems to assign a key to the port or interface, that is unique across the managed network. Examples would be "Node10Port5" and "VerizonPort5"

Admin State

Specifies the administrative state of the port.

Physical Layer - Field Definitions

Analog Line Profile

Analog line profiles allow users to change the impedance presented by the Sonus SBC 1000/2000 FXS ports. It should match the impedance of the specified country's Telco. Some countries use resistive impedance and some use complex impedance. For example, telephone companies in the United States use 600 ohm resistive impedance where as Australia uses 220 ohms in series with the parallel combination of 820 ohms and 120 nF.

Copyright © 2015 Sonus Networks. All rights reserved.

Relative Profile Adjustments

- Negative values represent signal attenuation (lower volume).
- Positive values represent signal amplification (higher volume).

Receive Gain

Allows you to control the gain or loss (in decibels) to either the received or transmitted signals(Packet ? PCM direction).

Transmit Gain

Specifies the gain or loss in decibels to apply to transmitted signals (PCM ? Packet direction).

Ring Validation

Enables and disables ring validation by the FXO analog port.

Maximum Ring Frequency

Specifies the upper frequency limit used for ring validation by analog FXO port.

Minimum Ring Frequency

Specifies the lower frequency limit used for ring validation by analog FXO port.

Ring Detection Threshold

Specifies the RMS ring voltage, above which ring detection is guaranteed.

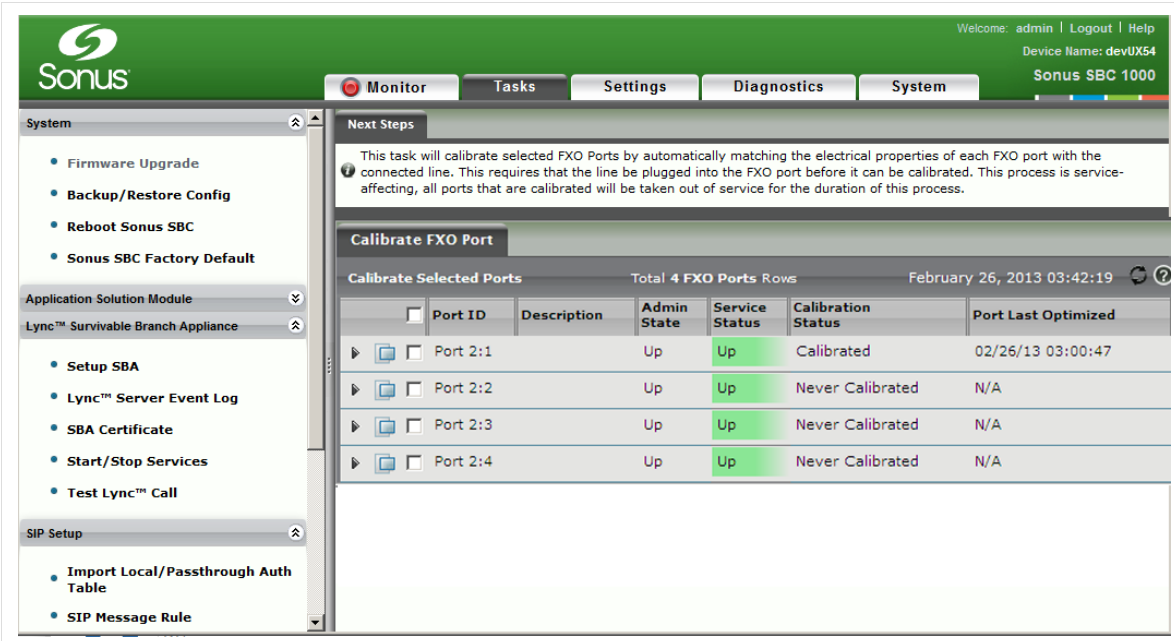
Calibrating FXO Ports

Impedance mismatching results in audible echos on the line and reduced call quality. Correctly matching the line impedance reduces or eliminates the echo. A number of factors influence the line impedance; line types which vary from country to country and vary between geographic regions, as well as the distance between the node and the central office.

The Sonus SBC 1000/2000 FXO Port Calibration function programmaticaly determines the optimum impedance and the local loop type settings and configures each selected port accordingly. The port calibration task is located in the WebUI under the Tasks tab and is performed as described in this section.

Calibrating FXO Ports

Copyright © 2015 Sonus Networks. All rights reserved.



Caution

The Calibration FXO function is an service affecting operation.

To calibrate an FXO port:

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, go to **Telephony Setup > Calibrate FXO Port**.
3. Select the port or ports you wish to calibrate.
4. Click the **Calibrate Selected Ports** link text at the top of the table.
5. Confirm that you wish to calibrate the selected FXO Ports.
6. Click **OK** to dismiss the successful completion dialog.

Working with SIP

This section contains information related to configuring the Sonus SBC 1000/2000 for SIP telephony, including but not limited to: Managing SIP Signaling Groups and Profiles, SIP Server Tables, Local Registrars, Registrant Tables, and more.

Managing SIP Signaling Groups

- Configuring the Sonus SBC 1000-2000 for Site Survivability
- Creating and Modifying SIP Signaling Groups
- Outbound Proxy Configuration
- Viewing SIP Counters and Channels
- Viewing Subscriber Data

Managing SIP Profiles

- Creating and Modifying SIP Profiles
- SIP Session Timer Configuration

Managing TLS Profiles

- Creating and Modifying TLS Profiles

Copyright © 2015 Sonus Networks. All rights reserved.

Managing SIP Server Tables

- Creating and Modifying Entries in SIP Server Tables

Managing Local Registrars

- Creating and Modifying SIP Local Registrars

Managing Contact Registrant Tables

- Creating and Modifying Entries in Contact Registrant Tables
- Viewing Registration Status for Entries in Contact Registrant Tables

Managing Remote Authorization Tables

- Creating and Modifying Entries to Remote Authorization Tables

Managing Local Pass-through Authorization Tables

- Creating and Modifying Entries to Local Pass-through Authorization Tables
- Importing Local Pass-through Authorization Entries

Managing SIP Trunk Groups

- Creating and Modifying SIP Trunk Groups

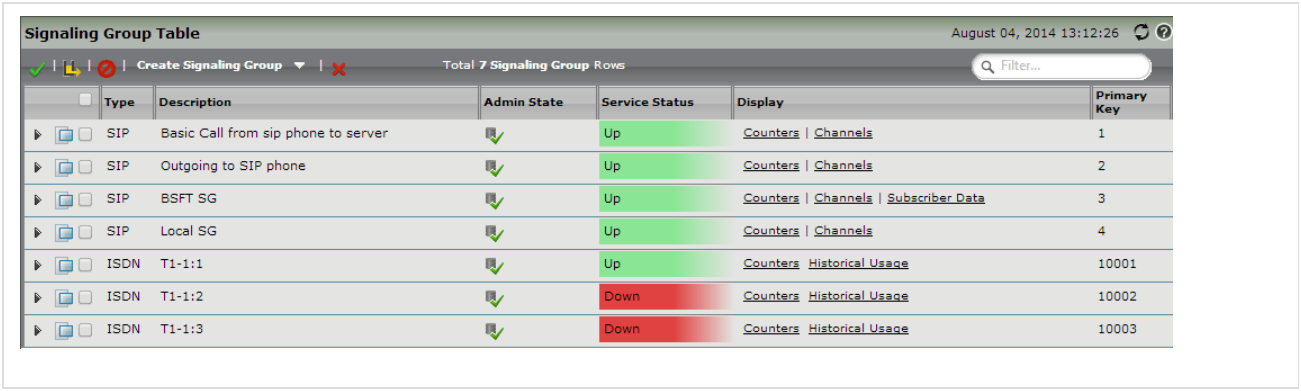
Miscellaneous SIP Information

Managing SIP Signaling Groups

Signaling groups allow telephony channels to be grouped together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which Call Routes are selected. They are also the location from which Tone Tables and Action Sets are selected. In the case of SIP, they specify protocol settings and link to server, media and mapping tables.

Working with SIP Signaling Groups

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. From the **Create Signaling Group** drop down box, select **SIP Signaling Group.**



To view an SIP Signaling Group's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Copyright © 2015 Sonus Networks. All rights reserved.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Configuring the Sonus SBC 1000-2000 for Site Survivability

Creating and Modifying SIP Signaling Groups

Outbound Proxy Configuration

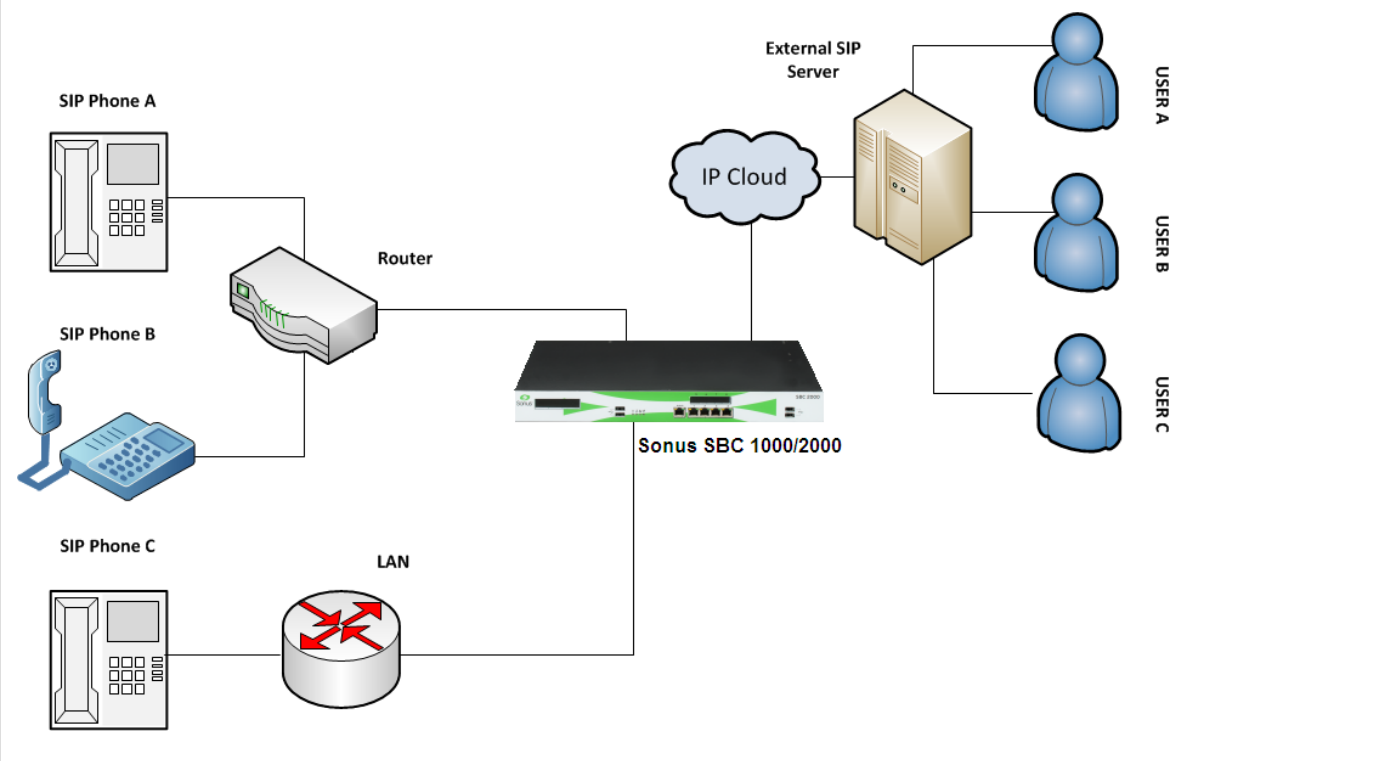
Viewing SIP Counters and Channels

Viewing Subscriber Data

Configuring the Sonus SBC 1000-2000 for Site Survivability

- Overview
- Forward After Registration Scenario
  - SIP Server Fail-over Scenario
- Setting up the Routing Tables

Overview



A SIP registrar is a server in an SIP network that accepts SIP REGISTER requests. The Sonus SBC 1000/2000 SIP Registrar operates in two modes, owner and Proxy.

In the owner mode the Sonus SBC 1000/2000 is the owner of the Address Of Record (AOR) for each SIP device and is responsible for maintaining the bindings for each number, and the registrar responds to registration

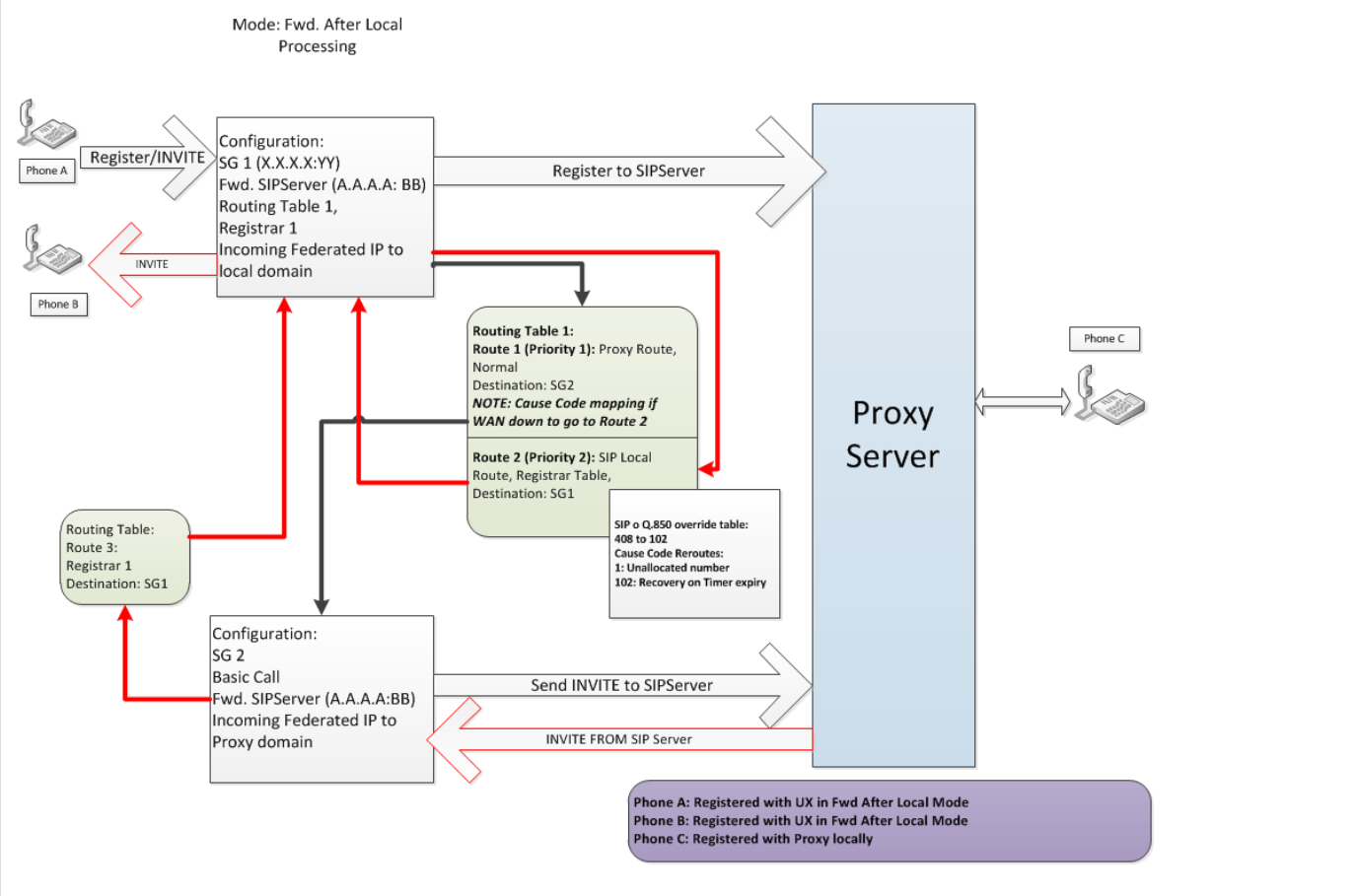
Copyright © 2015 Sonus Networks. All rights reserved.

messages with a time to live value configured in the UI.

In the proxy mode the AOR is owned by another network device and the Sonus SBC 1000/2000 Registrar obtains the AOR information as a proxy. Registration messages are sent to the Sonus SBC 1000/2000 which is responsible to forward the message to the AOR owner, bindings are maintained by the network device with the Sonus SBC 1000/2000 acting only as a relay point. In order to force the endpoint to register at regular and reasonable intervals when the network device becomes unavailable or has been restarted, the Sonus SBC 1000/2000 modifies the bindings and reduces the time-to-live values. The proxy mode allows the Sonus SBC 1000/2000 to obtain routing information while not requiring security credentials to be configured for each endpoint.If AOR is not a local domain the registration can be forwarded to Server Host. Contact information in responses will be retained in registrar.

The Sonus SBC 1000/2000 can be configured in in three SIP Modes: Basic Call, Forward Registration after Local Processing, and Local Registrar. Basic Call mode has no registrar functionality and therefore, registration functionality applies to only the last two modes.

The figure below illustrates how registration is processed in the *Forward After Local Processing* mode.



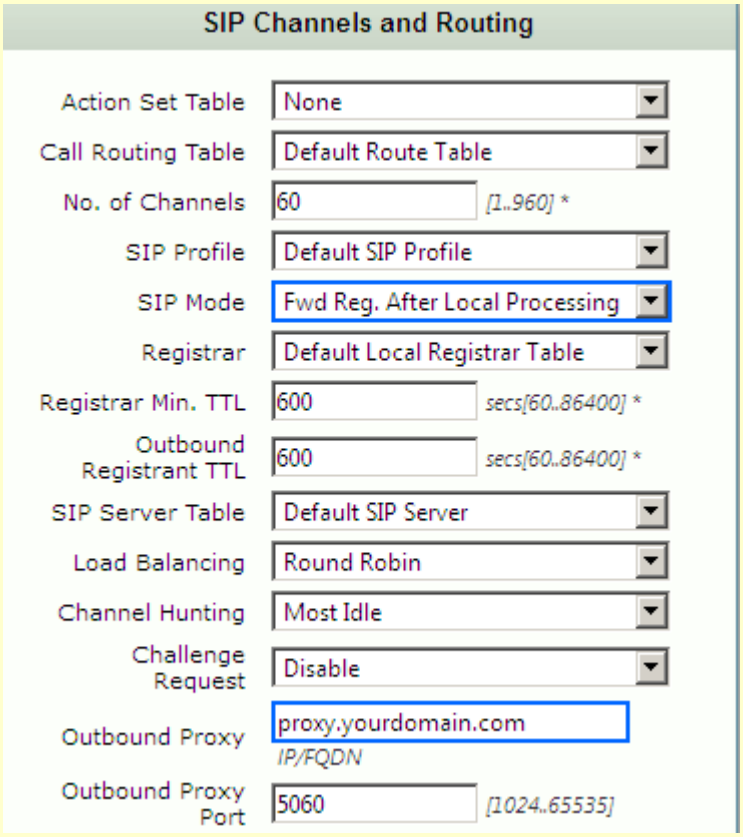
Forward After Registration Scenario

Under normal circumstances, when a device registers with the Sonus SBC 1000/2000 its information is captured in the local registrar and then forwarded to the SIP server for registration and the SIP server is responsible for all call bindings.

Copyright © 2015 Sonus Networks. All rights reserved.

IMPORTANT NOTE

If an ***Outbound Proxy*** is specified in the SIP Signaling Group, it takes precedence over the SIP Server. Therefore, proxy registration is moot.



SIP Server Fail-over Scenario

When Forward After Registration is the selected SIP mode and the SIP server becomes unavailable, the local registrar maintains the call bindings. However, for this to occur, Routing Tables and Cause Codes must be properly configured on the Sonus SBC 1000/2000.

Setting up the Routing Tables

In order for the fail-over scenario to function properly alternate call routes must be defined.

The primary call route entry of the Call Routing Table in the Signaling group must specify a Cause Code Reroute, defined under the Telephony Mapping Tables section of the UI.

The subsequent call route entry must specify the **Destination Type** as *Registrar Table*.

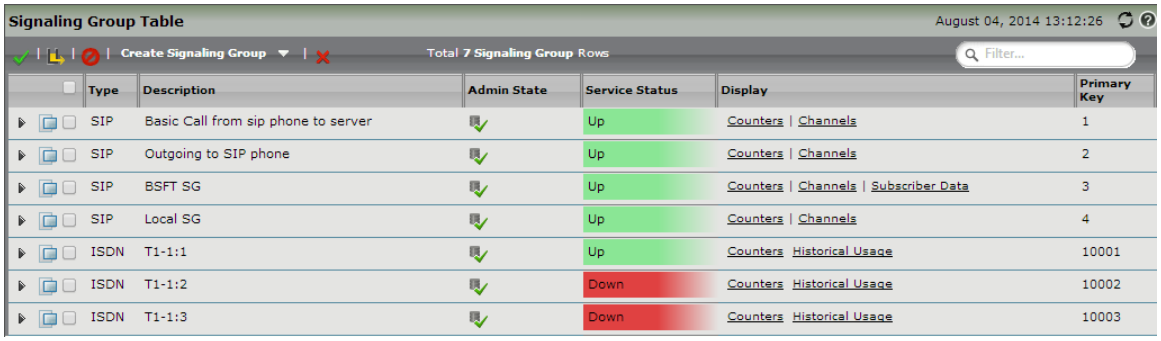
Creating and Modifying SIP Signaling Groups

To create or modify an existing SIP Signaling Group:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.

Copyright © 2015 Sonus Networks. All rights reserved.

3. From the **Create Signaling Group** drop down box, select **SIP Signaling Group.**



Modifying a SIP Signaling Group

1. Click the **expand** (▸) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a SIP Signaling Group

Prerequisites:

Before you can create a SIP Signaling Group, you must have defined at least the following configuration resource:

- Media List
- Tone Table
- Call Routing Table
- SIP Server Table (if you select Basic Call, Forward Registration, or Forward Registration after Local Processing for the SIP Mode)
- Local Registrar Table (if you select Forward Registration, Forward Registration after Local Processing, or Local Registrar for the SIP Mode)

To create a SIP Signaling Group:

1. From the **Create Signaling Group** drop down box at the top of the Signaling Group Table, select **SIP Signaling Group.**

Copyright © 2015 Sonus Networks. All rights reserved.



Description

Descriptive name for the signaling group.

Copyright © 2015 Sonus Networks. All rights reserved.

Admin State

Specifies the admin state of the Signaling group.

- **Enable:** Enables the signaling group.
- **Disable:** Disables the signaling group.
- **Drain:** When Drain is selected, calls that are currently up remain connected. However, new calls and forking are not allowed for the Signaling Group. This allows all the calls to be drained from the SG.

SIP Channels and Routing - Field Definitions

Action Set Table

Specifies a defined Action Set Table for this Signaling Group.

Call Routing Table

Specifies the Call Routing Table to be used by this Signaling Group.

Number of Channels

Specifies the number of SIP channels available for calls in this Signaling Group.

SIP Profile

Specifies the SIP Profile to use for this Signaling Group

SIP Mode

Specifies the SIP Registration Mode to use in this Signaling Group.

- **Basic Call:** Sends INVITEs to the selected server table.
- **Forward Reg. After Local Processing:** Forwards the REGISTER request after inserting it to the local registrar.
- **Local Registrar:** Maintains local registrar only. Uses registrar bindings to terminate a call.

> If **Fwd. Reg. After Local Processing** is configured as the SIP Mode**,** the selected SIP Server Table for that same Signaling Group should not be configured with a Contact Registrant Table. The SBC does not support **Fwd Reg. After Local Processing** and a Contact Registrant Table in the same Signaling Group.

See also: *Configuring the Sonus SBC 1000-2000 for Site Survivability*.

Agent Type

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the way in which SIP-SIP signaling will be handled by the SBC. Valid entries:

Back-to-Back User Agent. The SBC will maintain state and participate in all SIP signaling between both endpoints.

Access Mode: When AccessMode is enabled, the SBC allows certain SIP functions to be sent in a pass through mode:

- Non-call related methods (Register, Subscribe and Notify)
- Refer and Update
- Authentication handling

> **Access Mode SG Requirement**
>
> If Access Mode is specified, a source and destination signaling group must exist (e.g., Broadsoft Local Register SG to Broadworks Server SG).

Default selection: **Back-to-Back User Agent.**

Interop Mode

Indicates if the SBC should interoperate in a proprietary manner for certain functionality .This field is available only when **Agent Type** is set to **Access Mode**. Valid entries:

Standard: SBC will interoperate according to RFC standards.

BroadSoft Extension: SBC will support BroadSoft related extensions. Specifically, the SBC will use BroadSoft's subscriber data (BroadWorksSubscriberData) while in remote survivability mode. This feature allows the SBC to retrieve and store alternative user information for use when the BroadSoft server is unreachable.

Default entry: **Standard**.

Registrant TTL

Specifies the Time-To-Live (TTL) value for inbound registration. Inbound registration values should be equal to or greater than this. Valid entry: Enter value in seconds. Default value: **3600**.

Registrar

Specifies the Registrar Table attached to the Signaling Group for routing purpose and adding registration records.

Registrar Min. TTL

Specifies the Time-To-Live (TTL) value for inbound registrations. Inbound registration values should be equal to or greater than this. This is configured in all registration scenarios.

Outbound Registrar TTL

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the Time-To-Live (TTL) value for outbound registrations. This is configured only in the Forward modes of operation only.

SIP Server Table

Specifies the SIP Server Table to be used in the Signaling Group. The options in this field are derived from the configuration of SIP Server tables, see Creating and Modifying Entries in SIP Server Tables.

If a SIP Server Table is added which includes a server that has Stagger Registration enabled, Stagger Registration occurs. Also, if a SIP server table is removed which included a server that had Stagger Registration enabled, Stagger Un-registration occurs. For more information about Stagger Registration, see Creating and Modifying Entries in SIP Server Tables .

If you select an entry in the SIP Server table that is defined as DNS SRV, the Load Balancing field is not visible. See Load Balancing.

Load Balancing

This field applies only when the SIP Server Table selected from the drop down list is IP/FQDN based and does not contain SRV servers (load balancing is not required if the SIP Server Table which contains a SRV server). See SIP Server Table.

Specifies the load balancing method used with this Signaling Group. Used only in the SIP Basic Call Mode.

- **Round Robin:** Each initial INVITE sent to the next server in the pool. As the basic algorithm, the scheduler selects a resource pointed to by a counter from a list, after which the counter is incremented and if the end is reached, returned to the beginning of the list. Round-robin selection has a positive characteristic of preventing starvation, as every resource will be eventually chosen by the scheduler.
- **Priority:** The request goes to the server with highest priority.
- **First:** The initial request goes to the first available server.

Channel Hunting

Specifies the method that Call Control uses to allocate SIP channels.

- **Standard:** Specifies the first available low numbered channel.
- **Reverse Standard:** Specifies last available high numbered channel.
- **Round Robin:** Specifies channels based on next available from low numbered to high numbered.
- **Least Idle:** Specifies that channels are chosen based on the least idle channel.
- **Most Idle:** Specifies that channels are chosen based on the most idle channel.

Notify Lync CAC Profile

Enables whether any CAC Profile updates received locally are transmitted to the SIP servers listed in this Signaling Group Configuration. Valid entry: **Enable** (Default, updates received locally are transmitted to SIP servers), or **Disable** (updates received locally are not transmitted to SIP servers) .

Challenge Request

Copyright © 2015 Sonus Networks. All rights reserved.

Indicates whether or not incoming request messages are challenged for security purposes. If this option is set to **Enable**, you must specify a realm and at least one entry in the **Authorization Table**.

- **True:** All requests are challenged for realm, user, and password.
- **False:** No request messages are challenged.

Outbound Proxy

Specifies the outbound proxy through which all SIP messages are sent. For in-depth configuration detail, see Outbound Proxy Configuration.

Outbound Proxy Port

Specifies the port number for the outbound proxy, if one is configured. The port number must be in the range 1024 through 65535.

No Channel Available Override

In the event of a *No Channel/Circuit available* release cause code, the specified cause code is sent to the relevant protocol module. For more information see the list of Cause Codes.

Call Setup Response Timer

Specifies the interval of time, in seconds, after a call is initiated that the Sonus SBC 1000/2000 waits for a call to connect before terminating the incoming call.

QoE Reporting

Enables the QoE (Quality of Experience) reporting feature in the SBC. Valid options: **Enabled** (enables the feature) or **Disabled** (disables the feature). This field must be enabled for the QoE options to be available through the QoE Settings. See Configuring Quality of Experience (QoE) Settings

Media Information - Field Definitions

Audio/Fax Stream Proxy Mode

Enables whether the Signaling Groups supports Proxy mode. In Audio/Fax Stream Proxy mode, the SBC will proxy or switch the media stream between endpoints in order to negotiate common media capabilities and handle unsupported/unknown audio codecs. The media flows through the SBC without requiring DSP resources. Valid entries: **Enabled** (enables proxy mode) or **Disabled** (disables proxy mode). Default entry: **Enabled**.

Audio/Fax Stream DSP Mode

Enables whether the Signaling Group supports DSP mode. In Audio/Fax Stream DSP mode, the SBC uses DSP resources for media handling, but it does not facilitate the capabilities/features between endpoints that are not supported within the SBC (codec/capability mismatch). Valid entries: **Enabled** (enables DSP mode) or **Disabled** (disables DSP mode). Default entry: **Enable**.

Video/Application Stream Proxy Mode

Copyright © 2015 Sonus Networks. All rights reserved.

Enables whether the Signaling Groups supports Proxy mode. In Video/Application Stream Proxy mode, the SBC will proxy or switch the media stream between endpoints in order to negotiate common media capabilities. The media flows through the SBC without requiring DSP resources. Valid entries: **Enabled** (enables proxy mode) or **Disabled** (disables proxy mode). Default entry: **Enabled**.

Media List ID

Specifies the Media List used by this Signaling Group.

Play Ring Back

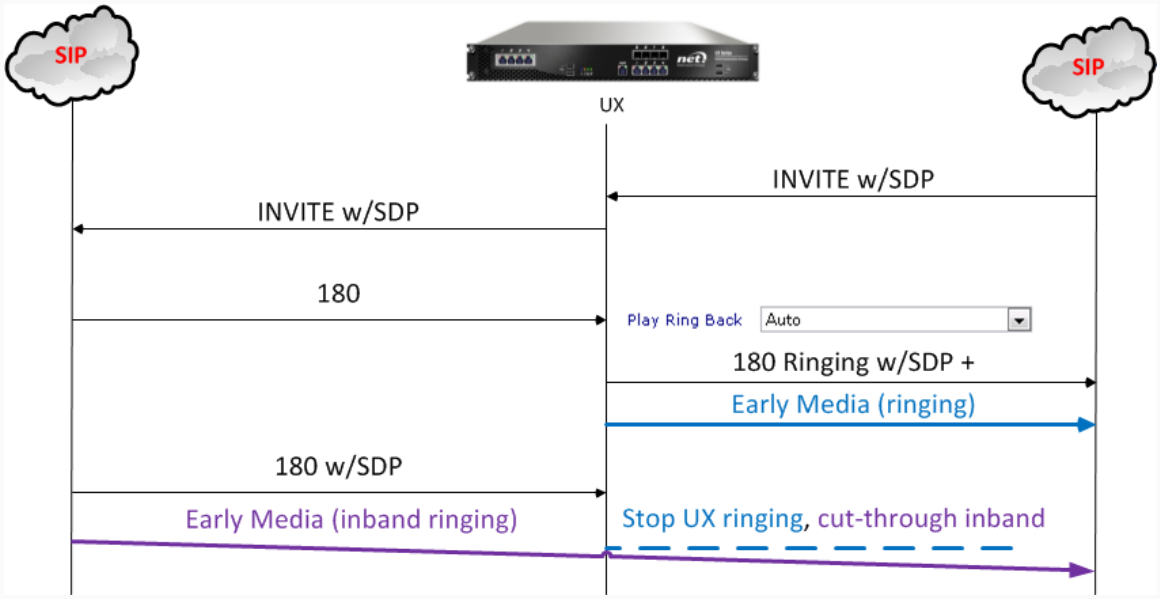
Specifies how ringback is played on a channel.

> The Play Ringback configuration functions with only 180 Ringing or ISDN Alert. The function is not executed for 183 w/SDP.

- **Auto:** Configured for Auto, the Sonus SBC 1000/2000 operates in the nominal *RFC 3960*pattern
  - Sonus SBC 1000/2000 generates ringback until in-band media arrives.
  - Sonus SBC 1000/2000-generated ringback is discontinued in the presence of in-band ringback.
  - Additionally, any ALERT is sent with PI=8 regardless of whether or not a SDP was received on the SIP side. Doing so allows the Sonus SBC 1000/2000 to send in-band audio without signaling PROGRESS.

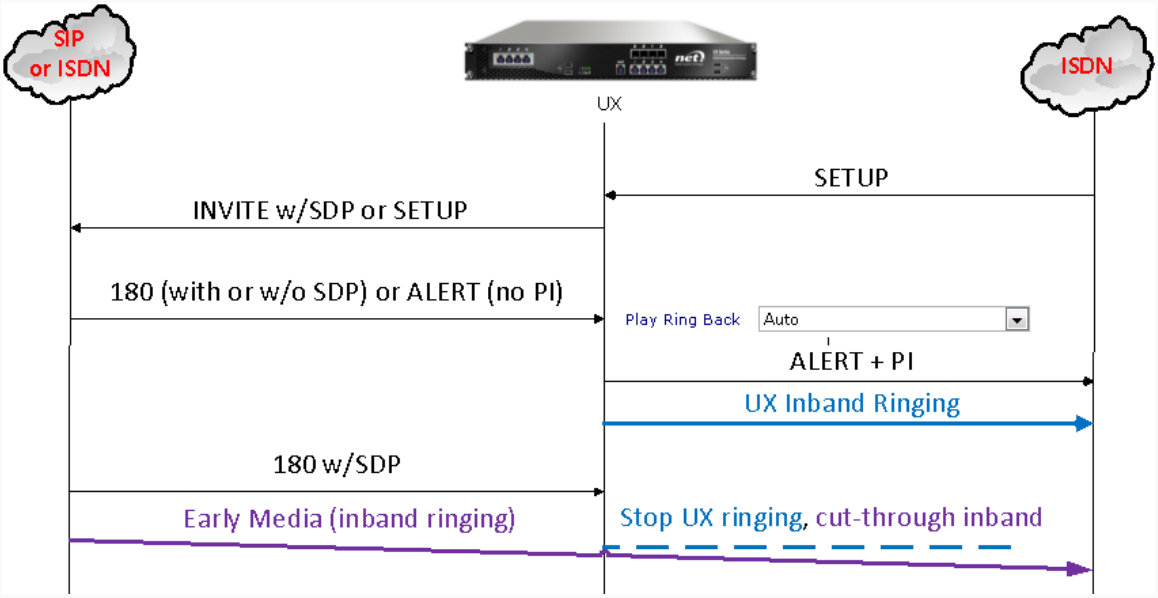
>> Click to see more information about this topic.

Auto — SIP SIP



Copyright © 2015 Sonus Networks. All rights reserved.

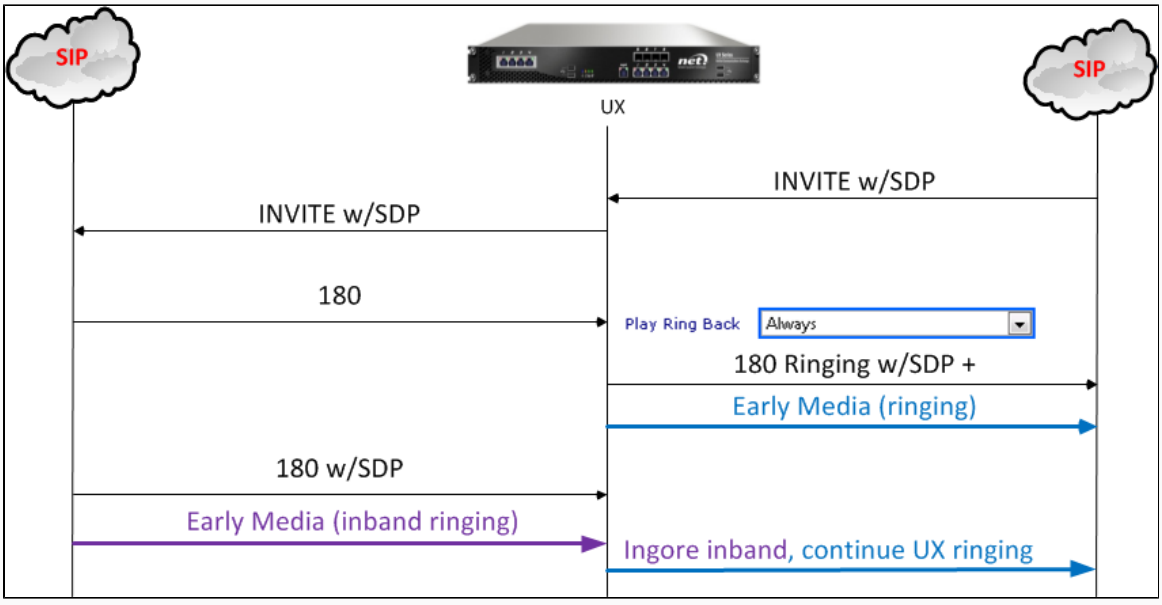
Auto — SIP/ISDN ISDN



- **Always:**Sonus SBC 1000/2000 provides ringback, ignoring any arriving in-band media.
  - For SIP-originated call legs, 180w/SDP will be sent to permit Sonus SBC 1000/2000 to provide in-band ringback via early media.
  - For ISDN-originated call legs, ALERT+PI will be sent along with Sonus SBC 1000/2000-inband ringing.

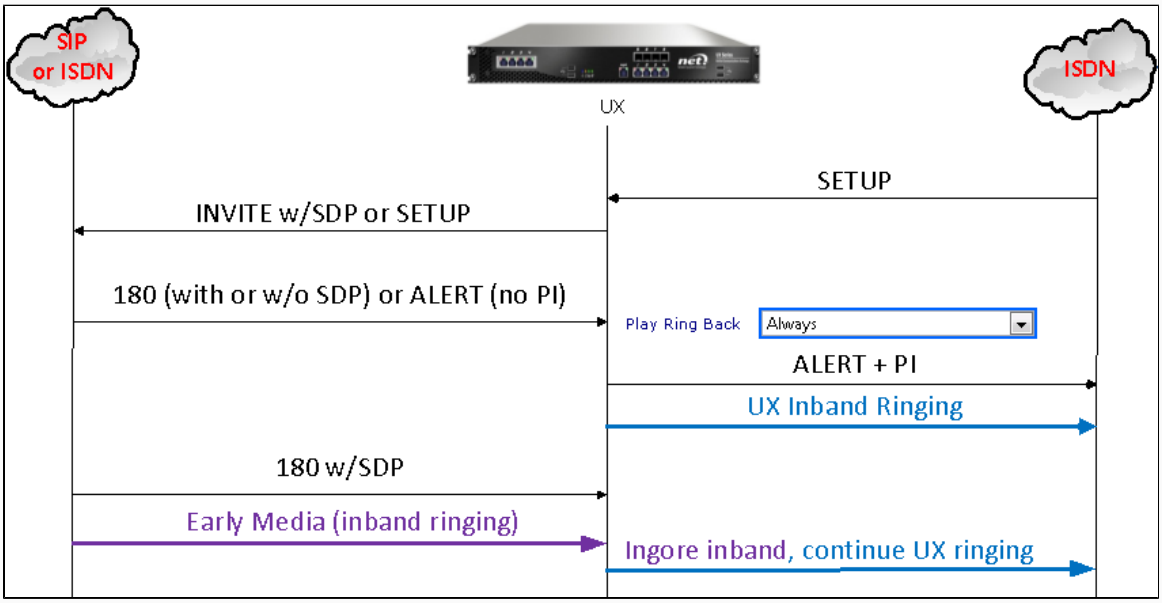
>> Click to see more information about this topic.

Always — SIP SIP



Copyright © 2015 Sonus Networks. All rights reserved.

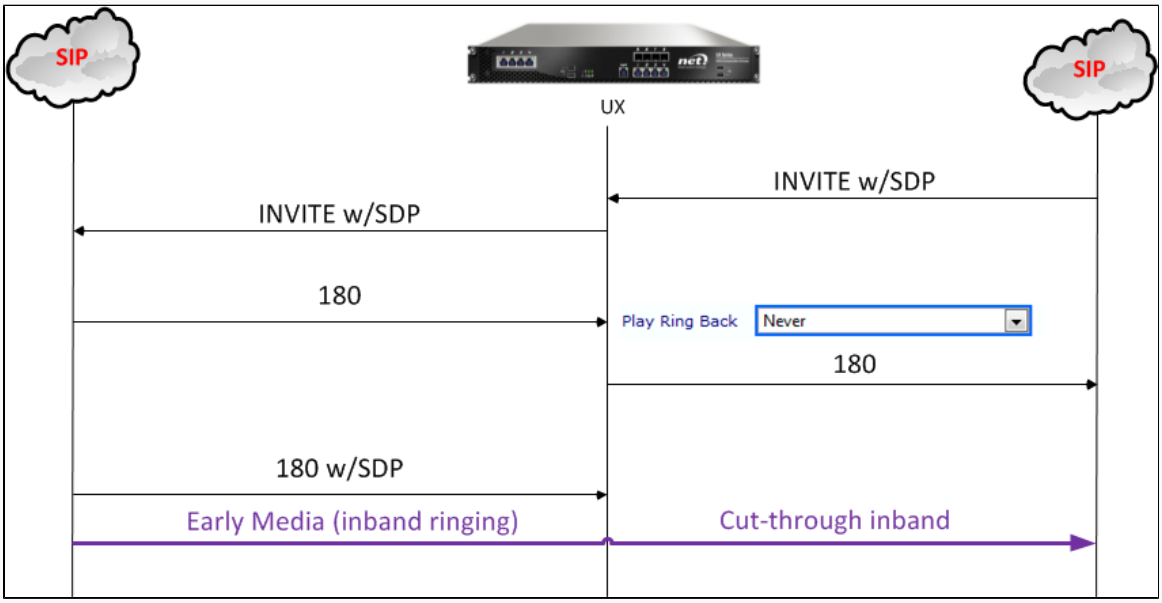
Always — SIP/ISDN ISDN



- **Never:**Sonus SBC 1000/2000 does not provide ringback and cuts through ringback from the source when/if it arrives.
    - With NEVER, Sonus SBC 1000/2000 will send 180/ALERT to the originating call leg without SDP/PI as in this configuration Sonus SBC 1000/2000 will not supply inband ringback.

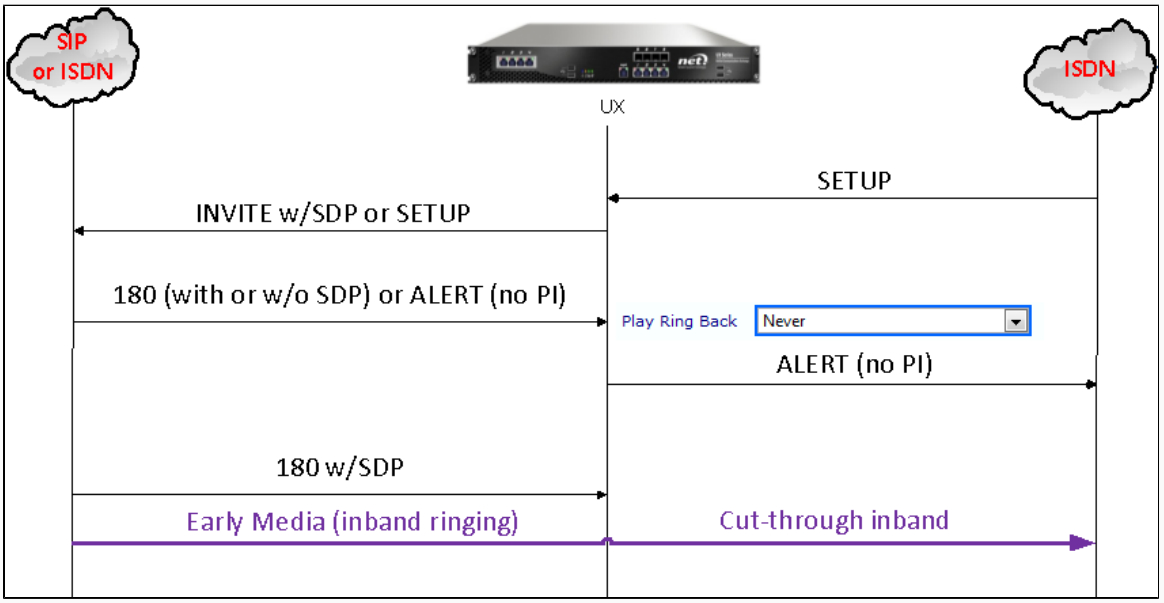
>> Click to see more information about this topic.

Never — SIP SIP



Copyright © 2015 Sonus Networks. All rights reserved.

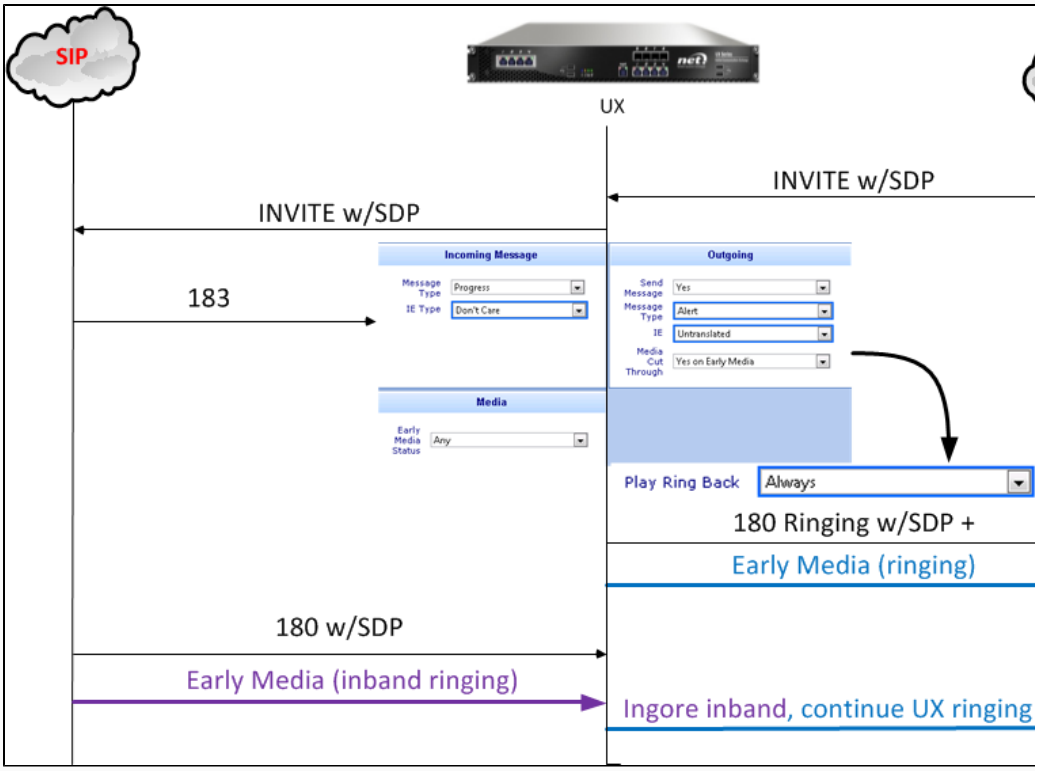
Never — SIP/ISDN ISDN



Note: The Play Ring Back setting is activated only after the channel receives an ALERT or 180 Ringing. Issues with ringback and 183 Session Progress must be addressed using a Message Translation.

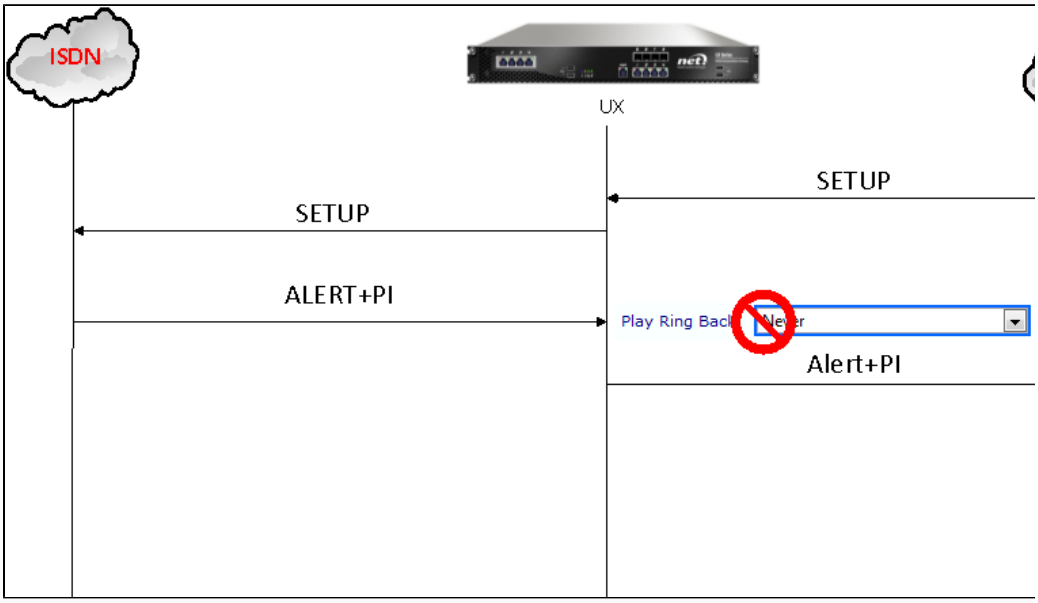
>> Click to see more information about Activating Play Ring Back.

The Ringback setting will be activated if a Message Translation's output is ALERT/180.



Copyright © 2015 Sonus Networks. All rights reserved.

The Ringback setting is not used for ISDN-to-ISDN calls when the ALERT contains a Progress Indicator. Sonus SBC 1000/2000 will always set the outgoing PI as it was received.



Tone Table

Specifies the Tone Table used by this Signaling Group. Only visible if Always or Auto is specified for Play Ring Back.

Early 183

Specifies whether to send a SIP 183 response immediately after receiving an Invite message. The early 183 Session Progress with SDP provides the SRTP key that will be used to decrypt the transmit stream from Sonus SBC 1000/2000 to the SIP peer. This setting is used to prevent the peer device (eg. Mediation server) from staying in the Trying state. This setting is required for Lync 2010 interoperability.

Early 183 is applicable only when Audio/Fax Stream DSP Mode is enabled as the media mode.

Music on Hold

The field enables Music on Hold at the SIP Signaling group level. Available options:

- **Enabled.** Enables Music on Hold for the SIP Signaling Group.
- **Disabled**. Disables Music on Hold for the SIP Signaling Group. Default entry.
- **Enables for 2-Way Hold Only**. The SBC will not play Music on Hold if the other side sends 1-way hold (a=sendonly), and the SBC will play Music On Hold if the other side sends 2-way hold (a-inactive). This is mainly used if the other system's Music on Hold is preferred.

For detailed information about enabling Music On Hold as part of the Media configuration, see Configuring the Media System. For detailed information about uploading music files, see Uploading Music on Hold Files.

Mapping Tables

Copyright © 2015 Sonus Networks. All rights reserved.

SIP To Q.850 Override Table

Specifies the SIP to Q.850 Override Table to be used for this Signaling Group.

Q.850 To SIP Override Table

Specifies the Q.850 To SIP Override Table to be used for this Signaling Group.

Pass-thru Peer SIP Response Code

The default value is Enabled. If you disable the pass-thru peer SIP response, then the mapping tables will be applied to SIP-SIP calls.

SIP IP Details - Field Definitions

NAT Traversal

Specifies whether or not the Signaling Group uses a third-party entity IP address inside SIP message to support network address translation (NAT). Only visible when NAT Traversal is set to Static NAT.

- **None:** Specifies that network address translation is not used.
- **Static NAT:** Specifies that network address translation is used.

> Symmetric NAT (port forwarding) is the only supported NAT type. This NAT configuration type means that packets received on a specific NAT server port are always forwarded to the same Sonus SBC 1000/2000 port, for example, packets on the NAT public IP, port 5060 are forwarded to a private (Sonus SBC 1000/2000) IP, port 5060.

Application Layer IP

Specifies how the Signaling Group will select the local IP.

- **Auto:** Means Sonus SBC 1000/2000 connects to the peer and queries the local IP which is used in SIP headers and SDP.
- **Bind:** Binds to specified interface and uses that IP (1st/2nd) in headers and SDP.

NAT Public IP Address

Specifies the public IP of the NAT server visible from Internet. The NAT server's ports must be configured to allow SIP and RTP traffic, for example: port range 5060-5061 for SIP and 16000-17000 for RTP.

> The IP address specified in this field must be publicly accessible.

Signaling/Media Source IP

Specifies the the logical port over which SIP session are conducted. Only visible when NAT Traversal is set to None

- **Auto:** The node automatically selects the port over which the session is conducted.
- **Ethernet IP :** Specifies the logical Ethernet port over which the session is conducted.

Signaling DSCP

Copyright © 2015 Sonus Networks. All rights reserved.

Each SIP-SG is configurable with the DSCP value to be used for signaling. This allows for improved quality of service in real time applications, such as conferencing and conversations.. The settings take effect for both client and server modes of SIP. The default value of 40 is the most common value used in the VOIP networks for signaling packets. The configured value should be chosen according to the QoS policies of the IP network in which the signaling packets travel.

Valid entry range: 0 to 63 (inclusive). Default value: 40.

Listen Ports - Field Definitions

This section defines a listening port and protocol for the SIP Signaling Group

Port

Specifies the port to listen for SIP messages.

Protocol

Specifies the protocol with which this port can receive SIP messages.

TLS Profile

If TLS is selected this specifies the TLS Profile this port will use for secure SIP messages.

Federated IP/FQDN - Field Definitions

The Federated IP/FQDN feature acts as an access control by defining from which server a SIP Signaling Group will accept messages.

IP Address/FQDN

Specifies the IP Address or Fully Qualified Domain Name of a server from which the Sonus SBC 1000/2000 will accept SIP messages.

> When an IP Address is specified the Netmask is mandatory.

> When an FQDN is specified all the all IPs in that domain are added. If the Netmask is not specified 255.255.255.255 is assumed.

Federated IP Netmask

Specifies the network address mask to apply against the specified server address.

Message Manipulation

This option enables or disables the ability for the Sonus SBC 1000/2000 to manipulate SIP messages using previously configured Message Tables.

Select from the drop down list: **Enable** (enables the feature) or **Disable** (disables the feature).

Inbound Message Manipulation - Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

The rules in these tables are used to manipulate inbound SIP messages in the Signaling Group. The Signaling Group will support a maximum of 10 Message Rule Tools allowed in the Signaling Group (inbound direction).

Up. Moves the message table entry up in the list.The rules are applied in the order the tables are listed.

Down. Moves the message table entry down in the list.The rules are applied in the order the tables are listed.

Add. Displays a drop down list of available message tables. Select an entry and click **Apply**.

Remove. Removes the message table entry from the list.



Outbound Message Manipulation - Field Definitions

The rules in these tables are used to manipulate inbound SIP messages in the Signaling Group. The Signaling Group will support a maximum of 10 Message Rule Tools allowed n the Signaling Group (outbound direction).

Up. Moves the message table entry up in the list. The rules are applied in the order the tables are listed.

Down. Moves the message table entry down in the list.The rules are applied in the order the tables are listed.

Add. Displays a drop down list of available Message Tables. Select an entry and click **Apply**.

Remove. Removes the message table entry from the list.



Outbound Proxy Configuration

This article describes the necessary steps to configure a SIP Outbound Proxy on the Sonus SBC 1000/2000 system.

- Overview
- Outbound Proxy Configuration or Basic Call mode

Copyright © 2015 Sonus Networks. All rights reserved.

- Usage Example

Overview

The Outbound Proxy feature sends all SIP outbound requests to an Outbound Proxy Server of choice regardless where the Request URI points to. Outbound Proxies are configured in the SIP Signaling Groups (SIP SG) and are valid for Signaling Groups who's SIP Mode is set to one of the following:

- Basic Call
- Forward Registration
- Forward Registration After Local Processing

In the **Basic Call** mode, the outbound INVITE request is constructed using the Server table as the destination. If an Outbound Proxy is configured, the outbound INVITE is sent to the outbound proxy instead of the available server from the Server table.

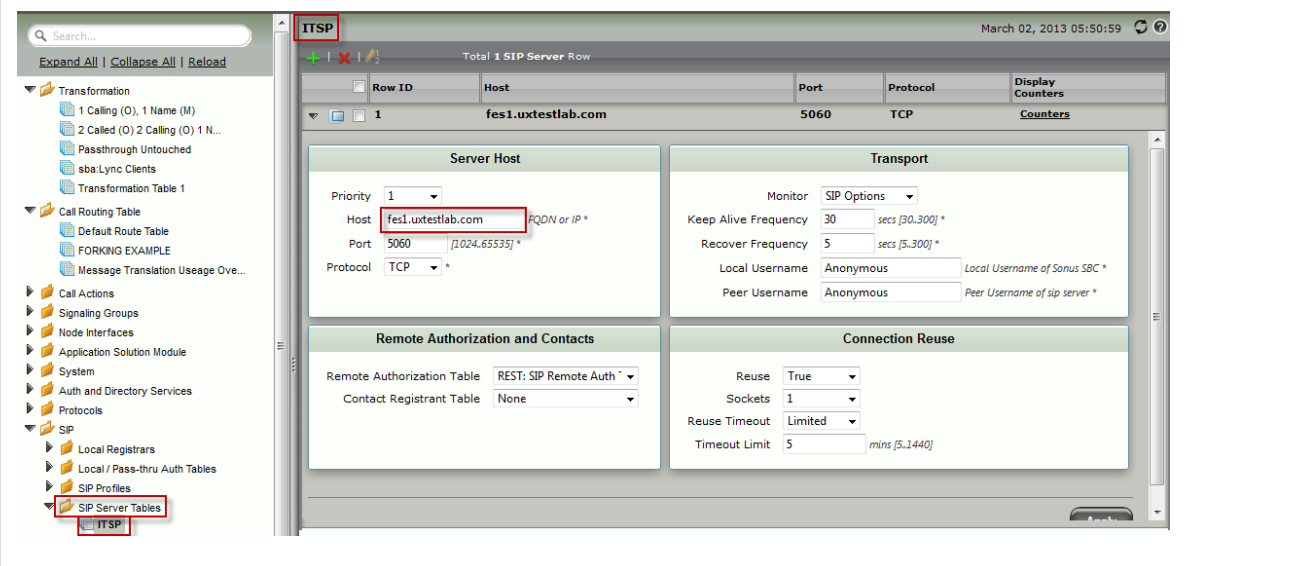
In both **Fwd Registration** and **Fwd Reg. After Local Processing** modes, the outbound REGISTER request is constructed using the Registrar address as the destination. If Outbound Proxy is configured, the outbound REGISTER is sent to the outbound proxy instead of the Registrar address.

Important Notes

- In **Local Registrar** mode, the Outbound Proxy configuration item is disabled and its value is not used.
- If a SIP Server table which has **Monitoring** enabled, is associated with a SG having an Outbound Proxy configured, all the SIP OPTIONS requests generated by the Sonus SBC 1000/2000 for monitoring purposes, are sent to the Outbound Proxy address configured on the SG.

Outbound Proxy Configuration or Basic Call mode

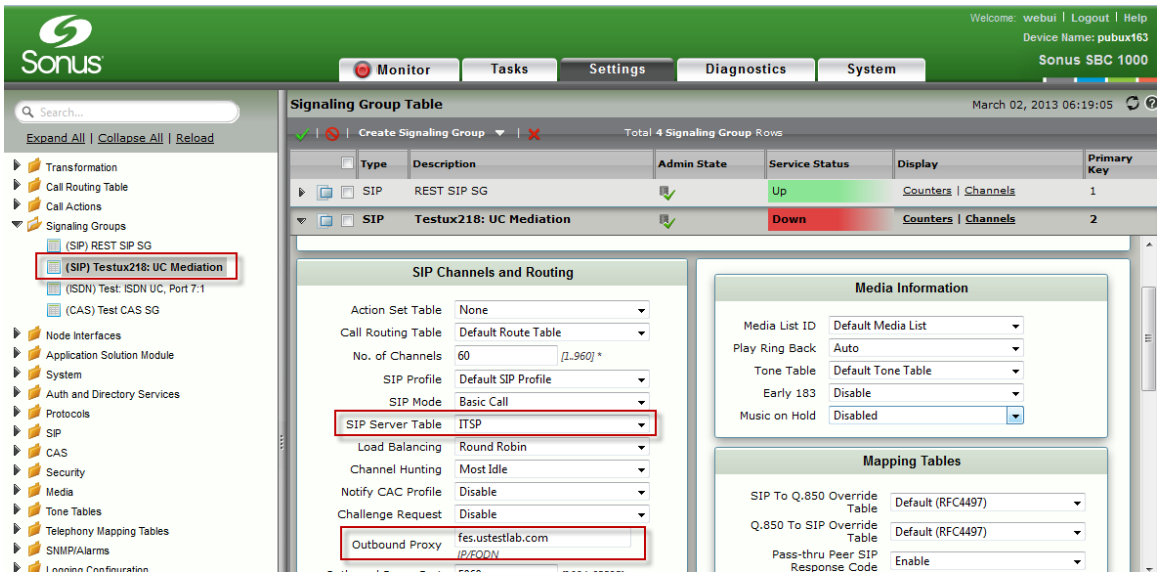
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP Server Tables**
3. Create a SIP Server Table (i.e., fe2.uxtestlab.com with the relevant port, protocol, profile, etc.)



4. In the left navigation pane, go to **Signaling Groups > (the SIP Signaling Group you plan to use for your deployment)**.
5. Configure the SIP Signaling Groupto use an Outbound Proxy.

Copyright © 2015 Sonus Networks. All rights reserved.

a. Select the SIP Server table you created above from the **SIP Server Table** list box.
b. Enter the IP Address of FQDN of the Proxy Server in the **Outbound Proxy** text box.
c. Enter the relevant port number in the **Outbound Proxy Port**text box.



Usage Example

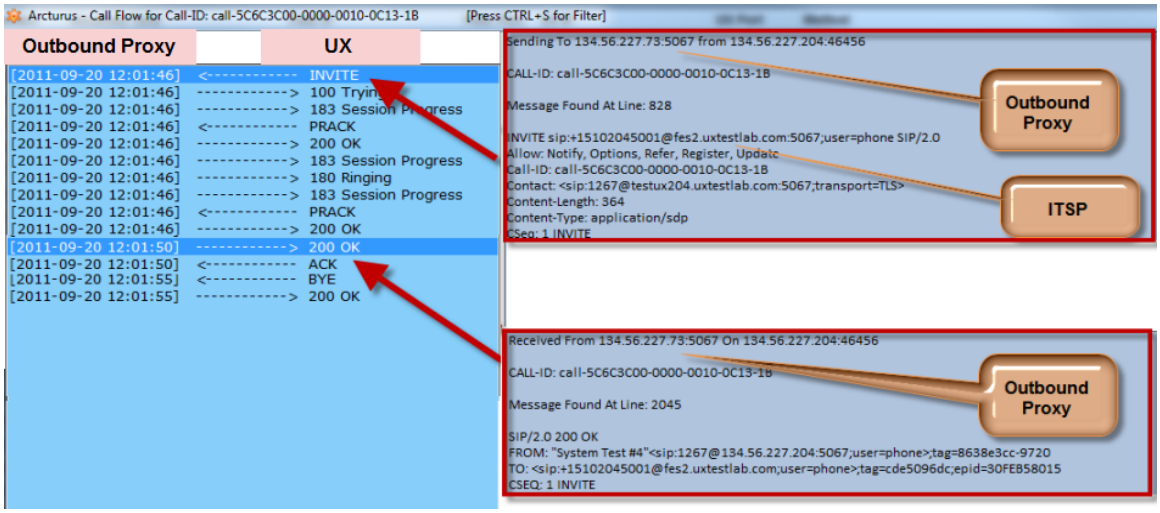
Once an Outbound Proxy is configured on a SIP Signaling group, all SIP calls landing on that SIP SG are routed through a Proxy to the actual end points. This is typical in a SIP Trunking scenarios whereby the Sonus SBC 1000/2000 offloads all the enterprise SIP traffic onto an ITSP (Internet Telephony Service Provider) SIP network which exposes a Proxy configured as an Outbound Proxy on the Sonus SBC 1000/2000.

In this example, entities are configured with following:

Sonus SBC 1000/2000	ITSP	Outbound Proxy
134.56.227.204	134.56.227.73	134.56.227.73
testux204.uxtestlab.com	fes1.uxtestlab.com	fes1.uxtestlab.com

Using the **Log Exchange** utility, you can verify the Outbound Proxy configuration in action —

Copyright © 2015 Sonus Networks. All rights reserved.



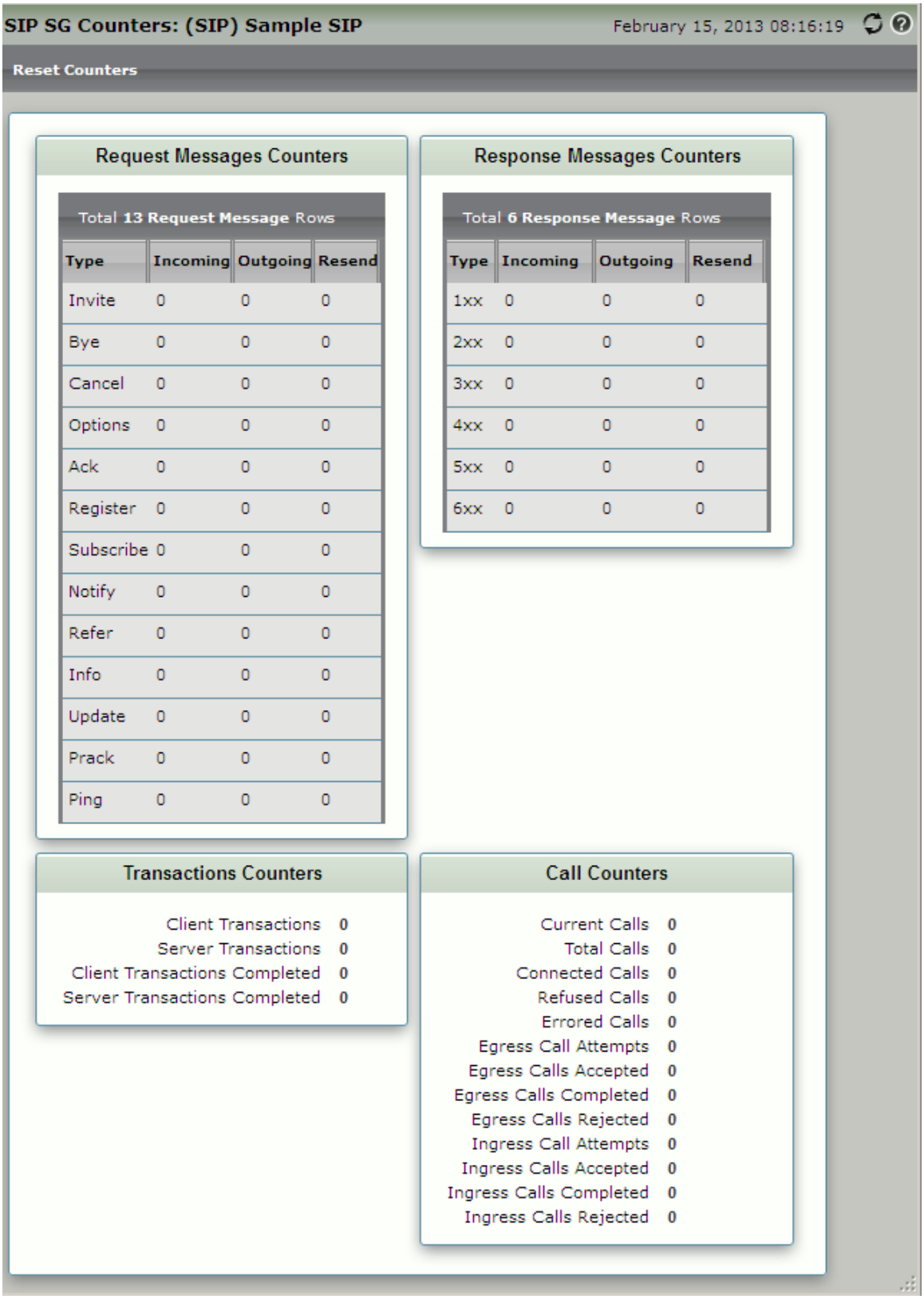
Viewing SIP Counters and Channels

The SIP SG Counters reflect the SIP messages sent/received at the Signalling group level. They are modeled based on the SIP RFC 3261. The request messages and its responses are incremented on send/receive directions. These counters are used mainly to troubleshoot issues and isolate failures.

- SIP Counters
  - Request Message Counters
  - Response Message Counters
  - Transaction Counters
  - Call Counters
- Channel Detail Information Pages
  - Channel Table Page
  - Detailed Call Information
  - Outbound Channel Details

SIP Counters

Copyright © 2015 Sonus Networks. All rights reserved.



Request Message Counters

SIP requests or methods are considered "verbs" in the protocol, since they request a specific action to be taken by another user agent or server. The INVITE, REGISTER, BYE, ACK, CANCEL, and OPTIONS methods are the original six methods in SIP. The REFER, SUBSCRIBE, NOTIFY, MESSAGE, UPDATE, INFO, and PRACK methods

Copyright © 2015 Sonus Networks. All rights reserved.

are described in separate RFCs. The call-flow counters in general give a broader view of the system to help identify high-level trends or see a systematic problem.

Response Message Counters

There are six classes of SIP responses. The first five classes were borrowed from HTTP, the sixth was created for SIP.

- **1xx:** Informational, Indicates status of call prior to completion. If first informational or provisional response.
- **2xx:** Success, Request has succeeded. If for an INVITE, ACK should be sent; otherwise, stop retransmissions of request.
- **3xx:** Redirection, Server has returned possible locations. The client should retry request at another server.
- **4xx:** Client error, The request has failed due to an error by the client. The client may retry the request if reformulated according to response.
- **5xx:** Server failure, The request has failed due to an error by the server. The request may be retried at another server.
- **6xx:** Global failure, The request has failed. The request should not be tried again at this or other servers.

For more information see RFC 3261.

A SIP response is a message generated by a UAS or a SIP server to reply to a request generated by a UAC. A response may contain additional header fields containing information needed by the UAC. Or, it may be a simple acknowledgment to prevent retransmissions of the request by the UAC. Many responses direct the UAC to take specific additional steps.

Responses counters can be helpful as a tool for developers and service engineers to identify high-level service affecting trends. It gives a broader view of the system in terms of call-flow specifics.

Transaction Counters

SIP transactions occur between a UAC and a UAS. A SIP transaction comprises all messages from the first request sent from the UAC to the UAS up to a final response (non-1xx) sent from the UAS to the UAC.

Transaction counters can be helpful as a tool for developers and service engineers to identify high-level service affecting trends. It gives a broader view of the system in terms of call-flow specifics.

Call Counters

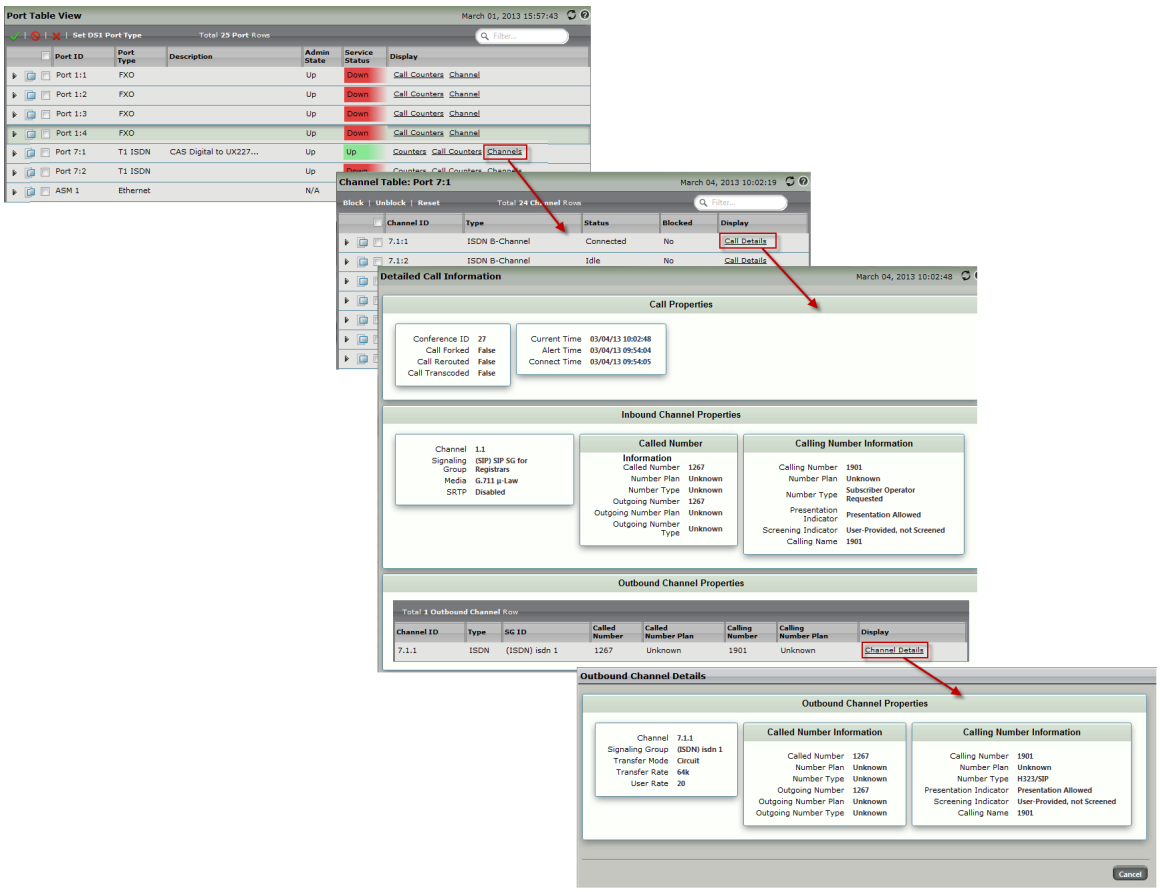
- **Current Calls:** Number of con-concurrent calls, both Inbound and Outbound, incremented on the start of Client/Server CallSession transactions.
- **Total Calls:** Total Number of completed and attempted calls. Incremented on the start of Client/Server CallSession transaction.;
- **Connected Calls:** Number of Accepted calls, usually incremented by receiving 200OK Response message.
- **Refused Calls:** Number of calls that were not accepted by Sonus SBC 1000/2000, incremented on receiving Response codes greater than 400 and CCNak.
- **Errored Calls**: Number of calls that resulted in an error, incremented on unexpected conditions that result in the call state to change to CallStateTerminated.
- **Blocked Calls:** This has not been defined yet.
- **Egress Call Attempts:** Number of outbound call attempts, incremented on start of Client transaction by UAC on Sonus SBC 1000/2000.
- **Egress Calls Accepted:** Number of outbound calls accepted, incremented on 200OK from UAS.
- **Egress Calls Completed:** Number of outbound calls completed, incremented on transaction state change to completed.
- **Egress Calls Rejected:** Number of outbound calls that were not accepted by Sonus SBC 1000/2000, incremented on receiving Response codes greater than 400 and CCNak.

Copyright © 2015 Sonus Networks. All rights reserved.

- **Ingress Call Attempts:** Number of inbound calls accepted, incremented on start of Server transaction by UAS on Sonus SBC 1000/2000.
- **Ingress Calls Accepted:** Number of inbound calls accepted, incremented on 200OK from UAC.
- **Ingress Calls Completed:** Number of inbound calls completed, incremented on transaction state change to completed.
- **IngressCalls Rejected:** Number of inbound calls that were not accepted by Sonus SBC 1000/2000, incremented on receiving Response codes greater than 400 and CCNak.

Channel Detail Information Pages

The Sonus SBC 1000/2000 provides a fine level of granularity of port/channel information, with nested dialogs.



Channel Table Page

The Channel Table allows you to see details about a call in progress on a selected channel.

To view the Channel Table:

- Click the **Channels** text in the row corresponding to the port who's Channel Table you want to view.

Copyright © 2015 Sonus Networks. All rights reserved.



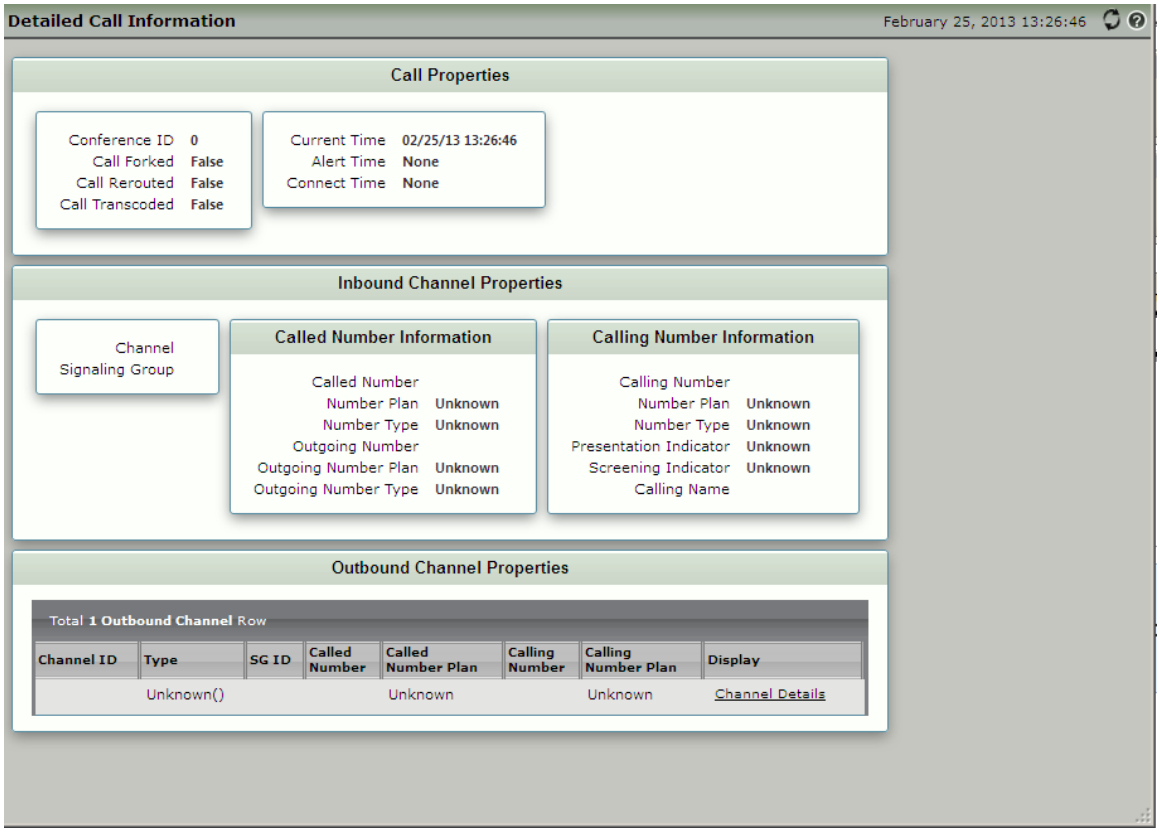
Detailed Call Information

This page provides you with a detailed list of information about a call which is currently up on the channel selected in the Channel Table.

To view the details of an active call in the Channel Table:

- Click the **Call Details** text in the row corresponding to the channel in the Channel Table panel.

Copyright © 2015 Sonus Networks. All rights reserved.

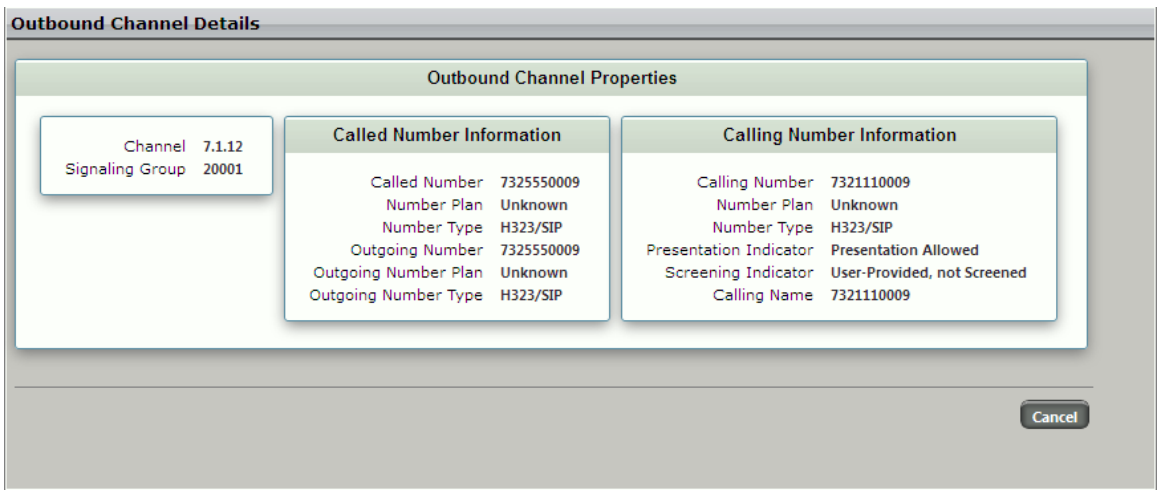


Outbound Channel Details

This page provides you with the finest granularity of detail, with information about the current call on the outbound channel.

To view information about a call on an outbound channel

- Click the **Channel Details** text in the Outbound Channel Properties pane of the Detailed Call Information panel:*



Copyright © 2015 Sonus Networks. All rights reserved.

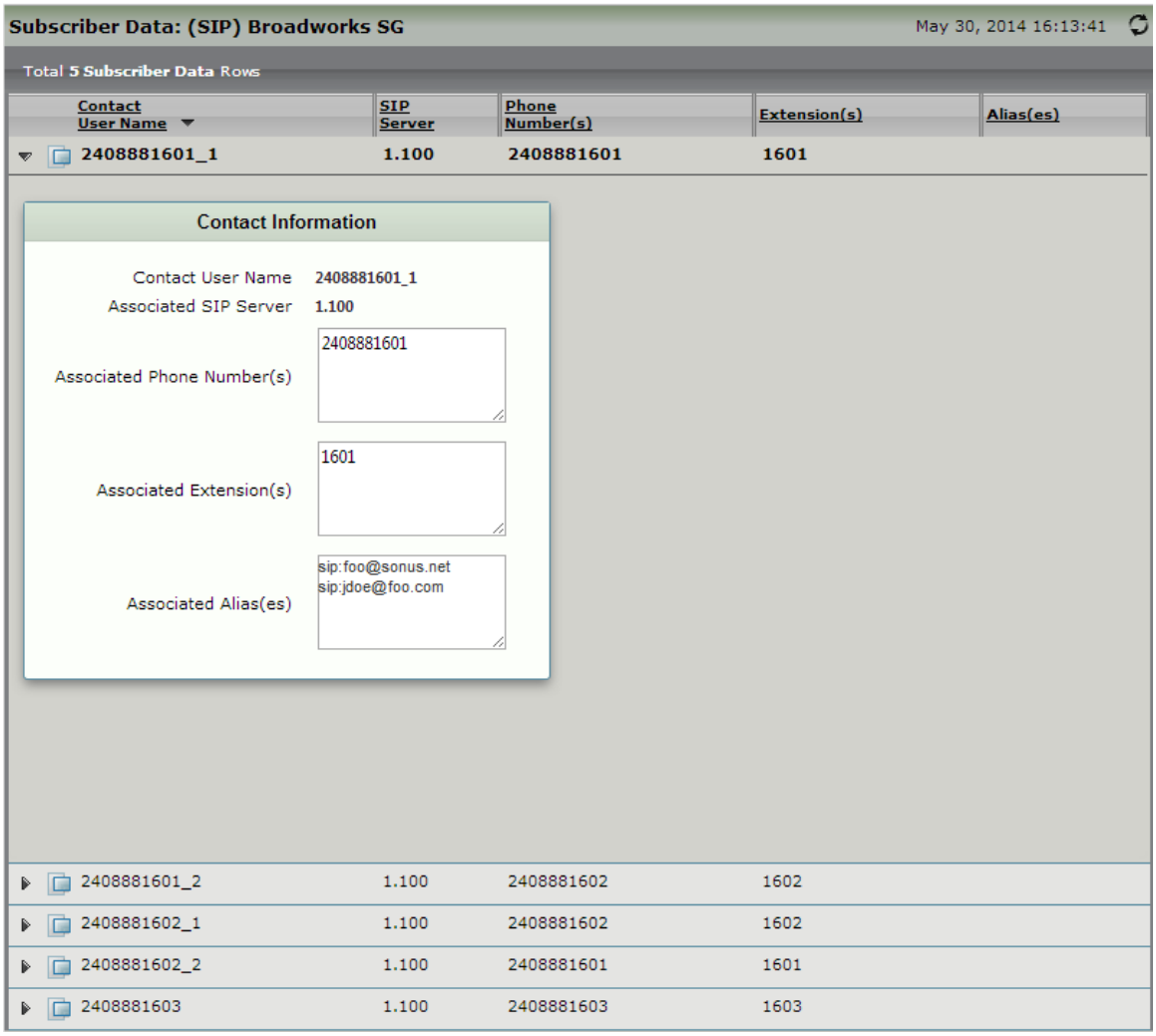
Viewing Subscriber Data

The Subscriber Data Table contains basic contact information for each subscriber that registers on the Broadsoft server via the SBC.

Viewing the Subscriber Data

To view subscriber data:

1. Click the **Settings** tab at the to of the User Interface.
2. In the left navigation pane, go to **Signaling Groups**.



3. In the **Signaling Group Table**, click the **Subscriber Data** link in the Signaling Group of interest.

Copyright © 2015 Sonus Networks. All rights reserved.

4. Click the **expand** ( ) Icon next to the entry you wish to expand for more information.

Contact Information - Field Definitions

Contact User Name

The registered user's contact name.

Associated SIP Server

The SIP Server associated with this contact. This is a reference to the internal SIP Server Table in the SBC 1000-2000 configuration.

Associated Phone Number(s)

A list of phone numbers associated with this contact. The phone number(s) appear in the national format associated with the user's location. Up to 10 additional numbers may be listed.

Associated Extension(s)

A list of extensions associated with this contact. Up to 10 additional extensions may be listed.

Associated Alias(es)

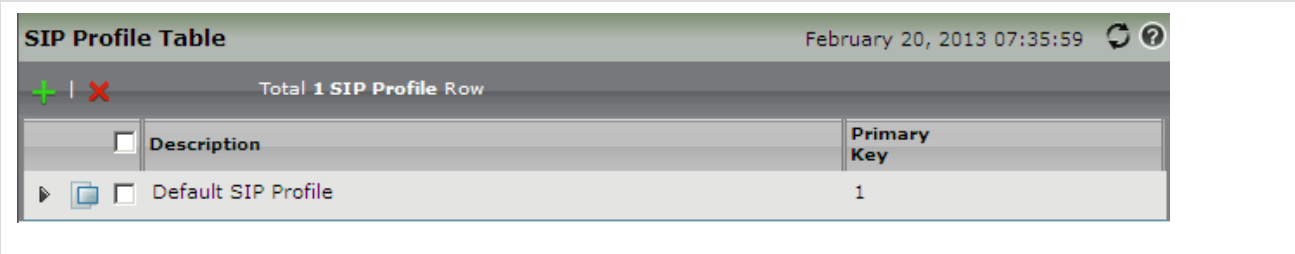
A list of aliases associated with this contact. These are SIP URIs associated with the user.

Managing SIP Profiles

SIP Profiles control the how the Sonus SBC 1000/2000 communicates with SIP devices. They control important characteristics such as: session timers, SIP header customization, SIP timers, MIME payloads, and option tags.

Working with SIP Profiles

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Profiles**.



To view a SIP Profile's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying SIP Profiles

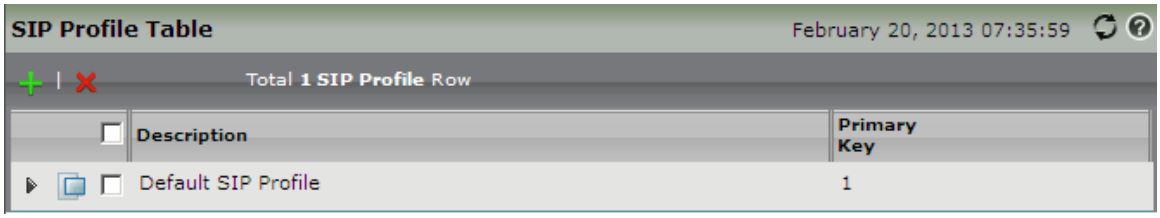
SIP Session Timer Configuration

Copyright © 2015 Sonus Networks. All rights reserved.

Creating and Modifying SIP Profiles

To create or modify an existing SIP Profile:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Profiles**.



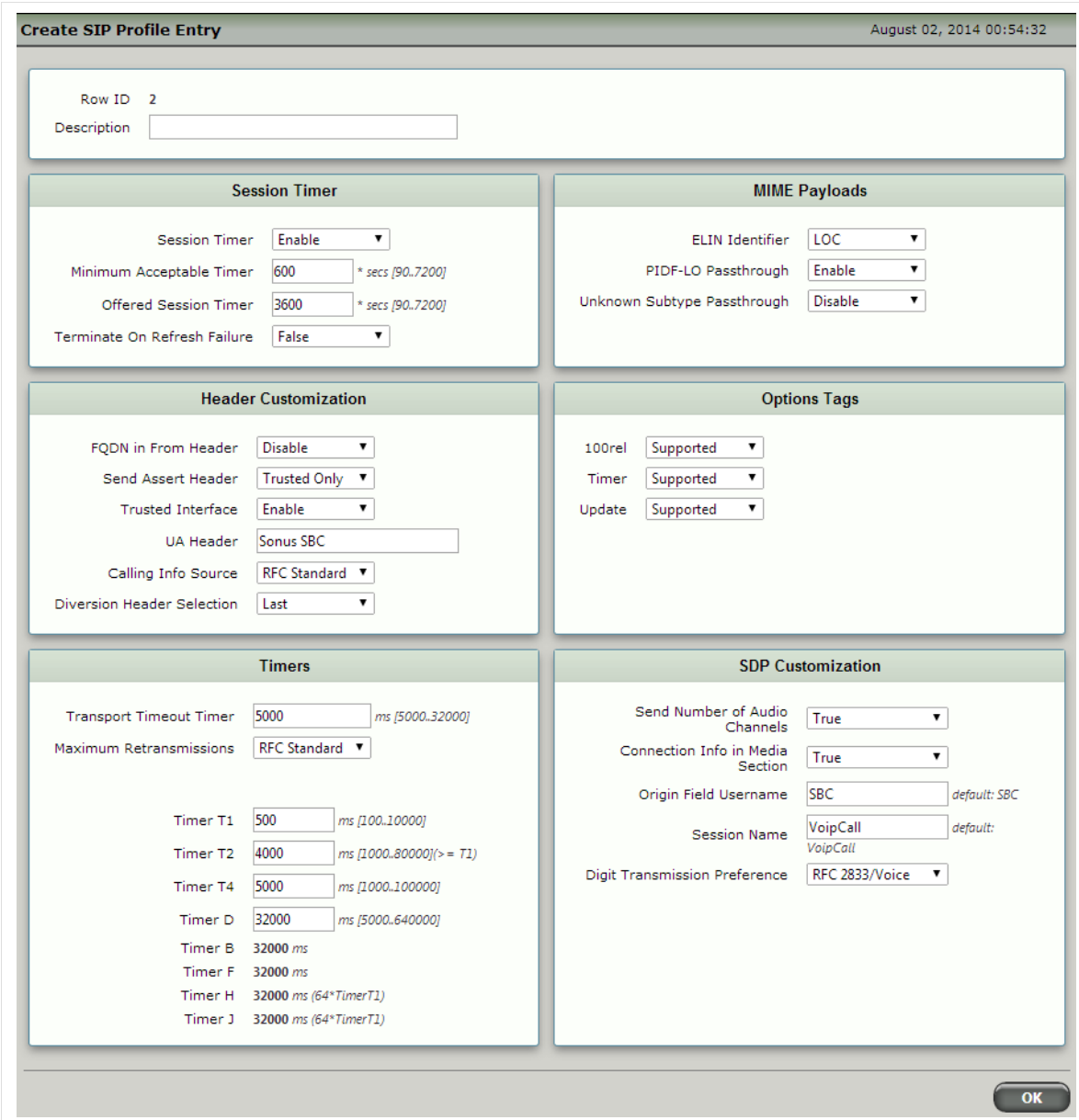
Modifying a SIP Profile

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a SIP Profile

1. Click the Create SIP Profile ( ) icon at the top of the SIP Profile View page.

Copyright © 2015 Sonus Networks. All rights reserved.



Session Timer - Field Definitions

The options in the Session Timer panel control the timers used to verify that the current SIP session is still valid.

Session Timer

Specifies whether or not to use the session timer to verify the SIP session. The remainder of the options in this panel are only visible of the Session Timer is **Enabled**.

Minimum Acceptable Timer

Specifies the minimum value to use for incoming session refresh in seconds. If the Sonus SBC 1000/2000 negotiates a session refresh this value will be used to indicate the minimum value acceptable for a session refresh.

Copyright © 2015 Sonus Networks. All rights reserved.

Offered Session Timer

Specifies an interval, proposed to a SIP peer, to use for a session refresh. At each interval, a session refresh occurs, if the remote does not respond the call is disconnected.

Terminate on Refresh Failure

Controls how the SBC responds if the session refresher fails. Valid entry: **True** (SBC ends the session by sending a BYE if refresher fails) or **False** (SBC sends a refresh, reinvite or update, if refresher fails). This field is available only when **Session Time** is enabled.

Header Customization - Field Definitions

The options in the Header Customization panel determine how certain headers in the SIP protocol are handled, what content from certain headers is used, and more.

UA (User Agent) Header

Specifies the contents of the SIP User-Agent header.

FQDN in From Header

Specifies which, if any, Fully Qualified Domain Name (FQDN) is used in the From header.

- **Disable:** Sonus SBC 1000/2000 IP address is used in the From Header.
- **Sonus SBC FQDN:** Sonus SBC 1000/2000 FQDN is used in the From Header.
- **Server FQDN:** Next hop SIP Server (IP address or FQDN depending of SIP server table entry) is used in the From Header.
- **Static**: Host portion (FQDN or IP) to be used in the From Header. If Static is selected, you must configure the host portion through the **Static Host** field.

> ⚠ FQDN in From Header will not function if the *Host Name* and/or *Domain Name* is not configured in *System* | *Node-Level Settings.*

Static Host

Specifies the host portion to be used in the From Header. This field is displayed only when the **FQDN in From Header** field is set as **Static**. Valid entry: **FQDN** or **IP[:port]**.

Send Assert Header

When enabled (set as **Always**), the Sonus SBC 1000/2000 always sends a P-Asserted-Identity header in the outbound INVITE message. When the Sonus SBC 1000/2000 receives an inbound INVITE message with a P-Preferred-Identity or P-Asserted-Identity header, the information from that header is used in the outbound P-Asserted-Identity header. However, when the Sonus SBC 1000/2000 receives a Privacy header, the identity is revealed in the outbound INVITE based on privacy header value.

When disabled, privacy information in the outbound INVITE is sent depending on the configuration of the Trusted Interface and the Privacy Pass-through Header.

Trusted Interface

Copyright © 2015 Sonus Networks. All rights reserved.

When enabled, the Sonus SBC 1000/2000 passes the Display Name (Calling Name), P-Asserted-Identity and Privacy header information from the inbound INVITE to the outbound INVITE message. The User-Agent header is also present.

When disabled, the Display Name (Calling Name), PAI/PPI and Privacy headers are not passed, and the User-Agent header is suppressed.

Calling Info Source

Enables SIP to use Calling Number and Name from FROM header always. By default, if P-Asserted-ID/P-Preferred-ID are present, Calling Number and Name are derived from P-Asserted-ID/P-Preferred-ID headers. Valid entry: **From RFC Standard** (default) or **"From" Header only.**

Diversion Header Selection

Determines which SIP Header to use in SIP call. Valid entry: **First** or **Last** (default).

Timers - Field Definitions

The options in this panel determine the duration of timers that control the behavior or SIP transmissions.

Transport Timeout Timer

Specifies the interval, in milliseconds, for which new TCP/TLS connections over SIP can be tried when no response is received from far end.

Maximum Retransmissions

Specifies the maximum number of retransmissions of client transaction messages over UDP. The default value disables this feature and maximum retransmissions are then controlled by Timer B and Timer F values. Any non-zero value modifies Timer B and Timer F and retransmissions are controlled by the selected value.

Timers

Copyright © 2015 Sonus Networks. All rights reserved.

Enter an integer value for each of the timers, if other than standard defaults are required.

Timer	Default Value	Meaning
T1	500 ms	Round-trip time (RTT) estimate
T2	4000 ms	Maximum retransmission interval for non-INVITE requests and INVITE responses
T4	5000 ms	Maximum duration that a message can remain in the network
C	180000 ms	Maximum duration to wait for a final response to an INVITE request
D	32000 ms	Wait time for response retransmissions
Transport Timeout Timer	5000 ms	Determines the duration of time to wait before ending a tired connection when far end blocks the connection.

MIME Payload - Field Definitions

The MIME Payload contains location information about the origin of the call. The Sonus SBC 1000/2000 processes the Multi-part MIME Content-Type header in the SIP INVITE message upon ingress to the Signaling Group. The Sonus SBC 1000/2000 passes through the **pidf+xml** Content-Type as is to the egress side Signaling Group in an SIP INVITE message. The Sonus SBC 1000/2000 does not process the XML body of the PDIF-LO content.

ELIN Identifier

ELIN identifier maps the selected label from PIDF-LO XML content to the call router translation table input field.

- **LOC:** Location information (Generic information, i.e., city or building)
- **FLR:** Floor location
- **HNO:** House number

PIDF-LO Passthrough

Specifies whether or not to allow the passthrough of pidf+xml content from Ingress to Egress.

- **PIDF-LO:** GEOPRIV Presence Information Data Format Location Object (PIDF-LO) The Presence Information Data Format Location Object (PIDF-LO) is the recommended way of encoding location information and associated privacy policies. Location information in a PIDF-LO may be described in a geospatial manner based on a subset of Geography Markup Language (GML) or as civic location information.

Unknown Subtype Passthrough

Specifies whether or not to allow the passthrough of unknown subtype content from Ingress to Egress.

Option Tags - Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

The SIP Option Tags determine in which SIP header, the **100rel, Timer** and **Update** tags will appear.

- **Supported:** means the specified tag is included in the Supported Header.
- **Required:** means the specified tag is included in the Required Header.
- **Not Present:** means the specified tag is included in neither the Supported Header nor the Required Header.

> When the Session Timer option is enabled, the SBC uses either INVITE or UPDATE to refresh the session. The method used is negotiated between the SBC and peer. The Option Tags selections simply specify in which header to specify the tag.

SDP Customization

The SDP customization fields enables you to customize configuration for SDP. The features in this section are applicable only when a DSP is in use for the call.

Send Number of Audio Channels

For interoperability purposes, enables the **/1** field to be removed from media attribute in SDP. In the a= line, the **/1** field is dropped if the value is configured as False.

Example: **a=rtpmap:4 g723/8000/1** becomes **a=rtpmap:4 g723/8000**

Valid entry: **True** (/1 field stays intact) or **False** (/1 field is dropped). Default value: **True**.

Origin Field Username

Value of the Origin (o=) username field. Valid entry: up to 64 alphanumeric characters. For security purposes, this field can be set as "-". Default value: **SBC**.

Session Name

Value of the Session (s=) field. Valid entry: up to 64 alphanumeric characters. For security purposes, this field can be set as "-". Default value: **VoipCall**.

Digit Transmission Preference

Determines how digits are sent to the far end during an ongoing call (Example, digits might be sent to an IVR system during a call). This argument specifies which digit transmission method to use when both are available to the call.

Selections:

- **RFC 2833/Voice**
- **SIP Info**

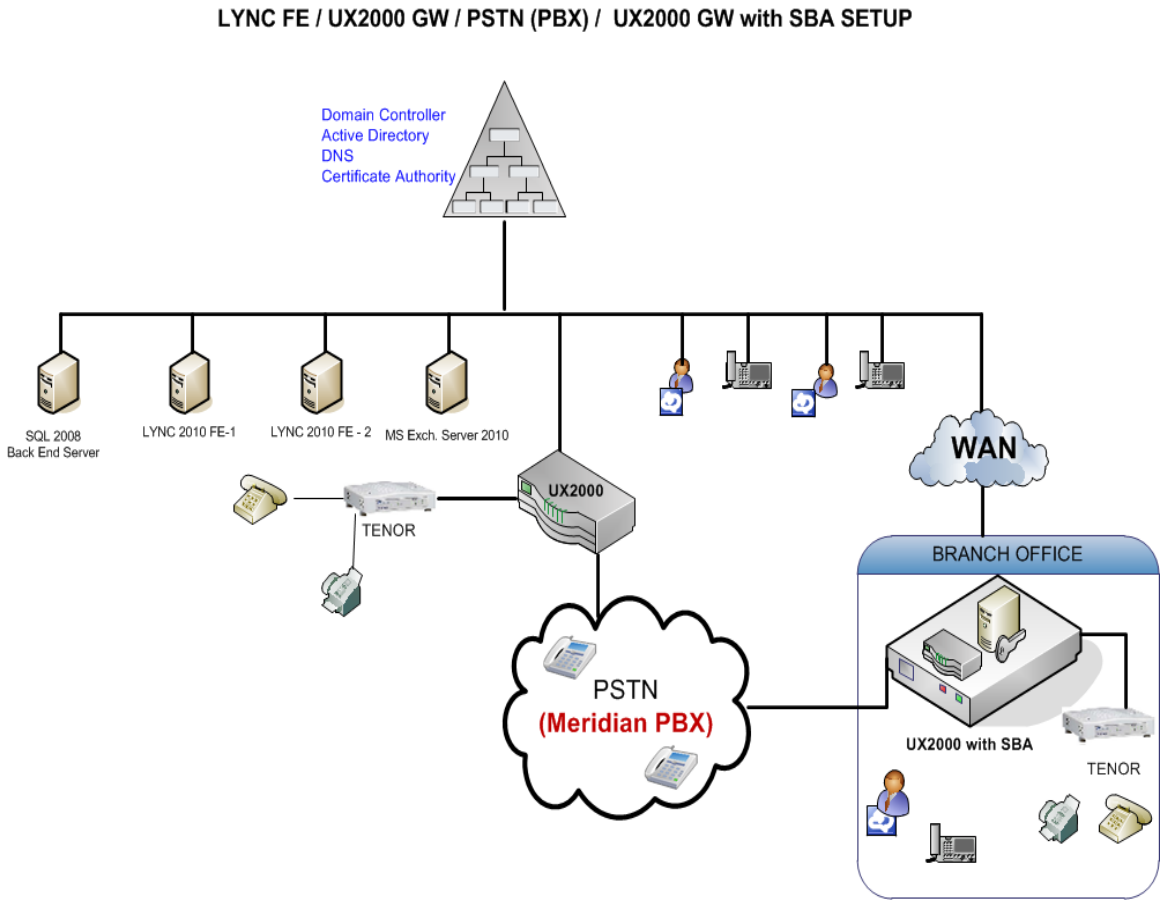
SIP Session Timer Configuration

In any SIP call scenario, two entities are involoved in the call flow: UAC and UAS. In this exercise, PSTN makes a call to the Lync client over the Sonus SBC 1000/2000, where the Sonus SBC 1000/2000 acts as a UAC and the Lync/SBA acts as a UAS. In our example we are assuming that a Sonus SBC 1000/2000 is integrated in the topology shown below.

Copyright © 2015 Sonus Networks. All rights reserved.

This article describes the steps necessary to configure a Sonus SBC 1000/2000 to employ the SIP Timer Functionality in the depicted topology:

Topology



Configuration

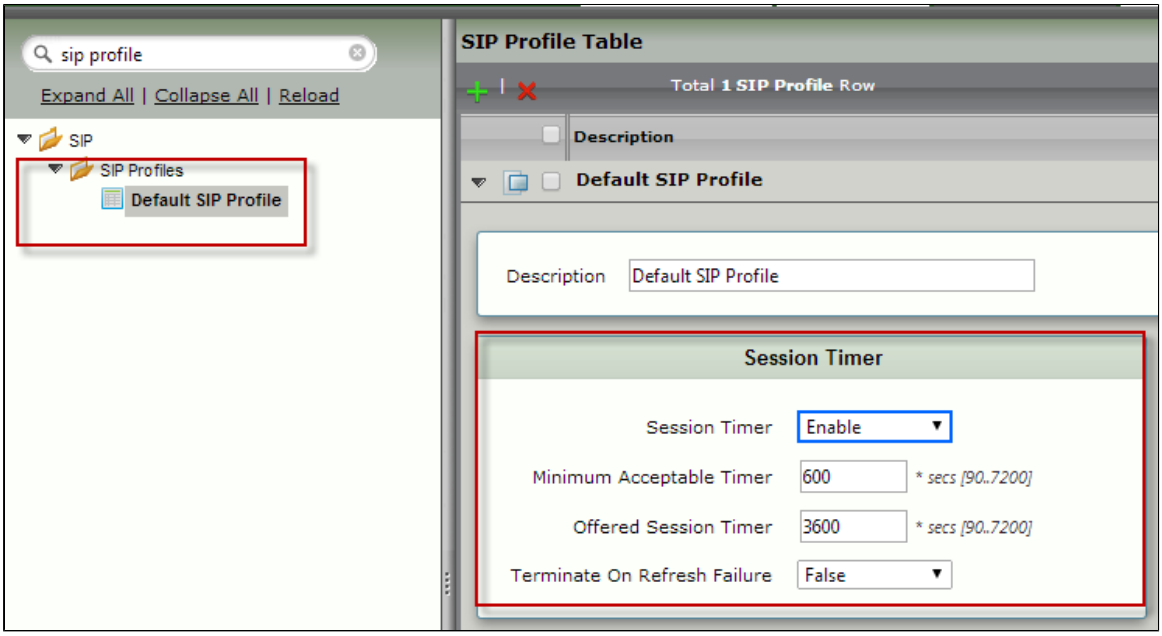
The configuration process comprises of two overall steps:

- Creating and Configuring a SIP Profile with the Session Timer Enabled
- Specifying the SIP Profile, created above, in a SIP Signaling Group

SIP Profile - Session Timer

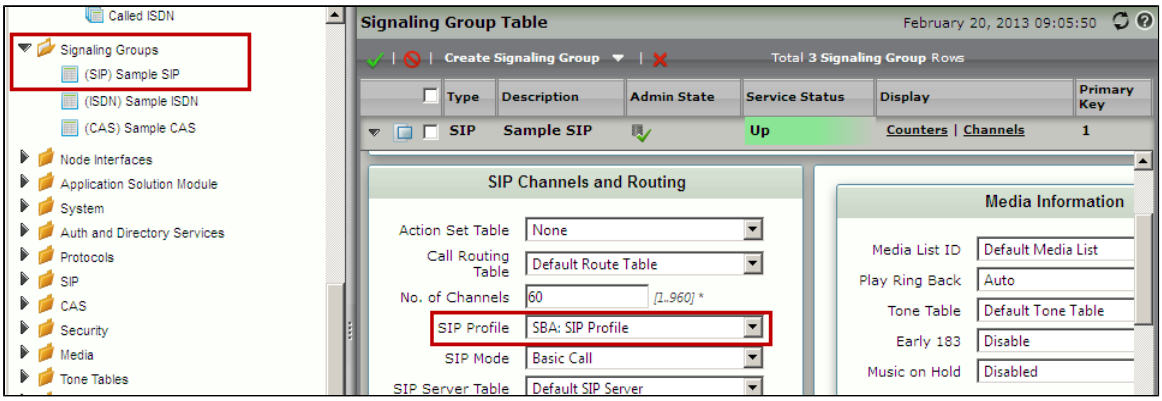
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Profiles**
3. Select the relevant SIP Profile.
4. Configure the Session Timer as shown in the figure below.
   Important: The **Offered Session Timer** value must be equal to or greater than the **Minimum Acceptable Value**.

Copyright © 2015 Sonus Networks. All rights reserved.



Signaling Group

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups > (relevant SIP Signaling Group)**.
3. Select the SIP Profile configured above from the SIP Profile selection list.
4. Click **Apply**



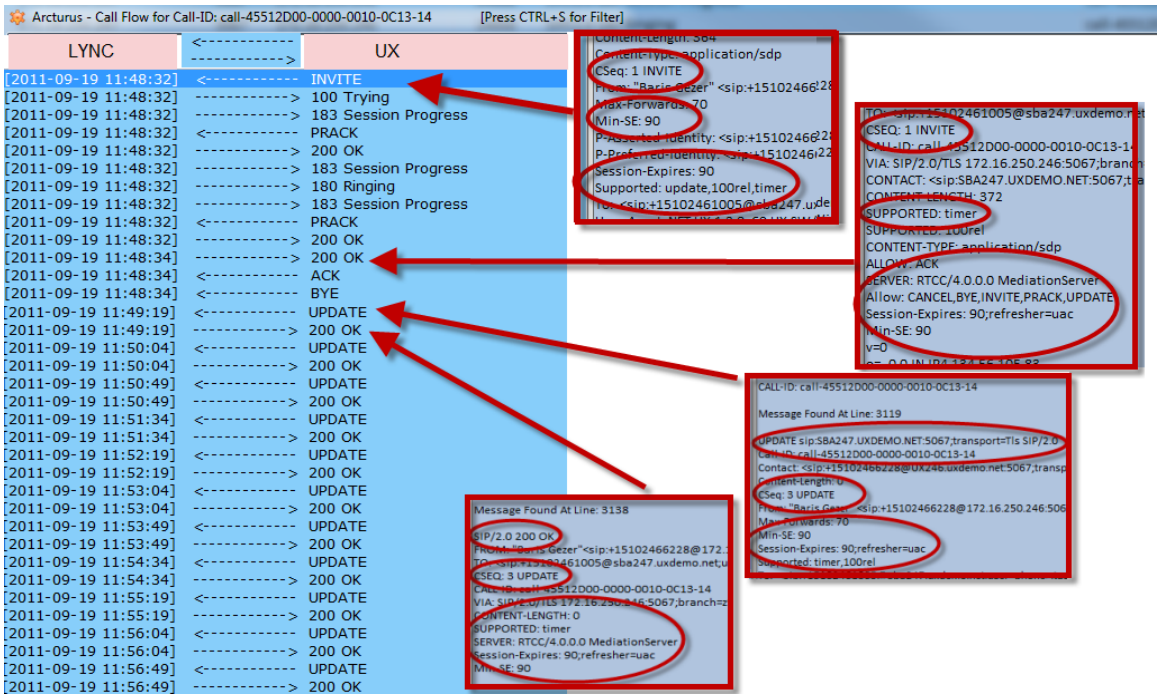
Call Flow

After having applied the configuration changes, in the call flow, the Sonus SBC 1000/2000 supports the UPDATE and INVITE methods for changing the media capabilities. Session Timer (RFC 4028) uses the INVITE or UPDATE as a mechanism for a periodic refresh of SIP sessions.

Currently the Sonus SBC 1000/2000 supports RTCP-based dead call detection. Session timers provide an alternate methodology for the detection of dead calls using SIP Signaling. If the SIP peer fails to respond to an UPDATE or INVITE message, this enhancement cleans up the call by sending a BYE which will enable the call stateful SIP proxies (Lync/SBA in this example) to clean up the resources associated with the call. Additionally, the relevant DISCONNECT is sent to the PSTN link by the Sonus SBC 1000/2000.

You can verify this using the **Log Exchange** utility — the following diagram depicts a Sonus SBC 1000/2000 to Lync/SBA call with the **Session Timer** enabled and in effect:

Copyright © 2015 Sonus Networks. All rights reserved.



Managing TLS Profiles

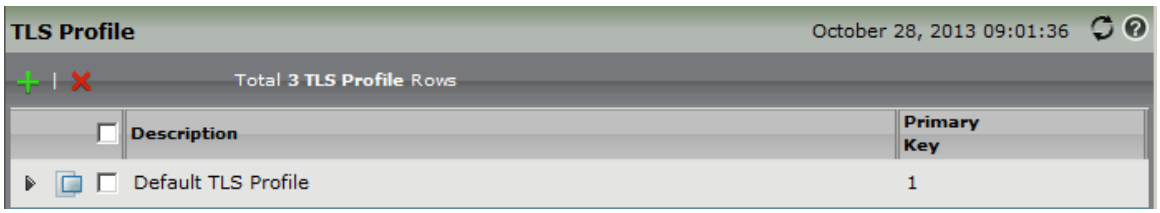
After the Sonus SBC 1000/2000 obtains the required certificates, configuration of several options/attributes on both the server and client is necessary before TLS can employ the certificate(s) in establishing a secure connection. The attributes are configured in TLS profiles. Attributes include, but are not limited to, such things as Client Ciphers, and inactivity timeouts.

TLS Profiles are used by SIP Signaling Groups when the TLS transport type is selected for incoming and outgoing SIP trunks (Listen Ports), and in SIP Server Tables when TLS is selected as the Server Host protocol.

Sonus SBC 1000/2000 supports only TLS 1.0, SSL 3.0 and SSL 2.0 are not supported due to security risks and vulnerabilities.

Working with TLS Profiles

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > TLS Profiles**.



To view a TLS Profile's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Copyright © 2015 Sonus Networks. All rights reserved.

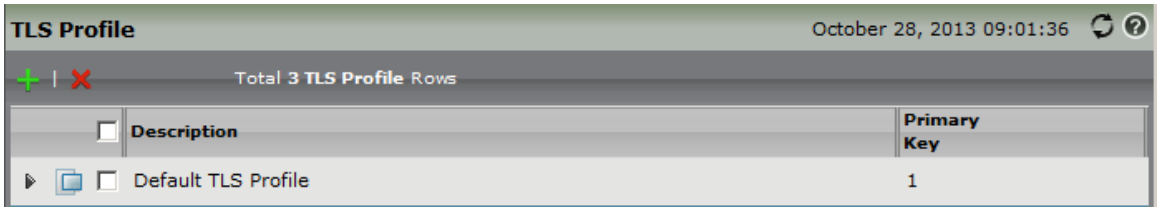
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying TLS Profiles

Creating and Modifying TLS Profiles

To create or modify a TLS Profile:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > TLS Profiles**.



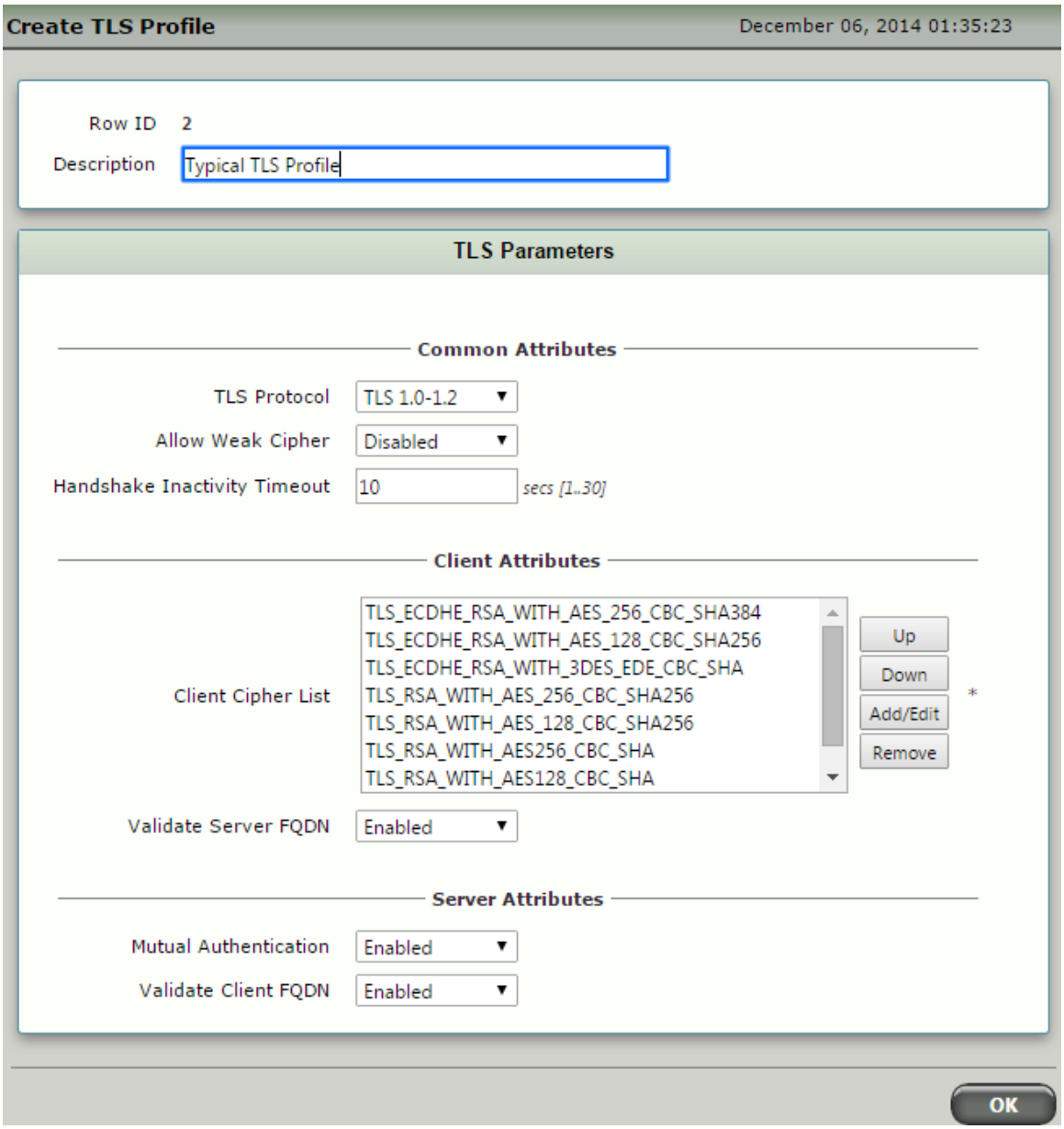
Modifying a TLS Profile

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a TLS Profile

1. Click the **CreateTLS Profile** ( ) icon at the top of the TLS Profile page.

Copyright © 2015 Sonus Networks. All rights reserved.



TLS Profile - Field Definitions

TLS Protocol

Specifies the TLS version. The Client Cipher List is automatically updated to display only the ciphers supported for the selected TLS version.

Allow Weak Cipher

When enabled, this option allows the use of a weak (older) cipher, and an additional (weak) cipher is added to the end of the client cipher list.

- SBC as the TLS server: When the SBC acts as the server it allows older clients to authenticate using older TLS ciphers.
- SBC as the TLS client: When the SBC acts as a client in the call, an the additional cipher added to the end of the list is offered to the server when negotiating the cipher. The ordered list of ciphers is presented to the server end with the preferred (by the SBC) cipher at the top.

Copyright © 2015 Sonus Networks. All rights reserved.

Handshake Inactivity Timeout

Specifies the SIP TLS client and server handshake inactivity timeout interval.

The Inactivity Timeout terminates the TLS session if there have been no handshakes in the specified period of time.
The handshake inactivity timeout should be adjusted to 30 seconds if there are network delays and/or timeouts.

Verify Peer Server Certificate

Specifies whether or not to verify the identity of a peer server. Available when **Mutual Authentication** is disabled.

> This setting is part of the standard level of Mutual TLS security. Verify Peer Server Certificate implies that Mutual Authentication is enabled first. Verify Peer Server Certificate includes a check on the certificate dates for certificate validity and whether the certificate is signed by a local trusted root CA.

Client Cipher

Specifies the cipher suite parameter exchanged and negotiated in the SIP TLS client handshake message. The list is automatically populated with the ciphers supported for the selected TLS Protocol.

The SBC 1000/2000 supports the following TLS cipher suites:

- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES256_CBC_SHA
- TLS_RSA_WITH_AES128_CBC_SHA
- TLS_RSA_WITH_DES_CBC_SHA

> **Lync Cipher Incompatability**
>
> The ***TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA*** is incompatible with Lync servers.

Validate Server FQDN

The *Validate Server FQDN* is an enhanced security feature of the Sonus SBC 1000/2000, which is disabled if the common name in the certificate is an IP address (a practice observed by some ITSP's). This field is only visible when **Validate Peer Server Certificate** is enabled and **Mutual Authentication** is disabled.

Validate Server FQDN (enabled) option allows the Sonus SBC 1000/2000 to perform an FQDN match of an incoming peer certificate common name (CN) or Subject Alternate Name (SAN) against the host that is configured in the SIP Server table of Sonus SBC 1000/2000 (protocol must be TLS and the Host must be in the form of FQDN).

> Sonus SBC 1000/2000 does not validate IP addresses to identify a peer server, but only Fully Qualified Domain Names (FQDN).

Copyright © 2015 Sonus Networks. All rights reserved.

Mutual Authentication

Enables the Mutual authentication request and verifications of the SIP peer client certificate.

> This setting is part of the standard level of Mutual TLS security. Mutual Authentication includes a check on the certificate dates for certificate validity and whether the certificate is signed by a local trusted root CA.

Validate Client FQDN

Specifies the reverse DNS lookup of a peer's FQDN. Used to verify the identity of the SIP peer client certificate.

This action takes place when both, MTLS and "Validate Client FQDN" are enabled. If MTLS is disabled, the "Validate Client FQDN" is also disabled. "Validate Client FQDN" is an enhanced security feature of Sonus SBC 1000/2000, which could be disabled if the common name in the certificate is an IP address (some ITSP's do that). "Validate Client FQDN" Enabled option allows Sonus SBC 1000/2000 to perform an FQDN match of an incoming peer certificate common name (CN) or Subject Alternate Name (SAN) against a reverse DNS lookup of the IP address to an FQDN.

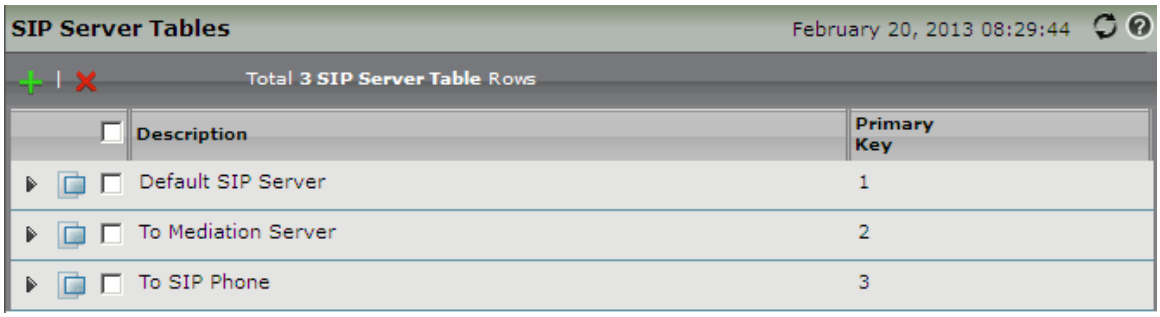
> Sonus SBC 1000/2000 does not validate IP addresses to identify a peer server, but only Fully Qualified Domain Names (FQDN).

Managing SIP Server Tables

SIP Server Tables contain information about the SIP devices connected to the Sonus SBC 1000/2000. The entries in the tables provide information about the IP Addresses, ports, and protocols used to communicate with each server. The Table Entries also contain links to counters that are useful for troubleshooting.

Working with SIP Server Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Server Tables**.



To view a SIP Server Table's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

To modify a SIP Server Table:

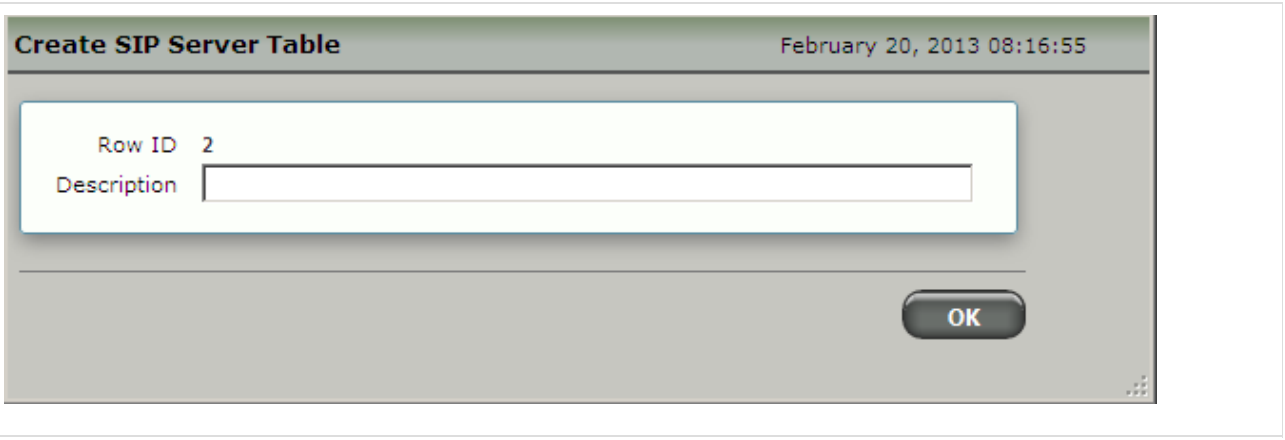
1. Click the **expand** ( ) Icon next to the entry you wish to modify.

Copyright © 2015 Sonus Networks. All rights reserved.

2. Modify the table's **Description** as desired
3. Click **OK**.

To add a SIP Server Table:

1. Click the **Create** ( ) icon.



2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Entries in SIP Server Tables

Creating and Modifying Entries in SIP Server Tables

Instructions for modifying/creating a SIP Server Table entry are below. To add a SIP Server table, see Managing SIP Server Tables.

Creating an Entry in a SIP Server Table

1. In the left navigation pane, go to **SIP > SIP Server Tables**. Click on the desired SIP Server Table.
2. From the **Create SIP Server** drop down list, select **IP/FQDN** or **DNS-SRV**. The associated configuration screen is displayed.

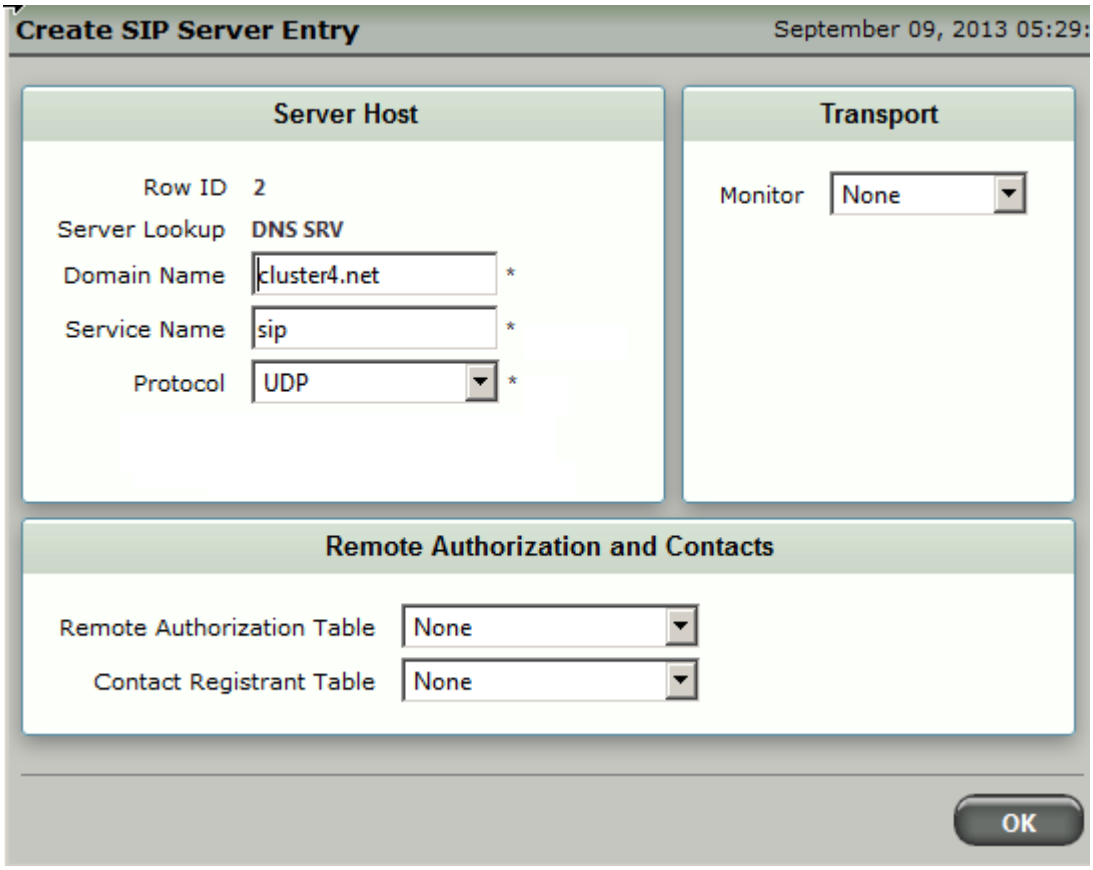
Configure the options,see details below

SIP Entry guidelines

- Multiple entries of the same server type (IP/FQDN or DNS-SRV) can be added to a SIP Server Table, but only **one** type of server is allowed per table. For example, if you add a SIP Server as DNS-SRV, the other entries in the same table must be specified as DNS-SRV; to add a Server Lookup as IP/FQDN, you must create another table.
- Only **one** domain name and protocol are permitted in a SIP Server Table. If the domain name and protocol are used in one entry, they cannot be used in an additional entry in that same table.
- Only **one** domain name per SIP Server table can be selected as the Server Host.

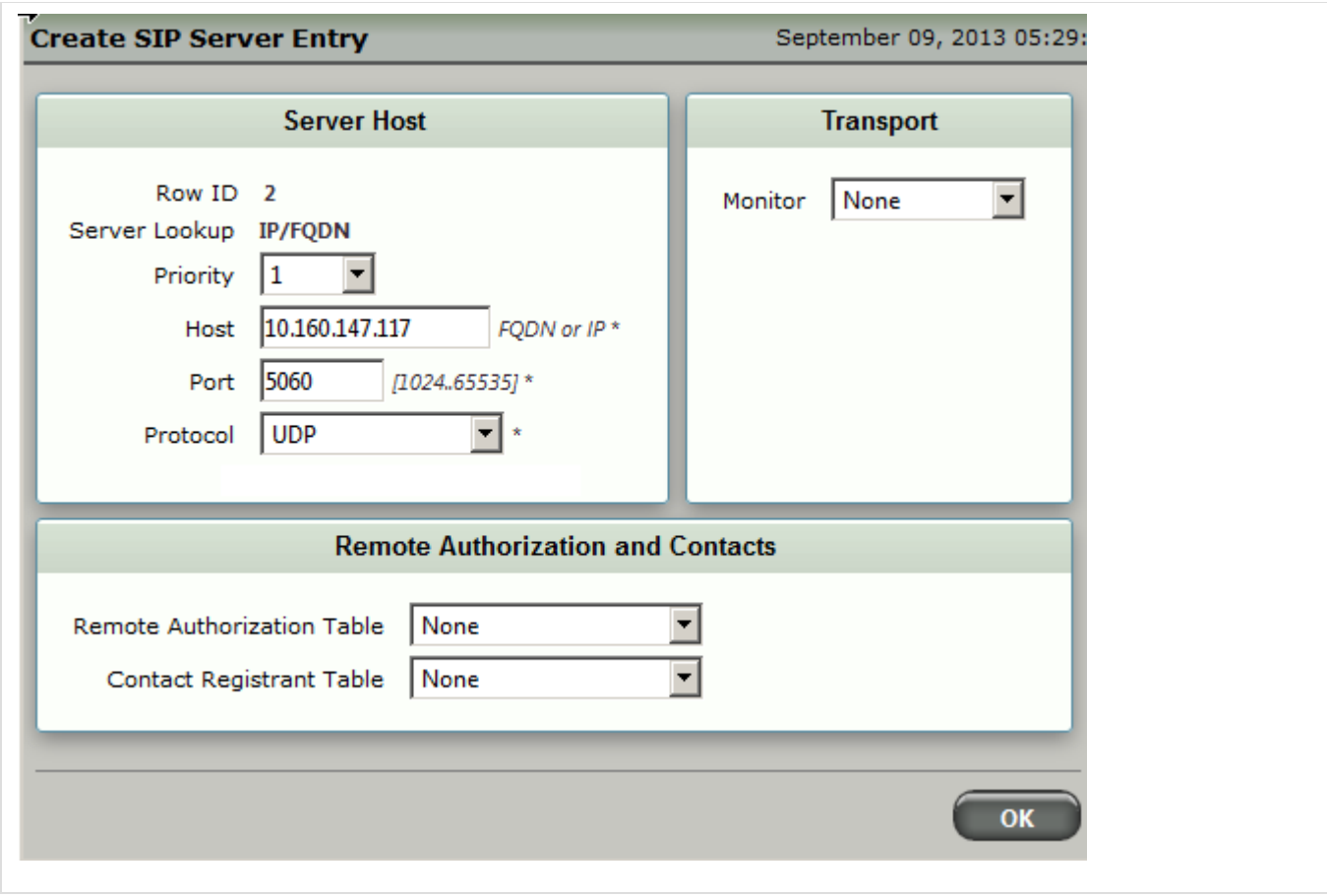
Create SIP Server: DNS SRV

Copyright © 2015 Sonus Networks. All rights reserved.



Create SIP Server: IP/FQDN

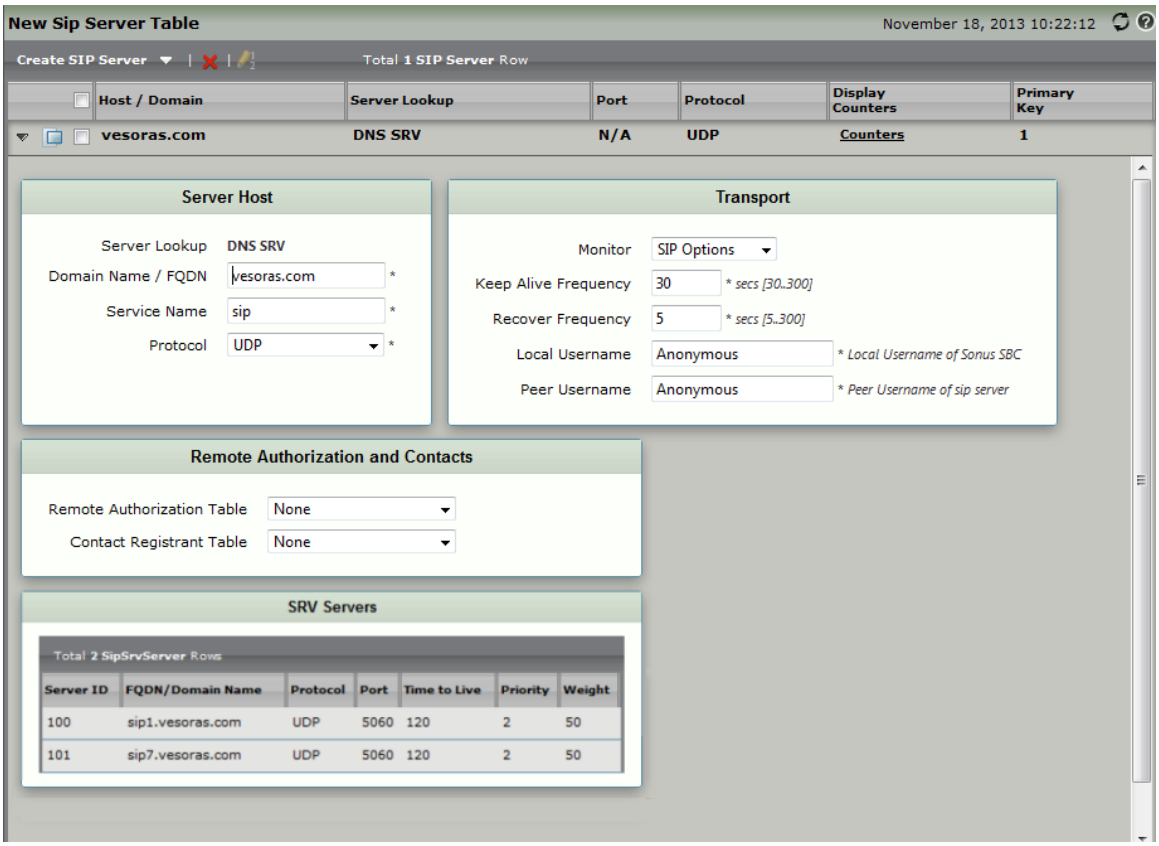
Copyright © 2015 Sonus Networks. All rights reserved.



Modifying an Entry in a SIP Server Table

1. In the left navigation pane, go to **SIP > SIP Server Tables.**
2. Select the desired SIP Server Table.
3. Click the expand ( ) icon next to the entry you wish to modify.
4. Edit the entry properties as required, see details below.

Copyright © 2015 Sonus Networks. All rights reserved.



Resequencing an Entry in a SIP Server Table

1. Click the **Resequence** icon ( ) at the top of the table.
2. Select the row(s) you want to move.
3. Click the **Move Selected Rows Up** ( ) or **Move Selected Rows Down** ( ) icon to reposition the row(s) in the table.
4. Click **Apply**.

Server Host - Field Definitions

Server Host - For IP/FQDN only

Server Lookup

This field is populated automatically when you add a SIP Server table entry and select **IP/FQDN Lookup** from the **Create SIP Server** drop down box. IP/FQDN enables the SBC to select the server containing the specified IP address or Fully Qualified Domain Name (FQDN) to which this Signaling Group sends SIP messages.

Priority

Specifies the priority of this server. The priority is used to order the server when more than one is configured. If Load Balancing is configured as Round Robin or First in the SIP Signaling group, the Priority field is not used to determine the priority of the server. See Creating and Modifying SIP Signaling Groups.

Copyright © 2015 Sonus Networks. All rights reserved.

Host

Specifies an IP address or Fully Qualified Domain Name (FQDN) to which this Signaling Group sends SIP messages.

If an FQDN is configured all the associated servers are included and used according to the server selection configuration element.

Port

Specifies the port number to which SIP messages are sent.

Protocol

Specifies the protocol to use for sending SIP messages. Valid entry: **UDP**, **TCP**, or **TLS**. Depending upon the entry you select, different configuration options are available. These are noted where necessary.

TLS Profile

If TLS is selected in the **Protocol** field, this specifies the TLS profile this server will use for secure SIP messages.

Server Host - For DNS SRV only

Server Lookup

This field is populated automatically when you add a SIP Server table entry and select **DNS-SRV Lookup** from the **SIP Server** drop down box. DNS SRV enables the SBC to populate SIP server entries in the SIP Server Table based on SRV records (specified by domain, service, and protocol supported). SIP entries are updated automatically as servers change and become available/unavailable.

Domain Name

This field specifies the domain name supported in a SIP server from which the SBC requests information (through the DNS SRV Query). This field is used in combination with the **Service** and **Protocol** fields in the DNS SRV Query to request a list of eligible SIP servers. Valid entry: name of domain (i.e., example.com).

Service Name

This field specifies the service name (i.e., SIP) that will be used in the DNS SRV query. This field defaults to "sip" but can be overwritten with any text string (i.e., sipinernaltls). This field is used in combination with the **Domain Name** and **Protocol** fields in the DNS SRV Query to request a list of eligible SIP servers. Valid entry: name of service (i.e., SIP).

Protocol

This field specifies the protocol (i.e, UDP, TCP, or TLS) supported in a SIP Server from which the SBC requests information (through the DNS SRV query). This field is used in combination with the **Domain Name** and **Service Name** fields in the DNS SRV Query to request a list of eligible SIP servers. Valid entry: select from the drop down list.

Copyright © 2015 Sonus Networks. All rights reserved.

Remote Authorization and Contacts - Field Definitions

Remote Authorization Table

Specifies a Remote Authorization table for this SIP Server from the list of authorization tables defined in the Remote Authorization Tables.

The Remote Authorization table is used by a Signaling group when a challenge (401/407) is issued by the server. The table contains a realm, user name, and password. They are used to provide credentials to the server issuing the challenge.

Contact Registrant Table

Specifies a Contact Registration Table for this SIP Server from the list of registration tables defined in the Contact Registrant Tables.

The Contact Registration is used by a Signaling Group to register one or more contacts to a registrar. The contact information contains the SIP address of record and the methods which can be used to establish sessions to this Signaling group. Valid entry: Select from the list of Contact Registrant Tables or select None. If you select a Contact Registrant from the list, the following fields are displayed: **Clear Remote Registration on Startup**, **Contact URI Randomizer**, and **Stagger Registration**.

> If **Fwd. Reg. After Local Processing** is selected as the SIP Mode**,** the selected SIP Server Table for that same Signaling Group should not be configured with a Contact Registrant Table. The SBC does not support **Fwd Reg. After Local Processing** and a Contact Registrant Table in the same Signaling Group.

Clear Remote Registration on Startup

Specifies whether Remote Registration is cleared upon startup. When enabled, on power-up a Register with Expires: 0 ("Unregister") is first sent. When complete, a Register with Expires: non-0 ("Register") is sent. Valid entries: **True** (enables remote registration to be cleared at power-up) or **False** (disables remote registration from being cleared at power-up). This field is visible only when **Contact Registrant Table** is set to a value other than **None**. Default entry: **False**.

Contact URI Randomizer

Enables the username portion of the Contact URI in the registration for Request-URIs to contain a randomized value. When enabled, this random value is generated and put into the username portion of the Contact-URI of each outgoing Register message. The random user portion is saved and compared to the incoming Invite Request-URIs. If the Prefix of the Request-URI contains Hz1q6R, and there is a match, Hz1q6R is stripped and the remaining number is used to route. If there is not a match, but the first six digits are Hz1q6, the Invite Request-URI is ignored and no response is sent. If Hz1q6R is not contained in the Prefix, the number is sent as-is for routing. This field is visible only when the **Contact Registrant Table** is set to a value other than **None**. Valid entries: **True** (contact URI Randomizer is used) or **False** (contact URI Randomizer is not used). Default entry: **False**.

Stagger Registration

Copyright © 2015 Sonus Networks. All rights reserved.

Enables Registration (and Unregistration) Requests to be staggered by one second if more than one Contact Registrant entry is in the Contact table. This field is visible only when Contact Registration Table is set to a configuration other than **None**. Valid entry: **True** (registration requests are staggered) or **False** (registration requests are not staggered). Default entry: **False**. When Stagger Registration is set to **True**, the maximum number of contact registrant entries configured should not exceed 500. If more than 500 are entered in configuration, they will be dropped and an ERROR trace is generated.

Retry Non-Stale Nonce

In 401 message, when stale = false, this field enables the SBC to either set the failed retry timer and re-attempt to send Register with same credentials at expiration (**True**) or not resend a Register with the same credentials (**False**).

Transport - Field Definitions

Monitor

Specifies the method to monitor server.

- **None:** No monitoring of this server occurs.
- **SIP options:** An OPTIONS message is sent to the server. When this option is selected, additional configuration items are displayed. These are noted below.

Keep Alive Frequency

Specifies how often, in seconds, the Sonus SBC 1000/2000 queries the server with an OPTIONS message to determine the server's availability. Visible only when **SIP Options** is selected from the **Monitor** field.

If the server does not respond, the Sonus SBC 1000/2000 marks the Signaling Group as down. When the server begins to respond to the OPTIONS messages again, it will be marked as up.

Recover Frequency

Specifies frequency in seconds to check server to determine whether it has become available. Default entry: **Anonymous**. Visible only when **SIP Options** is selected from the **Monitor** field.

Local Username

Local user name of the Sonus SBC 1000/2000 system. Default entry: **Anonymous**. Visible only when **SIP Options** is selected from the **Monitor** field.

Peer Username

User name of the SIP Server. Visible only when **SIP Options** is selected from the **Monitor** field.

Connection Reuse - Field Definitions

The configuration options in this section are available only when when **Protocol** is set as **TCP** or **TLS**.

Reuse

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies whether or not sockets will be reused or shared. Select from the drop down list: **True** (sockets are reused) or **False** (sockets are shared).

Sockets

Specifies number of re-usable sockets. Valid entry: 1 - 4.

Reuse Timeout

Specifies whether or not a socket will timeout. If set to **Limited**, the **Timeout Limit** field is displayed.

Timeout Limit

Specifies the number of minutes that a socket remains connected to the server. This field is displayed only if **Protocol** is set as **TCP** or **TLS,** and **Reuse Timeout** is set as **Limited**. Valid entry: 5 - 1440 minutes.

SRV Servers Table - Field Definitions

This table is in view-only mode and available only when the **Server Lookup** field is set as **DNS SRV** in the SIP Server Table. To view this table, go to **SIP > SIP Server Tables** and click on the desired SIP Server Table entry. The populated values in this table are determined by the administrator for the DNS server; ranges and possible values are detailed below.

Server ID

A number generated internally that is used to identify the SIP Server.

FQDN/Domain Name

Based on the response from the DNS SRV Query, the SBC populates this table with the configured SIP server entries (IP or FQDN). The SBC will refresh the server entries by re-trying the same DNS SRV query until the Time to Live for the SRV record expires. This table is updated automatically as servers change and become available/unavailable.

Protocol

This field specifies the protocol (i.e, UDP, TCP, or TLS) supported in the SIP Server.

Port

Specifies the port number to which SIP messages are sent.

Time to Live

Amount of time the SRV record is able to be retried. This range is dependent on the value sent from the DNS server.

Priority

Copyright © 2015 Sonus Networks. All rights reserved.

Priority determines how servers are selected. A server with a lower number priority is selected first. If that server is unavailable, the next server with the higher priority number is selected. Servers with the same priority value are selected based on weight parameter. For more information, see Weight.

Weight

The weight field specifies a relative weight for SIP server entries (range 0 - 65535), which is used to determine the selection of the server if the priority value is the same between two servers. A server with a larger weight is given a higher probability of being selected than a server with a lower weight. The weight selection algorithm is per RFC 2782.

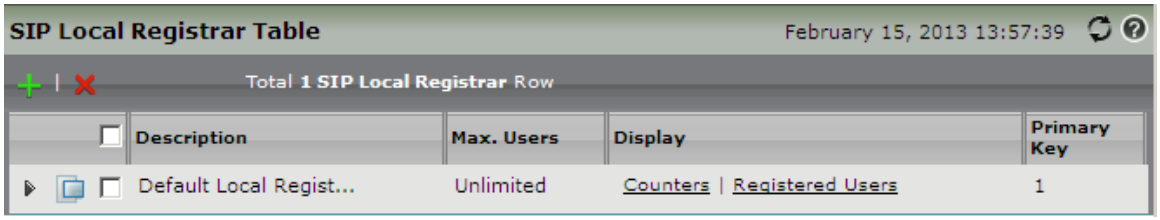
Managing Local Registrars

SIP provides a registration function that allows users to upload their current locations for use by proxy servers. Registration creates bindings in a location service for a particular domain that associates an address-of-record URI with one or more contact addresses.

Registration entails sending a REGISTER request to a special type of UAS (User-Agent Server) known as a registrar. A registrar acts as the front end to the location service for a domain, reading and writing mappings based on the contents of REGISTER requests. This location service is then typically consulted by a proxy server that is responsible for routing requests for that domain.

Working with Local Registrars

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Local Registrars**.



To view a Local Registrar's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

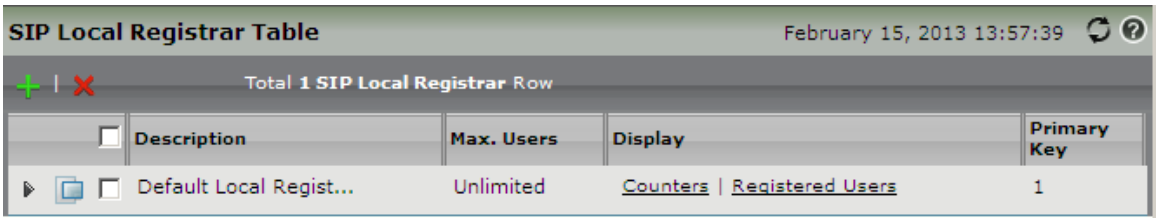
Creating and Modifying SIP Local Registrars

Creating and Modifying SIP Local Registrars

To create or modify an existing SIP Local Registrar:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Local Registrars**.

Copyright © 2015 Sonus Networks. All rights reserved.

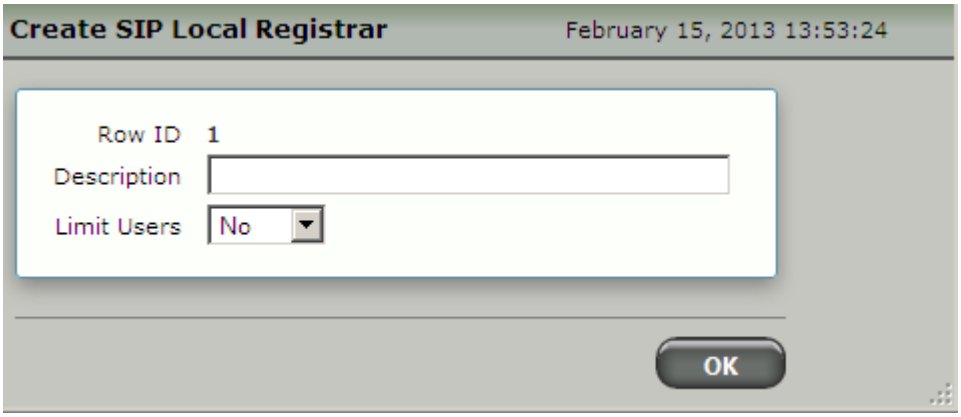


Modifying a SIP Local Registrar

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a SIP Local Registrar

1. Click the **Create SIP Local Registrar** icon ( ) at the top of the SIP Local Registrar Table page.



Local Registrar - Field Definitions

Limit Users

Specifies whether or not there is a limit to the number of users that can be added to this Registrar

Number of Users

Specifies the number of contacts that are allowed to register to this registrar, the maximum number of users is 1000. If the specified limit is exceeded the proxy will reject the registration request.

This field is available only when Limit Users option is set to **Yes**.

Managing Contact Registrant Tables

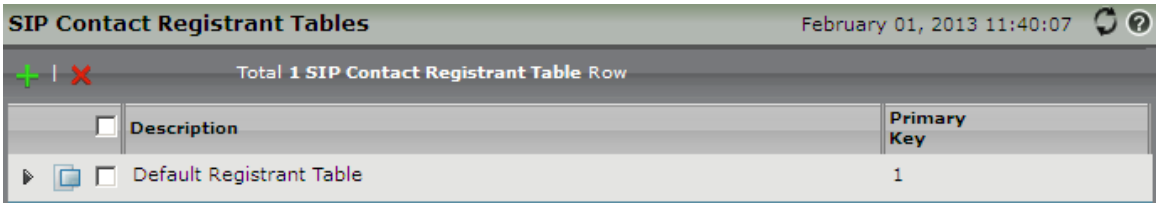
Contact Registrant Tables are used to manage contacts that are registered to a SIP server. The SIP Server Configuration can specify a Contact Registrant Table, and the ussername portion of the table will be used for outbound calls.

Working with Contact Registrant Tables

1. In the WebUI, click the **Settings** tab.

Copyright © 2015 Sonus Networks. All rights reserved.

2. In the left navigation pane, go to **SIP > Contact Registrant Tables**.



To view a Contact Registrant Table's properties:

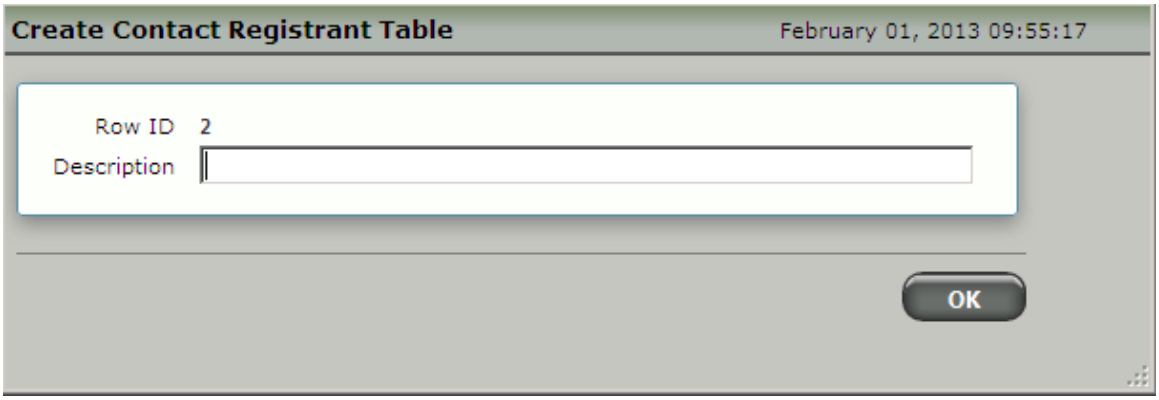
1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

To modify a Contact Registrant Table:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To add a Contact Registrant Table:

1. Click the **Add** ( ) icon.



2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Entries in Contact Registrant Tables

Viewing Registration Status for Entries in Contact Registrant Tables

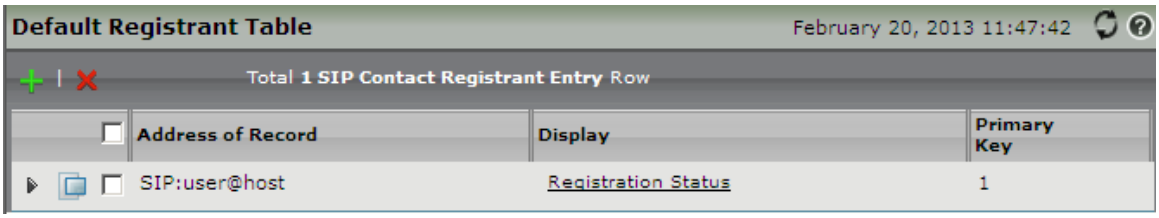
Creating and Modifying Entries in Contact Registrant Tables

To create or modify an Entry in the Contact Registrant Table:

1. In the WebUI, click the **Settings** tab.

Copyright © 2015 Sonus Networks. All rights reserved.

2. In the left navigation pane, go to **SIP > Contact Registrant Tables** and click on the **Create SIP Contact Registrant** icon ( ).



Modifying an Entry in the Contact Registrant Table

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Viewing an Entry's Registration Status

To view an entry's registration status, see Viewing Registration Status for Entries in Contact Registrant Tables.

Contact Registrant - Field Definitions

Type of Address of Record

Specifies how the Address of Record is populated in the REGISTER request.

- **Local:** The host portion of the Address of Record (AOR) URI will be the local IP/FQDN.
- **Remote:** The host portion of the Address of Record (AOR) URI will be the Server IP.
- **Static**. When set as Static, you enter the full Address of Record (AOR) through the **Address of Record URI** field.

Address of Record URI

Identifies the address of record for this client to be registered to the SIP server.

- **Local URI**. If the **Type of Address of Record** field is set to Local, enter the user.
- **Remote URI**. If the **Type of Address of Record** field is set to Remote, enter the user.
- **Static URI**. If the **Type of Address of Record** field is set to Static, the URI must contain **user@host[:port]**

Global time to Live (TTL)

Specifies the time, in seconds, between REGISTER messages for this contact. The Sonus SBC 1000/2000 will send a REGISTER at an interval specified for the Global TTL value for all bindings.

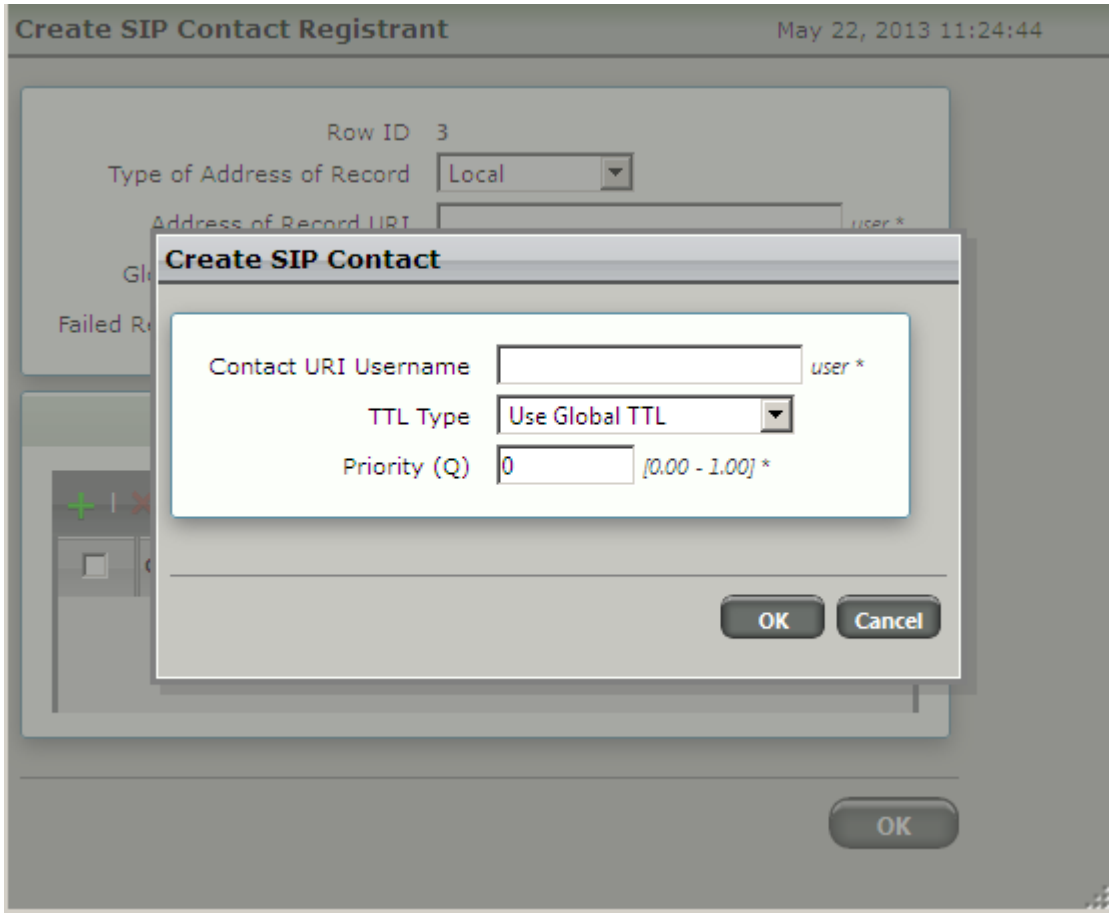
Failed Registration Retry Timer

Sets the time to wait after a failed registration to try again. Valid entry: numeric in seconds, range 30 - 86400. Default entry: 120 seconds.

SIP contacts - Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

Through the Create SIP Contact window, you can add, delete and edit SIP contact entries. See below for field definitions.



Contact URI Username

Specifies a unique SIP Uniform Resource Identifier (URI).

TTL Type

Specifies which Type of Time To Live value to use for this contact.

- **Use Global TTL:** Specifies that the Global TTL value is used for this contact.
- **Override Global TTL:** Specifies that a custom TTL value, entered in the Time to live field (below), is used for this contact.

Time to Live (TTL)

Specifies the time, in seconds, between REGISTER messages for this contact. However, the Sonus SBC 1000/2000 will send a REGISTER at an interval specified for the Global TTL value for all bindings. This field is visible only when **Override Global TTL** is specified for TTL Type.

Priority(Q)

Specifies the priority level for this binding.

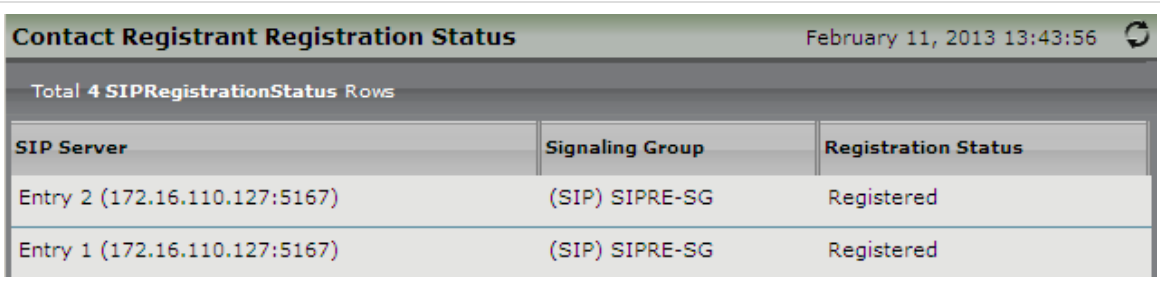
Copyright © 2015 Sonus Networks. All rights reserved.

Viewing Registration Status for Entries in Contact Registrant Tables

Through the Registration Status link on the Contact Registrant Table, you can view the registration status of the contacts registered to a SIP Server.

Access the registration status as follows:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Contact Registrant Tables.** Click on the desired table.
3. In the Contact Registrant Table, locate the desired entry and click on **Registration Status**.



Contact Registrant Status Field Definitions

SIP Server

Displays the ID of the SIP server followed by the hostname (in brackets).

Signaling Group

Displays the name of the Signaling Group which creates a REGISTER session for any entry in the SIP Server Table that contains a Contact Registrant.

Registration Status

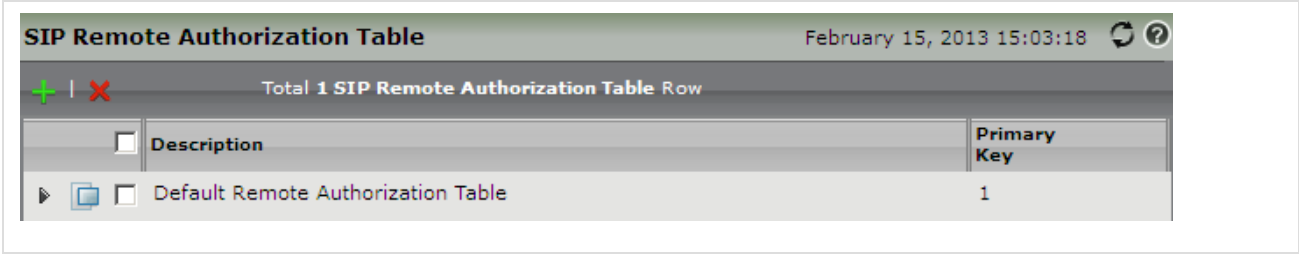
Displays the registration status. Valid fields: Registered or Not Registered.

Managing Remote Authorization Tables

Remote Authorization Tables and their entries contain information used to respond to request message challenges by an upstream server. The Remote Authorization tables defined in this page appear as options in the Remote Authorization and Contacts Panel for SIP Servers.

Working with Remote Authorization Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Remote Authorization Tables**.



Copyright © 2015 Sonus Networks. All rights reserved.

To view a Remote Authorization Table's properties:

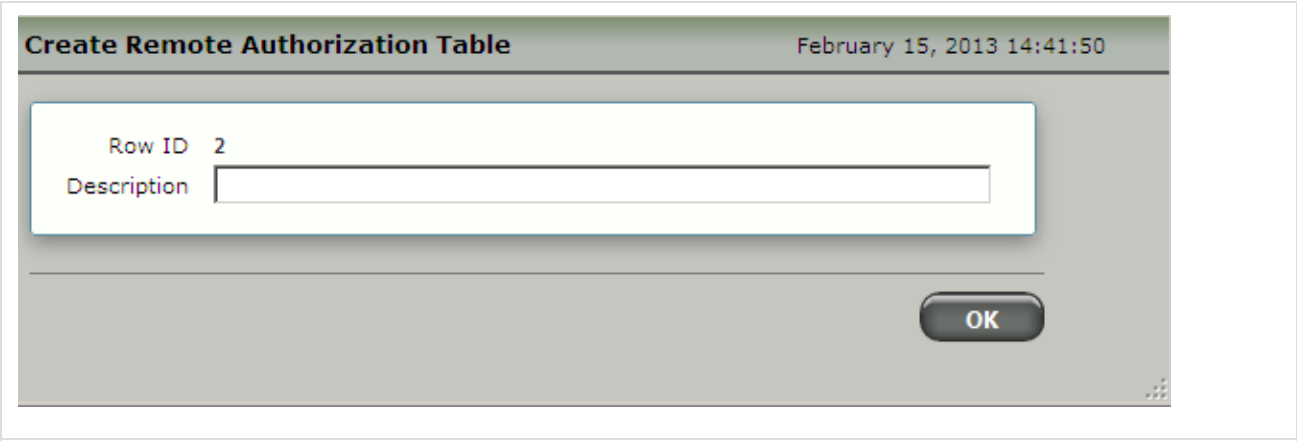
1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

To modify a Remote Authorization Table:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To create a Remote Authorization Table:

1. Click the Create ( ) icon.



2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

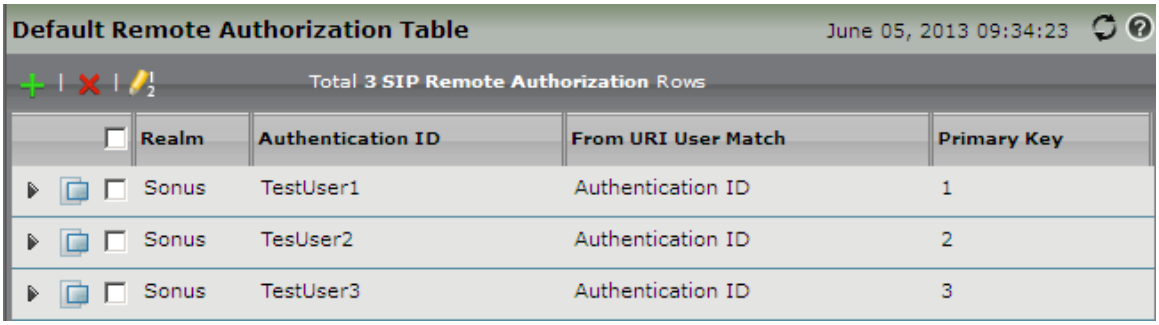
Creating and Modifying Entries to Remote Authorization Tables

Creating and Modifying Entries to Remote Authorization Tables

To create or modify an Entry to a Remote Authorization Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Remote Authorization Tables > Entry**.

Copyright © 2015 Sonus Networks. All rights reserved.



Modifying an Entry to a Remote Authorization Table

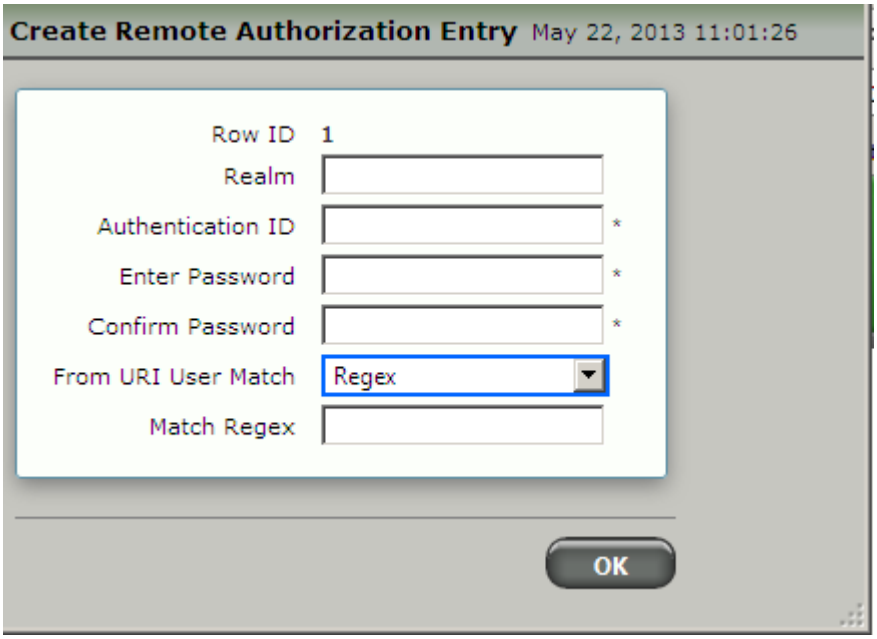
1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Resequencing an Entry in a Remote Authorization Table

1. Click the **Resequence** icon ( ) at the top of the table.
2. Select the row(s) you want to move.
3. Click the **Move Selected Rows Up** ( ) or **Move Selected Rows Down** ( ) icon to reposition the row(s) in the table.
4. Click **Apply**.

Creating an Entry to a Remote Authorization Table

1. Click the **Create Remote Authorization** ( ) icon.
2. Configure the fields. See below for valid field entries.
3. Click **Apply**.



Remote Authorization Entry - Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

Realm

Specifies a realm which is matched to an incoming challenges realm. Valid entry: maximum length = 512.

Authentication ID

Specifies a user name to use in response to a challenge, also known as Authentication ID. Valid entry: maximum length = 64.

Enter Password

The password to use with Authentication ID. Valid entry: maximum length = 64.

Confirm Password

Re-enter the password to use with Authentication ID (the same password you entered in the **Enter Password** field, maximum length = 64).

From URI User Match

Sets the matching criteria for which field the incoming From header URI User value will be matched against. Valid entry: **Authentication ID** or **Regex**. If **Regex** is selected, the **Match Regex** field is displayed.

Match Regex

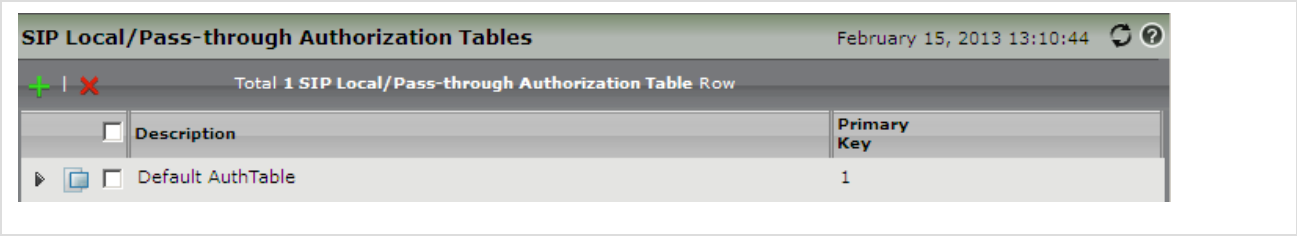
The value entered Regex matches against the incoming From Header (user name, AOR field). Valid entry: numeric, 0 - 128. This field is visible only when the **From URI User Match** field is configured as **Regex**.

Managing Local Pass-through Authorization Tables

Local Pass-through Tables contain entries with information about SIP endpoints, The Sonus SBC 1000/2000 uses this informatoin to challenge SIP request messages such as REGISTER. It is used in the SIP Signaling Group when the Challenge Request is enabled.

Working with Local Pass-through Authorization Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Local Pass-through Authorization Tables**.



To view a Local Pass-through Authorization Table's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

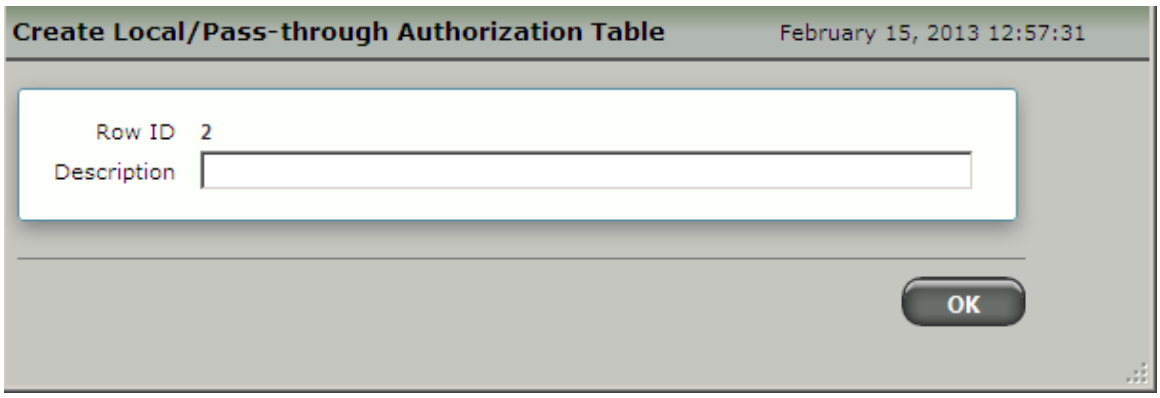
Copyright © 2015 Sonus Networks. All rights reserved.

To modify a Local Pass-through Authorization Table:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To create a Local Pass-through Authorization Table:

1. Click the **Create** ( ) icon.



2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

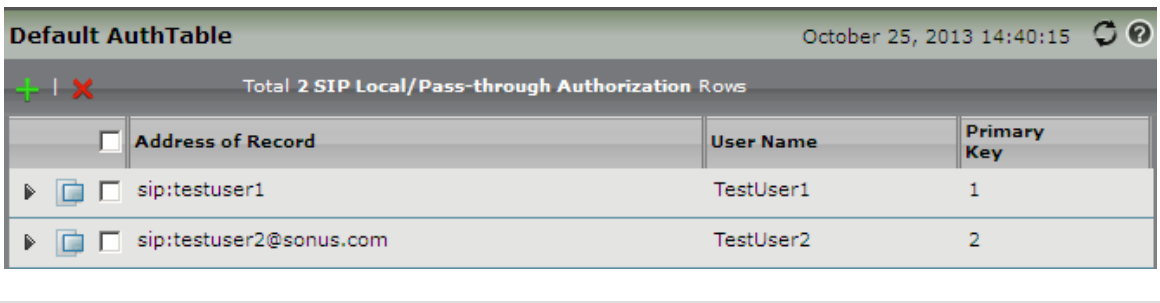
Creating and Modifying Entries to Local Pass-through Authorization Tables

Importing Local Pass-through Authorization Entries

Creating and Modifying Entries to Local Pass-through Authorization Tables

To create or modify an Entry to a Local Pass-through Authorization Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Local/Pass-thru Auth Tables.**



Modifying an Entry in a Local Pass-through Authorization Table

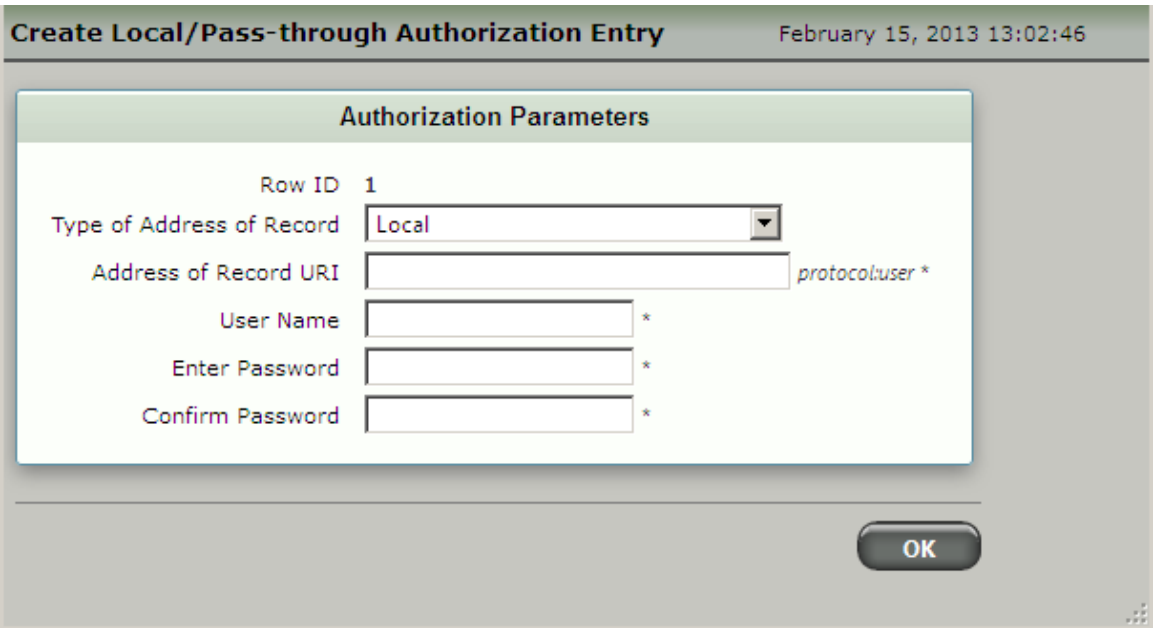
1. Click the **expand** ( ) Icon next to the entry you wish to modify.

Copyright © 2015 Sonus Networks. All rights reserved.

2. Edit the entry properties as required, see details below.

Creating an Entry to a Local Pass-through Authorization Table

1. Click the **Create Local Pass-through Authorization** ( ) icon.



Local Pass-through Authorization - Field Definitions

Type of Address Record

Specifies how the Address of Record (AOR) is received from a SIP endpoint

- **Local:** The contact registrant is the Sonus SBC 1000/2000 system
- **Remote:** The contact registrant is a separate SIP Server/Proxy host

Address of Record URI

Specifies the address of record for this client to be registered to the SIP server.

If Type of Address of Record is set to Remote, the URI must contain protocol:user@host, for example: sip:17324609000@remoterserver.com.
When a the Sonus SBC 1000/2000 system receives a SIP request, this authorization table is searched for a match and uses the realm/user/password to challenge the request.

User Name

Specifies the user name used by the proxy to challenge a REQUEST message.

Password

Specifies the password used in conjunction with the user name to calculate digest authentication.

Importing Local Pass-through Authorization Entries

Copyright © 2015 Sonus Networks. All rights reserved.

The Sonus SBC 1000/2000 provides the ability to create Local Pass-through Authorization Tables and import bulk entries into those tables in a single step under the Tasks tab.You can import entries into an existing table, or you can create a new table and import entries into it in a single step. If you import entries into an existing table, the existing entries in that table will be overwritten by the new entries from the CSV file.

Prerequisites

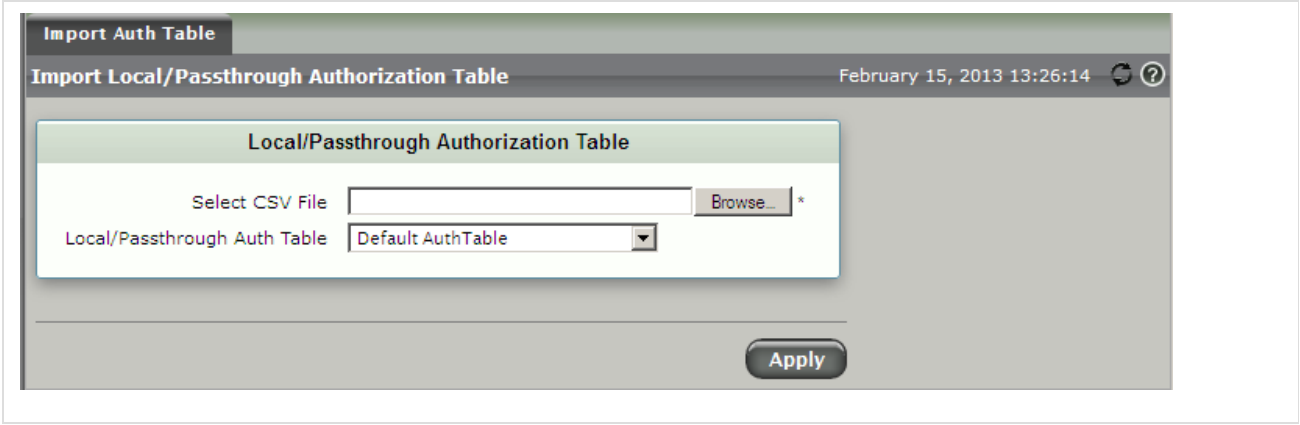
- A properly formatted CSV file.
  The file must contain one line per entry in the table, those lines must have three comma separated fields that conform to the following pattern:
  `protocol:user@host, User Name, Password`

⚠ Lines in the CSV file that contain improperly formatted *Address of Record* fields will be skipped and not appear in the table.
⚠ Lines in the CSV file that contain less than three fields (columns) will produce a task error and no table will be created or populated.

Importing Local Pass-through Authorization Entries

To import entries from a CSV file into an existing table.

1. In the webUI, click the **Tasks** tab.
2. In the left navigation pane, click **SIP Setup > Import Local/Passthrough Auth Table**



3. Select the Local/Passthrough Auth Table into which you want to import entries.
4. Browse for the CSV file.
5. Click Apply.

To create a <u>new</u> table and import entries into it:

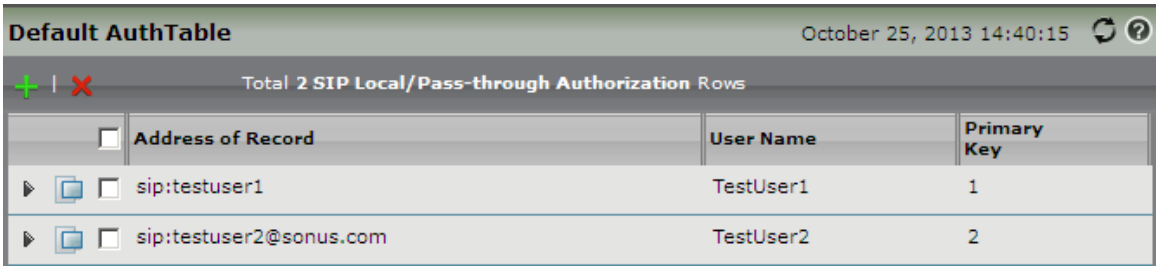
- Follow the instructions above, but select **Add New Table** from the Local/Passthrough Auth Table menu and add a name for the table in the Description field.

Verify The Import

To verify that the data was correctly imported:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Local Pass-thru Auth Tables**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Verify that the entries in the table match the entries from the CSV file.

Managing SIP Trunk Groups

> The SIP Trunk group applies to the SIP leg of the call only. This feature is available as part of the base license.

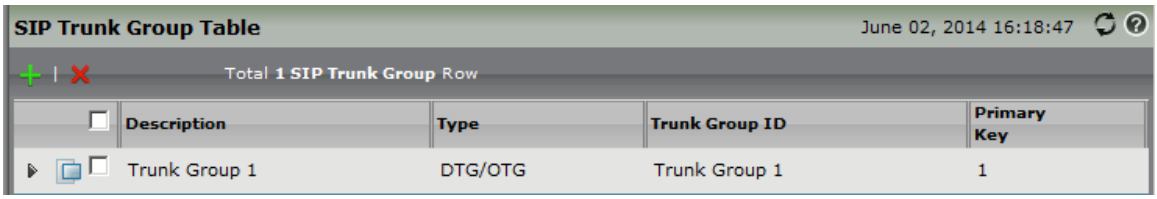
The SIP Trunk Group Table enables you to configure trunk groups in a profile that can be associated with specific SIP Signaling Groups. The SBC provides interoperaibility with different servers by transporting, identifying, and processing the trunk group (list of signaling groups) via enterprise trunking parameters. The trunk group helps provides a way to identify/choose the carrier at the gateway for a proxy or service provider.

Configuration for SIP Trunk groups consists of configuration in the following areas:

- Trunk Group Profiles (create/modify SIP Trunk Groups)
- Call Routing (configure Trunk Group as a destination type for a call route)
- Transformation (select destination Trunk Group ID for a call route)

Working with SIP Trunk Groups

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Trunk Groups.**



To view a SIP Trunk Group's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

> **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish to delete, then click the Delete ( ) icon located at the top of the window.

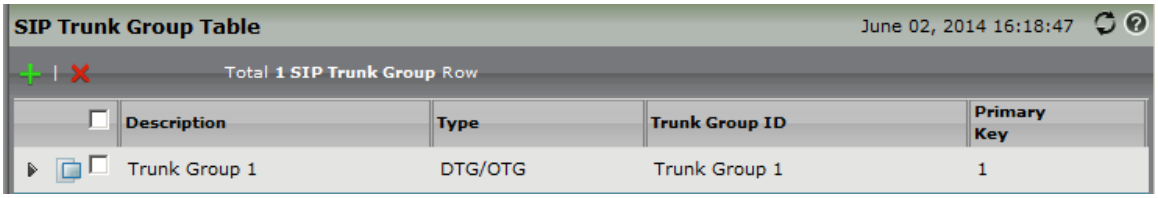
Creating and Modifying SIP Trunk Groups

Creating and Modifying SIP Trunk Groups

Copyright © 2015 Sonus Networks. All rights reserved.

To create or modify an existing SIP Trunk Group:

1. In the WebUI, click the **Settings** tab..
2. In the left navigation pane, go to **SIP >Trunk Groups.**

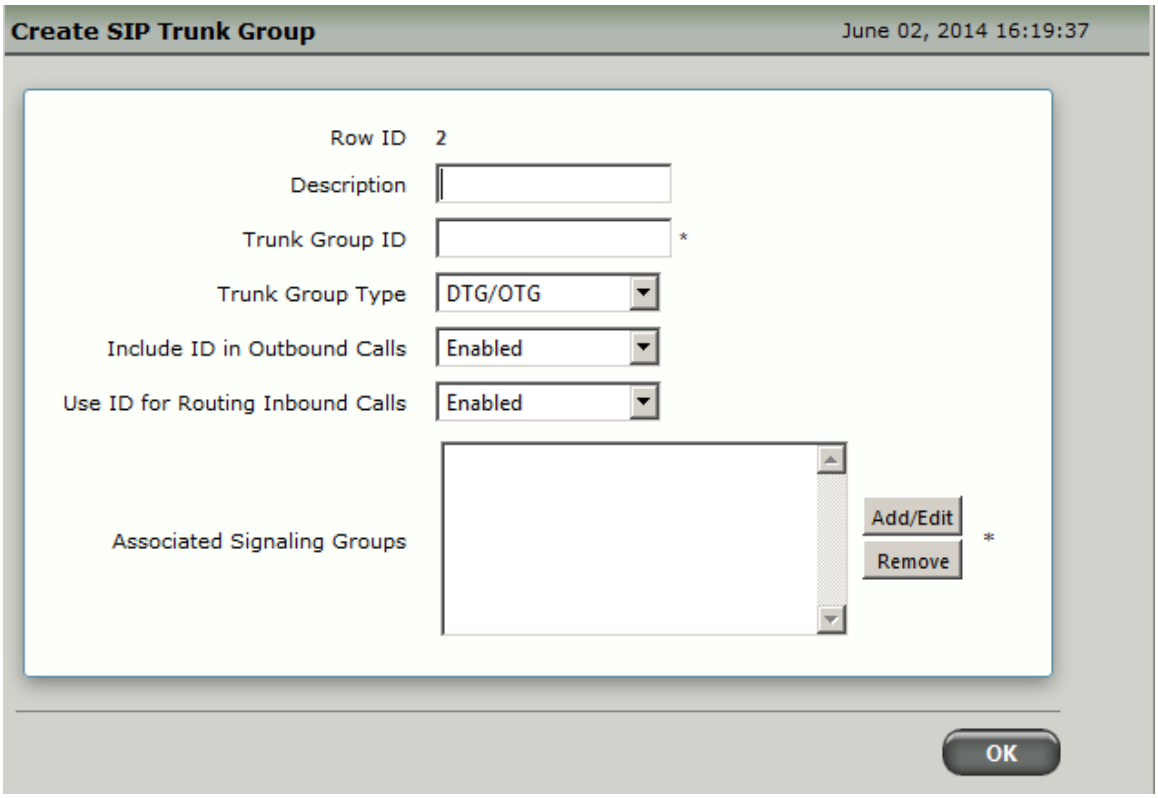


Modifying a SIP Trunk Group

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a SIP Trunk Group

1. Click the **Create SIP Trunk Group** ( ) icon at the top of the **SIP Trunk Group Table** page.
2. Enter the configuration options. See below for field definitions.



SIP Trunk Group Field Definitions

Description

Descriptive name for the SIP Trunk Group. Valid entry: up to 64 characters.

Trunk Group ID

The ID for the Trunk Group. Valid entry: up to 64 characters (i.e., TrunkGroupOne).

Copyright © 2015 Sonus Networks. All rights reserved.

Trunk Group Type

The type of Trunk Group. The selection determines whether the SBC uses **DTG/OTG** or **TGRP** as the Enterprise Trunking parameters used when handling SIP messages.Valid entries: **DTG/OTG** or **TGRP**.

DTG/OTG. DTG/OTG trunking parameters are used to handle SIP messages (i.e., INVITES). The DTG and OTG parameters are SIP URI parameters, as defined in RFC 3261.

TGRP. TGRP trunking parameters are used to handle SIP message (i.e., INVITES). The syntax of the TGRP and trunk-context parameters follows RFC 4904.

Default entry: **DTG/OTG.**

Include ID in Outbound Calls

Specifies whether the Trunk Group ID is included in calls originating from this Trunk Group. When enabled, depending on what is configured in the Trunk Group Type, this field used **OTG/DTG** or **TGRP**. Valid selection: **Enable** (Trunk Group ID is included in calls) or **Disable** (Trunk Group ID is not included in calls). Default entry: **Enable**.

Use ID for Routing Inbound Calls

Specifies whether the incoming Trunk Group ID is used when routing calls destined to this Trunk Group. When enabled, depending on what is configured in the Trunk Group Type, this field uses **OTG/DTG** or **TGRP**. Valid selection: **Enable** Trunk Group ID is used in routing calls destined to this Trunk Group) or **Disable** (Trunk Group ID is not used in routing calls destined to this Trunk Group). Default entry: **Enable**.

Associated Signaling Groups

Specifies the Signaling Groups that are associated with this trunk group. Through the selection panel, you can choose to Add/Edit/Remove a Signaling Group. The Signaling Groups available in the selection panel are taken from the Signaling Group table. See Creating and Modifying SIP Signaling Groups.



This field presents a multi-select widget.

To **Add/Edit** an entry, click the **Add/Entry** button.
Click here for more information about using the Multi-select widget.

To **Delete** an entry, click on the applicable entry and click **Remove**.

Miscellaneous SIP Information

This page provides miscellaneous information about how the SBC 1000/2000 implements the SIP protocol.

Supported SIP Methods

The following SIP methods are supported (declared in the allow header):

- INVITE
- UPDATE
- REFER
- NOTIFY
- SUBSCRIBE
- BYE

Copyright © 2015 Sonus Networks. All rights reserved.

- ACK
- PRACK

Working with Telephony Routing

In the Sonus SBC 1000/2000 system, all call routing occurs between **Signaling Groups**.

> *Signaling Groups are the logical representations of call-handling systems such as private branch extensions (PBX), Microsoft Lync 2010 Servers, fax machines and analog phones.*

In order to route any call to or from a call system connected to Sonus SBC 1000/2000, you must first configure a Signaling Group to represent that device or system. The following list illustrates the hierarchical relationships of the various Telephony routing components of a Sonus SBC 1000/2000 call system:

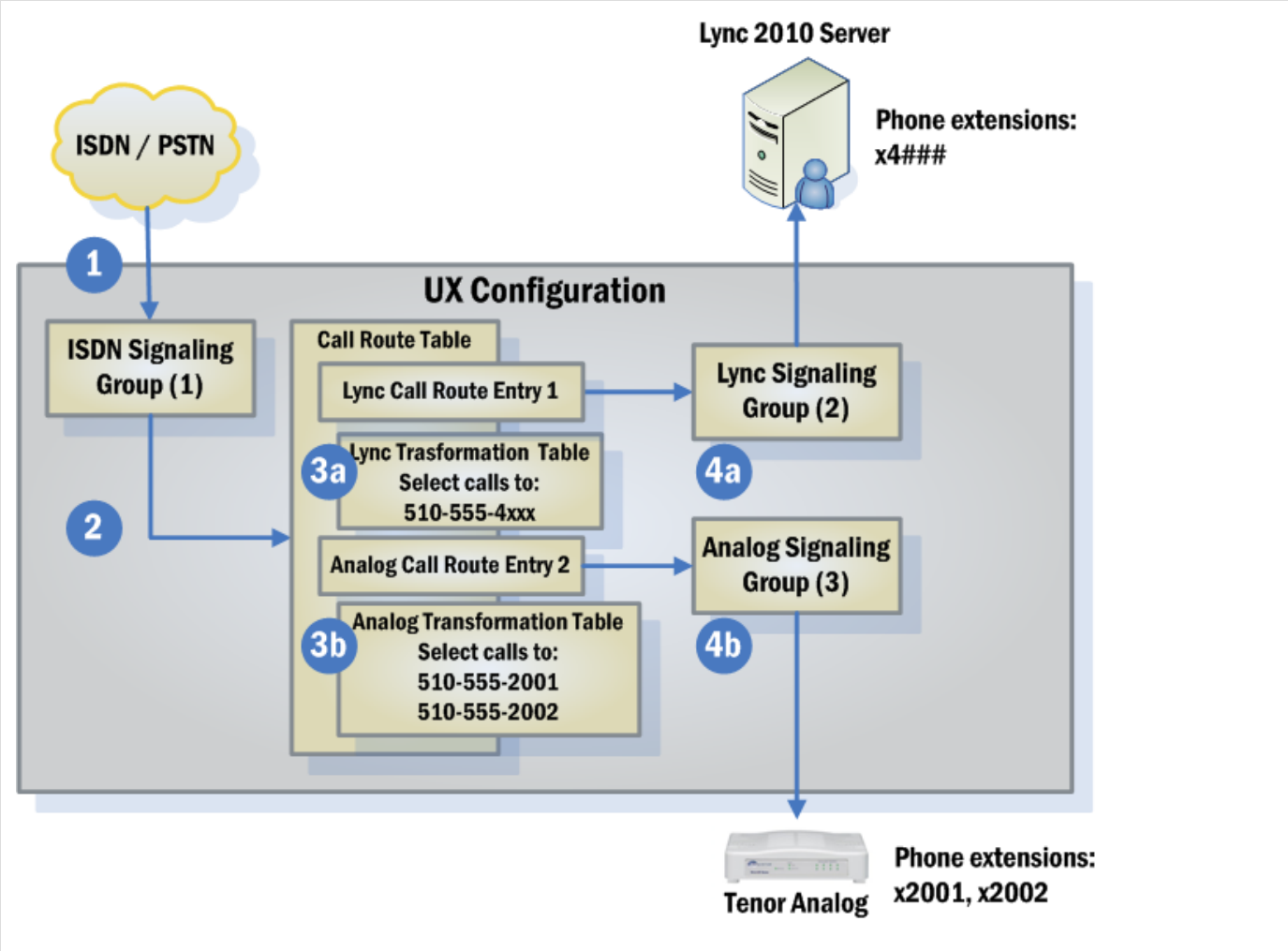
Signaling Group — describes the source call and points to a routing definition known as a Call Route Table
Call Route Table — contains one or more Call Route Entries
Call Route Entries points to the destination Signaling Group(s)

Each call routing entry describes how the call should be routed and also points to a Transformation Table which defines the conversion of names, numbers and other fields when routing a call.

Logic Path

The diagram below illustrates possible paths of a call from an external call from a ISDN PRI service line connected to the Sonus SBC 1000/2000 system to an internal Lync 2010 server or analog phone or fax devices connected to a Tenor Analog device.

Copyright © 2015 Sonus Networks. All rights reserved.



Sonus SBC 1000/2000 Call Logic Steps

1. An outside call comes through the ISDN PRI line connected to the Sonus SBC 1000/2000 system and is routed to the **ISDN Signaling Group**.
2. In order to route the call, the Sonus SBC 1000/2000 ISDN Signaling Group system engages the **Call Route Table** attached to it.
3. Sonus SBC 1000/2000 processes the **Call Route Table** entries and their attached **Transformation Table** entries, looking for a match to the called number.
    a. Sonus SBC 1000/2000 finds a match for a 4xxx local extension managed by a Lync 2010 Server.
    b. Sonus SBC 1000/2000 finds a match for a x2001 or x2002 local extension analog device, managed by a Tenor Analog system.
4. Sonus SBC 1000/2000 routes the call to the appropriate Signaling Group and the receiving system processes the call.

Related Topics

Managing Signaling Groups

Managing Call Routing Tables

- Call Forking Overview
- Creating and Modifying Entries to Call Routing Tables
- Viewing Call Routing Entry Counters

Copyright © 2015 Sonus Networks. All rights reserved.

Managing Transformation Tables

- Optional Matching Overview
- Creating and Modifying Entries to Transformation Tables
- Creating Call Routing Logic with Regular Expressions
  - Regular Expressions for Number Matching and Transformation
  - Understanding Regular Expressions

Managing Action Configurations

- Creating and Modifying Action Configurations

Managing Action Sets

- Creating and Modifying Entries to Action Set Tables

Routing Usage Examples

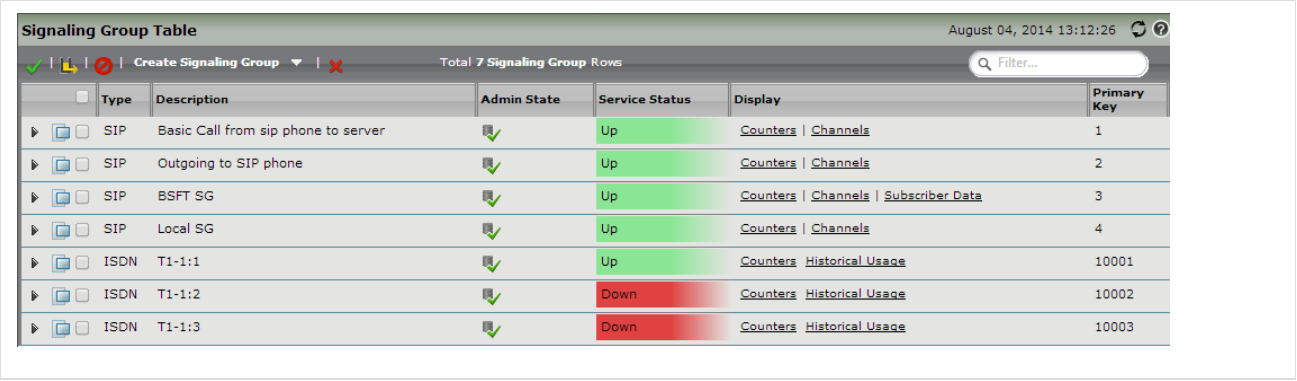
- SIP URI Manipulation
- Static Call Forking
- Dynamic Call Forking
- Call Routing for Active Directory Integration

Managing Signaling Groups

Signaling groups allow telephony channels to be grouped together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which Call Routes are selected. They are also the location from which Tone Tables and Action Sets are selected.

Working with Signaling Groups

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.



To view an Signaling Group's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Related Documents

Managing ISDN Signaling Groups

Copyright © 2015 Sonus Networks. All rights reserved.

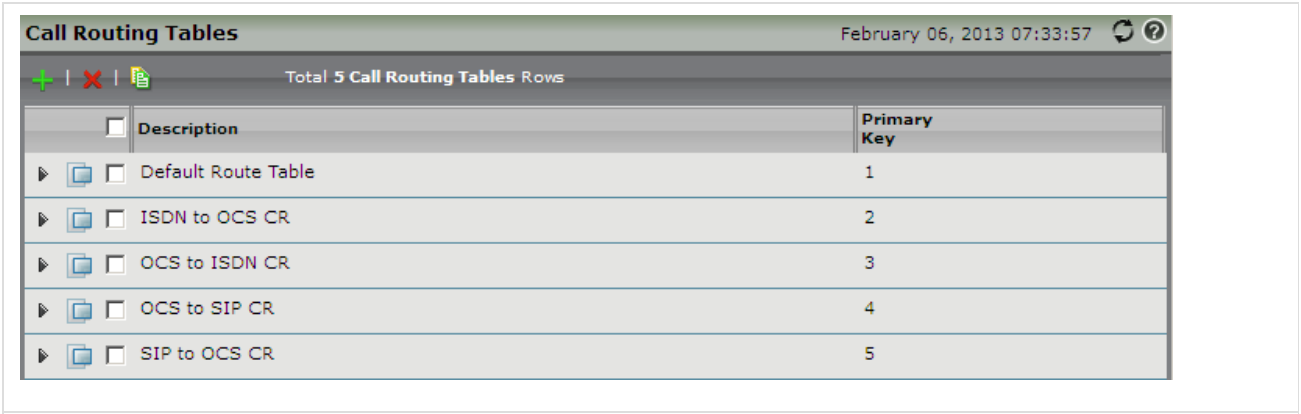
Managing SIP Signaling Groups
Managing CAS Signaling Groups

Managing Call Routing Tables

Call Routing allows calls to be carried between signalling groups, thus allowing calls to be carried between ports, and between protocols (like ISDN to SIP). Routes are defined by Call Routing Tables, which allow for flexible configuration of which calls are carried, and how they are translated. These tables are one of the central connection points of the system, linking Transformation Tables, Message Translations, Cause Code Reroute Tables, Media Lists and the three types of Signaling Groups (ISDN, SIP and CAS). For information on the Sonus SBC 1000/2000 call routing system as a whole, see Working with Telephony Routing.

Working with Call Routing Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table**.



To view a Call Routing Table's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

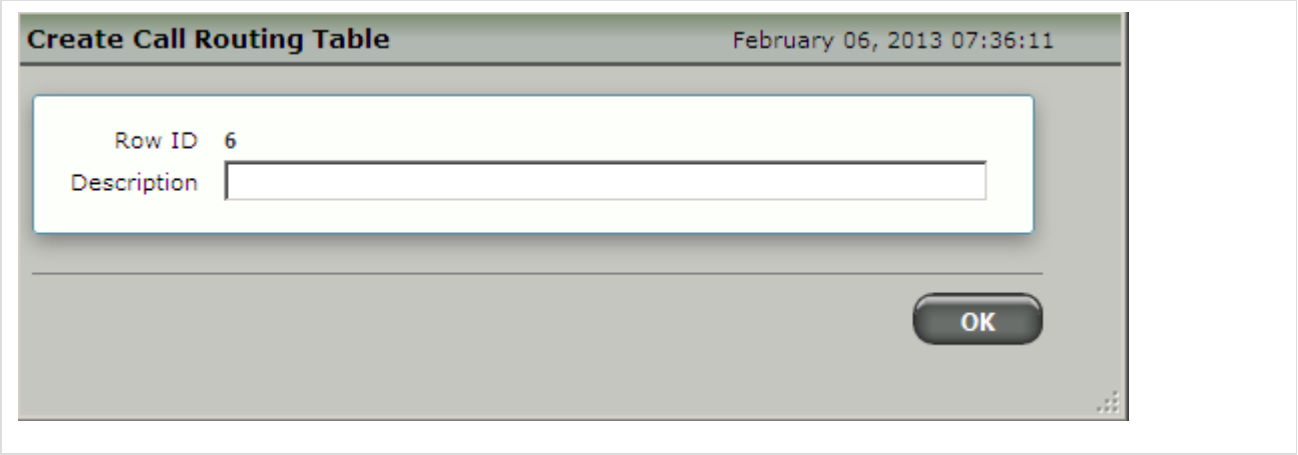
To modify a Message Translation Tables:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To create a Call Routing Table:

1. Click the **Add** ( ) icon at the top of the Call Routing Tables page.

Copyright © 2015 Sonus Networks. All rights reserved.



2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Call Forking Overview

Creating and Modifying Entries to Call Routing Tables

Viewing Call Routing Entry Counters

Call Forking Overview

Forking allows you to send a call to more than one Destination Signal Group simultaneously. This is useful for, for example, ringing a users' mobile phone and desk phone simultaneously.

We begin our discussion with no forking to help you understand how *normal* call flow occurs in a Call Routing Table, then we introduce the concept of forking.

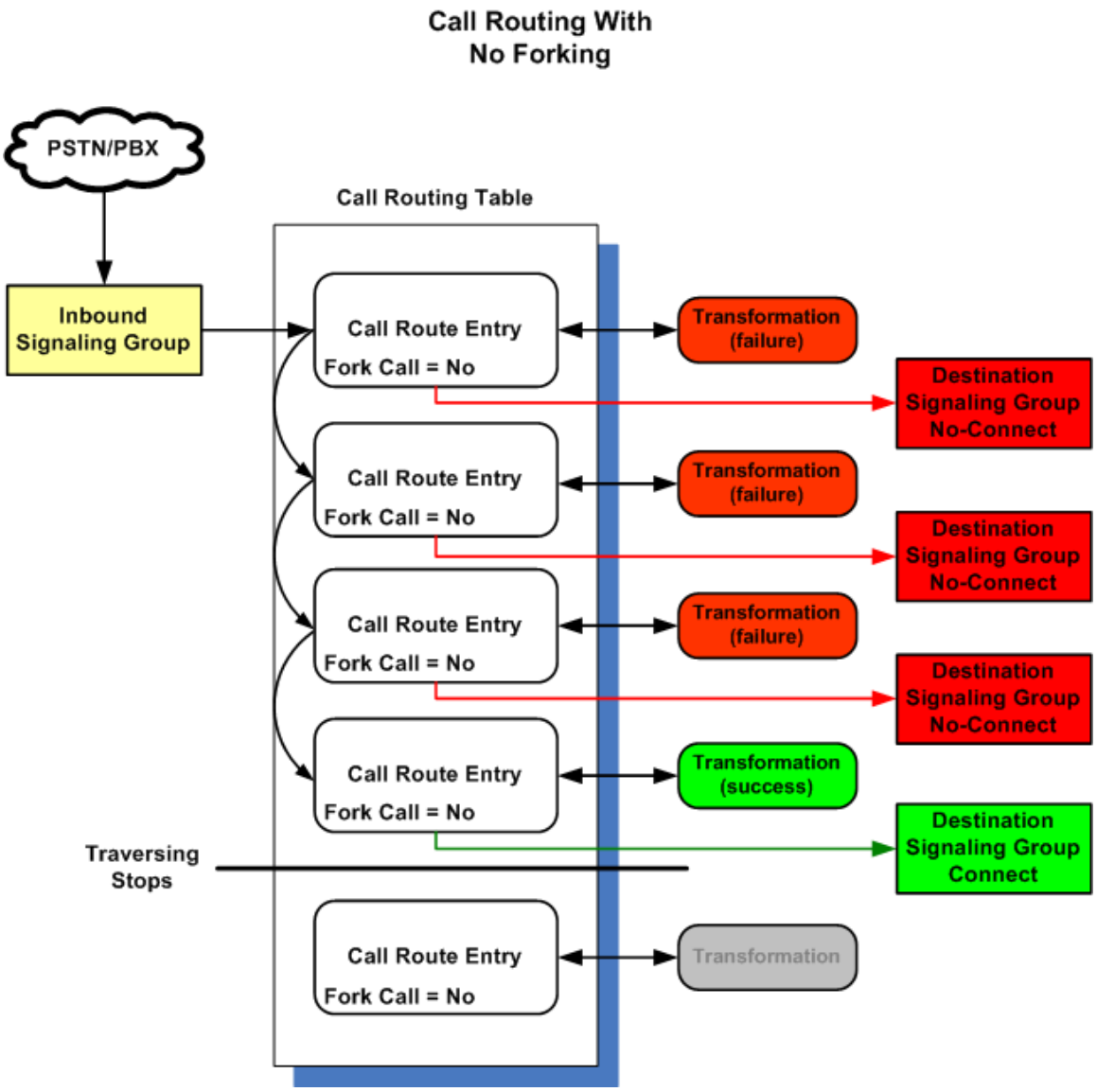
- Call Flow With No Forking
- Call Flow With Forking
  - Destination Information Panel
- More Information

Call Flow With No Forking

The call flow begins with an Inbound Signaling Group passing the call to a Call Routing Table (CRT). The routing table comprises one or more Call Route Entries (rows) that specify Transformation Tables where given aspects of the call are examined and matched, and then reported back to the Routing Table Entry as a success or failure.

Upon Success, the call is then routed to the Outbound Signaling Group as specified in the #Destination Information Panel of the Call Route Entry and no further routing is performed

Copyright © 2015 Sonus Networks. All rights reserved.

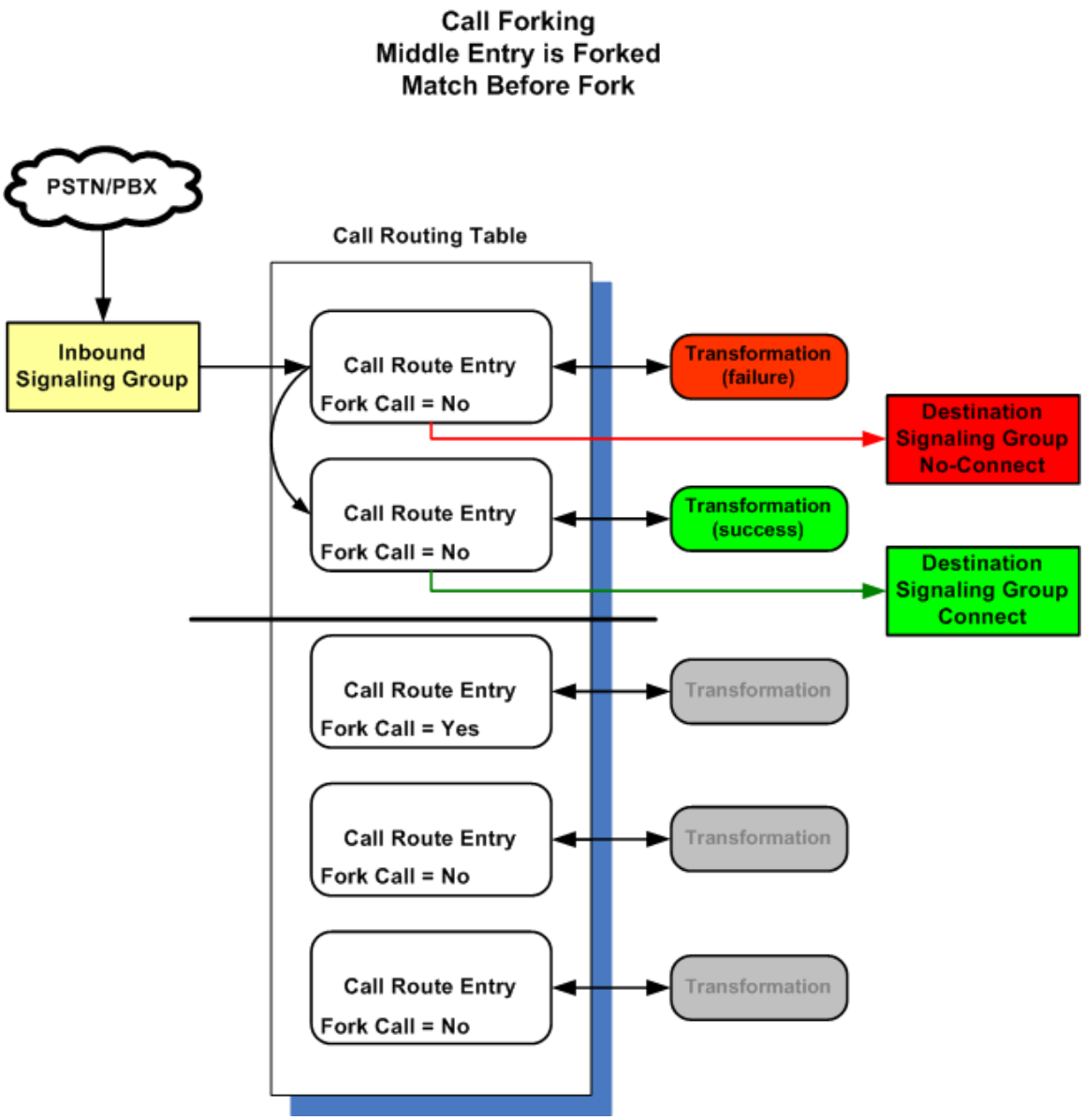


Call Flow With Forking

As with the example above, the call flow begins the same way with the call going to the CRT and the CRT passing the information to a Transformation Table and receiving a success or failure.

If a CRT entry is not forked and the transformation fails, the call is passed to the next element in the table and its associated transformation is tested. If the transformation is successful the call is sent to the destination Signaling Group and no further traversing of the table occurs.

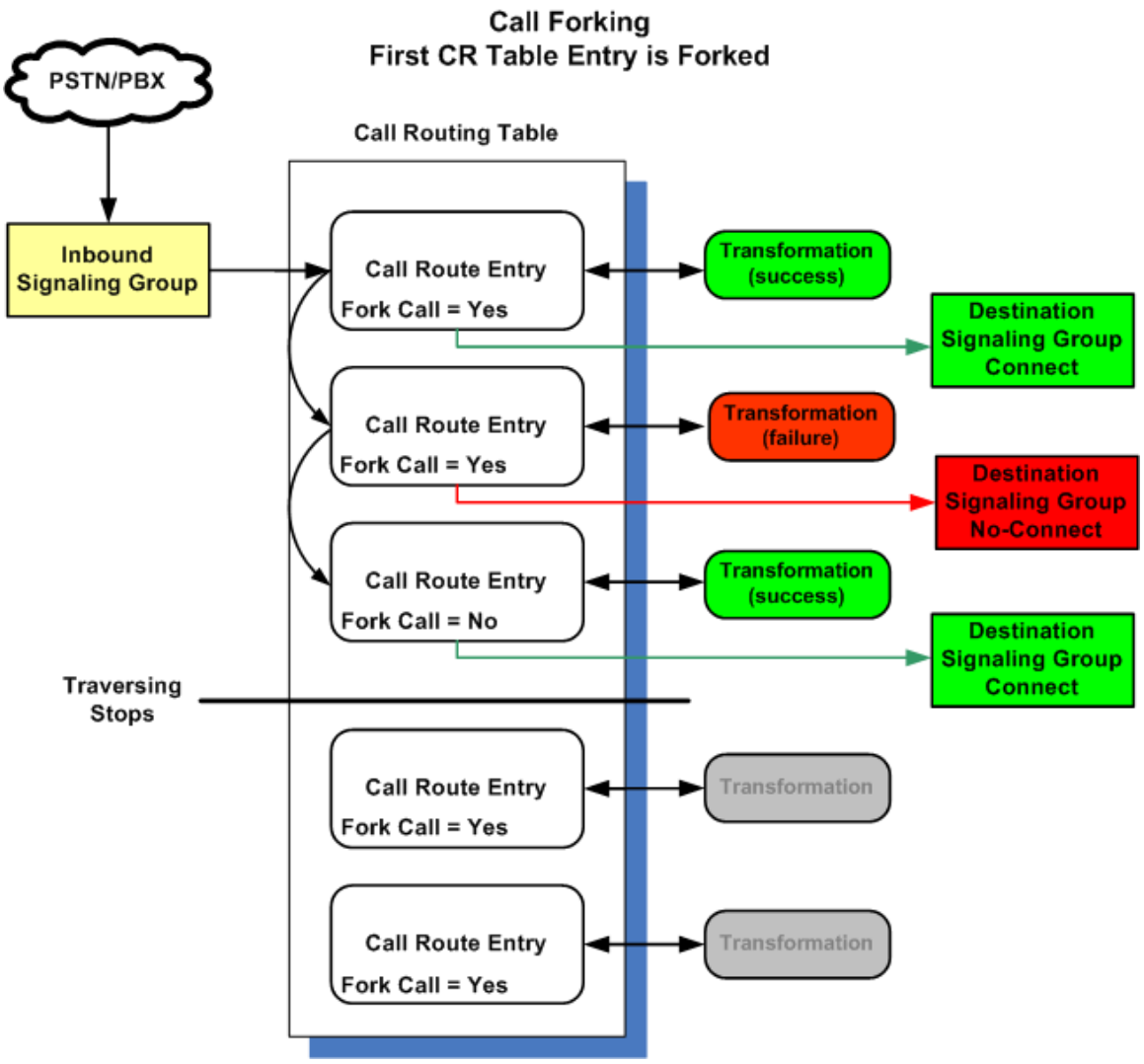
Copyright © 2015 Sonus Networks. All rights reserved.



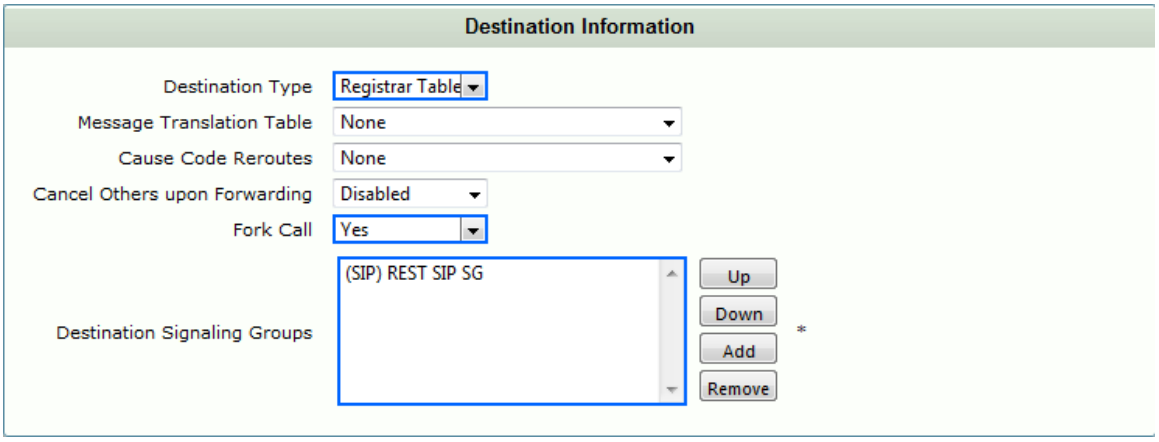
If a CRT entry **is forked** and the associated transformation fails, the call is passed to the next element in the table as above.

If that CRT entry is forked, whether or not its transformation fails, the call is passed to the next entry in the CRT. If that successive entry succeeds and it is **not** forked, the call is sent to the destination Signaling Group and no further traversing of the table occurs.

Copyright © 2015 Sonus Networks. All rights reserved.



Destination Information Panel



More Information

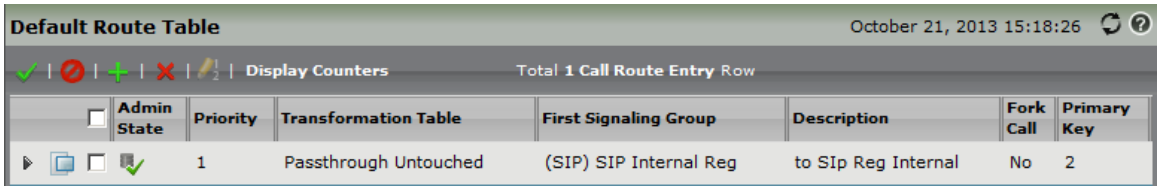
An incoming call may be forked up to 8 destinations.

Copyright © 2015 Sonus Networks. All rights reserved.

Creating and Modifying Entries to Call Routing Tables

To create or modify an Entry to a Call Routing Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table > Entry**.



Modifying an Entry to a Call Routing Table

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Resequencing an Entry in a Call Routing Table

1. Click the **Resequence** icon ( ) at the top of the table.
2. Select the row(s) you want to move.
3. Click the **Move Selected Rows Up** ( ) or **Move Selected Rows Down** ( ) icon to reposition the row(s) in the table.
4. Click **Apply**.

Enabling an Entry in a Call Routing Table

1. Select the check box next to the entry you wish to enable.
2. Click the **Enable** ( ) icon at the top of the table.

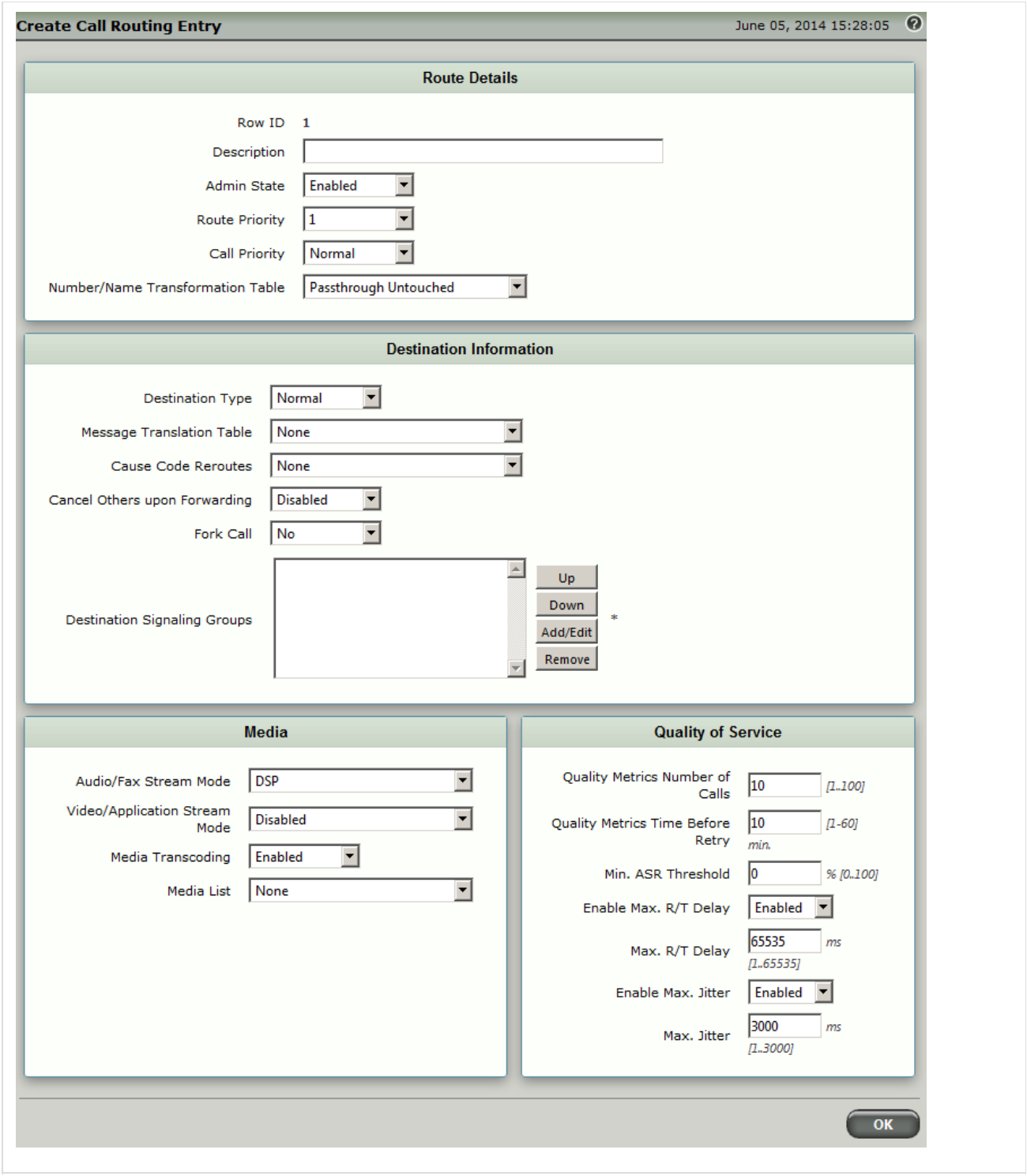
Disabling an Entry in a Call Routing Table

1. Select the check box next to the entry you wish to disable.
2. Click the **Disable** ( ) icon at the top of the table.

Creating an Entry to a Call Routing Table

1. Click the **Create Routing Entry** ( ) icon.

Copyright © 2015 Sonus Networks. All rights reserved.



Call Routing Entry - Field Definitions

Admin State

Specifies the admin state of the Call Route. Valid entry: **Enable** (enables the call route entry for routing the call, displays in configuration header as) or **Disable** (disables the call route entry from being used, displays in the configuration header as).

Copyright © 2015 Sonus Networks. All rights reserved.

Route Priority

Priority of the route from 1 (highest) to 10 (lowest).

Higher priority routes are matched against before lower priority routes regardless of the order of the routes in the table.

Call Priority

Call Priority is used for emergency (911) calls in the U.S. and other countries. This field is used if the Priority header is **not** received in the ingress SIP INVITE and for PSTN interfaces. The default value is Normal. When integrating with E911 providers, Priority may have to be set to Emergency.

Number/Name Transformation Table

Specifies the Transformation Table to be used for this routing entry. This drop down list is populated from the entries in the Transformation Table.

Destination Type

Specifies the destination type for calls using this route. Valid selections: **Normal**, **Registrar Table**, **Deny**, or **Trunk Group.**

Normal. Call routes to normal types such as ISDN or SIP signaling groups. Specify a list of signaling groups through Destination Signaling Groups.

Registrar Table. Call routes to a signaling group that contains the registrar table.

Deny. Call routes to a specific Q.850 cause code are rejected. Through the Deny Q.850 Cause Code field, select the specific Q.850 Cause code. When **Deny** is selected, the Deny Q.850 Cause Code field is displayed.

Trunk Group. Calls are routed to an incoming trunk group destination using the associated signaling group. This routing entry should be selected in order to route calls to a trunk group. When **Trunk Group** is selected, **Fork Call** and **Destination Signaling Groups** options are not available.

Deny Q.850 Cause Code

Specifies the Q.850 Cause Code for which the call is rejected. Select from the drop down list. This field is displayed only when **Deny** is selected as Destination Type.

Message Translation Table

Specifies which Message Translation Table to use.

Cause Code Reroutes

Specifies which Cause Code Reroute table to use.

Cancel Others upon Forwarding

Specifies whether or not forked calls should clear when one of the forked calls is forwarded.

Copyright © 2015 Sonus Networks. All rights reserved.

Fork Call

Specifies whether or not to fork a call if this route is selected

Destination Signaling Groups

Specifies the Signaling Groups used as the destination of calls.

> **Helpful Hint**
>
> This field presents a multi-select widget when the **Add/Edit** button is clicked.
> Click here for more information about using the Multi-select widget.

Audio/Fax Stream Mode

Copyright © 2015 Sonus Networks. All rights reserved.

Quick Start: How to Choose Media Mode

- To use DSP resources, (due to transcoding, Lync interoperability, etc.) select **DSP** mode.
- For SIP-to-SIP calls using Proxy, select **Proxy** mode.
- To use the same call routes where the inbound call route could be both TDM/SIP, select **Proxy preferred over DSP.**
- To use DSP resources, rather than proxy or switch media stream between endpoints, use **DSP preferred over Proxy.**

Media Mode enables you to choose how the SBC handles call signaling and Audio/Fax media stream during a call. Five options are available:

DSP (default entry). The SBC uses DSP resources for media handling (transcoding) but it does not facilitate the capabilities/features between endpoints that are not supported within the SBC (codec/capability mismatch). When **DSP** is configured, the Signaling Groups enabled to support **DSP** are attempted in order. To enable a Signaling Group for DSP mode, see Creating and Modifying SIP Signaling Groups.

Proxy. The SBC will proxy or switch the media stream between endpoints and let the endpoints negotiate common media capabilities and handle unsupported/unknown audio codecs. The media flows through the SBC without using DSP resources. For example, this mode is used when both inbound and outbound calls are SIP and both Signaling Groups are enabled for Proxy mode. If one Signaling Group has Proxy mode disabled or one of the inbound Signaling Groups is TDM, the call is rejected. Route configuration does not allow Destination Signaling Groups of TDM type if Stream Mode is set to Proxy. The failover mechanism can then be used to re-route to another Signaling Group. **We strongly recommend using Proxy preferred over DSP mode** since it allows the same routing entry with different Signaling Groups.

DSP preferred over Proxy. The SBC prefers to use DSP resources, rather than proxy or switch the media stream between endpoints. This mode is chosen during the call setup based on the call routing, and used for call routes where the inbound call route is both TDM and/or SIP (this avoids duplicate call routes). If the inbound Signaling Group is a SIP Signaling Group not enabled for DSP, then **Proxy** is used.

Proxy preferred over DSP. The SBC prefers to proxy the media stream between endpoints rather than choosing DSP mode (which uses the DSP resource). This mode is chosen during the call setup based on the call routing result, and used for call routes where the inbound call route is both TDM and/or SIP (this avoids duplicate call routes). If the inbound or outbound Signaling Group is NOT in Proxy mode (either SIP signaling group is not enabled for Proxy mode or Signaling Group is TDM), then DSP is used.

Disabled. The Audio/Fax media selection process is disabled. When **Disabled** is selected, the SBC will reject incoming Audio/Fax streams.

Video/Application Stream Mode

Copyright © 2015 Sonus Networks. All rights reserved.

Media Mode enables you to choose how the SBC handles call signaling and Video/Application media stream during a call.

Proxy. The SBC will proxy the media stream between endpoints. The media flows through the SBC without requiring DSP resources. For example, this mode is used when an inbound SIP call includes Video/Application streams and both inbound and outbound SIP Signaling Groups are enabled for Proxy mode. If one Signaling Group has Proxy mode disabled, the stream is disabled. If the outbound Signaling Group is TDM, the call will be connected using Audio/Fax media only and Video/Application media stream will be rejected.

Disabled. The Video/Application Stream Mode is disabled. The SBC will **not** proxy or switch media stream between endpoints.

Media Transcoding

Specifies whether or not to use media transcoding.

Media Transcoding requires a specific Transcoding License. Do not enable Media Transcoding unless your calling configuration requires it and Sonus SBC 1000/2000 is licensed for the Transcoding feature.

- If Media Transcoding is enabled without a Transcoding license, a critical alarm is generated regardless of whether or not the routed calls require transcoding.
- Transcoding must be enabled on SIP-to-SIP calls.

Media List

Specifies the Media List to use for this call route. This drop down list is populated with the Media List entries created through the Create Media list option. See Creating and Modifying Media Lists.

Quality Metrics Number of Calls

Specifies the number of calls over which the quality metrics are calculated.

Quality Metrics Time Before Retry

Specifies the period of time in minutes after which a route is tried again after failing quality metrics.

Min. ASR Threshold

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the minimum answer/seizure ratio for this rule to be considered for use.

Click here to read more about Answer Seizure Ratio.
The ASR is a measure of network quality defined by the ITU. The answer/seizure ratio (ASR) is a measurement of network quality and call success rate in telecommunications. It is the percentage of answered telephone calls with respect to the total call volume.

The answer/seizure ratio is defined as 100 times the ratio of sucessfully answered calls divided by the total number of call attempts (seizures).

Busy signals and other rejections by the called number count as call failures. This makes the ASR highly dependent on end-user action or behavior and is out of control by the telecommunications carrier. Low ASR values may be caused by far-end switch congestion, not answering by called parties and busy destination lines.

Enable Max. R/T Delay

Specifies whether or not to use Round Trip Delay

Click here to read more about Round Trip Delay.
In telecommunications, the round-trip delay time (RTD) or round-trip time (RTT) is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received. This time delay therefore consists of the transmission times between the two points of a signal.

The RTT was originally estimated in TCP by: RTT = (? - Old_RTT) + ((1 ? ?) - New_Round_Trip_Sample
Where ? is constant weighting factor(0 ? ? < 1). Choosing a value ? close to 1 makes the weighted average immune to changes that last a short time (e.g., a single segment that encounters long delay). Choosing a value for ? close to 0 makes the weighted average respond to changes in delay very quickly.

This was improved by the Jacobson/Karels algorithm, which takes standard deviation into account as well. Once a new RTT is calculated, it is entered into the equation above to obtain an average RTT for that connection, and the procedure continues for every new calculation.

Max. R/T Delay

Specifies the maximum average round trip (R/T) delay for this rule to be considered for use.

Enable Max. Jitter

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies whether or not Jitter will be considered as a quality metric for this Call Route.

Click here to read more about Jitter metrics.

Jitter is the undesired deviation from true periodicity of an assumed periodic signal in electronics and telecommunications, often in relation to a reference clock source. Jitter may be observed in characteristics such as the frequency of successive pulses, the signal amplitude, or phase of periodic signals. Jitter is a significant, and usually undesired, factor in the design of almost all communications links (e.g., USB, PCI-e, SATA, OC-48).

Jitter can be quantified in the same terms as all time-varying signals, e.g., RMS, or peak-to-peak displacement. Also like other time-varying signals, jitter can be expressed in terms of spectral density (frequency content).

Jitter period is the interval between two times of maximum effect (or minimum effect) of a signal characteristic that varies regularly with time. Jitter frequency, the more commonly quoted figure, is its inverse. ITU-T G.810 classifies jitter frequencies below 10 Hz as wander and frequencies at or above 10 Hz as jitter.

Jitter may be caused by electromagnetic interference (EMI) and crosstalk with carriers of other signals. Jitter can cause a display monitor to flicker, affect the performance of processors in personal computers, introduce clicks or other undesired effects in audio signals, and loss of transmitted data between network devices. The amount of tolerable jitter depends on the affected application.

Max. Jitter

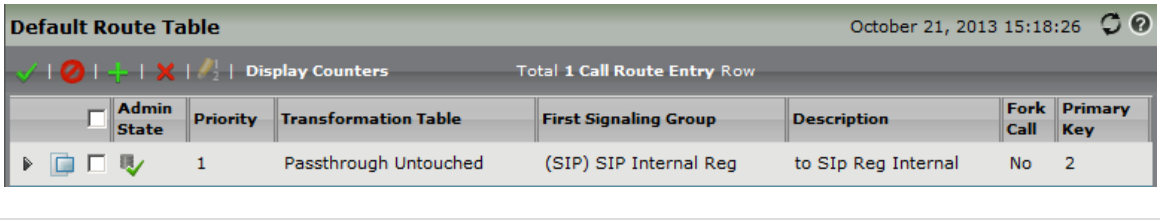
Specifies the maximum average jitter for this rule to be considered for use.

Viewing Call Routing Entry Counters

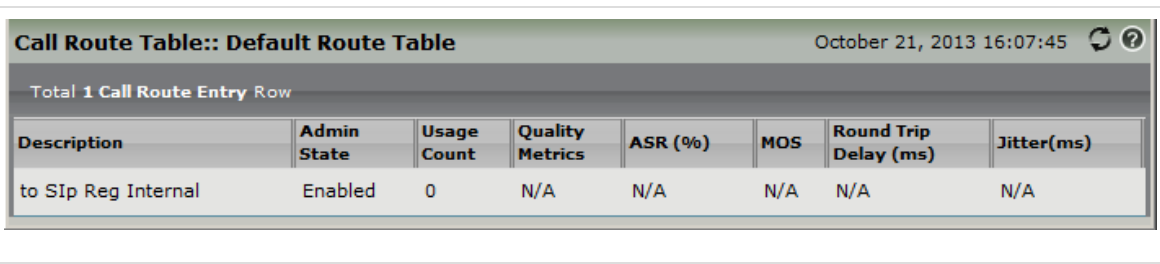
Route Entry counters display statistics about how Call Route Entries are performing and call quality.

To add or modify an Entry to a Call Routing Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table > Entry**.



3. Click the **Display Counters**text at the top of the panel.



Call Route Entry Counters - Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

Description

The description of the Call Route Entry as is appears in its parent Call Route Table.

Admin State

Indicates whether or not the entry is in an Enabled or Disabled State. For information about enabling and disabling entries, see Adding and Modifying Entries to Call Routing Tables.

Usage Count

Displays a count of how many times this route has been used.

Quality Metrics

Displays the average call quality for this call route.

ASR

Displays the Answer/Seizure Ratio for this call route.

The ASR is a measure of network quality defined by the ITU. The answer/seizure ratio (ASR) is a measurement of network quality and call success rate in telecommunications. It is the percentage of answered telephone calls with respect to the total call volume.

The answer/seizure ratio is defined as 100 times the ratio of sucessfully answered calls divided by the total number of call attempts (seizures).

Busy signals and other rejections by the called number count as call failures. This makes the ASR highly dependent on end-user action or behavior and is out of control by the telecommunications carrier. Low ASR values may be caused by far-end switch congestion, not answering by called parties and busy destination lines.

MOS

Copyright © 2015 Sonus Networks. All rights reserved.

Displays the Mean Opinion Score for this call route.

Click here to read more about MOS Scores.

The Mean Opinion Score (MOS) is used in telephony networks to obtain the human user's view of the quality of the network. In multimedia (audio, voice telephony, or video) especially when codecs are used to compress the bandwidth requirement (for example, of a digitized voice connection from the standard 64 kilobit/second PCM modulation), the mean opinion score (MOS) provides a numerical indication of the perceived quality from the users' perspective of received media after compression and/or transmission. The MOS is expressed as a single number in the range 1 to 5, where 1 is lowest perceived audio quality, and 5 is the highest perceived audio quality measurement.

MOS tests for voice are specified by ITU-T recommendation P.800.

The MOS is generated by averaging the results of a set of standard, subjective tests where a number of listeners rate the heard audio quality of test sentences read aloud by both male and female speakers over the communications medium being tested. A listener is required to give each sentence a rating using the following rating scheme:

MOS	Quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

The MOS is the arithmetic mean of all the individual scores, and can range from 1 (worst) to 5 (best).

Round Trip Delay

Ddisplays the average round trip delay for this call route.

In telecommunications, the round-trip delay time (RTD) or round-trip time (RTT) is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received. This time delay therefore consists of the transmission times between the two points of a signal.

Jitter(ms)

Copyright © 2015 Sonus Networks. All rights reserved.

Displays the average jitter for this call route.

Click here to read more about Jitter metrics.
Jitter is the undesired deviation from true periodicity of an assumed periodic signal in electronics and telecommunications, often in relation to a reference clock source. Jitter may be observed in characteristics such as the frequency of successive pulses, the signal amplitude, or phase of periodic signals. Jitter is a significant, and usually undesired, factor in the design of almost all communications links (e.g., USB, PCI-e, SATA, OC-48).

Jitter can be quantified in the same terms as all time-varying signals, e.g., RMS, or peak-to-peak displacement. Also like other time-varying signals, jitter can be expressed in terms of spectral density (frequency content).

Jitter period is the interval between two times of maximum effect (or minimum effect) of a signal characteristic that varies regularly with time. Jitter frequency, the more commonly quoted figure, is its inverse. ITU-T G.810 classifies jitter frequencies below 10 Hz as wander and frequencies at or above 10 Hz as jitter.

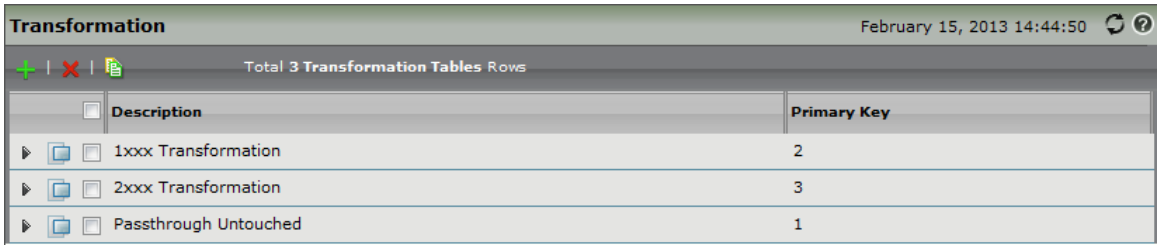
Jitter may be caused by electromagnetic interference (EMI) and crosstalk with carriers of other signals. Jitter can cause a display monitor to flicker, affect the performance of processors in personal computers, introduce clicks or other undesired effects in audio signals, and loss of transmitted data between network devices. The amount of tolerable jitter depends on the affected application.

Managing Transformation Tables

Transformation Tables facilitate the conversion of names, numbers and other fields when routing a call. They can, for example, convert a public PSTN number into a private extension number, or into a SIP address (URI). Every entry in a Call Routing Table requires a Transformation Table, and they are selected from there. In addition, Transformation tables will be configurable as a reusable pool that Action Sets can reference.

Working with Transformation Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Transformation**.



To view a Transformation Table's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

To modify a Transformation Table:

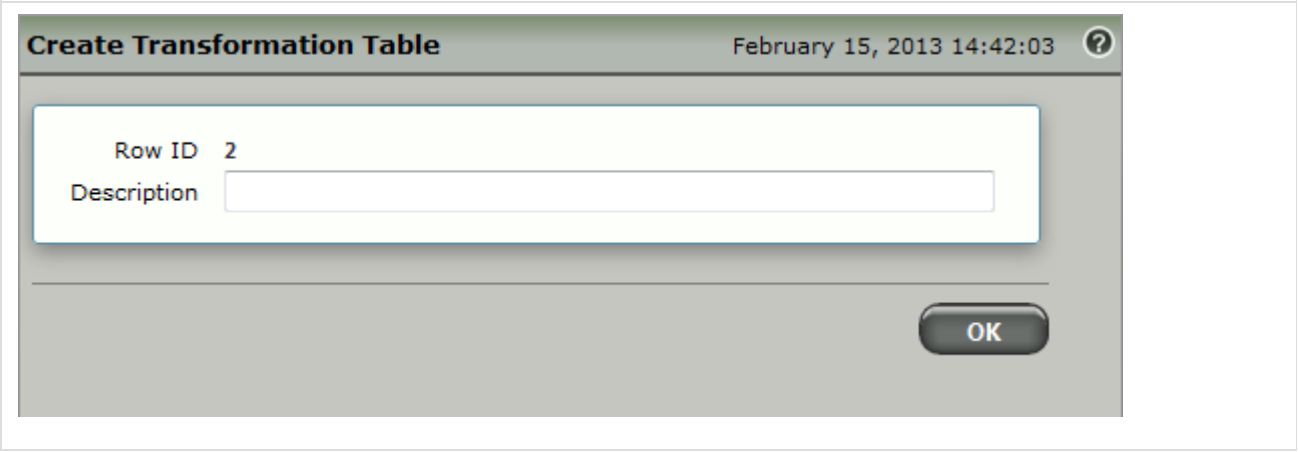
1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired

Copyright © 2015 Sonus Networks. All rights reserved.

3. Click **OK**.

To create a Transformation Table:

1. Click the **Create** ( ) icon.



2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Optional Matching Overview

Creating and Modifying Entries to Transformation Tables

Creating Call Routing Logic with Regular Expressions

- Regular Expressions for Number Matching and Transformation
- Understanding Regular Expressions

Optional Matching Overview

Optional Matching Rules

The rules for Optional Matching are very straightforward, but can be a little difficult to understand without some basic explanation. In this article, we provide you with several scenarios to illustrate how these simple rules can be applied.

An Optional Transformation is exactly that, optional. But remember that it is the **entry** in the Transformation Table which is optional and not the table itself. This means that the entry doesn't have to produce a match for the table to return a success, as long as some combination of entries match.

- **Rule 1: All** mandatory entries **must** match.
- **Rule 2:** For Optional Matching entries, **at least one** of each Input Field Type **must** match.
- **Multiple Matches:** When multiple input fields **of the same type** are matched, the output field of the **last to be matched** (i.e, the bottom most of that input type in the list) is the output which is passed upon success.

Scenario One - Uncommon

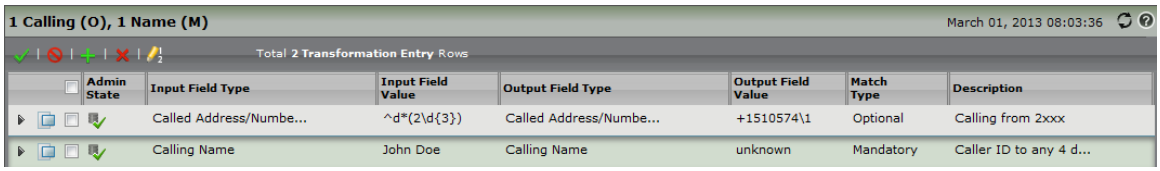
In this example we have a single optional entry and a single mandatory entry.

Copyright © 2015 Sonus Networks. All rights reserved.

While valid, a common use case should never have only one optional and one mandatory entry in a rule since having only one optional entry in a rule will always be considered mandatory.

For this transformation to produce a success, the first line *Calling from 2xxx* must match, **and** the second entry *Caller ID to any 4 digit ext* **must** match.

Given: A call is place to a number who's last four digits are between *2000 and 2999* (inclusive), the caller's name is *John Doe*, the transformation is a success with an output that appends the last four digits of the Called Number to *+1510574* and changes the Calling Name to *Unknown*.



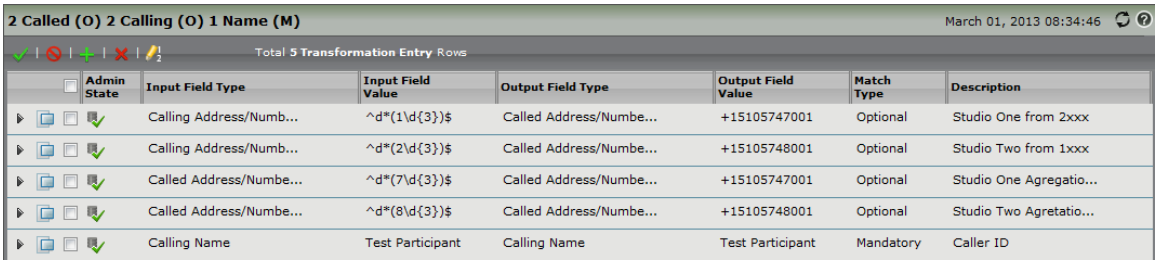
Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
	Called Address/Numbe...	^d*(2\d{3})	Called Address/Numbe...	+1510574\1	Optional	Calling from 2xxx
	Calling Name	John Doe	Calling Name	unknown	Mandatory	Caller ID to any 4 d...

Scenario Two - Common

In this example we have five entries, two optional with Input Field Types of Calling Address/Number, two optional with Called Address/Number, and mandatory with Calling Name as the Input Field Type.

At least **one each** of the Calling Address/Number and Called Address/Number must match, **and** the Calling Name input must match.

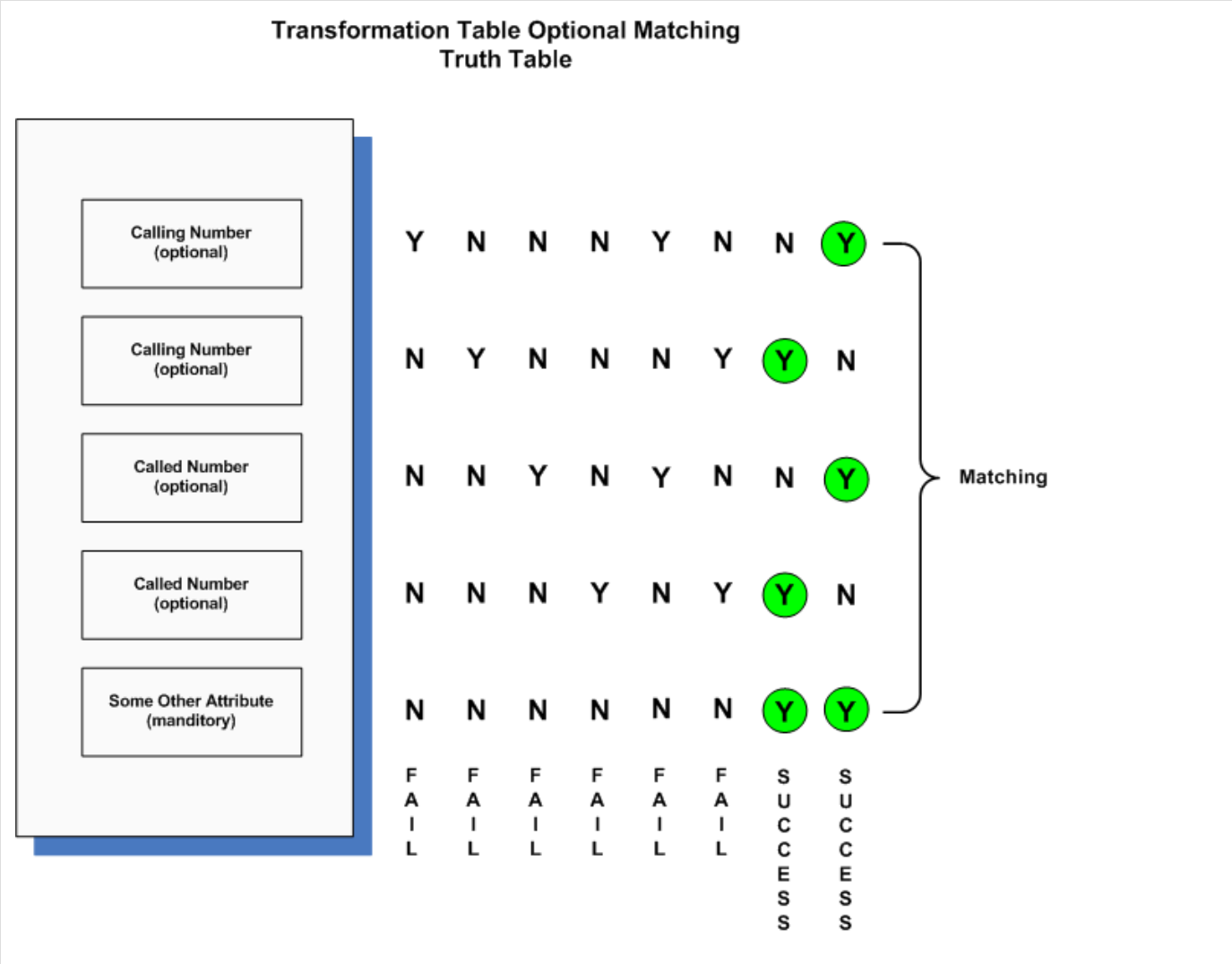
Given: The Calling Number is a number where the last four digits are *1nnn* **or** *2nnn*, and the last four digits of the Called number are either *7nnn* **or** *8nnn*, **and** the Calling Name is *Test Participan*t, transformation is successful.



Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
	Calling Address/Numb...	^d*(1\d{3})$	Called Address/Numbe...	+15105747001	Optional	Studio One from 2xxx
	Calling Address/Numb...	^d*(2\d{3})$	Called Address/Numbe...	+15105748001	Optional	Studio Two from 1xxx
	Called Address/Numbe...	^d*(7\d{3})$	Called Address/Numbe...	+15105747001	Optional	Studio One Agregatio...
	Called Address/Numbe...	^d*(8\d{3})$	Called Address/Numbe...	+15105748001	Optional	Studio Two Agretatio...
	Calling Name	Test Participant	Calling Name	Test Participant	Mandatory	Caller ID

The following truth table illustrates the second scenario:

Copyright © 2015 Sonus Networks. All rights reserved.



Creating and Modifying Entries to Transformation Tables

Each Transformation Table contains a list of entries considered as routing rules to execute on. Each rule is executed **in order until the end of the table is reached OR when a Mandatory entry fails to execute**.

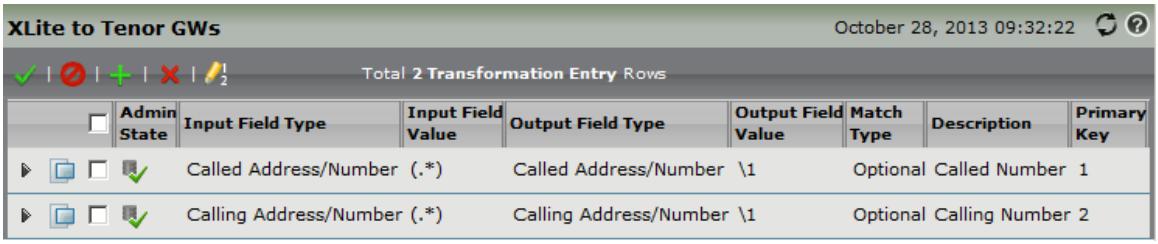
A Transformation Entry would be classified as failing to execute if:

- Any input field in in the row that has 'Match Type' set to 'Mandatory' does not match.
- All input fields of the same type, e.g. 'Called Number', having 'Match Type' set to 'Optional' don't match.
- The output field value is on non present Active Directory field.

To create or modify an Entry to a Transformation Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Transformation > Entry**.

Copyright © 2015 Sonus Networks. All rights reserved.



Modifying an Entry to a Message Transformation Table

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Resequencing an Entry in a Message Transformation Table

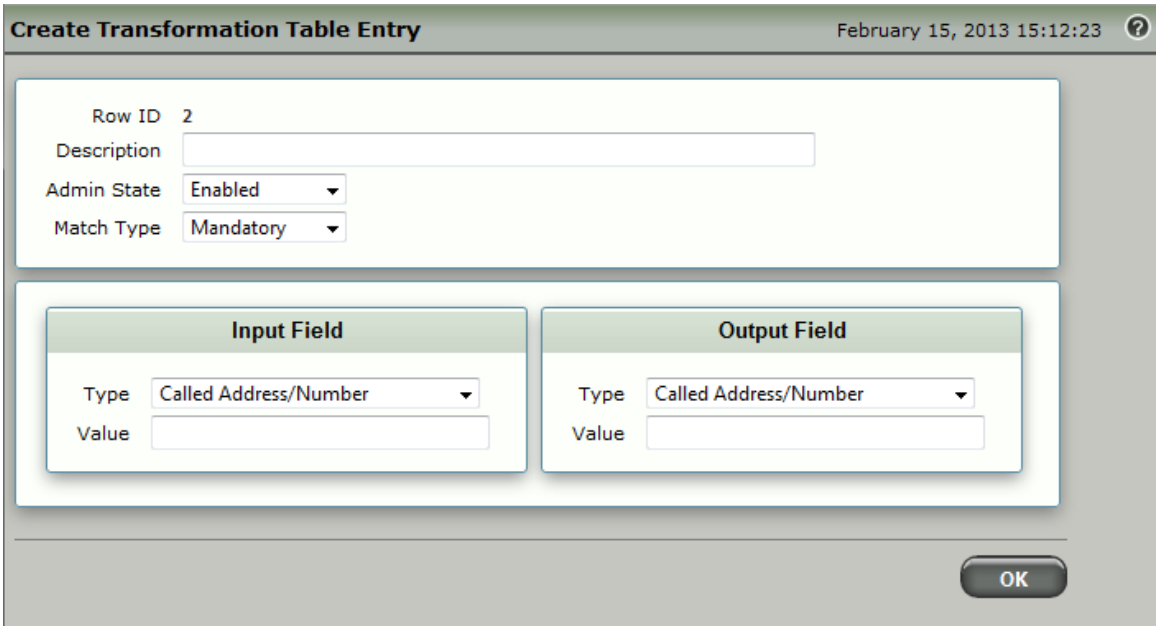
1. Click the **Resequence** icon ( ) at the top of the table.
2. Select the row(s) you want to move.
3. Click the **Move Selected Rows Up** ( ) or **Move Selected Rows Down** ( ) icon to reposition the row(s) in the table.
4. Click **Apply**.

Disabling an Entry in a Message Transformation Table

1. Click the **expand** ( ) Icon next to the entry you wish to disable.
2. In the **Admin State** list, click **Disabled**.

Creating an Entry to a Message Transformation Table

1. Click the **Create** ( ) icon.



Transformation Table Entry - Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

Admin State

Allows the transformation to be ignored, as if it did not exist, when **Disabled**. The default state is **Enabled**.

Match Type

Specifies whether or not this Translation Table Entry must be matched.

▼ **Click here to read more about mandatory matching.**
Mandatory entries must match, Optional entries must match at least one of that Input Field type. For more information see the Optional Matching Overview page.

Type (Input/Output)

Specifies the type of field to match against.

▼ **Click here to review the available Type values and their definitions**

Input /Output Fields are currently as follows

Field	ISDN Type	SIP Type	Description	Options	Special Notes
Callback Pool Identifier	None	None	Sets the Emergency Callback Numbers Table to be used for calls destined to 911.	Passthrough ELIN Number	The Input Field can be set to the public emergency number (like 911) or any other emergency number. Passthrough Elin Number enables the SBC to use the Elin number in the NAM field of an incoming SIP invite message. The Elin number from the "CompanyName" field configured in Lync location services is used as the authoritative callback number for outgoing E911 calls and is always preferred. In the Create Transformation Table Entry box, use the following configuration: • Input Field Type**: ELIN Identifier** • Output Field Type: **Callback Pool Identifier** • Output Field Value: **Passthrough Elin Number**
Called Address/Number	DNIS (ISDN IE 0x70)	Request URI	The called number	None	
Called Extension	None	Request URI	Sets the ;ext=	None	To: tel:2222<sip:2222;ext=2222@192.168.1.20>
Called Numbering Type	ISDN IE 0x70		Describes the *format* of the called number. Aids the receiving switch in understanding if this is a SIP or ISDN National formatted number, as an example.	Unknown Subscriber National National-specific Abbreviated International Subscriber (oper.req) National (oper.req) International (oper.req) Not Present (oper.req) Not present (cut through) 950 call Test Line Test Code h323/SIP	Setting to *ISDN* includes user=phone in the Request URI *H323/SIP* removes user=phone from the Request URI

Copyright © 2015 Sonus Networks. All rights reserved.

Called Phone Context	None	Request URI	Sets the phone context for tel uri calls	None	To: tel:2222<sip:2222;phone-context=example.com@192.168.1.20>
Called Numbering Plan	ISDN IE 0x70		Describes the called number's numbering scheme or standard.	Any/Untranslated: For Input, any type is accepted. For Output, the plan will remain unchanged. Unknown: The type is unknown. ISDN: E.164 format Data: ITU X.121 format Telex: ITU F.69 format National: The standard national numbering plan Private: A private numbering plan Telephony: same as ISDN	
Calling Address/Number	ANI (ISDN IE 0x6C)	FROM header	The Calling Number	None	
Calling Extension	None	Request URI	Sets the ;ext=	None	From: 5551234<sip:5551234;ext=1234@192.168.1.10>
Calling Address/Number, User Specified	ANI (ISDN IE 0x6c)	None?	Calling Number supplied by the user in addition to the one supplied by the telephony network	None	
Calling Numbering Type	ISDN Numbering Type, IE 0x6C		Describes the format of the calling number; aids the receiving switch in properly processing the number based upon the configured number type.	Unknown Subscriber National National-specific Abbreviated International Subscriber (oper.req) National (oper.req) International (oper.req) Not Present (oper.req) Not present (cut through) 950 call Test Line Test Code h323/SIP	Setting to *ISDN* includes user=phone in the Request URI *H323/SIP* removes user=phone from the Request URI

Copyright © 2015 Sonus Networks. All rights reserved.

Calling Numbering Plan	ISDN Numbering Plan, IE 0x6C		Describes the calling number's numbering plan.	Any/Untranslated: For Input, any type is accepted. For Output, the plan will remain unchanged. Unknown: The type is unknown. ISDN: E.164 format Data: ITU X.121 format Telex: ITU F.69 format National: The standard national numbering plan Private: A private numbering plan Telephony: same as ISDN	
Calling Number Presentation	ISDN Pres. Indicator, IE 0x6C		Controls how the downstream device displays/processes the Calling Number.	Allowed: Display the calling number Restricted: Do not display the calling number Not Available Reserved	May also affect how the downstream device processes the P-Asserted ID or the P-Preferred ID
Calling Number Screening	ISDN Screening Indicator, IE 0x6C		Denotes how/if the calling number has been verified	User - Not Screened: Set by the client, not checked by the sending switch User - Verified: Set by client, verified by the sending switch User - Failed: The sending switch confirms this number as invalid Network: The previous switch provided the calling number	May also affect how the downstream device processes the P-Asserted ID or the P-Preferred ID
Calling Name	ISDN IE 0x1C or IE 0x28	FROM header	The calling name	None	
Calling Phone Context	None	FROM header	Sets the phone context for tel uri calls	None	To: tel:2222<sip:2222;phone-context=example.com@192.168.1.20>
Calling SubAddress/Number	ISDN IE 0x6D	FROM header	Specifies the ISDN SubAddress in the FROM header.	None	
Called SubAddress/Number	ISDN IE 0x71	TO header	Specifies the ISDN SubAddress in the TO header.	None	
Destination Trunk Group	None	None	Sets the destination Trunk Group ID to match against.	All Trunk Groups Select Specific Trunk	The Input value must be the Trunk Group ID from a configured Trunk Group. When the Output field is set to the Destination Trunk Group, the Output field value is ignored.

Copyright © 2015 Sonus Networks. All rights reserved.

ELIN Identifier	ISDN IE 0x6c, Calling Number	FROM header	Sets the Emergency Line Identifier that the PSAP will use to lookup the location in the location database.	None	
Original Called Number	ISDN IE 0x1C	DIVERSION header	Specifies the original number when a call has been redirected	None	The redirecting number is the number the call was last redirected from. The original called number is just that, the very first called number, which in the case of multiple redirections can be different.
Original Destination Number	None	TO Header	Specifies the number in the TO header	None	This differs from the Called Number which is set from the SIP Request URI
Redirecting Number	ISDN 0x74	DIVERSION header HISTORY-INFO header	Specifies the number to which a call should be redirected to	None	For SIP calls, use the Redirecting IE to change the SIP Diversion Incoming HISTORY-INFO headers will be mapped to the Redirecting Number transformation IE
Redirecting Numbering Type	ISDN 0x74		Same as Types above	Same as Types above	
Redirecting Numbering Plan	ISDN 0x74		Same as Plans above	Same as Plans above	
Transfer Capability			Used for permanent circuits. Not presently supported by Sonus SBC 1000/2000		

Value (Input/Output)

Specifies the value to match against for the selected type. Depending on the type selected, values may be free-form or selected from a menu.

Related Topics

- SIP URI Manipulation

Creating Call Routing Logic with Regular Expressions

At the core of the Sonus SBC 1000/2000 system's call routing logic are sets for Regular Expressions used for selecting, and transforming called numbers and addresses. In the Sonus SBC 1000/2000 system, regular expressions are defined in Transformation Table Entries which are attached to Call Route Entries. Regular Expressions defined in Transformation Table entries are used to select calls for routing, typically based on the called number or address of the call. The following pages provide examples of Regular Expressions for selecting and transforming called numbers and addresses and a further discussion of Regular Expression Syntax:

Regular Expressions for Number Matching and Transformation Understanding Regular Expressions

Regular Expressions for Number Matching and Transformation

In the Sonus SBC 1000/2000 system, Regular Expressions can be used for phone number matching and transformation. Use of Regular Expressions for phone number transformation is supported in the Transformation Tables .

Examples of Regular Expressions for phone number matching and transformation are shown below. For more information about Regular Expression syntax, see Understanding Regular Expressions.

Copyright © 2015 Sonus Networks. All rights reserved.

- Examples of Phone Number Matching and Transformation using Regular Expressions
- Detailed Examples
  - Example 1: Using Regular Expression for Route Match
  - Example 2: Local calls transformed to National numbering plan
  - Example 3: 10-digit long distance (LD) calls transformed for 11-digit dialing
  - Example 4: Stripping +-sign from the number (when terminating to some ISDN providers)
  - Example 5: Replacing "011" (international prefix) with +-sign
  - Example 6: Transforming only URI's that start with "+999" and have a ".com" extension to E.164 format

Examples of Phone Number Matching and Transformation using Regular Expressions

> Phone number transformation is the process of matching phone number patterns and transforming them to a single standard format.
> In the context of Enterprise Voice, the single standard format could be the local numbering plan, the E.164 n umbering scheme, as well as a SIP URI.

The following table illustrates use of Regular Expressions for matching phone number patterns and phone number transformations:

Rule Name	Description	Input Pattern	Output Pattern	Result
4-digit Extension	Transforms 4-digit extensions	`(\d{4})`	`+1425555\1`	1234 is transformed to +14255551234
5-digit Extension	Transforms 5-digit extensions	`8(\d{4})`	`+1425558\1`	81234 is transformed to +14255581234
7-digit calling Fremont	Transforms 7-digit numbers to Fremont local number	`(\d{7})`	`+1510\1`	5551212 is transformed to +15105551212
7-digit calling Dallas	Transforms 7-digit numbers to Dallas local number	`(\d{7})`	`+1972\1`	5551212 is transformed to +19725551212
10-digit calling US	Transforms 10-digit numbers in US	`(\d{10})`	`+1\1`	5105551212 is transformed to +12065551212
Long Distance (LD) Calling US	Transforms numbers with LD prefix in US	`1(\d{10})`	`+1\1`	12145551212 is transformed to +12145551212
International Calling	Transforms numbers with US international prefix	`011(\d*)`	`+\1`	011914412345678 is transformed to +914412345678

Copyright © 2015 Sonus Networks. All rights reserved.

Fremont Operator	Transforms 0 to Fremont Operator	`0`	`+15105551212`	0 is transformed to +15105551212
Fremont Site Prefix	Transforms numbers with on-net prefix (6) and Fremont site code (222)	`6222(\d{4})`	`+1510555\1`	62221234 is transformed to +15105551234
New York Site Prefix	Transforms numbers with on-net prefix (6) and New York site code (333)	`6333(\d{4})`	`+1202555\1`	63331234 is transformed to +12025551234
Dallas Site Prefix	Transforms numbers with on-net prefix (6) and Dallas site code (444)	`6444(\d{4})`	`+1972555\1`	64441234 is transformed to +19725551234
URI to E.164 format	Transforms URI with on-net prefix (+999) to E.164 format	`\+999(.*)@.*`	`0119144\1`	+99912345678@net.com is transformed to 011914412345678



The use of caret symbol (^) for beginning of a number-matching pattern and the dollar sign ($) for the end of the pattern is implicit. The regular expression rule will work with or without them.

Detailed Examples

Example 1: Using Regular Expression for Route Match

1. Select **Using Regular Expression** option.
2. Match Rule:

```
(.*)@net\.com
```

3. Transformation :

```
\1
```

In this example, the input text *john.doe@net.com* matches the Match Rule and the output will be "john.doe". The Input text *john.doe@invalid.com*does not match.

Expression Input	Expression Output

Copyright © 2015 Sonus Networks. All rights reserved.

john.doe@net.com	john.doe
jane_doe@net.com	jane_doe
jdoe@net.com	jdoe
john.doe@invalid.com	expression does not match: no output

Example 2: Local calls transformed to National numbering plan

1. Select **Using Regular Expression** option.
2. Match Rule:

```
(\d{7})
```

3. Transformation:

```
1510\1
```

In this example, any 7 digit number as input matches the Match Rule and the output will be the same 7-digit number prefixed with 1510.

Expression Input	Expression Output
8889999	15108889999
4441234	15104441234

Example 3: 10-digit long distance (LD) calls transformed for 11-digit dialing

1. Select **Using Regular Expression** option.
2. Match Rule:

```
(\d{10})
```

3. Transformation:

```
1\1
```

In this example, any 10-digit number as input matches the Match Rule and the output will be the same 7-digit number prefixed with 1.

Expression Input	Expression Output

Copyright © 2015 Sonus Networks. All rights reserved.

5107779999	15107779999

Example 4: Stripping +-sign from the number (when terminating to some ISDN providers)

1. Select **Using Regular Expression** option.
2. Match Rule:

```
\+(.*)
```

3. Transformation:

```
\1
```

In this example, any destination number prefixed with a +-sign (plus-sign) as input matches the Match Rule and the output will be the same number without the +-sign.

Expression Input	Expression Output
+914412345678	914412345678

Example 5: Replacing "011" (international prefix) with +-sign

1. Select **Using Regular Expression** option.
2. Match Rule:

```
011(.*)
```

3. Transformation:

```
+\1
```

In this example, any destination number prefixed with a +-sign (plus-sign) as input matches the Match Rule and the output will be the same number without the +-sign.

Expression Input	Expression Output
011914412345678	+914412345678

Example 6: Transforming only URI's that start with "+999" and have a ".com" extension to E.164 format

1. Select **Using Regular Expression** option.
2. Match Rule:

Copyright © 2015 Sonus Networks. All rights reserved.

```
\+999(.*)@(.*)\.com
```

3. Transformation:

```
0119144\1
```

In this example, any destination URI +99912345678@net.com matches the pattern `+999`, followed any character set `(.*)`, followed by the @-sign, followed any character set `(.*)`, followed by and ending with `\.com`, the first character set is preserved and `0119144` is prefixed to it resulting in `011914412345678`.

Expression Input	Expression Output
+99912345678@net.com	011914412345678

Understanding Regular Expressions

Regular expressions are text pattern matching and manipulation technology than can be used for phone number matching and translation. The following topic provides a brief overview of regular expression syntax.

- Regular Expression Syntax
- Wildcard .
- Anchors ^,$
- Marked Group (expr)
- Non-Marking Grouping (?:)
- Shorthand Character Classes \d, \w, \s
- Repeaters *,+,?,{}
- Non-Greedy Repeats
- Back References \1, \2, \n
- Alternation |
- Character Sets [a-z], [A-Z], [0-9]
- Negation ^
- Escapes \

For more information on Regular Expressions, see Wikipedia or http://www.regular-expressions.info/.

Regular Expression Syntax

In regular expressions, all characters match themselves except for the following special characters:

```
. [ { ( ) * + ? | ^ $ \
```

Wildcard .

Copyright © 2015 Sonus Networks. All rights reserved.

The single character '.' when used outside of a character set will match any single character.

Pattern	Description
.	Matches any single character
\.	Matches the literal period . character

Anchors ^,$

The anchor characters are used to match the beginning or end of a line.

Pattern	Description
^	Matches the start of a line, not including the first character of the line
$	Matches the end of a line, not including the last character of the line

Marked Group (expr)

A section beginning with open parenthesis (and ending with a closed parenthesis) acts as a Marked Group. The string that matches the group pattern is preserved for later use. Marked Groups can also be repeated, or referred to by a *Back-Reference.*.

Pattern	Description
( )	Used to group expressions and to capture a set of characters for use in a back-reference.
\ (	Matches the open parenthesis (character
\ )	Matches the close parenthesis) character

Non-Marking Grouping (?:)

A *Marked Group* is useful to lexically group part of a regular expression, but has the side-effect of spitting out an extra field in the result. As an alternative, you can lexically group part of a regular expression, without generating a marked group by using (?: and) , for example (?:ab)+ repeats the "ab" match phrase without splitting out a separate marked group.

Pattern	Description
(?:)	Used to group expressions without capturing them for a back-reference

Shorthand Character Classes \d, \w, \s

These expressions provide a shorthand way to describe a class of characters, for example; \d matches any numeric digit. The capital versions of these shorthand express the negative version of this character, for example; \D matches any non-digit character.

Copyright © 2015 Sonus Networks. All rights reserved.

Pattern	Description
\d	Matches a numeric digit (0 to 9)
\w	Matches a word character (letters, digits, underscores)
\s	Matches a whitespace character (space, tab, line breaks)
\D	Matches a non-numeric character (no number 0 to 9)
\W	Matches a non-word character (not a letter, digit or underscore)
\S	Matches a non-whitespace character (not a space, tab or line break)

The `\d` shorthand is commonly used with the curly bracket repeater expression to match a specific number of digits, for example: **\d{4}** to match four consecutive digits.

Repeaters *,+,?,{}

The repeater characters (*, +, ?, and {}) enable matching of a character, expression or character class that is repeated.

Pattern	Description
*****	Match the preceding character or expression zero to unlimited times.
+	Match the preceding character or expression one to unlimited times.
{n}	Match the preceding character or expression exactly *n* times
{n,m}	Match the preceding character or expression at least *n* times and at most *m* times
{n,}	Match the preceding character or expression at least *n* times and unlimited times
?	Optionally match the preceding character or expression

** Examples*

The * operator matches the preceding atom zero or more times, for example the expression a*b matches the following input:

Pattern	Input	Match?
a*b	b	✅ Yes
a*b	ab	✅ Yes
a*b	aaaaaaaab	✅ Yes

Copyright © 2015 Sonus Networks. All rights reserved.

a*b	`acb`	❌ No
a*b	`aaaaaaacb`	❌ No

+ Examples

The + operator matches the preceding atom one or more times, for example the expression a+b matches the following input:

Pattern	Input	Match?
a+b	`b`	❌ No
a+b	`ab`	✅ Yes
a+b	`aaaaaaaab`	✅ Yes
a+b	`acb`	❌ No
a+b	`aaaaaaacb`	❌ No

? Examples

The ? operator matches the preceding atom zero or one times, for example the expression ca?b matches the following input:

Pattern	Input	Match?
ca?b	`b`	❌ No
ca?b	`ab`	❌ No
ca?b	`cb`	✅ Yes
ca?b	`cab`	✅ Yes
ca?b	`caab`	❌ No

{ } Examples

The curly bracket repeaters allow matching of a character or expression a specific number of times.

Pattern	Input	Match?
h{4}	`hhhh`	✅ Yes
h{4}	`hh`	❌ No
h{4}	`hhhhh`	❌ No

Copyright © 2015 Sonus Networks. All rights reserved.

Pattern	Input	Match?
h{2,5}	hhhh	✅ Yes
h{2,5}	hh	✅ Yes
h{2,5}	hhhhh	✅ Yes
h{2,5}	h	❌ No
h{2,5}	hhhhhh	❌ No

Pattern	Input	Match?
h{3,}	hh	❌ No
h{3,}	hhh	✅ Yes
h{3,}	hhhhhh	✅ Yes
h{3,}	hhhhhhhhhh	✅ Yes

Non-Greedy Repeats

The normal repeat operators try to match as much input as possible, and so are described as "greedy" expressions. Adding a question mark ? after a repeater symbol alters this matching behavior and makes the expression match as little input as possible while still producing a match. A regular expression altered in this way is sometimes referred to as a "lazy" expression.

Pattern	Description
***?**	Matches the previous character or expression zero or more times, while consuming as little input as possible
+?	Matches the previous character or expression one or more times, while consuming as little input as possible
??	Matches the previous character or expression zero or one times, while consuming as little input as possible
{n,}?	Matches the previous character or expression *n* or more times, while consuming as little input as possible
{n,m}?	Matches the previous character or expression at least *n* and at most *m* times, while consuming as little input as possible

Back References \1, \2, *n*

An escape character followed by a digit n, where n is in the range 1-9, matches the same string that was matched by *Marked Group*. Marked Groups are created with an open and close parenthesis pair ( ).

Copyright © 2015 Sonus Networks. All rights reserved.

Pattern	Description
\1	Outputs the content of the first capturing marked group
\2	Outputs the content of the second capturing marked group
\n	Outputs the content of the *n* capturing marked group (*n* must be a number, not the character n)

Examples

Pattern	Input	Match?
^(a*).*\1$	`aaabbaaa`	✅ Yes
^(a*).*\1$	`aaabba`	❌ No

Alternation |

The | operator match the characters or expressions to the left and right of the | symbol.

Pattern	Description
|	Match the character or expression on either side of the | character

Pattern	Input	Match?
abc|def	`abc`	✅ Yes
abc|def	`def`	✅ Yes

The alternation operator is typically used with parenthesis to separate the alternate expressions from the rest of the matching expression.

Pattern	Description
(|)	Match the character or expression on either side of the | character, contained within the parenthesis **( )**

Pattern	Input	Match?
(abc|def)	`abc`	✅ Yes
(abc|def)	`def`	✅ Yes
(abc|def)	`ab`	❌ No

Copyright © 2015 Sonus Networks. All rights reserved.

(abc|def)	`ef`	❌ No
a(bc|de)f	`abcf`	✅ Yes
a(bc|de)f	`adef`	✅ Yes
a(bc|de)f	`abcdef`	❌ No
a(bc|de)f	`af`	❌ No
a(bc|de)f	`acdf`	❌ No

Character Sets [a-z], [A-Z], [0-9]

A character set is a bracket-expression starting with [and ending with], it defines a set of characters, and matches any single character that is a member of that set.

Pattern	Description
[a-z]	Matches any lowercase letter in the range 'a' to 'z'
[A-Z]	Matches any UPPERCASE letter in the range 'A' to 'Z'
[a-c]	Matches any character in the range 'a' to 'c'
[abc]	Matches any of the characters 'a', 'b', or 'c'
[0-9]	Matches any number in the range '0' to '9'
[5-8]	Matches any number in the range '5' to '8'
[1234]	Matches any of the numbers '1', '2', '3' or '4'
[0-9a-zA-Z]	Matches any character in the ranges '0' to '9', 'a' to 'z' or 'A' to 'Z'

Negation ^

This expression is used within a square bracket pair to match any character that ***is not*** in the range or set of characters, for example; The regular expression [^a-c] matches any character that is not in the range a-c.

Pattern	Description
[^]	Matches any character that is not shown after the caret ^ character

Pattern	Input	Match?
[^a-z]	`1`	✅ Yes

Copyright © 2015 Sonus Networks. All rights reserved.

[^a-z]	9	✅ Yes
[^a-z]	B	✅ Yes (since 'B' is not lowercase)
[^1-9]	4	❌ No
[^1-9]	0	✅ Yes (since '0' is not in the range 1 through 9)
[^@]	@	❌ No
[^<]	<	❌ No
[^>]	>	❌ No

Escapes \

Any special character preceded by an escape character '\' shall match itself. The special characters are as follows:

```
. [ { ( ) * + ? | ^ $ \
```

Pattern	Description
`\`	If the following character is a special character, ignore its special meaning and match the literal character.
`\.`	Match the '.' character literally
`\[`	Match the '[' character literally

Copyright © 2015 Sonus Networks. All rights reserved.

\{	Match the '{' character literally
\(	Match the '(' character literally
\)	Match the ')' character literally
*	Match the '*' character literally
\+	Match the '+' character literally
|	Match the '|' character literally

Copyright © 2015 Sonus Networks. All rights reserved.

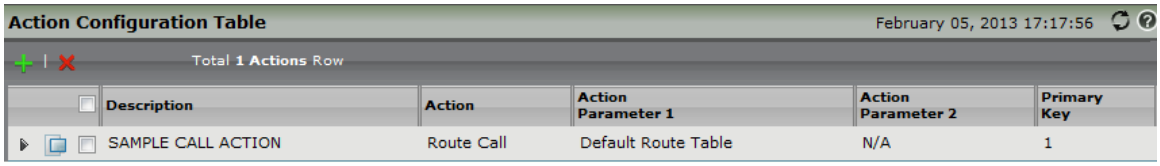
\^	Match the '^' character literally
\$	Match the '$' character literally
\\	Match the '\' character literally

Managing Action Configurations

Action configurations are the individual steps (actions) that make up an Action Set. For information about how they are used, see the page for Managing Action Sets.

Working with Action Configurations

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Actions > Action Configuration**.



To view a actions's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

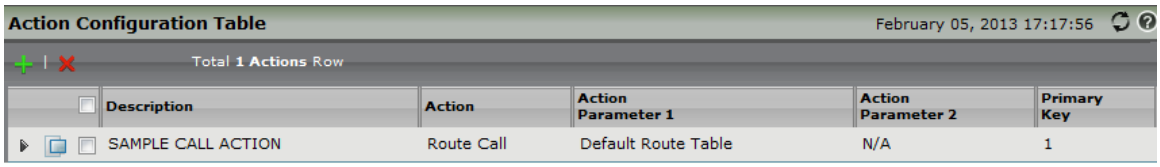
Creating and Modifying Action Configurations

Copyright © 2015 Sonus Networks. All rights reserved.

Creating and Modifying Action Configurations

To create or modify an existing Action Set:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Actions > Action Configuration**.

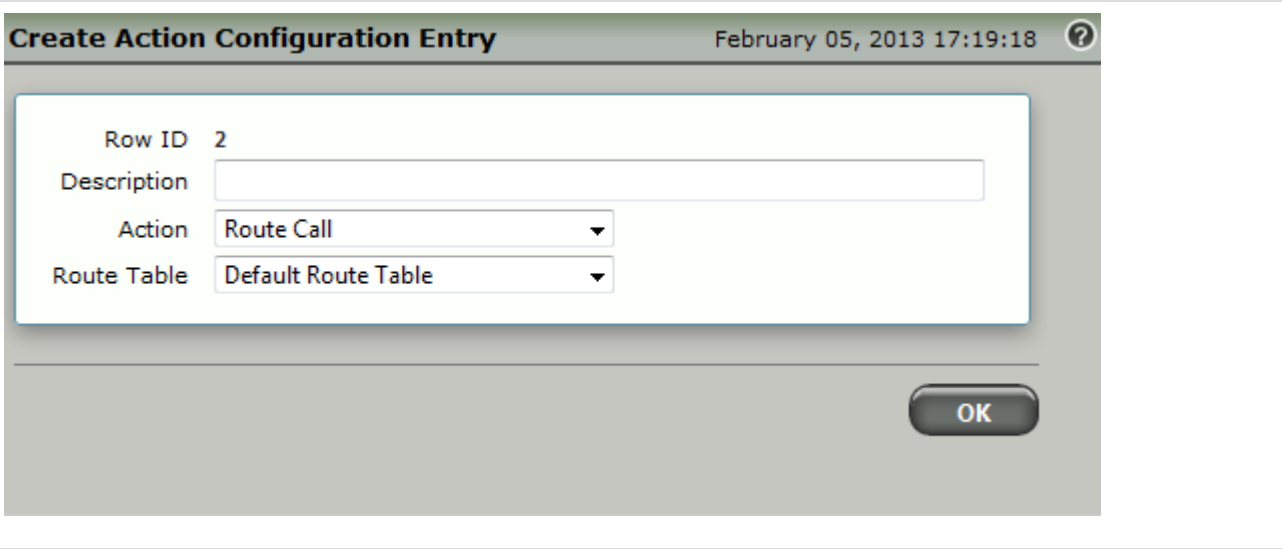


Modifying an Action Configuration

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating an Action Configuration

1. Click the **Create Action Configuration Entry** ( ) icon at the top of the Action Configuration Table page.



Action Configuration - Field Definitions

Action

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the action to be taken. The action tells the call routing function the next step to take when setting up a call

Possible actions include:

- Route Call
- Send Alert
- Send Connect
- Release Call
- Route call and await connect timer
- Generic timer
- Invoke Action Set

Route Table

Specifies the Routing Table to use in this action. The field is available only when **Route Call** and **Route Call, Await Connect Timer** are selected from the **Action** drop down list.

Q.850 Cause Code

Specifies the Cause Code to send when a call is released. This field is available only when **Release Call** is selected from the **Action** drop down list.

Connect Timer

Specifies the length of time the Sonus SBC 1000/2000 waits for the call to be connected. This option is used to adjust for different network delay conditions. This field is available only when **Route Call, Await Connect Timer** is selected from the **Action** drop down list.

Generic Timer

Specifies the length of time the Sonus SBC 1000/2000 pauses before proceeding to the next action. Use this action to get call routing to pause to allow some external event to occur, or delay the call connect process to match the far-end requirements.

Timeout

Specifies the length of time before a timeout occurs. This field is available only when **Generic Timer** is selected from the **Action** drop down list.

Invoke Action Set

Specifies another Action Set to be invoked when the condition is true. For more information on Action Sets, see Managing Action Sets.

Action Set

Specifies the Action Set to be invoked. Options for this field are populated from the Action Set Table. See Managing Action Sets.This field is available only when **Invoke Action Set** is selected from the **Action** drop down list.

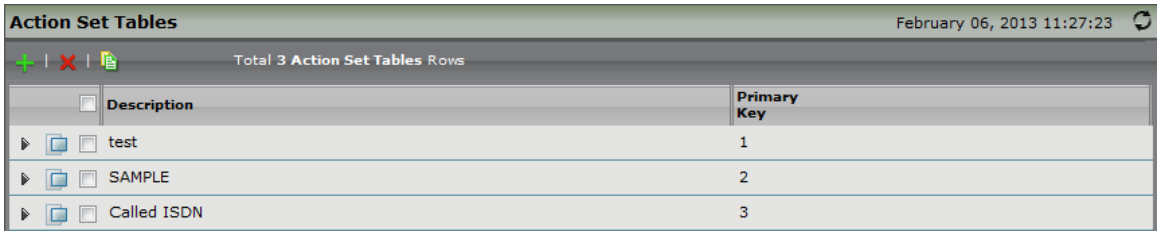
Managing Action Sets

Copyright © 2015 Sonus Networks. All rights reserved.

Action Sets allow you to perform additional actions before routing a call. They are comprised of a number of Actions, which must first be defined in Action Configurations. Once created, an Action Set Table is a sequence of steps to follow to route a call. To use an Action Set, select it from the Action Set Table field in a Signaling Group entry.

Working with Action Sets

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane. go to **Call Actions > Action Sets**.



To view an Action Set Table entry's properties:

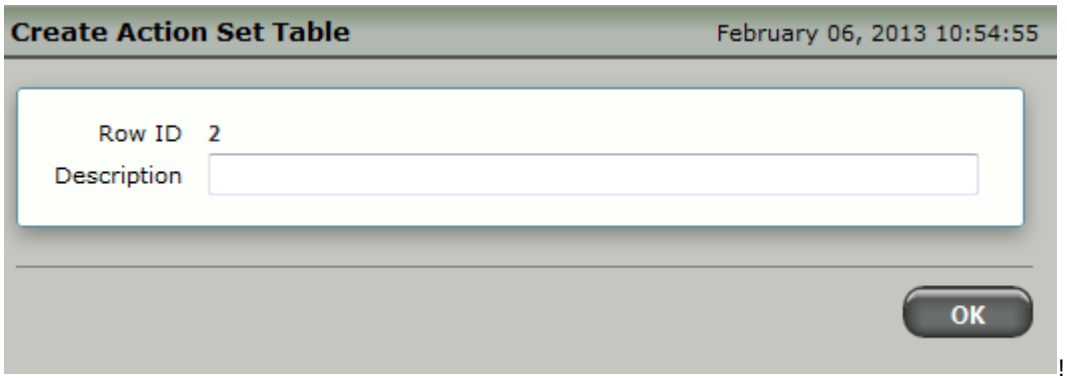
1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

To modify an Action Set Tables entry:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To add an Action Set Table:

1. Click the **Add** ( ) icon.



2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

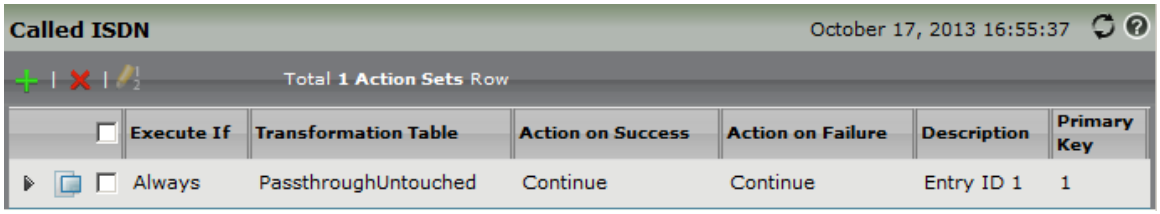
Creating and Modifying Entries to Action Set Tables

Copyright © 2015 Sonus Networks. All rights reserved.

Creating and Modifying Entries to Action Set Tables

To create or modify an Entry to an Action Set Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Actions > Action Sets > Entry**.



Modifying an Entry to an Action Set Table

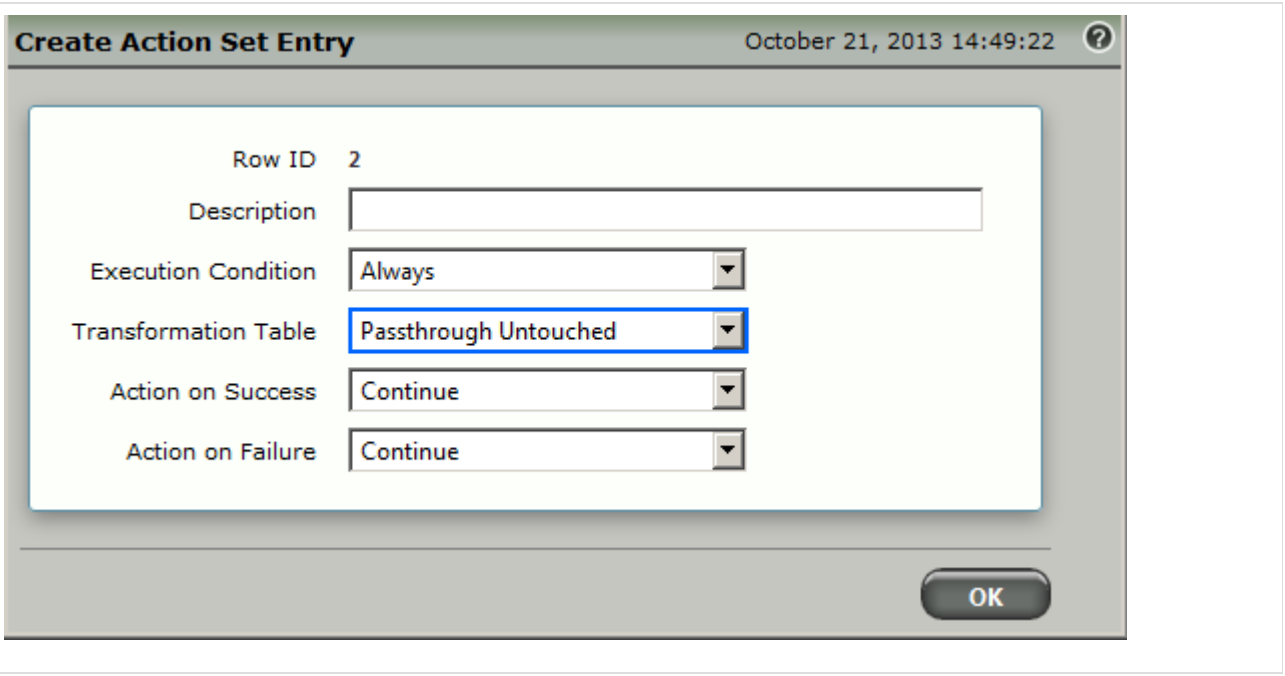
1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Resequencing an Entry in an Action Set Table

1. Click the **Resequence** icon ( ) at the top of the table.
2. Select the row(s) you want to move.
3. Click the **Move Selected Rows Up** ( ) or **Move Selected Rows Down** ( ) icon to reposition the row(s) in the table.
4. Click **Apply**.

Creating an Entry to an Action Set Table

1. Click the **Create** ( ) icon.



Copyright © 2015 Sonus Networks. All rights reserved.

Action Set Entry - Field Definitions

Description

Descriptive name for the Action Set entry.

Execution Condition

Specifies whether or not to execute this action and on what condition, if any, it is executed.

Transformation Table

Specifies which, if any, Transformation Table to use when executing the action. For detailed information about Transformation Tables, see Managing Transformation Tables.

Action on Success

Specifies the entry in the Action Configuration Table to use when the Transformation Table entry selected returns success.

Action on Failure

Specifies the entry in the Action Configuration Table to use when the Transformation Table entry returns failure.

Routing Usage Examples

This section contains a listing of Telephony Routing usage examples supported by the Sonus SBC 1000/2000 system intended to illustrate the relationship between the various routing components - namely: Call Routing Tables, Transformation Tables, Action Configurations, and Action Sets.

- SIP URI Manipulation
- Static Call Forking
- Dynamic Call Forking
- Call Routing for Active Directory Integration

SIP URI Manipulation

This page contains a simple example to demonstrate the manipulation of the `ext=` and `phone-context=` tags of the SIP URI for calls to and from Lync clients. The Sonus SBC 1000/2000 system will send calls to a Lync client with **ext** and **phone-context** configured properly, and when received, the Lync client will appropriately set the calling number based on the **phone-context** value:

- Call Route Table
- Transformation Tables
  - Local SIP Phone to Lync
  - PSTN to Lync
  - Lync to PSTN

Call Route Table

We create a call routing table with the following 3 call routing entries in it. Two of the entries point to Transformation tables for calls that originate from SIP and PSTN devices to a Lync client, and the third call routing entry points to a

Copyright © 2015 Sonus Networks. All rights reserved.

Transformation table for a call that originates from a Lync client to a PSTN device:

Row	Transformation Table	Destination Type	Signaling Group	Media Selection	Media Transcoding	Call Control Profile	Fork
1	#Local SIP Phone to Lync	normal	registra	G.711	Enabled	None	No
2	#PSTN to Lync	normal	ISDN	G.711	Enabled	None	No
3	#Lync to PSTN	normal	Lync	G.711	Enabled	None	No

✅ Click each Transformation table link above to view its summarized behavior.

Transformation Tables

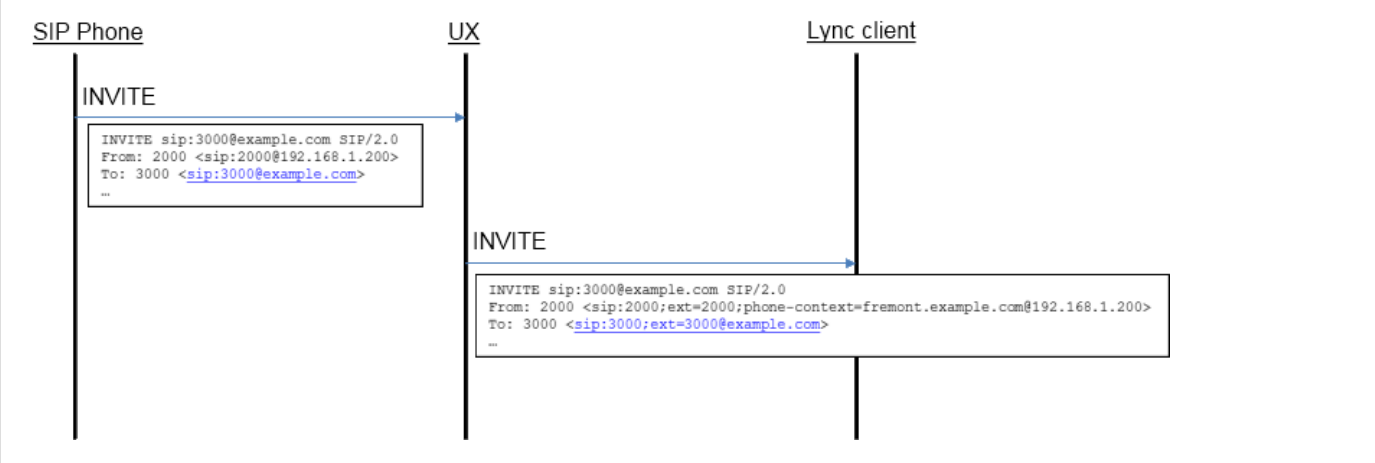
Local SIP Phone to Lync

Summarized transformation behavior:

- All **Called Number** of 4-digit whose number does not begin with '2' and **Calling Number** of 4-digit beginning with '2' will be sent to the Lync client. Sonus SBC 1000/2000 will set **phone-context** to **fremont.example.com** and **ext** to the **Calling Number**.

Row	Input Field	Match Field/ Field Value	Output Field/ Replaced by Field	Field Value	Match Type
1	Called Address/Number	`([^2]\d{3}$)`	Called Extension	`\1`	Mandatory
2	Calling Address/Number	`(2\d{3}$)`	Calling Extension	`\1`	Mandatory
3	Calling Address/Number	`(2\d{3}$)`	Calling Phone Context	`fremont.example.com`	Mandatory

Mmessage Flow:



Copyright © 2015 Sonus Networks. All rights reserved.

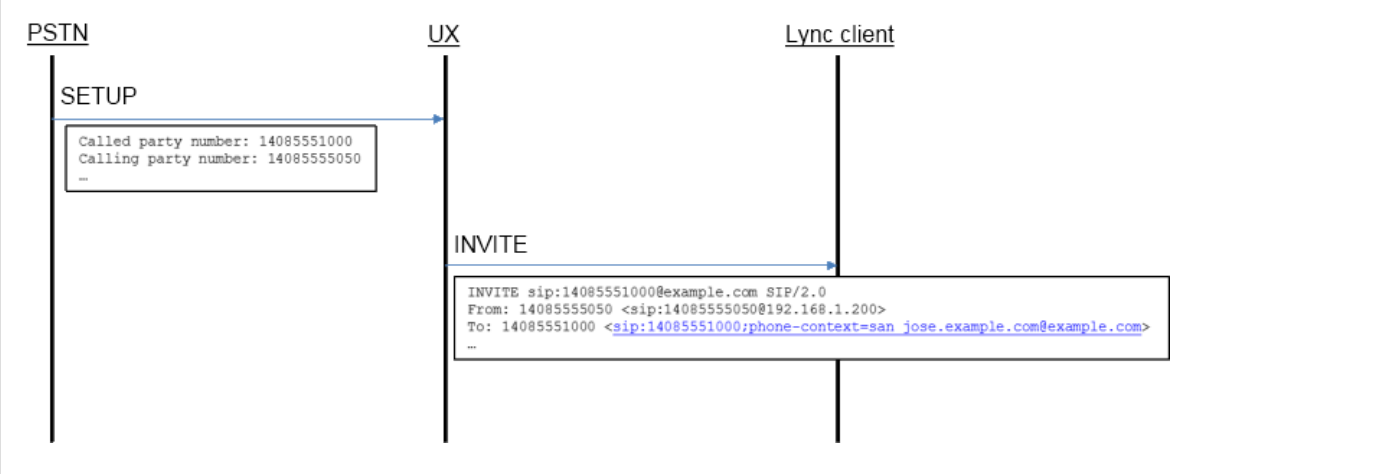
PSTN to Lync

Summarized transformation behavior:

- Calls with **Called Number** of **14085551000** will be sent to Lync with **phone-context** set to **san_jose.example.com**
- Calls with **Called Number** of **14155553000** will be sent to Lync with **phone-context** set to **san_francisco.example.com**

Row	Input Field	Match Field/ Field Value	Output Field/ Replaced by Field	Field Value	Match Type
1	Called Address/Number	`14085551000`	Calling phone context	`san_jose.example.com`	Optional
2	Called Address/Number	`14155553000`	Calling phone context	`san_francisco.example.com`	Optional

Mmessage Flow:



Lync to PSTN

Summarized transformation behavior:

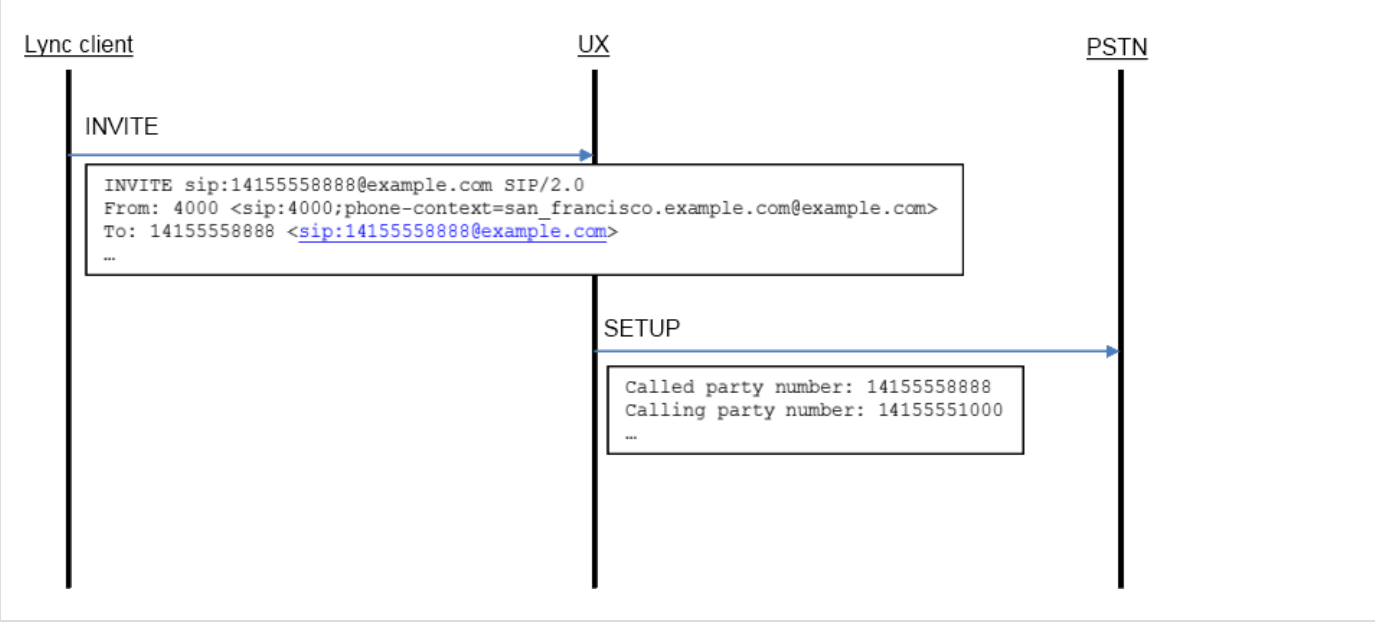
- Calls with **Called Number** of 1 plus ten digits and **phone-context** of **san_jose.example.com** will be sent to the PSTN with **Calling Number** set to **14085551000**
- Calls with **Called Number** of 1 plus ten digits and **phone-context** of **san_francisco.example.com** will be sent to the PSTN with **Calling Number set to 14155553000**

Row	Input Field	Match Field/ Field Value	Output Field/ Replaced by Field	Field Value	Match Type
1	Called Address/Number	`(1\d{10}$)`	Called Extension	`\1`	Mandatory
2	Calling phone context	`san_jose.example.com`	Calling Address/Number	`14085551000`	Optional

Copyright © 2015 Sonus Networks. All rights reserved.

3	Calling phone context	`san_francisco.example.com`	Calling Address/Number	`14155553000`	Optional

Mmessage Flow:



Note: SIP message sent by the Sonus SBC 1000/2000 system should have the **From** and **To** headers as follows:

From: 5551234<sip:5551234;ext=1234;phone-context=example.com@192.168.1.10>
To: tel:2222<sip:2222;ext=2222;phone-context=example.com@192.168.1.20>

Static Call Forking

Usage examples coming soon

Dynamic Call Forking

Usage examples coming soon

Call Routing for Active Directory Integration

Usage examples coming soon

Working with Users and Groups

This section describes how to manage users and groups, including adding, deleting, and monitoring users:

How User Authentication Works

Permissions Overview

Monitoring User Activity

Copyright © 2015 Sonus Networks. All rights reserved.

Changing The Current User's Password

Managing Remote Authentication

Managing Local Users

- Creating and Modifying Local Users
- Resetting a Local User Password

Managing Global Security Options

Recovering Admin Passwords

How User Authentication Works

The Sonus SBC 1000/2000 system supports multiple forms of authentication, which authentication method is used depends on the prototype of credentials presented by the user when attempting to login, either one of the following:

1. `username` simple alphanumeric format – applicable to local and RADIUS users
2. `user@domain` format – applicable to Active Directory and known as the **userPrincipalName** attribute
3. `domain\username` format – applicable to Active Directory and known as the **SAMAccountName** attribute in Active Directory

Active Directory Authentication

If the user presents credentials in either the `user@domain` or `domain\username` format, the Sonus SBC 1000/2000 attempts to authenticate the user against Active Directory. If the user is authenticated belongs to a group mapped with a Sonus SBC 1000/2000 access level, then they are given access and granted permissions. If the user fails to authenticate, they are denied access and no further attempt to authenticate the user is made.

Local and RADIUS Authentication

If the user presents credentials in the simple alphanumeric format, the Sonus SBC 1000/2000 first attempts to authenticate the user against the Local User Table. If the user's credentials are not found or the user's password does not match, authentication is then attempted against the RADIUS server with respect to the RADIUS User's class mapping with Sonus SBC 1000/2000 access level.

Permissions Overview

Access Levels

Administrators have the ability to grant access to users whose accounts have been locally created on Sonus SBC 1000/2000, and to users remotely authenticating.

The following table lists the different types of access roles and the functions they secure.

Access Role	Explanation
Administrator	Permission to manage (i.e. view/add/remove) the Sonus SBC 1000/2000 system through the User Interface.
Operator	Permission to manage a subset of the functions granted to Administrators. See details below.
Audit	Permissions to audit the logs on the Sonus SBC 1000/2000 system.

Copyright © 2015 Sonus Networks. All rights reserved.

Read-only	Permission to **only view** the Sonus SBC 1000/2000 system through the User Interface.
REST	Permission to manage (i.e. view/add/remove) the Sonus SBC 1000/2000 system through the Sonus SBC 1000/2000 API. Users with this access level will **not be able to access the web interface**.

Operator Role

Authenticated Sonus SBC 1000/2000 users with **Operator** access level have the ability to make non-service affecting changes to the Sonus SBC 1000/2000. Below are some examples of service affecting functions:

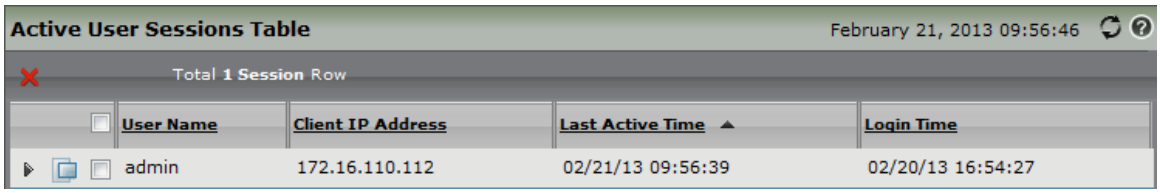
1. Installing ASM updates as it will reboot the ASM.
2. Changing the active partition as it will reboot the Sonus SBC 1000/2000 system.
3. Installing a new license as it could impact active calls.
4. Changing the Active Directory configuration as it could impact remotely authenticated users
5. etc...

Monitoring User Activity

The Active User Sessions Table shows current browser and REST sessions and their associated users. Information is also available about the user's access level

Working with User Activity

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > Users > Active User Sessions.**



To view a User Activity's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Terminating Active Sessions

You can terminate active user sessions by simply selecting the checkbox next to the session you wish to terminate, then click the Delete ( ) icon located at the top of the window.

User Sessions Information - Field Definitions

Access Level

The local Sonus SBC 1000/2000 permissions level associated with this user. For more information about Access Levels, see Permissions Overview page.

Client IP Address

Copyright © 2015 Sonus Networks. All rights reserved.

The IP Address of the computer from which the user is accessing the Sonus SBC 1000/2000.

Login Time

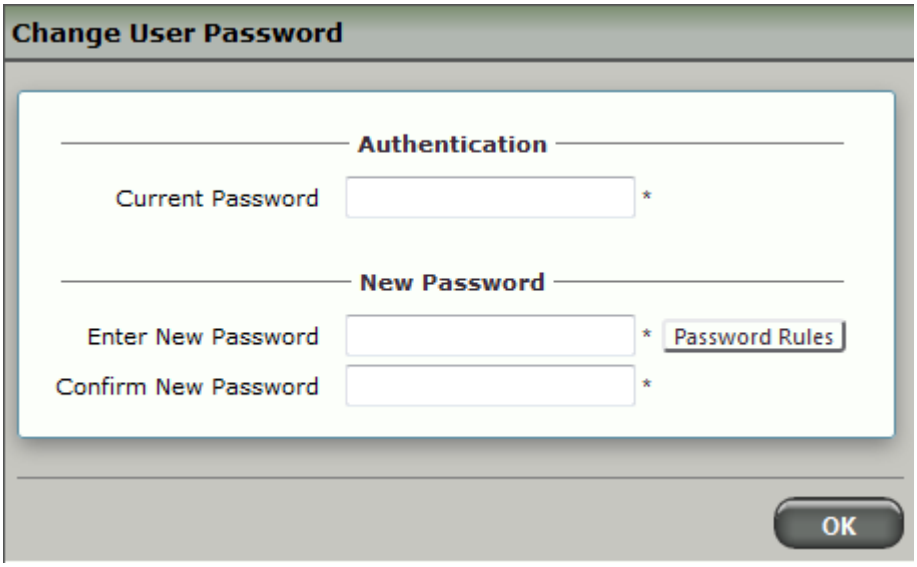
The local time and date at which the user last logged into the Sonus SBC 1000/2000.

Last Active Time

The local time and date at which the user last performed any action on the Sonus SBC 1000/2000.

Changing The Current User's Password

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > Change Password**.



3. Enter your old password in the **Current Password** text field.
4. Enter your new password in both the **Enter New Password** and **Confirm New Password** text fields.
5. Click **OK**.

The following procedure is applicable to change the password of the local user account currently logged into the Sonus SBC 1000/2000 system. If you are attempting to change the password of a remotely authenticated user via Active Directory or RADIUS, then this procedure will fail.

Managing Remote Authentication

In addition to local user management, the Sonus SBC 1000/2000 allows you to authenticate remote users using the following supported providers:

- Active Directory (AD)
- Remote Authentication Dial In User Service (RADIUS)

For these remote users to operate the Sonus SBC 1000/2000 system, you must configure their access level permissions by **mapping** their remote Group (in the case of AD) or Class (in the case of RADIUS) to the desired

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000/2000 access level. This mapping configuration will dictate the Sonus SBC 1000/2000-based permissions for your remotely authenticated users:

- Managing Active Directory Groups to Access Level Mapping
- Managing RADIUS User Class Access Level Mapping

> **Remote User Storage and Authentication**
>
> Remote users are **not stored on the Sonus SBC 1000/2000 system**, instead they live on the remote authentication providers. Remote user authentication happens over the network with the appropriate external provider which is transparent to the user.

Managing Local Users

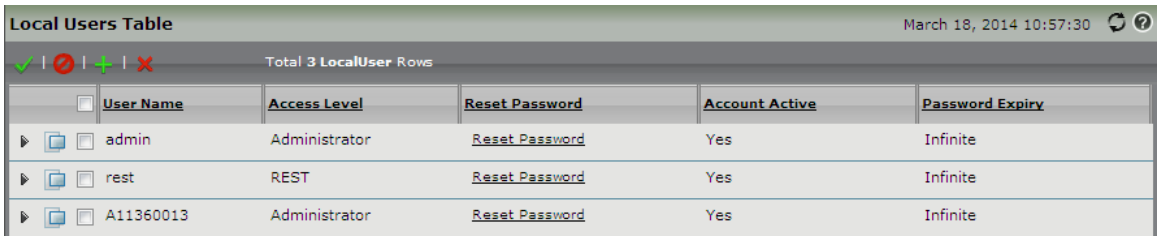
Unlike remote users, the Sonus SBC 1000/2000 manages local users whose accounts (and profiles) are stored directly on the Sonus SBC 1000/2000 system. Authentication for these users occurs locally. Once created, you can specify the access levels for these users.

Access Levels:

- `Administrator`
- `Operator`
- `Read-only`
- `Audit`
- `Reject User`: *This level is only applicable to RADIUS users. It works as a* ***disabled mode*** *for a RADIUS user for a particular class which doesn't map to one of the other four access levels.*

Working with Local Users

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > Users > Local User Management**.



To view a Local Users's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

> **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Local Users

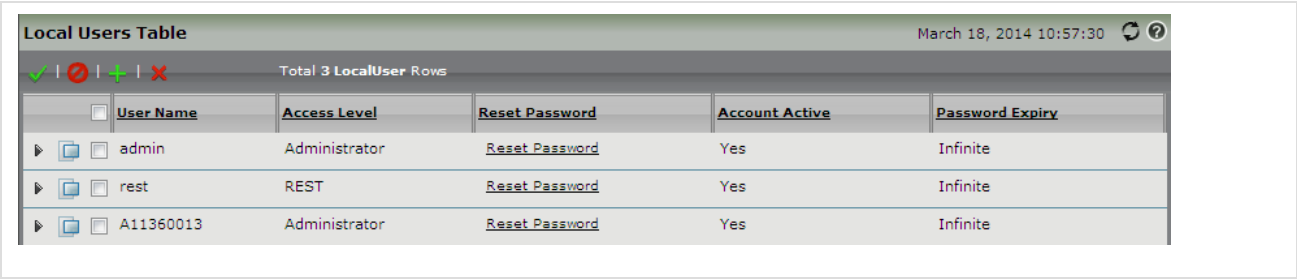
Resetting a Local User Password

Creating and Modifying Local Users

Copyright © 2015 Sonus Networks. All rights reserved.

To create or modify a Local User:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > Users > Local User Management**.



Modifying a Local User

To modify a user's access rights:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

> **Note:**
>
> Only the **Access Level** attribute can be modified.

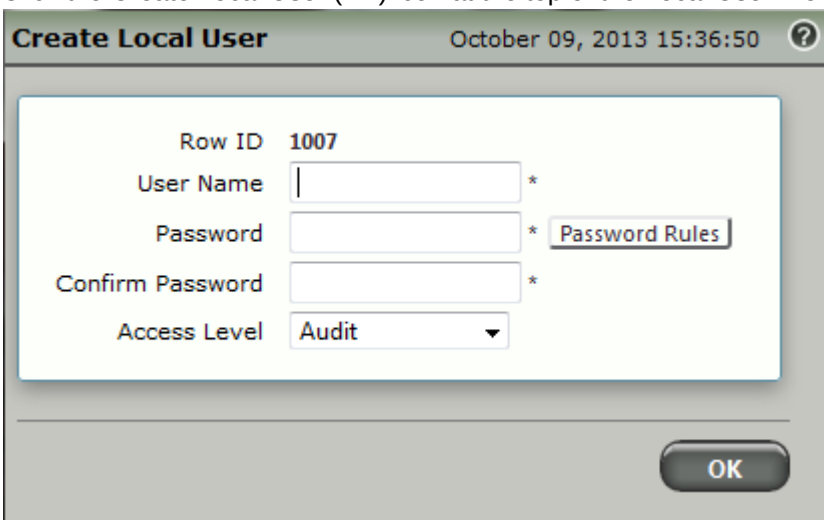
Disabling a Local User

To disable a user:

1. Select the check box next to the entry you wish to disable.
2. Click the **Disable** ( ) icon at the top of the table.

Creating a Local User

1. Click the Create Local User ( ) icon at the top of the Local User View page.



Copyright © 2015 Sonus Networks. All rights reserved.

Note

If Enhanced Password Security is enabled, the new user is prompted to enter a new password when they first attempt to log into the SBC. The user is not allowed to login until a new password that meets the specified criteria is successfully entered.

Local User - Field Definitions

User Name

Specifies the user name. The name must be 32 characters or less in length and may contain alphanumeric characters (A-Z, a-z, 0-9) only. Usernames may not begin with a digit (0 - 9).

Password/Confirm Password

Specifies the user's new password. Passwords must be 128 characters or less. Passwords may contain a combination of letters, numbers, and special characters. The minimum password length and combination of characters depend on the options specified in the Global Security Options page.

Access Level

Specifies the Access Level granted to the user. For more information about Access Levels, see the Permissions Overview page.

Resetting a Local User Password

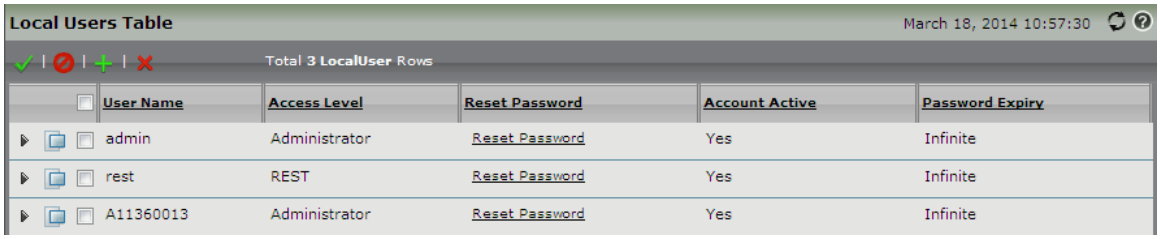
NOTE:

This function is available for Administrators only.

Helpful Tip: You can change your own password using the Change Password facility

To reset a local user password:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > Users > Local User Management**.

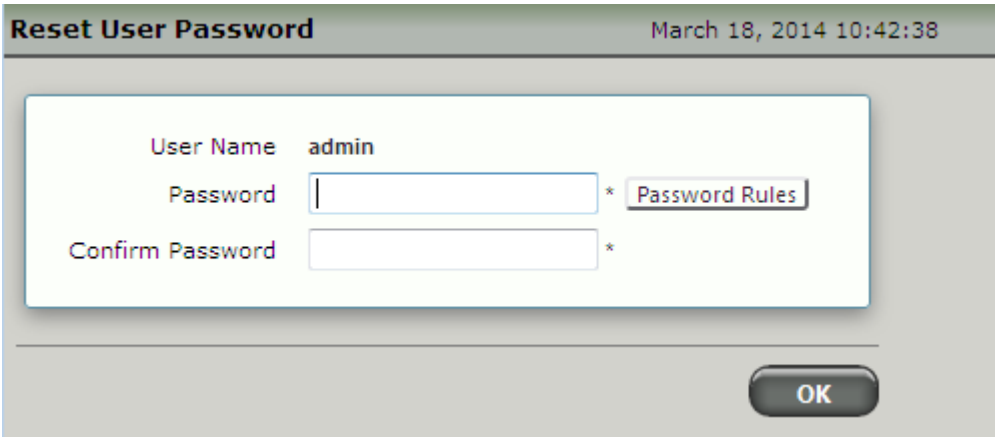


Reset a Local User Password

1. Click the **Reset Password** link on the far right side of the local user row for the user who's password you

Copyright © 2015 Sonus Networks. All rights reserved.

wish to reset.



Note

If Enhanced Password Security is enabled, the new user is prompted to enter a new password when they first attempt to log into the SBC. The user is not allowed to login until a new password that meets the specified criteria is successfully entered.

Reset User Password - Field Definitions

Password/Confirm Password

Specifies the user's new password. Passwords must be 128 characters or less. Passwords may contain a combination of letters, numbers, and special characters. The minimum password length and combination of characters depend on the options specified in the Global Security Options page.

Managing Global Security Options

The Global Security Options feature allows you to compel users to select strong passwords and set password lifetimes. The SBC also incorporates several anti-hacking features that help prevent unauthorized access. The restrictions and limits set by this feature apply to local users only.

Password construction and lifetimes for AD and RADIUS users are controlled by their respective authorization schemes. However, RADUIS and AD users are still subject to lockouts due to failed login attempts.

Note

Modifying the Global Security Options is available only to users with administrator level access.

Password Resets and New Users

After the administrator adds a new user, that user is prompted to enter a new password the first time they log into the SBC. Also, if an administrator resets a current user's password, the user's current session is terminated and the user is then prompted to enter a new password (compulsory password change).

Copyright © 2015 Sonus Networks. All rights reserved.

New password entry is forced in these situations and the user will not be allowed to proceed with the login process until they have correctly entered a new password.

Password Lockout

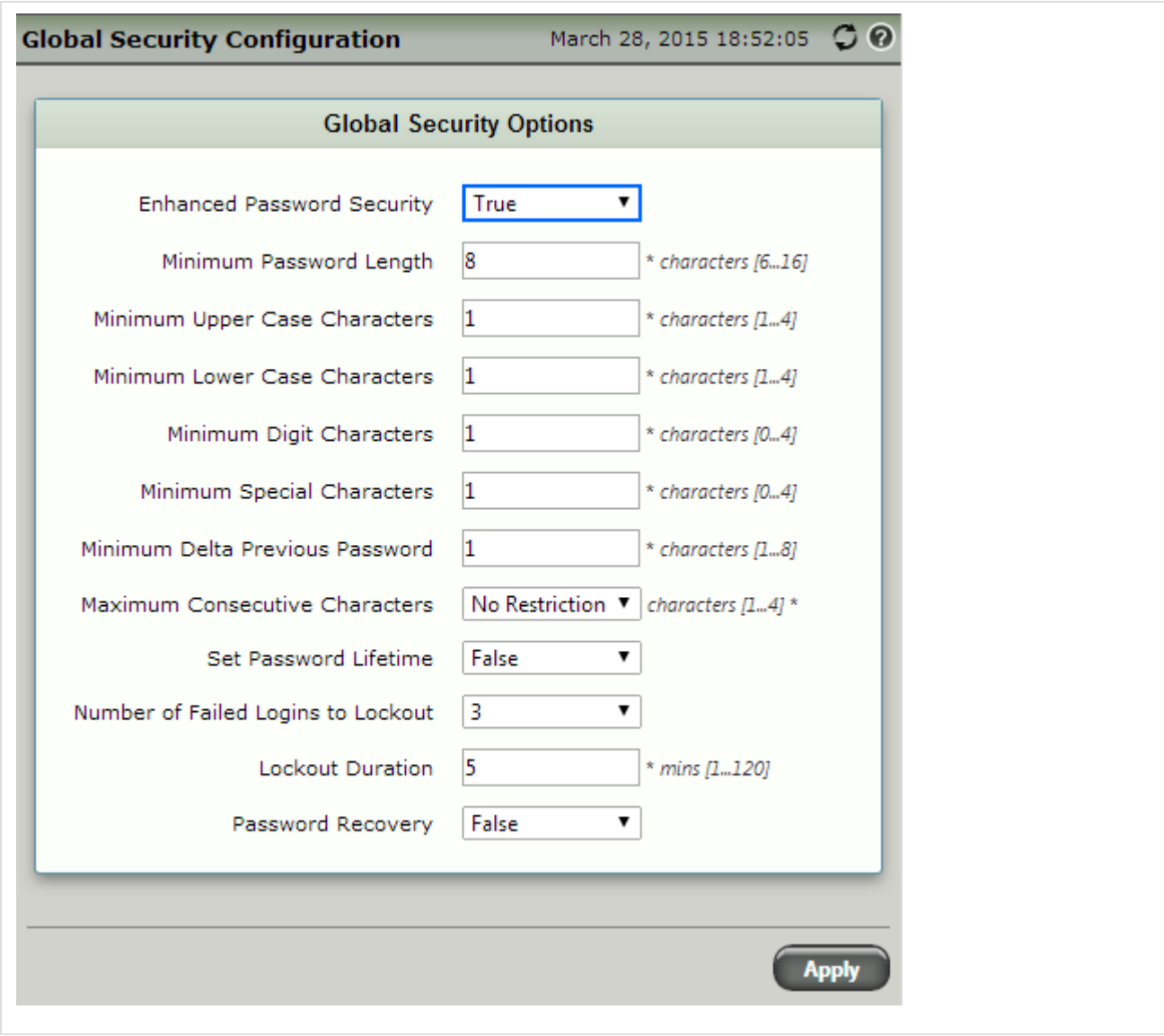
When a user exceeds the maximum number of failed attempts, they are locked out of the system for the time specified in the configuration, however if the SBC is rebooted, the lockout is terminated.

REST Users

Unlike the various WebUI access users (Admin, Read-Only, etc.), REST users are not subject to the constraints of password complexity, forced password reset, or password lifetimes.

Working with Global Security Options

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > Users > Global Security Options**.



Global Security Options - Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

Enhanced Password Security

Used to enable and disable Global Security Options.

Minimum Password Length

Specifies the minimum number of characters which must appear in a valid password. This field is only available when **Enhanced Password Security** is enabled.

Minimum Upper Case Characters

Specifies the minimum number of upper case alphabetical characters which must appear in a valid password. This field is only available when **Enhanced Password Security** is enabled.

Minimum Lower Case Characters

Specifies the minimum number of lower case alphabetical characters which must appear in a valid password. This field is only available when **Enhanced Password Security** is enabled.

Minimum Digit Characters

Specifies the minimum number of numeric characters which must appear in a valid password. This field is only available when **Enhanced Password Security** is enabled.

Minimum Special Characters

Specifies the minimum number of special characters which must appear in a valid password. This field is only available when **Enhanced Password Security** is enabled.

Mimimum Delta Previous Password

Specifies the minimum number of characters which must be different from the previous password. This field is only available when **Enhanced Password Security** is enabled.

Maximum Consecutive Characters

Specifies the maximum number of times any character may appear consecutively in a password. This field is only available when **Enhanced Password Security** is enabled.

Set Password Lifetime

Enables and disables password lifetimes.

Maximum Password Lifetime

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the maximum lifetime of a password in days. This field is only available when **Set Password Lifetime** is enabled.

> **Note**
>
> Users are required to enter a new conforming password at the next login subsequent to the expiration of their current password's lifetime.
> Although a user may not log into the SBC until they update their password, their account is not disabled.

Number Failed Logins To Lockout

Specifies the maximum number of failed log in attempts before the SBC locks out the user.

Lockout Duration

Specifies the period of time, in minutes, the user is locked out of the SBC after reaching the maximum number of failed log in attempts.

Recovering Admin Passwords

- Overview
- Enabling the Password Recovery Feature
- Resetting the Admin Password
  - Simple Admin Password Recovery Procedure
  - Recovering (restoring) Admin Passwords After a Factory Default Reset

Overview

The SBC 1000/2000 include a password recovery feature that allows for the recovery of (resetting) the admin password. This feature works by creating a temporary Admin user with a temporary password that allows an administrator to access the Local User Management page of the UI and reset at least one Admin level user's password.

Enabling the Password Recovery Feature

The Password Recovery feature is enabled (disabled by default) from the Global Security Options page of the UI.

Resetting the Admin Password

Simple Admin Password Recovery Procedure

Recovering the admin password(s) can be accomplished using the reset button.

To recover the admin password(s):

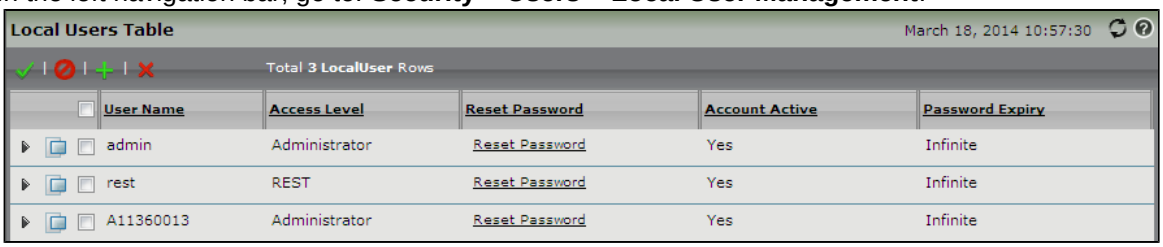
> ⚠ The temporary admin username and password are only valid for five minutes.

Copyright © 2015 Sonus Networks. All rights reserved.

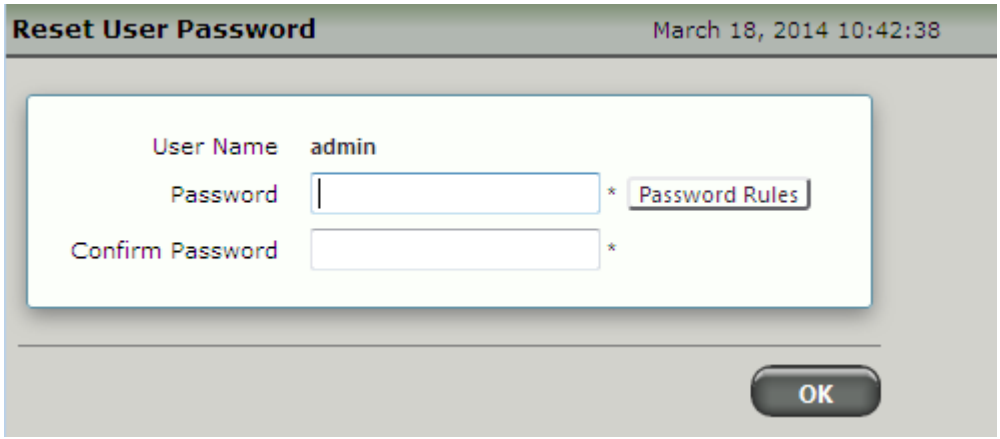
1. Push and hold the reset button for 4 to 5 seconds. See the SBC 1000 Front Panel or SBC 2000 Front Panel for details of button location.

> - When the SBC has detected the 4-5 second Reset Button push, the four LEDs on the front panel will flash four (4) times. See SBC 1000 Front Panel or SBC 2000 Front Panel for details about the location of the LEDs.
> - If the Reset Button is held for more than 6 seconds, the request will not be recognized and the push-and-hold operation must be repeated.
> - ***Do Not*** hold the Reset Button for a period of more than 20 seconds or this will initiate a factory default (see below).

2. Login to the SBC using the system generated temporary admin username and password.
   a. Temporary user name: A + last 8 characters of the the SBC serial number (e.g., A12345678).
   b. Temporary password: same as the temporary user name.
3. Click the **Settings** tab at the top of the UI.
4. In the left navigation bar, go to: **Security > Users > Local User Management**.



5. Click the **Reset Password** link in at least one Administrator level user row.



6. Enter a new password in the **Password** field, then re-enter the password in the **Confirm Password** field.
7. Click **OK**.

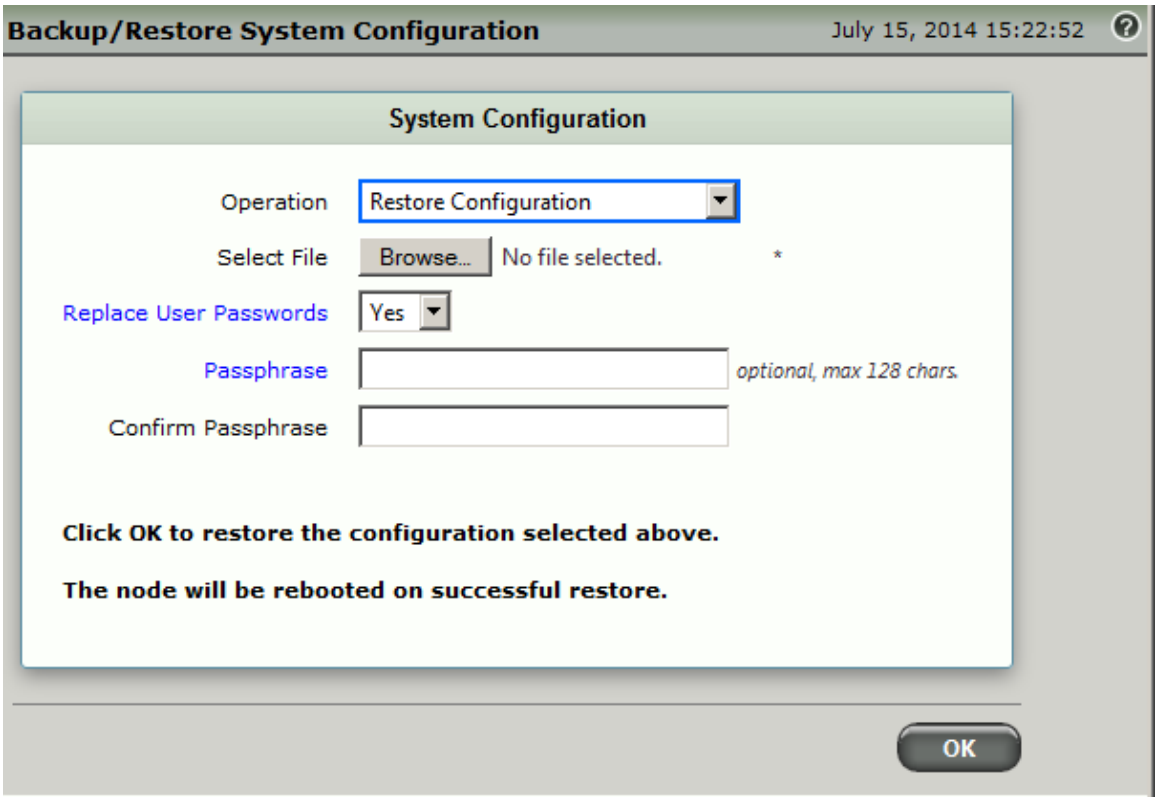
Recovering (restoring) Admin Passwords After a Factory Default Reset

After performing a factory default reset, the SBC configuration may be restored from a backup.

When you restore the configuration, there are options for retaining passwords:

- Restoring the configuration without recovering all existing users and passwords.
- Restoring the configuration and preserving only the admin user and password created in initial setup.

Copyright © 2015 Sonus Networks. All rights reserved.



The configuration restoration task can be initiated from either the Tasks or Settings tabs. For specific information about restoring a configuration, see the Restoring Data section in this documentation.

Working with Telephony Mapping Tables

This section contains information about Cause Code Reroutes, Message Translations, Override Tables, Cause and Response Codes.

Managing Cause Code Reroute Tables

- Creating and Modifying Cause Codes

Managing Message Translations

- Message Translation Usage Overview
- Message Translation Reference
- Creating and Modifying Entries to Message Translation Tables

Managing Q.850 to SIP Override Tables

- Creating and Modifying Entries to Q.850 to SIP Override Tables

Managing SIP to Q.850 Override Tables

- Creating and Modifying Entries to a SIP to Q.850 Override Tables

Q850 Cause Codes

Copyright © 2015 Sonus Networks. All rights reserved.

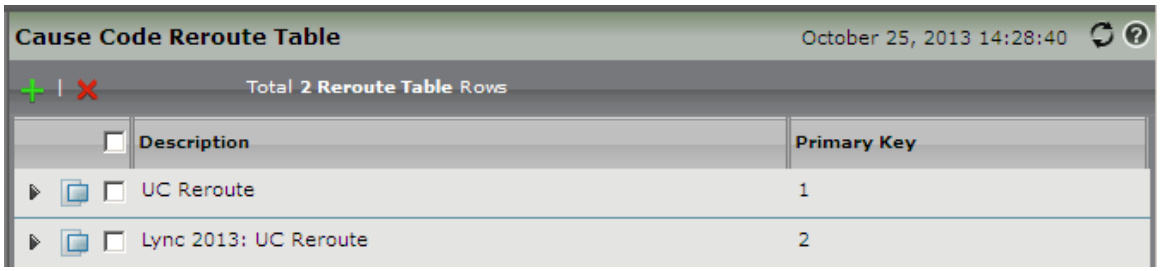
SIP Response Codes

Managing Cause Code Reroute Tables

Terminating ISDN calls return a Q.850 Cause Code when they end. We can use these codes to determine whether or not to reroute the call to another signalling group. A Cause Code Reroute table contains one or more Q.850 Cause Codes which, when matched, trigger a reroute. To use a table created here, select it from the Cause Code Reroute field in a Call Routing Table entry.

Working with Cause Code Reroute Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Telephony Mapping Tables > Cause Code Reroutes**.



To view a profile's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

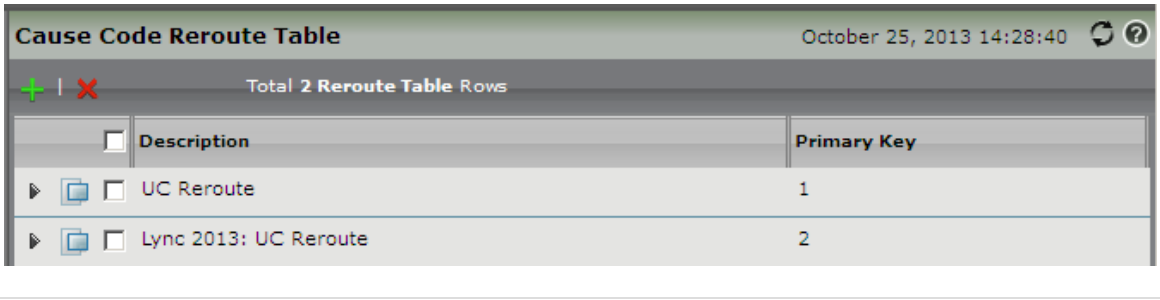
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Cause Codes

Creating and Modifying Cause Codes

To create a Cause Code:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Telephony Mapping Tables > Cause Code Reroutes**.



Modifying a Cause Code

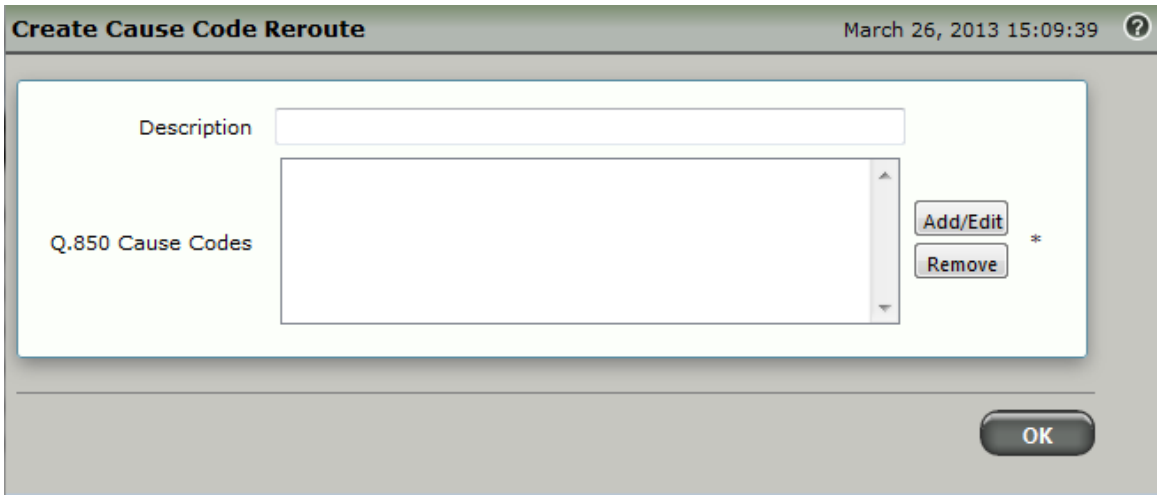
1. Click the **expand** ( ) Icon next to the entry you wish to modify.

Copyright © 2015 Sonus Networks. All rights reserved.

2. Edit the entry properties as required, see details below.

Creating a Cause Code

1. Click the **Create Cause Code** ( ) iconat the top of the Cause Code Reroute Table Page.



- Click **Add/Edit** next to the Q.850 Cause Codes field to specify one or more Q.850 Cause Codes.

> **Helpful Hint**
>
> This field presents a multi-select widget when the **Add/Edit** button is clicked.
> Click here for more information about using the Multi-select widget.

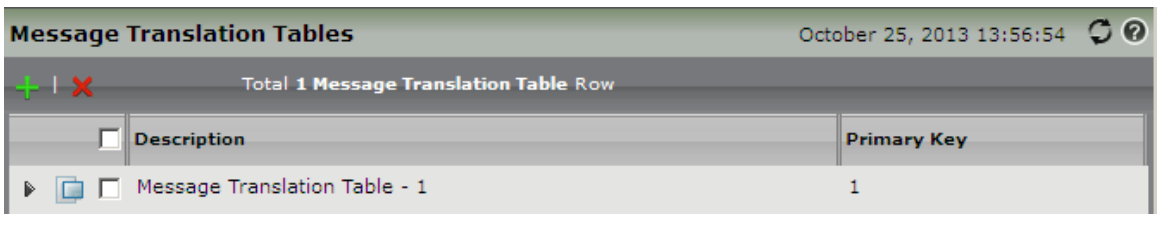
Managing Message Translations

Message Translation Tables aid in the interworking of differing protocols (like ISDN to SIP) by allowing control over how protocol messages are translated when calls are routed. They are useful for interworking with non-standard equipment and for specialized call routing. To use a table created here, select it from the Message Translation Table field in a Call Routing Table entry.

For more information, see Message Translation Usage Overview.

Working with Message Translation Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Telephony Mapping Tables > Message Translations**.



To view a Message Translation Table's properties:

1. Click the popup( ) icon next to the entry you want to view.

Copyright © 2015 Sonus Networks. All rights reserved.

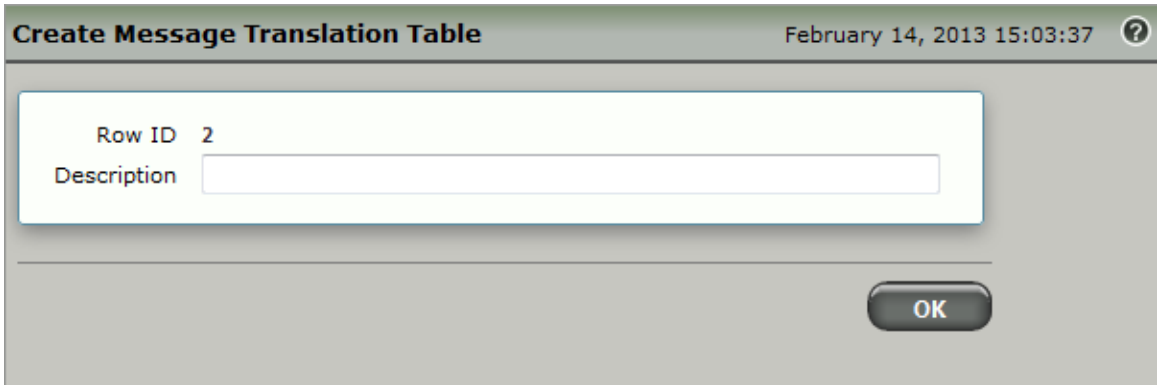
2. When you are finished, close the window.

To modify a Message Translation Table:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To Create a Message Translation Table:

1. Click the **Create** ( ) icon.



2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Message Translation Usage Overview

Message Translation Reference

Creating and Modifying Entries to Message Translation Tables

Message Translation Usage Overview

Each time a Sonus SBC 1000/2000 receives an ISDN Progress/Alert/Connect or a SIP 183/180/200 message, it is translated to the outgoing leg of the call. Although it may appear that incoming messages are simply copied from incomging to outgoing leg, in fact, they are run through an internal translation table to determine precisely what to send (on the outgoing leg).

The internal translation table is designed to work in the vast majority of circumstances; however, circumstance may dictate the need for a translation that differs from the pre-programmed translations. The Message Translation table provides the ability for the user to override the internal translations on a per Call Route basis.

This article outlines the various configuration parameters of the Message Translation functionality, how the parameters are used, and how to configure them to override the pre-programmed translations.

On this page:

Copyright © 2015 Sonus Networks. All rights reserved.

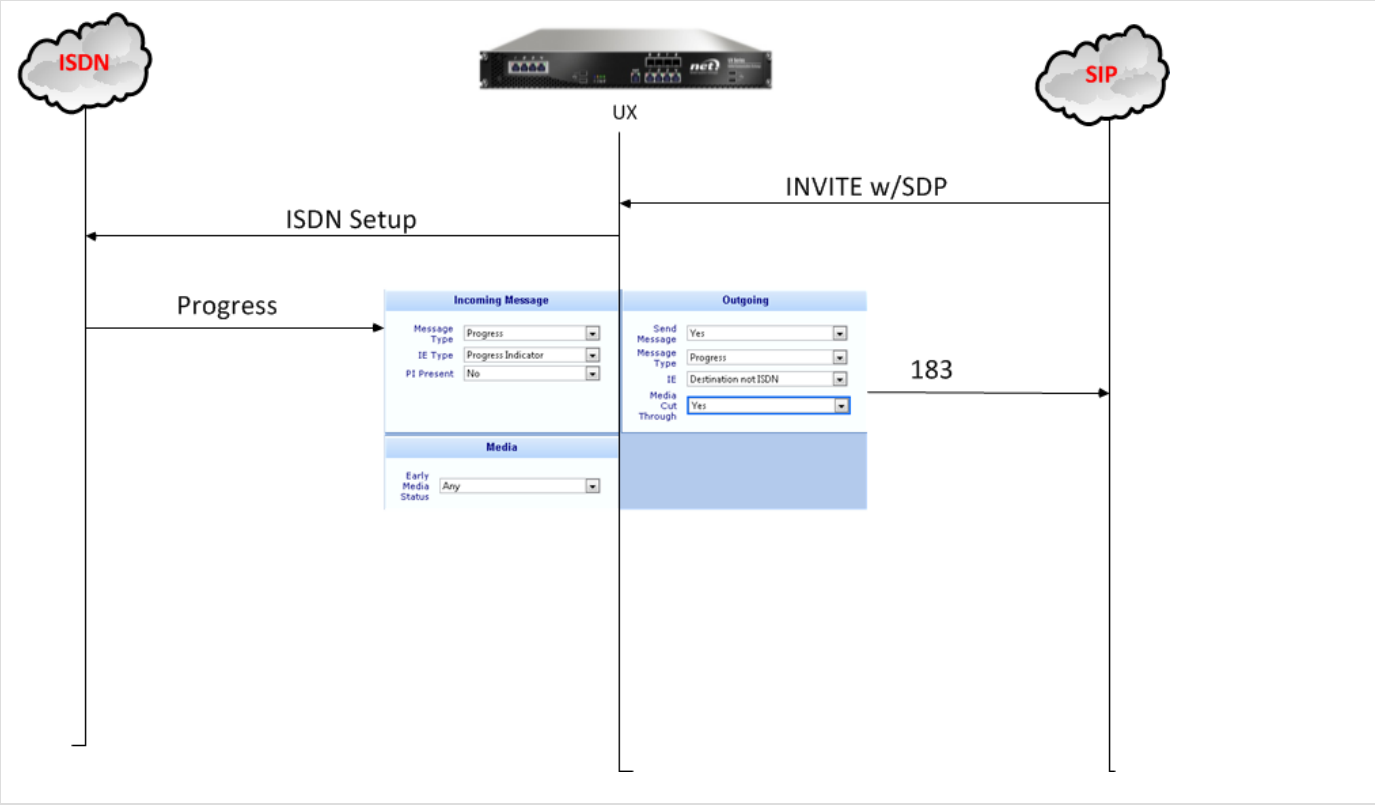
- Basic Message Translation
- How does the Message Translation Table work?
  - Incoming Message Matching
  - Special Considerations for Incoming Matching
  - Outgoing Message Translation
  - Media Cut Through
- Mismatching Input Translation Criteria
- Examples of Full Translations
- Invoking a Translation Table
- Message Translation Reference

Basic Message Translation

Looking at the diagram below:

- We can see an SIP INVITE to the Sonus SBC 1000/2000
- Which results in the Sonus SBC 1000/2000 generating an ISDN Setup.
- As the ISDN network routes the call, it returns a PROGRESS to the Sonus SBC 1000/2000.
- In turn, the Sonus SBC 1000/2000 sends a 183 to the SIP endpoint.

Whether it sends the 183 with or without SDP, or whether it even sends a 183, is controlled by the Sonus SBC 1000/2000's internal, pre-programmed translation table. The internal translation table controls the translation for ISDN Progress/Alert/Connect messages, as well as SIP 18x/200 messages for calls ISDN ? SIP, SIP ? ISDN, and SIP ? SIP.



How does the Message Translation Table work?

Although the internal translation table works for the majority of installations, it may be necessary to customize a translation. This is accomplished by creating an entry in the Message Translation table that

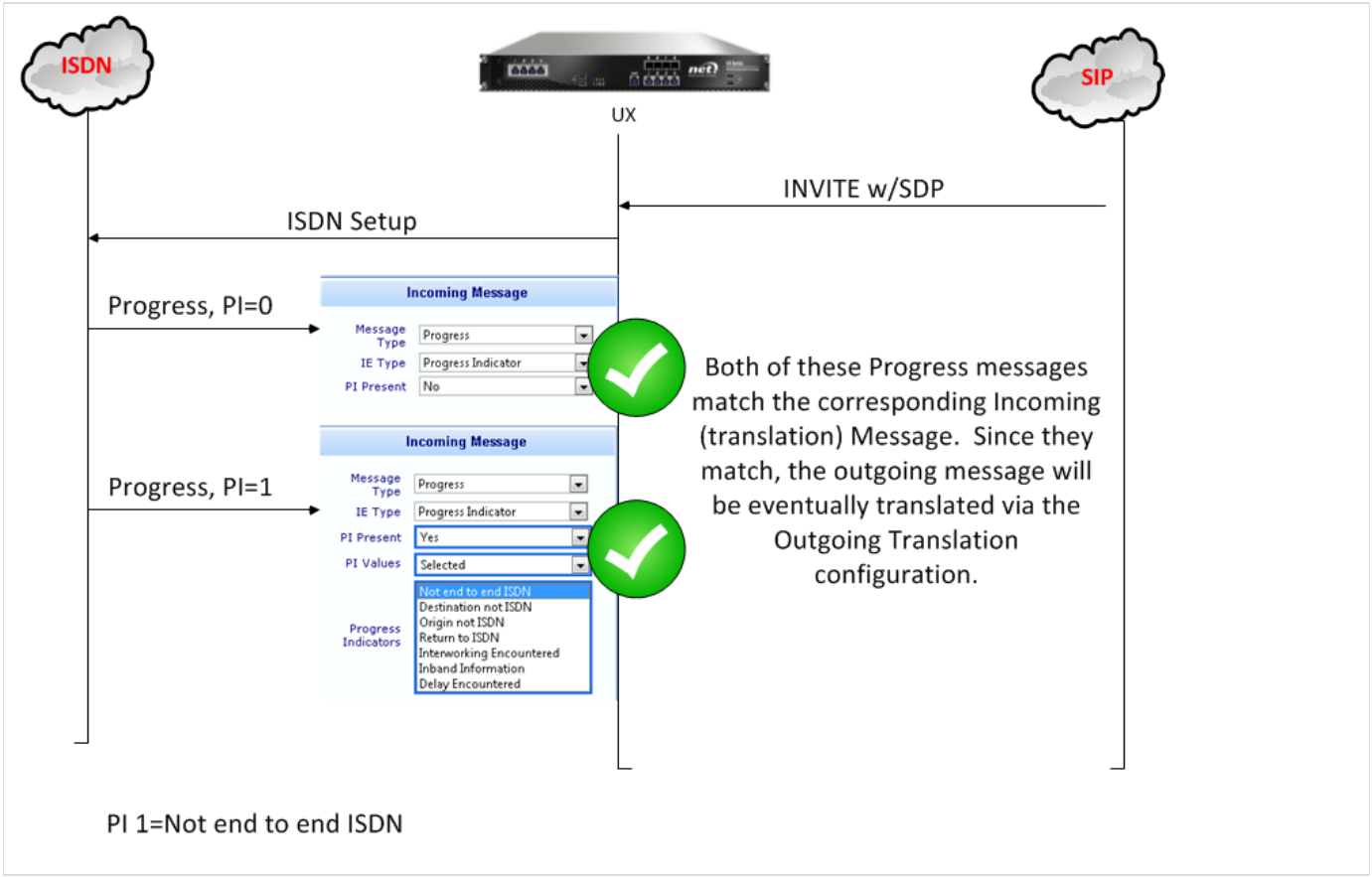
Copyright © 2015 Sonus Networks. All rights reserved.

1. Identifies specific incoming messages and
2. Converts them to the desired output.

Incoming Message Matching

The first phase of the the Message Translation table works on the incoming message. When a message arrives, it is checked against all of the translations entries in the table, specifically the *Incoming Message* configuration.

Below a Progress with no Progress Indicator (PI=0) is shown with it's matching Incoming Message configuration. Similarly, a Progress with PI=1 (Not end to end ISDN) is shown with it's matching Incoming Message configuration.



Special Considerations for Incoming Matching

Copyright © 2015 Sonus Networks. All rights reserved.

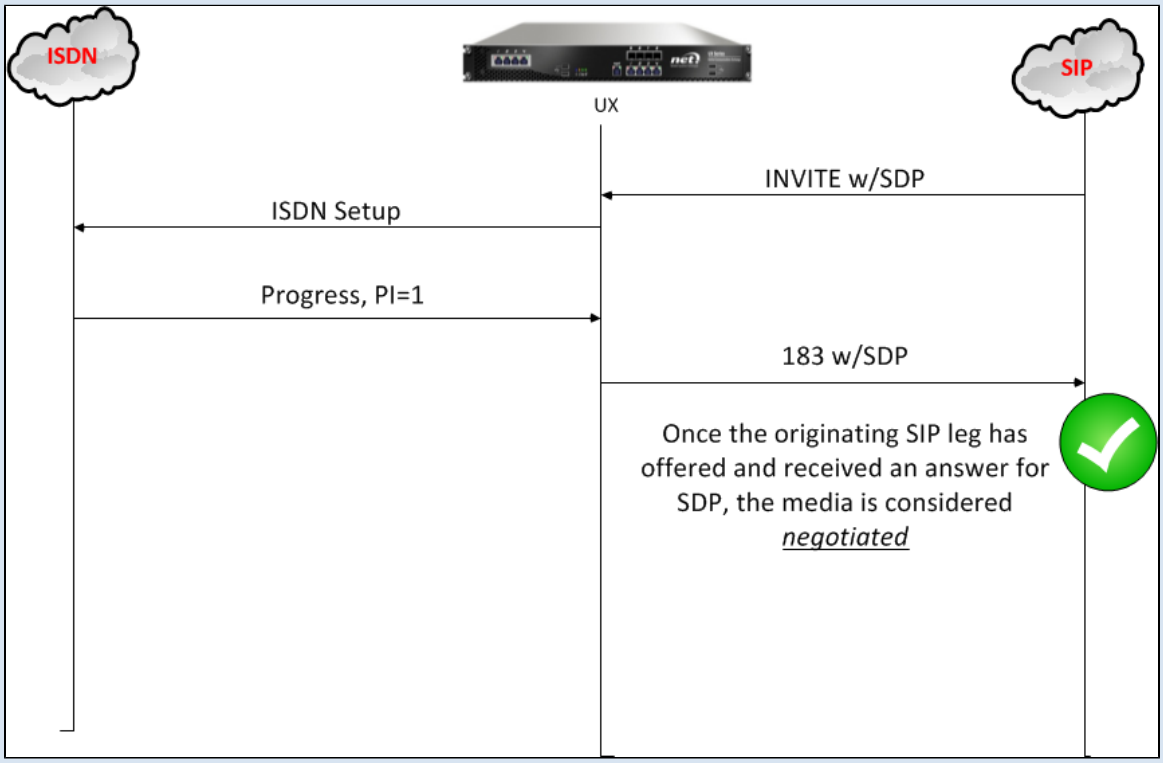
What is _SDP Media Negotiation_?

SIP uses SDP to negotiate media connections. To establish a common media framework (codec, endpoint addresses, etc), an endpoint will send an SDP Offer - a list of the media that the endpoint can support. The recipient will Answer the SDP Offer with a list of media attributes that it endpoint will support for this particular session.

Click here to see an example of Media Negotiation

In the diagram below, an INVITE with SDP is sent to the Sonus SBC 1000/2000. This SDP is an Offer - a list of the media that the endpoint is offering to support. Later, the Sonus SBC 1000/2000 replies with a 183 with SDP, essentially Answering the Offer with a media list that is acceptable for communication.

Once an SDP Offer has been Answered, the media is said to be Negotiated. Both sides are now able to send media based upon the negotiated SDP parameters.



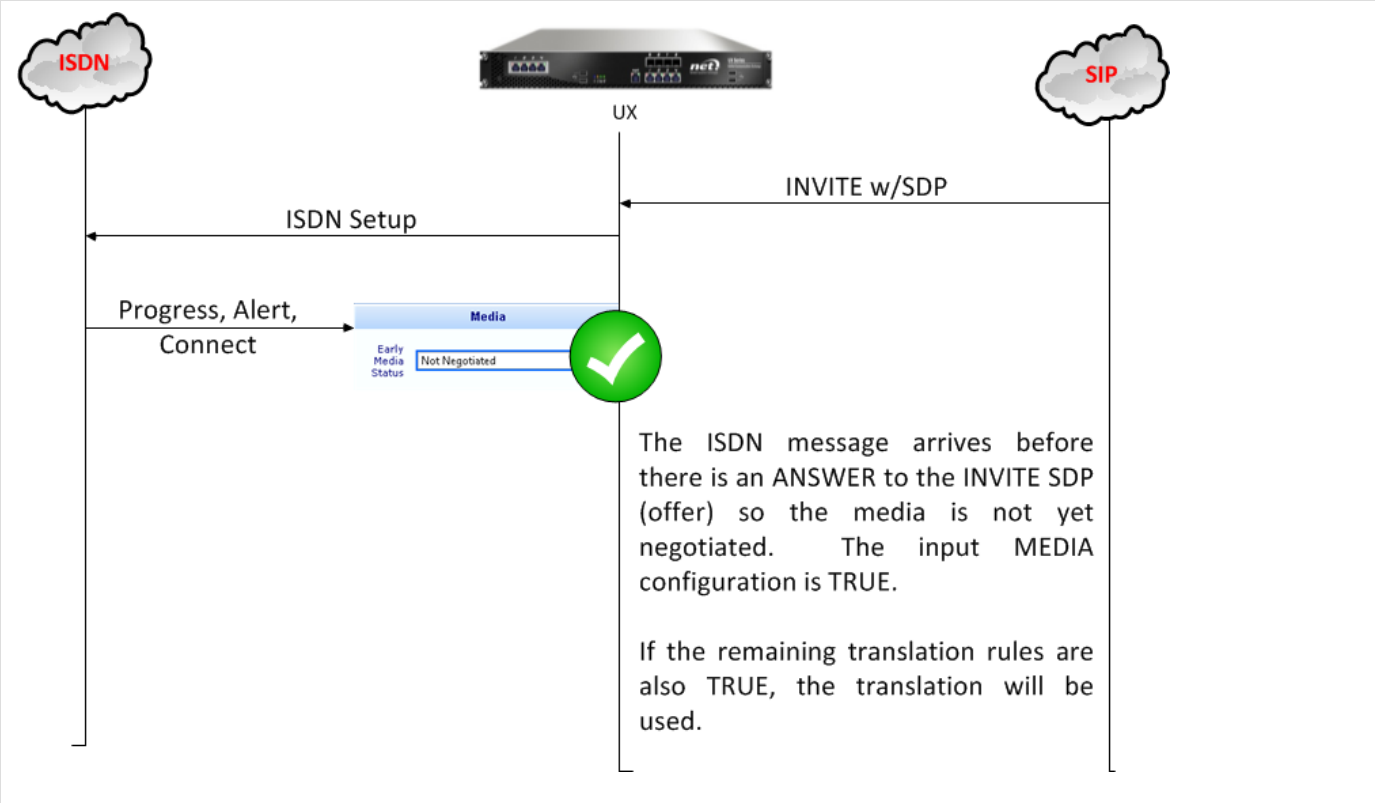
The Media Input Matching Type

Some applications cannot accept additional SDPs once the media has been negotiated, so the Sonus SBC 1000/2000 includes an additional Incoming Message criteria that permits a translation to be matched based on whether media negotiation has been completed.

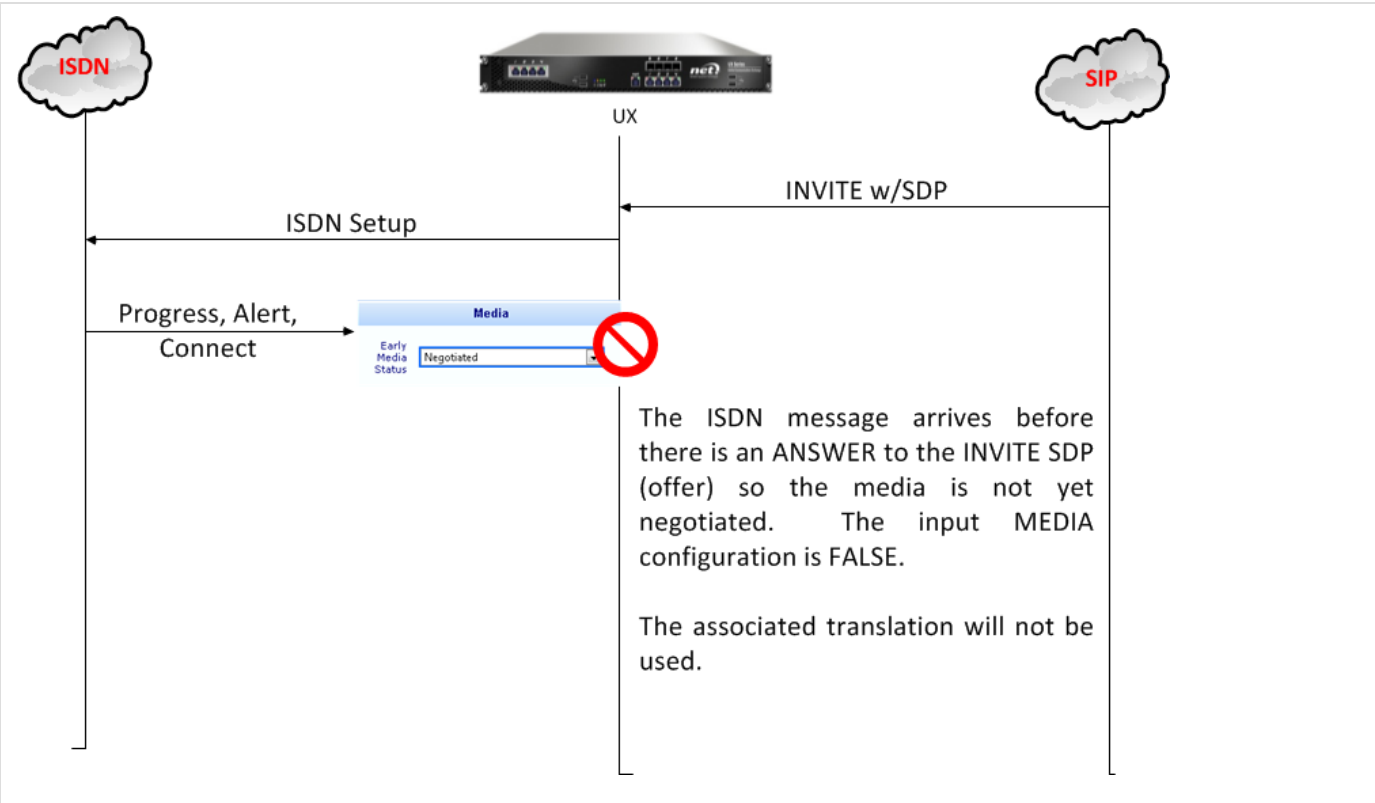
- Configuring the *Early Media Status* to *Negotiated* means that the incoming message will only be translated if the media is already negotiated
- Configuring the *Early Media Status* to *Not Negotiated* means that an incoming message will only be translated if the media has not yet been negotiated.

In the example below, the *Early Media Status* is set to *Not Negotiated*. As the SIP SDP Offer has not yet been answered, the media is indeed not yet negotiated and, therefore, the match passes. If the remaining Incoming Message matches as well, the translation entry will be used to translate the message to the SIP side.

Copyright © 2015 Sonus Networks. All rights reserved.



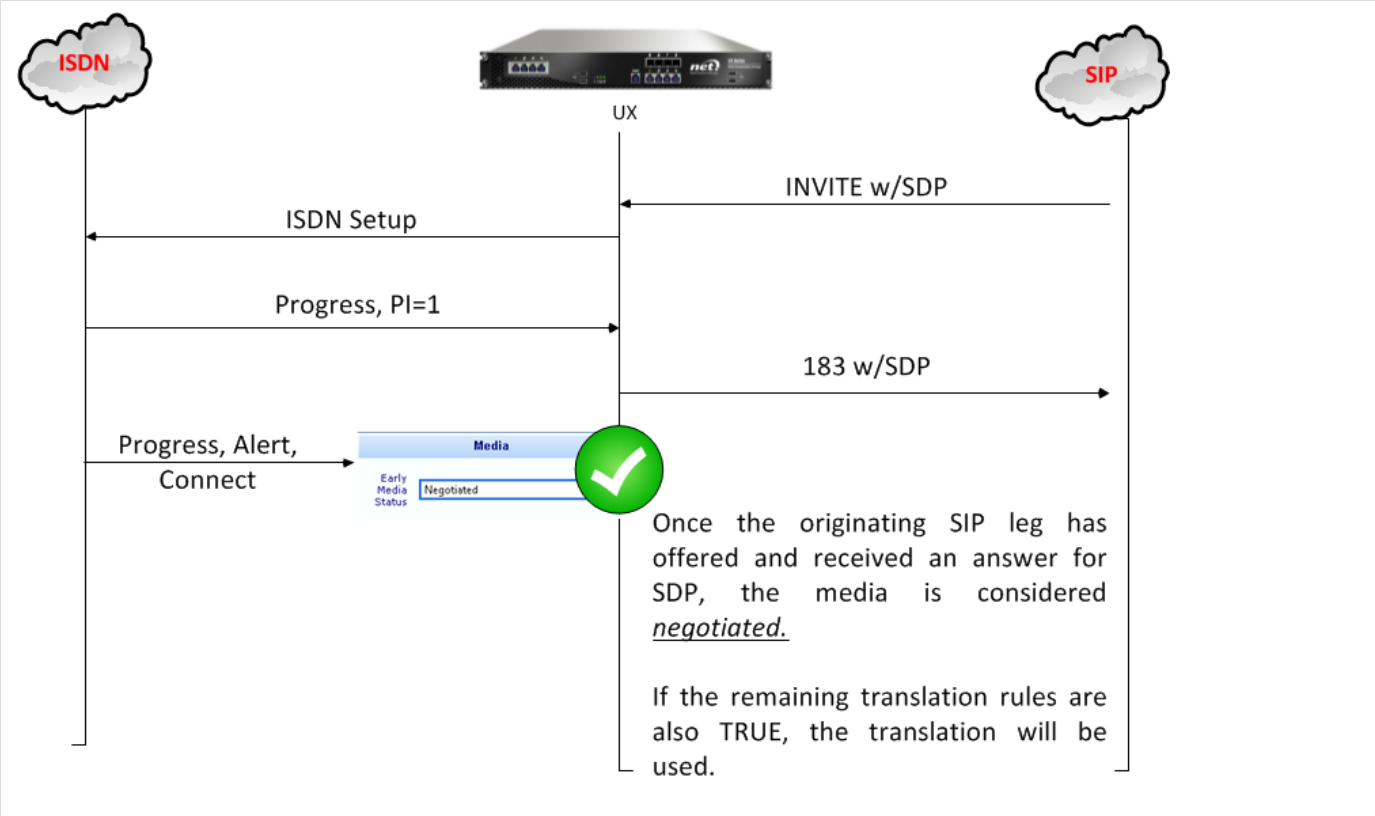
In the example below, the *Early Media Status* is set to *Negotiated*. Since the media has yet to be negotiated (no SDP Answer has been sent), the match fails. That particular translation entry fails. The next translation entry, if there is one, will be checked.



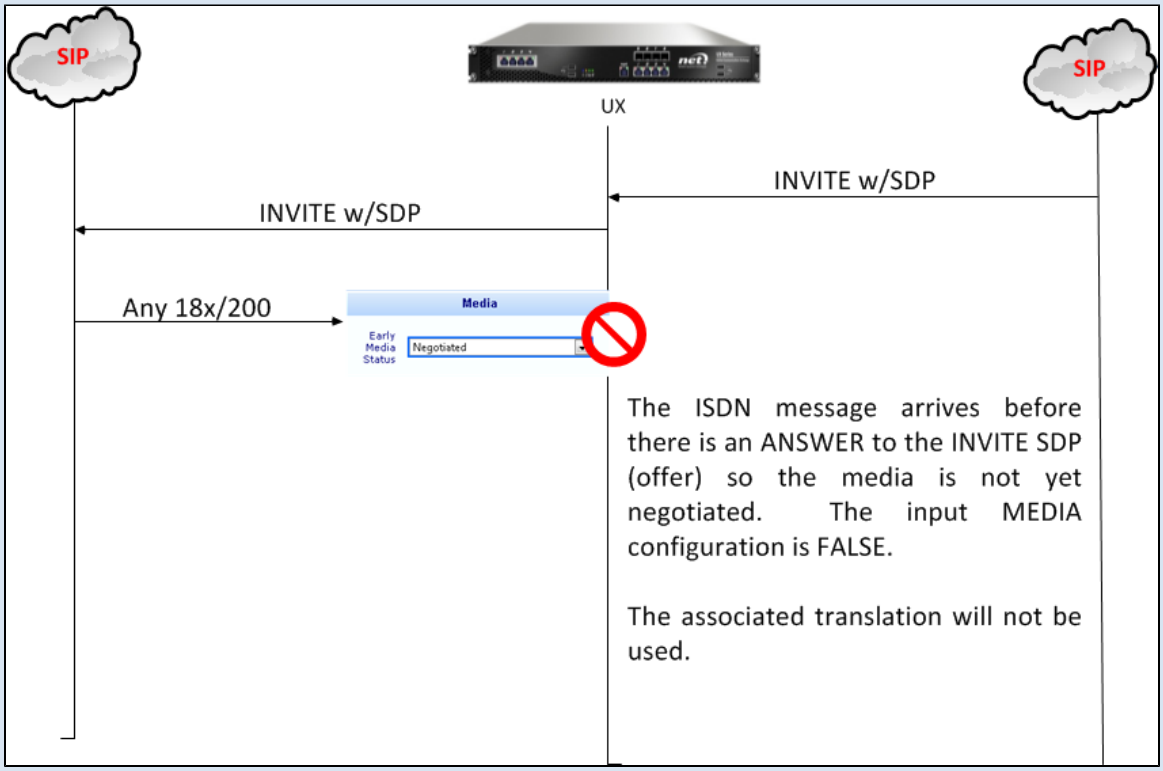
In the example below, the media has been negotiated therefore *Early Media Status* will be matched. If the rest of the

Copyright © 2015 Sonus Networks. All rights reserved.

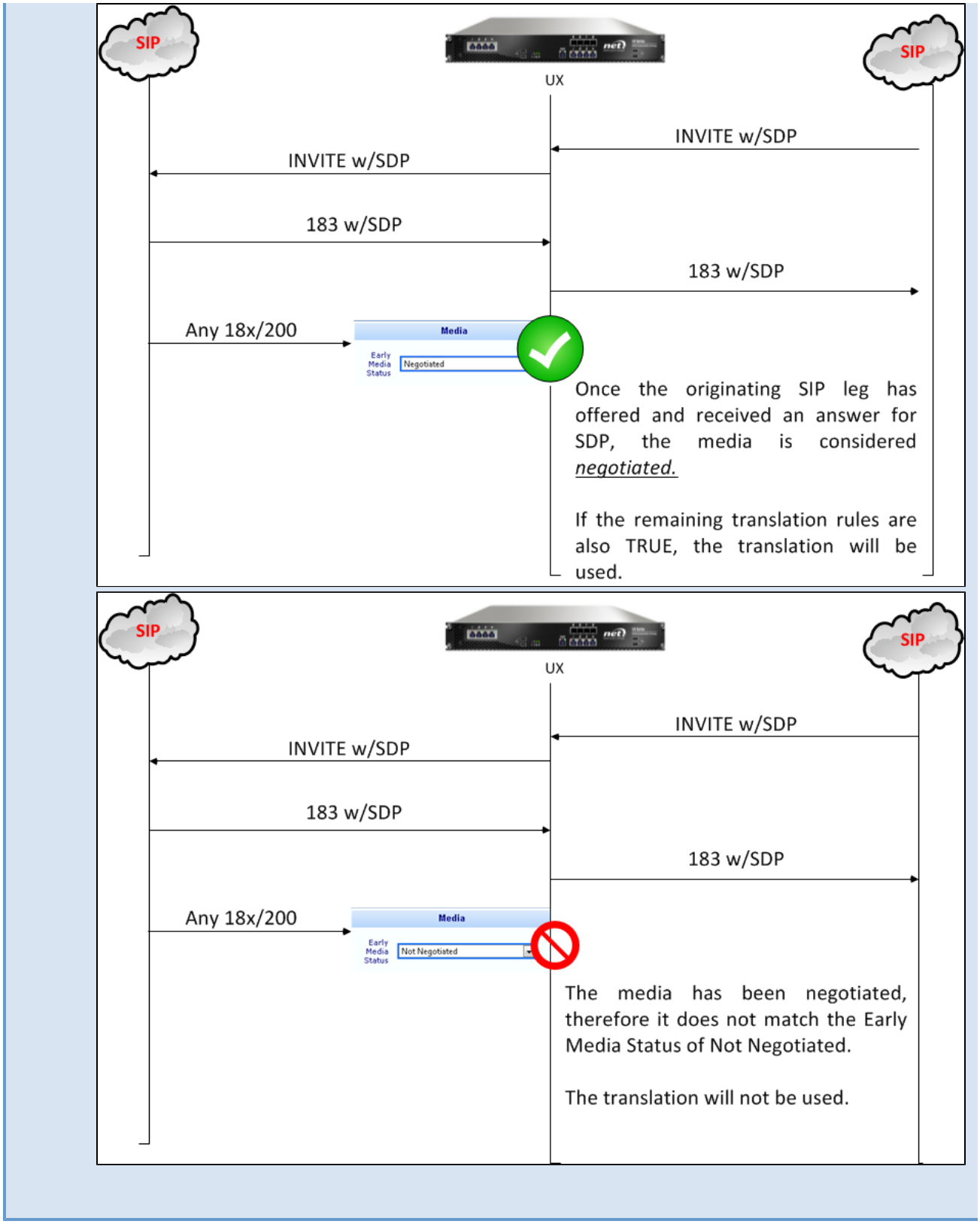
Incoming Message translation is matched, that translation will be used.



The same Early Media Status configuration also works for SIP to SIP calls. Click here to see the Incoming Message configuration for SIP messages

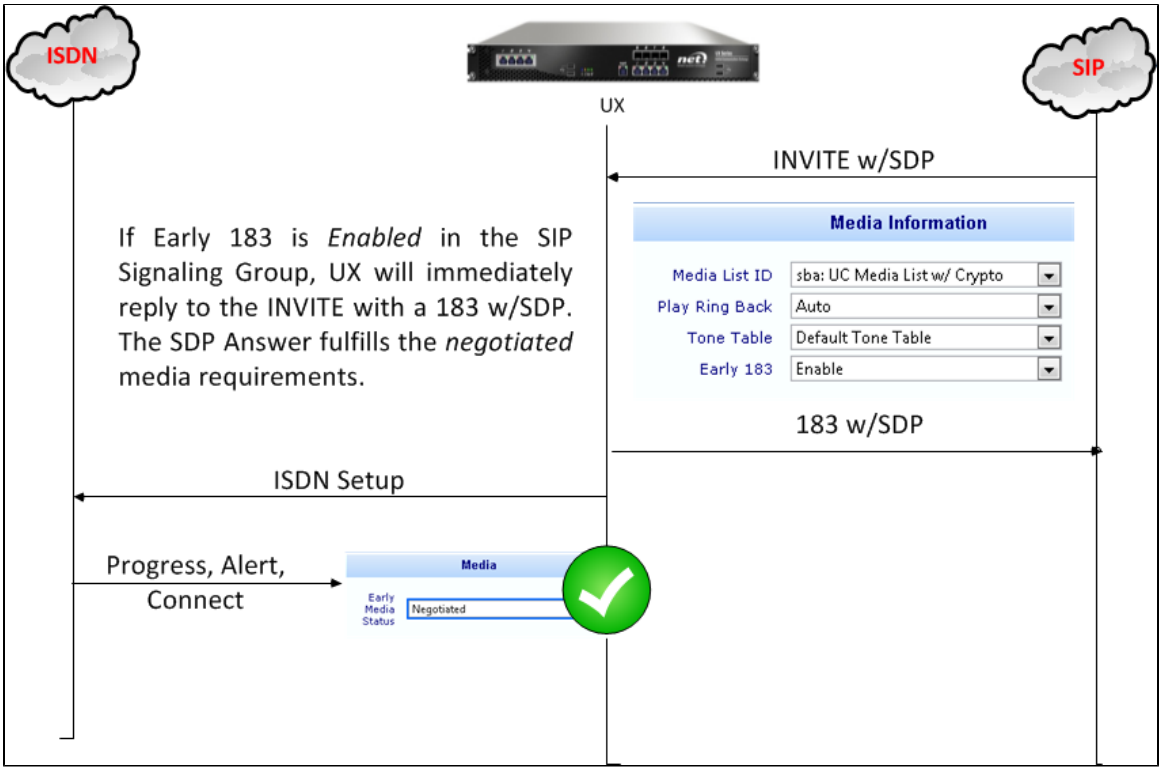


Copyright © 2015 Sonus Networks. All rights reserved.



Early 183 and Negotiated Media

Copyright © 2015 Sonus Networks. All rights reserved.



Setting the *Early Media Status* to *ANY* causes the translation to ignore the media state.

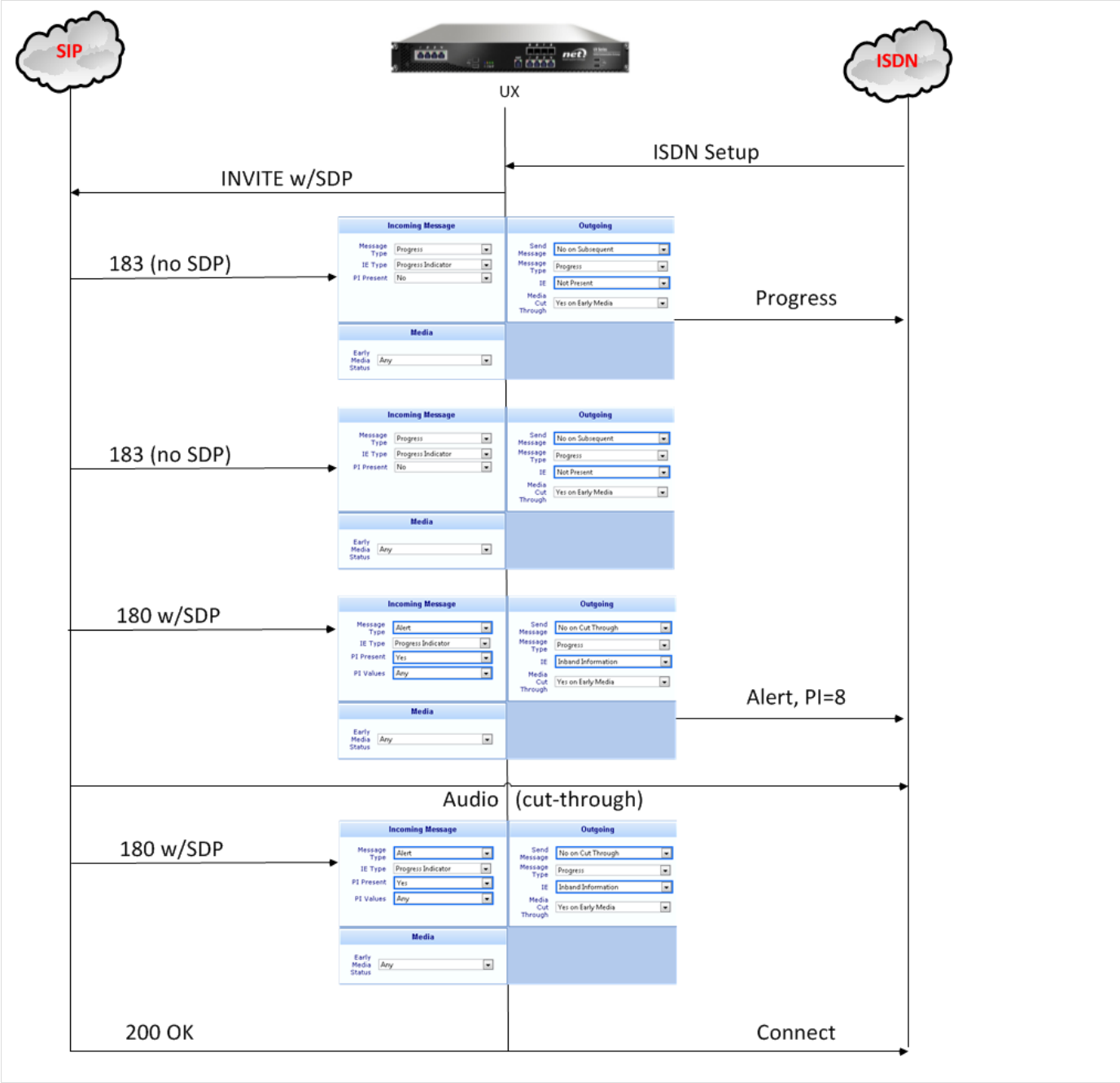
Because ISDN does not have a concept of negotiated media, set the *Early Media Status* to *ANY* for a translation that will be used by a call that originates from ISDN.

Outgoing Message Translation

When a incoming message matches in the *Incoming Message* configuration, the second phase of the process is to send an outgoing message that conforms to the corresponding *Outgoing* configuration.
In the call setup below:

- The first 183 matches the *Incoming Message* configuration and the corresponding Progress is sent based upon the *Outgoing* configuration.
- The second 183 also matches, but a Progress is not sent as the *Outgoing* translation configuration is set for *No on Subsequent*.
- The next SIP packet, 180 Ringing w/SDP, matches the *Incoming Message* and is translated accordingly. The SDP indicates early media is available, so the Sonus SBC 1000/2000 begins to receive/send media
- The subsequent 180 Ringing w/ SDP also matches in the *Incoming* configuration; however, it is not translated as the *Outgoing* is configured to *No on Cut Through*.

Copyright © 2015 Sonus Networks. All rights reserved.



The translation table above contains just two entries. Each time a packet arrives, each entry is tried sequentially in top-to-bottom order.

Copyright © 2015 Sonus Networks. All rights reserved.

You might notice that the Incoming Message format remains the same, even when the incoming message is SIP. The Message and IE Types do not change to SIP references because any given translation maybe used for either SIP or ISDN. A ISDN to SIP conversion table (below) will assist in selecting the appropriate desired parameters.

Message Type	SIP Message
Progress	183 Session Progress
Alert	180 Ringing
Connect	200 OK

Most ISDN endpoints do not tolerate receiving more than one Progress or Alert, so the *Outgoing* translation configuration includes *No on Subsquent* and *No on Cut Through* to ensure that only one Progress or Alert is sent regardless of the number of incoming SIP 18X messages. These configuration settings are generally only used for ISDN to SIP calls.

Media Cut Through

The *Media Cut Through* parameter controls how the Sonus SBC 1000/2000 handles early media for calls that have:

- Inband ringing
- Network error messages (like busy and reorder)
- IVR messages that play before CONNECT/200 OK is received

Because the Media Cut Through is part of Message Translation (which is applied at the call route), it is possible to override the Signal Group-level *Play Ringback* setting. In the table below, note how the Media Cut Through configuration interacts with Sonus SBC 1000/2000's Ringback setting.

Ringback Configuration/ Media Cut Through	Yes on Early Media	Yes	No
Auto	Local Ringback until 1st Inband Media	Inband Media	Local Ringback
Always	Local Ringback	Local Ringback	Local Ringback
Never	Inband media	Inband Media	Always silent

Remember that the Play Ringback function is only activated when the Sonus SBC 1000/2000 receives either ALERT or 180.

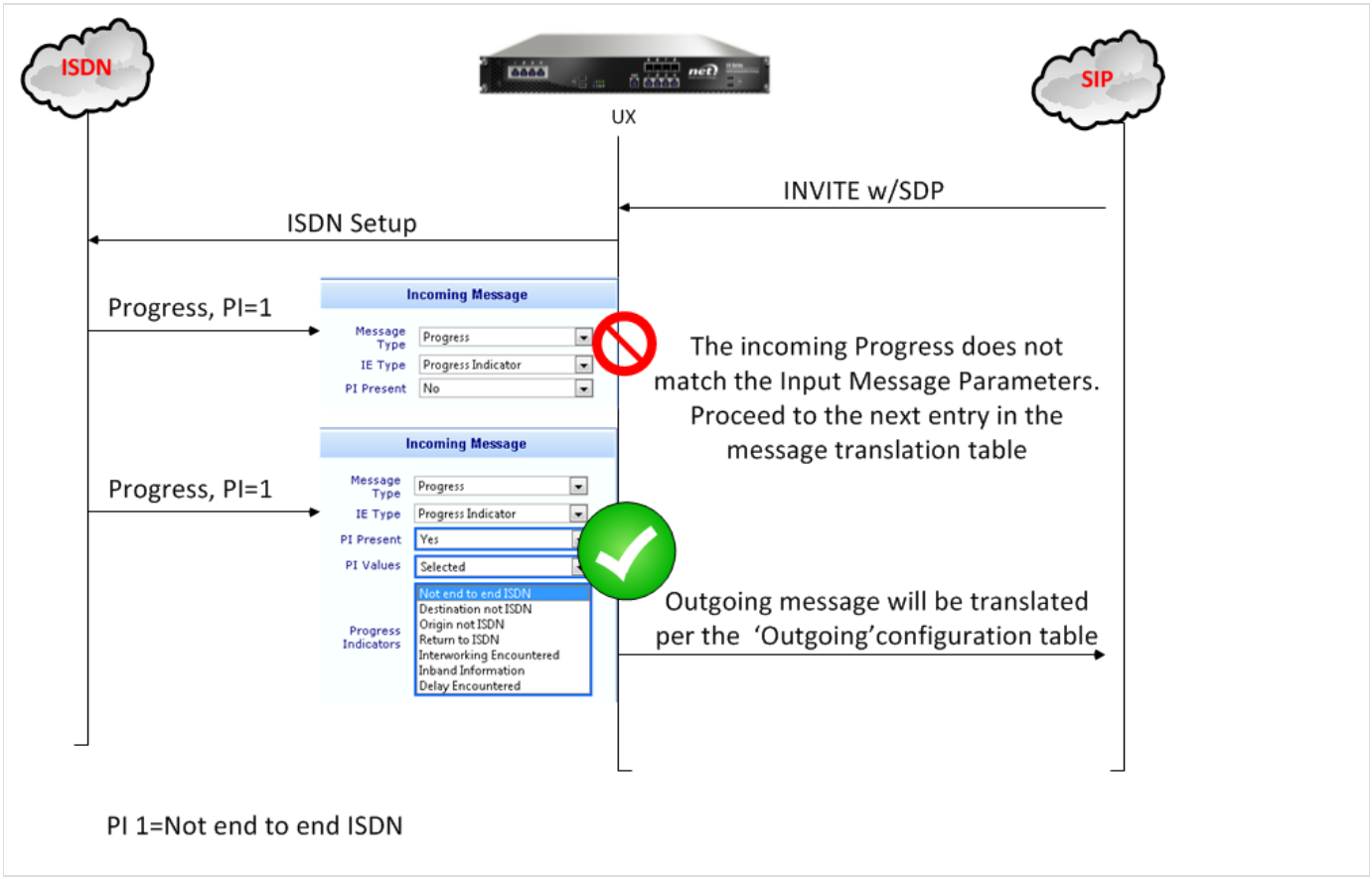
For SIP-originated calls, Media Cut Through should always be configured to *Yes* so that network signals like Busy can always be heard by the caller.

For ISDN-originated calls, configure the Media Cut Through to *Yes on Early Media* if you want the caller to hear inband ringing associated with 183w/SDP.

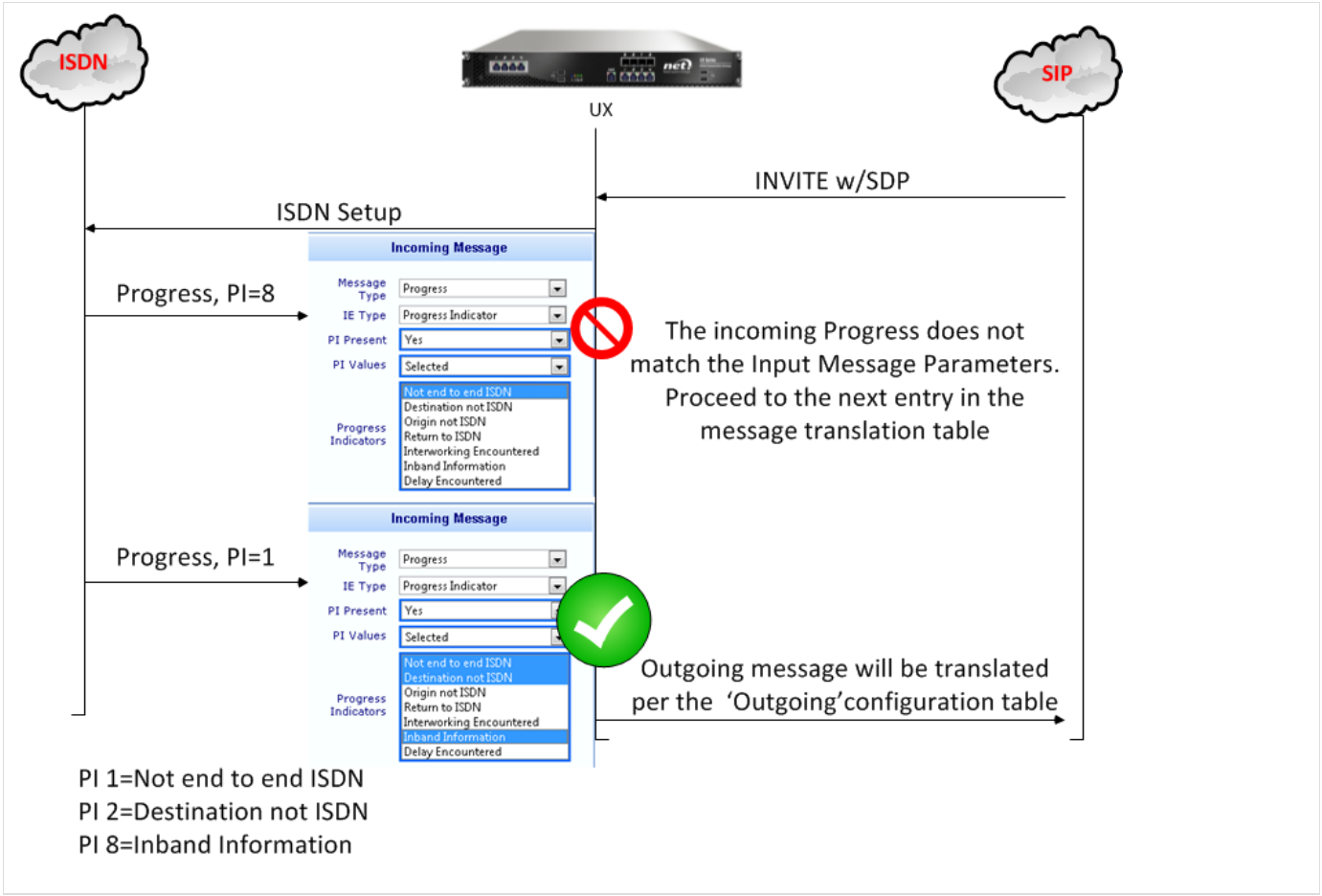
Copyright © 2015 Sonus Networks. All rights reserved.

Mismatching Input Translation Criteria

Below are some additional examples of ISDN messages and which Incoming Message configurations are matched and not matched.



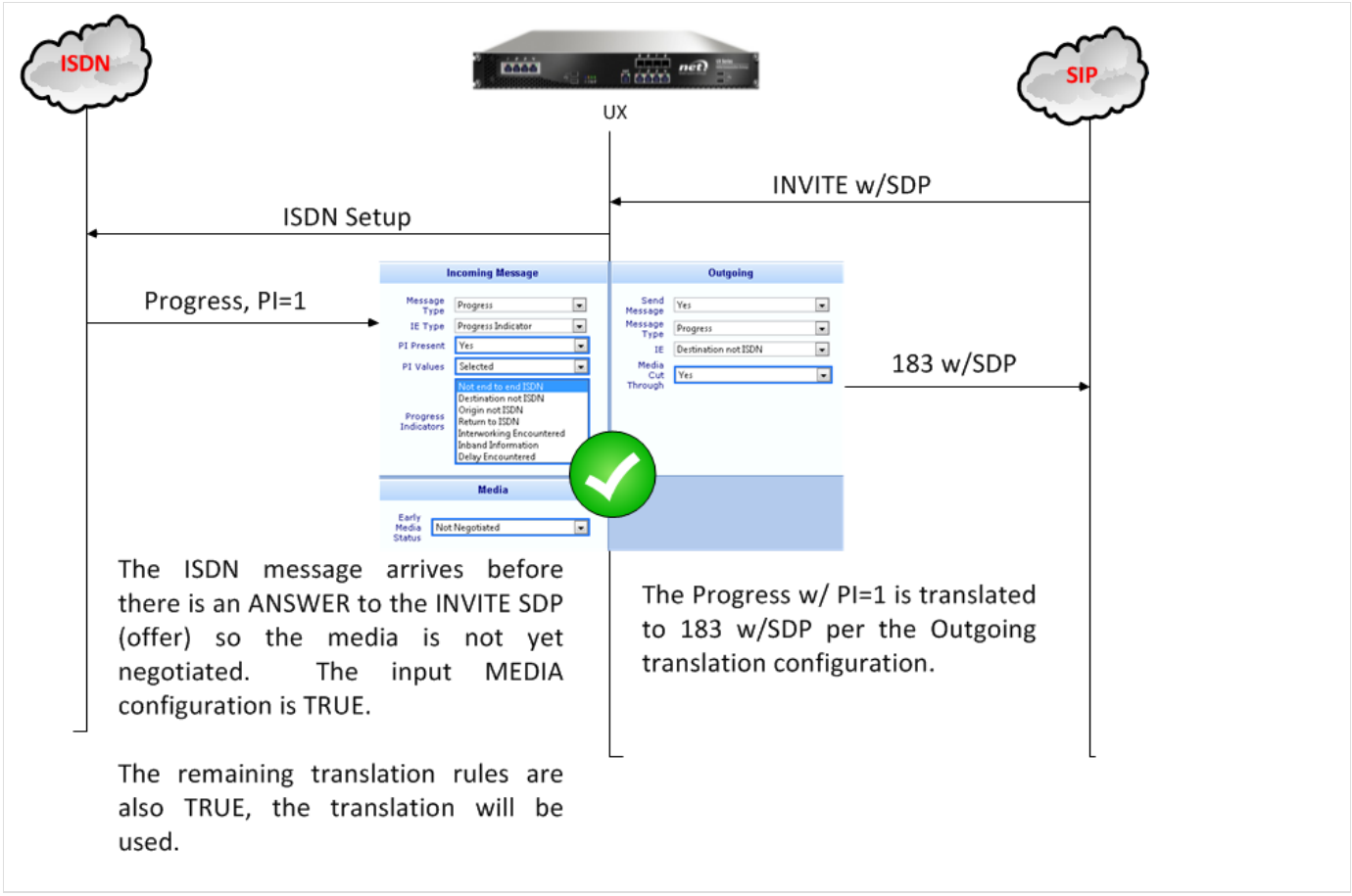
Copyright © 2015 Sonus Networks. All rights reserved.



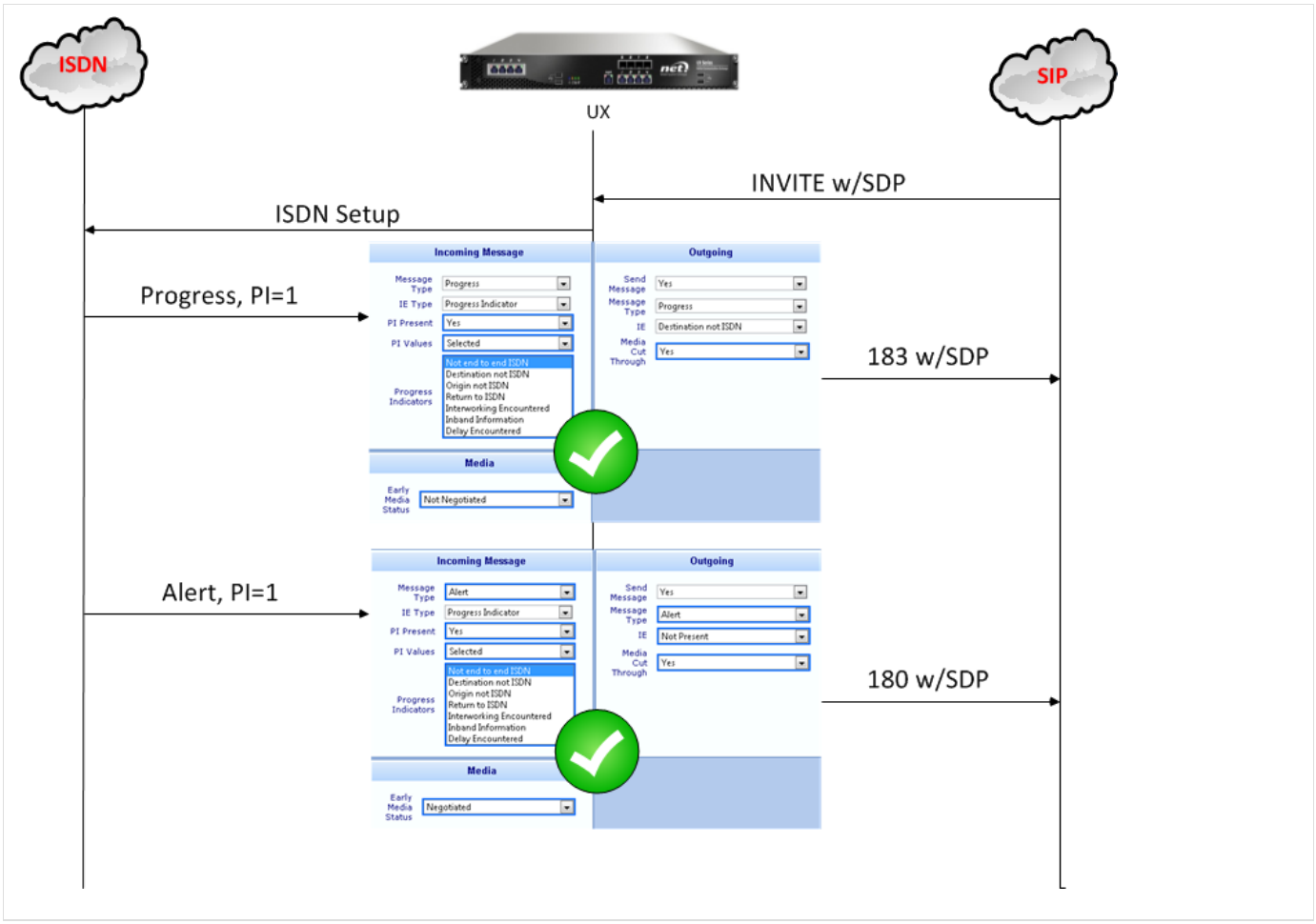
If no match is found, or no table is assigned to the call route, the message is translated using the internal translation table.

Examples of Full Translations

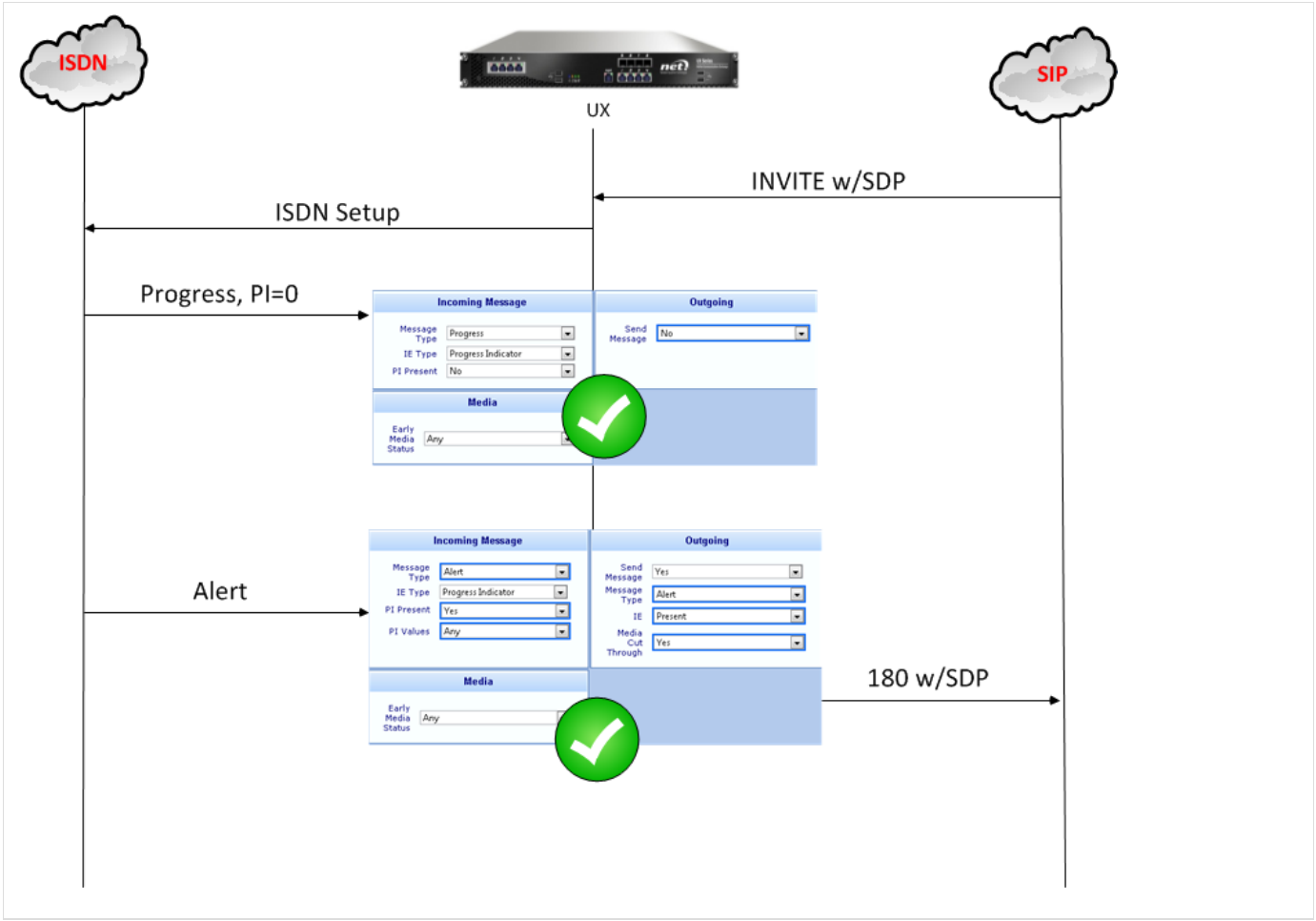
Copyright © 2015 Sonus Networks. All rights reserved.

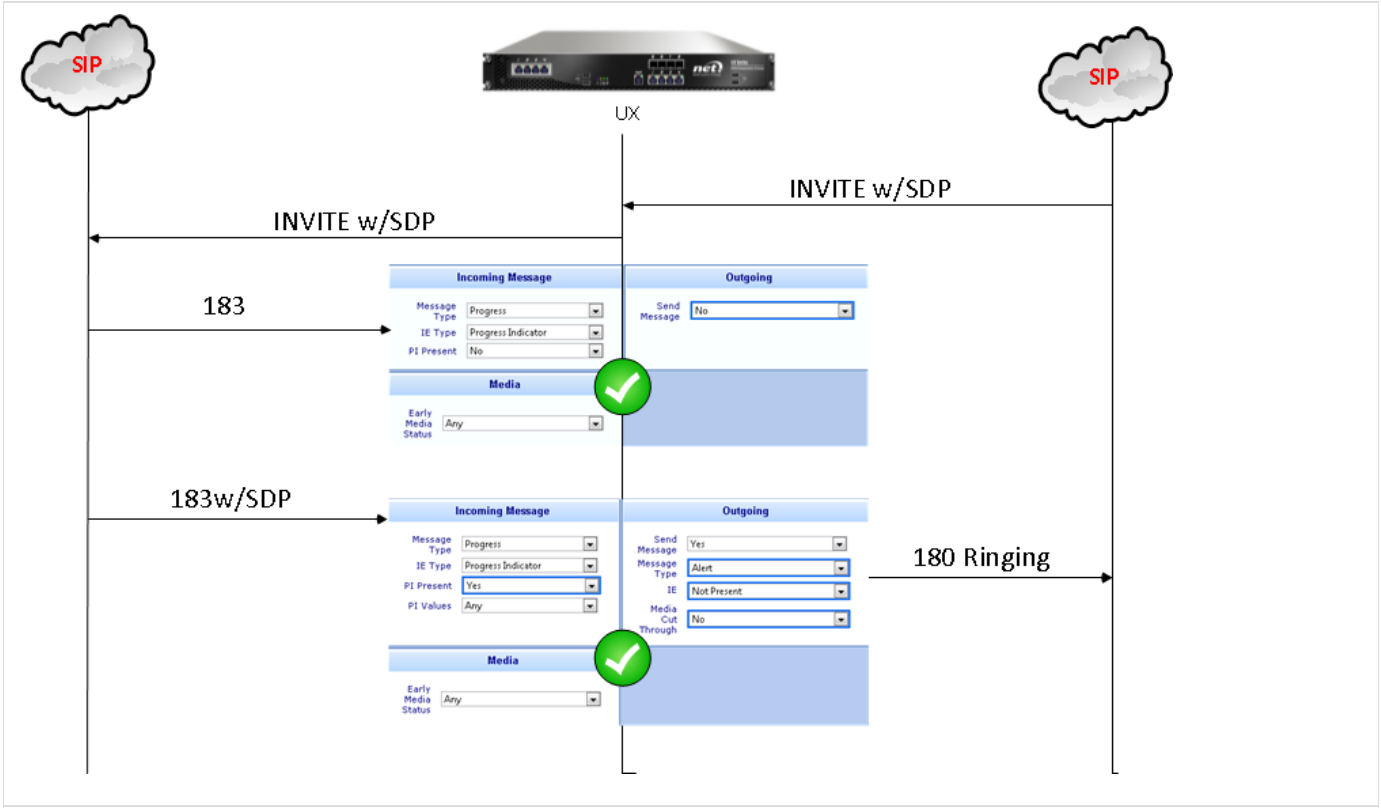


Copyright © 2015 Sonus Networks. All rights reserved.

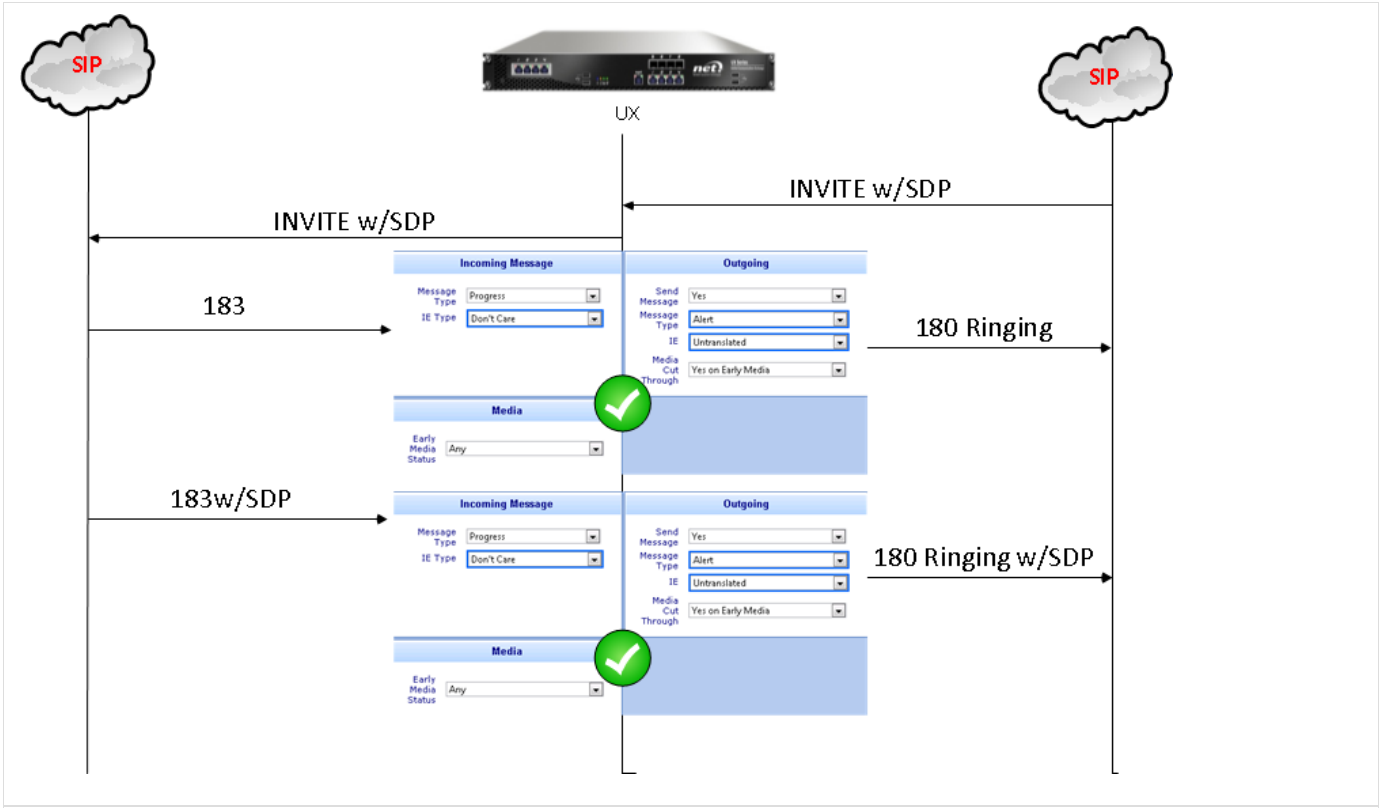


Copyright © 2015 Sonus Networks. All rights reserved.





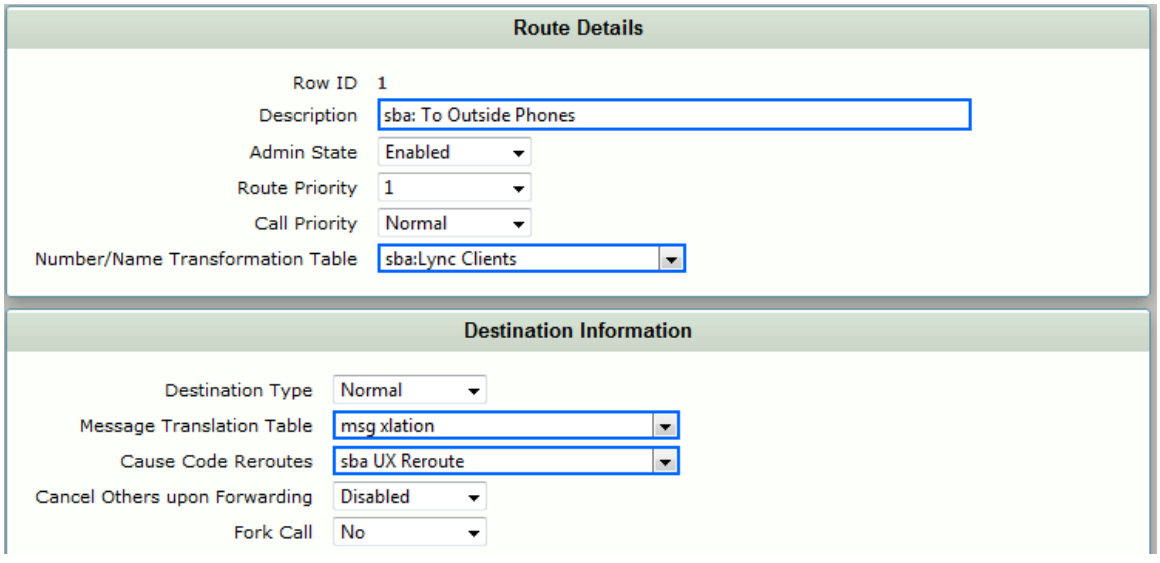
Copyright © 2015 Sonus Networks. All rights reserved.



The above translation is a commonly used to generate ringback when the inbound leg does not provide ALERT or 180.

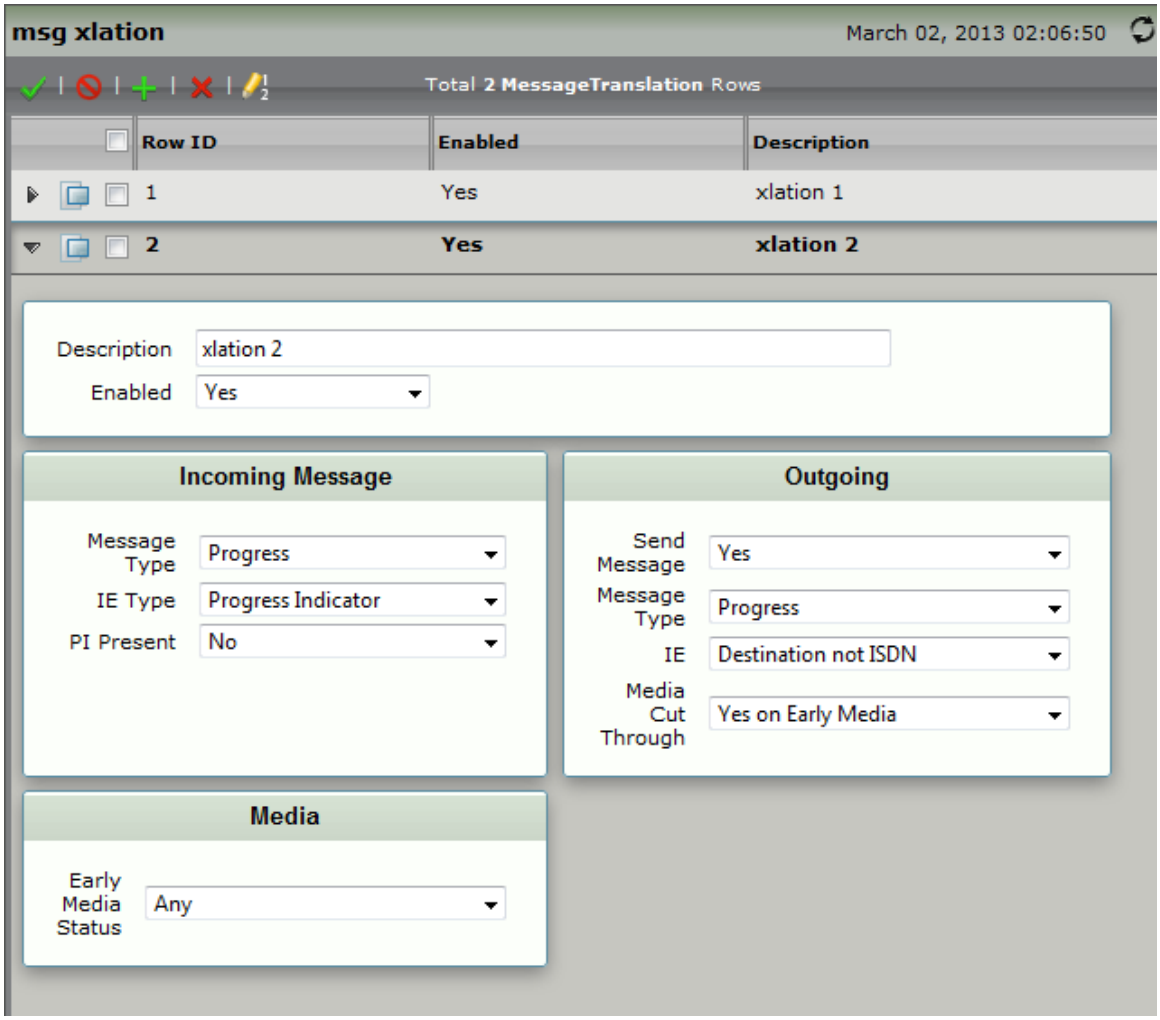
Invoking a Translation Table

Translation Tables are invoked at the Call Route level. The call route (below) is configured to use the Message Translation Table called *msg xlation.*



The *msg xlation* table contains two translation entries (detail for the second entry is displayed).

Copyright © 2015 Sonus Networks. All rights reserved.



When a route containing a message translation table is used to route a call, each reply message is checked again the entries in the selected table.

Message Translation Reference

For a listing of the pre-programmed Message Translations on the Sonus SBC 1000/2000, see Message Translation Reference.

Message Translation Reference

In addition to the Message Translation Usage Overview, the following article contains a listing of the pre-programmed Message Translations on the Sonus SBC 1000/2000.

Before you start - click here to view the ISDN Progress Indicator (PI) assignments

PI	Definition
0	No Progress Indicator included
1	Not end-to-end ISDN

Copyright © 2015 Sonus Networks. All rights reserved.

2	Destination address is not ISDN
3	Origination address is not ISDN
4	Call has returned to ISDN
5	Internetworking Encountered
8	Inband information available
10	Delay Encountered

Internal Translations ISDN to SIP

Listed are the default (internal) *message translations* for ISDN SIP:

#	Incoming ISDN side	Outgoing SIP side	How the Sonus SBC 1000/2000 Internally Processes the Translation
1	**Alert without PI**	**180 Ringing without SDP**	▼ Click here to view **Incoming Filter** **Early Media Status**: Any; **IN Message**: Alert; **IN IE Type**: PI; **IN Progress Indicator**: Not Present **Outgoing Translation** **OUT Message**: Alert; **Send Message**: Yes; **OUT IE**: Not Present; **Media Cut Through**: Yes

Copyright © 2015 Sonus Networks. All rights reserved.

<table>
<tr>
<td>2</td>
<td>Alert with PI 1, 8, 2</td>
<td>180 Ringing; if early media negotiated, don't include SDP</td>
<td>Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Early media negotiated</td><td>Alert</td><td>PI</td><td>1 | 8 | 2</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Alert</td><td>Yes</td><td>Not Present</td><td>Yes</td></tr>
</table>
</td>
</tr>
<tr>
<td>3</td>
<td>Alert with PI 1, 8, 2</td>
<td>180 Ringing; if early media not negotiated, include SDP</td>
<td>Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Early media not negotiated</td><td>Alert</td><td>PI</td><td>1 | 8 | 2</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Alert</td><td>Yes</td><td>Present</td><td>Yes</td></tr>
</table>
</td>
</tr>
</table>

Copyright © 2015 Sonus Networks. All rights reserved.

<table>
<tr>
<td>4</td>
<td>Progress with PI 1, 8, 2</td>
<td>183 Progress; if early media negotiated, don't include SDP</td>
<td>Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Early media negotiated</td><td>Progress</td><td>PI</td><td>1 | 8 | 2</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Progress</td><td>Yes</td><td>Not Present</td><td>Yes</td></tr>
</table>
</td>
</tr>
<tr>
<td>5</td>
<td>Progress with PI 1, 8, 2</td>
<td>183 Progress; if early media not negotiated, include SDP</td>
<td>Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Early media not negotiated</td><td>Progress</td><td>PI</td><td>1 | 8 | 2</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Progress</td><td>Yes</td><td>Present</td><td>Yes</td></tr>
</table>
</td>
</tr>
</table>

Copyright © 2015 Sonus Networks. All rights reserved.

<table>
<tr>
<td>6</td>
<td>Progress with PI 3, 4</td>
<td>183 Progress without SDP</td>
<td>Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Any</td><td>Progress</td><td>PI</td><td>3 | 4</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Progress</td><td>Yes</td><td>Not Present</td><td>Yes</td></tr>
</table>
</td>
</tr>
<tr>
<td>7</td>
<td>Progress without PI</td>
<td>Drop message</td>
<td>Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Any</td><td>Progress</td><td>PI</td><td>Not Present</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Progress</td><td>No</td><td>N/A</td><td>N/A</td></tr>
</table>
</td>
</tr>
</table>

Please note that ISDN SIP message translations are only used on SIP ISDN calls.

Internal Translations SIP to ISDN

Listed are the default (internal) *message translations* for SIP ISDN:

#	Incoming SIP side	Outgoing ISDN side	How the Sonus SBC 1000/2000 Internally Processes the Translation

Copyright © 2015 Sonus Networks. All rights reserved.

<table>
<tr>
<td>1</td>
<td>180 Ringing without SDP</td>
<td>Alerting without PI</td>
<td>Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Any</td><td>Alert</td><td>PI</td><td>Not Present</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Alert</td><td>No on cut through</td><td>Not Present</td><td>Yes On Early Media Detection</td></tr>
</table>
</td>
</tr>
<tr>
<td>2</td>
<td>180 Ringing with SDP</td>
<td>Alerting with PI = 8</td>
<td>Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Any</td><td>Alert</td><td>PI</td><td>Present</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Alert</td><td>No on cut through</td><td>PI=8</td><td>Yes On Early Media Detection</td></tr>
</table>
</td>
</tr>
<tr>
<td>3</td>
<td>183 Progress without SDP</td>
<td>Progress with PI = 1</td>
<td>Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Any</td><td>Progress</td><td>PI</td><td>Not Present</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Progress</td><td>No on subsequent</td><td>PI=1</td><td>Yes On Early Media Detection</td></tr>
</table>
</td>
</tr>
</table>

Copyright © 2015 Sonus Networks. All rights reserved.

<table>
<tr>
<td>4</td>
<td>183 Progress SDP</td>
<td>Progress with PI = 8</td>
<td>▼ Click here to view
Incoming Filter
<table>
<tr><th>Early Media Status</th><th>IN Message</th><th>IN IE Type</th><th>IN Progress Indicator</th></tr>
<tr><td>Any</td><td>Progress</td><td>PI</td><td>Present</td></tr>
</table>
Outgoing Translation
<table>
<tr><th>OUT Message</th><th>Send Message</th><th>OUT IE</th><th>Media Cut Through</th></tr>
<tr><td>Progress</td><td>No on subsequent</td><td>PI=8</td><td>Yes On Early Media Detection</td></tr>
</table>
</td>
</tr>
</table>

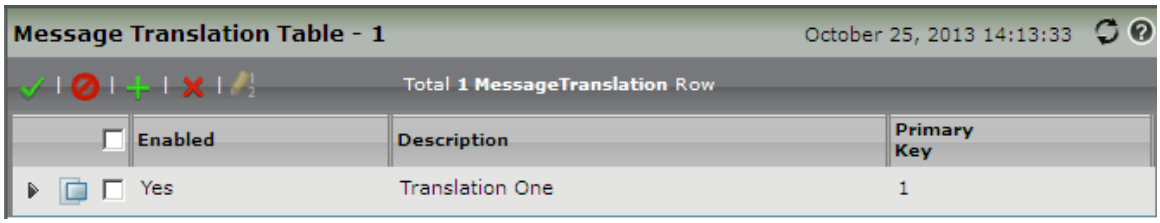
⚠ Please note that SIP ISDN message translations are only used on ISDN SIP calls.

Creating and Modifying Entries to Message Translation Tables

Message translation tables allow rules to be put in place so that unusual message interactions during the ringing stage of a call setup can be manipulated such that proper ringback is provided to the originator of the call. For more details, see Message Translation Usage Overview.

To create or modify an Entry to a Message Translation Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Telephony Mapping Tables > Message Translations > Entry**.



Modifying An Entry to a Message Translation Table

1. Click the **expand** (▸) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Resequencing an Entry in a Message Translation Table

1. Click the **Resequence** icon ( ) at the top of the table.
2. Select the row(s) you want to move.
3. Click the **Move Selected Rows Up** ( ) or **Move Selected Rows Down** ( ) icon to reposition the row(s) in the table.
4. Click **Apply**.

Copyright © 2015 Sonus Networks. All rights reserved.

Enabling an Entry in a Message Translation Table

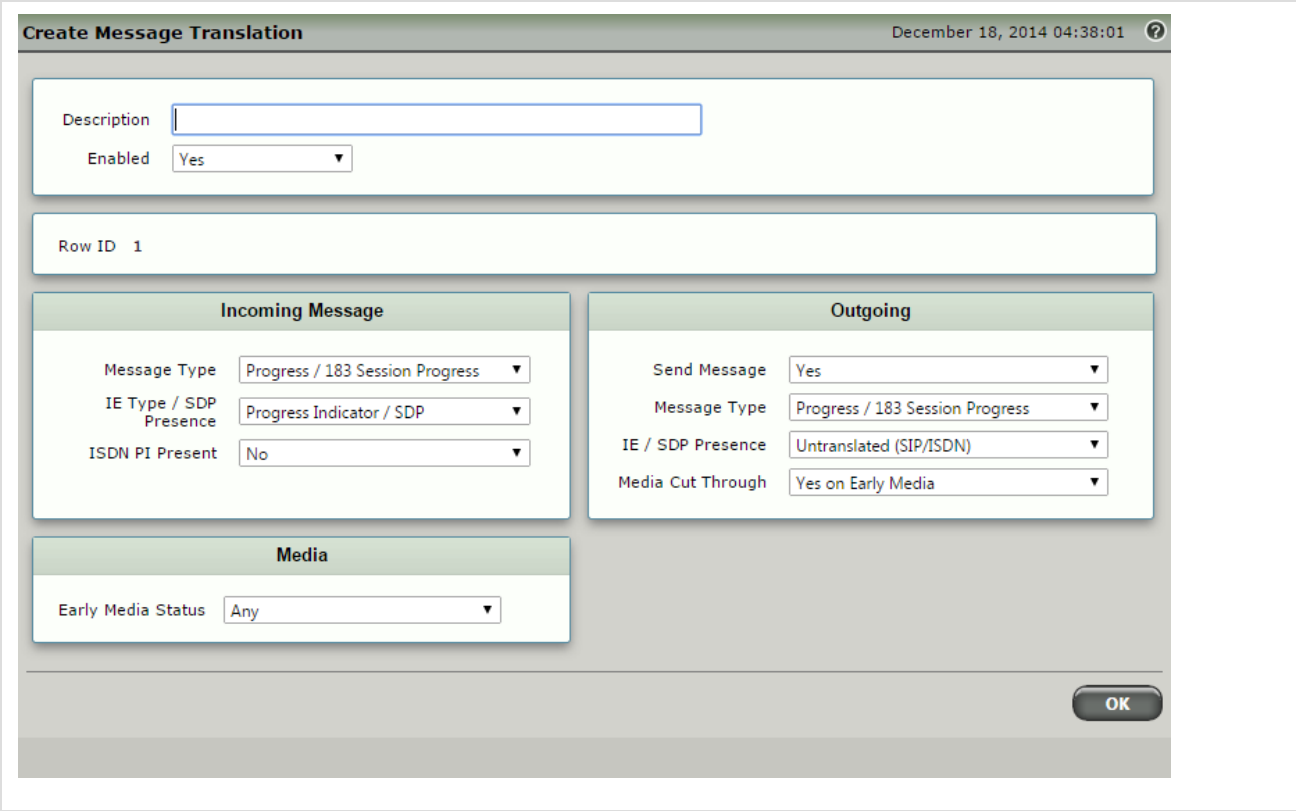
1. Select the check box next to the entry you wish to enable.
2. Click the **Enable** ( ) icon at the top of the table.

Disabling an Entry in a Message Translation Table

1. Select the check box next to the entry you wish to disable.
2. Click the **Disable** ( ) icon at the top of the table.

Creating an Entry to a Message Translation Table

1. Click the **Create Message Translation** ( ) icon.



Incoming Message Panel - Field Definitions

Message Type

Specifies the type of incoming message. Valid options: **Progress**, **Alert**, or **Connect.**

IE Type/SDP Presence

Specifies the Information Element (IE) type/Session Descriptor Protocol to be matched and translated.

ISDN PI Present

Specifies whether or not a Progress Indicator should be present in the message.

Copyright © 2015 Sonus Networks. All rights reserved.

PI Values

Specifies whether or not messages are filtered by a specific PI value or by a specified value. Available only when **Yes** is specified for the Incoming Message PI Present attribute.

Progress Indicators

One or more values may selected as values to match against an incoming message. Only available when **Yes** is selected for PI Present and **Selected** is specified for PI Values.

Outgoing Panel - Field Definitions

Send Message

Specifies when to send an outgoing message.

Message Type

Specifies the type of outgoing translated message. Valid options: **Progress**, **Alert**, or **Connect.**

IE/SDP Presence

Specifies the outgoing translated Information Element (IE) or Session Descriptor Protocol.

Media Cut Through

Specifies the use of media cut-through and when.

Media Panel - Field Definitions

Early Media Status

Specifies the handling for Early media status. Available only when the Incoming Message Type is Progress or Alert.

The available options for this filter are as follows:

- **Any** - this setting will match an incoming message regardless of whether early media has or has not been negotiated
- **Negotiated** - this setting will match an incoming message only if early media has already been negotiated
- **Not Negotiated** - this setting will match an incoming message only if early media has not yet been negotiated

For example, Sonus SBC 1000/2000 can receive 183 Session Progress with SDP and a following 180 Ringing with SDP. Since the early media audio path has already been negotiated with the 183 Session Progress message, Sonus SBC 1000/2000 can strip the SDP from the 180 Ringing. This can be done to either a SIP or an ISDN call leg. In order to do this, you would set the value of the Early Media Status to Negotiated. As a result, the message translation rule will only match calls if the early media path has already been negotiated.

You could also create a message translation rule that will match only if early media path has not been negotiated.

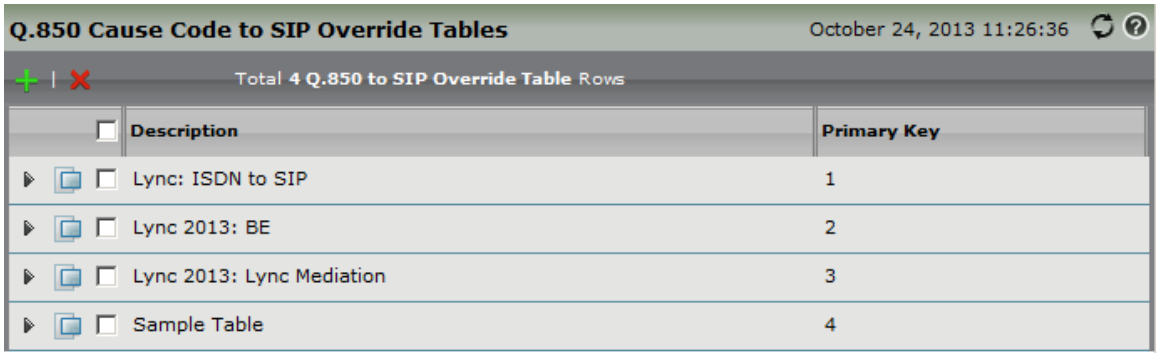
Copyright © 2015 Sonus Networks. All rights reserved.

Managing Q.850 to SIP Override Tables

SIP and ISDN use different response messages to communicate why a call failed or could not be connected (Q.850 for ISDN and SIP Responses for SIP). By default, the Sonus SBC 1000/2000 system uses RFC 3398 to map these to each other. Override Tables allow one to override one or more of these mappings to a different message, which is useful for interoperating with nonstandard equipment. To use a table created here, select it from the Q850 to SIP Override Tables field in a Managing SIP Signaling Groups entry.

Working with Q850 to SIP Override Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Telephony Mapping Tables > Q.850 to SIP Override Tables.**



To view a table's properties:

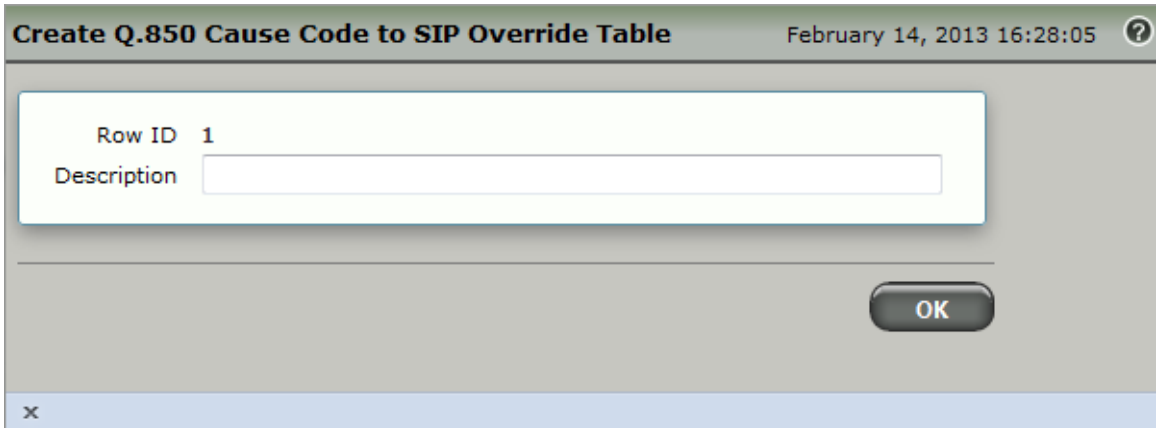
1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

To modify a Q.850 to SIP Override Table:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To create a Q.850 to SIP Override Table:

1. Click the Create ( ) icon.
2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.



Copyright © 2015 Sonus Networks. All rights reserved.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

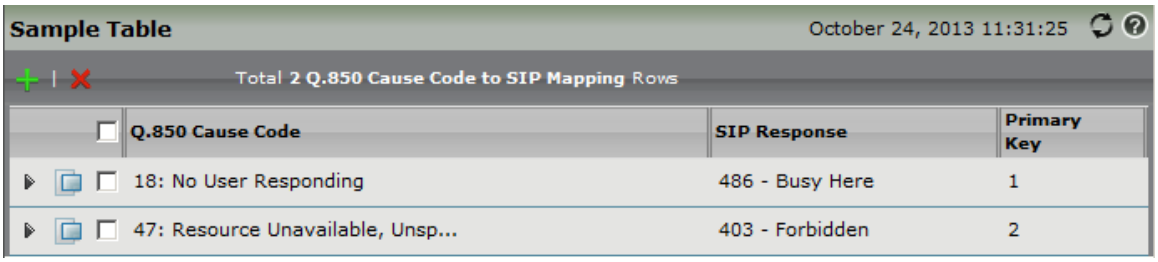
Creating and Modifying Entries to Q.850 to SIP Override Tables

Creating and Modifying Entries to Q.850 to SIP Override Tables

By default, the Sonus SBC 1000/2000 uses RFC 3398 cause code mappings. This table allows Sonus SBC 1000/2000 Administrators to define other cause code mappings between Q.850 and SIP

To create or modify an Entry to a Q.850 to SIP Override Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Telephony Mapping Tables** > **Q.850 to SIP Override Tables** > **Entry**.

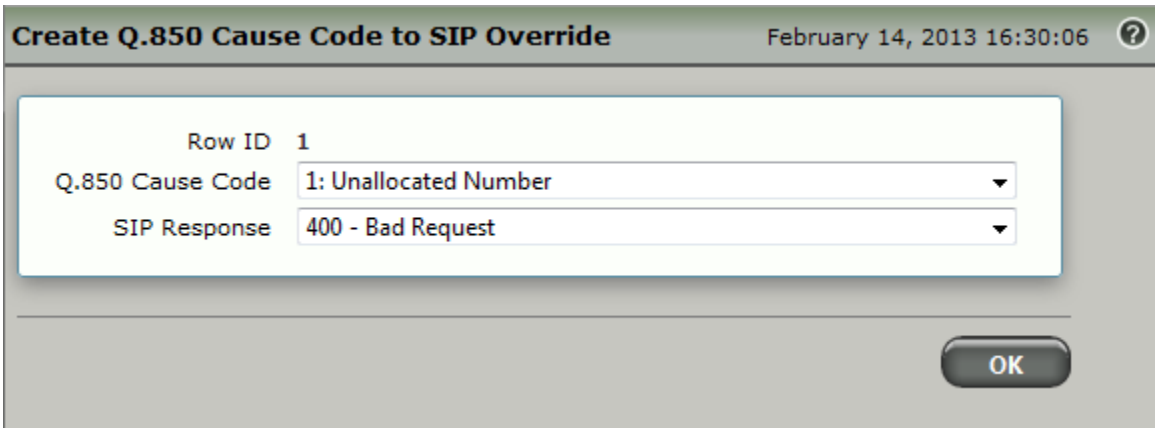


Modifying an Entry in a Q.850 to SIP Override Table

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating an Entry in a Q.850 to SIP Override Table

1. Click the **Create Q.850 Cause Code to SIP Override** ( ) icon.



Copyright © 2015 Sonus Networks. All rights reserved.

Q.850 Cause Code to SIP Override - Field Definitions

Q.850 Cause Code

Specifies the Q.850 Cause Codes to be mapped to a SIP Response Codes.

SIP Response

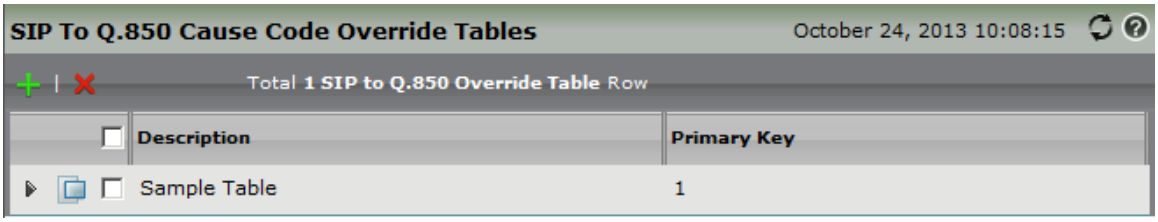
Specifies the SIP Response Codes to which the selected Q.850 Cause Codes is mapped.

Managing SIP to Q.850 Override Tables

SIP and ISDN use different response messages to communicate why a call failed or could not be connected (Q.850 for ISDN and SIP Responses for SIP). By default, the Sonus SBC 1000/2000 system uses RFC 3398 to map these to each other. Override Tables allow you to override one or more of these mappings to a different message, which is useful for interoperating with nonstandard equipment. To use a table created here, select it from the SIP to Q.850 Override Tables field in a SIP Signaling Groups entry.

Working with SIP to Q.850 Override Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Telephony Mapping Tables > SIP to Q.850 Override Tables.**



To view a table's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

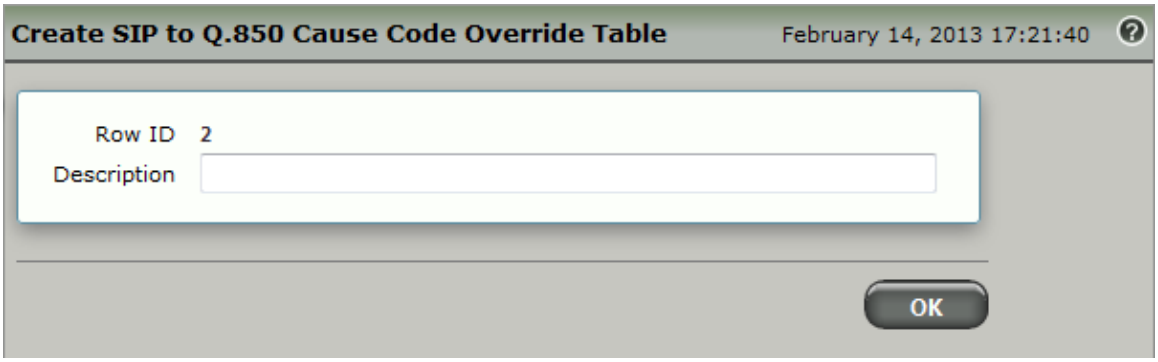
To modify a SIP to Q.850 Override Table:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To create a SIP to Q.850 Override Table:

1. Click the Create ( ) icon.
2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.



Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

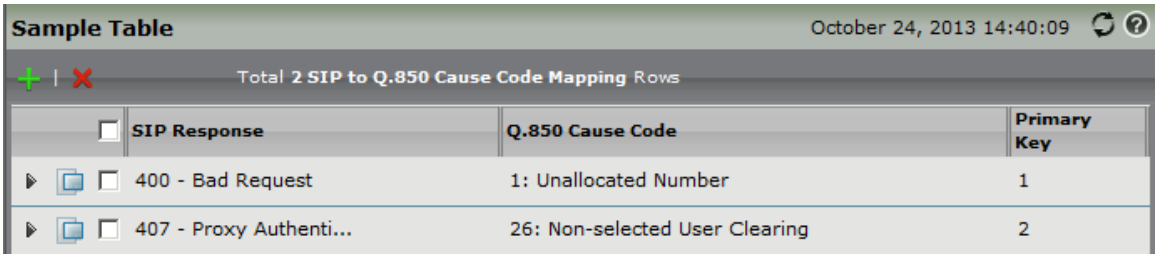
Creating and Modifying Entries to a SIP to Q.850 Override Tables

Creating and Modifying Entries to a SIP to Q.850 Override Tables

By default, the Sonus SBC 1000/2000 uses RFC 3398 cause code mappings. This table allows you to define other mappings for cause codes.

To create or modify an Entry to a SIP to Q.850 Override Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Telephony Mapping Tables** > **SIP to Q.850 Override Tables** > **Entry**.



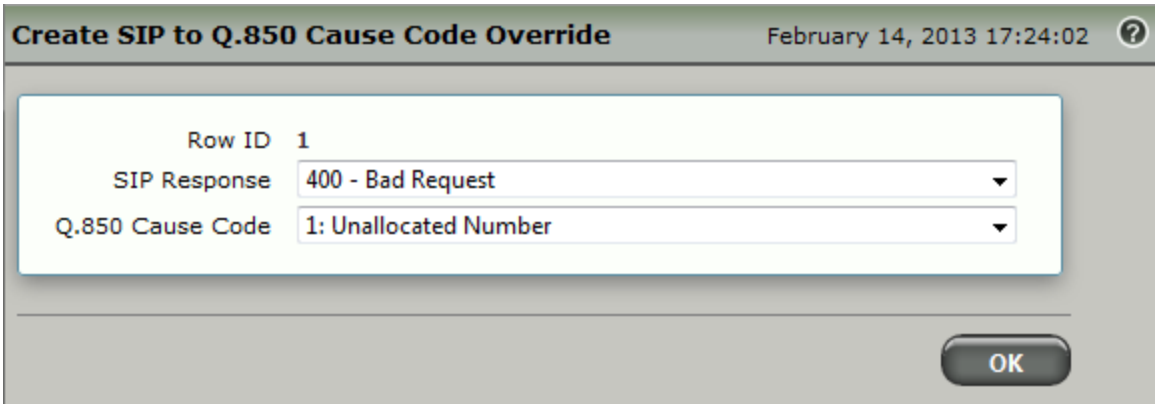
Modifying an Entry in a SIP to Q.850 Override Table

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating an Entry in a SIP to Q.850 Override Table

1. Click the **Create SIP to Q.850 Cause Code** ( ) icon.

Copyright © 2015 Sonus Networks. All rights reserved.



SIP Cause Code to Q.850 Override - Field Definitions

SIP Response

Specifies the SIP Response Codes to which the selected Q850 Cause Codes is mapped.

Q.850 Cause Code

Specifies the Q850 Cause Codes to be mapped to a SIP Response Codes.

Q850 Cause Codes

The following table lists the Q.850 Cause Codes from the ITU-T Recommendation, Series Q: Switching and Signalling.

Q.850 Cause Codes

Cause Code	Reason
l	Unallocated (unassigned) number. This cause indicates that the called party cannot be reached recluses although the called party number is in a valid format. It is not currently allocated (assigned).
2	No route to specified transit network (national use) This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular transit network. While it does exist. does not serve the equipment which is sending this cause.
3	No route to destination This cause indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination desired. This cause is supported on a network dependent basis.
4	Send special information tone This cause indicates that the called party cannot be reached for reasons that are of a long term nature and that the special information tone should be returned to the calling party|
5	Mis-dialed trunk prefix (national use) This cause indicates the erroneous inclusion of a trunk prefix in the called party number. This number is to sniped from the dialed number being sent to the network by the customer premises equipment.

Copyright © 2015 Sonus Networks. All rights reserved.

6	Channel unacceptable This cause indicates that the channel most recently identified is not acceptable to the sending entity for use in this call.
7	Call awarded. being delivered in an established channel This cause indicates that the user has been awarded the incoming call and that the incoming call is being connected to a channel already established to that user for similar calls (e.g. packet-mode x.25 virtual calls).
8	Preemption This cause indicates the call is being preempted.
9	preemption - circuit reserved for reuse This cause indicates that the call is being preempted and the circuit is reserved for reuse by the preempting exchange.
10	Normal call clearing This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared. Under normal situations, the source of this cause is not the network.
14	QoR: ported number This cause indicates that an exchange detected that the called number was ported out.
17	User busy This cause is used to indicate that the called party is unable to accept another call because the user busy condition has been encountered. This cause value may be generated by the called user or by the network. In the case of user determined user busy it is noted that the user equipment is compatible with the call.
18	No user responding This cause is used when a called party does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated.
19	No answer from user (user alerted) This cause is used when the called party has been alerted but does not respond with a connect indication within a prescribed period of time. Note This cause is not necessarily generated by Q.931 procedures but may be generated by internal network timers.
20	Subscriber absent This cause value is used when a mobile station has logged off. radio contact is not obtained with a mobile station or if a personal telecommunication user is temporarily not addressable at any user-network interface.
21	Call rejected This cause indicates that the equipment sending this cause does not wish to accept this call. although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible. This cause may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection.
22	Number changed This cause is returned to a calling party when the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this cause, cause no. 1, unallocated (unassigned) number shall be used.
23	Redirection to new destination This cause is used by a general ISUP protocol mechanism that can be invoked by an exchange that decides that the call should be set-up to a different called number. Such an exchange can invoke a redirection mechanism, by use of this cause value, to request a preceding exchange involved in the call to route the call to the new number.

Copyright © 2015 Sonus Networks. All rights reserved.

24	Call rejected due to feature at the destination This cause indicates that the call has been rejected due to feature at the destination.
25	Exchange – routing error This cause indicates that the destination indicated by the user cannot be reached, because an intermediate exchange has released the call due to reaching a limit in executing the hop counter procedure. This cause is generated by an intermediate node, which when decrementing the hop counter value, gives the result 0.
26	Non-selected user clearing This cause indicates that the user has not been awarded the incoming call.
27	Destination out of order This cause indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates that a signal message was unable to be delivered to the remote party; e.g., a physical layer or data link layer failure at the remote party or user equipment off-line.
28	Invalid number format (address incomplete) This cause indicates that the called party cannot be reached because the called party number is not in a valid format or is not complete.
29	Facilities rejected This cause is returned when a supplementary service requested by the user cannot be provide by the network.
30	Response to STATUS INQUIRY This cause is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS INQUIRY.
31	Normal. unspecified This cause is used to report a normal event only when no other cause in the normal class applies.
34	No circuit/channel available This cause indicates that there is no appropriate circuit/channel presently available to handle the call.
38	Network out of order This cause indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time e.g., immediately re-attempting the call is not likely to be successful.
39	Permanent frame mode connection out-of-service This cause is included in a STATUS message to indicate that a permanently established frame mode connection is out-of-service (e.g. due to equipment or section failure) (see Annex A/Q.933)
40	Permanent frame mode connection operational This cause is included in a STATUS message to indicate that a permanently established frame mode connection is operational and capable of carrying user information.
41	Temporary failure This cause indicates that the network is not functioning correctly and that the condition is no likely to last a long period of time; e.g., the user may wish to try another call attempt almost immediately.
42	Switching equipment congestion This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.

Copyright © 2015 Sonus Networks. All rights reserved.

43	Access information discarded This cause indicates that the network could not deliver access information to the remote user as requested. i.e., user-to-user information, low layer compatibility, high layer compatibility or sub-address as indicated in the diagnostic. It is noted that the particular type of access information discarded is optionally included in the diagnostic.
44	Requested circuit/channel not available This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.
46	Precedence call blocked This cause indicates that there are no predictable circuits or that the called user is busy with a call of equal or higher preventable level.
47	Resource unavailable, unspecified This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.
49	Quality of Service not available This cause is used to report that the requested Quality of Service. as defined in Recommendation X.213. cannot be provided (e.g., throughput of transit delay cannot be supported).
50	Requested facility not subscribed This cause indicates that the user has requested a supplementary service which is implemented by the equipment which generated this cause but the user is not authorized to use.
53	Outgoing calls barred within CUG This cause indicates that although the calling party is a member of the CUG for the outgoing CUG call. Outgoing calls are not allowed for this member of the CUG.
55	Incoming calls barred within CUG This cause indicates that although the calling party is a member of the CUG for the incoming CUG call. Incoming calls are not allowed for this member of the CUG.
57	Bearer capability not authorized This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but the user is not authorized to use.
58	Bearer capability not presently available This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but which is not available at this time.
62	Inconsistency in outgoing information element. This cause indicates an inconsistency in the designated outgoing access information and subscriber class.
63	Service or option not available. unspecified This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.
65	Bearer capability not implemented This cause indicates that the equipment sending this cause does not support the bearer capability requested.
66	Channel type not implemented This cause indicates that the equipment sending this cause does not support the channel type requested

Copyright © 2015 Sonus Networks. All rights reserved.

69	Requested facility not implemented This cause indicates that the equipment sending this cause does not support the requested supplementary services.
70	Only restricted digital information bearer capability is available (national use) This cause indicates that the calling party has requested an unrestricted bearer service but the equipment sending this cause only supports the restricted version of the requested bearer capability.
79	Service or option not implemented unspecified This cause is used to report a service or option not implemented event only when no other cause in the service or option not implemented class applies.
81	Invalid call reference value This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.
82	Identified channel does not exist This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example. if a user has subscribed to those channels on a primary rate interface numbered from l to 12 and the user equipment or the network attempts to use channels l 3 through 23, this cause is generated.
83	A suspended call exists, but this call identity does not This cause indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).|
84	Call identity in use This cause indicates that the network has received a call suspended request containing a call identity (including the null call identity) which is already in use for a suspended call within the domain of interfaces over which the call might be resumed.
85	No call suspended This cause indicates that the network has received a call resume request containing a Call identity information element which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed.
86	Call having the requested call identity has been cleared This cause indicates that the network has received a call resume request containing a Call identity information element indicating a suspended call that has in the meantime been cleared while suspended (either by network time-out or by the remote user).
87	User not a member of CUG This cause indicates that the called user for the incoming CUG call is not a member of the specified CUG or that the calling user is an ordinary subscriber calling a CUG subscriber.
88	Incompatible destination This cause indicates that the equipment sending this cause has received a request to establish a call which has low layer compatibility. high layer compatibility or other compatibility attributes (e.g., data rate) which cannot be accommodated.
90	Non-existent CUG This cause indicates that the specified CUG does not exist.
91	Invalid transit network selection (national use) This cause indicates that a transit network identification was received which is of an incorrect format as defined in Annex C/Q.931

Copyright © 2015 Sonus Networks. All rights reserved.

95	Invalid message, unspecified This cause is used to report an invalid message event only when no other cause in the invalid message class applies.
96	Mandatory information element is missing This cause indicates that the equipment sending this cause has received a message which is missing an information element which must be present in the message before that message can be processed.
97	Message type non-existent or not implemented This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined of defined but not implemented by the equipment sending this cause.
98	Message not compatible with call state or message type non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state. or a STATUS message was received indicating an incompatible call state.
99	Information element / parameter non-existent or not implemented This cause indicates that the equipment sending this cause has received a message which includes information element(s)/parameter(s) not recognized because the information element(s)/parameter name(s) are not defined or are defined but not implemented by the equipment sending the cause. This cause indicates that the information element(s)/parameter(s) were discarded. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.
100	Invalid information element contents This cause indicates that the equipment sending this cause has received and information element which it has implemented; however, one or more Gelds in the I.E. are coded in such a way which has not been implemented by the equipment sending this cause.
101	Message not compatible with call state This cause indicates that a message has been received which is incompatible with the call state.
102	Recovery on timer expiry This cause indicates that a procedure has been initiated by the expiration of a timer in association with error handling procedures.
103	Parameter non-existent or not implemented passed on (national use) This cause indicates that the equipment sending this cause has received a message which includes parameters not recognized because the parameters are not defined or are defined but not implemented by the equipment sending this cause. The cause indicates that the parameter(s) were ignored. In addition, if the equipment sending this cause is an intermediate point, then this cause indicates that the parameter(s) were passed unchanged.
110	Message with unrecognized parameter discarded This cause indicates that the equipment sending this cause has discarded a received message which includes a parameter that is not recognized.
111	Protocol error, unspecified This cause is used to report a protocol error event only when no other cause in the protocol error class applies.
127	Intel-working, unspecified This cause indicates that an interworking call (usually a call to 5W56 service) has ended.

SIP Response Codes

Copyright © 2015 Sonus Networks. All rights reserved.

SIP Response Code	Meaning
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
410	Gone
413	Request Entity Too Large
414	Request-URI Too Long
415	Unsupported Media Type
416	Unsupported URI Scheme
420	Bad Extension
421	Extension Required
423	Interval Too Brief
480	Temporarily Unavailable
481	Call-Transaction Does Not Exist
482	Loop Detected
483	Too Many Hops
484	Address Incomplete
485	Ambiguous
486	Busy Here

Copyright © 2015 Sonus Networks. All rights reserved.

487	Request Terminated
488	Not Acceptable Here
491	Request Pending
493	Undecipherable
500	Server Internal Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Server Time-out
505	Version Not Supported
513	Message Too Large
600	Busy Everywhere
603	Decline
604	Does Not Exist Anywhere
606	Not Acceptable

Working with CAS

The Sonus SBC 1000/2000 supports CAS Signaling through FXS, FXO, E&M, and R2 signaling interfaces.

Managing CAS Signaling Groups

- Creating and Modifying CAS Signaling Groups

Managing CAS Profiles

- Creating and Modifying E&M CAS Profiles
- Creating and Modifying FXO CAS Profiles
- Creating and Modifying FXS CAS Profiles
- Creating and Modifying R2 CAS Profiles

Managing Supplementary Service Profiles

- Creating and Modifying Supplementary Service Profiles

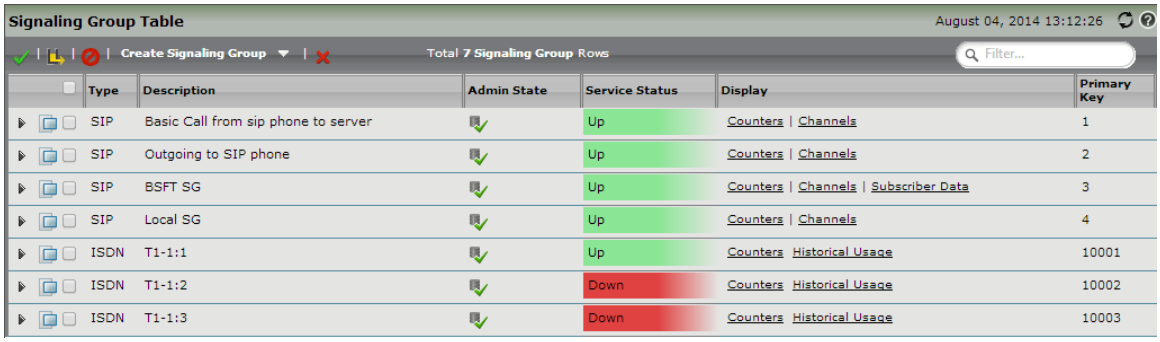
Managing CAS Signaling Groups

Copyright © 2015 Sonus Networks. All rights reserved.

Signaling groups allow telephony channels to be grouped together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which Call Routes are selected. They are also the location from which Tone Tables and Action Sets are selected. In the case of CAS, they select CAS Profiles, allowing you to specify protocol layer settings for CAS (the physical layer settings are configured from Ports).

Working with CAS Signaling Groups

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. From the **Create Signaling Group** drop down box, select **CAS Signaling Group.**



To view an CAS Signaling Group's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying CAS Signaling Groups

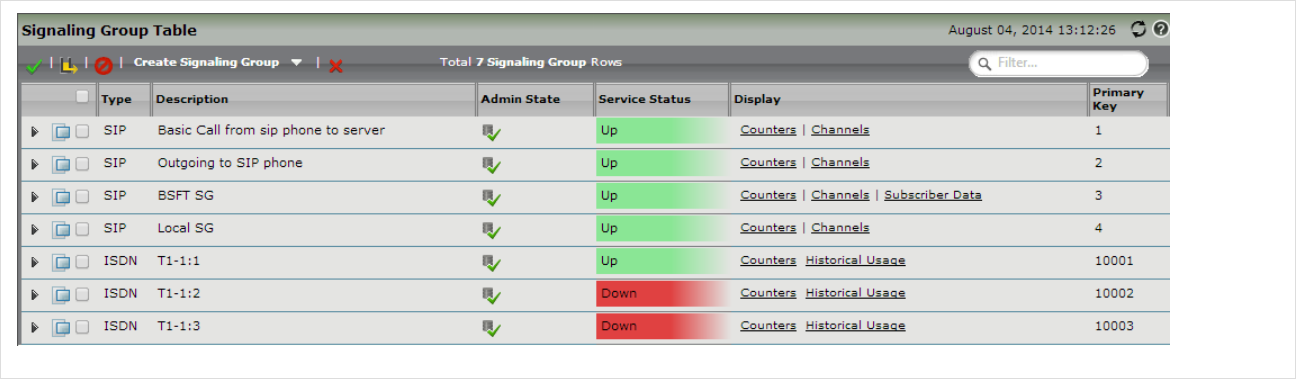
Creating and Modifying CAS Signaling Groups

For the Sonus SBC 2000, each Analog CAS Signaling Group is limited to a maximum of 24 FXS ports.

To create or modify an existing CAS Signaling Group:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. From the **Create Signaling Group** drop down box, select **CAS Signaling Group.**

Copyright © 2015 Sonus Networks. All rights reserved.



Modifying a CAS Signaling Group

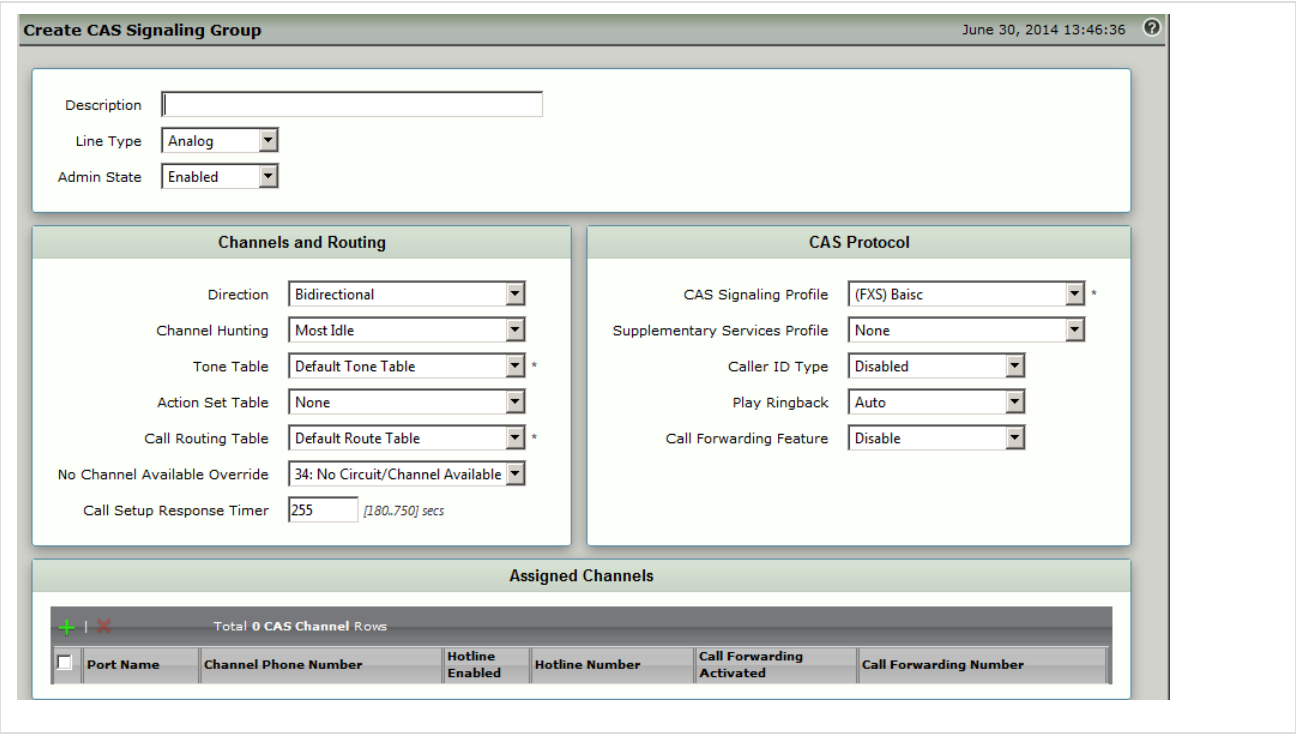
1. Click the **expand** (▸) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a CAS Signaling Group

⚠ Before you can configure a CAS Signaling Group, you must have defined at least one CAS Signaling Profile.

To create a CAS Signaling Group:

1. From the **Create Signaling Group** drop down box at the top of the Signaling Group Table, select **CAS Signaling Group.**



CAS Signaling - Field Definitions

Line Type

Specifies whether or not this CAS Signaling Group is applied to an analog or digital line.

Copyright © 2015 Sonus Networks. All rights reserved.

Admin State

Specifies the admin state of the Signaling group.

- **Enable:** Enables the signaling group.
- **Disable:** Disables the signaling group.
- **Drain:** When Drain is selected, calls that are currently up remain connected. However, new calls and forking are not allowed for the Signaling Group. This allows all the calls to be drained from the SG.

CAS Protocol - Field Definitions

CAS Signaling Profile

Specifies the CAS Signaling Profile to use with this CAS Signaling Group.

Supplementary Services Profile

Specifies whether or not Supplementary Services are supported in this CAS SG. Shown only when the specified CAS Signaling Profile is set to a Loop Start Signaling Profile.

Call Information Format

Species the format of call information sent and received using E&M as the CAS Signaling Profile (E&M Caller ID). Select from the drop down list. Valid entries:

- **Called Party.** Called Party number, default configuration where E&M Caller ID feature is not supported.
- **Calling-Called.** Calling party number is followed by Called party number. Example:<Start Digit> <Calling Party number> <Delimiter Digit> <Called Party number> <End Digit>.
- **Called-Calling.** Called party number is followed by Calling party number. Example:<Start Digit> <Called Party number> <Delimiter Digit> <Calling Party number> <End Digit>.

This field is available only when Line Type is set as Digital and CAS Signaling Profile is set as E&M. (Ensure E&M is configured as a CAS Signaling Profile. See Creating and Modifying E&M CAS Profiles.)

Start Digit

Specifies the first digit of call information sent or received. Select from the drop down list. Valid entry: **A**, **B**, **D**, # or *****. Default entry: *****.

This field is available only when Call Information Format is set to **Calling-Called** or **Called-Calling.**

Delimiter Digit

Specifies the call information digit separating calling and called numbers. Select from the drop down list. Valid entry: **A**, **B**, **D**, # or *****. Default entry: *****.

This field is available only when Call Information Format is set to **Calling-Called** or **Called-Calling.**

End Digit

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the last digit of call information sent or received. Select from the drop down list. Valid entry: **A**, **B**, **D**, # or *****. Default entry: *****.

This field is available only when Call Information Format is set to **Calling-Called** or **Called-Calling.**

Caller ID Type

Specifies the Caller ID Type for this signaling group. This field is visible only when the Line Type is set to Analog.

Typical Caller ID Types by Country

Not all countries are standardized on which Caller ID Type they use. This list contains suggested types for certain countries, and some countries use multiple types. If the Caller ID Type listed here for your country, you may need to contact your local service provider.

Caller ID Type	Countries
DTMF	Brazil, Belgium, Denmark, Finland, Iceland, India, Netherlands, Saudi Arabia, Sweden, Uruguay and some parts of Taiwan
DTMF - No Ring	Taiwan and some parts of China
DTMF - Reverse Battery	Taiwan and China
ETS - Reverse Battery	Taiwan
ETSI	France, Germany, Norway, Italy, Spain, South Africa, Turkey, and some parts of Taiwan
FSK	Mexico, USA, Canada, Australia, New Zealand Singapore, Hong Kong, and some parts of China
FSK - No Ring	UK, Taiwan, and some parts of China
NTT - Japan CID	Japan

Caller ID Start Delimiter

Specifies the DTMF tones used as the caller ID start delimiter. This attribute is applicable only if the signaling profile is of type FXS or FXO, only if the Line Type is Analog, and only if the Caller ID Type iss DTMF, DTMF No Ring, or DTMF Reverse Battery.

Caller ID End Delimiter

Specifies the DTMF tones used as the caller ID end delimiter. This attribute is applicable only if the signaling profile is of type FXS or FXO, only if the Line Type is Analog, and only if the Caller ID Type iss DTMF, DTMF No Ring, or DTMF Reverse Battery.

Play Ringback

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies when to play the ringback tone on the channel.

Caller ID Privacy Signaling

The Calling ID Privacy Signaling field can contain up to five characters that are sent in place of the calling party number in cases where the outgoing call is marked as blocked or restricted. The range of characters configured for privacy signaling is limited when it is configured for DTMF or FSK. See the following table for details.

Caller ID Type	Valid Characters	Calling Party Number Sent
FSK	Any	Characters configured in privacy signaling field
FSK	None entered	A single character 'P' to indicate private
DTMF	0-9, A-z, * and #	Characters configured in privacy signaling field
DTMF	None entered	Nothing is sent, calling party number is blank

Call Forwarding Feature

Used to enable/disable the Call Forward feature at the Signaling Group level. The Call Forward feature allows a phone connected to an FXS port to forward calls to another telephone number. Available options: **Enabled** or **Disabled**. Once this field is enabled, the **Call Forwarding Activate DTMF** and **Call Forwarding Deactivate DTMF** fields become visible. To enable at the channel level, you must activate at the Assigned Channel Table, Assigned Channels - Field Definitions, or activate through the physical phone, How to Operate Call Forward on Telephone. Once Call Forward is activated and a keycode is configured, you must configure a route on the SBC to route the forwarded number. If a route is not provided, the call will fail.

Call Forwarding Availability

Call forwarding is supported for Analog FXS only.

Field Behavior

The Call Forwarding Feature field is only visible when **Analog** is selected in the **Line Type** field. If the Line Type has been set to Analog and Call Forwarding has been enabled then Line Type is subsequently set to Digital:

- Call Forwarding is automatically disabled.
- The Call Forwarding Feature field is hidden.

Click here for detailed information about Call Forward

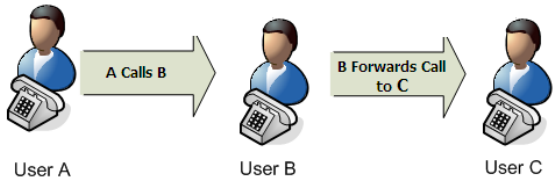
The Call Forwarding feature enables a phone connected to an FXS port to forward incoming calls to another configured telephone number. The SBC supports unconditional call forward on an individual port basis. Call Forward is activated/deactivated on a port with configured specific service codes, accompanied by the forward number. Once the user enters the configured keycode and forward telephone number, all outgoing calls to the port will then be redirected to the forwarding number. When the outgoing call routes to a port that is forwarded, the phone on that port generates a short ring.

In North America, the NANP defines *72<forward number> for activation and *73 for deactivation, but the SBC enables you to configure any 6 character combination for activation and/or deactivation. The SBC enables a

Copyright © 2015 Sonus Networks. All rights reserved.

keycode to have a minimum length of 3 characters and a maximum of 6; this is based on what is commonly used today.

> The SBC supports a basic Unconditional Call Forward, but it allows various characters to be configured for keycodes. This includes the '#' character, which is defined in the SBC as an End of Dial digit. In order to determine if an entry is part of a Call Forward activate or deactivate keycode, End of Dial behavior is ignored for the first 6 characters dialed. If the SBC finds that the digits do not match the call forward keycode, it will parse the number backwards to the last '#' (if there is one) and remove it before sending the number for routing. This means that '#' will not stop the inter-digit timer and immediately send the number during collection of the first 6 digits.



Click here to read how to activate Call Forward on a Telephone
Activate through a Telephone

The Call Forward feature can be initiated with the following steps:

- Lift the handset to the port (in which calls will be forwarded) and enter the activate **keycode** + **forwarded number,** followed by the **'#'** key on the telephone.
- A confirmation tone (fast beep) indicates a successful Call Forward. A congestion tone (busy tone) indicates call forward failed.
- An activation at the physical phone level automatically activates the feature for the applicable channel in the Assigned Channels table. See Assigned Channels - Field Definitions.

Deactivate through a Telephone

- Lift the handset connected to the port in which calls are being forwarded (that requires deactivation) and enter the deactivate **keycode.**
- A confirmation tone (fast beep) indicates a successful Call Forward deactivation. A congestion tone (busy tone) indicates call forward has not been deactivated.

Click here to read how to activate Call Forward on a Channel through the Channel Table
Activate on a Channel through the Channel Table

The Call Forward feature can be activated for a specific channel through the Assigned Channels table as follows:

> In order for the feature to be available at the channel level, ensure the Call Forwarding feature is enabled under CAS Protocol. See #Call Forwarding Feature.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click the expand ( ) icon next to the entry you wish to modify.
4. At the Assigned Channels table, click on the icon.

Copyright © 2015 Sonus Networks. All rights reserved.

5. From **Channel Selection Method,** select **Single Port.**
6. From **Call Forward Activated,** select **Yes.**
7. In **Call Forwarding Number** box, enter the number to which the call will be forwarded.
8. Click **Apply.**

Deactivate on a Channel through Channel Table

The Call Forward feature can be deactivated for a specific channel through the Assigned Channels table as follows:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click the expand ( ) icon next to the entry you wish to modify.
4. In the **Assigned Channels** table, click on the ( ) icon next to the entry in which you want to deactivate Call Forward.
5. From **Call Forward Activated,** select **Disable.**
6. Click **Apply.**

Call Forwarding Activate DTMF

Code used to activate the Call forward feature on a specific FXS port. This field is configurable up to a 6 character combination. Default entry: ***72.**

Call Forwarding Deactivate DTMF

Code used to deactivate the Call forward feature on a specific FXS port. This field is configurable up to a 6 character combination. Default entry: ***73.**

Channels and Routing - Field Definitions

Channel Hunting

Specifies the channel hunting method. Not Applicable when Direction is Incoming.

- **Standard:** This option assigns first available low numbered channel.
- **Reverse Standard:** This option assigns last available high numbered channel.
- **Round Robin:** This option assigns channels based on next available from low numbered to high numbered.
- **Least Idle:** This option chooses channels based on the least idle channel.
- **Most Idle:** This option chooses channels based on the most idle channel.
- **Own Number:** This option chooses it's own channel if the number dialed belongs to it.

Direction

Specifies the direction of calls handled by this signaling group.

Tone Table

Specifies the tone table to use with this signaling group. The Tone Table field is visible only when the Direction attribute is set to Bidirectional or Inbound.

Action Set Table

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the Action Set to use with this signaling group. Available only when the Direction attribute is set to Bidirectional or Inbound.

When an Action Set Table is specified (not "none") it takes precedence over Route Table.

Call Routing Table

Specifies which Routing Table to use with this Signaling Group. The Call Routing Table field is visible only when the Direction attribute is set to Bidirectional or inbound.

No Channel Available Override

In the event of a "No Channel/Circuit available" release cause code, the specified cause code will be sent to the relevant protocol module. For more information see the list of Cause Codes.

Call Setup Response Timer

Specifies the interval of time, in milliseconds, after an call is initiated that the Sonus SBC 1000/2000 waits for a call to connect before terminating the incoming call.

Assigned Channels - Field Definitions

Channels are assigned to specific Signaling Groups (SG). The channels for a digital SG can be made up of all or part of channels from one or more digital ports in the system. Likewise, "channels" for 1 analog SG can be made up of any analog ports in the system. When you click on the + icon, the **Create Assigned Channels** window is displayed. Field definitions are below.

For a CAS Signaling Group using E&M/Loop Start signaling (T1/Analog) or CAS R2 (E1), a maximum of 48 channels can be assigned to the signaling group.

For E1, limit channels to 30 (to not go over the maximum 48 channels). Otherwise, the following will occur:

- The span (48 channels) is split across two signaling groups.
- When the limit of 48 channels in the span is met, 18 channels from one of the signaling groups must be deleted before a new signaling group can be created.

DS1 Port Selection

Specifies the DS1 port from which channels will be assigned to this SG. This field is only visible when the Line Type is specified as Digital.

Channel Selection Method

Specifies the method by which to assign ports to analog cards or channels to digital ports. Available options: **Digital** (All Channels, Single Channel, or Range of Channels), **Analog** (All Ports on a Card or Single Port).

Analog Card Selection

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the analog card to which ports will be assigned. This field is only visible when the #Line Type is specified as Analog.

Channel Phone Number

Specifies a specific phone number to assign to a channel.

Enable FXS Hotline

Enables a user or device to seize an FXS line on the SBC and have it automatically routed to a pre-configured destination number. If enabled, this number is configured in the **Hotline Number** field. Valid entries: **Yes** or **No**.

Hotline Number

Number to which an FXS line is automatically routed. Available only if **Enable FXS Hotline** is set to **Yes**.

Call Forwarding Activated

Indicates whether the Call Forwarding feature is activated on that channel. Call Forward allows a phone connected to an FXS port to forward calls to another telephone number. Available options: **Yes** or **No**. An activation at the physical phone level automatically activates the feature in this field for the applicable channel

Call Forwarding Number

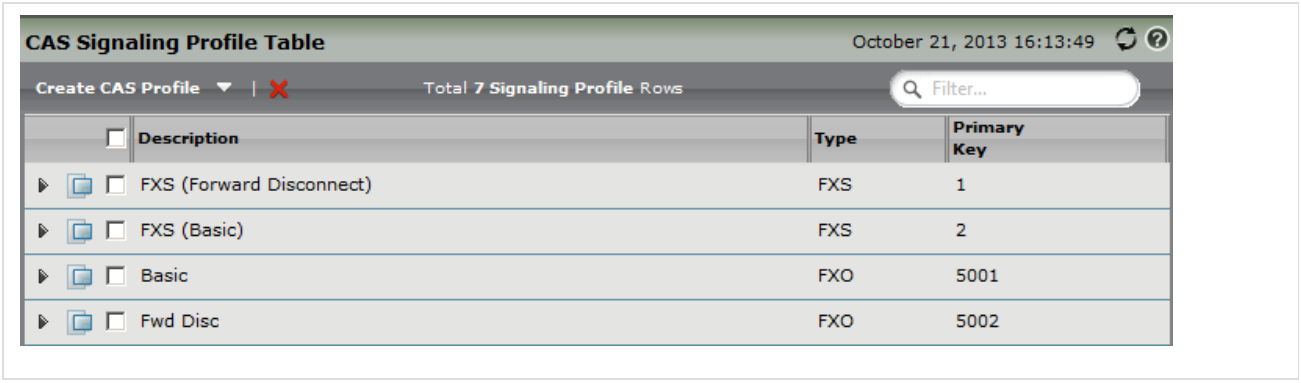
Specifies the telephone number in which forwarded calls are sent. Available only when Call Forwarding Activated is set to Yes. An activation at the physical phone level automatically activates the feature in this field for the applicable channel.

Managing CAS Profiles

CAS Profiles control various aspects of loop start, DTMF, tone detection and other features associated with the variants of CAS calls. The Sonus SBC 1000/2000 supports FXS, FXO, and E&M signaling through CAS. CAS R2 will be supported in a future release.

Working with CAS Profiles

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **CAS > CAS Signaling Profiles**.



Copyright © 2015 Sonus Networks. All rights reserved.

To view a profile's properties:

1. Click the popup() icon next to the entry you want to view.
2. When you are finished, close the window.

> **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete () icon located at the top of the window.

Creating and Modifying E&M CAS Profiles

Creating and Modifying FXO CAS Profiles

Creating and Modifying FXS CAS Profiles

Creating and Modifying R2 CAS Profiles

Creating and Modifying E&M CAS Profiles

To create or modify E&M CAS Profile:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **CAS > CAS Signaling Profiles**.
3. From the **Create CAS Profile** drop down box, select **E&M Profile.**

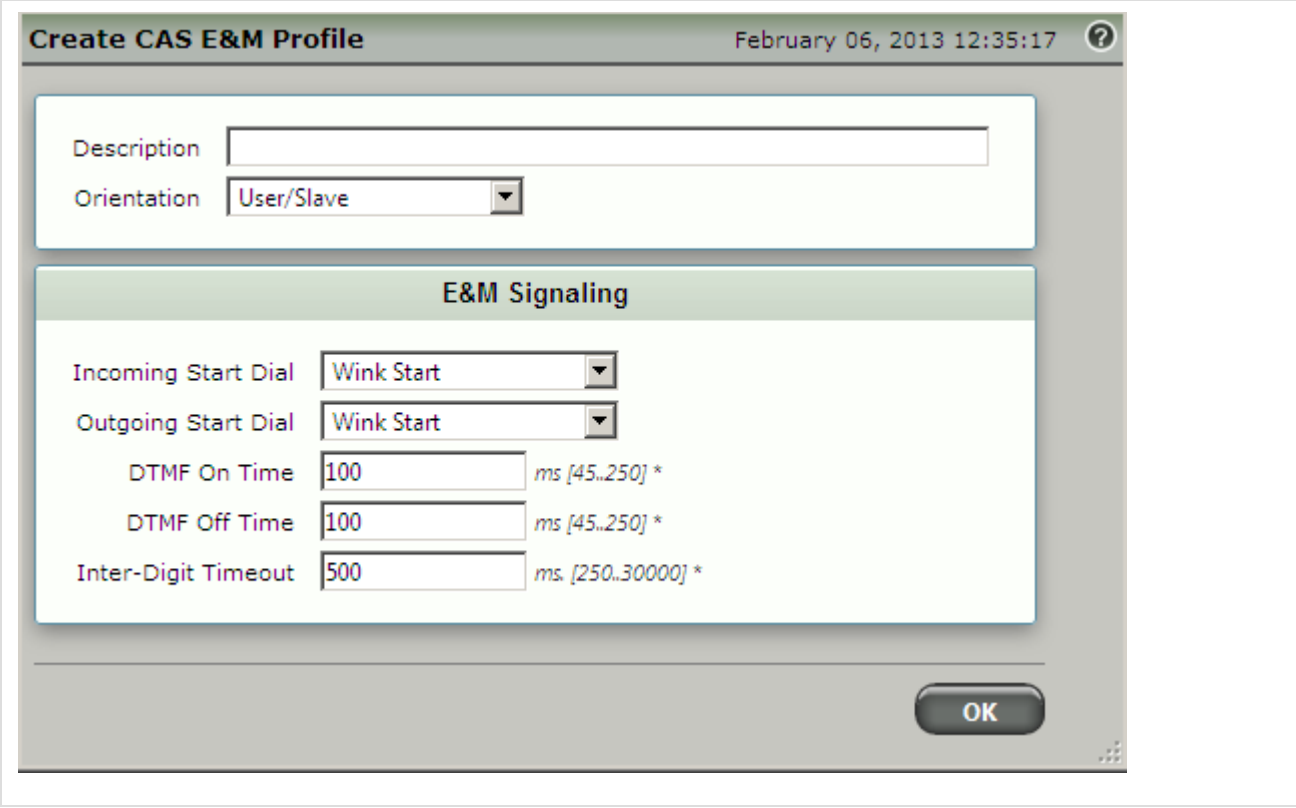
Modifying a E&M CAS Profile

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a E&M CAS Profile

1. From the **Create CAS Profile** drop down box at the top of the CAS Signaling Profile Table Page, select **E&M Profile**.

Copyright © 2015 Sonus Networks. All rights reserved.



E&M Signaling - Field Definitions

Orientation

⚠ This option is not supported. It will be addressed in a future release.

Specifies the CAS signaling orientation.

- **User/Slave:** Use this option when connecting to PSTN.
- **Network/Master:** Use this option when connected to a PBX.

Incoming and Outgoing Start Dial

Specifies the E&M protocol for incoming and outgoing calls respectively.

DTMF On Time

Specifies the duration, in milliseconds, that the tones are on.

DTMF Off Time

Specifies the duration, in milliseconds, of the pause between tones.

Inter-Digit Timeout

Used to set the timeout time, in milliseconds, between dialed numbers.
Because the Sonus SBC 1000/2000 does not currently support dial plans, the use of an inter-digit timeout is necessary to detect the end of digit dialing.

Copyright © 2015 Sonus Networks. All rights reserved.

Creating and Modifying FXO CAS Profiles

To create or modify an FXO CAS Profile:

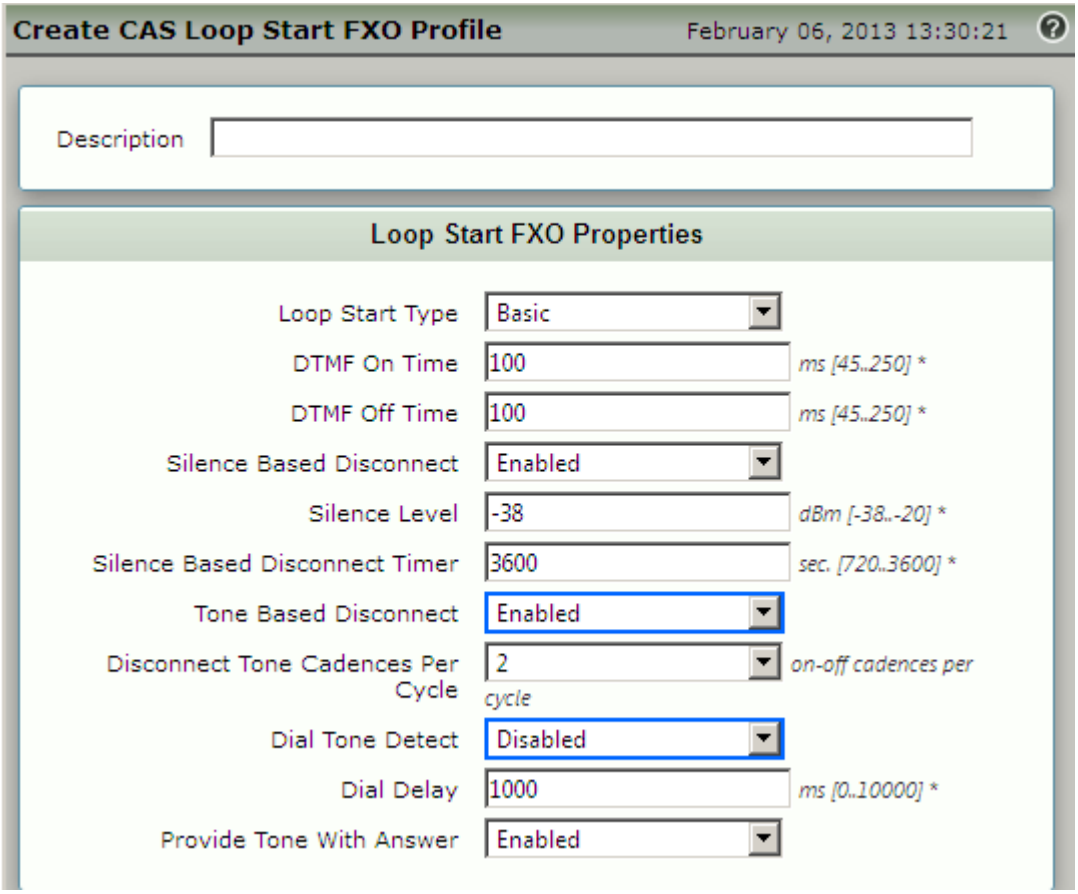
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **CAS > CAS Signaling Profiles.**
3. From the **Create CAS Profile** drop down box, select **FXO Profile.**

Modifying a FXO CAS Profile

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating FXO CAS Profile

1. From the **Create CAS Profile** drop down box at the top of the CAS Signaling Profile Table Page, select **FXO Profile.**



Loop Start FXO Properties - Field Definitions

Loop Start Type

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the signaling type for the Loop Start Type.

The options are as follows:

Basic	This type does not provide disconnect signal. Tone-based disconnect supervision should be used, which could take about 20 seconds.
Forward Disconnect	Disconnects the call based on battery removal received from the line. The duration is normally 800 ms and it can be configured.
Reverse Battery	The call is disconnected based on the tip and ring polarity reversal.

DTMF On Time

Specifies the duration, in milliseconds, that the tones are on.

DTMF Off Time

Specifies the duration, in milliseconds, of the pause between tones.

Dial Tone Detect

Specifies whether or not a dial tone must be detected before dialing out.

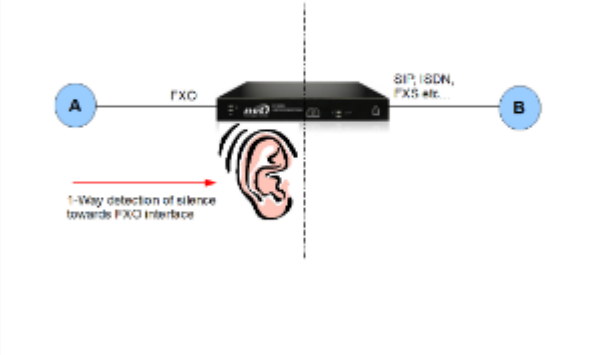
Mimimum Forward Disconnect Duration

Specifies the time which qualifies as a valid forward disconnect (battery removal). Valid only when Loop Start Type is set to "Forward Disconnect".

Silence Based Disconnect

Enables and disables the supervision that disconnects a call following silence for the length of time defined in the Silence Based Disconnect Timer field.

Silence is detected only on the audio stream coming into the FXO interface side of the call.



Copyright © 2015 Sonus Networks. All rights reserved.

Silence Level

The level below which line noise must remain to qualify for silence. This field is only visible when Silence Based Disconnect supervision is enabled.

Silence Based Disconnect Timer

Defines the duration of time, in seconds for silence based disconnect. This field is only visible when Silence Based Disconnect supervision is enabled.

Tone Based Disconnect

Enables and disables tone based disconnect supervision of the CAS line. This field is only visible when Loop Start Type is set to Basic.

Disconnect Tone Cadences Per Cycle

Defines the desired on/off cadence time in one cycle for disconnect tone detection. This field is only visible when Tone Based Disconnect is enabled.

Dial Delay (When Dial Tone Detection is disabled.)

Specifies the duration, in milliseconds, of the delay between the off-hook condition and sending digits.

Provide Tone With Answer

Specifies that, should an inbound FXO call fail before it connects, the Sonus SBC 1000/2000 attempts to connect and play a fast busy tone for a period of time before disconnecting the call.

Creating and Modifying FXS CAS Profiles

To create or modify a FXS CAS Profile:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **CAS > CAS Signaling Profiles.**
3. From the **Create CAS Profile** drop down box, select **FXS Profile.**

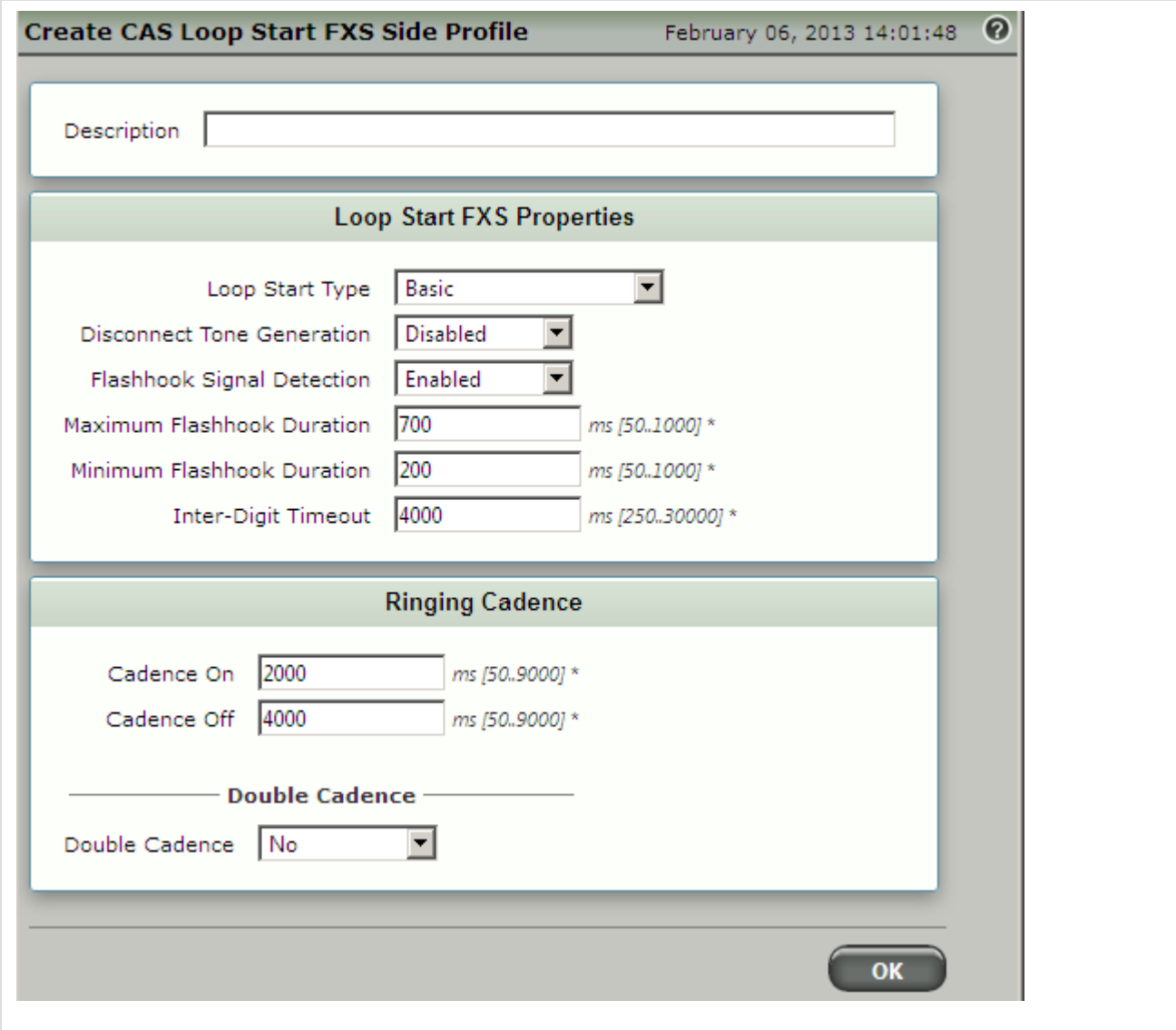
Modifying a FXS CAS Profile

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating an FXS CAS Profile

1. From the **Create CAS Profile** drop down box at the top of the CAS Signaling Profile Table Page, select **FXS Profile**.

Copyright © 2015 Sonus Networks. All rights reserved.



Loop Start FXS Properties - Field Definitions

Loop Start Type

Specifies the loop start method.

Disconnect Tone Generation

Specifies whether or not a disconnect tone is generated when a call is disconnected from the far end.

Forward Disconnect Duration

Specifies the time, in milliseconds, which qualifies as a valid forward disconnect (battery removal). Valid only when Loop Start Type is set to "Forward Disconnect".

Flashhook Duration - Minimum/Maximum

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the minimum and maximum duration, in milliseconds, the loop (circuit) can be open such that it is recognizable as a Flashhook signal. The minimum flashhook duration must not exceed the maximum flashook duration. Available only when Flashhook Detection is **Enabled**.

Inter-Digit Timeout

Used to set the timeout time, in milliseconds, between dialed numbers.
Because the Sonus SBC 1000/2000 does not currently support dial plans, the use of an inter-digit timeout is necessary to detect the end of digit dialing.

Ringing Cadence - Field Definiti8ons

Ringing cadence is the ring-pause-ring pattern used to indicate an incoming call.

This only applies to POTS fixed phones, where the high voltage ring signal is switched on and off to create the ringing pattern. In North America, the standard ring cadence is "2-4", or 2000 ms followed by 4000 ms of silence (default Sonus SBC 1000/2000 ring cadence). In Australia and the UK, the standard ring cadence is 400 ms on, 200 ms off, 400 ms on, 2000 ms off (or **double cadence**). Ringing cadence applies to digital FXS as well as analog.

Cadence On

Specifies the cadence on time (local Ring Tone is audible) for a ring generated on the analog FXS side. The value is specified in milliseconds.

Cadence Off

Specifies the cadence off time (Ring Tone is inaudible) for a ring generated on the analog FXS side. The value is specified in milliseconds.

Double Cadence

Specifies the use of a second cadence on the FXS side. See the expanded description under #Ringing Cadence, above.

Double Cadence - Cadence On/Off

Specifies the on and off times for the local ring tones in the same manner as described above.

Creating and Modifying R2 CAS Profiles

To add or modify an R2 CAS Profile:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **CAS > CAS Signaling Profiles**.
3. From the **Create CAS Profile** drop down box, select **R2 Profile.**

Modifying an R2 CAS Profile

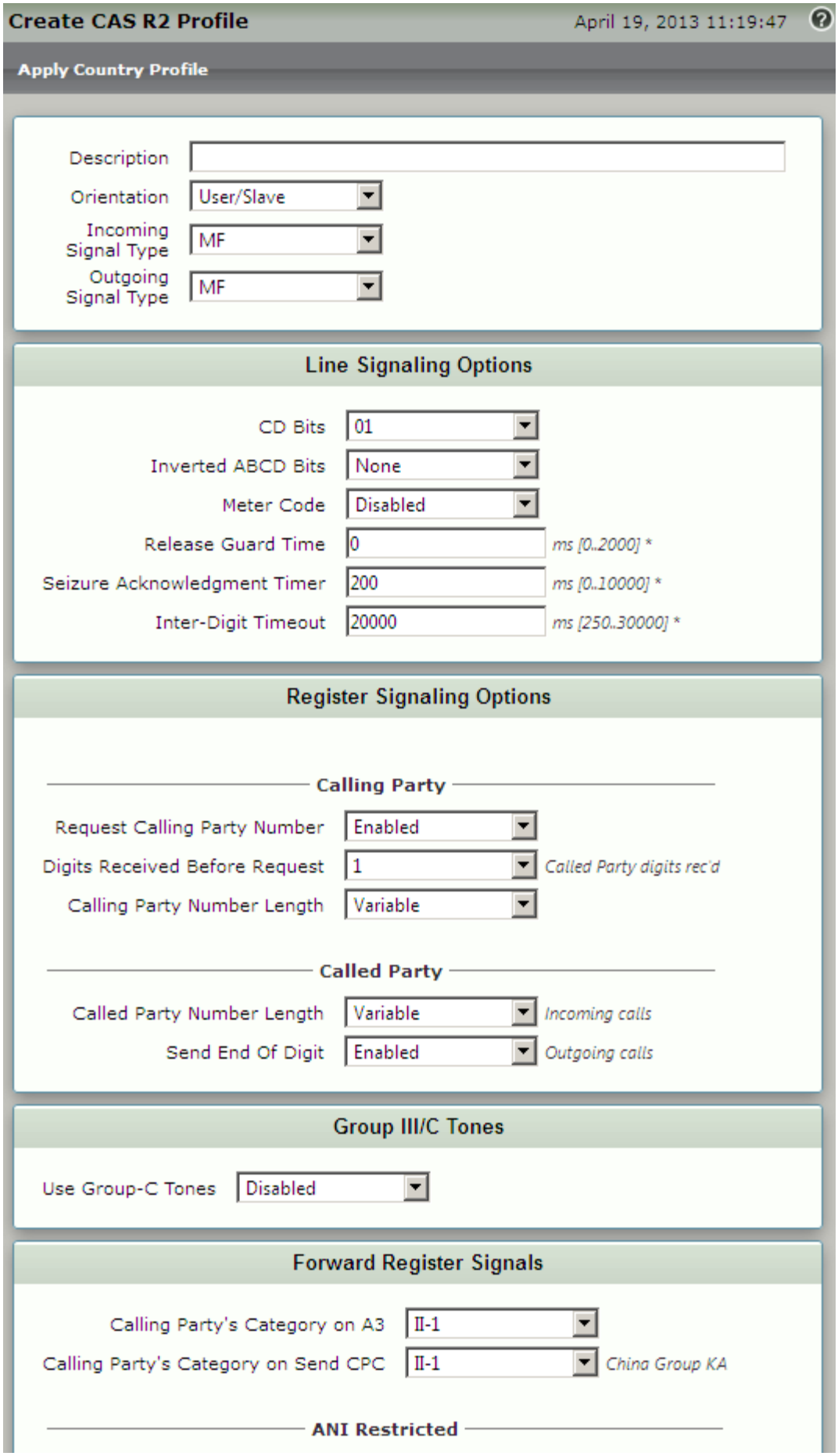
1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a R2 CAS Profile

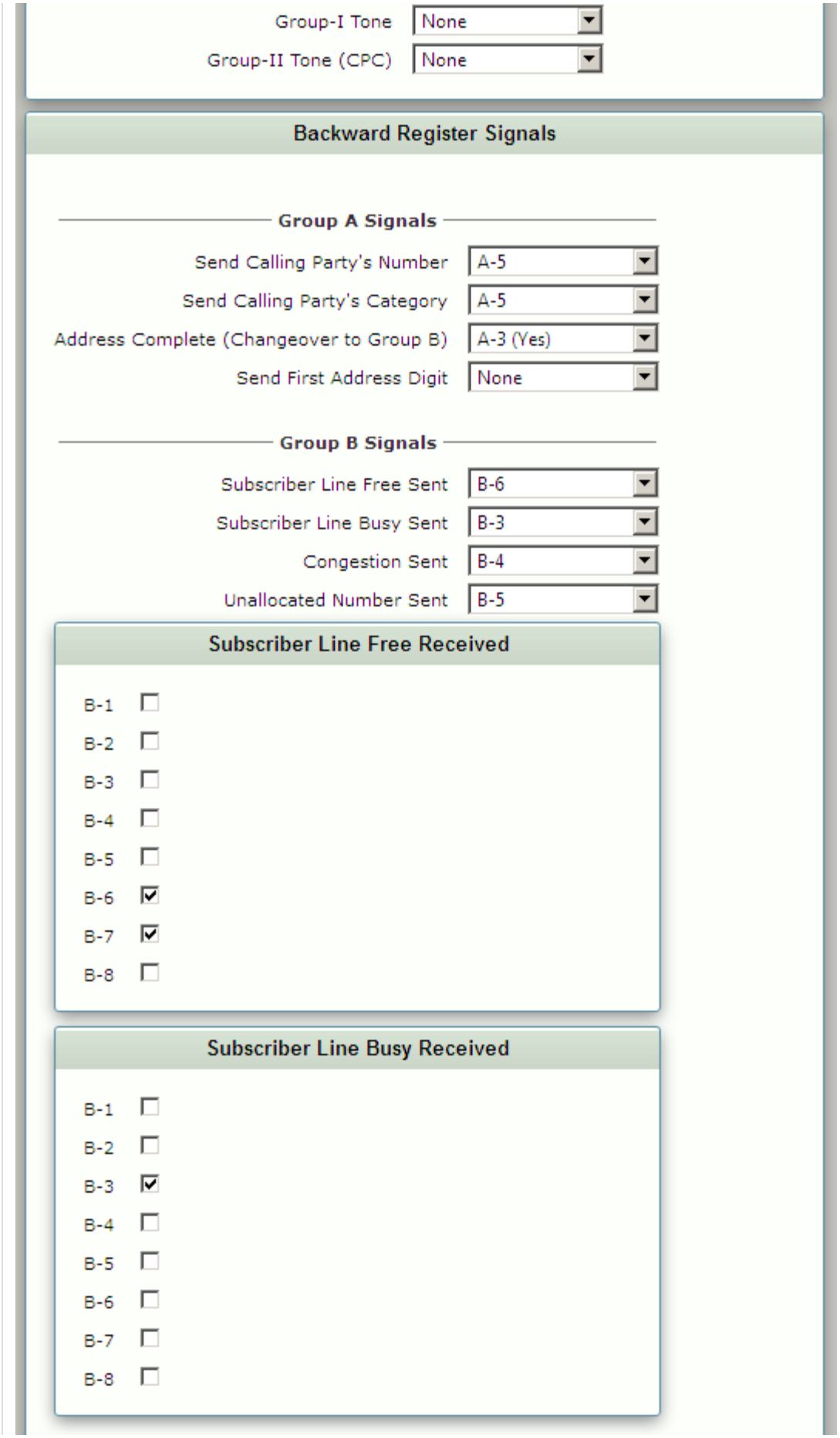
Copyright © 2015 Sonus Networks. All rights reserved.

1. From the **Create CAS Profile** drop down box at the top of the CAS Signaling Profile Table Page, select **R2 Profile.**

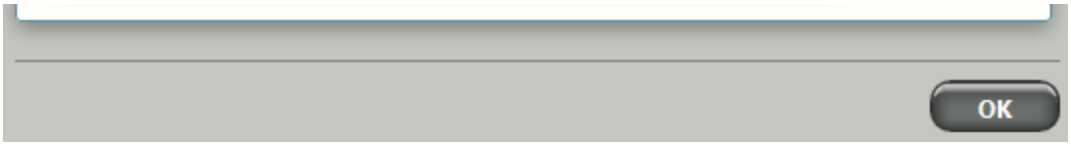
Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.



Applying a Preconfigured Country Profile

The Sonus SBC 1000/2000 contains a set of preconfigured Country Profiles that you can apply to an R2 CAS Profile.

To apply a preconfigured profile:

1. Click the **Apply Country Profile** text at the top of the Add CAS R2 Profile panel.
2. Select the Country Profile of your choice.
3. Click **Apply**.

R2 Signaling - Field Definitions

Description

Specifies a brief description of the R2 Profile. For example: Basic R2 CAS Profile.

Orientation

Specifies the handling of inbound and outbound call collision.

- **User/Slave:** inbound call is accepted, outbound call is released.
- **Network/Master:** the system waits for the remote side to back off.

Incoming Signal Type

Specifies whether the CAS R2 profile uses MF or DTMF signaling for incoming calls. Default entry: MF.

Outgoing Signal Type

Specifies whether the CAS R2 profile uses MF or DTMF signaling for outgoing calls. Default entry: MF.

Line Signaling Options - Field Definitions

CD Bits

Specifies how the C and D bits are transmitted.

Used to specify the setting of the C and D bits transmitted, configured as a bit mask. The value specified is the decimal representation of a 2 bit binary bit mask. For example: to set the 'C' bit to one, binary 10 would be used and entered as 2.

Inverted ABCD Bits

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the inverted A, B, C, or D bits, configured as a bit mask.

Used to specify the inverted A, B, C, or D bits, configured as a bit mask. The line signals are inverted according to this parameter before being transmitted. Received line signals are inverted before being interpreted. The value specified is the decimal representation of a 4 bit binary bit mask. For example: to invert the 'B' bit, binary 0100 would be used and entered as 4.

Meter Code

Specifies whether or not to send a metering signal and how it is implemented.

Metering signals are pulse type signals transmitted backwards during the call from call charging point to subscriber's call meter in the originating exchange.

Release Guard Time

Specifies the release guard time in milliseconds.

Release Guard Time is the interval during which an incoming R2 register waits when a clear forward line signal is received before sending an idle line signal. The value is specified in milliseconds. Zero indicates that the idle signal is to be returned immediately.

Seizure Acknowledgment Timer

Specifies the maximum time, in milliseconds, the outgoing R2 line waits for the seizure acknowledgment signal after sending sending the seizure signal. Zero indicates no time out is to be used.

Inter-Digit Timeout

Used to set the timeout time, in seconds, between dialed numbers. The Sonus SBC 1000/2000 does not currently support dial plans; the use of an inter-digit timeout is necessary to detect the end of digit dialing.

Register Signaling Options - Field Definitions

Request Calling Party Number

Specifies whether or not the Calling Party Number is requested.

Digits Received Before Request

Specifies the number of DNIS digits received before requesting the ANI. This parameter is not displayed if the **Request Calling Party Number** is set to **Disabled**.

Calling Party Number Length

Specifies the number of Called Party Number Digits received before requesting the Calling Party Number. This parameter is displayed only when **Request Calling Party Number** is set to **Enabled**.

Calling Party Digits

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the fixed length of the Calling Party Number requested or sent. This parameter is displayed only when **Calling Party Number length** is set to **Fixed.**

Called Party Number Length

Specifies whether the length of the Calling Party Number requested or sent is variable or fixed. When variable Calling Party Number length is specified, the Group I-15 signal is used to indicate the end of Calling Party Number. Available only when **Request Calling Party Number** is set to **Enabled**.

Called Party Digits

Specifies the length of the expected Called Party Number. This parameter is displayed only when **Called Party Number Length** is set to **Fixed**.

Send End of Digit

Specifies whether or not the SBC sends I-15 to indicate the end of digits for the Called Party Number (DNIS). Available entries: **Enabled** or **Disabled**. Default entry: Enabled.

Forward Register Signals - Field Definitions

Calling Party's Category

Specifies the Group II forward signal sent after receiving an Address Complete backward signal.

Group III/C Tones - Field Definitions

Use Group-C Tones

Specifies whether the Sonus SBC 1000/2000 will use the Axtel switch implementation of R2 Group-C tones for Calling Party Number request. Default entry: **Disabled**.

Forward Register Signals - Field Definitions

Calling Party's Category on A3

Used to specify the Group II calling party's category signal to be sent on receiving the A-3 "Address Complete, Changeover to Group B" backward signal.

Calling Party's Category on Send CPC

Used to specify the Group II calling party's category signal to be sent on receiving "Send Calling Party's Category" backward signal. This parameter is not displayed if the **Request Calling Party Number** is set to **Disabled**.

Group-I Tone

Specifies the Group-I tone sent in response to an ANI Request to indicate that ANI is restricted

Group-II Tone (CPC)

Specifies the Group-II tone sent in response to an ANI Category request to indicate that ANI is restricted.

Copyright © 2015 Sonus Networks. All rights reserved.

Backward Register Signals - Field Definitions

Send Calling Party's Number

Specifies the the backward group A signal used to request the calling party's number. This parameter is displayed only if the **Calling Party Number Request** is set to **Enabled.**

Send Calling Party's Category

Specifies the backward group A signal used to request the calling party's category. This parameter is displayed only if the **Calling Party Number Request** is set to **Enabled.**

Address Complete (Changeover to Group B)

Used to specify whether Group B signals are transmitted after the SBC has received address digits. If configured to **Yes**, the A-3 signal is transmitted to indicate that the SBC does not require additional address digits, and will transmit Group B signal to indicate the condition of the called party. If configured to **No**, the A-6 signal is transmitted to indicate that the SBC does not require additional address digits, but it will not send a Group B signal.

Send First Address Digit

Specifies the group A backward signal used to request the retransmission of the Called Party Number (starting with the first digit).

Subscriber Line Free Sent

Specifies the group B backward signal sent by the incoming R2 register indicating an idle condition of the destination party.

Subscriber Line Busy Sent

Specifies the group B backward signal sent by the incoming R2 register indicating a busy condition of the destination party.

Congestion Sent

Used to specify the group B backward signal sent by the incoming R2 register to indicate that the destination party dialed is congested.

Unallocated Number Sent

Used to specify the group B backward signal sent by the incoming R2 register to indicate that the destination party dialed is unallocated.

Subscriber Line Free Received - Field Definition

Subscriber Line Free Received B1 - B8

Specifies the group B-1 through B-8 backward signal received by the outgoing R2 register for an idle condition of the destination party.

Subscriber LIne Busy Received - Field Definition

Copyright © 2015 Sonus Networks. All rights reserved.

Subscriber Line Busy Received B1 - B8

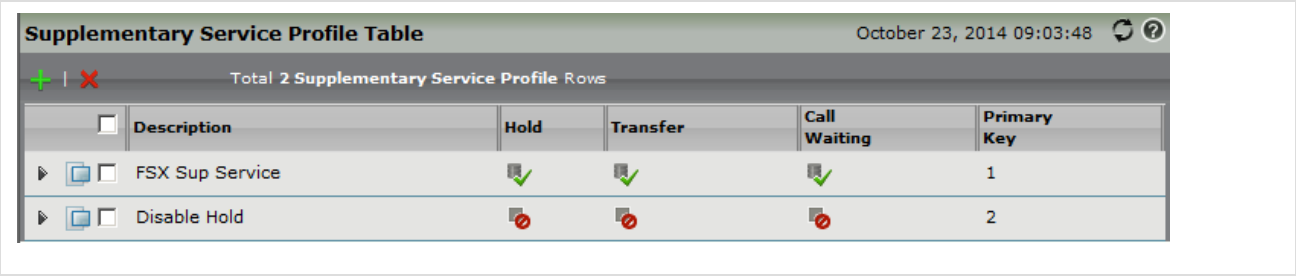
Specifies the group B-1 through B-8 backward signal received by the outgoing R2 register for a busy condition of a destination party.

Managing Supplementary Service Profiles

Supplementary Service Profiles allow a user to define a generic set of supplementary services that are supported. The profile can then be attached to one or more CAS Signaling Groups (SG).

Working with Supplementary Service Profiles

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **CAS > Supplementary Service Profiles**.



To view a profile's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

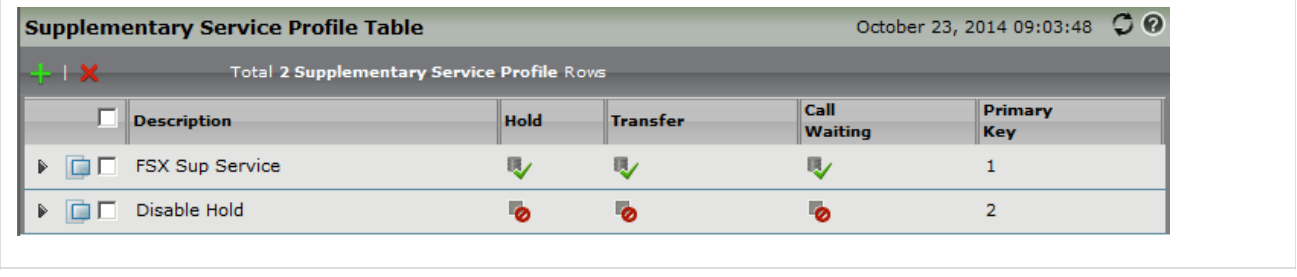
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Supplementary Service Profiles

Creating and Modifying Supplementary Service Profiles

To create or modify a Supplementary Service Profile:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **CAS > Supplementary Service Profiles**.



Modifying a Supplementary Service Profile

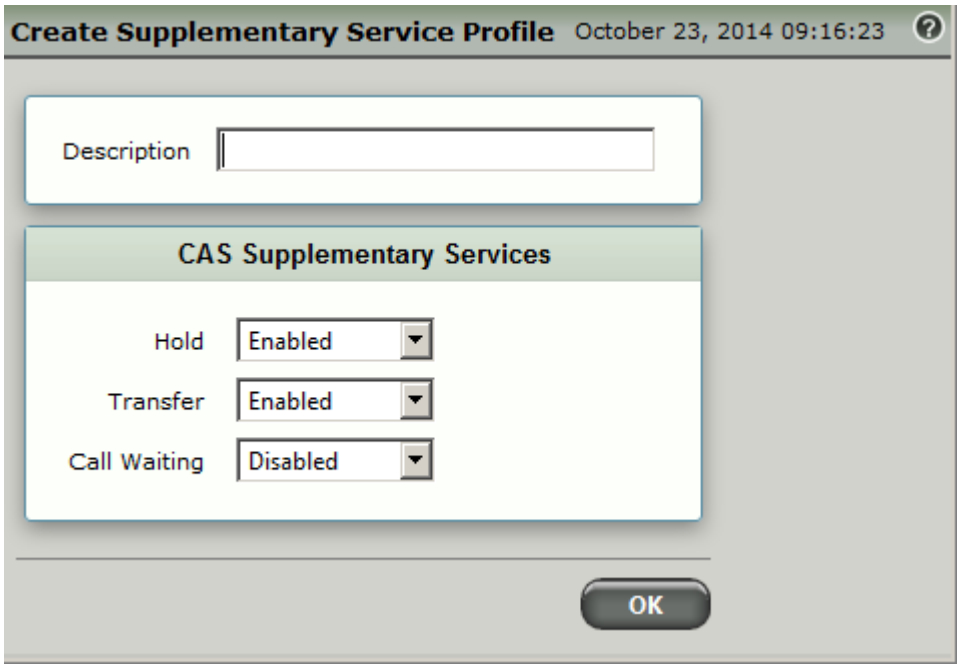
1. Click the **expand** ( ) Icon next to the entry you wish to modify.

Copyright © 2015 Sonus Networks. All rights reserved.

2. Edit the entry properties as required, see details below.

Creating a Supplementary Service Profile

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, click **CAS > Supplementary Service Profiles**.
3. At the top of the screen, click **+**. The **Create Supplementary Service Profile** window is displayed.
4. Enter data in the fields, see details below.
5. Click **OK**.



Supplementary Service Profile - Field Definitions

Hold

Used to enable/disable the Hold/Off Hold feature.

When enabled, the user can perform a flash hook (quickly depressing button on the handset cradle) to put the active call on hold, after which they will hear a dial tone. To take the call off hold and resume speaking, the user performs a second flash hook. If the call remains on hold for more than 20 seconds, the dial tone changes to a fast busy tone. The user can perform a flash hook at anytime to resume the call.

Transfer

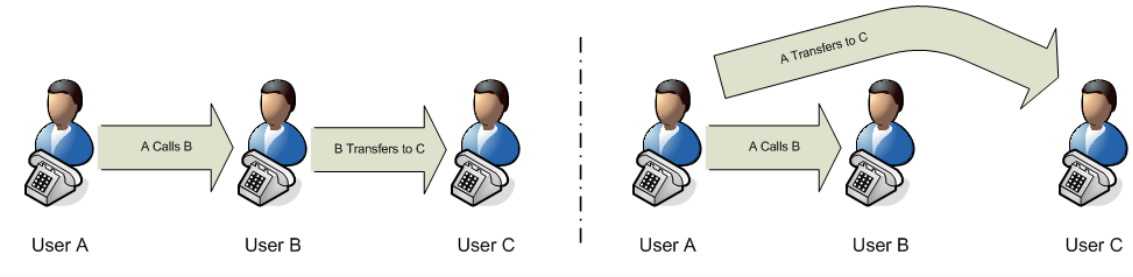
Copyright © 2015 Sonus Networks. All rights reserved.

Used to enable/disable the Transfer feature. If enabled, the user can perform a flash hook to get a dial tone (the active call will be put on hold) and to start dialing the phone number that the active call will be transferred to.

Click here to read more about this feature.

The Sonus SBC 1000/2000 supports two transfer modes, **attended** and **unattended**, both work similarly by transferring a call from one receiving extension to another receiving extension.

An attended transfer is that transfer scenario in which the user at the new receiving extension answers the call before the user transferring the call (original recipient) hangs up. An unattended (or blind) transfer is that transfer scenario in which the user transferring call hangs up after the new recipient's extension begins to ring and before they answer.



Normal Transfer (attended or unattended)

To transfer a call, one of the parties (User B) on the call performs a flash hook (quickly depressing button on the handset cradle), dials the number of the user (User C) to which they want to transfer the call, and then hangs up.

No Answer

If the new recipient of the call fails to answer within a predetermined length of time, the ring back tone heard by the connected caller(s) with become a fast busy tone. If this is an attended transfer, both will hear the ring tone, then fast busy.

Rejected Transfer

Assume that **User A** is connected to **User B**, then **User B** transfers the call to **User C**. **User C** answers the call. If **User C** hangs up before **User B** the call reverts to a call between **User A** and **User B**.

Call Waiting

Used to enable/disable the Call Waiting feature. If enabled, Call Waiting allows an FXS port to handle two calls at the same time. When Call Waiting is enabled on an FXS port, the user on the FXS port is notified of an incoming new call even though the user is already on an existing call. At the same time, the second caller hears ring back. Call waiting notification is in the form of a double-tone with configurable frequency and on/off intervals.

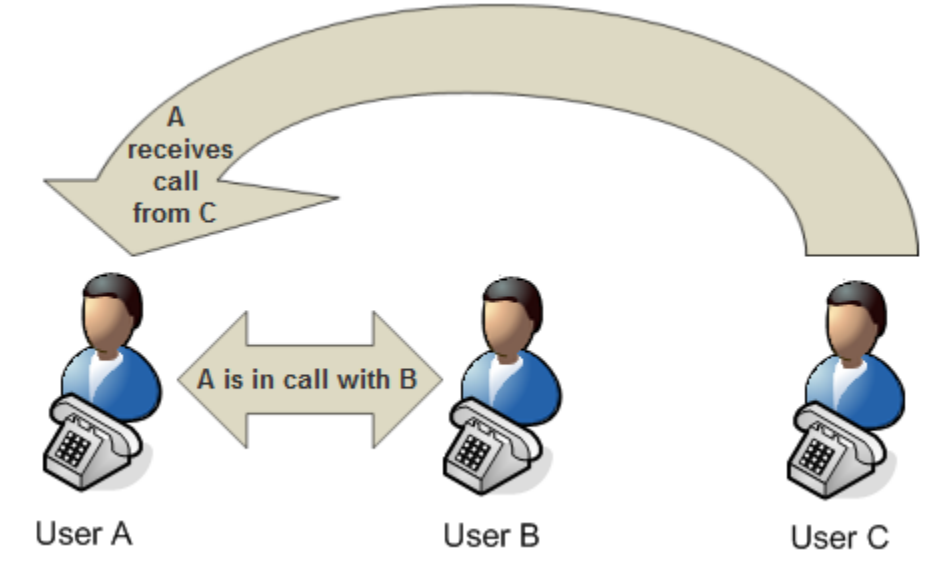
Available options: **Enabled** (the FXS port will receive call waiting notification when a second call destined for the same port comes into the port) or **Disabled** (any incoming call destined for the FXS port engaged in another call receives a busy signal). Default entry: **Disabled**.

Click here to read more about this feature.

Call Waiting - How does it work?

Copyright © 2015 Sonus Networks. All rights reserved.

Call Waiting is triggered when a user at the FXS port is in a call and another call from another user gets routed to the same FXS port.



When the user receives a call waiting notification (a double-tone), the following options are available:

Conversation is placed on hold.
User can place the existing call on hold and answer the new call by hitting the flash button on the analog phone. The on-hold caller hears silence.

Existing conversation is ended.
User can end the existing conversation by simply hanging up the phone and answering the new call. The current call is disconnected and the phone rings to answer the second call.

Ignore the new call.
User can ignore the new call by continuing the conversation on the existing call. The SBC will stop the call waiting notification tone after three cycles.

New caller disconnects call.
The new caller can disconnect the call. As a result, the call waiting notification stops.

Far end of active call disconnects.
The far end of the active call disconnects. The user on the FXO port hears silence until the flash button is hit to answer the new call, or the user hangs up (in which case the phone will ring).

How to configure Call Waiting

The following configuration must be completed for Call Waiting:

- Enable Call Waiting through the CAS Supplementary Profile.
- Configure the Call Waiting tones through Creating and Modifying Tone Tables. The tone parameters must match the country where the SBC 1000/2000 is hosted. For more information about country-specific values for these tone parameters, see Various Tone Used in Nation Networks.
- Configure the FXS CAS Signaling Group (which uses the CAS Supplementary profile) as follows: From the **Channel Hunting** drop down box, select **Own Number**. See Creating and Modifying CAS Signaling Groups.

Copyright © 2015 Sonus Networks. All rights reserved.

Working with System Settings

This section contains procedures for managing system settings, such as; system configuration, time source, and system date and time.

Backing Up Data

Restoring Data

Using the Custom Passphrase

Configuring Host Information and DNS

Configuring the System Clock Source

Configuring an NTP Time Source

Configuring the System Companding Law

Configuring the System Date and Time

Configuring Quality of Experience (QoE) Settings

- QoE Counters

Partial Configuration Imports

Importing and Exporting Transformation Tables

Backing Up Data

Overview

This page describes the procedure for backing up your Sonus SBC 1000/2000 system configuration to a file. The backup data will include the following Sonus SBC 1000/2000 data elements:

1. The configuration file (including any imported certificates)
2. The local users and passwords
3. The pre and post login messages

Sonus SBC 1000/2000 with a Built-in ASM

If your Sonus SBC 1000/2000 unit has a built-in Application Solution Module (ASM), then the following configuration data elements are also stored:

1. The ASM's Network Settings
2. The ASM's Remote-Desktop Setting

Important Note:

If the ASM is deployed as a Lync SBA, the SBA configuration **are not** stored in the backup file. |

Copyright © 2015 Sonus Networks. All rights reserved.

Screens shown below reflect Release 3.2.1 and later.

For Release 3.2, the instructions for the Passphrase appear on the screen; for Release 3.2.1 and later, the instructions appear only when you scroll the mouse over the **Passphrase** option in blue.

Backing up a Sonus SBC 1000/2000 Configuration

For specific information about the Passphrase, see Using the Custom Passphrase.

This operation can be accessed either via the **Tasks Tab** or the **Settings Tab**.

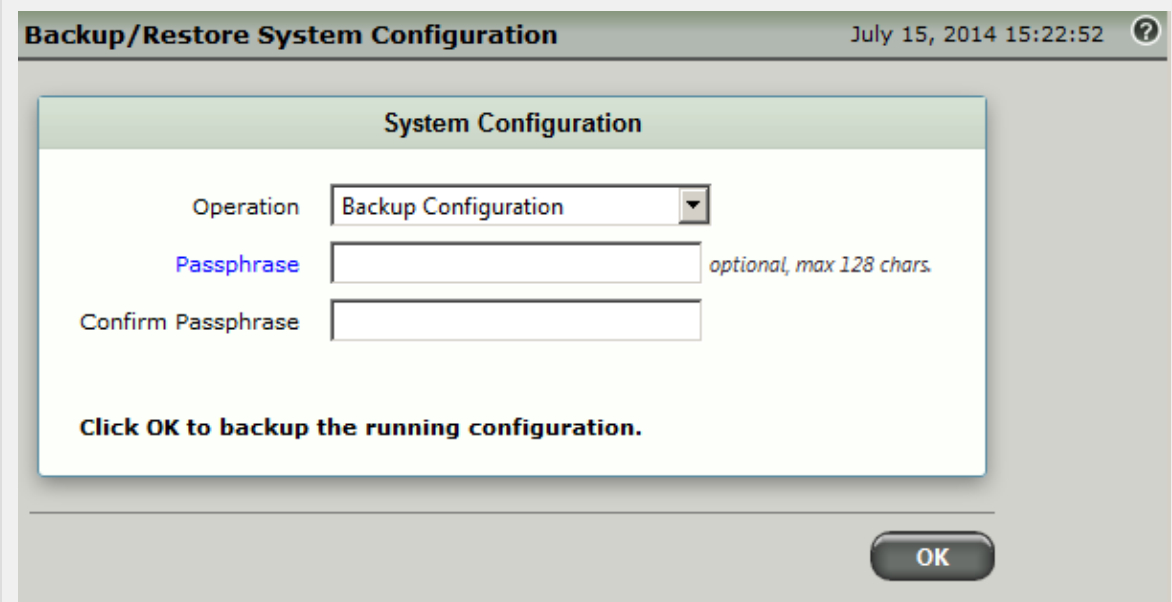
Tasks Tab

Copyright © 2015 Sonus Networks. All rights reserved.

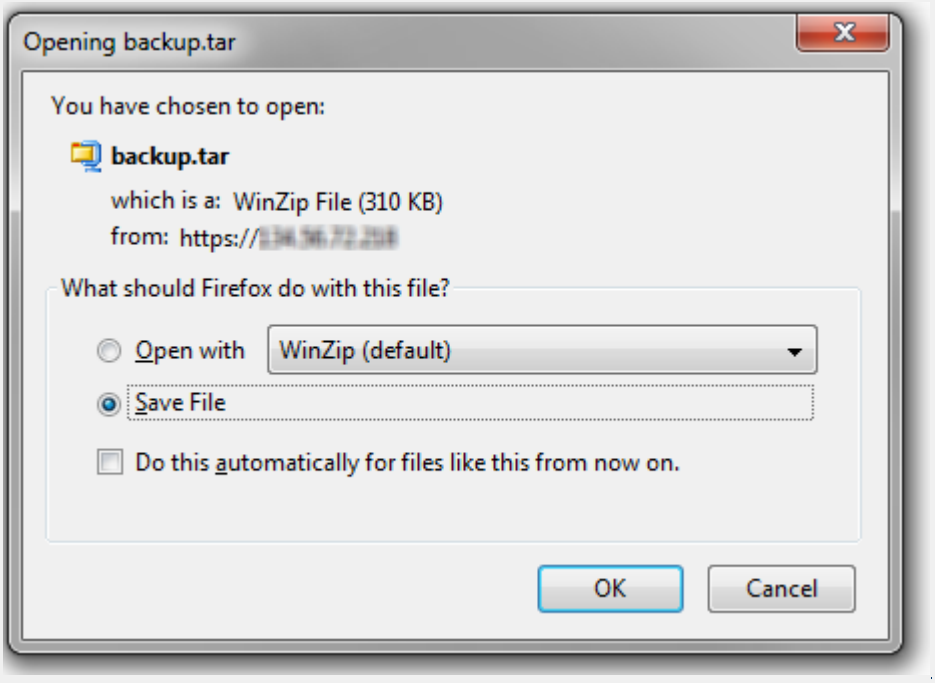
1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, click **System** > **Backup/Restore Config**.
3. From the **Operation** drop down box, select **Backup Configuration**.
4. Enter a **Passphrase** for configuration back up (optional; up to 128 alpha-numeric characters). In the WebUI, scroll the mouse over the Passphrase field (in blue) for additional information.

   > A passphrase is optional and, if provided, will be used in place of a node-specific cipher key to protect AD Credentials, Shared Keys, and other sensitive data.

5. Enter the same password in the **Confirm Passphrase** box.



6. Click **OK** (if you enter a passphrase or leave blank, the **Open** dialog is displayed).
7. Choose a location in which to save the file.



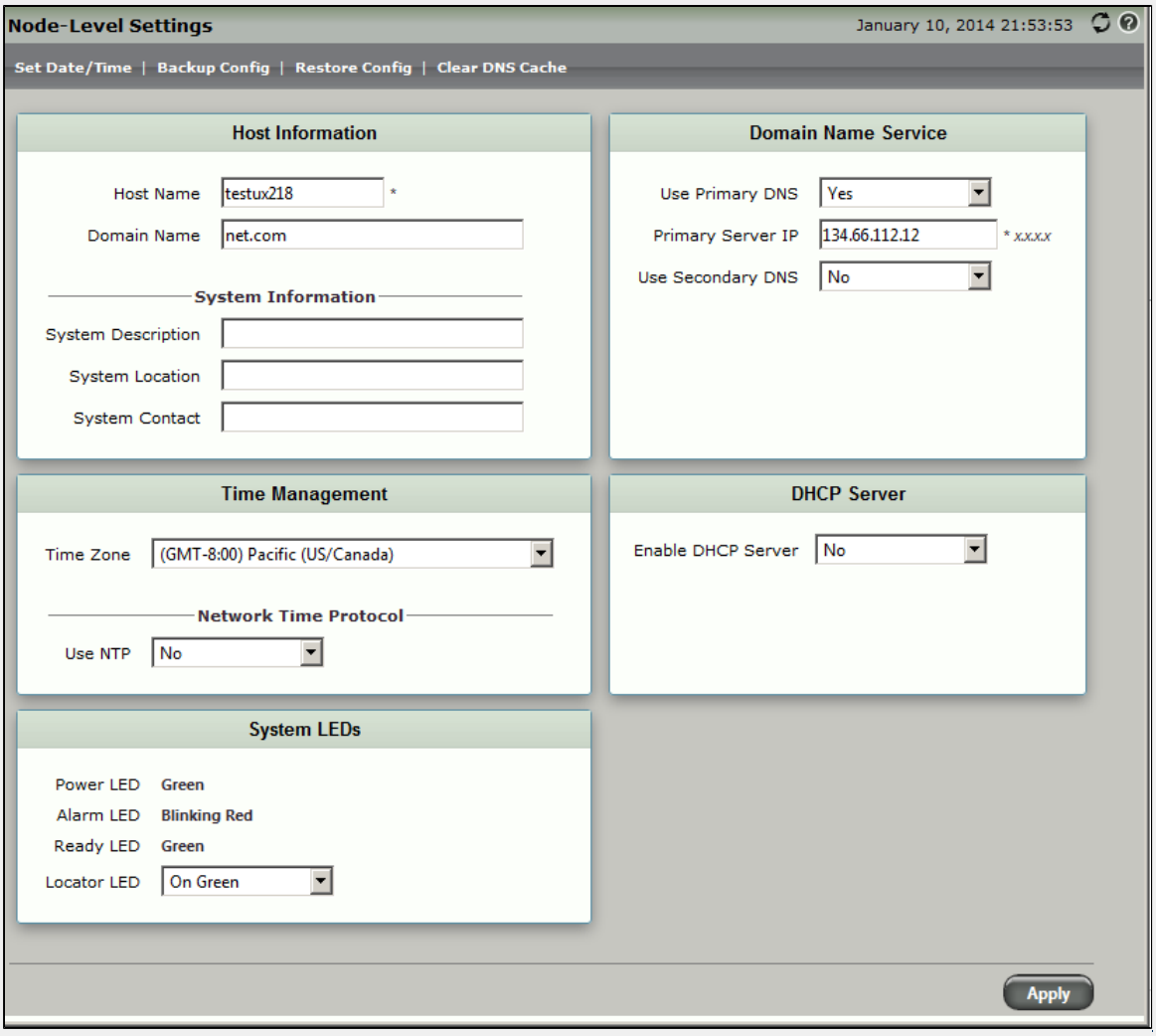
8. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.

The SBC 1000/2000 saves your configuration information as a *.tar* file only.

Settings Tab

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Node-Level Settings**.

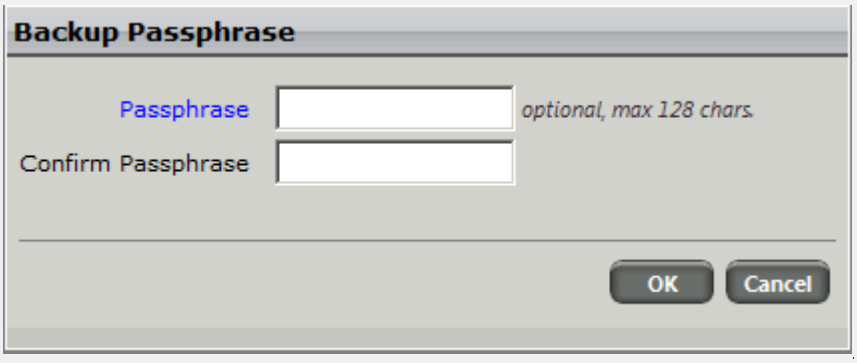


3. Click the **Backup Config** link in the upper left hand side of the Node-Level Settings window.
4. Enter a **Passphrase** for configuration back up (optional; up to 128 alpha-numeric characters). In the WebUI, scroll the mouse over the Passphrase field (in blue) for additional information.

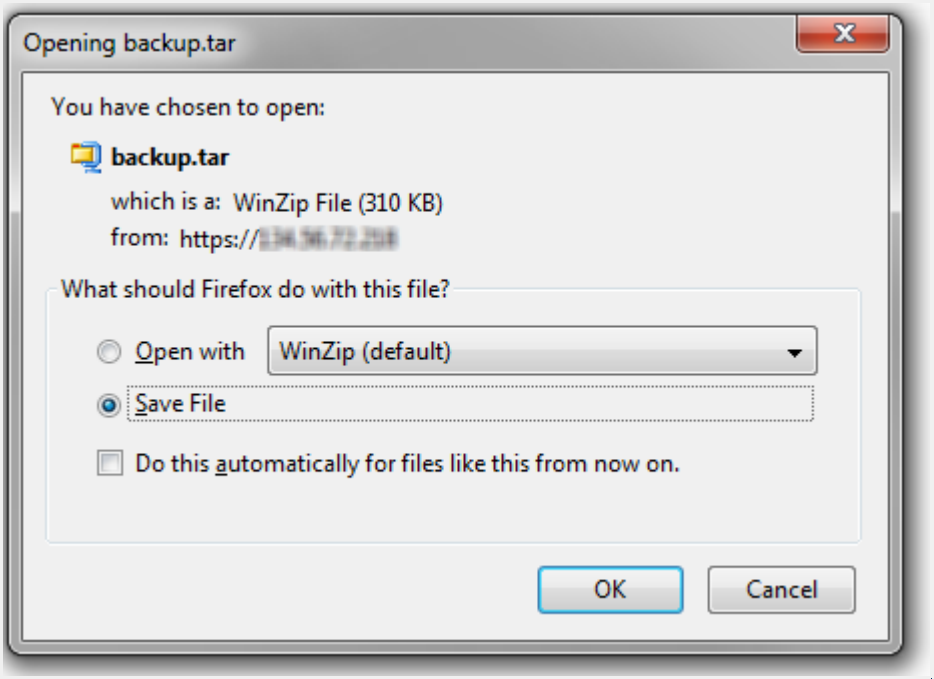
A passphrase is optional and, if provided, will be used in place of a node-specific cipher key to protect AD Credentials, Shared Keys, and other sensitive data.

Copyright © 2015 Sonus Networks. All rights reserved.

5. Enter the same password in the **Confirm Passphrase** box.



6. Click **OK** (if you enter a passphrase or leave blank, the **Open** dialog is displayed).
7. Choose a location in which to save the file.



8. Click **OK**.

> **Note:**
>
> The SBC 1000/2000 saves your configuration information as a *.tar* file only.

> **Helpful Tip:** You may want to rename your backup file to a name that indicates the current software version and/or system configuration.

Restoring Data

Overview

This page describes the procedure for backing up your Sonus SBC 1000/2000 system configuration to a file. The backup data will include the following Sonus SBC 1000/2000 data elements:

1. The configuration file (including any imported certificates)

Copyright © 2015 Sonus Networks. All rights reserved.

2. The local users and passwords
3. The pre and post login messages

Sonus SBC 1000/2000 with a Built-in ASM

If your Sonus SBC 1000/2000 unit has a built-in Application Solution Module (ASM), then the following configuration data elements are also stored:

1. The ASM's Network Settings
2. The ASM's Remote-Desktop Setting

> **Important Note:**
>
> If the ASM is deployed as a Lync SBA, the SBA configuration **are not** stored in the backup file. |

> Screens shown below reflect Release 3.2.1 and later.
>
> For Release 3.2, the instructions for the Passphrase appear on the screen; for Release 3.2.1 and later, the instructions appear only when you scroll the mouse over the **Passphrase** option in blue.

Backing up a Sonus SBC 1000/2000 Configuration

> For specific information about the Passphrase, see Using the Custom Passphrase.

This operation can be accessed either via the **Tasks Tab** or the **Settings Tab**.

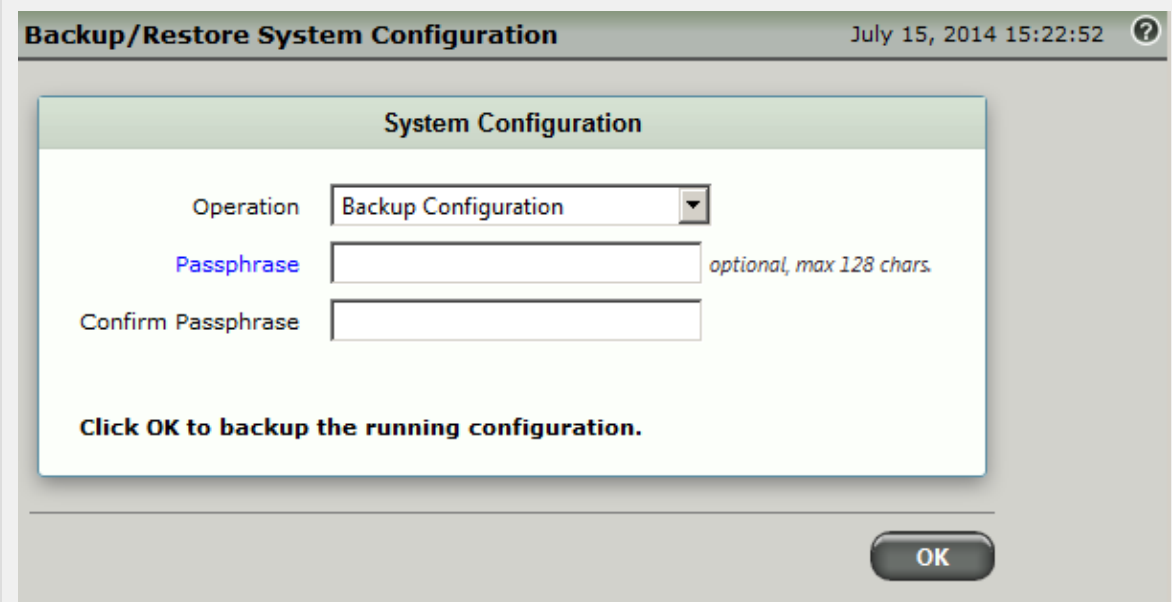
Tasks Tab

Copyright © 2015 Sonus Networks. All rights reserved.

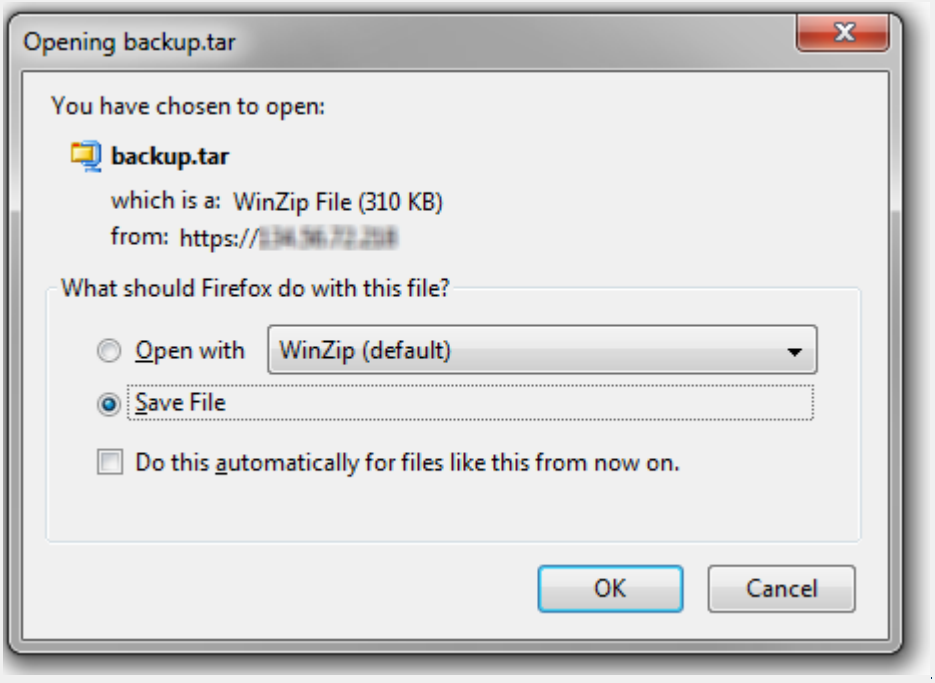
1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, click **System** > **Backup/Restore Config**.
3. From the **Operation** drop down box, select **Backup Configuration**.
4. Enter a **Passphrase** for configuration back up (optional; up to 128 alpha-numeric characters). In the WebUI, scroll the mouse over the Passphrase field (in blue) for additional information.

> A passphrase is optional and, if provided, will be used in place of a node-specific cipher key to protect AD Credentials, Shared Keys, and other sensitive data.

5. Enter the same password in the **Confirm Passphrase** box.



6. Click **OK** (if you enter a passphrase or leave blank, the **Open** dialog is displayed).
7. Choose a location in which to save the file.



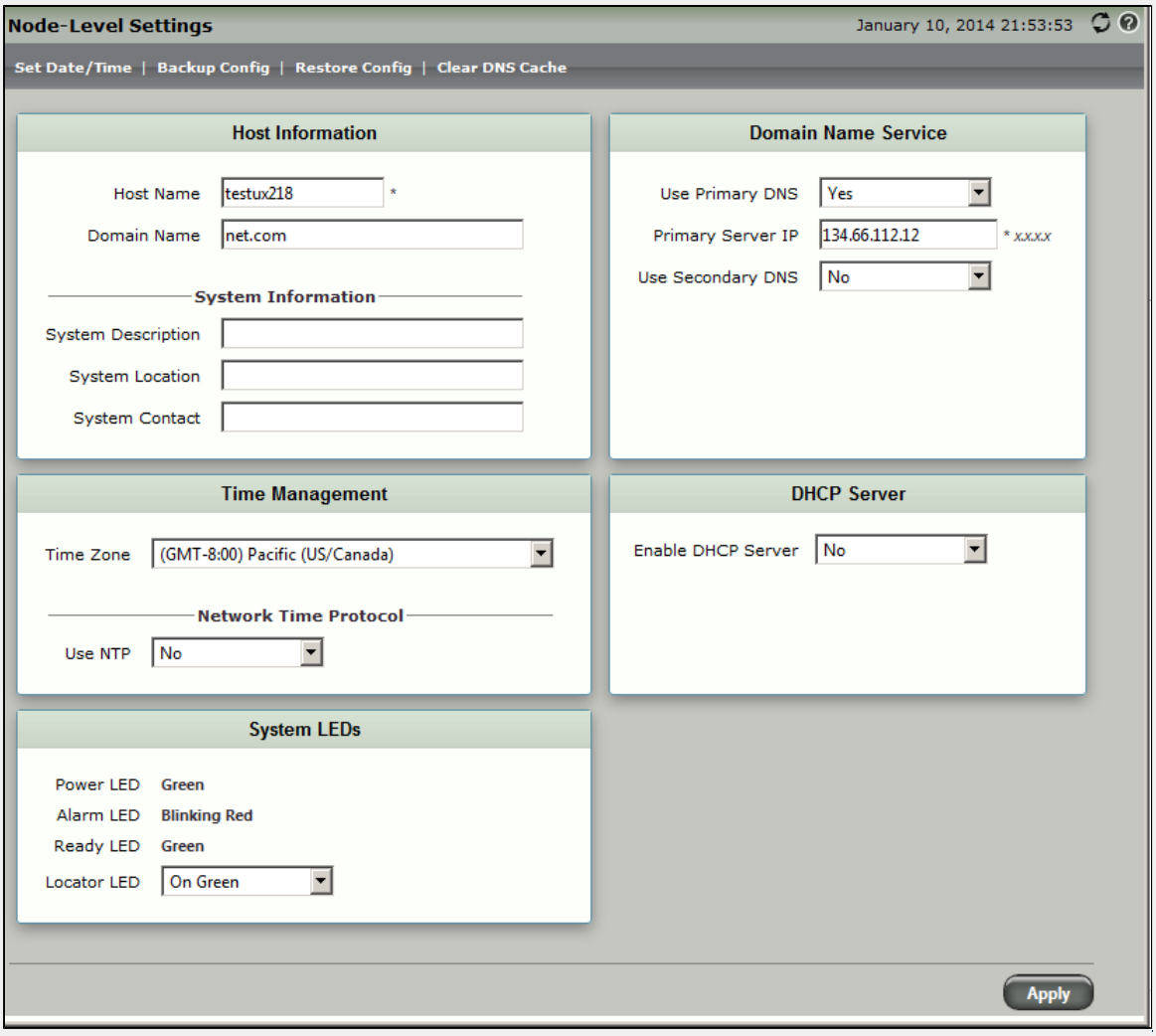
8. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.

The SBC 1000/2000 saves your configuration information as a *.tar* file only.

Settings Tab

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Node-Level Settings**.

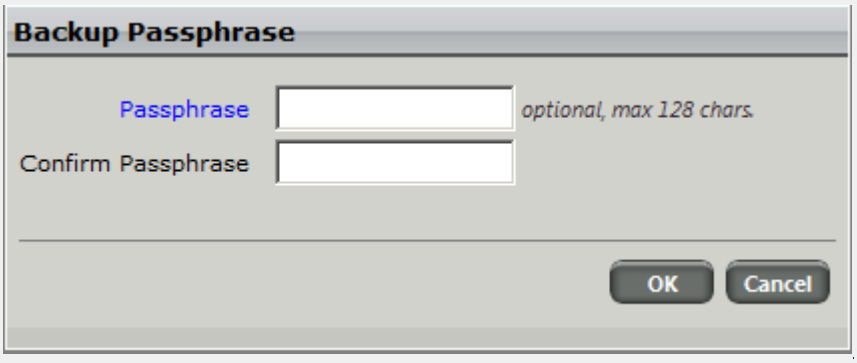


3. Click the **Backup Config** link in the upper left hand side of the Node-Level Settings window.
4. Enter a **Passphrase** for configuration back up (optional; up to 128 alpha-numeric characters) In the WebUI, scroll the mouse over the Passphrase field (in blue) for additional information.

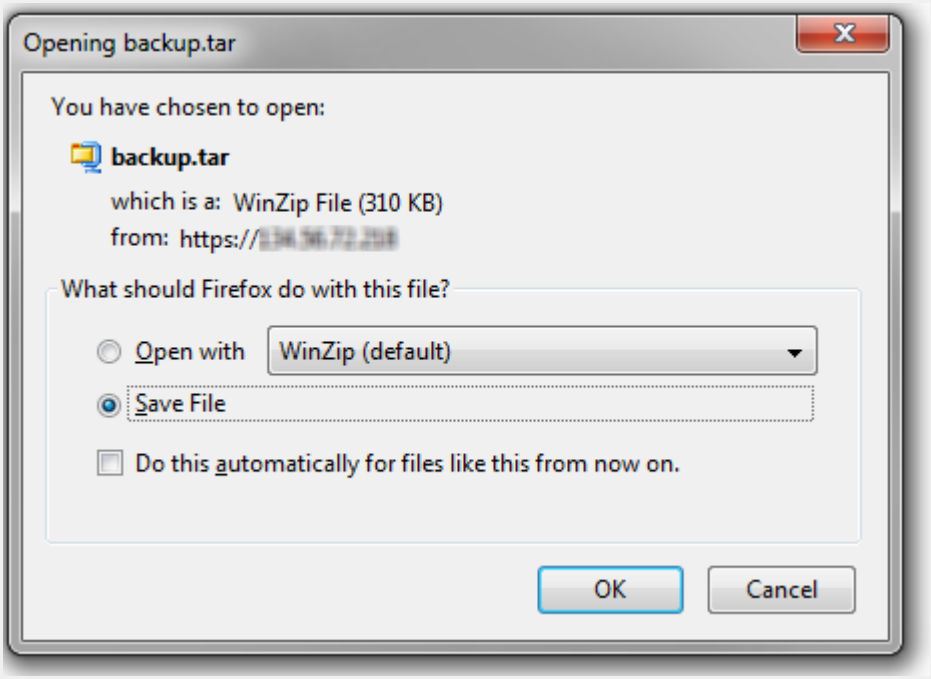
A passphrase is optional and, if provided, will be used in place of a node-specific cipher key to protect AD Credentials, Shared Keys, and other sensitive data.

Copyright © 2015 Sonus Networks. All rights reserved.

5. Enter the same password in the **Confirm Passphrase** box.



6. Click **OK** (if you enter a passphrase or leave blank, the **Open** dialog is displayed).
7. Choose a location in which to save the file.



8. Click **OK**.

Note:

The SBC 1000/2000 saves your configuration information as a *.tar* file only.

Helpful Tip: You may want to rename your backup file to a name that indicates the current software version and/or system configuration.

Using the Custom Passphrase

Using the Custom Passphrase

Once the custom passphrase is defined, it must be kept confidential for security purposes. The **same** passp hrase must be used during the Backup and Restore procedure in order for the passwords to be encrypted/decrypted successfully.

Copyright © 2015 Sonus Networks. All rights reserved.

A user-defined passphrase (up to 128 alpha-numeric characters) option is available when you Backup (export), Restore, and Import, a configuration file in the SBC. Custom passphrase is used when there is a need for duplicating similar configurations in different nodes; the configuration is exported from one node and imported into another node.

On Backup (export), the passphrase is used to encrypt the following passwords in an exported configuration file:

- SIP - Local Pass through Authorization and Remote Authorization tables
- AD Domain\Controller Password
- Radius Shared Secret Key
- IPsec Shared Secret Key

On Restore and Import, these same passwords can then be decrypted by the importing node.

The passphrase will not encrypt the already-encrypted user passwords which are used for Login credentials.

> ⚠ The Restore and Import functions are restricted to the same platform (i.e., restoring a configuration from SBC1000 to SBC2000 or vice versa is not permitted; an error message will display).

Using Custom Passphrase with Backup

When a passphrase is entered during the Backup procedure, the passwords in the downloaded configuration (noted above) are encrypted using the passphrase. If a password is not entered, the passwords are downloaded in their original form and are not usable in a different node.

Using Custom Passphrase with Restore (via WebUI)

The Restore function through the WebUI, is normally used to restore a configuration on the same node, or as a way to duplicate the configuration of the source node (which includes IP address and IP routing). When a passphrase is entered, the passwords (noted above) in the imported configuration are decrypted using the passphrase. If a passphrase is not entered, the configuration will not be usable in a different node. If the decryption fails, the restore will continue, but the passwords will be lost and an error message is displayed.

Using Custom Passphrase with Import (via REST)

The Import function through REST, is normally used to duplicate the configuration on multiple nodes without changing the node's IP address and IP routing. When a passphrase is entered, the passwords (noted above) in the imported configuration are decrypted using the passphrase. If a passphrase is not entered, the configuration will not be usable in a different node. If the decryption fails, the restore will continue, but the passwords will be lost and an error message is displayed.

Import through REST will not import the Local and Remote Authorization tables to the target node, but Restore will decrypt and restore the local and remote authorization tables on the target node.

Configuring Host Information and DNS

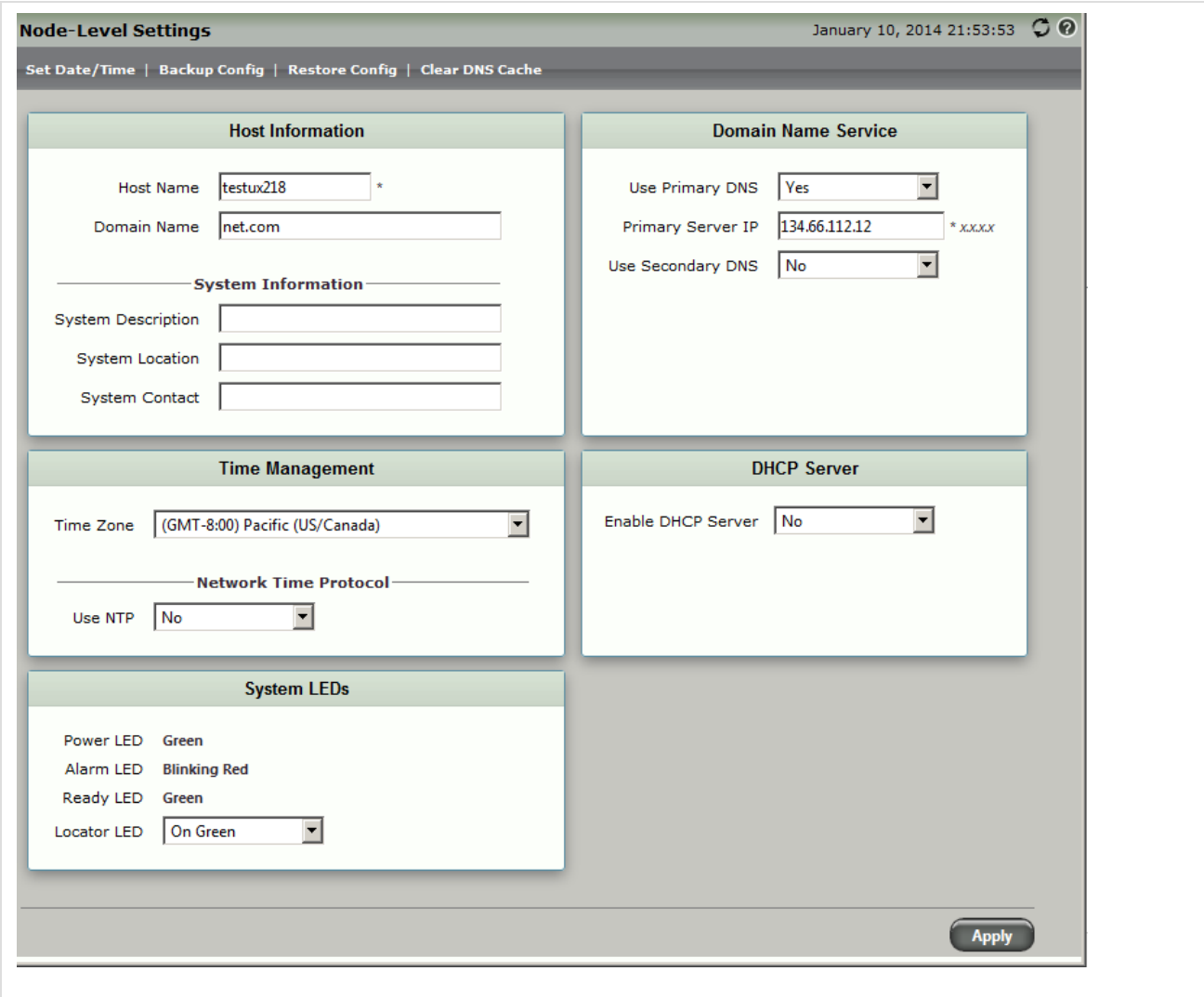
You can configure the Sonus SBC 1000/2000 host information and DNS settings via the WebUI as outlined below. The Host Information contains system information attributes that are used by the SNMP manager.

Changing Host Information

Copyright © 2015 Sonus Networks. All rights reserved.

To change the host information for your Sonus SBC 1000/2000:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation page, go to **System > Node-Level Settings**.



Node-Level - Field Definitions

Node-Level Network Settings

Defines whether the node level settings are set through dynamic or static configuration. Available options: Dynamic (configured by system) or Static (configured manually). The Dynamic option is available only when one or more logical interfaces are configured to use Dynamic addressing.

Host Information - Field Definitions

Host Name

Specifies the DNS host name for the system.

Domain Name

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the DNS domain name for the system. This field is available only if the Node-Level Network Settings field is set to Static.

System Description

Sets the SNMP attribute 'sysDescription' in the System-Group MIB. Operator may use this field to record a short description of the system. By convention, this field should include the full name and the hardware type.

System Location

Sets the SNMP attribute 'sysLocation' in the System-Group MIB. Operator may use this field to record the physical location of the system.

System Contact

Sets the SNMP attribute 'sysContact' in the System-Group MIB. Operator may use this field to record the contact person for this system and information about how to contact this person.

Domain Name Service - Field Definitions

Use Primary DNS

Specifies whether or not the Sonus SBC 1000/2000 uses DNS. Available options: Yes or No. This field is available only if the Node-Level Network Settings field is set to Static.

Primary Server IP

Specifies the IP Address of the Primary DNS server. If the Node-Level Network settings drop down box is set to Dynamic, this field is configured automatically. Field is displayed when User Primary DNS is configured to Yes.

Use Secondary DNS

Specifies whether or not a secondary DNS server is used. Available options: Yes or No.

Secondary Server IP

Specifies the IP Address of the Secondary DNS server. If the Node-Level Network settings is set to Dynamic, this field is configured automatically. Field is displayed when the Use Secondary DNS drop down box is set to Yes.

Time Management - Field Definitions

Time Zone

Sets the time zone for the node. Select from the drop down list.

Use NTP

Determines whether to use Network Time Protocol (NTP) as a time source. Available options: Yes or No.

Copyright © 2015 Sonus Networks. All rights reserved.

NTP Server

Specifies the host name or IP address of the first NTP server. If the hostname is supplied, the SBC uses DNS to connect to the NTP server. This field is available only when the Use NTP field is set to Yes.

NTP Server Authentication

Specifies whether or not to use authentication when communicating with the NTP server. Available options: Enabled or Disabled. This field is available only when the Use NTP field is set to Yes.

NTP Server - MD5 Key ID

Specifies the MD5 Key ID to be used in authenticating the first NTP server. This field is available only when the NTP Server Authentication field is Enabled.

NTP MD5 Key

Specifies the MD5 key used when authenticating the first NTP Server. This field is available only when the NTP Server Authentication field is Enabled.

Use NTP Server 2

Specifies whether or not to use a second NTP Server as a time source. Available options: Yes or No.

NTP Server 2

Specifies the host name or IP address of the second NTP server. If the hostname is supplied, the SBC uses DNS to connect to the NTP server. This field is available only when the Use NTP Server 2 field is set to Yes.

NTP Server 2 Authentication

Specifies whether or not to use authentication when communicating with the second NTP server. Available options: Enabled or Disabled. This field is available only when the Use NTP Server 2 field is set to Yes.

NTP Server 2 - MD5 Key ID

Specifies the MD5 Key ID to be used in authenticating the second NTP server. This field is available only when the NTP Server 2 Authentication field is Enabled.

NTP Server 2 - MD5 Key

Specifies the MD5 key used when authenticating the second NTP Server. This field is available only when the NTP Server 2 Authentication field is Enabled.

DHCP Server - Field Definitions

Enable DHCP Server

Copyright © 2015 Sonus Networks. All rights reserved.

Enables whether or not the Sonus SBC 1000/2000 behaves as a DHCP server (grants leases to other hosts on the network). Available options: No or Yes.

System LEDs

Power LED

This field is automatically populated with the current status of the Power LED. Options are: **Green** (indicates the system is connected to a power source) or **Off** (unit is not connected to power source). For additional information about the Power LED's color and status definitions, see Sonus SBC 1000-2000 Status LEDs.

Alarm LED

This field is automatically populated with the current status of the Alarm LED on the front panel. Possible entries: **Green** (no alarm), **Off** (warning), **Amber** (minor alarm), **Red** (major alarm), **Red Blinking** (critical alarm). For additional information about the Alarm LED's color and status definitions, see Sonus SBC 1000-2000 Status LEDs.

Ready LED

This field is automatically populated with the current status of the Ready LED on the front panel. Options are: **Green** (indicates the system is fully initialized) or **Off** (system is not fully initialized). For additional information about the Ready LED's color and status definitions, see Sonus SBC 1000-2000 Status LEDs.

Locator LED

This field provides the option to set the Locater LED on the front of the SBC unit to either **Off** (LED is off), **On Green** (LED is green) or **Blinking Green** (LED blinks one time per second). Default entry: **On Green**. This option helps network personnel easily locate the SBC unit in a rack with other equipment. This LED is also recognized as the Peer Node Status LED. For additional information about the Locator LED's color and status definitions, see Sonus SBC 1000-2000 Status LEDs.

Configuring the System Clock Source

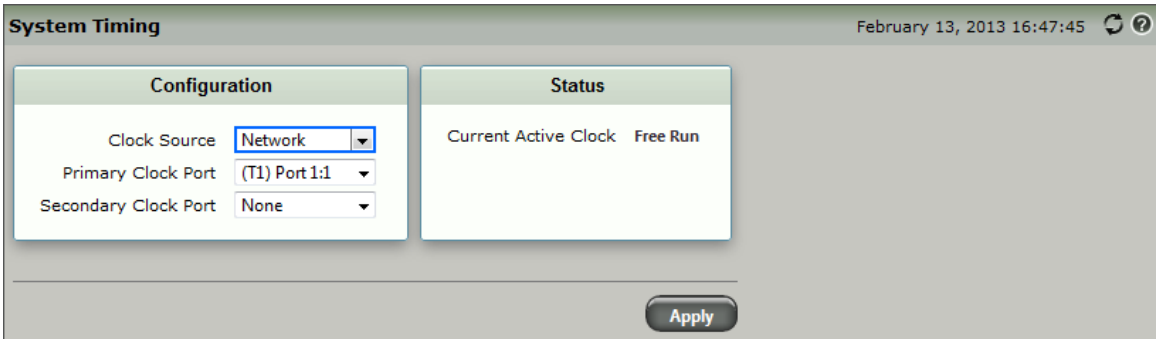
It is important that timing be consistent between elements of a VoIP topology. Sourcing the Sonus SBC 1000/2000 clock is critical in keeping the Sonus SBC 1000/2000 synchronized with other elements of the topology. The Sonus SBC 1000/2000 may obtain it's clock from a network (T1/E1) source such as a PBX or Central Office, or it may use its own internal clock which may itself by synchronized to an NTP source. Where the clock source originates depends entirely on the topology itself and varies on a case-by-case basis.

Configuring System Timing

Copyright © 2015 Sonus Networks. All rights reserved.

To configure system timing using a network clock source:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > System Timing**.



Configuration - Field Definitions

Clock Source

Specifies the source of the systems transmit clock.

- **System:** The built-in oscillator is used to transmit data over synchronous links. The system's internal clock can be modified by the system administrator, see Configuring the System Date and Time and Configuring an NTP Time Source.
- **Network:** The clock is derived from the data received from the peer devices on the network.

Primary Clock Port

Specifies the DS1 port from which the clock will be derived. This field is visible only if Network is specified as the Clock Source.

Secondary Clock Port

Specifies the DS1 port from which the clock will be derived. This field is visible only if Network is specified as the Clock Source.
The Secondary Clock Source is used only if the primary clock source is not of sufficient quality or becomes unavailable.

Configuring an NTP Time Source

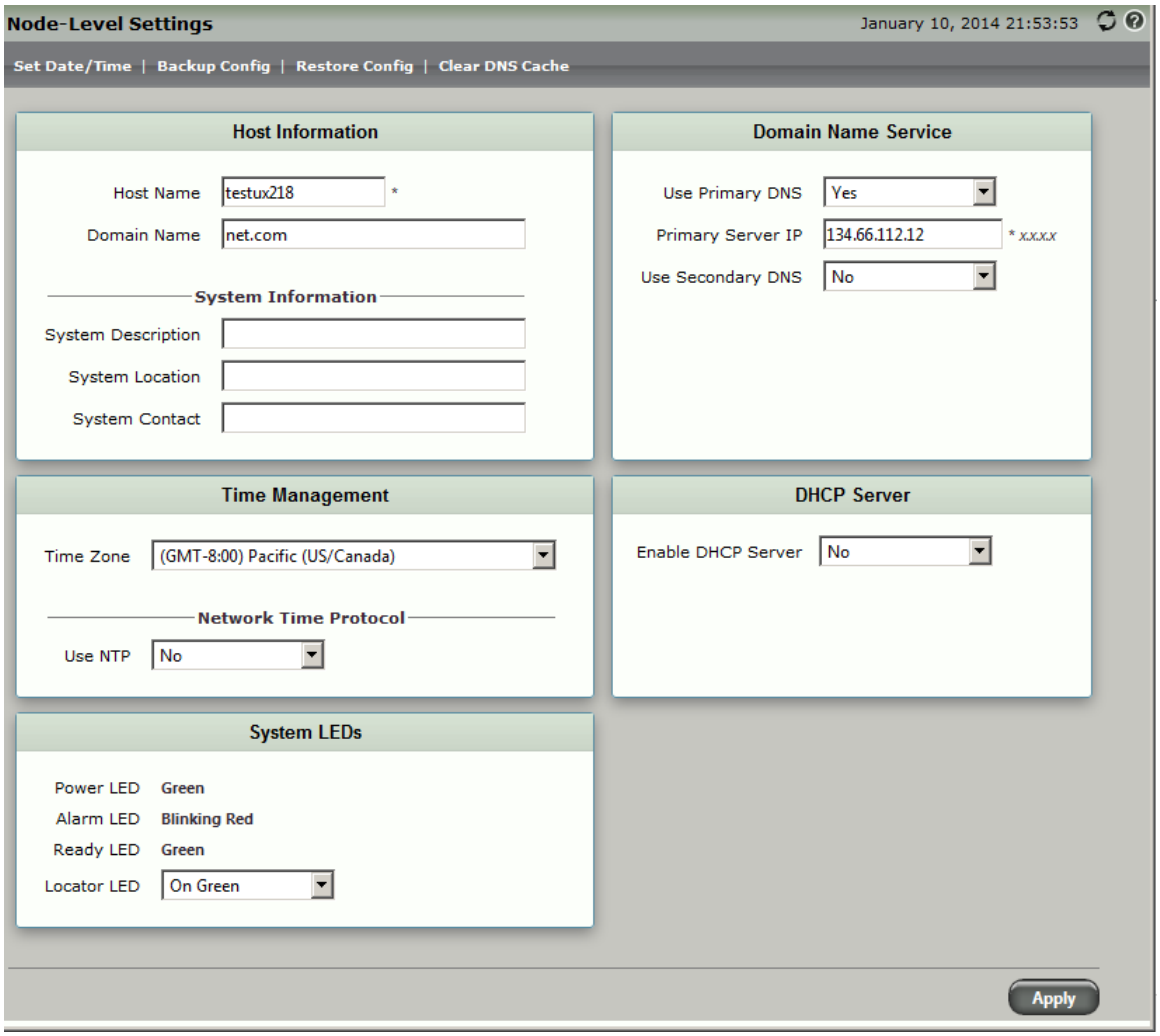
Accurate System timing is important for the proper operation of the Sonus SBC 1000/2000. The system time may be sourced from different places depending upon the specific topology where the Sonus SBC 1000/2000 is deployed. In some cases the Sonus SBC 1000/2000 itself may serve as a time source for the topology. In such cases, the Sonus SBC 1000/2000 may use its own independent internal clock, or it may be synchronized with a network time source through Network Time Protocol (NTP). The NTP source may be a public source such as NTP.org or NIST, or a private source such as an internal enterprise time server.

The Sonus SBC 1000/2000 allows you to configure a maximum of two NTP time servers from which to source time and date information.

Configuring the Sonus SBC 1000/2000 to Use an NTP Server

Copyright © 2015 Sonus Networks. All rights reserved.

To configure your Sonus SBC 1000/2000 to use NTP:



Time Management/Network Time Protocol - Field Definitions

The Time Management panel contains fields that enable you to set the time zone and configure one or more network time sources (NTP).

Use NTP

Specifies whether or not to use NTP as a time source.

NTP Server

Specifies the host name or IP address of the first NTP server. If the hostname is supplied, the Sonus SBC 1000/2000 uses DNS to connect to the NTP server.

NTP Server Authentication

Specifies whether or not to use authentication when communicating with the NTP server.

NTP Server - MD5 Key ID

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the MD5 Key ID to be used in authenticating the first NTP server. This field is visible only when Enabled is selected for the NTP Server Authentication option.

NTP MD5 Key

Specifies the MD5 key used when authenticating the first NTP Server.

Use NTP Server 2

Specifies whether or not to use a second NTP Server as a time source.

NTP Server 2: The fields used to configure the second NTP server are exactly the same as those used for the first server.

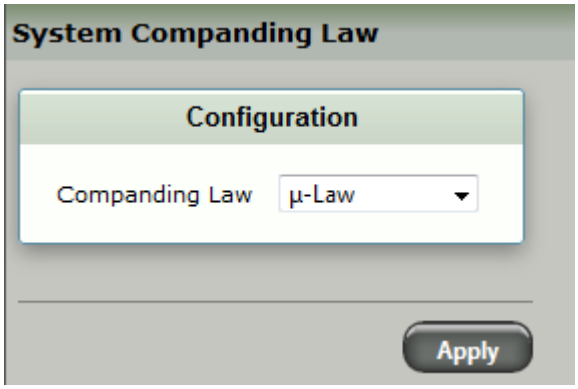
Configuring the System Companding Law

This feature is only available on the Sonus SBC 1000. Companding law is determined automatically on the Sonus SBC 2000 as a function of system hardware.

Setting the Companding Law

To set the companding law:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > System Companing Law**.



Configuration - Field Definitions

Companding Law

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies which companing law the system uses.

>> Click to see more information.

The correct companding law is dependent upon the physical interface type and switch variant.

Port Type	Protocol/Switch Variant	Companding Law
T1	ISDN/CAS	Mu-Law
E1	ISDN/CAS	A-Law
BRI	Japan ISDN	Mu-Law
BRI	ETSI/QSIG	A-Law

Caution

Misconfigured Companding Laws may result in dropped calls and/or poor audio quality. Symptoms include dropped outgoing ISDN/BRI calls and loud crackling noises on ISDN/Analog and BRI/Analog calls.

Configuring the System Date and Time

The Sonus SBC 1000/2000 system allows you to either set the date and time manually, or have it configured such that the system clock gets automatically synchronized with a Time Server via Network Time Protocol (NTP).

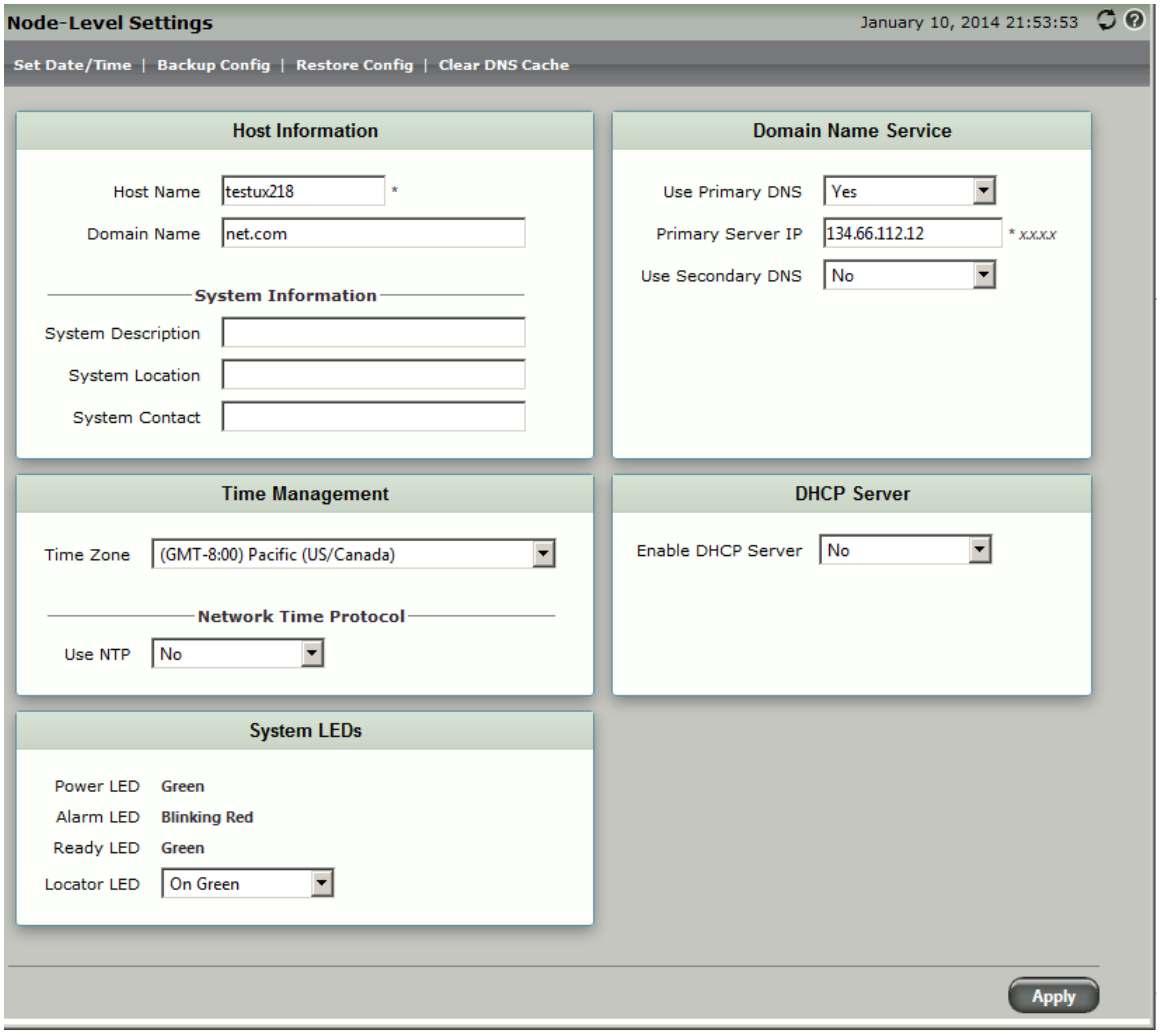
Setting the Date and Time on Sonus SBC 1000/2000

It is always **recommended to configure the Sonus SBC 1000/2000 with a Time Server** via NTP. This ensures the Sonus SBC 1000/2000's clock settings are accurate and will minimize common certificate issues when integrating with devices via TLS.

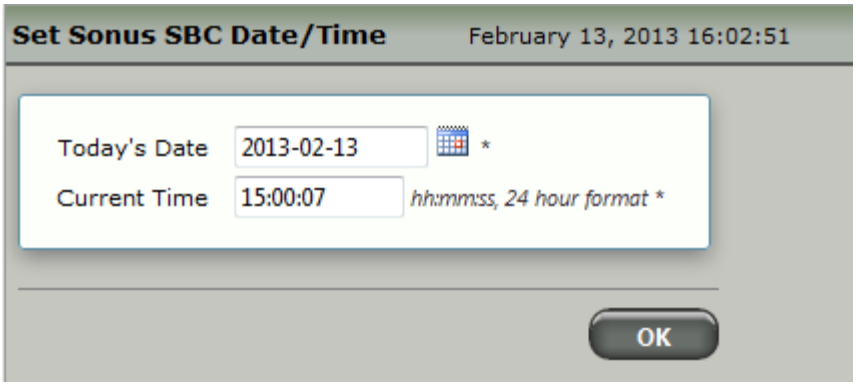
To set the date and time:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Node-Level Settings**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Click the **Set Date/Time**link at the top of the Node-Level Settings page.



4. Click on the **Calendar Widget** and select a date, or manually enter a date in the **Today's Date** text field.
5. Enter a time in the **Current Time** text field.
   The time must be entered in the form *hh:mm:ss* and must be in a 24-hour format (e.g., 14:25:55).
6. Click **OK**.

Configuring Quality of Experience (QoE) Settings

Copyright © 2015 Sonus Networks. All rights reserved.

Note

QoE Reporting must be enabled in the SIP Channels and Routing Panel of the relevant SIP Signaling group before statistics can be collected.

Related Documents
• Configuring the QoE Feature

Overview

The SBC Quality of Experience (QoE) feature collects data about call RTP streams, generates MOS information, and sends them to a MS Lync QoE server.

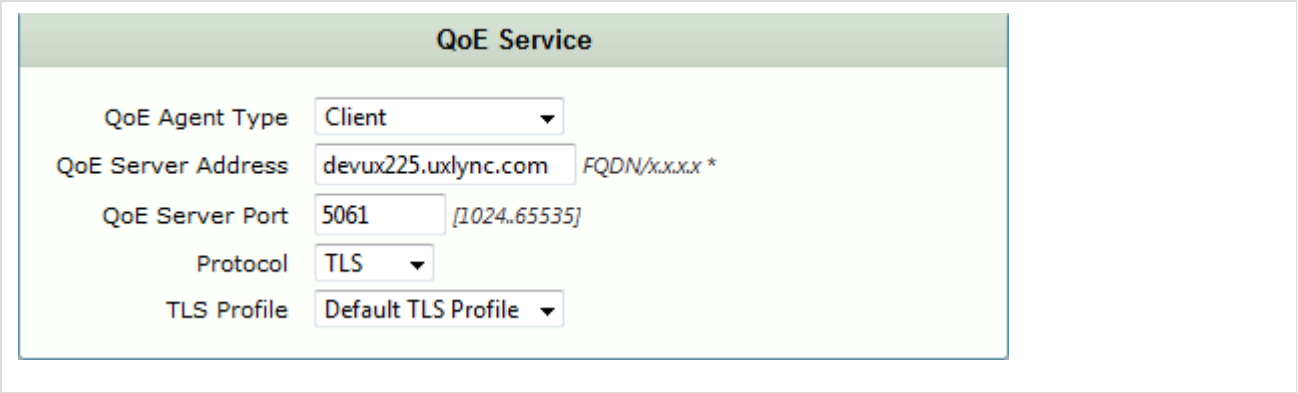
For more information about RTCP and MOS see the following:

- RFC 3611
- Mean Opinion Score and Metrics

Enabling QoE and Configuring the QoE Service

*To enable and configure the QoE service:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > QoE**.



QoE Service - Field Definitions

QoE Agent Type

Specifies whether the node is a QoE client or the QoE server.

QoE Server Address

The IP address of the QoE server node receiving the SIP NOTIFY message. QoE Reporting must be enabled in the SIP Signaling Group.

QoE Server Port

Copyright © 2015 Sonus Networks. All rights reserved.

The IP address of the QoE server node receiving the SIP NOTIFY message. QoE Reporting must be enabled in the SIP Signaling Group.

Protocol

Specifies the transport protocol used to send the NOTIFY.

TLS Profile

If TLS is selected this specifies the TLS Profile this port will use for secure SIP messages.

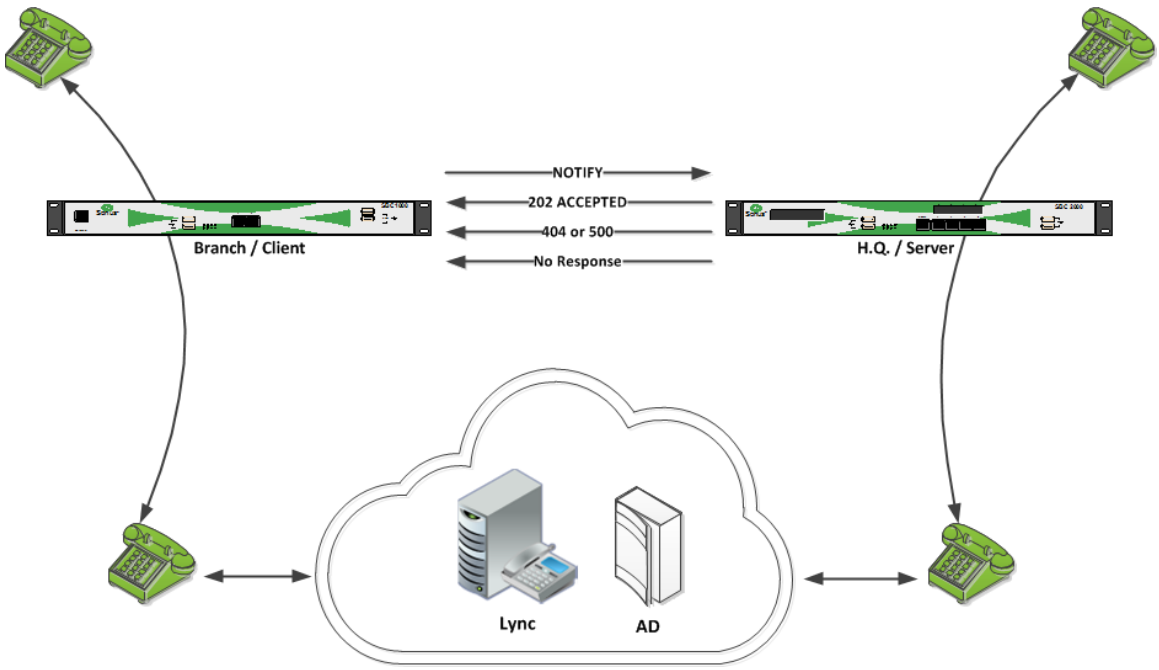
QoE Counters

This page discusses the counters associated with the Quality of Experience (QoE) Feature.

On This Page

- How The Counters Work
  - Branch/Client Counters
  - Headquarters/Server Counters

How The Counters Work



Branch/Client Counters

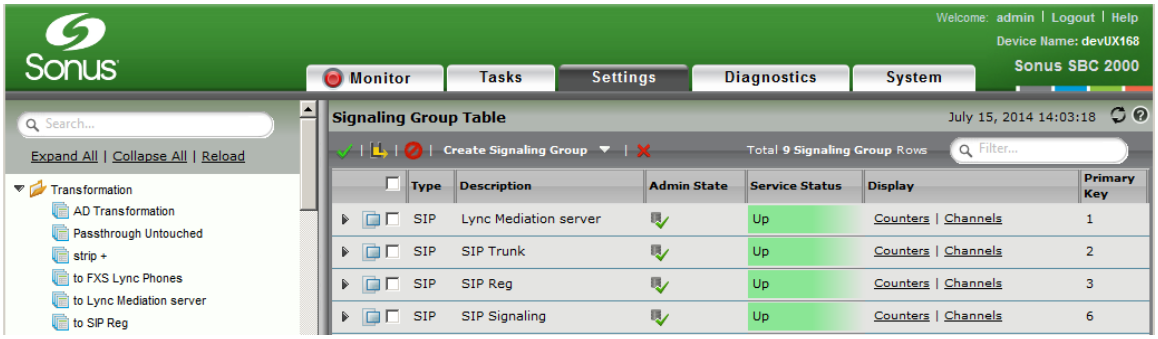
On a branch/client SBC, when a SIP call is terminated the SBC sends a NOTIFY and the QoE data to the server and the server normally responds with a 202 ACCEPTED message. If a 202 is received, the ***Successful QoE Reports*** counter is incremented. If the the server does not respond or it responds with a 404, 500, or other error, or there is no response, the ***Failed QoE Reports Sent*** counter is incremented.

Copyright © 2015 Sonus Networks. All rights reserved.

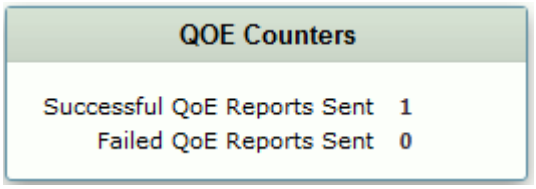
The branch or client side counters can be found in the associated SIP Signaling Group.

To view the branch/client counters:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups >*<SIPSG associated with the Lync Mediation Server>.***



3. Click the **Counters** link next to the signaling group used to communicate with the Lync Mediation Server.
4. Scroll to the bottom of the counters window.



Headquarters/Server Counters

Similar to the Client side, the Headquarters/Server also records successful transfers of QoE records. In the case of the HQ/Server side the transfers are between the SBC and the SBA. The transfers consists of data about SIP calls made on the HQ SBC as well as those records successfully transmitted from a branch/client SBC.

To views the QoE counters on the HQ/Server SBC:

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane go to, **Application Solution Module > Operational Status**.
3. Scroll down to the bottom of the page.

Partial Configuration Imports

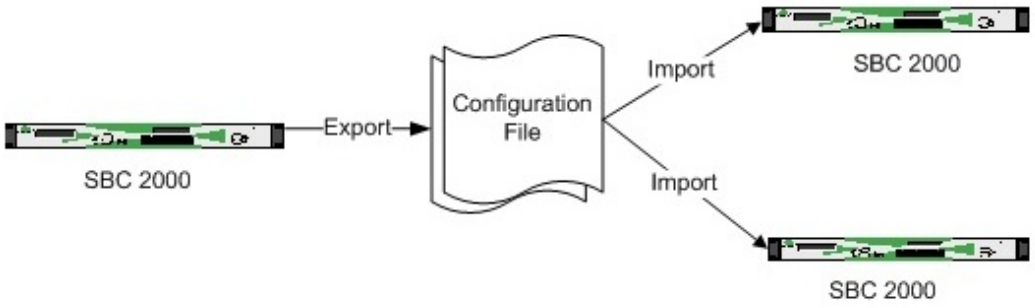
Overview

The SBC 1000/2000 allows you to import partial configurations from another SBC 1000/2000. This feature allows the system administrator to configure one or more units rapidly without the necessity of an EMS for auto-provisioning.

The process is similar to the restore process using a backup configuration file previously exported from another node. The difference is that when performing a partial configuration import, not all the configuration items in the backup file are applied to the target node.

> ⚠ You may not import across platform types (e.g. SBC 1000 to SBC 2000 or SBC 2000 to SBC 1000.

Copyright © 2015 Sonus Networks. All rights reserved.



Resources Not Imported

Several resources are not imported, mainly those that define the node as an identifiable individual and network related attributes. Those items not imported include:

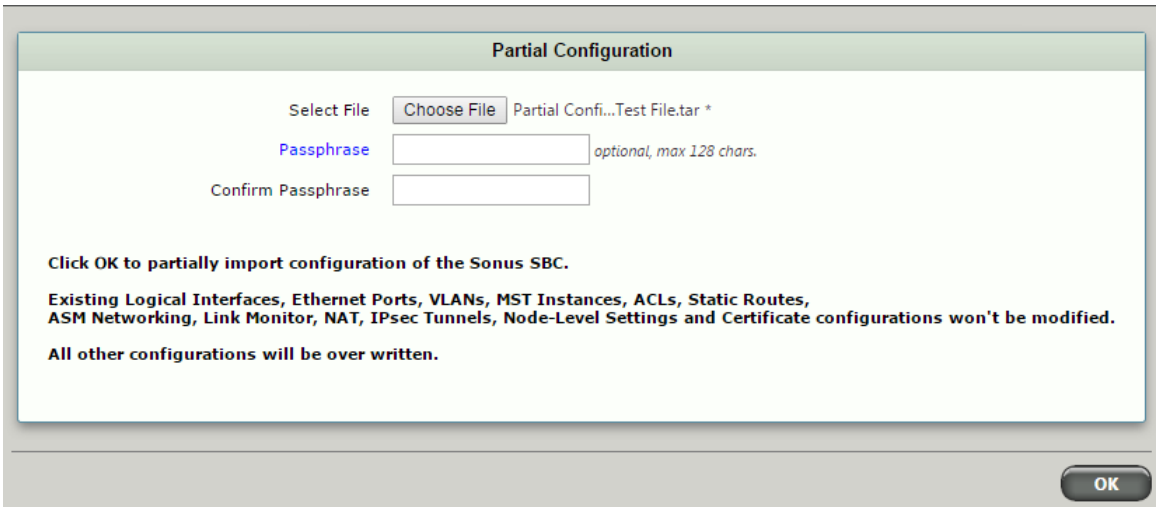
- System information
- Telco interface configurations
- Local/Pass-Through authorization tables
- SIP registration tables
- SIP user credentials
- Server/CA certificates
- SBA configuration information
- VLAN configurations
- ACL tables
- ACL rules
- Port membership information
- MSTP instances
- IPSec configuration
- NAT configuration
- Link monitor configuration

Importing A Partial Configuration

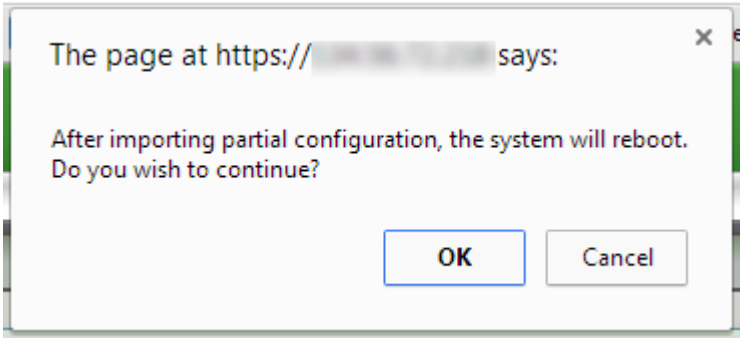
To import a partial configuration:

1. In the WebUI, click the **Tasks** tab.
2. In the left nave pane, go to **System > Import Partial Configuration**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Click **Choose File**.
4. Browse for the configuration file and click **Open**.
5. Click **OK**.



6. In the confirmation alert dialog, click **OK**.

Importing and Exporting Transformation Tables

Transformation tables may be exported from one SBC 1000/2000 node and imported into another in order to save time when deploying additional nodes at one or more sites without the aid of an EMS auto-provisioning system. Transformation tables are exported as XML files.

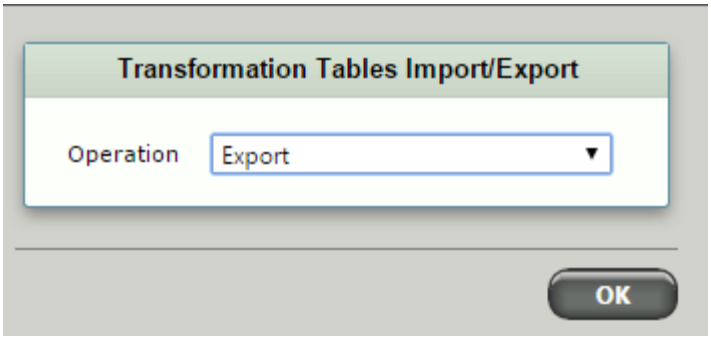
Imported transformation tables are appended to pre-existing tables on the target node, no transformation tables on the target node are deleted or modified by the import operation.

Exporting Transformation Tables

To export transformation tables:

1. In the WebUI, click the Tasks tab.
2. In the left navigation pane, go to: **Import/Export Configuration Items > Transformation Tables**.

Copyright © 2015 Sonus Networks. All rights reserved.

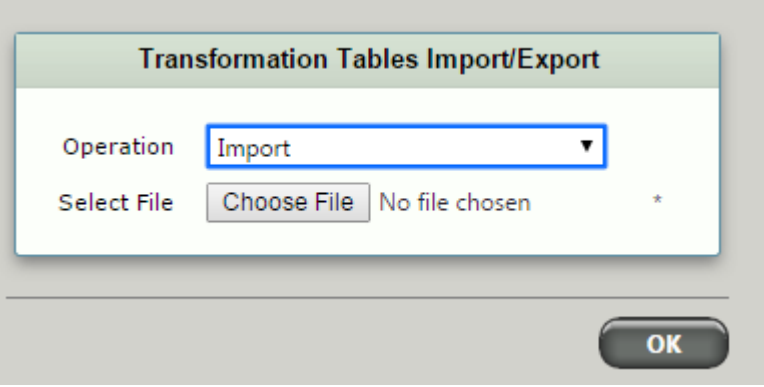


3. Select **Export** from the select box in the Transformation Tables Import/Export dialog.
4. Click **OK**.
   You will be prompted to save the file, if you do not choose a custom name, the file will be saved as *TransTableConfig.xml* .

Importing Transformation Tables

To import transformation tables:

1. In the WebUI, click the Tasks tab.
2. In the left navigation pane, go to: **Import/Export Configuration Items > Transformation Tables**.



3. Select **Import** from the select box in the Transformation Tables Import/Export dialog
4. Click Select **Export** from the select box in the Transformation Tables Import/Export dialog.
5. Browse and select the transformation table XML file to be imported.
6. Click **OK**.

Working with Microsoft Unified Communications

This section shows you how to setup Microsoft Unified Communications on Office Communication Server 2007 (OCS 2007) and Lync 2010 using the wizards in the Task tab.

OCS 2007 Setup

- Deploying the Sonus SBC 1000-2000 and OCS 2007 with a PSTN Provider
- Deploying the Sonus SBC 1000-2000 and OCS 2007 with a SIP Trunk Provider

Lync Setup

- Deploying Sonus SBC 1000-2000 and Lync with a SIP Trunk Provider
- Deploying the SBC 1000-2000 and Lync with a PSTN Provider
- Using Lync Setup for E911 Configuration

Copyright © 2015 Sonus Networks. All rights reserved.

Related Topics

- Deploying the Survivable Branch Appliance
- Deploying an F5 Load Balancer in a PBX-SBC-Lync Topology
- Using Tenor as an Analog Device in a Lync SBC SBA Deployment
- Configuring the Sonus SBC 1000-2000 for DNS Load Balancing
- Deployment in PSTN - SBC - Microsoft OCS 2007 R2 Topology
- LYNC side Gateway Failover Configuration
- Deploying the Sonus SBC 1000-2000 with OCS2007 R2 using the ASM as a Mediation Server

OCS 2007 Setup

The Sonus SBC 1000/2000 Web Interface includes a built-in step-by-step setup configuration wizard allowing end-users to quickly deploy Sonus SBC 1000/2000 and OCS 2007.

This functionality is accessible in the WebUI via the **Tasks** tab under **Microsoft© UC Setup** > **OCS 2007 Setup**.

The wizard produces two different configurations depending on the desired deployment:

- Deploying the Sonus SBC 1000-2000 and OCS 2007 with a PSTN Provider
- Deploying the Sonus SBC 1000-2000 and OCS 2007 with a SIP Trunk Provider

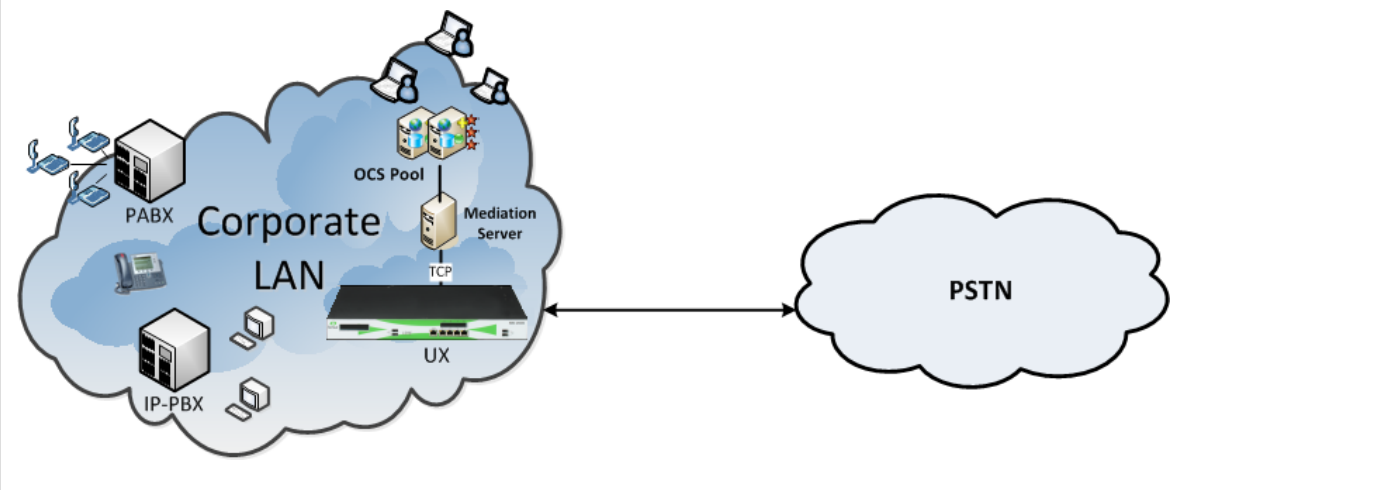
Deploying the Sonus SBC 1000-2000 and OCS 2007 with a PSTN Provider

The Sonus SBC 1000/2000 Web Interface includes a built-in step-by-step setup configuration wizard allowing end-users to quickly deploy Sonus SBC 1000/2000 and OCS 2007.

This functionality is accessible in the WebUI via the **Tasks** tab under **Microsoft© UC Setup** > **OCS 2007 Setup**.

Topology Overview

Sonus SBC 1000/2000 can be configured to connect an Enterprise's OCS environment to the PSTN via PRI using an automatic setup wizard as described in the section below.



Helpful Tip

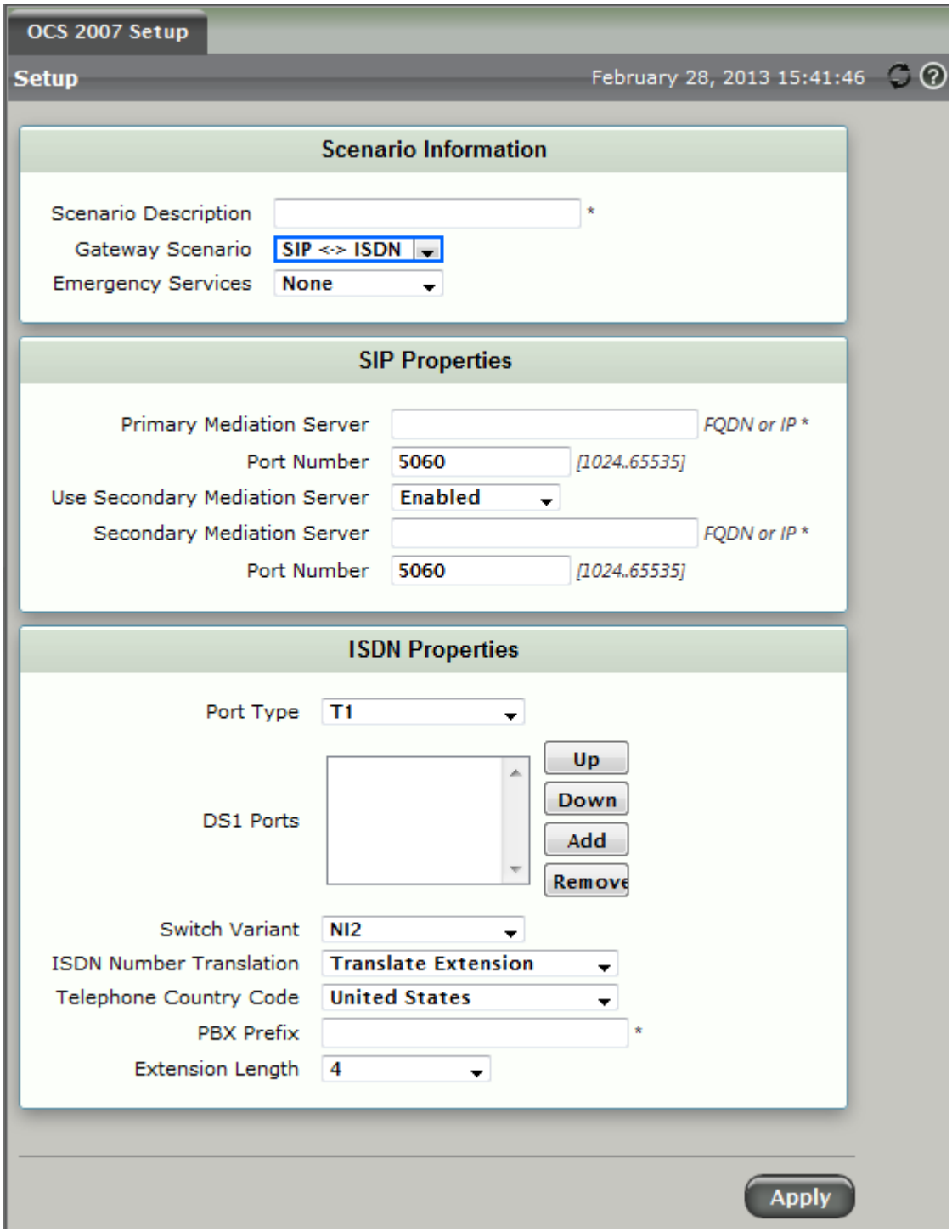
Usage of the deployment wizard to configure the Sonus SBC 1000/2000 does not modify existing configuration. The wizard will simply add the new configuration elements to the Sonus SBC 1000/2000.

OCS 2007 Setup Field Configuration

Copyright © 2015 Sonus Networks. All rights reserved.

Enter the scenario configuration details based on your deployment settings:

> When you click the **Apply** on this final step, it may take up to 15 seconds before you receive a final confirmation status screen. During this time, no progress indicator will be shown, and it is recommended that you wait until the operation completes. This issue was resolved in Sonus SBC 1000/2000 software, SYM-8453.



Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

- Scenario Description
- Gateway Scenario
- Primary Mediation Server
- Port Number
- Use Secondary Mediation Server
- DS1 Ports
- Port Type
- Switch Variant
- ISDN Number Translation
- Telephone Country Code
- PBX Prefix
- Extension Length

Scenario Information - Field Definitions

Scenario Description

Name describing the OCS setup.
This value entered will be prefixed on all the Sonus SBC 1000/2000 configuration elements created by the Setup Wizard pertaining to this deployment.

Gateway Scenario

Select **`SIP <-> PSTN`** for this deployment

SIP Properties - Field Definitions

Primary Mediation Server

The Pool name of the OCS Mediation Server

Port Number

The SIP Server Port number (via TCP) to use for sending and receiving SIP messages between Sonus SBC 1000/2000 and the Primary Mediation Server

Use Secondary Mediation Server

Select **enable** if you wish to have a secondary Mediation Server configured

ISDN Properties - Field Definitions

DS1 Ports

The physical T1/E1 port number to which the PSTN line is physically connected.

Port Type

The desired port type from the list - this will re-configure the DS1 ports selected above.

Switch Variant

Copyright © 2015 Sonus Networks. All rights reserved.

The ISDN flavor to be configured for the port type in the ISDN Signaling Group.

ISDN Number Translation

Select whether or not Sonus SBC 1000/2000 should translate dialed PSTN digits as phone extensions.

Telephone Country Code

Available when **Translation type** is configured as **Translate Extension**. The country code you wish to be used in the translated phone extension.

PBX Prefix

Available when **Translation type** is configured as **Translate Extension**. The numbers to prefix to the translated phone extension.

Extension Length

The number of digits used to account for the PSTN extension.

Deploying the Sonus SBC 1000-2000 and OCS 2007 with a SIP Trunk Provider

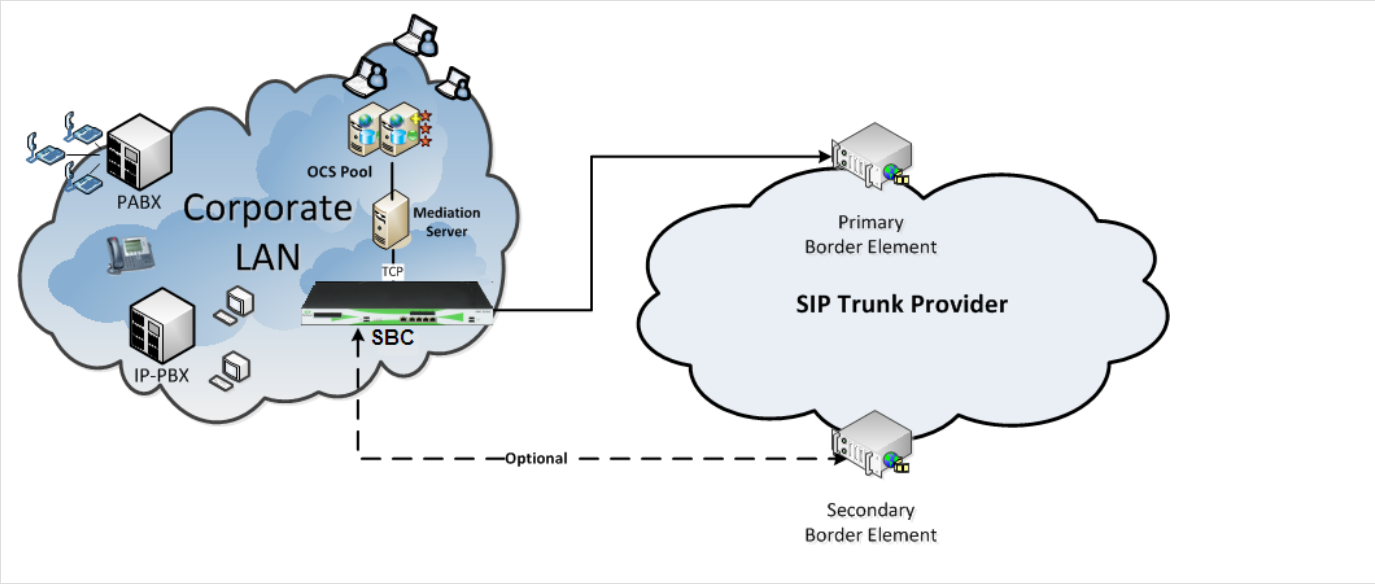
The Sonus SBC 1000/2000 Web Interface includes a built-in step-by-step setup configuration wizard allowing end-users to quickly deploy Sonus SBC 1000/2000 and OCS 2007.

This functionality is accessible in the WebUI via the **Tasks** tab under **Microsoft© UC Setup** > **OCS 2007 Setup**.

Copyright © 2015 Sonus Networks. All rights reserved.

Topology Overview

SIP Trunk is a popular alternative to PSTN connectivity via PRI. Sonus SBC 1000/2000 can be configured to connect an Enterprise's OCS environment to a SIP trunk using an automatic setup wizard as described in the section below.



Helpful Tip

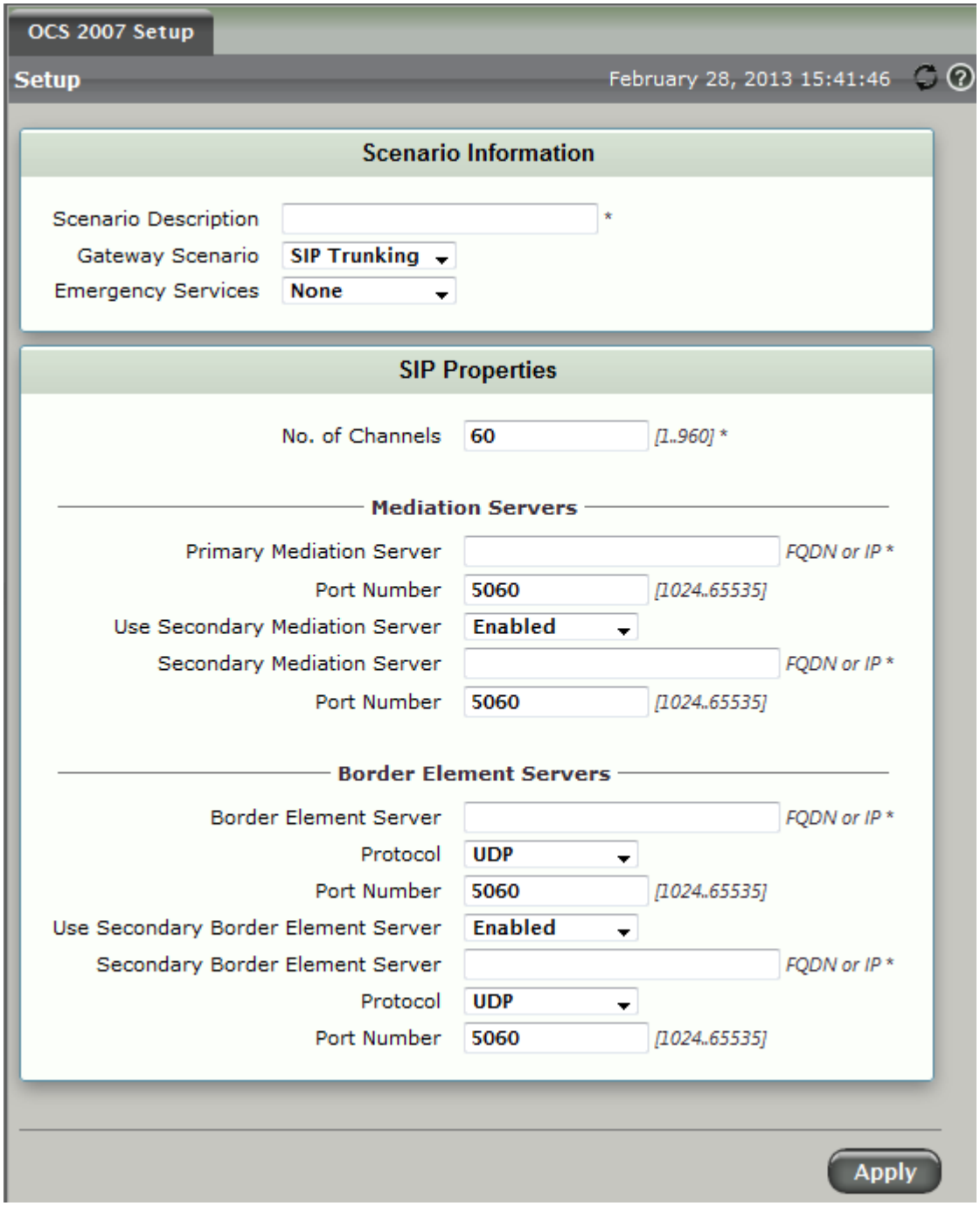
Usage of the deployment wizard to configure the Sonus SBC 1000/2000 does not modify existing configuration. The wizard will simply add the new configuration elements to the Sonus SBC 1000/2000.

OCS 2007 Setup Field Configuration

Enter the scenario configuration details based on your deployment settings:

When you click the **Apply** on this final step, it may take up to 15 seconds before you receive a final confirmation status screen. During this time, no progress indicator will be shown, and it is recommended that you wait until the operation completes. This issue was resolved in Sonus SBC 1000/2000 software, SYM-8453.

Copyright © 2015 Sonus Networks. All rights reserved.



Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

- Scenario Description
- Gateway Scenario
- No. of Channels
- Primary Mediation Server
- Port Number
- Use Secondary Mediation Server
- Border Element Server
- Protocol
- Port Number
- Use Secondary Border Element Server

Scenario Information - Field Definitions

Scenario Description

Name describing the OCS setup.
ℹ️ This value entered will be prefixed on all the Sonus SBC 1000/2000 configuration elements created by the Setup Wizard pertaining to this deployment.

Gateway Scenario

Select **`SIP Trunking`** for this deployment

SIP Properties - Field Definitions

No. of Channels

The number of SIP channels you would like the wizard to allocated in the SIP Signalling Group.
⚠️ Make sure you have enough SIP licenses to account for the entered value.

Primary Mediation Server

The Pool name of the OCS Mediation Server

Port Number

The SIP Server Port number (via TCP) to use for sending and receiving SIP messages between Sonus SBC 1000/2000 and the Primary Mediation Server

Use Secondary Mediation Server

Select **enable** if you wish to have a secondary Mediation Server configured

Border Element Server

The FQDN or IP address of the Session Border Controller service provider

Protocol

The IP protocol to use for sending and receiving SIP messages between Sonus SBC 1000/2000 and the Server Pool Host

Copyright © 2015 Sonus Networks. All rights reserved.

Port Number

The SIP Server Port number to use for sending and receiving SIP messages between Sonus SBC 1000/2000 and the Server Pool Host

Use Secondary Border Element Server

Select **enable** if you wish to have a secondary Session Border Controller service provider configured

Lync Setup

The Sonus SBC 1000/2000 Web Interface includes a built-in step-by-step setup configuration wizard allowing end-users to quickly deploy Sonus SBC 1000/2000 and Lync Server 2010 and 2013.

This functionality is accessible in the WebUI via the **Tasks** tab under **Microsoft© UC Setup** > **Lync™ Setup**.

The wizard produces two different configurations depending on the desired deployment. MS Lync Server Deployment reguires MTLS to be used as the SIP Transport on the Enhanced Media Gateway. In order to comply with Microsoft Lync 2010 Enhance Media Gateway Certification requirements, both the Trusted Root CA and the CA signed Sonus SBC 1000/2000 node certificate must be imported into the Sonus SBC 1000/2000 system. Before you proceed with the final #Lync 2010 Setup step, please follow these prerequisite steps:

Step 1 - Trusted CA's

In this step, you will need to obtain a trusted root certificate from your CA, and import it on the Sonus SBC 1000/2000.

Copyright © 2015 Sonus Networks. All rights reserved.

If you are using a **Standalone Windows Certificate Authority**, you may follow the instructions outlined in Downloading a CA Certificate using a Standalone Windows CA.

Once downloaded, import the trusted CA on the Sonus SBC 1000/2000, and proceed to the next step.

Step 2 - Generate CSR

In this step, you'll need to generates a certificate signing request from Sonus SBC 1000/2000 to send it to the Trusted CA for signing.

The **Common Name** field should be of the form `Host.Domain` specified as specified while Running Initial Setup .

Important Note: the **Subject Alternative Name DNS** field should not be entered unless required by your Lync 2010 setup.

If you are using a **Standalone Windows Certificate Authority**, you may send your certificate signing request to the CA by following the instructions outlined in Requesting a Signed Certificate using a Standalone Windows CA. Once you have obtained your signed certificate, you may proceed with the final prerequisite step.

Step 3 - Sonus SBC 1000/2000 Certificate

In this step, you will install the signed certificate on Sonus SBC 1000/2000. To do this, you may follow the instructions outlined in Importing a Sonus SBC 1000-2000 Server Certificate.

Step 4 - Lync Setup

This step is the final configuration deployment by the setup wizard, and it supports the following deployments:

- Deploying Sonus SBC 1000-2000 and Lync with a SIP Trunk Provider
- Deploying the SBC 1000-2000 and Lync with a PSTN Provider
- Using Lync Setup for E911 Configuration

Helpful Tip

Usage of the deployment wizard to configure the Sonus SBC 1000/2000 does not modify existing configuration. The wizard will simply add the new configuration elements to the Sonus SBC 1000/2000.

Deploying Sonus SBC 1000-2000 and Lync with a SIP Trunk Provider

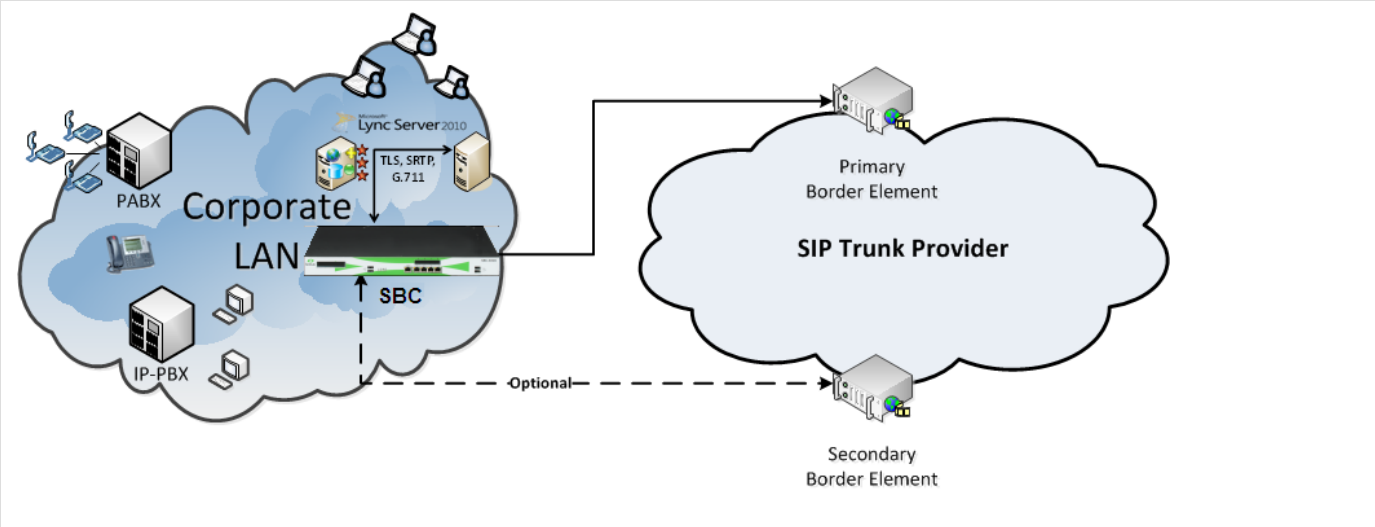
Before you begin

This page describes the final deployment step produced by the Lync wizard for a Sonus SBC 1000/2000 in a Lync environment with a SIP Trunk Provider. Before you proceed, ensure you have completed the prerequisites.

Topology Overview

Using a SIP Trunk is a popular alternative to PSTN connectivity via PRI. The Sonus SBC 1000/2000 can be configured to connect an Enterprise's Lync environment to a SIP trunk using the automatic setup wizard as described in the section below. Although the configuration example includes specific configuration, all WebUI field definitions are noted.

Copyright © 2015 Sonus Networks. All rights reserved.



Helpful Tip

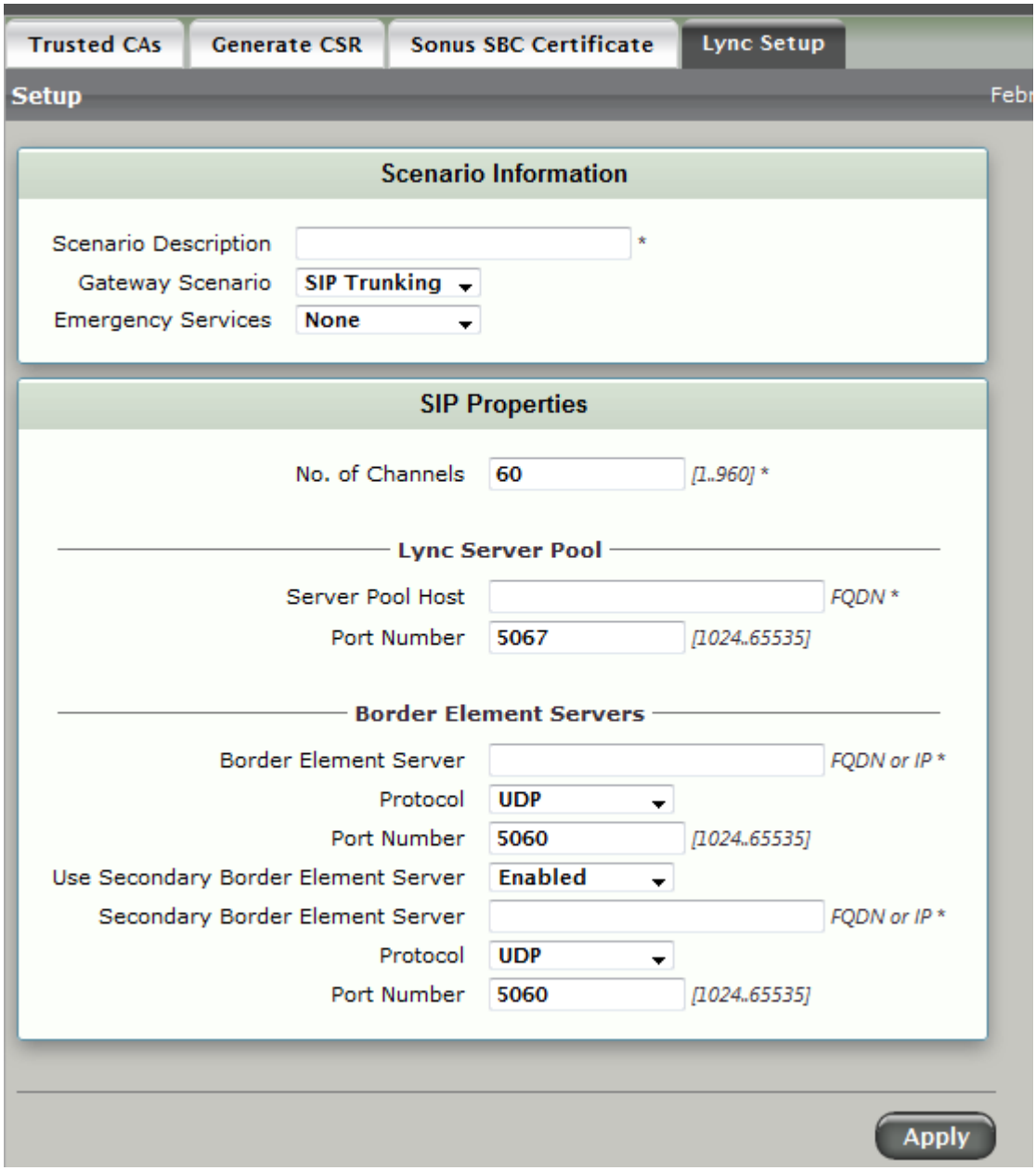
Usage of the deployment wizard to configure the Sonus SBC 1000/2000 does not modify existing configuration. The wizard will simply add the new configuration elements to the Sonus SBC 1000/2000.

Lync Setup Field Configuration

Enter the scenario configuration details based on your deployment settings:

When you click the **Apply** on this final step, it may take up to 15 seconds before you receive a final confirmation status screen. During this time, no progress indicator will be shown, and it is recommended that you wait until the operation completes. This issue was resolved in Sonus SBC 1000/2000 software, SYM-8453.

Copyright © 2015 Sonus Networks. All rights reserved.



Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

- Scenario Description
- Gateway Scenario
- Emergency Services
- Emergency Callback Number 1
- Emergency Callback Number 2
- PSAP Number
- No. of Channels
- Server Pool Host
- Port Number
- Border Element Server
- Protocol
- Port Number
- Use Secondary Border Element Server
- Secondary Border Element Server
- Protocol
- Port Number

Scenario Information - Field Definitions

Scenario Description

Name describing the Lync setup.

> This value entered will be prefixed on all the Sonus SBC 1000/2000 configuration elements created by the Setup Wizard pertaining to this deployment.

Gateway Scenario

Select SIP Trunking for this deployment. For **SIP <-> PSTN**, see Deploying the SBC 1000-2000 and Lync with a PSTN Provider.

Emergency Services

> For the purpose of this illustration above, Emergency Services is not selected. Field definitions are defined below.

> The E911 Elin number from the "CompanyName" field configured in Lync location services is used as the authoritative Call Back number for outgoing E911 calls, and is always the preferred configuration. Specifically, it will take precedence over any Callback Number number configuration in Lync Setup. For more information, see Creating and Modifying Entries to Transformation Tables.

Options include: **Lync E911**, **911** or **None**.

Emergency Callback Number 1

Call Back Number in string format. This field is displayed only when **Lync E911** or **911** is selected from Emergency Services.

Emergency Callback Number 2

Copyright © 2015 Sonus Networks. All rights reserved.

Second Call Back Number in string format. This field is displayed only when **Lync E911** or **911** is selected from Emergency Services.

PSAP Number

Defines the Public Safety Answering Point Number. Valid entry 1 - 127 characters.

SIP Properties - Field Definitions

No. of Channels

The number of SIP channels you would like the wizard to allocate in the SIP Signaling Group.

> ⚠ Ensure you have enough SIP licenses to account for the entered value.

Server Pool Host

The Pool name of the Lync Server (FQDN).

Port Number

The Port Number (via TLS) is used for sending and receiving SIP messages between Sonus SBC 1000/2000 and the Server Pool Host.

Border Element Server

The FQDN or IP address of the Session Border Controller service provider.

Protocol

The IP protocol to use for sending and receiving SIP messages between Sonus SBC 1000/2000 and the Server Pool Host.

Port Number

The SIP Server Port number to use for sending and receiving SIP messages between Sonus SBC 1000/2000 and the Server Pool Host.

Use Secondary Border Element Server

Enables or disables the secondary Session Border Controller service provider configured.

Secondary Border Element Server

Specifies the Secondary Border Element Service provider. Valid entry: IP Address or FQDN.

Protocol

The Protocol used for communicating with the Border Element Server. Valid entries: UDP or TCP.

Port Number

Copyright © 2015 Sonus Networks. All rights reserved.

The Port Number (used for sending and receiving messages between Sonus SBC 1000/2000 and the Border Element server.

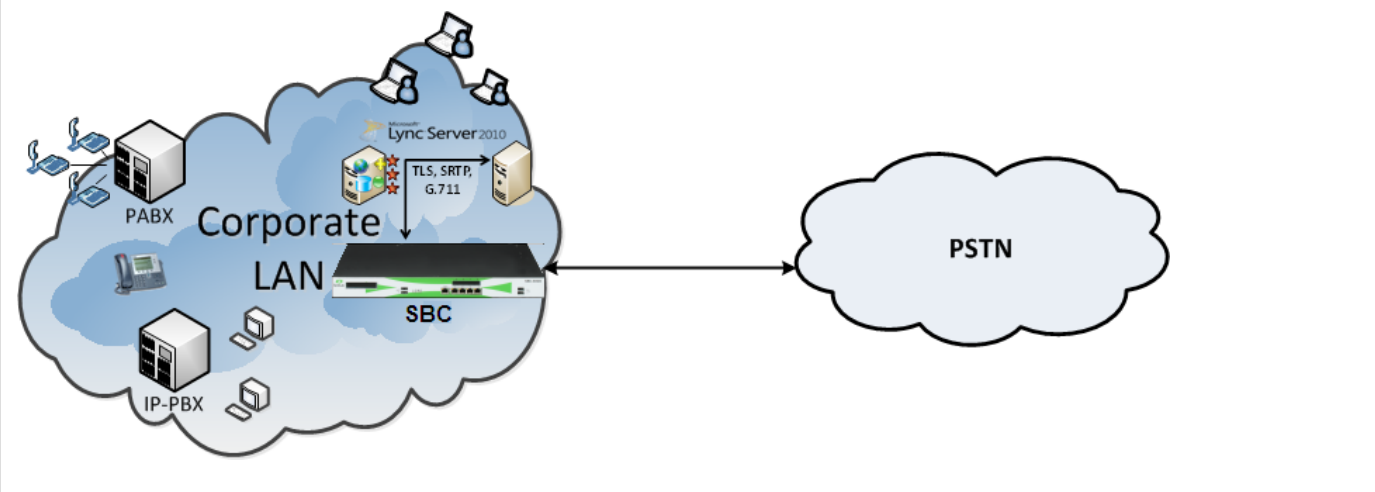
Deploying the SBC 1000-2000 and Lync with a PSTN Provider

Before you begin

This page describes the final deployment step produced by the Lync wizard for a Sonus SBC 1000/2000 in a Lync environment with a PSTN Provider. Before you proceed, ensure you have completed the prerequisites.

Topology Overview

Sonus SBC 1000/2000 can be configured to connect an Enterprise's Lync environment to the PSTN via PRI using an automatic setup wizard as described in the section below.



Helpful Tip

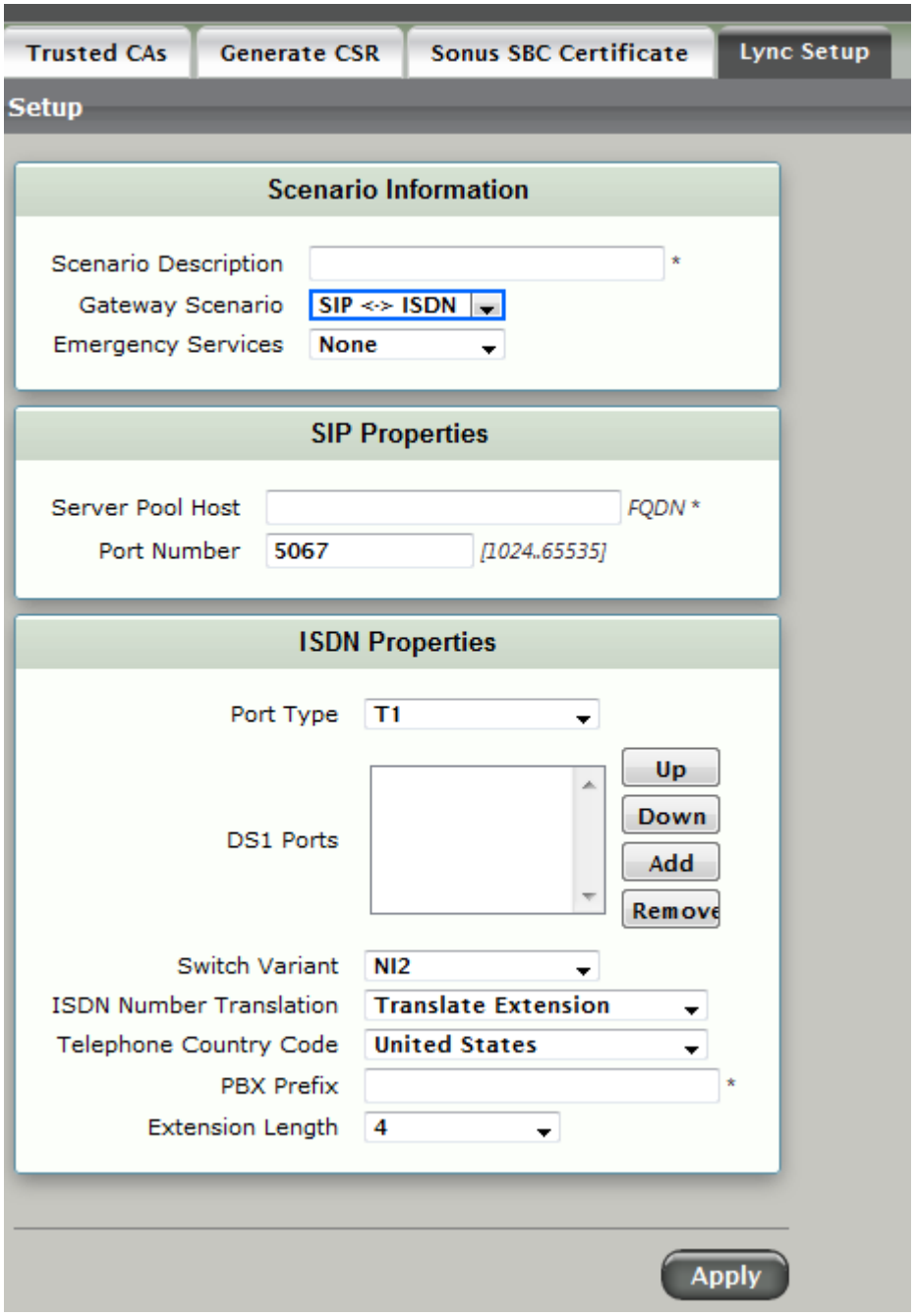
Usage of the deployment wizard to configure the Sonus SBC 1000/2000 does not modify existing configuration. The wizard will simply add the new configuration elements to the Sonus SBC 1000/2000.

Lync Setup Field Configuration

Enter the scenario configuration details based on your deployment settings:

When you click the **Apply** on this final step, it may take up to 15 seconds before you receive a final confirmation status screen. During this time, no progress indicator will be shown, and it is recommended that you wait until the operation completes. This issue was resolved in Sonus SBC 1000/2000 software, SYM-8453.

Copyright © 2015 Sonus Networks. All rights reserved.



Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

- Scenario Description
- Gateway Scenario
- Emergency Services
- Emergency Callback Number 1
- Emergency Callback Number 2
- PSAP Number
- Server Pool Host
- Port Number
- DS1 Ports
- Port Type
- Switch Variant
- ISDN Number Translation
- Telephone Country Code
- PBX Prefix
- Extension Length

Scenario Information - Field Definitions

Scenario Description

Name describing the Lync setup.

> This value entered will be prefixed on all the Sonus SBC 1000/2000 configuration elements created by the Setup Wizard pertaining to this deployment.

Gateway Scenario

Select **SIP <-> PSTN** deployment. For **SIP Trunking** see Deploying the SBC 1000-2000 and Lync with a PSTN Provider. Select **SIP <-> PSTN** for this deployment.

Emergency Services

> For the purpose of this illustration above, Emergency Services is not selected. Field definitions are defined below.

> The E911 Elin number from the "CompanyName" field configured in Lync location services is used as the authoritative Call Back number for outgoing E911 calls, and is always the preferred configuration. Specifically, it will take precedence over any Callback Number number configuration in Lync Setup. For more information, see Creating and Modifying Entries to Transformation Tables.

Options include: **Lync E911**, **911** or **None**.

Emergency Callback Number 1

Call Back Number in string format. This field is displayed only when **Lync E911** or **911** is selected from Emergency Services.

Emergency Callback Number 2

Second Call Back Number in string format. This field is displayed only when **Lync E911** or **911** is selected from Emergency Services.

Copyright © 2015 Sonus Networks. All rights reserved.

PSAP Number

Defines the Public Safety Answering Point Number. Valid entry 1 - 127 characters.

SIP Properties - Field Definitions

Server Pool Host

The Pool name of the Lync Server (FQDN).

Port Number

The SIP Server Port number (via TLS) is used for sending and receiving SIP messages between Sonus SBC 1000/2000 and the Server Pool Host.

ISDN Properties - Field Definitions

DS1 Ports

The physical T1/E1 port number to which the PSTN line is physically connected.

Port Type

The desired port type from the list - this will re-configure the DS1 ports selected above.

Switch Variant

The ISDN flavor to be configured for the port type in the ISDN Signaling Group.

ISDN Number Translation

Select whether or not Sonus SBC 1000/2000 should translate dialed PSTN digits as phone extensions.

Telephone Country Code

Available when **Translation type** is configured as **Translate Extension**. The country code you wish to be used in the translated phone extension.

PBX Prefix

Available when **Translation type** is configured as **Translate Extension**. The numbers to prefix to the translated phone extension.

Extension Length

The number of digits used to account for the PSTN extension.

Using Lync Setup for E911 Configuration

As part of the Sonus SBC 1000/2000 Web Interface's built-in step-by-step setup configuration wizard, the **Lync Setup** option (available from the **Tasks** tab, under **Microsoft© UC Setup** > **Lync™ Setup**) enables you to

Copyright © 2015 Sonus Networks. All rights reserved.

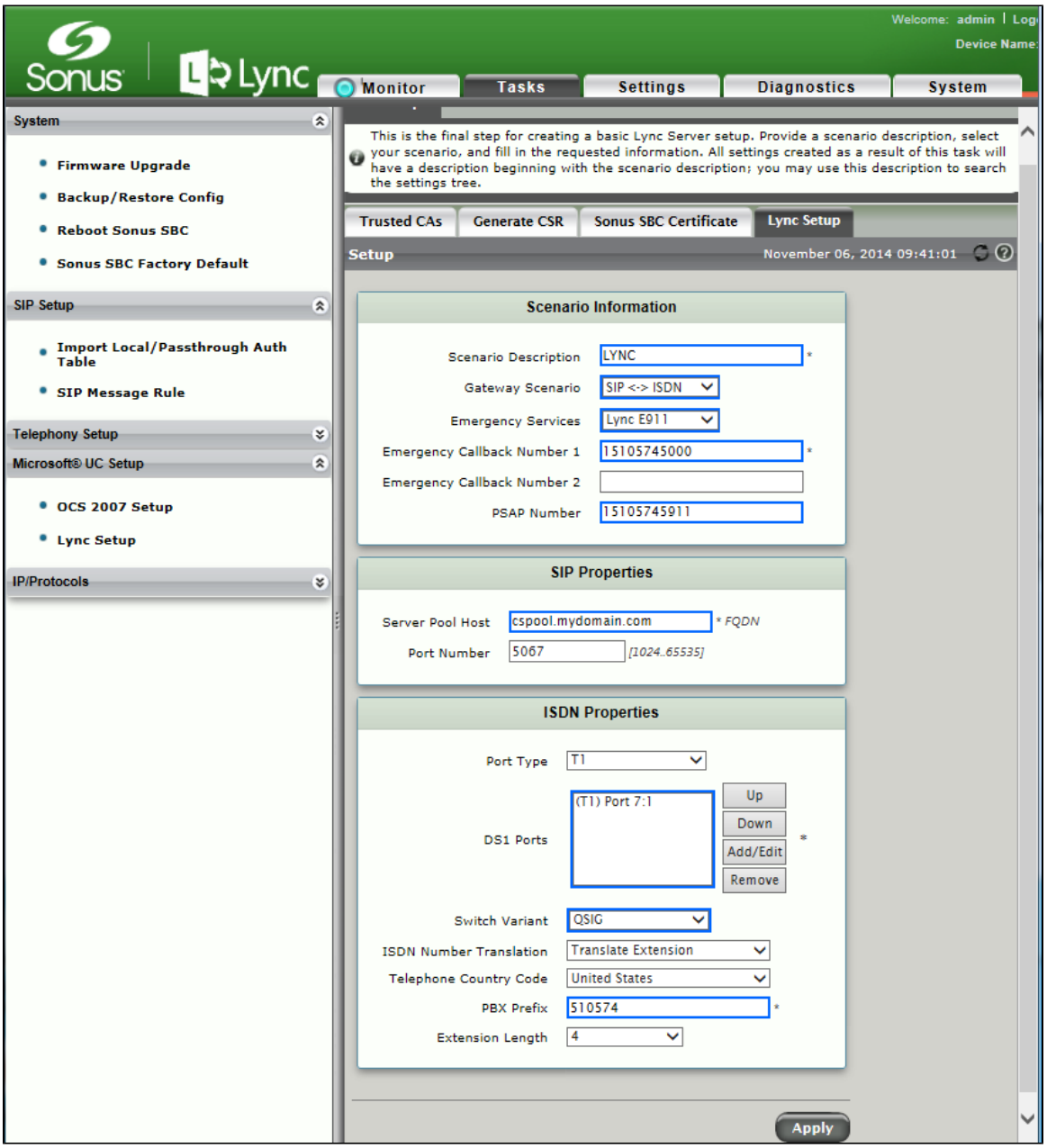
configure Emergency Services. When **Lync E911** or **911** is selected as the Emergency Services option, the system automatically creates the emergency services information in the following WebUI locations:

- Transformation Table
- Call Routing Table
- SIP Profile
- Callback Number Pool
- Emergency Services Configuration

Below details a sample configuration for E911 (Emergency Services), along with the resulting WebUI configuration options that are created.

Sample E911 (Emergency Services) Configuration

The following is an example of E911 configuration for a **SIP <-> ISDN** scenario using Lync E911.



Copyright © 2015 Sonus Networks. All rights reserved.

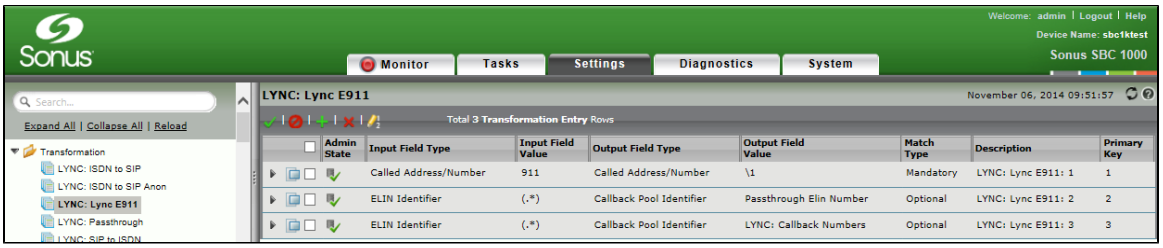
Configuration options created as a result of E911 Changes

> The E911 Elin number from the "CompanyName" field configured in Lync location services is used as the authoritative Call Back number for outgoing E911 calls, and is always the preferred configuration. Specifically, it will take precedence over any Callback Number number configuration in Lync Setup. For more information, see Creating and Modifying Entries to Transformation Tables.

Transformation Table

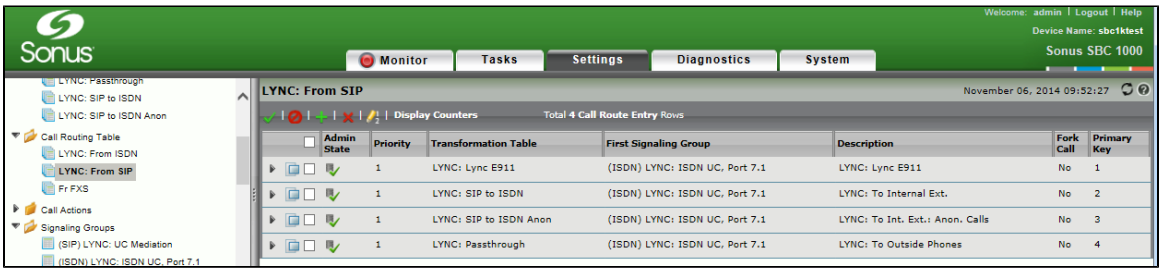
A Transformation entry is created for Lync E911, which includes table entries for Called Address/Number, ELIN Identifier, and Callback Pool Identifier (the emergency call back number table or Pasthrough ELIN number used for calls destined to 911). For specific information about the Passthrough ELIN Number, see Creating and Modifying Entries to Transformation Tables.

For easy identification, the **Description** field matches the Scenario description you configured in Lync Setup. For more information about Tranformation Tables, see Managing Transformation Tables.



Call Routing Table

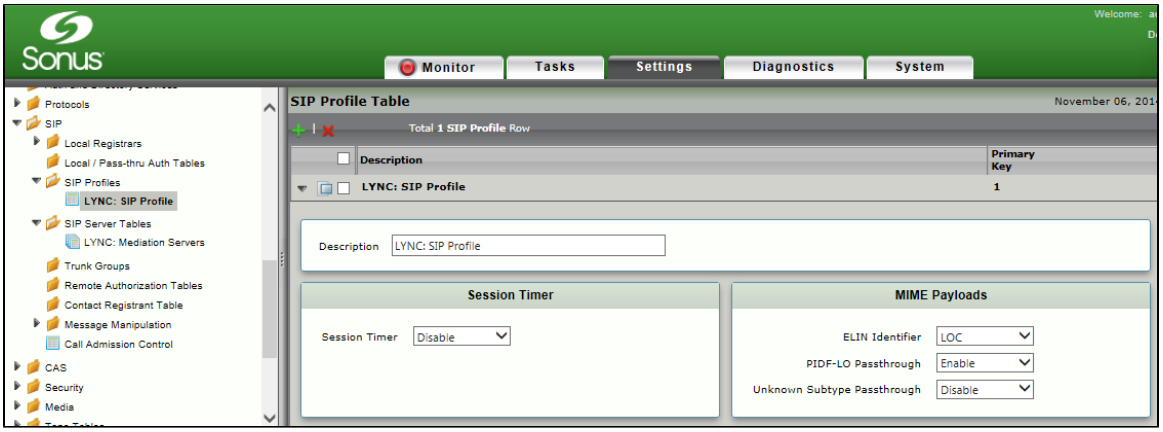
A Lync E911 entry is created in the Call Routing Table for routing calls from SIP to ISDN. For more information about Call Routing Tables, see Managing Call Routing Tables.



SIP Profile

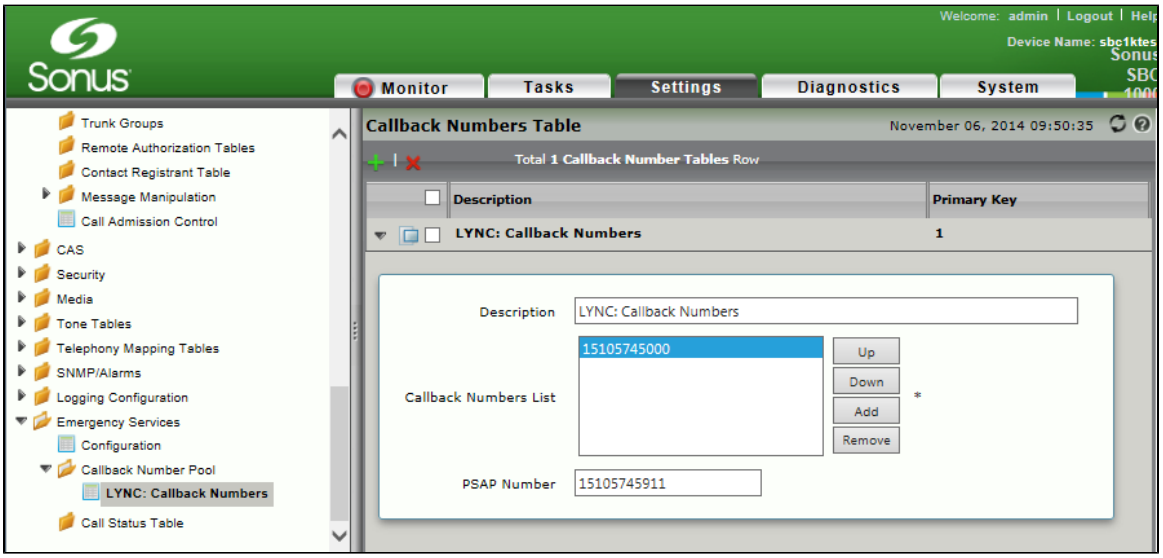
A Lync SIP Profile is created in the SIP Profile table. SIP Profiles control the how the Sonus SBC 1000/2000 communicates with SIP devices. For more information about SIP Profiles, see Managing SIP Profiles.

Copyright © 2015 Sonus Networks. All rights reserved.



Callback Number Pool

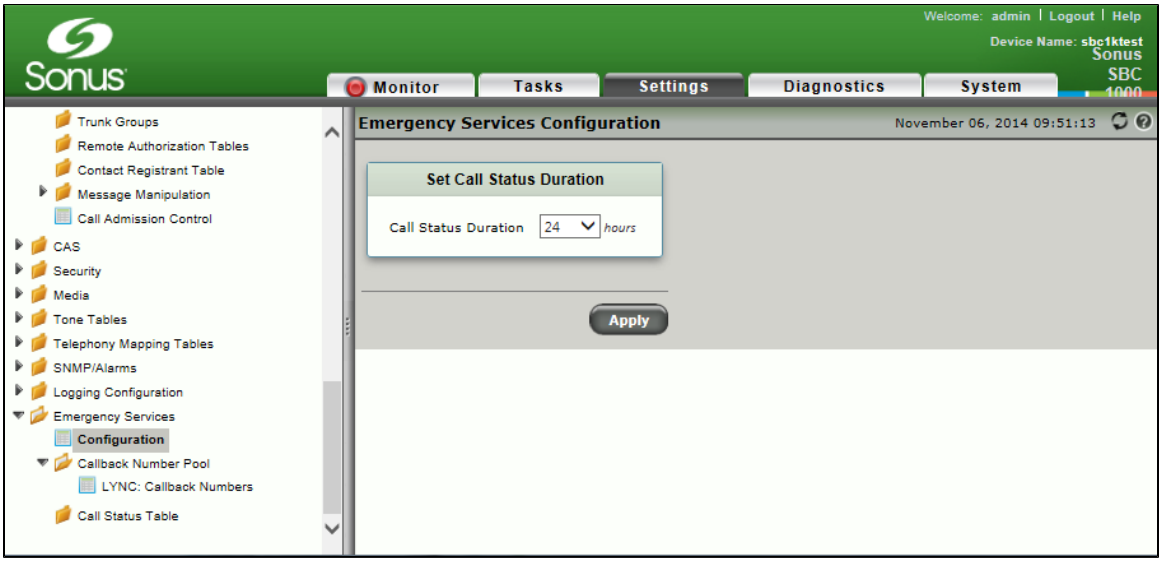
An entry is added to the Callback Numbers Table with the Emergency Callback number configured in the Lync Setup. For more information about Callback Numbers, see Creating and Modifying Callback Number Lists.



Emergency Services Configuration

The Call Status Duration for Emergency Services is configured. For more information about Emergency Services Configuration, see Configuring Emergency Services.

Copyright © 2015 Sonus Networks. All rights reserved.



Working with the ASM and SBA

The **Application Solution Module** (ASM) module is a separate, fully-functional server installed inside the Sonus SBC 1000/2000 chassis. The ASM can host a variety of applications that support the Sonus SBC 1000/2000 system.

If purchased with the Sonus SBC 1000/2000, the ASM module is factory installed and typically comes pre-loaded with the Lync Survivable Branch Appliance (SBA).

Managing the ASM

- Starting the SBA Services
- Generate and Import an SBA Certificate
- Deploying the SBA
- Joining the ASM to a Domain
- Powering the ASM ON and OFF
- Updating the ASM Recovery Partition
- Viewing the Installed Packages on the ASM
- Installing an ASM Package
- Configuring the ASM IP Settings
- Enabling and Disabling Remote Desktop on the ASM
- Changing the ASM Admin Password
- Rebooting and Resetting the ASM
- Re-initializing the ASM
- Viewing and Exporting Windows Event Logs on the ASM
- Managing the Windows Firewall on the ASM
    - Configuring the ASM Firewall
    - Resetting and Listing Windows Firewall Rules on the ASM

Applying an SBA Security Template

Managing the Lync SBA

- Viewing the SBA Operational Status
- Installing Cumulative Updates for Lync SBA
- Starting and Stopping SBA Services
- Importing an SBA Certificate
- Exporting an SBA Certificate
- Testing a Lync Call

Copyright © 2015 Sonus Networks. All rights reserved.

Managing the SBC Communication Service

- Viewing the SBC Communication Service Version
- Upgrading the SBC Communication Service Version

Managing the ASM

The **Application Solution Module** (ASM) module is a separate, fully-functional server installed inside the Sonus SBC 1000/2000 chassis. Features of this ASM are managed from the Sonus SBC 1000/2000 Web Interface via the Sonus SBC 1000/2000 Communication Service.

An operating ASM has two software partitions:

- The **Live partition**, from which the system actively runs. Unlike the Sonus SBC 1000/2000 application partitions, this partition is always active on a running ASM.
- The **Recovery partition**, which contains a spare software image. Users have the ability to re-initialize the ASM from this partition; an operation which replaces the live partition with the recovery image. This partition can also be updated directly as needed; refer to Updating the ASM Recovery Partition.

Software application support on the Application Solution Module (ASM) is limited as follows:

- Microsoft Lync Survivable Branch Appliance (SBA)
- Microsoft Lync Resilient Branch Appliance (RBA) communicating with the Lync Front End
- Quality of Experience (QoE) Agent Server Gateway

Software must be provided by Sonus and configured via the Sonus provided provisioning and management interface.

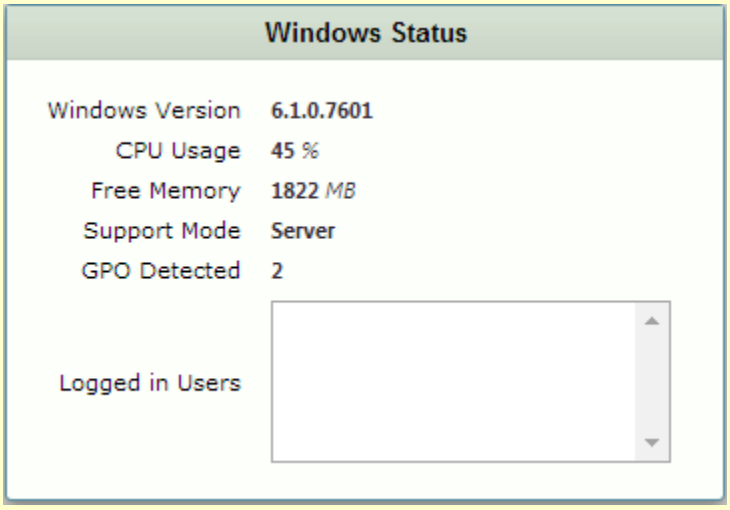
ASM Support Mode

The ASM operates in either of two models, appliance or server. In the appliance mode, the SBA utilizes Sonus' solution to guarantee security. In the Server mode, the SBA relies on customer installed software to provide security/firewall protection.

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus service support is not provided in the case where any non-Sonus supplied software is installed on the module.

A Support Mode of Server in the Windows Status panel indicates that a non-Sonus entity has installed unsupported software in the ASM. In such a case, Sonus supports only the ASM hardware and not customer supported software.



Support Mode Definitions

Appliance Certified Mode: The ASM image contains v3.2 SbcComms or later and no third-party software has been installed.

Appliance Controlled Mode: The original ASM image was a version previous to 3.2 and has been upgraded.

Server: A third-party software installation has been detected by the ASM.

Related Topics

- Starting the SBA Services
- Generate and Import an SBA Certificate
- Deploying the SBA
- Joining the ASM to a Domain
- Powering the ASM ON and OFF
- Updating the ASM Recovery Partition
- Viewing the Installed Packages on the ASM
- Installing an ASM Package
- Configuring the ASM IP Settings
- Enabling and Disabling Remote Desktop on the ASM
- Changing the ASM Admin Password
- Rebooting and Resetting the ASM

Copyright © 2015 Sonus Networks. All rights reserved.

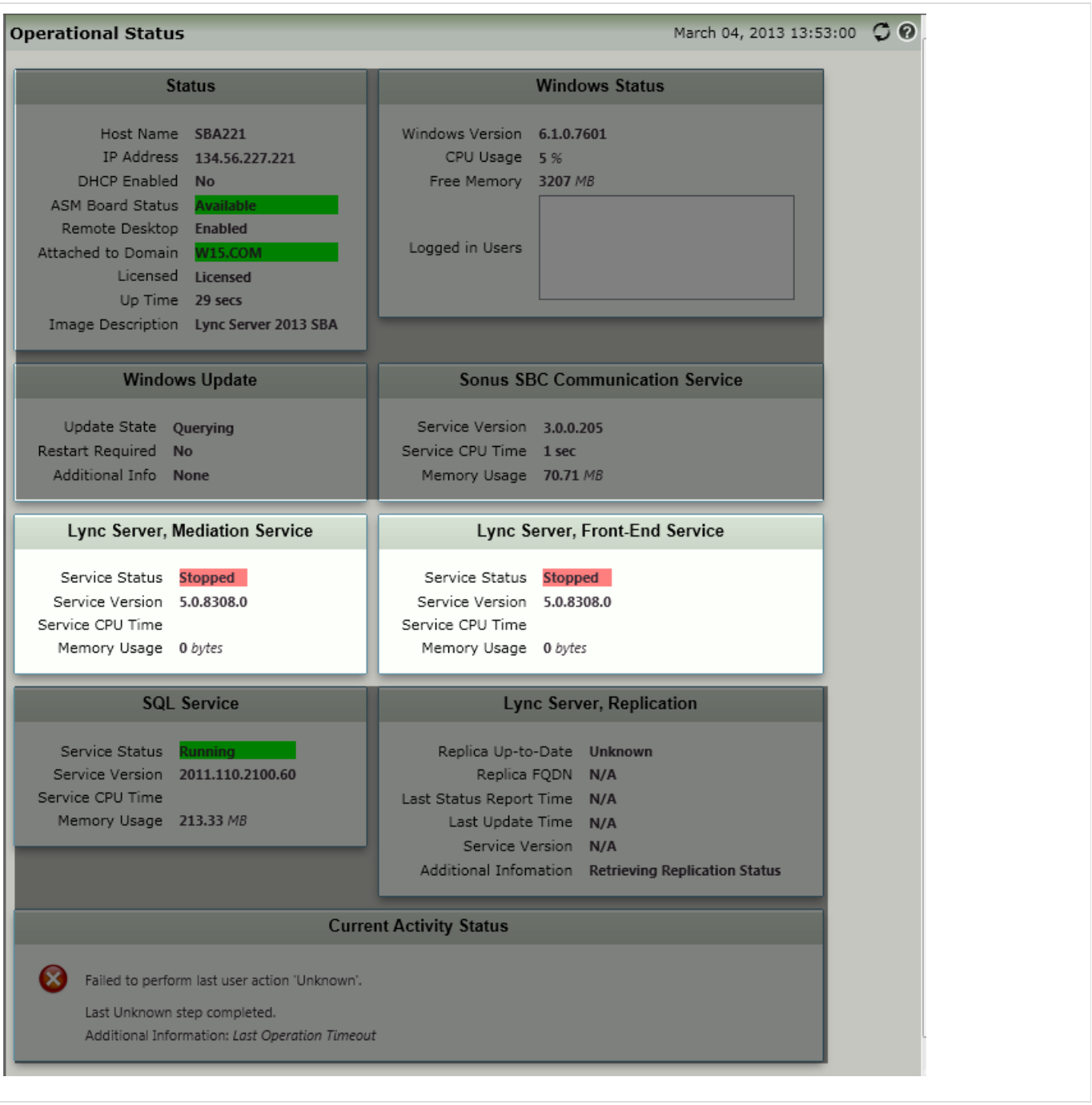
- Re-initializing the ASM
- Viewing and Exporting Windows Event Logs on the ASM
- Managing the Windows Firewall on the ASM

Starting the SBA Services

To complete the deployment, you must start the following Lync Services on the ASM in order for it to function as a Survivable Branch Appliance (SBA):

1. Lync Server 2010, Front-End Service
2. Lync Server 2010, Mediation Service

At this stage those services are **Not Running**, you can verify this by Viewing the SBA Operational Status:

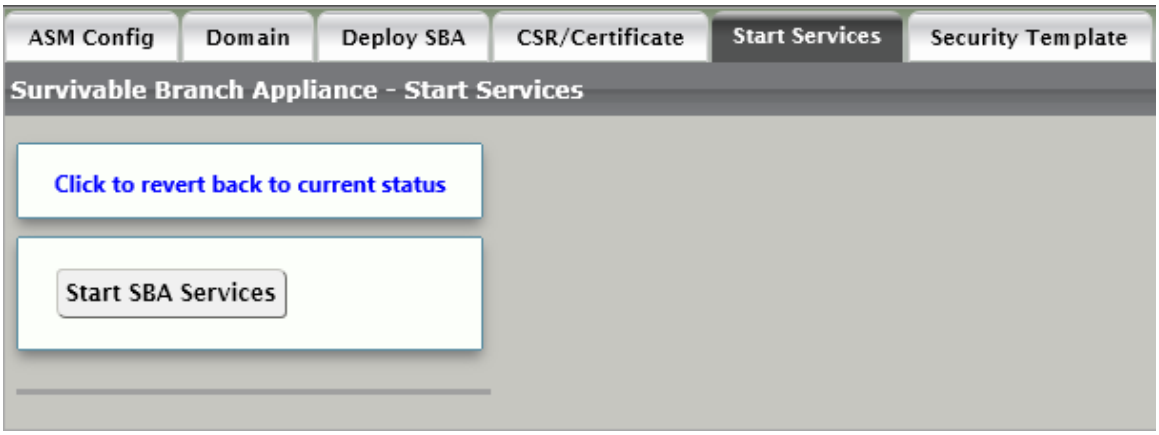


Copyright © 2015 Sonus Networks. All rights reserved.

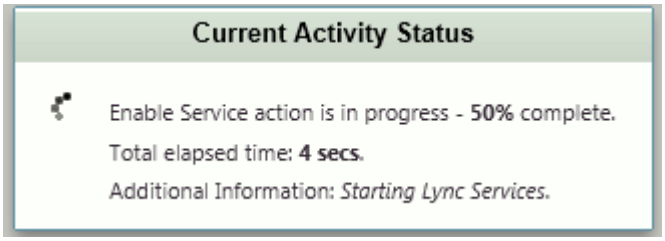
Status	Lync SBA Branch Site Tasks
✅	Step 1 - Configuring the ASM IP Settings
✅	Step 2 - Joining the ASM to a Domain
✅	Step 3 - Deploying the SBA
✅	Step 4 - Generate and Import an SBA Certificate
Now	Step 5 - Starting the SBA Services
❌	Step 6 - Applying an SBA Security Template

To Start the Lync SBA Services

1. Click the **Start SBA Services**

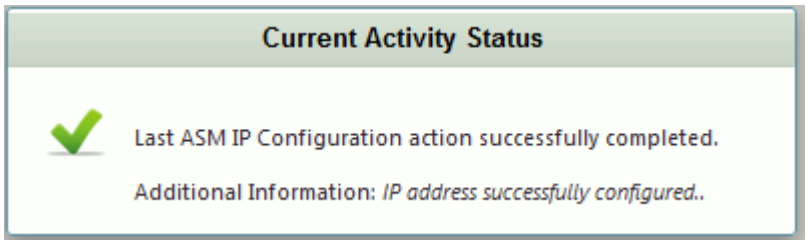


2. A series of status messages will be dispatched:
   a. The Lync services are started:



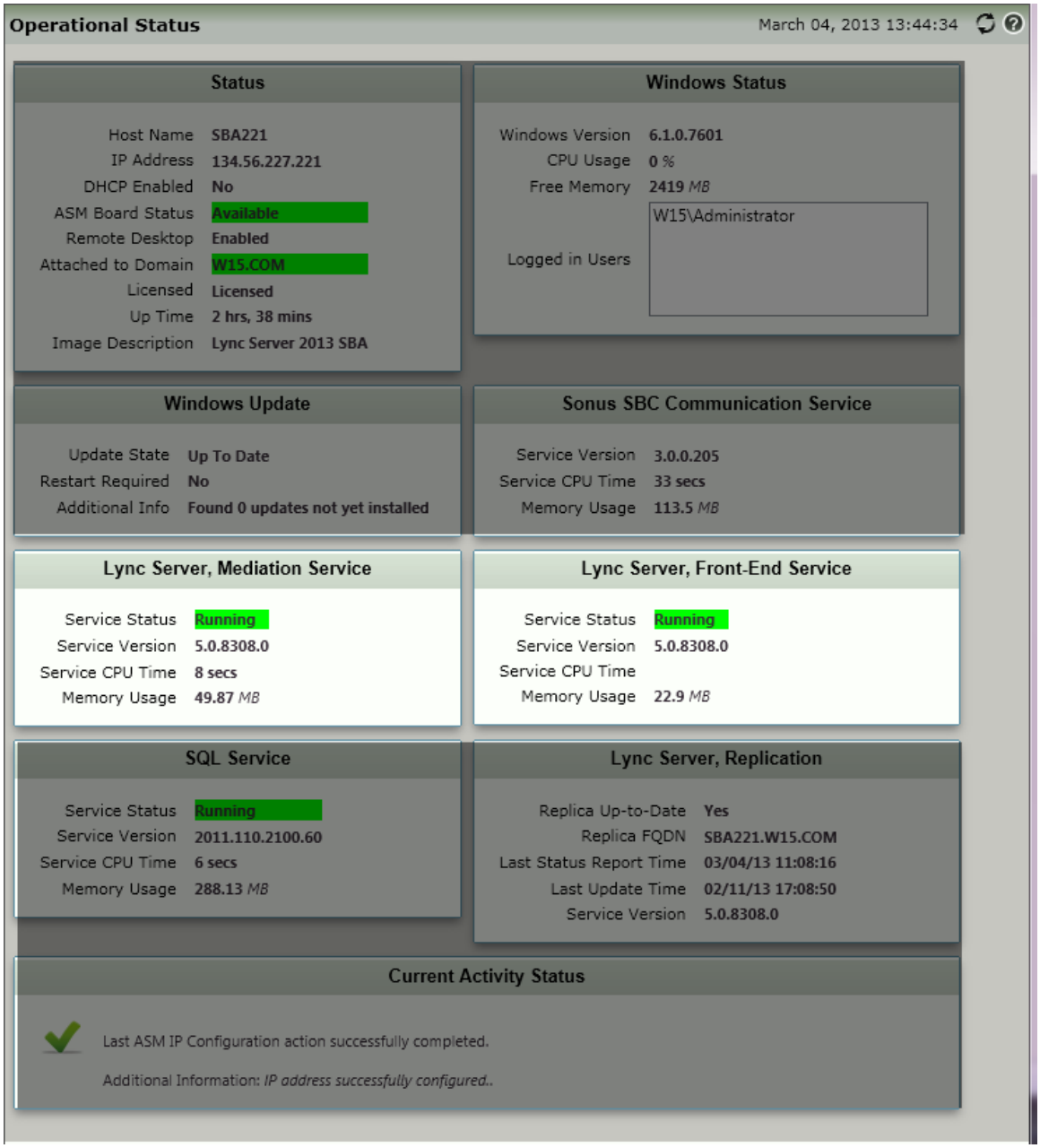
   b. The action succeeds:

Copyright © 2015 Sonus Networks. All rights reserved.



Verifying the Lync SBA Services are Running

When Viewing the SBA Operational Status, these services will appear as **Running** as shown below:



The Lync services can be stopped (and restarted) at anytime. See Starting and Stopping SBA Services

Copyright © 2015 Sonus Networks. All rights reserved.

Generate and Import an SBA Certificate

In order to complete the Branch Site Tasks, the following series of steps must be completed:

1. Generate a certificate signing request for the SBA.
2. Submit the certificate signing request to a Trusted Certificate Authority (CA)
3. Import the signed certificate (received from the CA) onto the ASM

These steps can be achieved in a single step by #Auto-Generate and Importing an SBA Certificate, or you can #Generate an SBA Certificate Signing Request and have it signed by the Trusted CA of your choice and later importing it manually onto the SBA.

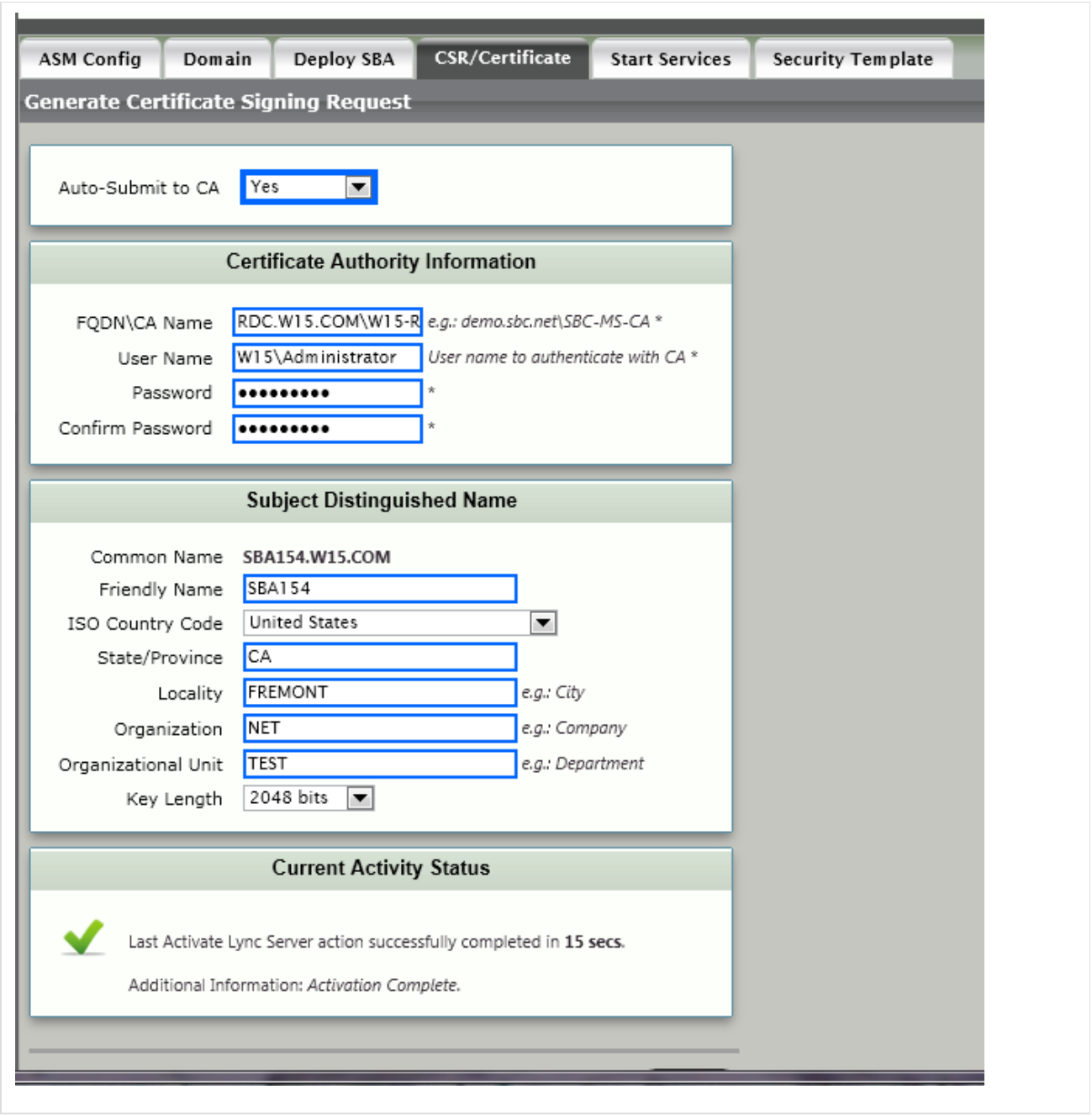
Status	Lync SBA Branch Site Tasks
✅	Step 1 - Configuring the ASM IP Settings
✅	Step 2 - Joining the ASM to a Domain
✅	Step 3 - Deploying the SBA
Now	Step 4 - Generate and Import an SBA Certificate
❌	Step 5 - Starting the SBA Services
❌	Step 6 - Applying an SBA Security Template

Auto-Generate and Importing an SBA Certificate

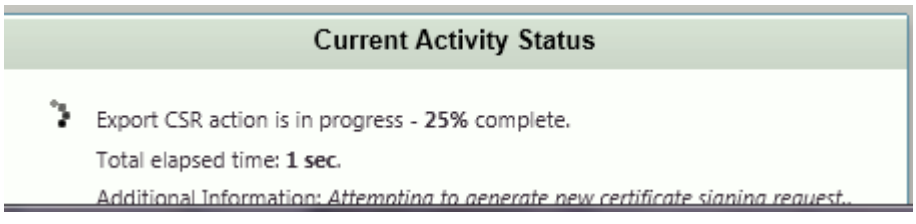
When using this option, the certificate signing request is sent to a Trusted **Windows Certificate Authority** server:

1. In the **Auto-Submit to CA**, select **Yes**
2. In **FQDN\CA Name**, enter the fully qualified domain name (FQDN) and the name of the certificate authority (CA) server.
3. In the **User Name** field, enter the username to use to be authenticated with the CA server.
   ℹ Depending on the CA server used, the signing request can be processed *only if* the User Name is supplied in the `username@domain` format.
4. In the **Password** field, enter (and re-enter to confirm) the password associated with the username entered above.
5. The **Common Name** will be automatically set after having successfully joined the ASM to the domain
6. Enter the information pertaining to your environment:

Copyright © 2015 Sonus Networks. All rights reserved.

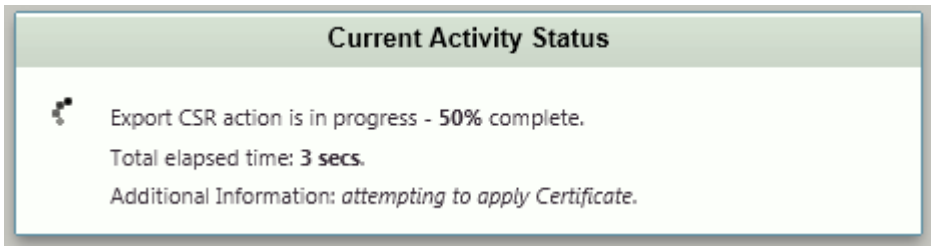


7. Click **OK**. A series of status messages will be dispatched:
   a. Creation of a new certificate signing request:

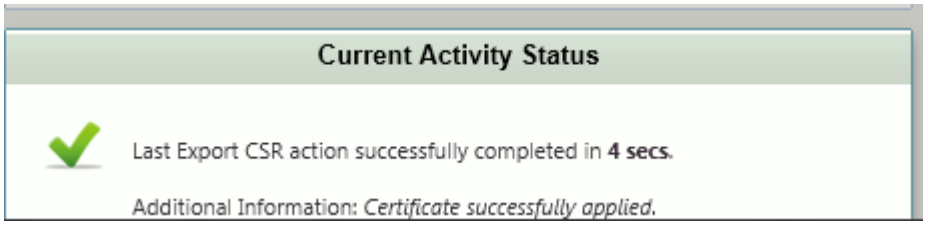


   b. Import of the certificate

Copyright © 2015 Sonus Networks. All rights reserved.



c. The action succeeds

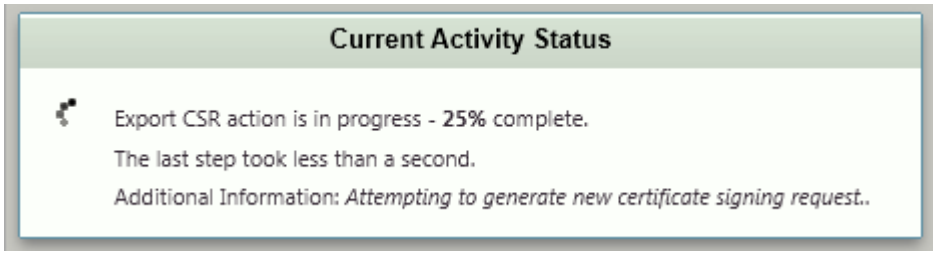


Generating an SBA Certificate Signing Request

You can chose this option if you wish to send the certificate signing request to a CA of your choice:

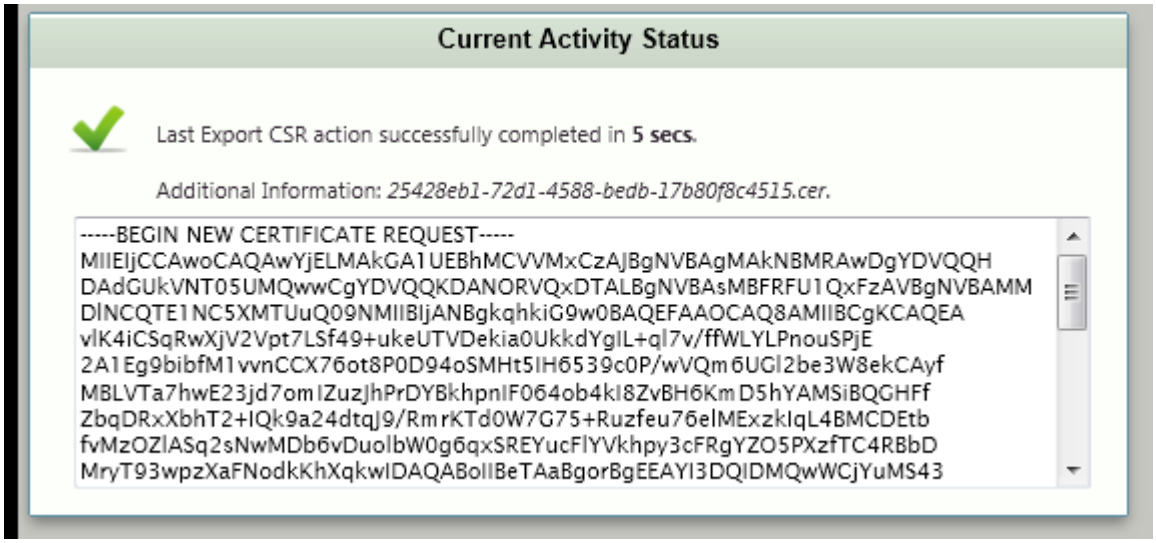
1. In the **Auto-Submit to CA**, select **No**

1. In the **Subject Distinguished Name** panel, enter the information pertaining to your environment.
2. Click **OK**. The following status message will be dispatched:



3. Once complete - the certificate signing request is presented:

Copyright © 2015 Sonus Networks. All rights reserved.



Once this certificate signing request has been sent to a desired CA, the certificate that you receive from the CA must be imported in order to complete the SBA deployment.

Deploying the SBA

To deploy the SBA, you must execute the following steps in order:

- Step 1 - Prepare the SBA
- Step 2 - Start Replication
- Step 3 - Activate the SBA

In the event an issue arises while executing any of the steps, you can troubleshoot and resolve the issue and redo the step.

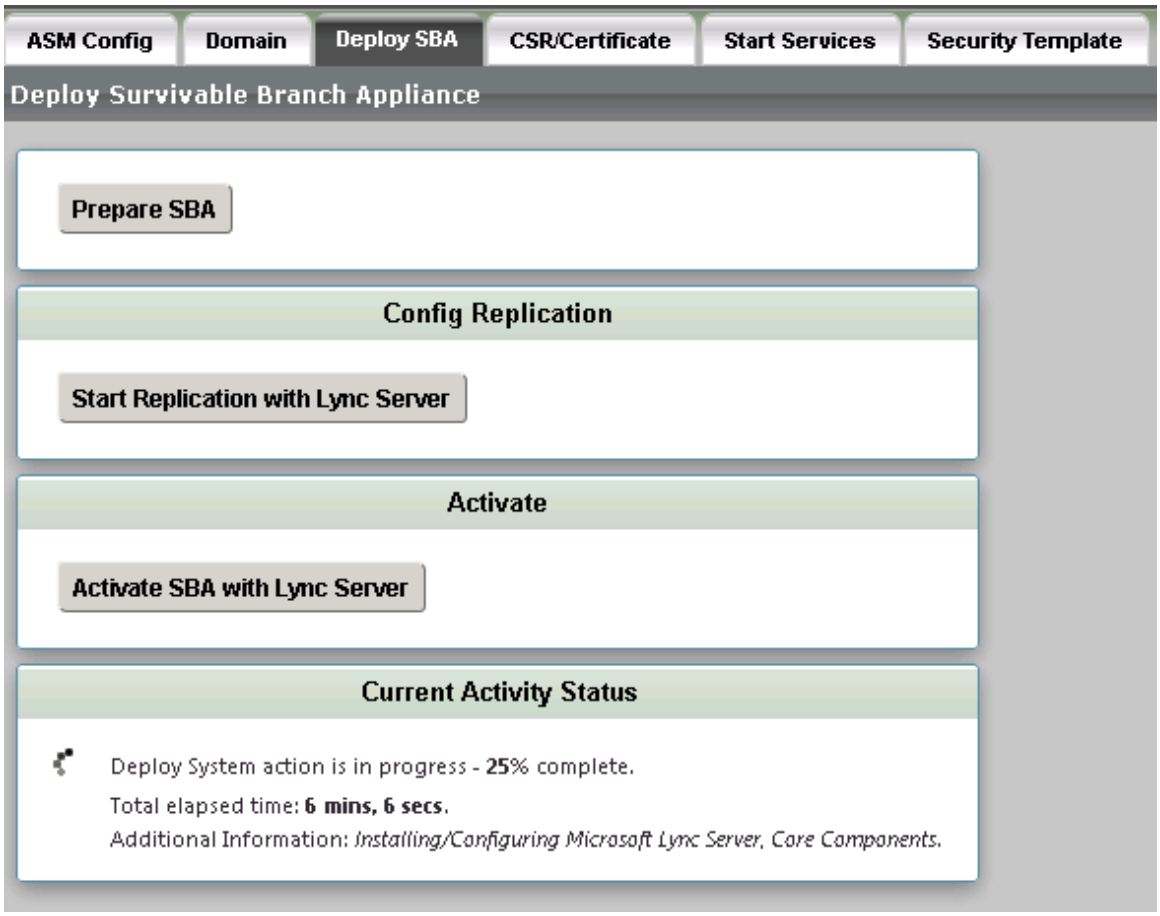
Status	Lync SBA Branch Site Tasks
✅	Step 1 - Configuring the ASM IP Settings
✅	Step 2 - Joining the ASM to a Domain
Now	Step 3 - Deploying the SBA
❌	Step 4 - Generate and Import an SBA Certificate
❌	Step 5 - Starting the SBA Services
❌	Step 6 - Applying an SBA Security Template

Step 1 - Prepare the SBA

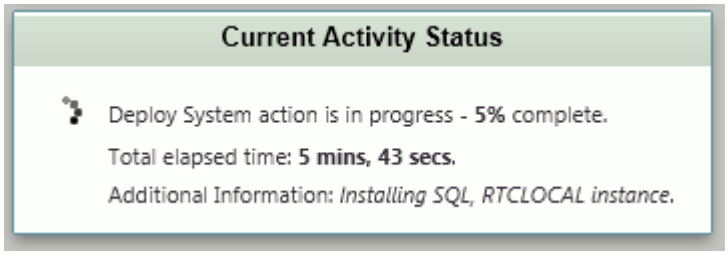
This step prepares the SBA by installing all components of the local Survivable Branch packages onto the ASM.

1. Click **Prepare SBA**

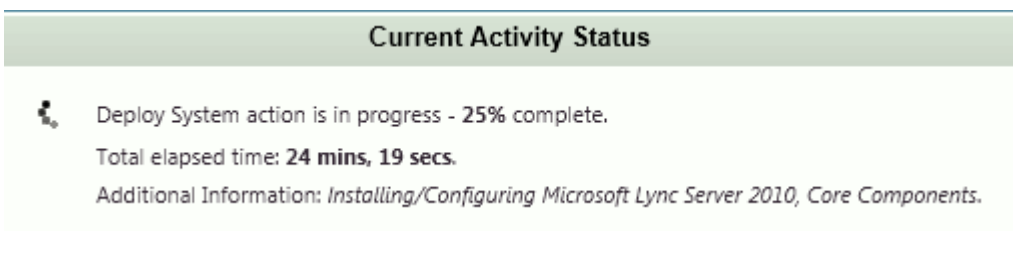
Copyright © 2015 Sonus Networks. All rights reserved.



2. A series of status messages will be dispatched when executing this step:
   a. Installs SQL Server:

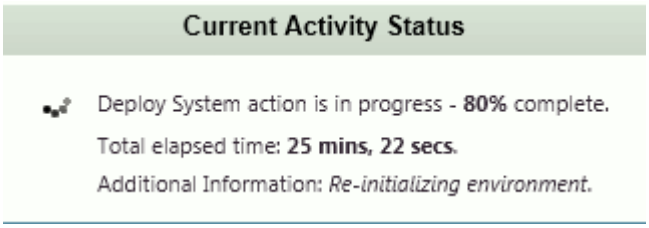


   b. Installs the Lync Core Components:



   c. Installs the Lync Front End (FE) Server:

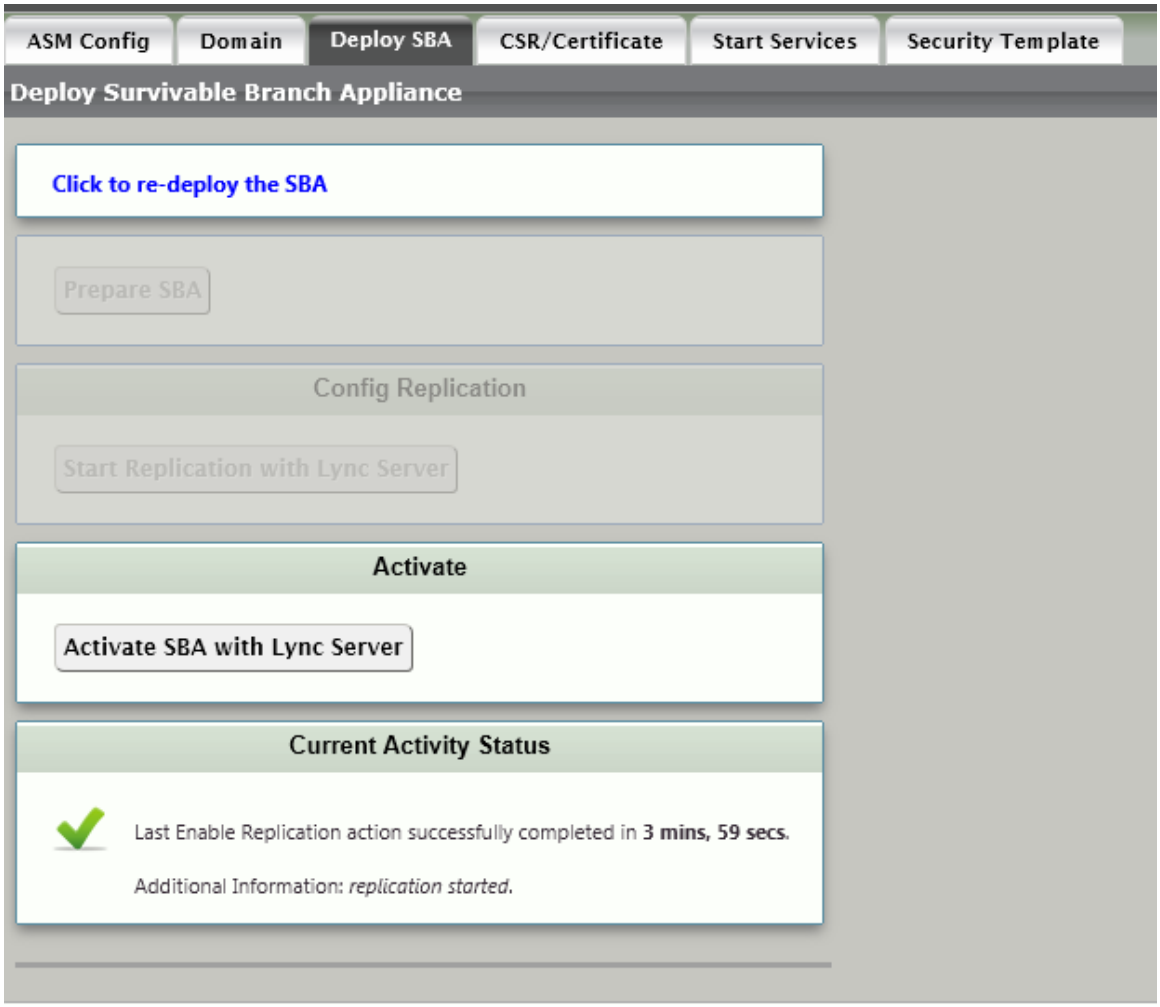
Copyright © 2015 Sonus Networks. All rights reserved.



Step 2 - Start Replication

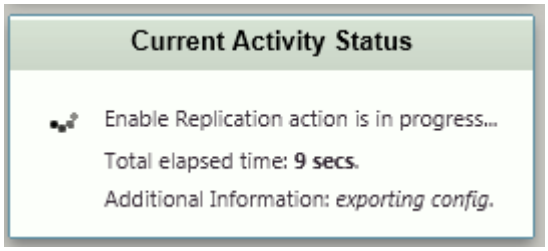
This step starts the configuration replication from the Lync Topology

1. Click **Start Replication with Lync Server**

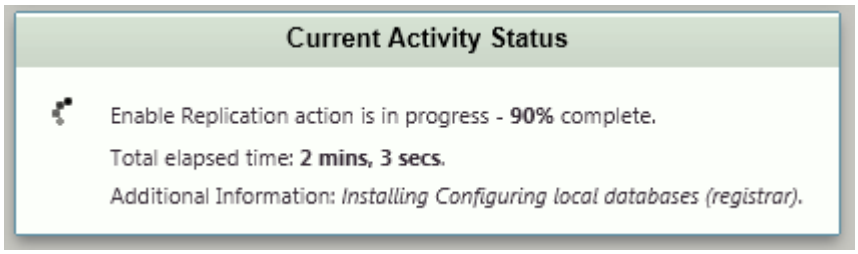


2. A series of status messages will be dispatched when executing this step:
    a. The Lync topology configuration is exported and imported into the SBA:

Copyright © 2015 Sonus Networks. All rights reserved.



b. The replication starts:

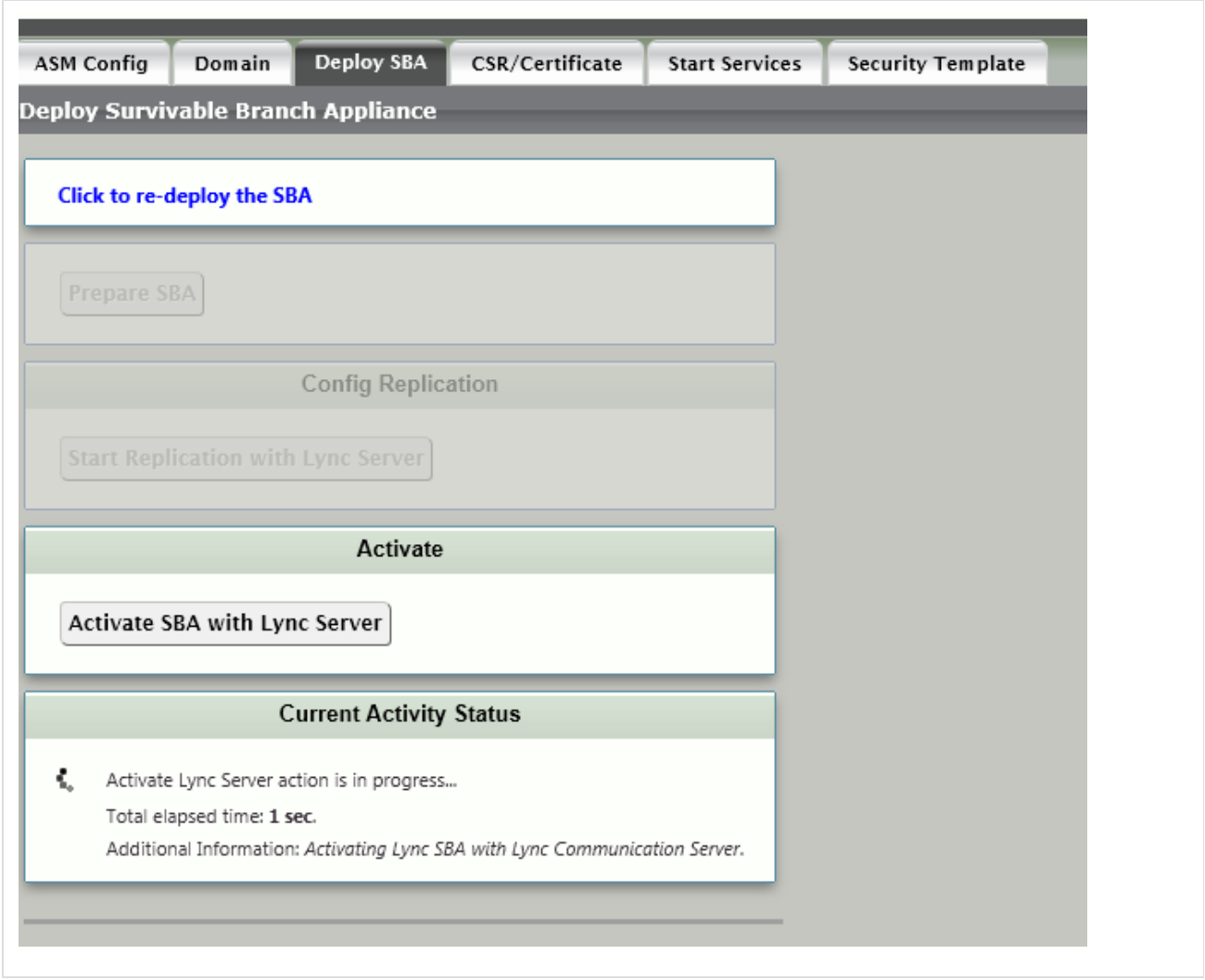


Step 3 - Activate the SBA

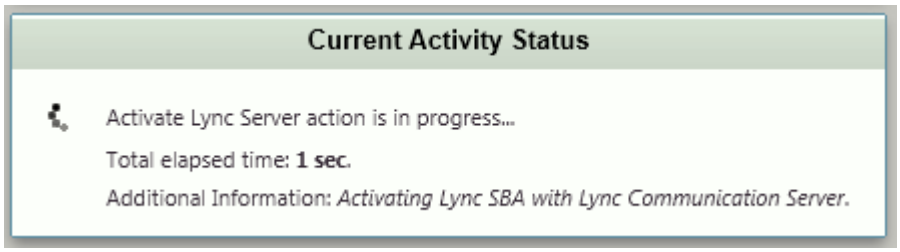
This step activates the SBA software with the Lync Server (enables its role as an SBA with the Lync Server)

1. Click the **Activate SBA with Lync Server**

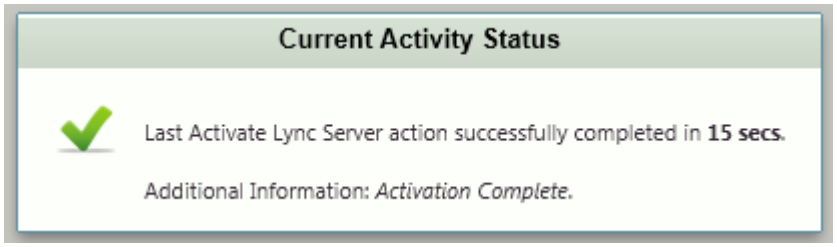
Copyright © 2015 Sonus Networks. All rights reserved.



2. A series of status messages will be dispatched when executing this step:
   a. The Lync SBA is activated with the Lync Communication Server:



   b. The execution completes:



Copyright © 2015 Sonus Networks. All rights reserved.

Joining the ASM to a Domain

Joining the ASM to a domain **may impact the availability of services** on the ASM such as Remote Desktop by denying access to these services through security policies.

Before joining the ASM server to a domain, we recommend for you to review your domain's default security and group policies to verify that required services and access are allowed. You may need to create exceptions for the ASM host to allow the use of services such as Remote Desktop.

Status	Lync SBA Branch Site Tasks
✅	Step 1 - Configuring the ASM IP Settings
Now	Step 2 - Joining the ASM to a Domain
❌	Step 3 - Deploying the SBA
❌	Step 4 - Generate and Import an SBA Certificate
❌	Step 5 - Starting the SBA Services
❌	Step 6 - Applying an SBA Security Template

Joining the ASM to a Domain

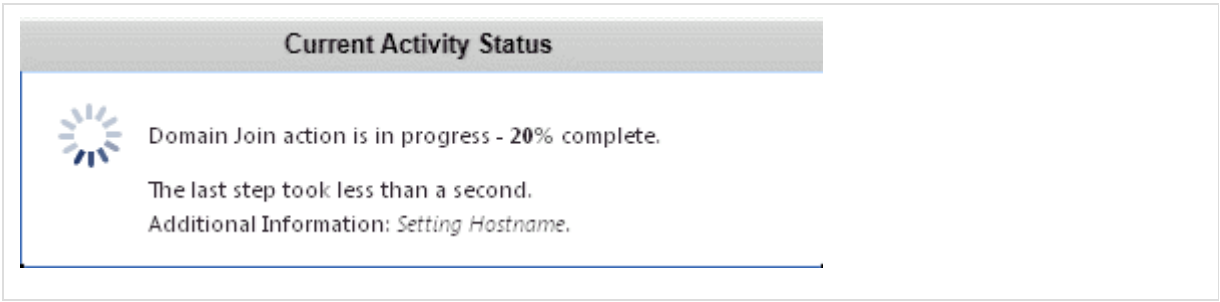
Please note that this operation automatically reboots the ASM to complete.

1. In **Domain Action**, select **Join to a Domain**. Notes:
   - The ASM computer **name must be SonusBIOS compliant** with a maximum length of 15 characters.
   - The name used must match the name used during the Central Site Tasks steps
2. In **Domain Name**, enter the name of the domain used by your Microsoft Lync environment.
3. In **User Name**, enter the user name of the account with **domain administrator privileges.**
   ℹ This can be entered in the form of `username@domain` or `domain\username`
4. In **Password**, enter the password of the account with domain administrator privileges.

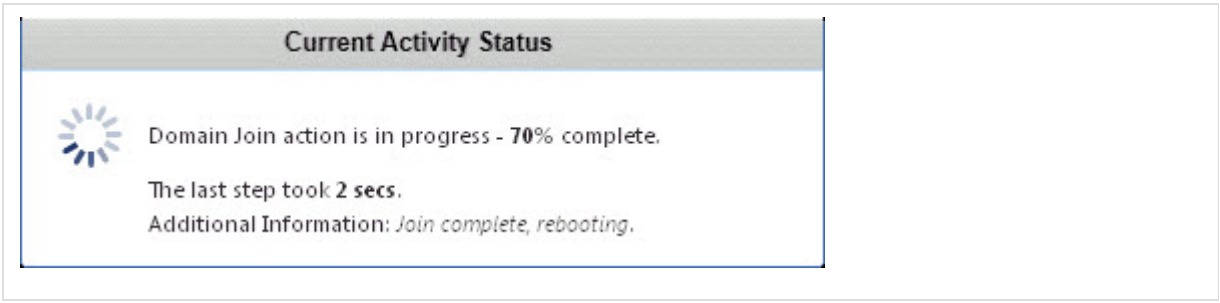
Copyright © 2015 Sonus Networks. All rights reserved.



5. Click the **OK**button to join to the Domain. A series of status messages will be dispatched when joining to the domain:
    a. Setting hostname step:

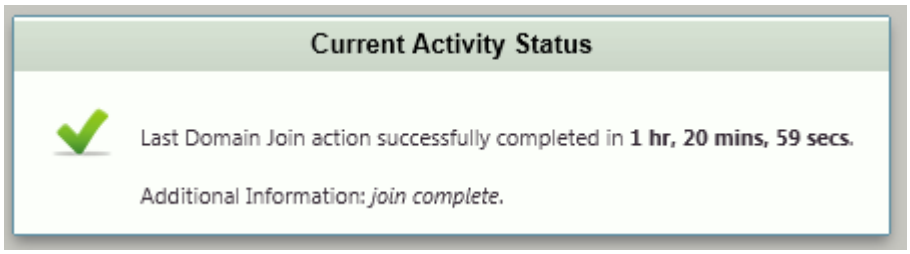


    b. Joining to domain step:



    c. ASM Reboot complete:

Copyright © 2015 Sonus Networks. All rights reserved.

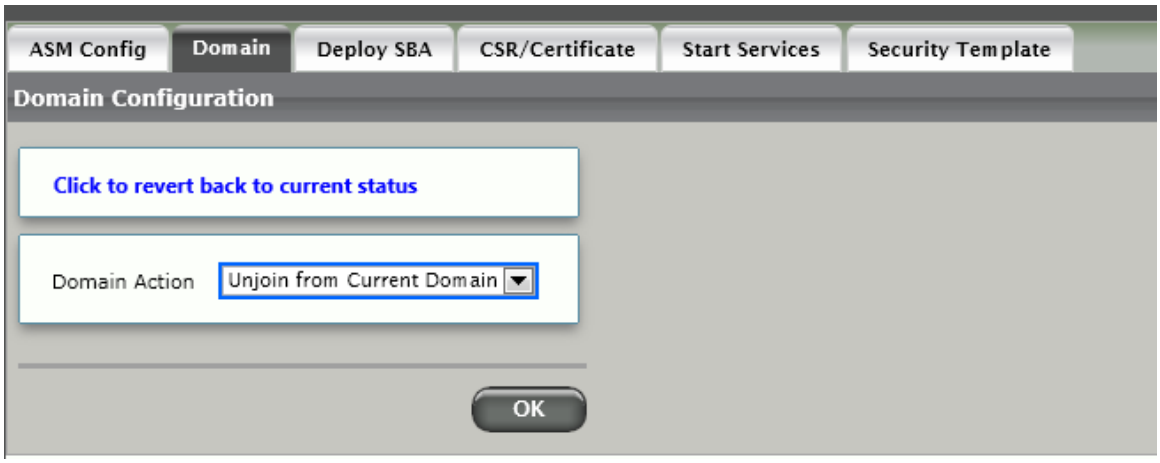


Un-joining the ASM from a Domain

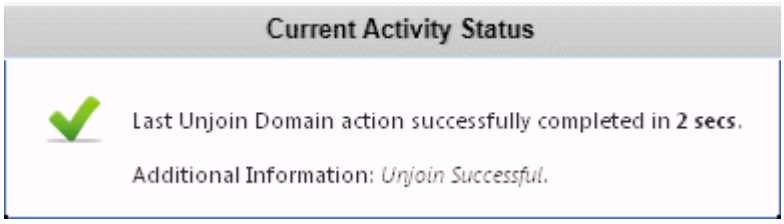
This is not a common operation, but can be used in the event you have incorrectly joined to the wrong domain. This operation does not reboot the ASM.

If you have already started Deploying the SBA, unjoining will damage the deployment and a Re-initializing the ASM must be performed.

1. In **Domain Action**, select **Unjoin from Current Domain**.



2. Click **OK**. The following status message is dispatched:



Powering the ASM ON and OFF

The Sonus SBC 1000/2000 system allows you to remotely shut down and power up the Application Solution Module (ASM) via the WebUI. Below are some of the common reasons why System Administrators would want to shut down the ASM:

- If you plan on physically re-locating the Sonus SBC 1000/2000 system, it is recommended to shut down the ASM first
- If the ASM is running and wish to temporarily disable it
- Useful when troubleshooting

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000/2000 Model Differences

- **Sonus SBC 1000**
  - Does not shutdown or restart when Sonus SBC 1000/2000 is rebooted.
  - The Power off is achieved via the hardware and does not need Sonus SBC 1000/2000 communication service to be operational.
- **Sonus SBC 2000**
  - If the Sonus SBC 1000/2000 is rebooted, the ASM is automatically restarted. This makes it more important to shutdown the ASM **before powering off** (or relocating) the Sonus SBC 1000/2000 unit.
  - The power off is initiated via the Sonus SBC 1000/2000 communications service and thus needs the service to be operational for the command to work.

Never Power Off the ASM via Remote-Desktop

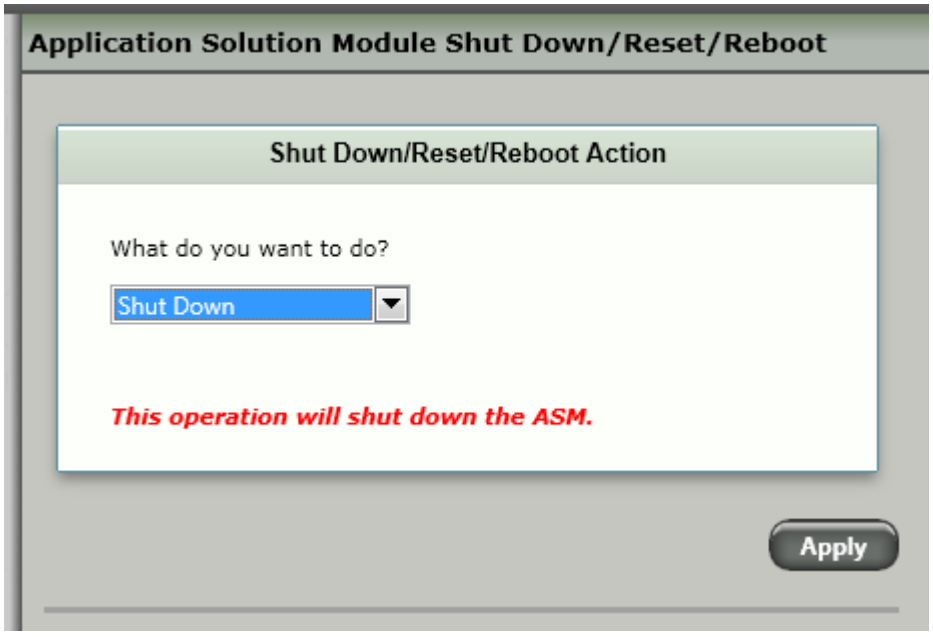
Always power off the ASM via the Sonus SBC 1000/2000 WebUI. If you have mistakenly shutdown the ASM via remote desktop - the only way power the ASM back on is as follows:

- **Sonus SBC 1000** — Issue an ASM Hardware Reset via the WebUI
- **Sonus SBC 2000** — Physically power-cycle the Sonus SBC 1000/2000 unit

Powering the ASM OFF

Once ASM is powered off several ASM related alarms will be generated.

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Application Solution Module**, click **Shut Down/Reset/Reboot**.



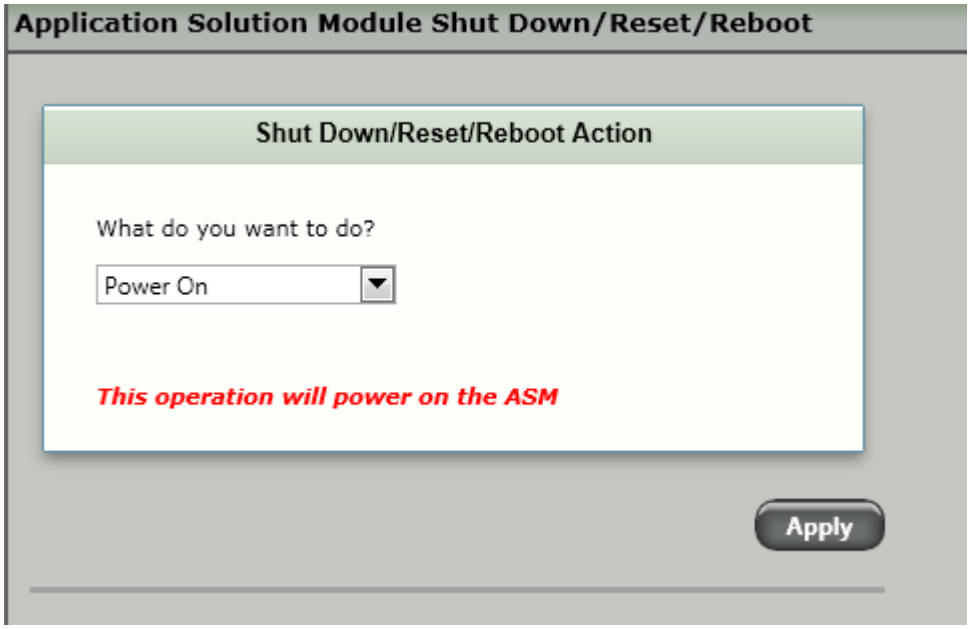
3. Select **Shut Down**
4. Click **Apply**

Powering the ASM ON

1. In the WebUI, click the **Tasks** tab.

Copyright © 2015 Sonus Networks. All rights reserved.

2. In the left navigation pane, under the **Application Solution Module**, click **Shut Down/Reset/Reboot**.



3. Select **Power On**
4. Click **Apply**

This operation typically takes a few minutes to complete

Updating the ASM Recovery Partition

This operation allows you to load new software into the Recovery partition of the ASM. There are a number of reasons why you would want to do this:

- To update the recovery partition with newer software, allowing one to be better prepared should they need to Re-initialize the ASM at a later date.
- To put a completely different software load onto the ASM. For example, convert a Windows only ASM to an SBA ASM or vise versa. To do so, follow this procedure then perform the procedure described in the Re-initializing the ASM section.

> ☑ This operation does not actually erase, replace or load the ASM software itself - it only updates the recovery partition. To apply an image installed here, see Re-initializing the ASM.

Before You Begin

This operation can only be performed when the Sonus SBC 1000/2000 Communication service becomes operational. In other words, only when a valid ASM IP address has been configured either via the Initial Setup or the ASM IP Settings.

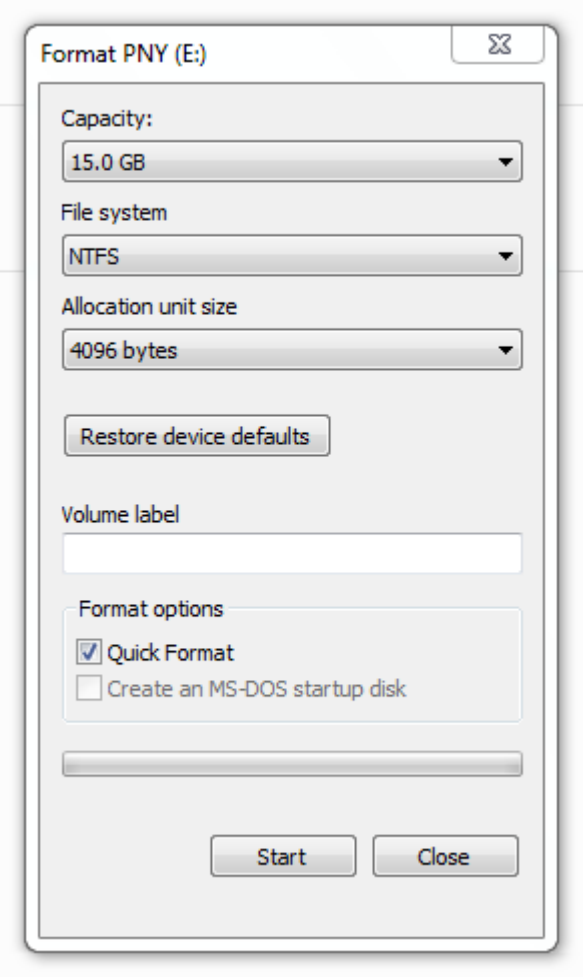
In addition, you will need to obtain:

- An empty USB flash drive, 8GB or larger.
- The software image you would like to load. These can be obtained from the Sonus SBC 1000-2000 Download Center.

Preparing the USB Flash Drive

Copyright © 2015 Sonus Networks. All rights reserved.

1. Insert the flash drive into your PC.
2. Format the flash drive for the NTFS file system (if you have not done so already). This is necessary due to the large size of the image files.
   To perform this in Windows, do the following:
   a. Browse to Computer and find the flash drive.
   b. Right-click it, and select **Format...**.
   c. Select **NTFS** from the **File system** dropdown, and click **Start**.



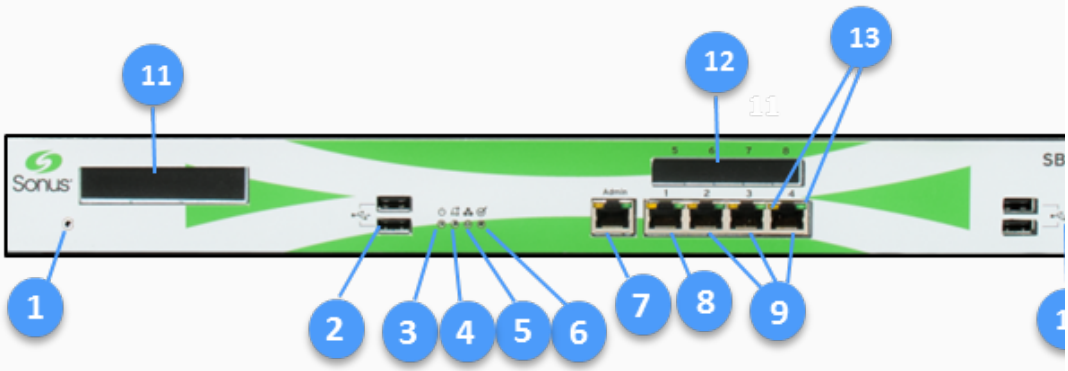
3. Locate the image file mentioned above - we require a file called **ASMimage.tar**.
4. Copy **ASMimage.tar** to the root directory of the USB drive.

> Make sure that the image file is not located in a subdirectory of the flash drive.

Load a New ASM Image from USB

1. Insert the prepared flash drive into one of the ASM USB ports of the Sonus SBC 1000/2000 system.
   - **Updating the ASM Recovery Partition on the Sonus SBC 2000**- directly plug it into the USB Port for the ASM.
     - Click here to see where the ASM USB port is on the front of the Sonus SBC 2000 chassis

Copyright © 2015 Sonus Networks. All rights reserved.



#	Name	Description
1	**Reset**	System reset button. For more information, see Resetting the Sonus SBC 1000-2000 to Factory Defaults.
2	**USB Ports**	USB ports for Sonus SBC 1000/2000 main board
3	**Power**	Power Status LED
4	**Alarm**	Alarm Status LED
5	**Peer Node**	Peer Node Status LED (also recognized as the Locator LED)
6	**Ready**	Ready Status LED
7	**Admin Port**	System Administration Ethernet Port – **do not connect to your live network - see warning below**
8	**Port 1**	Primary Application Ethernet Port 1
9	**Ports 2 - 4**	Ethernet Ports 2 - 4
10	**USB Ports**	USB ports for the Application Service Module (ASM) (when installed)
11	**Expansion Bay**	Future expansion bay
12	**Expansion Bay**	Networking expansion bay
13	**Ethernet Port Status**	Ethernet Status LED

Warnings

Admin Port

Copyright © 2015 Sonus Networks. All rights reserved.

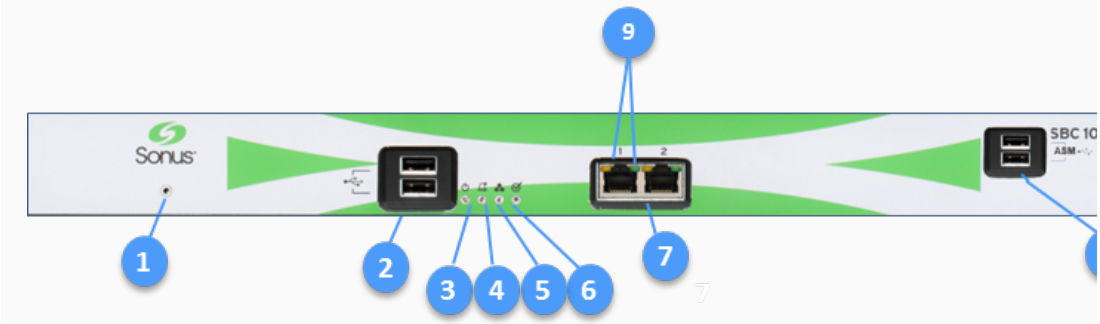
The Administrative IP port should only be used for Running Initial Setup and disconnected when not in use (especially to avoid conflicts with your network). This interface **cannot be used for VOIP media or protocols**.

Application Ethernet Ports

When two or more LAN Ethernet ports are on the same Bridge (as in the factory-default Sonus SBC 1000/2000 configuration), **they must not be connected to the same Ethernet switch or Ethernet network**. Doing so creates a broadcast loop in the Ethernet network, rendering the network unusable. You may work around this issue by connecting the Ethernet ports directly to an intelligent switch or router running a *spanning tree* protocol.

- **Updating the ASM Recovery Partition on the Sonus SBC 1000**- directly plug it into the USB Port for the ASM.
  - Click here to see where the ASM USB port is on the front of the Sonus SBC 1000 chassis

Copyright © 2015 Sonus Networks. All rights reserved.



#	Name	Description
1	**Reset**	System reset button. For more information, see Resetting the Sonus SBC 1000-2000 to Factory Defaults.
2	**USB Ports**	USB ports for Sonus SBC 1000/2000 main board — see USB Ports detail section below
3	**Power**	Power Status LED
4	**Alarm**	Alarm Status LED
5	**Peer Node**	Peer Node Status LED (also recognized as the Locator LED)
6	**Ready**	Ready Status LED
7	**Port 1 - 2**	Ethernet Ports 1 and 2
8	**USB Ports**	USB ports for the Application Service Module (ASM) (when installed)
9	**Ethernet Port Status**	Ethernet Status LED

USB Ports

Usage

The Sonus SBC 1000 sports two pairs of USB ports (as illustrated above) — each pair serves a particular purpose:

Location	USB Port Intent and Usage Detail

Copyright © 2015 Sonus Networks. All rights reserved.

2	These ports are optionally used to attach an external USB drive to store core dumps for troubleshooting (in the event they occur), and as a survivability mechanism for Active Directory Caching (when configured). See Support section below for proper usage.
8	If your Sonus SBC 1000 has a built-in Application Service Module (ASM), this USB port is primarily used for Updating the ASM Recovery Partition, and to (optionally) transfer files between a USB drive and the ASM.

Support

⚠ The following section is applicable only to the USB ports on **location #2** on the Sonus SBC 1000's front panel.

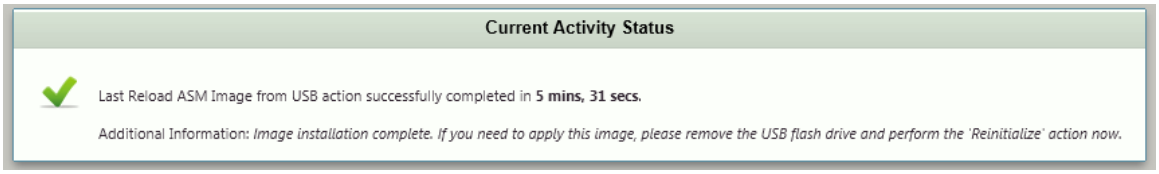
For the Sonus SBC 1000/2000 system to properly recognize the USB thumb drive, you must ensure the following prerequisites are satisfied:

- The USB storage must be of **FAT32 file format**.
- The storage must be at least 1GB (or more) in size.
- The SBC does not require a reboot after the USB drive is installed.

2. In the WebUI, click the **Tasks** tab.
3. In the left navigation pane, under **Application Solution Module**, click **Update ASM Recovery Partition**.
4. Click the **Apply** button to begin the installation of the new image.

> ⚠ Loading and installing the new image can take up to 10 minutes.

5. Wait for the following message to be displayed:



6. Remove the USB flash drive from the system.

The Recovery partition has now been updated.

> ℹ In most cases, updating the recovery partition should not require re-initializing the ASM. Updating the recovery partition as part of an upgrade to SBC firmware in order to keep the Application Solution Module (ASM) in step with the current SBC code version does not require re-initializing the ASM. If you do re-initialize to apply the image you just installed, the ASM task restores the ASM to an unconfigured state, and replaces all software and settings with the image in the Recovering partition of the ASM. See Re-initializing the ASM for specific information.

Viewing the Installed Packages on the ASM

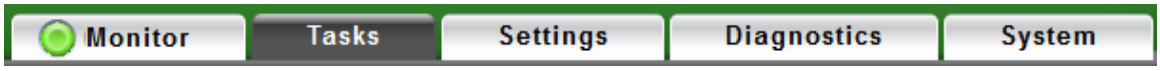
This view is used to verify installed packages on the ASM, including their current versions. The list of items displayed in this view are dynamically queried from the Windows "Installed Programs" Control Panel view.

Copyright © 2015 Sonus Networks. All rights reserved.

Viewing the Installed Packages on the ASM

> **Important Note:** This view will not function until the Sonus SBC 1000/2000 Communication Service becom es operational. In other words, only when a valid ASM IP address has been configured either via the Initial Setup or the ASM IP Settings.

This operation can be accessed via the **Tasks** tab or **Settings** tab:



Viewing Installed Packages on the ASM through the Tasks Tab

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Application Solution Module**, click **Installed Packages.**



Row ID	Name	Version	Install Date
1	Microsoft Application Error Reporting	12.0.6015.5000	09-28-2012
2	Microsoft Visual C++ 2008 Redistributable - x...	9.0.30729.4148	09-28-2012
3	SQL Server 2008 R2 SP1 Database Engine Servic...	10.51.2500.0	09-28-2012
4	Microsoft SQL Server 2005 Backward compatibil...	8.05.2312	09-28-2012
5	SQL Server 2008 R2 SP1 Database Engine Shared	10.51.2500.0	09-28-2012
6	Microsoft Unified Communications Managed API ...	4.0.7577.0	09-28-2012
7	Microsoft SQL Server Browser	10.51.2500.0	09-28-2012
8	Microsoft SQL Server 2008 R2 Setup (English)	10.51.2500.0	09-28-2012
9	SBC Communication Service	3.00.0198	02-12-2013
10	Microsoft SQL Server 2008 Setup Support Files...	10.1.2731.0	09-28-2012
11	Microsoft SQL Server 2008 R2 Native Client	10.51.2500.0	09-28-2012
12	SQL Server 2008 R2 SP1 Common Files	10.51.2500.0	09-28-2012
13	Microsoft SQL Server 2008 R2 RsFx Driver	10.51.2500.0	09-28-2012
14	Microsoft SQL Server VSS Writer	10.51.2500.0	09-28-2012
15	Sql Server Customer Experience Improvement Pr...	10.50.1600.1	09-28-2012
16	Service Pack 1 for SQL Server 2008 R2 (KB2528...	10.51.2500.0	09-28-2012
17	Microsoft SQL Server 2008 R2 (64-bit)		01-01-1970

Viewing Installed Packages on the ASM through the Settings Tab

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > Installed Packages**.

Copyright © 2015 Sonus Networks. All rights reserved.



Row ID	Name	Version	Install Date
1	Microsoft Application Error Reporting	12.0.6015.5000	09-28-2012
2	Microsoft Visual C++ 2008 Redistributable - x...	9.0.30729.4148	09-28-2012
3	SQL Server 2008 R2 SP1 Database Engine Servic...	10.51.2500.0	09-28-2012
4	Microsoft SQL Server 2005 Backward compatibil...	8.05.2312	09-28-2012
5	SQL Server 2008 R2 SP1 Database Engine Shared	10.51.2500.0	09-28-2012
6	Microsoft Unified Communications Managed API ...	4.0.7577.0	09-28-2012
7	Microsoft SQL Server Browser	10.51.2500.0	09-28-2012
8	Microsoft SQL Server 2008 R2 Setup (English)	10.51.2500.0	09-28-2012
9	SBC Communication Service	3.00.0198	02-12-2013
10	Microsoft SQL Server 2008 Setup Support Files...	10.1.2731.0	09-28-2012
11	Microsoft SQL Server 2008 R2 Native Client	10.51.2500.0	09-28-2012
12	SQL Server 2008 R2 SP1 Common Files	10.51.2500.0	09-28-2012
13	Microsoft SQL Server 2008 R2 RsFx Driver	10.51.2500.0	09-28-2012
14	Microsoft SQL Server VSS Writer	10.51.2500.0	09-28-2012
15	Sql Server Customer Experience Improvement Pr...	10.50.1600.1	09-28-2012
16	Service Pack 1 for SQL Server 2008 R2 (KB2528...	10.51.2500.0	09-28-2012
17	Microsoft SQL Server 2008 R2 (64-bit)		01-01-1970

To view an Installed Package's details:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Installing an ASM Package

ASM package updates can be installed by Sonus SBC 1000/2000 System Administrators via the web interface. This functionality is typically used under the following circumstances:

- Updating the Sonus SBC 1000/2000 Communication Service on the ASM
- Installing Lync Cumulative Update (CU) patches on the ASM
- Installing other Roll-up packs such as windows update authorization lists.

> ⚠ This update will accept signed windows *.msi* and *.msp* files as well as published .pkg files

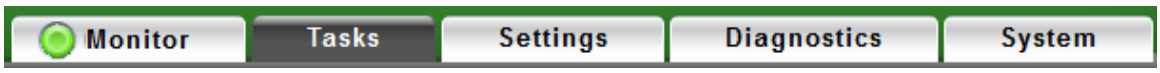
On this page, we illustrate how to install packages on the ASM via the WebUI.

Installing an ASM Package

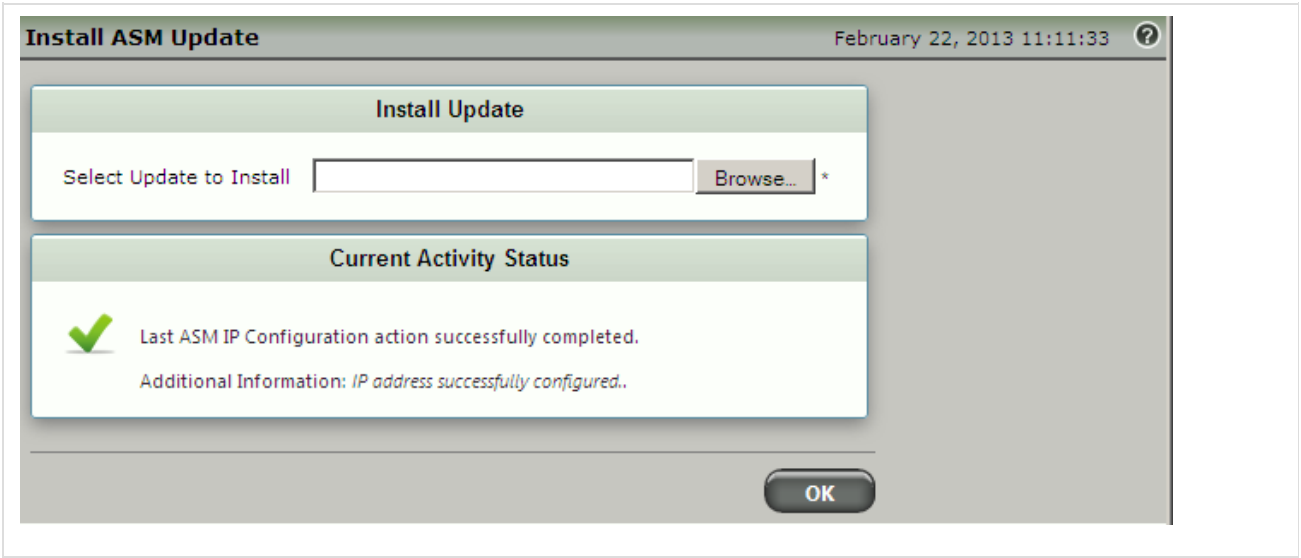
Copyright © 2015 Sonus Networks. All rights reserved.

Before you Begin
This operation can only be performed when the Sonus SBC 1000/2000 Communication service becomes operational. In other words, only when a valid ASM IP address has been configured either via the Initial Setup or the ASM IP Settings.

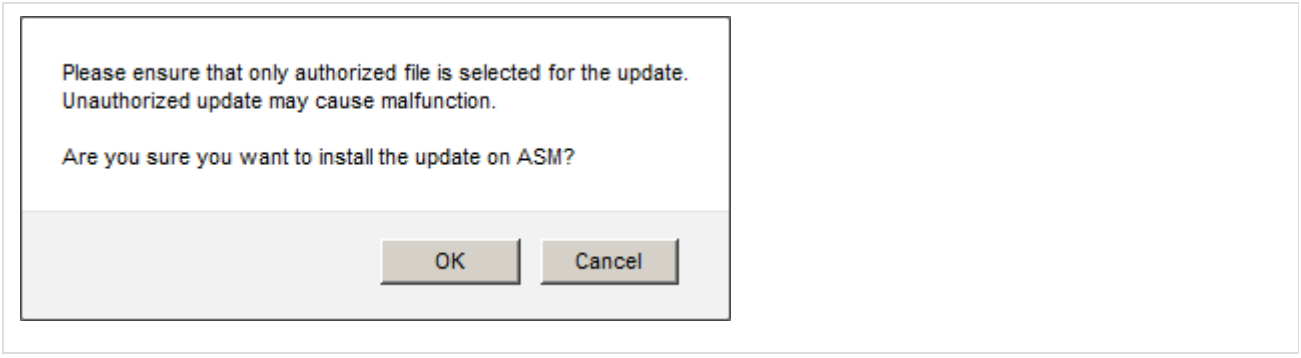
This operation can be accessed either via the **Tasks** tab or the **Settings** tab:



1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Application Solution Module**, click **Install ASM Update**.

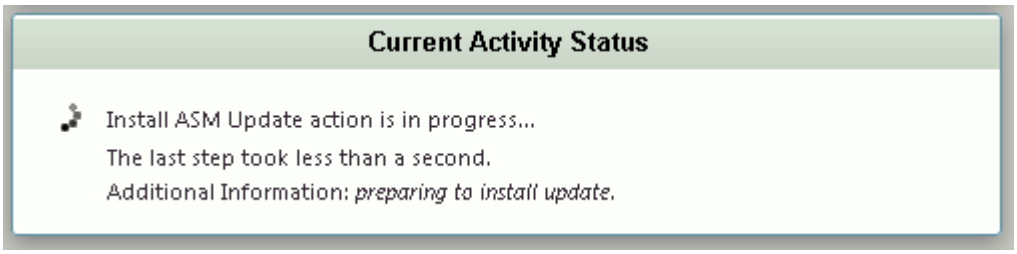


3. Select the ASM **package file** you wish to install
4. Click **OK**
5. You will be presented with the following popup to confirm the action:

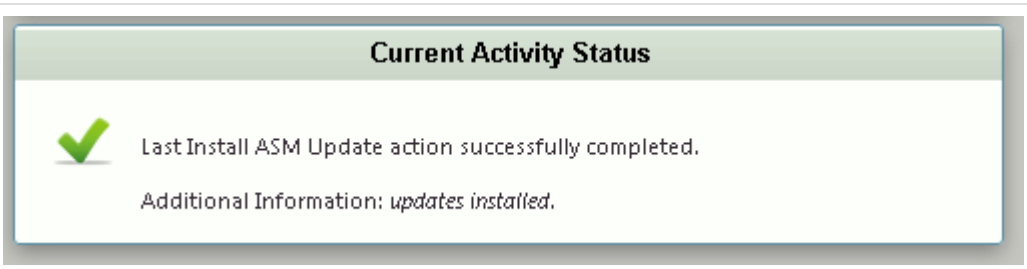


6. Click **OK** to install the package
7. Throughout the installation process, the User interface will dispatch a series of status messages:

Copyright © 2015 Sonus Networks. All rights reserved.

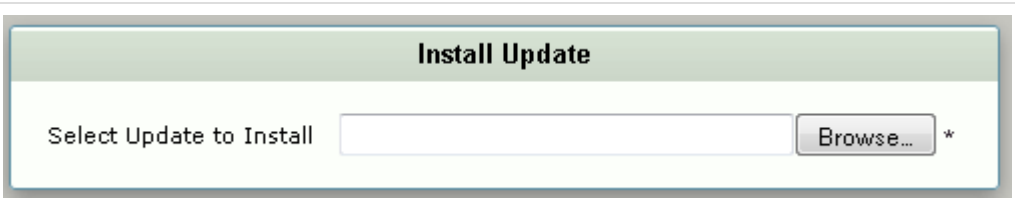


8. When the installation succeeds, the following status message is dispatched:

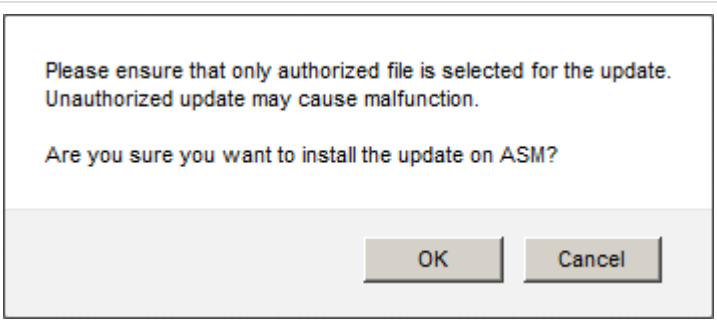


- Should the update be a windows update .pkg pack, refer to the operation status page to initiate windows update install
- If the installation failed a detailed status message indicating the reason for the failure will be displayed

9. In the WebUI, click the **Settings** tab.
10. In the left navigation pane, go to **Application Solution Module > Install ASM Update**.

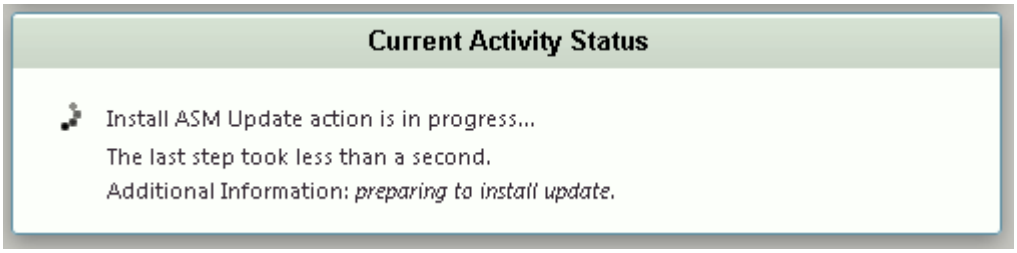


11. Select the ASM **package file** you wish to install
12. Click **OK**
13. You will be presented with the following popup to confirm the action:

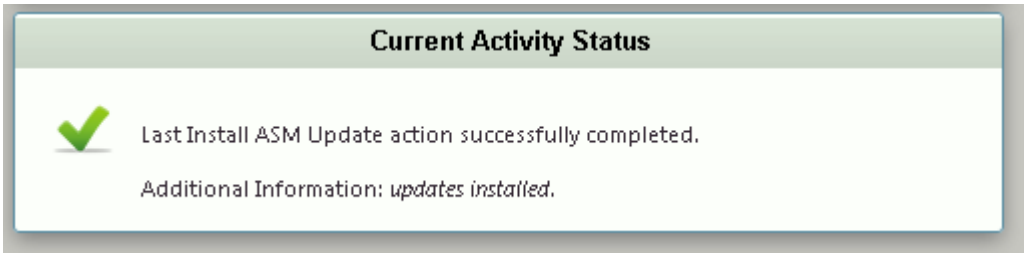


14. Click **OK** to install the package
15. Throughout the installation process, the User interface will dispatch a series of status messages:

Copyright © 2015 Sonus Networks. All rights reserved.



16. When the installation succeeds, the following status message is dispatched:



- Should the update be a windows update .pkg pack, refer to the operation status page to initiate windows update install
- If the installation failed a detailed status message indicating the reason for the failure will be displayed

Verification Tip

- If you have installed a Sonus SBC 1000/2000 Communication Service update, verify the update by Viewing the Sonus SBC 1000/2000 Communication Service Version.
- If you have installed a Lync CU patch, verify the update by checking the versions of each Lync Service.
- For further information in windows update refer to ASM Roll-up Update

Configuring the ASM IP Settings

This operation is used to configure the IP settings for the Application Solution Module (ASM). This is an essential requirement in order to ensure that the Sonus SBC 1000/2000 Communication Service becomes operational.

Important Note

In order for the Sonus SBC 1000/2000 communication service to be operational, the assigned ASM IP address **must be configured** on the same subnet as the Sonus SBC 1000/2000 host. If this has not been done correctly, the only operations that can be performed on the ASM are:

- Hardware Reset of the ASM
- IP Configuration of the ASM (this page)

The Application Solution Module IP Settings can be configured in two different ways:

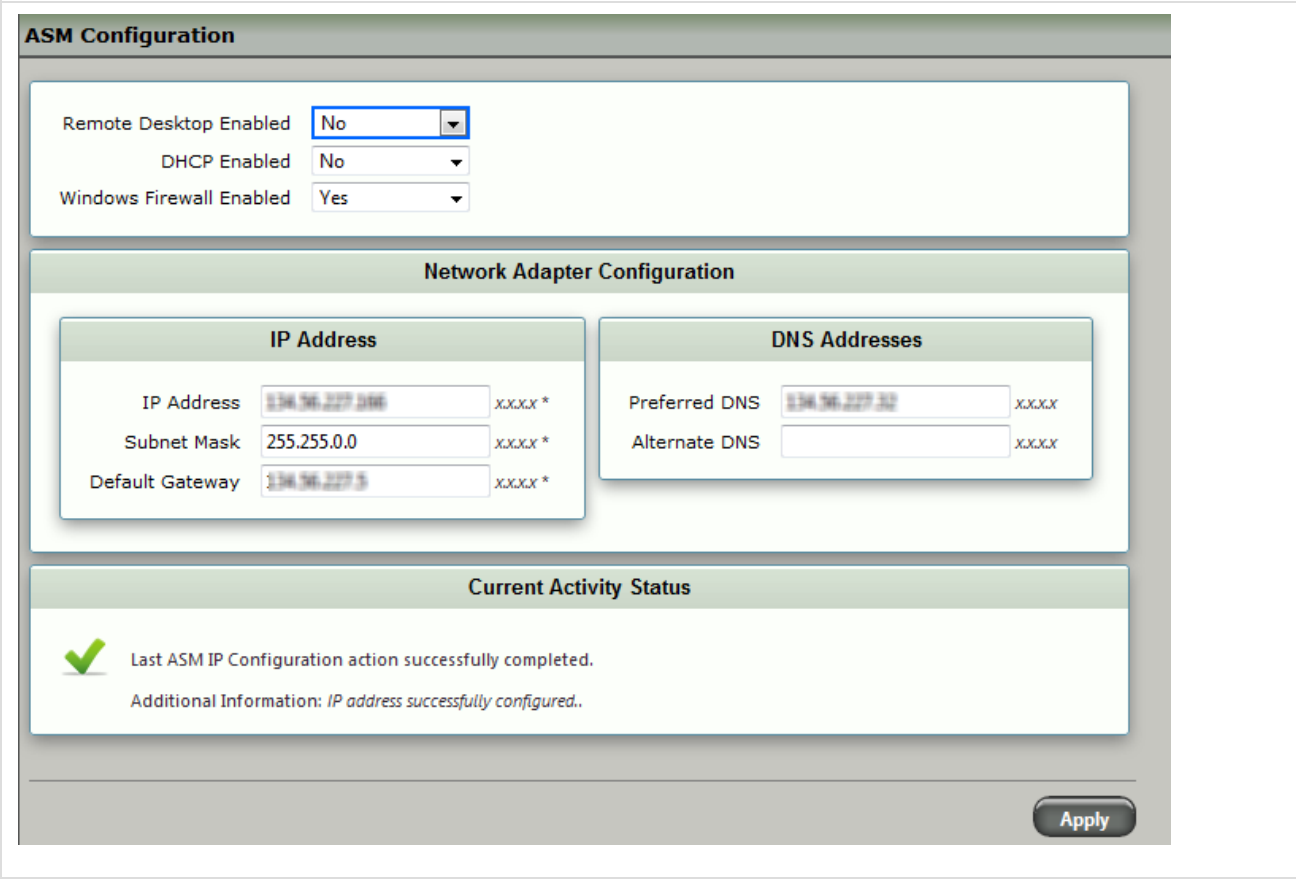
- Configuring the ASM Network Settings with DHCP Disabled
- Configuring the ASM Network Settings with DHCP Enabled

Configuring the ASM Network Settings with DHCP Disabled

Copyright © 2015 Sonus Networks. All rights reserved.

If you wish to statically define the IP address of the ASM, follow these instructions:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > ASM Configuration**.



3. Select **No** from the **DHCP Enabled** menu.
4. Enter the required IP settings
5. A "Configuring IP address" status window will be displayed indicating the progress of the change, the operation typically takes a few seconds.

Configuring the ASM Network Settings with DHCP Enabled

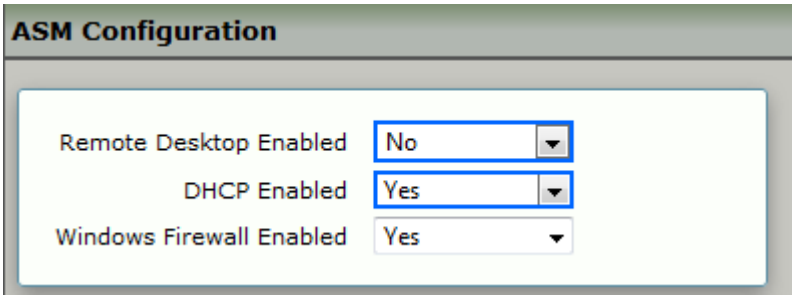
Using DHCP for ASM ip address allows for the ASM to automatically receive an IP address from a DHCP server on the network.

> The IP address assigned by the DHCP server must be on the same subnet as Sonus SBC 1000/2000 in order for Sonus SBC 1000/2000 Communication Service to function, consult with your network administrator to ensure this.
> If there is no DHCP server answering requests, then a 169 addressing scheme will be assigned to the ASM after a timeout period

Once the DHCP address assignment is complete, the IP address assigned to the ASM can be viewed via the Viewing the SBA Operational Status page

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > ASM Configuration**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Select **Yes** from the **DHCP Enabled** menu.
4. A "Configuring IP address" status window will be displayed indicating the progress of the change, the operation typically takes a few seconds to a few minutes depending on the DHCP server answering for queries.

Enabling and Disabling Remote Desktop on the ASM

The Application Solution Module (ASM) can be accessed via Remote Desktop. By default, the ASM is configured with Remote Desktop Disabled. Remote Desktop is typically used only for more advanced system changes on the ASM or troubleshooting is required, and should not be required to perform basic administration and deployment of the Lync SBA.

Never Power Off the ASM via Remote-Desktop

Always power off the ASM via the Sonus SBC 1000/2000 WebUI. If you have mistakenly shutdown the ASM via remote desktop - the only way power the ASM back on is as follows:

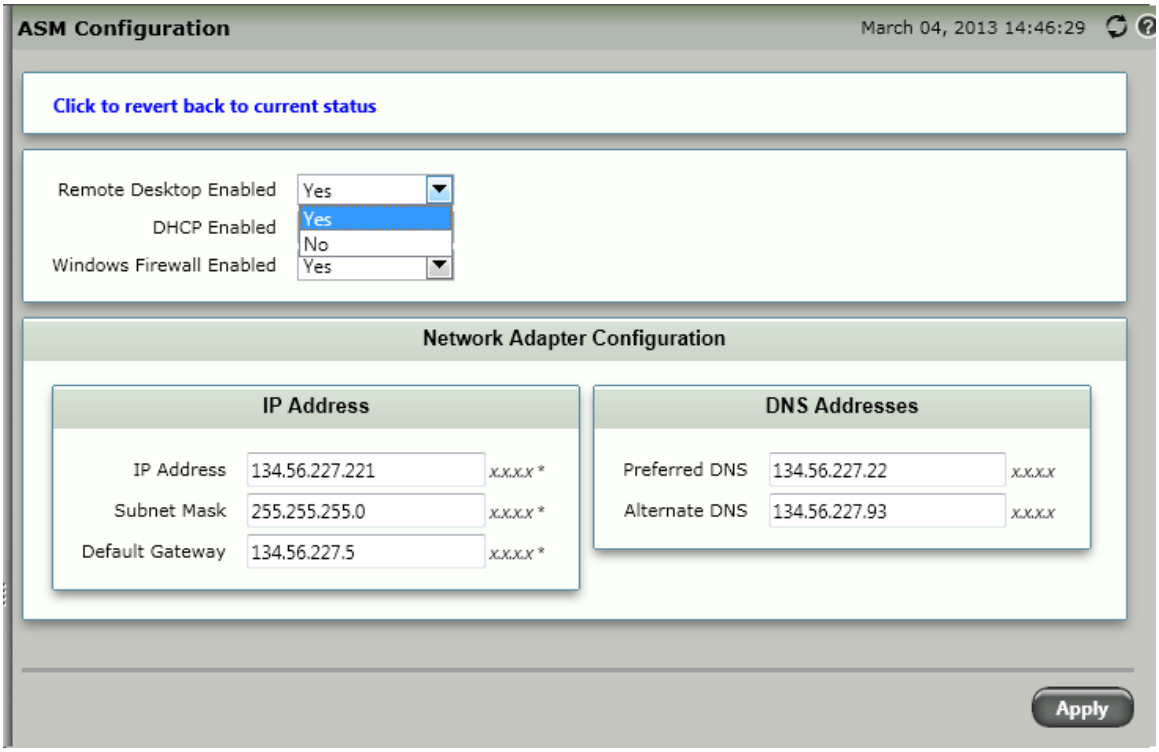
- **Sonus SBC 1000** — Issue an ASM Hardware Reset via the WebUI
- **Sonus SBC 2000** — Physically power-cycle the Sonus SBC 1000/2000 unit

Enabling and Disabling Remote Desktop on the ASM

Before you Begin
This operation can only be performed when the Sonus SBC 1000/2000 Communication service becomes operational. In other words, only when a valid ASM IP address has been configured either via the Initial Setup or the ASM IP Settings.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > ASM Configuration**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Select an option from the **Remote Desktop Enable** menu.

Helpful Tips

If you have not already ioined the ASM to a domain, you can access the ASM with a user defined Administrator Password.

Changing the ASM Admin Password

Before you Begin
This operation can only be performed when the Sonus SBC 1000/2000 Communication service becomes operational. In other words, only when a valid ASM IP address has been configured either via the Initial Setup or the ASM IP Settings.

Sonus SBC 1000/2000 System Administrators can access the Application Solution Module (ASM) directly via Remote Desktop. To do so they will need to login with username "Administrator" and the password defined below.

The ASM's Administrator password can be configured in two different ways:

- Change the Admin Password to User Configured
- Change the Admin Password to System Generated

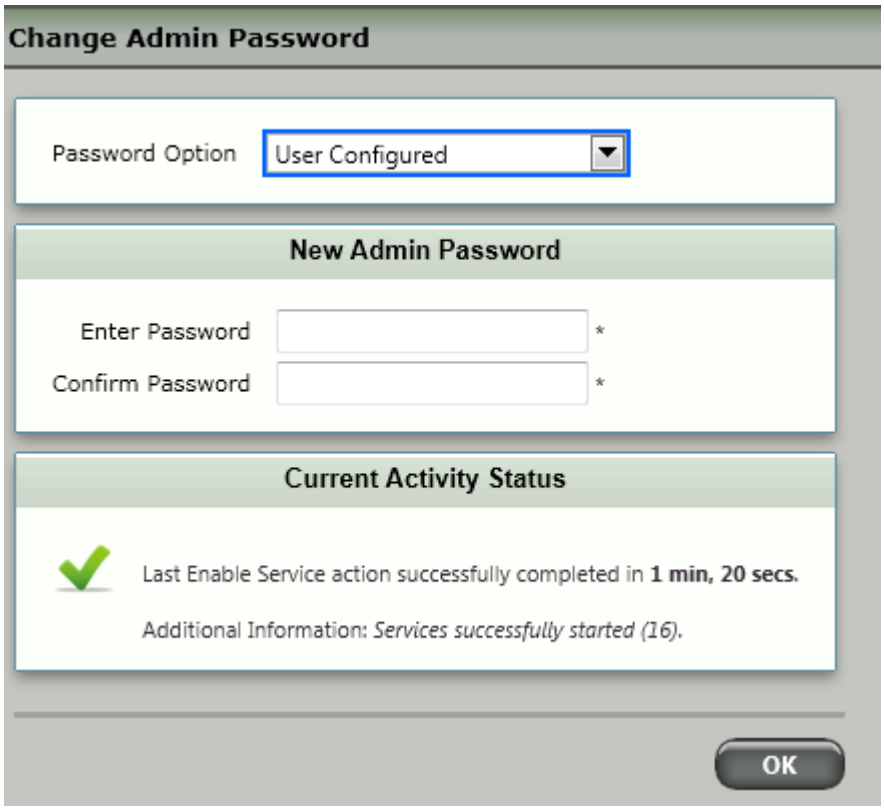
Helpful Tips

- This operation typically takes a few seconds to complete, and the password change takes immediate effect. Note that this operation does not affect a domain-joined ASM since the password is only for the local system administrator account.
- In some cases a domain-joined ASM (depending on the domain controller policies), will rename the administrator account. If this does occur these password change operations will fail, stating that it cannot find the administrator account. Remote Desktop access to the ASM will need to occur via a domain authorized account.

Copyright © 2015 Sonus Networks. All rights reserved.

Change the Admin Password to User Configured

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > Change Admin Password**.
3. Select **User Configured** from the **Password Option**menu.



4. Enter the desired Administrator Password
5. Click **OK**.

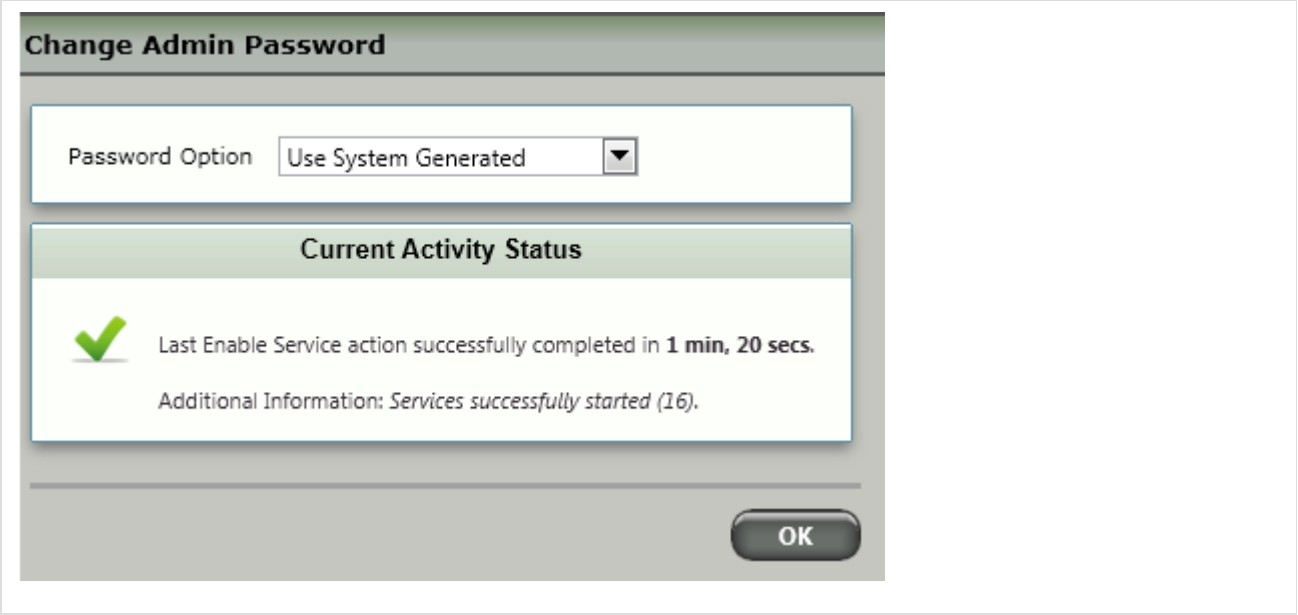
There will be a **Current Activity Status** dialog display indicating the progress and completion of the password change.

Change the Admin Password to System Generated

> This resets the the ASM admin password to the factory system generated password, once this is changed you would need to obtain a the password from TAC or change the password back using a user generated password.
> It is useful to change the password to system generated, if you want to remove local admin access to the device or you are re-preparing it from another deployment.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > Change Admin Password**.
3. Select **Use System Generated** from the **Password Option**menu.

Copyright © 2015 Sonus Networks. All rights reserved.



4. Click **OK**.

There will be a **Current Activity Status** dialog display indicating the progress and completion of the password change.

Rebooting and Resetting the ASM

Should it be necessary, you can reboot or reset the ASM from this task. The Reboot task instructs the ASM operating system to restart (a "clean" reboot), equivalent to rebooting a PC from the Start menu. The Hardware Reset task abruptly resets the ASM (a "dirty" reboot), equivalent to interrupting the power.

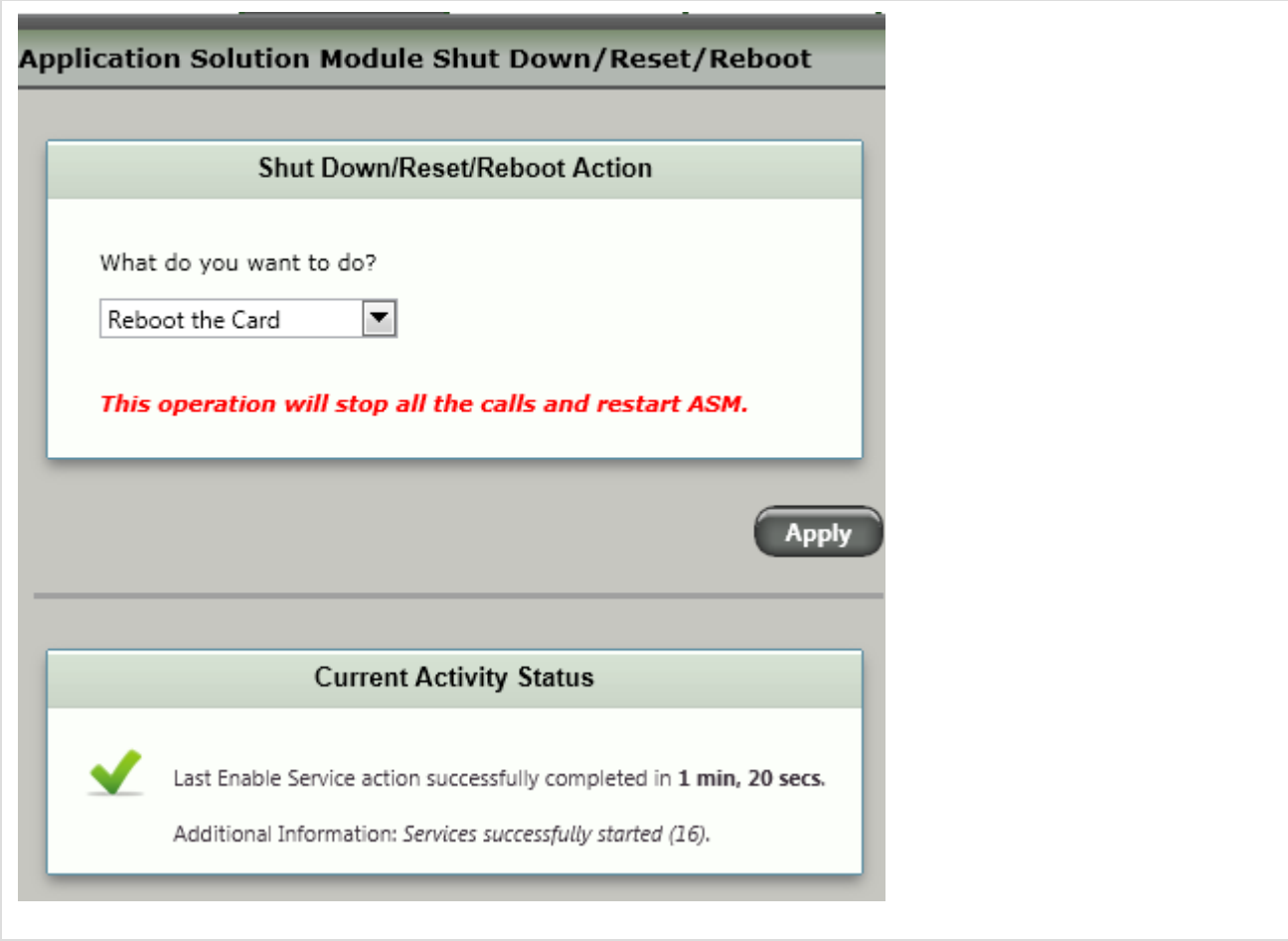
The Reboot option is recommended in all cases, and Reset should only be used when the ASM is not responding to other commands.

Rebooting the ASM

Before you Begin
This operation can only be performed when the Sonus SBC 1000/2000 Communication service becomes operational. In other words, only when a valid ASM IP address has been configured either via the Initial Setup or the ASM IP Settings.

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Application Solution Module**, click **Shut Down/Reset/Reboot**.

Copyright © 2015 Sonus Networks. All rights reserved.



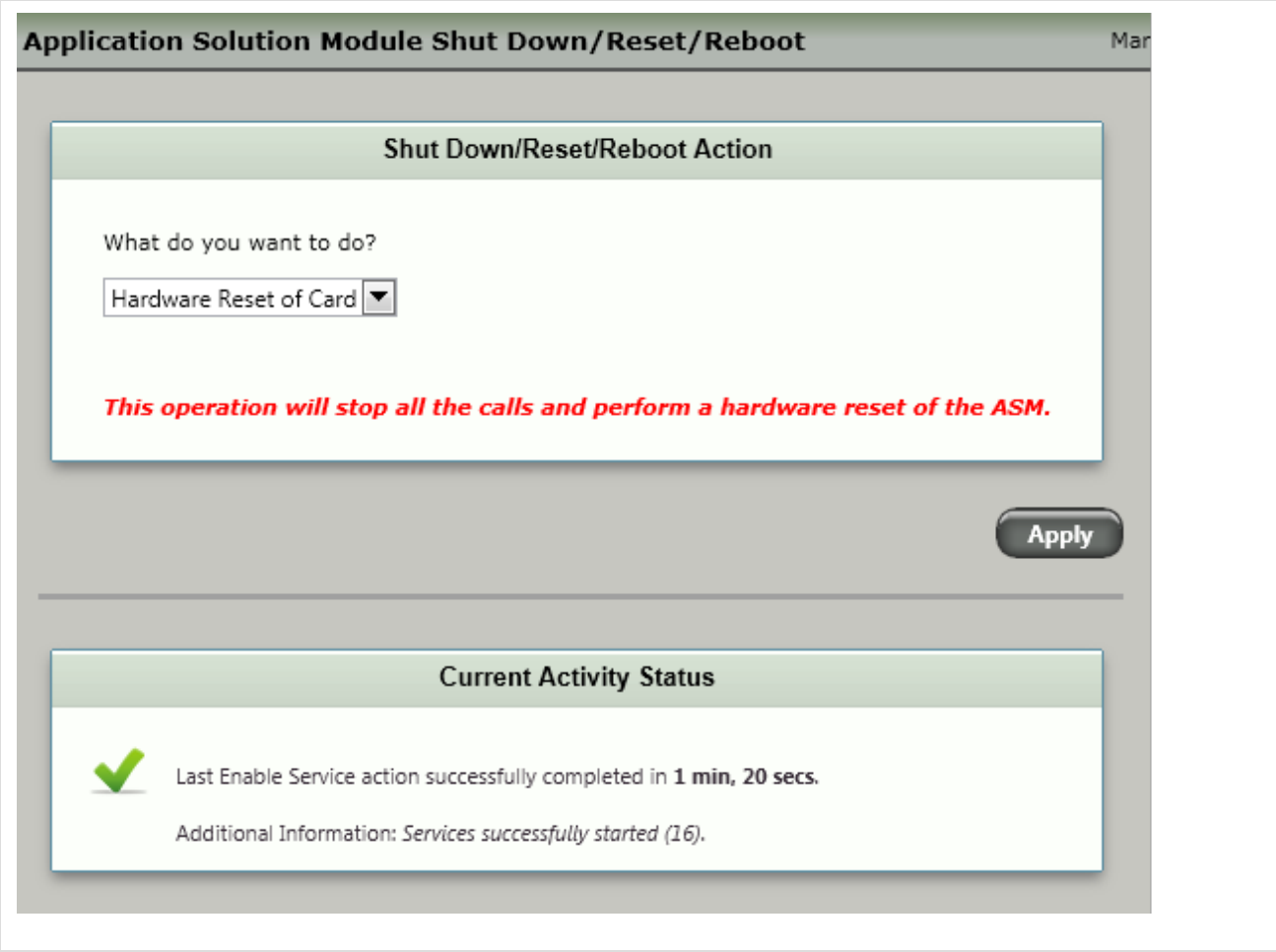
3. Select **Reboot the Card**
4. Click **Apply**

A current activity status window will be displayed until the reboot is complete and the node is reachable

Resetting the ASM

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Application Solution Module**, click **Shut Down/Reset/Reboot**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Select **Hardware Reset of Card**
4. Click **Apply**

A current activity status window will be displayed until the reboot is complete and the card is reachable.

Re-initializing the ASM

The Re-initialize ASM task restores the ASM to an unconfigured state, replacing all software and settings with the image in the Recovery partition of the ASM.

This operation is typically useful when a Lync SBA needs to be re-deployed, for disaster recovery, or as a means of clearing all software and configuration. Sometimes, it is also used in conjunction after Updating the ASM Recovery Partition in order to load updated software onto the ASM.

This operation can also be used to run a different type of image on the ASM to achieve another role. The ASM is shipped running Lync SBA 2013, with the following four images available on the recovery partition:

- Lync 2013 SBA image, which allows use of the ASM as a Survivable Branch Appliance for Lync 2013
- Lync 2010 SBA image, which allows use of the ASM as a Survivable Branch Appliance for Lync 2010
- Lync 2013 RBA image, which allows use of the ASM in a RBA HQ-Side SBC or QoE Agent Server SBC (see Configuring the RBA 3G4G Feature or Configuring the QoE Feature)
- Windows Server image, which allows use of the ASM as a customer-maintained server

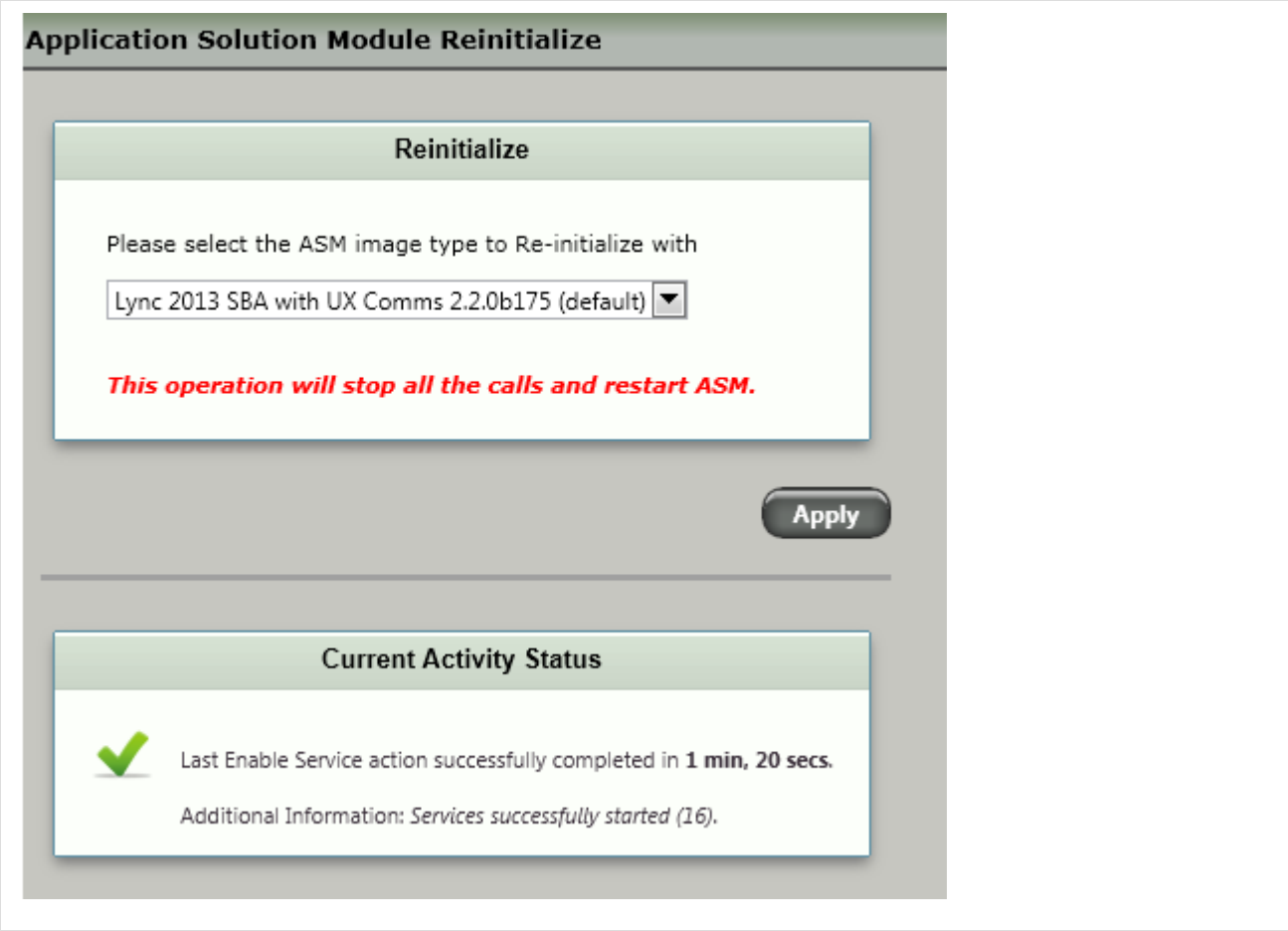
Performing the re-initialization

Copyright © 2015 Sonus Networks. All rights reserved.

Before you Begin
This operation can only be performed when the Sonus SBC 1000/2000 Communication service becomes operational. In other words, only when a valid ASM IP address has been configured either via the Initial Setup or the ASM IP Settings.

This operation is both disruptive (it leaves the ASM unavailable for up to 40 minutes) and destructive (it deletes and replaces all software and configuration on the ASM).

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Application Solution Module**, click **Reinitialize**.



3. Select an image type from the Image Type select list.
4. Click **Apply**

Upon starting the operation, the ASM will become unavailable for up to 40 minutes. It will not provide progress updates (there is no way to see how far along it is), but the **Current Activity Status** panel will report when the operation is complete.

Required Post Actions

After having successfully re-initialized the ASM, you must proceed with the following actions:

1. Upgrading the Sonus SBC 1000/2000 Communication Service Version
2. If you plan to re-deploy the ASM as a Lync SBA,
   a. You must first install the latest Cumulative Updates for Lync SBA
   b. You may skip over the Central Site Tasks in the deployment, and continue starting with the Branch

Copyright © 2015 Sonus Networks. All rights reserved.

Site Tasks.

Viewing and Exporting Windows Event Logs on the ASM

The System Event Log provides a means to view the Windows events occurring on the ASM. This page applies to both the ASM System Event Log facility and the Lync Server Event Log facility. ASM event logs are found in **TASKS > Application Solution Module > System Event Log**, Lync server event logs are found in **TASKS > Lync Survivable Branch Appliance > Lync Server Event Log**. Both event log facilities work in exactly the same manner. For the purposes of this article only the System Event Log facility has been shown.

> ***System Event.evtx*** files are only viewable using the Microsoft Event Viewer. ***Lync Server.evtx*** files are viewable using the Microsoft Event View. However, the textual meaning of the event IDs are only available when viewed using the Microsoft Event Viewer on a Lync server.

Viewing the Event Log

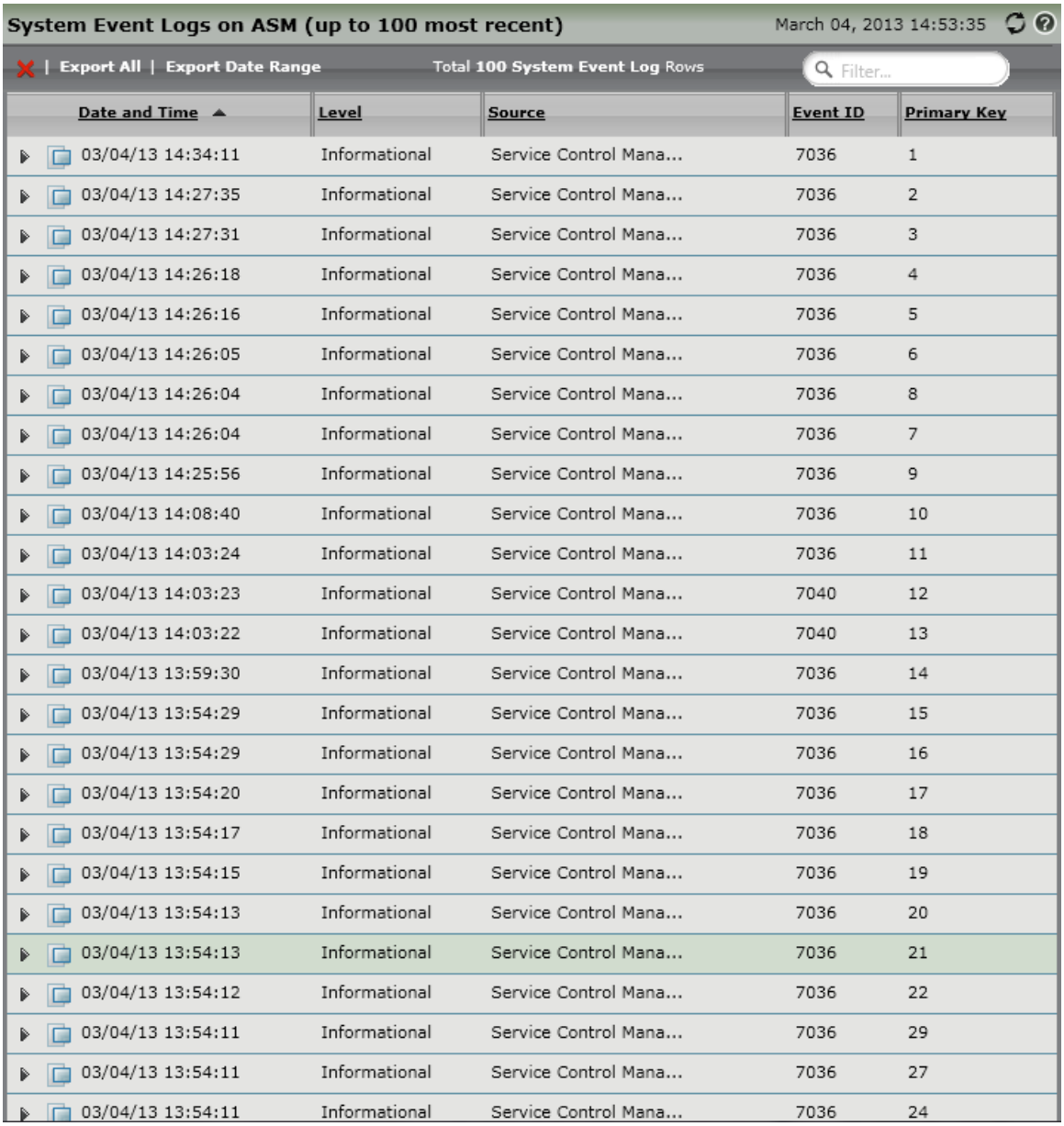
To view the Event Log:

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under **Application Solution Module**, click **System Event Log**.

OR

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > System Event Logs**.

Copyright © 2015 Sonus Networks. All rights reserved.



Date and Time	Level	Source	Event ID	Primary Key
03/04/13 14:34:11	Informational	Service Control Mana...	7036	1
03/04/13 14:27:35	Informational	Service Control Mana...	7036	2
03/04/13 14:27:31	Informational	Service Control Mana...	7036	3
03/04/13 14:26:18	Informational	Service Control Mana...	7036	4
03/04/13 14:26:16	Informational	Service Control Mana...	7036	5
03/04/13 14:26:05	Informational	Service Control Mana...	7036	6
03/04/13 14:26:04	Informational	Service Control Mana...	7036	8
03/04/13 14:26:04	Informational	Service Control Mana...	7036	7
03/04/13 14:25:56	Informational	Service Control Mana...	7036	9
03/04/13 14:08:40	Informational	Service Control Mana...	7036	10
03/04/13 14:03:24	Informational	Service Control Mana...	7036	11
03/04/13 14:03:23	Informational	Service Control Mana...	7040	12
03/04/13 14:03:22	Informational	Service Control Mana...	7040	13
03/04/13 13:59:30	Informational	Service Control Mana...	7036	14
03/04/13 13:54:29	Informational	Service Control Mana...	7036	15
03/04/13 13:54:29	Informational	Service Control Mana...	7036	16
03/04/13 13:54:20	Informational	Service Control Mana...	7036	17
03/04/13 13:54:17	Informational	Service Control Mana...	7036	18
03/04/13 13:54:15	Informational	Service Control Mana...	7036	19
03/04/13 13:54:13	Informational	Service Control Mana...	7036	20
03/04/13 13:54:13	Informational	Service Control Mana...	7036	21
03/04/13 13:54:12	Informational	Service Control Mana...	7036	22
03/04/13 13:54:11	Informational	Service Control Mana...	7036	29
03/04/13 13:54:11	Informational	Service Control Mana...	7036	27
03/04/13 13:54:11	Informational	Service Control Mana...	7036	24

System Event Logs – Field Description

Level

Shows the level of severity of the event. For more information see Event Level Guidelines on the Microsoft MSDN website.

Source

Shows the Windows Service that is source of the event log entry.

Event ID

The Microsoft Event ID associated with the specific cause of the log entry. For more information about Event IDs, see the Microsoft Support Site.

Copyright © 2015 Sonus Networks. All rights reserved.

Primary Key

Internal index for sorting, Sonus use only.

Sorting the Event Log

The Event Logs can be sorted on any of the columns by clicking the column name, i.e., *Date and Time*, *Level*, etc.

The column on which the last sort was performed is indicated by the presence of a sort order arrow (▲▼).

Refreshing and Clearing the Event Log

Refreshing

The Event Log does not update dynamically. Therefore, if you are viewing the log and wish to see any events which have occurred after the System Event Logs page was opened, the view must be refreshed.
To refresh the view:

- Click the **refresh** icon ( ) on the right-hand side of the page, near the top.

Clearing

Clearing the logs removes all the entries from the table.
To clear the event log:

- Click the **Clear Event Log** icon ( ) at the top of the page.

Viewing Event Log Details

To view the details of an event log entry:

- Click the expand icon ( ) at the left-hand side of the entry.

Exporting System Event Logs

Event logs can be exported a Windows Event Log format(.evtx)file. The event log can be exported in whole or by date range.

Exporting All Events

To export all events:

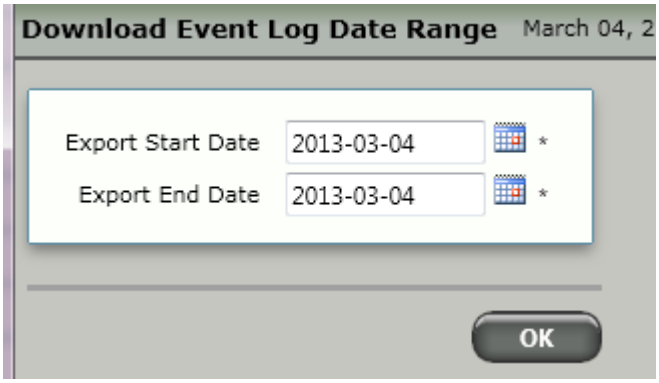
1. Click the **Export All** link at the top of the page.
2. Save the **System Events.evtx** file in a convenient location.

Exporting Events by Date Range

To export events by date range:

1. Click the **Export Date Range**link at the top of the page.

Copyright © 2015 Sonus Networks. All rights reserved.



2. Select the start and end dates from the date picker dialog.
3. Click **OK**.
4. Save the **System Events.evtx**file in a convenient location.

> The start date implies a start time of 00:00:00 and the end date implies an end time of 23:59:59 on the date specified.

Managing the Windows Firewall on the ASM

The SBC 1000/2000 ASM module provides the ability to configure the Windows Firewall on the ASM for incoming traffic. This feature is separate from the SBC 1000/2000 IP Protocol ACLs which may be applied to the ASM Port for inbound and forwarding traffic on the SBC 2000.

By default, inbound connections that do not match a rule are denied and specific rules must be added to allow specific traffic. The order of the rules is not important, network traffic that matches both an active deny and an active allow rule is blocked.

The Windows Firewall can have three types of rules:

- Original Windows rules seen when the ASM is first installed.
- Lync-required rules created when Lync is deployed and SBC-Comms required rules created when the ASM is first installed.
- SBC User-Created rules via the WEBUI.

> **CAUTION**
>
> Sonus highly recommends that the Windows Firewall on the ASM ***never*** be changed via Remote Desktop. Any change made by Remote Desktop on the SBC User-Created rules will be overwritten each time a SBC User-Created rules are modified or added via the WebUI, ASM or SBC chassis restarts.

The Windows Firewall may be turned off in the ASM Configuration page of the UI. While the Windows Firewall is disabled, the SBC User-Created rules Admin State will not be acted on.

SBC User-Created rules can apply to:

- A source IP address.
- A destination IP address.
- A specific protocol.
- A source Port for TCP or UDP protocol.
- A destination Port for TCP or UDP protocol.
- An application hosted inside the ASM.

Copyright © 2015 Sonus Networks. All rights reserved.

WARNING

The following ports are required for the SBC and ASM to communicate, do not Deny one of them:

- UDP 111, 1048 and 2049
- TCP 111

Configuring the ASM Firewall
- Creating and Modifying Windows Firewall Rules

Resetting and Listing Windows Firewall Rules on the ASM

Configuring the ASM Firewall

The feature provides traffic filtering functionality similar to that of the SBC 2000 through the Access Control List feature and provides the same ability to provide layer-3 filtering.

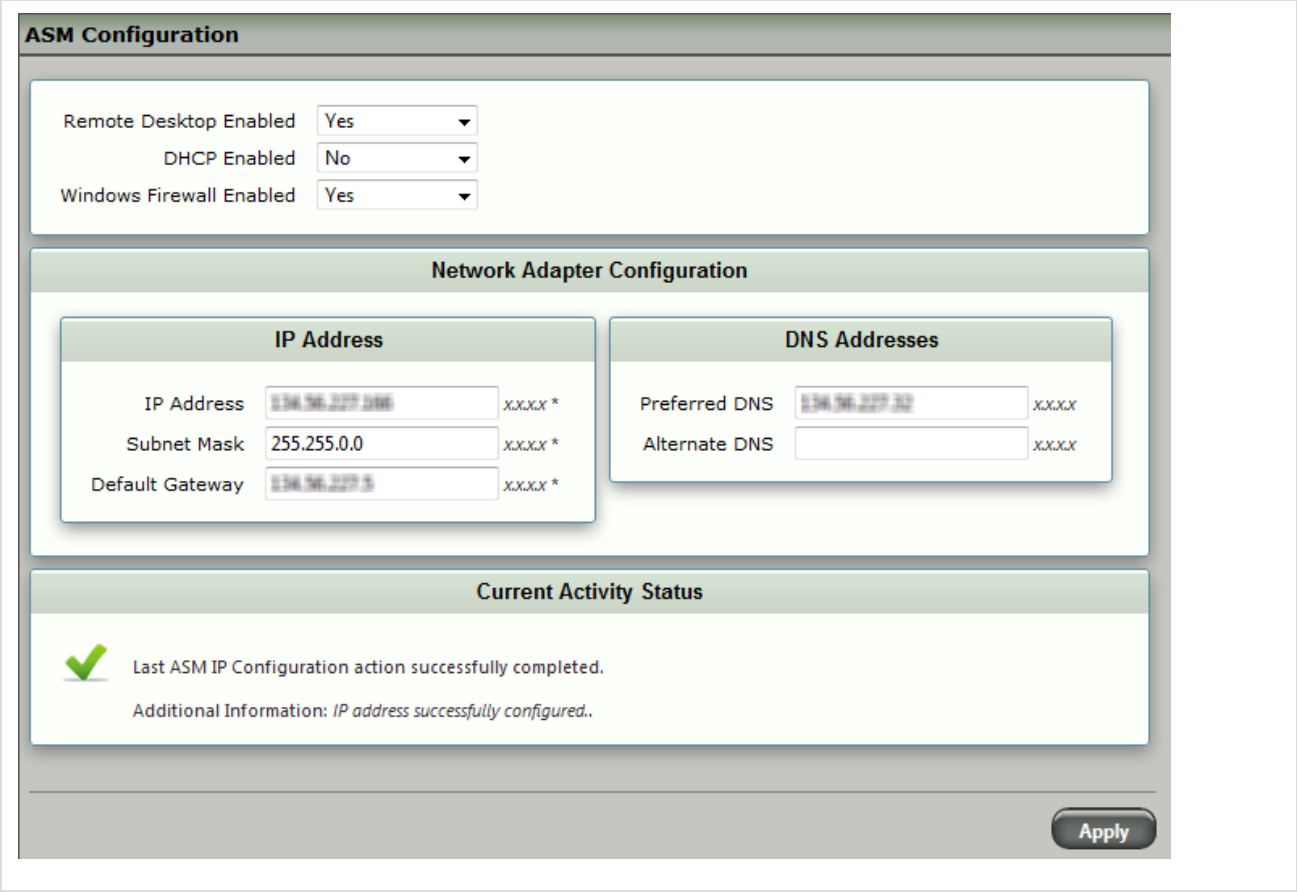
The ASM Firewall feature functions in concert with the native Windows Firewall on the ASM, supplementing the built-in Windows Firewall rules with custom rules defined using this feature. For more information about how the Windows Firewall operates and how rules are applied, see the Managing Windows Firewall with Advanced Security section on the Microsoft Technet site.

Enabling the ASM Windows Firewall

To enable the ASM Windows firewall:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > ASM Configuration**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. In the **Windows Firewall Enabled** list, click "Yes*.
4. Click **Apply**.

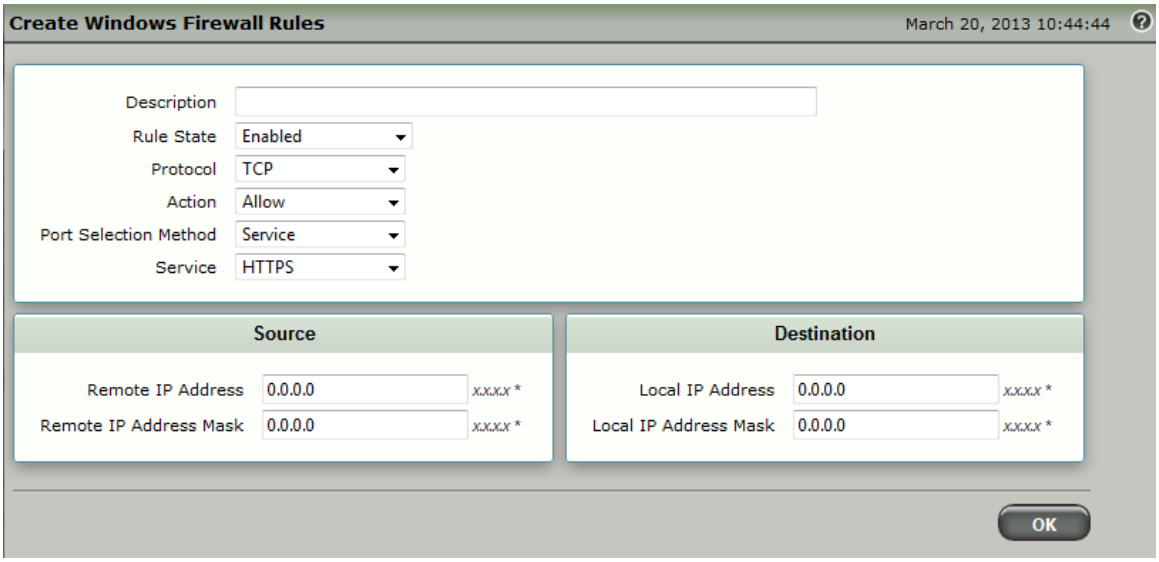
Creating and Modifying Windows Firewall Rules

Creating and Modifying Windows Firewall Rules

To create or modify a Windows Firewall Rule:

1. In the WebUI, click the **Setting** tab.
2. In the left navigation pane, go to **Application Solution Module > Windows Firewall**.

Copyright © 2015 Sonus Networks. All rights reserved.



Modifying a Rule

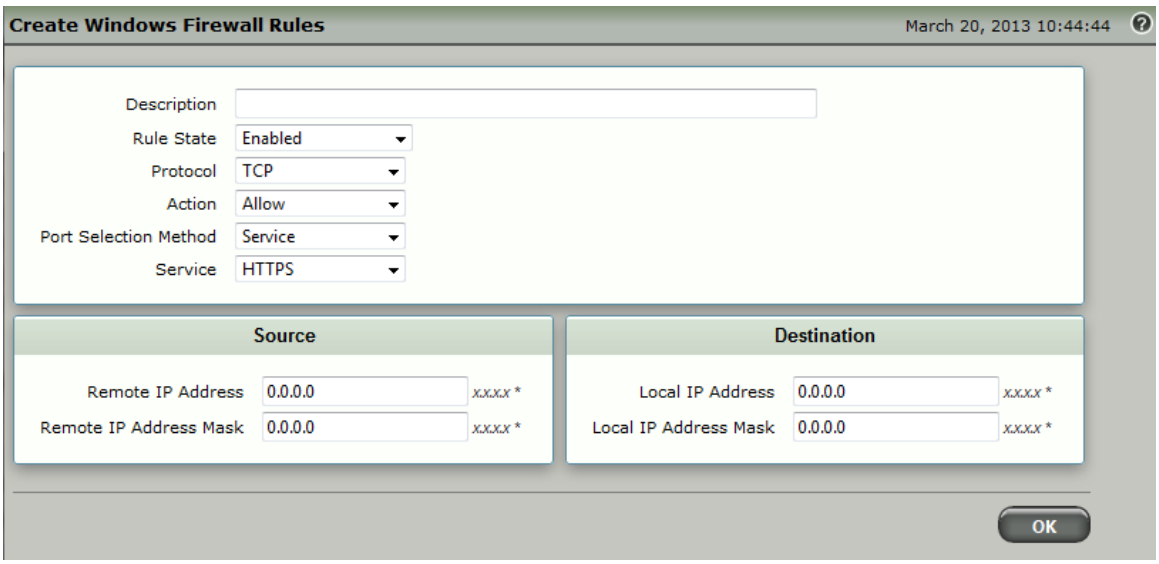
1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating a Rule

To create a rule :

1. Click the **Create a Windows Firewall Rule** ( )icon .



General Information Panel - Field Definitions Description

Copyright © 2015 Sonus Networks. All rights reserved.

A descriptive name for the rule. The name should reflect the purpose of the rule.

Rule State

Specifies whether or not the rule is enabled.

Protocol

Specifies the protocol to which the rule applies.

IANA Protocol Number

The Internet Assigned Numbers Authority (IANA) port number for various protocols. This field is only visible when Custom is selected in the Protocol list box.

Action

Specifies whether the rule allows or denies traffic matching the parameters of the rule.

Port Selection Method

Specified whether Service, Port Range, or Application type is used to select the port. This field is only visible when the Protocol option is TCP or UDP.

Service

Specifies whether the rule is for a particular IP Protocol service, or a range of ports in the IP Protocol, or a Windows application can be specified. This field is only visible when the Protocol option is TCP or UDP.

Application

Specifies the Windows application to which the rule applies. Specify the full path name to the *.exe* file for the application. This field is only visible when **Application** is selected from the **Port Selection Method** list.

Source Panel - Field Definitions Remote IP Address

The IPv4 source address of the packets subject to this rule.

Remote IP Address Mask

The subnet mask of the source IP address.

Remote Port Min.

The minimum port number associated with the source packets subject to this rule. Visible only when **Range** is selected in the **Port Selection Method** list.

Copyright © 2015 Sonus Networks. All rights reserved.

Remote Port Max.

The maximum port number associated with the source packets subject to this rule. Visible only when **Range** is selected in the **Port Selection Method** list.

Destination Panel - Field Definitions Local IP Address

The IPv4 destination address of the packets subject to this rule.

Local IP Address Mask

The subnet mask of the destination IP address.

Local Port Min.

The minimum port number associated with the destination packets subject to this rule.Visible only when **Range** is selected in the **Port Selection Method** list.

Local Port Max.

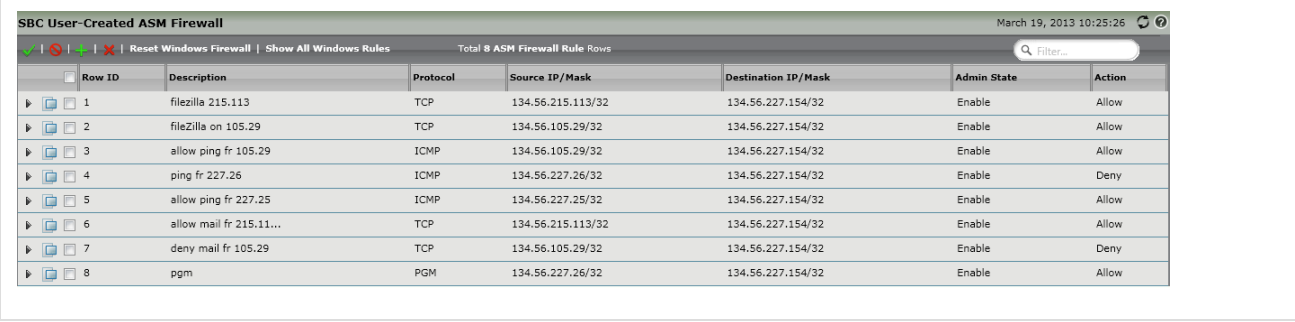
The maximum port number associated with the destination packets subject to this rule. Visible only when **Range** is selected in the **Port Selection Method** list.

Resetting and Listing Windows Firewall Rules on the ASM

Listing Windows Firewall Rules on the ASM

To list the Windows Firewall rules:

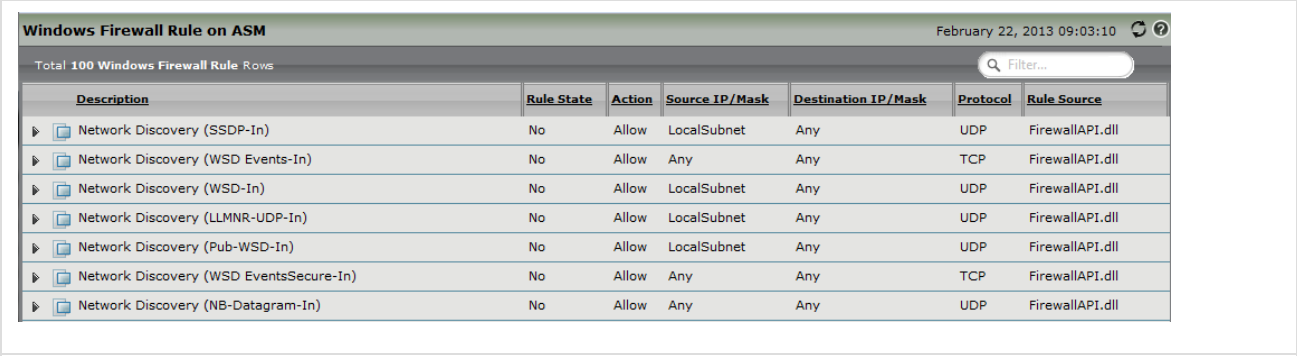
1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, go to **Application Solution Module > Windows Firewall**.



Row ID	Description	Protocol	Source IP/Mask	Destination IP/Mask	Admin State	Action
1	filezilla 215.113	TCP	134.56.215.113/32	134.56.227.154/32	Enable	Allow
2	fileZilla on 105.29	TCP	134.56.105.29/32	134.56.227.154/32	Enable	Allow
3	allow ping fr 105.29	ICMP	134.56.105.29/32	134.56.227.154/32	Enable	Allow
4	ping fr 227.26	ICMP	134.56.227.26/32	134.56.227.154/32	Enable	Deny
5	allow ping fr 227.25	ICMP	134.56.227.25/32	134.56.227.154/32	Enable	Allow
6	allow mail fr 215.11...	TCP	134.56.215.113/32	134.56.227.154/32	Enable	Allow
7	deny mail fr 105.29	TCP	134.56.105.29/32	134.56.227.154/32	Enable	Deny
8	pgm	PGM	134.56.227.26/32	134.56.227.154/32	Enable	Allow

3. Click the **Show All Windows Rules** link at the top of the table.

Copyright © 2015 Sonus Networks. All rights reserved.

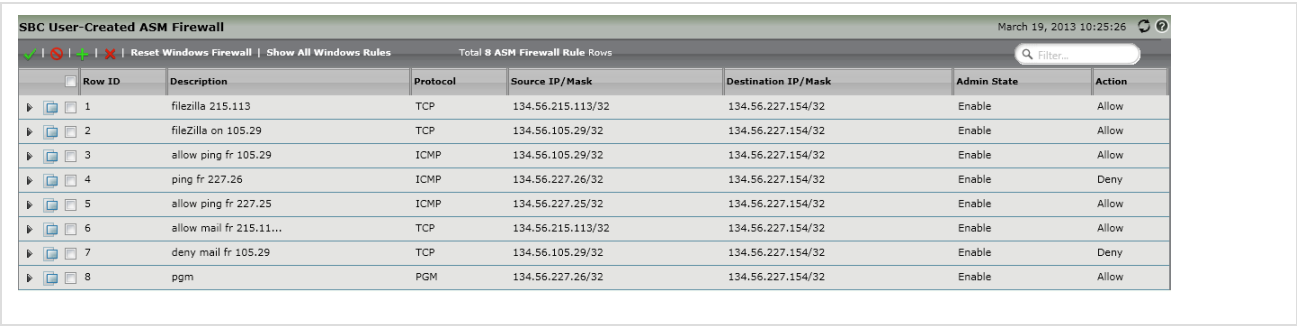


Description	Rule State	Action	Source IP/Mask	Destination IP/Mask	Protocol	Rule Source
Network Discovery (SSDP-In)	No	Allow	LocalSubnet	Any	UDP	FirewallAPI.dll
Network Discovery (WSD Events-In)	No	Allow	Any	Any	TCP	FirewallAPI.dll
Network Discovery (WSD-In)	No	Allow	LocalSubnet	Any	UDP	FirewallAPI.dll
Network Discovery (LLMNR-UDP-In)	No	Allow	LocalSubnet	Any	UDP	FirewallAPI.dll
Network Discovery (Pub-WSD-In)	No	Allow	LocalSubnet	Any	UDP	FirewallAPI.dll
Network Discovery (WSD EventsSecure-In)	No	Allow	Any	Any	TCP	FirewallAPI.dll
Network Discovery (NB-Datagram-In)	No	Allow	Any	Any	UDP	FirewallAPI.dll

Resetting the Windows Firewall Rules

Reset Windows Firewall returns the Windows Firewall to a default state. Any rules required by Lync, or added by applied security templates will be retained. Doing so removes any SBC User-Created rules.
To reset the Windows Firewall:

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, go to **Application Solution Module > Windows Firewall**.



Row ID	Description	Protocol	Source IP/Mask	Destination IP/Mask	Admin State	Action
1	filezilla 215.113	TCP	134.56.215.113/32	134.56.227.154/32	Enable	Allow
2	fileZilla on 105.29	TCP	134.56.105.29/32	134.56.227.154/32	Enable	Allow
3	allow ping fr 105.29	ICMP	134.56.105.29/32	134.56.227.154/32	Enable	Allow
4	ping fr 227.26	ICMP	134.56.227.26/32	134.56.227.154/32	Enable	Deny
5	allow ping fr 227.25	ICMP	134.56.227.25/32	134.56.227.154/32	Enable	Allow
6	allow mail fr 215.11...	TCP	134.56.215.113/32	134.56.227.154/32	Enable	Allow
7	deny mail fr 105.29	TCP	134.56.105.29/32	134.56.227.154/32	Enable	Deny
8	pgm	PGM	134.56.227.26/32	134.56.227.154/32	Enable	Allow

3. Click the **Reset Windows Firewall** link at the top of the table.

Applying an SBA Security Template

This operation is optional allowing SBA administrators to configure the security settings for roles, role services, and features on the SBA. This basically applies security rules to the Windows Server 2008 R2 operating system on the ASM hosting the SBA.

You can do so by either #Applying a Predefined Security Template, or #Importing a Custom Security Template of choice. The following is a list of the main groups of security rules that are modified:

- Microsoft OS Services
- Microsoft OS Networking Firewall
- Microsoft OS Registry Values
- Microsoft OS Audit
- Microsoft OS SCE Templates

Status	Lync SBA Branch Site Tasks
✅	Step 1 - Configuring the ASM IP Settings
✅	Step 2 - Joining the ASM to a Domain
✅	Step 3 - Deploying the SBA
✅	Step 4 - Generate and Import an SBA Certificate

Copyright © 2015 Sonus Networks. All rights reserved.

✅	Step 5 - Starting the SBA Services
Now	Step 6 - Applying an SBA Security Template

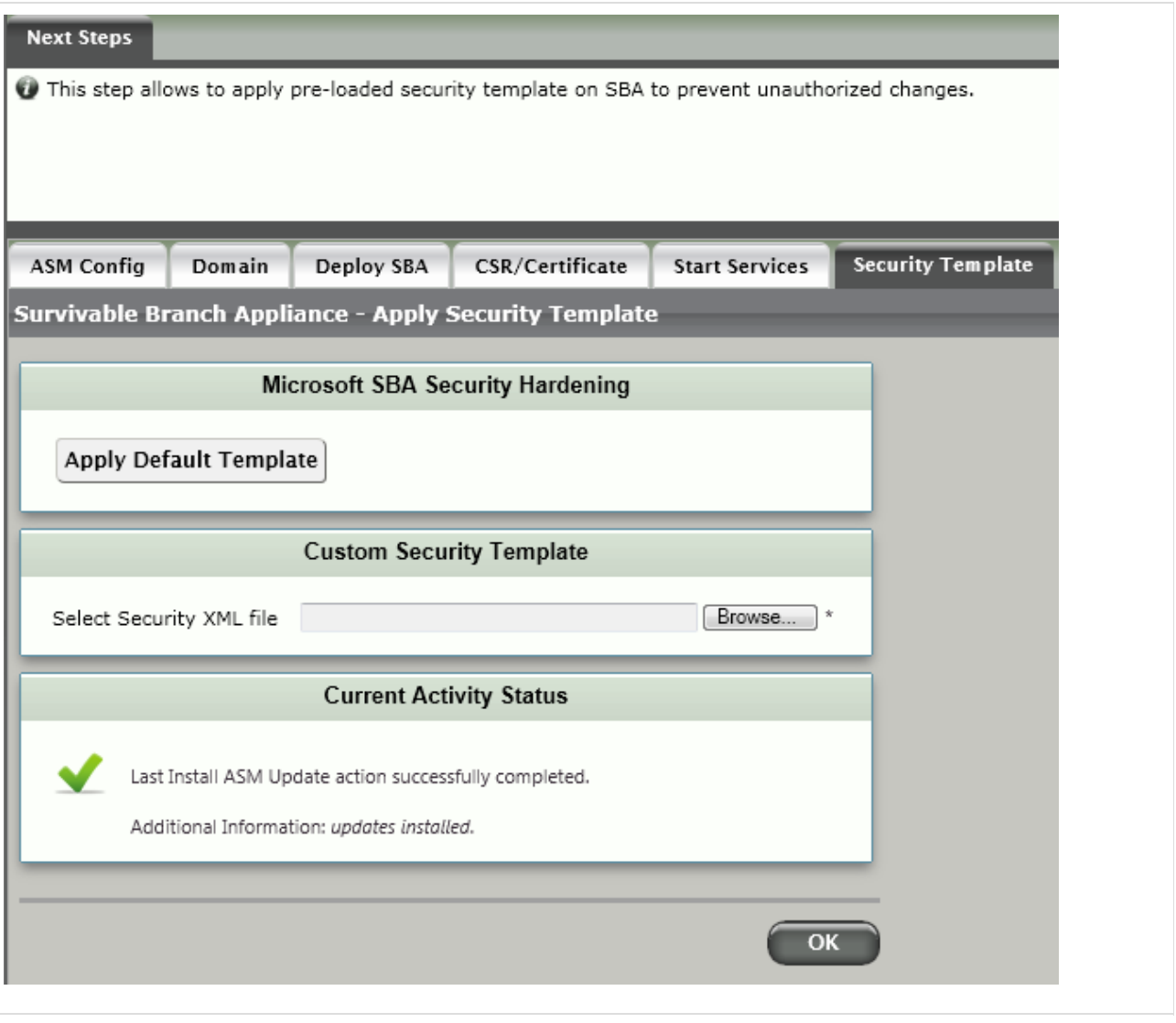
Applying a Predefined Security Template

> ⛔ Once the security template is applied, the action cannot be reversed. In order to disable the security template, the ASM has to be re-initialized.

Below is a summarized list of the primary security settings that will be applied by the stronger security rules template :

- Enables data execution protection
- Enables firewall
- Disables domain users from logging into the ASM
- Enables only local administrator login

1. Click the **Apply Stronger Security Rules Template**.



2. Click **OK**. The operation will take up to to 5 minutes to complete.

Copyright © 2015 Sonus Networks. All rights reserved.

Importing a Custom Security Template

You will need a Windows Server 2008 security template XML file created using the Microsoft Security Configuration Wizard (SCW) to proceed with this operation.

Managing the Lync SBA

The Lync **Survivable Branch Appliance** (SBA) software includes Microsoft Lync Server running on Windows Server 2008 R2 hosted on the Application Solution Module (ASM). The SBA is typically installed in a Branch Office and provides basic voice services to branch users during WAN outage.

Viewing the SBA Operational Status

Installing Cumulative Updates for Lync SBA

Starting and Stopping SBA Services

Importing an SBA Certificate

Exporting an SBA Certificate

Testing a Lync Call

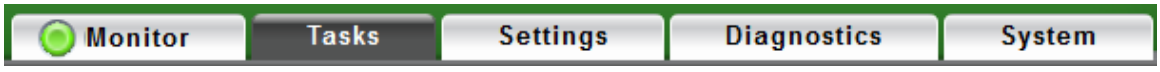
Viewing the SBA Operational Status

The Lync SBA Operation Status view contains the following status panels (from left to right):

1. Status - details the health and runtime status of the ASM.
2. Windows Status - details the host Windows operating system (and the list of currently connected remote desktop users).
3. ASM Roll-up Update Windows Update status - details when update packs need installing.
4. The Sonus SBC 1000/2000 Communication Service shows version and runtime details.
5. The operational status and runtime details of the Lync Services - useful when Deploying the Survivable Branch Appliance:
    - Lync Server, Mediation Service
    - Lync Server, Front-End Service
    - SQL Service
    - Lync Server, Replication

Viewing the SBA Operational Status

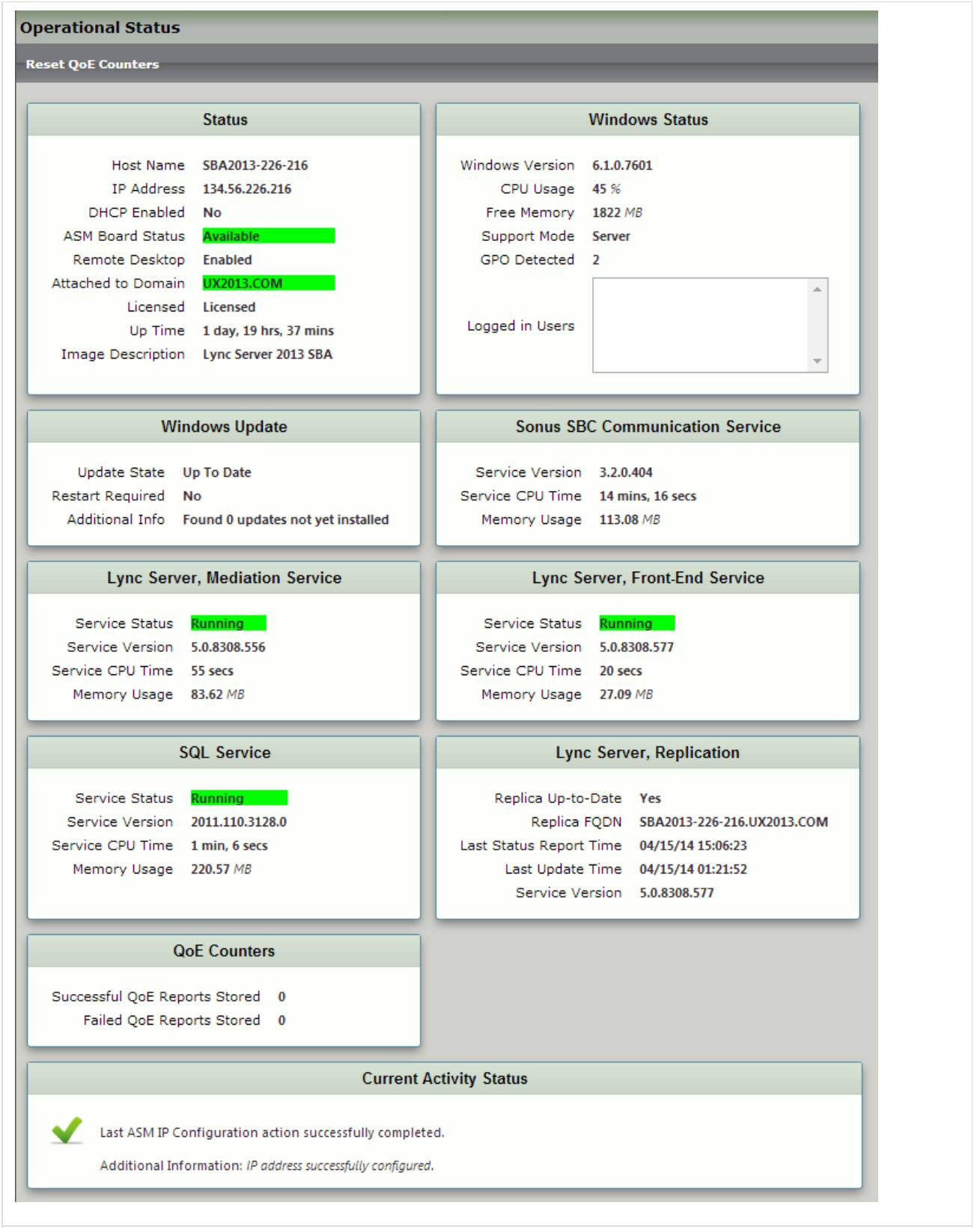
This operation can be accessed either via the Tasks tab or Settings tab:



Viewing the SBA Operation Status through the Tasks Tab

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Lync™ Survivable Branch Appliance**, click **Operational Status**.

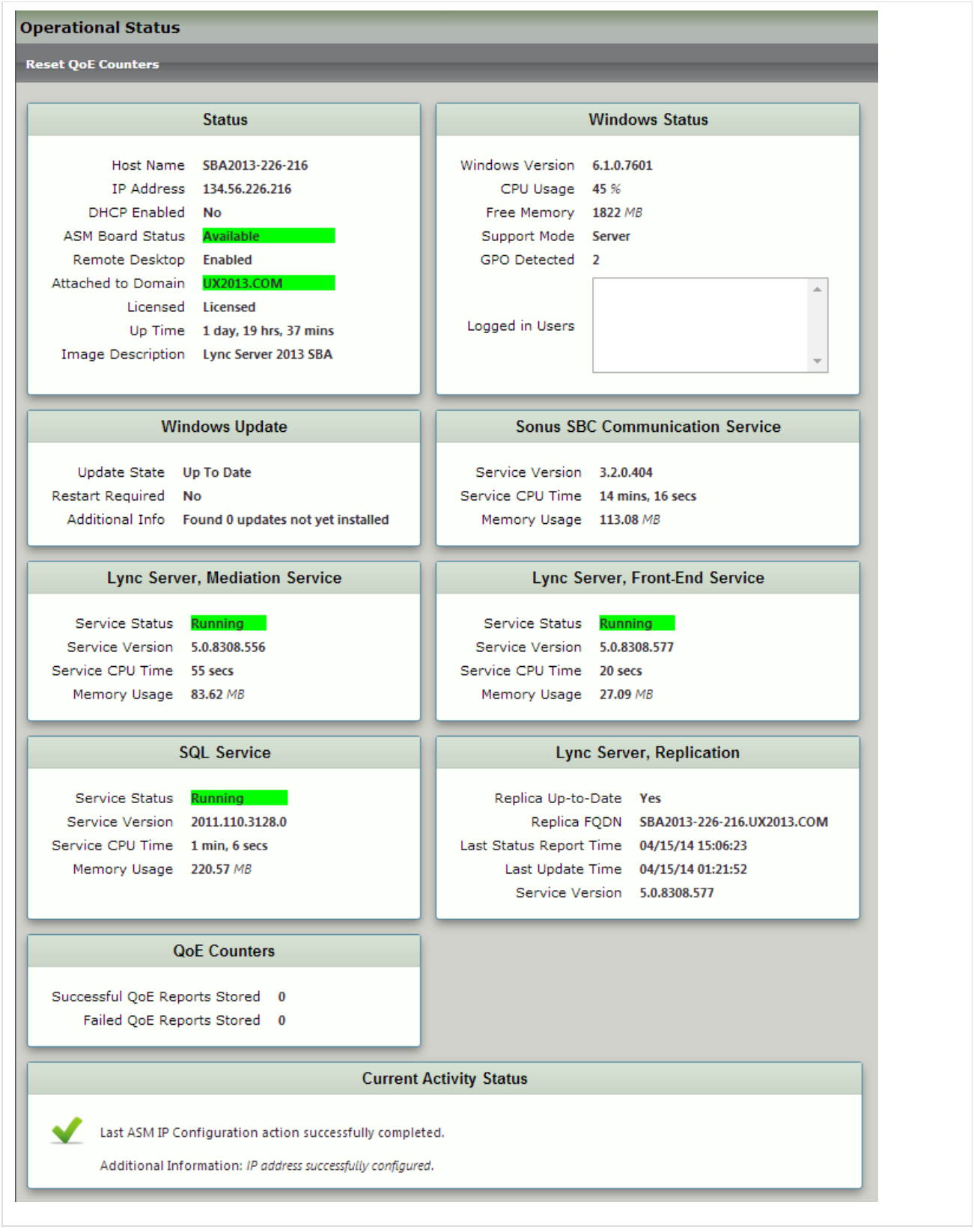
Copyright © 2015 Sonus Networks. All rights reserved.



Viewing the SBA Operation Status through the Settings Tab

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > Microsoft Lync SBA > Operational Status**.

Copyright © 2015 Sonus Networks. All rights reserved.



Installing Cumulative Updates for Lync SBA

When the ASM is deployed as a Lync SBA, it is important that you always install the latest Cumulative Updates (CU) for Lync Server.

Copyright © 2015 Sonus Networks. All rights reserved.

> For Releases prior to 2.2 please refer to the previous release documentation

Installation Step

> **Before you begin**
>
> Your Lync SBA must be fully deployed, and all Lync services must be running before applying the CU.

1. From the Sonus SBC 1000/2000 Download Center, download the latest **SBA-Lync-CU** update `.pkg` file.
2. Install the package by following the instructions outlined in Installing an ASM Package.

Verification Step

You can verify which Cumulative Update was installed for Lync SBA by Viewing the Installed Packages on the ASM. Each cumulative update replaces the following previously released cumulative update. Below is a listing of Lync Services (and their associated version) that are expected to change after applying the CU update:

Checking When No Cumulative Updates are Installed

When Deploying the Survivable Branch Appliance for the first time, the Lync SBA will have no Cumulative Updates to start with. The following services will appear with version of 4.0.7577.**0** which indicates that no updates are installed:

Lync Server 2010 Updates

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**0**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**0**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**0**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**0**

Lync Server 2010 CU2 - April 2011 - Services Updated

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**139**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**139**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**139**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**139**

Lync Server 2010 CU3 - July 2011 - Services Updated

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**139** — remains the same as CU2
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**166**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**166**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**166**

Lync Server 2010 CU4 - November 2011 - Services Updated

Copyright © 2015 Sonus Networks. All rights reserved.

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**183**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**183**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**183**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**183**

Lync Server 2010 CU5 - February 2012 - Services Updated

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**183**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**190**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**190**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**190**

Lync Server 2010 CU6 - June 2012 - Services Updated

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**183**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**199**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**199**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**199**

Lync Server 2010 CU7 - October 2012 - Services Updated

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**183**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**205**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**203**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**203**

Lync Server 2010 CU8 - March 2013 - Services Updated

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**183**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**216**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**216**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**216**

Lync Server 2010 CU9 - July 2013 - Services Updated

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**183**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**217**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**217**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**217**

Lync Server 2010 CU10 - October 2013 - Services Updated

Copyright © 2015 Sonus Networks. All rights reserved.

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**183**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**223**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**223**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**217**

Lync Server 2010 CU11 - January 2014 - Services Updated

1. Microsoft Lync Server 2010, Mediation Server 4.0.7577.**183**
2. Microsoft Lync Server 2010, Core Components 4.0.7577.**225**
3. Microsoft Lync Server 2010, Front End Server 4.0.7577.**225**
4. Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit 4.0.7577.**217**

Lync Server 2013 Updates

Lync Server 2013 CU1 - February 2013 - Services Updated

1. Microsoft Lync Server 2013, Mediation Server 5.0.8308.**291**
2. Microsoft Lync Server 2013, Core Components 5.0.8308.**291**
3. Microsoft Lync Server 2013, Front End Server 5.0.8308.**291**
4. Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit 5.0.8308.**291**

Lync Server 2013 CU2 - July 2013 - Services Updated

1. Microsoft Lync Server 2013, Mediation Server 5.0.8308.**291**
2. Microsoft Lync Server 2013, Core Components 5.0.8308.**420**
3. Microsoft Lync Server 2013, Front End Server 5.0.8308.**420**
4. Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit 5.0.8308.**420**

Lync Server 2013 CU3 - October 2013 - Services Updated

1. Microsoft Lync Server 2013, Mediation Server 5.0.8308.**556**
2. Microsoft Lync Server 2013, Core Components 5.0.8308.**556**
3. Microsoft Lync Server 2013, Front End Server 5.0.8308.**556**
4. Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit 5.0.8308.**556**

Lync Server 2013 CU4 - January 2014 - Services Updated

1. Microsoft Lync Server 2013, Mediation Server 5.0.8308.**556**
2. Microsoft Lync Server 2013, Core Components 5.0.8308.**577**
3. Microsoft Lync Server 2013, Front End Server 5.0.8308.**577**
4. Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit 5.0.8308.**577**

Lync Server 2013 CU5 - August 2014 - Services Updated

Copyright © 2015 Sonus Networks. All rights reserved.

1. Microsoft Lync Server 2013, Mediation Server 5.0.8308.**556**
2. Microsoft Lync Server 2013, Core Components 5.0.8308.738
3. Microsoft Lync Server 2013, Front End Server 5.0.8308.7**33**
4. Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit 5.0.8308.726

Lync Server 2013 CU6 - September 2014 - Services Updated

1. Microsoft Lync Server 2013, Mediation Server 5.0.8308.**556**
2. Microsoft Lync Server 2013, Core Components 5.0.8308.**815**
3. Microsoft Lync Server 2013, Front End Server 5.0.8308.**815**
4. Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit 5.0.8308.**815**

Related Articles

- When installing cumulative updates for Lync SBA, can we skip CUs in between?

Starting and Stopping SBA Services

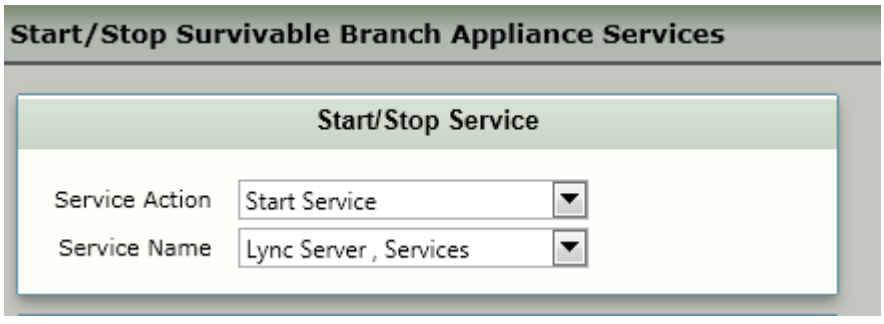
This operation allows you to start and stop the following SBA services from the WebUI:

- Lync Server 2010 Services:
  - Mediation Service
  - Front-End Service
- Remote Desktop Service for the ASM

> If stopped, the Remote Desktop service will start after the ASM is restarted only if it is configured as enabled in the ASM IP settings.

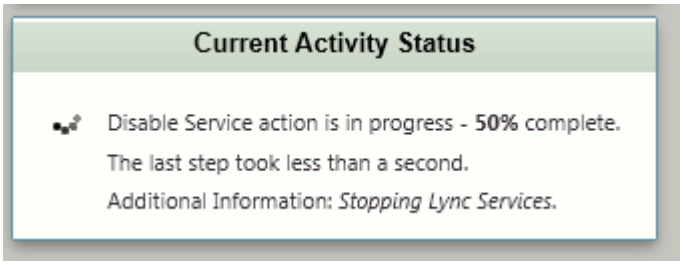
Starting and Stopping an SBA Service

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Lync™ Survivable Branch Appliance**, click **Start/Stop Services**.

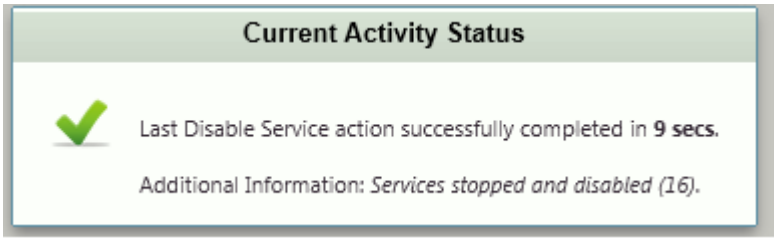


3. In the **Service Action**, select the desired operation
4. In the **Service Name**, select the service you wish to start/stop
5. Click **OK**- the following status messages will be dispatched:
   a. The operation being applied on the ASM:

Copyright © 2015 Sonus Networks. All rights reserved.



b. The operation completes:



Importing an SBA Certificate

When Deploying the Survivable Branch Appliance, the **Branch Site Tasks** requires to Generate and Import an SBA Certificate. If you do not wish to send the signing request automatically to a **Windows Certificate Authority**, and would rather send it to a Trusted CA of your choice, then you'll need to import the signed certificate manually as outlined on this page.

Importing a Signed SBA Certificate

There are two types of certificates that can be imported:

- X.509 Signed Certificate
- PKCS12 Certificate and Key

> Before importing a new Signed Server Certificate, you must first import a valid Trusted CA Certificate.

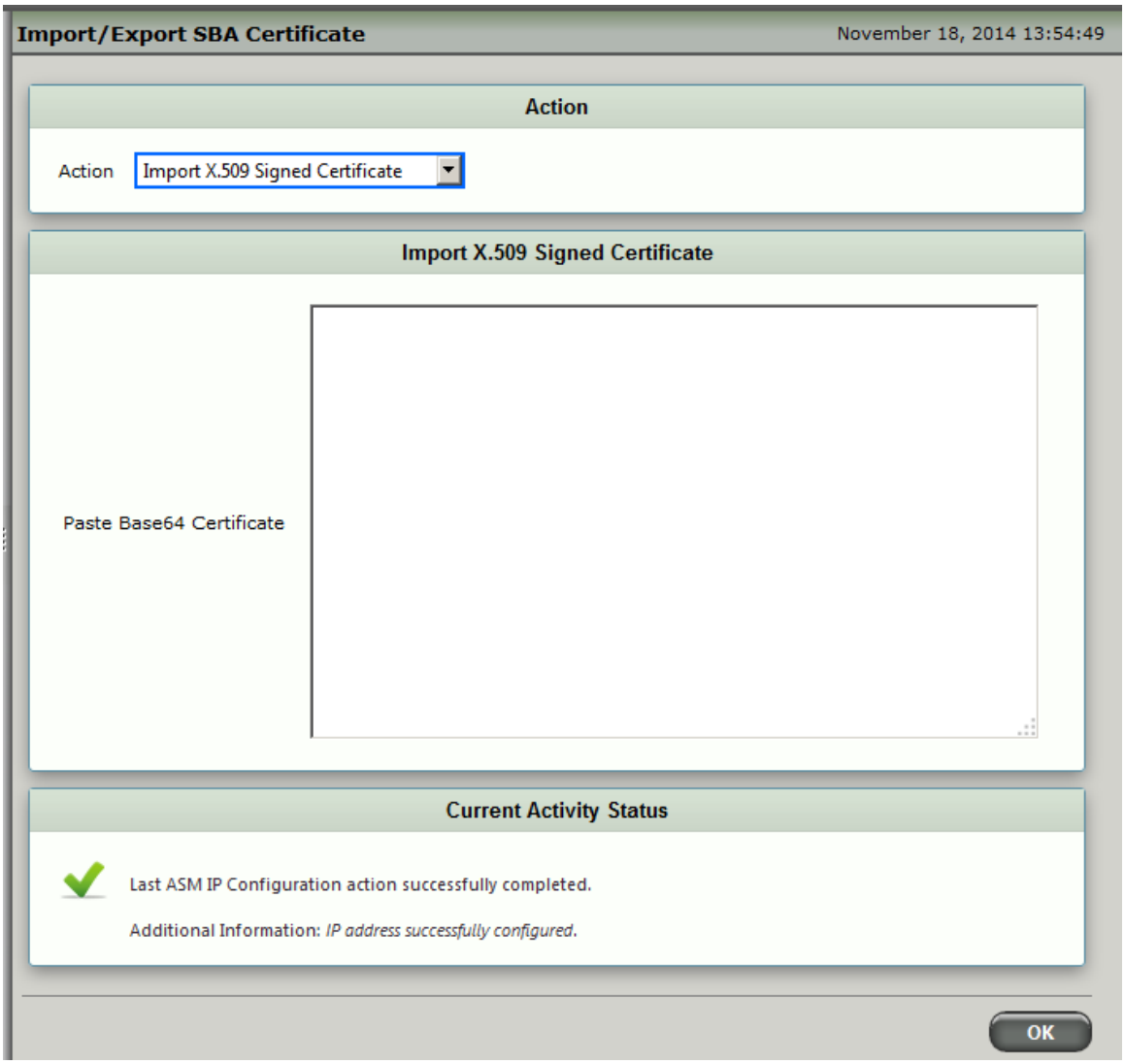
> If your node has a SHA-2 256 signed server certificate, the SBC will not interoperate with Lync 2010 or earlier OCS/Lync versions. The signature algorithm (sha256WithRSAEncryption) is shown in the Certificate panel of the Sonus SBC Certificate page in the UI.

> **SHA2-256 Certificate Compatibility**
>
> SHA2-256 CA Certificates may be used for the SBA, SBC, and Lync 2013 Servers. Lync 2010 requires that all devices employ ALL SHA1 Certificates. For more information see the Microsoft SHA1 Deprecation Policy .

Import X.509 Signed Certificate

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under **Lync™ Survivable Branch Appliance**, click **SBA Certificate.**
3. From the **Action** drop down list, select **Import X.509 Signed Certificate.**

Copyright © 2015 Sonus Networks. All rights reserved.



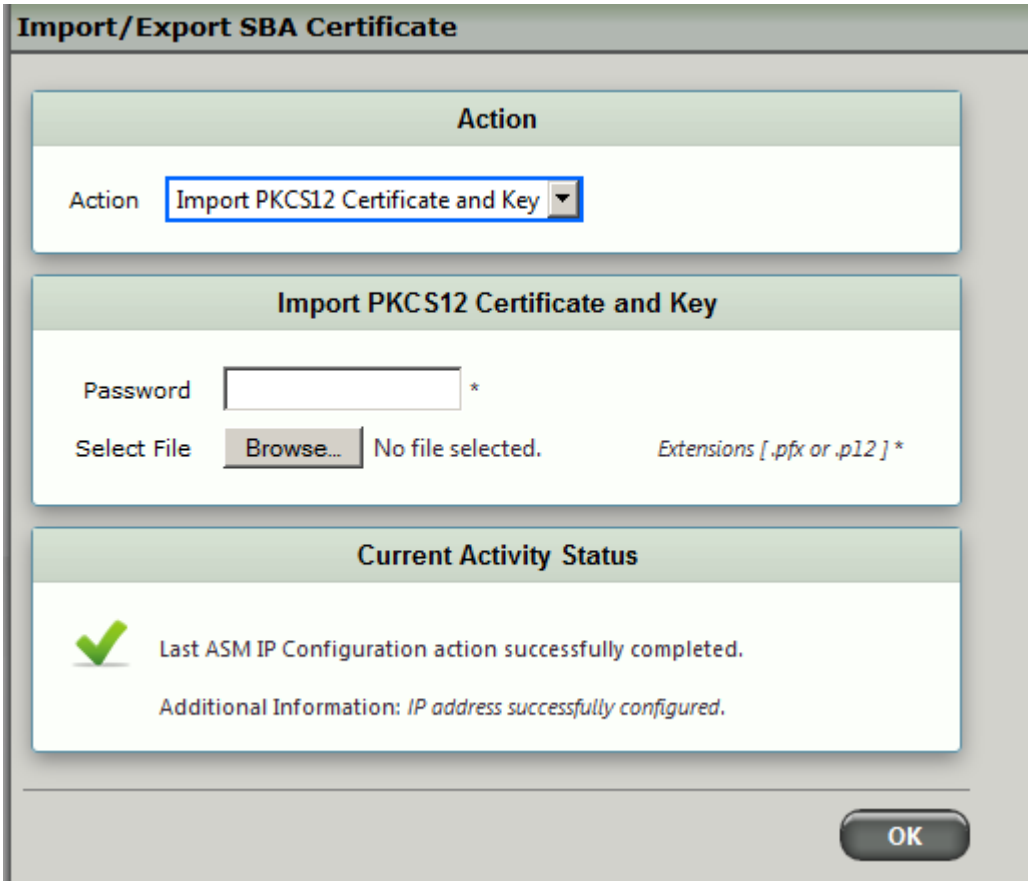
4. Paste the **Base 64** format signed certificate.
5. Click **OK**.

Import PKCS12 Certificate and Key

> **Before you begin:** This operation requires that you paste in a **Base 64 format** Signed Certificate.

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under **Lync™ Survivable Branch Appliance**, click **SBA Certificate.**
3. From the **Action** drop down list, select **Import PKCS12 Certificate and Key.**

Copyright © 2015 Sonus Networks. All rights reserved.



4. In the **Password** field, enter the same password you created to export the certificate. See Exporting an SBA Certificate.
5. Click **Browse** and select the desired PKCS12 file and key.

> You must use the same password as you used to export the certificate and key. See Exporting an SBA Certificate.

6. Click **OK**.

Exporting an SBA Certificate

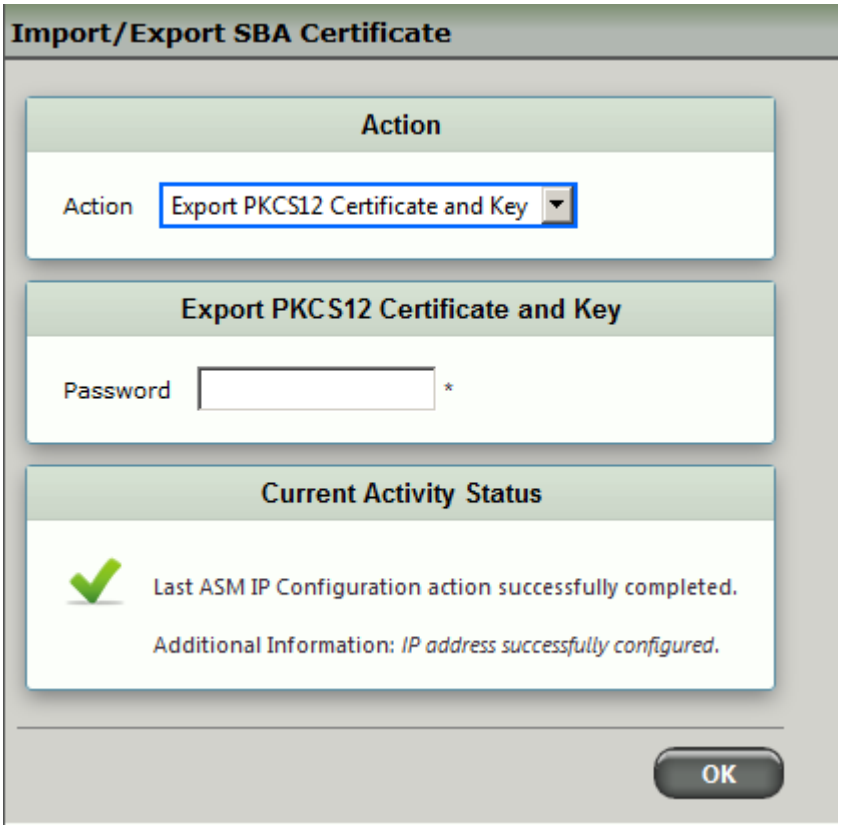
You can export the existing certificate installed on the Sonus SBA at anytime by following these simple steps:

Exporting a Signed SBA Certificate

You are able to export a **PKCS12 Certificate and Key** as follows:

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under **Lync™ Survivable Branch Appliance**, click **SBA Certificate.**
3. From the **Action** drop down list, select **Export PKCS12 Certificate and Key.**

Copyright © 2015 Sonus Networks. All rights reserved.



4. In the **Password** box, enter the password. See Importing an SBA Certificate.

> The password is user generated/supplied. This will be required when Importing an SBA Certificate fo r this certificate on another node.

5. Click **OK**.

Testing a Lync Call

This task allows you to initiate a simple test call from Lync SBA (via the Front End Service itself) to the Sonus SBC 1000/2000 gateway. The purpose of the test is to exercise the gateway's connectivity and call routing setup. This call is initiated by internally invoking the `Test-CSPstnOutboundCall` via the Lync powershell on the ASM.

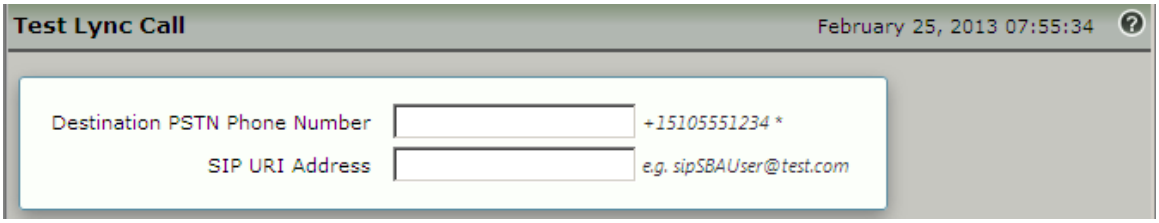
Unlike the plain Testing a Call operation, this functionality initiates the call from the Lync SBA and not from within the Sonus SBC 1000/2000 itself.

Testing a Lync Call

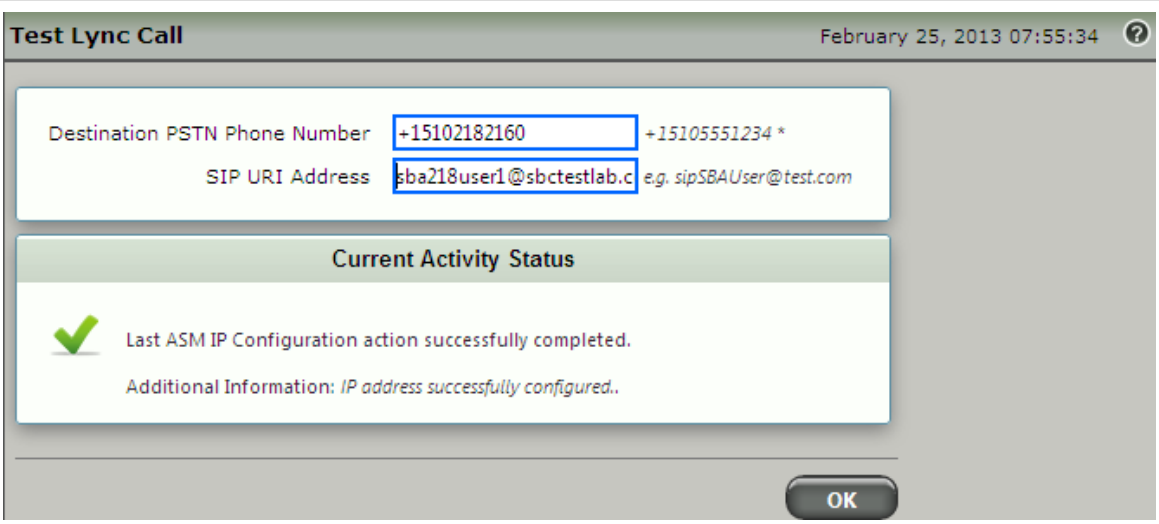
> **Before you begin:** It is assumed that:
>
> 1. The Lync SBA is deployed
> 2. The Sonus SBC 1000/2000 and Lync 2010 are deployed with a PSTN Provider

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Lync™ Survivable Branch Appliance**, click **Test Lync™ Call**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Enter the **Destination PSTN Phone Number** and the **optionally the SIP URI Address**



- The **PSTN Phone Number** is mandatory and should be in an E.164 format matching the Lync default dial plan.
- The **SIP URI Address** is an optional parameter. If used, it must be a valid user ID configured on the Lync server.

1. click **OK**

Expected Outcome

The system will place a call from the Lync SBA to the Sonus SBC 1000/2000 and expect the call to be routed via the PSTN number provided. Once the number is physically answered by a user, the call will automatically hang up and the webUI will return success. **Note that no audio will be sent from the Lync SBA** - the intent is to simply test the signalling and routing.

If the phone is never answered it will eventually timeout and return an error. Similarly, an error will immediately return if either the Lync SBA and/or Sonus SBC 1000/2000 have a misconfiguration or routing problem.

Managing the SBC Communication Service

The **SBC Communication Service** is a Sonus-based application installed on the Application Solution Module (ASM) allowing communication to be sent and received between the Sonus SBC 1000/2000 software and the ASM.

All ASM-related functions operated via the Sonus SBC 1000/2000 Web Interface are sent via the Sonus SBC 1000/2000 Communication Service.

Viewing the SBC Communication Service Version

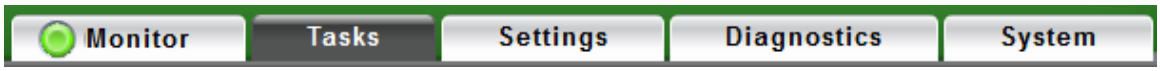
Upgrading the SBC Communication Service Version

Copyright © 2015 Sonus Networks. All rights reserved.

Viewing the SBC Communication Service Version

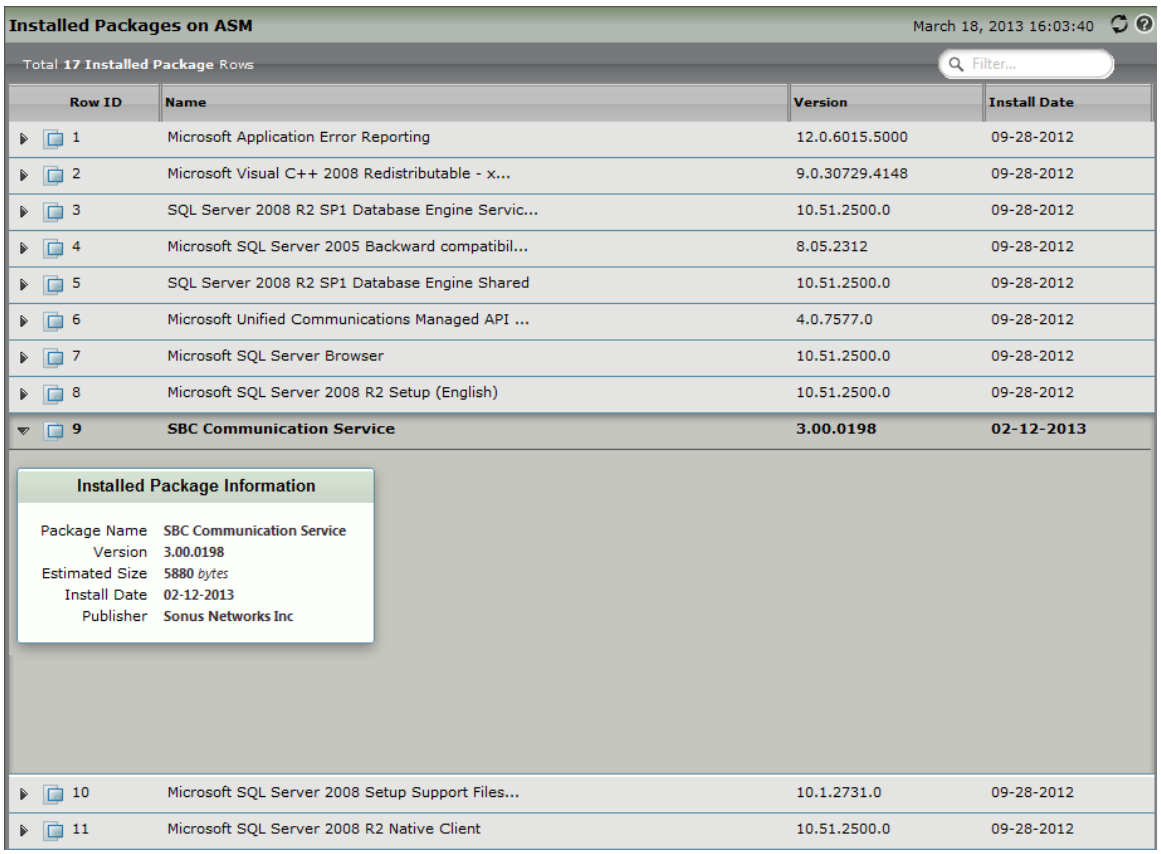
The Application Service Module (ASM) communicates with the Sonus SBC 1000/2000 system using a **SBC Communication Service**. This page describes how you can view the Sonus SBC 1000/2000 Communication Service's property detail including its current version:

This operation can be accessed either via the **Tasks** tab or the **Settings** tab:



Viewing the SBC Communications Service Version through the Tasks tab

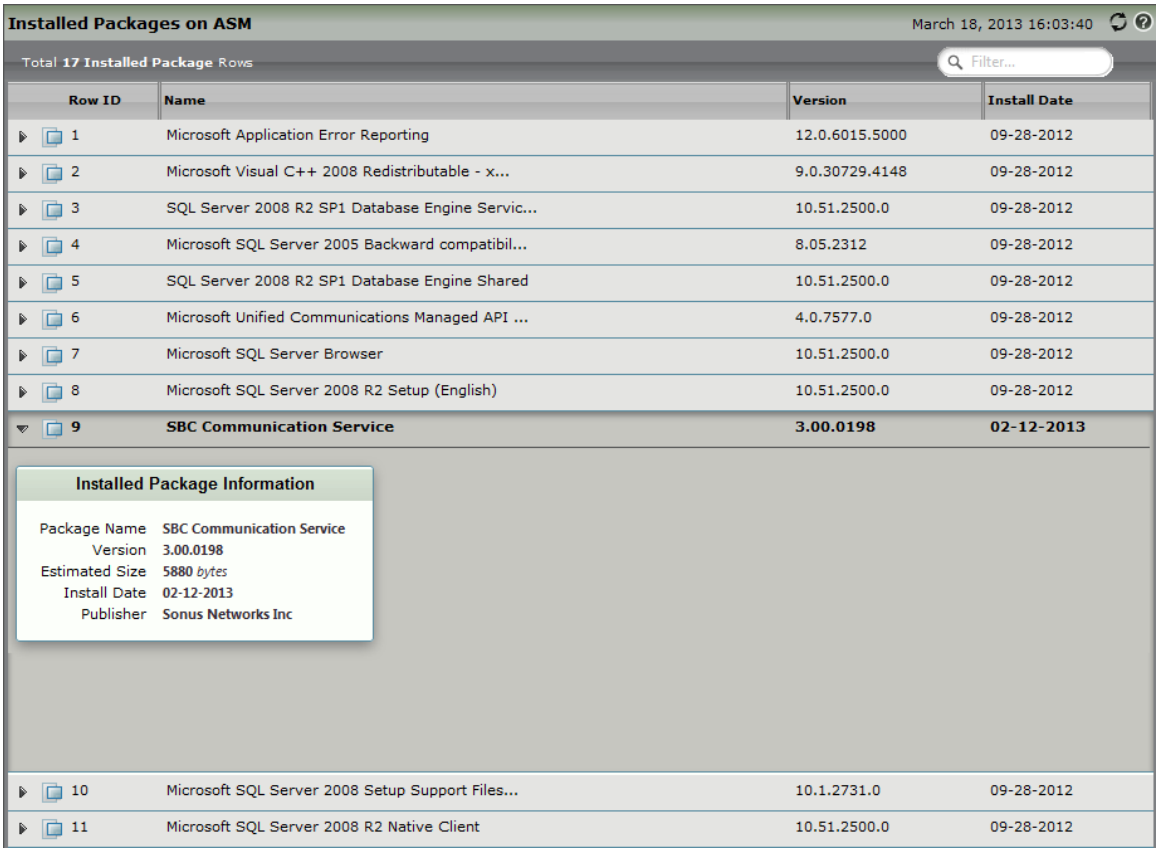
1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Application Solution Module**, click **Installed Packages**.
3. Click the **expand** (▸) Icon next to the **SBC Communication Service**service entry.



Viewing the SBC Communications Service Version through the Settings tab

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Application Solution Module > Installed Packages**.
3. Click the **expand** (▸) Icon next to the **SBC Communication Service**service entry.

Copyright © 2015 Sonus Networks. All rights reserved.



Upgrading the SBC Communication Service Version

To ensure the Sonus SBC 1000/2000 can communicate with the ASM, you must **always upgrade the SBC Communication Service before upgrading the Sonus SBC 1000/2000 software**.

> The ASM may become unavailable if you upgrade the Sonus SBC 1000/2000 firmware before upgrading the ASM SBC Communication Service.

Follow these steps to upgrade the SBC Communication Service:

1. From the Sonus SBC 1000-2000 Download Center, download the **SBC Communication Service** update — file name `uxcommsvc-release-A.B.C.zip`, where A.B.C refers to the version you are upgrading to.
2. Open the `.zip` file and unpack it to a temporary folder. This will produce a `Setup.msi` file.
3. Apply this SBC Communication Service update by following the instructions outlined in Installing an ASM Package.
4. To ensure the SBC Communication Service was properly updated, verify the Sonus SBC 1000/2000 Communication Service Version has changed to the intended version.

Working with Media

This topics in this section describe the procedures for configuring the media system and managing the various aspects of that system.

Media in the Sonus SBC 1000/2000 system refers to the "payload" portion of SIP calls (RTP, RTCP, SRTP etc). It is that which carries the actual voice traffic (as well as fax and data), while SIP itself only carries signalling and call setup information.

Configuring the Media System

Copyright © 2015 Sonus Networks. All rights reserved.

- Uploading Music on Hold Files

Managing Media Profiles

- Creating and Modifying Fax Profiles
- Creating and Modifying Voice Codec Profiles

Managing Media Crypto Profiles

- Creating and Modifying Media Crypto Profiles

Managing Media Lists

- Creating and Modifying Media Lists

Configuring the Media System

The Media System Configuration contains system-wide settings for the Media System, configuring the media system means setting the number of RTP/RTCP port pairs and the starting port. Other aspects of media handling, such as Media Profiles, Lists, and Media Crypto Profiles are handled in different sections of the UI and are explained on their own topic pages.

UDP ports are used for transmission of VoIP calls employing RTP protocols (RTP over UDP). The start port is the first port that can be used for a call. Calls require a pair of ports, one for the voice the other for the control information (RTP/RTCP). The number of ***port pairs*** determines the number of simultaneous IP Call Legs on the Sonus SBC 1000/2000. For example; if you have 100 pairs, you can have a maximum of 100 simultaneous IP Call Legs. This does not affect the number of TDM/TDM calls.

SBC Reserved Ports

Port	Protocol	Port	Protocol
1	RAW	500	UDP
22	TCP	514	UDP
53	TCP	4500	UDP
80	TCP	30000	UDP
161	UDP	30001	UDP
443	TCP	16384 through 16984	RTP

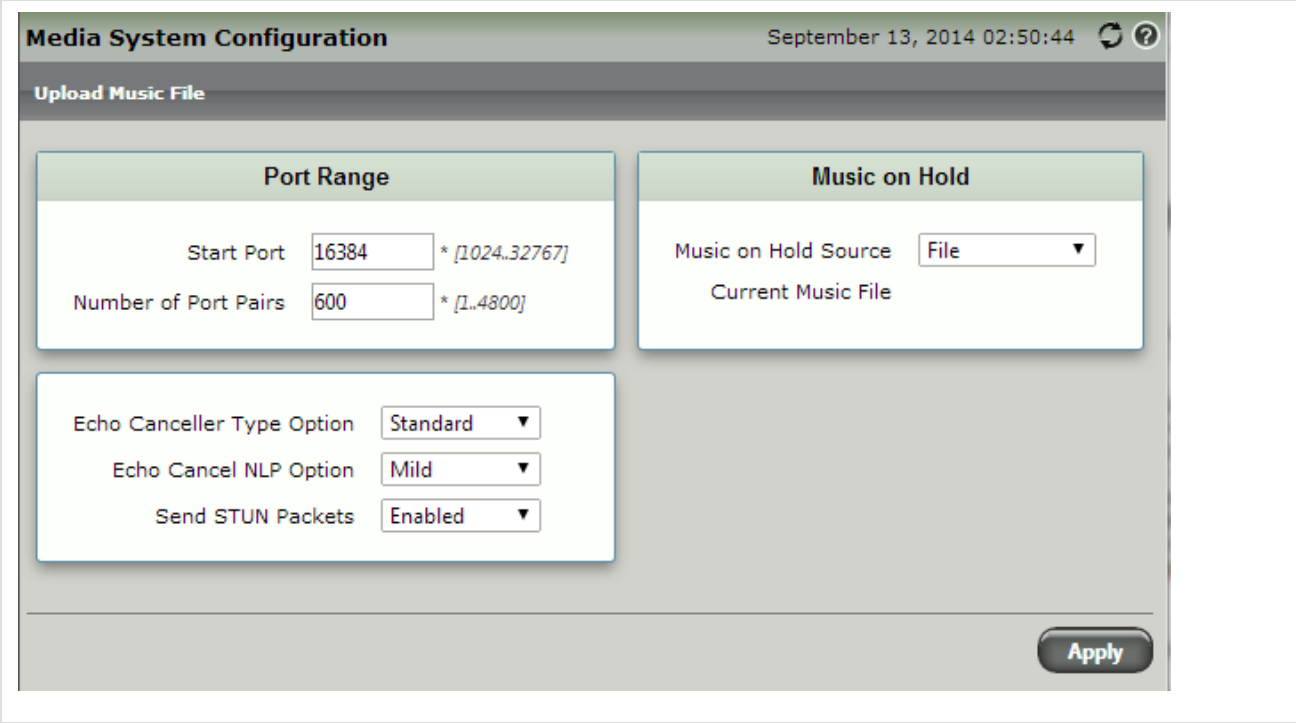
Note:

If you have 100 ***pairs***, and every call has one IP call leg, and one TDM call leg, then you can have 100 calls. However, if a call is IP on the inbound, and also IP on the outbound leg, then it requires two port pairs and this reduces the total number of simultaneous call accordingly (i.e., maximum of 50 IP/IP calls vs. Max 100 IP/TDM calls).

Configuring the Media System

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Media > Media System Configuration**.

Copyright © 2015 Sonus Networks. All rights reserved.



Media System Configuration

Port Range - Field Definitions

Start Port

Specifies the starting number for the RTP and RTCP port range.

To determine the last port number:

First Port Number + (2*Number of Port pairs) - 1.

Example:
Given: default value for starting port number (16384) and the (default) number for port pairs is 600. There are 600 pairs, meaning there are 1200 individual ports. 16384 + (1200-1) = 17583

Number of Port Pairs

The number of media port pairs used by the Sonus SBC 1000/2000 system. For example, if the default values are used for starting port number and number of ports, the last port number would be 10959. Valid entry: **1** to **4800**.

DSCP

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the DSCP value for all RTP/RTCP packets from the Sonus SBC 1000/2000.

This is used whenever the Sonus SBC 1000/2000 is connected to an external gateway that handles both data and voice traffic. When large volumes of data traffic as well as all VoIP traffic flow through the same router, a policy may be created that used the DSCP value of the media packets. The policy should be structured such that VoIP media packets receive higher priority and are expedited while other packets receive a lower priority and are queued. Network administrators should ensure that the non-VOIP packets are tagged with a different DSCP value on their network. Typically, the choice of DSCP for various kinds of packet flows in the network is determined by the network administrator and is configured on all routers within that IP network.

Music on Hold - Field Definitions

Music on Hold Source

Specifies the audio source. Sources can be an uploaded music file (**File**) or live audio sourced from an FXS port (**Live**). Default option is File. If you select **Live**, the **FXS Port** option is displayed.

When uploading a Music file, the maximum file sizes are as follows:

- For Sonus SBC 1000: 1MB
- For Sonus SBC 2000: 4MB

Music files must be one of the following formats:

- WAV
- PCMA
- PCMU
- PCM
- G726

For detailed information about how to upload a Music on Hold file, see Uploading Music on Hold Files.

FXS Port

A list of available FSX ports from which live audio may be sourced. The FXS Port field is only visible when **Live** is selected from the **Music on Hold Service** drop down list.

Other Options - Field Definitions

Echo Canceller Type Option

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the type of Line Echo Cancellation (standard or dual filter).

The standard LEC covers 128ms tail length (echo delay) and employs a 24ms sparse (non-zero coefficients) filter. The Dual Filter (background and foreground) Line Echo Canceller (LEC) covers 128ms tail length and uses 48ms sparse foreground filter. The Dual Filter is expected to provide better performance during double talk or slow echo-path change. Selection of the Dual Filter option may result in reduced channel densities.

Warning

Sonus recommends that you not **Apply** any change to the Echo Canceller Type Option unless the system is idle (no calls). Applying a change while the system is not idle may result in unknown behavior.

Echo Cancel NLP Option

Specifies the level of echo cancellation employed by the Sonus SBC 1000/2000 Nonlinear Signal Processor.

The default value is **Mild**. However there are two additional levels of echo cancellation, **Strong** and **Aggressive**. As each telephony system implementation varies, their echo characteristics similarly vary. Adjust the level of echo cancellation to suit your particular deployment. Too little cancellation may result in a persistent echo, too aggressive and you may experience voice "clipping".

Send Stun Packets

Specifies whether STUN packets are generated from the Sonus SBC 1000/2000. The Sonus SBC 1000/2000 sends STUN packets on the RTP and RTCP ports on all outbound IP call legs to open ports in the firewall (between the Sonus SBC 1000/2000 and the Internet). The ability to enable/disable this option is for customers who do not have a firewall and would like a way to disable STUN packet generation. Two options are available: **Enable** (STUN packets are generated and sent by the Sonus SBC 1000/2000) or **Disable** (STUN packets are not generated). Default option: Enable.

Uploading Music on Hold Files

Uploading Music on Hold Files

Uploading Music On Hold Audio Files

For detailed information about how to use the Music on Hold feature, along with how to verify the Music on Hold files were uploaded correctly, see Configuring the Sonus SBC 1000-2000 for Music On Hold.

Copyright © 2015 Sonus Networks. All rights reserved.

Audio File Requirements

File Size Limitations

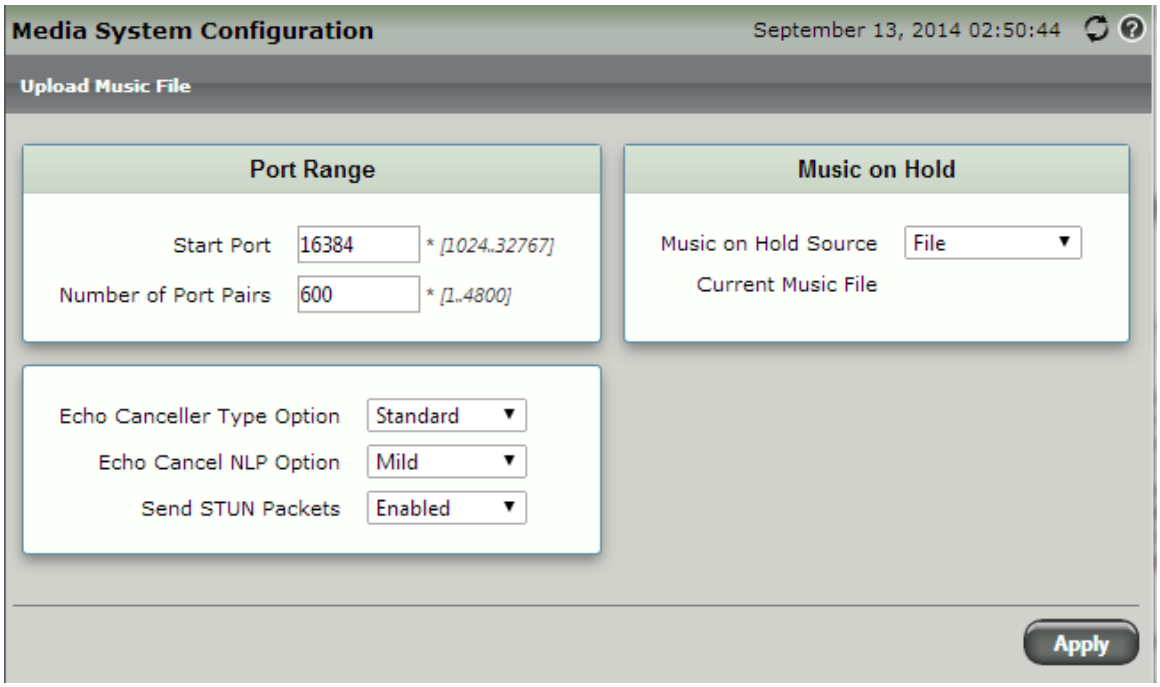
Platform	Maximum File Size
Sonus SBC 1000	1MB
Sonus SBC 2000	4MB

Valid Audio File Types

Audio File Type	Encoding Format	Sampling Rate
WAV (mono)	• 16-bit linear PCM • g711 a-law • g711 u-law	8 or 16 Khz 8 or 16 Khz 8 or 16 Khz
PCMA	g711 a-law	8 Khz
PCMU	g711 u-law	8 Khz
PCM	16 bit linear PCM	8 Khz

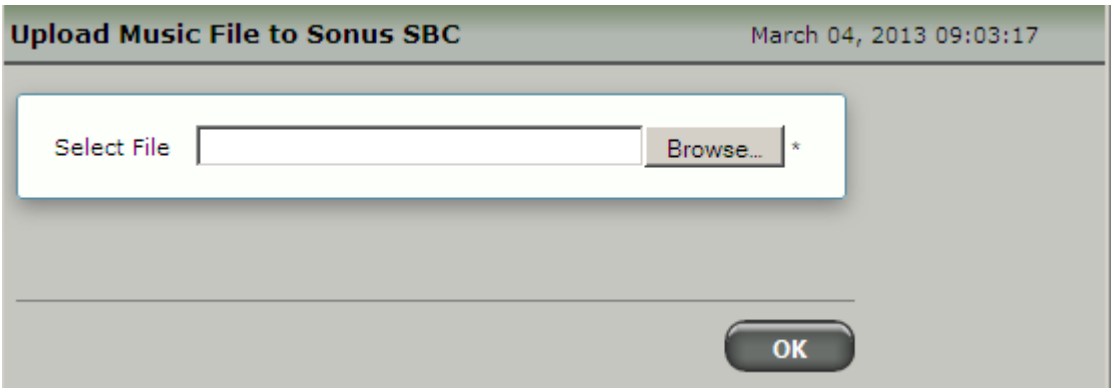
To upload a Music on Hold audio source file :

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane. go to **Media > Media System Configuration**.

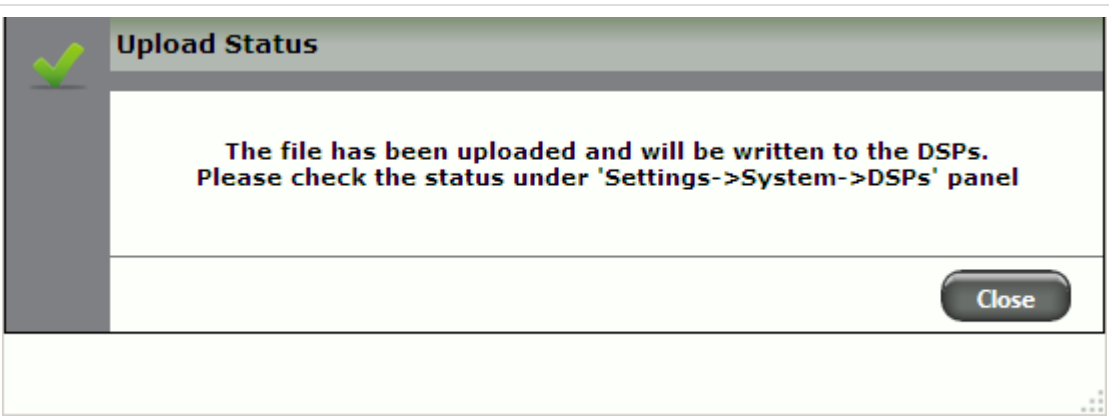


3. Click the **Upload Music File**link near the top of the page.

Copyright © 2015 Sonus Networks. All rights reserved.



4. Browse for the desired music file.
5. Click **OK**.
   When the Sonus SBC 1000/2000 has completed the upload process, the **Upload Status**dialog appears:



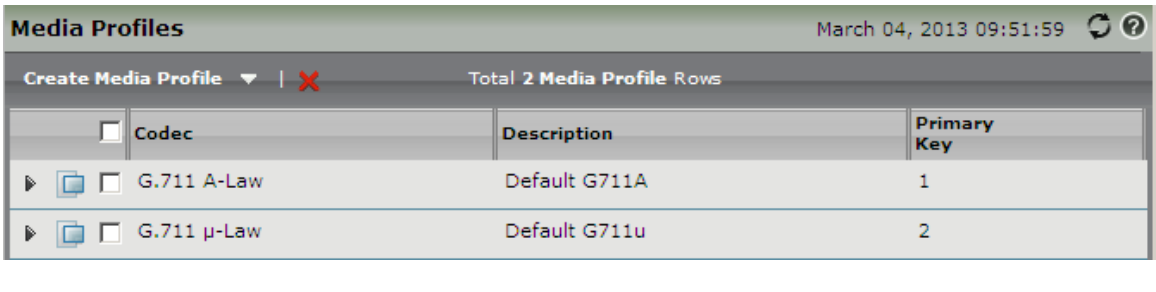
6. Click **Close**.

Managing Media Profiles

Media Profiles allow you to specify the individual voice and fax compression codecs and their associated settings, for inclusion in a Media List. Different codecs provide varying levels of compression, allowing one to reduce bandwidth requirements at the expense of voice quality.

Working with Media Profiles

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Media > Media Profiles**.



Copyright © 2015 Sonus Networks. All rights reserved.

To view a profile's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

> **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Fax Profiles

Creating and Modifying Voice Codec Profiles

Creating and Modifying Fax Profiles

> T.38 support is not available in call forking and call transfer scenarios.

To create or modify a Fax Profile:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Media > Media Profiles**.
3. From the **Create Media Profile** drop down box, select **Fax Codec Profile**.

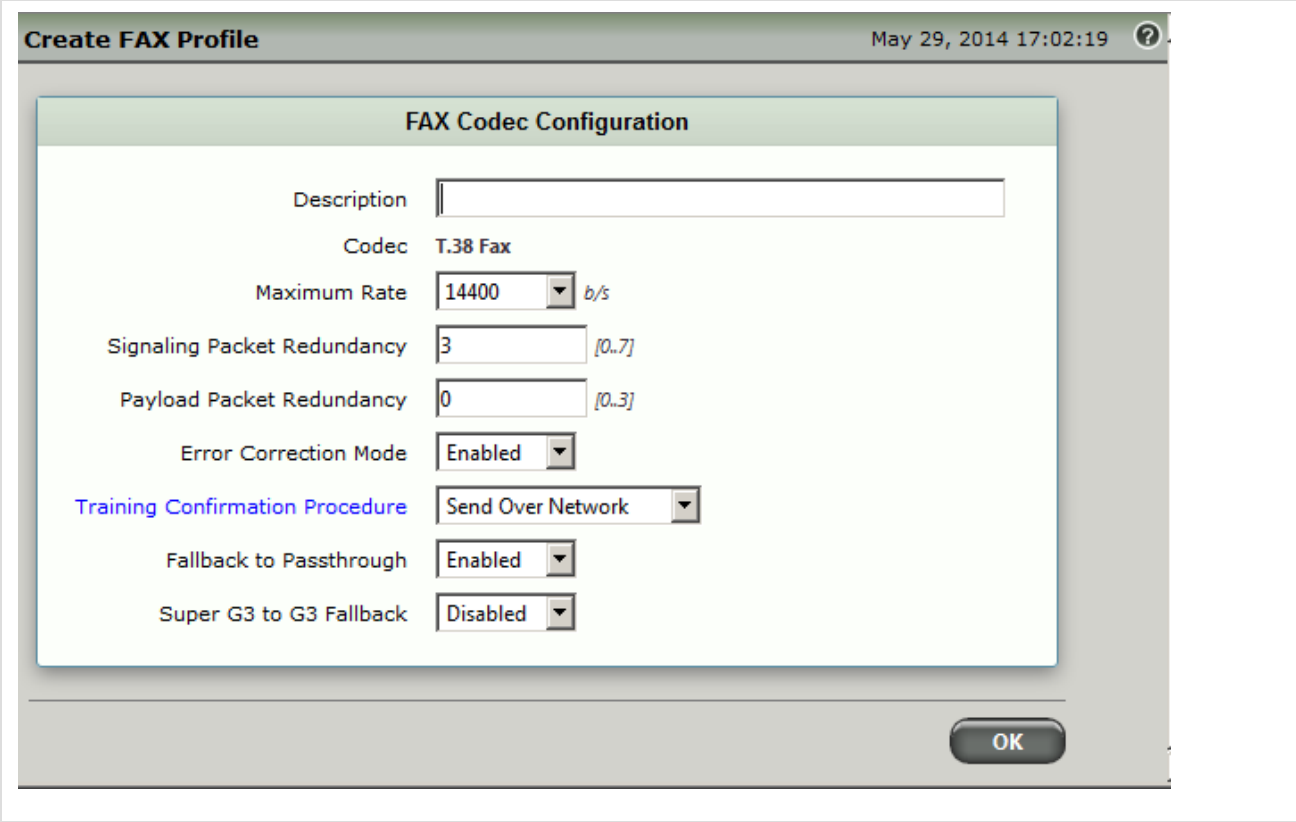
Modifying a Fax Profile

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a Fax Profile

1. From the **Create Media Profile** drop down box at the top of the **Media Profiles** page, select **Fax Codec Profile.**

Copyright © 2015 Sonus Networks. All rights reserved.



Fax Profile - Field Definitions

Fallback to Passthrough

Specifies whether or not the T.38 will fall back to Fax Passthrough if not supported by peer.

If fallback is disabled, and Sonus SBC 1000/2000 detects a fax call and attempts to switch-over to T.38 mode and the peer gateway does not support T.38 protocol, the call will fail.

If fallback is enabled, under the same circumstances as above, then when T.38 switch-over fails, the Sonus SBC 1000/2000 will attempt to switch-over to G.711 codec (if the peer supports it).

Maximum Rate

Specifies the maximum FAX connection bit rate (bits/second).

This is the maximum rate at which a fax call will be negotiated between the Sonus SBC 1000/2000 and the fax machine. It takes longer to transfer a page at lower rate, however, lower rate may make the fax call more reliable.

Signaling Packet Redundancy

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the number of redundant packets sent for each T.30 (signaling) message.

In a T.38 fax call, there are two types of packets exchanged between the two gateways: signaling packets carrying fax call control information and payload packets carrying page data. The Signaling Packet Redundancy parameter controls the number of redundant packets sent by Sonus SBC 1000/2000 for each T.38 signaling packet. Use a low value for this parameter if the data network is of good quality with no or little packet loss.

Payload Packet Redundancy

Specifies the number of redundant packets sent for each packet containing page data.

This feature is similar to the Signaling Packet Redundancy feature, except that it applies to the payload packets instead of signaling packets.

Error Correction Mode

Specifies the error correction mode (ECM) for fax calls.

ECM is used to make the fax call reliable (using retransmissions between fax machines). When disabled in the Sonus SBC 1000/2000 configuration, ECM will not be used, even if both fax machines support it.

Training Confirmation Procedure

Specifies the Training Confirmation (TCF) procedure for fax calls.

- **Locally Generate:** The TCF data is not passed across the IP network. Each gateway independently generates or checks the TCF and only the result of the training is passed over the network.
- **Send over the Network:** The TCF data is passed across the IP network in the same way as any other page data.

Super G3 to G3 Fallback

⚠ Super G3 to G3 Fallback is applicable to fax calls in TDM-to-IP or IP-to-TDM directions. It is not applicable to TDM-to-TDM or IP-to-IP fax calls.

Copyright © 2015 Sonus Networks. All rights reserved.

The Super G3 to G3 Fallback feature enables the SBC to unconditionally use T.38 protocol between two Super G3 fax machines. The call is always negotiated as if it were a G3-to-G3 fax call. Available options: **Enabled** (T.38 protocol is always negotiated between two Super G3 fax machines), or **Disabled** (T.38 protocol may not be negotiated between two Super G3 fax machines. Under many conditions, the call may come up as a modem pass-through call).

T.38 must be properly configured in the SBC according to the following guidelines:

- **T.38** must be added/selected in the Media Profiles List for both ends of the call. See Creating and Modifying Media Lists.
- The **Super G3 to G3 Fallback** option must be enabled (through Fax Codec Configuration) on the fax origination side, termination side, or both sides.
- If the Signaling Group (for which the SG3 to G3 Fax Fallback is activated) is dedicated to voice and fax calls only (i.e. modem calls are not expected and the Modem Passthrough parameter in the Media List is disabled), the TDM switch inside the SBC is used to manipulate the connection to the called fax machine to force fallback to T.38 mode. This method is very reliable but it will disrupt modem calls--that is why it is used only if modem calls are not expected over the signaling group.
- If all call types (voice, fax and modem) are allowed over the signaling group, then a DSP based method is used to squelch some signals to the called fax machine. This method will not disrupt modem calling, however, it may not work reliably if the IP network has excessive packet loss and/or jitter.

Creating and Modifying Voice Codec Profiles

To create or modify a Voice Codec Profile:

1. In the WebUI, click the Settings tab.
2. In the left navigation pane, go to **Media > Media Profiles**.
3. From the **Create Media Profile** drop down box, select **Voice Codec Profile**.

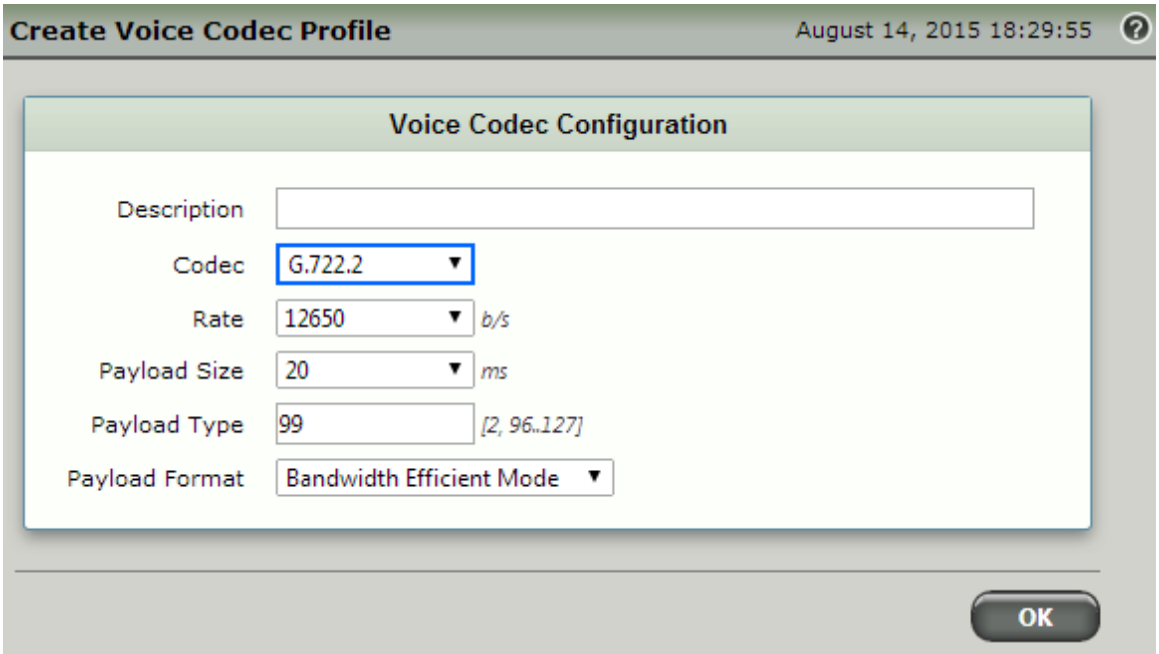
Modifying a Voice Codec Profile

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a Voice Codec Profile

1. From the **Create Media Profile** drop down box at the top of the **Media Profiles** page, select **Voice Codec Profile.**

Copyright © 2015 Sonus Networks. All rights reserved.



Voice Codec Profiles - Field Definitions

Codec

Specifies the voice codec and encoding scheme used towards the IP side of a VoIP call.

The chosen codec affects the audio quality and bandwidth consumption of VoIP calls to which you apply this Voice Codec Profile (in the Media List Profile). The choice for codec will depend on the interoperability requirements for connecting to other voice peers, as well as on the bandwidth requirements. Most codecs use data compression algorithms, which saves the bandwidth, but it slightly reduces the voice quality, whereas G.711 does not use compression and therefore requires most bandwidth.

Note: The G.722.2 Codec only appears in the list box if the AMR license is installed.

- G.722 Wideband Codec: this codec supports only 20ms packet sized and a bit-rate of 64Kbps.
- There is no fax data tone detection support in the G.772 or AMR-WB channels.

Rate

Specifies the voice sampling rate in bits/sec to be used by the codec.

This setting applies to G.723.1 and G.726 codecs only.
For all other codecs, the voice sampling rate is fixed and defined in the appropriate specification for that codec.

Payload Size

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies (indirectly) the number of bytes in a single packet.
The payload size is a multiple of the codec sample size. For example: the codec sample interval for G.711u/a is 10 ms. Therefore, the voice payload sizes are 10, 20, 30, 40, 50, 60. The codec sample interval for G.723.1 is 30 ms and therefore the payload sizes are 30, 60, 90.

Smaller payload sizes decrease audio transport latency at the expense of higher bandwidth consumption.

Larger packet sizes reduce the use of bandwidth. The larger the payload size, the fewer and larger the packets. When larger payload sizes are used, fewer L2/Ethernet headers as well as fewer IP/UDP/RTP headers are used. The disadvantage is that if UDP packets get lost, the impact on the voice quality will be much higher because a single packet contains more raw voice data.

```
Total packet size = (L2 header: MP or FRF.12 or Ethernet) + (IP/UDP/RTP
header) + (voice payload size)
```

Payload Type

Specifies the payload type for this profile. Only available when either G722.2 and G.726 is the specified codec.

Payload Format

Specifies the payload format for this profile. This field is only available when the G.722.2 codec is selected.

- **Bandwidth-Efficient Mode**
- **Octet-Aligned Mode**

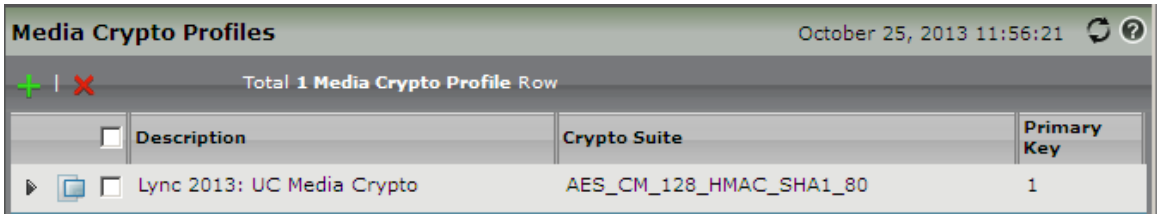
For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means. In the octet-aligned format, all the fields in a payload, including payload header, table of contents entries, and speech frames themselves, are individually aligned to octet boundaries to make implementations efficient. In the bandwidth-efficient format, only the full payload is octet aligned, so fewer padding bits are added.

Managing Media Crypto Profiles

Media Crypto Profiles define a cryptographic contexts which are used in SRTP negotiation. Media Crypto Profiles required for enabling encryption and SRTP and are applies to Media Lists.

Working with Media Crypto Profiles

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane. go to **Media > Media Crypto Profiles**.



To view a profile's properties:

Copyright © 2015 Sonus Networks. All rights reserved.

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

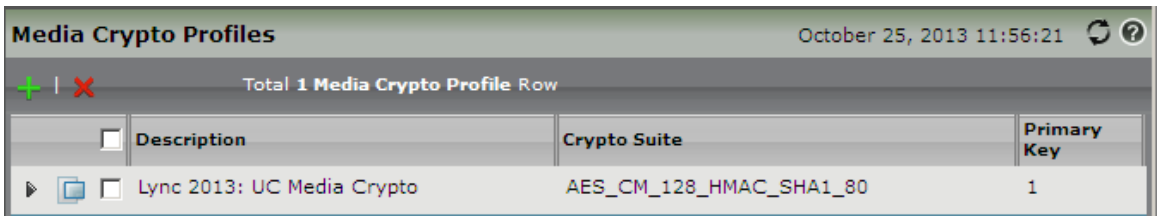
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Media Crypto Profiles

Creating and Modifying Media Crypto Profiles

To create or modify a Media Crypto Profile:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane. go to **Media > Media Crypto Profiles**.



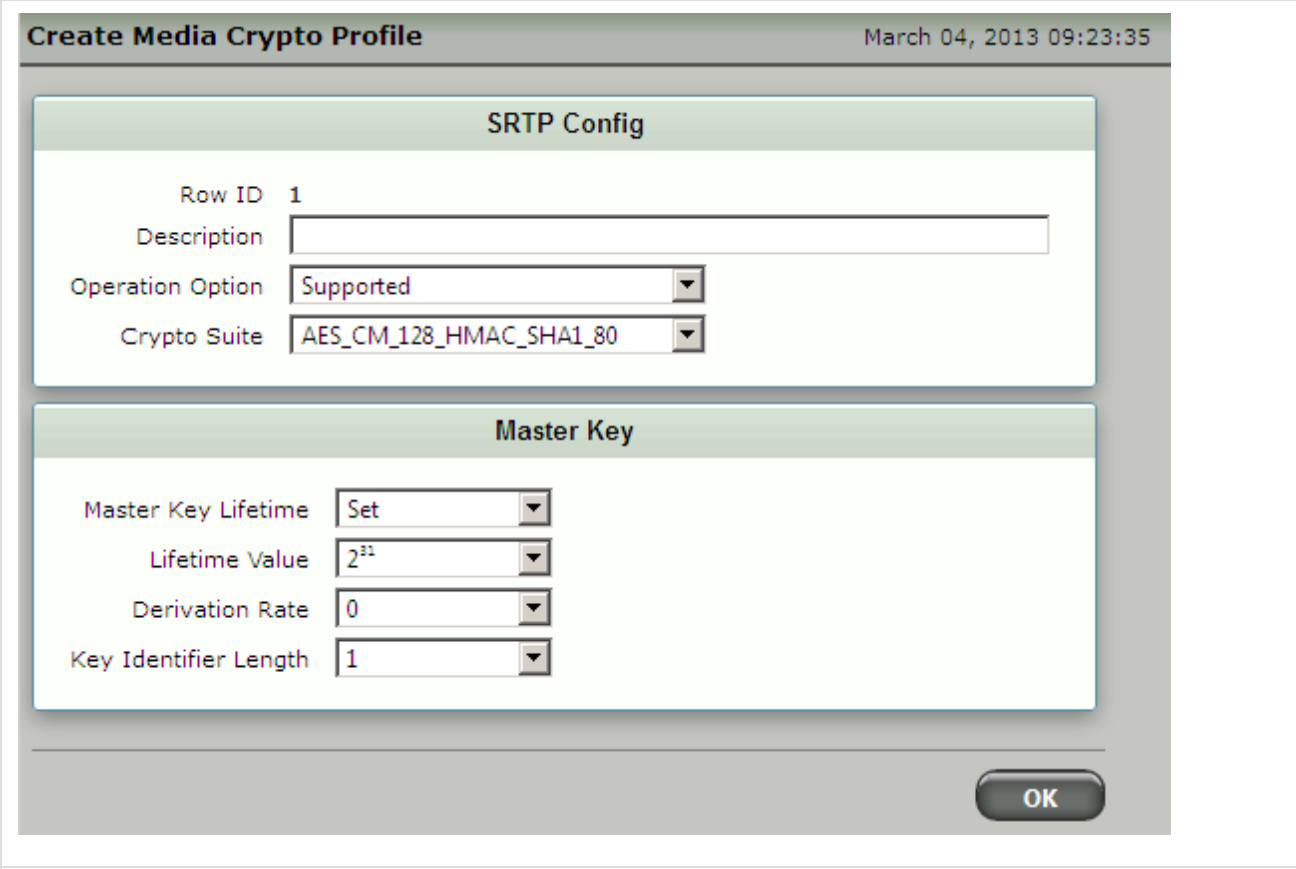
Modifying a Media Crypto Profile

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a Media Crypto Profile

1. Click the **Create Media Crypto Profile** ( ) icon at the top of the Media Crypto Profiles page.

Copyright © 2015 Sonus Networks. All rights reserved.



SRTP Config - Field Definitions

CAUTION

Anytime **Supported** is selected in the **Operation Option** field and the SIP transport is TCP/UDP, the SDP Crypto attributes are sent in plain text. Sonus recommends the use of TLS to protect the keys.

Operation Option

Specifies the manner in which encryption is supported in the profile.

- **Required:** This setting permits call connections only if encryption can be used for the call. If the peer device does not support SRTP (Secure Real Time Protocol) for voice encryption over the IP network, the call setup will fail.
- **Supported:** This setting advertises to the peer device that the Sonus SBC 1000/2000 implements SRTP. However, a call connection is allowed in secure or unsecure mode depending on the peer preference and capability.
- **Off:** This setting disables the use of SRTP for encrypted calling.

Crypto Suite

Specifies the crypto suite that the Sonus SBC 1000/2000 uses to negotiate with a peer device

Master Key - Field Definitions

Copyright © 2015 Sonus Networks. All rights reserved.

Master Key Lifetime

Specifies whether or not the Master Key has an expiry.

Lifetime Value

Specifies the lifetime of the Master Key, measured in numbers of SRTP packets expressed as a power of 2 (e.g. 2^n SRTP Packets). If the value is set to zero, the Master Key never expires.

Derivation Rate

Specifies the rate at which the session key is refreshed during the SRTP session, measured in numbers of SRTP packets expressed as a power of 2 (e.g. 2^n SRTP Packets). If the value is set to zero, the session key is never refreshed.

This option is available when **Derive Session Key** is Set to a range 16 to 24.

Key Identifier Length

Specifies the length of the Master Key Identifier, in bytes, sent in the SRTP packet.

The key identifier (MKI) identifies the master key from which the session key(s) were derived that authenticate and/or encrypt the particular packet.

If the MKI indicator is set to one(key identifier length > 0), the length (in octets) of the MKI field, and (for the sender) the actual value of the currently active MKI (the value of the MKI indicator and length MUST be kept fixed for the lifetime of the context).

Set this value to **0** to disable the MKI in SDP.

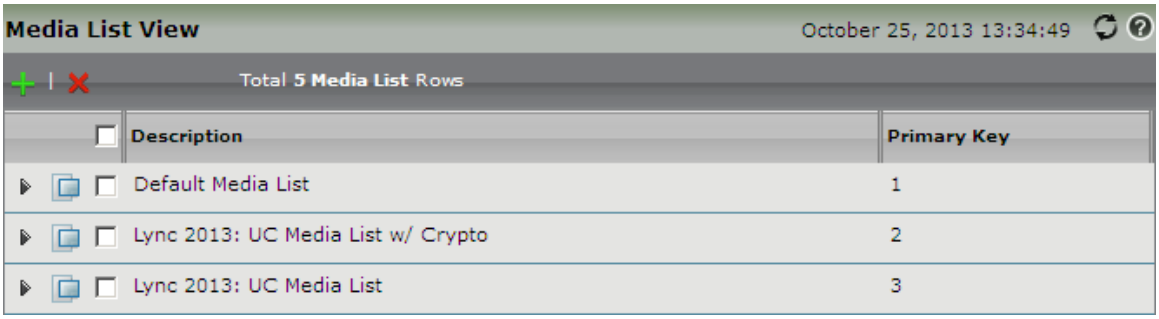
Managing Media Lists

Media Lists allow you to specify a set of codecs and fax profiles that are allowed on a given SIP Signaling Group. They contain one or more Media Profiles, which must first be defined in Media Profiles. These lists allow you to accommodate specific transmission requirements, and SIP devices that only implement a subset of the available voice codecs. See Working with Media for general information about SIP media. To use a Media List, select it from the Media List field of a SIP Signaling Group or Call Routing Table entry.

Working with Media Lists

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Media > Media Lists**.

Copyright © 2015 Sonus Networks. All rights reserved.



To view a media list's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

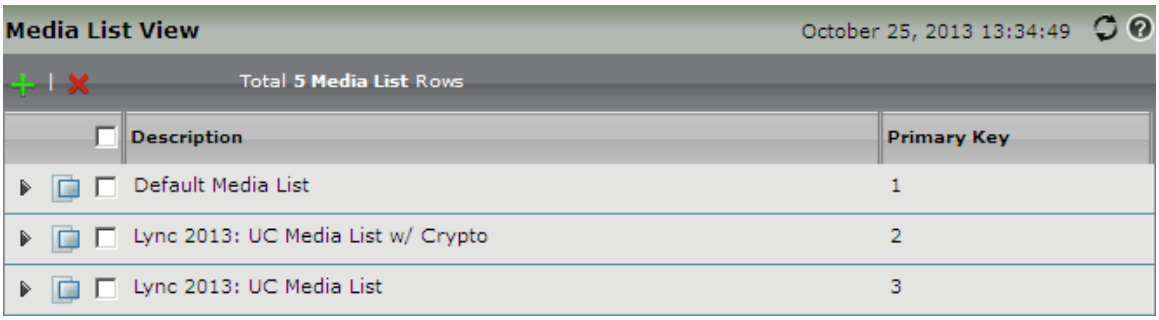
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Media Lists

Creating and Modifying Media Lists

To create or modify a Media List:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Media > Media Lists**.



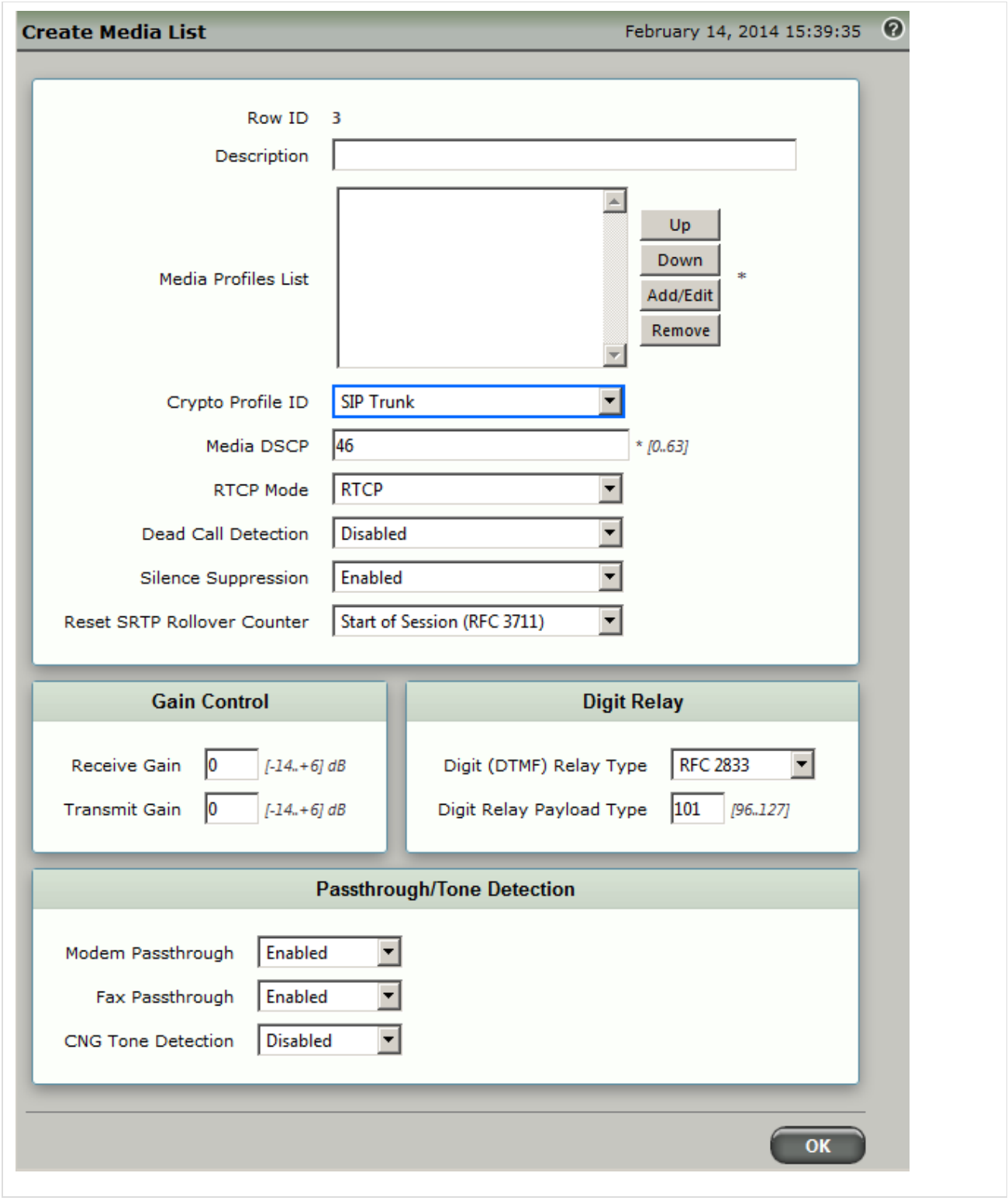
Modifying a Media List

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a Media List

1. Click the Create Media List ( ) icon at the top of the Media List View page.

Copyright © 2015 Sonus Networks. All rights reserved.



Media List - Field Definitions

Description

Name/description for the Media List.

Media Profiles List

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies a list of Media Profiles to be used in this Media List.

The order of the codec profile controls the order in which the codecs will be listed in the SIP message(s) sent to the peer. They should be listed in the order of user preference; the more desirable codecs listed first (above). The following are options to move/add/edit the profile:

- **Up**. Moves the profile up in the list.
- **Down**. Moves the profile down in the list.
- **Add/Edit.** From the **Select Media Profile** box, click to select a profile and click **OK**. The profile is added to the list.
- **Remove**. Removes the profile from the list.

Helpful Hint

This field presents a multi-select widget when the **Add/Edit** button is clicked.
Click here for more information about using the Multi-select widget.

When selecting the G729 profile: If your device supports only G729a, then be sure to configure *Silence Suppression* to *Disable*. The G729a codec does not support Silence Suppression.

Crypto Profile ID

Specifies the Media Crypto Profiles to be used with this Media List.

If you are not using (Secure Real Time Protocol (SRTP), set this parameter to **None**.

Media DSCP

Each Media List is configurable with the DSCP value to be used for media flow. All media flows that are created using this media list share the same DSCP value. Typically, a SIP Signaling Group selects the media list to be used for the calls using that Signaling Group. The default value is 46 and the allowed range is [0..63]. The configured value should be chosen according to the QoS policies of the IP network traversed by the media packets.

RTCP Mode

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies either RTCP or RTCP-XR usage for this profile

RTCP: The Sonus SBC 1000/2000 sends basic RTCP messages to the peer.

RTCP-XR(Extended Reports): The RTCP-XR packets have more information, however, some SIP endpoints may not be handle the \-XR packets, in which case basic RTCP should be specified.

RTCP-XR (Real Time Control Protocol - Extended Reports) provides packet transport quality metrics. The metrics are designed to supplement the packet-loss metric in RTCP and the roundtrip delay measurement provided by RTCP. They provide metrics for IP Packet Delay Variation based on the IPDV metric defined in, metrics reporting the activity of the RTP end system's receiver's jitter buffer, and metrics reporting "errored" and "severely errored" seconds.

For more information about this topic, see RFC 5093.

> ⚠ If the RTCP mode you have selected is RTCP-XR, then the **far end must support it.**

Dead Call Detection

Specifies whether or not to use RTCP-based Dead Call Detection (DCD).

DCD is accomplished by monitoring incoming RTCP packets. If this feature is enabled, and if no RTCP packets are received from the peer for a period of 30 seconds, the call will be considered "dead", and disconnected. DCD should be disabled if the peer does not send RTCP packets.

Silence Suppression

Specifies where or not to use Voice Activity Detection and send PT13 packets when on.

- If Silence Suppression is enabled, the Sonus SBC 1000/2000 monitors outgoing audio (towards the IP network). If silence is detected, voice packet transmission will cease to save network bandwidth. The enable setting saves network bandwidth, however, voice quality may be slightly degraded.
- If Silence Suppression is disabled, voice packets are sent regardless of whether or not audio is present.

Reset SRTP Rollover Counter

For SRTP ROC, this configuration option specifies whether to reset the ROC or maintain the ROC. Available options: **Start of Session (RFC 3711)** (SBC will maintain the ROC, even if there is a key change) and **Upon New Remote Session Key** (the SBC will reset the ROC if the call is from Lync Mediation Server and SRTP key is changed). Default entry: **Start of Session (RFC 3711)**.

This field is available only when the a Crypto Profile is selected from the **Crypto Profile ID** drop down box through creating or modifying a Media List. See Crypto Profile ID.

Gain Control - Field Definitions

Allows you to control the gain or loss (in decibels) to either the received or transmitted signals.

- Negative values represent signal attenuation (lower volume).
- Positive values represent signal amplification (higher volume).

Copyright © 2015 Sonus Networks. All rights reserved.

Receive Gain

Specifies the gain or loss in decibels to apply to received signals. (Packet ? PCM direction).

Transmit Gain

Specifies the gain or loss in decibels to apply to transmitted signals (PCM ? Packet direction).

Passthrough/Tone Detection - Field Definitions

Modem Passthrough

Specifies whether or not modem passthrough is enabled when using the G.711 codec.

If the user wants to support modem calls, this option should be Enabled. When Disabled, the Sonus SBC 1000/2000 does not distinguish between voice and modem calls. When Enabled, and the Sonus SBC 1000/2000 detects a modem call, it switches to Modem Passthrough mode (based on G.711 codec).

Fax Passthrough

Controls whether or not the Sonus SBC 1000/2000 supports G.711 faxing.

- If you wish to force fax calls to use G.711 (uLaw/aLaw) codec, then Fax Passthrough must be Enabled. Also, G.711 must be the only codec in the Sonus SBC 1000/2000 Media List. In this configuration, the Sonus SBC 1000/2000 will only offer/accept G.711 in the reINVITE.
- If you wish to support both G.711 and T.38 faxing simultaneously, the Fax Passthrough must be Enabled, and the Sonus SBC 1000/2000 must be configured with both G.711 and T.38 codecs. Which faxing type is selected will depend upon the codecs offered/accepted in the reINVITE.
- If you wish to force fax calls to use T.38 codec, configure the Fax Passthrough to Disable. Sonus SBC 1000/2000 must be configured for both G.711 and T.38 codecs. In this configuration, the Sonus SBC 1000/2000 will only offer/accept T.38 in the reINVITE.

> If your fax destination only offers T.38 in the reINVITE, then the Sonus SBC 1000/2000 must be configured for both G.711 and T.38. As noted above, T.38 fax negotiation is possible with Fax Passthrough configured to either Enable or Disable.

CNG Tone Detection

Specifies whether or not the Sonus SBC 1000/2000 system will detect Fax tones produced by the origination side fax machine. CNG tone detection is used when Fax calls are received from TDM to a Fax server and the voice call needs to be switched to a Fax call using T.38. If CNG tone detection is enabled, the Sonus SBC 1000/2000 detects the Fax tone from TDM and switches to Fax mode (it will initiate a re-INVITE with T.38 support to the Fax Server). If CNG tone detection is disabled, Sonus SBC 1000/2000 will pass-through the Fax tones to the Fax server and the Fax server will have to detect them and initiate a re-INVITE to switch to Fax mode with T.38.

Digit Relay - Field Definitions

Digit (DTMF) Relay Type

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies how DTMF digits are passed through the data network; as normal voice or encoded as specified in RFC 4733 (RFC 2833).

RFC 4733 (RFC 2833): When a DTMF digit is detected in the voice stream coming from the TDM side, the digit is removed from the voice stream (going to the IP network), and is sent out-of-band using the RFC 4733 (RFC 2833) mechanism.

As Voice: The DTMF digits are sent in the voice stream without any special treatment.

Digit Relay Payload Type

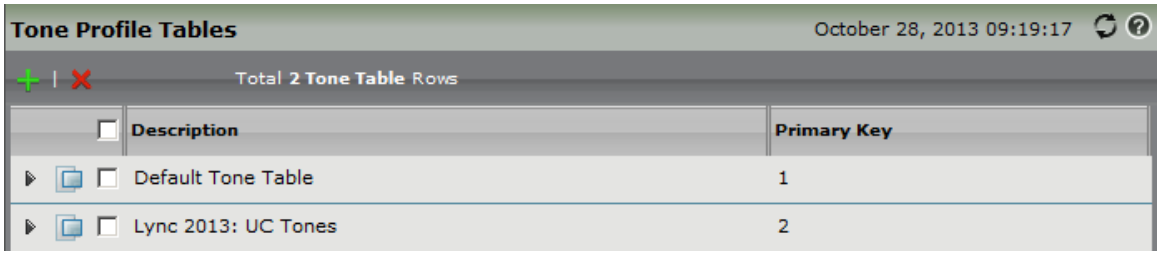
Specifies the payload type used for RFC 4733 (RFC 2833) packets. Available only when RFC 4733 (listed as RFC 2833) is specified for Relay Type.

Working with Tones

Tone tables contain entries that specify how tones are presented for conditions during a call, such as: ringback, dial, busy, etc.. Each tone can be customized to match individual or regional preferences by modifying the frequencies and cadence.

Working with Tone Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Tone Tables**.



To view a table's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Tone Tables

Creating and Modifying Tone Tables

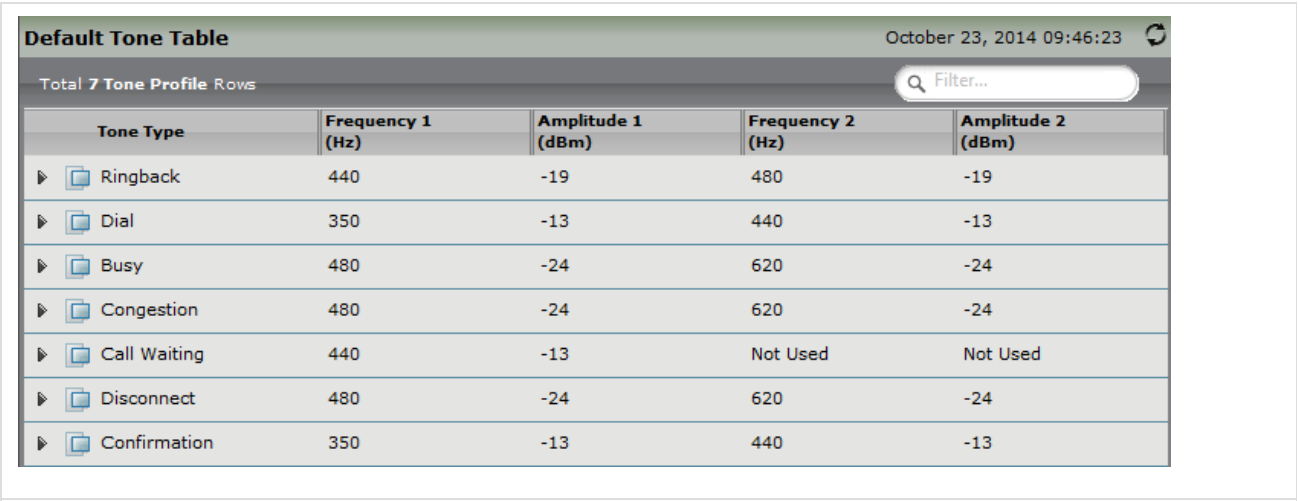
Tone tables allow the Sonus SBC 1000/2000 Administrator to customize the tones a user hears when placing a call. You can modify the tone to match your local PSTN or PBX. The default tone table is configured for the values used

Copyright © 2015 Sonus Networks. All rights reserved.

in the United States for the following categories: Ringback, Dial, Busy, Congestion, Call Waiting, Disconnect, and Confirmation.

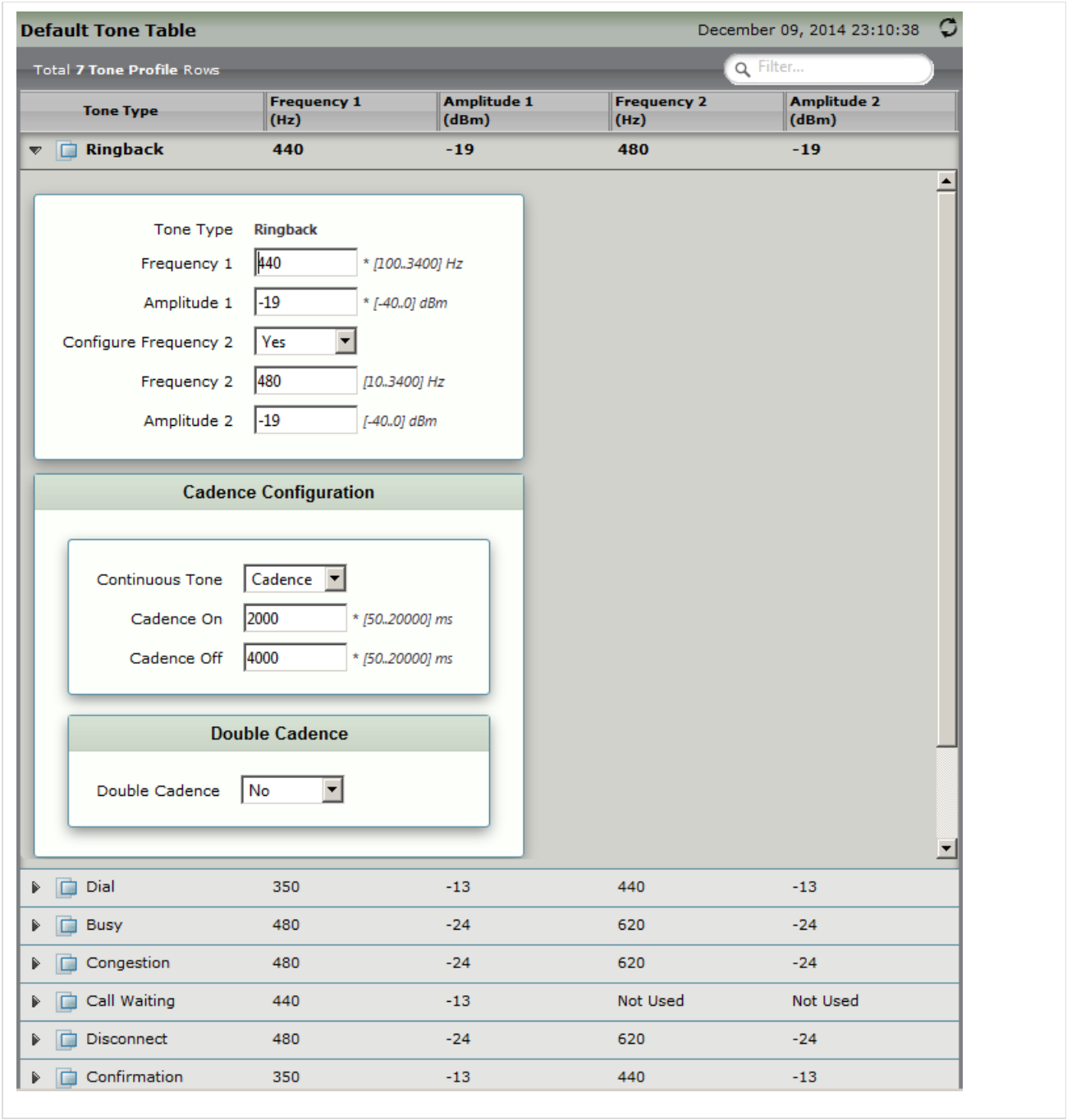
To create or modify an Entry to a Tone Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, click **Tone Tables > Default Tone Table**.



3. Click the expand ( ) icon.

Copyright © 2015 Sonus Networks. All rights reserved.



Tone Tables - Field Definitions

Frequency 1 and Frequency 2

Specifies the frequency in Hertz.

Frequency 2 is optional

Amplitude 1 and Amplitude 2

Specifies the amplitude in decibles per milliwatt (dBm) for Frequency 1 and Frequency 2.

Amplitude 2 is available only when Configure Frequency 2 is set to Yes.

Copyright © 2015 Sonus Networks. All rights reserved.

Continuous Tone

Specifies whether to use a continuous tone or a cadence.

Cadence On

Specifies the duration of time, in milliseconds, that the tone is on. Available only when Continuous Tone is set to Cadence.
Also applies in the Double Cadence pane.

Cadence Off

Specifies the duration of time, in milliseconds, that the tone is off. Available only when Continuous Tone is set to Cadence.
Also applies in the Double Cadence pane.

Double Cadence

Specifies that the tone is used in a double cadence form.

This only applies to POTS fixed phones, where the high voltage ring signal is switched on and off to create the ringing pattern. In North America, the standard ring cadence is "2-4", or 2000 ms followed by 4000 ms of silence (default Sonus SBC 1000/2000 ring cadence). In Australia and the UK, the standard ring cadence is 400 ms on, 200 ms off, 400 ms on, 2000 ms off (or **double cadence**).

Working with SNMP and Alarms

This section provides procedure for configuring SNMP Management Server addresses, and categories and severity of individual alarms and events.

Configuring Alarms and Events

Managing SNMP Management Addresses

- Creating and Modifying SNMP Management Addresses

Configuring Sonus SBC 1000-2000 for SNMP Management

SNMP MIBs Reference

Configuring Alarms and Events

The severity level and the category of all Sonus SBC 1000/2000 Alarms and Events as they appear on the WebUI are configurable. This is particularly useful if you wish to have the Sonus SBC 1000/2000's alarms/events conform with a particular scheme followed in your lab environment, or you wish to highlight and/or group alarms and events that may be of particular interest.

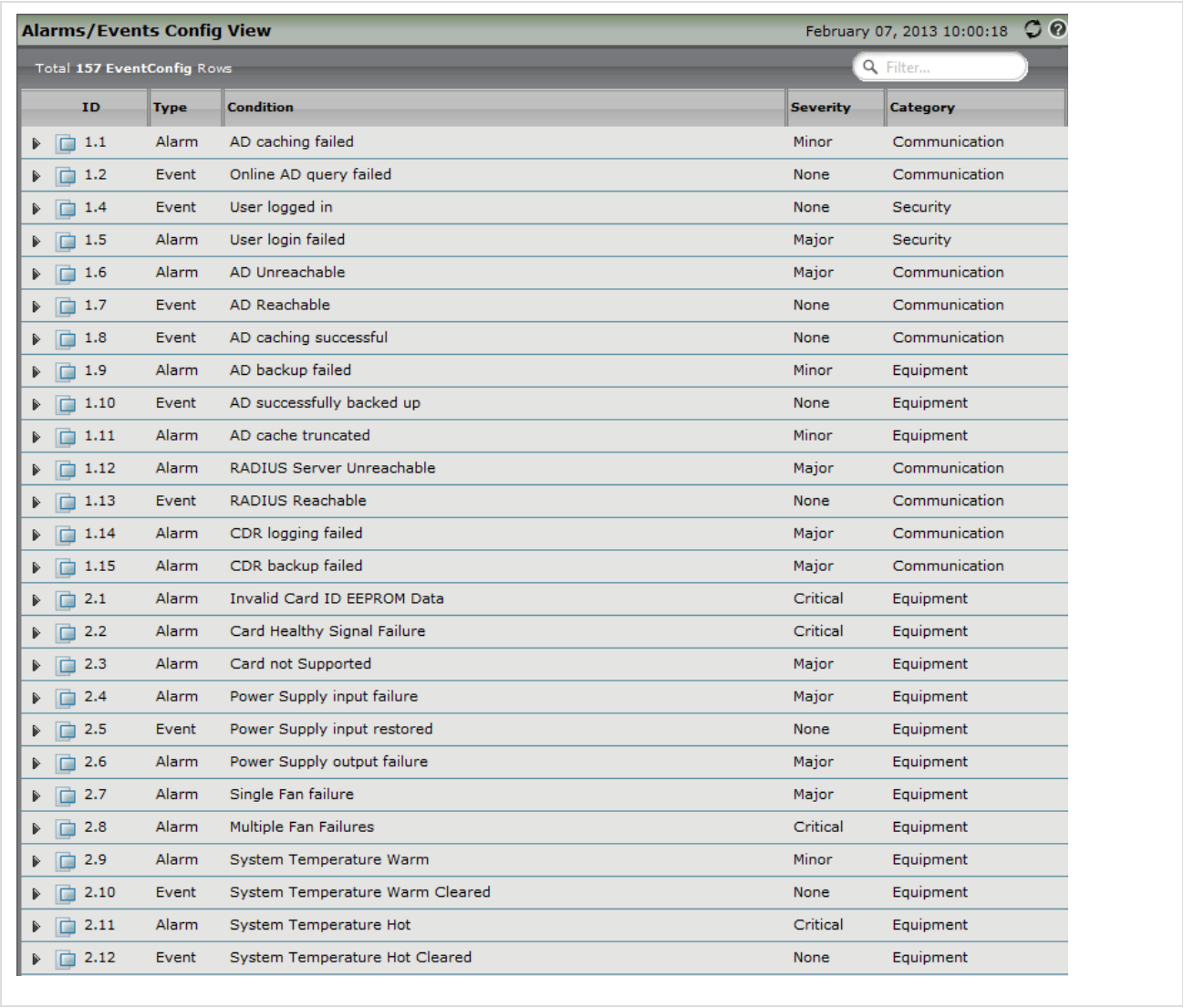
✅ Changing the Severity and/or Category of an alarm has no impact on system performance or function.

How to Configure Alarms and Events

Copyright © 2015 Sonus Networks. All rights reserved.

To configure an alarm or event:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SNMP/Alarms > Alarms/Events Config**.



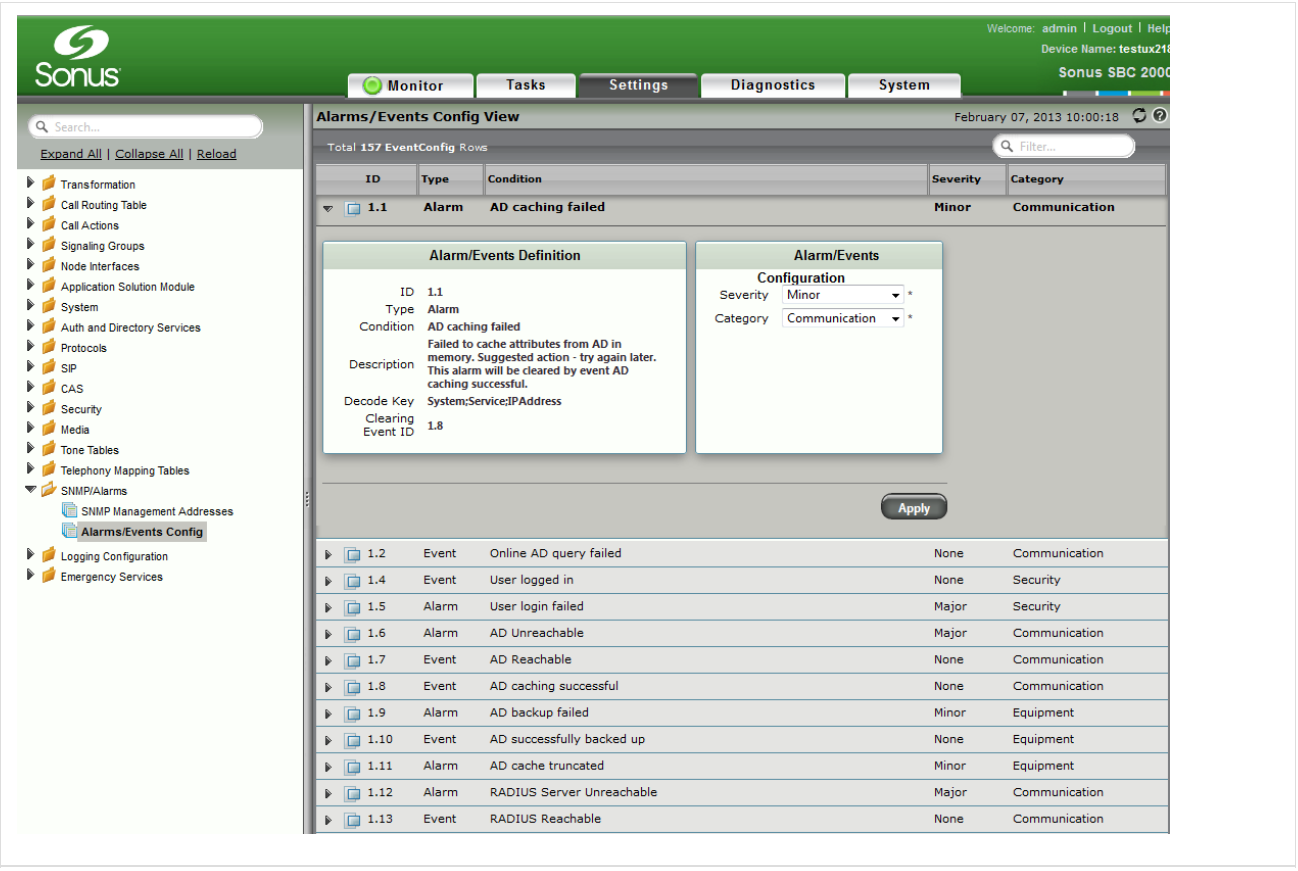
Alarms/Events Config View — February 07, 2013 10:00:18

Total **157 EventConfig** Rows — Filter...

ID	Type	Condition	Severity	Category
1.1	Alarm	AD caching failed	Minor	Communication
1.2	Event	Online AD query failed	None	Communication
1.4	Event	User logged in	None	Security
1.5	Alarm	User login failed	Major	Security
1.6	Alarm	AD Unreachable	Major	Communication
1.7	Event	AD Reachable	None	Communication
1.8	Event	AD caching successful	None	Communication
1.9	Alarm	AD backup failed	Minor	Equipment
1.10	Event	AD successfully backed up	None	Equipment
1.11	Alarm	AD cache truncated	Minor	Equipment
1.12	Alarm	RADIUS Server Unreachable	Major	Communication
1.13	Event	RADIUS Reachable	None	Communication
1.14	Alarm	CDR logging failed	Major	Communication
1.15	Alarm	CDR backup failed	Major	Communication
2.1	Alarm	Invalid Card ID EEPROM Data	Critical	Equipment
2.2	Alarm	Card Healthy Signal Failure	Critical	Equipment
2.3	Alarm	Card not Supported	Major	Equipment
2.4	Alarm	Power Supply input failure	Major	Equipment
2.5	Event	Power Supply input restored	None	Equipment
2.6	Alarm	Power Supply output failure	Major	Equipment
2.7	Alarm	Single Fan failure	Major	Equipment
2.8	Alarm	Multiple Fan Failures	Critical	Equipment
2.9	Alarm	System Temperature Warm	Minor	Equipment
2.10	Event	System Temperature Warm Cleared	None	Equipment
2.11	Alarm	System Temperature Hot	Critical	Equipment
2.12	Event	System Temperature Hot Cleared	None	Equipment

3. Click the expand (▸) icon next to the alarm or event you wish to configure.

Copyright © 2015 Sonus Networks. All rights reserved.

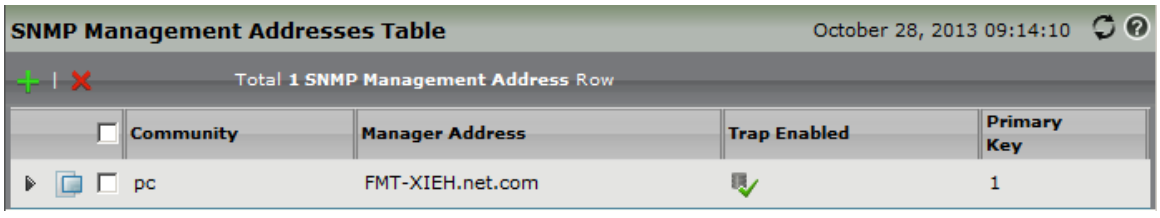


4. Select a severity level from the **Severity** menu.
5. Select a category from the **Category** menu.
6. Click **Apply**.

Managing SNMP Management Addresses

The SNMP Management Addresses Table is a list of the SNMP managers that may query the Sonus SBC 1000/2000 for SNMP information. You can configure a maximum of 10 management addresses.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SNMP/Alarms > SNMP Management Addresses**.



To view a Management Address' properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Copyright © 2015 Sonus Networks. All rights reserved.

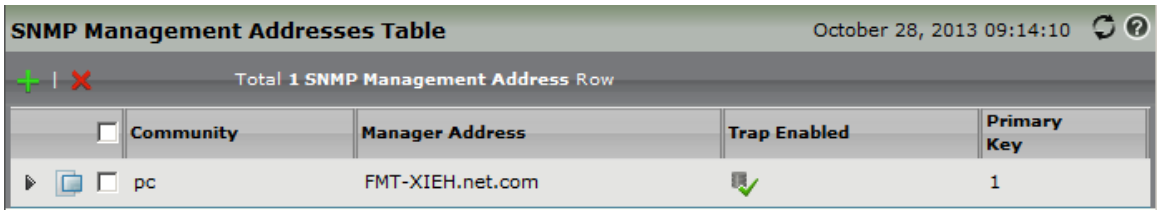
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying SNMP Management Addresses

Creating and Modifying SNMP Management Addresses

To create or modify an existing SNMP Management Address:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SNMP/Alarms > SNMP Management Addresses**.

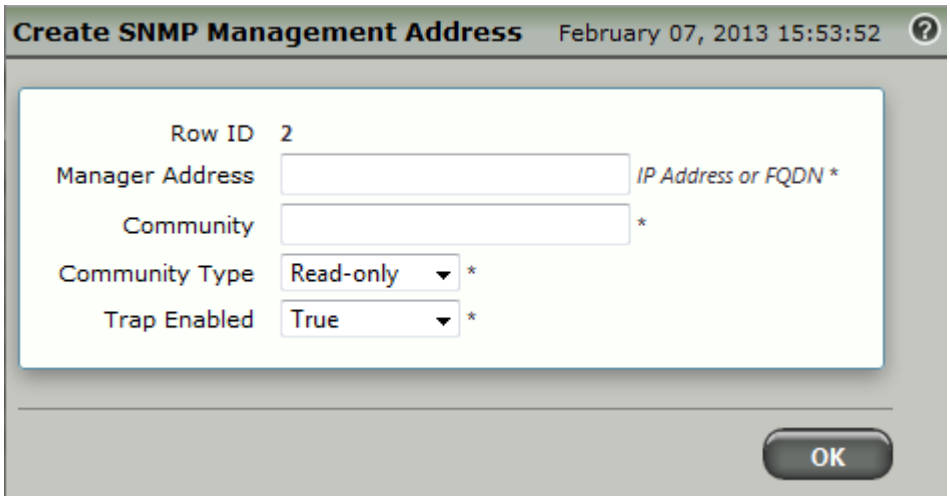


Modifying SNMP Management Addresses

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating SNMP Management Addresses

1. Click the **Create SNMP Manager Address** ( ) icon at the top of the SNMP Management Addresses Table page.



SNMP Management Address - Field Definitions

Manager Address

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the SMNP Manager IP Address or Fully Qualified Domain Name (FQDN).

Community

A password used between the SNMP Manager and the agent (Sonus SBC 1000/2000).

Community Type

Specifies whether the community is read-only or Read/Write.

Trap

Specifies whether or not the manager accepts traps.

Configuring Sonus SBC 1000-2000 for SNMP Management

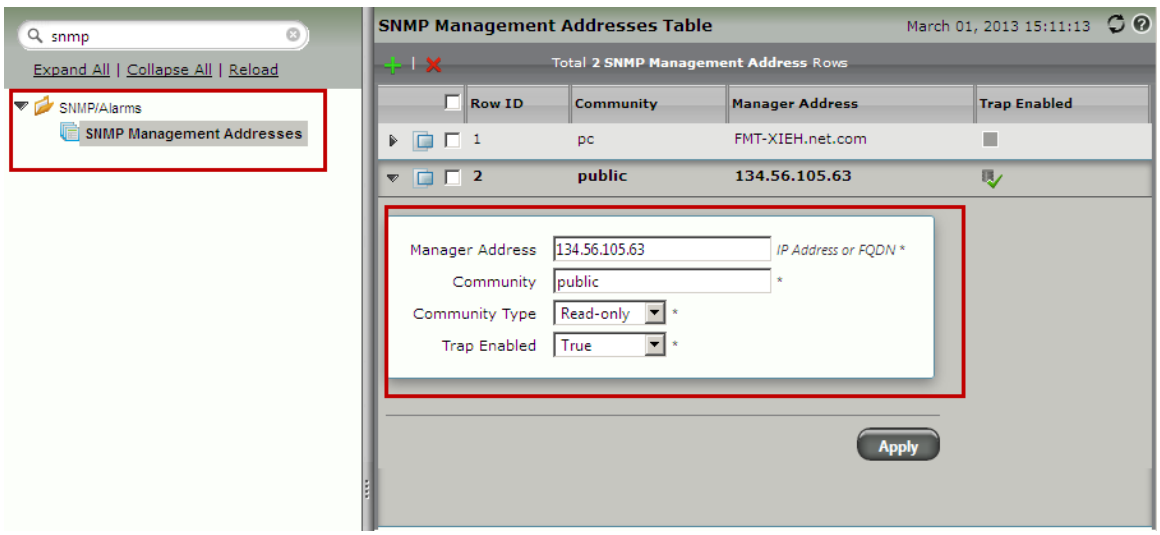
This page describes how to configure SNMP on Sonus SBC 1000/2000 and manage it using the iReasoning MIB Browser:

- Step 1 - Configuring SNMP on Sonus SBC 1000/2000
- Step 2 - Installing an SNMP Management Client
- Step 3 - Start Managing Sonus SBC 1000/2000 via SNMP

Step 1 - Configuring SNMP on Sonus SBC 1000/2000

Sonus SBC 1000/2000 SNMP Management Address Table entry should be created and configured with following information:

- **SNMP Manager Address:** IP address or the FQDN of the SNMP manager when a **MIB browser** is running
- **Community:** Enter a desired community name. In this exercise we use **public** as the community name
- **Community Type:** Must be set to **Read-only**
- **Trap Enabled:** Not required but for this exercise we are setting it up as **True**



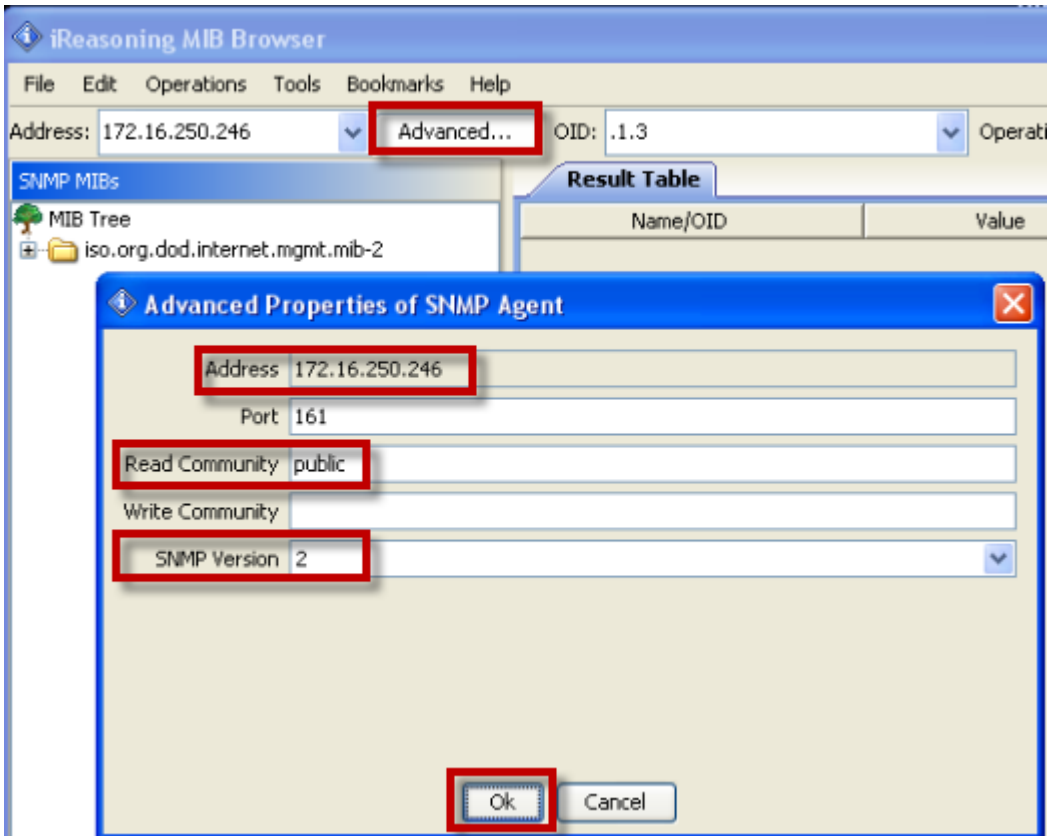
Step 2 - Installing an SNMP Management Client

Copyright © 2015 Sonus Networks. All rights reserved.

There are a various number of MIB Browsers available to download and use on the internet. For this exercise, we will be using a free edition of the iReasoning MIB Browser.

Follow the steps below to install, configure, and use the iReasoning MIB Browser:

1. On a PC that is dedicated to be the **SNMP Manager** download iReasoning MIB Browser and install using the default settings
2. Launch iReasoning from the start menu
3. Click the **Advanced...** button as shown below and enter the following information:
    - **Address:** IP Aaddress of Sonus SBC 1000/2000
    - **Port:** Keep the default value (161)
    - **Read Community:** public
    - **Write Community:** Leave it blank
    - **SNMP Version:** 2



Step 3 - Start Managing Sonus SBC 1000/2000 via SNMP

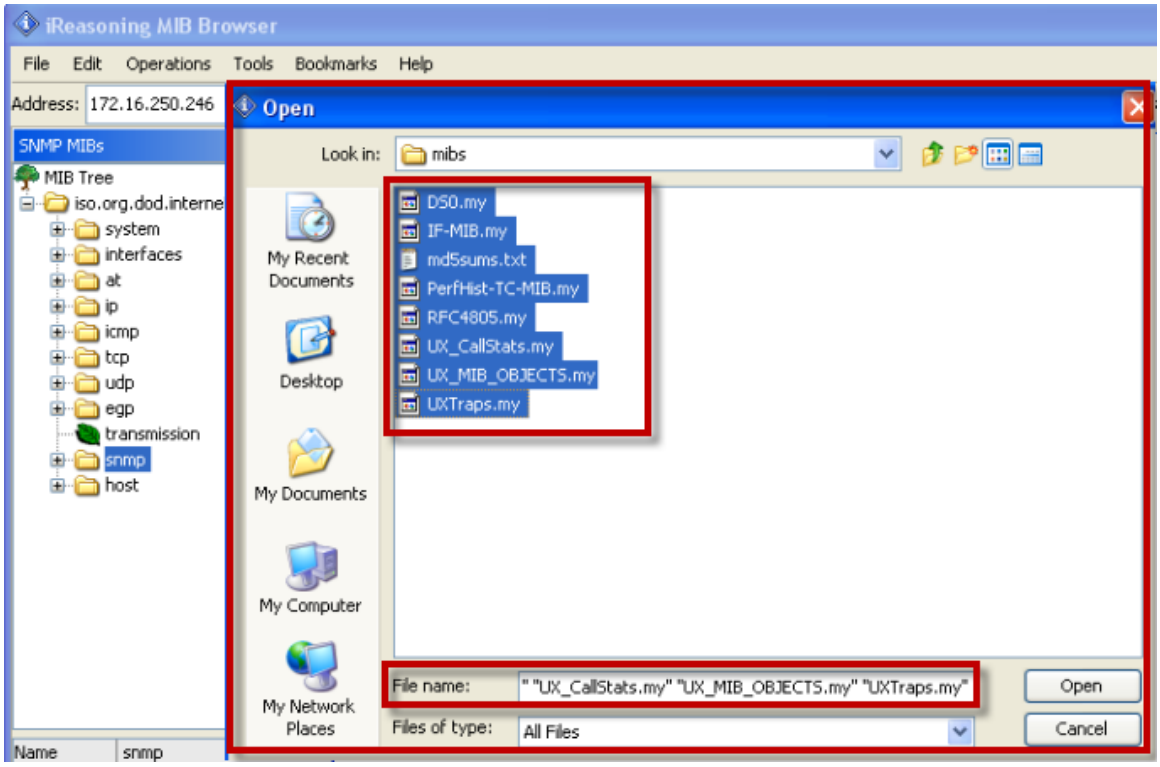
To start managing Sonus SBC 1000/2000 via SNMP, we'll need to load Sonus SBC 1000/2000's SNMP MIB files files into the iReasoning MIB Browser:

1. Download the MIB files located on the SNMP MIBs Reference page
2. In the iReasoning MIB Browser, click the **File** menu and select **Load MIBs**

Copyright © 2015 Sonus Networks. All rights reserved.

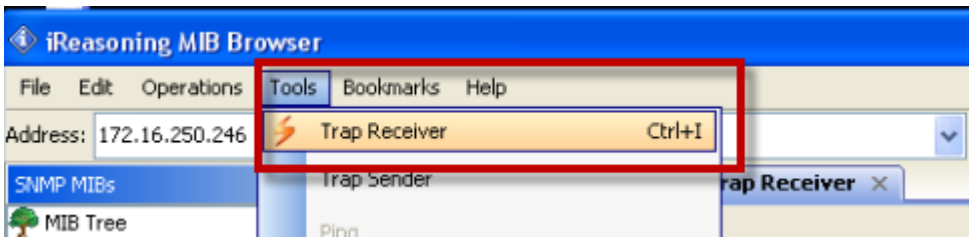


3. Browse to location where you saved the MIB files obtained in the initial step
4. Select all MIB files and hit **Open**



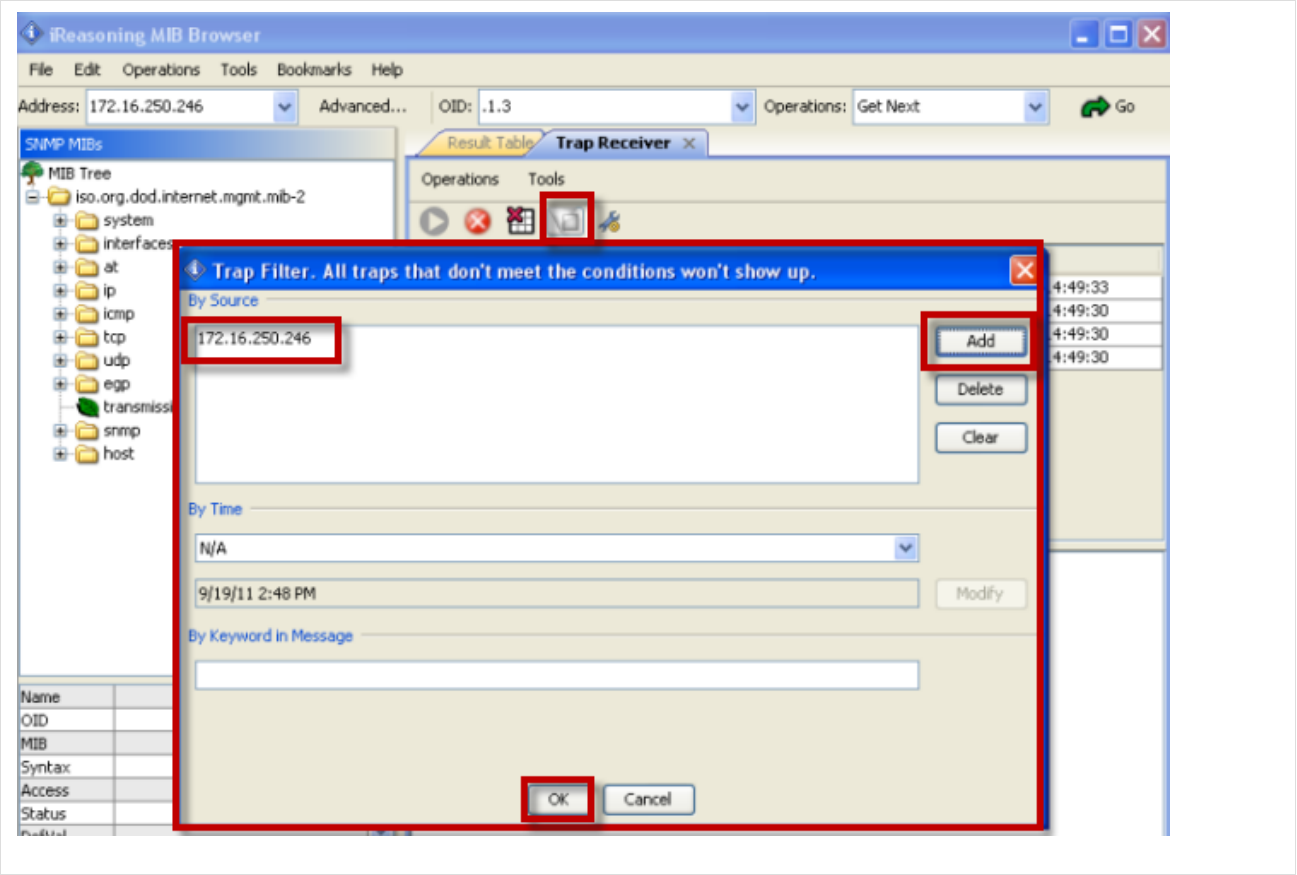
Traps include both alarms and events. If you want to receive Trap for alarms and events from Sonus SBC 1000/2000, perform the following steps:

1. In the iReasoning MIB Browser, click the **Tools** menu item and select **Trap Receiver** as shown below:



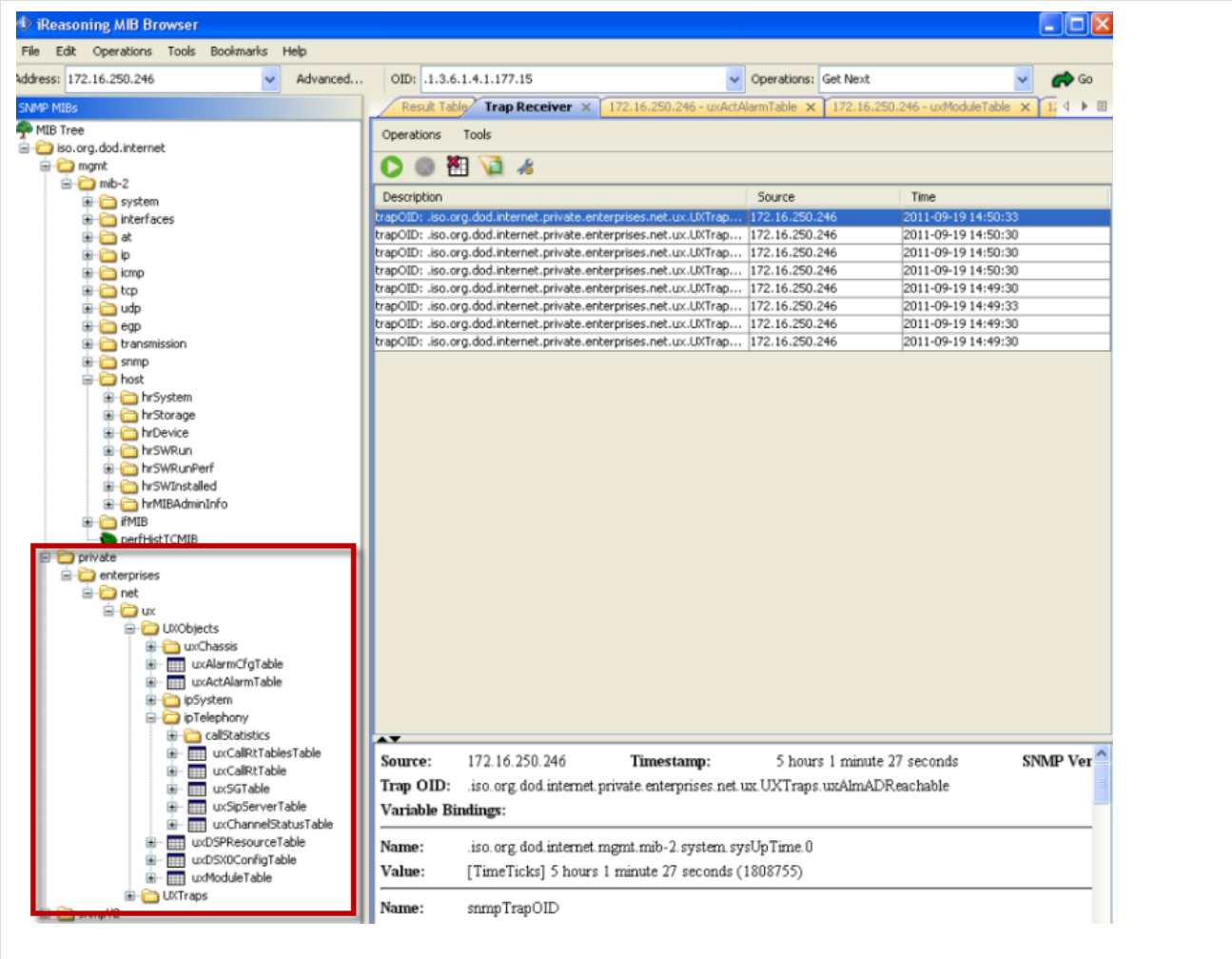
2. Click **Trap Filter**, add the **IP address of Sonus SBC 1000/2000 node**, and hit **OK**

Copyright © 2015 Sonus Networks. All rights reserved.



3. Navigate to the **private** folder* navigation pane to see the relevant Sonus SBC 1000/2000 MIBs as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



SNMP MIBs Reference

- Overview
- Standard MIB Support
- IF MIB
- DS0 MIB
- DS1 MIB
- Host Resources MIB
- MIB File Downloads

Overview

In addition to the standard MIBs, the Sonus SBC 1000/2000 system supports the following MIBs.

1. **Sonus SBC 1000/2000 Objects MIB** - This MIB file contains the following:
    - Sonus SBC 1000/2000 chassis information
    - Sonus SBC 1000/2000 Alarm Configuration Table
    - Sonus SBC 1000/2000 Active Alarm Table details
    - Sonus SBC 1000/2000 DSP Resource Table
    - Sonus SBC 1000/2000 DSX0 Config Table (augments the standard DSX0 Config Table)
    - Sonus SBC 1000/2000 Module Table
2. **Sonus SBC 1000/2000 Call Statistics MIB** - This MIB file contains the following:

Copyright © 2015 Sonus Networks. All rights reserved.

- Sonus SBC 1000/2000 system version information
- Sonus SBC 1000/2000 Port Table(Sonus SBC 1000/2000 call statistics details)
- Sonus SBC 1000/2000 Channel Status Table
- Sonus SBC 1000/2000 Call Route Tables Table (a table of tables)
- Sonus SBC 1000/2000 Call Route Table
- Sonus SBC 1000/2000 Signaling Group Table
- Sonus SBC 1000/2000 SIP Server Table

3. **Sonus SBC 1000/2000 Traps MIB** - This MIB file lists the Sonus SBC 1000/2000 traps sent to the managers.

Standard MIB Support

Sonus SBC 1000/2000 also extends the standard interface table MIB to include partial support for the following:

IF MIB

The Sonus SBC 1000/2000 supports the IF MIB as described here:

- The ifStack and ifRcvAddress tables list only the physical interfaces.

The ifIndex attribute inthe ifTable is interpreted as follows:

Bit	Description
0-9	Channel number
10-15	Port number
16-17	Reserved
18-21	Card number
22-25	Shelf number
26-29	Unused
30	0 = Kernel, 1 = User. All Ethernet interfaces are 0 and DS1 are 1.
31	No Used, always 0.

The kernel assigns ***ifIndex*** sequentially based on the order the interfaces are brought up.

DS0 MIB

The Sonus SBC 1000/2000 supports partial DS0 MIB support through the dsx0Configtable table. The DS0 MIB is based on RFC 2494.

DS1 MIB

The Sonus SBC 1000/2000 provides partial support for the DS1 MIB. The DS1 MIB is based on RFC 4805.

Host Resources MIB

The Sonus SBC 1000/2000 provides partial support for the Host Resources MIB. The Host Resources MIB is based on RFC 2790.

Copyright © 2015 Sonus Networks. All rights reserved.

MIB File Downloads

- **UXTraps**
- **UX-OBJECTS-MIB**
- **UX-CallStats**
- **PerfHist-TC-MIB**
- **IF-MIB**
- **DS0**
- **RFC4805**
- **SNMPv2-MIB**
- **Zipped Collection**

Working with Logging

The Sonus SBC 1000/2000 logging service allows you to troubleshoot issues such as call signaling, call quality and performance by collecting activity logs from its subsystems. These logging records can then be analyzed to diagnose problems and optimize the performance of Sonus SBC 1000/2000 for your environment.

The Sonus SBC 1000/2000 system supports the following methods for recording logs:

- **Remote Syslog** configuration, uses a syslog server to store a larger amount of log activity for extended period of time. Using a Remote Logging configuration is the recommended logging method since it allows for a greater logging history and level of detail. You must use this method of logging when working with Sonus Technical Support (TAC).
- **Local Log** (available only on the Sonus SBC 2000 chassis model) configuration, stores temporary log files directly on the Sonus SBC 1000/2000 system. Each local log file retains a limited amount of recorded log messages. Local logging is only useful for quick, high level, troubleshooting, and is not recommended (nor suited) for extended troubleshooting sessions.

> **Local Logging at Debug or Trace Level**
>
> - Increasing the local log level of any subsystem to Debug or Trace levels should be performed only if requested by Sonus Technical Support (TAC).
> - After completing the collection of logs from the tests, all subsystems with custom log level must be reset to the Default local log level (Warning) or deleted.
> - Avoid performing this action on a production system.

A fully running Sonus SBC 1000/2000 system can generate a large amount of logging information. For this reason, the Sonus SBC 1000/2000 logging service allows you to customize the types of logging messages (and level of detail) you wish to be recorded by Managing Subsystems Logging.

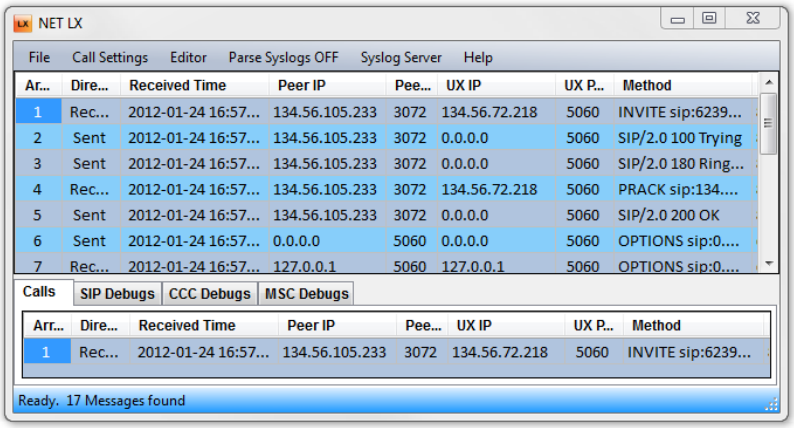
Debug Sonus SBC 1000/2000 Logs using LX

Copyright © 2015 Sonus Networks. All rights reserved.

LX is available **free of charge** for all customers and partners with a license agreement.

For **Release Notes** and **File Download** information, please visit the Global Services Toolbox.

Log Exchange Screenshot



Log Exchange (LX) is a multipurpose debugging tool for the SBC 1000/2000, SBC 5000 series, and VX series gateways

LX parses log files and displays SIP call flows, ISDN call flows, and advanced call details in real-time - making it easy for end-users to analyze and troubleshoot issues.

When using the SBC 1000/2000, users have the ability to parse log messages on the fly using LX's built in Syslog listening capabilities.

For more information about Log Exchange, click one of the links below.

Table of Contents

- Installing LX
- LX Overview
- Working with Settings and Filters
- Configuring LX as a Syslog Server on SBC 1000-2000
- Working with Syslogs
- Working with Syslogs from External Servers
- Working with Call Flows
- Copyright and Trademarks

Related Topics

Managing Remote Log Servers

- Creating and Modifying Remote Log Servers

Managing Subsystems Logging

- Creating and Modifying Subsystem Logging

Managing Local Logs

Copyright © 2015 Sonus Networks. All rights reserved.

- Setting the Local Log Level
- Understanding Local Log Rotation Rules

Supported Logging Levels

Working with Port Mirroring

Managing Remote Log Servers

The Sonus SBC 1000/2000 Remote Log functionality uses a syslog server per the RFC 5424 standard. Unlike Managing Local Logs, configuring a syslog server for Sonus SBC 1000/2000 system logging allows you to manage logging resources separately from the system being monitored.

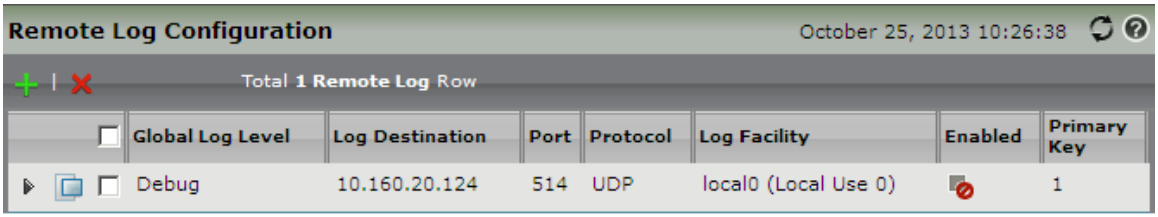
Depending on the size and configuration of your existing network infrastructure you may already have a syslog server. If your existing network infrastructure does not have a syslog server, there are many products available, including servers for Microsoft Windows (Kiwi Sys Log Server, SL4NT) and Linux systems (syslogd).

Recommendations

- **Network**: It is highly recommended that the syslog server used to monitor Sonus SBC 1000/2000 log activity be located on the same subnet as the Sonus SBC 1000/2000 system. If Sonus SBC 1000/2000 and syslog server are not on the same network, increased log level detail and large amount of calls may result in high bandwidth utilization.
- **Total Destinations**: While you can *configure up to 6 remote log server destinations* on the Sonus SBC 1000/2000, it is not advisable to have this many destinations configured during high call churn.

Working with Remote Log Servers

1. **In the WebUI, click the Settings** tab.
2. In the left navigation pane, go to **Logging Configuration** > **Remote Log Servers**.



To view a Remote Log Server's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

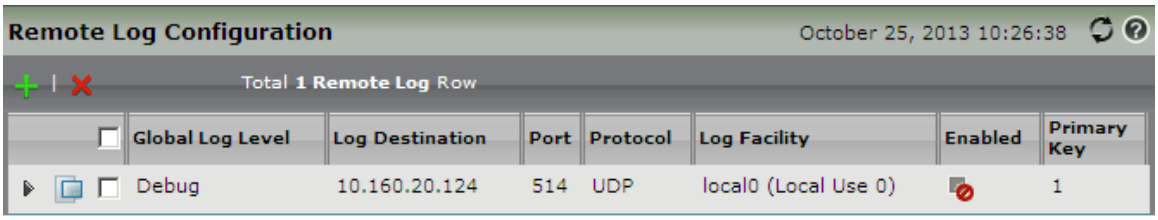
- Creating and Modifying Remote Log Servers

Copyright © 2015 Sonus Networks. All rights reserved.

Creating and Modifying Remote Log Servers

To create or modify a Remote Log Server:

1. **In the WebUI, click the Settings** tab.
2. In the left navigation pane, go to **Logging Configuration** > **Remote Log Servers**.

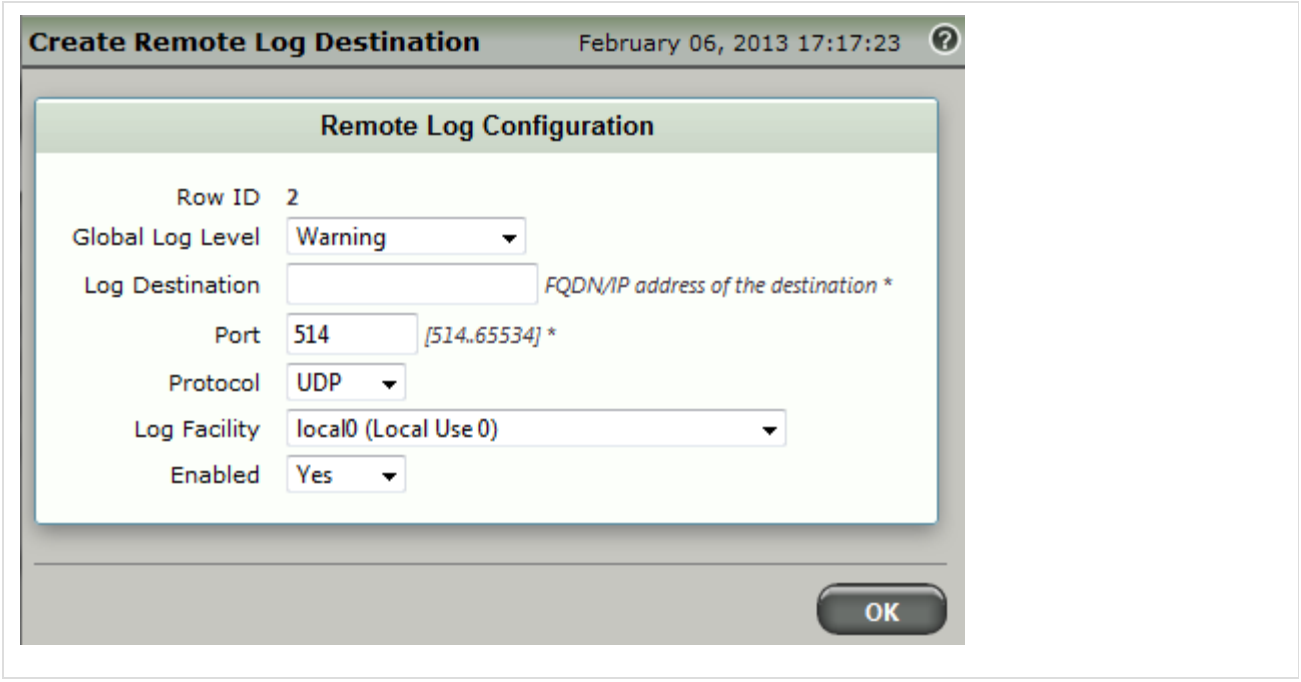


Modifying a Remote Log Server

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a Remote Log Server

1. Click the **Create Remote Log** ( ) icon at the top of the Remote Log Configuration page.



2. Select an entry from the **Global Log Level** menu.
3. Enter the **IP Address** or **Fully Qualified Domain Name** (FQDN) of the log server you are adding.
4. Select an entry from the **Log Facility** menu.
5. Select **Yes** from the **Enabled** menu to enable the server.
6. Click **OK**.

Managing Subsystems Logging

Copyright © 2015 Sonus Networks. All rights reserved.

The Sonus SBC 1000/2000 system comprises of multiple software modules known as **Subsystems** to operate. Each Subsystem provides its own set of log messages that can be tuned and monitored independently. Subsystem level logging is typically used when diagnosing a problem on the Sonus SBC 1000/2000 system.

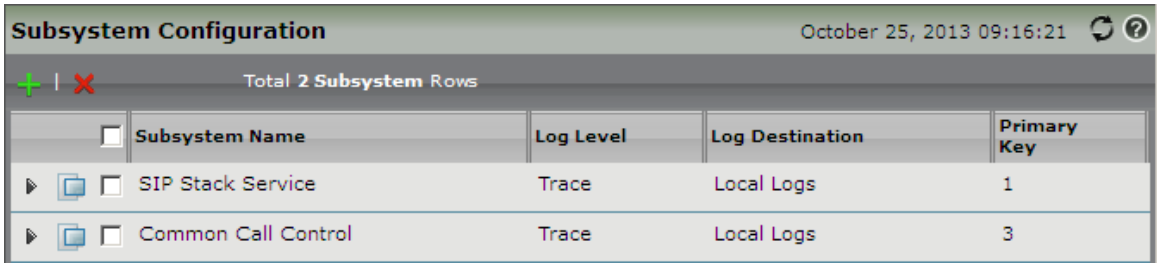
Suggested Subsystems when troubleshooting telephony-related issues:

- Common Call Control
- Media Stream Controller Service
- SIP Stack Service
- Call Routing Service
- Core Switching/Routing
- ISDN Protocol

During high call churn, it is recommended that no more than 3 subsystems be configured with logging levels higher than 'Informational'.

Working with Subsystems Logging

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Logging Configuration > Subsystems**.



To view a Subsystem's Logging properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

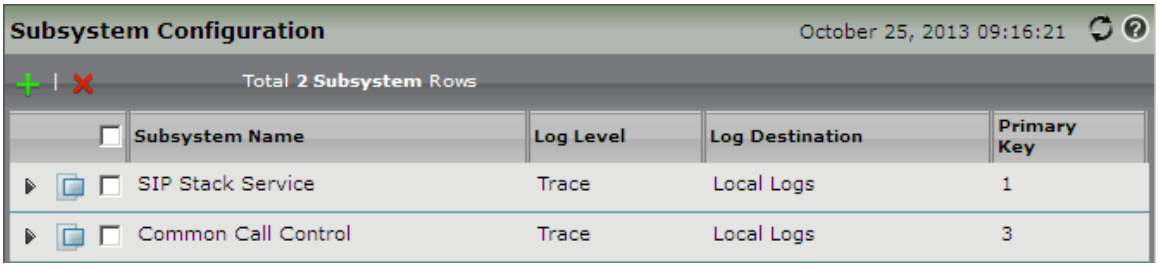
Creating and Modifying Subsystem Logging

Creating and Modifying Subsystem Logging

To create or modify a Subsystem Logging:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Logging Configuration > Subsystems**.

Copyright © 2015 Sonus Networks. All rights reserved.

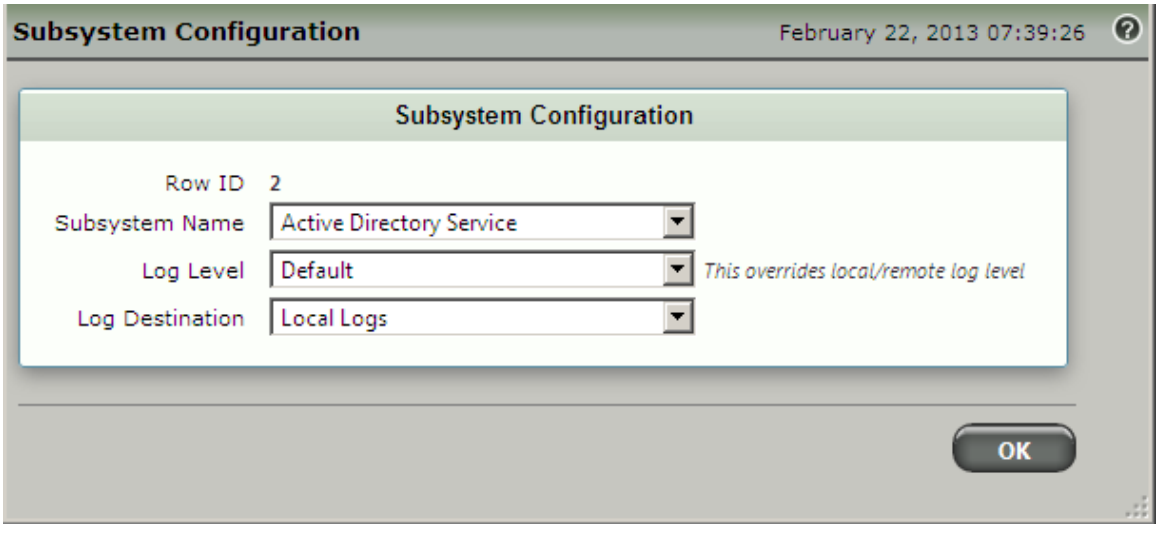


Modifying a Subsystem Logging

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a Subsystem Logging

1. Click the **Create Subsystem Logger** ( ) icon at the top of the Subsystem Configuration page.



2. Select a subsystem to log from the **Subsystem Name** menu.
3. Select a logging level to use for this subsystem from the **Log Level** menu.
4. Select a location to send the log from the **Log Destination** menu.
5. Click **OK**

Helpful Tip

If **Default** was selected in the **Log Level** menu, then the **Global Logging Level** configuration will be assumed for the associated **Log Destination**.

Managing Local Logs

Getting Started with Local Logs

The **Diagnostics** tab displays a listing of log files stored locally on the Sonus SBC 2000 file system. Sonus SBC 2000 system logs can record every internal and external action the Sonus SBC 2000 system performs, including user visible actions (such as placing calls), as well as internal parsing and messaging operations. The actual level of logging detail is configurable by Setting the Local Log Level.

Copyright © 2015 Sonus Networks. All rights reserved.

Preview

Locally stored log files can be directly viewed from the Sonus SBC 2000 Web interface. To do so, simply click the **expand** ( ) icon next to the log file you wish to preview the log in place, or click the **popup** ( ) icon to preview in a separate window.

> Previewing logs files larger than 2 Megabytes is not recommended as this may slow down your browser. Please consider downloading the logs instead.

Download

To download a copy of any local log file (or Web Access/Error log), simply click the **Download** button located under the **Actions** column.

Rotate

Aside from automatic log rotation, you can directly rotate the current **webui.log** from memory to disk from the Sonus SBC 2000 Web interface. To do so, simply click the **Rotate** button located under the **Actions** column.

Please note that the system can store up to 6 local log files. When rotating the current log file, the 6th local log file on disk is deleted to make way for the newly rotated file.

Working with Local Logs

> **Local logging is not supported on Sonus SBC 1000 models**. Instead, please use Remote logging.

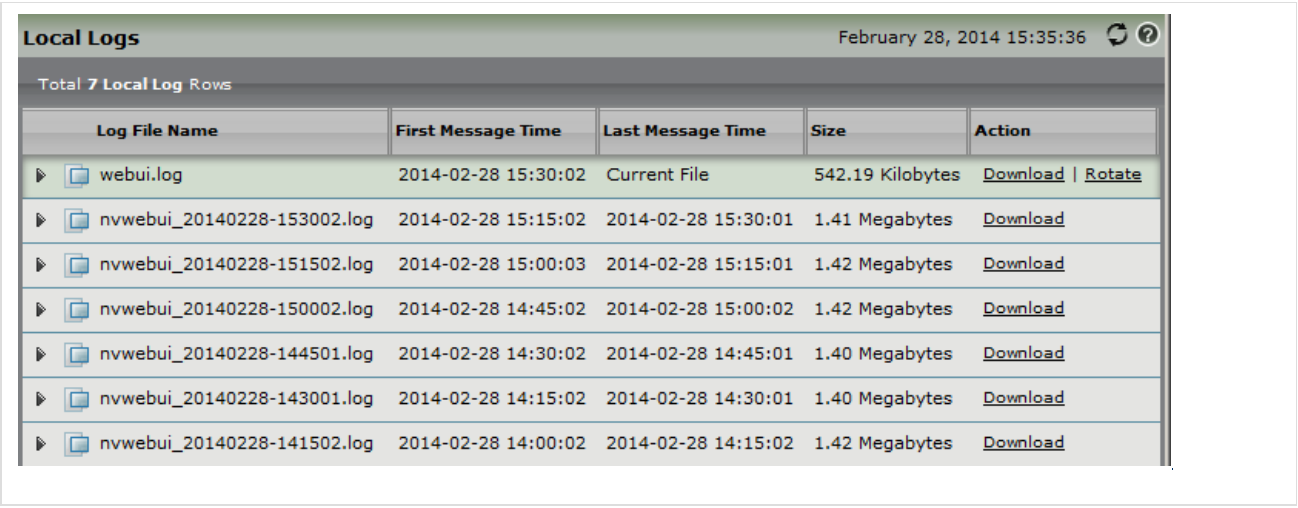
The Local logging facility maintains two differently named log files:

- **webui.log**: This file contains the current log messages being sent by the Sonus SBC 2000 System. The contents of this file are directly stored in-memory to reduce the I/O overhead on the overall Sonus SBC 2000 system. This log file gets automatically rotated, see Understanding Local Log Rotation Rules.
- **nvwebui_<timestamp>.log**: When the **webui.log** file is rotated manually (or automatically) its contents are copied from memory to the local Sonus SBC 1000/2000 disk. The file is then named `nvwebui_<timestamp>.log` where `<timestamp>` represents the time when **webui.log** was rotated. The Sonus SBC 1000/2000 system **stores a maximum of 6 local log files on disk**.

Access Local Logs as follows:

1. In the WebUI, click the **Diagnostics** tab.
2. In the Logs page, click the **Logs** > **Local System Logs** tab.

Copyright © 2015 Sonus Networks. All rights reserved.



Local Logs — February 28, 2014 15:35:36

Total **7 Local Log** Rows

Log File Name	First Message Time	Last Message Time	Size	Action
webui.log	2014-02-28 15:30:02	Current File	542.19 Kilobytes	Download | Rotate
nvwebui_20140228-153002.log	2014-02-28 15:15:02	2014-02-28 15:30:01	1.41 Megabytes	Download
nvwebui_20140228-151502.log	2014-02-28 15:00:03	2014-02-28 15:15:01	1.42 Megabytes	Download
nvwebui_20140228-150002.log	2014-02-28 14:45:02	2014-02-28 15:00:02	1.42 Megabytes	Download
nvwebui_20140228-144501.log	2014-02-28 14:30:02	2014-02-28 14:45:01	1.40 Megabytes	Download
nvwebui_20140228-143001.log	2014-02-28 14:15:02	2014-02-28 14:30:01	1.40 Megabytes	Download
nvwebui_20140228-141502.log	2014-02-28 14:00:02	2014-02-28 14:15:02	1.42 Megabytes	Download

Working with Web Access and Web Error Logs

> **Web Access and Web Error Logs are supported on Sonus SBC 1000/2000 models.**

The Sonus SBC 1000/2000 system keeps exclusive tracking of the internal and external actions strictly having to do with the system's Web Server. The Web Server on Sonus SBC 1000/2000 is responsible for serving requests to and from the Web Interface and the Sonus SBC 1000/2000 REST API. These logs are typically used only when troubleshooting issues with Sonus SBC 1000/2000 that do not have to do with telephony traffic.

Similarly to the Local logging facility, the automatic log rotation rules applies, and user are able to **Preview**, **Download**, and **Rotate** those files.

To access Local Logs:

1. In the WebUI, click the **Diagnostics** tab.
2. In the Logs page, click the **Logs** > **Web Access Logs** OR **Web Error Logs.**

Web Access Logs — February 28, 2014 15:33:45

Total **4 Web Access Log** Rows

Log File Name	First Message Time	Last Message Time	Size	Action
lighttpd.access.log	2014-02-28 15:00:02	Current File	17.91 Kilobytes	Download
lighttpd.access.log_20140228-150002	2014-02-28 13:00:01	2014-02-28 15:00:01	7.63 Kilobytes	Download
lighttpd.access.log_20140228-130002	2014-02-28 01:00:02	2014-02-28 12:00:02	1.03 Kilobytes	Download
lighttpd.access.log_20140228-010002	2014-02-27 13:00:01	2014-02-28 00:00:01	1.03 Kilobytes	Download

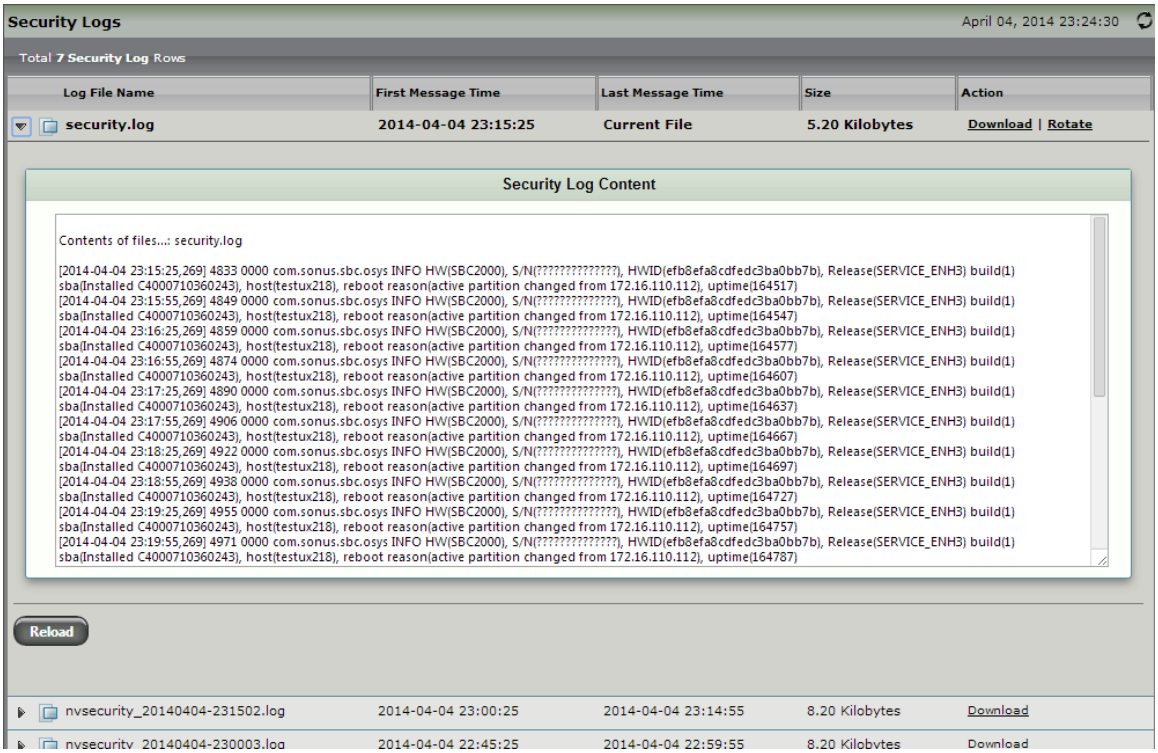
Web Error Logs — February 28, 2014 14:54:34

Total **3 Web Error Log** Rows

Log File Name	First Message Time	Last Message Time	Size	Action
lighttpd.error.log	2014-02-24 10:00:01	Current File	4.10 Kilobytes	Download
lighttpd.error.log_20140224-100002	2014-02-24 09:34:00	2014-02-24 09:34:07	1.60 Kilobytes	Download
lighttpd.error.log_20140224-090002	2014-02-20 14:00:01	2014-02-24 08:59:06	2.49 Kilobytes	Download

Working with Security Logs

Copyright © 2015 Sonus Networks. All rights reserved.



Working with System Vitals Logs

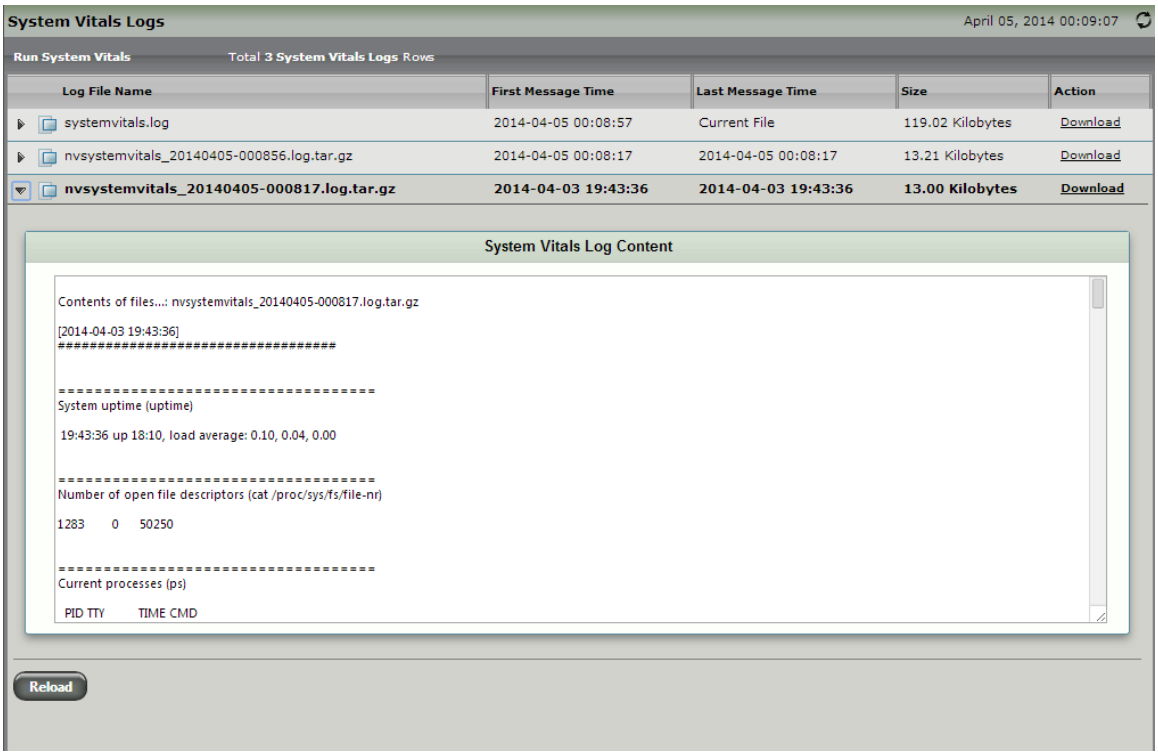
The System Vitals Log contains system statistics crucial for understanding the overall health of the system. The SBC retains the current system vitals log, plus the previous five archived as tar.gz files. When a new current file is generated the oldest archive is rotated out of the list.

Each file, current and archived, is downloadable from the WebUI.

To access the System Vitals Logs:

1. Click the **Diagnostics** tab at the top of the WebUI.
2. In the left navigation pane, go to: **Logs > System Vitals Logs**.

Copyright © 2015 Sonus Networks. All rights reserved.



Generating System Vitals Logs

To generate a System Vitals Log:

1. Click the **Diagnostics** tab at the top of the WebUI.
2. In the left navigation pane, go to: **Logs > System Vitals Logs**.
3. Click **Run System Vitals** at the top of the page.

Downloading System Vitals Logs

To download a System Vitals Log:

1. **In the System Vitals Logs table, click the Download link in the row for the log you wish to download.**
2. Browse for the location in which to save the downloaded log.
3. Click **Save**.

Setting the Local Log Level

The system-wide Local logging can be tuned to a specific Supported Logging Levels. Once the level has been set, all local logging messages with the desired level will be stored in the Sonus SBC 1000/2000 internal storage.

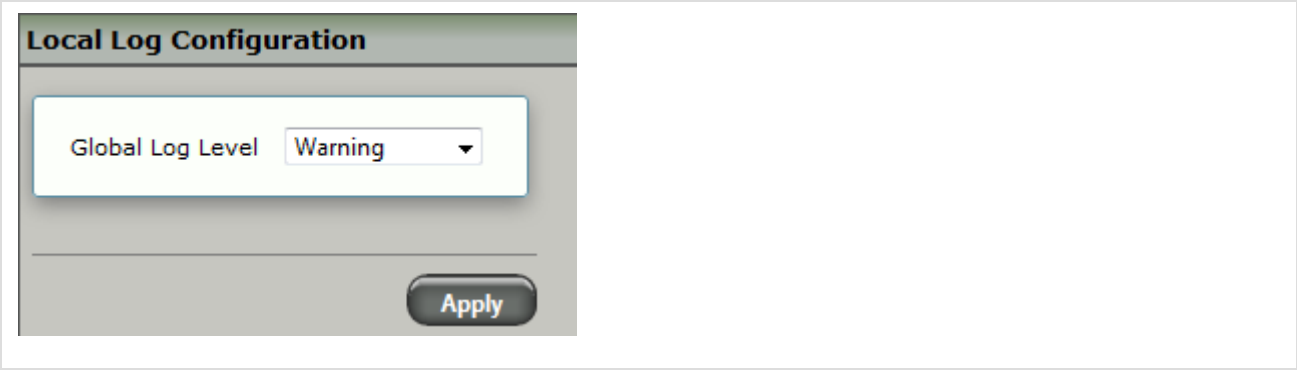
> This configurable setting also represents the **default local logging level** on the Sonus SBC 1000/2000 System. This default setting can be reused when configuring logging at the Subsystem level.

How to Set the Local Log Level

To set the local log level

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Logging Configuration > Local Log**

Copyright © 2015 Sonus Networks. All rights reserved.



3. Select a logging level from the **Global Log Level** menu.
4. Click **Apply**.

Understanding Local Log Rotation Rules

The **webui.log** (in-memory) log file automatically rotates from memory to the internal storage if any one of the following three events occurs:

- A period of 15 minutes elapses
- The log file grows to > 50MB in size (this is an approximate size checked by the system every 1-2 minutes)
- The user manually forces the rotation of the log file to the internal storage via the Web interface (to start with a fresh log for a tracing session)

Regardless of which case causes the logs to be rotated to the internal storage, only the newest 6 log files will be retained at any time. Older log files are automatically deleted from the internal storage. As a result, a maximum of 300MB (6 * 50MB) of logs can be retained in the Sonus SBC2000 internal storage.

> **NOTE:**
>
> There is no internal storage of logs on the SBC 1000.

Supported Logging Levels

The Sonus SBC 1000/2000 system supports the following logging levels ---- each level provides more logging information than the level before it:

Log Level	Local Logging (1)	Remote Logging	Guideline
Trace	✗	✓	Debug level trace used by developers. Logs the inner working of each module and could impact system performance.
Debug	✗	✓	Includes code issues. This level and lower are intended to solve bugs in the relevant code, or possibly may be required when encountering an interoperability issue.
Informational	✓	✓	Includes call path and connection tracing information. This level and higher is sufficient to troubleshoot all configuration, setup, and interoperability issues.
Warning	✓	✓	An error has been detected, probably from an external source, which may require operator intervention. A call or other connection may have failed, or be in danger of failing.

Copyright © 2015 Sonus Networks. All rights reserved.

Error	✅	✅	An error has been detected from an internal source, which may require operator intervention. A call has failed or capacity is reduced.
Fatal	✅	✅	An error so severe that the entire system is in danger of shutdown or reboot. This condition has probably triggered one or more alarms as well.

Trace provides the most verbose logging and **Fatal** provides the least verbose logging. The default level is **Informational**, meaning warnings and errors are displayed in addition to basic telephony and system-wide logging. Sometimes it is useful to adjust this level to see more detail.

> **(1) Local Logging**
>
> The 'Trace' and 'Debug' levels are not configurable when Setting the Local Log Level because they produce the most output and may impact overall system performance. These levels are however available when configuring Local logging at the Subsystems level.

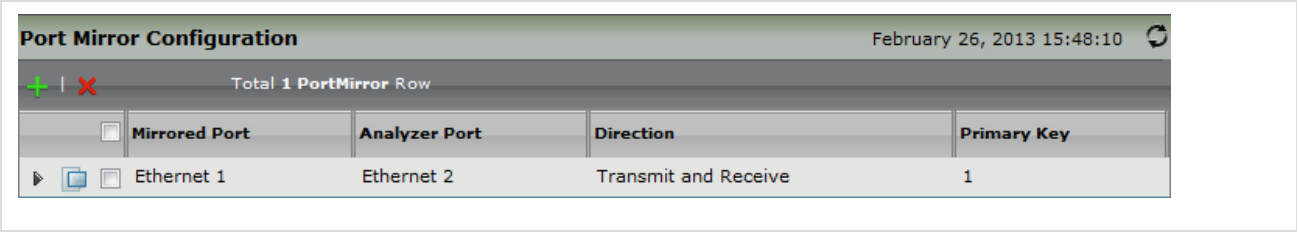
Working with Port Mirroring

Port mirroring allows the network traffic on one port to be passively copied onto another port. That traffic can then be captured and analyzed.

Configuring Port Mirroring

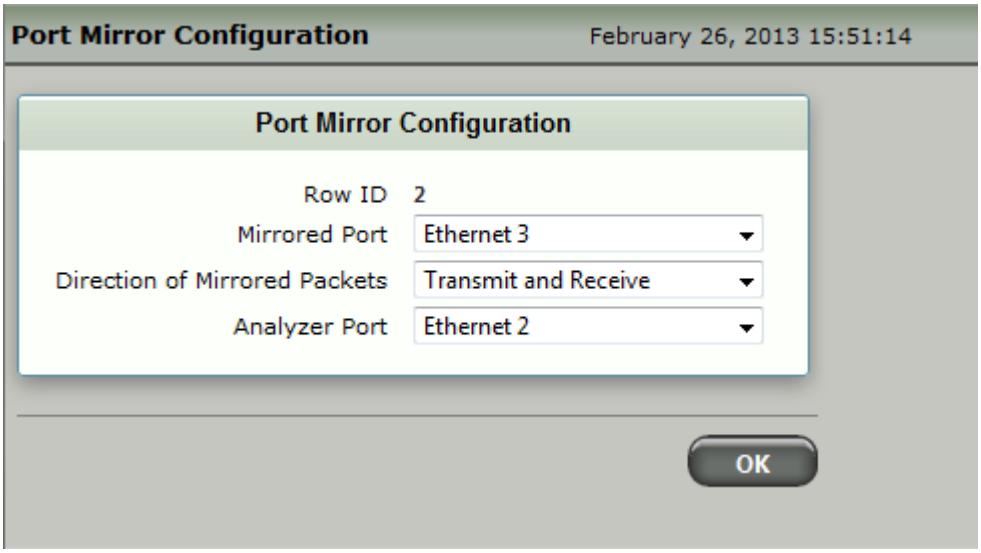
To configure port mirroring:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Logging Configuration > Port Mirror**.



3. Click the **Create Mirror Port** (+) icon at the top of the page.

Copyright © 2015 Sonus Networks. All rights reserved.



Port Mirror Configuration - Field Definitions

The mirrored port and the analyzer port must not be members of the same VLAN

Mirrored Port

Specifies the port to be mirrored.

The Mirrored Port cannot be the same port as the Analyzer Port.

Direction of Mirrored Packets

Specified the directionality of the mirrored packets.

Analyzer Port

Specifies the analyzer (destination) port of the mirrored packets. There may only be one analyzer port specified for the Sonus SBC 1000/2000 at any time. To change the analyzer port, all entries in the Port Mirror Configuration table must be deleted and re-entered with the new analyzer port.

Working with Ethernet Interfaces and IP

This section contains information about how to manage the way the Sonus SBC 1000/2000 interfaces with the network.

Managing Logical Interfaces

- Configuring and Modifying Logical Interfaces
- Configuring and Modifying Loopback Addresses

Managing Static IP Route Tables

- Creating Entries in a Static IP Route Table

Copyright © 2015 Sonus Networks. All rights reserved.

Managing Static ARP Tables

- Creating Entries in a Static ARP Table

Modifying the Sonus SBC 1000-2000 IP Address

- Modifying the Sonus SBC 1000 IP Address
- Modifying the Sonus SBC 2000 IP Address

How the Sonus SBC 1000-2000 Routes IP Traffic to a NIC

Managing the Hosts Table

- Creating Entries in the Hosts Table

Managing VLANs

- Creating and Modifying VLANs
- Viewing VLAN Counters
- Modifying Default VLAN

Managing Logical Interfaces

The Logical Interfaces section configures IP addresses for the Ethernet ports and VLANs. Detailed description of the IP addresses for each of the Sonus SBC 1000/2000 platforms is given below. To configure the physical layer settings and VLANs for the Ethernet ports, go to Ports.

On this page:

- About Logical Interfaces - Sonus SBC 1000
  - Ethernet IP
- About Logical Interfaces - Sonus SBC 2000
  - Administrative IP
  - Ethernet IP
- About Logical Interfaces - VLAN Interfaces
- Managing Logical Interfaces
  - Configuring and Modifying Logical Interfaces
  - Configuring and Modifying Loopback Addresses

About Logical Interfaces - Sonus SBC 1000

The Sonus SBC 1000 supports two system created logical interfaces (known as **Ethernet 1 IP** and **Ethernet 2 IP**) used to hold the IP addresses of the Ethernet ports 1 and 2 respectively (see item #8 on the Sonus SBC 1000 Front Panel). In addition to the system created logical interfaces, the Sonus SBC 1000/2000 also supports user created VLAN logical interfaces. VLAN logical interfaces are created each time a VLAN is added to the system, and are further described in the About Logical Interfaces - VLAN Interfaces subsection below.

Ethernet IP

When delivered from the factory, **Ethernet 1 IP** is enabled with DHCP by default, and an IP address is acquired via a connected DHCP server. This IP address is used for performing Initial Setup on the Sonus SBC 1000. See Running Initial Setup for more information.

The default IP address for the logical interface named **Ethernet 2 IP** is 192.168.129.2. After initial configuration, you

Copyright © 2015 Sonus Networks. All rights reserved.

may configure this logical interface using Settings or Tasks tabs in the WebUI.

The IP addresses configured on the two logical interfaces and the VLAN interfaces are used for transporting all the VOIP media packets (e.g., RTP, SRTP) and all protocol packets (e.g., SIP, RTCP, TLS). DNS servers of the customer's network should map the Sonus SBC 1000/2000 system hostname to the configured IP addresses. The hostname or these IP addresses may be used by UC-enabling systems such as SIP-phones, IP-PBX and Microsoft Lync Servers and for accessing Sonus SBC 1000/2000 WebUI.

About Logical Interfaces - Sonus SBC 2000

The Sonus SBC 2000 supports five system created logical interfaces (known as **Administrative IP**, **Ethernet 1 IP**, **Ethernet 2 IP**, **Ethernet 3 IP**, and **Ethernet 4 IP**) used to hold the IP addresses of the Admin port and each of the four Ethernet ports (see item #7, 8, 9 on the Sonus SBC 2000 Front Panel). In addition to the system created logical interfaces, the Sonus SBC 1000/2000 also supports user created VLAN logical interfaces. VLAN logical interfaces are created each time a VLAN is added to the system, and are further described in the About Logical Interfaces - VLAN Interfaces subsection below.

Administrative IP

The Sonus SBC 2000 system defines a logical interface called the Admin IP (Administrative IP, also known as the Management IP). This logical interface is used to hold the IP address of the Admin Ethernet port (see item #7 on the Sonus SBC 2000 Front Panel). A secondary IP address may be configured for this logical interface. The primary IP address is a factory-default IP address of 192.168.128.2/24 and it is used for running Initial Setup of the Sonus SBC 1000/2000 system.

> The Administrative IP port should only be used for Running Initial Setup and disconnected when not in use (especially to avoid conflicts with your network). This interface **cannot be used for VOIP media or protocols**.

Ethernet IP

The Sonus SBC 1000/2000 system has one predefined logical interface for each of the four Ethernet ports. In most deployments, one of these logical interfaces (typically **Ethernet 1 IP**) and its assigned IP address is used for transporting all the VOIP media packets (e.g., RTP, SRTP) and all protocol packets (e.g., SIP, RTCP, TLS). DNS servers of the customer's network should map the Sonus SBC 1000/2000 system hostname to this IP address. The hostname or these IP addresses may be used by UC-enabling systems such as SIP-phones, IP-PBX and Microsoft Lync Servers and for accessing Sonus SBC 1000/2000 WebUI.

By default, each of the four Ethernet ports is set up to use its matching logical interface (e.g. **Port Ethernet X** uses **Ethernet X IP**) for IP layer communication, but this can be changed by configuring the VLAN settings on the Ethernet port.

When delivered from the factory, **Ethernet 1 IP** is enabled with DHCP by default, and an IP address is acquired via a connected DHCP server. This IP address is used for performing Initial Setup on the Sonus SBC 1000. See for Running Initial Setup more information. The default IP address for the logical interface named **Ethernet 2 IP** is 192.168.129.2. After initial configuration, you may configure this logical interface using Settings or Tasks tabs in the WebUI.

About Logical Interfaces - VLAN Interfaces

As described in the Managing VLANs section, each time a VLAN is created, a matching Logical Interface is also automatically created. This Logical Interface allows you to configure an IP address and have IP layer access for this

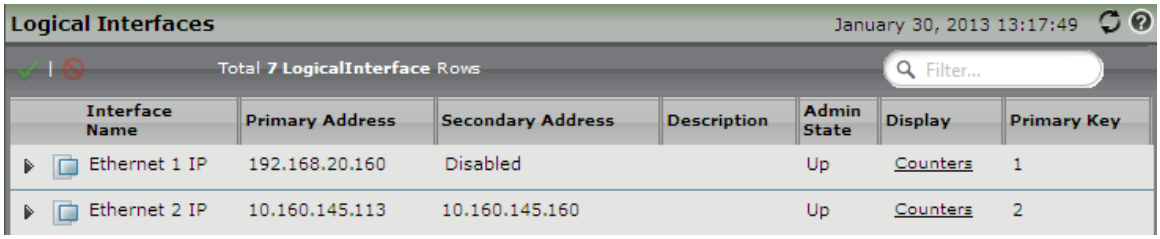
Copyright © 2015 Sonus Networks. All rights reserved.

VLAN. The configured IP address can be accessed through any Ethernet port that is associated with the given VLAN. VLAN Logical Interfaces behave the same as any other Logical Interface, and can be used for transporting VOIP media packets (e.g. RTP, SRTP), protocol packets (e.g. SIP, RTCP, TLS), and/or dynamic routing.

> When a VLAN Logical Interface is first created, it will be disabled by default.

Managing Logical Interfaces

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Logical Interfaces**.



To view an interface's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

> **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

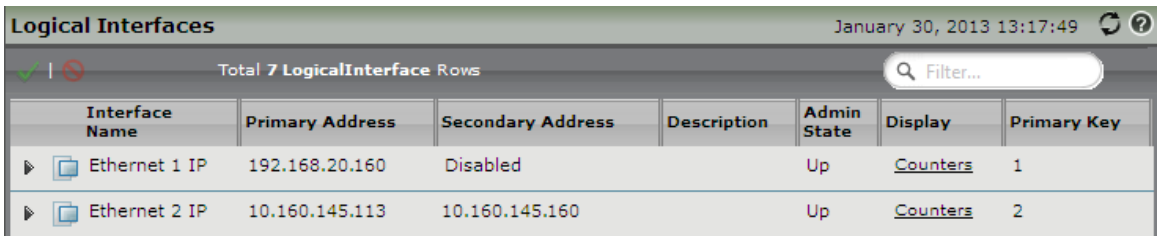
Configuring and Modifying Logical Interfaces

Configuring and Modifying Loopback Addresses

Configuring and Modifying Logical Interfaces

Modifying, Enabling, and Disabling a Logical Interface

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Logical Interfaces**.



> The Administrative IP port should only be used for Running Initial Setup and disconnected when not in use (especially to avoid conflicts with your network). This interface **cannot be used for VOIP media or protocols**.

Copyright © 2015 Sonus Networks. All rights reserved.

Each logical interface can have a primary IP address and a secondary IP address (as illustrated above). The secondary IP address is useful for WebUI or Sonus SBC 1000-2000 API User's Guide operations only, and should not be used for VOIP media or protocols such as SIP, RTP and SRTP.

By configuring the **IP Assign Method** to DHCP, the DNS server(s), NTP server(s), domain name and the default IP Route will be overwritten and configured dynamically.

Note: The functionality of enabling and disabling system created logical interfaces (e.g. Ethernet 1, Ethernet 2, etc.) is available on the Sonus SBC 2000 only. Enabling and disabling VLAN logical interfaces can be done on all platforms.

To modify a Logical Interface:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required.

To enable a Logical Interface:

1. Select the check box next to the entry you wish to enable.
2. Click the **Enable** ( ) icon at the top of the table.

To disable a Logical Interface:

1. Select the check box next to the entry you wish to disable.
2. Click the **Disable** ( ) icon at the top of the table.

Configuring Logical Interfaces

The Logical Interfaces are configured when Running Initial Setup. Once initial configuration is complete, the fields below are able to be modified.

Identification/Status - Field Definitions

Alias

Specifies an alias for the interface.

Description

Specifies a description for the interface.

Admin State

Specifies the administrative state of the port. Valid entries: **Enabled** or **Disabled**.

Networking - Field Definitions

IP Assign Method

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies how the IP address is assigned for that interface. Select from the drop down box. Available options: **Static** (User configured IPv4 address, netmask and system network configuration) or **DHCP** (DHCP is used to automatically acquire IPv4 address, netmask, and other system network configuration). **WARNING:** If you set the IP Assign method to DHCP, the DNS server(s), NTP server(s), domain name and the default IP Route will be overwritten and configured dynamically.

If you are configuring the IP Assign method from DHCP to Static, you should add a new default static route. We recommend this be done through the **Modify Ethernet IP** task (this allows you to set the IP address and the default route in one step). See Modifying the Sonus SBC 1000 IP Address and Modifying the Sonus SBC 2000 IP Address.

Primary Address

Specifies the Primary IP Address through which the Sonus SBC 1000/2000 communicates over Ethernet, and by which the application may be accessed. This field is available only when the IP Assign Method field is set to **Static**.

Primary Netmask

Specifies the network mask applied to the Primary IP Address. This field is available only when the IP Assign Method field is set to **Static**.

Configure Secondary Interface

Specifies whether a Secondary IP address and Secondary Netmask should be configured. Available options: **Enabled** (enables the Secondary Address/Netmask options) or **Disabled** (disables the Secondary Address/Netmask options). This field is available only when the IP Assign Method field is set to **Static**.

Secondary Address

Specifies the Secondary IP Address through which the Sonus SBC 1000/2000 communicates over Ethernet, and by which the application may be accessed. This field is available only when the **Configure Secondary Interface** field is set to Enabled.

Secondary Netmask

Specifies the network mask applied to the Secondary IP Address. This field is available only when the **Configure Secondary Interface** field is set to Enabled.

ACL IN

Specifies the Access Control List to be used on this interface when filtering incoming packets. Select from the drop down list (populated from the Access Control List table). For more information about Access Control Lists, see Managing Access Control Lists.

ACL Out

Specifies the Access Control List to be used on this interface when filtering outgoing packets. Select from the drop down list (populated from the Access Control List table). For more information about Access Control Lists, see Managing Access Control Lists.

Copyright © 2015 Sonus Networks. All rights reserved.

ACL Forward

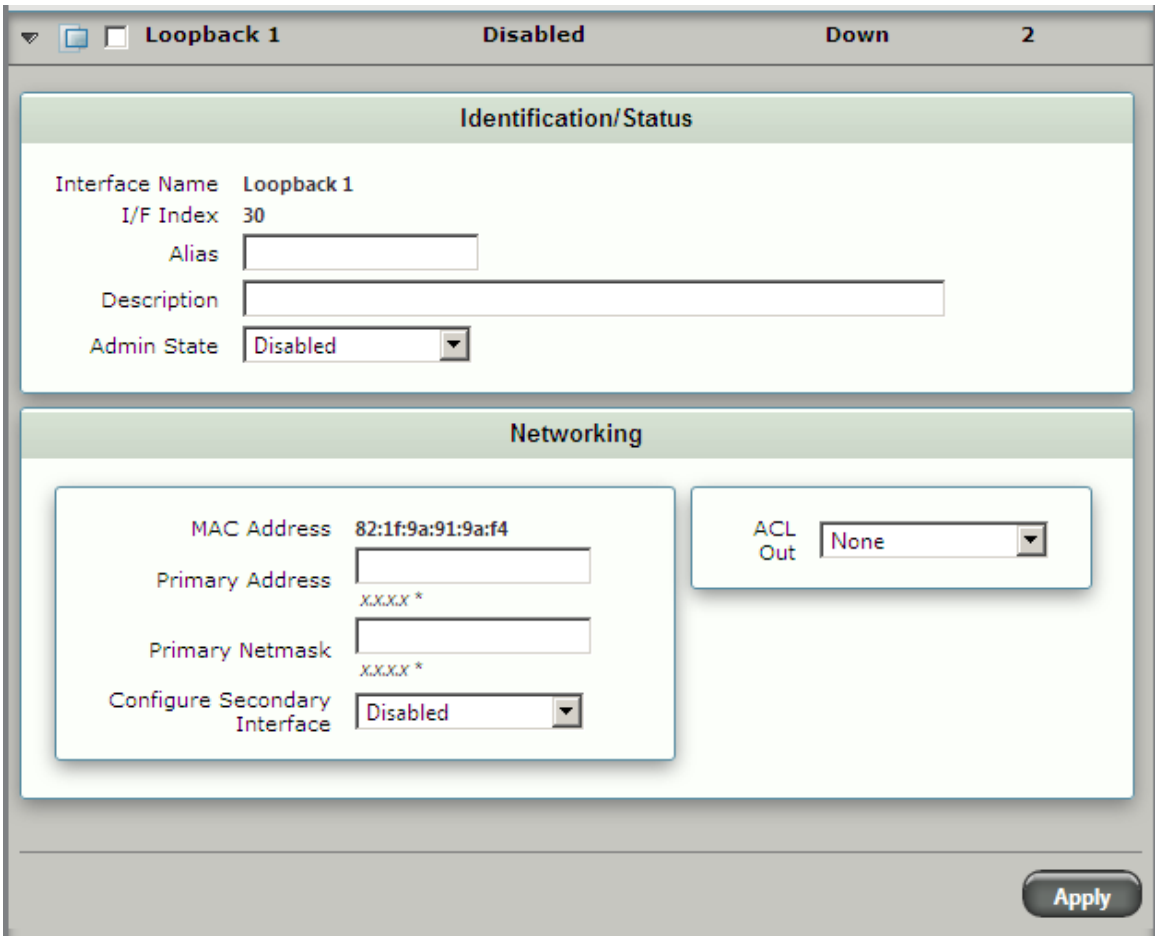
Specifies the Access Control List to be used when filtering forwarded (i.e. routed) packets received on this interface. Select from the drop down list (populated from the Access Control List table). For more information about Access Control lists, see Managing Access Control Lists.

Configuring and Modifying Loopback Addresses

This procedure describes how to add or modify a Loopback Address.

Modifying, Enabling and Disabling a Loopback Interface

Note: The functionality of enabling and disabling logical interfaces is available on the Sonus SBC 2000 only.



To modify a Loopback Interface:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required.

To enable a Loopback Interface:

1. Select the check box next to the entry you wish to enable.
2. Click the **Enable** ( ) icon at the top of the table.

Copyright © 2015 Sonus Networks. All rights reserved.

To disable a Loopback Interface:

1. Select the check box next to the entry you wish to disable.
2. Click the **Disable** ( ) icon at the top of the table.

Configuring Loopback Interfaces

> Before you configure a loopback interface, make sure that static and/or dynamic routing has been correctly configured to handle a Sonus SBC 1000/2000 with a loopback interface.
> **Example:**

Sonus SBC 1000/2000	Loopback IP: 172.16.40/24	App-IP: 138.51.200.220/24
Cisco Router	Eth4/0: 138.51.200.220/24	

In this example the Cisco device can ping 138.51.200.220. But, by default, it is unable ping 172.16.40.1. So a static route must be established on the Cisco device before it can reach 172.16.40.0/24 through 138.51.200.220.

> Note that both 172.16.40.1 and 138.51.200.220 identify the same Sonus SBC 1000/2000.

The advantage of using a loopback interface is that SIP may use 172.16.40.1 in its configuration, and the interface IP addresses may be changed without impacting current calls in progress or SG configurations. When interface IP addresses are changed, it may affect RTP/RTCP packets using that interface, as would any network-level change. Calls in progress or SG configurations on the Sonus SBC 1000/2000 and other SIP-layer peers of Sonus SBC 1000/2000 will not have to be suspended, re-configured, torn-down, or re-established in any way. The applications use IP addresses completely isolated from the IP addresses that are used on the links/networks.

Identification/Status - Field Definitions

The Identification/Status Panel controls the network identity of the port and its administrative state (Up or Down). It also provides the port's current service status and when that status last changed.

Port Alias

Specifies an alias for the port. This text is configured by the operator for exclusive use by SNMP-based element and network management systems to assign a key to the port or interface, that is unique across the managed network. Examples would be "Node10Port5" and "VerizonPort5"

Admin State

Specifies the administrative state of the port. Valid entries: **Enabled** or **Disabled**.

Networking - Field Definitions

Primary/Secondary Address

Specifies the Primary or Secondary IP Address of this loopback interface.

Primary/Secondary Netmask

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the network mask applied to either the Primary or Secondary IP Address.

Configure Secondary Interface

Specifies whether or not a secondary IP address is configured for this loopback interface.

ACL Out

Specifies the Access Control List to be used on this interface when filtering outgoing packets. Select from the drop down list (populated from the Access Control List table). For more information about Access Control Lists, see Managing Access Control Lists.

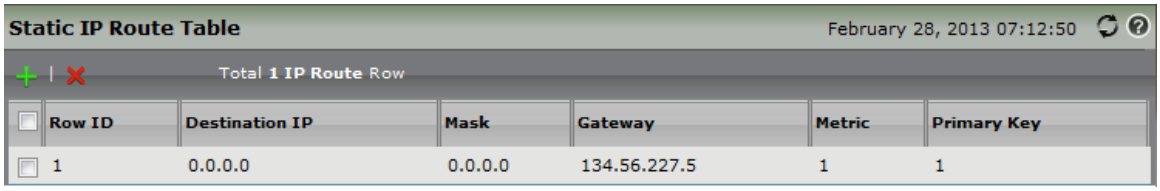
Managing Static IP Route Tables

Static IP Routes allow one to manually specify the next hop routers used to reach other networks. This is also where you specify the default routes for the connected IP networks (which use `0.0.0.0` as the Destination and Mask).

When DHCP is configured on an interface, the default Static Route (0.0.0.0/0) will be removed and configured dynamically. To view the dynamically created default route, access the WebUI and navigate to **Protocols > IP > Routing Table**.

Working with Static IP Route Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Static Route Table**.



To view a Static IP Route Table's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating Entries in a Static IP Route Table

Creating Entries in a Static IP Route Table

To create an Entry in a Static IP Route Table (via Settings Menu):

1. In the WebUI, click the **Settings** tab.

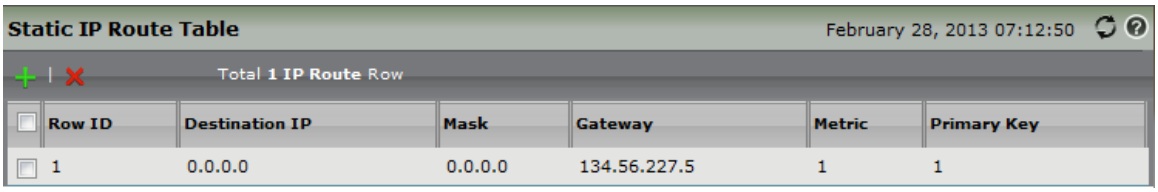
Copyright © 2015 Sonus Networks. All rights reserved.

2. In the left navigation pane, go to **Protocols > IP > Static Route Table**.

OR

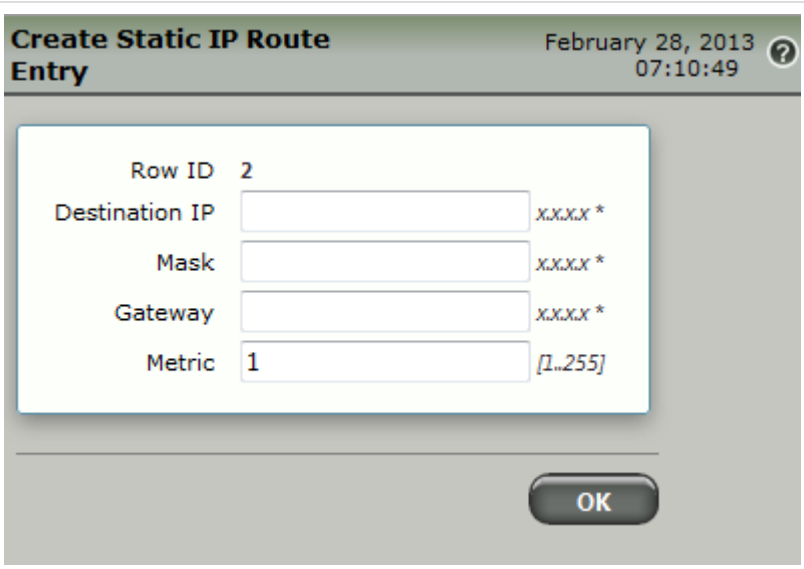
To create an Entry in a Static IP Route Table (via Tasks Tab)

1. In the WebUI, click the **Tasks**tab.
2. In the left navigation pane, go to **IP/Protocols** and click **Setup Static Route.**



Creating an Entry in a Static IP Route Table

1. Click the **Create Static IP Route** (+) icon at the top of the Static IP Route Table page.



Destination IP

Specifies the destination IP Address

Mask

Specifies the network mask of the destination host or subnet. If the 'Destination IP Address' field and 'Mask' field are both 0.0.0.0, the static route is called 'default static route'.

Gateway

Specifies the IP Address of the next-hop router to use for this Static Route.

Metric

Copyright © 2015 Sonus Networks. All rights reserved.

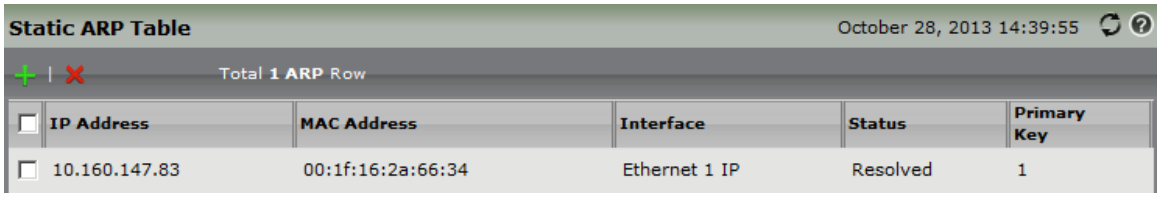
Specifies the cost of this route and hence indirectly specifies the preference of the route. Lower values indicate more preferred routes. Typical value is 1 for most static routes indicating that static routes are preferred to dynamic routes.

Managing Static ARP Tables

Static ARP tables manually map IP addresses to physical MAC addresses. This mapping is normally performed automatically, so Static ARP's are seldom used. They can be useful for troubleshooting and very specific performance optimization.

Working with Static ARP Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Static ARP Tables**.



To view a Static ARP Table's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

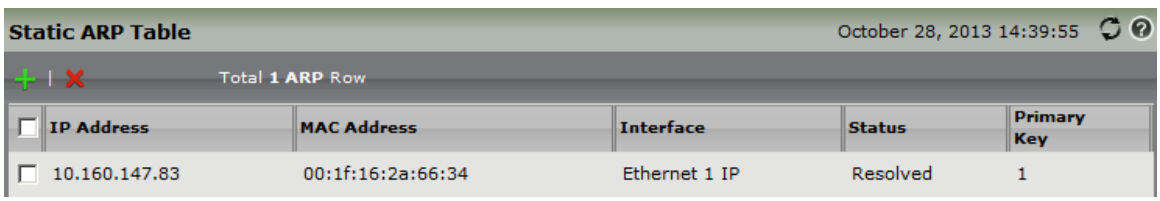
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating Entries in a Static ARP Table

Creating Entries in a Static ARP Table

To create an Entry in a Static ARP Table:

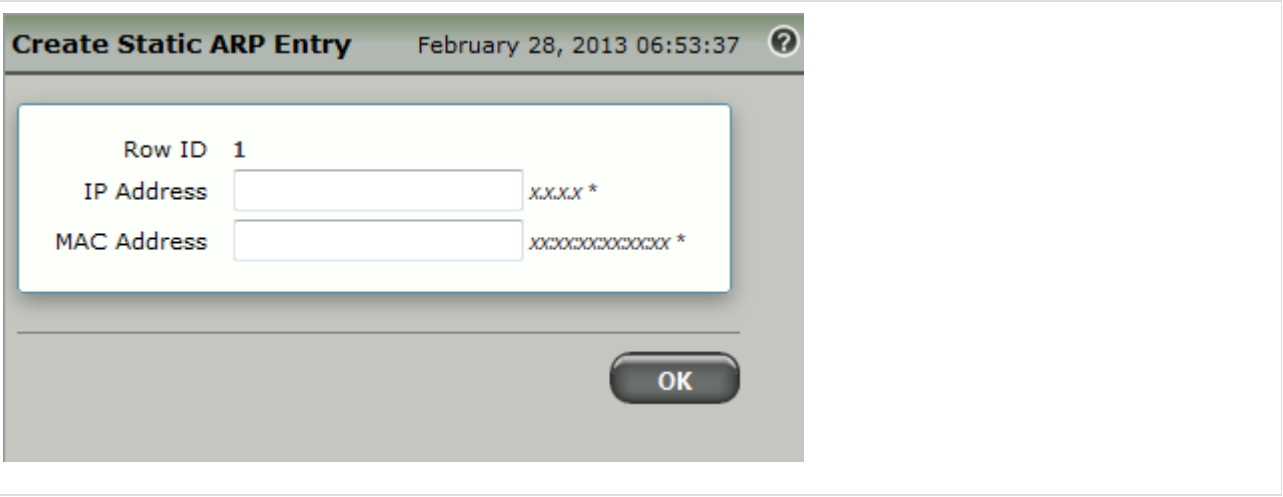
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Static ARP Tables**.



Creating an Entry in a Static ARP Table

Copyright © 2015 Sonus Networks. All rights reserved.

1. Click the **Create Static ARP Table Entry** ( ) icon at the top of the Static ARP Table page.



2. Enter an IP Address (IPv4 only).
3. Enter a MAC Address.
4. Click **OK**

> The IP address (and subsequent MAC address) must belong to a device which is a member of a subnet defined for the Sonus SBC 1000/2000.

Modifying the Sonus SBC 1000-2000 IP Address

You may for various reasons, such as change in your network topology, need to change the IP Address and/or the Default Gateway on your Sonus SBC 1000/2000. You may also wish to configure a Secondary IP Address for the Sonus SBC 1000/2000. A secondary IP address gives the Sonus SBC 1000/2000 the ability to be part of another IP subnet on the same Ethernet port. Configuring a Secondary IP Address is accomplished using the same UI elements as changing the IP Address.

> The recommended method of changing the Sonus SBC 1000/2000 IP and/or Default gateway is through the **Tasks Tab** in the WebUI. This is because the IP Addresses and Default Gateway IP Address must be changed simultaneously. Other methods of accomplishing this task are strongly discouraged as they will, in all likelihood, result in a loss of communication with the Sonus SBC 1000/2000.

Modifying the Sonus SBC 1000 IP Address

Modifying the Sonus SBC 2000 IP Address

Modifying the Sonus SBC 1000 IP Address

The **Sonus SBC 1000** requires that you explicitly configure each Ethernet port. At least one IP address must be configured and it is not necessary to configure both IP addresses. An optional Secondary IP address may be configured on each of the Ethernet ports.

> The secondary IP address is useful for WebUI or API operations only, and should not be used for VOIP media or protocols such as SIP, RTP and SRTP.

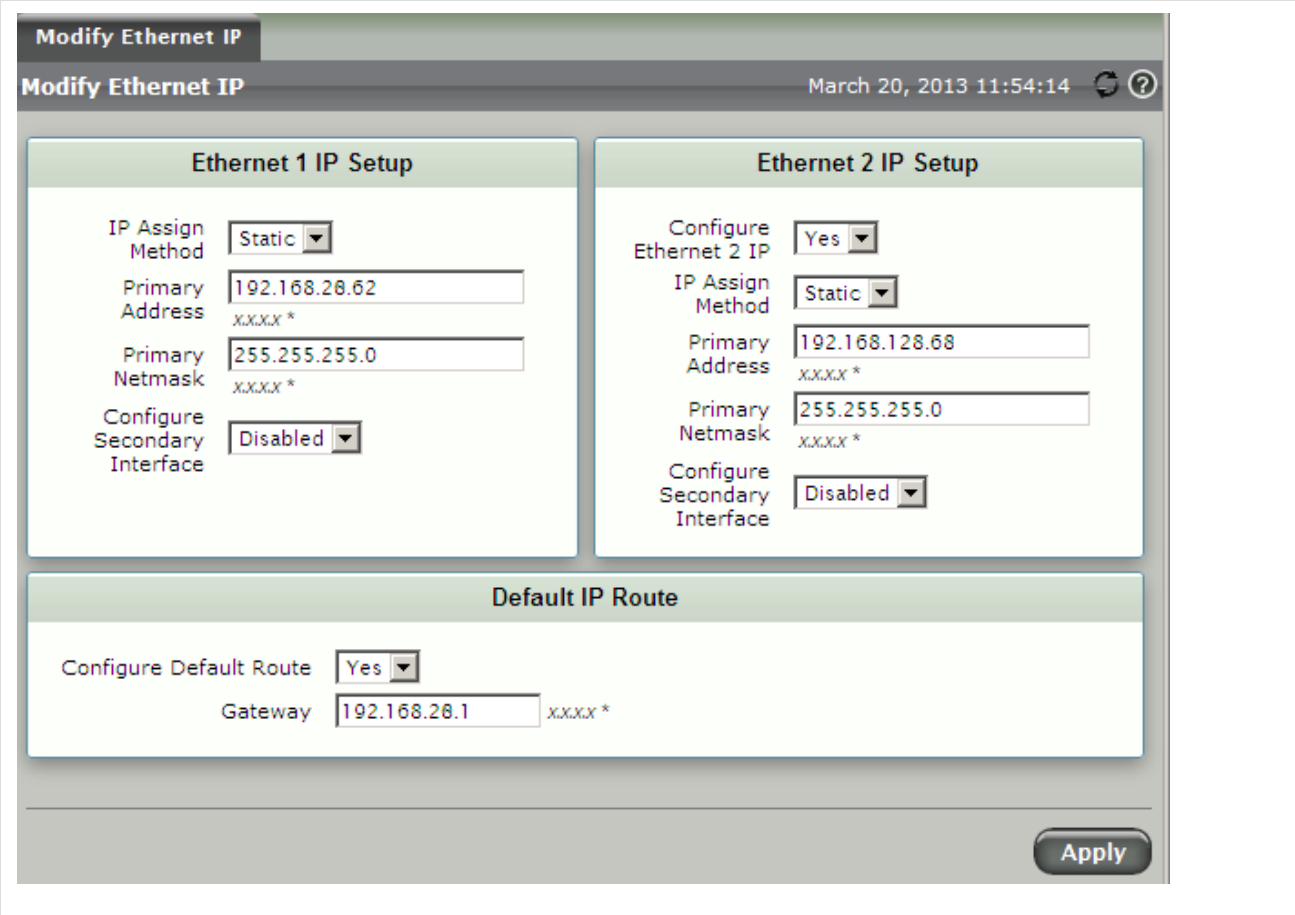
Copyright © 2015 Sonus Networks. All rights reserved.

Important Notes

- The primary IP address assigned to **Ethernet 1 IP** cannot be removed.
- The primary IP address assigned to **Ethernet 2 IP** can be removed by setting the IP address to **0.0.0.0** and setting the Netmask to a valid non-zero value (e.g. **255.255.255.0**).
- If configuring a default route, then the **Gateway** must set such that it is part of exactly one of the configured IP subnets.

To Modify the IP Address on the Sonus SBC 1000

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **IP Protocols**, click **Modify Ethernet IP Address**.



3. Modify the Ethernet 1 IP Setup information as necessary (if required, modify the Ethernet 2 IP Setup information).
4. Modify the Default IP Route information as necessary.

Ethernet IP Setup- Field Definitions

IP Assign Method

Specifies how the IP address is assigned for that interface. Select from the drop down box. Available options: **Static** (user configured IP address) or **DHCP** (DHCP is used to automatically acquire the IP address). When this field is set to DHCP, the remaining fields are not displayed.

Primary/Secondary Address

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the Primary or Secondary IP Address through which the Sonus SBC 1000/2000 communicates over Ethernet, and by which the application may be accessed. In order to remove a primary IP address assigned to **Ethernet 2 IP** specifically, refer to the note at the top of the page.

Primary/Secondary Netmask

Specifies the network mask applied to either the Primary or Secondary IP Address.

Configure Secondary Interface

Specifies whether or not a secondary Application IP address is configured for the Sonus SBC 1000/2000.

Configure Default Route

Specifies whether or not a Default Static IP Route is configured. If this option is enabled, a Default Static IP Route will be created in the Static IP Route Table. The Gateway IP Address for this route will be the IP Address specified in the **Gateway** field, and a value of **0.0.0.0** will be applied in the Destination IP field such that any address on the gateway is reachable.

The Configure Default Route field is not visible if any of the interfaces are using DHCP.

Gateway

Specifies the IPv4 Address of the Default Gateway used by the Sonus SBC 1000/2000. This field is only available if the **Configure Default Route** field was set to **Yes**.

The Gateway field is not visible if any of the interfaces are using DHCP.

Modifying the Sonus SBC 2000 IP Address

The following procedure describes how to change the SBC2000 Ethernet IP address. When configuring the IP address, an optional Secondary IP address may also be configured on the Ethernet port.

The secondary IP address is useful for WebUI or API operations only, and should not be used for VOIP media or protocols such as SIP, RTP and SRTP.

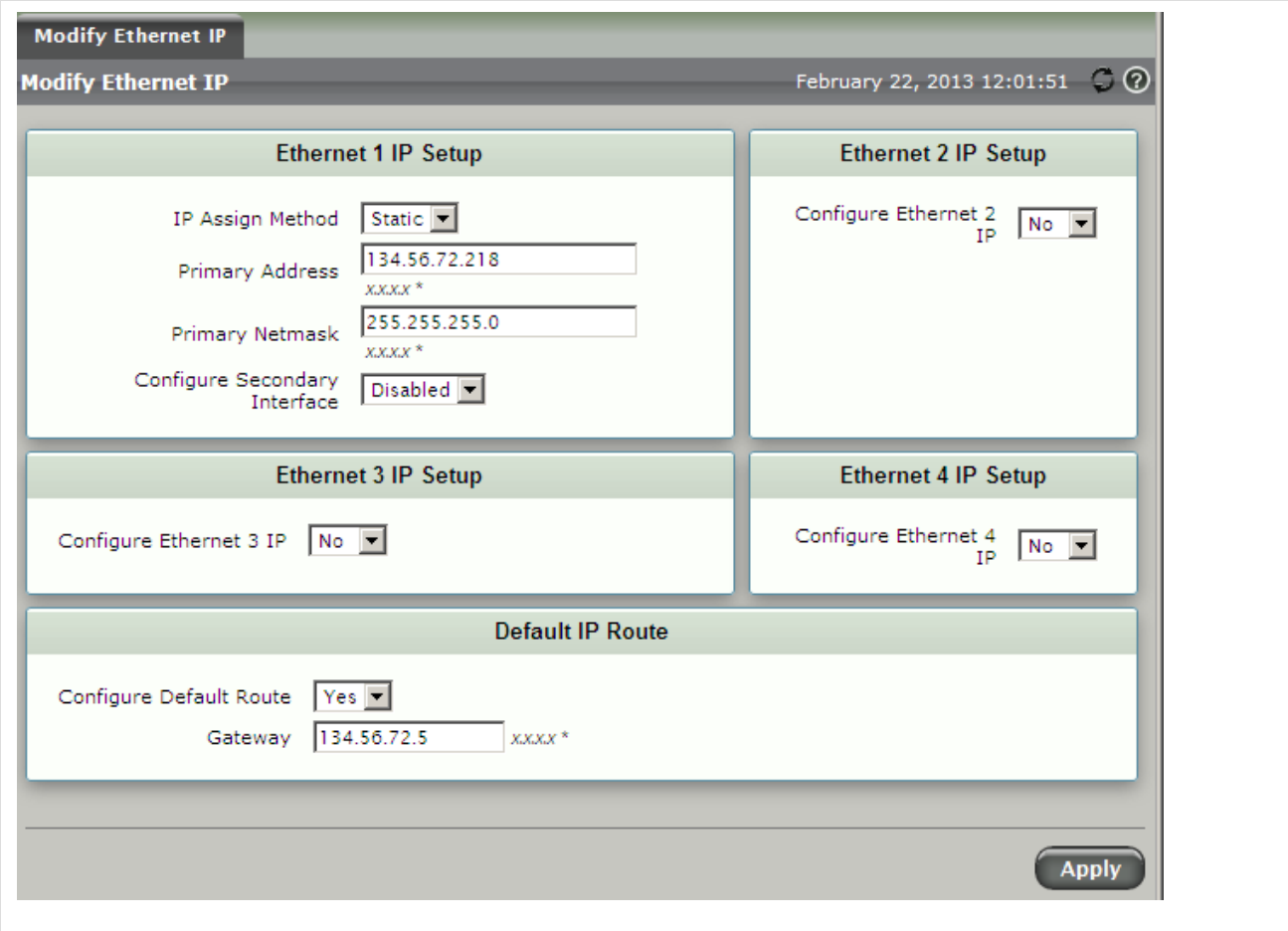
Helpful Tips

- The primary IP address assigned to **Ethernet IP** may be removed by setting the IP address to **0.0.0.0** and setting the Netmask to a valid non-zero value (e.g. **255.255.255.0**).
- The **Ethernet IP Address** assigned to any Sonus SBC 2000 Logical Interface may also be removed using the same procedure.

To Modify the IP Address on the SBC

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **IP Protocols** section, click **Modify Ethernet IP Address**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Modify the Ethernet 1 IP Setup information as necessary (if required, modify the Ethernet 2 IP, Ethernet 3 IP, and Ethernet 4 IP Setup information).
4. Modify the Default IP Route information as necessary.

Ethernet IP Setup - Field Definitions

IP Assign Method

Specifies how the IP address is assigned for that interface. Select from the drop down box. Available options: **Static** (user configured IP address) or **DHCP** (DHCP is used to automatically acquire the IP address). When this field is set to DHCP, the remaining fields are not displayed.

Primary/Secondary Address

Specifies the Primary or Secondary IP Address through which the SBC communicates over Ethernet, and by which the applications may be accessed. Refer to the note at the top of the page.

Primary/Secondary Netmask

Specifies the network mask applied to either the Primary or Secondary IP Address.

Configure Secondary Interface

Specifies whether or not a secondary Ethernet IP address is configured for the SBC.

Copyright © 2015 Sonus Networks. All rights reserved.

Configure Default Route

Specifies whether or not a Default Static IP Route is configured.

If this option is enabled, a Default Static IP Route will be created in the Static IP Route Table. The Gateway IP Address for this route will be the IP Address specified in the **Gateway** field, and a value of **0.0.0.0** will be applied in the Destination IP field such that any address on the gateway is reachable.

The Configure Default Route field is not visible if any of the interfaces are using DHCP.

Gateway

Specifies the IPv4 Address of the Default Gateway used by the Sonus SBC 1000/2000. This field is only available if the **Configure Default Route** field was set to **Yes**.

The Gateway field is not visible if any of the interfaces are using DHCP.

How the Sonus SBC 1000-2000 Routes IP Traffic to a NIC

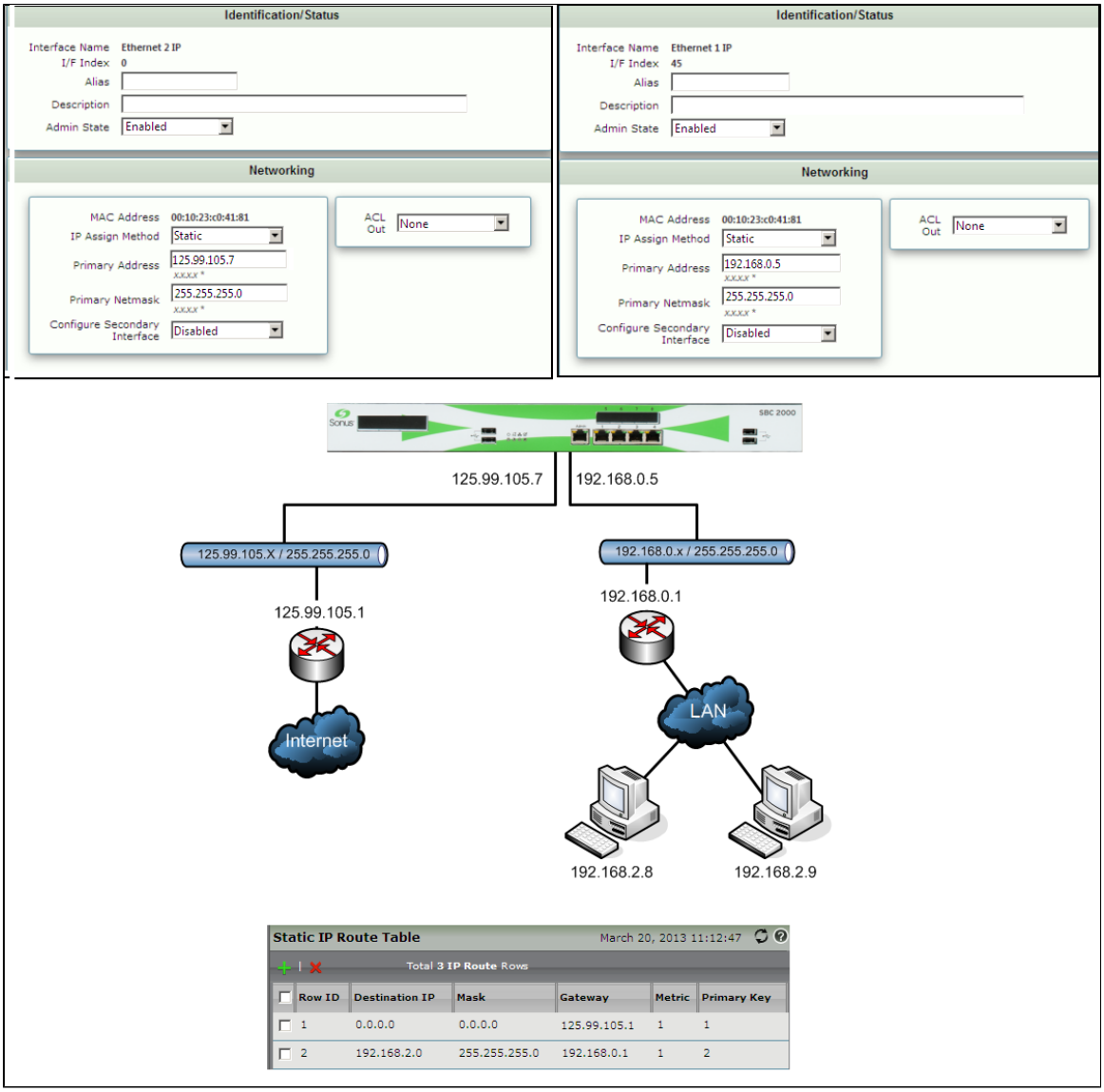
The Sonus SBC 1000/2000 Routes IP traffic to a NIC based on the Subnet to which the NIC and the traffic belong. If the destination address is on the same subnet as the NIC, then that NIC will receive the traffic.

Example:

> *The Sonus SBC 1000/2000 receives traffic with a destination address of 192.168.2.9. For the traffic to be routed to the endpoint, two valid conditions must exist.*
> ⚠ *There must exist a (1) valid Static Route which contains a gateway on a (2) subnet defined for one of the Sonus SBC 1000/2000's NICs.*

In this example, see the figure below, the call with a destination IP of 192.168.2.9 is received and matches the static route specifying anything with a destination subnet of 192.168.2.x is routed to the gateway address 192.168.0.1, which is on the same network as the NIC with an address of 192.168.0.5/255.255.255.0.

Copyright © 2015 Sonus Networks. All rights reserved.



Managing the Hosts Table

The Hosts Table enables you to edit the */etc/hosts* file through the WebUI or REST interface. Each line in the *Hosts* file contains one IP address and at least one FQDN/Host name/Domain name.

When you create a FQDN/Hostname entry in the Host Table, you have the option to enter an IP address to resolve the FQDN/Host name, or allow the SBC to dynamically resolve the FQDN/Host name. The Dynamic Refresh option allows dynamic resolution of the FQDN/Hostname, as well as provides auto-updates in case of dynamic IP changes.

Hosts File Example

```
127.0.0.1 localhost testux218
192.168.199.15 anon.who.com
192.168.72.99 somemachine.anywhere.com
192.168.99.215 anothermachine.nowhere.net
```

Usage Examples

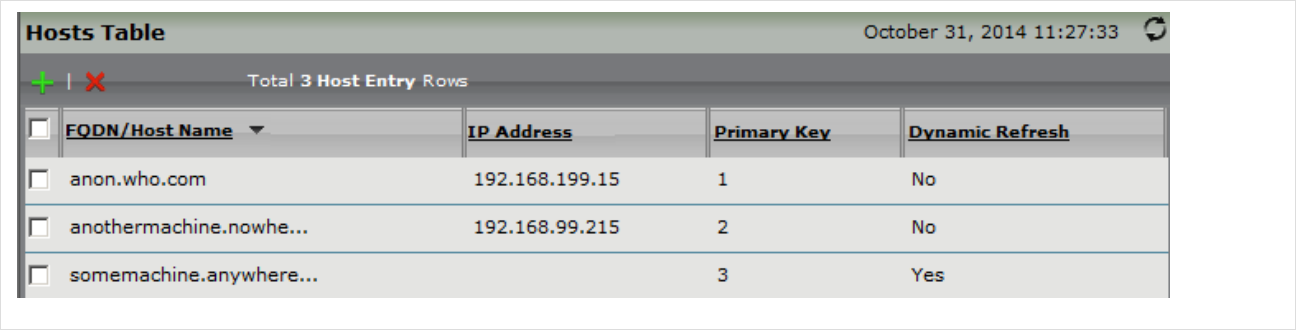
Copyright © 2015 Sonus Networks. All rights reserved.

The Hosts Table allows applications on the Sonus SBC 1000/2000, such as SIP Signaling Groups, AD, RADIUS, etc. to resolve FQDNs when a DNS server is not reachable. We recommend that only a few, very critical, host-IP pairs be stored on the Sonus SBC 1000/2000.

Another use-case is in a pre-deployment scenario in which an administrator would like to divert traffic by mapping the same FQDN to a different IP address. For example, a Sonus SBC 1000/2000 can communicate with a Lync server under test before it is added to the production network, using the same FQDN, but with a different IP address.

Working with Host Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Hosts**.



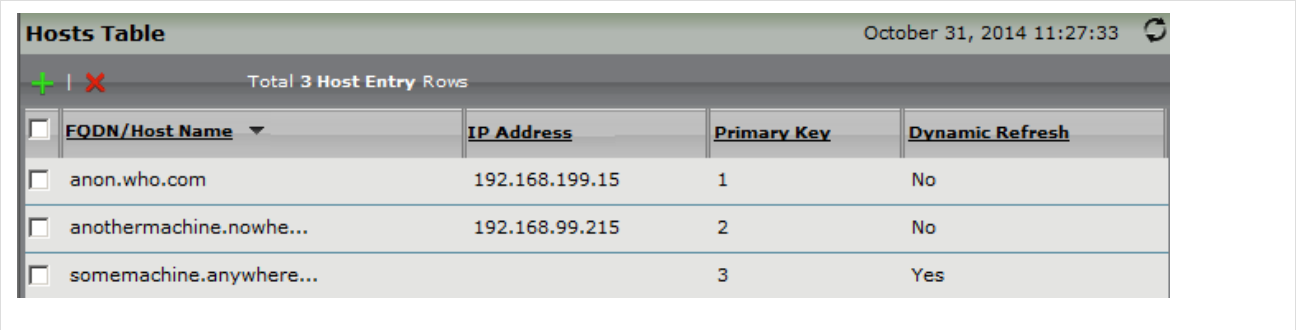
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating Entries in the Hosts Table

Changes to the Hosts Table are not dynamically applied. Reboot the Sonus SBC 1000/2000 following any modification to the Hosts Table.

Creating Entries in the Hosts Table

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Hosts**.



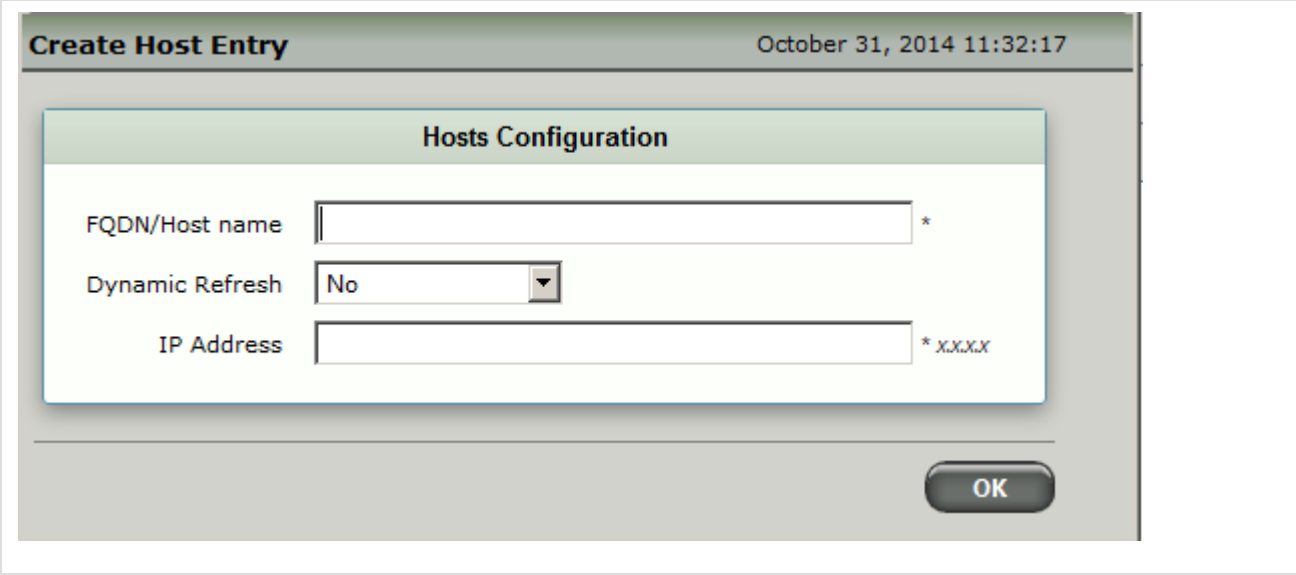
Create an Entry in the Hosts Table

A maximum of 50 Host entries are allowed in the Hosts Table.

To create an entry in the Hosts Table:

Copyright © 2015 Sonus Networks. All rights reserved.

1. Click the **Create Host** ( ) icon at the top of the Hosts Table page.



Host Configuration - Field Definitions

FQDN/Host name

Specifies the FQDN or Host name. Maximum length: 255 characters.

Dynamic Refresh

Specifies whether the Dynamic Refresh option is enabled. This option allows dynamic resolution of the FQDN/HostName entered in the Hosts Table, as well as auto updates in case of dynamic IP changes. When Dynamic Refresh is enabled and the configuration is applied, a DNS lookup for the FQDN is performed and the resolved IP address is updated and retained in the */etc/hosts* file.

Valid entries: **Yes** (dynamic resolution is enabled and the IP Address field is optional) or **No** (dynamic resolution is disabled and the IP Address field is required). Default entry: **No**.

> For all Hosts previously configured, Dynamic Refresh will be disabled by default. These hosts will not be refreshed dynamically unless you enable the Dynamic Refresh option.

IP Address

Specifies the IP address associated with the FQDN/Host Name. Maximum length: 16 characters. This field is optional when the Dynamic Refresh option is set to **Yes**.

- If an IP Address is resolved as part of Dynamic Refresh option, it is saved in the */etc/hosts* file and and an entry is populated in the Hosts Table.
- If the IP Address field is unresolved as part of the Dynamic Refresh option, the entry is not added to the */etc/hosts* file and the field is left blank in the Hosts Table.

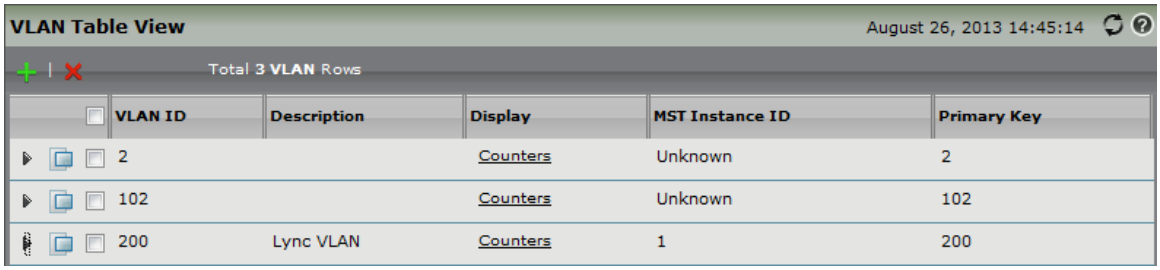
Copyright © 2015 Sonus Networks. All rights reserved.

Managing VLANs

The Sonus SBC 1000/2000 platform supports user created VLANs. User created VLANs are restricted to the range: 2 – 3999. When a VLAN is created, the Sonus SBC 1000/2000 automatically creates a logical interface with the name **VLAN <VLAN-ID> IP**. For example, when **VLAN 100** is created, a logical interface named **VLAN 100 IP** is also created. This logical interface is then used for IP layer communication for the VLAN. More information on VLAN logical interfaces can be found in the Configuring and Modifying Logical Interfaces section. Also note, that in order for a VLAN to be active in the system, you must associate it with one or more Ethernet ports. More information on ports and VLAN associations can be found in the Managing Ethernet Ports section.

Working with VLANs

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Bridge > VLAN**.



To view VLAN properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying VLANs

Viewing VLAN Counters

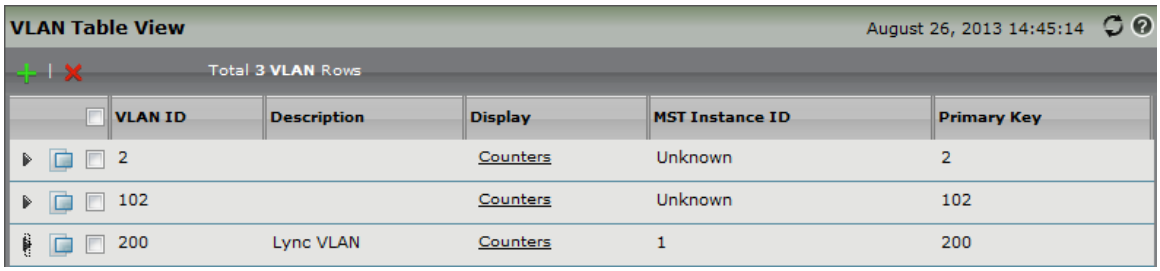
Modifying Default VLAN

Creating and Modifying VLANs

To create or modify an existing VLAN:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Bridge > VLAN**.

Copyright © 2015 Sonus Networks. All rights reserved.



Modifying a VLAN

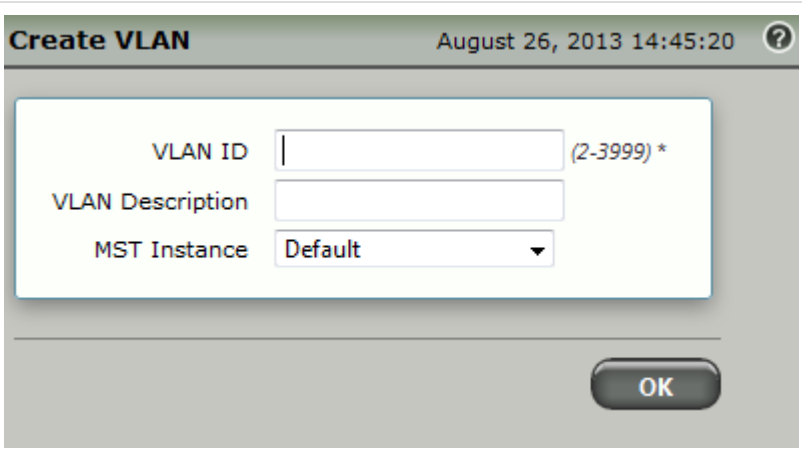
To modify a VLAN:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a VLAN

To Create a VLAN:

1. Click the Create ( ) icon.



VLAN - Properties

VLAN ID

An integer value that identifies the VLAN and used in assigning port membership.

VLAN Description

A human readable description of the VLAN.

MST Instance

Specifies the Multiple Spanning Tree (MST) Instance to use.
For more information about MST see Working with Multiple Spanning Trees.

Copyright © 2015 Sonus Networks. All rights reserved.

Viewing VLAN Counters

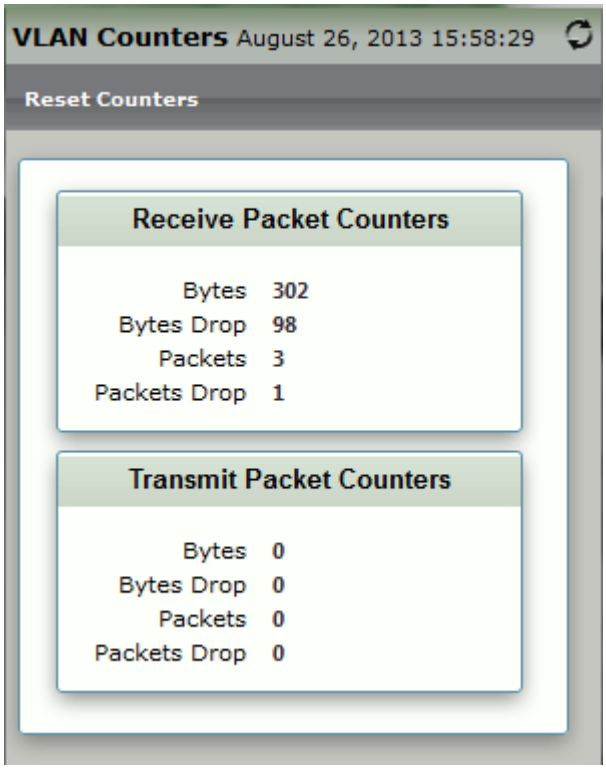
VLAN counters are supported on the Sonus SBC 2000 only at this time.

VLAN Counter will count VLAN packets entering from all possible ports.

How to View VLAN Counters

To view a VLAN counter:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Bridge > VLAN**.
3. Click the Counters link in the row of the VLAN in which you want to view the counters.



Modifying Default VLAN

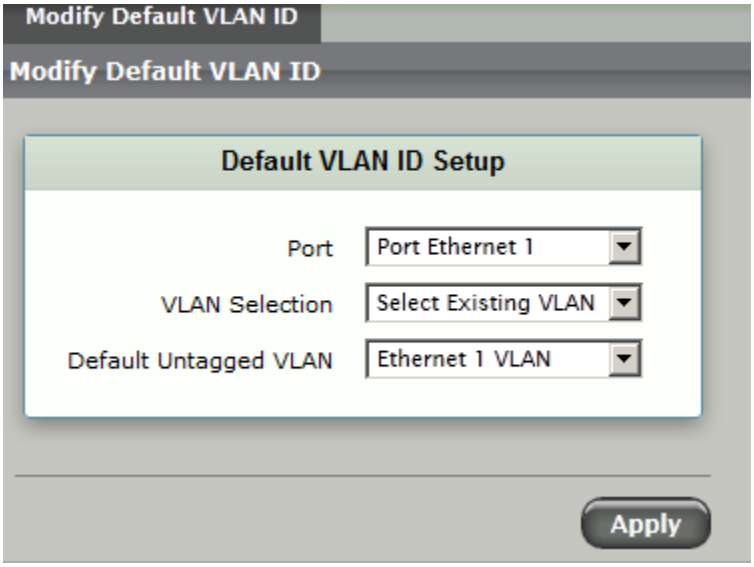
The Modify Default VLAN task enables you to modify the VLAN used as the default on the selected port. You can either select an existing VLAN or create a new one. The IP address from the existing VLAN will be migrated to the new default VLAN in the cases listed below.

- If the new VLAN interface does not have an IP address configured, the IP will be migrated from the previous VLAN.
- If the Default VLAN being modified is used by another port (except the ASM port), the IP address will not be migrated.
- If the selected Port and the ASM Port are configured with the same Default VLAN, then modifying the Default VLAN on the selected Port will change the ASM Port's Default VLAN as well.

Copyright © 2015 Sonus Networks. All rights reserved.

Set the default VLAN as follows:

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under **IP/Protocols**, click **Modify Default VLAN.**
3. Edit the Default VLAN ID Setup information as necessary.
4. Click **Apply**.



Default VLAN ID Setup - Field Definitions

Port

The port in which the selected VLAN will be configured as the Default VLAN. Valid entry: select from the drop down list of available ports.

VLAN Selection

Determines whether an existing or new VLAN is used as the Default VLAN. Valid entry: **Select Existing VLAN** (you select an existing VLAN as the default), or **Create New VLAN** (you create a new VLAN as the default). If you select **Create New VLAN,** the following fields are displayed: VLAN ID, VLAN Description, MST Instance. When a new VLAN is created, it is added to the Logical Interfaces table. See Managing Logical Interfaces.

VLAN ID

An integer value that identifies the VLAN and is used in assigning port membership. Valid entry: **2 - 3999.**

VLAN Description

A description of the VLAN (i.e., **Lync VLAN**, **Sonus VLAN**, etc.). This field is available only when **Create New VLAN** is selected from VLAN Selection.

MST Instance

Specifies the list of available Multiple Spanning Tree (MST) Instances. For more information about MST, see Working with Multiple Spanning Trees. Valid entry: select from the drop down list. This field is available only when **Create New VLAN** is selected from VLAN Selection.

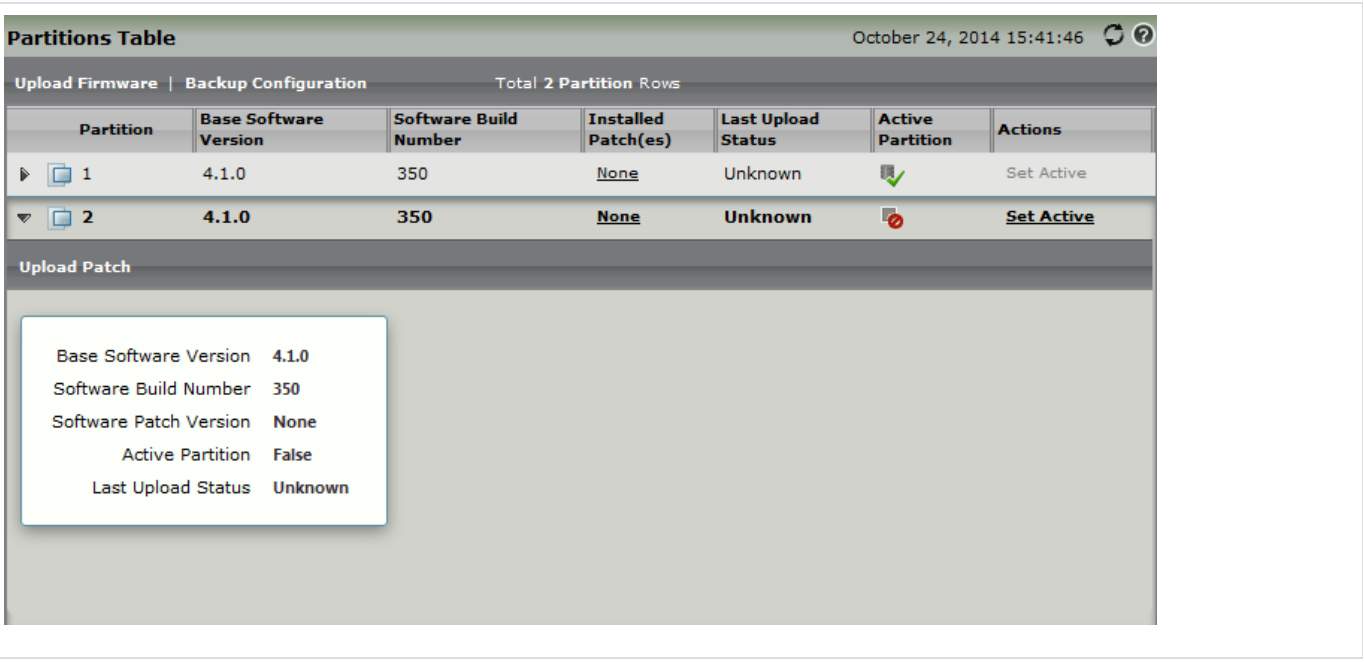
Copyright © 2015 Sonus Networks. All rights reserved.

Default Untagged VLAN

Specifies the list of existing VLANs associated with this port. This list is populated with the entries in the VLAN Table. See Managing VLANs. Valid entry: select an entry from the drop down list. This field is available only when **Select Existing VLAN** is selected from VLAN Selection.

Working with System Software

The Sonus SBC 1000/2000 keeps its system software (firmware) in containers known as "Application Partitions". There are **two** application partitions, one of which is **Active**. When the Sonus SBC 1000/2000 system is operational, it is running off of the **Active Partition**, and the remaining (inactive) partition serves as a spare.



The Active partition cannot be upgraded while the Sonus SBC 1000/2000 system is running, so all upgrades are performed by replacing the Inactive Partition with the new firmware version.

When a software upgrade is performed, the spare partition is replaced by the upgrade. To use the firmware version just uploaded, you must activate the partition that it was uploaded to. You can either activate the partition immediately (also known as a One-Step Upgrade), or in a controlled manner during a scheduled service downtime (by Upgrading the Inactive Partition and manually Setting the Active Partition).

See also: Upgrading the SBC Communication Service Version
See also: Installing an ASM Package

One-Step Upgrade

Managing Application Partitions

- Upgrading the Inactive Partition
- Setting the Active Partition

Copyright © 2015 Sonus Networks. All rights reserved.

- Uploading Firmware Patches

Managing the Boot Partition

- Upgrading the Boot Image
- Viewing the Boot Image Version

One-Step Upgrade

Unlike a Controlled Partition Upgrade, the Sonus SBC 1000/2000 provides a "One-Step Upgrade" solution which automatically upgrades the currently inactive partition, makes it active, and boots the Sonus SBC 1000/2000 from the newly upgraded partition. Sonus recommends using this One-Step Upgrade operation after Running Initial Setup , or during scheduled downtime.

Please Read!

You must follow the instructions outlined in the general Sonus SBC 1000/2000 Upgrade guide before you proceed with the steps outlined on this page. The general upgrade guide includes **important prerequisites** for Sonus SBC 1000/2000 systems with a built-In Application Solution Module (ASM), and also describes which firmware files to use depending on the Sonus SBC 1000/2000 Model you are using.

The Software Upload progress bar is supported in the following browsers:

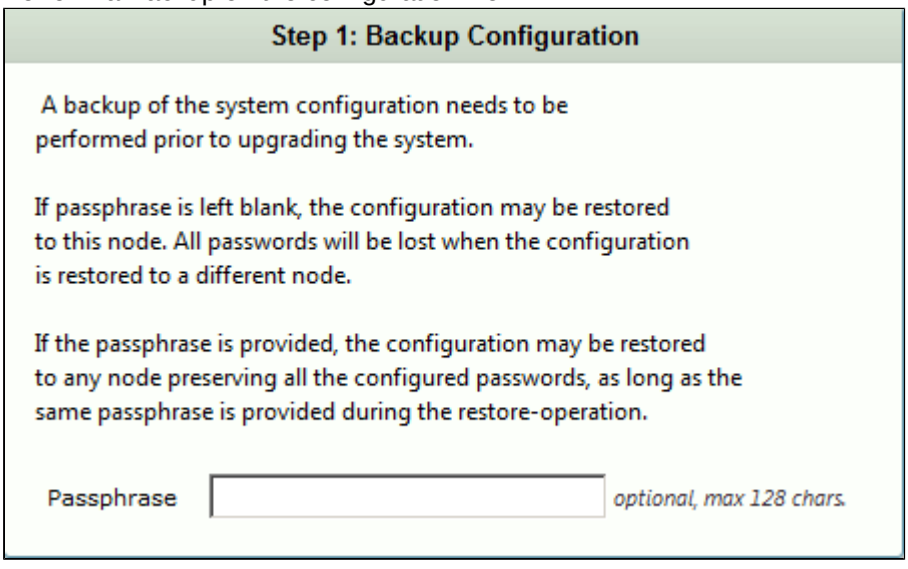
- Internet Explorer, Releases 10 and 11
- Firefox, Release 24 and later
- Chrome, Release 31 and later

In browsers that do not support this feature, the software upgrade process will be presented the way it is shown in Release 4.0 and previous.

Automatically Upgrading the Sonus SBC 1000/2000 Software/Firmware Version

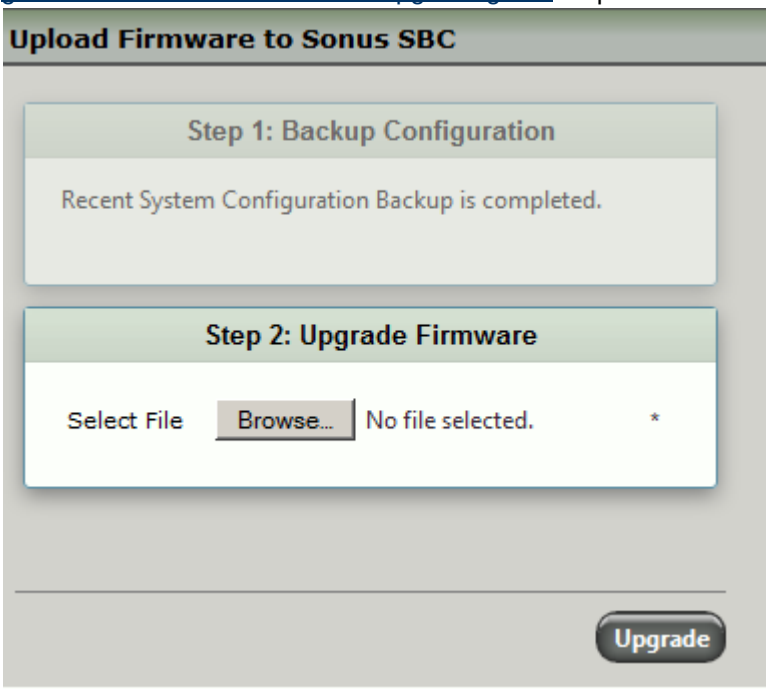
To automatically upgrade the Sonus SBC 1000/2000 software:

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, click **System > Firmware Upgrade**.
3. Perform a Backup on the configuration file.

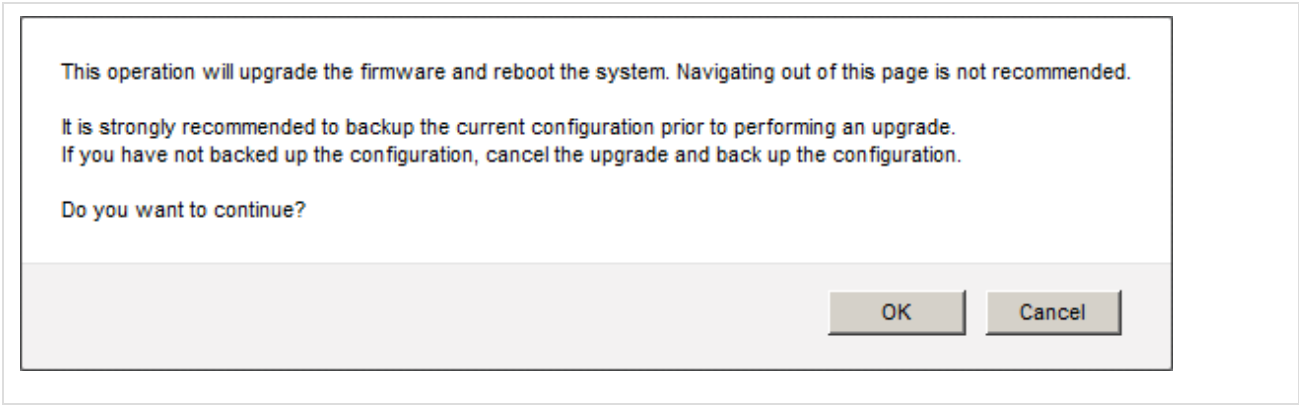


Copyright © 2015 Sonus Networks. All rights reserved.

4. Enter an optional Passphrase (see Using the Custom Passphrase).
5. Under **Select File**, click the **Browse** button and select the Sonus SBC 1000/2000 firmware file listed in the general Sonus SBC 1000/2000 Upgrade guideto upload.

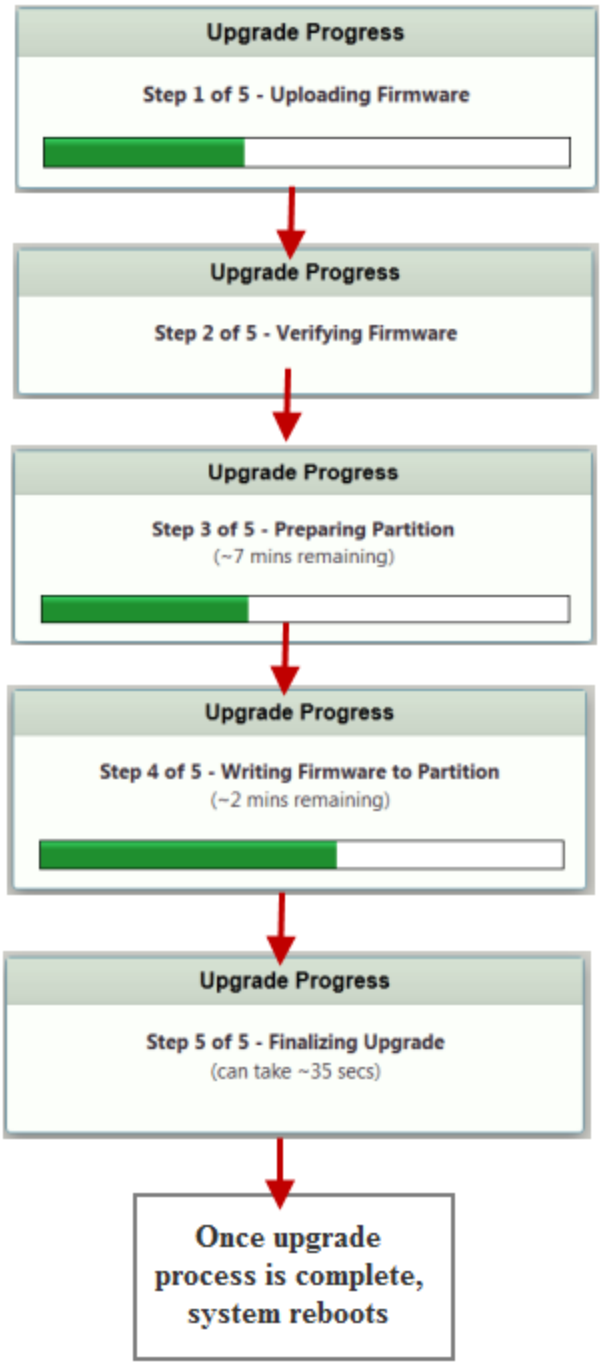


6. Click **Upgrade**. The following warning popup will be displayed:



7. Click **OK** to upload the new firmware. **Do not close or navigate away from the browser window, or you may receive partial results.** Throughout the upload process, the web interface displays update messages to indicate the progression of the upgrade, as shown below. (If you navigate to this view from another browser, it will also display the progress.) Once the upgrade is complete, the system automatically reboots.

Copyright © 2015 Sonus Networks. All rights reserved.



An average upgrade takes about 8 - 9 minutes. During the upgrade process, the remaining time estimates in the different steps becomes more accurate as the process progresses.

Helpful Tip

On average, the **Sonus SBC 1000/2000 system takes between 3 to 4 minutes to fully reboot** and become reachable again through the web interface. Upon completion, you will be automatically redirected to the Login screen. Verify that you are booting from the new partition either by checking the active partition, or by Viewing the Software Version.

Managing Application Partitions

Copyright © 2015 Sonus Networks. All rights reserved.

This task could have a negative impact on the performance. Perform this task only on a lightly loaded system or during scheduled maintenance.

Sonus SBC 1000/2000 provides a **controlled upgrade** of the inactive partition. Unlike the One-Step Upgrade, the controlled upgrade does not automatically reboot the Sonus SBC 1000/2000 after the upgrade procedure has finished. In order to boot from the newly upgraded partition, you must set it as the active partition which will prompt you to authorize the Sonus SBC 1000/2000 reboot. This option may be convenient if you wish to upgrade the partition during active call services, and only activating it during a scheduled service downtime.

Upgrading the Inactive Partition

Setting the Active Partition

Uploading Firmware Patches

Upgrading the Inactive Partition

Please Read!

You must follow the instructions outlined in the general Sonus SBC 1000/2000 Upgrade guide before you proceed with the steps outlined on this page. The general upgrade guide includes **important prerequisites** for Sonus SBC 1000/2000 systems with a built-In Application Solution Module (ASM), and also describes which firmware files to use depending on the Sonus SBC 1000/2000 Model you are using.

The Software Upload progress bar is supported in the following browsers:

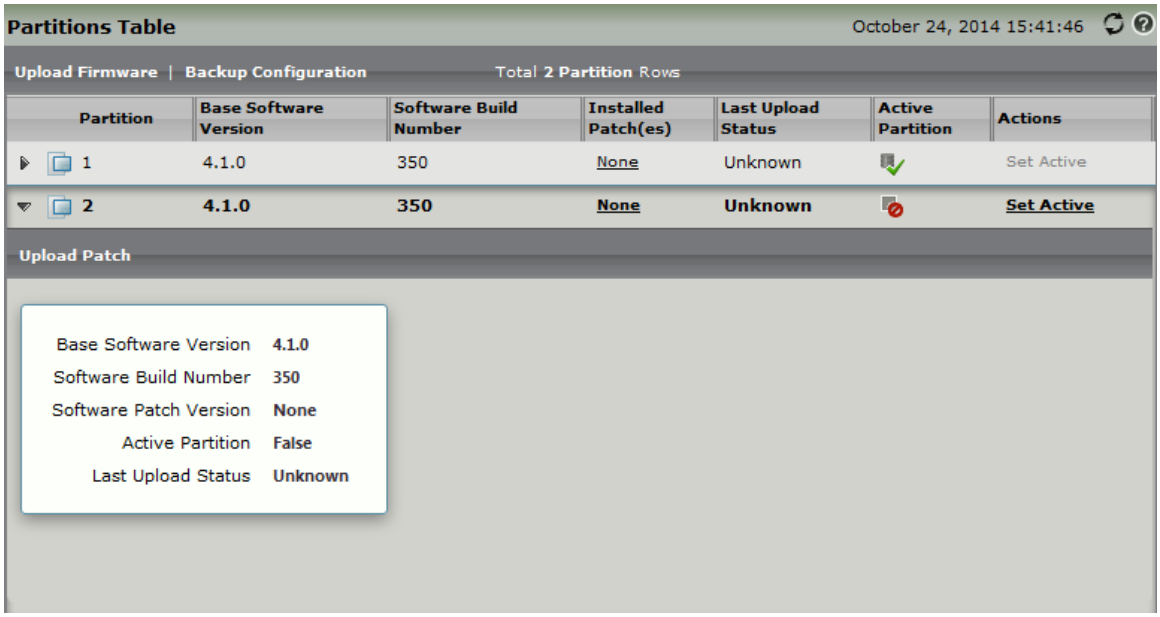
- Internet Explorer, Releases 10 and 11
- Firefox, Release 24 and later
- Chrome, Release 31 and later

In browsers that do not support this feature, the software upgrade process will be presented the way it is shown in Release 4.0 and previous.

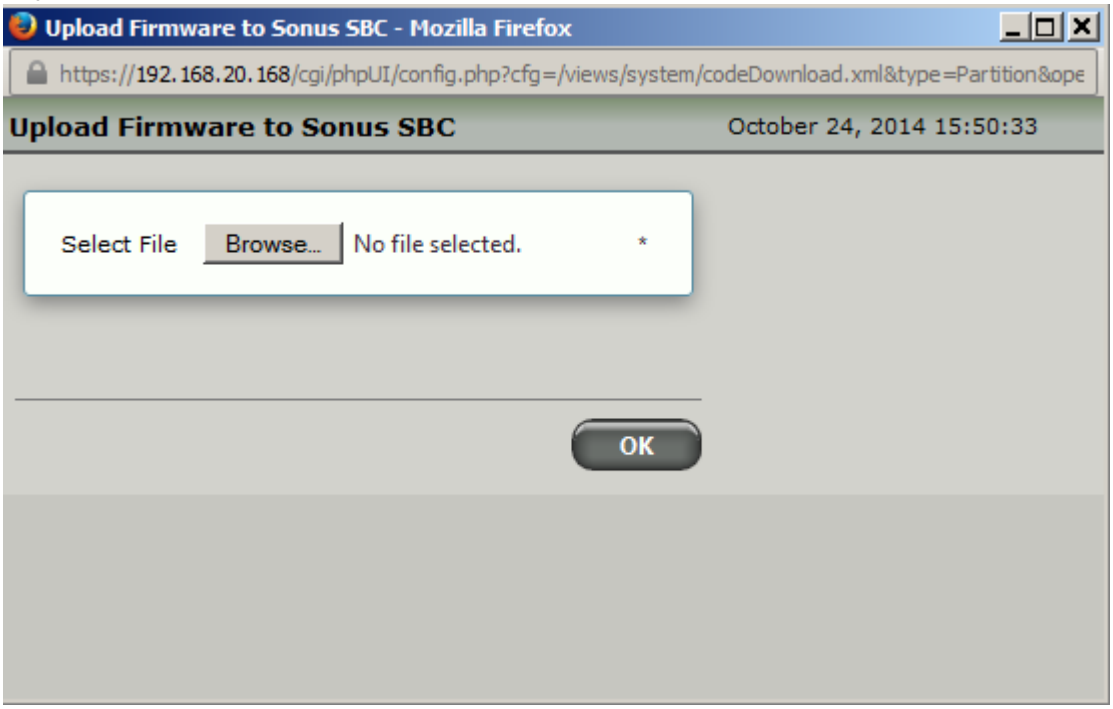
To upgrade the inactive partition:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Software Management > Application Partitions**.

Copyright © 2015 Sonus Networks. All rights reserved.

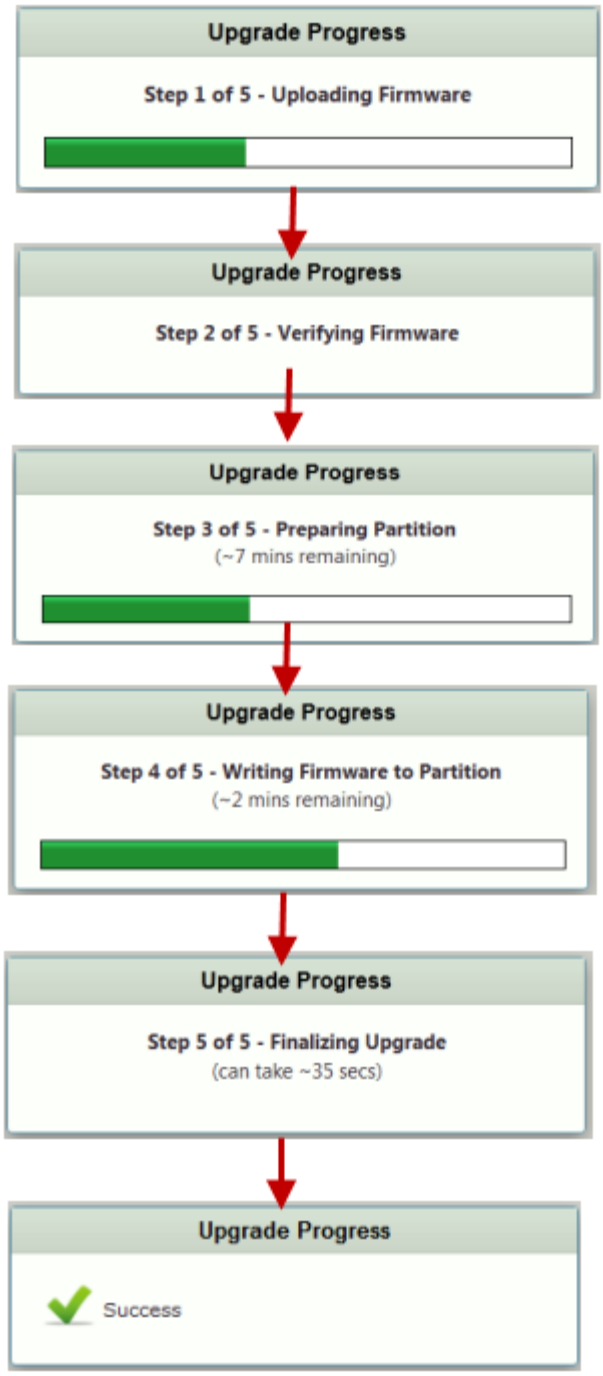


3. Make note of the inactive **partition number** you are upgrading the firmware to (the table entry listed without a tick mark under the 'Active Partition' column)
   This will be important towards the end when verifying the **last upload status** of the inactive partition.
4. Click the **Upload Firmware** link located on the top right hand side of the pane - a popup window will be dispatched:



5. Under the **Select File**, click the **Browse** button and select the Sonus SBC 1000/2000 firmware file listed in the general Sonus SBC 1000/2000 Upgrade guide to upload.
6. Click **OK**. **Do not close or navigate away from the browser window or you may receive partial results.** Throughout the upload process, the web interface displays update messages to indicate the progression of the upgrade of the inactive partition, as shown below. (If you navigate to this view from another browser, it will also display the progress.) Once the upgrade is complete, the system automatically reboots.

Copyright © 2015 Sonus Networks. All rights reserved.



Under normal conditions, an average upgrade takes about 8 - 9 minutes. During the upgrade process, the remaining time estimates in the different steps becomes more accurate as the process progresses.

7. Once the upgrade has completed, click the **X** in the corner of the box to dismiss the popup window.
8. On the partition page, verify the **Last Upload Status** associated with the inactive partition is listed as **Success**.

Copyright © 2015 Sonus Networks. All rights reserved.

At this stage, the inactive partition is upgraded to the the new firmware without rebooting the Sonus SBC 1000/2000 system and without interrupting active call services.

If you wish to boot your Sonus SBC 1000/2000 from this partition, you must set it as the active partition.

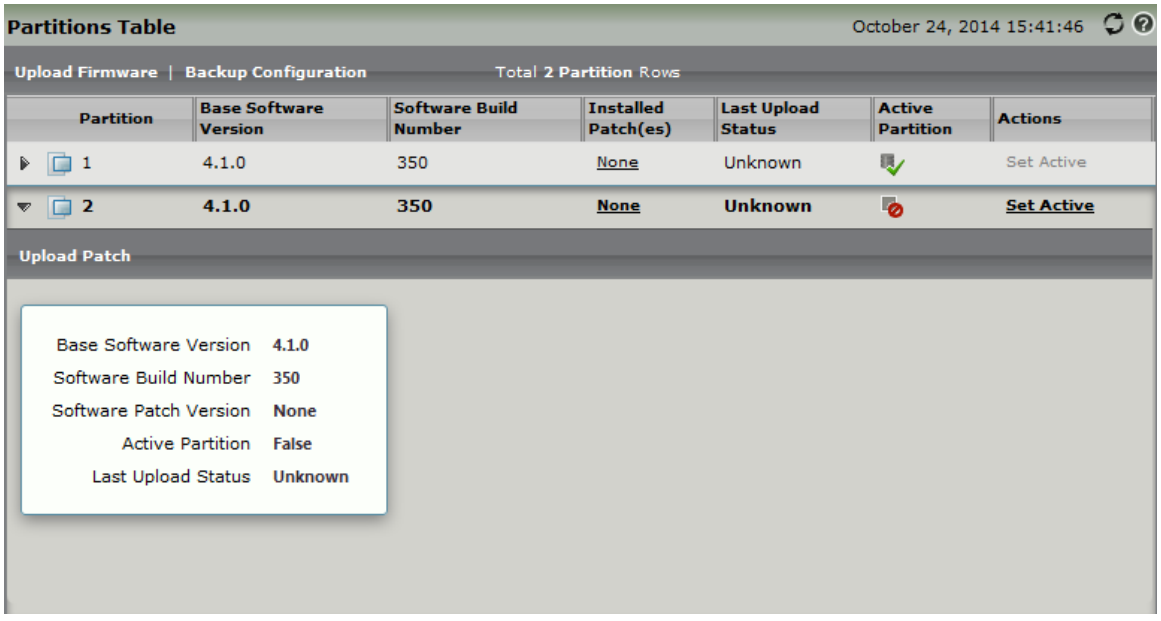
Setting the Active Partition

Once you have updated the inactive partition either by Upgrading the Inactive Partition or by Uploading Firmware Patches, new software does not take effect until you activate newly updated partition. When you activate the partition, the system must reboot to boot from the desired partition. All configuration is preserved when you activate the partition.

The instructions outlined include rebooting the Sonus SBC 1000/2000 system. This will disrupt call services on the Sonus SBC 1000/2000 and should only be completed during a planned service outage.

To set the Active Partition:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Software Management > Application Partitions**.

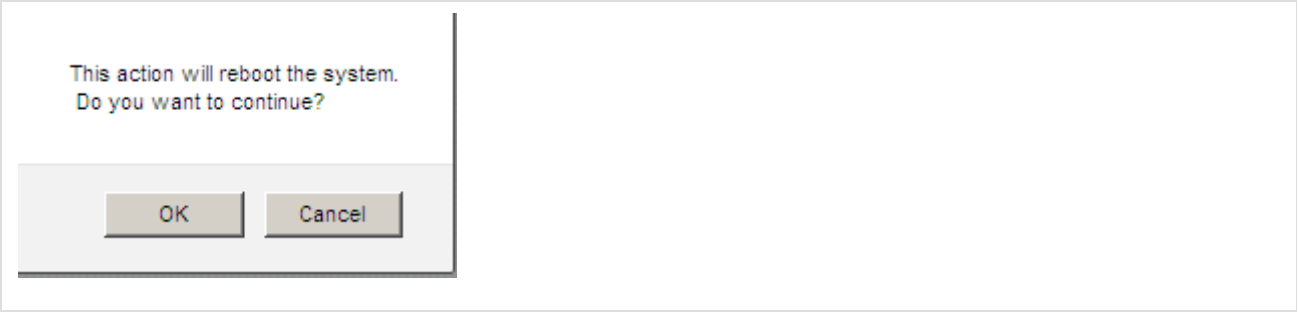


3. Click the **Set Active** link in the row entry associated with the partition that you wish to activate.

Copyright © 2015 Sonus Networks. All rights reserved.

The inactive partition is the row entry listed without a tick mark under the 'Active Partition' column

4. You will be prompted to reboot the Sonus SBC 1000/2000, click **OK**.



> **It will take up to 15 seconds for the action to be processed**, and you will not see any visible indication during this short period of time.

5. The following status message will be dispatched indicating that the system is rebooting off of the new partition



> **Helpful Tip**
>
> On average, the **Sonus SBC 1000/2000 system takes between 3 to 4 minutes to fully reboot** and become reachable again through the web interface.. Upon completion, you will be automatically redirected to the Login screen. Verify that you are booting from the new partition either by checking the active partition, or by Viewing the Software Version.

Uploading Firmware Patches

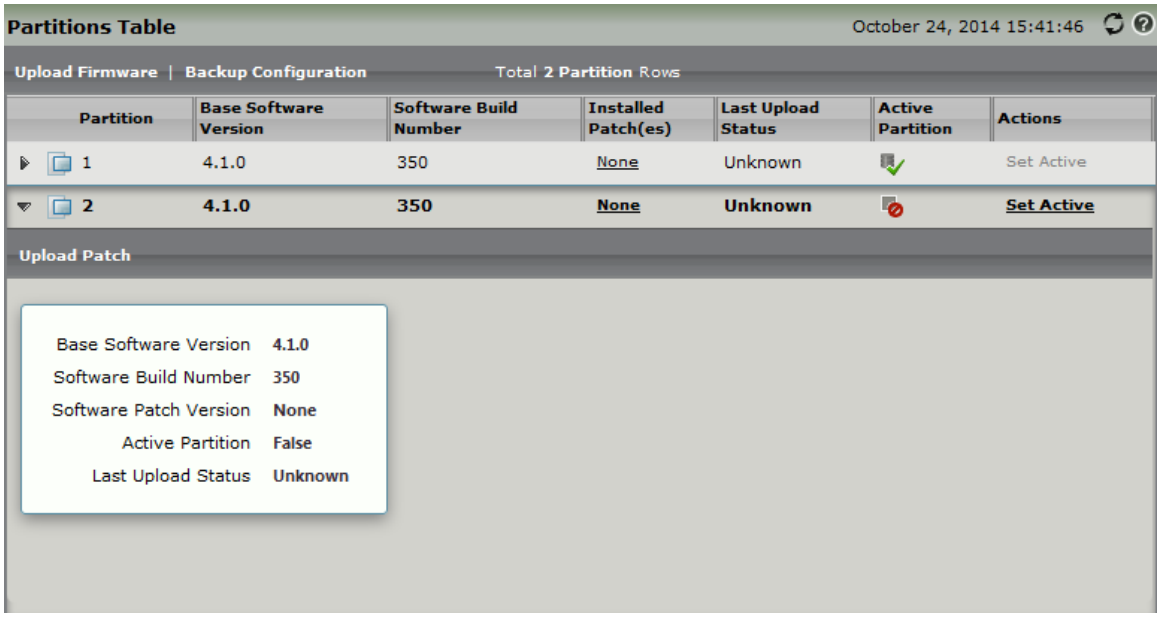
Some Application software changes are delivered as patch, which is substantially smaller than a firmware upgrade. A Patch is always based on specific Major or Minor release, so you must apply patch only to the specific Base Software Version for which it is designed. Unlike Sonus SBC 1000/2000 software/firmware versions, patches can be applied to currently active partition or the non-active application partition. All system configuration is preserved when you apply a Patch.

> **Applying a patch to the active (running) partition may disconnect your active calls.**
>
> If you uploaded the patch to the currently active partition, the system restarts the patched components. Depending on which components were patched, this process may disrupt currently active calls. Sonus recommends that you only apply patches to inactive partitions or to active partitions during a planned service outage.

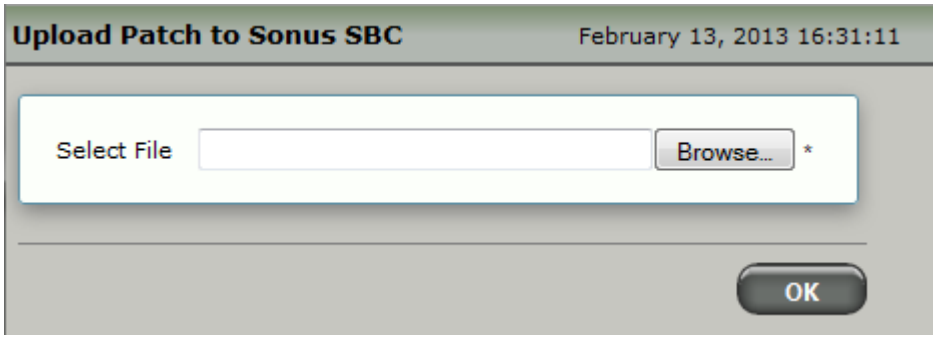
To upload a Sonus SBC 1000/2000 firmware patch:

1. Download the patch from the Sonus SBC 1000/2000 Download Center (or from your Sonus service representative for more information)
2. In the WebUI, click the **Settings** tab.
3. In the left navigation pane, go to **System > Software Management > Application Partitions**.

Copyright © 2015 Sonus Networks. All rights reserved.



4. Click the **expand** ( ) in the row of the partition to which you want to apply the patch.
5. Click the **Upload Patch** link - a popup window will appear:



6. Under **Select File**, click the **Browse** button and select the patch file to upload.
7. Click **OK** to upload the patch.

Depending on the size of the patch, it may take a few minutes to update the Sonus SBC 1000/2000 system.

Managing the Boot Partition

The Sonus SBC 1000/2000 Boot Image initializes the hardware and boots the **active** Sonus SBC 1000/2000 application partition. This boot image version is updated much less frequently than the Sonus SBC 1000/2000 application software.

The boot image version may be different depending on the Sonus SBC 1000/2000 model you are using. In **Sonus SBC 1000/2000 4.1.x**, verify that your unit's boot image version matches what is listed below:

Sonus SBC 1000/2000 Model	Boot Image Version
Sonus SBC 1000	3.1.6o

Copyright © 2015 Sonus Networks. All rights reserved.

Upgrading the Boot Image

Viewing the Boot Image Version

Upgrading the Boot Image

- Upgrades of the Sonus SBC 1000/2000 boot partition are infrequent and - in general - end users should not need to perform this procedure.
- If you are unsure whether or not your Sonus SBC 1000/2000 requires a boot code upgrade, see the *upgrade notes* for your version of the Sonus SBC 1000/2000 software.

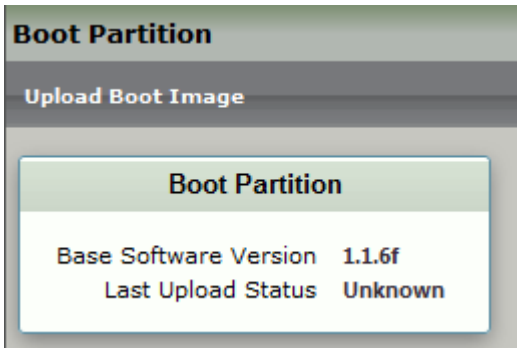
Changing the Sonus SBC 1000/2000 Boot Image disrupts call services on the Sonus SBC 1000/2000, when the restart required to make the upgrade effective is performed, and should only be completed during a scheduled service outage.

To upgrade the Boot Image:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Software Management > Boot Partition**.

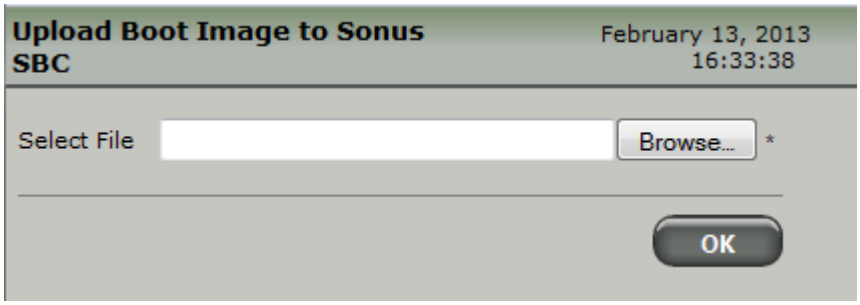
Important Note:

Remember that you are upgrading the **Boot** partition and not the **Application** partition.

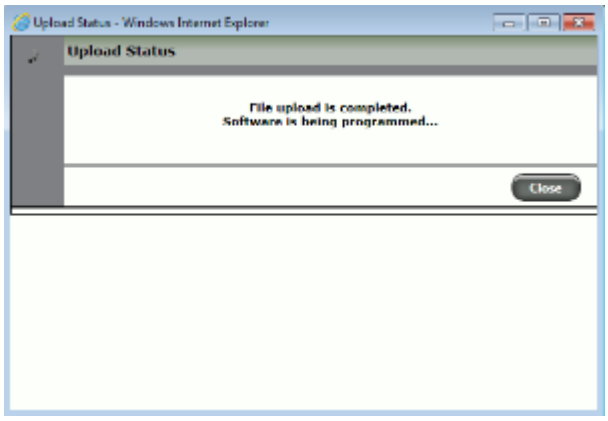
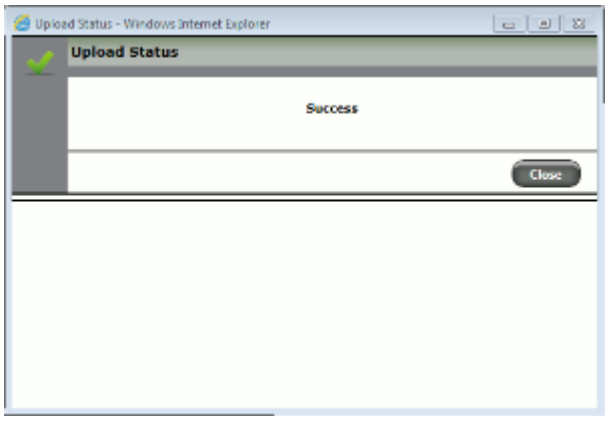


3. Click the **Upload Boot Image**link located on the top right hand side of the pane.

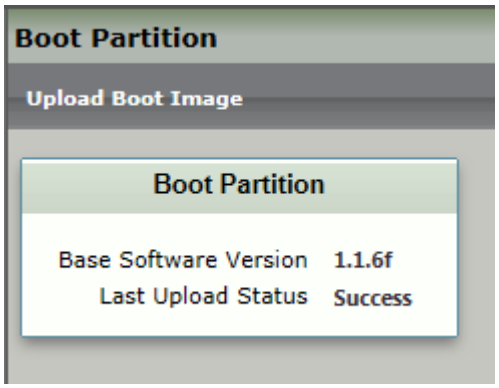
Copyright © 2015 Sonus Networks. All rights reserved.



4. Under **Select File**, click the **Browse** button and select the Sonus SBC 1000/2000 Boot image to which you wish to upgrade.
5. Click **OK**.
   Throughout the upload process, the web interface will dispatch a series of status messages: *click image thumbnails to see them in full resolution*

(1) Upgrading the Boot Image (approx. 2 mins)	(2) Boot Image Successfully Upgraded
	

6. Once the upgrade has completed, click **Close**.
7. On the Boot Partition page, verify that the **Last Upload Status** is listed as **Success**



After the Boot Image is successfully upgraded, you must reboot the Sonus SBC 1000/2000 for the changes to take

Copyright © 2015 Sonus Networks. All rights reserved.

effect.

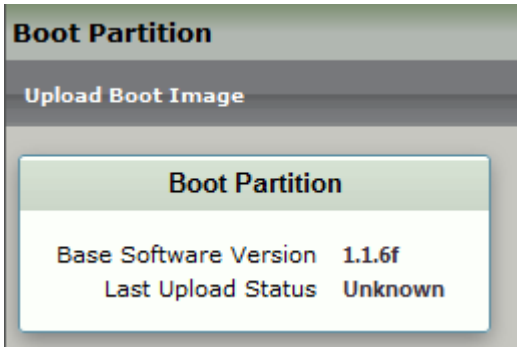
Viewing the Boot Image Version

In some cases, you will be tasked to verify the Boot Image version loaded on your Sonus SBC 1000/2000 model.

> The boot image version may be different depending on your Sonus SBC 1000/2000 model. You can check what version you should be running - click here for more details.

To view the Boot Image version:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Software Management > Boot Partition**.



Working with Call Detail Records

The Sonus SBC 1000/2000 supports the logging of accounting and call metrics related data on RADIUS based accounting servers, functioning as a RADIUS client sending Call Detail Records (CDR) to RADIUS accounting servers.

The CDR feature of the Sonus SBC 1000/2000 enables administrators and users to gather a wealth of information specific to calls placed and/or received through the Sonus SBC 1000/2000. Call Detail Records are stored on a RADIUS server using both a standard Radius Dictionary and an Sonus specific RADIUS Dictionary that can be retrieved from the server at anytime. Depending on your RADIUS server configuration, records can be stored either in plain text format in date coded log files, or directly in a relational database.

The CDR feature provides information on incoming and outgoing calls for accounting and administration purposes. The Sonus SBC 1000/2000 collects data for every call and reports it to a third-party RADIUS-based accounting server in the form of Call Detail Records which consist of attribute/value pairs. This data includes, but is not limited to attributes such as:

- Date, time and call duration for all calls
- Dialed number and calling number for all calls
- Codec negotiated for all calls
- Call Quality metrics, values from RTCP-XR

A typical CDR contains entries similar to those shown below:

Copyright © 2015 Sonus Networks. All rights reserved.

```
Acct-Status-Type = Start
        Acct-Authentic = 0
        NET-Session-Ingress-CallId = "0"
        NET-Session-Egress-CallId = "65535"
        NET-Session-Generic-Id = "2"
        Acct-Multi-Session-Id = "13201689112"
        NET-Ingress-Signaling-Group = "1"
        NET-Egress-Signaling-Group = "0"
        NET-Ingress-Channel-Number = 1
        NET-Egress-Channel-Number = 0
        NET-Call-Origin = "1"
        NET-Calling-Number = "4009"
        NET-Called-Number = "6239"
        NET-Calling-Name = "Snom870-226.246"
        NET-Ingress-Channel-Id = "0:1:1"
        NET-Setup-Time = "1320168911"
        Acct-Session-Id = "0"
        NET-Firmware-Version = "2.0.0v85"
        NET-Local-Time-Zone = "PST8PDT"
        NET-Gw-Id = "efb8efa8cdfedc3ba0bb7b"
        NET-Time-And-Day = "1320168911"
        NAS-Port = 1813
        Acct-Delay-Time = 0
        NAS-IP-Address = 134.56.72.218
        Acct-Unique-Session-Id = "4d1f78f67a5c582e"
        Timestamp = 1320168888
```


Call Detail Records Primer

Configuring the Sonus SBC 1000-2000 for CDR

Retreiving Call Detail Records From a RADIUS Server

Vendor Specific Attributes Reference

Viewing Call Detail Record Statistics

Call Detail Records Primer

This page outlines the Call Detail Record (CDR) process. Before you begin reading this section, please make sure you first read the information in Working with Call Detail Records.

CDR Data Collection

Call Detail Record data collection is an ongoing process. When any call-related action occurs, the common call control (CCC) module of Sonus SBC 1000/2000 actively sends information messages to the Sonus SBC 1000/2000 RADIUS service. The RADIUS service converts the messages into RADIUS messages and sends it to the RADIUS accounting server to start accounting. At the end of every call, all the signaling groups involved in the call and MSC push all call related statistics and information to CCC which in turn informs the RADIUS service. The Sonus SBC

Copyright © 2015 Sonus Networks. All rights reserved.

1000/2000 RADIUS service sends the CDRs to the RADIUS accounting server and ceases accounting. Accounting is performed separately for each call leg involved. Each of the call-legs in a call are linked via the Acct-Multi-Session-Id attribute.

Queuing

Transmitting CDRs over the network one at a time is an unacceptably slow process. In order to ensure that other Sonus SBC 1000/2000 processes are not kept waiting for the successful delivery of CDRs to RADIUS based accounting servers, Sonus SBC 1000/2000 implements a queue system. The queue is populated with the information that comes from CCC, and CCC is immediately relieved of any further action. The Sonus SBC 1000/2000 RADIUS service then attempts to send CDRs from the queue based on the order in which they were received.

Backup

In the event of lost communications between the Sonus SBC 1000/2000 and it's configured RADIUS accounting server(s), CDRs can be backed up and stored locally and/or cached for resending to the server(s) when communications has been restored. For the Sonus SBC 2000, backups and caching are done on the internal data storage up to a maximum of 1,500 records. On the Sonus SBC 1000, caching and backup of CDR data is done via an eUSB device (if installed) up to a maximum of 1,500 records.

When the RADIUS server becomes available again, the Sonus SBC 1000/2000 sends the backed up CDRs to the server in the order in which they were written in the local file.

Retry on CDR Logging Failure

Status-Server (RFC 5997)

Each time the Sonus SBC 1000/2000 attempts to send a CDR to the RADIUS server, it expects an acknowledgement (ACK) to be returned within three seconds. If the ACK is not received within the three seconds, a timeout occurs. The Sonus SBC 1000/2000 then makes a second attempt to send the CDR to the server. If the second attempt fails due to the three second timeout, the Sonus SBC 1000/2000 writes the CDR to a backup for a retry after all other pending CDRs in the queue have been successfully sent.

Request Mode

Each time the Sonus SBC 1000/2000 attempts to send a CDR to the RADIUS server, it expects an acknowledgement (ACK) to be returned within one second. If the ACK is not received within one second, a timeout occurs. The Sonus SBC 1000/2000 then makes a second attempt to send the CDR to the server. If the second attempt fails due to 1 second timeout, the Sonus SBC 1000/2000 writes the CDR to a backup for a retry after all other pending CDRs in the queue have been successfully sent.

Sonus 1000/2000 attempts to send a CDR to the RADIUS server on every 100th consecutive call record logging failure once the server connectivity is marked 'down'.

In the event there were queued records on system idle for period of 10 minutes, the SBC 1000/2000 attempts to send a maximum of 2 consecutive queued CDRs to the RADIUS server. Each consecutive queued CDR is retransmitted with 2 retries at 1 second intervals. The 2 consecutive queued CDR will be backed up again on a logging failure when all servers are unreachable.

RADIUS CDR Logging Failure Scenarios

There are three scenarios in which a logging failure might occur, each of which is described in the following

Copyright © 2015 Sonus Networks. All rights reserved.

sections.

CDR Logging Quarantine on Sonus SBC 1000/2000 Reboot

After the Sonus SBC 1000/2000 boots or restarts, it begins the process of establishing communication with the RADIUS servers. The process requires the the Sonus SBC 1000/2000 successfully ping the server three consecutive times before changing the server status to **Up**. This process requires approximately one minute. If calls are made during this one minute "quarantine" period, CDRs are queued and re-sent when at least one accounting server is declared to be UP in one minute window time.

In Status-Server mode, after the Sonus SBC 1000/2000 boots or restarts, the SBC begins the process of establishing communication with the RADIUS servers. The process requires that the Sonus SBC 1000/2000 successfully ping the server three consecutive times before changing the server status to **Up**. This process requires approximately three minutes, with each ping one minute apart. If calls are made during this *quarantine* period, CDRs are queued and re-sent when at least one accounting server is declared to be **UP**.

Timeout While Logging a CDR

The Sonus SBC 1000/2000 implements a three second timeout (Status-Server mode) when logging CDRs on accounting servers. If the Sonus SBC 1000/2000 times out, it makes a second attempt to log the CDR on the server. Sonus SBC 1000/2000 makes a maximum of two attempts before caching or backing up the record. The Sonus SBC 1000/2000 retries the send after all other pending CDRs in the queue have been successfully sent.

Failure Response Received from the RADIUS Server

If, upon a CDR send attempt, the Sonus SBC 1000/2000 receives a failure response from the RADIUS server, it makes a second attempt. Should the Sonus SBC 1000/2000 receive a second failure response, it backs up the data for a later attempt to send it.

Failure to Send the CDR data from Backup or Cache

The Sonus SBC 1000/2000 makes a maximum of four attempts to send a CDR to the RADIUS accounting server before abandoning the effort and logging the CDR in a CDR failure log. When a CDR has been abandoned and written in a failure log, it raises an alarm, alerting the administrator to take the appropriate action(s).

Network Connectivity Failure

The Sonus SBC 1000/2000 monitors its connectivity with the server(s), in the event of a network connectivity failure the Sonus SBC 1000/2000 will set the server(s) status to Down. When the server's status is **Down**, CDRs are automatically cached and backed up for a later attempt to send them after the server connectivity is restored. For specifics, see Failure Handling Scenarios.

Failure Handling Scenarios

Depending on the selected operating mode (Active-Active, Active-Standby, Round Robin) and how many servers are configured, the Sonus SBC 1000/2000 handles the logging slightly differently. For a description on how logging works under normal circumstances, see the Accounting Mode Options section of the Configuring Sonus SBC 1000/2000 for RADIUS page.

A Single Server Configuration

In this scenario, there is only one accounting server configured.

Copyright © 2015 Sonus Networks. All rights reserved.

RADIUS Accounting Mode	Active-Active	Active-Standby	Round-Robin
Number of Retries	2	2	2

Two Configured Accounting Servers

RADIUS Accounting Mode	Active-Active	Active-Standby	Round-Robin
Number of Retries	2	2	2
Order of Retry (first Send)	Server 1 and Server 2	Server 1	Server 1 and Server 2 in alternation
Order of Retry on Error or timeout	Retry sending to failed server	Server 2	Retry sending to failed server

Call Detail Records are not associated (tagged) with a specific server. When the resend mechanism attempts to send queued CDRs, they are sent to whichever server is available, regardless of the selected accounting mode.

Round-Robin Mode

In the Round-Robin mode, alternate logging occurs only if both servers are in an **Up** status, If one server is **Down** then all CDRs are sent to the other server, if both servers are **Down** the CDRs are queued.

Active-Standby Mode

In this mode, when Active (Server 1) is **Down** or CDR Logging fails for any other reason, all CDRs are sent to stand-by server (Server 2). If Server 1 becomes available again, logging to that server will resume and Server 2 will then revert to standby status.

Vendor Specific Attributes Dictionary

Each build of the Sonus SBC 1000/2000 System software contains the latest version of the Sonus Vendor Specific Attributes Dictionary (dictionary.net). The dictionary specifies Sonus's RADIUS attributes for capturing call related information.

Vendor Specific Attributes fall into seven general categories:

- Media Attributes
- Session Signaling Attributes
- Call Attributes
- SIP Attributes
- Generic Attributes

For a complete description of vendor specific attributes, see the Vendor Specific Attributes Reference.

Configuring the Sonus SBC 1000-2000 for CDR

This page describes the process of setting up the Sonus SBC 1000/2000 for Call Detail Recording on a RADIUS server. Read this section carefully and make sure you have satisfied all the prerequisites before performing the procedure.

Copyright © 2015 Sonus Networks. All rights reserved.

Requirements

Item	Description
CDR License	Permits the implementation of CDR on a Sonus SBC 1000/2000. See, Viewing Licenses.
RADIUS Accounting Server	You must have at least one correctly configured RADIUS accounting server
Sonus Specific VSA Dictionary	Filename: dictionary.net

The VSA is incorporated in the Sonus SBC 1000/2000 as a part of the build. However, the dictionary file must be copied to the RADIUS server. The dictionary is also available for download in the Sonus SBC 1000-2000 Download Center. For a complete listing of attributes and their meanings, see the Vendor Specific Attributes Reference.

Setup Procedure

> Please read the Call Detail Records Primer before continuing with the setup procedure.

To configure the Sonus SBC 1000/2000 for CDR:

1. If you have not already done so, add a RADIUS account server(s).
2. Configure your Sonus SBC 1000/2000 to use the RADIUS accounting server(s) for accounting.

Retreiving Call Detail Records From a RADIUS Server

File Naming and Location

Retrieving Call Detail Records (CDR) from the RADIUS accounting server is relatively straight forward. Call Detail Records are stored on the RADIUS server in plain text in a directory named with the IP Address of the client Sonus SBC 1000/2000 system.

Each file in the directory represents one 24-hour period and is named for the date of the day it represents. Example: Filenames = detail-YYYYMMDD. The path for any particular CDR file is: /usr/local/var/log/radius/radacct/<client-ip-address>/detail-YYYYMMDD

Call Detail Record Format

The following is an example of a typical Call Detail Record.

```
Tue Nov 22 15:20:33 2011
 NET-Log-Time = "Tue Nov 22 15:20:31 2011\n"
 Acct-Status-Type = Start
 NET-Session-Ingress-CallId = 0
 NET-Session-Egress-CallId = 65535
 NET-Session-Generic-Id = 14
 Acct-Multi-Session-Id = "132200403114"
 NET-Ingress-Signaling-Group = 19992
 NET-Egress-Signaling-Group = 0
 NET-Ingress-Channel-Number = 23
 NET-Egress-Channel-Number = 0
 NET-Call-Origin = 1
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
 NET-Calling-Number = "1029"
 NET-Called-Number = "2006"
 NET-Calling-Name = "System Test"
 NET-Ingress-Channel-Id = "1:1:23"
 NET-Setup-Time = "1322004031"
 Acct-Session-Id = "0"
 NET-Firmware-Version = "2.0.0v107"
 NET-Local-Time-Zone = "PST8PDT"
 NET-Gw-Id = "f5a4fdc8f970ae35addf36"
 NET-Time-And-Day = "1322004031"
 NAS-Port = 1813
 Acct-Delay-Time = 0
 NAS-IP-Address = 134.56.227.230
 Acct-Unique-Session-Id = "df05da217dbe16e4"
 Timestamp = 1322004033
 Request-Authenticator = Verified

Tue Nov 22 15:20:33 2011
 NET-Log-Time = "Tue Nov 22 15:20:31 2011\n"
 Acct-Status-Type = Start
 NET-Session-Ingress-CallId = 65535
 NET-Session-Egress-CallId = 1
 NET-Session-Generic-Id = 14
 Acct-Multi-Session-Id = "132200403114"
 NET-Ingress-Signaling-Group = 0
 NET-Egress-Signaling-Group = 5
 NET-Ingress-Channel-Number = 0
 NET-Egress-Channel-Number = 1
 NET-Call-Origin = 2
 NET-Calling-Number = "1029"
 NET-Called-Number = "2006"
 NET-Calling-Name = "System Test"
 NET-Egress-Channel-Id = "0:5:1"
 NET-Setup-Time = "1322004031"
 Acct-Session-Id = "1"
 NET-Firmware-Version = "2.0.0v107"
 NET-Local-Time-Zone = "PST8PDT"
 NET-Gw-Id = "f5a4fdc8f970ae35addf36"
 NET-Time-And-Day = "1322004031"
 NAS-Port = 1813
 Acct-Delay-Time = 0
 NAS-IP-Address = 134.56.227.230
 Acct-Unique-Session-Id = "cb61066babf7983e"
 Timestamp = 1322004033
 Request-Authenticator = Verified

Tue Nov 22 15:20:57 2011
 NET-Log-Time = "Tue Nov 22 15:20:55 2011\n"
 Acct-Status-Type = Stop
 NET-Session-Ingress-CallId = 65535
 NET-Session-Egress-CallId = 1
 NET-Session-Generic-Id = 14
 Acct-Multi-Session-Id = "132200403114"
 NET-Ingress-Signaling-Group = 0
 NET-Egress-Signaling-Group = 5
 NET-Ingress-Channel-Number = 0
 NET-Egress-Channel-Number = 1
 NET-Call-Origin = 2
 NET-Call-Type = 1
 NET-Routing-Table-Number = 0
 NET-Primary-Routing-Number = "2006"
 NET-Disconnect-Cause = 16
 NET-Abort-Cause = 0
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
 Acct-Terminate-Cause = User-Request
 NET-Calling-Number = "1029"
 NET-Called-Number = "2006"
 NET-Calling-Name = "System Test"
 NET-Egress-Channel-Id = "0:5:1"
 Acct-Output-Packets = 228
 Acct-Output-Octets = 36321
 Acct-Input-Packets = 1159
 Acct-Input-Octets = 185440
 NET-Fwd-Flow-In-Src-Addr = "134.56.227.230"
 NET-Bwd-Flow-Out-Dst-Addr = "134.56.227.230"
 NET-Fwd-Flow-Out-Dst-Addr = "134.56.225.90"
 NET-Bwd-Flow-In-Src-Addr = "134.56.225.90"
 NET-Fwd-Flow-In-Dst-Addr = "134.56.227.230"
 NET-Fwd-Flow-Out-Src-Addr = "134.56.227.230"
 NET-Bwd-Flow-In-Dst-Addr = "134.56.227.230"
 NET-Bwd-Flow-Out-Src-Addr = "134.56.227.230"
 NET-Fwd-Flow-Out-Src-Port = 16428
 NET-Bwd-Flow-In-Dst-Port = 2232
 NET-Fwd-Flow-Media-Type = "3"
 NET-Fwd-Flow-PTime = 20
 NET-Bwd-RTP-Avg-Latency = 0
 NET-Bwd-RTP-MaxLatency = 0
 NET-Fwd-RTP-Avg-Jitter = 0
 NET-Bwd-RTP-MaxJitter = 0
 NET-Bwd-RTP-Packets-Lost = 0
 NET-Bwd-Octets = 185440
 NET-Fwd-Flow-Out-Dst-Port = 2232
 NET-Bwd-Packets = 1159
 NET-Setup-Time = "1322004031"
 Acct-Session-Id = "1"
 Acct-Session-Time = 23
 NET-Alert-Time = "1322004031"
 NET-Connect-Time = "1322004032"
 NET-Disconnect-Time = "1322004055"
 NET-Call-Duration = 23
 NET-Disconnect-Initiator = 1
 NET-Outbound-Seize-Time = "1322004031"
 NET-Post-Dial-Delay = 119091
 NET-Egress-Local-Addr = "134.56.227.230"
 NET-Egress-Remote-Addr = "134.56.225.90"
 NET-Ingress-Net-Interface-Id = 775159856
 NET-Egress-Net-Interface-Id = 775159858
 NET-Ingress-Signaling-Port-Num = 5060
 NET-Egress-Signaling-Port-Num = 5060
 NET-Transport-Type = 2
 NET-Firmware-Version = "2.0.0v107"
 NET-Local-Time-Zone = "PST8PDT"
 NET-Gw-Id = "f5a4fdc8f970ae35addf36"
 NET-Time-And-Day = "1322004055"
 NAS-Port = 1813
 Acct-Delay-Time = 0
 NAS-IP-Address = 134.56.227.230
 Acct-Unique-Session-Id = "cb61066babf7983e"
 Timestamp = 1322004057
 Request-Authenticator = Verified

Tue Nov 22 15:20:57 2011
 NET-Log-Time = "Tue Nov 22 15:20:55 2011\n"
 Acct-Status-Type = Stop
 NET-Session-Ingress-CallId = 0
 NET-Session-Egress-CallId = 65535
 NET-Session-Generic-Id = 14
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
Acct-Multi-Session-Id = "132200403114"
NET-Ingress-Signaling-Group = 19992
NET-Egress-Signaling-Group = 0
NET-Ingress-Channel-Number = 23
NET-Egress-Channel-Number = 0
NET-Call-Origin = 1
NET-Call-Type = 1
NET-Routing-Table-Number = 1
NET-Primary-Routing-Number = "2006"
NET-Disconnect-Cause = 16
NET-Abort-Cause = 0
Acct-Terminate-Cause = User-Request
NET-Egress-Final-Routing-Num = "2006"
NET-Calling-Number = "1029"
NET-Called-Number = "2006"
NET-Calling-Name = "System Test"
NET-Ingress-Channel-Id = "1:1:23"
NET-Call-Number-Type = "0"
NET-Call-Plan = "5"
NET-Original-Called-Type = "-1"
NET-Original-Called-Plan = "-1"
NET-Namespace = "-3"
NET-Precedence = "-1"
NET-Presentation = "0"
NET-Screening = "0"
NET-Transfer-Capability = "0"
NET-Transfer-Mode = "0"
NET-Transfer-Rate = "1"
NET-User-Rate = "20"
NET-Setup-Time = "1322004031"
Acct-Session-Id = "0"
Acct-Session-Time = 23
NET-Inbound-Seize-Time = "1322004031"
NET-Alert-Time = "1322004031"
NET-Connect-Time = "1322004032"
NET-Disconnect-Time = "1322004055"
NET-Call-Duration = 23
NET-Disconnect-Initiator = 0
NET-Post-Dial-Delay = 2124
NET-Firmware-Version = "2.0.0v107"
NET-Local-Time-Zone = "PST8PDT"
NET-Gw-Id = "f5a4fdc8f970ae35addf36"
NET-Time-And-Day = "1322004055"
NAS-Port = 1813
Acct-Delay-Time = 0
NAS-IP-Address = 134.56.227.230
Acct-Unique-Session-Id = "df05da217dbe16e4"
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
Timestamp = 1322004057
Request-Authenticator = Verified
```

Vendor Specific Attributes Reference

This page contains a complete current list of the Sonus specific attributes captured and recorded in Call Detail Records (CDR).

- Media Attributes
- Session Signaling Attributes
- Call Attributes
- Time Attributes
- SIP Attributes
- Generic Attributes

Media Attributes

attribute_name	data_type	Call Type	VSA Number	Default Value	Attribute Sent Only On Stop	Description
NET-Fwd-Flow-In-Realm	string	SIP	11		Yes	Not supported:Realm associated with this forward stream.
NET-Fwd-Flow-In-Src-Addr	string	SIP	12		Yes	Source IP for this forward stream.
NET-Fwd-Flow-In-Src-Port	integer	SIP	13	0	Yes	Source port for this forward stream.
NET-Fwd-Flow-In-Dst-Addr	string	SIP	14		Yes	Destination IP for this forward stream.
NET-Fwd-Flow-In-Dst-Port	integer	SIP	15	0	Yes	Destination port for this forward stream.
NET-Fwd-Flow-Out-Realm	string	SIP	16		Yes	Not supported:Realm associated with this forward stream.
NET-Fwd-Flow-Out-Src-Addr	string	SIP	17		Yes	Describes source IP for this reverse stream.
NET-Fwd-Flow-Out-Src-Port	integer	SIP	18	0	Yes	Describes source port for this forward stream.
NET-Fwd-Flow-Out-Dst-Addr	string	SIP	19		Yes	Describes destination IP for this forward stream.
NET-Fwd-Flow-Out-Dst-Port	integer	SIP	20	0	Yes	Describes destination port for this forward stream.
NET-Bwd-Flow-In-Realm	string	SIP	21		Yes	Not supported:Realm associated with this reverse stream.
NET-Bwd-Flow-In-Src-Addr	string	SIP	22		Yes	Source IP for this reverse stream.
NET-Bwd-Flow-In-Src-Port	integer	SIP	23	0	Yes	Source port for this reverse stream.
NET-Bwd-Flow-In-Dst-Addr	string	SIP	24		Yes	Destination IP for this reverse stream.
NET-Bwd-Flow-In-Dst-Port	integer	SIP	25	0	Yes	Destination port for this reverse stream.
NET-Bwd-Flow-Out-Realm	string	SIP	26		Yes	Not supported:Realm associated with this reverse stream.
NET-Bwd-Flow-Out-Src-Addr	string	SIP	27		Yes	Source IP for this reverse stream.

Copyright © 2015 Sonus Networks. All rights reserved.

NET-Bwd-Flow-Out-Src-Port	integer	SIP	28	0	Yes	Source port for this reverse stream.
NET-Bwd-Flow-Out-Dst-Addr	string	SIP	29		Yes	Destination IP for this reverse stream.
NET-Bwd-Flow-Out-Dst-Port	integer	SIP	30	0	Yes	Destination port for this reverse stream.
NET-Fwd-Flow-Media-Type	string	SIP	31		Yes	The media type - voice, fax, data, etc.
NET-Fwd-Flow-PTime	integer	SIP	32	0	Yes	Describes packet ptime in micro seconds.
NET-Fwd-Octets	integer	SIP	33	0	Yes	Number bytes of stream in forward direction.
NET-Fwd-Packets	integer	SIP	34	0	Yes	Total number of packets in forward stream/direction.
NET-Fwd-RTCP-Packets-Lost	integer	SIP	35	0	Yes	Future scope.Total number of RTCP packets lost in forward stream/direction.
NET-Fwd-RTCP-Avg-Jitter	integer	SIP	36	0	Yes	Future scope.RTCP average jitter in forward stream/direction.
NET-Fwd-RTP-Avg-Latency	integer	SIP	37	0	Yes	RTP average latency in forward stream/direction.
NET-Fwd-RTCP-MaxJitter	integer	SIP	38	0	Yes	Future scope.RTCP max jitter in forward stream/direction.
NET-Fwd-RTP-MaxLatency	integer	SIP	39	0	Yes	RTP max latency in forward stream/direction.
NET-Fwd-RTP-Packets-Lost	integer	SIP	40	0	Yes	RTP packets lost in forward stream/direction.
NET-Fwd-RTP-Avg-Jitter	integer	SIP	41	0	Yes	RTP average jitter in forward stream/direction.
NET-Fwd-RTP-MaxJitter	integer	SIP	42	0	Yes	RTP max jitter in forward stream/direction.
NET-Bwd-Octets	integer	SIP	43	0	Yes	Number bytes of stream in backward direction.
NET-Bwd-Packets	integer	SIP	44	0	Yes	Total number of packets in reverse stream/direction.
NET-Bwd-RTCP-Packets-Lost	integer	SIP	45	0	Yes	Future scope.Total number of RTCP packets lost in reverse stream/direction.
NET-Bwd-RTCP-Avg-Jitter	integer	SIP	46	0	Yes	Future scope.RTCP average jitter in reverse stream/direction.
NET-Bwd-RTP-Avg-Latency	integer	SIP	47	0	Yes	RTP average latency in reverse stream/direction.
NET-Bwd-RTCP-MaxJitter	integer	SIP	48	0	Yes	Future scope.RTCP max jitter in reverse stream/direction.
NET-Bwd-RTP-MaxLatency	integer	SIP	49	0	Yes	RTP max latency in reverse stream/direction.
NET-Bwd-RTP-Packets-Lost	integer	SIP	50	0	Yes	RTP packets lost in reverse stream/direction.
NET-Bwd-RTP-Avg-Jitter	integer	SIP	51	0	Yes	RTP average jitter in reverse stream/direction.
NET-Bwd-RTP-MaxJitter	integer	SIP	52	0	Yes	RTP max jitter in reverse stream/direction.

Session Signaling Attributes

attribute_name	data_type	Call Type	VSA Number	Default Value	Attribute Sent Only On Stop	Description

Copyright © 2015 Sonus Networks. All rights reserved.

NET-Session-Ingress-CallId	integer	ISDN/CAS/SIP	60	65535	No	This ID corresponds to INBOUND Call leg of the same call.0xFFFF(65535) is INVALID number and would be used to indicate that the value needs to be ignored.
NET-Session-Egress-CallId	integer	ISDN/CAS/SIP	61	65535	No	This ID corresponds to OUTBOUND Call leg of the same call.0xFFFF(65535) is INVALID number and would be used to indicate that the value needs to be ignored.
NET-Session-Generic-Id	integer	ISDN/CAS/SIP	62	0	No	Describes call identifier (conference ID)0 - Invalid
NET-Routing-Table-Number	integer	ISDN/CAS/SIP	63	0	Yes	Routing table number selected for this call. 0 is INVALID number and would be used to indicate that the value needs to be ignored.
NET-Ingress-Signaling-Group	integer	ISDN/CAS/SIP	64	0	No	Incoming signaling group. 0 is INVALID number and would be used to indicate that the value needs to be ignored. Valid range:1 - 10000 - SIP SG,10001 - 20000 - ISDN SG,20001 - 30000 - CAS SG This attribute is applicable only for INBOUND Call legs.
NET-Egress-Signaling-Group	integer	ISDN/CAS/SIP	65	0	No	Outgoing signaling group. 0 is INVALID number and would be used to indicate that the value needs to be ignored. Valid range: 1 - 10000 - SIP SG,10001 - 20000 - ISDN SG,20001 - 30000 - CAS SG This attribute is applicable only for OUTBOUND Call legs.
NET-Primary-Routing-Number	string	ISDN/CAS/SIP	66		Yes	Primary routing number. Empty string is used to indicate that the value needs to be ignored. "" - Invalid
NET-Egress-Final-Routing-Num	string	ISDN/CAS/SIP	67		Yes	Final routing number. Empty string is used to indicate that the value needs to be ignored. " - Invalid this is valid only for Ingress call. For Egress call, it will have default value of 0.
NET-Ingress-Channel-Number	integer	ISDN/CAS/SIP	68	0	No	Incoming channel number. 0 is INVALID number and would be used to indicate that the value needs to be ignored. Valid range: 1 - 1000This attribute are applicable only for INBOUND Call legs.
NET-Egress-Channel-Number	integer	ISDN/CAS/SIP	69	0	No	Outgoing channel number. 0 is INVALID number and would be used to indicate that the value needs to be ignored. Valid range:1 - 1000. This attribute are applicable only for OUTBOUND Call legs.
NET-Call-Type	integer	ISDN/CAS/SIP	70	0	Yes	Describes the call type. 0= unset, 1 = voice, 2 = T38Fax, 11 = Fax_PassThrough 12 = Modem_PassThrough Note: In case of TDM to TDM calls only "1=voice" is supported.ZERO is used to indicate that the value needs to be ignored
NET-Call-Origin	integer	ISDN/CAS/SIP	71	0	No	Describes the call direction. 0=eINVALID,1=eINBOUND,2=eOUTBOUND,0 is INVALID number and would be used to indicate that the value needs to be ignored.
NET-Calling-Number	string	ISDN/CAS/SIP	72		No	Calling number. "" - Invalid. Note: Special config setting required for CAS. NET-Calling-Number attribute for FXS requires assigning Own Number to applied ports. Under Web UI - System tab Select the CAS SG entry from the Signaling Group, click on Channel Hunting pull down list and select the Own Number. Assign the ports with calling phone number.
NET-Called-Number	string	ISDN/CAS/SIP	73		No	Called Number. "" - Invalid
NET-Calling-Name	string	ISDN/CAS/SIP	74		No	Calling Name, if present
NET-Disconnect-Cause	integer	ISDN/CAS/SIP	75	0	Yes	Disconnect cause - Must for Disconnect case. 0 is used to indicate that the value needs to be ignored.
NET-Abort-Cause	integer	ISDN/CAS/SIP	76	0	Yes	Abort cause - Must for Abort case. 0 is used to indicate that the value needs to be ignored.
NET-Ingress-Channel-Id	string	ISDN/CAS/SIP	77		No	ISDN/CAS : Card:Port:Channel, SIP : Card:SGID:Channel. Null indicates no value provided and needs to be ignored. This attribute are applicable only for INBOUND Call legs.

Copyright © 2015 Sonus Networks. All rights reserved.

NET-Egress-Channel-Id	string	ISDN/CAS/SIP	78		No	ISDN/CAS : Card:Port:Channel, SIP : Card:SGID:Channel. Null indicates no value provided and needs to be ignored. This attribute are applicable only for OUTBOUND Call legs.
NET-Call-Priority	string	ISDN/CAS/SIP	79		No	Call priority, if present.

Call Attributes

attribute_name	data_type	Call Type	VSA Number	Default Value	Attribute Sent Only On Stop	Description
NET-Call-Number-Type	string	ISDN	90	-1	Yes	Describes call number type. 0 = Unknown ,1 = International Number,2 = National Number,3 = Network Specific Number,4 = Subscriber Number ,5 = Abbreviated number,-1 - would be used to indicate that the value needs to be ignored.
NET-Call-Plan	string	ISDN	91	-1	Yes	Describes call plan. 0 = Unknown, 1 = ISDN/Telephony numbering plan, 2 = Data Numbering plan, 3 = Telex Numbering plan, 4 = National Standard numbering plan, 5 = Private numbering plan, 6 = Reserved for extension, -1 - would be used to indicate that the value needs to be ignored.
NET-Original-Called-Number	string	ISDN	92		Yes	Describes original called number
NET-Original-Called-Type	string	ISDN	93	-1	Yes	Describes original called number type. 0 = Unknown ,1 = International Number, 2 = National Number, 3 = Network Specific Number, 4 = Subscriber Number, 5 = Abbreviated number.-1 - Would be used to indicate that the value needs to be ignored.
NET-Original-Called-Plan	string	ISDN	94	-1	Yes	Describes original called number plan.0 = Unknown, 1 = ISDN/Telephony numbering plan, 2 = Data Numbering plan, 3 = Telex Numbering plan, 4 = National Standard numbering plan, 5 = Private numbering plan,6 = Reserved for extension. -1 - Would be used to indicate that the value needs to be ignored.
NET-Called-Name	string	ISDN	95		Yes	Describes called name.
NET-Namespace	string	ISDN	96	-3	Yes	Describes Namespace used. -2 = Disabled, -1 = Transparent, 0 = Unset / Untranslated, 1 = DSN, 2 = DRSN, 3 = Q.735, 4 = Maximum value ,0 - Unset/Untranslated used for configuring transformation only and never seen at protocol level.-3 - would be used to indicate that the value needs to be ignored.
NET-Precedence	string	ISDN	97	-1	Yes	Describes call precedence.0 = Unset, 1 = Lowest, 5 = Routine, 10 = Priority, 15 = Immediate, 20 = Flash, 25 = Flash Override, 31 = Flash Override always, 32 = Maximum value.-1 - Would be used to indicate that the value needs to be ignored
NET-Presentation	string	ISDN	98	-1	Yes	Describes call presentation. 0 = Presentation Allowed, 1 = Presentation Restricted, 2 = Number not available due to interworking, 3 = Reserved. -1 - Would be used to indicate that the value needs to be ignored.
NET-Screening	string	ISDN	99	-1	Yes	Describes call screening.0 = User provided(not screened), 1 = User provided(verified and passed), 2 = User provided(verified and failed), 3 = Network provided. -1 - Would be used to indicate that the value needs to be ignored.
NET-Transfer-Capability	string	ISDN	100	-1	Yes	Describes Transfer capability.0 = Speech, 1 = Unrestricted Digital Information, 2 = Restricted Digital information, 3 = 3.1 kHz audio, 4 = Unrestricted digital information with tones/announcements, 5 = Video.-1 - Would be used to indicate that the value needs to be ignored.
NET-Transfer-Mode	string	ISDN	101	-1	Yes	Describes transfer mode.0 = Circuit-mode, 1 = Packet-mode.-1 - Would be used to indicate that the value needs to be ignored.
NET-Transfer-Rate	string	ISDN	102	-1	Yes	Describes transfer rate.0 = This code shall be used for all packet calls, 1 = 64 kbit/s circuit mode, 2 = 2 x 64 kbit/s circuit mode, 3 = 384 kbit/s circuit mode, 4 = 1472 kbit/s, 5 = 1536 kbit/s circuit mode, 6 = 1920 kbit/s circuit mode, 7 = Multirate (64 kbit/s base rate).-1 - Would be used to indicate that the value needs to be ignored.
NET-User-Rate	string	ISDN	103	-1	Yes	Describes user rate.18 = 56 kbit/s, 20 = 64 kbit/s Recommendation X.1.-1 - Would be used to indicate that the value needs to be ignored.

Copyright © 2015 Sonus Networks. All rights reserved.

Time Attributes

attribute_name	data_type	Call Type	VSA Number	Default Value	Attribute Sent Only On Stop	Description
NET-Setup-Time	string	ISDN/CAS/SIP	110		No	Call setup time. This value indicates time in terms of Seconds in UNIX EPOCH format.
NET-Alert-Time	string	ISDN/CAS/SIP	111		Yes	Call alert time. This value indicates time in terms of Seconds in UNIX EPOCH format.
NET-Connect-Time	string	ISDN/CAS/SIP	112		Yes	Call connect time, the date and time the call was actually connected, in UNIX EPOCH format. The time will be the local time configured on the Sonus SBC 1000/2000
NET-Disconnect-Time	string	ISDN/CAS/SIP	113		Yes	Call disconnect time ,the date and time the call terminated, in UNIX EPOCH format. The time will be the local time configured on the Sonus SBC 1000/2000
NET-Inbound-Seize-Time	string	ISDN/CAS/SIP	114		Yes	Inbound seize time. This value indicates time in terms of Seconds in UNIX EPOCH format.
NET-Outbound-Seize-Time	string	ISDN/CAS/SIP	115		Yes	Outbound seize time. This value indicates time in terms of Seconds in UNIX EPOCH format.
NET-Call-Duration	integer	ISDN/CAS/SIP	116	0	Yes	Call duration (call length) in seconds (rounded to nearest second). The value will be 0 if never connected.
NET-Post-Dial-Delay	integer	ISDN/CAS/SIP	117	0	Yes	Post dial delay in micro seconds.
NET-Disconnect-Initiator	integer	ISDN/CAS/SIP	118	0	Yes	Disconnect initiator: 0 - Indicates that this Channel did not initiate the Call disconnect from CCC standpoint, i.e. it received Disconnect from other call leg associated with the call.1 - Indicates that this Channel initiated the Call disconnect from CCC standpoint, i.e. it received Disconnect from external interface.

SIP Attributes

attribute_name	data_type	Call Type	VSA Number	Default Value	Attribute Sent Only On Stop	Description
NET-P-Asserted-ID	string	SIP	130		Yes	Indicates P-Asserted ID.
NET-SIP-Diversion	string	SIP	131		Yes	Describes SIP diversion header.
NET-Ingress-Local-Addr	string	SIP	132		Yes	Incoming local IP-This attribute will be applicable for Inbound call leg. For Outbound call leg this will be NULL.
NET-Ingress-Remote-Addr	string	SIP	133		Yes	Incoming Remote IP. This attribute will be applicable for Outbound call leg. For Inbound call leg this will be NULL.
NET-Egress-Local-Addr	string	SIP	134		Yes	Outgoing local IP. This attribute will be applicable for Outbound call leg. For Inbound call leg this will be NULL.
NET-Egress-Remote-Addr	string	SIP	135		Yes	Outgoing remote IP. This attribute will be applicable for Outbound call leg. For Inbound call leg this will be NULL.
NET-Ingress-Net-Interface-Id	integer	SIP	136	0	Yes	Incoming network interface ID. This attribute are applicable only for INBOUND Call legs.
NET-Egress-Net-Interface-Id	integer	SIP	137	0	Yes	Outgoing network interface ID. This attribute are applicable only for OUTBOUND Call legs.
NET-Refer-Call-Transfer-Id	string	SIP	138		Yes	REFER call transfer ID.

Copyright © 2015 Sonus Networks. All rights reserved.

NET-Session-Forked-Call-Id	string	SIP	139		Yes	Session forked call ID.
NET-Redirect-Number	string	SIP	140		Yes	Redirect number.
NET-Redirect-Ip-Address	string	SIP	141		Yes	Redirect IP address.
NET-Session-Ingress-Realm	string	SIP	142		Yes	Incoming IP realm- Will be provided only if realm is present. IP will be ignored.
NET-Session-Egress-Realm	string	SIP	143		Yes	Outgoing IP realm- Will be provided only if realm is present. IP will be ignored.
NET-Ingress-Signaling-Port-Num	integer	SIP	144	0	Yes	Incoming signaling port number 0 is used to indicate that the value needs to be ignored. This attribute are applicable only for INBOUND Call legs.
NET-Egress-Signaling-Port-Num	integer	SIP	145	0	Yes	Outgoing signaling port number 0 is used to indicate that the value needs to be ignored. This attribute are applicable only for OUTBOUND Call legs.
NET-Transport-Type	integer	SIP	146	0	Yes	Provides the last snapshot of Transport type used in the call. Possible values UDP, TCP or TLS 0=eNONE,1=eUDP,2=eTCP,3=eTLS
NET-P-Preferred-ID	string	SIP	147		No	P-Preferred-Identity header from SIP Invite message

Generic Attributes

attribute_name	data_type	Call Type	VSA Number	Default Value	Attribute Sent Only On Stop	Description
NET-Firmware-Version	string	ISDN/CAS/SIP	160		No	Indicates Sonus SBC 1000/2000 firmware version.
NET-Local-Time-Zone	string	ISDN/CAS/SIP	161		No	Indicates Sonus SBC 1000/2000 local time zone.
NET-Gw-Id	string	ISDN/CAS/SIP	162		No	Indicates Sonus SBC 1000/2000 gateway ID.
NET-Time-And-Day	string	ISDN/CAS/SIP	163		No	Indicates CDR creation Date and time, Sonus SBC 1000/2000 local time in terms of seconds in UNIX EPOCH format.
NET-Log-Time	string	ISDN/CAS/SIP	164		No	Indicates CDR log time. Format:Day Month dd hh:mm:ss yyyy Example:Thu Nov 17 16:56:12 2011

Viewing Call Detail Record Statistics

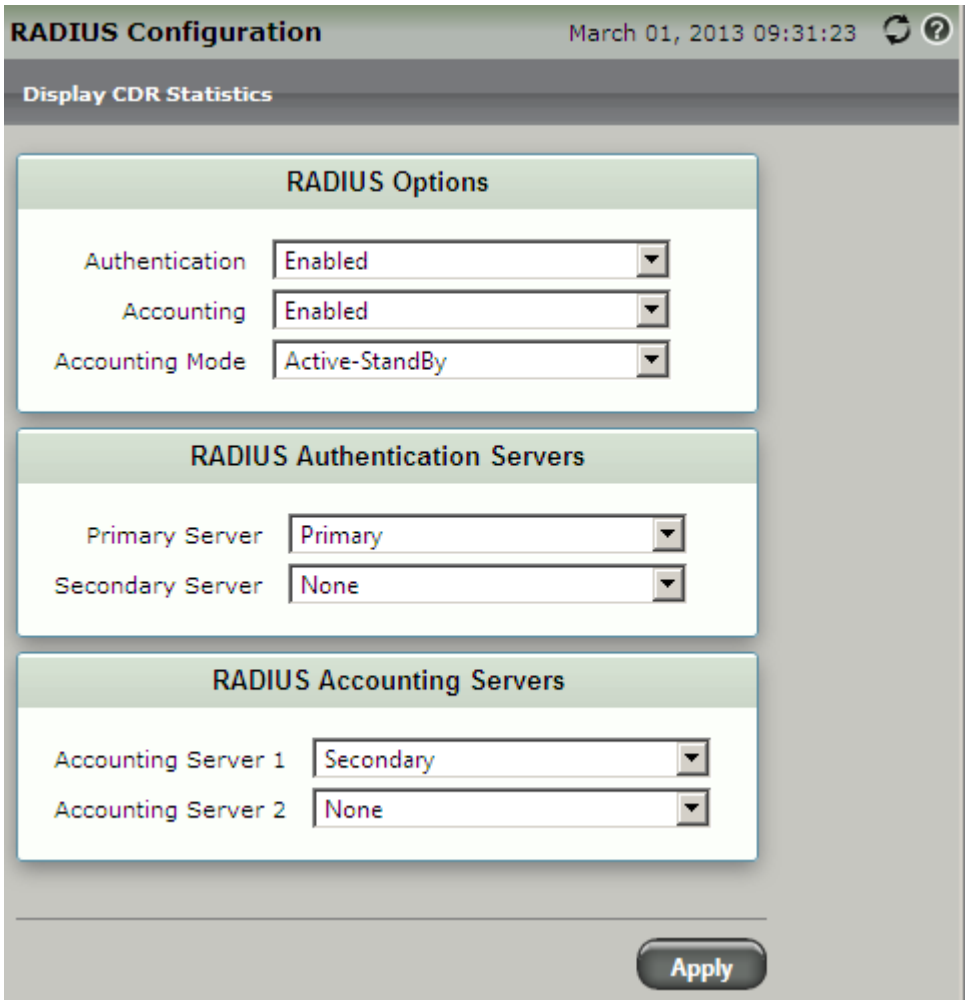
The Sonus SBC 1000/2000 provides Call Detail Record statistics that keep track of the transactions between the Sonus SBC 1000/2000 and the accounting server(s). Related information about RADIUS server specific counters that provide insight into their health and communication status can be found on the Managing RADIUS Servers page.

Viewing Call Detail Record Statistics

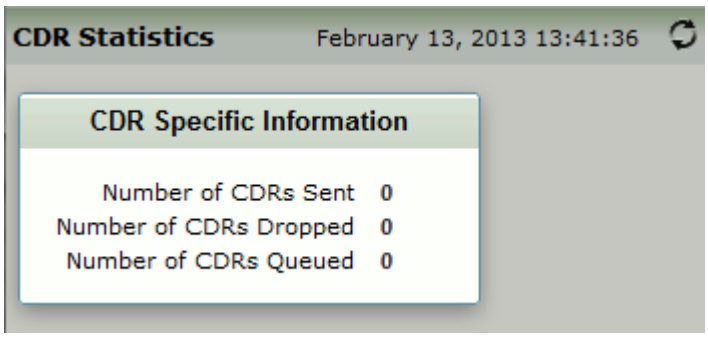
To view Call Detail Record Statistics:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Auth and Directory Services > RADIUS > Configuration**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Click the **Display CDR Statistics**text at the top of the page.



Number of CDRs Sent

The number of records sent to accounting server since last counter reset.

Number of CDRs Dropped

The number or Call Detail Records removed from the queue after reaching the maximum number or re-tries for a failed server.

Copyright © 2015 Sonus Networks. All rights reserved.

Number of CDRs Queued

The number of currently queued records ready to be sent to the server.

Working with the Web Interface

Out of the box, the Sonus SBC 1000/2000 is configured primarily using a web browser via a web interface hosted on the Sonus SBC 1000/2000 system.

The **Sonus SBC 1000/2000 Web Interface** (WebUI) provides System Administrators with the following functionality:

Configuration

The WebUI provides a full range of configuration options to end-users. To list a few, the ability to configure IP interfaces, setting the telephony ports, configuring routes and digit manipulation, and managing Users and Groups.

> ✅ System administrators managing multiple Sonus SBC 1000/2000 systems should consider using the Sonus SBC 1000/2000 REST API for quick and consistent configuration/deployment.

Monitoring

The WebUI provides real-time monitoring of channels, in-progress calls and system alarms.

Logging

The WebUI provides end-users the ability to access and finely tune the log settings from debug-level detail to critical messages only.

Management

On-going system management is handled through the WebUI, from changing the system settings, updating system licenses, to software upgrades and system restarts.

Start Using the WebUI

In order to configure Sonus SBC 1000/2000 after your have completed the Initial Setup process, you must use a compatible web browser to access the Sonus SBC 1000/2000 and configure it for your environment.

- Logging in to Sonus SBC 1000-2000
- Managing Login Messages
- Monitoring Real Time Status
- Viewing Alarms and Events

Logging in to Sonus SBC 1000-2000

The Sonus SBC 1000/2000 login page is displayed upon completing the steps outlined in Running Initial Setup, when Rebooting Sonus SBC 1000-2000, when Upgrading Sonus SBC 1000-2000, or when the user's browser session expires. Typically, the session between a logged in user and the Sonus SBC 1000/2000 expires when the user closes their browser.

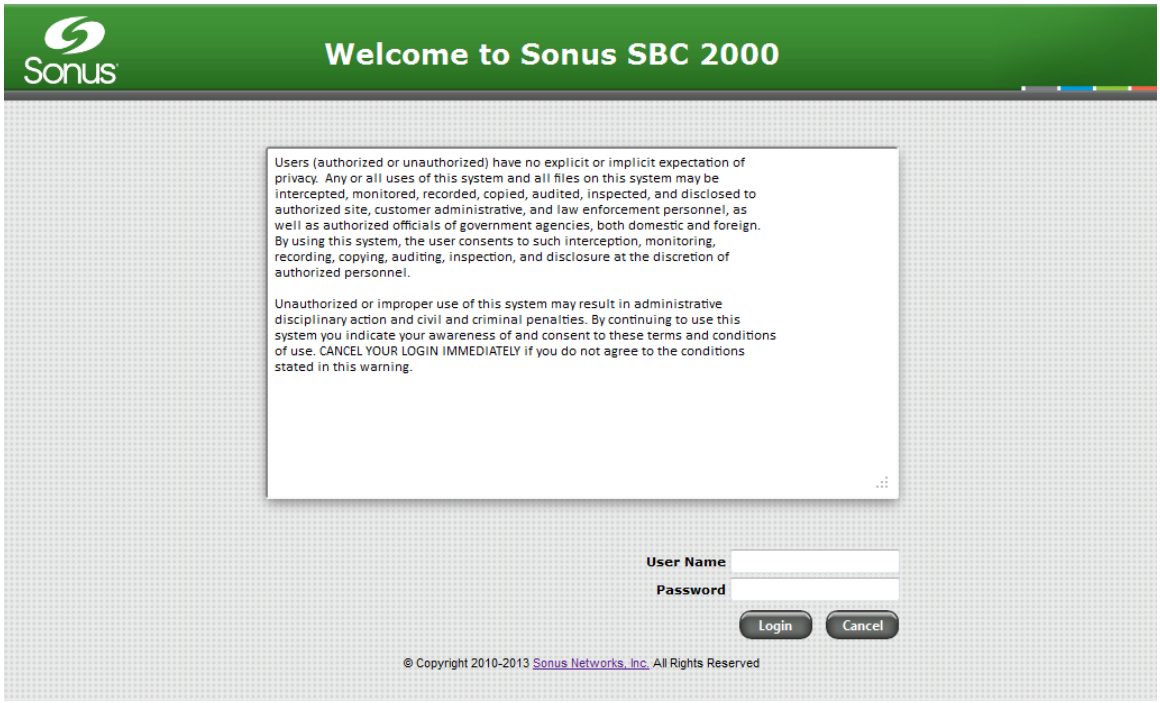
Copyright © 2015 Sonus Networks. All rights reserved.

Once logged in, depending on the the user's permissions, the user may have some limited functionality. See related topics:

- How User Authentication Works
- Managing Local Users, Managing Remote Authentication
- Changing The Current User's Password
- Monitoring User Activity

Secured Login

Because the Sonus SBC 1000/2000 is accessed over HTTPs, the user's credentials (and Sonus SBC 1000/2000 browser cookies) are sent securely.



Managing Login Messages

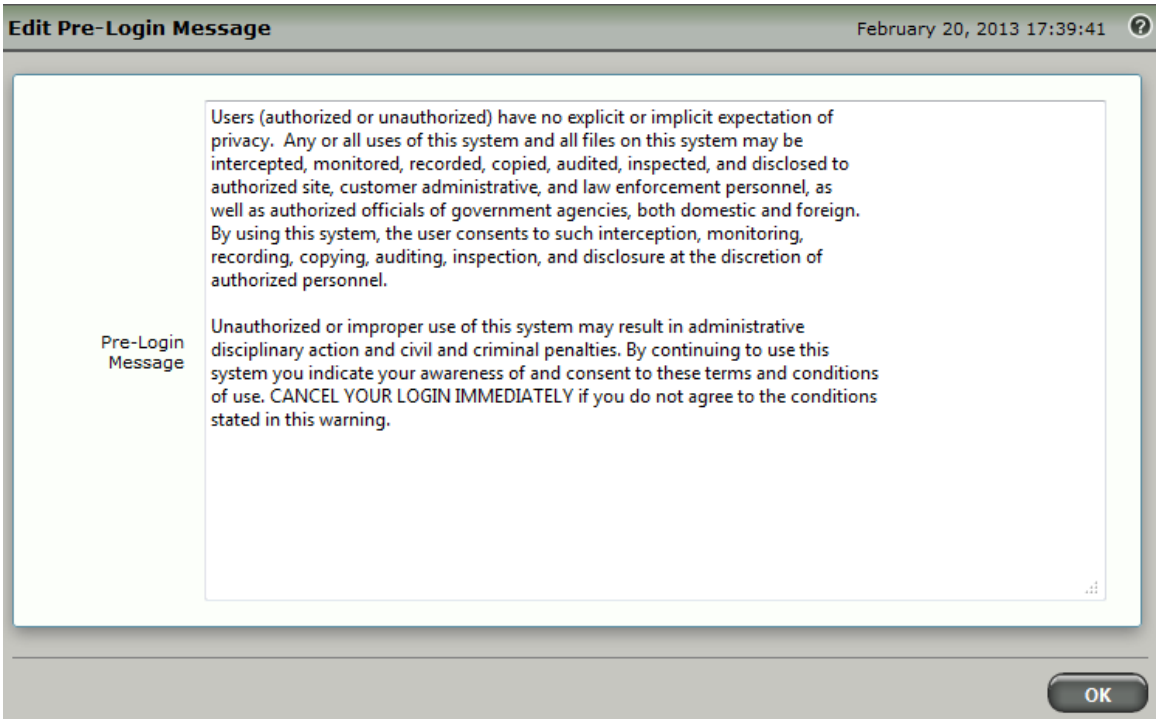
Administrators can configure the Sonus SBC 1000/2000 to display pre-login and post-login messages to users. If one is configured, a pre-login message appears just above the login dialog, and a post-login message is presented as a dialog following successful login.

Modifying the Pre-Login Messages

This message is presented to the user on the login screen

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > Login Messages > Pre-Login Message**.

Copyright © 2015 Sonus Networks. All rights reserved.



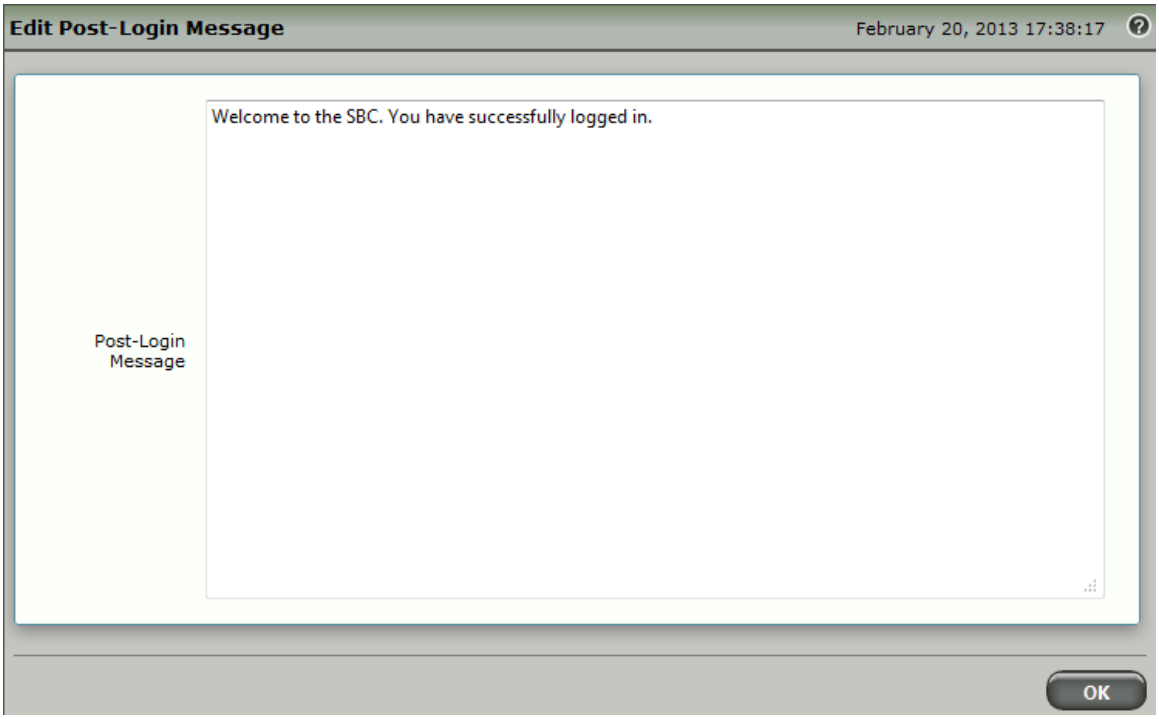
3. Enter the messge in the **Pre-Login Message** text field.
4. Click **OK**.

Modifying the Post-Login Messages

This message is presented to the user immediately following a successful login

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Security > Login Messages > Post-Login Message**.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Enter the message text in the **Post-Login Message** text field.
   If no text is entered, no message will be presented to the user.
4. Click **OK**.

Monitoring Real Time Status

This panel provides current information on the status of Ports, Channels and in-progress Calls on the Sonus SBC 1000/2000 system.

Browser Support

See the Supported Platforms page for a list of supported browsers.

Real Time Status View

To view real-time status:

- Click the **Monitor** tab in the WebUI.

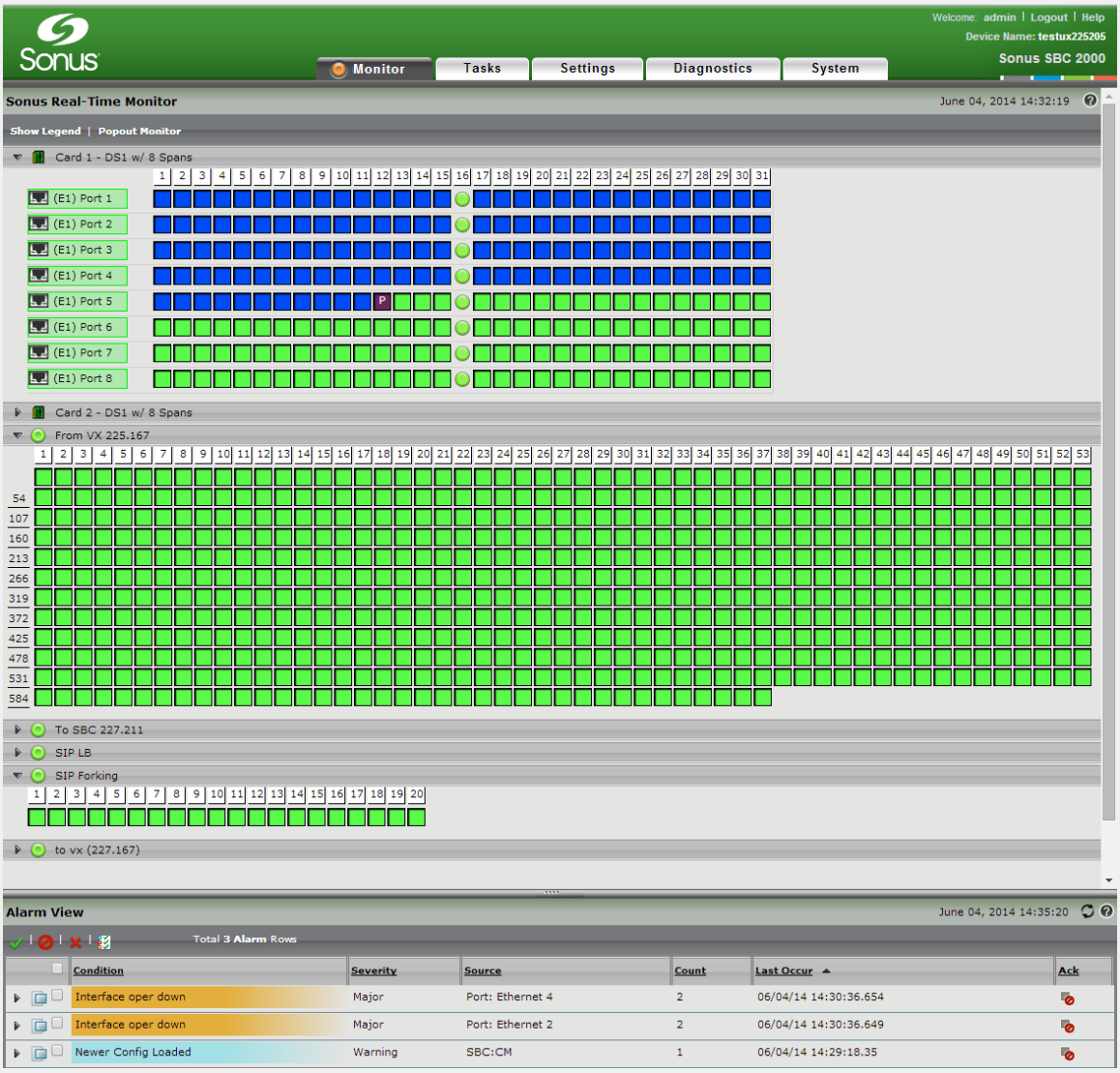
SBC1000

Copyright © 2015 Sonus Networks. All rights reserved.



SBC2000

Copyright © 2015 Sonus Networks. All rights reserved.



For more information about Alarms and Events, see the Alarms and Events Reference page.

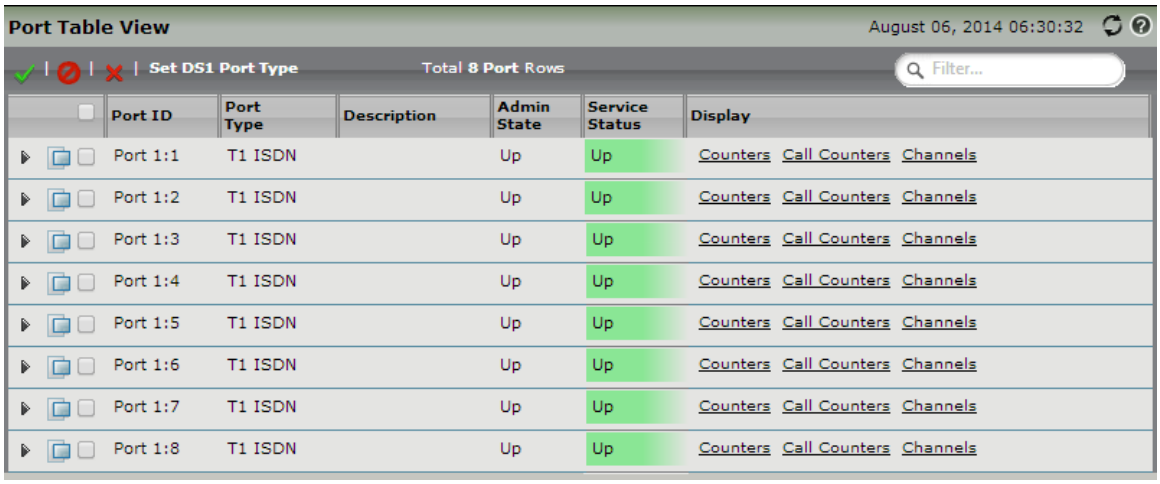
Module/Card, Port, and Signaling Group Information

Viewing Port and Card/Module Status

To access card/module status:

- In the monitor view, click the card/module icon ( ) for the card you wish to check.
  The Port Table View for that card/module is displayed. It contains port status information as well as links to the various counters.

Copyright © 2015 Sonus Networks. All rights reserved.

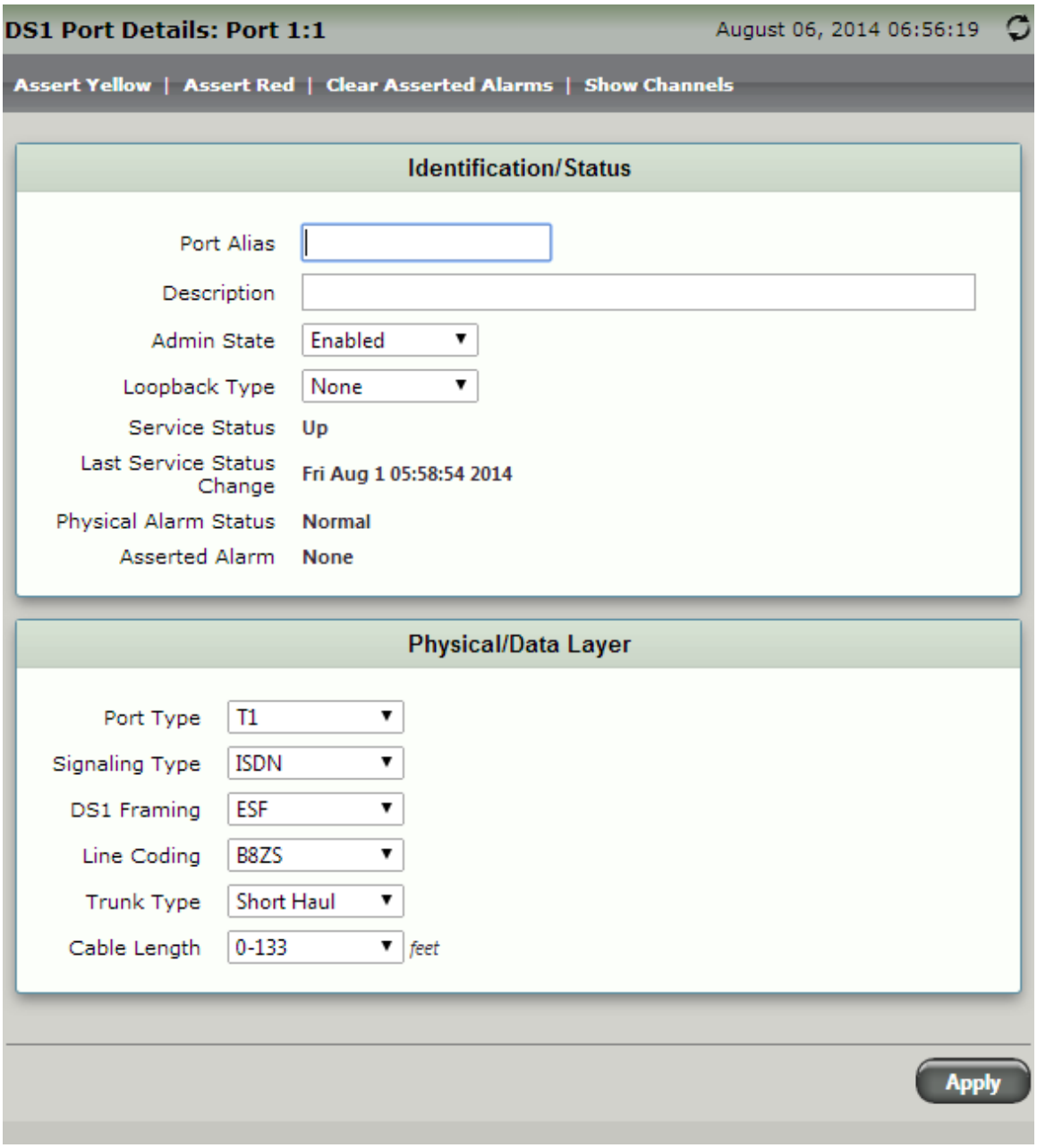


For information about counters see, Viewing Port Counters and Channel Details.

Viewing Port Configuration Details

- To view port configuration details, click the port icon ( ).
  The DS1 Port Details view is displayed. It contains port configuration information.

Copyright © 2015 Sonus Networks. All rights reserved.

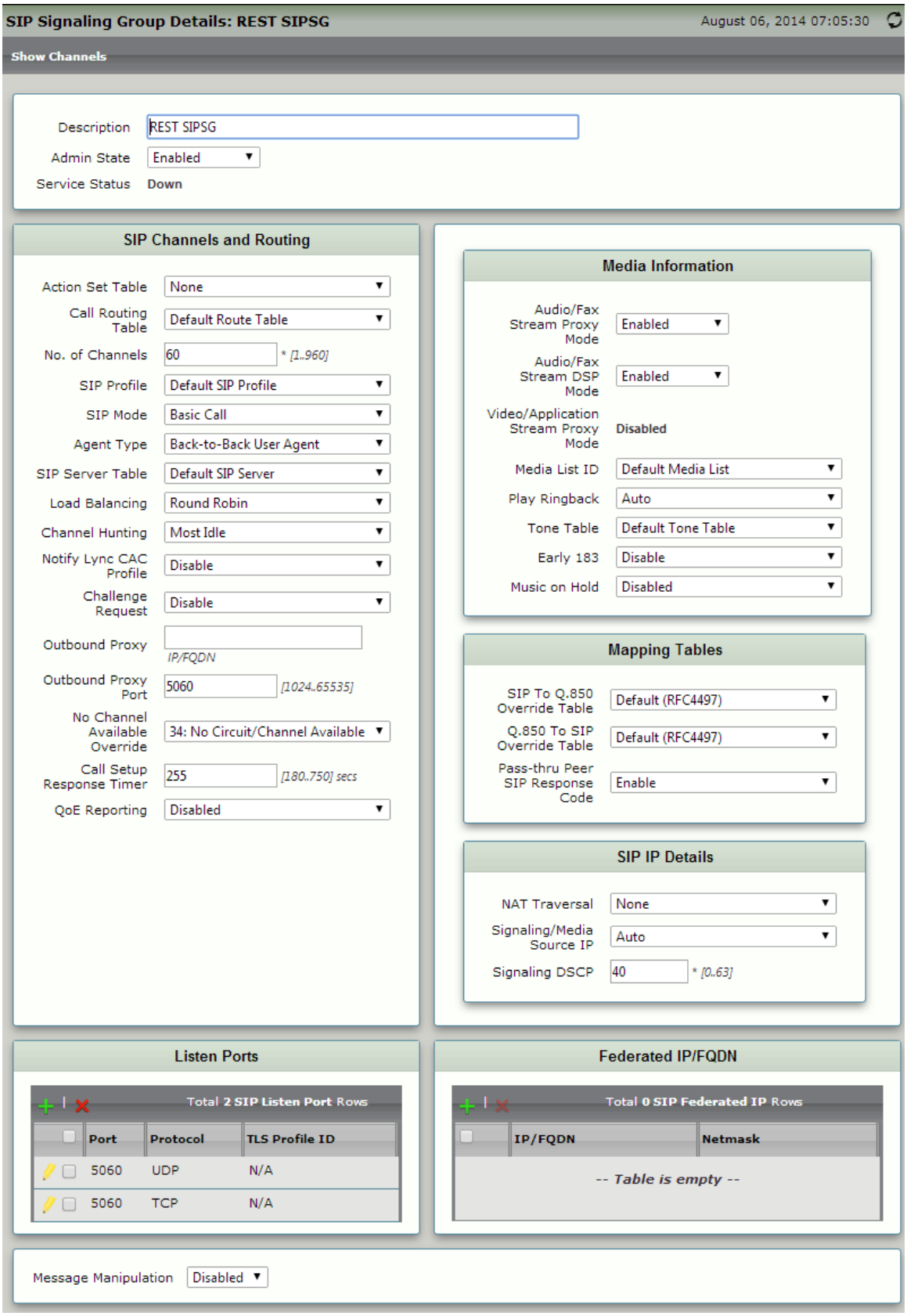


Viewing Signaling Groups

To view details about a Signaling Group:

- Click the Signaling Group icon ( ).
  The Signaling Group Details dialog is displayed.

Copyright © 2015 Sonus Networks. All rights reserved.



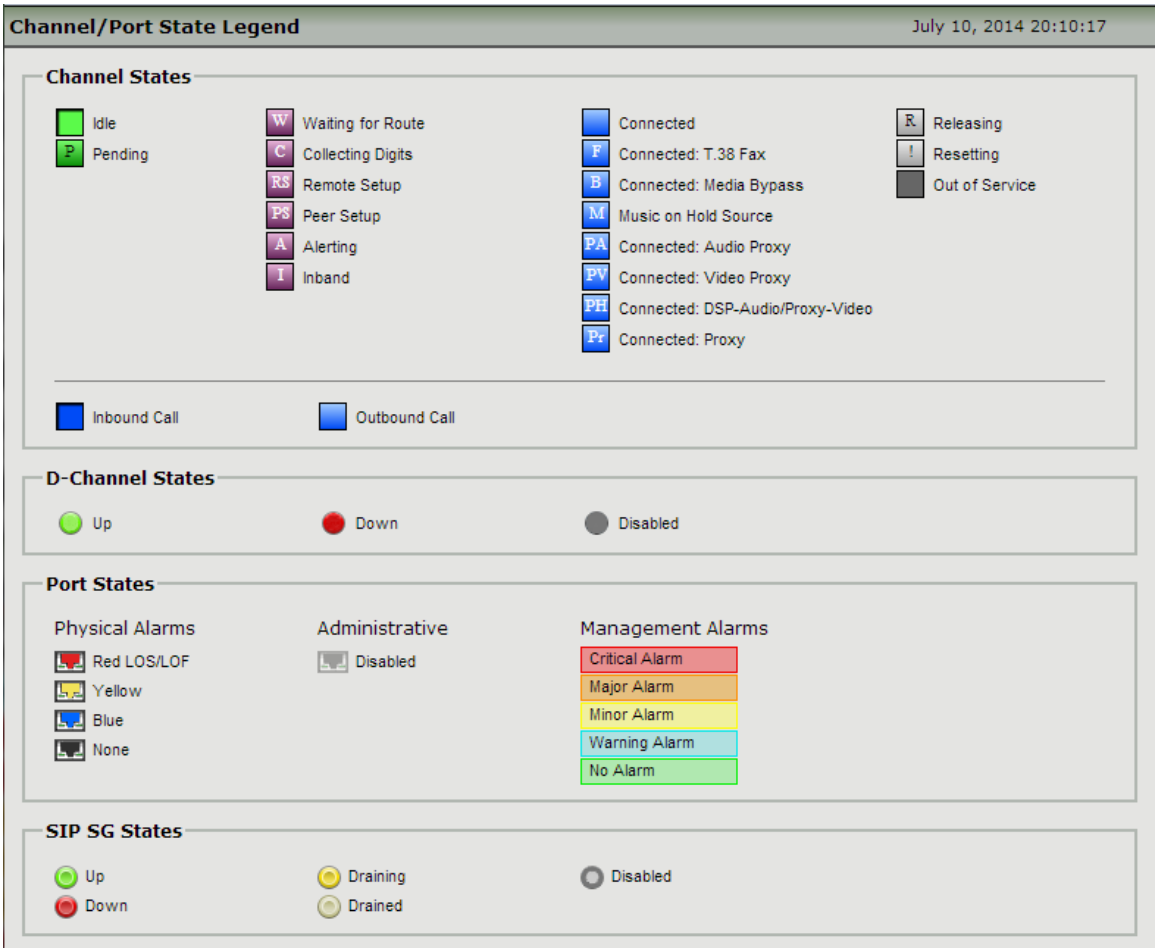
For more information about Signaling Groups, see Managing Signaling Groups.

Channel/Port State Legend

Copyright © 2015 Sonus Networks. All rights reserved.

To view the Status Icon Legend:

- Click the **Show Legend** link text at the top of the **Real-Time Monitor** page.



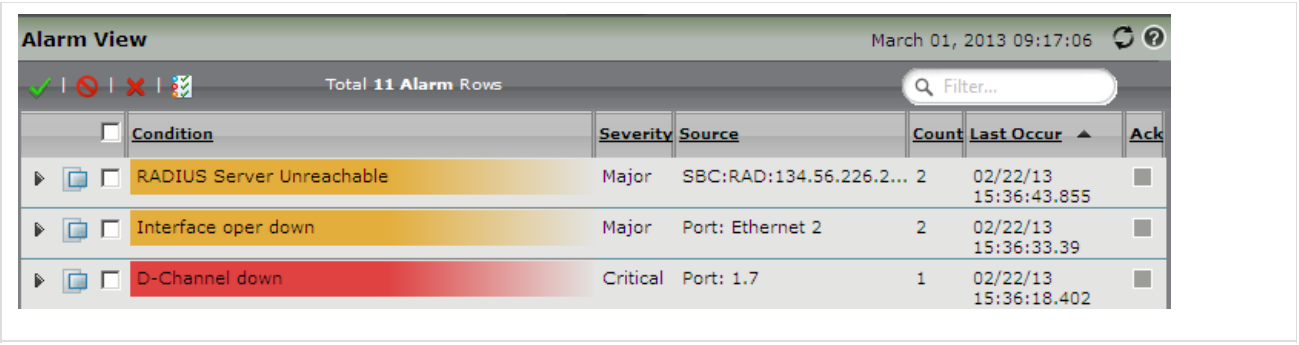
Viewing Alarms and Events

The Sonus SBC 1000/2000 captures system-wide alarms and events which can be viewed (and configurable) directly from the WebUI. In addition to logging, These alarms/events serve a very useful purpose when troubleshooting configuration issues or when diagnosing problems.

Accessing the Alarms View

1. In the WebUI, click the **Monitor** tab.
2. The **Alarm View** pane is located at the bottom of the screen.

Copyright © 2015 Sonus Networks. All rights reserved.



3. In the row listing the alarm, click the arrow icon or the popup icon .

Alarm Color Reference and Types

Active alarms are displayed with different colors based on the severity.

Severity Level	Color	Description
Critical	Red	This represents the highest severity an alarm can have and the system needs immediate attention.
Major	Orange	Alarm that has a significant impact on the system, for example: *Signaling group is down*
Minor	Yellow	Alarm that has a moderate impact on the system, for example: *AD cashing failed*
Warning	Blue/Cyan	Lowest severity level of the alarm, for example: *Route temporarily disabled*

For more information about individual alarms and events, see the Alarms and Events Reference.

Acting on Displayed Alarms

In the event of finding new alarms, address what is causing them by following these instructions:

1. In the WebUI, click the **Monitor** tab.
2. The **Alarm View** pane is located at the bottom of the screen.
3. In the list of alarms, select one or more alarms.
4. Click one of the icons above the list of alarms:
   - - **Acknowledge** - Click this icon to indicate that corrective action is being taken by a system administrator.
   - - **Unacknowledge** - Click this icon to indicate that this alarm is to be considered by a system

Copyright © 2015 Sonus Networks. All rights reserved.

administrator.

- - **Clear** - Click this icon to indicate that the alarm is resolved.

Changing the Refresh Rate

1. In the WebUI, click the **Monitor** tab.
2. The **Alarm View** pane is located at the bottom of the screen.
3. Click the **Properties** icon.
4. In the **Refresh Interval** field, enter an interval in seconds (default is 60 seconds).
5. Click **OK**.

Working with ISDN

ISDN is supported on the Sonus SBC 1000/2000 DS1 interface. Each DS1 interface can be configured for T1 or E1. Sonus SBC 1000/2000 supports both "ISDN to ISDN" and "ISDN to/from SIP" calls.

Sonus SBC 1000/2000 Supports ISDN PRI trunks with the following ISDN variants:

- Q.SIG
- EuroISDN
- Nortel DMS-100
- National ISDN Number 2 (NI-2)
- AT&T 4ESS
- AT&T 5ESS
- NTT INS NET 1500

Managing ISDN Signaling Groups

Copyright © 2015 Sonus Networks. All rights reserved.

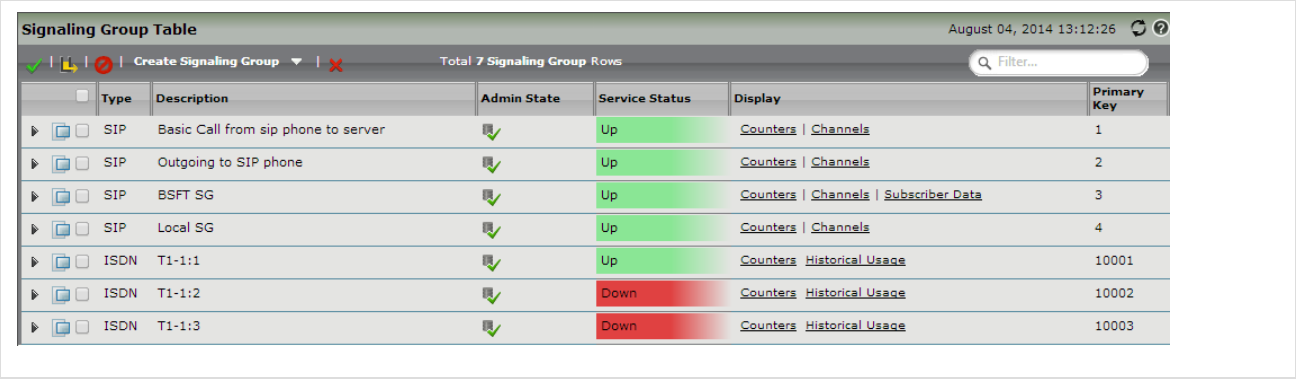
- Viewing ISDN Counters
  - Viewing ISDN BRI Counters
  - Viewing ISDN T1 - E1 Counters
- Creating and Modifying ISDN Signaling Groups

Managing ISDN Signaling Groups

Signaling groups allow telephony channels to be grouped together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which Call Routes are selected. They are also the location from which Tone Tables and Action Sets are selected. In the case of ISDN, they specify the protocol layer settings, like Switch Variant (the physical layer settings are configured from Ports).

Working with ISDN Signaling Groups

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. From the **Create Signaling Group** drop down box, select **ISDN Signaling Group.**



To view an ISDN Signaling Group's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

> **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Viewing ISDN Counters

- Viewing ISDN BRI Counters
- Viewing ISDN T1 - E1 Counters

Creating and Modifying ISDN Signaling Groups

Viewing ISDN Counters

- Viewing ISDN BRI Counters
- Viewing ISDN T1 - E1 Counters

Viewing ISDN BRI Counters

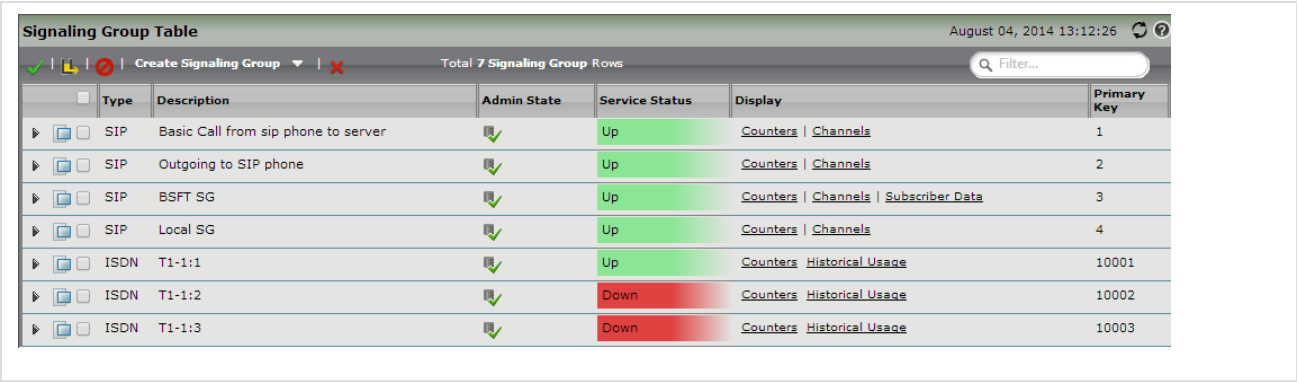
Copyright © 2015 Sonus Networks. All rights reserved.

The ISDN counters allow you to see the communications statistics for an ISDN Signaling Group.

Viewing ISDN Counters

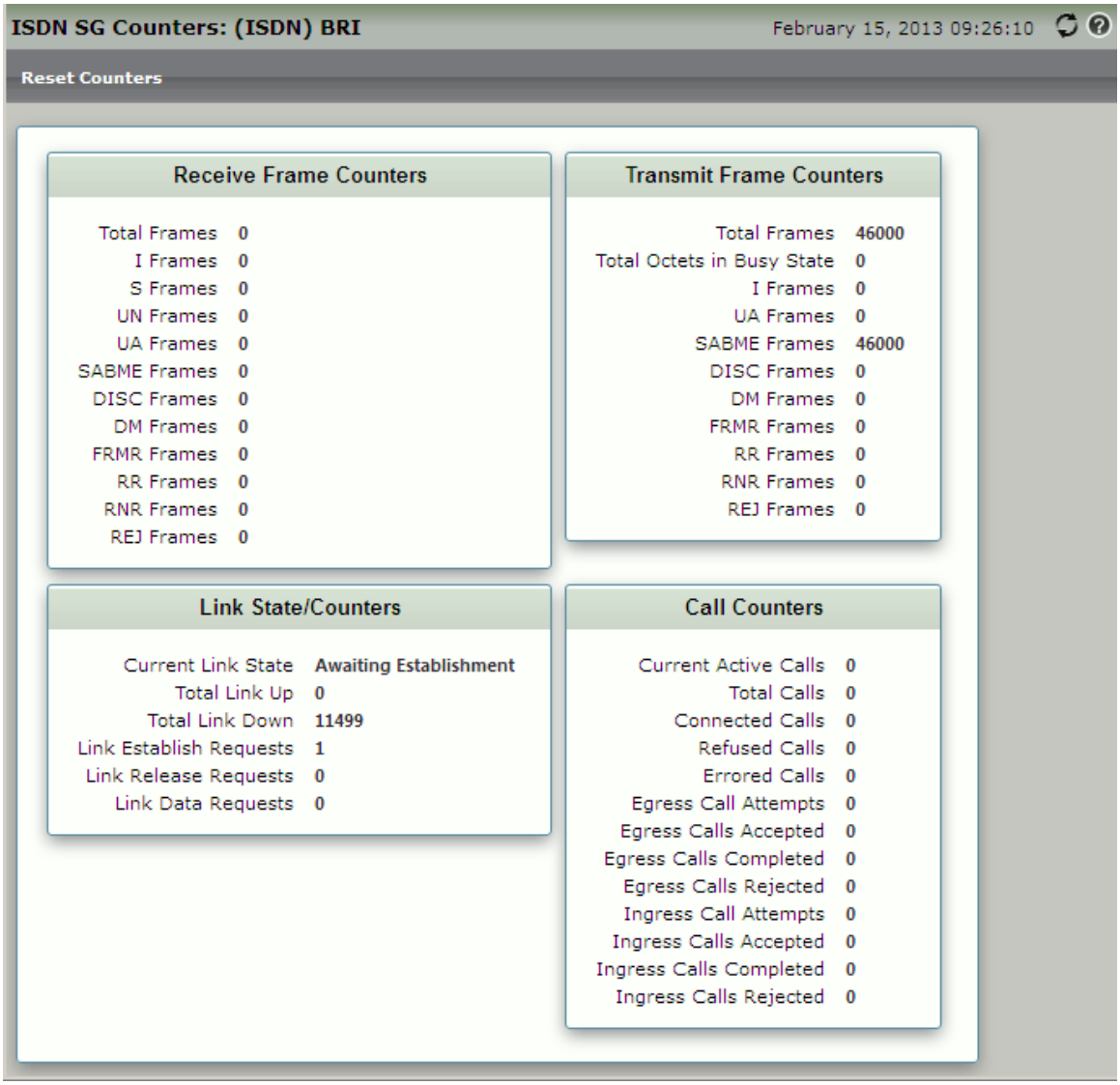
To view the ISDN counters:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. From the **Create Signaling Group** drop down box, select **ISDN Signaling Group.**



4. Click the **Counters** text next to the BRI Signaling Group in which you are interested.

Copyright © 2015 Sonus Networks. All rights reserved.



Receive Octet/Frame Counters

This group of counters displays the number of Q.921 Layer 2 ISDN frames received. For more information about this topic, see the ITU Q.921 Recommendation.

Link State/Counters

The Link State/Counters display the Current State of Q921 and the number of times the link has gone up/down.

Transmit Octet/Frame Counters

This group of counters displays the number of Q.921 Layer 2 ISDN frames transmitted. For more information about this topic, see the ITU Q.921 Recommendation.

Call Counters

- **Current Active Calls:** Number of con-concurrent calls, both Inbound and Outbound, incremented on the start of Client/Server CallSession transactions.
- **Total Calls:** Total Number of completed and attempted calls. Incremented on the start of Client/Server

Copyright © 2015 Sonus Networks. All rights reserved.

CallSession transaction.;

- **Connected Calls:** Number of Accepted calls, usually incremented by receiving 200OK Response message.
- **Refused Calls:** Number of calls that were not accepted by Sonus SBC 1000/2000, incremented on receiving Response codes greater than 400 and CCNak.
- **Errored Calls:** Number of calls that resulted in an error, incremented on unexpected conditions that result in the call state to change to CallStateTerminated.
- **Blocked Calls:** This has not been defined yet.
- **Egress Call Attempts:** Number of outbound call attempts, incremented on start of Client transaction by UAC on Sonus SBC 1000/2000.
- **Egress Calls Accepted:** Number of outbound calls accepted, incremented on 200OK from UAS.
- **Egress Calls Completed:** Number of outbound calls completed, incremented on transaction state change to completed.
- **Egress Calls Rejected:** Number of outbound calls that were not accepted by Sonus SBC 1000/2000, incremented on receiving Response codes greater than 400 and CCNak.
- **Ingress Call Attempts:** Number of inbound calls accepted, incremented on start of Server transaction by UAS on Sonus SBC 1000/2000.
- **Ingress Calls Accepted:** Number of inbound calls accepted, incremented on 200OK from UAC.
- **Ingress Calls Completed:** Number of inbound calls completed, incremented on transaction state change to completed.

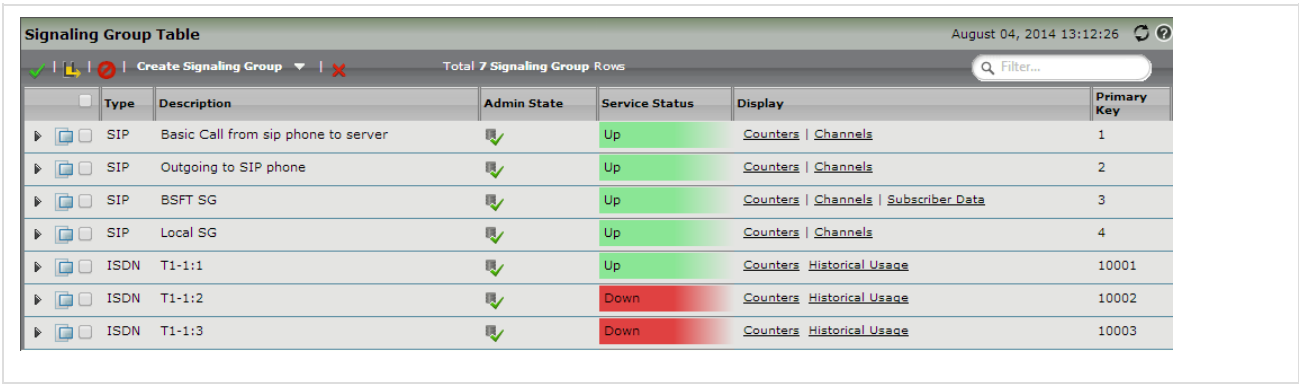
Viewing ISDN T1 - E1 Counters

The ISDN counters allow you to see the communications statistics for an ISDN Signaling Group.

Viewing ISDN Counters

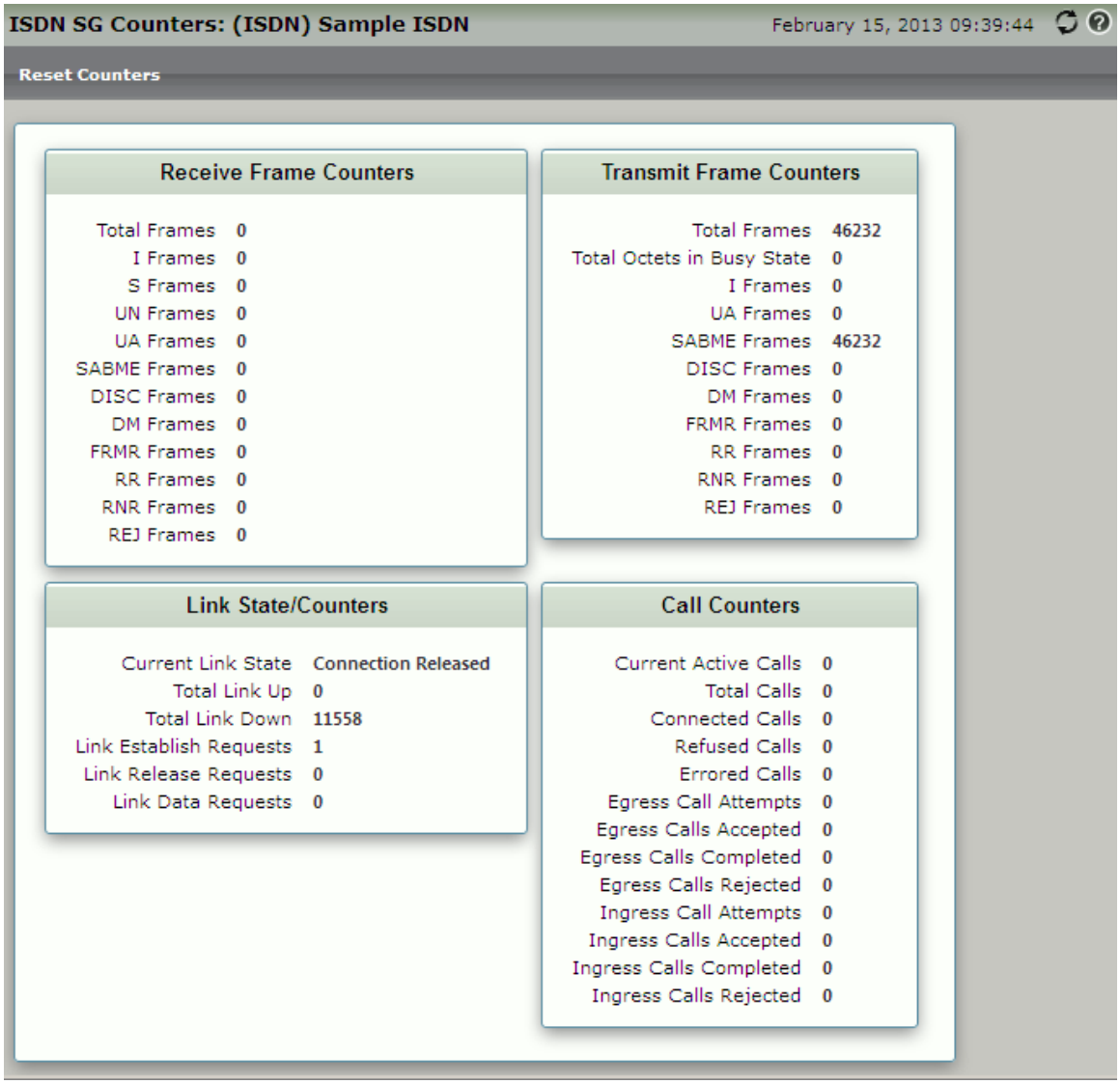
To view the ISDN counters:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. From the **Create Signaling Group** drop down box, select **ISDN Signaling Group.**



4. Click the **Counters** text next to the ISDN Signaling Group in which you are interested.

Copyright © 2015 Sonus Networks. All rights reserved.



Receive Octet/Frame Counters

This group of counters displays the number of Q.921 Layer 2 ISDN frames received. For more information about this topic, see the ITU Q.921 Recommendation.

Link State/Counters

The Link State/Counters display the Current State of Q921 and the number of times the link has gone up/down.

Transmit Octet/Frame Counters

This group of counters displays the number of Q.921 Layer 2 ISDN frames transmitted. For more information about this topic, see the ITU Q.921 Recommendation.

Call Counters

- **Current Active Calls:** Number of con-concurrent calls, both Inbound and Outbound, incremented on the start of Client/Server CallSession transactions.
- **Total Calls:** Total Number of completed and attempted calls. Incremented on the start of Client/Server

Copyright © 2015 Sonus Networks. All rights reserved.

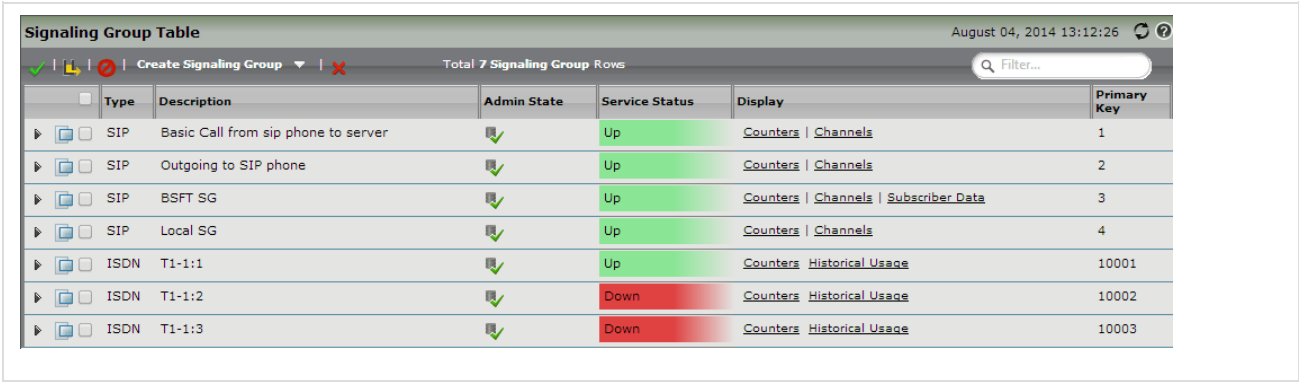
CallSession transaction.;

- **Connected Calls:** Number of Accepted calls, usually incremented by receiving 200OK Response message.
- **Refused Calls:** Number of calls that were not accepted by Sonus SBC 1000/2000, incremented on receiving Response codes greater than 400 and CCNak.
- **Errored Calls:** Number of calls that resulted in an error, incremented on unexpected conditions that result in the call state to change to CallStateTerminated.
- **Blocked Calls:** This has not been defined yet.
- **Egress Call Attempts:** Number of outbound call attempts, incremented on start of Client transaction by UAC on Sonus SBC 1000/2000.
- **Egress Calls Accepted:** Number of outbound calls accepted, incremented on 200OK from UAS.
- **Egress Calls Completed:** Number of outbound calls completed, incremented on transaction state change to completed.
- **Egress Calls Rejected:** Number of outbound calls that were not accepted by Sonus SBC 1000/2000, incremented on receiving Response codes greater than 400 and CCNak.
- **Ingress Call Attempts:** Number of inbound calls accepted, incremented on start of Server transaction by UAS on Sonus SBC 1000/2000.
- **Ingress Calls Accepted:** Number of inbound calls accepted, incremented on 200OK from UAC.
- **Ingress Calls Completed:** Number of inbound calls completed, incremented on transaction state change to completed.

Creating and Modifying ISDN Signaling Groups

To create or modify an existing ISDN Signaling Group:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. From the **Create Signaling Group** drop down box, select **ISDN Signaling Group.**



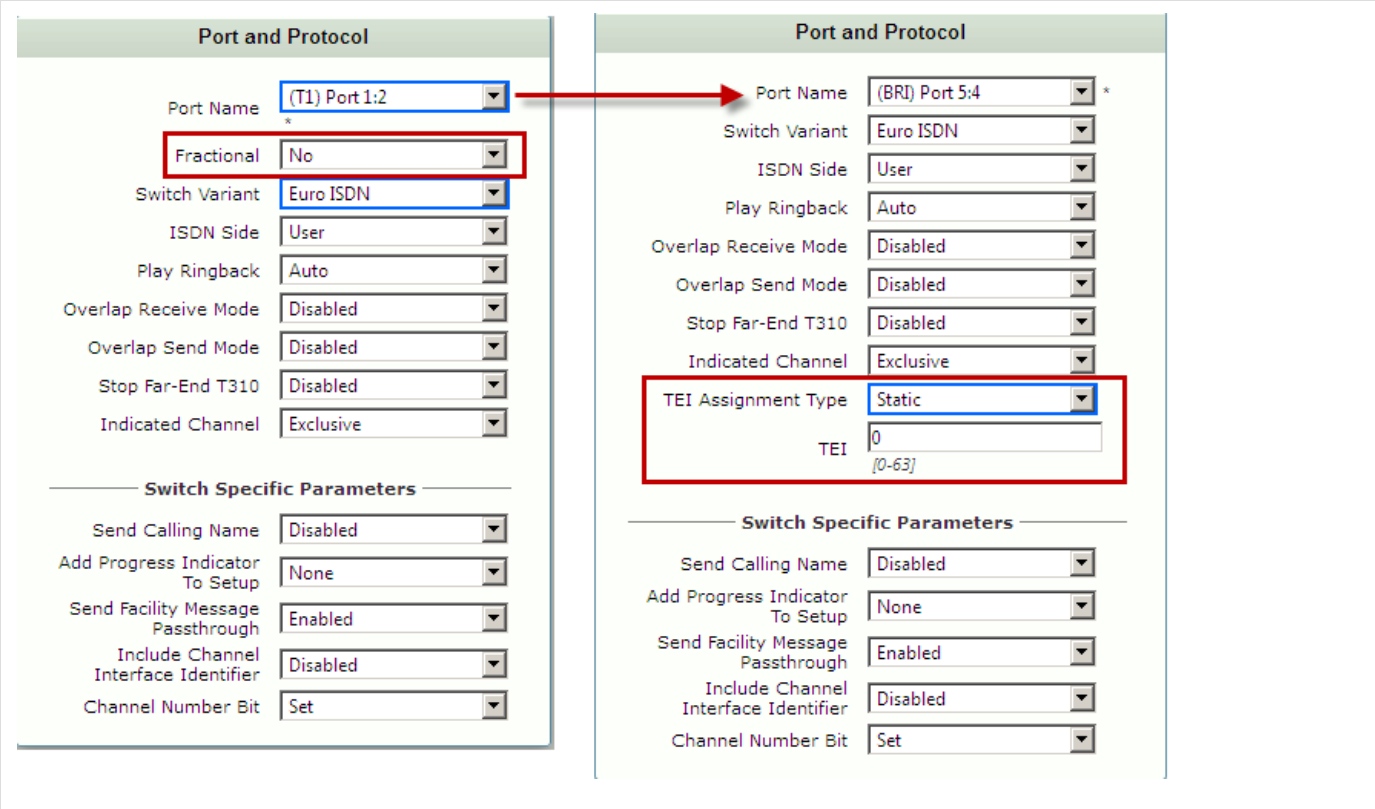
Modifying an ISDN Signaling Group

1. Click the **expand** (▸) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Copyright © 2015 Sonus Networks. All rights reserved.

BRI vs. PRI(T1) Ports

There is a subtle but very important difference in the UI between ISDN/BRI Signaling Groups and ISDN/PRI Signaling Groups. These differences appear in the Port and Protocol panels.



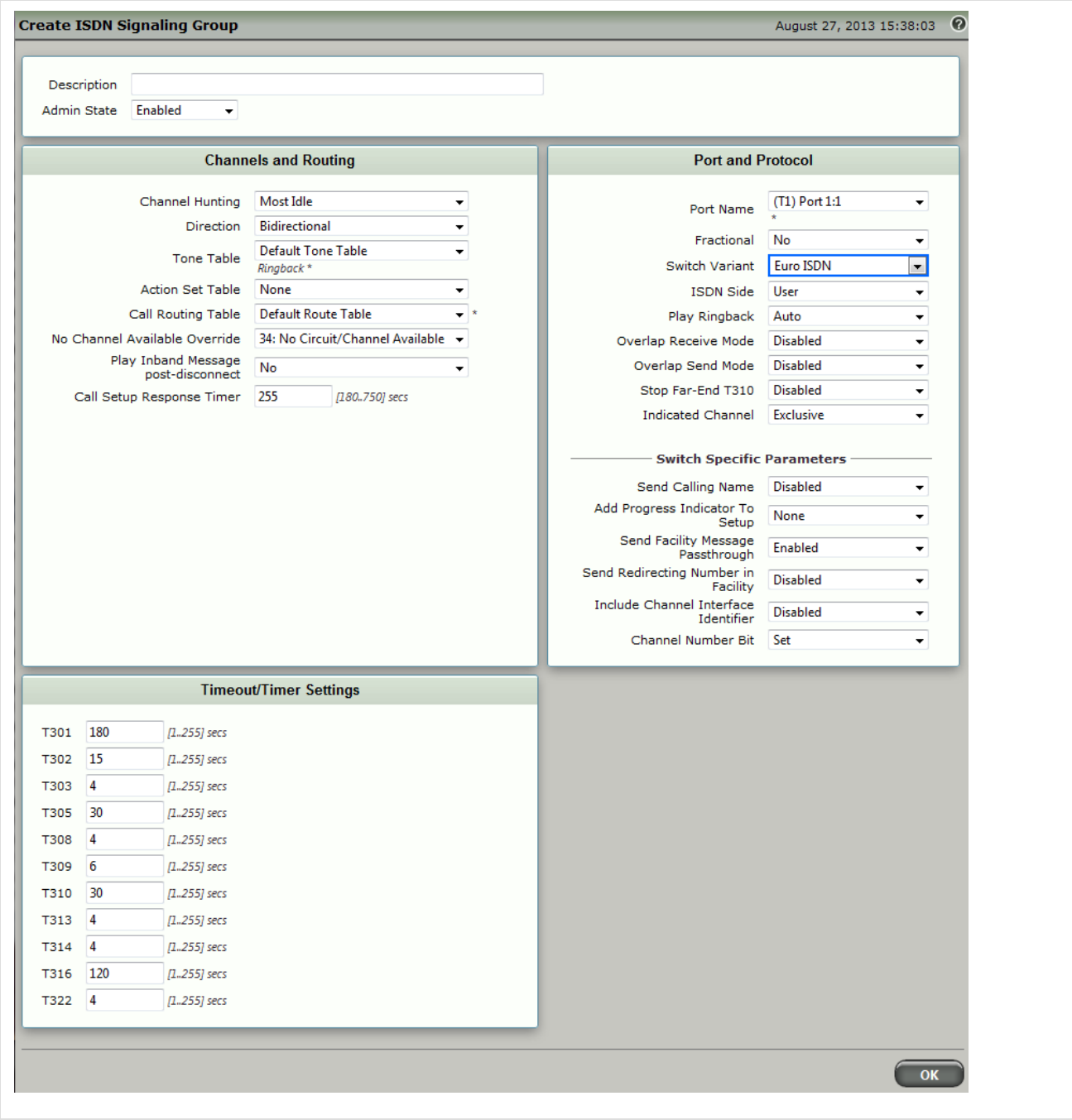
Configuration Field	PRI (T1)	BRI
Fractional	✅	❌
TEI Assignment	❌	✅
TEI	❌	✅

Creating an ISDN Signaling Group

To create an ISDN Signaling Group:

1. From the **Create Signaling Group** drop down box at the top of the Signaling Group Table, select **ISDN Signaling Group.**

Copyright © 2015 Sonus Networks. All rights reserved.



ISDN Signaling Group - Field Definitions

Specifies the admin state of the Signaling group.

- **Enable:** Enables the signaling group.
- **Disable:** Disables the signaling group.
- **Drain:** When Drain is selected, calls that are currently up remain connected. However, new calls and forking are not allowed for the Signaling Group. This allows all the calls to be drained from the SG.

Port and Protocol - Field Definitions

Port Name

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the physical T1/E1 port used for this Signaling Group.

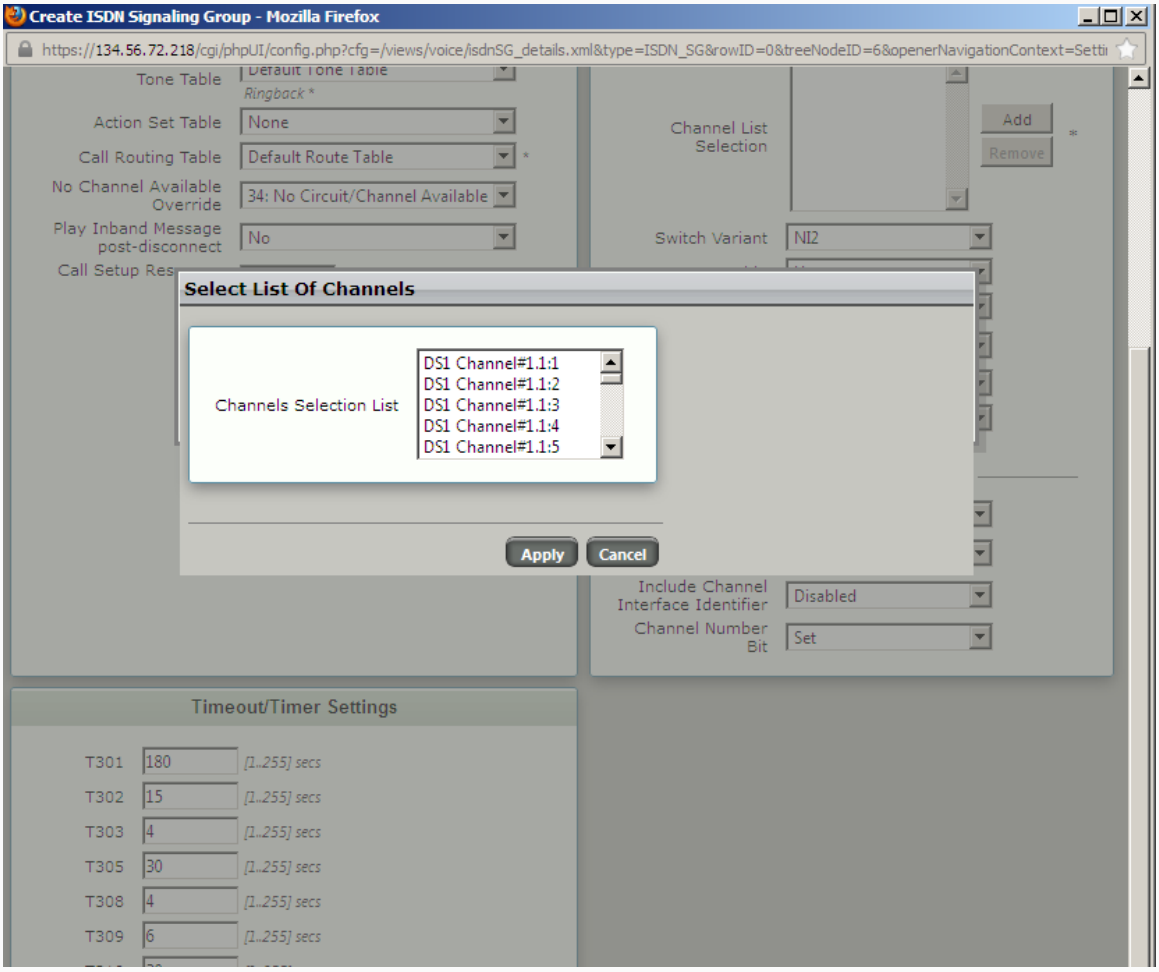
Fractional

Specifies whether or not the port is fractional. If selected, you must add a list of channels

Channel list Selection

Specifies to which channels the Signaling Group is applied if the port is fractional

Click here to see how the channel list is configured



Switch Variant

Specifies the ISDN variant for this signaling group.

ISDN Side

Specifies the ISDN user/network side for this signaling group .

Play Ringback

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies when to generate local ring back

- **Auto:** Depends if inband audio is available
- **Always:** Always generate inband ringback
- **Never:** Never generate inband ringback

Service Msg Capability

Specifies if service messaging is used on the signaling group. Only valid for ATT 4ESS, ATT 5ESS, NI2 and INS Sonus 1500 Switch Variants.

Overlap Receive Mode

Specifies if received overlap dialing is enabled on the signaling group. Only valid for Euro ISDN (ETSI) and QSIG Switch Variants.

Overlap Send Mode

Specifies whether or not overlap sending is enabled. Overlap sending is not executed if an ActionSet is configured for the inbound Signaling Group of if **Fork Call** is set to **Yes** in the call route. Only valid when QSIG or Euro ISDN are selected in the Switch Variant list box.

Stop Far-End T310

Specifies whether or not a Q.931 PROGRESS message is sent to the far-end so that it does not timeout (T310) while the SIP response is pending from the SIP leg, causing the call to release.

This setting should be enabled when Deploying the SBC 1000-2000 and Lync with a PSTN Provider. Only disable this parameter if your PSTN environment does not support PROGRESS sent before ALERT.

Indicated Channel

Specifies the ISDN Q931 Channel Identification attribute, telling the far end whether the channel identification selected in the Sonus SBC 1000/2000 setup message to the far end is *fixed* or *suggested*.

⚠ Always use **Exclusive** unless it is not supported by the peer switch.

TEI Assignment Type

Specifies the way the Terminal Equipment Identifier (TEI) is assigned by the Sonus SBC 1000/2000. The TEI is a numbering mechanism used by the network termination (NT) side to distinguish between more than one terminal equipment (TE) devices to which it is physically connected.

TEI

Specifies the TEI to assign for BRI when set to user side. 0 through 63 are absolute values to assign. If signaling group is PRI or network side BRI this parameter is not used. This field is available only when the TEI Assignment Type is set to Static.

⚠ The value of 0 for Static TEI is valid only for NTT. Other BRI specifications allow a value of 0 through 63 for Static TEI.

Copyright © 2015 Sonus Networks. All rights reserved.

Send Calling Name

Specifies whether or not the Q.931 SETUP message is sent to the far-end should include the DISPLAY Information Element (IE).
Available only when **ISDN Side** is set to User and the **Switch Variant** is set to NI2 or Euro-ISDN.

If this option is enabled, the DISPLAY IE is populated for NI2 or Euro-ISDN switch types, otherwise the DISPLAY IE is not populated for these switch types.

In general, the DISPLAY IE is populated according to ISDN communication standards. The NI2 and Euro-ISDN specifications state that the DISPLAY IE should not be populated. This option allows you to override that configuration for your environment.

Add Progress Indicator to Setup

This configuration option enables the ISDN Signaling Group to add/configure a Progress IE to the outbound SETUP message if it is not present. Options are as follows:

- **None** (a Progress IE is not added if there is none present, and not modified if present)
- **Not end to end ISDN** (call is not end to end ISDN)
- **Destination not ISDN** (destination address is not ISDN)
- **Origination not ISDN** (originiation address is not ISDN)
- **Return to ISDN** (call has returned to the ISDN)
- **Interworking Encountered** (interworking has been encountered)
- **Inband Information** (in-band information or appropriate pattern now available)
- **Delay Encountered** (delay in response at destination interface)

Default entry: **None**.

Include Channel Interface Identifier

Specifies whether to include the Interface Identifier in the Channel Identification Information Element.

Send Facility Message Passthrough

Specifies whether the Signaling Group transmits a Facility message passed through from another ISDN Signaling Group. This field is available only when Euro ISDN or QSIG are selected as a Switch Variant.

Send Redirecting Number in Facility

Controls whether the redirecting number is sent in the Facility IE for EuroISDN (ETSI). This configuration also uses the following ASN.1 hard coded fields which are hidden for EuroISDN:

- **ASN.1** Protocol Identifier (set as default **ROSE**)
- **ASN.1** Numbering Space (set as default **Local**)

Valid entries: **Enabled** (sends the Redirecting number in Facility IE) or **Disabled** (default; does not send Redirecting number in Facility IE). This field is available only when EuroISDN is selected as the Switch Variant. All ETSI specific ISDN Signaling groups must be configured the same system-wide for this field.

ASN.1 Protocol Identifier

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the Protocol Identifier to use within ASN.1 for QSIG. All QSIG specific ISDN Signaling groups must be configured the same system-wide for this field.

ASN.1 Numbering Space

Specifies the ASN.1 numbering space for QSIG. All QSIG specific ISDN Signaling groups must be configured the same system-wide for this field.

Include NFE and IA PDU

Specifies whether or not to include the Network Facility Extension and Interpretation APDU in ASN.1 for QSIG. All QSIG specific ISDN Signaling groups must be configured the same system-wide for this field.

Channels and Routing - Field Definitions

Channel Hunting

Method that Call Control uses to allocate ISDN channels. This is only valid for Outbound or Bidirectional Direction settings.

- **Standard:** This option assigns the first available low numbered channel.
- **Reverse Standard:** This option assigns the last available high numbered channel.
- **Round Robin:** This option assigns channels based on next available from low numbered to high numbered.
- **Least Idle:** This option chooses channels based on the least idle channel.
- **Most Idle:** This option chooses channels based on the most idle channel.

Direction

Indicates the direction of calls supported

- **Inbound:** Support only incoming calls from ISDN endpoints.
- **Outbound:** Support only outgoing call to ISDN endpoints.
- **Bidirectional:** Support both incoming or outgoing calls to ISDN endpoints.

Tone Table

Specifies the Tone Table to use on this signaling group. This option is only available when Inbound or Bidirectional are specified for Direction.

Action Set Table

Specifies the Action Set Table to use on this signaling group. This option is only available for Inbound and Bidirectional.

Call Routing Table

Specifies the Call Route Table to use on the signaling group to route calls with. This option is only available when Inbound or Bidirectional are specified for Direction.

No channel Available Override

Copyright © 2015 Sonus Networks. All rights reserved.

In the event of a "No Channel/Circuit available" release cause code, the specified cause code will be sent to the relevant protocol module. For more information see the list of Cause Codes.

Play Inband Message post-disconnect

Enables an inband message to be played when a Progress Indicator is provided on the ISDN disconnect message. Valid entries: Yes (inband message is played post-disconnect) or No (inband message is not played).

Maximum Message Play Time

This parameter defines the timeout value for the inband message play time (when Play Inband Message post-disconnect is configured as **Yes**). Valid range: **1 - 300** seconds. Default value: **10** Seconds. This field is displayed only when Play Inband Message post-disconnect is set to **Yes**.

Call Setup Response Timer

Specifies the interval of time, in seconds, after an call is initiated that the Sonus SBC 1000/2000 waits for a call to connect before terminating the incoming call.

Timeout/Timer Settings - Timer Definitions

Timer	Timer Definition
T301	Started when an ISDN call enters the alerting state (i.e.receive an ALERT message) and if it expires clears the call. Prevents the call from ringing forever.
T302	Specifies the time between digits in overlapped dialing. If it expires it is assumed all digits have been received.
T303	Specifies the time after sending a ISDN SETUP message to wait for a response. First expiration will resend the SETUP and second expiration will fail the call.
T305	Specifies the time to wait after sending an ISDN DISCONNECT message to wait for the RELEASE message response. If it expires we then send an ISDN RELEASE message.
T308	Specifies the time to wait after sending an ISDN RELEASE message to wait for the RELEASE COMPLETE message response. First expiration will resend the RELEASE message and second expiration will send a RELEASE COMPLETE message.
T309	Specifies the time to wait after the D channel goes down for B channels with calls in the active state to wait for the D channel to come back up. If it expires and the D channel has not come back up the call on the B channel is cleared.
T310	Specifies the time to wait after receiving a CALL PROCEEDING message to wait for some form of call progress, i.e. a PROGRESS, ALERT or CONNECT message. If it expires the call is cleared.
T313	Specifies the time for user side ISDN to wait after sending a CONNECT message to wait for the CONNECT ACKNOWLEDGE message. If it expires then the call is cleared.
T314	Specifies the time to wait between SEGMENT messages for segmented message support in QSIG. If it expires all previously received SEGMENT messages are discarded and ignored.

Copyright © 2015 Sonus Networks. All rights reserved.

T316	Specifies the time to wait after sending a RESTART message to wait for the RESTART ACKNOWLEDGE. First expiration will resend the RESTART message and second expiration will put the channel in local maintenance state for protocols that support service messaging. For protocols that don't support service messaging channel will be returned to the idle state.
T322	Specifies the time to wait after sending a STATUS ENQUIRY message to get the STATUS message response. First expiration will resent the STATUS ENQUIRY message and second expiration will clear an active call. Only started if T309 doesn't expire and the D channel comes back up before T309 expires on B channels with active calls.
T3M1(T323)	Specifies the time to wait after sending a SERVICE message to get the SERVICE ACKNOWLEDGE response. If it expires the SERVICE message will be resent. For NI-2 this is a maximum of 3 attempts before leaving the B channel in the state it was before and not changing its state.

Working with SCOM

The Sonus SBC 1000/2000 SCOM Management Pack allows customers in a Microsoft Server Environment to monitor the health of their Sonus SBC 1000/2000 systems using SCOM.

This page guides you through the import and installation procedure of the **Sonus SCOM** Management Pack onto the Microsoft System Center Operations Manager 2007 R2 tool.

- Downloading the Sonus SCOM Management Pack
- Importing the Management Pack into SCOM 2007
- Installing the Management Pack
- Importing the Management Pack into SCOM 2012
- Verify the Installation
- Troubleshooting

Downloading the Sonus SCOM Management Pack

The Sonus SCOM management pack is available for download from the Sonus SBC 1000-2000 Download Center.

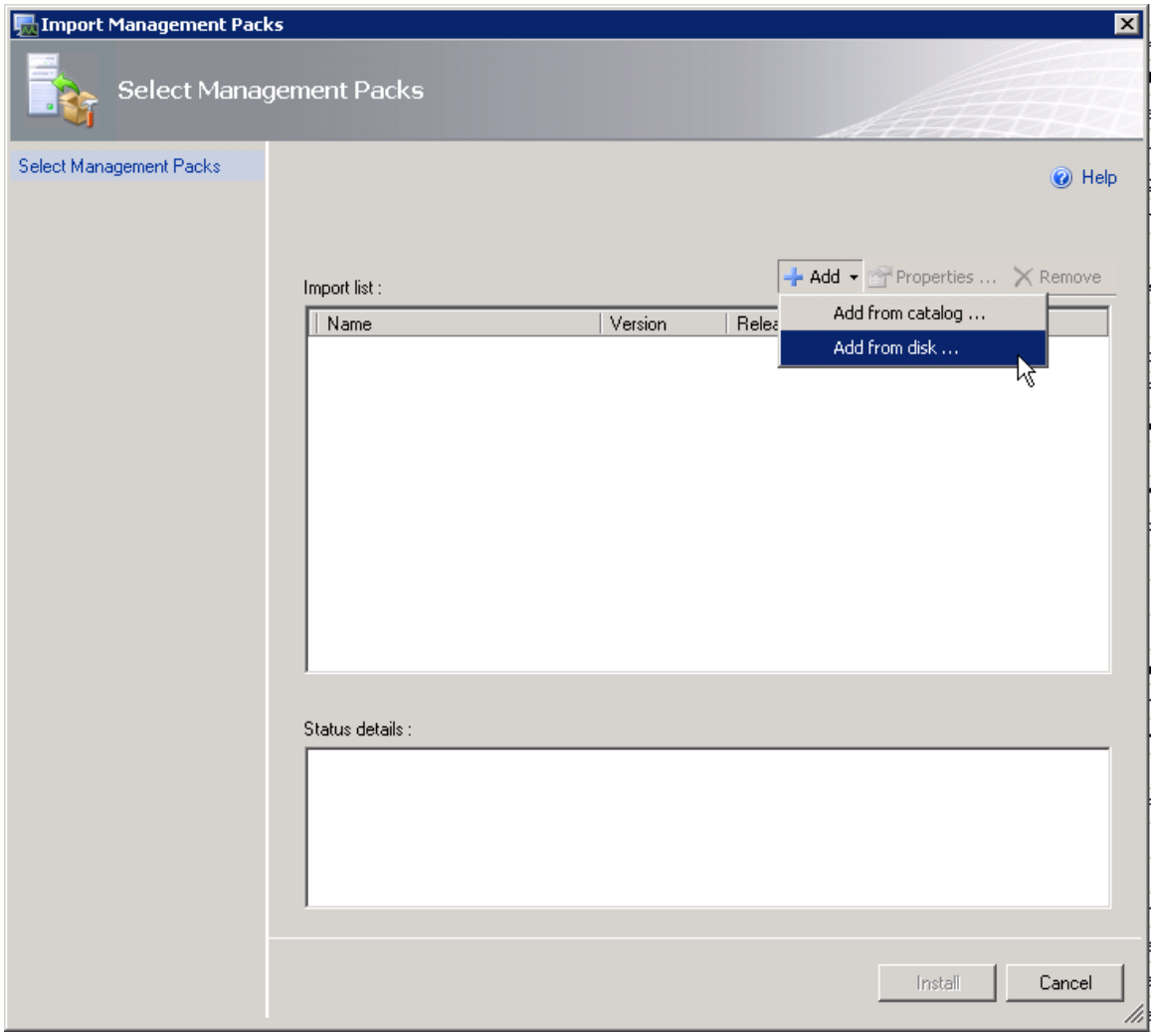
1. From the Sonus SBC 1000-2000 Download Center
   a. For SCOM 2007, download the `SBC1K2K_SCOM.MP` file
   b. For SCOM 2012, download the `SBC1K2K_SCOM.MPB` file
2. Save the Management Pack file in a convenient location on the the SCOM host machine

> ⚠ Ensure that you import the `SBC1K2K_SCOM.MP` into SCOM 2007 and `SBC1K2K_SCOM.MPB` into SCOM 2012. If the SCOM 2007 Management Pack file is imported into SCOM 2012, the import will not return meaningful errors, but the discovery will fail.

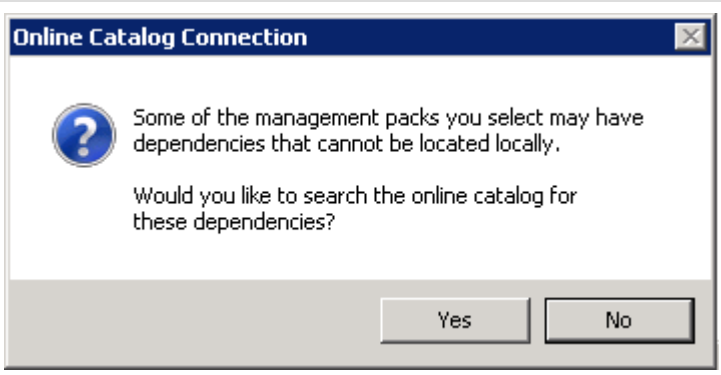
Importing the Management Pack into SCOM 2007

1. Launch the System Center Operations Manager.
2. Go to Administration.
3. In the navigation tree, go to **Management Packs > Import Management Packs...**.

Copyright © 2015 Sonus Networks. All rights reserved.

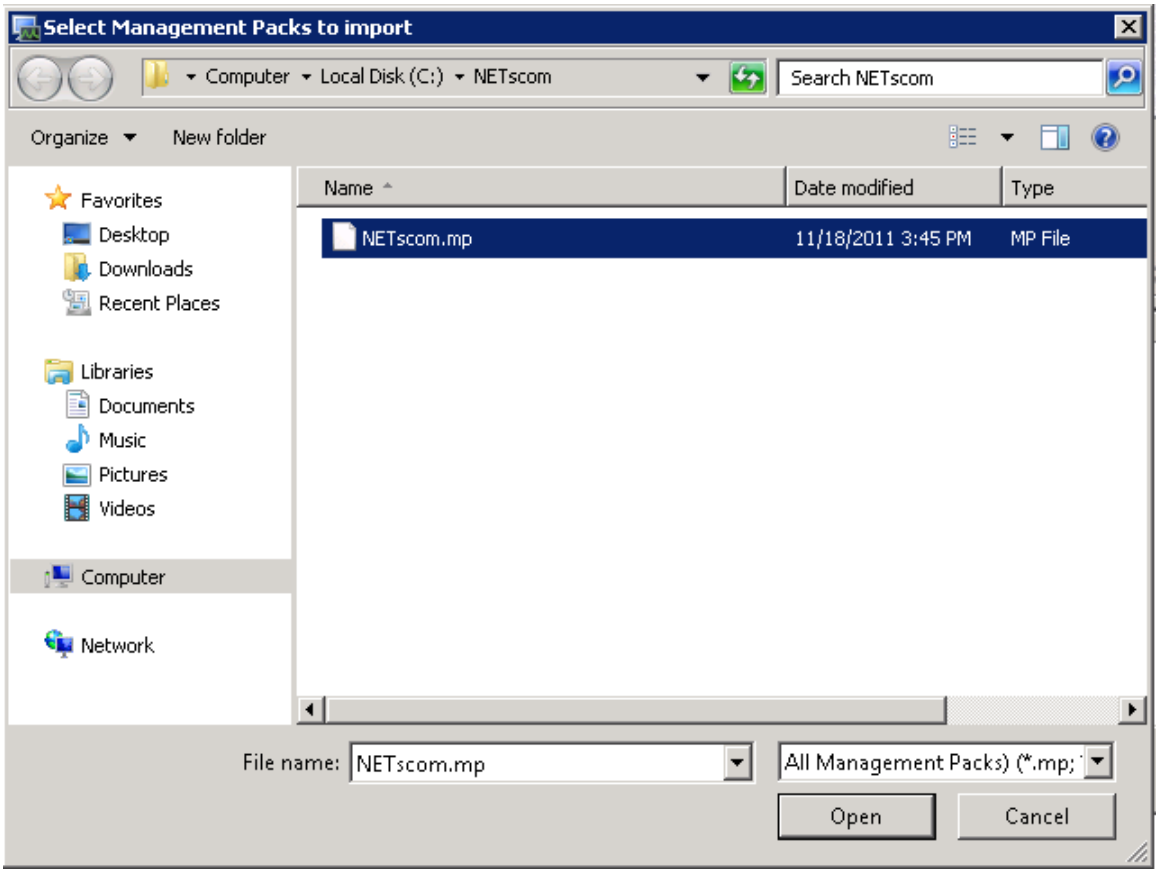


4. Click **Add**.
5. Select **Add from disk...**.



6. Click **Yes**in the Online Catalog Connection dialog.

Copyright © 2015 Sonus Networks. All rights reserved.

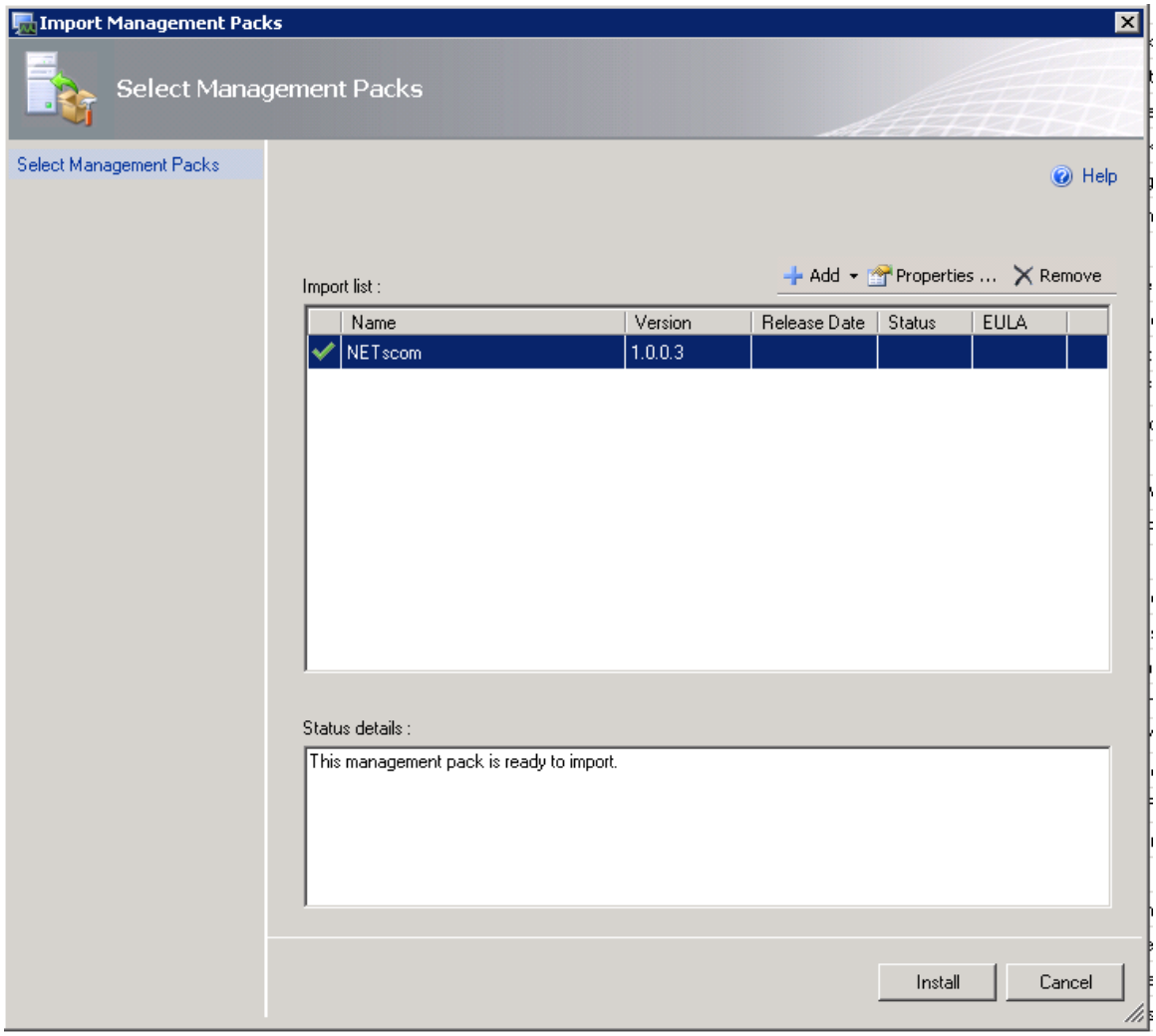


7. Click the file in the file list.
8. Click **Open**.

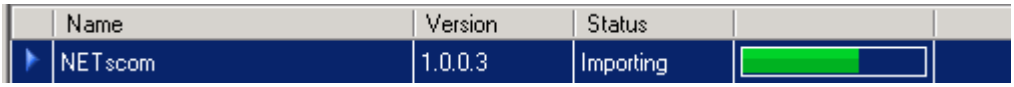
You are now ready to Install the Management Pack.

Installing the Management Pack

Copyright © 2015 Sonus Networks. All rights reserved.



1. In the Select Management Packs window, click **Install**.
   You will see the progress indicator scrolling as the file is installed.



2. When the installation process has finished, click **Close**.

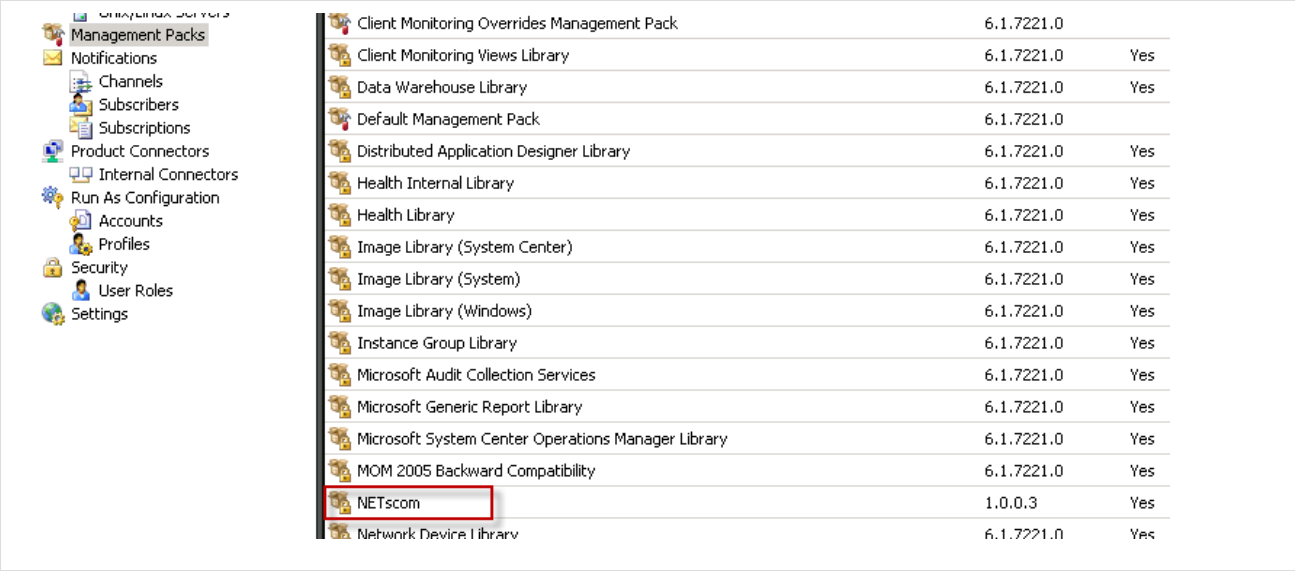
Importing the Management Pack into SCOM 2012

Include SCOM 2012 specific instructions!

Verify the Installation

1. Press **F5** on your keyboard to refresh the list.
2. Verify that the **Sonus SCOM** Management Pack appears in the list.

Copyright © 2015 Sonus Networks. All rights reserved.



Troubleshooting

SBC 1000 and SBC 2000 support SNMPv2c and the standard port 161 is used. The SCOM Management Pack (MP) is related to the discovery of the SBC by mapping the object identifiers (OID's) to various components in the SCOM object model. Once the Management Pack is downloaded and imported into SCOM, the SNMP management address has to be created in the SBC.

To troubleshoot issues, use a MIB browser tool to perform SNMP walks from the SCOM host computer. If the walks are working then there should not be a network connectivity issue and the issue can be narrowed down to SCOM configuration (e.g.: community) or an issue related to the MP import. If they are not working, then there would be a network issue, or a SBC target address configuration issue.

SBC SCOM Object Model and Health Monitoring

- SBC SCOM Health Monitors
  - SBC SCOM Monitors
  - Health States Associated with SBC SCOM Object Classes
- Object Model Overview
  - Supported Object Relationships
- SBC SCOM Object Classes
  - SCOM Object Class Diagram

SBC SCOM Health Monitors

SCOM classes define Health as a tri-state attribute: Error, Warning, and Healthy. A device is in Error state when it's not working correctly and requires attention, it's in Warning state when it appears to be working but a condition is detected that should be attended to, and it's Healthy otherwise.

SBC SCOM Monitors

A SCOM Monitor is a periodic poll that runs in order to determine health state. The SBC SCOM Management Pack

Copyright © 2015 Sonus Networks. All rights reserved.

will define monitors that poll the SBC for the following information:

- Highest Alarm State (not currently returned through SNMP)
- Operational Status for ports, DSPs, and power supplies.
- Administrative State for Ports

The results of this poll will be used to set the Health state of SBC classes as follows:

Health States Associated with SBC SCOM Object Classes

SBC SCOM Class	Error Criteria	Warning Criteria	Healthy Criteria	Notes
SBCSeries	Highest Alarm Severity is either Critical or Major. Where SLAs are present, these severities require immediate attention.	Highest Alarm Severity is Minor	Highest Alarm Severity is Warning or None	SBCSeries is an abstract class, these criteria apply to all inherited classes
SBCLineCard	The card has configured ports and is either not present or is operationally down.	Not used	The card either has no configured ports, or is operationally up.	SBCLineCard is an abstract class representing pluggable cards (e.g.: SBC2000 DS1), these criteria apply to all inherited classes. When administrative state support is provided for cards the error criteria will include the card being administratively up.
SBCModule	Not used	Not Used	This state always applies	SBCModule is an abstract class representing non-pluggable feature modules (e.g.: SBC1000 DS1). No service status information is supported for these modules.
SBCPort	The port is administratively up and operationally down	Not used	The port is either administratively down, or operationally up.	
SBCDSPCard	The DSP card is out of service	Not used	The DSP card is in service	DSP Service Status is added via SNMP in the Flute release.
SBCPowerSupply	The power supply is out of service	NOTE: Warning can be indicated based upon temp or voltage-out being out-of-spec.	The power supply is in service	Only applicable to SBC2000 with dual power supplies, otherwise the node will simply become SNMP-unreachable.

Copyright © 2015 Sonus Networks. All rights reserved.

SBCAdminPort	Not used	Not Used	Always	This is a recovery port , it is not mandatory to keep the cable plugged-in always in this port. Un-plugging the cable will make the port status down . This is a typical state in the customer location. So instead of showing the port down and alarming the operator , keep the port status healthy alway

Object Model Overview

Within SCOM object classes represent entities whose health state is monitored by SCOM and presented to the user. SBC SCOM object classes are defined for persistent objects in the system.

Supported Object Relationships

SCOM supports the following relationships:

- Inheritance: An inheritance relationship has the common object-oriented meaning.
- Hosting: A hosting relationship is one where an instance of the hosted class cannot exist without it's host, and where removing the host from the system causes the hosted objects to be removed.
- Containment: A containment relationship allows instances of the two classes to exist independently, but provides for health state roll-up.
- Reference: A reference relationship has the common object-oriented meaning. The only relationships that exist between SBC SCOM classes are Inheritance and Hosting.

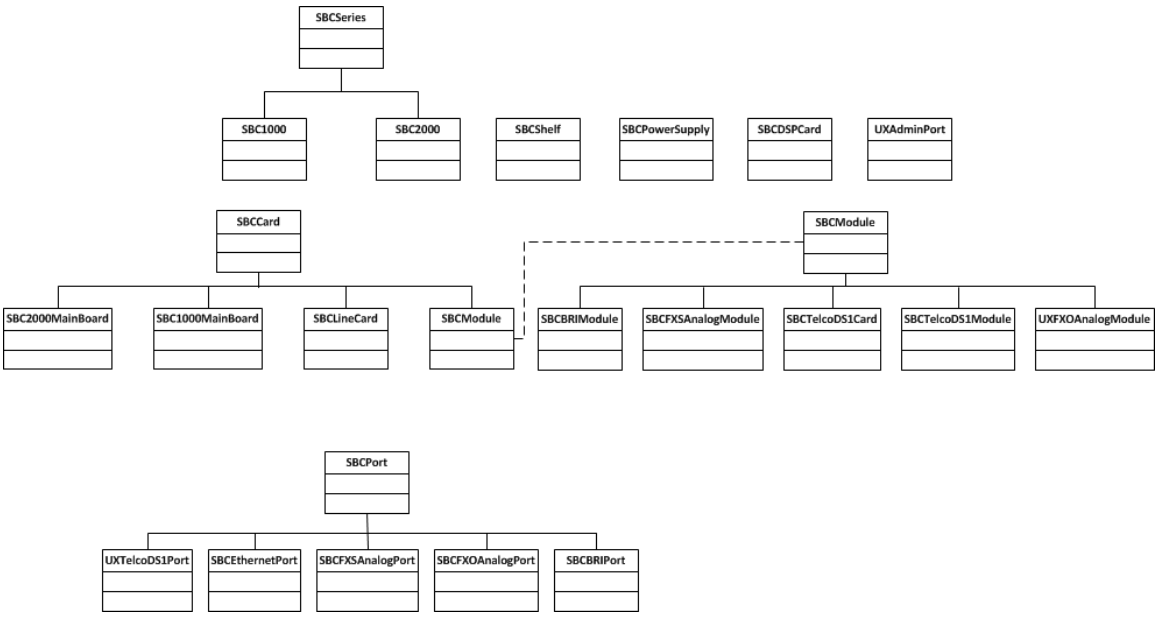
SBC SCOM Object Classes

- **SBCSeries:** This will be an abstract object class for all "SBC" network devices.
- **SBC2000:** This inherits from SBCSeries and represents a SBC2000 node. This is the "chassis" object for the SBC2000.
- **SBC1000:** This inherits from SBCSeries and represents a SBC1000 node. This is the "chassis" object for the SBC1000.
- **SBCShelf:** This object class is hosted by SBCSeries. There will be one instance for each SBC2000 and 1000, the 5000 will have multiple instances.
- **SBCCard:** This will be an abstract object class for cards and modules. It will be Hosted by SBCShelf.
- **SBCLineCard:** This will be an abstract object class for all user-pluggable SBC Cards. It will inherit from SBCCard.
- **SBCModule:** This will be an abstract object class for all non-pluggable SBC Cards. It will inherit from SBCCard.
- **SBC1000MainBoard:** This class represents a SBC1000 'main board', and inherits from SBCCard. It provides a container for all ports on the SBC1000.
- **SBC2000MainBoard:** This class represents a SBC2000 'main board', and inherits from SBCCard. It provides a container for non-SPI SBC2000 Ethernet Ports.
- **SBCTelcoDS1Card:** This inherits from SBCLineCard and represents a Telco DS1 line card.
- **SBCTelcoDS1Module:** This inherits from SBCModule and represents a Telco DS1 Module.
- **SBCFXSAnalogModule:** This inherits from SBCModule and represents a FXS Analog Module.
- **SBCFXOAnalogModule:** This inherits from SBCModule and represents a FXO Analog Module.
- **SBCBRIModule:** This inherits from SBCModule and represents a BRI Module.
- **SBCPort:** This is an abstract class and represents a SBC Series Port.
- **SBCTelcoDS1Port:** This class inherits from SBCPort and represents a Telco DS1 Port. It will be Hosted by SBCTelcoDS1Card and SBCTelcoDS1Module.
- **SBCEthernetPort:** This class inherits from SBCPort and represents an Ethernet port. It will be Hosted by SBC1000MainBoard and SBC2000MainBoard.

Copyright © 2015 Sonus Networks. All rights reserved.

- **SBCFXSAnalogPort:** This class inherits from SBCPort and represents an FXS analog port. It will be hosted by SBCFXSAnalogModule.
- **SBCFXOAnalogPort:** This class inherits from SBCPort and represents an FXO Analog Port. It will be hosted by SBCFXOAnalogModule.
- **SBCBRIPort:** This class inherits from SBCPort and represents a BRI port. It will be hosted by SBCBRIModule.
- **SBCPowerSupply:** This class represents a pluggable SBC Power Supply. It will be Hosted by SBCShelf. The SBC1000 does not have a SBCPowerSupply object because it's not pluggable.
- **SBCDSPCard:** This class represents a DSP. It will be Hosted by SBC1000MainBoard and SBC2000MainBoard.
- **SBCAdminPort:** This class represents the SBC2000 Admin port which is hosted by SBC2000MainBoard.

SCOM Object Class Diagram



Working with Enhanced 911 Devices

This page covers the use and configuration of the Sonus SBC 1000/2000 E911 Feature.

Configuring Emergency Services

Managing Callback Number Pools

- Creating and Modifying Callback Number Lists

Viewing Emergency Calls

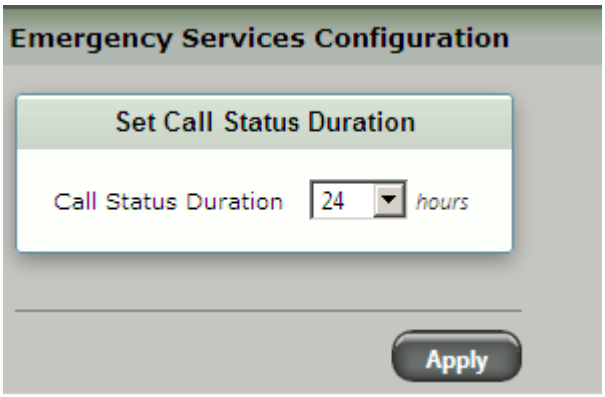
Configuring Emergency Services

The Emergency Services Configuration page contains a setting for specifying the duration of Call Status entries.

Configuring Call Status Duration

1. in the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Emergency Services > Configuration**.

Copyright © 2015 Sonus Networks. All rights reserved.



Set Call Status Duration - Field Definitions

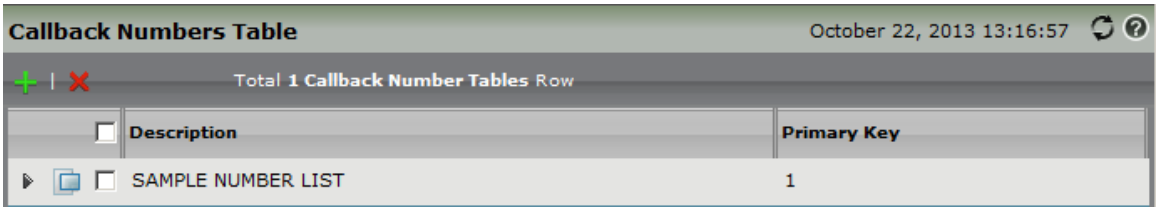
Call Status Duration

Specifies the duration of time, in hours, that a call remains in the Call Status Table.

Managing Callback Number Pools

Working with Callback Number Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Emergency Services > Callback Number Pool**.



To view a pool's content:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Callback Number Lists

Creating and Modifying Callback Number Lists

Callback number lists contain up to 16 numbers. These numbers replace the actual number of the calling party when the call is sent to the Emergency Services Operator (PSAP). If the PSAP operator calls back (to the callback number) the call is routed using a Transformation Table entry back to the original calling extension.

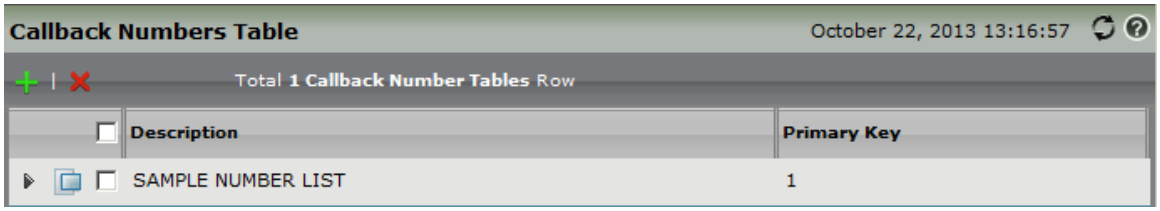
- See also: Working with Telephony Routing.
- See also: Managing Transformation Tables.

Copyright © 2015 Sonus Networks. All rights reserved.

- See also: Adding and Modifying Entries to Transformation Tables].

To create or modify Callback Number List:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Emergency Services > Callback Number Pool**.

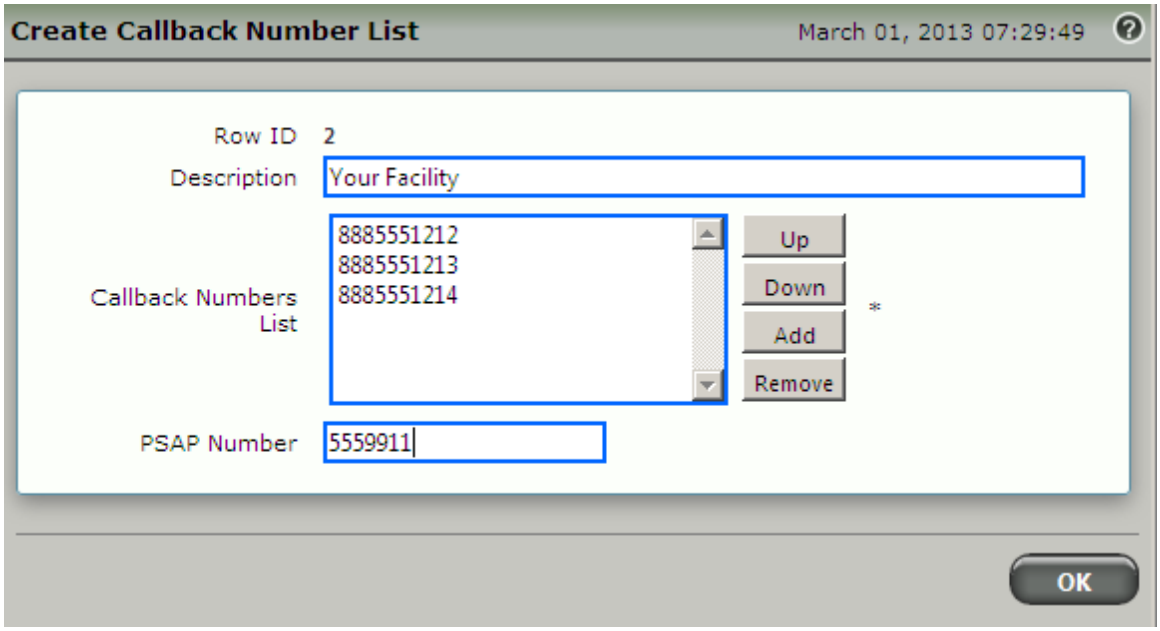


Modifying a Callback Number list

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a Callback Number List

1. Click the Create Callback Numbers List ( ) icon at the top of the Callback Numbers Table page.



Callback Number List - Field Definitions

Callback Numbers List

A list of numbers which are substituted in a Transformation for the actual number from which the call was initiated. These numbers are used in a round-robin scheme.

PSAP Number

Copyright © 2015 Sonus Networks. All rights reserved.

Use this field to specify the **Public Safety Answering Point** (PSAP) number. This is the number to which the call is connected when an extension calls 911. If no value is specified in this field, the call is connected to the local **911** facility.

Viewing Emergency Calls

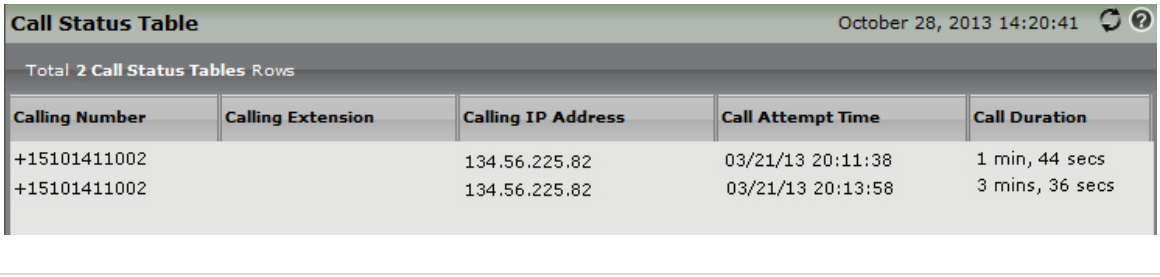
The Call Status Table allows you to see what calls have been made to 911 or a PSAP number. The Sonus SBC 1000/2000 maintains bindings between the Lync user extension and the ELIN number so that if there is a PSAP callback, the Sonus SBC 1000/2000 can route the call to the originating Lync Extension.

The Call Status Table displays information about the calling number/extension, the calling IP Address, when the call was placed and its duration. The information in the table is maintained for a period of time specified the Emergency Services Configuration page of the User Interface.

Viewing the Call Status Table

To view the Call Status Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Emergency Services > Call Status Table.**



Working with Dynamic Routing

Overview

Both the Sonus SBC 1000 and Sonus SBC 2000 support dynamic routing protocols such that the Sonus SBC 1000/2000 dynamically learns destinations routes and advertises those route to other routers. Sonus SBC 1000/2000 nodes enabled with dynamic routing learn the routes to all networks that are directly connected to the device. Sonus SBC 1000/2000 nodes also learns routes from other routers that run the same routing protocols for with the Sonus SBC 1000/2000 node is configured.

Following routing protocols are supported in release 2.2:

- RIPv2
- OSPF

Managing Router Instances

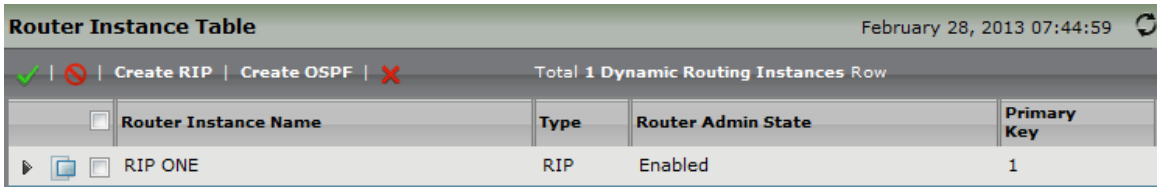
- Creating and Modifying OSPF Router Instances
- Creating and Modifying RIP Router Instances

Managing Router Instances

Copyright © 2015 Sonus Networks. All rights reserved.

Working with Router Instances

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Router Instances**.



To view a Router Instance's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

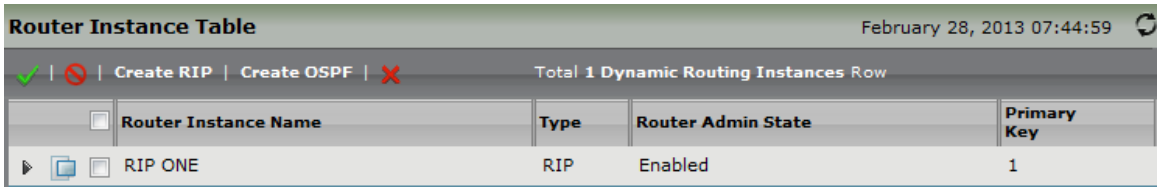
Creating and Modifying OSPF Router Instances

Creating and Modifying RIP Router Instances

Creating and Modifying OSPF Router Instances

To create or modify an existing OSPF Router Instance:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Router Instances**.



Modifying a OSPF Router Instance

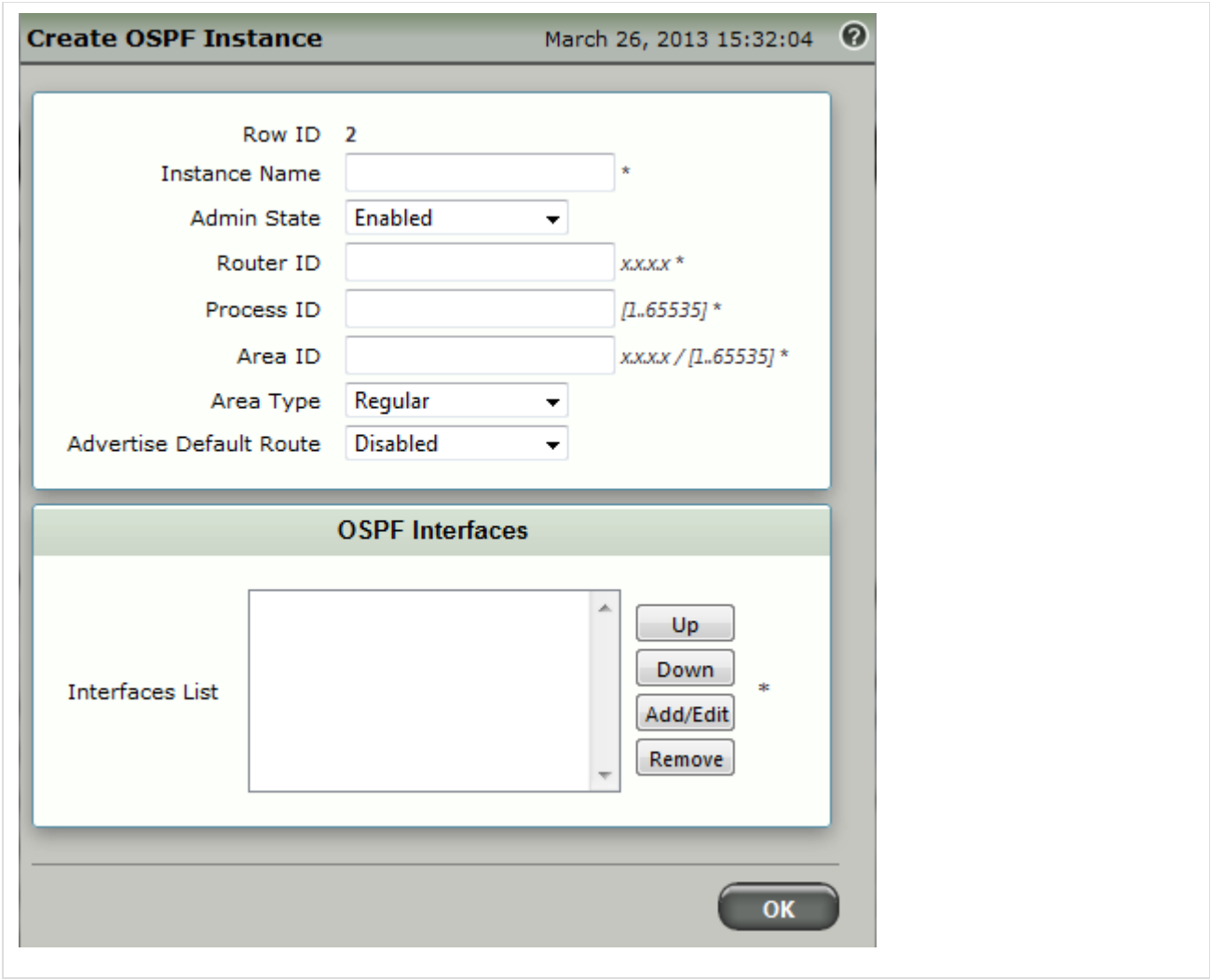
1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating an OSPF Router Instance

To create an OSPF router instance:

1. Click the **Create OSPF**link at the top of the Router Instance Table.

Copyright © 2015 Sonus Networks. All rights reserved.



OSPF Instance - Field Definitions

OSPF Router Instance Name

Specifies a name for this OSPF router instance.

Router ID

Specifies a router ID in either dotted decimal or decimal format.

Admin State

Specifies the administrative state of the instance.

Process ID

Specifies a process ID for this router instance.

Area ID

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies a numeric identifier for the OSPF area associated with this instance. The ID is specified in either dotted decimal or plain decimal format.

Area Type

Specifies the OSPF Area created for this router instance.

Advertise Default Route

Specifies whether or not default information originate is enabled or disabled.

OSPF Interfaces Panel - Field Definitions

Interfaces List

Specifies the interfaces on which the OSPF router instance appears.

Helpful Hint

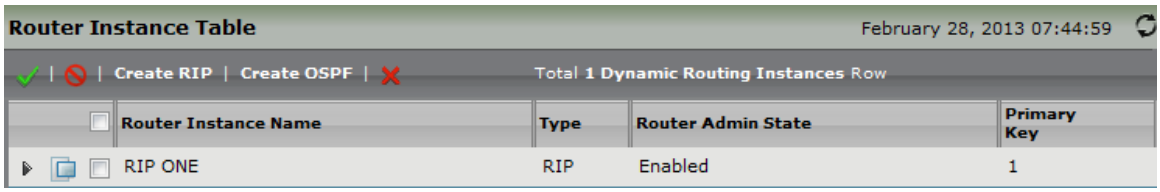
This field presents a multi-select widget when the **Add/Edit** button is clicked.
Click here for more information about using the Multi-select widget.

Creating and Modifying RIP Router Instances

The Sonus SBC 1000/2000 permits only ONE RIP router instance.

To create or modify an existing RIP Router Instance:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Router Instances**.



Modifying a RIP Router Instance

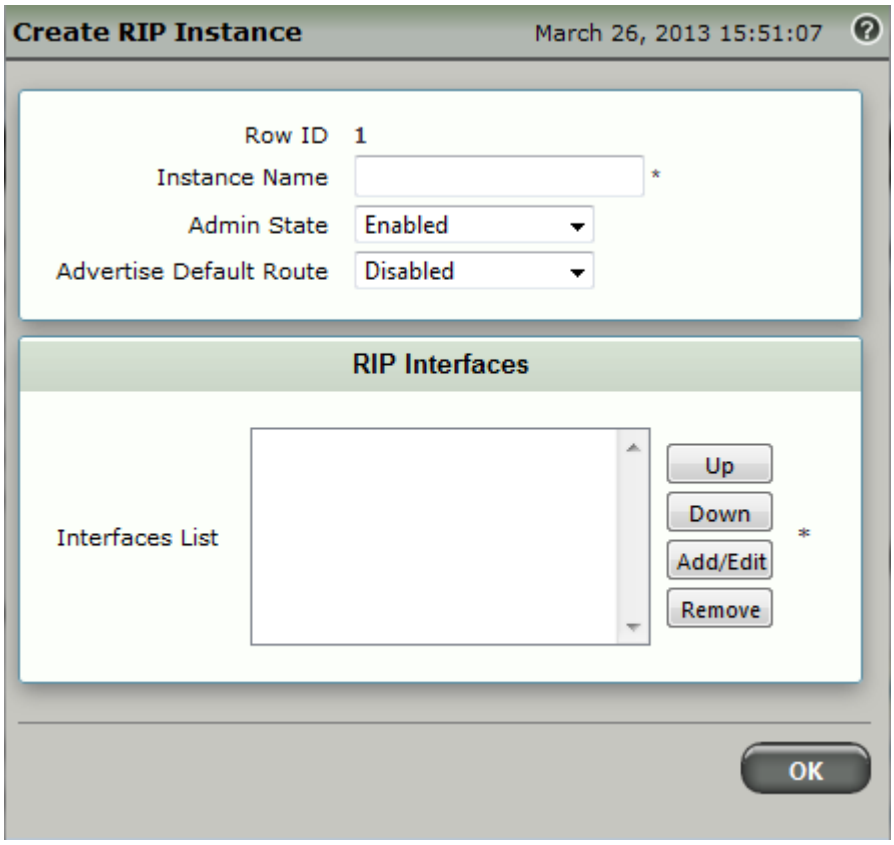
1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a RIP Router Instance

To create a RIP Router:

1. Click the **Create RIP**link at the top of the Router Instance Table.

Copyright © 2015 Sonus Networks. All rights reserved.



Instance General Field Definitions

RIP Instance Name

Specifies the name of the RIP Instance. Maximum length of 16 characters.

RIP Admin State

Specifies the administrative state of the router instance.

Default Info Originate

If enabled, generates a default route into the Routing Information Protocol (RIP).

RIP Interfaces - Field Definitions

Interfaces List

Specifies the logical interface to which the router is connected.

Helpful Hint

This field presents a multi-select widget when the **Add/Edit** button is clicked.
Click here for more information about using the Multi-select widget.

Copyright © 2015 Sonus Networks. All rights reserved.

Working with Access Control Lists and Session Control

Managing Access Control Lists

- Creating and Modifying Rules in Access Control Lists

See also: Configuring the ASM Firewall under the Managing the ASM section of this documentation.

Managing Access Control Lists

About ACLs

Access Controls List (ACL) filter the type of traffic that is allowed or denied access to the network or portion of the network. ACLs act as packet filters based on the criteria defined in the access list. ACLs defined on the Sonus SBC 1000/2000 do not take effect until they are applied to a port.

- Access Lists can filter incoming or outgoing packets on an interface, thereby controlling access based on source addresses, destination addresses, source layer4 ports, destination layer4 ports and IP protocol.
- ACLs are composed of a sequence of rules and the order of the rules is important. If an incoming packet matches multiple rules, the first matching rule is applied.
- A port may have only one input ACL and one output ACL.

After an ACL is created, it is bound (or applied) to the following interface/ports:

On the Sonus SBC 2000:

- Ethernet ports for inbound and forwarded traffic.
- Logical interfaces for inbound/outbound/forwarded traffic.
- ASM ACLs are applied to inbound and forwarded traffic only, and they are bound on the ASM interface.

On the Sonus SBC 1000:

- ACLs are bound to logical interfaces only.

Important Things to Remember When Creating an ACL

- Because the Sonus SBC 1000/2000 stops testing conditions after the first match, the order of the conditions is critical. The same permit or deny statements specified in a different order may result in a packet being passed under one circumstance and denied in another.
- Input-ACL process packets arriving at the Sonus SBC 1000/2000 before routing to an outbound interface. An inbound access list is efficient because it saves the overhead of routing look-ups if the packet is discarded because it is denied by the filtering tests.
- Output-ACLs process packets before they leave the Sonus SBC 1000/2000.
- Forward-ACLs process packets that are forwarded from one Sonus SBC 1000/2000 port to another.

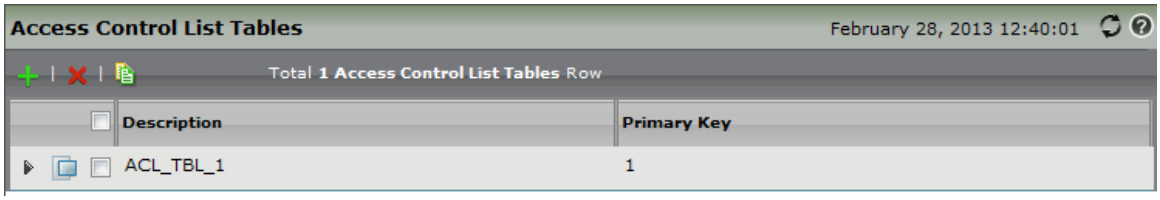
Copyright © 2015 Sonus Networks. All rights reserved.

SBC Support when ACL is applied

- Pinholing and RTP-Pinholing is not supported in Sonus SBC 1000/2000.
- SBC 2000 support is as follows:
  - ACL may be applied to an Ethernet port and it takes effect for all the VLANs on that port.
  - ACL may be applied to a Logical Interface and it is equivalent to applying ACL to a VLAN (note that a VLAN may have many Ethernet ports as members).
- SBC 1000 support is as follows:
  - ACLs cannot be applied to Ethernet ports.
  - ACL may be applied to a Logical Interface and it is equivalent to applying ACL to a VLAN (note that a VLAN may have many Ethernet ports as members).

Working with Access Control List Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Access Control Lists**.



To view an Access Control List's properties:

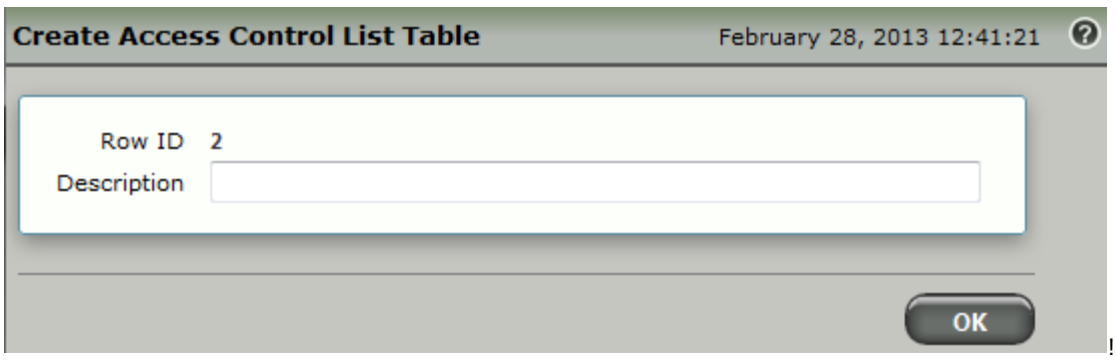
1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

To modify an Access Control List:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To create an Access Control List table:

1. Click the **Create** ( ) icon.



!

2. Enter a descriptive name in the **Description** text field.

Copyright © 2015 Sonus Networks. All rights reserved.

3. Click **OK**.

> **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

> **Restrictions on Deleting ACLs**
>
> An ACL may not be deleted if it is bound to any port or logical interface. However, you may delete or modify a rule within a bound ACL. Any modification or deletion is effective immediately.

Creating and Modifying Rules in Access Control Lists

Creating and Modifying Rules in Access Control Lists

- Creating a Rule Entry
- Modifying a Rule
- Resequencing Rules
- Sample ACL Rule Configuration

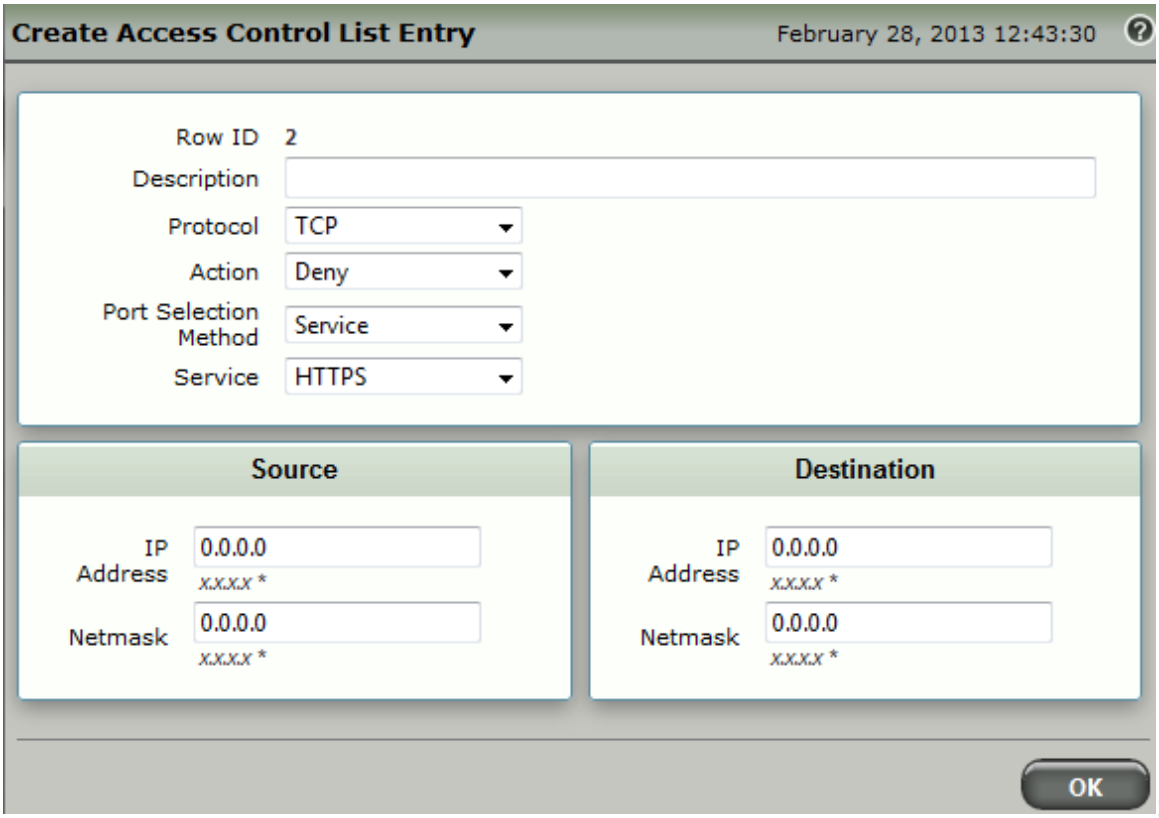
To add or modify an ACL rule:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > Access Control Lists.**

Creating a Rule Entry

1. In the left navigation panel, click on **Access Control Lists** and click on the desired table.
2. Click the **Create ACL Rule** ( ) icon.
3. Enter the desired configuration. See General Information Panel - Field Definitions. For sample configurations, see Sample ACL Rule Configuration.
4. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.



Modifying a Rule

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Restrictions on Deleting ACLs

An ACL may not be deleted if it is bound to any port or logical interface. However, you may delete or modify a rule within a bound ACL. Any modification or deletion is effective immediately.

Resequencing Rules

1. Click the **Resequence** icon ( ) at the top of the table.
2. Select the row(s) you want to move.
3. Click the **Move Selected Rows Up** ( ) or **Move Selected Rows Down** ( ) icon to reposition the row(s) in the table.
4. Click **Apply**.

General Information Panel - Field Definitions

Protocol

Copyright © 2015 Sonus Networks. All rights reserved.

The protocol of the IP packets subject to this rule. Valid options: **TCP, UDP, ICMP, OSPF, Any,** or **Other**. Default value: **TCP**.

Action

Specifies the action to be taken upon packets matching this rule. Valid selections: **Deny** (default, packets matching this rule are not accepted) or **Allow** (packets matching this rule are accepted).

IANA IP Protocol Number

The Internet Assigned Numbers Authority (IANA) port number for various protocols. This field is available only when Other is selected from the Protocol drop down box.

Port Selection Method

Either **Service** or **Range**. The **Services** option allows you to define the service for either UDP or TCP protocol. The **Range** option should be used to specify a specific source or destination port number or port number range. This field is available only when either TCP or UDP is selected from the Protocol drop down box.

Service

Services available for either TCP or UPD. Only those Ports for which the SBC 1000/2000 is a server are available as Services. This field is available only when UDP or TCP is selected from the Port Selection Method drop down box.

Source Panel - Field Definitions

IP Address

The IPv4 source address of the packets subject to this rule.

Netmask

The subnet mask of the source IP address.

Minimum Port Number

The minimum port number associated with the source packets subject to this rule. This field is available only when TCP or UDP is selected from the Protocol drop down box and Range is selected from the Port Selection Method drop down box.

Maximum Port Number

The maximum port number associated with the source packets subject to this rule. This field is available only when TCP or UDP is selected from the Protocol drop down box and Range is selected from the Port Selection Method drop down box.

Destination Panel - Field Definitions

IP Address

Copyright © 2015 Sonus Networks. All rights reserved.

The IPv4 destination address of the packets subject to this rule.

Netmask

The subnet mask of the destination IP address.

Minimum Port Number

The minimum port number associated with the destination packets subject to this rule. This field is available only when TCP or UDP is selected from the Protocol drop down box and Range is selected from the Port Selection Method drop down box.

Maximum Port Number

The maximum port number associated with the destination packets subject to this rule. This field is available only when TCP or UDP is selected from the Protocol drop down box and Range is selected from the Port Selection Method drop down box.

Sample ACL Rule Configuration

Isolated Management Traffic

Click here for Sample ACL configuration

These are sample ACLs and should be customized for your specific deployment.

One use-case for access controls lists is to isolate management traffic on the SBC 2000 to accomplish the following: the SBC WebUI is available only through certain ports on the SBC (i.e., Admin port) and the SBC WebUI is not accessible on those ports.

In a hosted or multi-tenant environment, the SBC is managed by a service provider and is shared with multiple end-customers. The ADMIN port is used solely for managing the SBC by the service provider. In order to configure this ACL, you must do the following:

- Create ACLs that describe the type of traffic that should be accepted or denied.
- Bind the ACLs to the ports for the designated purpose.

Sample ACL "usertraffic"

This ACL allows packets related to VoIP application only and bound to all user ports. This example is for SBC 2000 and should be customized for your specific requirements.

ID	Source IP Subnet	Dest IP Subnet	Protocol	Source port	Destination port	Action	Notes
1	192.168.7.7/24	ANY	ANY	ANY	5060	ACCEPT	Accepts all traffic from Lync server to the SBC's SIP port 5060 or ASM's SIP port 5060.

Copyright © 2015 Sonus Networks. All rights reserved.

2	192.168.9.8/24	ANY	UDP	53	ANY	ACCEPT	Accepts DNS traffic from the DNS server 192.168.9.8.
3	ANY	ANY	UDP	ANY	16000-17000	ACCEPT	Accepts all UDP traffic carrying RTP and RTCP payload from other devices to the SBC. The port range should be same as the range configured under Media System Configuration. See Configuring the Media System.
4	192.168.33.3/24	ANY	UDP	30000	30000	ACCEPT	Accepts control packets between ASM installed on the same SBC and the SBC CPU. UDP/30000 is a reserved port.
5	192.168.33.3/24	ANY	UDP	30001	30001	ACCEPT	Accepts control packets between ASM installed on the same SBC and the SBC CPU. UDP/30001 is a reserved port.
6	ANY	ANY	UDP	30000	30000	DROP	Drops any other source that uses the reserved port 30000.
7	ANY	ANY	UDP	30001	30001	DROP	Drops any other source that uses the reserved port 30001.
8	ANY	ANY	ANY	ANY	ANY	DROP	By default discards all traffic, if the above rules don't match.

Sample ACL "admintraffic"

This ACL accepts specified management traffic and discards all other packets. Also the ACLs should be bound to all ports used only for administration.This example is for SBC 2000 and should be customized for your specific requirements.

ID	Source IP Subnet	Dest IP Subnet	Protocol	Source port	Destination port	Action	Notes
1	ANY	ANY	TCP	ANY	443	ACCEPT	Accepts incoming HTTPS request.
2	ANY	ANY	TCP	ANY	80	ACCEPT	Accepts incoming HTTP request.
3	ANY	ANY	UDP	ANY	161	ACCEPT	Accepts incoming SNMP requests.
4	ANY	ANY	TCP	ANY	22	ACCEPT	Accepts incoming SSH requests.

Copyright © 2015 Sonus Networks. All rights reserved.

5	ANY	192.168.33.3/28	TCP	ANY	3389	ACCEPT	Accepts incoming RDP packets to ASM (assuming ASM's IP address is 192.168.33.3).
6	ANY	ANY	ANY	ANY	ANY	DROP	By default, drops all traffic, if the above rules don't match.

Sample ACL Binding

The ACLs in this example are applied only to the inbound direction of the ports. Once the ACLs are bound to the ports, ports Ethernet 1-4 are used only for VoIP and not for management. The ADMIN port is used only for management and not for user traffic.

Port	ACL Name	Direction	Notes
Ethernet 1	usertraffic	INBOUND	Ethernet 1 is used primarily only for user's traffic such as VoIP calls. The WebUI or any management traffic will be discarded.
Ethernet 2	usertraffic	INBOUND	same as above.
Ethernet 3	usertraffic	INBOUND	same as above.
Ethernet 4	usertraffic	INBOUND	same as above.
ADMIN	admintraffic	INBOUND	ADMIN port is used only for administration. All user traffic (i.e., SIP, RTP) is discarded.

Typical WAN/LAN Deployment

Click here for Sample ACL Rule (Packet Filter)

> These are sample ACLs and should be customized for your specific deployment.

A typical SBC deployment may have two 'sides'. One side is the LAN-side or the corporate-network side, and the other is the Internet-side, WAN-side or the provider-network side. Neither side should be trusted entirely. ACLs must be configured so that only SIP/VOIP/RTP traffic is allowed on both sides. An additional task is usually to determine the IP interface WebUI/REST management is allowed on.

> When configuring ACLs, it is possible to isolate the SBC out of the network. Ensure there are rules in place to accept HTTPS on at least one IP interface. The order of rules in the ACL is important.

For this example, consider that the Sonus SBC 1000 has two IP interfaces

1. Ethernet 1 IP: 12.3.10.10/24 (LAN-side, office-side, branch-side, corporate network-side)
2. Ethernet 2 IP: 10.1.10.10/24 (SIP trunk side, WAN-side, Provider-side, Internet-side)

LAN Side ACL

Copyright © 2015 Sonus Networks. All rights reserved.

(For this example, this ACL must be applied to 'Ethernet 1 IP' as "Input ACL")

Description	Protocol	Action	Port Selection	Service	Source IP	Source Mask	Source Min Port	Source Max Port	Dest IP
Allow WebUI/HTTPS	TCP	Allow	Service	HTTPS	0.0.0.0	0.0.0.0			0.0.0.0
Allow WebUI/HTTP to redirect to HTTPS	TCP	Allow	Service	HTTP	0.0.0.0	0.0.0.0			0.0.0.0
Accept SIP Signaling over UDP	UDP	Allow	Range		40.1.1.1	255.255.255.255	1024	65535	0.0.0.0
Accept SIP Signaling over TCP and TLS	TCP	Allow	Range		50.1.1.2	255.255.255.255	1024	65535	0.0.0.0

Copyright © 2015 Sonus Networks. All rights reserved.

Accept SIP Signaling TCP and TLS ACKs	TCP	Allow	Range		50.1.1.2	255.255.255.255	5067	5067	0.0.0.0
Accept RTP/RTCP packets	UDP	Allow	Range		0.0.0.0	0.0.0.0	1024	65535	0.0.0.0
Accept DNS responses	UDP	Allow	Range		0.0.0.0	0.0.0.0	53	53	0.0.0.0
Discard all other packets	ANY	Deny			0.0.0.0	0.0.0.0			0.0.0.0

SIP Trunk Side ACL

(For this example, this ACL must be applied to 'Ethernet 2 IP' as "Input ACL")

Description	Protocol	Action	Port Selection	Source IP	Source Mask	Source Min Port	Source Max Port	Dest IP	Dest Mask

Copyright © 2015 Sonus Networks. All rights reserved.

Accept SIP Signaling over UDP	UDP	Allow	Range	20.5.1.20	255.255.255.255	1024	65535	10.1.10.10	255.2
Accept RTP/RTCP packets	UDP	Allow	Range	20.5.1.20	255.255.255.255	1024	65535	10.1.10.10	255.2
Accept DNS responses	UDP	Allow	Range	0.0.0.0	0.0.0.0	53	53	0.0.0.0	0.0.0.
Discard all other packets	ANY	Deny		0.0.0.0	0.0.0.0			0.0.0.0	0.0.0.

Working with Network Services

This group of pages contains topics related to networking services provided by the Sonus SBC 1000/2000.

Copyright © 2015 Sonus Networks. All rights reserved.

Managing the DHCP Server

- Creating and Modifying DHCP Pools
- Creating and Modifying Static DHCP Clients
- Enabling the DHCP Server
- Viewing Client DHCP Leases

Managing the DHCP Client

- Enabling the DHCP Client
- Configuring DHCP Client - Sample Deployment

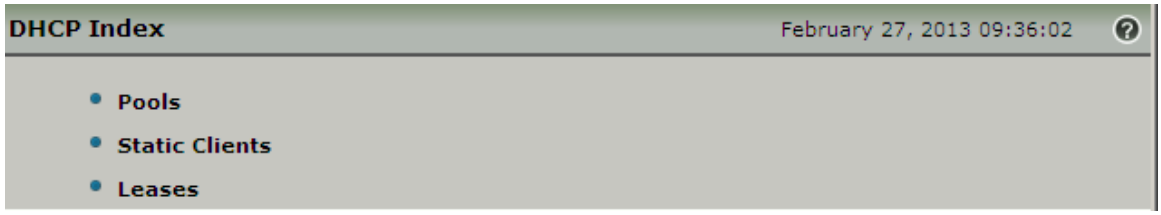
Managing the DHCP Server

The Sonus SBC 1000/2000 has the ability to function as a DHCP server. This includes granting IP address leases and providing other network parameters to any network connected device. In addition to being able to enable/disable the server at a global level, the user can create DHCP address pools and static DHCP client configurations. All DHCP Server functionality is supported on all Sonus SBC 1000/2000 platforms.

Although the primary use case for the DHCP server functionality is in the branch office configuration, it is by no means limited to only this scenario. With the proper configuration, the Sonus SBC 1000/2000 can serve multiple subnets on different Ethernet interfaces, and host a multitude of both dynamically and statically configured clients.

Working with the DHCP Server

1. In the WebUI, click the **Settings** tab.
2. in the left navigation pane, go to **Protocols > IP > DHCP**.



Creating and Modifying DHCP Pools

Creating and Modifying Static DHCP Clients

Enabling the DHCP Server

Viewing Client DHCP Leases

Creating and Modifying DHCP Pools

For the Sonus SBC 1000/2000 to function as a DHCP server, it must be enabled and have a DHCP pool configured on the at least one of its interfaces. The Sonus SBC 1000/2000 will only perform DHCP server functionality on those interfaces that have a DHCP pool associated with them.

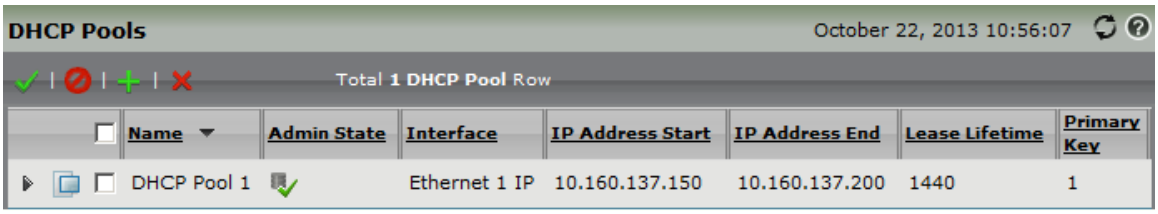
The Sonus SBC 1000/2000 DHCP Server supports serving up to a maximum of 20 address pools. A DHCP pool typically consists of a name, an IP address range, netmask, default router, and other various network parameters,

Copyright © 2015 Sonus Networks. All rights reserved.

allowing the Sonus SBC 1000/2000 to serve as a DHCP server to multiple connected subnets. It also allows the Sonus SBC 1000/2000 to provide different DHCP parameters to different pools of clients (e.g. SIP phones, engineering workstations, VPN users, etc.).

To create or to modify an existing DHCP Pool:

1. In the WebUI, click the **Settings** tab.
2. From the left navigation pane, go to **Protocols > IP > DHCP > Pools**.



Modifying a DHCP Pool

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Enabling an Entry in a DHCP Pool

1. Select the check box next to the entry you wish to enable.
2. Click the **Enable** ( ) icon at the top of the table.

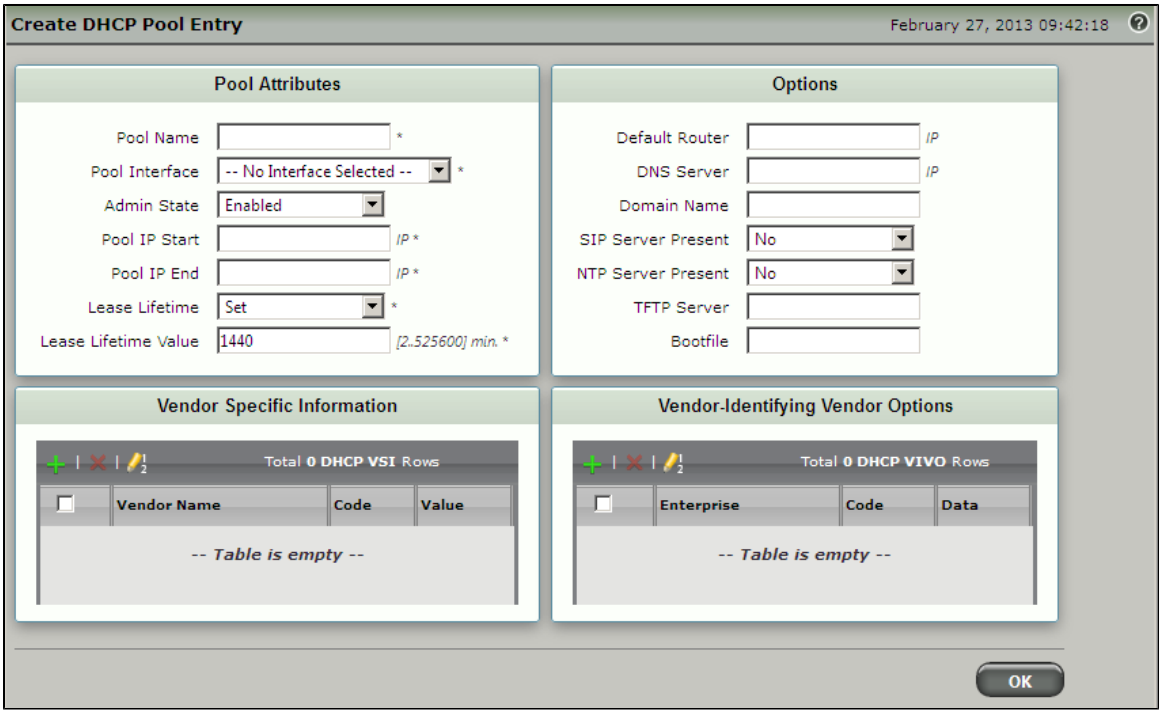
Disabling an Entry in a DHCP Pool

1. Select the check box next to the entry you wish to disable.
2. Click the **Disable** ( ) icon at the top of the table.

Creating a DHCP Pool

1. From the DHCP Pools window, click on the ( ) at the top of the screen.

Copyright © 2015 Sonus Networks. All rights reserved.



Pool Attributes - Field Definitions

Pool Name

Specifies the name of the DHCP pool.

Pool Interface

Specifies the interface with which this pool is associated. This drop down list is populated with the interfaces configured in Logical Interfaces.

Pool IP Start

Specifies the beginning address for the range of addresses in the DHCP pool (the pool from which the DHCP clients will get their IP addresses).

Pool IP End

Specifies the ending address for the range of addresses in the DHCP pool (the pool from which the DHCP clients will get their IP addresses).

Lease Lifetime

Specifies whether the duration of the lease is infinite or a specified value. Valid values: **Set** (lease is set to a specific value, see Lease Lifetime Value) or **Never Expires** (there is no expiration time on lease).

Lease Lifetime Value

Specifies the duration of the lease, in minutes. Valid entry: **2** - **525600** minutes. Visible only when **Set** is selected from the **Lease Lifetime** drop down list.

Copyright © 2015 Sonus Networks. All rights reserved.

Options - Field Definitions

Default Router

Specifies the default router used for DHCP Clients. Must be an IPv4 address.

DNS Server

Specifies the DNS server used for DHCP Clients. Must be an IPv4 address.

Domain Name

Specifies the domain name for DHCP clients to use when connecting to the pool.

SIP Server Present

Specifies whether or not the node uses a SIP server attached to an available network.

Primary SIP Server

Specifies the Primary SIP server to be used by the DHCP client. Must be an IPv4 address. Visible only when **Yes** is selected in the **SIP Server Present** list box.

Secondary SIP Server Present

Specifies whether or not the node uses a SIP server attached to an available network. Visible only when **Yes** is selected in the **SIP Server Present** list box.

Secondary SIP Server

Specifies the Secondary SIP server to be used by the DHCP client. Must be an IPv4 address. Visible only when **Yes** is selected in the **Secondary SIP Server Present** list box.

NTP Server Present

Specifies whether or not the node uses an NTP server attached to an available network.

Primary NTP Server

Specifies the Primary NTP server to be used by the DHCP client. Must be an IPv4 address. Visible only when **Yes** is selected in the **NTP Server Present** list box.

Secondary NTP Server Present

Specifies whether or not the node uses a Secondary NTP server attached to an available network. Visible only when **Yes** is selected in the **NTP Server Present** list box.

Secondary NTP Server

Specifies the Secondary NTP server to be used by the DHCP client. Must be an IPv4 address. Visible only when **Yes** is selected in the **Secondary NTP Server Present** list box.

Copyright © 2015 Sonus Networks. All rights reserved.

TFTP Server

Specifies the TFTP server to be used by the DHCP client. May be any server name or IP address

Bootfile

Specifies the bootfile used by the DHCP client.

Vendor Options - Overview

Vendor Options allows the Sonus SBC 1000/2000 to provide vendor parameters for different pools of clients (i.e, SIP phones, engineering workstations, VPN users, etc.). The configuration values are specific to the phone or device being configured. For valid values, consult the manual that accompanied the phone/device.

The **Vendor Specific Information** is for Dynamic Host Configuration Protocol (DHCP) option 43 (defined here: http://tools.ietf.org/html/rfc2132#section-8.4). These options indicate the vendor type, and the DHCP client pool and server to exchange vendor specific information.

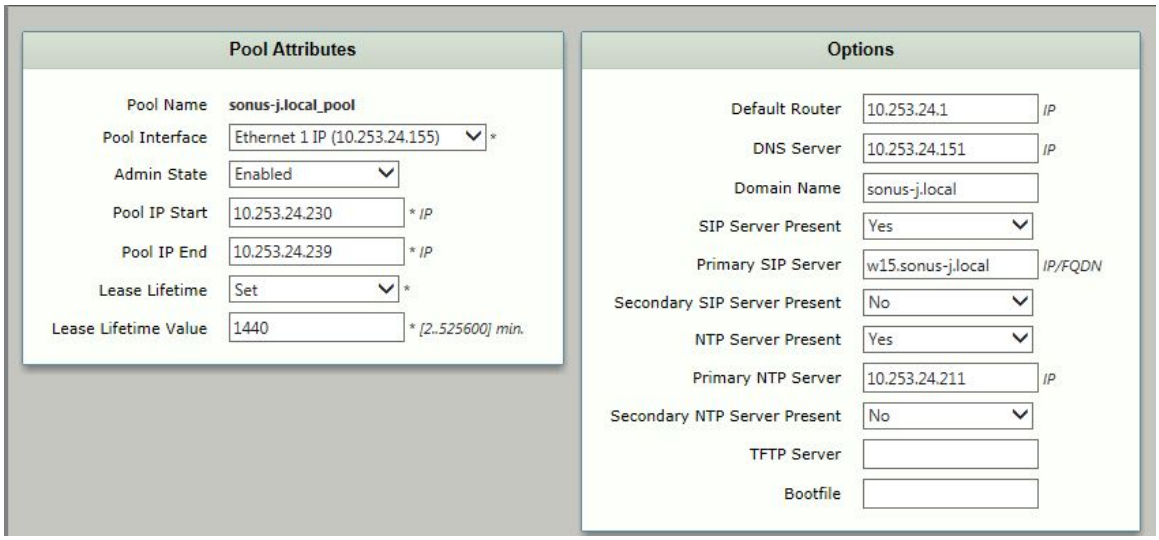
The **Vendor-Identifying Vendor Options** are DHCP option 124/125 (defined here: http://tools.ietf.org/html/rfc3925).

Click here for example

Pool Attribute Configuration - Example

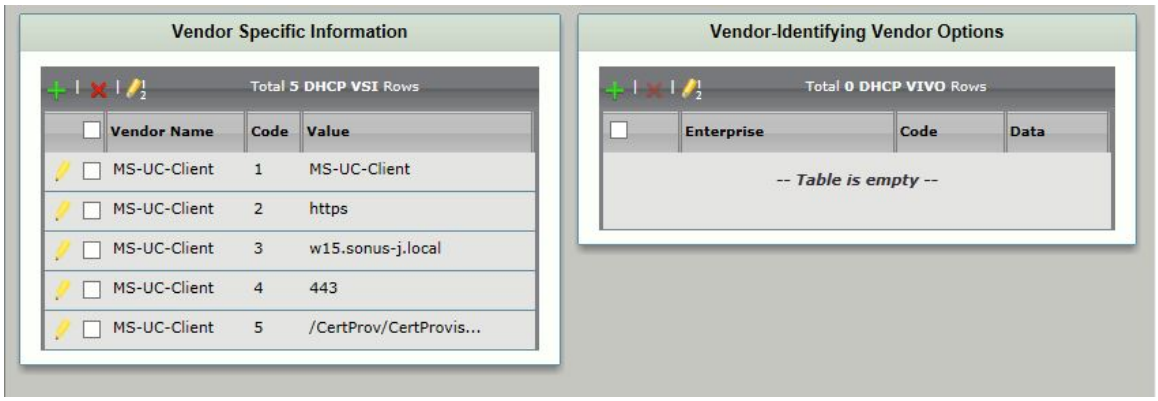
Below is an example configuration for a **Polycom (CX500)** phone. Follow the initial instructions for Creating and Modifying DHCP Pools and configure as shown below.

These fields must be configured before the Vendor specific configuration below.



Vendor Specific Configuration

Copyright © 2015 Sonus Networks. All rights reserved.



Vendor Specific Information - Field Definitions

Vendor Name

Specifies the vendor name for the Vendor Specific Information. Used to match against the client's vendor name and send the vendor attribute if a match occurs. Maximum length: 64 characters.

Code

Specifies the Vendor Specific Information option code sent. Valid entry: 0 - 254 characters.

Value

Specifies the Vendor Specific Information user data sent to the matching DHCP client. This is dependent upon the option code used, and can be an ASCII string or hex string of the *00:aa:bb* format. Valid entry: maximum length of 64 characters.

Vendor-Identifying Vendor Options - Field Definitions

Enterprise Number

Specifies the vendor enterprise number for the Vendor-Identifying Vendor Options. Used to match against the client's vendor enterprise number and send a vendor attribute if a match occurs.

> Enterprise numbers are defined by IANA and can be found here.

Code

Specifies the Vendor-Identifying Vendor Option code to be sent.

Data

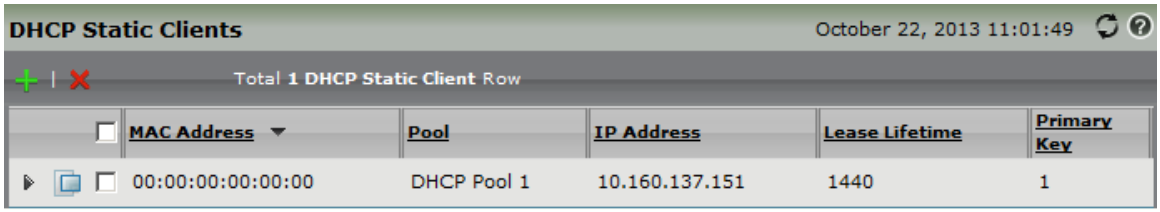
Specifies the Vendor-Identifying Vendor Option data to be sent. A valid entry can be either an ascii string of the attribute or a hex string in the aa:bb:cc format. Maximum length: 64 characters.

Copyright © 2015 Sonus Networks. All rights reserved.

Creating and Modifying Static DHCP Clients

To create or to modify an existing Static DHCP Client:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > DHCP > Static Clients**.



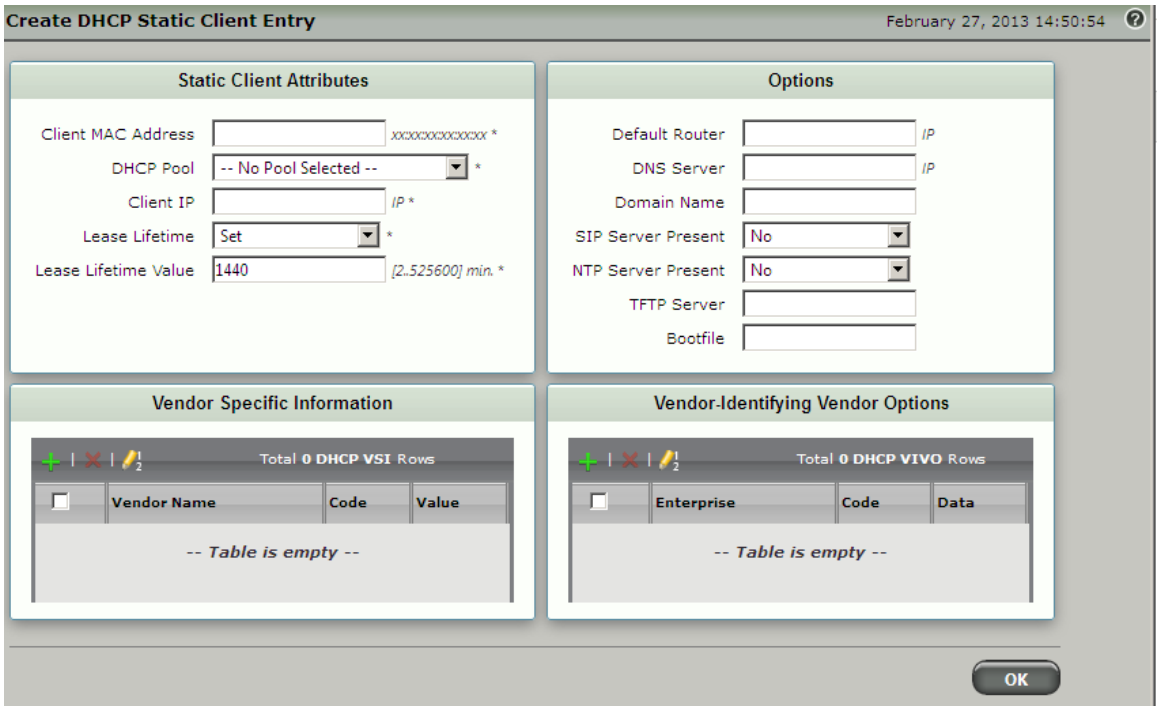
Modifying a Static DHCP client Pool.

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

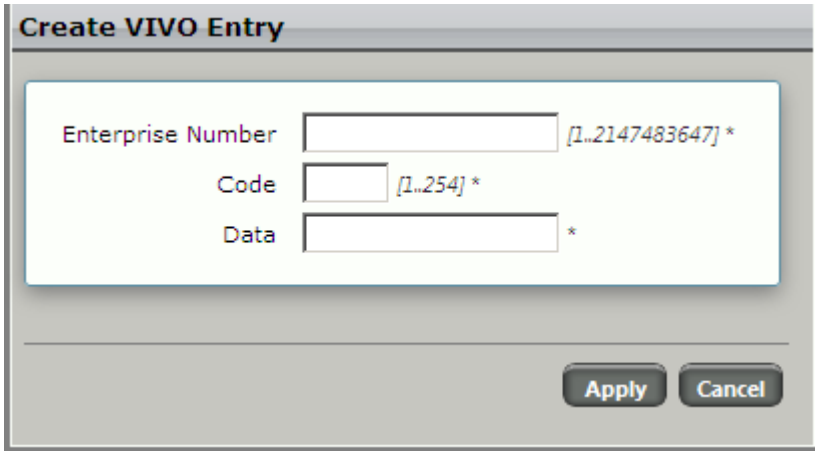
Creating a Static DHCP Client

To create a static client:

1. Click the **Create DHCP Static Client** ( ) icon at the top of the page.



Copyright © 2015 Sonus Networks. All rights reserved.



Static Client Attributes- Field Definitions

Client MAC Address

Specifies the MAC address of the DHCP Client

DHCP Pool

Specifies the pool of which this static client is a member.

Client IP

Specifies the IP address to be assigned to this DHCP client.

Lease Lifetime

Specifies whether the duration of the lease is infinite or a specified value.

Lease Lifetime Value

Specifies the duration of the lease, in minutes. Visible only when **Set** is selected from the **Lease Lifetime** list box.

Options - Field Definitions

Default Router

Specifies the default router used for DHCP Clients. Must be an IPv4 address.

DNS Server

Specifies the DNS server used for DHCP Clients. Must be an IPv4 address.

Domain Name

Specifies the domain name for DHCP clients to use when connecting to the pool.

Copyright © 2015 Sonus Networks. All rights reserved.

SIP Server Present

Specifies whether or not the node uses a SIP server attached to an available network.

Primary SIP Server

Specifies the Primary SIP server to be used by the DHCP client. Must be an IPv4 address. Visible only when **Yes** is selected in the **SIP Server Present** list box.

Secondary SIP Server Present

Specifies whether or not the node uses a SIP server attached to an available network. Visible only when **Yes** is selected in the **SIP Server Present** list box.

Secondary SIP Server

Specifies the Secondary SIP server to be used by the DHCP client. Must be an IPv4 address. Visible only when **Yes** is selected in the **Secondary SIP Server Present** list box.

NTP Server Present

Specifies whether or not the node uses an NTP server attached to an available network.

Primary NTP Server

Specifies the Primary NTP server to be used by the DHCP client. Must be an IPv4 address. Visible only when **Yes** is selected in the **NTP Server Present** list box.

Secondary NTP Server Present

Specifies whether or not the node uses a Secondary NTP server attached to an available network. Visible only when **Yes** is selected in the **NTP Server Present** list box.

Secondary NTP Server

Specifies the Secondary NTP server to be used by the DHCP client. Must be an IPv4 address. Visible only when **Yes** is selected in the **Secondary NTP Server Present** list box.

TFTP Server

Specifies the TFTP server to be used by the DHCP client. May be any server name or IP address

Bootfile

Specifies the filename of the bootfile used by the client.

Vendor Options - Overview

Vendor Options allows the Sonus SBC 1000/2000 to provide vendor parameters for a specific static DHCP client (i.e, SIP phones, engineering workstations, VPN users, etc.). The configuration values are specific to the phone or device being configured. For valid values, consult the manual that accompanied the phone/device.

Copyright © 2015 Sonus Networks. All rights reserved.

The **Vendor Specific Information** is for Dynamic Host Configuration Protocol (DHCP) option 43 (defined here: http://tools.ietf.org/html/rfc2132#section-8.4). These options allows a client (phone or device) to indicate its vendor type, and the DHCP client and server to exchange vendor specific information.

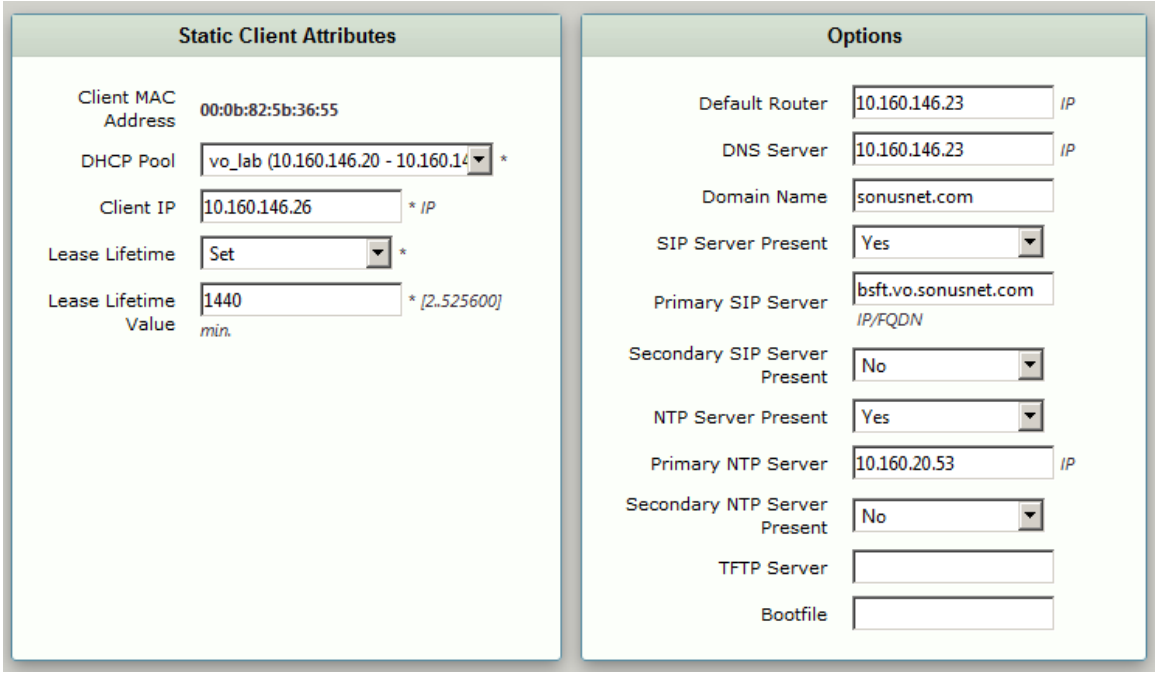
The **Vendor-Identifying Vendor Options** are DHCP option 124/125 (defined here: http://tools.ietf.org/html/rfc3925).

Click here for example

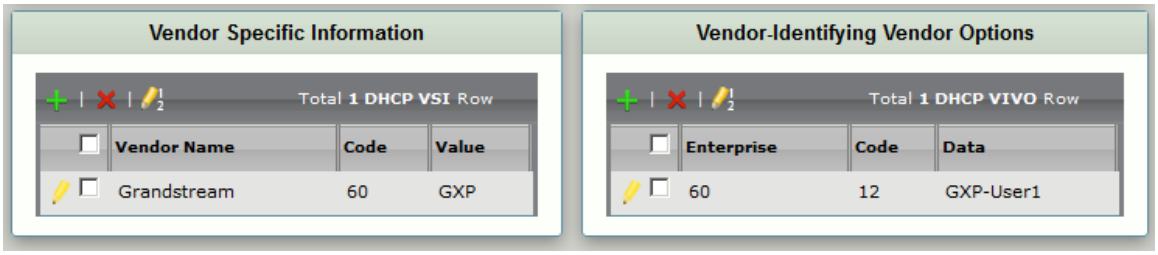
Static Client Attribute Configuration - Example

Below is an example configuration for a **Grandstream (GXP2200)** phone. Follow the initial instructions for Creating and Modifying Static DHCP Clients and configure as show below.

These fields must be configured before the Vendor specific configuration below.



Vendor Specific Configuration



Vendor Specific Information - Field Definitions

Vendor Name

Specifies the vendor name for the Vendor Specific Information. Used to match against the client's vendor name and send the vendor attribute if a match occurs. Maximum length: 64 characters.

Copyright © 2015 Sonus Networks. All rights reserved.

Code

Specifies the Vendor Specific Information option code sent. Valid entry: 0 - 254 characters.

Value

Specifies the Vendor Specific Information user data sent to the matching DHCP client. This is dependent upon the option code used, and can be an ASCII string or hex string of the *00:aa:bb* format. Maximum length: 64 characters.

Vendor-Identifying Vendor Options - Field Definitions

Enterprise Number

Specifies the vendor enterprise number for the Vendor-Identifying Vendor Options. Used to match against the client's vendor enterprise number and send a vendor attribute if a match occurs.

> Enterprise numbers are defined by IANA and can be found here.

Code

Specifies the Vendor Specific Information option code sent. Valid entry: 0 - 254 characters.

Data

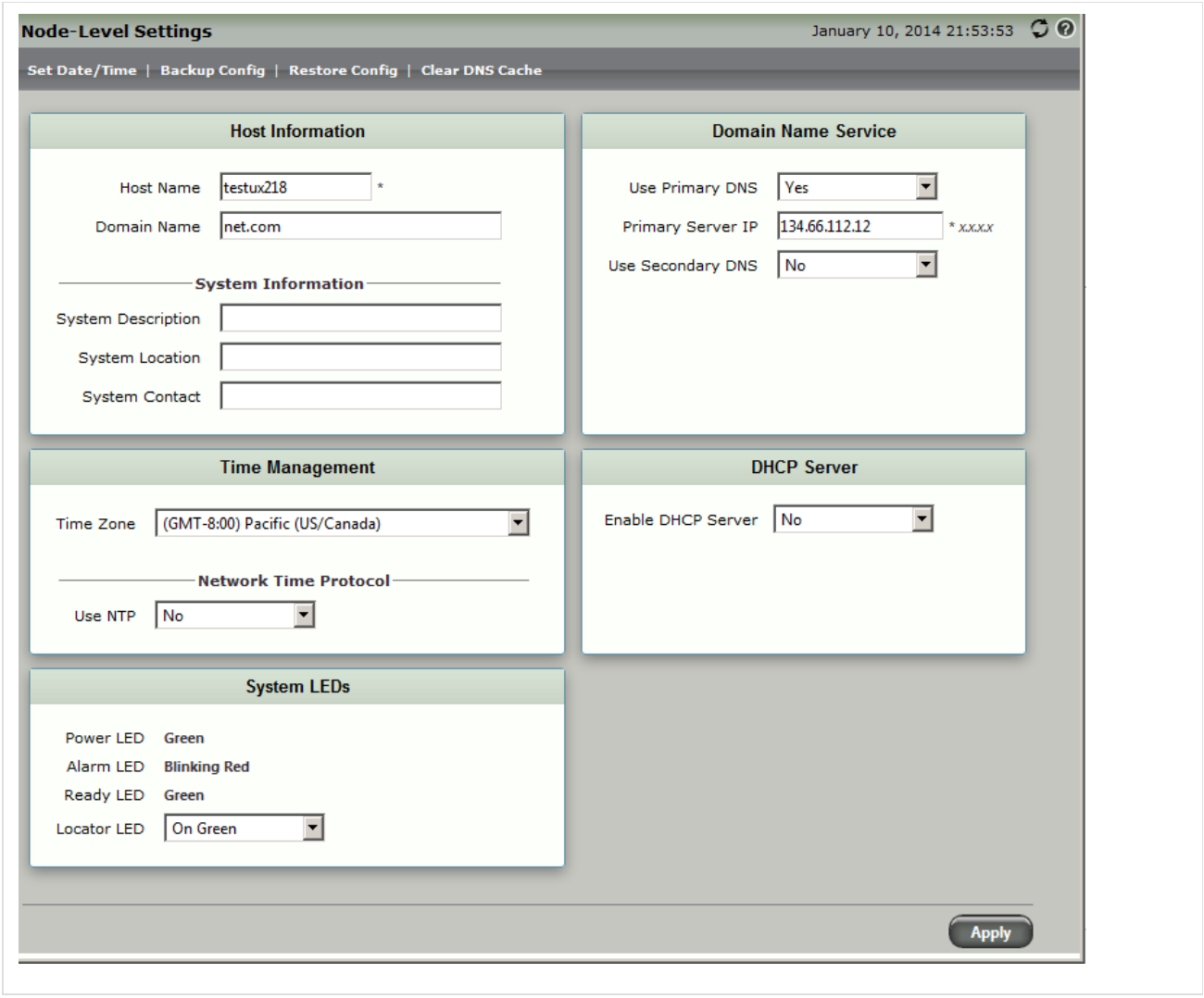
Specifies the Vendor-Identifying Vendor Option data to be sent. A valid entry can be either an ascii string of the attribute or a hex string in the aa:bb:cc format. Maximum length: 64 characters.

Enabling the DHCP Server

To enable the DHCP Server:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Node-Level Settings**

Copyright © 2015 Sonus Networks. All rights reserved.



3. In the Enable DHCP list, click **Yes**.
4. Click **Apply**.

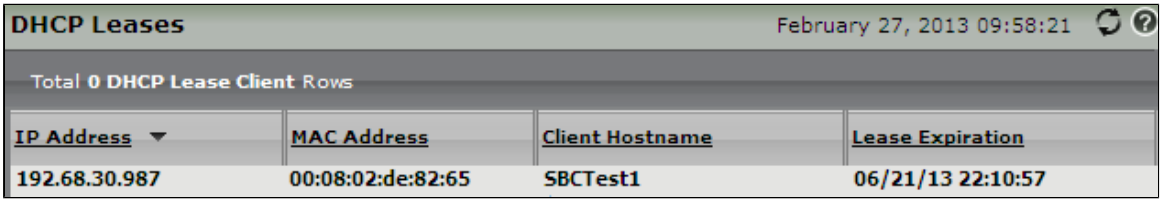
- See also, Configuring Host Information and DNS

Viewing Client DHCP Leases

Viewing DHCP Leases

To view DHCP Leases:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > DHCP > Leases**.



Copyright © 2015 Sonus Networks. All rights reserved.

Managing the DHCP Client

When enabled in the SBC, the DHCP client acquires the interface's IP configuration dynamically from a reachable DHCP server. Once initial configuration takes place, the DHCP client can be enabled on a per logical interface basis in the SBC. DHCP address assignment can be configured on both VLAN interfaces (VLAN 1 IP, VLAN 2 IP, etc) and port specific interfaces (i.e., Ethernet 1 IP, Ethernet 2 IP). DHCP is not supported on loopback or Admin interfaces. When enabled in the SBC, the DHCP client configures the following interface-specific attributes:

- IP Address
- IP Netmask
- IP Broadcast Address

The DHCP client also dynamically configures several node-level attributes. Upon configuration of these attributes, any existing configuration is removed.

- Default Route
- DNS Server(s)
- NTP Server(s)
- Domain Name

Note

Although enabling DHCP on multiple interfaces is supported, the recommendation is to enable only one interface with DHCP, or unexpected results may occur. If using multiple interfaces, you should assign the additional IP addresses via static configuration.

In case of IP lease renew for DHCP, or change of static IP where the new IP address is different, the existing calls will be disconnected.

Prerequisites - Setting up the DHCP client

In order to use the DHCP client on your network, the DHCP server must be on the network.

Using DHCP for System Access During Initial Configuration

When a system is in Factory Default mode, the DHCP client is enabled on **Ethernet 1** and the DHCP server is enabled on **Ethernet 2**. This allows you to connect to the Sonus SBC without having to assign your computer a static IP.

The DHCP client acquires an IP address from DHCP server. During DHCP lease acquisition, the SBC provides the DHCP server with its hostname, which is set to the SBC node's hardware ID. If your network's DHCP and DNS servers have Dynamic DNS configured properly, the DHCP server will inform the DNS server that the SBC is reachable via its default hostname (i.e., the SBC's serial number). As a result, during initial configuration, you can access the SBC node on the network by directing your PC's browser to the node's serial number (i.e., *A4025511270005.yourdocaldomain.doc*). The serial number can be found on the back of the SBC unit (i.e., A4025511270005).

This default configuration is present only until initial configuration is complete. Following that, you can configure any desired DHCP functionality. The default IP addresses assigned before initial configuration are as follows:

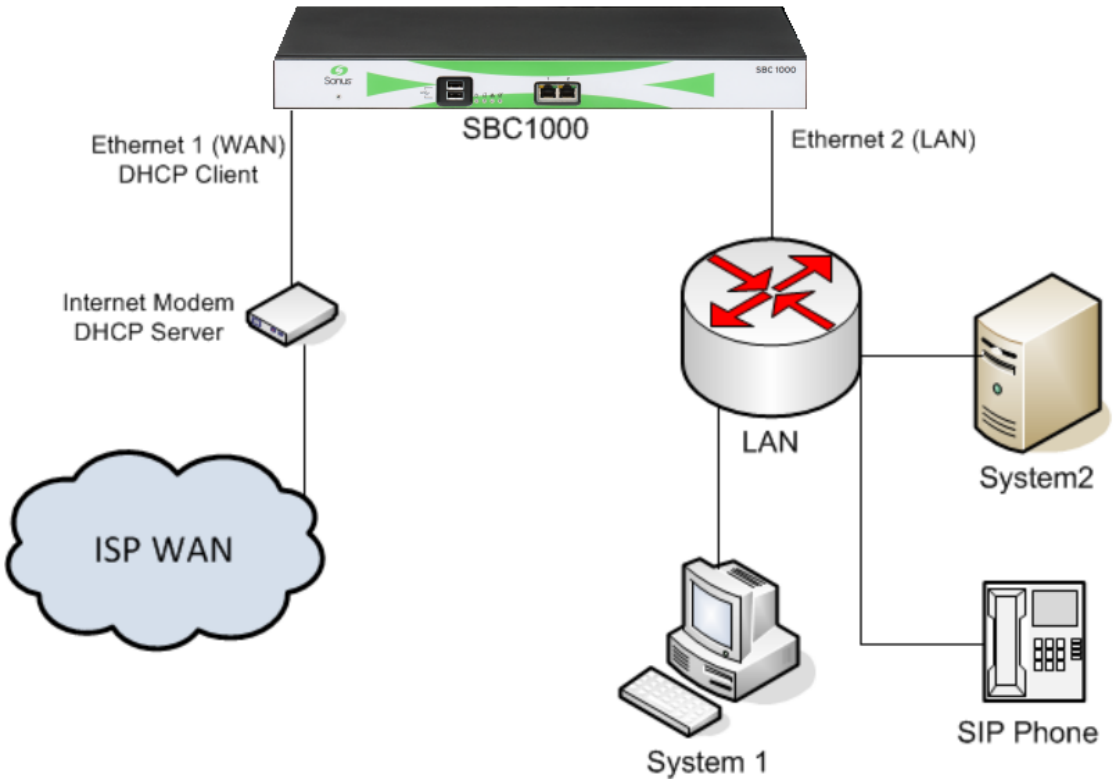
- **Sonus SBC 2000 only**:
  - **Admin Port** - Default address of 192.168.128.2. You can statically assign the PC an address in the 192.168.128.x subnet (i.e.,. 192.168.128.8) to connect to the Sonus SBC 2000.

Copyright © 2015 Sonus Networks. All rights reserved.

- **Sonus SBC 2000 and Sonus SBC 1000**:
  - **Ethernet 1** – Acquires an address via a connected DHCP server.
  - **Ethernet 2** – Default address of 192.168.129.2. You can either statically assign an address to the PC in the 192.168.129.x subnet (e.g. 192.168.129.8) or the Sonus SBC 1000/2000's DHCP server will assign one (192.168.129.3).

How a DHCP Client works - Example Scenario

The DHCP client can be configured on any interface in any network layout as along as there is a DHCP server. For example, in a typical SBC1000 branch office deployment, the SBC will have **Ethernet 1** connected to the ISP WAN, and **Ethernet 2** connected to the office LAN. In this scenario, the SBC's Ethernet 1 interface will acquire an IP address via DHCP from the ISP provided internet modem.



Enabling the DHCP Client

Configuring DHCP Client - Sample Deployment

Enabling the DHCP Client

The DHCP client can be enabled during initial configuration, or later on a per interface basis through the Logical Interface configuration.

Copyright © 2015 Sonus Networks. All rights reserved.

Note

Although enabling DHCP on multiple interfaces is supported, the recommendation is to enable only one interface with DHCP, or unexpected results may occur. If two interfaces are configured with DHCP enabled, there will be two different default routes, DNS servers, and/or NTP servers. Because of this, it could be unpredictable which servers will be used. If using multiple interfaces, you should assign the additional IP addresses via static configuration.

Enable DHCP on a logical interface as follows:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interface> Logical Interfaces.**
3. Select the desired Interface (i.e., **Ethernet 1 IP)**.
4. Click the **expand** ( ) next to the interface you wish to modify.
5. From the **IP Assign Method** drop down box, select **DHCP**. For more information about the Logical Interfaces fields, see Configuring and Modifying Logical Interfaces.

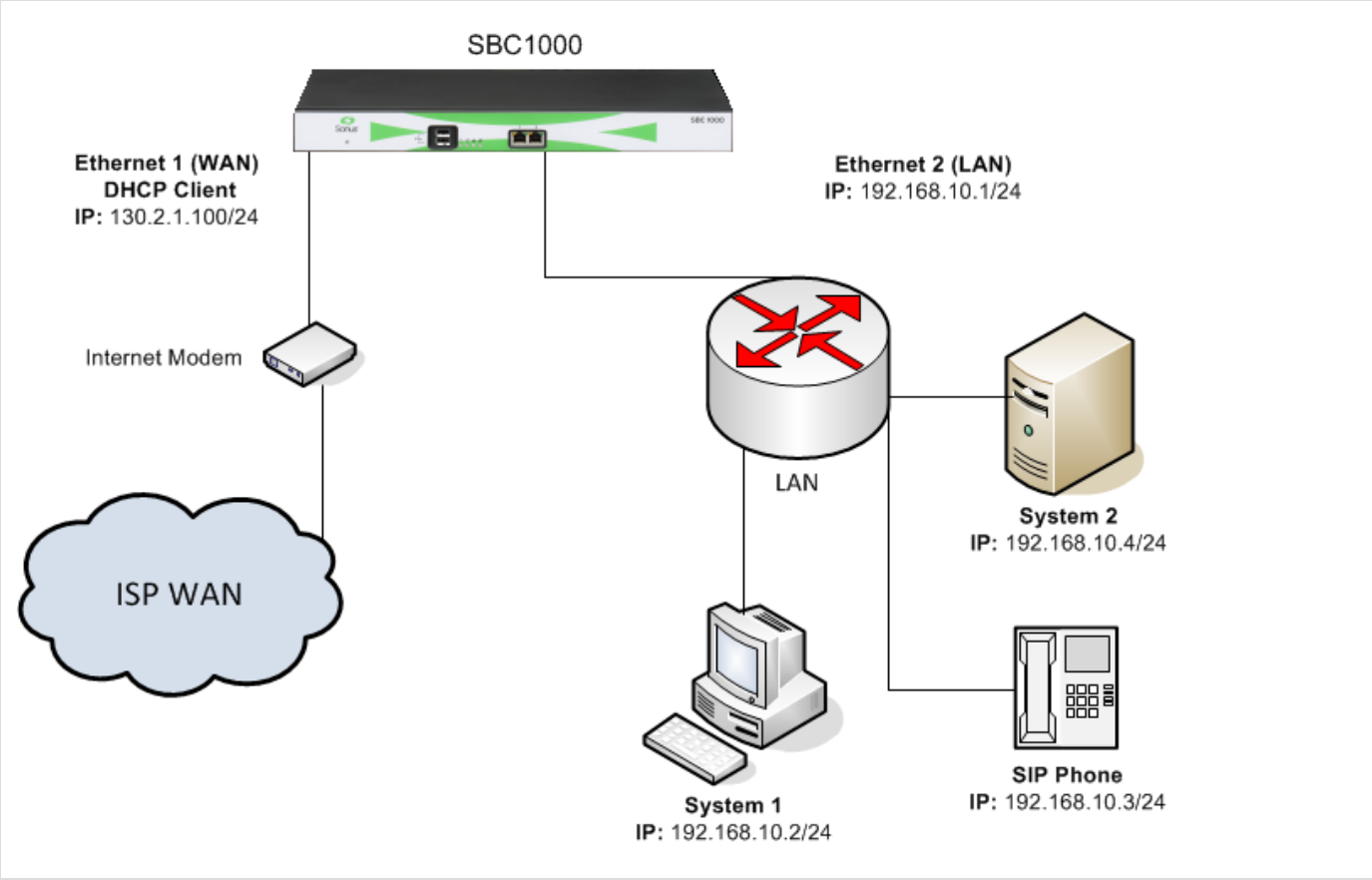
Configuring DHCP Client - Sample Deployment

For the DHCP client, one of the more common configurations is a small office deployment where the SBC1000 behaves as a gateway between the WAN and the LAN. From a basic networking standpoint, the following configuration steps need to take place. Use these instructions as a sample for base configuration only; your network needs may require network-specific configuration.

This deployment uses NAT, and an optional DHCP Server.

1. For **Ethernet 1**, set the *IP Assign Method* as DHCP. This can be configured through Initial Configuration or from the Settings tree (through **Node Interfaces**> **Logical Interfaces**> **Ethernet 1 IP**).
2. For **Ethernet 2**, set the private IP Address (ex: 192.168.10.1). From the Settings tree, this can be configured through **Node Interfaces**> **Logical Interfaces**> **Ethernet 2 IP**.
3. Create a NAT entry. From the Setting tree, this can be configured through **Protocols**> **IP**> **NAT > NAT Interface**in the settings tree, with the following attributes:
    a. *External Network Interface.* Select the SBC logical interface connected to the external network.
    b. *Private Network IP Address.* Specify the IPv4 IP address used to identify the host or network to which NAT will be applied.
    c. *Private Network Netmask.* Specify the IP Netmask used to identify the host or network to which NAT will be applied.
4. **Optional:** Enable DHCP Server. This can be configured through **System**> **Node-Level Settings**.
5. **Optional:** Add a DHCP Pool to **Ethernet 2**. This can be configured through **Protocols**> **IP**> **DHCP**> **Pools**.

Copyright © 2015 Sonus Networks. All rights reserved.



SIP Message Manipulation

> This feature is intended for advanced users who are familiar with the details of RFC-3261. The feature is only available to Admin users. Incorrect use of this feature may adversely impact system performance or may disable SIP call processing.

Overview

SIP Message Manipulation feature is used by a SIP Signaling Group to manipulate the incoming or outgoing messages. This feature is intended to enhance interoperability with different vendor equipment and applications, and for correcting any fixable protocol errors in SIP messages on fly without any changes to firmware/software.

Although SIP is considered a mature protocol there are still devices running old firmware and systems that interpret the standard in a non-conforming way. In addition there are cases where a compliant message may be modified to adapt to an application specific requirement. In a typical deployment there may be hundreds or even thousands of endpoints that use the services of the SBC. In these environments when an interoperability issue arises or an application expects a specific behavior the only remedy is to escalate the issue and wait for a maintenance release. This is neither scalable nor very responsive so the SIP Message Manipulation feature was developed to solve this issue.

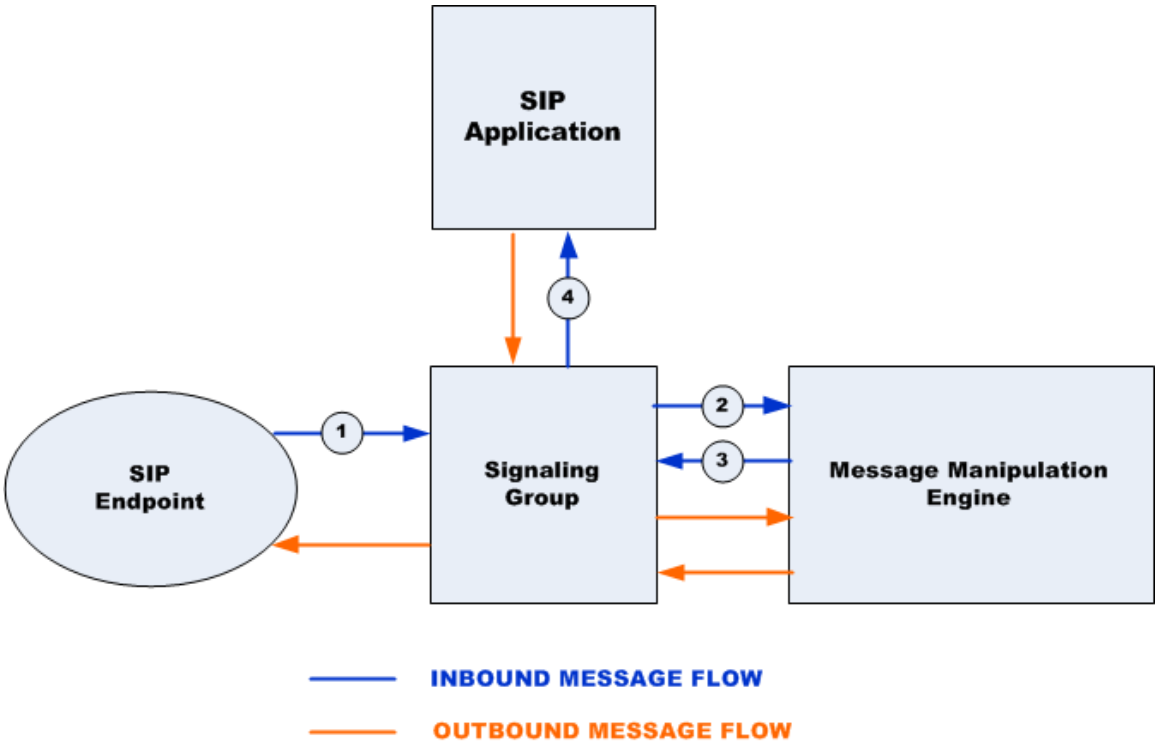
This capability consists of two components, condition rules and message rules. Condition rules provide a means to identify which messages and what components in the message must present before any modifications are performed. For example, I want to modify all INVITE messages with a from uri host of "sonus.net".

The message rule does the actual modification of a message. Once the conditions of a rule have been met the message rule(s) are applied. Continuing with the example above, a message rule may change the from uri display name to "Sonus Networks".

Copyright © 2015 Sonus Networks. All rights reserved.

Another common problem in the field is decoding failures from endpoints that are not in compliance with the SIP protocol. In these instances the protocol problems can be fixed before the message is passed to the applications, and broken (restored) when the message is sent back to the non-conforming endpoint.

The feature's Message Manipulation Engine (MME) manipulates SIP messages in order to compensate for interoperability issues between differing vendor equipment and for dynamically correcting reparable protocol errors in SIP messages. The flows described in this article are **message** flows and should not be confused with **call** flows.



Message Flow

Inbound Messages

(1) The SIP Signaling Group receives a message from a SIP endpoint and(2) passes that message to the Message Manipulation Engine (MME) the message is examined using Rule and Condition Tables, then manipulated as required and (3)sent back to the SIP Signaling Group which then sends (4) it to the SIP Application.

Outbound Messages

Outbound message flows are essentially a mirror image of inbound message flows. The SIP application sends messages, which could be replies, request, or responses, to an endpoint. The Messages move from the SIP application to the Signaling Group, to the MME where they are modified appropriately to be successfully understood by the endpoint, passed back to the Signaling Group, and then transmitted to the end point.

Message Manipulation Components

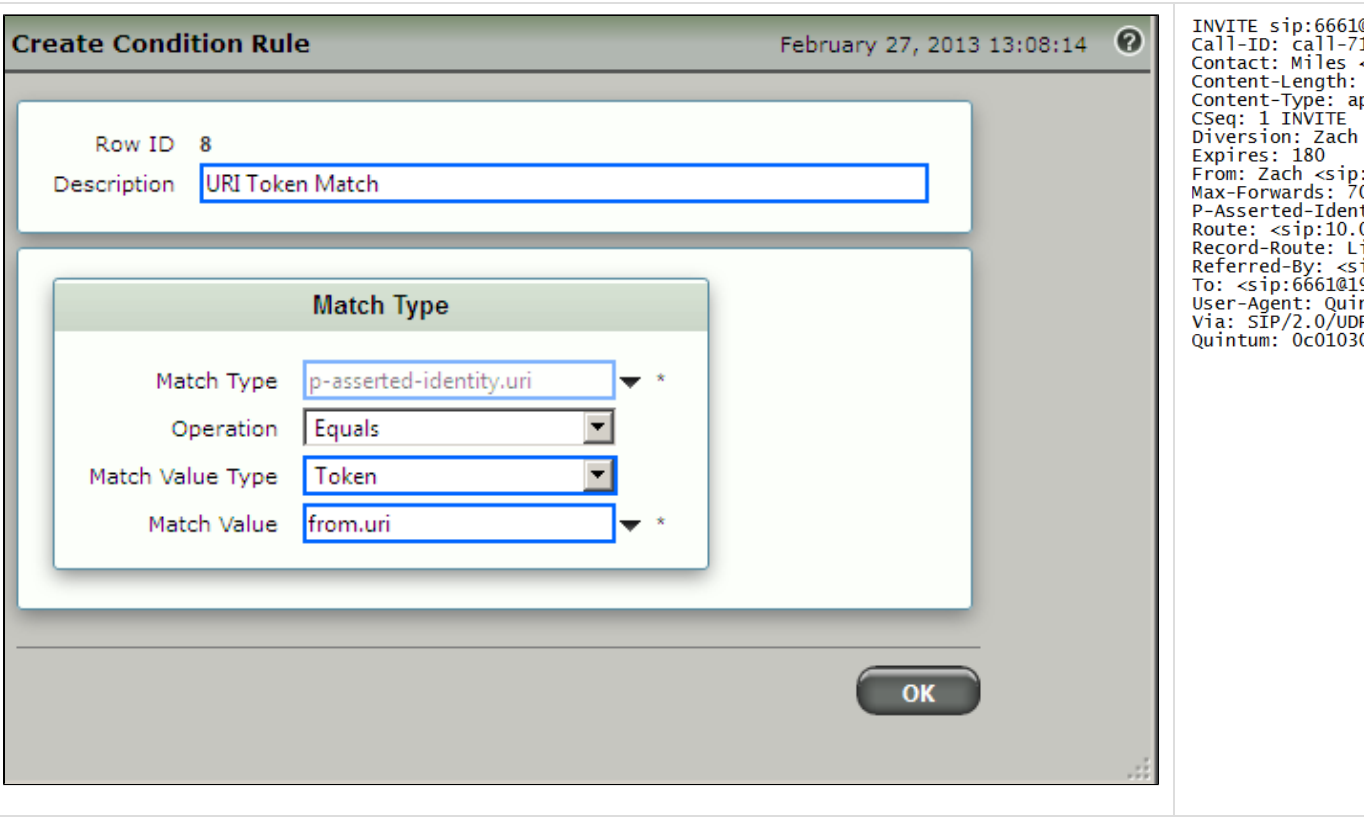
The Message Manipulation feature comprises two primary components that work in concert to modify SIP messages. Those component are Condition Rules and Rule Tables.

Condition Rules

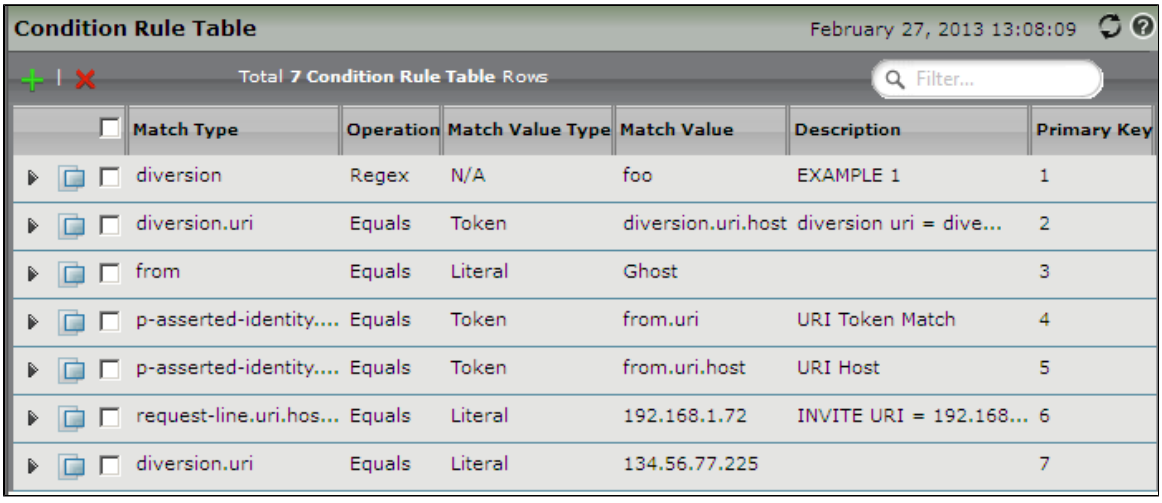
Copyright © 2015 Sonus Networks. All rights reserved.

Condition rules are simple rules that apply to a specific component of a message (e.g., diversion.uri.host, from.uri.host, etc.) the value of the field specified in the Match Type list box can be matched against a; literal value, token, or REGEX.

The following example demonstrates a token match where the URI in the *p-asserted-identity* header is matched against the URI in the *From* header



Condition Rule Table



Match Type	Operation	Match Value Type	Match Value	Description	Primary Key
diversion	Regex	N/A	foo	EXAMPLE 1	1
diversion.uri	Equals	Token	diversion.uri.host	diversion uri = dive...	2
from	Equals	Literal	Ghost		3
p-asserted-identity....	Equals	Token	from.uri	URI Token Match	4
p-asserted-identity....	Equals	Token	from.uri.host	URI Host	5
request-line.uri.hos...	Equals	Literal	192.168.1.72	INVITE URI = 192.168...	6
diversion.uri	Equals	Literal	134.56.77.225		7

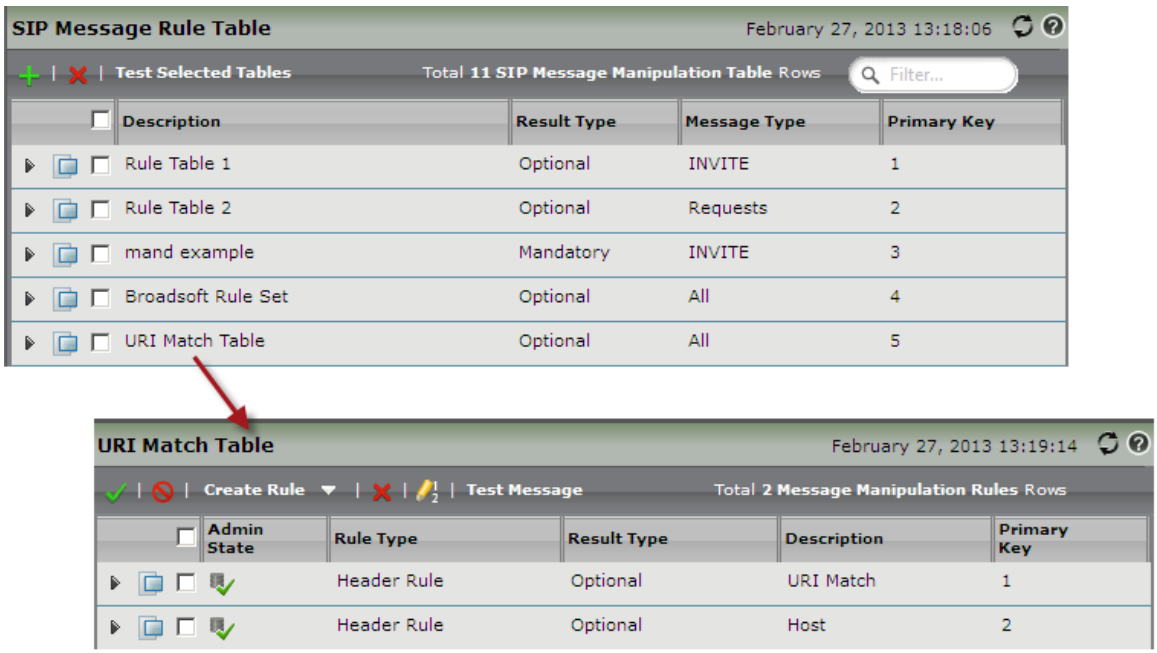
The Condition Rule Table a collection of all the user created Condition Rules.

Message Rule Tables

Copyright © 2015 Sonus Networks. All rights reserved.

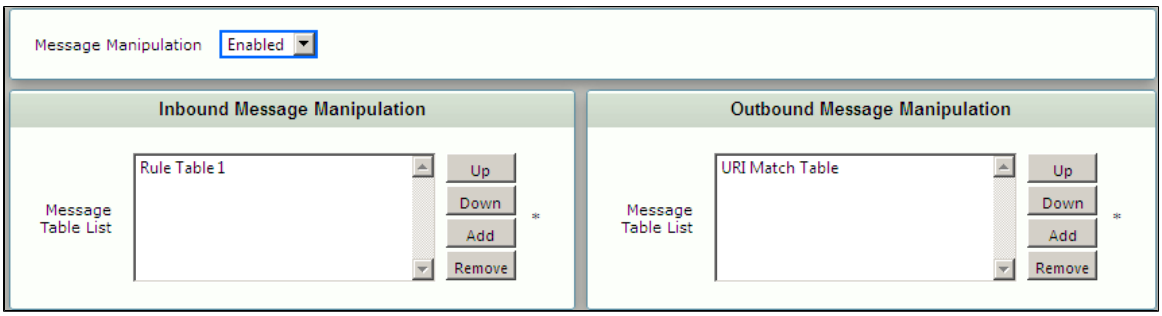
Rule Tables and Condition Rules

Message Rule tables are tables of tables. The *inner* tables are essentially sets (tables) of Condition Rules.



Application of Rule Tables

Message Rule Tables are simply sets of Condition Rules and are applied in SIP Signaling Groups when Message Manipulation is enabled.



Managing Condition Rule Tables

- Creating and Modifying Condition Rules

Managing Message Rule Tables

- Adding and Modifying Entries to Message Rule Tables
  - Creating Header Rules
  - Creating Raw Rules
  - Creating Request Rules
  - Creating Status Rules

Copyright © 2015 Sonus Networks. All rights reserved.

- Testing Message Rules

Using the Condition Expression Builder

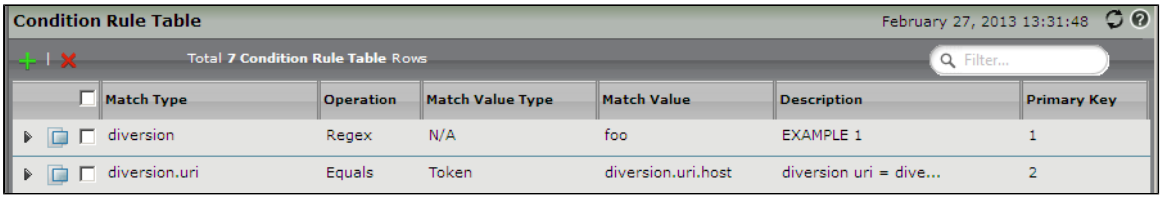
Managing Call Admission Control Profile

Export/Import SIP Message Rule

Exporting and Importing SIP Message Rules

Managing Condition Rule Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Message Manipulation > Condition Rule Table**.



To view a rule's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

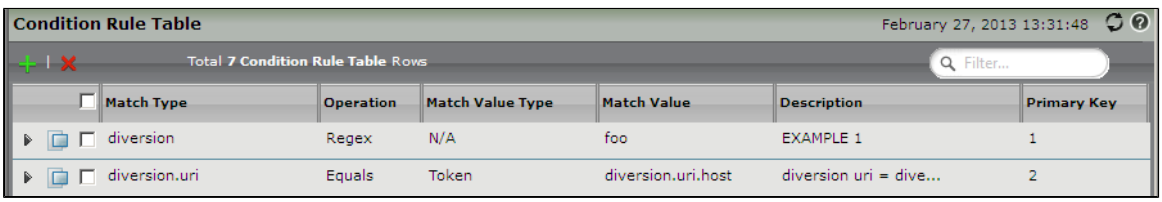
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Condition Rules

Creating and Modifying Condition Rules

To create or modify an existing Condition Rule:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Message Manipulation > Condition Rule Table**.



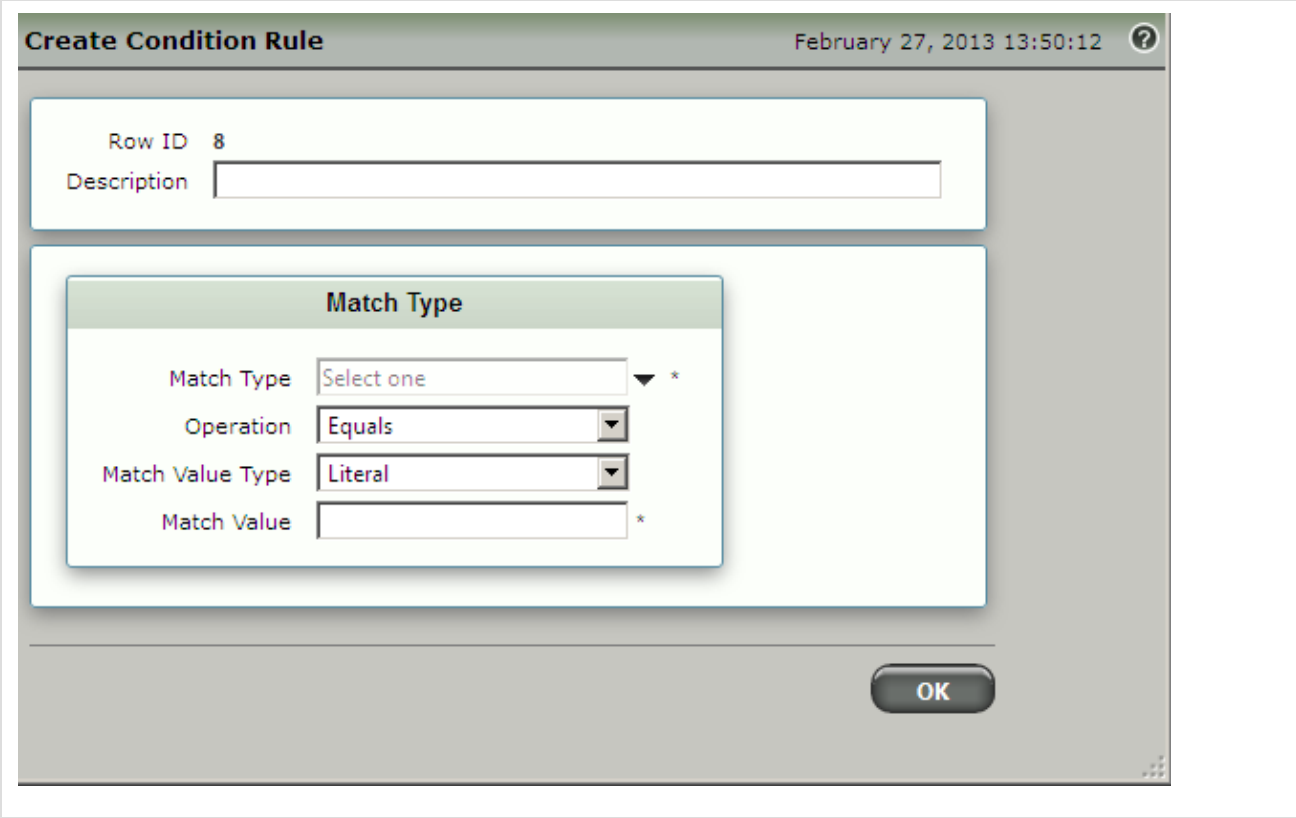
Modifying a Condition Rule

Copyright © 2015 Sonus Networks. All rights reserved.

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a Condition Rule

1. Click the Create ( ) icon at the top of the Condition Rule Table page.



Match Type - Field Properties

Match Type

Specifies the first operand for the logical condition expressed by this rule. The operand must be a parameter tree token identifier.
Example: From.sipuri.username or Contact.sipuri.host

Operation

Specifies the match type for this condition.

Match Value Type

Specifies the value type associated with the second operand.

Match Value

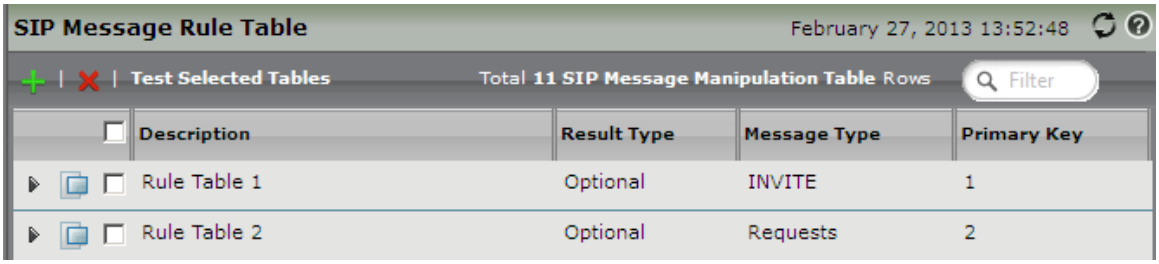
Specifies the value to be matched. Visible only if **Equals** is selected from the **Operation** list box.

Copyright © 2015 Sonus Networks. All rights reserved.

Managing Message Rule Tables

Working with Message Rule Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Message Manipulation > Message Rule Table**.



To view a table entry's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

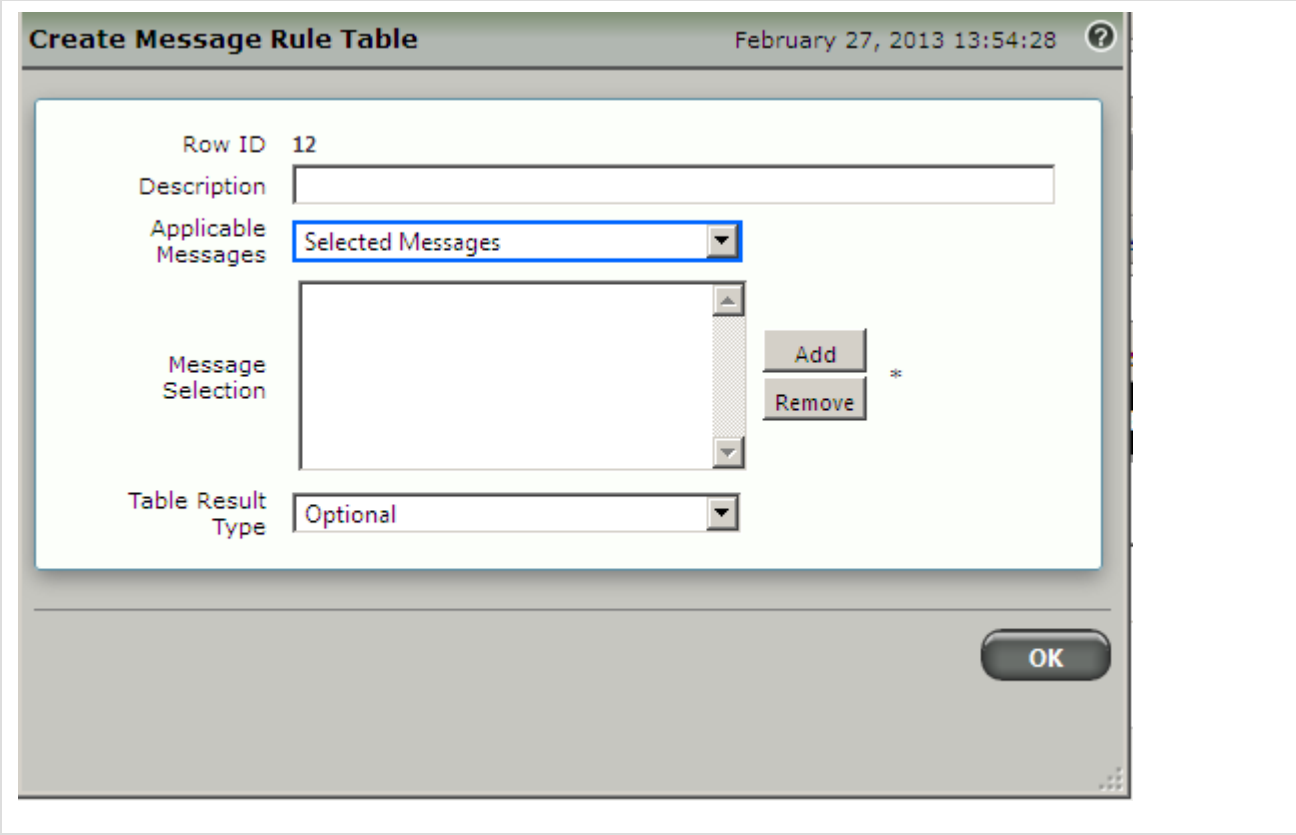
To modify a Message Rule Table:

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

To create a Message Rule Table:

1. Click the **Create Message Rule Table** ( ) icon.

Copyright © 2015 Sonus Networks. All rights reserved.



Message Rule Table Entry - Field Definitions

Applicable Messages

Specifies the message types for which this message table is applicable. For the Selected List option the Message Type List must be provided.

Message Selection

A list of message types to which this table applies. Maximum 20 Message Types. Visible only when Selected Message is chosen from the Applicable Message list box.

Table Result Type

Specifies whether failure of this Message Table causes subsequent Message Tables configured for a given Signaling Group to terminate or not. Optional means subsequent Message Tables will be applied, Mandatory means they will not.

Adding and Modifying Entries to Message Rule Tables

- Creating Header Rules
- Creating Raw Rules
- Creating Request Rules
- Creating Status Rules

Testing Message Rules

Adding and Modifying Entries to Message Rule Tables

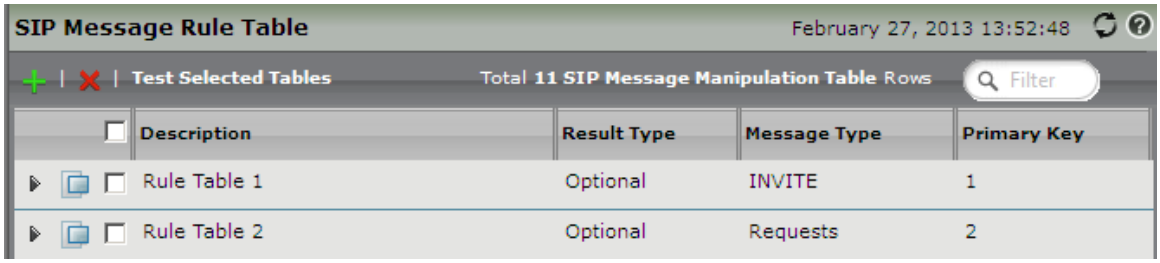
Copyright © 2015 Sonus Networks. All rights reserved.

Four types of rules may be added to a Rule Table:

- Header
- Request
- Status
- Raw

To add or modify an entry to a Message Rule Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Message Manipulation > Message Rule Table**.



Modifying an Entry in a Message Rule Table

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired
3. Click **OK**.

Resequencing an Entry in a Message Translation Table

1. Click the **Resequence** icon ( ) at the top of the table.
2. Select the row(s) you want to move.
3. Click the **Move Selected Rows Up** ( ) or **Move Selected Rows Down** ( ) icon to reposition the row(s) in the table.
4. Click **Apply**.

Adding an Entry to a Message Rule Table

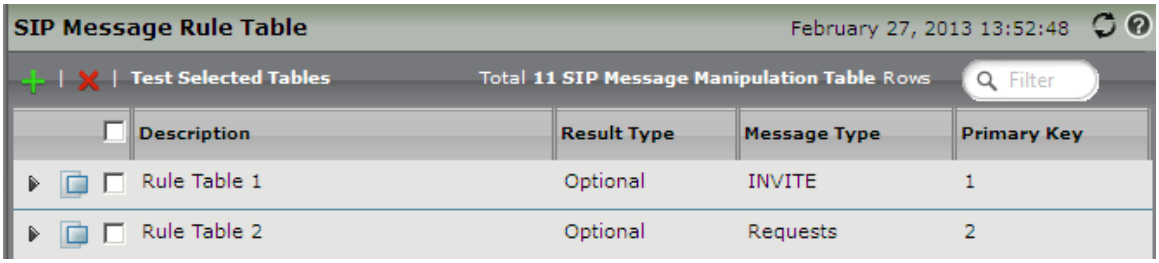
You can add a Message Rule for; all messages, all requests, all responses, or selected messages.
The following pages explain how to add entries for each of these categories.

Creating Header Rules Creating Raw Rules Creating Request Rules Creating Status Rules

Creating Header Rules

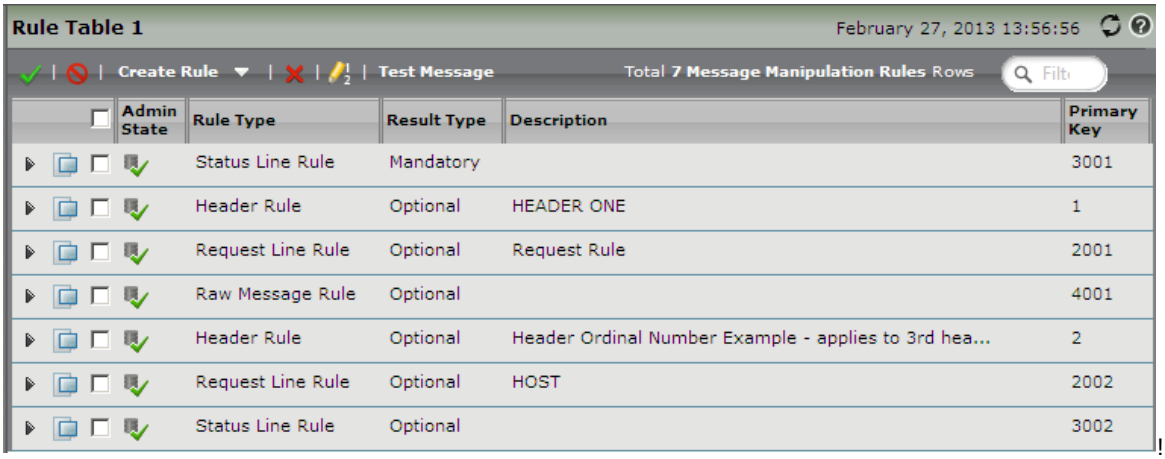
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Message Manipulation > Message Rule Table**.

Copyright © 2015 Sonus Networks. All rights reserved.



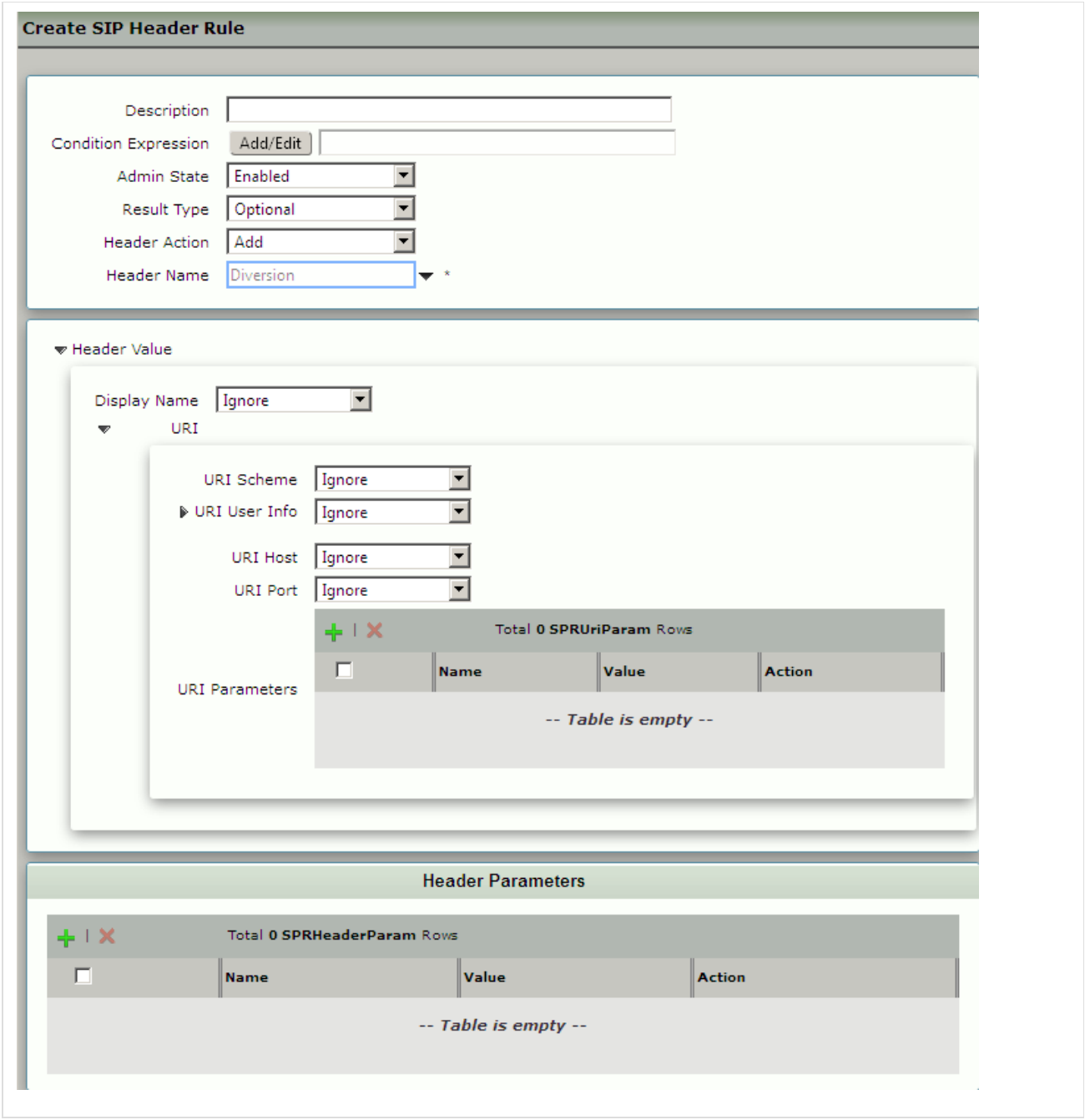
To create a header rule:

1. In the left navigation pane, click the Rule Table entry to which you want to add a Header Rule.



2. From the **Create Rule** drop down box, select **Header Rule**.

Copyright © 2015 Sonus Networks. All rights reserved.



Field Definitions

Condition Expression

Copyright © 2015 Sonus Networks. All rights reserved.

This logical expression is evaluated in order to determine whether the rule should be applied or not. An empty expression is evaluated as unconditionally true.
Example Rule:

```
${1} && (${2} || ${3})
```

Click the **Add/Edit** button to launch the Condition Expression Builder. The Condition Expression Builder enables you to create logical expressions using an interactive interface.

Admin State

Specifies whether or not the rule is enabled.

Result Type

Specifies the whether the true evaluation of the expression is optional or mandatory. Optional means subsequent rules are applied if this rule fails, mandatory means subsequent rules are not applied if this rule fails.

Header Action

Specifies the action applied to the header by this rule if the condition expression evaluates true.

- Add: a header is added to the message by the specified rule (unconditional add: new Header added even if Header type already exists).
- Modify: if the header is present in the message it is modified as specified by this rule. If it is not present, it will not be added.
- Drop: if the header is present, it is dropped from the message.

Header Name

Specifies the type of header referenced by this rule.

Header Ordinal Number

Specifies which of group of the same header to modify. This is only available awhen the header name is: **Contact**, **Route**, **Record-Route**, or **History-Info**.

Header Value

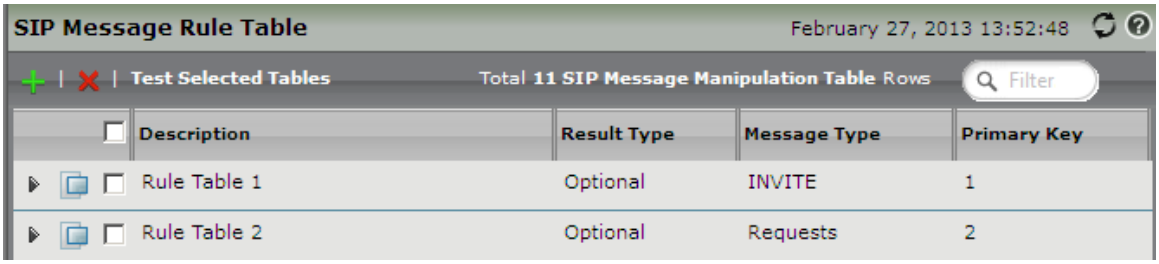
Each type of SIP header varies in its content and structure. The Header Value field holds a value that is provided for the entire header rule, or it can be opened to update its various components in the sub-panels.

Creating Raw Rules

Copyright © 2015 Sonus Networks. All rights reserved.

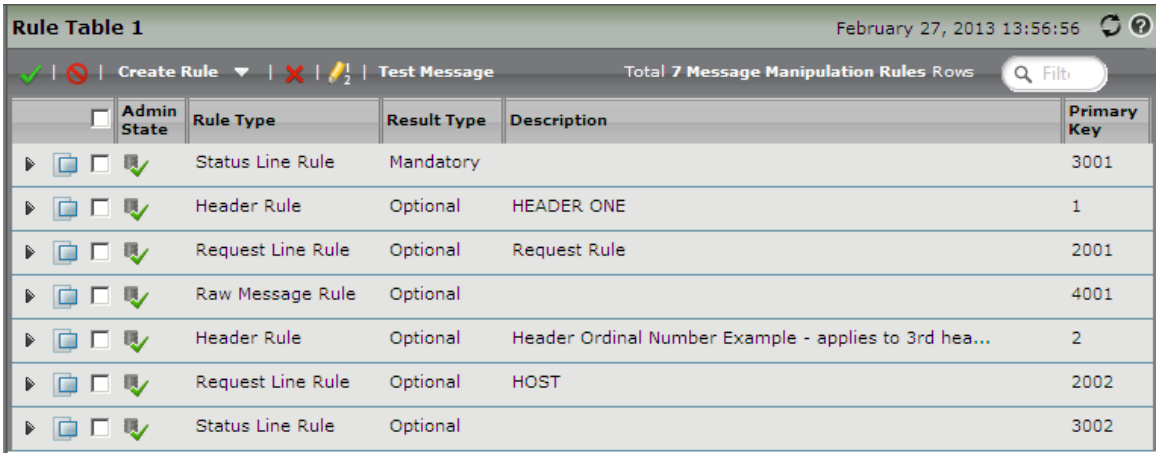
Raw rules allow you to manipulate any string in the entire message; request, headers, and payload. If the condition rule evaluates true, the MME will search the message for content matching the **Match Regex** and replace it with the content specified in the **Replace Regex**.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Message Manipulation > Message Rule Table**.



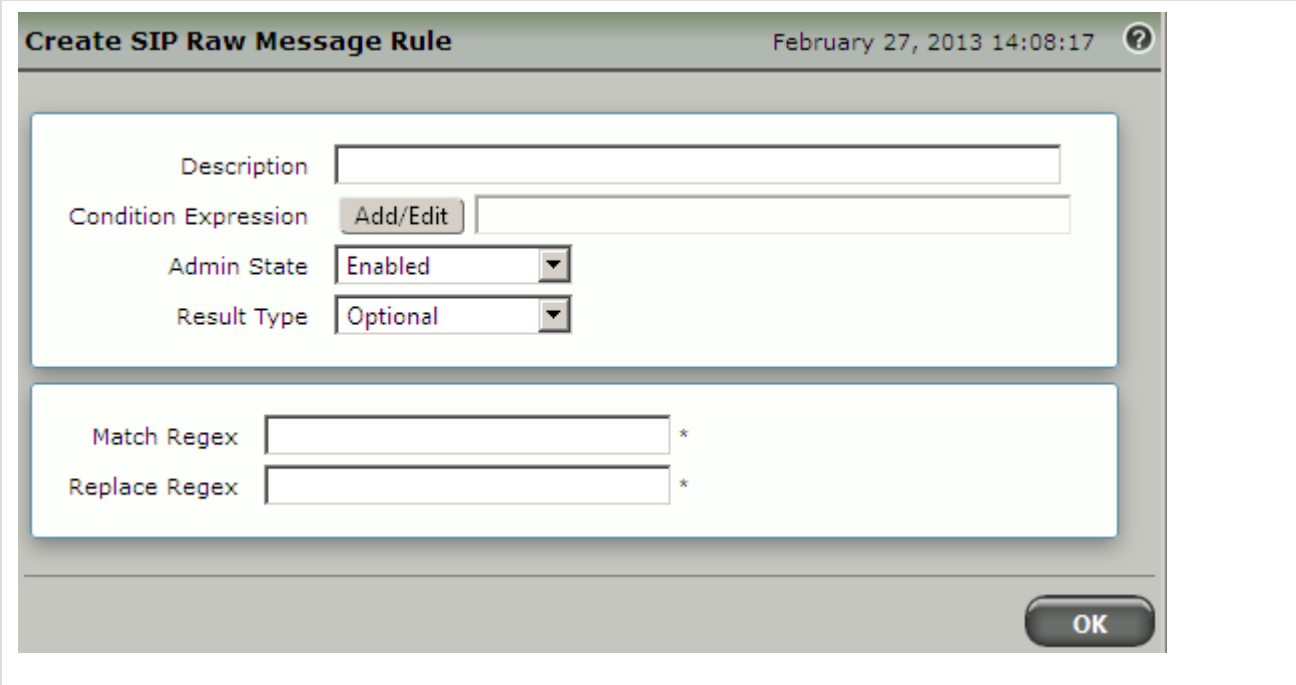
To create a raw rule:

1. In the left navigation pane, click the Rule Table entry to which you want to create a Raw Rule.



2. From the **Create Rule** drop down box, select **Raw Message Rule.**

Copyright © 2015 Sonus Networks. All rights reserved.



Field Descriptions

Condition Expression

This logical expression is evaluated in order to determine whether the rule should be applied or not. An empty expression is evaluated as unconditionally true.
Example Rule:

```
${1} && (${2} || ${3})
```

Click the **Add/Edit** button to launch the Condition Expression Builder. The Condition Expression Builder enables you to create logical expressions using an interactive interface.

Admin State

Specifies whether or not the rule is enabled.

Result Type

Specifies the whether the true evaluation of the expression is optional or mandatory. Optional means subsequent rules are applied if this rule fails, mandatory means subsequent rules are not applied if this rule fails.

Match Regex

The regular expression matched against the original message

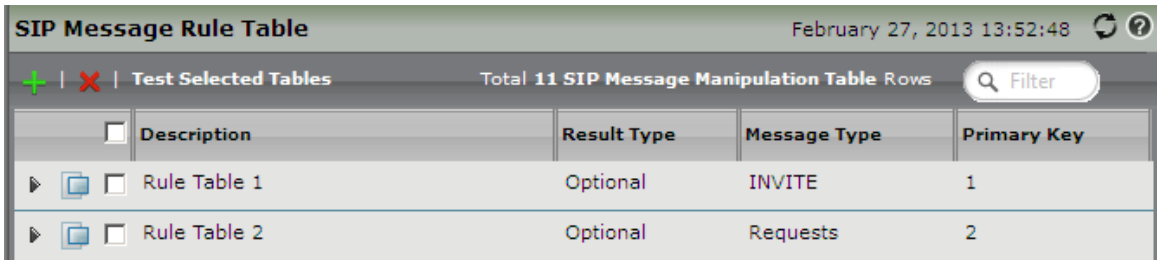
Replace Regex

Copyright © 2015 Sonus Networks. All rights reserved.

The regular expression that replaces the information found in the message by the match regex, if any.

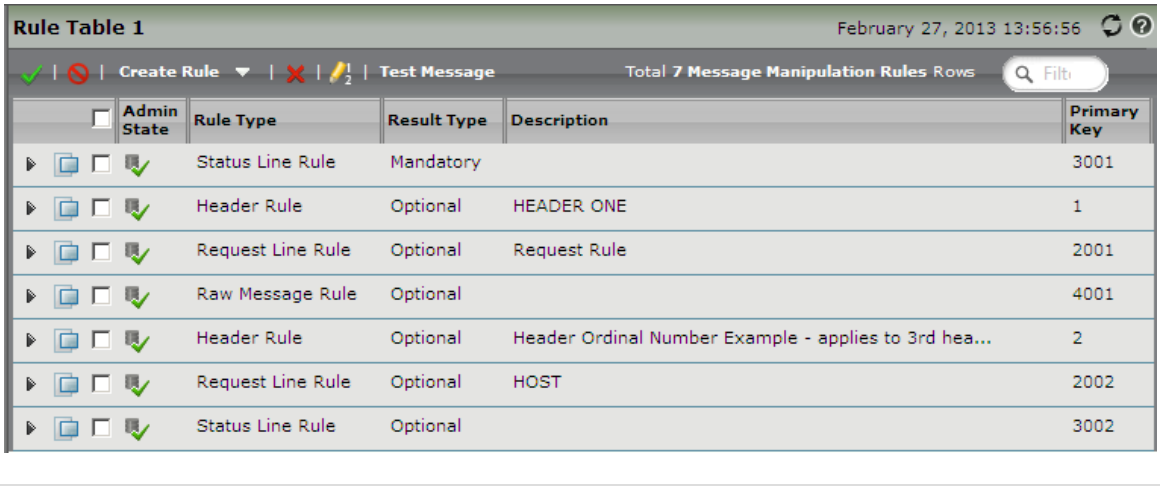
Creating Request Rules

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Message Manipulation > Message Rule Table**.



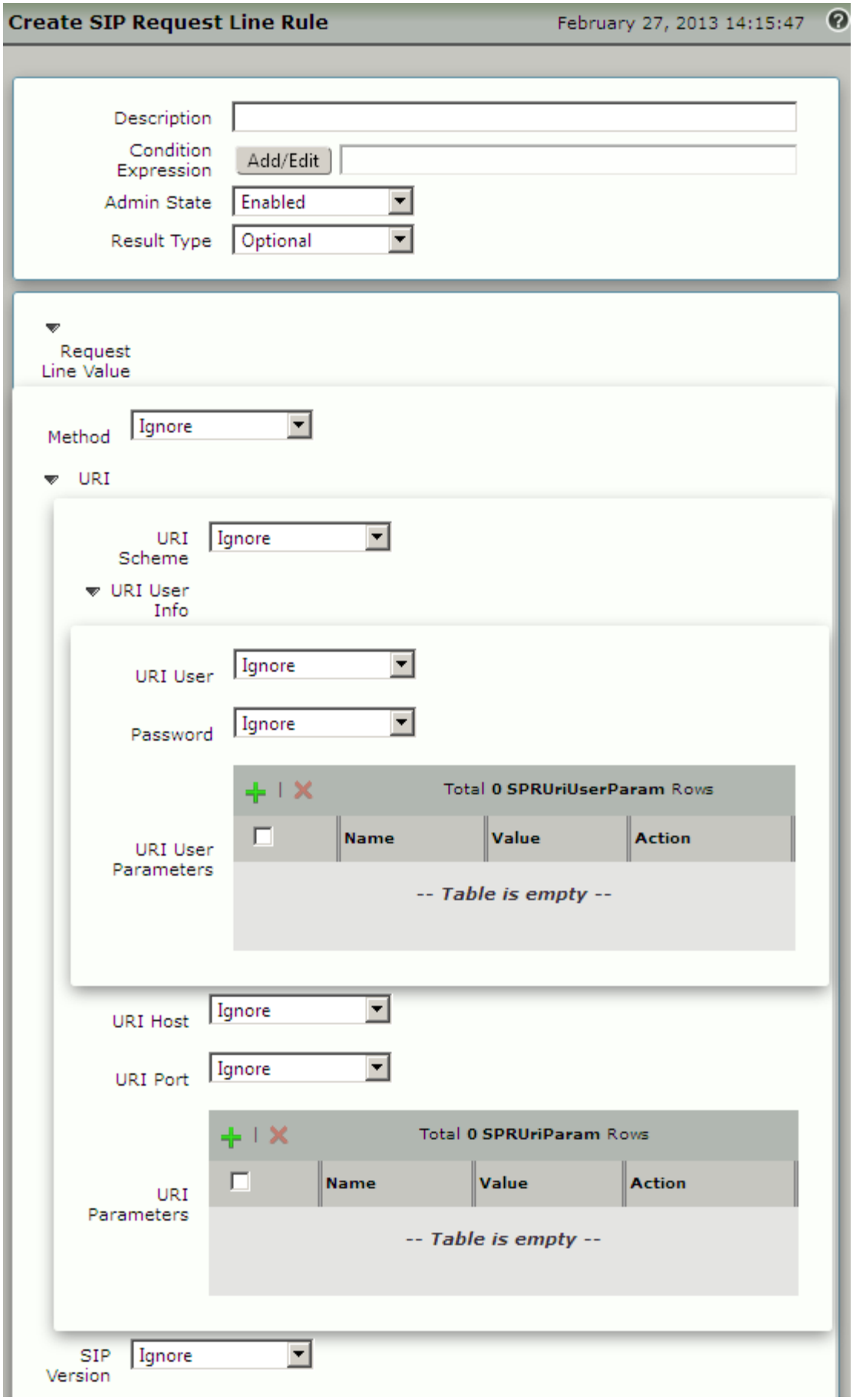
To create a request line rule entry to a table:

1. In the left navigation pane, click the Rule Table entry to which you want to add a Request Line Rule.



2. From the **Create Rule** drop down box, select **Request Line Rule.**

Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.

Field Definitions

Condition Expression

This logical expression is evaluated in order to determine whether the rule should be applied or not. An empty expression is evaluated as unconditionally true.
Example Rule:

```
${1} && (${2} || ${3})
```

Click the **Add/Edit** button to launch the Condition Expression Builder. The Condition Expression Builder enables you to create logical expressions using an interactive interface.

Admin State

Specifies whether or not the rule is enabled.

Result Type

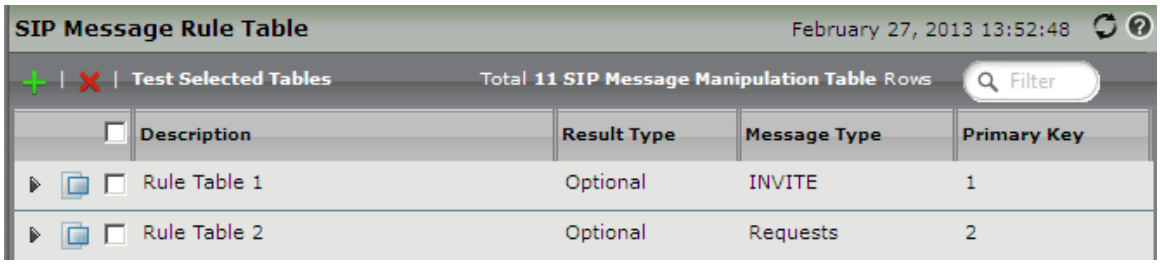
Specifies the whether the true evaluation of the expression is optional or mandatory. Optional means subsequent rules are applied if this rule fails, mandatory means subsequent rules are not applied if this rule fails.

Request Line Value

The Request Line Value holds a value that is provided by the SIP REQUEST. The request can be opened to updates it components in the sub-panels.

Creating Status Rules

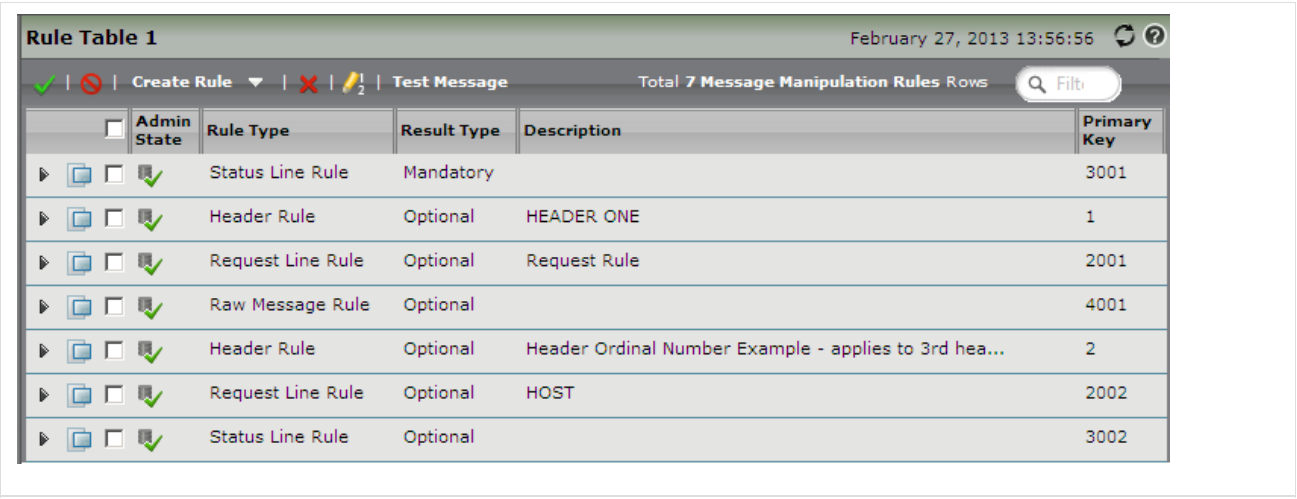
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Message Manipulation > Message Rule Table**.



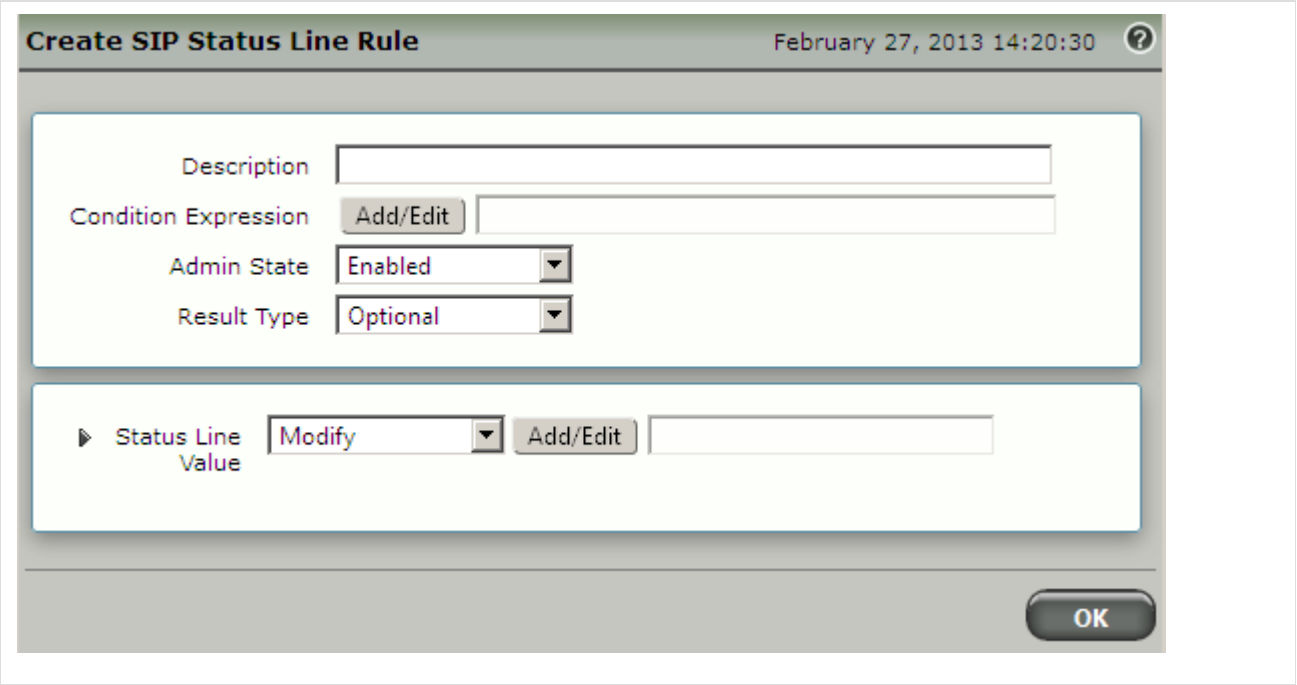
To create a status line rule entry to a table:

1. In the left navigation pane, click the Rule Table entry to which you want to create a Status Line Rule.

Copyright © 2015 Sonus Networks. All rights reserved.



2. From the **Create Rule** drop down box, select **Status Line Rule.**



Field Definitions

Condition Expression

This logical expression is evaluated in order to determine whether the rule should be applied or not. An empty expression is evaluated as unconditionally true.
Example Rule:

```
${1} && (${2} || ${3})
```

Click the **Add/Edit** button to launch the Condition Expression Builder. The Condition Expression Builder enables you to create logical expressions using an interactive interface.

Copyright © 2015 Sonus Networks. All rights reserved.

Admin State

Specifies whether or not the rule is enabled.

Result Type

Specifies the whether the true evaluation of the expression is optional or mandatory. Optional means subsequent rules are applied if this rule fails, mandatory means subsequent rules are not applied if this rule fails.

Status Line Value

The Request Line Value holds a value that is provided by the STATUS message. The request can be opened to updates it components in the sub-panels.

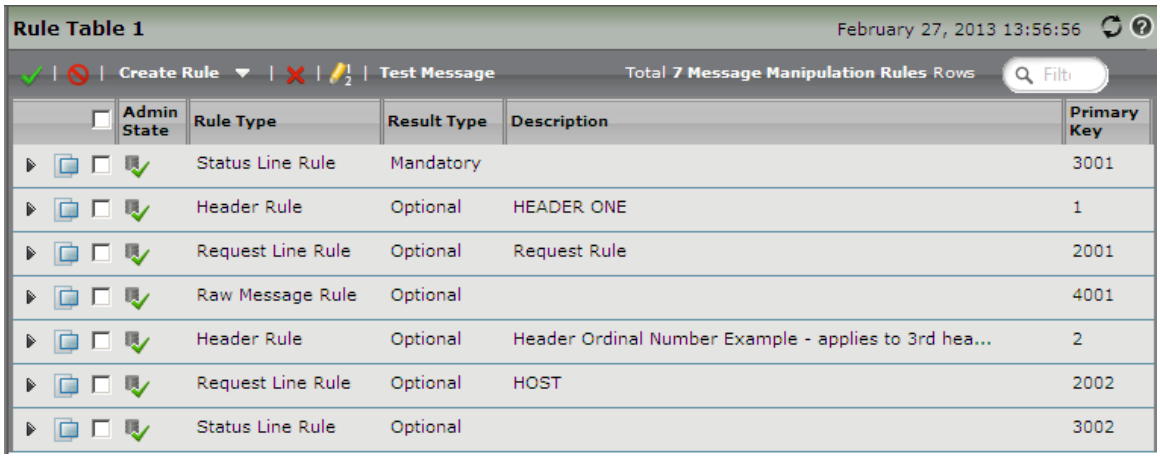
Testing Message Rules

Testing a Message Rule

Once a rule is created, the rules can be applied on a SIP message to see how the manipulation works. The "TestMessage" can be applied to the entire table or a particular rule. The top panel is to provide the raw SIP message. On Apply the parser decodes the raw message, and encodes it. Then the rules are applied and the manipulated message is provided.

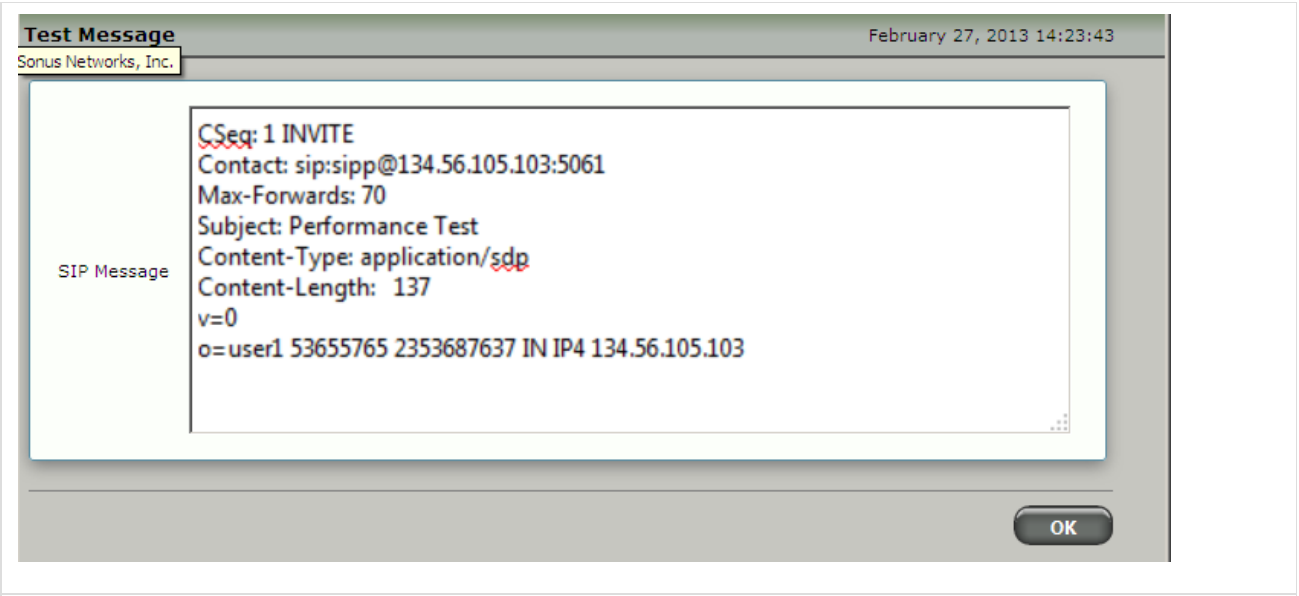
To test a message rule:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Message Manipulation > Message Rule Tables >*Rule Table.***



3. Click the **Test Message**text at the top of the page.

Copyright © 2015 Sonus Networks. All rights reserved.



4. Copy and paste a test message or type a message in the **SIP Message** text field.
5. Click **OK**.



Using the Condition Expression Builder

How the Expression Builder works

> For detailed information about SIP Message Manipulation, see SIP Message Manipulation.

Through the Condition Expression Builder, you can add a Condition Expression to a Message Rule Table. The Expression Builder allows you to combine multiple Condition Rules in a set of expressions (or a single expression) in order to determine whether a rule is executed.

The configured expressions may be nested (maximum nesting level of 3). For example, you can apply Condition1 OR Condition3; the system evaluates the nested OR expression before the outer AND expression.

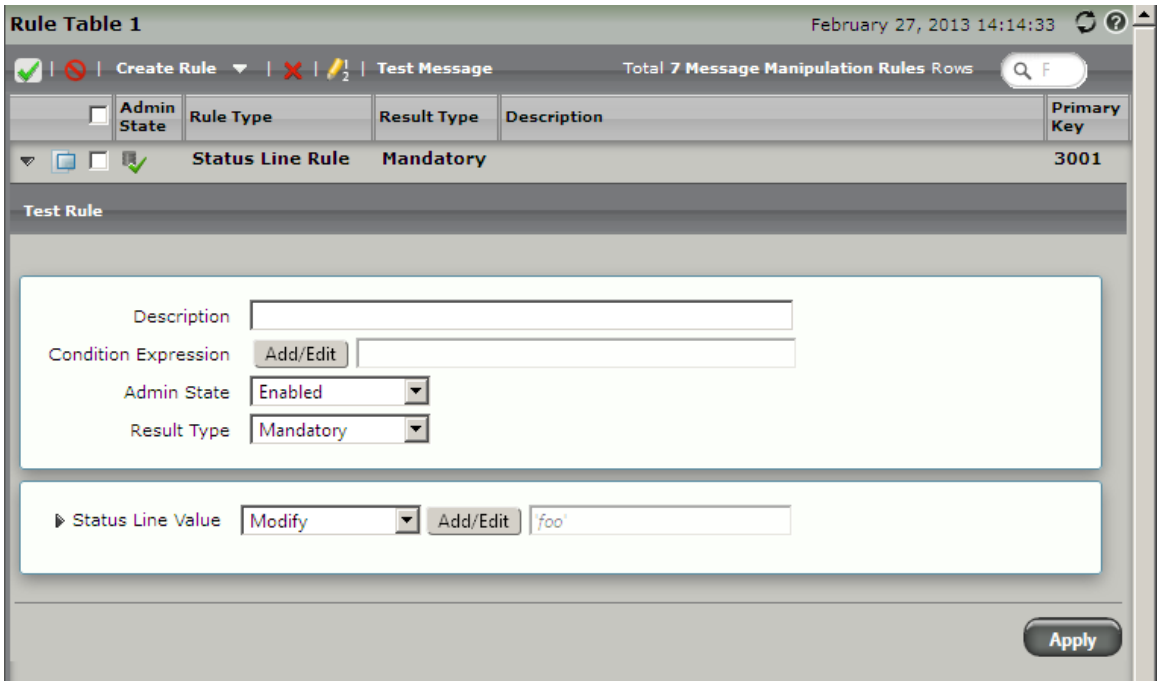
Adding Condition Expression to a Message Rule Table

Copyright © 2015 Sonus Networks. All rights reserved.

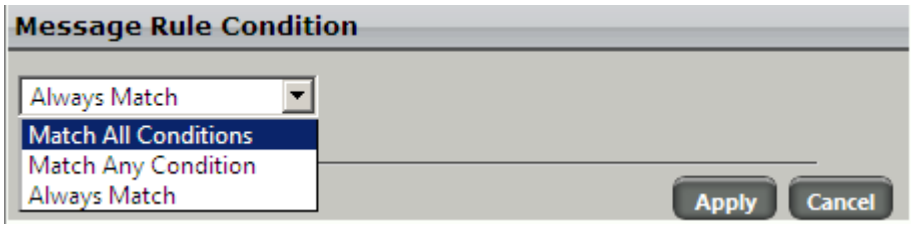
These instructions assume the Message Rule Table has been previously created. For more information about creating a table, see Managing Message Rule Tables.

To add a condition expression to a message rule:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, select **SIP > Message Manipulation > Message Rule Table**. Click the desired Message Rule Table.
3. In the **Settings** tab, click the **expand** (▶) icon next to the entry in which you want to add a Condition Expression.



4. In the Condition Expression field, click **Add/Edit.**



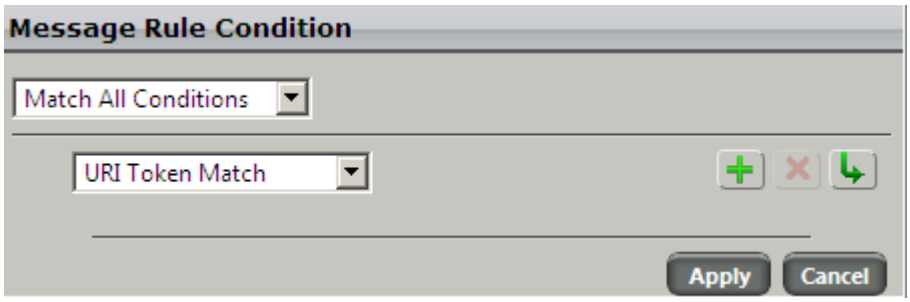
5. From the drop down box, select an option: **Match All Conditions, Match Any Condition**, or **Always Match.** See below for details.

Match Drop Down List Option	Definition
Match Any Conditions	Expression is matched to any conditions that are considered "true"; the condition rule executes if **any** of the selected condition rules are the outermost nesting level are true.

Copyright © 2015 Sonus Networks. All rights reserved.

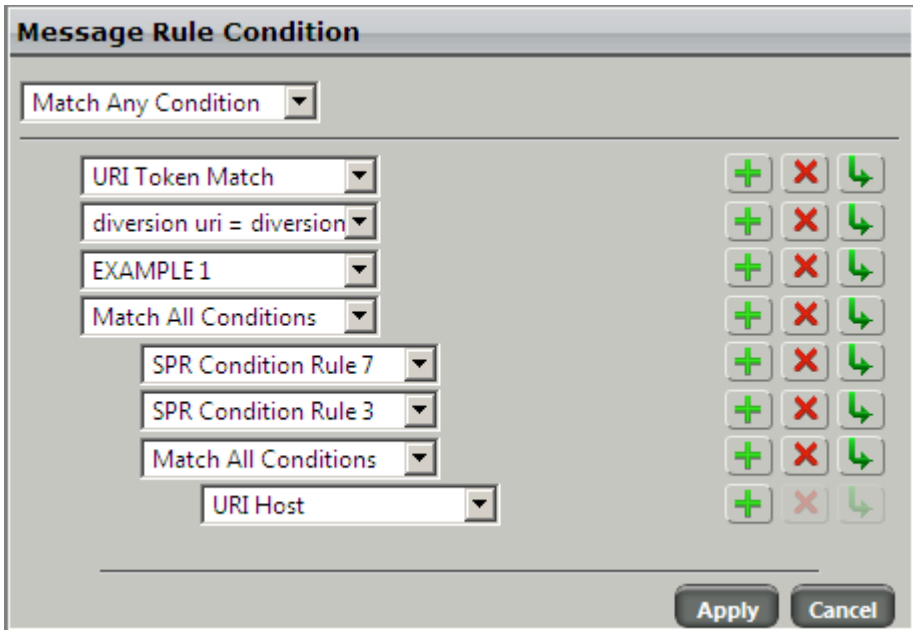
Match All Conditions	Expression is matched to any conditions that are considered "true"; the condition rule executes only if **all** the selected condition rules at the outermost nesting level are true.
Always Match	Expression is unconditional; the condition rule is always matched. When Always Match is selected, Condition Rule options are not visible.

6. Click **Apply**. For **Match Any Conditions** or **Match All Conditions** options, a conditions expression drop down box is displayed. (For **Always Match**, your are returned to the Condition Expression field).
7. Select the desired condition for that rule (this drop down box is generated from the Conditions configured in the Condition Rule Table). See Creating and Modifying Condition Rules.



8. Select subsequent condition rules (if applicable). See below for how to use the window options.

> You can add up the 3 nesting levels for each condition, for an aggregate total of 10 rows.



Condition Option	How to Use
Condition Drop down Box	Select expression from the drop down box.The options are derived from the entries in the Condition Rule Table. See Managing Condition Rule Tables. For each additional condition selected, the Match All/Any Condition drop down is displayed.

Copyright © 2015 Sonus Networks. All rights reserved.

+	Adds a new condition rule directly beneath the current row. A maximum of 10 rows is supported. This icon is disabled when the maximum of 10 rows is reached.
✕	Deletes the selected condition rule or Match All/Any Condition. If a Match All/Any condition is selected, all condition rules within that group are also removed. This icon is disabled for condition rule rows which are the only member of a Match All/Any group. Click the "X" at the group level to remove the entire group.
↳	Adds a group directly underneath the current row, and also adds one condition rule row to that group. This icon is disabled for any rows which are at the deepest-allowed nesting level.

Managing Call Admission Control Profile

Overview

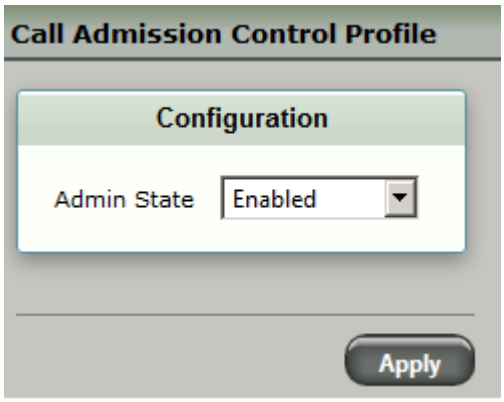
A Call Admission Profile provides SIP level call admission control by regulating call attempts per second, and the rate of new invite/non-invite sessions. Once the SBC limits are met, SIP will no longer accept/issue new invite or non-invite sessions (except 911 calls). This feature protects the SBC from overload conditions (an overload condition is detected if the average rate of invite and non-invite sessions exceeds the pre-determined limit or the CPU threshold is exceeded). It also prevents internal/external DOS attacks in an otherwise normal network using overload detection and resource leaks/malfunction detection.

When rejecting calls or sessions on account of admission-control, SBC sends "480 Temporarily Unavailable" response to the peers.

> This functionality applies to SIP calls only.

Managing Call Admission Control

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP> Call Admission Control Profile.** The **Call Admission Control Profile** window is displayed.
3. From the **Admin State** drop down box, select **Enable** (default; enables Call Control feature) or **Disable** (disables Call Control feature).
4. Click **Apply.**



Export/Import SIP Message Rule

- Overview
- Export SIP Message Rule

Copyright © 2015 Sonus Networks. All rights reserved.

- Import SIP Message Rule

Overview

The SIP Message Rule option enables you to export/import SIP Message Manipulation (SMM) rules. This function allows the SMM rules to be moved from one node to another, which eliminates re-configung multiple nodes with the same configuration. Rules can be exported/imported from a selected Message Table or Signaling Group. This task will export all required data, including any condition rules associated with the message rules (condition rules are simple rules that apply to a specific component of a message, such as diversion.uri.host, from.uri.host, etc.)

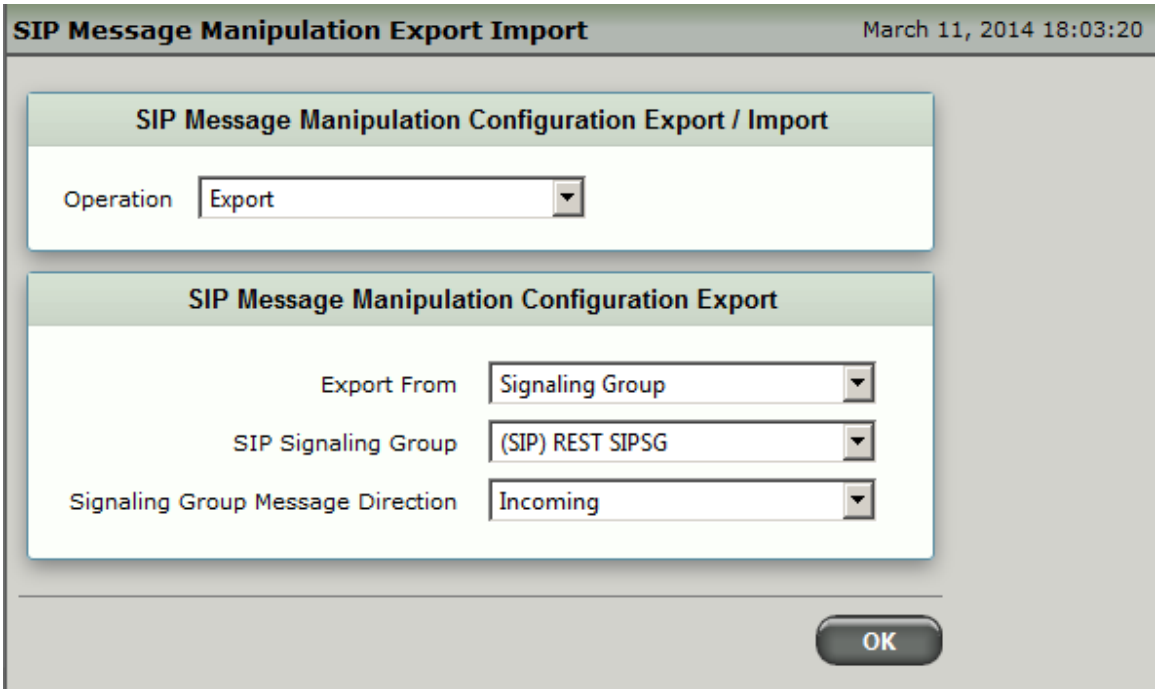
See SIP Message Manipulation for how SIP Message Rules and Condition Rules are used with SIP messages.

Export SIP Message Rule

To export a SIP Message Rule

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, go to **SIP Setup > SIP Message Rule.**
3. Enter the configuration. See SIP Message Manipulation Configuration Export - Field Properties.
4. Click **OK**. A message asks you to confirm export of the SIP configuration.
5. Click **OK**. A message asks you to save the file (file name is **SMMConfiguration.xml**). Select a location and save. This saved location will be used when you import this configuration file to another node. See Import SIP Message Rule.
6. Perform a save and click **OK**.

Export SIP Message Rule



Import SIP Message Rule

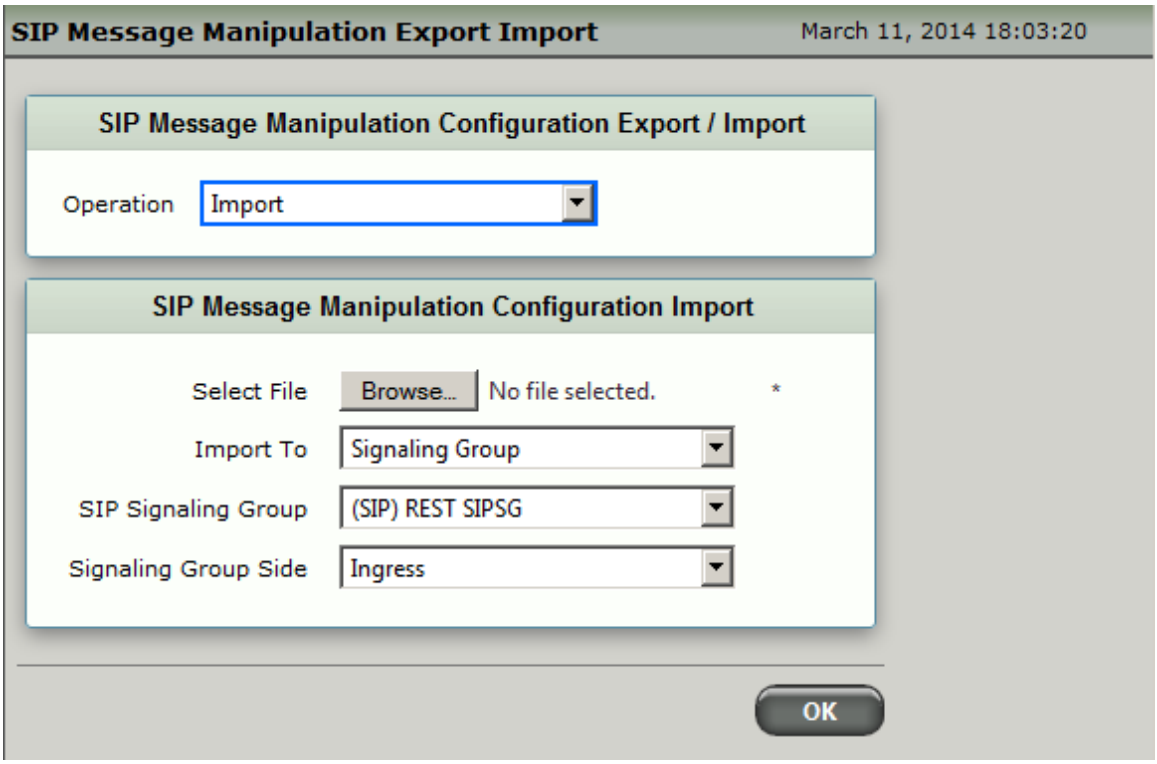
> The imported SIP Message manipulation rules will override the existing configuration in the SBC.

To import a SIP Message Rule

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, go to **SIP Setup > SIP Message Rule.**
3. Enter the configuration. See SIP Message Manipulation Configuration Import - Field Properties.
4. Click **Browse** to select the **SMMconfiguration.xml** file (located in the directory in which you saved the exported configuration file, see Export SIP Message Rule).
5. Click **OK**. A message asks you to confirm import of the SIP configuration.
6. Click **OK**. The **SMMConfiguration.xml** file is imported into the SBC and overwrites the existing configuration.

Import SIP Message Rule



SIP Message Manipulation Configuration Export/Import - Field Properties

Operation

Determines whether the SBC will import or export the SIP Message Manipulation rules. Select from the drop down list. Valid entries: **Export** or **Import**.

Depending on the option chosen, specific configuration fields are displayed. These are noted below.

SIP Message Manipulation Configuration Export - Field Properties

The fields below are displayed when **Export** is selected from the **Operation** drop down list. These fields define the configuration required for exporting Sip Manipulation Message rules. The rules are exported into a file, which can then be imported into another node.

Export From

Determines from where the SIP Message Manipulation rules are exported. Select from the drop down list. Available options: **Signaling Group** or **Message Table**. Depending on the option you choose, specific configuration fields are displayed.

Copyright © 2015 Sonus Networks. All rights reserved.

SIP Signaling Group

Allows you to choose the SIP Signaling group from which the SIP Message Manipulation rules are exported. The options in this drop down list are generated from the SIP Signaling Groups already created in the SBC. This field is available only when **Signaling Group** is selected from the **Export From** drop down list. For more information about creating SIP Signaling Groups, see Creating and Modifying SIP Signaling Groups.

Signaling Group Message Direction

For the selected Signaling Group, determines the message direction from which SIP Message Manipulation rules are exported. Select from the drop down list. Valid entry: **Incoming** or **Outgoing**.

SIP Message Manipulation Configuration Import - Field Properties

The fields below are displayed when **Import** is selected from the **Operation** drop down list. These fields define the configuration for importing SIP Message Manipulation rules. Rules are imported from a filethat were previously exported.

Select File

Selects the file from which the SIP Manipulation Message rules are imported. Click the **Browse...** button and locate **SMMConfiguration.xml** (this file contains the SIP Message Manipulation rules that was previously exported from another node, see Export). Click **OK**.

Import To

Determines the location to which the SIP Message Manipulation rules are imported. Select from the drop down list. Available options: **Signaling Group** or **Message Table**. Depending on the option you choose, specific configuration fields are displayed.

SIP Signaling Group

Determines the SIP Signaling Group to which the SIP Message Manipulation rules are imported. The options in this drop down list are generated from the SIP Signaling Groups already created in the SBC. This field is available only when **Signaling Group** is selected from the **Import To** drop down list. For more information about creating SIP Signaling Groups, see Creating and Modifying SIP Signaling Groups .

Signaling Group side

For the selected Signaling Group, determines the signaling side to which SIP Message Manipulation rules are imported. Select from the drop down list. Valid entry: **Ingress** or **Egress**.

Exporting and Importing SIP Message Rules

- Overview
- Export SIP Message Rule
- Import SIP Message Rule

Copyright © 2015 Sonus Networks. All rights reserved.

Overview

The SIP Message Rule option enables you to export/import SIP Message Manipulation (SMM) rules. This function allows the SMM rules to be moved from one node to another, which eliminates re-configung multiple nodes with the same configuration. Rules can be exported/imported from a selected Message Table or Signaling Group. This task will export all required data, including any condition rules associated with the message rules (condition rules are simple rules that apply to a specific component of a message, such as diversion.uri.host, from.uri.host, etc.)

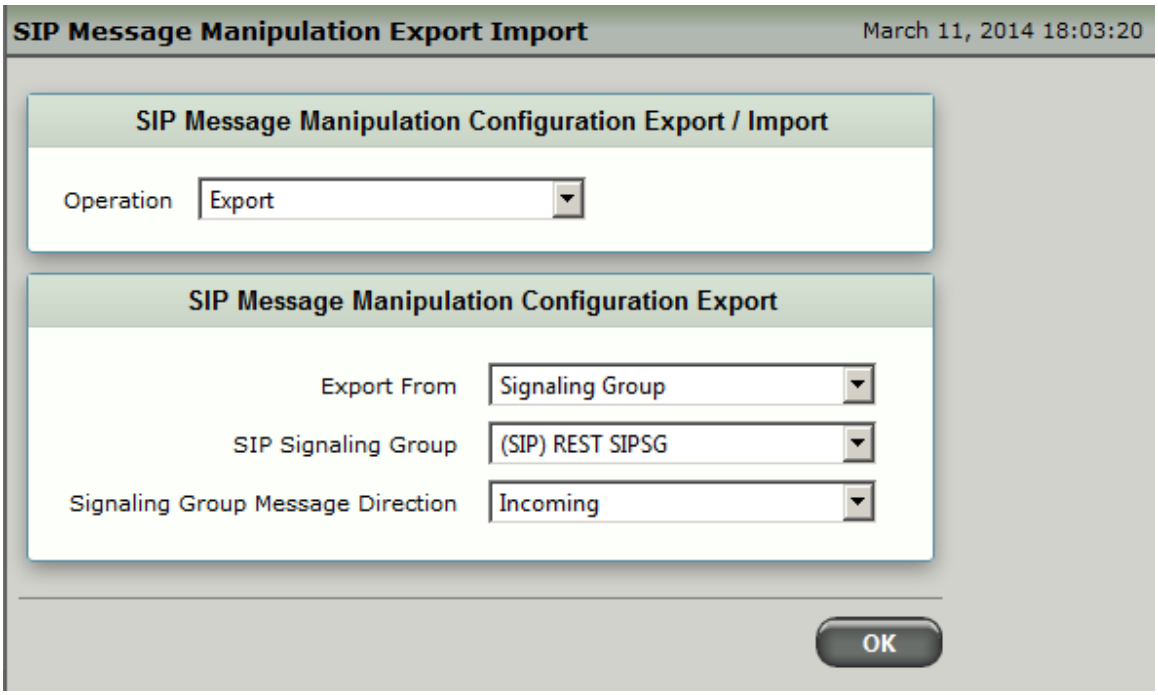
See SIP Message Manipulation for how SIP Message Rules and Condition Rules are used with SIP messages.

Export SIP Message Rule

To export a SIP Message Rule

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, go to **SIP Setup > SIP Message Rule.**
3. Enter the configuration. See SIP Message Manipulation Configuration Export - Field Properties.
4. Click **OK**. A message asks you to confirm export of the SIP configuration.
5. Click **OK**. A message asks you to save the file (file name is **SMMConfiguration.xml**). Select a location and save. This saved location will be used when you import this configuration file to another node. See Import SIP Message Rule.
6. Perform a save and click **OK**.

Export SIP Message Rule



Import SIP Message Rule

> ⚠ The imported SIP Message manipulation rules will override the existing configuration in the SBC.

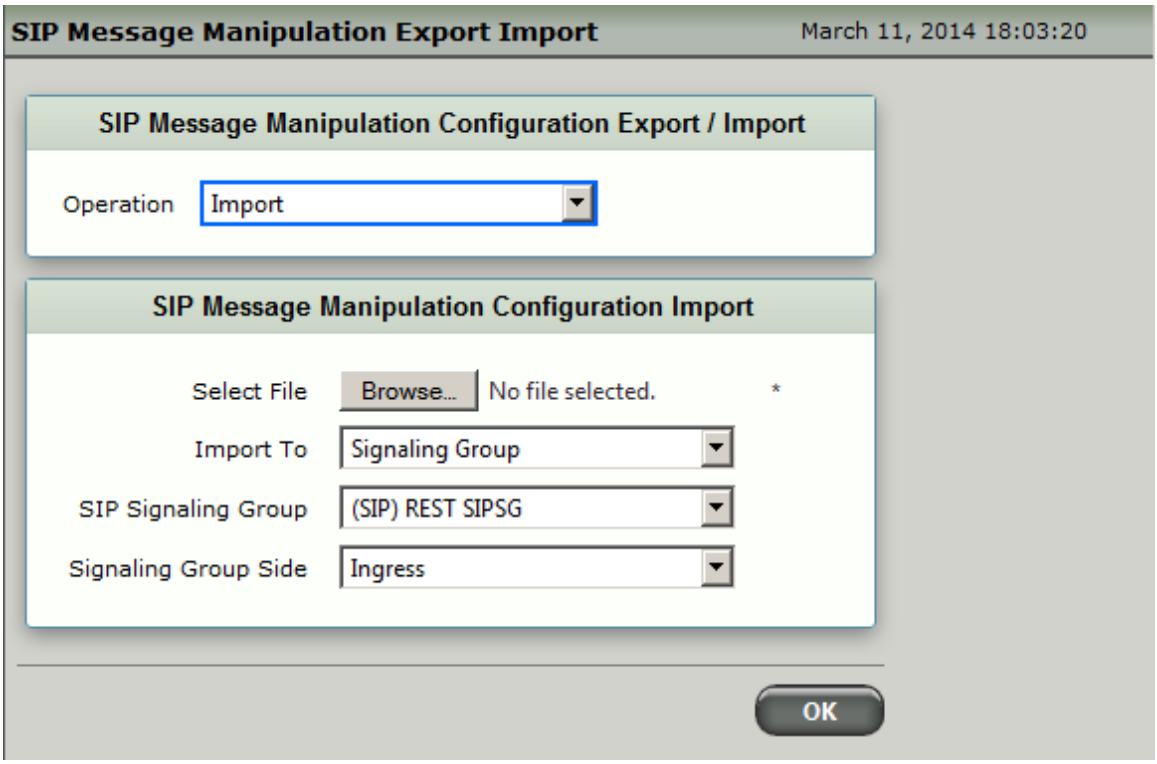
To import a SIP Message Rule

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, go to **SIP Setup > SIP Message Rule.**

Copyright © 2015 Sonus Networks. All rights reserved.

3. Enter the configuration. See SIP Message Manipulation Configuration Import - Field Properties.
4. Click **Browse** to select the **SMMconfiguration.xml** file (located in the directory in which you saved the exported configuration file, see Export SIP Message Rule).
5. Click **OK**. A message asks you to confirm import of the SIP configuration.
6. Click **OK**. The **SMMConfiguration.xml** file is imported into the SBC and overwrites the existing configuration.

Import SIP Message Rule



SIP Message Manipulation Configuration Export/Import - Field Properties

Operation

Determines whether the SBC will import or export the SIP Message Manipulation rules. Select from the drop down list. Valid entries: **Export** or **Import**.

Depending on the option chosen, specific configuration fields are displayed. These are noted below.

SIP Message Manipulation Configuration Export - Field Properties

The fields below are displayed when **Export** is selected from the **Operation** drop down list. These fields define the configuration required for exporting Sip Manipulation Message rules. The rules are exported into a file, which can then be imported into another node.

Export From

Determines from where the SIP Message Manipulation rules are exported. Select from the drop down list. Available options: **Signaling Group** or **Message Table**. Depending on the option you choose, specific configuration fields are displayed.

SIP Signaling Group

Copyright © 2015 Sonus Networks. All rights reserved.

Allows you to choose the SIP Signaling group from which the SIP Message Manipulation rules are exported. The options in this drop down list are generated from the SIP Signaling Groups already created in the SBC. This field is available only when **Signaling Group** is selected from the **Export From** drop down list. For more information about creating SIP Signaling Groups, see Creating and Modifying SIP Signaling Groups.

Signaling Group Message Direction

For the selected Signaling Group, determines the message direction from which SIP Message Manipulation rules are exported. Select from the drop down list. Valid entry: **Incoming** or **Outgoing**.

SIP Message Manipulation Configuration Import - Field Properties

The fields below are displayed when **Import** is selected from the **Operation** drop down list. These fields define the configuration for importing SIP Message Manipulation rules. Rules are imported from a filethat were previously exported.

Select File

Selects the file from which the SIP Manipulation Message rules are imported. Click the **Browse...** button and locate **SMMConfiguration.xml** (this file contains the SIP Message Manipulation rules that was previously exported from another node, see Export). Click **OK**.

Import To

Determines the location to which the SIP Message Manipulation rules are imported. Select from the drop down list. Available options: **Signaling Group** or **Message Table**. Depending on the option you choose, specific configuration fields are displayed.

SIP Signaling Group

Determines the SIP Signaling Group to which the SIP Message Manipulation rules are imported. The options in this drop down list are generated from the SIP Signaling Groups already created in the SBC. This field is available only when **Signaling Group** is selected from the **Import To** drop down list. For more information about creating SIP Signaling Groups, see Creating and Modifying SIP Signaling Groups .

Signaling Group side

For the selected Signaling Group, determines the signaling side to which SIP Message Manipulation rules are imported. Select from the drop down list. Valid entry: **Ingress** or **Egress**.

Miscellaneous Topics

Resequencing Tables

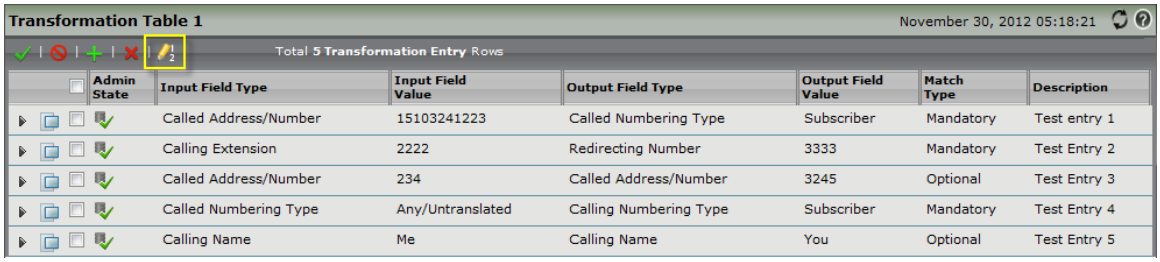
The Multiselect Widget

Resequencing Tables

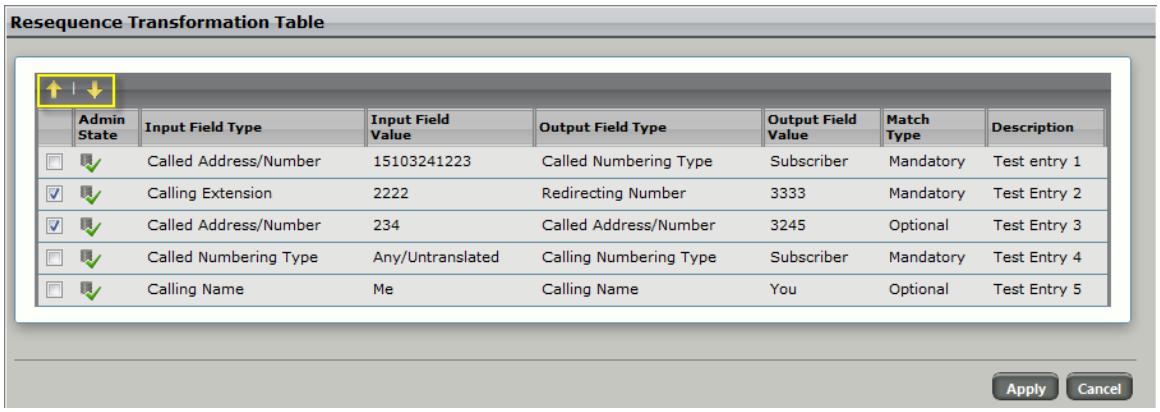
Copyright © 2015 Sonus Networks. All rights reserved.

The process for resequencing a table is the same for all tables on the SBC.

To resequence a table:

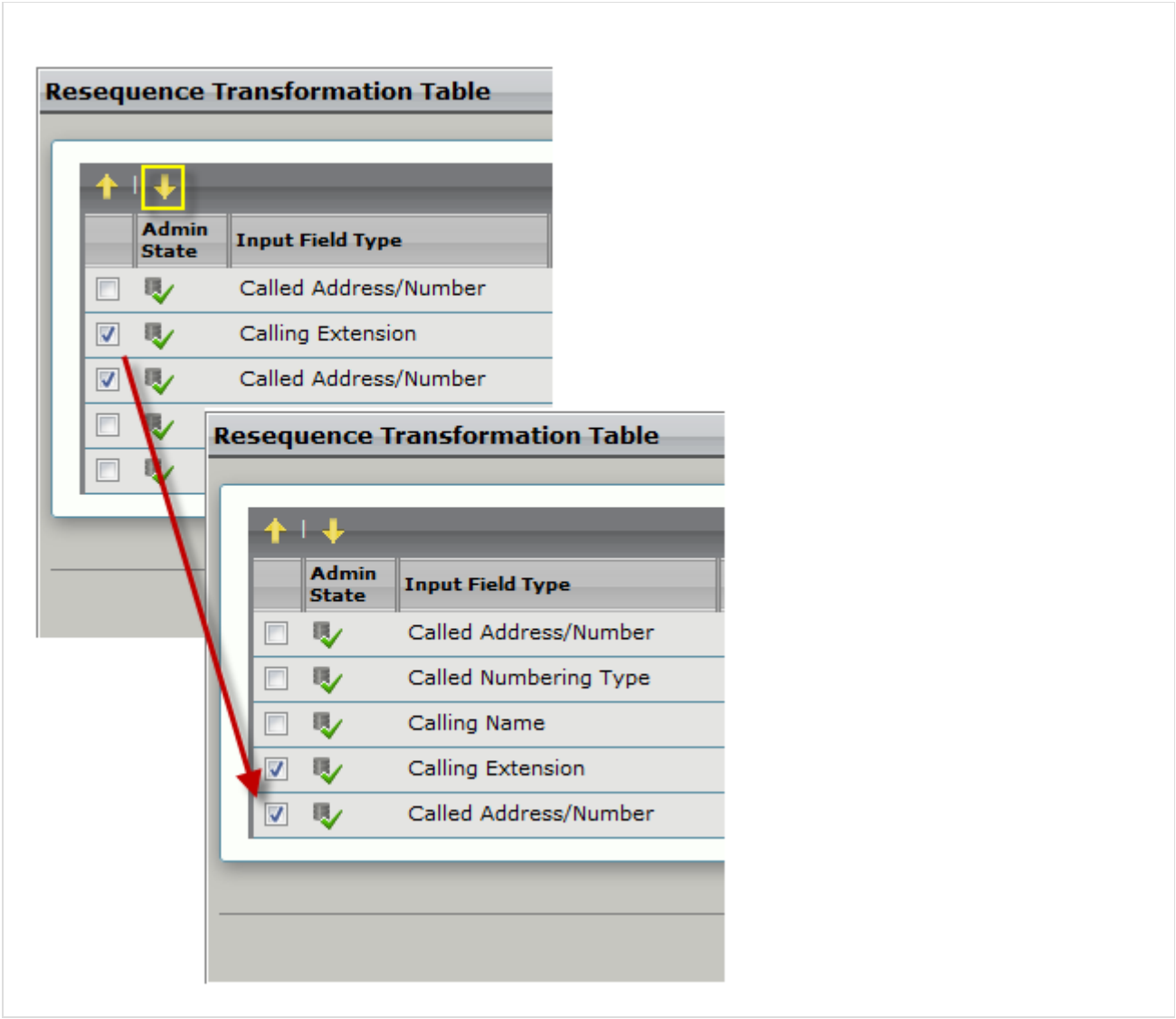


1. click the **Resequence** icon ( ) at the top of the table.



2. Select the row(s) you want to move.
3. Click the **Move Selected Rows Up** ( ) or **Move Selected Rows Down** ( ) icon to reposition the row(s) in the table.
4. Click **Apply**.

Copyright © 2015 Sonus Networks. All rights reserved.



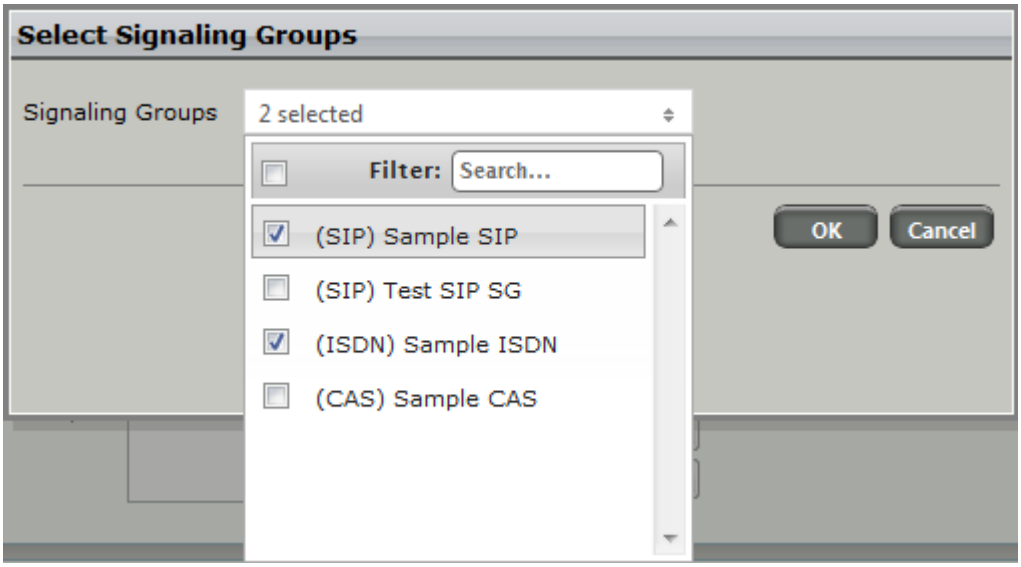
The Multiselect Widget

This page describes the functionality of the multiselect widget used on a number of pages in the SBC 1000/2000 User Interface. The multiselect widget found on a number of pages in the SBC 1002/2000 User Interface (UI) allows you to select one or more items from the list.

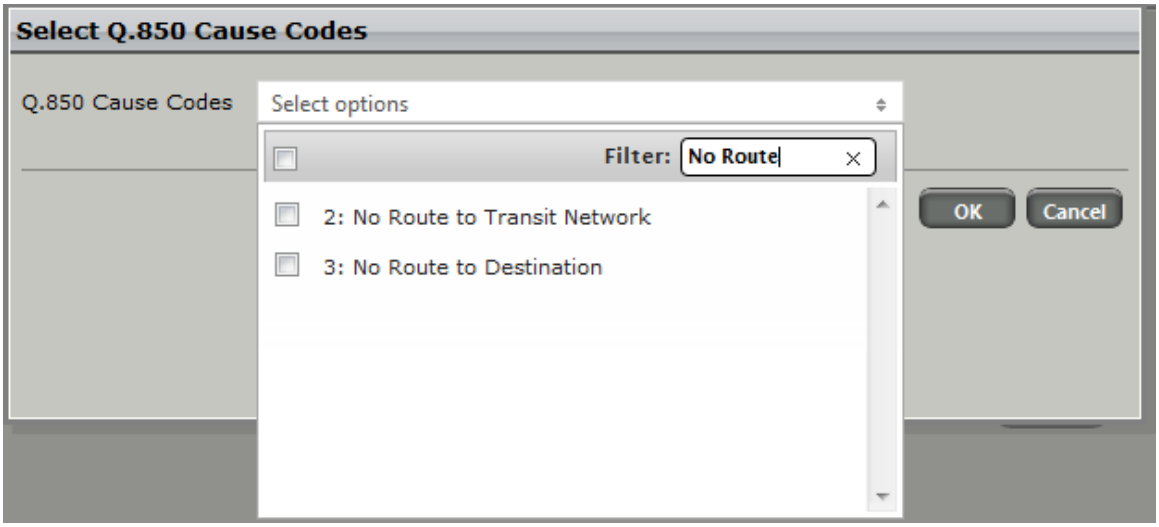
Selecting Items in the List

- To select an item(s) simply select the check box next to the item to be included in the list

Copyright © 2015 Sonus Networks. All rights reserved.



- The Multiselect widget include a search feature, use this to search for an item(s) in a large list (e.g., Cause Codes) by entering part of all of an item's name.



- Select the check boxes next to the desired items and click **OK**.

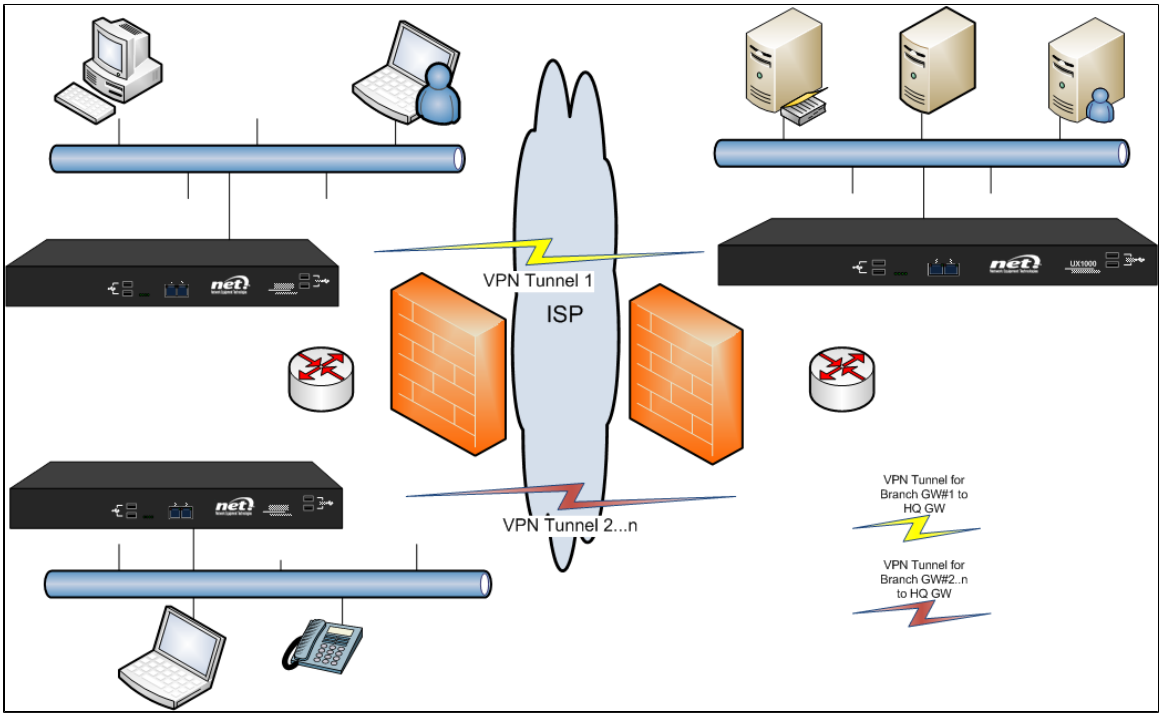
Working with IPsec

The SBC supports two methods of peer authentication for each connection name entry in the connection table: digital certificate/PKI-based authentication, and pre-shared key. IPsec allows the branch office SBC to reside behind the corporate firewall by means of VPN tunneling. IPsec tunneling is also an enabling technology for the 3G/4G Branch Survivability feature.

> **Note:** The IPsec feature is implemented as a means of establishing IPsec tunnels in support of the Branch Survivability feature. IPsec tunneling is NOT a stand-alone feature at this time.

Overview

Copyright © 2015 Sonus Networks. All rights reserved.



The diagram depicts a VPN connection(IPsec tunnel) between the local and remote subnets as site-to-site tunneling on SBC gateways. Traffic between the trusted subnet networks is tunneled to fully encapsulate the packets on its way across an untrusted network, protected by both encryption and authentication.

Managing IPsec Tunnels

- Creating and Modifying IPsec Tunnel Entries

Configuring a Site to Site IPsec between the SBC Gateways

Viewing IPsec Statistics

Managing IPsec Tunnels

Prerequisites

Before you can create an IPsec Tunnel Entry you must have done the following:

- A Sonus SBC Certificate and Trusted CA Certificate must be obtained and imported to the SBC when **Certificate** is selected **Authentication Mode** list box in the **Authentication Parameters** panel. Refer to Working with Certificates for information about configuring certificates on the SBC.
- An IPsec license is required to manage IPsec tunnels.

Copyright © 2015 Sonus Networks. All rights reserved.

Important Information for Previous SIP-TLS Users:

- When upgrading to version 3.0 existing Sonus SBC Certificates will fail authentication due to *key integrity verification errors* when used to bring up the IPsec tunnel in the **Certificate** authentication mode.
- Before beginning to manage an IPsec tunnel for **Certificate** authentication, you must generate a new Certificate Signing Request (CSR), re-sign, and re-import a new Sonus SBC Certificate.

Note: Multiple Tunnel Configuration

- **Branch Office SBC:** If multiple tunnel connection entries are configured for IKE preshared key authentication on the branch office SBC, both the **Remote Address** and the **Preshared Secret** must be unique.
- **Headquarters SBC:** If multiple tunnel connection entries are configured for IKE Preshared key authentication on the headquarters SBC, either the **Remote Address** *(only visible when **Allow Any Remote Address** is disabled)* or the **Remote Identifier** *(only visible when **Allow Any Remote Address** is enabled)* values must be unique.
- By default, the SBC VPN gateway supports policy-based source routing. The policy-based routing entries in the routing table are created automatically when an IPsec tunnel is established. In similar fashion, the policy-based routing entries in the routing table are deleted when an IPsec tunnel is torn down.

  The table entries force the source address of the IP packets leaving the SBC gateway through the outer interface to take on the IP address of the inner interface. This allows the SIP Option exchange messages and other traffic flows between the SBC VPN trunking gateways to pass thru the tunnel with the packet encapsulation and decapsulation at both SBC gateway tunnel endpoints. Adding the inner interface address *(private LAN connected to the local subnet network)* to the **Local Subnet Address** field and the external interface address *(private LAN connected to the remote subnet network)* to the Remote Subnet Address field on both the branch office and headquarters SBC gateways enables the IPsec source routing capabilities.

  In complex topology situations involving either a third-party VPN router and/or multiple nexthop devices, the traffic flow between the tunnel subnets is not properly source routed. As a workaround, default static routes can be manually added to the SBC VPN gateway.

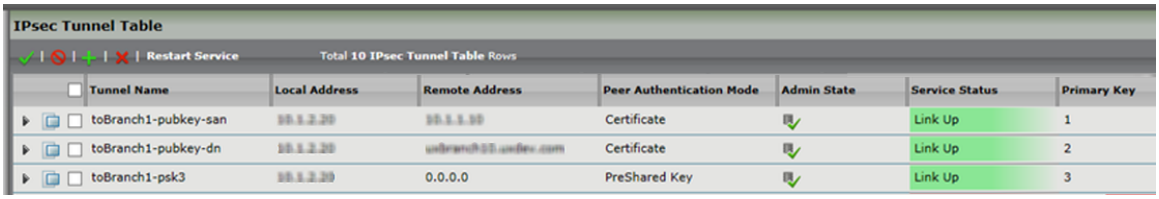
Note: Restart Services after IPsec Certificate Change

For existing tunnel entries in the IPsec Tunnel table: any changes to the certificates will take effect when a Restart Service is executed. See Creating and Modifying IPsec Tunnel Entries.

Working with IPsec Connections

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IPsec > Connection Tables**.

Copyright © 2015 Sonus Networks. All rights reserved.



To view an IPsec Connection Table entry's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying IPsec Tunnel Entries

Creating and Modifying IPsec Tunnel Entries

Prerequisites

Before you can create an IPsec Tunnel Entry you must have done the one of the following:

- A Sonus SBC Certificate and Trusted CA Certificate must be obtained and imported to the SBC when **Certificate** is selected **Authentication Mode** list box in the **Authentication Parameters** panel. Refer to Working with Certificates for information about configuring certificates on the SBC.
- An IPsec license is required to manage IPsec tunnels.

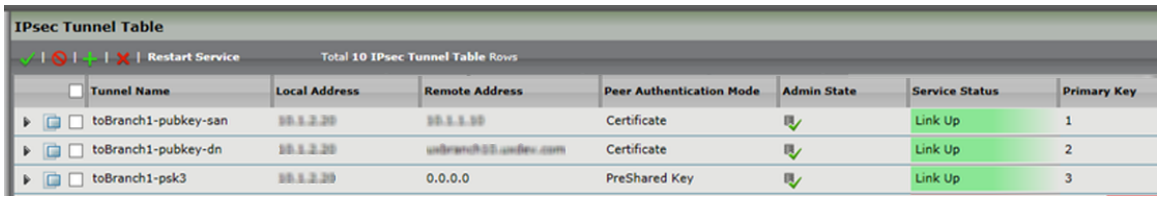
Important Information for Previous SIP-TLS Users:

- When upgrading to version 3.0 existing Sonus SBC Certificates will fail authentication due to *key integrity verification errors* when used to bring up the IPsec tunnel in the ***Certificate*** authentication mode.
- Before beginning to manage an IPsec tunnel for ***Certificate*** authentication, you must generate a new Certificate Signing Request (CSR), re-sign, and re-import a new Sonus SBC Certificate.

To create or modify an existing IPsec Tunnel:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IPsec > Connection Tables**.

Copyright © 2015 Sonus Networks. All rights reserved.



Enabling/Disabling Tunnel entries

To enable all selected tunnel entries

1. Click the **Enable all selected tunnels** ( ) icon on the IPsec Tunnel Table page. All tunnel entries selected are enabled.

To disable all selected tunnel entries

1. Click the **Disable all selected tunnels** ( ) icon on the IPsec Tunnel Table page. All tunnel entries selected are disabled.

Restart Service for Tunnel entries

The Restart Service button on the IPsec Tunnel Table page enables you to restart the services in order for any changes to the system certificates to become effective. For more information about system certificates, see Managing IPsec Tunnels.

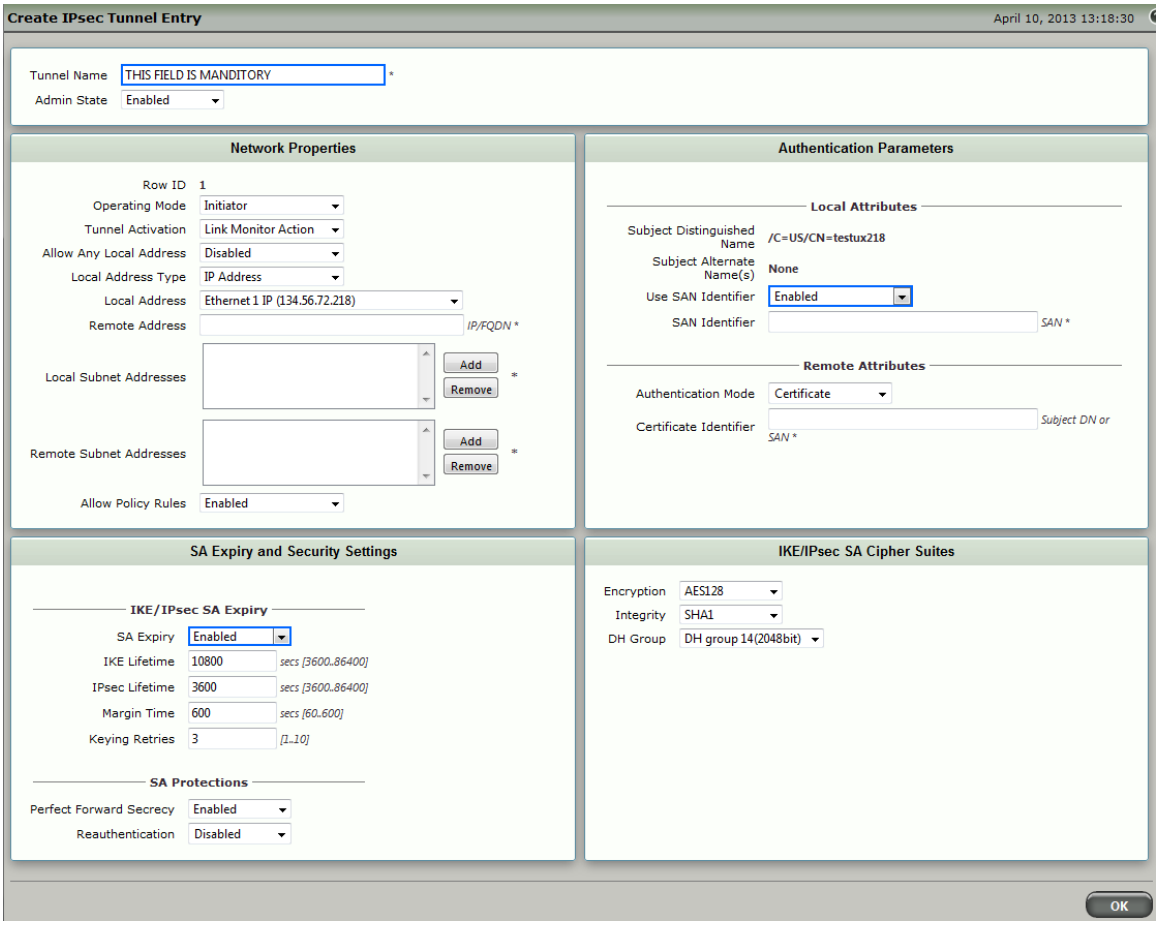
1. Click on **Restart Services** on the IPsec Tunnel Table page. A confirmation window is displayed.
2. Click **OK**.

Creating an IPsec Tunnel

To create an IPsec Tunnel

1. Click the **Create IPsec Tunnel Entry** ( ) icon on the IPsec Connection Table page.

Copyright © 2015 Sonus Networks. All rights reserved.



Network Properties - Field Definitions

Operating Mode

Specifies the operating mode for communication with the remote VPN peer for IKE negotiations and IPsec connections.

Initiator: Enables the branch office SBC gateway to initiate the IKE Security Association(SA) and IPsec tunnel negotiation request.
Responder: Enables the corporate SBC gateway to receive the request to establish an IKE/IPsec tunnel connection.

Tunnel Activation

Specifies the how SBC communications with the remote VPN peer is initiated. The IKE and IPsec phase negotiations are initiated as either permanent or on-demand depending on the type of activation selected. This field is only visible when "Initiator" is selected in the **Operating Mode** list box.
Always: Initiates the IKE Security Association(SA) and IPsec phase negotiations permanently with the remote VPN peer.
Link Monitor Action: Initiates the IKE and IPsec phase negotiations with the remote VPN peer as on-demand upon request from the link monitor switch-over action.

Allow Any Local Address

Copyright © 2015 Sonus Networks. All rights reserved.

Enabled: The local address is acquired during negotiation by automatic keying. Overrides any assigned local address.
Disabled: The value in the **Local Address** field is used.

Local Address

Specifies the IP address or fully-qualified domain name of the local network interface. If Allow Any Local Address is enabled, then the SBC allows any outgoing address during negotiations.

Allow Any Remote Address

Enabled: The remote address is acquired during negotiation by automatic keying. Overrides any assigned remote address.
Disabled: The value in the **Remote Address** field is used.
This field is only visible when **Responder** is selected in the **Operator Mode** select list.

Remote Address

Specifies the IP address or fully-qualified domain name of the remote network interface. If Allow any remote address is enabled, the SBC allows any incoming address during negotiations.

Local Subnet Address

Specifies the IP address of the private subnet behind the local network interface. This can be expressed as network/netmask. Maximum of 10 subnets can be specified. Allow traffic on any address is represented as 0.0.0.0/0. Setting both the Local Subnet Address and the Remote Subnet Address to all traffic ***0.0.0.0/0*** is not a valid configuration for security concerns.

Remote Subnet Address

Specifies the IP address of the private subnet behind the remote network interface. This can be expressed as network/netmask. A maximum of 10 subnets can be specified. Allow traffic on any address is represented as 0.0.0.0/0. Setting both the Local Subnet Address and the Remote Subnet Address to all traffic ***0.0.0.0/0*** is not a valid configuration for security concerns.

Allow Policy Rules

Enabled: Speicifes that the local VPN gateway performs forwarding and firewalling using IP tables for traffic from Local Subnet Address and Remote Subnet Address fields.
Disabled: Specifies that IP tables policy rules are not created for traffic to and from the peer endpoint.

SA Expiry and Security Settings - Field Definitions

SA Expiry

Specifies whether or not the SBC requests a renegotiation when the connection expires.

Enabled: Initiate SA Negotiation upon connection expiry. Applies to both IKE SA and IPsec SA.
Disabled: SA Negotiation is not initiated upon connection expiry.

Keying Retries

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the number of times the SBC will attempt to negotiate a connection. Applies to both IKE SA and IPsec SA.

If the number of number of retries value is exceeded, the SBC issues a Tunnel Link Lost alarm."

IKE Lifetime

Specifies the duration, in seconds, of an IKE SA connection keying channel.

IPsec Lifetime

Specifies the duration, in seconds, of the IPsec SA connection, from successful negotiation to expiry.

Margin Time

Specifies the length of time, in seconds, before SA expiry that the rekeying should start. Applies to both IKE SA and IPsec SA.

Perfect Forward Secrecy

When enabled, a new ISAKMP SA is created for each IPsec SA negotiation and a Diffie-Hellman exchange is performed for each IPsec SA negotiation.

Reauthencation

Specifies whether or not the SBC reauthenticates when a re-key is accomplished.

Enabled: IKE SA Rekeying also initiates Peer Authentication. IKE and IPsec SA's are uninstalled then recreated.
Disabled: IKE SA Rekeying performed without the Peer Authentication.

Authentication Parameters - Field Definitions

Use SAN Identifier

Specifies whether or not the Subject Alternative Name (SAN) Identifier is used for peer authentication. This field is only visible when **Certificate** is selected from the "Authentication Mode* select list.

Enabled: The SAN Identifier is sent to the remote gateway for an authentication match. The SAN identifier must be configured in the Local SAN Identifier attribute when this option is **Enabled**.
Disabled: By default, the Sonus SBC Certificate's Subject Distinguished Name(Subject DN) identifier is automatically extracted from the certificate and sent to the remote gateway for an authentication config match.

SAN Identifier

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the SAN identifier to be sent to the remote gateway for a peer authentication config match. This field is only available if **Enabled** is selected in the **Use SAN Identifier** select list.

If the Peer Authentication Identifier on the remote gateway is configured to authenticate a SAN identifier from the peer's certificate, it will attempt to match its configured SAN identifier with the expected SAN identifier retrieved from the peer authentication config.

If Use SAN Identifier is enabled, the SAN identifier must be picked from a list of DNS names displayed under the local attributes for the **Sonus SBC Certificate**.

Authentication Mode

Specifies the authentication method required from the remote side.

Certificate: Specifies the use of public key signature when authenticating the peer VPN gateway. The SBC must contain a valid server certificate/private key, the Certificate Authority(CA) that signed the SBC server certificate, and the CA that signed the peer's Server Certificate.

Preshared Key: Specifies the key to be shared with the peer. This key must match the same key configured on the peer system.

Peer Identifier

Specifies an identifier for a peer.

When **Preshared Key** is selected from the **Peer Authentication Mode** list box, the identifier may be an IP address, fully qualified domain name, or *any*.

When **Certificate** is selected from the **Peer Authentication Mode** list box, the identifier may be the peer certificate's Subject Alternative Name (SAN) or Subject Distinguished Name (DN). If the SAN or DN are unknown a vaalue of *any* may be used allowing any peer with a trusted and non-revoked certificate.

Remote Identifier

Specifies how the peer is identified for IKE preshared key authentication.

The identifier selector can be an all host address(0.0.0.0), a specific IP address or a fully-qualified domain name of the remote LAN network interface. This option is available when "Allow any address" is set to "True" and the "Peer Authentication Mode" is set to "Preshared Key".'

Preshared Secret

A strong passphrase used for authentication.

IKE/IPsec Cipher Suites - Field Definitions

Encryption

Specifies the Internet Key Exchange(IKE)and Encapsulating Security Payload (ESP) encryption algorithm.

Integrity

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies Internet Key Exchange(IKE) Encapsulating Security Payload (ESP) and hash algorithm.

DH Group

Specifies which Diffie-Hellman group to use for exchanging keys (IKE and ESP).

Configuring a Site to Site IPsec between the SBC Gateways

This article describes the steps necessary to configure the Sonus SBC 1000/2000 for IPsec.

On this Page

- Overview
  - Site to Site IPsec Settings in a Nutshell
    - Phase 1 Settings
    - Phase 2 Settings
    - Final steps
    - IKEv2 SA Message Exchange Flow
      - IKE SA
      - IPsec SA
      - Dead Peer Detection Keep-Alive
- Prerequisites
- Related Documentation
- Network Topology Diagram

Copyright © 2015 Sonus Networks. All rights reserved.

- General Configuration Notes
  - Networking Properties
    - Operating Mode
    - Tunnel Activation
    - Branch1_SBC Tunnel Connection Definition
    - Branch2_SBC Tunnel Connection Definition
    - HQ_SBC Tunnel Connection Definitions
    - Firewall and Policy Based Routing
      - Policy-based Firewall Rules
      - Policy-based Source Routing Table
  - Tunnel Setup using Preshared Key Authentication
    - Using the Same Secret Key Between All Sites
      - Branch1_SBC Tunnel Connection Definition
      - Branch2_SBC Tunnel Connection Definition
      - HQ_SBC Tunnel Connection Definitions
        - Single Tunnel Connection for all Branch Sites
        - Multiple Tunnel Connections for each Branch Site
    - Using Different Secret Keys at Each Branch Site
      - Branch1_SBC Tunnel Connection Definition
      - Branch2_SBC Tunnel Connection Definition
      - HQ_SBC Tunnel Connection Definitions
  - Tunnel Setup Using Certificate Key Authentication
    - Using the Subject Alternative Names (SAN) Identifier
      - Branch1_SBC Tunnel Connection Definition
      - Branch2_SBC Tunnel Connection Definition
      - HQ_SBC Tunnel Connection Definitions
    - Using the Distinguished Name(DN) Identifier
      - Branch1_SBC Tunnel Connection Definition
      - Branch2_SBC Tunnel Connection Definition
      - HQ_SBC Tunnel Connection Definitions
    - Using Any Identifier
      - HQ_SBC Tunnel Connection Definition using Any SAN Identifier
      - HQ_SBC Tunnel Connection Definition using Any DN Identifier
    - Certificate and Preshared Key Using Any Identifier
      - Branch1_SBC Tunnel Connection Definition
      - Branch2_SBC Tunnel Connection Definition
      - HQ_SBC Tunnel Connection Definitions
  - IKE/IPsec SA Cipher Suites
    - Proposal selection process
    - Performance Considerations
  - SA Expiry and Security Settings
    - IKE/IPsec SA Expiry and Protections
    - Refactoring Significance Using Margin Time
      - Initiator Mode
      - Responder Mode
      - Example
    - Other Performance Considerations

Related Articles

- Creating and Modifying IPsec Tunnel Entries

Copyright © 2015 Sonus Networks. All rights reserved.

Overview

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. The IPsec enabled SBC gateway secures data transmission between the subnets behind the branch remote offices and the corporate headsquarters (HQ). IPsec tunnels are established and maintained to provide for data privacy, integrity, authenticity, and anti-replay protection for network traffic over Internet-based connections.

Site to Site IPsec Settings in a Nutshell

The procedures outlined in this document are best practice recommendations and guidelines for the steps requires to set up an IKEv2 connection between Sonus SBC 1000/2000 gateways with IPSec Tunnel Tables.

First, determine how to authenticate both SBC IPsec enabled peers to each other. Configure a preshared key as a strong pass-phrase or install a digital RSA certificate with a stronger 2048-bit key option. This is used for authentication and to ensure the IPsec gateways are authorized by proving their identities to each other. Both gateways must use the same type of credentials – either preshared keys or digital certificates. Preshared keys are shared with the gateway peer, therefore both keys must match.

The tunnel connection definition is configured and negotiated in two phases. In phase 1, set up a secure and encrypted channel (required to protect the phase 2 negotiations). In phase 2, establish the IPSec Security Association (SA) to tell the gateway what traffic is being sent over the tunnel, and how to encrypt and authenticate it.

Phase 1 Settings

- Specify both SBC gateway addresses. Specify the address of the local SBC gateway and the address of the remote SBC gateway as an IP address or a Fully Qualified Domain Name(FQDN).
- Specify the authentication mode as preshared key or certificate. When using the digital certificate, specify the subject Distinguished Name (DN) field or the Subject Alternative Name (x509v3 Extension SAN field) of the peer's certificate. If certificates is not used, as recommended for larger deployments where security measures are of concern, then specify a long and complex preshared key. The preshared key must be a strong password or a pass-phrase represented as hexadecimal or Base64 encoded binary values.
- Choose a transform set, which includes the type of encryption, authentication and how long the security association will last. Select Sha256 if required to use a stronger authentication algorithm. Select either 3DES or AES 128, 256 bit key strength for encryption. Select AES 256 as this is the strongest encryption protocol. Specify a Diffie-Hellman key group, usually 1, 2, 5 or 14 (14 is the most secure group).
- Specify an IKE lifetime for the IKE SA, which adds more security to SBC gateway if the keys have been hacked. Although this will also have a slight affect on performance as well.

Phase 2 Settings

- Specify what traffic will go across the tunnel using the IP address, Network address, or IP address range. This is access to the SBC gateway's internal network, so either remote users from home, or the peer office can have access to resources behind the SBC IPsec enabled gateway.
- Choose whether to use Perfect Forward Secrecy (PFS), for optional and an extra layer of security. When enabling PFS, both SBC gateway peers must support and use PFS. Select which Diffie-Hellman group to use for new keying material. The higher the group selected such as DH Group 14, the stronger the key.
- Specify the encryption and authentication algorithms, securing the data in the IPsec SA (Phase 2 Proposal). The only type of proposal supported on the SBC gateway is ESP to provide authentication and encryption. Specify the authentication and encryption algorithm and protocol which will be the same as ones chosen for

Copyright © 2015 Sonus Networks. All rights reserved.

Phase 1 settings as to simplify the configuration steps when establishing the tunnel with another SBC gateway peer.

- Specify the IPsec lifetime for the IPsec SA. This ensures that the encryption keys change over a period of time and have them recreated, adding more security, as well as having a slight affect on performance.

Final steps

- Create policies or rules that allow the tunneled traffic in and out of the firewall based on the topology firewalling requirements. The option to either enable or disable the firewall policy rules on SBC IPsec enabled gateway will automatically insert the policy based match traffic rules.
- Configure the SBC gateway peer with the exactly the same settings and/or the reverse of its peer's settings as configured on the local gateway for some of the fields. If the peer settings are not reversed, this will result in a failure to establish a tunnel and it's service status will appear as **Down**.

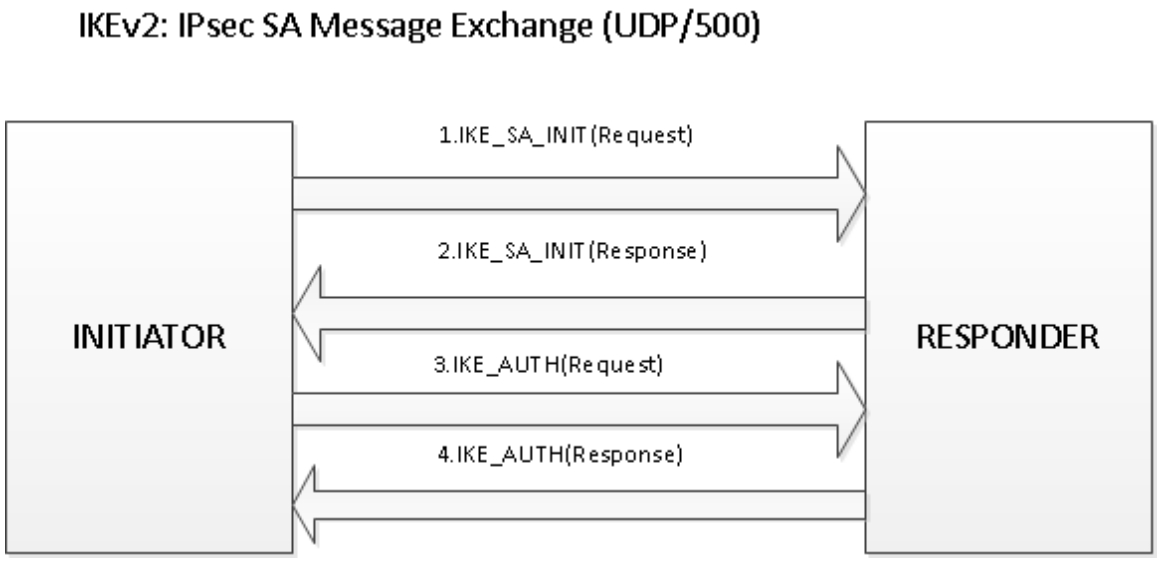
IKEv2 SA Message Exchange Flow

Internet Key Exchange (IKE) is accessed via UDP port 500. IP port 50 must be used for the Encapsulating Security Payload (ESP). The NAT Traversal is assigned to UDP port 4500.

When NAT is present, UDP port 4500 is used in the tunnel path.

IKE SA

The establishment of a single IKE SA using the IKEv2 protocol requires an exchange of four UDP datagrams as shown in the illustration below.
The task of resending messages falls to the initiator only. The IKE_SA_INIT message carries the selection of cryptographic transforms for the IKE SA, the derivation of a common Diffie-Hellman secret and the nonces into a single exchange. The IKE_AUTH message authenticates the peers using the pre-shared keys(PSK)or the RSA signatures supported by the SBC to create the first so-called Child SA by defining the traffic selectors and cryptographic transforms for the IPsec connection.



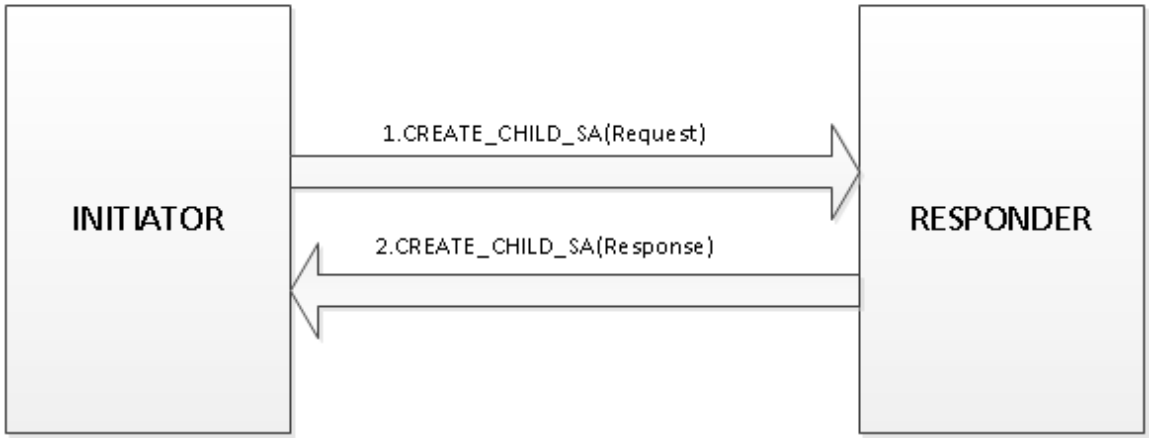
IPsec SA

The establishment of a single or multiple Child SA using the IKEv2 protocol requires an exchange of a CREATE_CHILD_SA request/response pair as shown in the following illustration. The message carries the cryptographic transforms, a pair of fresh nonces, an optional Diffie-Hellman exchange if PFS is desired and the

Copyright © 2015 Sonus Networks. All rights reserved.

additional traffic selectors.

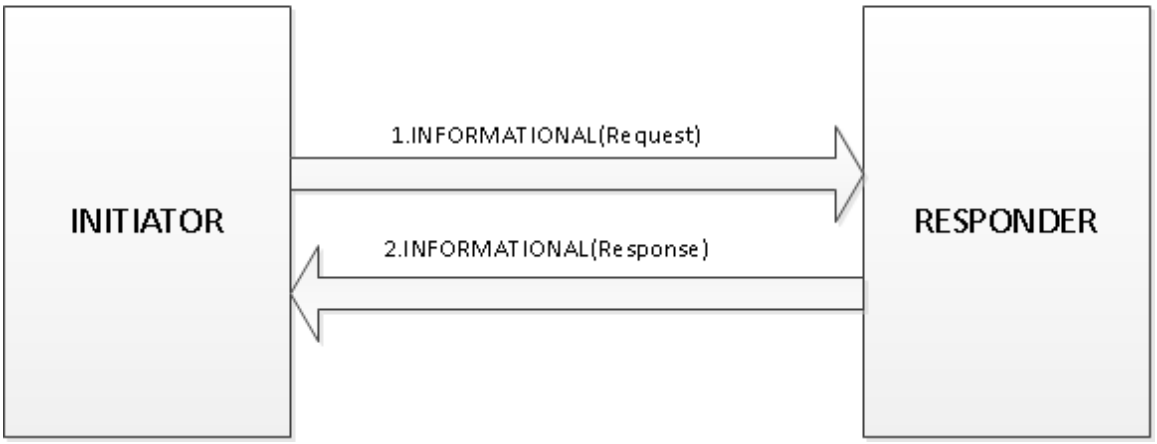
IKEv2: CREATE_CHILD_SA Message Exchange (UDP/500)



Dead Peer Detection Keep-Alive

The SBC gateway defines a hard-coded time interval of 30s with which keep-alive INFORMATIONAL exchanges are sent to the peer. These are only sent if no other traffic is received. All connections with a dead peer are stopped and unrouted. The gateway also defines a hard-coded timeout interval of 60s, after which all connections to a peer are deleted and the IKE and Child Security Associations(SA) are cleared in case of inactivity.

IKEv2: INFORMATIONAL Message Exchange (UDP/500)



Prerequisites

- An IPsec license is required to manage IPsec tunnels.
- A Sonus SBC Certificate and Trusted CA Certificate must be obtained and imported to the SBC when Certificate is selected from the Authentication Mode list box in the Authentication Parameters panel. Refer to Working with Certificates for information about configuring certificates on the SBC.
- When upgrading to version 3.0 existing Sonus SBC Certificates will fail authentication due to key integrity verification errors when used to bring up the IPsec tunnel in the Certificate authentication mode. Before beginning to manage an IPsec tunnel for Certificate authentication, must generate a new Certificate Signing

Copyright © 2015 Sonus Networks. All rights reserved.

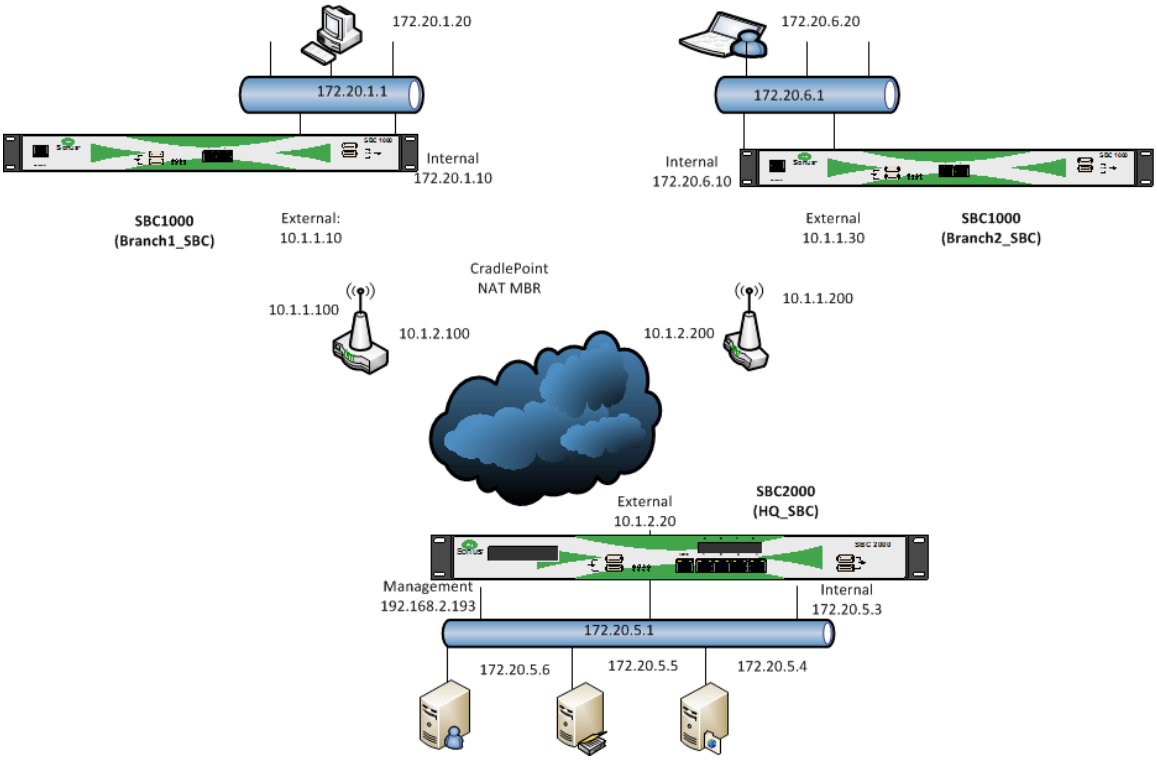
Request (CSR), re-sign, and re-import a new Sonus SBC Certificate.

Related Documentation

Working with Certificates
Working with IPsec
Managing IPsec Tunnels
Viewing IPsec Statistics

Network Topology Diagram

The configuration settings and examples in following sections are based on network a topology comprising a single SBC gateway at two different branch sites, behind an external NAT accessing the corporate gateway or the servers in the subnet behind the corporate gateway over public internet access.



General Configuration Notes

The following information refers to the Create IPsec Tunnel Entry page of the SBC 1000/2000 user interface. For more information see: Managing IPsec Tunnels and Creating and Modifying IPsec Tunnel Entries.

Networking Properties

- Specify the local and remote site peer address (outside interface IP of the SBC gateway).
- Configure the local host internal subnet to allow traffic to and from the selected hosts/networks at the remote site.

Copyright © 2015 Sonus Networks. All rights reserved.

Information Note:

Any or all IP traffic (0.0.0.0/0) subnets is not a supported configuration for the Local Subnet Addresses attribute. It is supported for the Remote Subnet Addresses attribute as the peer needs to define the specific host addresses in properly establishing the IPsec SA traffic selector policies.

- A maximum of 10 subnet addresses can be configured per tunnel connection entry.
- When specifying the local and/or remote site peer address as an FQDN address type, the DNS Server must be configured to resolve the FQDN.

Important Note:

The local and remote site peer address type selected as either IP or FQDN on the branch office SBC, must be the same address type configured on the headquarters SBC. The address type on both peers must be the same type (e.g., IP or FQDN). For example, the **Local Address** configured with an IP on branch office SBC will not be able match the peer config that has the **Remote Address** configured as FQDN address type on the headquarters SBC. This can be addressed by one of two possible ways: 1) Configure the **Remote Address** as FQDN on the headquarters SBC which is the same address type configured on the peer SBC. or 2) Enable **Allow any Remote Address** field on the headquarters SBC to match either address type.

Operating Mode

- **Initiator**
  Either an SBC 1000 or an SBC 2000 IPsec enabled gateway can be deployed at branch offices sites which will negotiate the tunnel in an active mode of operation.

- **Responder**
  An SBC 2000 IPsec enabled gateway must be deployed at the corporate site premises and waits, in a passive mode, for tunnels to be initiated by the branch office IPsec enabled gateway peer(s).

Tunnel Activation

This setting is applicable for the IPsec enabled gateway configured in an **Initiator** mode of operation.

- **Always**
  It is used to activate a permanent and/or stand-alone tunnel establishment. This setting should be used mainly for the purposes of confirming that the tunnel is being established with the proper configurations and/or troubleshooting the connection failures in the field.
- **Link Monitor Action**
  This is the default recommended setting for the tunnel to be activated and negotiated with the peer in an on-demand mode. The on-demand tunnel activation is performed by the branch survivability 3G4G fail-over feature. Refer to Configuring 3G4G Failover guidelines which covers configuration of the 3G4G fail-over feature on the Sonus SBC 1000/2000 under the Working with Branch Survivability section.

Branch1_SBC Tunnel Connection Definition

1. **Tunnel Name**: Branch1_SBC
2. **Local Address**: Ethernet 2 IP(10.1.1.10)

Note:

Alternatively configured as FQDN (eg: branch1sbc.uxdev.com), when the **Remote Address** is also configured the same on the headquarters SBC. Another alternative is to enable the **Allow Any Local Address** which automatically selects any local or outside interface IP.

3. **Remote Address**: 10.1.2.20

Copyright © 2015 Sonus Networks. All rights reserved.

> **Note:**
>
> Alternatively configured as FQDN (eg: hqsbc.uxdev.com), when the **Local Address** is also configured the same on the headquarters SBC.

4. **Local Subnet Addresses**: 172.20.1.10/32,172.20.1.20/32

> **Note:**
>
> Alternatively configured as subnet address range such as 172.20.1.0/24.

5. **Remote Subnet Addresses**: 172.20.5.0/24

> **Note:**
>
> Alternatively configured as specific host addresses with CIDR mask value 32. Also, can be configured as 0.0.0.0/0 to accept all IP traffic which the HQ SBC peer specifically defines in the **Local Subnet Addresses**.

Branch2_SBC Tunnel Connection Definition

1. **Tunnel Name**: Branch2_SBC
2. **Local Address**: branch2sbc.uxdev.com
3. **Remote Address**: hqsbc.uxdev.com
4. **Local Subnet Addresses**: 172.20.6.0/24
5. **Remote Subnet Addresses**: 172.20.5.3/32,172.20.5.4/32,172.20.5.5/32,172.20.5.6/32

HQ_SBC Tunnel Connection Definitions

The networking configuration must be the exact opposite of those configured on each branch office sites, that is, reverse the **Local Address**, **Remote Address**, **Local Subnet Addresses** and **Remote Subnet Addresses** used on the branch office when setting up a one-to-one tunnel connection entry on the headquarters SBC.

- Tunnel ID 1

1. **Tunnel Name**: HQ_to_Branch1_SBC
2. **Local Address**: Ethernet 2 IP(10.1.2.20)

> **Note:**
>
> Alternatively configured as FQDN (eg: hqsbc.uxdev.com), when the **Remote Address** is also configured the same on the branch office SBC.

3. **Remote Address**: 10.1.1.10

> **Note:**
>
> Alternatively configured as FQDN (eg: branch1sbc.uxdev.com), when the **Remote Address** is also configured the same on the branch office SBC. Another alternative is to enable the **Allow Any Remote Address** to accept any remote external interface required in case of the remote host behind NAT.

4. **Local Subnet Addresses**: 172.20.5.3/32,172.20.5.4/32,172.20.5.5/32,172.20.5.6/32
5. **Remote Subnet Addresses**: 172.20.1.0/24

Copyright © 2015 Sonus Networks. All rights reserved.

> **Note:**
>
> Alternatively configured as specific host addresses with CIDR mask value 32. Also, can be configured as 0.0.0.0/0 to accept all IP traffic which the Branch SBC peer specifically defines in the **Local Subnet Addresses**.

- Tunnel ID 2

1. **Tunnel Name**: HQ_to_Branch2_SBC
2. **Local Address**: hqsbc.uxdev.com
3. **Remote Address**: branch2sbc.uxdev.com

> **Note:**
>
> Another alternative is to enable the **Allow Any Remote Address** to accept any remote external interface required in case of the remote host behind NAT.

4. **Local Subnet Addresses**: 172.20.5.0/24
5. **Remote Subnet Addresses**: 172.20.6.0/24

Firewall and Policy Based Routing

Policy-based Firewall Rules

The **Apply Policy Rules** field is enabled by default and automatically inserts bi-directional FORWARD rules on gateways or an INPUT and OUTPUT rule on single hosts, and adds an INPUT and OUTPUT rule to reach the gateway itself when the tunnel is established. Likewise, these rules are deleted when the tunnel is disconnected.

Use of the policy module depends on how the rest of the firewall is configured and the exact requirements.
When the forwarding-firewalling feature is enabled, the iptables policy module rules-matches packets based on their relation to IPsec policies which will do everything related to only allow traffic from/to the tunneled subnet and not the whole subnet via the IPsec tunnels. The **Apply Policy Rules** field can be disabled if there is a business case requirement to configure custom IPsec ACCEPT/DROP rules which take precedence in relation to the automatically created IPsec rules.

Policy-based Source Routing Table

In a simple network topology with no nexthop gateway between the subnet and the local internal network interface on the SBC gateway, the policy-based source routing entries are created automatically.

To enable the policy-based source routing capabilities: the source address must be the local internal network interface. The **Local Subnet Addresses** list must include the local internal network address, and the **Remote Subnet Addresses** must contain the peer's internal network address.

For example:
1) On the Branch1_SBC gateway (Refer to Network Topology Diagram section), the Ethernet 1 IP(172.20.1.10) is the local internal network interface. This address should be added to the **Local Subnet Addresses** as 172.20.1.10/32 or automatically included when specifying the address range such as 172.20.1.0/24. Likewise, on the Branch1_SBC gateway, the Ethernet 1 IP(172.20.5.3) which is the remote internal network interface configured on the HQ_SBC gateway should be added to the **Remote Subnet Addresses** as 172.20.5.3/32 or automatically included when specifying the address range such as 172.20.5.0/24.

2) On the HQ_SBC gateway (Refer to Network Topology Diagram), the networking configuration must be the exact

Copyright © 2015 Sonus Networks. All rights reserved.

opposites of the ones configured on each branch office sites. Reverse the **Local Subnet Addresses** and **Remote Subnet Addresses** used on the branch office when setting up a one-to-one tunnel connection entry on the headquarters SBC.

> **Note:**
>
> With a complex network topology involving one or multiple nexthop gateways, may need to create static default gateway routes on the SBC gateways (**Protocols** navigation pane -> **IP** -> **Static Routes**).

Tunnel Setup using Preshared Key Authentication

Specify either the peer address of the remote site (outside interface IP of the peer SBC gateway) or the remote identifier when enabling the **Allow Any Remote Address** field in case of the remote host behind NAT. Use either an existing or new pre-shared key to be configured the same between the SBC gateway peers.

Using the Same Secret Key Between All Sites

Branch1_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key
2. **New Preshared Secret**: Testing123@#

Branch2_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key
2. **New Preshared Secret**: Testing123@#

HQ_SBC Tunnel Connection Definitions

Tunnel connection definitions on headquarters SBC gateway can be configured in two possible ways as indicated by the examples below.

Single Tunnel Connection for all Branch Sites

A single tunnel ID can be configured on the headquarters SBC to negotiate the traffic selectors from any branch office by specifying *any* remote address as an identifier selector.

> **(!) Caution:**
>
> At present, the IPsec Statistics table does not report the statistics details for all the branch CHILD_SAs created over a single IKE_SA tunnel connection. This is known limitation and will be supported in future releases. Therefore, it is recommended to configure the one-to-one tunnel connection per the example provided below in the **Multiple Tunnel Connections for Specific Branch Sites** section.

1. **Allow Any Remote Address**: Enabled
2. **Remote Subnet Addresses**: 172.20.1.0/24,172.20.6.0/24
3. **Authentication Mode**: Preshared Key
4. **Remote Identifier**: 0.0.0.0
5. **New Preshared Secret**: Testing123@#

Multiple Tunnel Connections for each Branch Site

The need to create multiple tunnels on the headquarters SBC as one-to-one mapping with branch sites is highly recommended when there is a greater interest in maintaining separate tunnels and/or analyzing the **IPsec Statistics** data corresponding to each branch sites.

Copyright © 2015 Sonus Networks. All rights reserved.

- Tunnel ID 1

1. **Remote Address**: 10.1.1.10

> **Note:**
>
> Alternatively configured as an FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative is to enable the **Allow Any Remote Address**. When any remote address is enabled, the **Remote Identifier** must be configured as the peer's local address such as 10.1.1.10 for a successful look-up and match of an expected identifier against the configured identifier.

2. **Remote Subnet Addresses**: 172.20.1.10/32,172,20.1.20/32
3. **Authentication Mode**: Preshared Key
4. **New Preshared Secret**: Testing123@#

- Tunnel ID 2

1. **Remote Address**: 10.1.1.30

> **Note:**
>
> Alternatively configured as an FQDN such as branch2sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address**. When any remote address is enabled, the **Remote Identifier** must be configured as the peer's local address such as 10.1.1.30 for a successful look-up and match of an expected identifier against the configured identifier.

2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Authentication Mode**: Preshared Key
4. **New Preshared Secret**: Testing123@#

Using Different Secret Keys at Each Branch Site

Branch1_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key
2. **New Preshared Secret**: ABC123

Branch2_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key
2. **New Preshared Secret**: XYZ456

HQ_SBC Tunnel Connection Definitions

- Tunnel ID 1

1. **Remote Address**: 10.1.1.10

> **Note:**
>
> Alternatively configured as an FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address**. When any remote address is enabled, the **Remote Identifier** must be configured as the peer's local interface address such as 10.1.1.10 for a successful look-up and match of an expected identifier against the configured identifier.

2. **Remote Subnet Addresses**: 172.20.1.10/32,172,20.1.20/32
3. **Authentication Mode**: Preshared Key

Copyright © 2015 Sonus Networks. All rights reserved.

4. **New Preshared Secret**: ABC123

- Tunnel ID 2

1. **Remote Address**: 10.1.1.30

> **Note:**
>
> Alternatively configured as an FQDN such as branch2sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address**. When any remote address is enabled, the **Remote Identifier** must be configured as the peer's local interface address such as 10.1.1.30 for a successful look-up and match of an expected identifier against the configured identifier.

2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Authentication Mode**: Preshared Key
4. **New Preshared Secret**: XYZ456

Tunnel Setup Using Certificate Key Authentication

As a best practice where security is of concern for multiple branch office SBC deployments, generating a new Certificate Signing Request, acquiring and installing a digital signed certificate and Trusted Certificate Authority (CA) root chain is recommended.

The CA file(s) which signed the **Sonus SBC Certificate** must be exported from each branch office SBC (if these are different CA vendors) and imported on the headquarters SBC.
Likewise, the CA file(s) which signed the **Sonus SBC Certificate** must be exported from the headquarters SBC and imported on each of the branch office SBC gateways.
The CA file(s) must be imported/exported under the Web UI **Security** navigation pane * > Certificates > Trusted CA* folder.

> **Warning:**
>
> With the current release (version 3.0), when replacing an existing **Sonus SBC Certificate and/or *Trusted CA Certificates**, the SBC gateway must be rebooted for the tunnels to be re-established with the new certificate installments and/or replacements. This is a known limitation and will be supported in future releases.

Using the Subject Alternative Names (SAN) Identifier

Specify the **Certificate Identifier** as Subject Alternative Name (**IPsec Tunnel Table** navigation pane **> Remote Attributes** panel) on the branch office SBC. To do this, copy one of the Subject Alternative Names display text (**IPsec Tunnel Table** navigation pane **> Local Attributes** read-only panel) from the headquarters SBC gateway and paste it in the **Certificate Identifier** field text box under the Remote Attributes panel of the branch office SBC.
Likewise, copy the Subject Alternative Name text (**IPsec Tunnel Table** navigation pane **> Local Attributes** read-only panel) on the branch office SBC gateway and paste it in the Certificate Identifier field text box under the Remote Attributes section of the headquarters SBC. When specifying a peer certificate's SAN identifier, enable and specify the local SAN identifier under the Local Attributes section on the branch office and headquarters SBC gateways. These additional field configurations are mandatory in order to perform a successful look-up and match of an expected SAN identifier against the configured SAN identifier.

The following sections are examples for authenticating a peer gateway using the SAN identifier:

Branch1_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Enabled
2. **SAN Identifier**: branchgw1.uxdev.com

Copyright © 2015 Sonus Networks. All rights reserved.

3. **Authentication Mode**: Certificate
4. **Certificate Identifier**: hqgw.uxdev.com

Branch2_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Enabled
2. **SAN Identifier**: branchgw2.uxdev.com
3. **Authentication Mode**: Certificate
4. **Certificate Identifier**: hqgw.uxdev.com

HQ_SBC Tunnel Connection Definitions

- Tunnel ID 1

1. **Remote Address**: 10.1.1.10

> **Note:**
>
> Alternatively configured as an FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address** in case of remote host behind NAT.

2. **Remote Subnet Addresses**: 172.20.1.10/32,172,20.1.20/32
3. **Use SAN Identifier**: Enabled
4. **SAN Identifier**: hqgw.uxdev.com
5. **Authentication Mode**: Certificate
6. **Certificate Identifier**: branchgw1.uxdev.com

- Tunnel ID 2

1. **Remote Address**: 10.1.1.30

> **Note:**
>
> Alternatively configured as an FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on the branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address** in case of remote host behind NAT.

2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Use SAN Identifier**: Enabled
4. **SAN Identifier**: hqgw.uxdev.com
5. **Authentication Mode**: Certificate
6. **Certificate Identifier**: branchgw2.uxdev.com

Using the Distinguished Name(DN) Identifier

Specify the **Certificate Identifier** as Subject Distinguished Name(**IPsec Tunnel Table** navigation pane -> **Remote Attributes** panel) on the branch office SBC. To do this, copy the Subject Distinguished Name display text(**IPsec Tunnel Table** navigation pane -> **Local Attributes** read-only panel) from the headquarters SBC and paste it in the **Certificate Identifier** field text box under the Remote Attributes panel of the branch office SBC. Likewise, copy the Subject Distinguished Name display text(**IPsec Tunnel Table** navigation pane -> **Local Attributes** read-only panel) from the branch office SBC gateway and paste it in the Certificate Identifier field text box under the Remote Attributes panel on the headquarters SBC gateway.

Branch1_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Disabled
2. **Authentication Mode**: Certificate

Copyright © 2015 Sonus Networks. All rights reserved.

3. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testhq.uxdev.com

Branch2_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Disabled
2. **Authentication Mode**: Certificate
3. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testhq.uxdev.com

HQ_SBC Tunnel Connection Definitions

- Tunnel ID 1

1. **Remote Address**: 10.1.1.10

> **Note:**
>
> Alternatively configured as FQDN such as branch1sbc.uxdev.com, when the **Local Address** is also configured the same on branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address** in case of remote host behind NAT.

2. **Remote Subnet Addresses**: 172.20.1.10/32,172,20.1.20/32
3. **Use SAN Identifier**: Disabled
4. **Authentication Mode**: Certificate
5. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testbranch1.uxdev.com

- Tunnel ID 2

1. **Remote Address**: 10.1.1.30

> **Note:**
>
> Alternatively configured as FQDN such as branch2sbc.uxdev.com, when the **Local Address** is also configured the same on branch office SBC. Another alternative configuration is to enable the **Allow Any Remote Address** in case of remote host behind NAT.

2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Use SAN Identifier**: Disabled
4. **Authentication Mode**: Certificate
5. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testbranch2.uxdev.com

Using Any Identifier

One significance of configuring 'any' certificate identifier is to simplify the configuration steps at the headquarters SBC gateway in larger deployments.

The Trusted Certificate Authority file(s) must be exported from each branch office SBC gateway and imported to the headquarters SBC gateway. This is the only configuration step required in order to perform a successful look-up and match of an expected SAN or DN dentifier against the 'any' identifier configured on the SBC gateway peer,

The configuration examples for authenticating the peer gateway using 'any' SAN or DN identifier is provided below.

HQ_SBC Tunnel Connection Definition using Any SAN Identifier

A single tunnel ID can be configured to negotiate the traffic selectors from any branch offices by specifying a local SAN identifier, 'any' remote address and 'any' peer certificate's SAN identifier.
The branch sites SBC tunnel connection is unchanged from the example provided in 'Using SAN Identifier' section above.

Copyright © 2015 Sonus Networks. All rights reserved.

1. **Allow Any Remote Address**: Enabled
2. **Remote Subnet Addresses**: 172.20.1.0/24,172.20.6.0/24
3. **Use SAN Identifier**: Enabled
4. **SAN Identifier**: hqgw.uxdev.com
5. **Authentication Mode**: Certificate
6. **Certificate Identifier**: any

HQ_SBC Tunnel Connection Definition using Any DN Identifier

A single tunnel ID can be configured to negotiate the traffic selectors from any branch offices by specifying 'any' remote address and 'any' certificate DN identifier.
The branch sites SBC tunnel connection is unchanged from the example provided in 'Using DN Identifier' section above.

1. **Allow Any Remote Address**: Enabled
2. **Remote Subnet Addresses**: 172.20.1.0/24,172.20.6.0/24
3. **Use SAN Identifier**: Disabled
4. **Authentication Mode**: Certificate
5. **Certificate Identifier**: any

Certificate and Preshared Key Using Any Identifier

Each branch office site can specify various authentication mode(Certificate or PSK) and identifier type(same secret, different secret, SAN or DN).
The headquarters SBC should create a one-to-one tunnel connection mapping to match whichever authentication mode specified on the branch office SBC.

Branch1_SBC Tunnel Connection Definition

1. **Use SAN Identifier**: Disabled
2. **Authentication Mode**: Certificate
3. **Certificate Identifier**: /C=US/L=IL/OU=Research and Development/CN=testhq.uxdev.com

Branch2_SBC Tunnel Connection Definition

1. **Authentication Mode**: Preshared Key
2. **New Preshared Secret**: Testing123@#

HQ_SBC Tunnel Connection Definitions

- Tunnel ID 1

1. **Allow Any Remote Address**: Enabled
2. **Remote Subnet Addresses**: 172.20.1.0/24
3. **Use SAN Identifier**: Disabled
4. **Authentication Mode**: Certificate
5. **Certificate Identifier**: any

- Tunnel ID 2

1. **Allow Any Remote Address**: Enabled
2. **Remote Subnet Addresses**: 172.20.6.0/24
3. **Authentication Mode**: Preshared Key
4. **Remote Identifier**: 0.0.0.0
5. **New Preshared Secret**: Testing123@#

IKE/IPsec SA Cipher Suites

Copyright © 2015 Sonus Networks. All rights reserved.

Proposal selection process

It is recommended that the transform data such as selection of encryption level, authentication algorithm and diffie-hellman group (DH Group) be configured the same way on the SBC gateway deployed at each branch office sites communicating with another SBC gateway at the headquarters site.

Choose the default settings: 1) IKE: aes128-sha1-modp2048 and IPSEC: aes128-sha1 or consider selecting stronger transform algorithms 2) IKE: aes256-sha256-modp2048 and IPSEC: aes256-sha256 when considering security measures.

IPsec connection can be successfully established between the SBC peers in case of non-matching Encryption, Integrity or DH Group parameters.
In case of mismatched encryption settings, the **Responder** gateway's configured cipher settings will take precedence over the proposed one received from the **Initiator** gateway. In case of a DH Group mismatch, the initiator or responder side with stronger key takes the precedence.

Performance Considerations

Selection of 3DES is supported mainly for the purpose of compatibility with non-SBC devices that do not support AES.
It is recommended to select AES encryption level since the throughput rate with the 3DES encryption will be significantly less and slower than the AES.

SA Expiry and Security Settings

IKE/IPsec SA Expiry and Protections

By default, both the **SA Expiry** and **Reauthentication** key protection measures are disabled since achieving better throughput and low latency for high call load traffic going in and out of the tunnel may be a bigger concern. Based on the business case requirements, whether a low or high degree of security measures are to be taken to protect the keys, then the **SA Expiry**, **Reauthentication**, and/or **Perfect Forward Secrecy** should be enabled under the **SA Expiry and Security Settings** panel.

The negotiation of IKE SAs and IPsec SAs can be configured to expire after a specific amount of time. By default, the **IKE Lifetime** is set to 3 hours, whereas the IPsec lifetime is set to 1 hour as to avoid collisions of these SAs expiring at same time.

Refactoring Significance Using Margin Time

The **Margin Time** field is supported to avoid collisions when the **SA Expiry** and **Reauthentication** are enabled on the SBC gateway deployed at both branch offices and the headquarters sites.
The specified margins are increased randomly(hard-coded percentage on initiator and responder gateway by which margins are randomly increased) before subtracting them from the expiration limits.
The formula shown below is used to calculate the rekey time of IKE and IPsec SAs.

Initiator Mode

Copyright © 2015 Sonus Networks. All rights reserved.

```
Actual IKE rekey time = *IKE Lifetime* - (*Margin Time* + random(0, *Margin Time* *
100%))
Actual IPsec rekey time = *IPsec Lifetime* - (*Margin Time* + random(0, *Margin
Time* * 100%))
```

Responder Mode

```
Actual IKE rekey time = *IKE Lifetime* - (*Margin Time* + random(0, *Margin Time* *
10%))
Actual IPsec rekey time = *IPsec Lifetime* - (*Margin Time* + random(0, *Margin
Time* * 10%))
```

Example

The IPsec tunnel will attempt to rekey the IPsec SA at a random time between 40 and 50 minutes after establishing the SA.
In other words, between 10 and 20 minutes before the SA expires.
1. **IPsec Lifetime**: 1h
2. **Margin Time**: 600s(10m)

```
Actual Minimum IPsec rekey time = 1h - (10m + 10m) = 40m
Actual Maximum IPsec rekey time = 1h - (10m + 0m) = 50m
```

Other Performance Considerations

- Furthermore, for a business case where some level of security measures and performance are both of concerns, then it is recommended to enable the SA Expiry and Security Setting fields on the SBC gateways are deployed at each of the branch office sites or at the headquarters but not required at both tunnel endpoints.
- It is recommended that the **IKE Lifetime** and **IPsec Lifetime** fields be configured with different timeout value to avoid the possibility of collisions although the refactoring using **Margin Time** should prevent that.
- The rekeying of an SA needs some time, the margin values must not be too low.
- Depending on the level of security that would be required for a business case, both reauthentication and rekeying can be enabled for providing maximum security level. If **Reauthentication** is enabled, it is recommended to set the **IKE Lifetime** to a high timeout value when re-authenticating the peer where key hacking is not likely on every hour. The reauthentication unlike the rekeying protection measure not only creates the IKE_SA from scratch but also the IPsec_SAs. During the reauthentication expiry process, performance may be impacted with some packet drops as it is computationally expensive to perform the Diffie-Hellman exchange and signature verifications for reauthentication purposes.

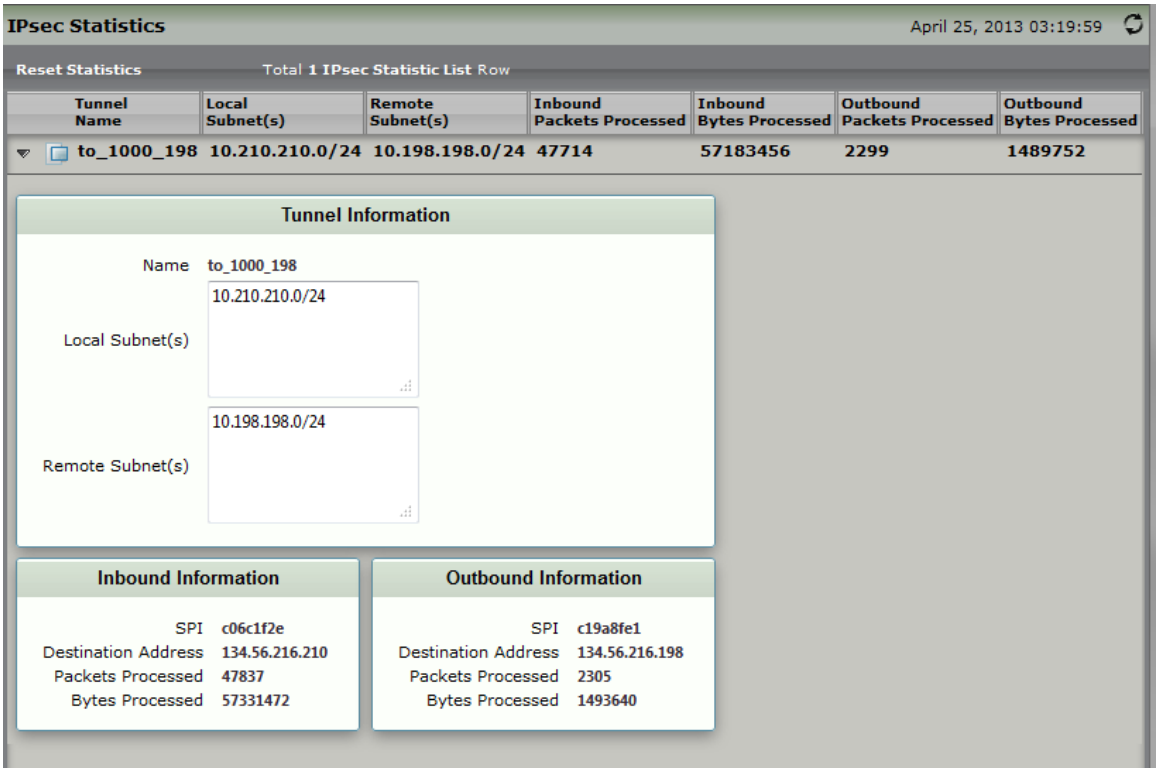
Viewing IPsec Statistics

How to View IPsec Statistics

Copyright © 2015 Sonus Networks. All rights reserved.

To view a VLAN counter:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IPsec > Statistics**.



Tunnel Information - Field Definitions

Local Subnet(s)

The IP address(es) of the private subnet(s) behind the local network interface.

Remote Subnet(s)

The IP address(es) of the private subnet(s) behind the remote network interface.

Inbound Information - Field Definitions

SPI

Security Parameter Index: an identification tag added to the header while using IPsec for tunneling the IP traffic.

Destination Address

The destination address for an Inbound Security Association entry.

Packets Processed

Copyright © 2015 Sonus Networks. All rights reserved.

The number of IPsec packets carried on a fast-forward Inbound Security Association entry.

Bytes Processed

The number of bytes of IPsec traffic transmitted on a fast-forward Inbound Security Association entry.

Outbound Information - Field Definitions

SPI

Security Parameter Index: an identification tag added to the header while using IPsec for tunneling the IP traffic.

Destination Address

The destination address for an Outbound Security Association entry.

Packets Processed

The number of IPsec packets carried on a fast-forward Outbound Security Association entry.

Bytes Processed

The number of bytes of IPsec traffic transmitted on a fast-forward Outbound Security Association entry.

Working with NAT and Port Forwarding

Overview

The SBC is capable of functioning as the only edge device between the office LAN and the ISP connected WAN. The SBC implements Network Address Translation (NAT) functionality providing internet connectivity between hosts on a local, private network, and the public domain. NAT and port forwarding on the SBC 1000/2000 are configured independently. However, in most cases NAT is required in order to enable hosts on the private network to reach the external network.

Private vs. Public IP Addresses

Sonus recommends that you use non-routable address assignments, however private non-routable addresses are not required. For more information about non-routable address assignments see RFC 1918.

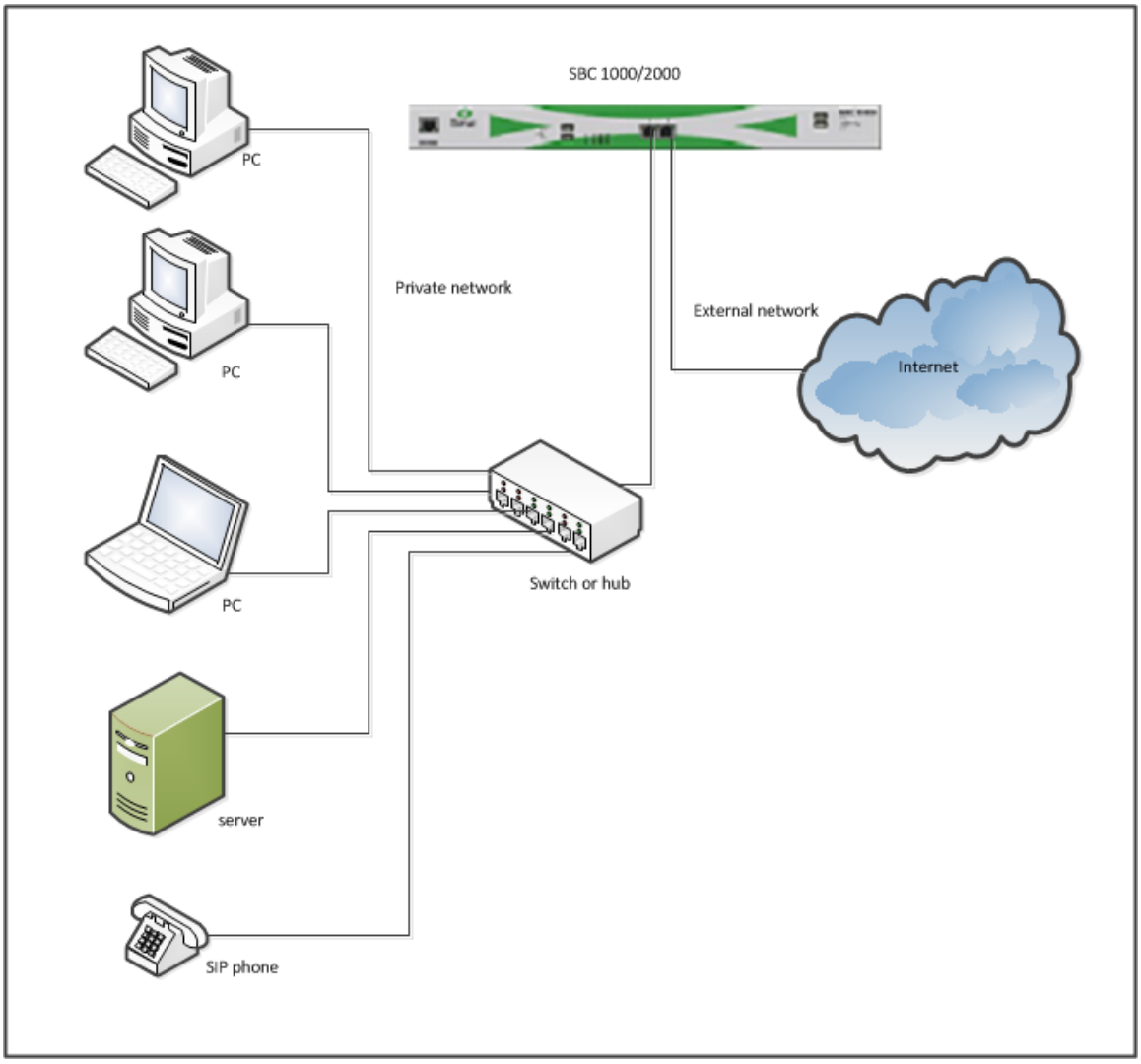
IPv4 vs IPv6

The NAT functionality of the SBC applies only to IPv4 Addresses.

Configuration Example

The following is an example of an SBC configured to function as an edge device with a private LAN and external WAN interfaces. In the illustrated example, PCs, IP phones, and servers attached to Interface 1 on the SBC with private, IP addresses are able to communicate with the public network attached to Interface 2 when NAT is configured.

Copyright © 2015 Sonus Networks. All rights reserved.



Address and Port Forwarding on the Sonus SBC 1000/2000

The Network Address Translation feature on allows you to configure Network Port Translation (NAPT) and port forwarding (PF) independently. The SBC 1000/2000 system employs NAPT rather than basic NAT (see RFC 3022 for more information) such that the SBC only exposes a single IP address (Node IP Address) to the public network instead of a range of IP addresses.

If you intend to use both NAT and port forwarding, Sonus recommends that you first make sure that the NAT configuration is tested and working properly.

General Feature Configuration

The feature must be configured such that distinct private and public (external) networks are connected to separate Ethernet (ETH1 and ETH2) interfaces. The SBC logical interfaces are specified in the NAT Interface Table page of the UI. The private networks are all networks not connected to the external (public) interface.

Network devices and servers connected to the private network must be configured such that the SBC 1000/2000 private interface is specified as their gateway address.

Copyright © 2015 Sonus Networks. All rights reserved.

Secondary IP Address Restrictions

Neither the internal (private) or the external (public) network may be connected to a secondary IP address.

Access Control List (ACL) Restrictions

If you are using ACLs, you must assure that the defined rules do not block the forwarded port connections. For more information about Access Control Lists on the Sonus SBC 1000/2000 see: Managing Access Control Lists.

Maximum Port Forwarding Entries

The Port Forwarding Table is limited to a maximum of 20 entries.

Internal Device Firewall Settings

When port forwarding is used, assure that the firewall (if applicable) on the destination device or server allows traffic to through those ports specified in the port forwarding table entry associated with the device's IP address.

Reserved TCP and UDP Ports

There are a number of ports that are reserved by the SBC for internal functions, none of which may be specified when configuring port forwarding. A list of reserved ports can be found on the Creating and Modifying Entries to the NAT Port Forward Table documentation page.

Managing NAT Interface Tables

- Creating and Modifying Entries to the NAT Interface Table

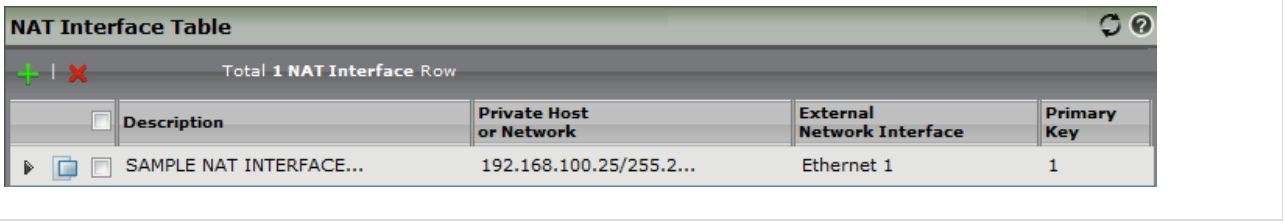
Managing Port Forwarding Tables

- Creating and Modifying Entries to the NAT Port Forward Table

Managing NAT Interface Tables

Working with NAT Interface Tables

1. In the WebUI, click the **Setting** tab.
2. In the left navigation pane, go to **Protocols > IP > NAT > NAT Interface**.



To view a table entry's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

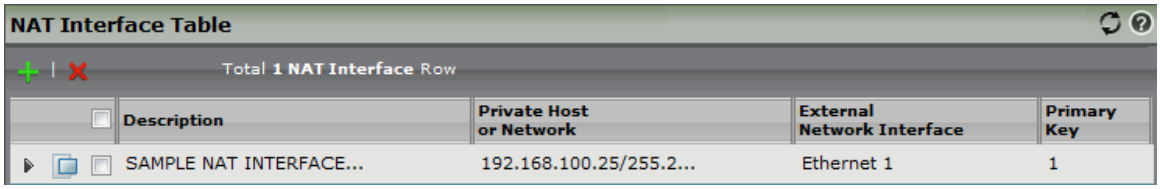
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Copyright © 2015 Sonus Networks. All rights reserved.

Creating and Modifying Entries to the NAT Interface Table

To create or modify an existing NAT Interface Table entry:

1. In the WebUI, click the **Setting** tab.
2. In the left navigation pane, go to **Protocols > IP > NAT > NAT Interface**.



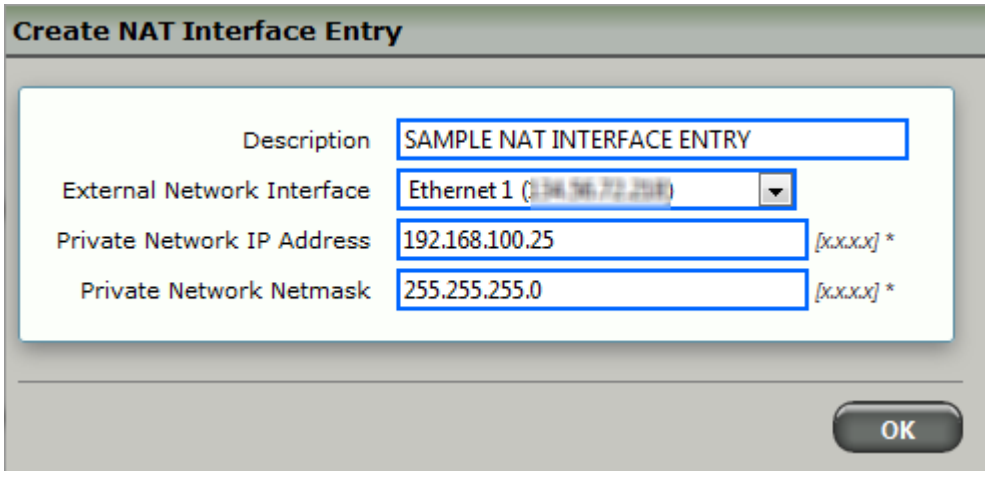
Modifying a NAT Interface Table Entry

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a NAT Interface Table Entry

To create an entry:

1. Click the **Create NAT Interface Entry** ( ) icon.



NAT Interface Table Entry - Field Definitions

External Network Interface

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the SBC logical interface connected to the external network. Any of the SBC's Ethernet or VLAN, except the Loopback Interface, may be used.
For more information about network interfaces see: Managing Logical Interfaces.

Private Network IP Address

Specifies the IPv4 IP address used to identify the host or network to which NAT will be applied.

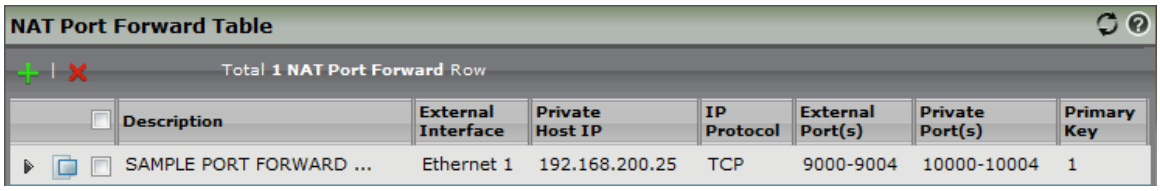
Private Network Netmask

Specifies the IP Netmask used to identify the host or network to which NAT will be applied. A value of **255.255.255.255** in this field indicates that the IP Address specified in the **IP Address** field is a specific host.

Managing Port Forwarding Tables

Working with NAT Port Forwarding Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > NAT > Port Forward**.



To view a Port Forwarding Table entry's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

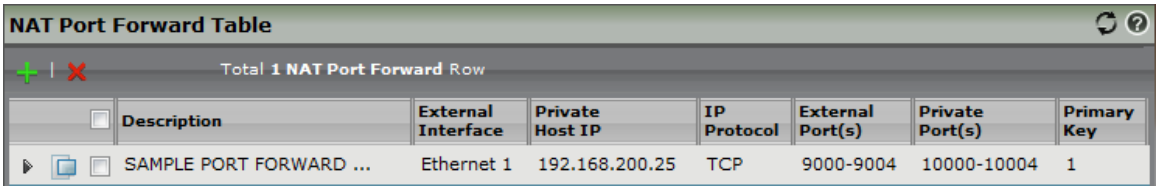
Creating and Modifying Entries to the NAT Port Forward Table

Creating and Modifying Entries to the NAT Port Forward Table

To create or modify an existing Port Forward Table entry:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > IP > NAT > Port Forward**.

Copyright © 2015 Sonus Networks. All rights reserved.



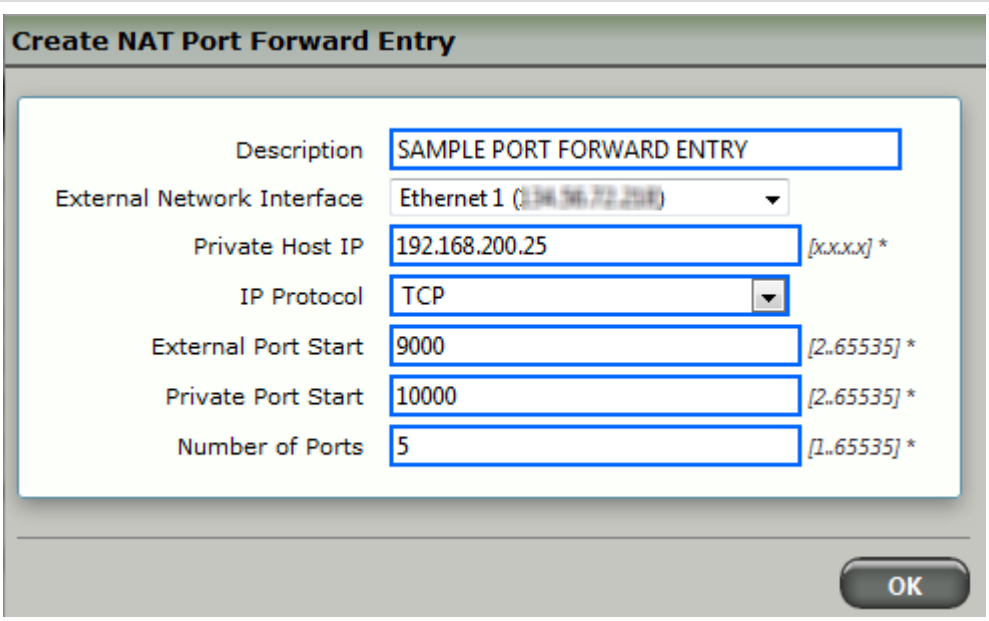
Modifying a Port Forward Table Entry

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating a Port Forward Table Entry

To create a Port Forward Table entry:

1. Click the Create NAT Port Forward Entry ( )icon.



NAT Port Forward Table Entry - Field Definitions

External Network Interface

Specifies the SBC logical interface connected to the external network. Any of the SBC's Ethernet or VLAN, except the Loopback Interface, may be used.

Private Host IP

Specifies the IPv4 address of the port forward destination on the private network.

IP Protocol

Specifies the IP protocol allowed in the port forwarded connection.

Copyright © 2015 Sonus Networks. All rights reserved.

External Port Start

Specifies the first IP port number to use on the external network. The specified port may not be one of the SBC1000/2000 reserved ports.

Private Port Start

Specifies the first IP port number to use on the private network.

Number of Ports

Specifies the number of ports to map from the external network to the private. No port in the resulting range may be one of the SBC1000/2000 reserved ports.

SBC Reserved Ports

Port	Protocol
1	RAW
22	TCP
53	TCP
80	TCP
161	UDP
443	TCP
500	UDP
514	UDP
4500	UDP
30000	UDP
30001	UDP
16384 through 16984	RTP

Note: RTP ports are configurable as part of the Media System configuration. Ports used by Media System may not be used for port forwarding.

Working with Branch Survivability

The Branch Survivability feature monitors multiple network links between a branch office and Headquarters. I employs the preferred/low-cost link to provide automatic fail-over to operational links

Copyright © 2015 Sonus Networks. All rights reserved.

The Branch Survivability module monitors the primary WAN connection, when it detects a failure and if that failure persists for predetermined amount of time, it makes the necessary changes in the routing table to route all IP packets through the 3G/4G network. Additionally, it sends a notification to the IPSec module when fail-over event occurs, so that IPSec can create secure tunnel if necessary. It also sends a notification to the Lync ASM module at the HQ site to modify the bandwidth control on the Lync server(s).

Configuring 3G4G Failover

Managing Link Monitor Configuration Tables

- Creating and Modifying Link Monitor Configuration Table Entries

Managing Lync CAC Profiles

- Creating and Modifying Lync CAC Profile Table Entries

Configuring 3G4G Failover

The following describes the process for configuring and testing the 3G4G fail-over feature on the Sonus SBC 1000/2000.

Feature Overview

Many enterprises employ multiple branch sites connected to the headquarters (HQ) facility through a WAN link provided by a telecom vendor. Microsoft Lync ® clients at the branch office maintain connectivity with the corporate Lync server located at the headquarters. In the event of a telecommunication failure the WAN link may fail, thereby breaking connectivity between the branch and the HQ.

Sonus SBC devices are capable of interoperating with Microsoft's Lync solution for branch survivability in the event of such network failures. An SBC 1000 or SBC 2000 deployed at the branch-site can monitor the network links, identify such failures and switchover to a backup network connection, restoring IP layer connectivity between the branch.and HQ. Thereafter by using the configuration data, voice and data connectivity may be restored between the branch and HQ, taking into account the security of data over the public Internet and the fact that the 3G/4G backup network connection usually has less bandwidth than the WAN link.

Related Documentation

Working with Branch Survivability
Managing Link Monitor Configuration Tables
Managing Lync CAC Profiles

Prerequisites

1. Licenses: RBA and IPsec license must be installed on the HQ-SBC, and IPsec on the branch office SBA. The IPsec license is bundled with the RBA license.
2. Backup Network connection - typically in the form of a 3G/4G/DSL/cable-modem router.
3. VLAN Capable Ethernet Switch - If an SBC 1000 is used in the branch-site, there may be a requirement for an external VLAN Capable Ethernet switch, as SBC 1000 has only two Ethernet ports. One such Ethernet port is typically connected to the branch network. The other Ethernet link must be shared for communication with the two gateways (primary WAN, secondary 3G4G) by using tagged VLANs.
4. An ASM Module at the HQ-site running the RBA image.
5. A functional 3G/4G network, always online (some of the 3G/4G routers disable the cellular uplink in idle conditions).

Copyright © 2015 Sonus Networks. All rights reserved.

6. The HQ SBC must be reachable on the DMZ without VPN on its WAN-side IP address (this IP address is typically configured as the "remote address" in IPsec tunnel configuration).
7. When host monitoring is enabled, the monitored host must be a system in the HQ network. This system is monitored by the Branch SBC using ICMP. Hence the firewall at the HQ must be configured such that the ICMP packet exchange between the Branch SBC and the monitored-host are accepted/forwarded over the 3G network as well as the WAN network.

About the ICMP-Reachability Requirement

We expect that the typical deployment has:

1. Branch-SBC monitoring both the primary gateway and the secondary gateway.
2. Branch-SBC monitoring a host at the HQ (to help detect failures along the path).

The host must be made reachable with ICMP on both the primary path and the secondary path. Customers networks differ in these aspects (which is of course why we have the beta process). The following two issues may arise:

1. If the host is in the DMZ zone, it is reachable through the secondary(3G) path, but may not be reachable through the primary path.
2. If the host in the corporate network, it is reachable through the primary path, but may not be ICMP-reachable unless IPsec is setup.

One of the above two scenarios must work, in order for host-monitoring to work. For comparison, at Sonus/NET, both the examples above work. Hosts in the DMZ zone are reachable on both the paths. Hosts in the corporate network are also ICMP-reachable on both the paths without IPsec/VPN (only ICMP, but for all other protocols, IPsec/VPN is required). We will have to use one of the above two methods at the customer sites to enable/configure host-monitoring.

Configuration

HQ Lync Configuration

A full Lync configuration must be deployed at the HQ location. The following steps must be performed in addition to the usual configuration procedure.

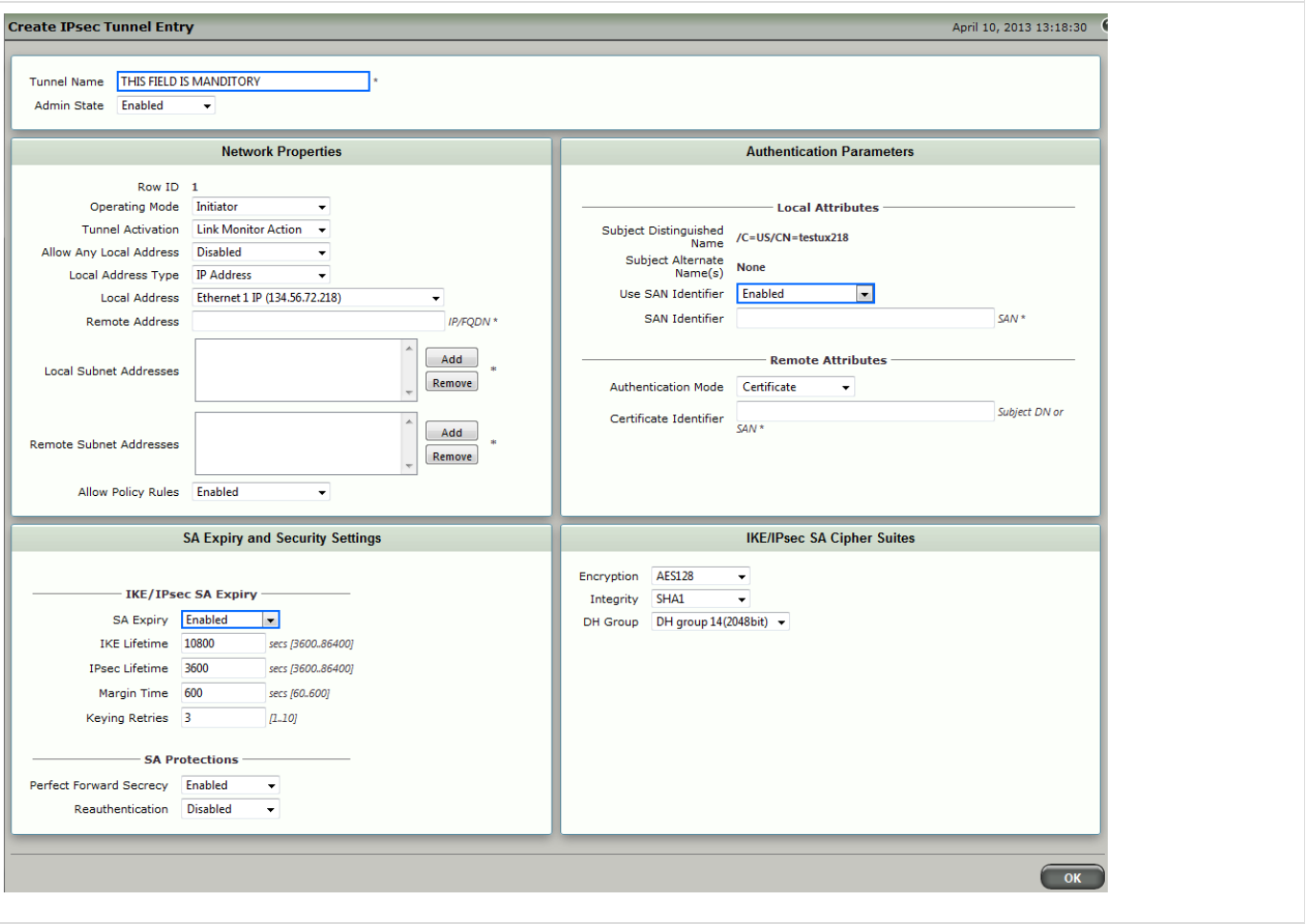
1. Create a Policy Profile for the branch.
   For example, if the name of the branch is *Taveuni*, the policy-profile should be appropriately named as *TaveuniCAC*. The name of the Policy Profile is extremely important and is required when the Branch SBC is configured.
2. On the Lync server, a *subnet* is associated with a *site*. A site is associated with a region. Region-to-region links may then be created and associated with a CAC Profile. These steps must be performed on the Lync server using the standard Lync configuration procedure.
3. Configure a PSTN Gateway on Lync using the IP address of the Branch SBC.
4. At the HQ Active Directory server used by the Lync setup, the HQ-ASM computer must be made a member of the RTCUniversalServerAdmins group. All CAC updates are performed by the HQ ASM computer with the computer's token and not the user's token.
   a. While setting the group membership, Group Policy Refresh settings must be verified. Since AD settings are propagated to the domain computers based solely on the AD Group Policy Setting configurations, the HQ ASM might not have the correct permissions immediately. To ensure the proper operation of the HQ ASM in updating the CAC Policy on the Lync server database, the ASM module may require a reboot. The specific settings are: *Group Policy Refresh Interval* and *Turn off group policy refresh*.

Copyright © 2015 Sonus Networks. All rights reserved.

HQ-RBA (HQ-ASM) Configuration

1. In Active Directory the HQ ASM computer (hostname) must be a member of the group RTCUniversalServerAdmin. The membership enables the HQ RBA software to modify CAC profiles on the Lync server's data base.
2. The HQ ASM must use the RBA image that is delivered as part of the 3.0.0 release. The deployment steps must involve the following at a minimum.
    a. Configure IP addressing, DNS servers and default gateways (unchanged from any SBA deployment).
    b. It must join the same Windows domain as the Lync server (unchanged from SBA deployment). In order to join the domain, a Domain User account is required. This account does not have any special group membership or security requirements. It only needs to be a regular Domain User account.

Branch IPsec Configuration



1. **Tunnel Activation**: Link Monitor Action.
   This field indicates that this tunnel is activated/deactivated automatically, when a specific gateway is in use (configured under Link Monitor).
2. **Local address**: Any.
3. **Remote address**: HQ SBC's IP address that leads to the Internet. Must be on the DMZ so that it is reachable for setting up the IPsec tunnel.
4. **Local Subnet Address**: Branch subnet.
5. **Remote Subnet Address**: Subnets in the branches that house the Lync and Exchange server.

HQ IPsec Configuration

Copyright © 2015 Sonus Networks. All rights reserved.

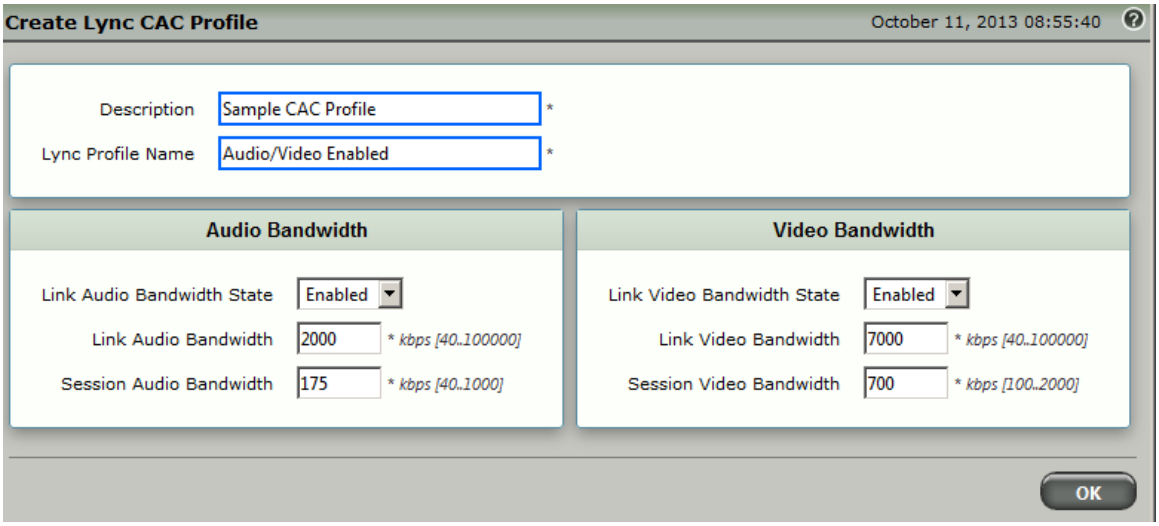
See Figure Above

1. **Operating Mode**: Responder.
2. **Local Address**: Select the interface leading to the Internet.
3. **Remote Address**: Any.
4. **Local Subnet Addresses**: Choose the subnets that have the Lync server, Exchange server.
5. **Remote Subnet Addresses**: branch subnet(s).

Branch Site CAC Profiles

At the branch site, one CAC Profile must be configured for each of the next-hop gateways.

Lync maintains only one bandwidth policy for each branch. The same name must be used as *Lync Profile Name* in the CAC Profile.



The CAC Profile description is a free-form text field. However, the operator should write a concise description such that it identifies the type of the nexthop gateway or the network. For example, one would configure the Lync profile for the Taveuni branch as *TaveuniCAC*. The CAC Profile description for the MPLS gateway would be *Taveuni CAC over MPLS Sprint* and for the 3G-gateway, *Taveuni CAC over Verizon 3G*.

Typically, the CAC Profile associated with the MPLS-gateway enables both video and audio depending on the bandwidth of that link. The CAC Profile associated with the 3G/4G link may enable audio but typically not video as the bandwidth over a cellular WAN link is much lower than a wired WAN link. The audio may be completely disabled on the 3G/4G link so that PSTN/TDM ports are used for the media traffic from Lync calls.

At the HQ, it is still permissible to have a gateway for each of the possible paths into the Internet or to the branch sites. Each gateway must still be associated with a reasonable CAC profile, even though there is no real end-use for configuring CAC profiles at the HQ. The Lync configuration does not use CAC profile information for the HQ, it uses only the CAC profiles associated with the branch sites.

Branch Site Link Monitor

1. Configure two default static routes, one for the WAN gateway and one for the 3G/4G gateway.
2. Make sure that the Lync setup works between the branch and the HQ over the MPLS WAN gateway.
3. Configure two link-monitor entries, one for each of the gateways.
    a. If a host is monitored in addition to the gateways, then it must be the FQDN or IP address of a host on the HQ network and not on the DMZ network. For example, this can be the FQDN or IP address of the

Copyright © 2015 Sonus Networks. All rights reserved.

Lync server or the IP address of the HQ SBC on the HQ side (not on the DMZ/Internet side) interface. In more precise terms, the selected FQDN satisfies all the following conditions.

i. On a path that does not require IPsec, the monitored host must be reachable without IPsec.
ii. On a path that requires IPsec, the monitored host must not be reachable unless and until the IPsec tunnel set up. As an example, the monitored host must not be the same as the remote address of a IPsec tunnel in the 3G network.

4. On the 3G/4G gateway, associate the IPsec tunnel from branch to HQ.
5. Perform a switchover from the WAN link and make sure that the IPsec tunnel is automatically established over the 3g/4g link.

Branch and HQ SIP SG and SIP Server Configuration

1. SIP SG between Branch SBC and HQ SBC, and the SIP SG used between Branch SBC and HQ Lync must be in the bind/bind mode. The IP address must be the IP address of the Branch SBC on the branch subnet side. It must not be from the interface leading to the HQ/Internet.
2. The SIP SG between HQ SBC to Branch SBC must be in the bind/bind mode. The IP address must be the IP address of the HQ SBC on the HQ subnet side. It must not be the one leading to the branch/Internet.
3. (All systems in all branches and HQ know the Branch SBC by its FQDN or by its address on its branch subnet)
4. SIP Server Config
    a. The Branch SBC must use the remote subnet side IP address of the HQ SBC as the SIP server IP address for the SIP SG between the Branch SBC and the HQ SBC.
    b. The HQ SBC must use the remote subnet side IP address of the Branch SBC as the SIP server IP address for the SIP SG between the HQ SBC and the Branch SBC.
5. Federated IP/FQDN - Configuration of this depends on the SIP server configuration. HQ side SIP SG should use the branch subnet as the Federated IP/FQDN and vice versa. The IP addresses of the subnets between the HQ SBC and the Branch SBC should not be used.

STUN Setting

- STUN must be enabled (Media System Configuration) on branch SBC and HQ SBC. It is required for the IPsec feature to work.

Branch Site SIP Notification

- In the SIP SG from Branch SBC to HQ SBC, select **Enabled** in the *Notify CAC Profile* list box. This allows the CAC Profile information to be sent as a header in the NOTIFY messages sent from the branch to all SIP servers configured for that SIP SG.

Branch Site PSTN Connectivity

When Lync realizes that the branch-SBC is connected to the HQ over a low-bandwidth link, as identified by the parameters of the CAC Profile, it forwards all Lync calls (from the branch Lync clients) to a different destination, by sending a new INVITE directly to the branch-SBC. In this context, the branch SBC is configured as the PSTN Gateway on the Lync server.

1. In order for this to work, SIP signaling groups between the Branch SBC and the the HQ Lync server must use TLS.
2. The Branch SBC must be configured such that the SIP INVITE packets trigger call set up over the PSTN (TDM). Note that all signaling packets to establish such calls are occurring over the 3G/IPsec link, but only the media is rerouted over the PSTN call.
    a. Typically the branch site has PSTN connectivity over a T1/E1 link or FXO ports.

Managing Link Monitor Configuration Tables

Copyright © 2015 Sonus Networks. All rights reserved.

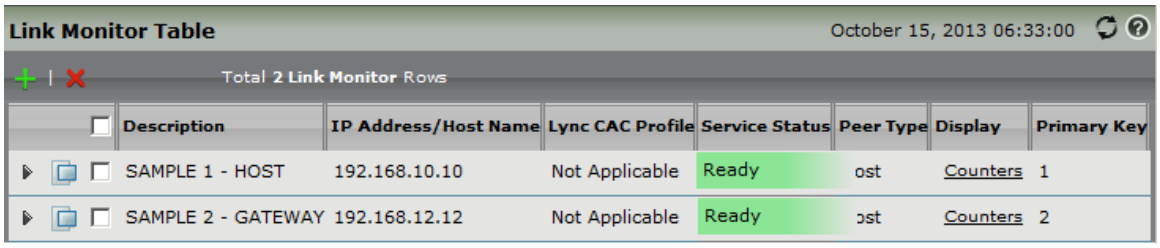
Prerequisites

The following items must be configured before a Link Monitor Configuration Table entry can be successfully created:

- At least one Lync CAC Profile must exist before a Link Monitor Configuration can be created.
- At least one IPsec Connection Table must exist.

Working with Link Monitor Configuration Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > Network Monitoring > Link Monitor Configuration**.



To view a Link Monitor Configuration Table entry;s properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

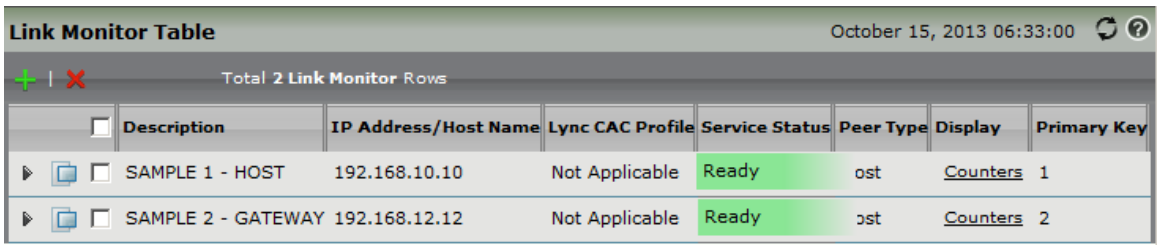
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Creating and Modifying Link Monitor Configuration Table Entries

Creating and Modifying Link Monitor Configuration Table Entries

To Create a Link Monitor Table entry:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > Network Monitoring > Link Monitor Configuration**.



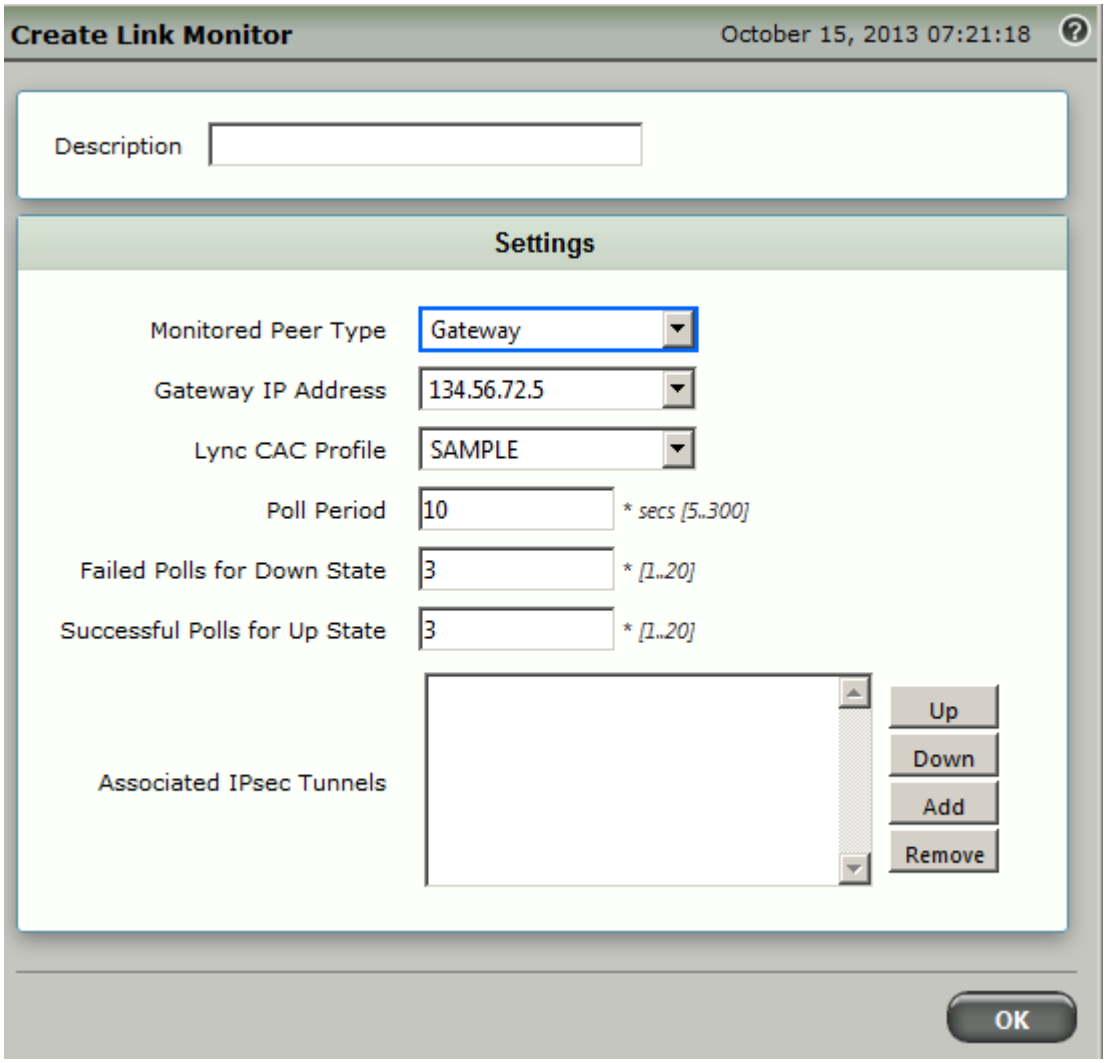
Modifying a Link Monitor Configuration Table entry

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Copyright © 2015 Sonus Networks. All rights reserved.

Creating a Link Monitor Configuration Table Entry

1. Click the **Create Link Monitor Configuration** (✚) icon at the top of the Link Monitor Confituration Table Page.



Settings - Field Definitions

Monitored Peer Type

Specifies the type, either host or gatway, that the link is monitoring.
If the peer type is host, the ICMP Echo and Echo Reply is the the protocol used. If the peer is a gateway, the protocol is ARP request/reply.

Host Name

Specifies the address of the host to monitor. The entry must be in IPv4 format or the Fully Qualified Domain Name (FQDN) of the host being monitored. This field is only visible when **Host** is selected in the **Monitored Peer Type** select list.

Gateway IP Address

Copyright © 2015 Sonus Networks. All rights reserved.

The IPv4 address of the gateway. This field is only visible when **Gateway** is selected in the **Monitored Peer Type** select list.

Lync CAC Profile

Use this to select a pre-configured Lync CAC profile. The Lync CAC profile information is sent to the HQ Lync server once each five minutes and after performing an IP layer reroute following a failure (if configured).

Poll Period

Specifies the polling interval, in seconds, for testing the link status. The host or the nexthop gateway specified by HostIpAddress is probed once each specified interval.

Failed Polls for Down State

Specifies the number of consecutive failed polling attempts made against the host specified in Host IP Address field after which the host is declared to be in a **down** state. When the gateway is declared **down**, the associated IPsec tunnel is torn down.

Successful Polls for Up State

Specifies the number of unreplied or unsuccessful polls made against the host specified in Host IP Address field before declaring this gateway or host as service ready.

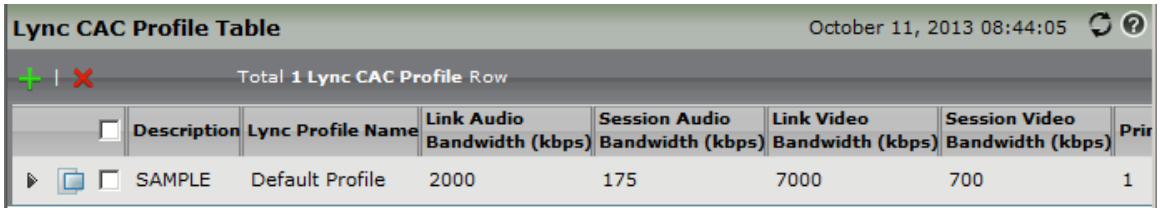
Associated IPsec Tunnels

Use this field to select a maximum of four pre-configured IPsec tunnels. Only visible when **Gateway** is selected in the **Monitored Peer Type** list box.

Managing Lync CAC Profiles

Working with Lync CAC Profiles

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > Network Monitoring > Lync CAC Profiles**.



To view a Lync CAC profile's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

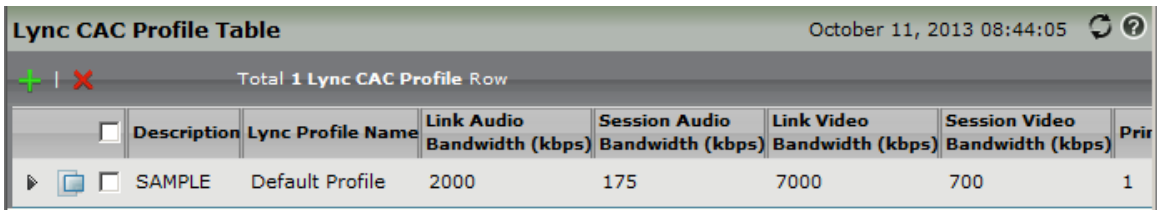
Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Copyright © 2015 Sonus Networks. All rights reserved.

Creating and Modifying Lync CAC Profile Table Entries

To Create a Lync CAC Profile Table entry:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Protocols > Network Monitoring > Lync CAC Profiles**.

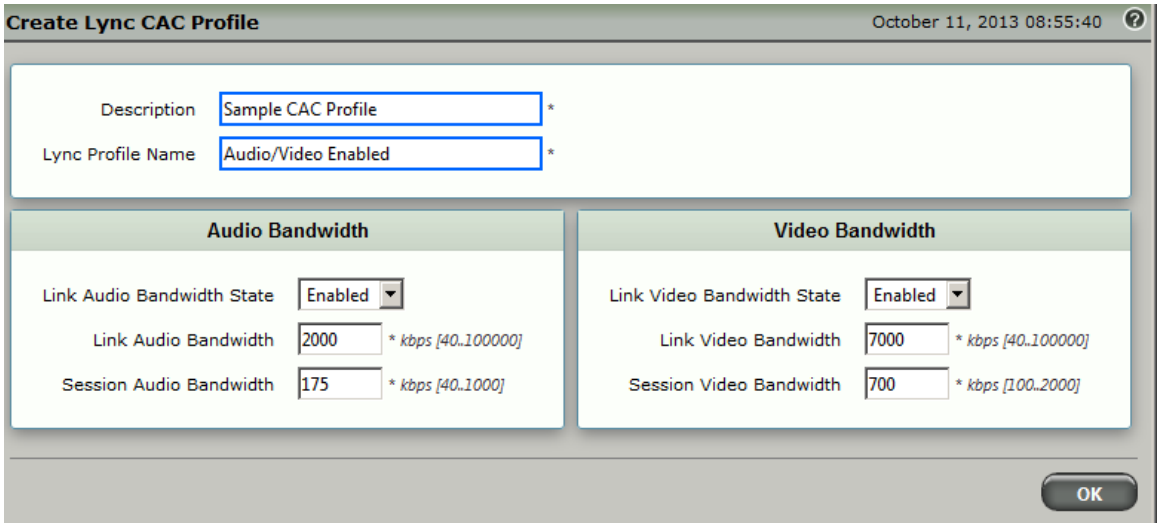


Modifying a Lync CAC Profile Table entry

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Adding a Lync CAC Profile Table Entry

1. Click the **Create CAC Profile** ( ) icon at the top of the Lync CAC Profile Table Page.



Audio Bandwidth - Field Definitions

Link Audio Bandwidth State

Enables or disables audio on this link.

Total Link Audio Bandwidth

Copyright © 2015 Sonus Networks. All rights reserved.

Specifies the total link audio bandwidth.

Total Session Audio Bandwidth

Specifies the maximum audio bandwidth for a single session (call).

Video Bandwidth - Field Definitions

Link Video Bandwidth State

Enables or disables video on this link.

Total Link Video Bandwidth

Specifies the total link video bandwidth

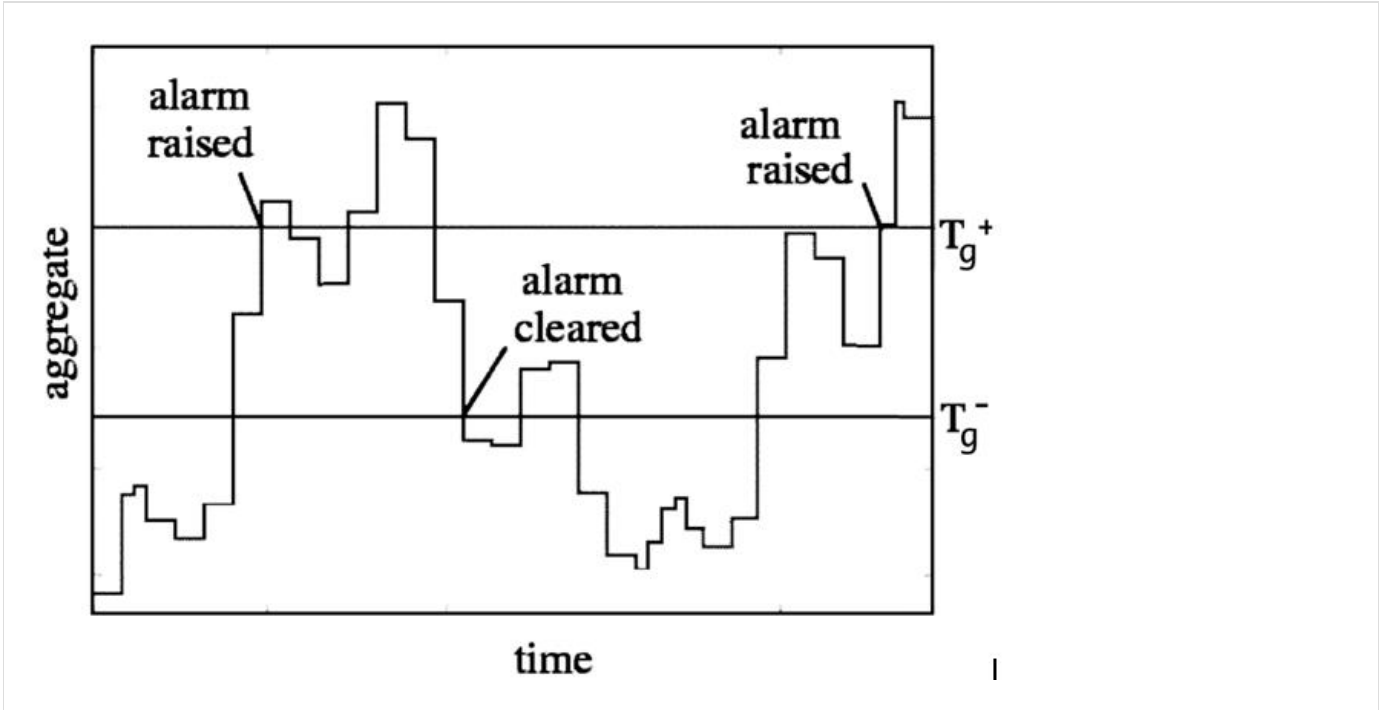
Total Link Audio Bandwidth

Specifies the maximum audio bandwidth for a single session (call).

Working with Historical Data and TCA Thresholds

Overview

The collection of historical data and Threshold Crossing Alerts (TCA) provides a facility for understanding the long-term utilization and call traffic characteristics of the SBC 1000/2000. The collection and analysis of this data over an extended period of time produces a clearer picture of how the node is being utilized and provides information necessary to properly modify its capacity. The TCA Thresholds feature allows the administrator to configure thresholds for monitoring real-time statistics. An alarm is raised when a user defined threshold for a particular attribute is crossed.



Copyright © 2015 Sonus Networks. All rights reserved.

Statistics

The node collects the statistics listed in the table below. Each statistic has user configurable ***Raise*** and ***Clear*** alarm thresholds. An alarm is raised when the Raise threshold is exceeded, and conversely the alarm is cleared when the statistical value drops below the Clear threshold

Statistic	Minimum Threshold Range	Maximum Threshold Range	Period	History Range
Signaling Group Channel Usage (peak)	0 (Number of channel per Signaling Group minus 1)	1 - Number of channels per Signaling Group	1 Min	1 Day
SIP Call license Usage	0 (Number of licenses minus 1)	600	1 Min	1 Day
SIP Registration	0 (Configured registrations minus 1)	500	10 Minutes	1 Day
DSP Usage (peak)	0%	100%	1 Min	1 Day
CPU Usage	0%	100%	1 Min	1 Day
Memory Usage	0%	100%	1 Min	1 Day
File Descriptor Usage	0	4000	1 min	1 Day
1 Minute Load Average	1 (increments of 100% CPU usage)	5	1 min	1 Day
5 Minute Load Average	1	5	5 min	1 Day
15 Minute Load Average	1	5	15 min	1 Day
Temporary Partition Usage	0%	100%	1 min	1 Day
Logging Partition Usage (SBC2000 Only)	0%	100%	1 min	1 Day

Logging Partition Usage Applicability

The Logging Partition Usage statistics and its related alarms and events are only applicable to the SBC2000.

- Period: How often the statistic is collected.
- History Ranges: How long the collected statistic is retained.

Alarms and Events

TCA Type	Alarm (ID)	Event (ID)
Signaling Group Channel Usage	TCA Threshold Exceeded	TCA Threshold Cleared
SIP Call license Usage	TCA Threshold Exceeded	TCA Threshold Cleared
SIP Registration	TCA Threshold Exceeded	TCA Threshold Cleared

Copyright © 2015 Sonus Networks. All rights reserved.

DSP Usage	TCA Threshold Exceeded	TCA Threshold Cleared
CPU Usage	TCA Threshold Exceeded	TCA Threshold Cleared
Memory Usage	TCA Threshold Exceeded	TCA Threshold Cleared
File Descriptor Usage	TCA Threshold Exceeded	TCA Threshold Cleared
1 Minute Load Average	TCA Threshold Exceeded	TCA Threshold Cleared
5 Minute Load Average	TCA Threshold Exceeded	TCA Threshold Cleared
15 Minute Load Average	TCA Threshold Exceeded	TCA Threshold Cleared
Temporary Partition Usage	TCA Threshold Exceeded	TCA Threshold Cleared
Logging Partition Usage	TCA Threshold Exceeded	TCA Threshold Cleared

Managing TCA Thresholds

- Configuring TCA Thresholds

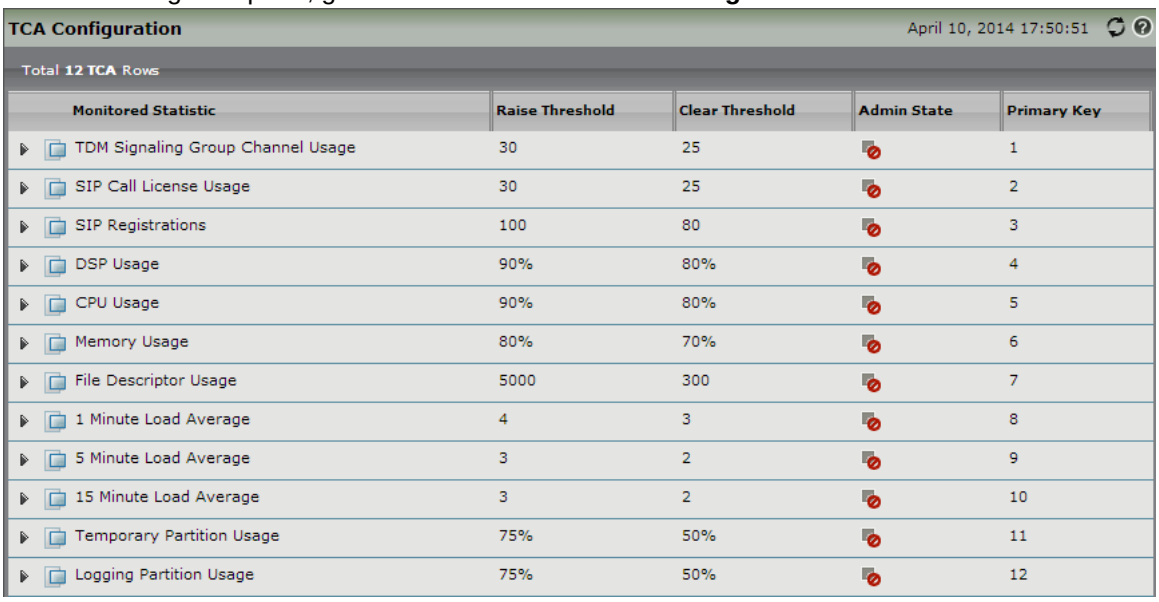
Retrieving Data

Statistics data are available through the REST interface. For more information about using the REST interface see the SBC 1000/2000 REST Documentation.

Managing TCA Thresholds

Working with TCA Thresholds

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SNMP/Alarms > TCA Configuration**.



Copyright © 2015 Sonus Networks. All rights reserved.

To view a monitored statistic's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

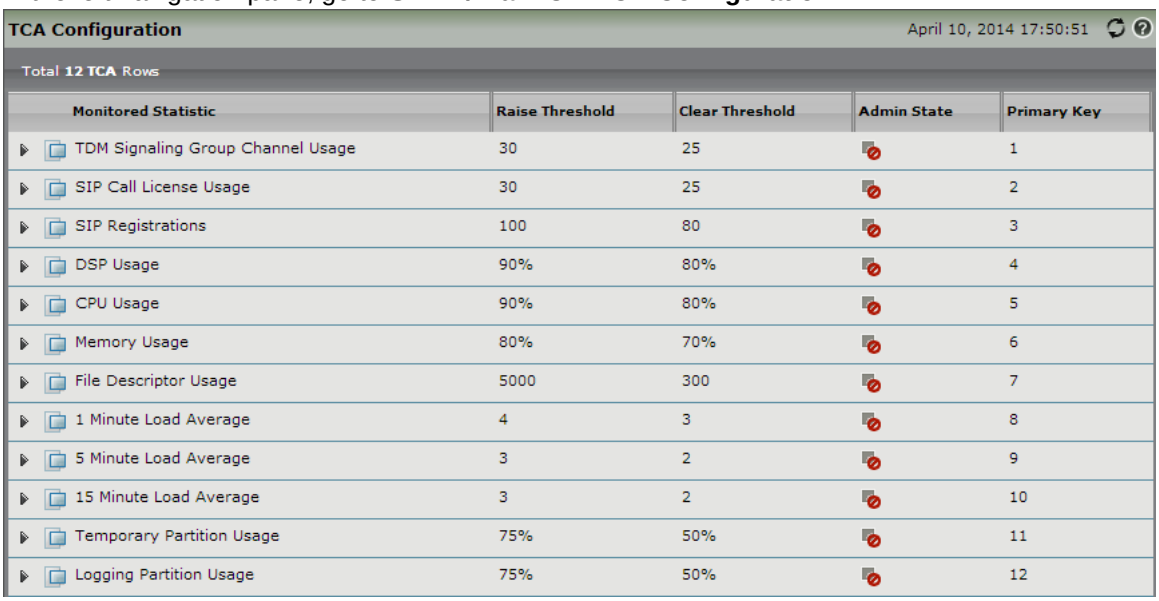
> **Helpful Tip:** To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

Configuring TCA Thresholds

Configuring TCA Thresholds

To create or modify an existing SIP Signaling Group:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SNMP/Alarms > TCA Configuration**.



Monitored Statistic	Raise Threshold	Clear Threshold	Admin State	Primary Key
TDM Signaling Group Channel Usage	30	25		1
SIP Call License Usage	30	25		2
SIP Registrations	100	80		3
DSP Usage	90%	80%		4
CPU Usage	90%	80%		5
Memory Usage	80%	70%		6
File Descriptor Usage	5000	300		7
1 Minute Load Average	4	3		8
5 Minute Load Average	3	2		9
15 Minute Load Average	3	2		10
Temporary Partition Usage	75%	50%		11
Logging Partition Usage	75%	50%		12

Configuring a TCA Threshold

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

TCA Statistic Attribute - Field Definitions

Admin State

When enabled, the feature raises and clears the the alarm for the statistic. When disabled, the SBC continues to collect data but does not raise or clear alarms.

Copyright © 2015 Sonus Networks. All rights reserved.

Raise Threshold

Specifies the value which the monitored statistic must match or exceed for the alarm to be raised.

Clear Threshold

Specifies the value which the monitored statistic must match or fall below for the clearing even to be sent.

Working with Multiple Spanning Trees

This section contains information about configuring the SBC 1000/2000 to operate within multiple spanning trees in a network.

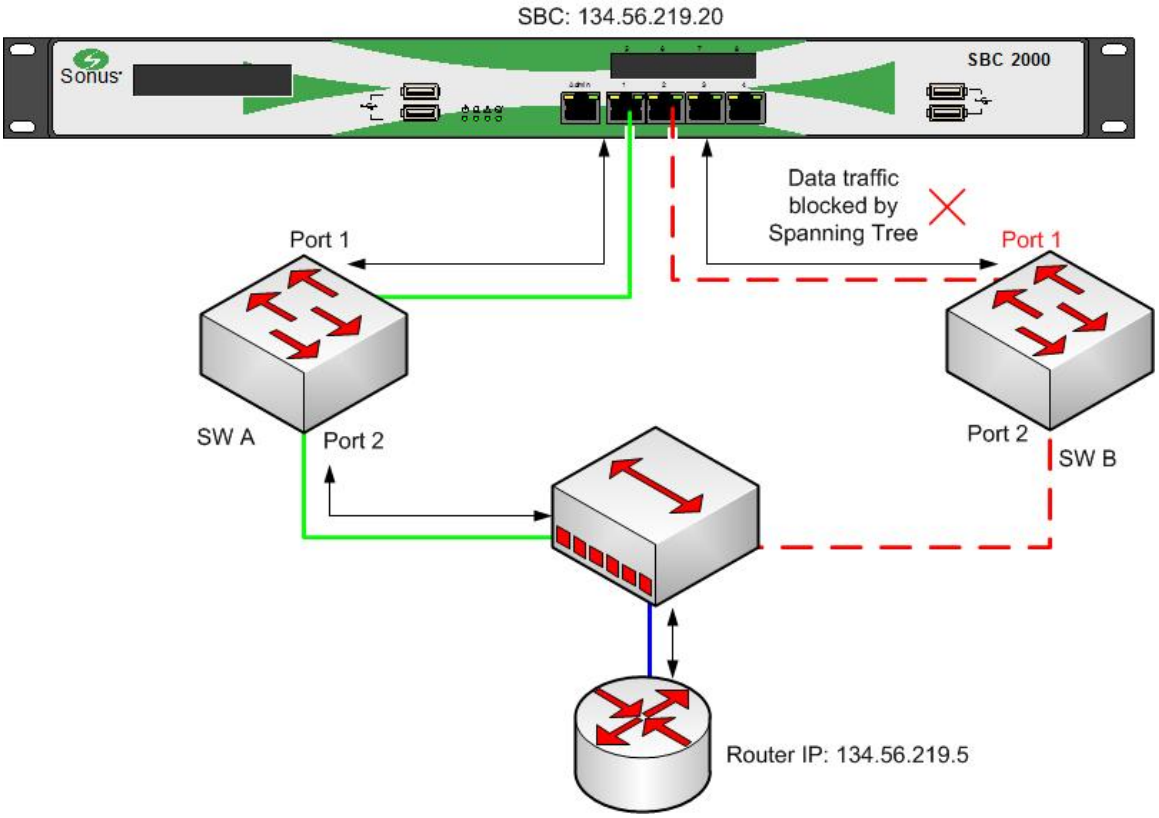
Important Notes:

- Region Settings
  - The Region Name must be the same on all switches and nodes in the tree.
  - The Revision must be the same on all switches and nodes in the tree.
- MSTP Instances
  - The MST ID & VLAN associated to a given Instance ID must be configured identically on all MSTP capable devices on the network.

Introduction

A network topology of bridges typically contains redundant connections to provide alternate paths in case of link failures. Since there is no concept of time-to-live (TTL) in Ethernet frames, this could result in permanent circulation of frames if there are loops in the network. To prevent loops, a spanning tree connecting all the bridges is formed in real time. The standby/redundant ports are put in a discarding (non-forwarding) state. They are enabled when required.

Copyright © 2015 Sonus Networks. All rights reserved.



Default Conditions

On initial startup, the all ports are members of the default MSTP instance, which is disabled by default.

Limitations

A maximum of 32 user defined MSTP instances may be created.

Child Pages

Managing MST Instances

- Creating and Modifying MST Instances
- Viewing MSTI Statistics

Modifying Region Settings

Managing MST Instances

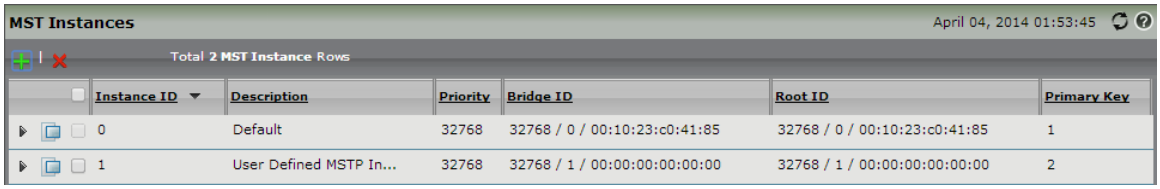
Important Note

- Port priority (lowest number has highest priority) determines the order in which the node will attempt to associate its ports to a spanning tree. If all the ports are assigned the same priority (default: all = 128) then node will prioritize as ETH1, ETH2, ... ETH4. This in order of ascending value of MAC addresses.

Working with MST Instances

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Bridge > MSTP > MST Instances**.



To view an MST Instance's properties:

1. Click the popup( ) icon next to the entry you want to view.
2. When you are finished, close the window.

Helpful Tip: To delete an entry, simply select the checkbox next to the entry you wish delete, then click the Delete ( ) icon located at the top of the window.

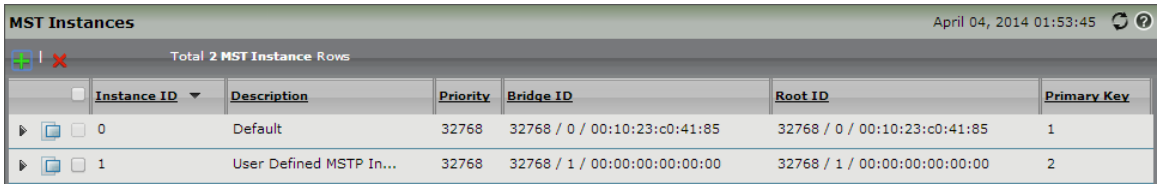
Creating and Modifying MST Instances

Viewing MSTI Statistics

Creating and Modifying MST Instances

To create or modify an MST Instance:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Bridge > MSTP > MST Instances**.



Modifying an MST Instance

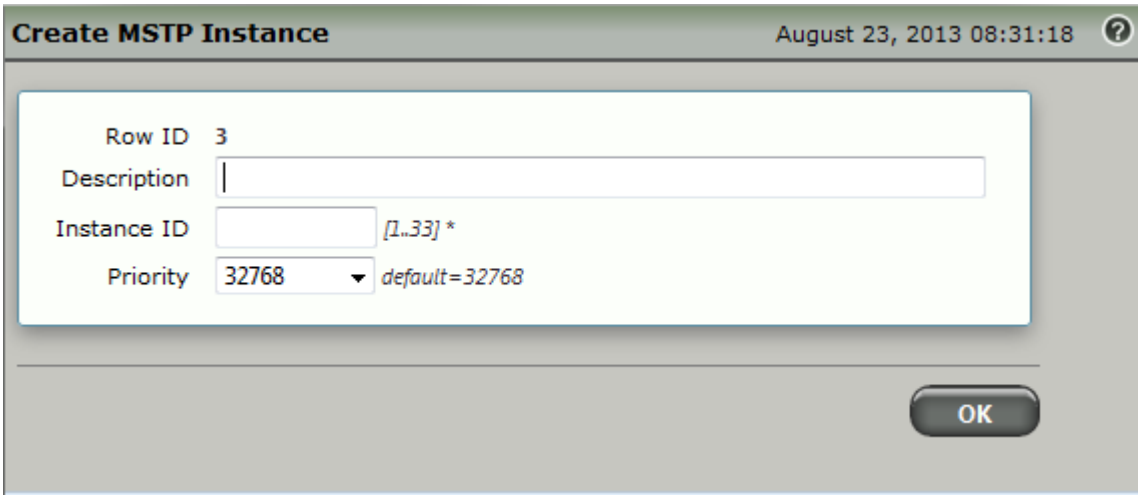
1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Creating an MST Instance

You may create a maximum of 31 MST Instances,

1. Click the Create MST Instance ( ) icon at the top of the MST Instances page.

Copyright © 2015 Sonus Networks. All rights reserved.



MST Instance - Field Definitions

Description

A descriptive name for the instance.

Instance ID

A unique integer identifier for this instance.

Priority

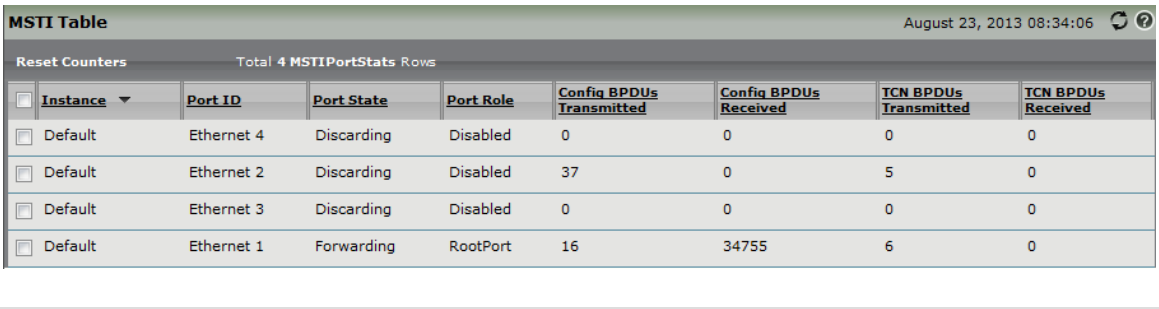
MSTP instance's priority in increments of 4096. The lower the priority, the higher the chances of this SBC becoming the root bridge.

Viewing MSTI Statistics

Viewing MSTI Statistics

To view MSTI Statistics:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Bridge > MSTP > MSTI Statistics**.



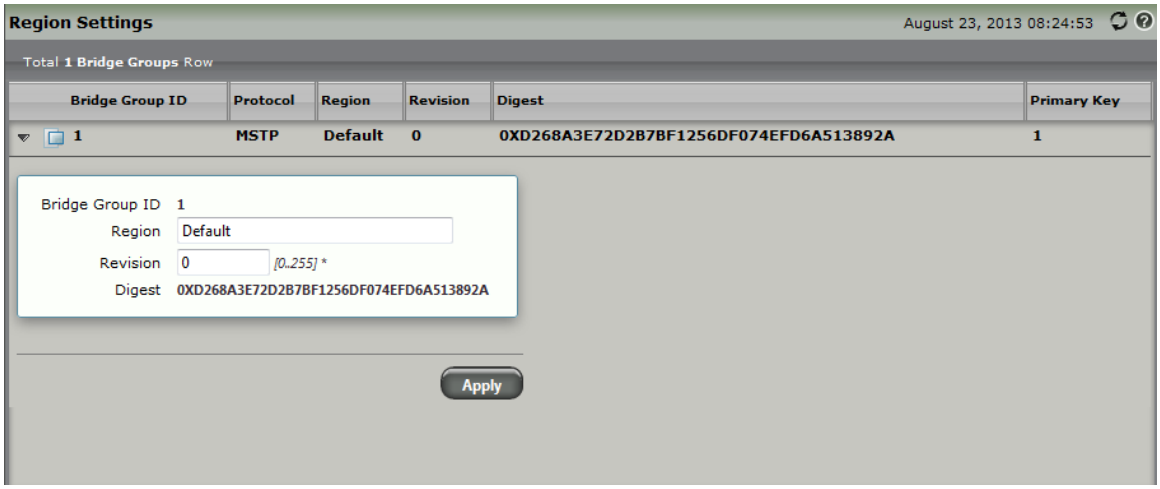
Instance	Port ID	Port State	Port Role	Config BPDUs Transmitted	Config BPDUs Received	TCN BPDUs Transmitted	TCN BPDUs Received
Default	Ethernet 4	Discarding	Disabled	0	0	0	0
Default	Ethernet 2	Discarding	Disabled	37	0	5	0
Default	Ethernet 3	Discarding	Disabled	0	0	0	0
Default	Ethernet 1	Forwarding	RootPort	16	34755	6	0

Modifying Region Settings

To modify the region settings:

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Bridge > Region Settings**.



Modifying the Region Settings

1. Click the **expand** ( ) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.

Region Settings - Field Definitions

Region

Region name of the MSTP region to which SBC is being connected.

Revision

Revision ID for the MSTP region to which SBC is being connected.

About Signaling Groups
Working with RTP Proxies

Overview

When RTP proxy is enabled and properly configured, SIP signaling is processed by the SBC 1000/2000 and the audio packets are switched without being processed through one of the DSPs. This enables endpoints on either side of the SBC to negotiate codecs and media capabilities without the need for the SBC to know about or support them. This feature is customizable through SIP Signaling Groups and Call Routing.

When to Use RTP Mode

Endpoints have some common capabilities, that would negotiate the Offer/Answer (codec negotiation) either direction. In other words, should both endpoints make a direct call without SBC 1000/2000 it should work

Advantages of Using RTP Mode

- It allows the SBC to establish calls that it otherwise cannot.

Copyright © 2015 Sonus Networks. All rights reserved.

- This improves the CPS of SBC1k/2K.
- RTP Proxy calls use use no DSPs or SDP licenses.
- Improved call quality.
- Less internal call processing.

Call Routing Notes

- Default mode of operation is the DSP mode.
- RTP Proxy mode shall be used if the SBC doesn't have DSPs or the endpoints on both sides of SBC1K/2K are the same or have similar capabilities.
- RTP Proxy preferred mode guarantees RTP proxy mode if the inbound and outbound SGs are SIP and allow proxy mode otherwise the call will be connected in DSP mode.
- Note that if inbound and out bound SG don't have common media mode the call will be rejected in any media mode of operation defined in the routing entry.
- Once the media mode is determined by CCC, SIP and MSC will be set to either DSP or RTP proxy mode and the call cannot transition to another mode until it gets released.
- RTP Proxy preferred mode is mode known only by the Call Router and CCC. This should be used when routing entries can be used by different (TDM, SIP).

Limitations

- Dynamic switching between DSP and Proxy modes is not supported in the same call.
- Does not provide capability mismatch resolution.
- All Forked responses are sent to caller. Endpoints may not handle it very well.
- SRTP mandatory/optional, crypto keys, RTP payload packet size, order of codecs, all endpoints negotiated.
- Calls can fail should endpoints fail. (e.g., RTP proxy does not work between Lync client and Tenor).
- Transferred calls are not supported.
- Endpoint-to-endpoint issues, such as on-way audio and no audio, usually manifest as call failures.
- No support for local ring back, music on hold, etc. (these require the DSP).

Video

Working With Security

SBC 100/2000 security is managed through a number of methods and protocols found in the user interface Security folder. The encompass Users, Login Messages, Certificates, TLS Profiles, and Passwords.

For more information about specific security features see the following sections in the User's Guide:

Working with Users and Groups

Managing Login Messages

Working With Certificates

Managing TLS Profiles

Copyright © 2015 Sonus Networks. All rights reserved.

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000-2000 API User's Guide

The REST APIs are provided for developers who want to programmatically integrate the Sonus SBC 1000/2000 into their application, and for administrators who want to script interactions with the Sonus SBC 1000/2000 gateway.

Sonus SBC 1000/2000's REST APIs provide access to resources via URI paths. To use a REST API, your application makes HTTPs requests and parses the responses. Currently, the only supported response format is XML. Methods used by developers are standard HTTP methods such as; GET, PUT, POST, and DELETE.

> Because the REST API is based on open standards, **you can use any Web Development Programming Language or HTTP Client Library to access the API**. Refer to API Requirements for more details.

Developer's Guide

API Requirements

What you need to have/consider before developing a REST client using the Sonus SBC 1000/2000 API

REST Resource Design

How the system works under the hood

API Authentication

How to authenticate with Sonus SBC 1000-2000 API requests

REST Samples

Samples for performing REST requests

Deployment Workflow

A quick guide for administrators who wish to deploy a single Sonus SBC 1000/2000 configuration onto multiple Sonus SBC 1000/2000 gateways using the REST API

API Reference

The following pages are located in the API Reference space - clicking any of these links will navigate you out of this documentation space:

> Please note that this release exposes a major subset of all existing Sonus SBC 1000/2000 resources via the REST API. New (and existing) resources will be incrementally added in upcoming versions of Sonus SBC 1000/2000.

Configuration Resources

- Resource - aclrule
- Resource - acltable
- Resource - actionconfig
- Resource - actionsetentry

Copyright © 2015 Sonus Networks. All rights reserved.

- Resource - actionsettable
- Resource - activealarm
- Resource - adconfig
- Resource - asmaclrule
- Resource - asmfactoryimage
- Resource - asmlyncevent
- Resource - asmsystemevent
- Resource - bricard
- Resource - bridge
- Resource - cacprofile
- Resource - cassg
- Resource - certificate
- Resource - chassis
- Resource - compandinglaw
- Resource - corefile
- Resource - csr
- Resource - decodelicense
- Resource - dhcpleaseclient
- Resource - dhcppool
- Resource - dhcpstaticclient
- Resource - diskpartition
- Resource - domaincontroller
- Resource - ds1callinfo
- Resource - ds1channel
- Resource - ds1portgroup
- Resource - dspcard
- Resource - emergencysvccallbktable
- Resource - emergencysvccallstats
- Resource - emergencysvccallstatus
- Resource - emergencysvcconfig
- Resource - enmsignalingprofile
- Resource - ethernetport
- Resource - fan
- Resource - faxcodecprofile
- Resource - fxocard
- Resource - fxosignalingprofile
- Resource - fxscard
- Resource - fxschannel
- Resource - fxsport
- Resource - fxssignalingprofile
- Resource - globalsecurityoptions
- Resource - highestalarm
- Resource - hosts
- Resource - ipsecstatistics
- Resource - ipsectunnel
- Resource - isdnsg
- Resource - license
- Resource - licensekey
- Resource - linecard
- Resource - linkmonitor
- Resource - linkmonitorcounters
- Resource - locallogfile
- Resource - localuser

Copyright © 2015 Sonus Networks. All rights reserved.

- Resource - logger
- Resource - logicalinterface
- Resource - login
- Resource - logout
- Resource - media
- Resource - mediacryptoprofile
- Resource - medialistprofile
- Resource - messagetransentry
- Resource - messagetranstable
- Resource - mstiportstats
- Resource - mstp
- Resource - natinterface
- Resource - natportforward
- Resource - ospfconfig
- Resource - partition
- Resource - portmembership
- Resource - portmirror
- Resource - postlogcontent
- Resource - postloginmessage
- Resource - powersupply
- Resource - preloginmessage
- Resource - processstats
- Resource - q850tosipmapping
- Resource - q850tosipmappingtable
- Resource - qoe
- Resource - r2signalingprofile
- Resource - radiusconfig
- Resource - radiusserver
- Resource - registrantstatus
- Resource - relay
- Resource - remotelog
- Resource - reroutetable
- Resource - restarthistory
- Resource - ripconfig
- Resource - routingentry
- Resource - routingtable
- Resource - sbaactionstatus
- Resource - sbaconfig
- Resource - sbacsr
- Resource - sbainstalledpackage
- Resource - securitylogfile
- Resource - session
- Resource - sipcallinfo
- Resource - sipcfgcacprofile
- Resource - sipchannel
- Resource - sipcontactregistrant
- Resource - siplocalauthentry
- Resource - siplocalauthtable
- Resource - siplocalregistrarentry
- Resource - siplocalregistrartable
- Resource - sipprofile
- Resource - sipregistrantentry
- Resource - sipremoteauthentry

Copyright © 2015 Sonus Networks. All rights reserved.

- Resource - sipremoteauthtable
- Resource - sipserver
- Resource - sipservertable
- Resource - sipsg
- Resource - siptlsprofile
- Resource - siptoq850mapping
- Resource - siptoq850mappingtable
- Resource - snmptargetaddress
- Resource - spmconditionrule
- Resource - spmelementdescriptor
- Resource - spmheaderrule
- Resource - spmmessagetable
- Resource - spmrawmessagerule
- Resource - spmrequestlinerule
- Resource - spmstatuslinerule
- Resource - staticarp
- Resource - staticiproute
- Resource - supplementarysvcprofile
- Resource - system
- Resource - systemcallstats
- Resource - systemlog
- Resource - systemvitalslogfile
- Resource - tca
- Resource - telcobriport
- Resource - telcods1port
- Resource - telcofxoport
- Resource - timing
- Resource - toneprofile
- Resource - tonetable
- Resource - transformationentry
- Resource - transformationtable
- Resource - usergroup
- Resource - vlan
- Resource - voicecodecprofile
- Resource - webaccesslogfile
- Resource - weberrorlogfile

Task Resources

- Resource - initialsetup
- Resource - modifydefaultvlan

Sonus SBC 1000-2000 API - Requirements

Sonus SBC 1000/2000 Requirements

To use the REST API, you must have the following Sonus SBC 1000/2000 system requirements fulfilled:

- Create a Local User with REST access level

REST Client Requirements

Copyright © 2015 Sonus Networks. All rights reserved.

The client is free to use any HTTP compliant (1.1) client library or Web Development Programming Language satisifying the following requirements:

1. Support for HTTPS
2. Supports HTTP methods GET, POST, PUT, DELETE
3. Supports cookies for session management

Sonus SBC 1000-2000 API - Resource Design

1. Introduction

Objects in the system are represented as resources. A resource is identified using a logical URL. The URL along with the HTTP method will identify the resource and the operation to be performed by the server. All REST services are stateless, which means that the request must contain enough state to answer the request. Every resource will have a specified URI which will be documented.

Users can perform lookup, create, modify and delete on the resources in Sonus SBC 1000/2000. The response to a REST request will be in XML format, containing a status block and a resource block where applicable.

2. Response Format

The response to the REST requests is in XML format. The response has two parts:

- Status - contains status code in case of success or error.
- Resource - contains the returned state of the resource from the system as part of the request. The resource block will not be present in case of DELETE requests. Also, the resource block will be present if the request did not fail.

The HTTP header will contain the HTTP status code 200.

```
<?xml version="1.0">
<root>
 <status>
  Status of the request indicating success or failure.
 </status>
 <resource>
  Data relevant to the particular request.
 </resource>
</root>
</xml>
```

2.1 Response Status Block

The status block in the response XML contains the following structure:

Copyright © 2015 Sonus Networks. All rights reserved.

```
<status>
    <http_code></http_code>
    <app_status href=" ">
 <app_status_entry code=" " params=" "/>
    </app_status>
</status>
```

XML Tag	Description	Child Elements
`<status>`	Present is all responses.	`<http_code>` `<app_status>`
`<http_code>`	Standard HTTP code. Application error codes will be mapped to HTTP status code. If the request is successful http_code will be 200. **Attributes**: • *None*	None
`<app_status>`	Present only if there are application errors. **Attributes:** • *href* - This contains the URI of the resource that the request was made on.	`<app_status_entry>`
`<app_status_entry>`	There will be one of these tags for every application error for this request. **Attributes:** • *code* - This is a non-zero number that represents the application error code. • *params* - This is a string that contains the error tokens in a '|' separated format. *Refer to 2.1.1 to see how to use the code and params to obtain the error message.*	None

Many of the application errors will have to be mapped to an appropriate HTTP status code. For e.g, if the resource does not exist in case of a modify, the response would contain HTTP status code 404. Application processing error codes that do not match logically to any particular HTTP status code can be mapped to HTTP error 500.

2.1.1 How to obtain error message from *code* and *params*

The `<app_status_entry>` tag will contain the application error code and params as attributes. The `code` is a non-zero number and the `params` is a string that contains the tokens in a '|' separated format. These tokens need to be substituted into a detailed error message for the corresponding error code. The error messages for each error code is published in XML format - access the full application error code listing from the API reference doc. Users can substitute the tokens in sequential order in the error message to get the actual error description. The following status block provides an example of an error code with the params.

Copyright © 2015 Sonus Networks. All rights reserved.

```
<status>
 <http_code>200</http_code>
        <app_status href=" ">
            <app_status_entry code="31003" params="1|1"/>
        </app_status>
</status>
```

In this case, the error message for error code `31003` is: "Cannot delete SIP to Q.850 mapping (%1%). It is in use by SG (%2%).". Substituting the error params in the response in the message, gives the error message as: "Cannot delete SIP to Q.850 mapping 1. It is in use by SG 1."
Message params and error code can be used to construct any custom application level error that the client wants to construct.

2.2 Response Resource Block

The resource block in the response contains the state of the resource returned after the request. The resource tag is the resource name that the request was made upon. Sometimes a POST can result in a resource name in the response being different from the resource sent in the request. Usually actions on resources return only status block.

The resource block in the response XML contains the following structure:

XML Tag	Description	Child Elements
`<resource_list>`	Present only if a bulk lookup is performed, where multiple instances are listed. **Attributes:** • *count* - This contains the number of resources in the list	`<resource_pk>` `<resource>`
`<resource_pk>`	Present only if a bulk lookup is performed without *details=true* quer y parameter. **Attributes:** • *id* - This represents the resource identifier. • *href* - This represents the resource URI for the resource.	None

Copyright © 2015 Sonus Networks. All rights reserved.

`<resource>`	Present if a bulk lookup with *details=true* query parameter is performed or if a single GET, PUT or POST without action query parameter is performed. **Attributes**: • *id* - This represents the resource identifier. • href - This represents the resource URI for the resource. • *app_code_config* - This is an error code into the error messages file. This is present only in case of GET and if there were errors in looking up the config attributes of the resource, if applicable. • *app_params_config* - This is a '|' separated string of the error tokens to be substituted into the error message. This is present only in case of GET and if there were errors in looking up the config attributes of the resource, if applicable. • *app_code_runtime* - This is an error code into the error messages file. This is present only in case of GET and if there were errors in looking up the runtime attributes of the resource, if applicable. • *app_params_runtime* - This is a '|' separated string of the error tokens to be substituted into the error message. This is present only in case of GET and if there were errors in looking up the runtime attributes of the resource, if applicable. • *app_code_statistics* - This is an error code into the error messages file. This is present only in case of GET and if there were errors in looking up the statistics attributes of the resource, if applicable. • *app_params_statistics* - This is a '|' separated string of the error tokens to be substituted into the error message. This is present only in case of GET and if there were errors in looking up the statistics attributes of the resource, if applicable. • *app_code_inventory* - This is an error code into the error messages file. This is present only in case of GET and if there were errors in looking up the inventory attributes of the resource, if applicable. • *app_params_inventory* - This is a '|' separated string of the error tokens to be substituted into the error message. This is present only in case of GET and if there were errors in looking up the inventory attributes of the resource, if applicable.	`<resource_attr>` `<resource_attr_list>`
`<resource_attr>`	Every resource attribute in the resource schema is shown as a separate tag. **Attributes**: • *href* - This is present when the attribute is a link to another resource and contains the URI for that resource.	None

Copyright © 2015 Sonus Networks. All rights reserved.

<resource_attr_list>	This is present only when the resource attribute contains multiple instances of another resource. **Attributes**: • *count* - This represents the number of <entry> tags within this list.	<entry>
<entry>	This is present within a <resource_attr_list> tag and represents an individual resource. **Attributes**: • *href* - This represents a link to another resource and contains the URI for that resource.	None

3. Resource Methods

Lookup, create, modify, delete, action methods can be performed on resources. Some resources do not have all methods applicable.

3.1 Lookup Resource(s)

3.1.1 Lookup Request

Lookup of a resource will be performed using HTTP method GET. For lookup of all resources of a certain type, the resource URI needs to be provided as:

```
/rest/<resource>

For e.g., /rest/routingtable --> looks up all call route tables in the system.

For looking up all child resources under a parent resource, the URI needs to have
the parent id in it.
/rest/linecard/1/telcods1   --> looks up all TelcoDS1 ports under linecard 1.
```

For lookup of a single object, the resource URL needs to be provided as:

```
/rest/<resource>/<id>

For e.g., /rest/routingtable/1 --> looks up call route table with ID as 1.

If a lookup is performed on a child object the entire id of the child needs to be
provided in the URI:

/rest/linecard/1/telcods1/1  --> looks up TelcoDS1 port under line card 1. The port
id is 1:1
```

Copyright © 2015 Sonus Networks. All rights reserved.

The id is the actual instance (rowID) of the resource in the system. This can be obtained by doing a bulk lookup first, which will return the list of instances, each having an id. This in turn can then be used to do single lookup for details of that particular resource. Singleton resources do not have any id, hence lookup of a singleton resource does not require an id.

```
For lookup of a singleton resource, the URL needs to be provided as:
/rest/<resource>

For e.g. /rest/system  --> looks up the system resource
```

Tthere will be no bulk lookup for a singleton - the response will always be the details of the singleton resource.

The response for a lookup will be either a link to all the individual resources (bulk lookup) or the details of the resource itself. In case of bulk lookup, an additional query parameter "***details=true***" can be passed in to get the details of the resources along with the link.

3.1.2 Bulk Lookup Response

The response to a bulk lookup of a resource contains links to the existing resources of that type. These links can be used to further get the details of the individual resource.

```
<?xml version="1.0">
<root>
 <status>
 </status>
 <resource_list count="2">
  <resource_pk id="1" href="...."/>
  <resource_pk id="2" href="...."/>
 </resource_list>
</root>
```

If the `details=true` parameter was passed in the request, the response will contain individual resource blocks for each resource present in the system of that type.

Copyright © 2015 Sonus Networks. All rights reserved.

```
<?xml version="1.0">
<root>
 <status>
 </status>
 <resource_list count="2">
  <resource id="1" href="....">
                    <attr1></attr1>
                    <attr2></attr2>
                    ....
                </resource>
  <resource id="2" href="....">
                    <attr1></attr1>
                    <attr2></attr2>
                    ....
                </resource>
 </resource_list>
</root>
```

3.1.3 Single Lookup Response

Lookup of a single resource returns the resource along with all the attributes in it. Also, if an resource contains an attribute which is an index to another resource, then the attribute contains a link to that referred resource, along with the attribute value. The client can then use the link provided to get the details of that resource.

The attributes are all listed one after the other without any ordering.

```
<?xml version="1.0">
<root>
 <status>
 </status>
 <resource id="1" href="....">
  <attr1></attr1>
  <attr2></attr2>
  <attr3 href="....">id</attr3>
  .....
  .....
 </resource>
</root>
```

3.1.4 Categories of Resource Attributes

A resource has attributes which are of type *configuration*, *runtime*, *statistics* or *inventory*. Most runtime and statistics attribute names are prefixed with an '*rt_*'. On lookup, the user will have the option to provide a filter for looking up only the certain category of attributes. A filter is a certain view of the resource. The default behavior will return attributes belonging to all categories applicable for that resource.

The filter will be passed as a URL parameter. Multiple filters can be passed in the same request as a comma-separated string, as shown in the example below. Every resource has a specified set of applicable filters. Providing an invalid filter for a resource will result in error. If multiple filters are passed, each filter will be validated. If any filter is invalid, the request will fail. **Filter parameter will be applicable only for HTTP GET**.

Copyright © 2015 Sonus Networks. All rights reserved.

```
/rest/linecard/1/telcods1/1?filter=config --> returns only config attributes for the
DS1 port with ID 1.

/rest/linecard/1/telcods1/1?filter=config,runtime --> returns config and runtime
attributes for the DS1 port with ID 1
```

The response for a GET operation can have success from one filter and failure from another. This will be sent back to the user as error codes in the response.

3.2 Create Resource

3.2.1 Create Request

A resource can be created on the system using the HTTP method PUT.

The resource URI for creating a resource needs to be provided as:

```
/rest/<resource>/<id>

For e.g., /rest/routingtable/1 --> creates a new call route table with id 1.
```

For creation of a resource, only config attributes need to be provided in the form elements.

The request needs to have the ID of the resource that is being created. Absence of an ID in the request will cause it to fail. The REST service will assume that the resource is provided in its entire state for the provision.

The response to a Create Request will contain the details of the newly created resource if it was a success.

3.2.2 Create Response

The response to a create request returns the newly created resource along with a link to it. The link can be used to get the details of the resource.

```
<?xml version="1.0">
<root>
 <status>
 </status>
 <resource id="1" href="....">
  <attr1></attr1>
  <attr2></attr2>
  ...
  <attr3 href="....">id</attr3>
 </resource>
</root>
```

Copyright © 2015 Sonus Networks. All rights reserved.

3.3 Modify Resource

3.3.1 Modify Request

A resource can be modified or updated using the HTTP method POST.

The resource URI for modifying an object needs to be provided as:

```
/rest/<resource>/<id>

For e.g., /rest/routingtable/1 -->modifies an existing call route table with id 1.
```

For a modify, the user has a choice to send the whole resource (all configuration attributes) or just the attributes that are being modified. If the resource contains only the set of the attributes to be modified, the server will apply the changes on top of the existing values for the other attributes in the resource. This is done so that the resource is preserved in its current state and the updated attributes are applied to the current state of the resource, instead of applying the default values for the attributes that are not being updated.

For e.g., if the client wants to enable or disable a resource, the request can just contain the appropriate attribute to enable or disable the resource, and all other attributes will hold their current value.

The response to a modify resource request will contain the details of the modified resource if the request was a success. The resource will represent the new state of the resource.

3.3.2 Modify Response

The response to a modify request returns the whole resource in its new state.

```
<?xml version="1.0">
<root>
 <status>
 </status>
 <resource id="1" href="....">
  <attr1></attr1>
  <attr2></attr2>
  <attr3 href="....">id</attr3>
  ....
  ....
 </resource>
</root>
```

3.4 Delete Resource

3.4.1 Request

A resource can be deleted from the system using the HTTP method DELETE.

The resource URI for deleting an object needs to be provided as:

Copyright © 2015 Sonus Networks. All rights reserved.

```
/rest/<resource>/<id>

For e.g., /rest/routingtable/1 --> deletes an existing call route table with id 1.
```

The response to a delete resource request will contain only a status block, indicating a success or failure.

3.4.2 Delete Response

The response to a delete request has only a status block. There is no resource data to be provided.

```
<?xml version="1.0">
<root>
 <status>
  ....
 </status>
</root>
```

3.5 Actions on Resources

3.5.1 Action Request

A resource can have actions performed on it. Actions can be performed on a resource by passing the action name as a value to the query parameter "*action*" in the resource URI. The permitted actions for a resource will be documented.

The HTTP method needs to be POST.

The resource URI for performing an action on a resource needs to be provided as:

```
/rest/<resource>/<id>?action=<action name>

For e.g., /rest/system?action=reboot--> performs "reboot" action on the system
resource
```

If an action requires certain attributes, they need to be provided in the request as POST parameters. The list of attributes for every action is documented.

The response to an action on a resource usually contains only the status block. There is no resource returned as a response to an action. There are very few exceptions where the response to an action on a resource returns the same/different resource. If the action failed, the status would contain the error code, otherwise it would report a success.

3.5.2 Action Response

Copyright © 2015 Sonus Networks. All rights reserved.

The response to an action request contains just the status block showing success or error.

```
<?xml version="1.0">
<root>
 <status>
  ....
 </status>
</root>
```

Sonus SBC 1000-2000 API - Authentication

A REST client is required to first authenticate with the Sonus SBC 1000/2000 REST service to acquire a uniquely assigned session token. This token must be used in any subsequent REST API call during the lifetime of the session.

This page is intended to walk you through a simple example of establishing a session between a REST client and the Sonus SBC 1000/2000 API. All code snippets below use a combination of PHP and libcurl. You may use any other language/library as long as it meets the Sonus SBC 1000/2000 API requirements.

On this Page

- Prerequisite - Setting up the HTTP Options
- How to Acquire a Sonus SBC 1000/2000 Session Token
- How to Use the Session Token
- How to Close a Sonus SBC 1000/2000 Session

Prerequisite - Setting up the HTTP Options

Sonus SBC 1000/2000 Web Service (REST) runs on a secure channel i.e. HTTPS, which requires Web Services clients to establish secure communication channel with the service.

If you're not using PHP+libcurl, please refer to documentation of the library you are using to determine the HTTP configuration necessary to properly import and trust the server certificate for secure HTTP

Copyright © 2015 Sonus Networks. All rights reserved.

Setup cURL Options

```
// initialize curl
$curlHandle = curl_init();

// uncomment for debug porposes
//curl_setopt($curlHandle, CURLOPT_VERBOSE, true)

// set the appropriate timeout
curl_setopt($curlHandle, CURLOPT_TIMEOUT, 10);

curl_setopt($curlHandle, CURLOPT_HEADER, false);
// Set so curl_exec returns the result instead of outputting it.
curl_setopt($curlHandle, CURLOPT_RETURNTRANSFER, true);

// This example blindly accepts any server certificate, without doing any
// verification as to which CA signed it, and whether or not that CA is trusted.

// For the sake of simplicity, configure cURL to accept any server(peer) certificate
curl_setopt($curlHandle, CURLOPT_SSL_VERIFYPEER, false);
```

```
// Following captures the details on how libcurl options can be configured to use
secure HTTP.

//curl_setopt($curlHandle , CURLOPT_SSL_VERIFYPEER, true);

// 2, means, check that the common name exists and that it matches the host name of
the server
//curl_setopt($curlHandle , CURLOPT_SSL_VERIFYHOST, 2);

// previously downloaded server cert
//$certLocation = getcwd() . "/CAcerts/ux_rest.crt";
//curl_setopt($curlHandle , CURLOPT_CAINFO, $certLocation);
```

How to Acquire a Sonus SBC 1000/2000 Session Token

Upon successful authentication via **/rest/login**, HTTP response HEADER carries the session token in a cookie. REST clients need to lookup this cookie in the response header and cache it to use it for subsequent REST calls by setting the cookie back in the HTTP request header.



The REST client cookie session expires after **10 minutes of idle session**

Copyright © 2015 Sonus Networks. All rights reserved.

POST Request to */rest/login* Resource and Extract Session Token

```
// define an array where we would cache the Session Token Cookie with value
$cookieArr = array();

// Sonus SBC 1000/2000 REST login resource URL
$loginResource = "https://ux_host_or_ipaddress/rest/login";

// set the login resource url in curl
curl_setopt($curlHandle, CURLOPT_URL, $loginResource );

// setup a callback handler for reading and processing the response header fields
// that would come in response to REST login resource POST call
curl_setopt($curlHandle, CURLOPT_HEADERFUNCTION, array($this,
'responseHeaderCallback'));

// tell cURL that we are doing a HTTP POST
curl_setopt($curlHandle, CURLOPT_POST, true);

// set the login resource POST params. The user must be of the REST access level and
created from the WebUI prior to using the API.
$loginPropsArr = array('Username'=>'admin', 'Password'=>'admin');
curl_setopt($curlHandle, CURLOPT_POSTFIELDS, http_build_query($loginPropsArr, '',
'&'));

// exec the HTTP/REST request
$response = curl_exec($curlHandle);

// HTTP response header callback function which processes the header fields
function responseHeaderCallback($curlHandle, $header) {
    if(!strncmp($header, "Set-Cookie:", 11)) {
        $cookiestr = trim(substr($header, 11, -1));
        $cookie = explode(';', $cookiestr);
        $cookie = explode('=', $cookie[0]);
        $cookiename = trim(array_shift($cookie));
        $cookieArr[$cookiename] = trim(implode('=', $cookie));
    }
    return strlen($header);
}
```

How to Use the Session Token

Copyright © 2015 Sonus Networks. All rights reserved.

GET on System Resource (/rest/system) Using the Session Token

```
// init cURL handle
$curlHandle = curl_init();

$cookieHeader = '';
// previously extracted cookies in $cookieArr (above), is used to add the
// session token in HTTP request header for subsequent REST call
foreach ($cookieArr as $key=>$value) {
    $cookieHeader .= "$key=$value; ";
}
if (!empty($cookieHeader)) {
    curl_setopt($curlHandle, CURLOPT_COOKIE, $cookieHeader);
}

// set other relevant HTTP option as shows in above section _Setting up the HTTP
Options_
curl_setopt($curlHandle, CURLOPT_HTTPGET, true);

// Sonus SBC 1000/2000 REST system resource URL
$systemResource = "https://ux_host_or_ipaddress/rest/system";

// set the system resource url in curl
curl_setopt($curlHandle, CURLOPT_URL, $systemResource );

// exec the HTTP/REST request
$response = curl_exec($curlHandle);
```

How to Close a Sonus SBC 1000/2000 Session

It is recommended that an explicit POST is done on logout resource to cleanup session specific resources the Sonus SBC 1000/2000 node.

Copyright © 2015 Sonus Networks. All rights reserved.

POST on logout Resource (/rest/logout)

```
// init cURL handle
$curlHandle = curl_init();

$cookieHeader = '';
// previously extracted cookies in $cookieArr (above), is used to add the
// session token in HTTP request header for this REST call
foreach ($cookieArr as $key=>$value) {
    $cookieHeader .= "$key=$value; ";
}
if (!empty($cookieHeader)) {
    curl_setopt($curlHandle, CURLOPT_COOKIE, $cookieHeader);
}

// tell cURL that we are doing a HTTP POST
curl_setopt($curlHandle, CURLOPT_POST, true);

// set other relevant HTTP option as shows in above section _Setting up the HTTP
Options_

// Sonus SBC 1000/2000 REST logout resource URL
$logoutResource = "https://ux_host_or_ipaddress/rest/logout";

// set the system resource url in curl
curl_setopt($curlHandle, CURLOPT_URL, $logoutResource);
// logout resource does not require any POST parameter.

// exec the HTTP/REST request
$response = curl_exec($curlHandle);

// any subsequent REST call should result in HTTP Error 401 Unauthorized status
```

Sonus SBC 1000-2000 API - REST Samples

The following page links provide Samples of GET, PUT, POST, DELETE and REST operations to send/recieve data to/from the Sonus SBC 1000/2000 REST Resrouces

About cURL

cURL is a free cross-platform library and command-line tool that can be used to send/receive data using URL syntax.

REST Sample - DELETE Resource

The DELETE method allows you to delete a Sonus SBC 1000/2000 REST Resource.

REST Sample - GET Resource

The GET method allows you to retrieve data from the Sonus SBC 1000/2000 REST Resource.

Copyright © 2015 Sonus Networks. All rights reserved.

REST Sample - Login Resource

The Login Resource is used to establish a secure session with the Sonus SBC 1000/2000. The user provided in the URI parameters of this resource must be created through the WebUI prior to using the API and must be of the REST access level.

REST Sample - POST Resource

The POST method can be performed on a Sonus SBC 1000/2000 resource to modify the resource with or without an action parameter in the URL.

REST Sample - PUT Resource

The PUT method allows you to create and modify Sonus SBC 1000/2000 REST Resource. Unlinke the POST Resource, modifying a resource with PUT requires all parameters to be sent in the request (including the resource's identifier).

About cURL

cURL is a free cross-platform library and command-line tool that can be used to send/receive data using URL syntax.

Due to its simpleton installation and usage, the cURL command-line tool is used throughout this API documentation to demonstrate the basic usage of the Sonus SBC 1000/2000 REST Resources.

REST Sample - DELETE Resource

The DELETE method allows you to delete a Sonus SBC 1000/2000 REST Resource.The following examples demonstrate how to use the DELETE Method on a resource using cURL:

DELETE on a Resource /rest/isdnsg/{identifier}

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-X DELETE -i https://192.168.1.183/rest/isdnsg/10011
```

Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 17 May 2011 19:51:33 GMT
```

Copyright © 2015 Sonus Networks. All rights reserved.

XML Response

Sample XML Response

```
<?xml version="1.0">
<root>
 <status>
  <http_code>200</http_code>
 </status>
</root>
```

REST Sample - GET Resource

The GET method allows you to retrieve data from the Sonus SBC 1000/2000 REST Resource. The following examples demonstrate how to use the GET Method on a resource using cURL. The API allows you to GET a resource in bulk or a in a single instance:

- Bulk Lookup: GET /rest/isdnsg
- Single Lookup: GET /rest/isdnsg/{identifier}

Bulk Lookup: GET /rest/isdnsg

Get all Resources

Copyright © 2015 Sonus Networks. All rights reserved.

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/isdnsg
```

Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 17 May 2011 19:12:54 GMT
```

XML Response

Sample XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
    <status>
        <http_code>200</http_code>
    </status>
    <isdnsg_list count="1">
        <isdnsg_pk id="10001"
href="https://192.168.1.183/rest/isdnsg/10001"/>
    </isdnsg_list>
</root>
```

Get Details for all Resources

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/isdnsg?details=true
```

Header Response

Copyright © 2015 Sonus Networks. All rights reserved.

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2011 18:45:10 GMT
```

XML Response

Sample XML Response

```
<?xml version="1.0">
<root>
    <status>
        <http_code>200</http_code>
    </status>
    <isdnsg_list count="1">
        <isdnsg id="10001" href="https://192.168.1.183/rest/isdnsg/10001">
            <ActionsetTableNumber>0</ActionsetTableNumber>
            <ApplyToPortName
href="https://192.168.1.183/linecard/1/telcods1port/1">1.1</ApplyToPortName>
<ConfigIEState>1</ConfigIEState>
            <Description>REST ISDN SG</Description>

<IsdnAllowCallingNameDisplayToSwitch>0</IsdnAllowCallingNameDisplayToSwitch>
<IsdnServiceMessageCapability>1</IsdnServiceMessageCapability>
            <IsdnSgDirection>2</IsdnSgDirection>
            <IsdnSgHuntMethod>0</IsdnSgHuntMethod>
            <IsdnSgOverlapRxMode>0</IsdnSgOverlapRxMode>
            <IsdnSgRingbackPlayPolicy>0</IsdnSgRingbackPlayPolicy>
            <IsdnSgSideOrientation>0</IsdnSgSideOrientation>
            <IsdnSgSwitchVariant>3</IsdnSgSwitchVariant>
            <IsdnSgTimerT301>180</IsdnSgTimerT301>
            <IsdnSgTimerT302>15</IsdnSgTimerT302>
            <IsdnSgTimerT303>4</IsdnSgTimerT303>
            <IsdnSgTimerT305>30</IsdnSgTimerT305>
            <IsdnSgTimerT308>4</IsdnSgTimerT308>
            <IsdnSgTimerT309>6</IsdnSgTimerT309>
            <IsdnSgTimerT310>30</IsdnSgTimerT310>
            <IsdnSgTimerT313>4</IsdnSgTimerT313>
            <IsdnSgTimerT314>4</IsdnSgTimerT314>
            <IsdnSgTimerT316>120</IsdnSgTimerT316>
            <IsdnSgTimerT322>4</IsdnSgTimerT322>
            <IsdnSgTimerT3M1>120</IsdnSgTimerT3M1>

<IsdnStopFarEndT310UponTryingFromSip>0</IsdnStopFarEndT310UponTryingFromSip>
<RouteTableNumber
href="https://192.168.1.183/routingtable/1">1</RouteTableNumber>
            <ToneTableNumber
href="https://192.168.1.183/tonetable/1">1</ToneTableNumber>
            <rt_CurrentActiveCalls>0</rt_CurrentActiveCalls>
            <rt_IncomingCallaccepts>0</rt_IncomingCallaccepts>
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
        <rt_IncomingCallattempts>0</rt_IncomingCallattempts>
        <rt_IncomingCallcompletes>0</rt_IncomingCallcompletes>
        <rt_IncomingCallrejects>0</rt_IncomingCallrejects>
        <rt_IsdnSgQ921State>0</rt_IsdnSgQ921State>
        <rt_OutgoingCallaccepts>0</rt_OutgoingCallaccepts>
        <rt_OutgoingCallattempts>0</rt_OutgoingCallattempts>
        <rt_OutgoingCallcompletes>0</rt_OutgoingCallcompletes>
        <rt_OutgoingCallrejects>0</rt_OutgoingCallrejects>
        <rt_TotalCallsProcessed>0</rt_TotalCallsProcessed>
        <rt_TotalConnectedCalls>0</rt_TotalConnectedCalls>
        <rt_TotalErroredCalls>0</rt_TotalErroredCalls>
        <rt_TotalRefusedCalls>0</rt_TotalRefusedCalls>
        <rt_linkDownCount>33</rt_linkDownCount>
        <rt_linkUpCount>0</rt_linkUpCount>
        <rt_rxCount>0</rt_rxCount>
        <rt_rxDISC>0</rt_rxDISC>
        <rt_rxDM>0</rt_rxDM>
        <rt_rxDataReq>0</rt_rxDataReq>
        <rt_rxEstReq>1</rt_rxEstReq>
        <rt_rxFRMR>0</rt_rxFRMR>
        <rt_rxICount>0</rt_rxICount>
        <rt_rxREJ>0</rt_rxREJ>
        <rt_rxRNR>0</rt_rxRNR>
        <rt_rxRR>0</rt_rxRR>
        <rt_rxRelReq>0</rt_rxRelReq>
        <rt_rxSABME>0</rt_rxSABME>
        <rt_rxSCount>0</rt_rxSCount>
        <rt_rxUA>0</rt_rxUA>
        <rt_rxUNCount>0</rt_rxUNCount>
        <rt_txCount>134</rt_txCount>
        <rt_txCountBusy>0</rt_txCountBusy>
        <rt_txDISC>0</rt_txDISC>
        <rt_txDM>0</rt_txDM>
        <rt_txFRMR>0</rt_txFRMR>
        <rt_txICount>0</rt_txICount>
        <rt_txREJ>0</rt_txREJ>
        <rt_txRNR>0</rt_txRNR>
        <rt_txRR>0</rt_txRR>
        <rt_txSABME>134</rt_txSABME>
        <rt_txUA>0</rt_txUA>
    </isdnsg>
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
    </isdnsg_list>
</root>
```

Get only Config Details for all Resources

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i "https://192.168.1.183/rest/isdnsg?details=true&filter=config"
```

Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2011 18:54:30 GMT
```

XML Response

Copyright © 2015 Sonus Networks. All rights reserved.

Sample XML Response

```
<?xml version="1.0">
<root>
    <status>
        <http_code>200</http_code>
    </status>
    <isdnsg_list count="1">
        <isdnsg id="10001" href="https://192.168.1.183/rest/isdnsg/10001">
            <ActionsetTableNumber>0</ActionsetTableNumber>
            <ApplyToPortName
href="https://192.168.1.183/linecard/1/telcods1port/1">1.1</ApplyToPortName>
<ConfigIEState>1</ConfigIEState>
            <Description>REST ISDN SG</Description>

<IsdnAllowCallingNameDisplayToSwitch>0</IsdnAllowCallingNameDisplayToSwitch>
<IsdnServiceMessageCapability>1</IsdnServiceMessageCapability>
            <IsdnSgDirection>2</IsdnSgDirection>
            <IsdnSgHuntMethod>0</IsdnSgHuntMethod>
            <IsdnSgOverlapRxMode>0</IsdnSgOverlapRxMode>
            <IsdnSgRingbackPlayPolicy>0</IsdnSgRingbackPlayPolicy>
            <IsdnSgSideOrientation>0</IsdnSgSideOrientation>
            <IsdnSgSwitchVariant>3</IsdnSgSwitchVariant>
            <IsdnSgTimerT301>180</IsdnSgTimerT301>
            <IsdnSgTimerT302>15</IsdnSgTimerT302>
            <IsdnSgTimerT303>4</IsdnSgTimerT303>
            <IsdnSgTimerT305>30</IsdnSgTimerT305>
            <IsdnSgTimerT308>4</IsdnSgTimerT308>
            <IsdnSgTimerT309>6</IsdnSgTimerT309>
            <IsdnSgTimerT310>30</IsdnSgTimerT310>
            <IsdnSgTimerT313>4</IsdnSgTimerT313>
            <IsdnSgTimerT314>4</IsdnSgTimerT314>
            <IsdnSgTimerT316>120</IsdnSgTimerT316>
            <IsdnSgTimerT322>4</IsdnSgTimerT322>
            <IsdnSgTimerT3M1>120</IsdnSgTimerT3M1>

<IsdnStopFarEndT310UponTryingFromSip>0</IsdnStopFarEndT310UponTryingFromSip>
<RouteTableNumber
href="https://192.168.1.183/routingtable/1">1</RouteTableNumber>
            <ToneTableNumber
href="https://192.168.1.183/tonetable/1">1</ToneTableNumber>
        </isdnsg>
    </isdnsg_list>
</root>
```

Get only Statistics Details for all Resources

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i "https://192.168.1.183/rest/isdnsg?details=true&filter=statistics"
```

Header Response

Copyright © 2015 Sonus Networks. All rights reserved.

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2011 19:04:40 GMT
```

XML Response

Copyright © 2015 Sonus Networks. All rights reserved.

Sample XML Response

```
<?xml version="1.0">
<root>
    <status>
        <http_code>200</http_code>
    </status>
    <isdnsg_list count="1">
        <isdnsg id="10001" href="https://192.168.1.183/rest/isdnsg/10001">
            <rt_CurrentActiveCalls>0</rt_CurrentActiveCalls>
            <rt_IncomingCallaccepts>0</rt_IncomingCallaccepts>
            <rt_IncomingCallattempts>0</rt_IncomingCallattempts>
            <rt_IncomingCallcompletes>0</rt_IncomingCallcompletes>
            <rt_IncomingCallrejects>0</rt_IncomingCallrejects>
            <rt_IsdnSgQ921State>0</rt_IsdnSgQ921State>
            <rt_OutgoingCallaccepts>0</rt_OutgoingCallaccepts>
            <rt_OutgoingCallattempts>0</rt_OutgoingCallattempts>
            <rt_OutgoingCallcompletes>0</rt_OutgoingCallcompletes>
            <rt_OutgoingCallrejects>0</rt_OutgoingCallrejects>
            <rt_TotalCallsProcessed>0</rt_TotalCallsProcessed>
            <rt_TotalConnectedCalls>0</rt_TotalConnectedCalls>
            <rt_TotalErroredCalls>0</rt_TotalErroredCalls>
            <rt_TotalRefusedCalls>0</rt_TotalRefusedCalls>
            <rt_linkDownCount>118</rt_linkDownCount>
            <rt_linkUpCount>0</rt_linkUpCount>
            <rt_rxCount>0</rt_rxCount>
            <rt_rxDISC>0</rt_rxDISC>
            <rt_rxDM>0</rt_rxDM>
            <rt_rxDataReq>0</rt_rxDataReq>
            <rt_rxEstReq>1</rt_rxEstReq>
            <rt_rxFRMR>0</rt_rxFRMR>
            <rt_rxICount>0</rt_rxICount>
            <rt_rxREJ>0</rt_rxREJ>
            <rt_rxRNR>0</rt_rxRNR>
            <rt_rxRR>0</rt_rxRR>
            <rt_rxRelReq>0</rt_rxRelReq>
            <rt_rxSABME>0</rt_rxSABME>
            <rt_rxSCount>0</rt_rxSCount>
            <rt_rxUA>0</rt_rxUA>
            <rt_rxUNCount>0</rt_rxUNCount>
            <rt_txCount>472</rt_txCount>
            <rt_txCountBusy>0</rt_txCountBusy>
            <rt_txDISC>0</rt_txDISC>
            <rt_txDM>0</rt_txDM>
            <rt_txFRMR>0</rt_txFRMR>
            <rt_txICount>0</rt_txICount>
            <rt_txREJ>0</rt_txREJ>
            <rt_txRNR>0</rt_txRNR>
            <rt_txRR>0</rt_txRR>
            <rt_txSABME>472</rt_txSABME>
            <rt_txUA>0</rt_txUA>
        </isdnsg>
    </isdnsg_list>
</root>
```

Copyright © 2015 Sonus Networks. All rights reserved.

Single Lookup:

GET /rest/isdnsg/{identifier}

Get resource

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/isdnsg/10001
```

Header Response:

Sample Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 17 May 2011 19:13:56 GMT
```

XML Response:

Sample XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
    <status>
        <http_code>200</http_code>
    </status>
    <isdnsg id="10001" href="https://192.168.1.183/rest/isdnsg/10001">
        <ActionsetTableNumber>0</ActionsetTableNumber>
        <ApplyToPortName
href="https://192.168.1.183/linecard/1/telcods1port/2">1.2</ApplyToPortName>

        <ConfigIEState>1</ConfigIEState>
        <Description>Renamed Description: ISDN UC, Port 1.2</Description>

<IsdnAllowCallingNameDisplayToSwitch>0</IsdnAllowCallingNameDisplayToSwitch>

        <IsdnServiceMessageCapability>1</IsdnServiceMessageCapability>
        <IsdnSgDirection>2</IsdnSgDirection>
        <IsdnSgHuntMethod>0</IsdnSgHuntMethod>
        <IsdnSgOverlapRxMode>0</IsdnSgOverlapRxMode>
        <IsdnSgRingbackPlayPolicy>0</IsdnSgRingbackPlayPolicy>
        <IsdnSgSideOrientation>0</IsdnSgSideOrientation>
        <IsdnSgSwitchVariant>6</IsdnSgSwitchVariant>
        <IsdnSgTimerT301>180</IsdnSgTimerT301>
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
        <IsdnSgTimerT302>15</IsdnSgTimerT302>
        <IsdnSgTimerT303>4</IsdnSgTimerT303>
        <IsdnSgTimerT305>30</IsdnSgTimerT305>
        <IsdnSgTimerT308>4</IsdnSgTimerT308>
        <IsdnSgTimerT309>6</IsdnSgTimerT309>
        <IsdnSgTimerT310>30</IsdnSgTimerT310>
        <IsdnSgTimerT313>4</IsdnSgTimerT313>
        <IsdnSgTimerT314>4</IsdnSgTimerT314>
        <IsdnSgTimerT316>120</IsdnSgTimerT316>
        <IsdnSgTimerT322>4</IsdnSgTimerT322>
        <IsdnSgTimerT3M1>120</IsdnSgTimerT3M1>

<IsdnStopFarEndT310UponTryingFromSip>1</IsdnStopFarEndT310UponTryingFromSip>

        <RouteTableNumber
href="https://192.168.1.183/routingtable/2">2</RouteTableNumber>
        <ToneTableNumber
href="https://192.168.1.183/tonetable/10">10</ToneTableNumber>
        <rt_CurrentActiveCalls>0</rt_CurrentActiveCalls>
        <rt_IncomingCallaccepts>0</rt_IncomingCallaccepts>
        <rt_IncomingCallattempts>0</rt_IncomingCallattempts>
        <rt_IncomingCallcompletes>0</rt_IncomingCallcompletes>
        <rt_IncomingCallrejects>0</rt_IncomingCallrejects>
        <rt_IsdnSgQ921State>0</rt_IsdnSgQ921State>
        <rt_OutgoingCallaccepts>0</rt_OutgoingCallaccepts>
        <rt_OutgoingCallattempts>0</rt_OutgoingCallattempts>
        <rt_OutgoingCallcompletes>0</rt_OutgoingCallcompletes>
        <rt_OutgoingCallrejects>0</rt_OutgoingCallrejects>
        <rt_TotalCallsProcessed>0</rt_TotalCallsProcessed>
        <rt_TotalConnectedCalls>0</rt_TotalConnectedCalls>
        <rt_TotalErroredCalls>0</rt_TotalErroredCalls>
        <rt_TotalRefusedCalls>0</rt_TotalRefusedCalls>
        <rt_linkDownCount>154</rt_linkDownCount>
        <rt_linkUpCount>0</rt_linkUpCount>
        <rt_rxCount>0</rt_rxCount>
        <rt_rxDISC>0</rt_rxDISC>
        <rt_rxDM>0</rt_rxDM>
        <rt_rxDataReq>0</rt_rxDataReq>
        <rt_rxEstReq>1</rt_rxEstReq>
        <rt_rxFRMR>0</rt_rxFRMR>
        <rt_rxICount>0</rt_rxICount>
        <rt_rxREJ>0</rt_rxREJ>
        <rt_rxRNR>0</rt_rxRNR>
        <rt_rxRR>0</rt_rxRR>
        <rt_rxRelReq>0</rt_rxRelReq>
        <rt_rxSABME>0</rt_rxSABME>
        <rt_rxSCount>0</rt_rxSCount>
        <rt_rxUA>0</rt_rxUA>
        <rt_rxUNCount>0</rt_rxUNCount>
        <rt_txCount>618</rt_txCount>
        <rt_txCountBusy>0</rt_txCountBusy>
        <rt_txDISC>0</rt_txDISC>
        <rt_txDM>0</rt_txDM>
        <rt_txFRMR>0</rt_txFRMR>
        <rt_txICount>0</rt_txICount>
        <rt_txREJ>0</rt_txREJ>
        <rt_txRNR>0</rt_txRNR>
        <rt_txRR>0</rt_txRR>
        <rt_txSABME>618</rt_txSABME>
        <rt_txUA>0</rt_txUA>
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
    </isdnsg>
</root>
```

Get Resource with only Config

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/isdnsg/10001?filter=config
```

Header Response:

Sample Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 17 May 2011 19:13:56 GMT
```

XML Response:

Copyright © 2015 Sonus Networks. All rights reserved.

Sample XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
    <status>
        <http_code>200</http_code>
    </status>
    <isdnsg id="10001" href="https://192.168.1.183/rest/isdnsg/10001">
        <ActionsetTableNumber>0</ActionsetTableNumber>
        <ApplyToPortName
href="https://192.168.1.183/linecard/1/telcods1port/1">1.1</ApplyToPortName>
<ConfigIEState>1</ConfigIEState>
        <Description>REST ISDN SG</Description>

<IsdnAllowCallingNameDisplayToSwitch>0</IsdnAllowCallingNameDisplayToSwitch>
<IsdnServiceMessageCapability>1</IsdnServiceMessageCapability>
        <IsdnSgDirection>2</IsdnSgDirection>
        <IsdnSgHuntMethod>0</IsdnSgHuntMethod>
        <IsdnSgOverlapRxMode>0</IsdnSgOverlapRxMode>
        <IsdnSgRingbackPlayPolicy>0</IsdnSgRingbackPlayPolicy>
        <IsdnSgSideOrientation>0</IsdnSgSideOrientation>
        <IsdnSgSwitchVariant>3</IsdnSgSwitchVariant>
        <IsdnSgTimerT301>180</IsdnSgTimerT301>
        <IsdnSgTimerT302>15</IsdnSgTimerT302>
        <IsdnSgTimerT303>4</IsdnSgTimerT303>
        <IsdnSgTimerT305>30</IsdnSgTimerT305>
        <IsdnSgTimerT308>4</IsdnSgTimerT308>
        <IsdnSgTimerT309>6</IsdnSgTimerT309>
        <IsdnSgTimerT310>30</IsdnSgTimerT310>
        <IsdnSgTimerT313>4</IsdnSgTimerT313>
        <IsdnSgTimerT314>4</IsdnSgTimerT314>
        <IsdnSgTimerT316>120</IsdnSgTimerT316>
        <IsdnSgTimerT322>4</IsdnSgTimerT322>
        <IsdnSgTimerT3M1>120</IsdnSgTimerT3M1>

<IsdnStopFarEndT310UponTryingFromSip>0</IsdnStopFarEndT310UponTryingFromSip>
<RouteTableNumber
href="https://192.168.1.183/routingtable/1">1</RouteTableNumber>
        <ToneTableNumber
href="https://192.168.1.183/tonetable/1">1</ToneTableNumber>
    </isdnsg>
</root>
```

Get Resource with only Statistics

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/isdnsg/10001?filter=statistics
```

Header Response:

Copyright © 2015 Sonus Networks. All rights reserved.

Sample Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2011 19:58:07 GMT
```

XML Response:

Copyright © 2015 Sonus Networks. All rights reserved.

Sample XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
    <status>
        <http_code>200</http_code>
    </status>
    <isdnsg id="10001" href="https://192.168.1.183/rest/isdnsg/10001">
        <rt_CurrentActiveCalls>0</rt_CurrentActiveCalls>
        <rt_IncomingCallaccepts>0</rt_IncomingCallaccepts>
        <rt_IncomingCallattempts>0</rt_IncomingCallattempts>
        <rt_IncomingCallcompletes>0</rt_IncomingCallcompletes>
        <rt_IncomingCallrejects>0</rt_IncomingCallrejects>
        <rt_IsdnSgQ921State>0</rt_IsdnSgQ921State>
        <rt_OutgoingCallaccepts>0</rt_OutgoingCallaccepts>
        <rt_OutgoingCallattempts>0</rt_OutgoingCallattempts>
        <rt_OutgoingCallcompletes>0</rt_OutgoingCallcompletes>
        <rt_OutgoingCallrejects>0</rt_OutgoingCallrejects>
        <rt_TotalCallsProcessed>0</rt_TotalCallsProcessed>
        <rt_TotalConnectedCalls>0</rt_TotalConnectedCalls>
        <rt_TotalErroredCalls>0</rt_TotalErroredCalls>
        <rt_TotalRefusedCalls>0</rt_TotalRefusedCalls>
        <rt_linkDownCount>350</rt_linkDownCount>
        <rt_linkUpCount>0</rt_linkUpCount>
        <rt_rxCount>0</rt_rxCount>
        <rt_rxDISC>0</rt_rxDISC>
        <rt_rxDM>0</rt_rxDM>
        <rt_rxDataReq>0</rt_rxDataReq>
        <rt_rxEstReq>1</rt_rxEstReq>
        <rt_rxFRMR>0</rt_rxFRMR>
        <rt_rxICount>0</rt_rxICount>
        <rt_rxREJ>0</rt_rxREJ>
        <rt_rxRNR>0</rt_rxRNR>
        <rt_rxRR>0</rt_rxRR>
        <rt_rxRelReq>0</rt_rxRelReq>
        <rt_rxSABME>0</rt_rxSABME>
        <rt_rxSCount>0</rt_rxSCount>
        <rt_rxUA>0</rt_rxUA>
        <rt_rxUNCount>0</rt_rxUNCount>
        <rt_txCount>1401</rt_txCount>
        <rt_txCountBusy>0</rt_txCountBusy>
        <rt_txDISC>0</rt_txDISC>
        <rt_txDM>0</rt_txDM>
        <rt_txFRMR>0</rt_txFRMR>
        <rt_txICount>0</rt_txICount>
        <rt_txREJ>0</rt_txREJ>
        <rt_txRNR>0</rt_txRNR>
        <rt_txRR>0</rt_txRR>
        <rt_txSABME>1401</rt_txSABME>
        <rt_txUA>0</rt_txUA>
    </isdnsg>
</root>
```

Get config and statistics (default)

Usage Example:

Copyright © 2015 Sonus Networks. All rights reserved.

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/isdnsg/10001?filter="config,statistics"
```

Header Response:

Sample Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2011 20:31:26 GMT
```

XML Response:

Sample XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
    <status>
        <http_code>200</http_code>
    </status>
    <isdnsg id="10001" href="https://192.168.1.183/rest/isdnsg/10001">
        <ActionsetTableNumber>0</ActionsetTableNumber>
        <ApplyToPortName
href="https://192.168.1.183/linecard/1/telcods1port/1">1.1</ApplyToPortName>
<ConfigIEState>1</ConfigIEState>
        <Description>REST ISDN SG</Description>

<IsdnAllowCallingNameDisplayToSwitch>0</IsdnAllowCallingNameDisplayToSwitch>
<IsdnServiceMessageCapability>1</IsdnServiceMessageCapability>
        <IsdnSgDirection>2</IsdnSgDirection>
        <IsdnSgHuntMethod>0</IsdnSgHuntMethod>
        <IsdnSgOverlapRxMode>0</IsdnSgOverlapRxMode>
        <IsdnSgRingbackPlayPolicy>0</IsdnSgRingbackPlayPolicy>
        <IsdnSgSideOrientation>0</IsdnSgSideOrientation>
        <IsdnSgSwitchVariant>3</IsdnSgSwitchVariant>
        <IsdnSgTimerT301>180</IsdnSgTimerT301>
        <IsdnSgTimerT302>15</IsdnSgTimerT302>
        <IsdnSgTimerT303>4</IsdnSgTimerT303>
        <IsdnSgTimerT305>30</IsdnSgTimerT305>
        <IsdnSgTimerT308>4</IsdnSgTimerT308>
        <IsdnSgTimerT309>6</IsdnSgTimerT309>
        <IsdnSgTimerT310>30</IsdnSgTimerT310>
        <IsdnSgTimerT313>4</IsdnSgTimerT313>
        <IsdnSgTimerT314>4</IsdnSgTimerT314>
        <IsdnSgTimerT316>120</IsdnSgTimerT316>
        <IsdnSgTimerT322>4</IsdnSgTimerT322>
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
        <IsdnSgTimerT3M1>120</IsdnSgTimerT3M1>

<IsdnStopFarEndT310UponTryingFromSip>0</IsdnStopFarEndT310UponTryingFromSip>
<RouteTableNumber
href="https://192.168.1.183/routingtable/1">1</RouteTableNumber>
        <ToneTableNumber
href="https://192.168.1.183/tonetable/1">1</ToneTableNumber>
        <rt_CurrentActiveCalls>0</rt_CurrentActiveCalls>
        <rt_IncomingCallaccepts>0</rt_IncomingCallaccepts>
        <rt_IncomingCallattempts>0</rt_IncomingCallattempts>
        <rt_IncomingCallcompletes>0</rt_IncomingCallcompletes>
        <rt_IncomingCallrejects>0</rt_IncomingCallrejects>
        <rt_IsdnSgQ921State>0</rt_IsdnSgQ921State>
        <rt_OutgoingCallaccepts>0</rt_OutgoingCallaccepts>
        <rt_OutgoingCallattempts>0</rt_OutgoingCallattempts>
        <rt_OutgoingCallcompletes>0</rt_OutgoingCallcompletes>
        <rt_OutgoingCallrejects>0</rt_OutgoingCallrejects>
        <rt_TotalCallsProcessed>0</rt_TotalCallsProcessed>
        <rt_TotalConnectedCalls>0</rt_TotalConnectedCalls>
        <rt_TotalErroredCalls>0</rt_TotalErroredCalls>
        <rt_TotalRefusedCalls>0</rt_TotalRefusedCalls>
        <rt_linkDownCount>495</rt_linkDownCount>
        <rt_linkUpCount>0</rt_linkUpCount>
        <rt_rxCount>0</rt_rxCount>
        <rt_rxDISC>0</rt_rxDISC>
        <rt_rxDM>0</rt_rxDM>
        <rt_rxDataReq>0</rt_rxDataReq>
        <rt_rxEstReq>1</rt_rxEstReq>
        <rt_rxFRMR>0</rt_rxFRMR>
        <rt_rxICount>0</rt_rxICount>
        <rt_rxREJ>0</rt_rxREJ>
        <rt_rxRNR>0</rt_rxRNR>
        <rt_rxRR>0</rt_rxRR>
        <rt_rxRelReq>0</rt_rxRelReq>
        <rt_rxSABME>0</rt_rxSABME>
        <rt_rxSCount>0</rt_rxSCount>
        <rt_rxUA>0</rt_rxUA>
        <rt_rxUNCount>0</rt_rxUNCount>
        <rt_txCount>1980</rt_txCount>
        <rt_txCountBusy>0</rt_txCountBusy>
        <rt_txDISC>0</rt_txDISC>
        <rt_txDM>0</rt_txDM>
        <rt_txFRMR>0</rt_txFRMR>
        <rt_txICount>0</rt_txICount>
        <rt_txREJ>0</rt_txREJ>
        <rt_txRNR>0</rt_txRNR>
        <rt_txRR>0</rt_txRR>
        <rt_txSABME>1980</rt_txSABME>
        <rt_txUA>0</rt_txUA>
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
    </isdnsg>
</root>
```

REST Sample - Login Resource

The Login Resource is used to establish a secure session with the Sonus SBC 1000/2000. The user provided in the URI parameters of this resource must be created through the WebUI prior to using the API and must be of the REST access level. On this page we demonstrate the usage of a POST request using cURL to establish a secure session with the Sonus SBC 1000/2000 system.

Request

```
./curl.exe --cacert 192.168.1.183.crt --data
"Username=admin&Password=admin" -i -v https://192.168.1.183/rest/login
```

Response

```
HTTP/1.1 200 OK
Set-Cookie: PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7; path=/; secure
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 17 May 2011 18:57:03 GMT

<?xml version="1.0">
<root>
 <status>
  <http_code>200</http_code>
 </status>
</root>
```

Session Token

Use the **PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7** cookie from **Set-Cookie** from above login resource response for subsequent CURL Rest calls.

REST Sample - POST Resource

The POST method can be performed on a Sonus SBC 1000/2000 resource to modify the resource with or without an action parameter in the URL.The following examples demonstrate how to use the POST Method on a resource using cURL:

POST on a Resource without action query parameter /rest/isdnsg/{identifier}

Copyright © 2015 Sonus Networks. All rights reserved.

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/isdnsg/10001 --data "Description=Set from cURL&IsdnSgTimerT301=90"
```

Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 17 May 2011 19:39:35 GMT
```

XML Response

Copyright © 2015 Sonus Networks. All rights reserved.

Sample XML Response

```
<?xml version="1.0">
<root>
 <status>
  <http_code>200</http_code>
 </status>
 <isdnsg id="10001" href="https://192.168.1.183/rest/isdnsg/10001">
  <ActionsetTableNumber>0</ActionsetTableNumber>
  <ApplyToPortName
href="https://192.168.1.183/linecard/1/telcods1port/2">1.2</ApplyToPortName>
  <ConfigIEState>1</ConfigIEState>
  <Description>Set from cURL</Description>
  <IsdnAllowCallingNameDisplayToSwitch>0</IsdnAllowCallingNameDisplayToSwitch>
  <IsdnServiceMessageCapability>1</IsdnServiceMessageCapability>
  <IsdnSgDirection>2</IsdnSgDirection>
  <IsdnSgHuntMethod>0</IsdnSgHuntMethod>
  <IsdnSgOverlapRxMode>0</IsdnSgOverlapRxMode>
  <IsdnSgRingbackPlayPolicy>0</IsdnSgRingbackPlayPolicy>
  <IsdnSgSideOrientation>0</IsdnSgSideOrientation>
  <IsdnSgSwitchVariant>6</IsdnSgSwitchVariant>
  <IsdnSgTimerT301>90</IsdnSgTimerT301>
  <IsdnSgTimerT302>15</IsdnSgTimerT302>
  <IsdnSgTimerT303>4</IsdnSgTimerT303>
  <IsdnSgTimerT305>30</IsdnSgTimerT305>
  <IsdnSgTimerT308>4</IsdnSgTimerT308>
  <IsdnSgTimerT309>6</IsdnSgTimerT309>
  <IsdnSgTimerT310>30</IsdnSgTimerT310>
  <IsdnSgTimerT313>4</IsdnSgTimerT313>
  <IsdnSgTimerT314>4</IsdnSgTimerT314>
  <IsdnSgTimerT316>120</IsdnSgTimerT316>
  <IsdnSgTimerT322>4</IsdnSgTimerT322>
  <IsdnSgTimerT3M1>120</IsdnSgTimerT3M1>
  <IsdnStopFarEndT310UponTryingFromSip>1</IsdnStopFarEndT310UponTryingFromSip>
  <RouteTableNumber href="https://192.168.1.183/routingtable/2">2</RouteTableNumber>
  <ToneTableNumber href="https://192.168.1.183/tonetable/10">10</ToneTableNumber>
 </isdnsg>
</root>
```

POST with action query parameter /rest/system?action=setdatetime

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/system?action=setdatetime --data "epochTime=1305759192"
```

Header Response

Copyright © 2015 Sonus Networks. All rights reserved.

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 17 May 2011 19:39:35 GMT
```

XML Response

Sample XML Response

```
<?xml version="1.0">
<root>
<status>
<http_code>200</http_code>
</status>
```

File Upload using POST /rest/system?action=importconfig

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/system?action=importconfig -F "Filename=@symphonyconfig.xml"
```

Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 17 May 2011 19:39:35 GMT
```

XML Response

Copyright © 2015 Sonus Networks. All rights reserved.

Sample XML Response

```
<?xml version="1.0">
<root>
<status>
<http_code>200</http_code>
</status>
```

File Download using POST /rest/system?action=backup

Usage Example:

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-i https://192.168.1.183/rest/system?action=backup -o backup.tar.gz
```

XML Response

Sample XML Response

```
Not Applicable.
The file is sent as a MIME type of application/x-tgz. Client will have to write the
contents into a local file.
```

REST Sample - PUT Resource

The PUT method allows you to create and modify Sonus SBC 1000/2000 REST Resource. Unlinke the POST Resource, modifying a resource with PUT requires all parameters to be sent in the request (including the resource's identifier).The following examples demonstrate how to use the PUT Method on a resource using cURL:

PUT on a Resource /rest/isdnsg/{identifier}

Usage Example:

Copyright © 2015 Sonus Networks. All rights reserved.

```
./curl.exe --cookie PHPSESSID=ima0r3nkaeg8mo0suln67vg4m7 --cacert 192.168.1.183.crt \
-X PUT -i https://192.168.1.183/rest/isdnsg/10011 --data \
"ActionsetTableNumber=0&ApplyToPortName=1.3&IsdnAllowCallingNameDisplayToSwitch=0
&IsdnServiceMessageCapability=1&IsdnSgDirection=2&IsdnSgHuntMethod=0&IsdnSgOverlapRxMode=0
&IsdnSgRingbackPlayPolicy=0&IsdnSgSideOrientation=0&IsdnSgSwitchVariant=6
&Description=Created using cURL&IsdnSgTimerT301=90&IsdnSgTimerT302=15&IsdnSgTimerT303=4
&IsdnSgTimerT305=30&IsdnSgTimerT308=4&IsdnSgTimerT309=6&IsdnSgTimerT310=30
&IsdnSgTimerT313=4&IsdnSgTimerT314=4&IsdnSgTimerT316=120&IsdnSgTimerT322=4
&IsdnSgTimerT3M1=120&IsdnStopFarEndT310UponTryingFromSip=1&RouteTableNumber=1&ToneTableNumber=12"
```

Header Response

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 17 May 2011 20:29:45 GMT
```

XML Response

Copyright © 2015 Sonus Networks. All rights reserved.

Sample XML Response

```
<?xml version="1.0">
<root>
 <status>
  <http_code>200</http_code>
 </status>
 <isdnsg id="10011" href="https://192.168.1.183/rest/isdnsg/10011">
  <ActionsetTableNumber>0</ActionsetTableNumber>
  <ApplyToPortName
href="https://192.168.1.183/linecard/1/telcods1port/3">1.3</ApplyToPortName>
  <ConfigIEState>1</ConfigIEState>
  <Description>Created using cURL</Description>
  <IsdnAllowCallingNameDisplayToSwitch>0</IsdnAllowCallingNameDisplayToSwitch>
  <IsdnServiceMessageCapability>1</IsdnServiceMessageCapability>
  <IsdnSgDirection>2</IsdnSgDirection>
  <IsdnSgHuntMethod>0</IsdnSgHuntMethod>
  <IsdnSgOverlapRxMode>0</IsdnSgOverlapRxMode>
  <IsdnSgRingbackPlayPolicy>0</IsdnSgRingbackPlayPolicy>
  <IsdnSgSideOrientation>0</IsdnSgSideOrientation>
  <IsdnSgSwitchVariant>6</IsdnSgSwitchVariant>
  <IsdnSgTimerT301>90</IsdnSgTimerT301>
  <IsdnSgTimerT302>15</IsdnSgTimerT302>
  <IsdnSgTimerT303>4</IsdnSgTimerT303>
  <IsdnSgTimerT305>30</IsdnSgTimerT305>
  <IsdnSgTimerT308>4</IsdnSgTimerT308>
  <IsdnSgTimerT309>6</IsdnSgTimerT309>
  <IsdnSgTimerT310>30</IsdnSgTimerT310>
  <IsdnSgTimerT313>4</IsdnSgTimerT313>
  <IsdnSgTimerT314>4</IsdnSgTimerT314>
  <IsdnSgTimerT316>120</IsdnSgTimerT316>
  <IsdnSgTimerT322>4</IsdnSgTimerT322>
  <IsdnSgTimerT3M1>120</IsdnSgTimerT3M1>
  <IsdnStopFarEndT310UponTryingFromSip>1</IsdnStopFarEndT310UponTryingFromSip>
  <RouteTableNumber href="https://192.168.1.183/routingtable/1">1</RouteTableNumber>
  <ToneTableNumber href="https://192.168.1.183/tonetable/12">12</ToneTableNumber>
 </isdnsg>
</root>
```

Sonus SBC 1000-2000 API - Deployment Workflow

This page describes a typical deployment workflow where a sample "master" Sonus SBC 1000/2000 configuration is to be applied or copied onto hundreds or thousands of Sonus SBC 1000/2000 nodes. This can be very desirable when system administrators are trying to deploy numerous Sonus SBC 1000/2000 systems in a network sharing the exact same configuration for all resources other than the system specific information.

Note: This is only applicable for Sonus SBC 1000/2000 nodes sharing the same hardware configuration and release version.

Copyright © 2015 Sonus Networks. All rights reserved.

The following steps outline the deployment scenario:

1. Bootstrap the node. This step is the initial set up of the node using the WebUI. This step will create the admin user that can be used for performing the REST APIs.
    a. If any additional routes need to be setup for performing REST requests, they can be configured after the initial setup through the WebUI.
    b. If a specific user needs to be created for running the REST requests, it can be added after the initial setup through the WebUI.
2. Login with the REST user from the REST client.
3. Import the master configuration file using the REST API - for more details, refer to the System Import Config Action
   If the request is successful, the node will reboot.
4. Login from the REST client again.
   This is necessary the previous session was destroyed when the node rebooted as part of Step 3.
5. Perform REST API requests to do any other system specific configuration on any resource.

Sample Code to Perform Deployment Workflow

A REST client is required to first authenticate with the Sonus SBC 1000/2000 REST service to acquire a uniquely assigned session token. This token must be used in any subsequent REST API call during the lifetime of the session.

This page is intended to walk you through a simple example of establishing a session between a REST client and the Sonus SBC 1000/2000 API. All code snippets below use a combination of PHP and libcurl. You may use any other language/library as long as it meets the Sonus SBC 1000/2000 API requirements.

1 Prerequisite - Setting up the HTTP Options
2 How to Acquire a Sonus SBC 1000/2000 Session Token
3 How to Use the Session Token for Import Configuration Request
4 How to Close a Sonus SBC 1000/2000 Session

Prerequisite - Setting up the HTTP Options

Sonus SBC 1000/2000 Web Service (REST) runs on a secure channel i.e. HTTPS, which requires Web Services clients to establish secure communication channel with the service.



If you're not using PHP+libcurl, please refer to documentation of the library you are using to determine the HTTP configuration necessary to properly import and trust the server certificate for secure HTTP

Copyright © 2015 Sonus Networks. All rights reserved.

Setup cURL Options

```
// initialize curl
$curlHandle = curl_init();

// uncomment for debug porposes
//curl_setopt($curlHandle, CURLOPT_VERBOSE, true)

// set the appropriate timeout
curl_setopt($curlHandle, CURLOPT_TIMEOUT, 10);

curl_setopt($curlHandle, CURLOPT_HEADER, false);
// Set so curl_exec returns the result instead of outputting it.
curl_setopt($curlHandle, CURLOPT_RETURNTRANSFER, true);

// This example blindly accepts any server certificate, without doing any
// verification as to which CA signed it, and whether or not that CA is trusted.

// For the sake of simplicity, configure cURL to accept any server(peer) certificate
curl_setopt($curlHandle, CURLOPT_SSL_VERIFYPEER, false);
```

```
// Following captures the details on how libcurl options can be configured to use
secure HTTP.

//curl_setopt($curlHandle , CURLOPT_SSL_VERIFYPEER, true);

// 2, means, check that the common name exists and that it matches the host name of
the server
//curl_setopt($curlHandle , CURLOPT_SSL_VERIFYHOST, 2);

// previously downloaded server cert
//$certLocation = getcwd() . "/CAcerts/ux_rest.crt";
//curl_setopt($curlHandle , CURLOPT_CAINFO, $certLocation);
```

How to Acquire a Sonus SBC 1000/2000 Session Token

Upon successful authentication via **/rest/login**, HTTP response HEADER carries the session token in a cookie. REST clients need to lookup this cookie in the response header and cache it to use it for subsequent REST calls by setting the cookie back in the HTTP request header.



The REST client cookie session expires after **10 minutes of idle session**

Copyright © 2015 Sonus Networks. All rights reserved.

POST Request to /rest/login Resource and Extract Session Token

```
// define an array where we would cache the Session Token Cookie with value
$cookieArr = array();

// Sonus SBC 1000/2000 REST login resource URL
$loginResource = "https://ux_host_or_ipaddress/rest/login";

// set the login resource url in curl
curl_setopt($curlHandle, CURLOPT_URL, $loginResource );

// setup a callback handler for reading and processing the response header fields
// that would come in response to REST login resource POST call
curl_setopt($curlHandle, CURLOPT_HEADERFUNCTION, array($this,
'responseHeaderCallback'));

// tell cURL that we are doing a HTTP POST
curl_setopt($curlHandle, CURLOPT_POST, true);

// set the login resource POST params. The user must be of the REST access level and
created from the WebUI prior to using the API.
$loginPropsArr = array('Username'=>'admin', 'Password'=>'admin');
curl_setopt($curlHandle, CURLOPT_POSTFIELDS, http_build_query($loginPropsArr, '',
'&'));

// exec the HTTP/REST request
$response = curl_exec($curlHandle);

// HTTP response header callback function which processes the header fields
function responseHeaderCallback($curlHandle, $header) {
    if(!strncmp($header, "Set-Cookie:", 11)) {
        $cookiestr = trim(substr($header, 11, -1));
        $cookie = explode(';', $cookiestr);
        $cookie = explode('=', $cookie[0]);
        $cookiename = trim(array_shift($cookie));
        $cookieArr[$cookiename] = trim(implode('=', $cookie));
    }
    return strlen($header);
}
```

How to Use the Session Token for Import Configuration Request

Copyright © 2015 Sonus Networks. All rights reserved.

POST on System Resource (/rest/system?action=importconfig) Using the Session Token

```
// init cURL handle
$curlHandle = curl_init();

$cookieHeader = '';
// previously extracted cookies in $cookieArr (above), is used to add the
// session token in HTTP request header for subsequent REST call
foreach ($cookieArr as $key=>$value) {
    $cookieHeader .= "$key=$value; ";
}
if (!empty($cookieHeader)) {
    curl_setopt($curlHandle, CURLOPT_COOKIE, $cookieHeader);
}

// set other relevant HTTP option as shows in above section _Setting up the HTTP
Options_
$headerArr = array('Accept: ' . $this->acceptType, 'Expect: 100-continue');
$requestBody = array('Filename'=>'@'.$fileName);
curl_setopt($this->curlHandle, CURLOPT_POST, true);
curl_setopt($this->curlHandle, CURLOPT_HTTPHEADER, $headerArr);
curl_setopt($this->curlHandle, CURLOPT_POSTFIELDS, $requestBody);

// Sonus SBC 1000/2000 REST system resource URL
$systemResource = "https://ux_host_or_ipaddress/rest/system?action=importconfig";

// set the system resource url in curl
curl_setopt($curlHandle, CURLOPT_URL, $systemResource );

// exec the HTTP/REST request
$response = curl_exec($curlHandle);
```

How to Close a Sonus SBC 1000/2000 Session

It is recommended that an explicit POST is done on logout resource to cleanup session specific resources the Sonus SBC 1000/2000 node.

Copyright © 2015 Sonus Networks. All rights reserved.

POST on logout Resource (/rest/logout)

```
// init cURL handle
$curlHandle = curl_init();

$cookieHeader = '';
// previously extracted cookies in $cookieArr (above), is used to add the
// session token in HTTP request header for this REST call
foreach ($cookieArr as $key=>$value) {
    $cookieHeader .= "$key=$value; ";
}
if (!empty($cookieHeader)) {
    curl_setopt($curlHandle, CURLOPT_COOKIE, $cookieHeader);
}

// tell cURL that we are doing a HTTP POST
curl_setopt($curlHandle, CURLOPT_POST, true);

// set other relevant HTTP option as shows in above section _Setting up the HTTP
Options_

// Sonus SBC 1000/2000 REST logout resource URL
$logoutResource = "https://ux_host_or_ipaddress/rest/logout";

// set the system resource url in curl
curl_setopt($curlHandle, CURLOPT_URL, $logoutResource);
// logout resource does not require any POST parameter.

// exec the HTTP/REST request
$response = curl_exec($curlHandle);

// any subsequent REST call should result in HTTP Error 401 Unauthorized status
```

Copyright © 2015 Sonus Networks. All rights reserved.

SBC 1000-2000 Installation and Upgrade Guide

This section contains topics for system administrators responsible for installing, initializing, and maintaining the **Sonus SBC 1000/2000 system** and the Application Solution Module (ASM).

SBC 1000-2000 Requirements

- Safety Requirements
- Equipment Rack Requirements
- Power Connection Requirements
- Chassis Mounting Space Requirements
- Restricted Access Location Requirements
- System Grounding Requirements

Installing the Sonus SBC 1000-2000 Hardware

- Installing the SBC 1000 Hardware
- Installing the SBC 2000 Hardware

Running Initial Setup

- Sonus SBC 1000 - Initial Setup
- Sonus SBC 2000 - Initial Setup

Upgrading Sonus SBC 1000-2000

- ASM Roll-up Update
- Downgrading (rolling-back) a Sonus SBC 1000-2000 Upgrade

Supported Platforms

- End of Support Announcements for Sonus SBC 1000-2000
- Internet Explorer Compatibility Mode

Related Articles

Deploying the Survivable Branch Appliance

SBC 1000-2000 Requirements

The Sonus SBC 1000/2000 system is controlled by a "web application", and users interact with it through web browsers from any computer.

Sonus SBC 1000/2000 Client Software Requirements

Please read the Supported Platforms page for Sonus SBC 1000/2000, which lists the required server and client software supported by **Sonus SBC 1000/2000 4.1.x**, including:

- Browsers
- Devices (if you are connecting SIP end-points)
- Application software (if you integrating Sonus SBC 1000/2000 with remote authentication systems)

Copyright © 2015 Sonus Networks. All rights reserved.

Please also read the information below regarding client software requirements for Sonus SBC 1000/2000.

Browser

- If you have disabled JavaScript in your browser or are using a script blocking tool like NoScript, you must enable your browser to execute JavaScript to access Sonus SBC 1000/2000's core WebUI functionality.
- If you have disabled pop-up's in your browser or are using a pop-up blocking software, you must configure your browser to allow popups to access Sonus SBC 1000/2000's core WebUI functionality
- If you have disabled Java applets in your browser, you must enable your browser to execute Java applets. The applet is required for Monitoring Real Time Status on the Sonus SBC 1000/2000 system.

Sonus SBC 1000/2000 Hardware Requirements

Before installing a Sonus SBC 1000/2000 chassis, verify that your installation site meets the following requirements:

- Safety Requirements
- Equipment Rack Requirements
- Power Connection Requirements
- Chassis Mounting Space Requirements
- Restricted Access Location Requirements
- System Grounding Requirements

Safety Requirements

This section details the requirements for safe installation and operation of the Sonus SBC 1000/2000 system. Be sure to review this information before placing the system into operation.

1. **Restricted Access** - The product is for use in a Restricted Access Location only.

2. **Grounding the Sonus SBC 2000 equipment** - The equipment has provision for a permanently connected protective earthing conductor. Attach a 14 AWG copper wire and a 1-hole UL approved lug to the grounding connection. Use Panduit PN14-6R or equivalent.

3. **Rack Mount Instructions**
(a) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature specified by the manufacturer.
(b) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
(c) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
(d) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
(e) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

4. **CAUTION** - Notes for Replaceable batteries and Telephone line cord.
(a) Replaceable Batteries - CAUTION: Risk of Explosion if Battery is replaced by an Incorrect Type. Dispose of Used Batteries According to the Instructions.

Copyright © 2015 Sonus Networks. All rights reserved.

(b) Telephone Line Cord - CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord.

5.**Nordic Country Notice**
(a) For Finland: "Laite on liitettävä suojamaadoitus¬koskettimilla varustettuun pistorasiaan"
For Norway: "Apparatet må tilkoples jordet stikkontakt"
For Sweden: "Apparaten skall anslutas till jordat uttag"
(b) The equipment must be installed only in a Restricted Access Location.
(c) The systems installed in Sweden, Finland and Norway must have supplementary grounding terminal at the chassis frame for the permanent connection of grounding conductor described in System Grounding Requirements.

Equipment Rack Requirements

Sonus SBC 1000/2000 Series rack-mounted equipment requires an EIA-standard 19 inch equipment rack with either 4 posts or 2 posts.

> **4-Post Rack Depths**
>
> Mounting equipment is provided for 4-post equipment racks with a depth of 24 or 30 inches (Sonus SBC 2000 only).

Power Connection Requirements

This section describes the requirements for wiring of power connections to the Sonus SBC 1000/2000 system.

- Power Connections and Wiring
  - United States and Canada
  - Europe

For more information about grounding requirements for the Sonus SBC 1000/2000 system, see System Grounding Requirements. For more information the power supply units installed inside the Sonus SBC 1000/2000 chassis, see Sonus SBC 1000/2000 System Power Supplies.

Power Connections and Wiring

Provide AC power of nominal 120V/60Hz or 240V/50Hz for the equipment rack or shelf where the Sonus SBC 1000/2000 system is installed. For each line feed supplied to the rack or shelf, a dedicated primary branch circuit protection is required.

> Sonus SBC 1000/2000 Series equipment must be provided with dedicated branch circuit protection as a means of disconnecting the (electric) main to ensure the proper operation of and the safety of the persons servicing and operating this equipment. Therefore, the customer must provide an external circuit breaker that conforms to local electrical codes.

Power connections to Sonus SBC 1000/2000 Series equipment must be provided from branch mains installed by a trained service personnel. For minimum wire requirements, see the tables below.

United States and Canada

Requirements	

Copyright © 2015 Sonus Networks. All rights reserved.

Minimum Wire Size	14 AWG
Minimum Voltage Rating	300 V
Insulation	PVC
Conductor	Stranded

Europe

Requirements	
Minimum Wire Size	1.63 mm
Minimum Voltage Rating	300 V
Insulation	PVC
Conductor	Stranded

Use only the AC power cord(s) supplied with the Sonus SBC 1000/2000 system.

Sonus SBC 2000 Only: After the IEC power cord is plugged into the power supply module, secure by engaging the retaining clip over the power cord grip.

Chassis Mounting Space Requirements

To ensure proper chassis cooling, allow a minimum of 3 inches (7.5 cm) horizontal (side-to-side) clearance between the chassis and any adjacent equipment. Allow a minimum clearance of 32 inches (81 cm) behind the chassis for proper insertion and extraction of interface cards and power supplies. There are no clearance requirements above or below the chassis. More than one chassis can be mounted in a standard seven (7) foot rack. These space requirements must be met to comply with Telcordia and Euro ISDN (ETSI) standards.

When installing the chassis, allow space around the chassis for proper air flow through the unit. **Do not block the air vents** on either side of the Sonus SBC 1000/2000 system to ensure proper cooling of the unit.

To ensure proper cooling, the heat and exhaust generated by adjacent equipment must be considered when installing the Sonus SBC 1000/2000 chassis.

The air inlet is on the left side. The air exhaust for the power supplies is towards the rear. The air exhaust for the rest of the system is towards the right side of the chassis.

Restricted Access Location Requirements

Sonus SBC 1000/2000 Series equipment must be installed in restricted access areas such as dedicated equipment room, or electrical closet, in accordance with Articles 110-26 and 110-27 of the 1999 United States National Electrical Code ANSI/NFPA 70.

Copyright © 2015 Sonus Networks. All rights reserved.

A ***RESTRICTED ACCESS LOCATION*** is a location for equipment where both of the following apply:

1. Access can only be gained by service persons or by users who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken; and
2. Access is through the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.

System Grounding Requirements

This section describes the grounding requirements for Sonus SBC 1000/2000 systems.

- Grounding Requirements
  - United States and Canada Grounding Connections
  - Europe Grounding Connections
- Connecting the Sonus SBC 1000/2000 Chassis to Earth Ground
  - To Ground the Sonus SBC 2000 System
  - To Ground the Sonus SBC 1000 System

Grounding Requirements

Sonus SBC 1000/2000 Series equipment must be grounded to the building ground network. For ground wire specifics, see the tables below for the United States, Canada and Europe.

⚠ Only qualified service personnel should perform the electrical procedures for grounding wire installation.

United States and Canada Grounding Connections

Requirements	
Minimum Wire Size	14 AWG
Minimum Voltage Rating	300 V
Conductor	Stranded

Europe Grounding Connections

Requirements	
Minimum Wire Size	1.63 mm
Minimum Voltage Rating	300 V
Conductor	Stranded

Connecting the Sonus SBC 1000/2000 Chassis to Earth Ground

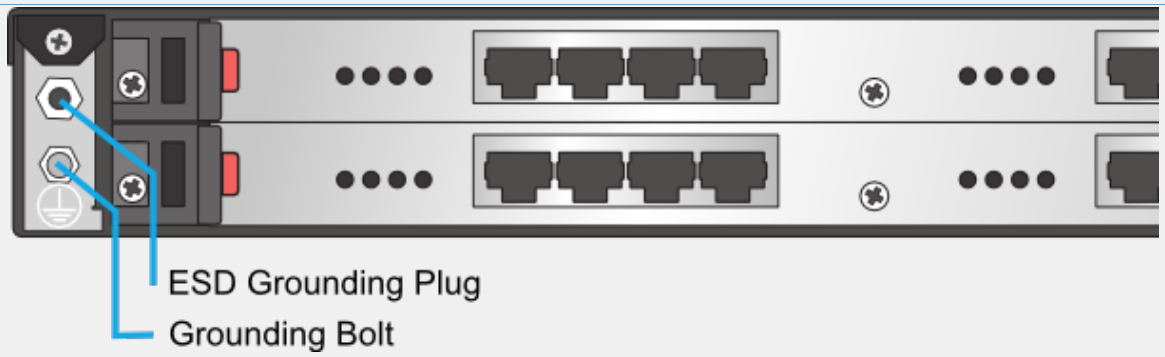
When installing the chassis, connect the earth ground wires from the Sonus SBC 1000/2000 chassis to the facility ground bus.

Copyright © 2015 Sonus Networks. All rights reserved.

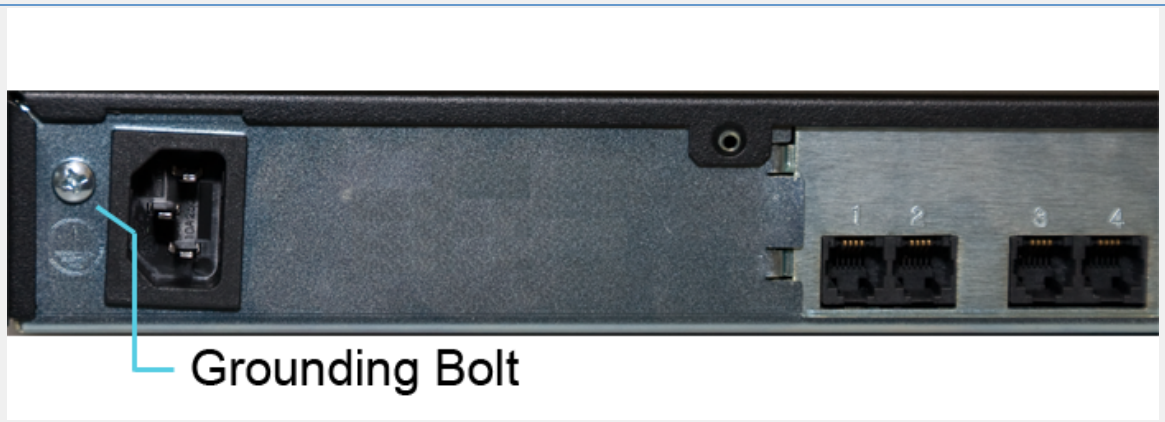
You must provide connections between the earth ground connection points on the chassis and the facility ground bus. To avoid a potential electrical hazard, be sure to confirm that the system power supplies are physically disconnected from the power feed before installing the wires.

Use the grometed holes on the right and left flanges of the rack, as the attachment points for the safety ground wiring described in the following procedure.

Ground Connections on Left Rear Panel of the Sonus SBC 2000



Ground Connections on Left Rear Panel of the Sonus SBC 1000



To Ground the Sonus SBC 2000 System

1. Locate the ground connection bolt at the back left corner of the chassis.
2. For Sonus SBC 2000, attach 14 AWG copper wire and a 1-hole UL approved lug to the grounding bolt. Use Panduit PN14-6R or equivalent.

To Ground the Sonus SBC 1000 System

1. Locate the ground connection bolt at the back left corner of the chassis.
2. For Sonus SBC 1000, attach 14 AWG copper wire and a 1-hole UL approved lug to the grounding bolt. Use Panduit PN14-6R or equivalent.

Installing the Sonus SBC 1000-2000 Hardware

Do not remove the top panel of the Sonus SBC 1000/2000 chassis. Operating the Sonus SBC 1000/2000 system with the top panel removed will cause hardware components to overheat and fail. Unauthorized removal of the top panel will void your product warranty and service agreement.

Preparing for Installation

Copyright © 2015 Sonus Networks. All rights reserved.

To Prepare for Sonus SBC 1000/2000 Chassis Installation

1. Unpack and inspect the Sonus SBC 1000/2000 unit
    - Inspect the unit for any damage, and contact Sonus to report any problems.
    - Unpack and inspect the interface cards shipped in separate cartons with your order.
    - Keep all packing material until you have successfully placed your Sonus SBC 1000/2000 unit into service.
2. Review the Safety Requirements and Precautions.
3. Identify an installation site that meets the following Sonus SBC 1000/2000 hardware requirements:
    - Safety Requirements
    - Equipment Rack Requirements
    - Power Connection Requirements
    - Chassis Mounting Space Requirements
    - Restricted Access Location Requirements
    - System Grounding Requirements

Installing the Sonus SBC 1000/2000 Chassis

Follow the instructions for your Sonus SBC 1000/2000 model:

- Installing the SBC 1000 Hardware
- Installing the SBC 2000 Hardware

Installing the SBC 1000 Hardware

This section describes how to prepare for and physically install a Sonus SBC 1000 system.

- Installing the Sonus SBC 1000 Chassis in an Equipment Rack
- Installing Ground Wire, Power Cables and Connect Power
- Next Steps

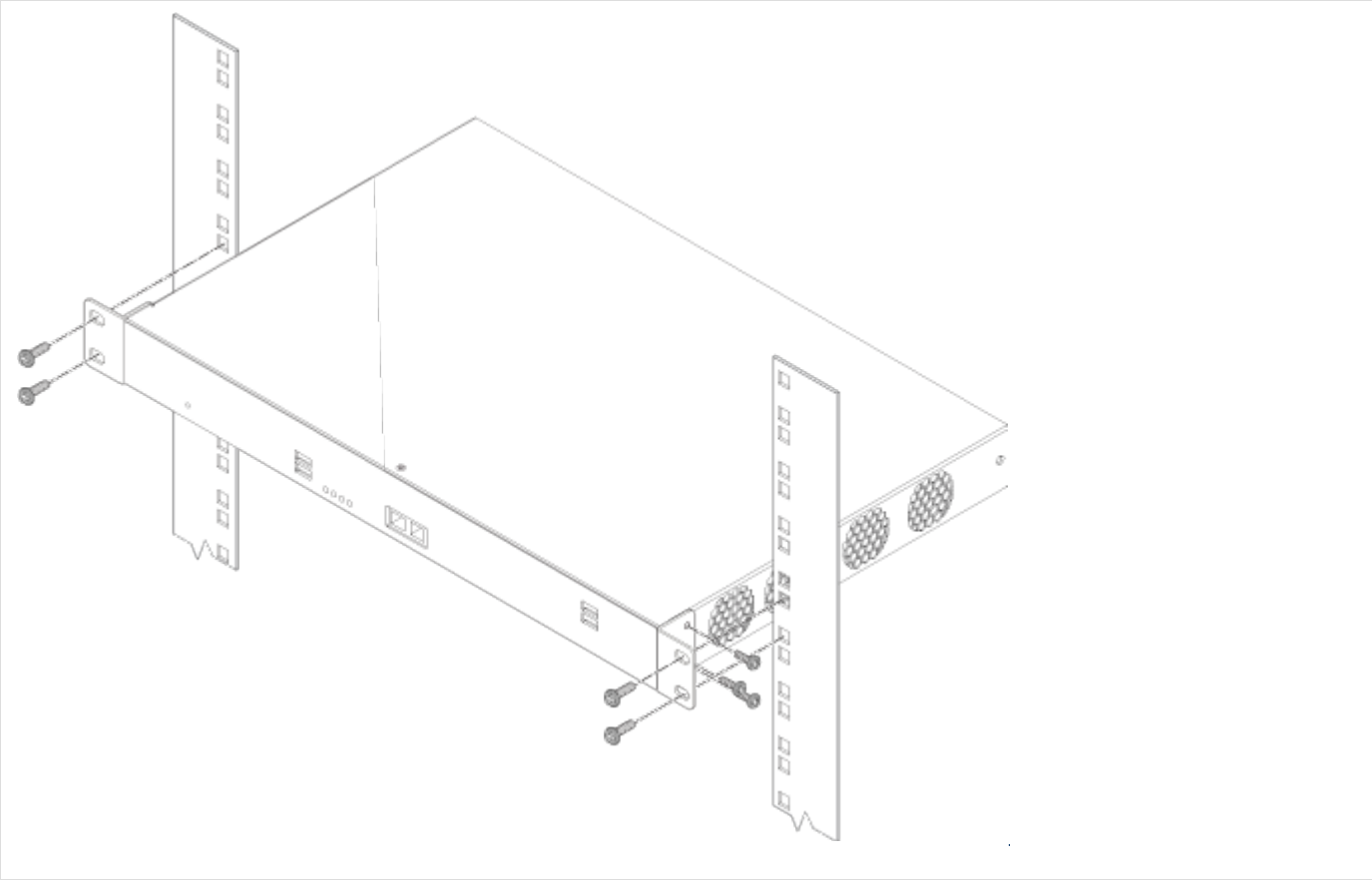
Installing the Sonus SBC 1000 Chassis in an Equipment Rack

The Sonus SBC 1000 chassis can be installed in a standard 19-inch, 2-post or 4-post equipment rack by attaching the rack mounting ears to the front attachment points on both sides of the chassis.

To Install Sonus SBC 2000 in a 2-Post Equipment Rack

1. Attach the 2 rack mounting ears securely to the front mounting points on both sides of the Sonus SBC 1000 chassis.
2. Attach the 2 rack mounting ears securely to the mounting posts of the equipment rack. Refer to the illustration below for visual details of the installation (click to enlarge).

Copyright © 2015 Sonus Networks. All rights reserved.



Installing Ground Wire, Power Cables and Connect Power

After you have completed the physical installation of the Sonus SBC 1000 chassis, connect the grounding wire and power cables

To Install the Grounding Wire and Power Cables

1. Connect a grounding wire to the grounding bolt on the left side of the rear panel, in accordance with System Grounding Requirements.
2. Connect power cords to the power supply and electrical sockets.

DO NOT INSTALL EITHER Sonus or TELECOM CABLES. You must complete the Initial Configuration *before* connecting the Sonus SBC 1000 system to your network.

Next Steps

You are now ready to complete the initial configuration of the Sonus SBC 1000 system. Proceed to Running Initial Setup.

Installing the SBC 2000 Hardware

This section describes how to prepare for and physically install a Sonus SBC 2000 system.

Copyright © 2015 Sonus Networks. All rights reserved.

- Installing the Sonus SBC 2000 Chassis in a 4-Post Equipment Rack
- Installing the Sonus SBC 2000 Chassis in a 2-Post Equipment Rack
- Installing Interface Cards
- Installing Ground Wire, Power Cables and Connect Power
- Installing the Cable Management Bracket
- Next Steps

Installing the Sonus SBC 2000 Chassis in a 4-Post Equipment Rack

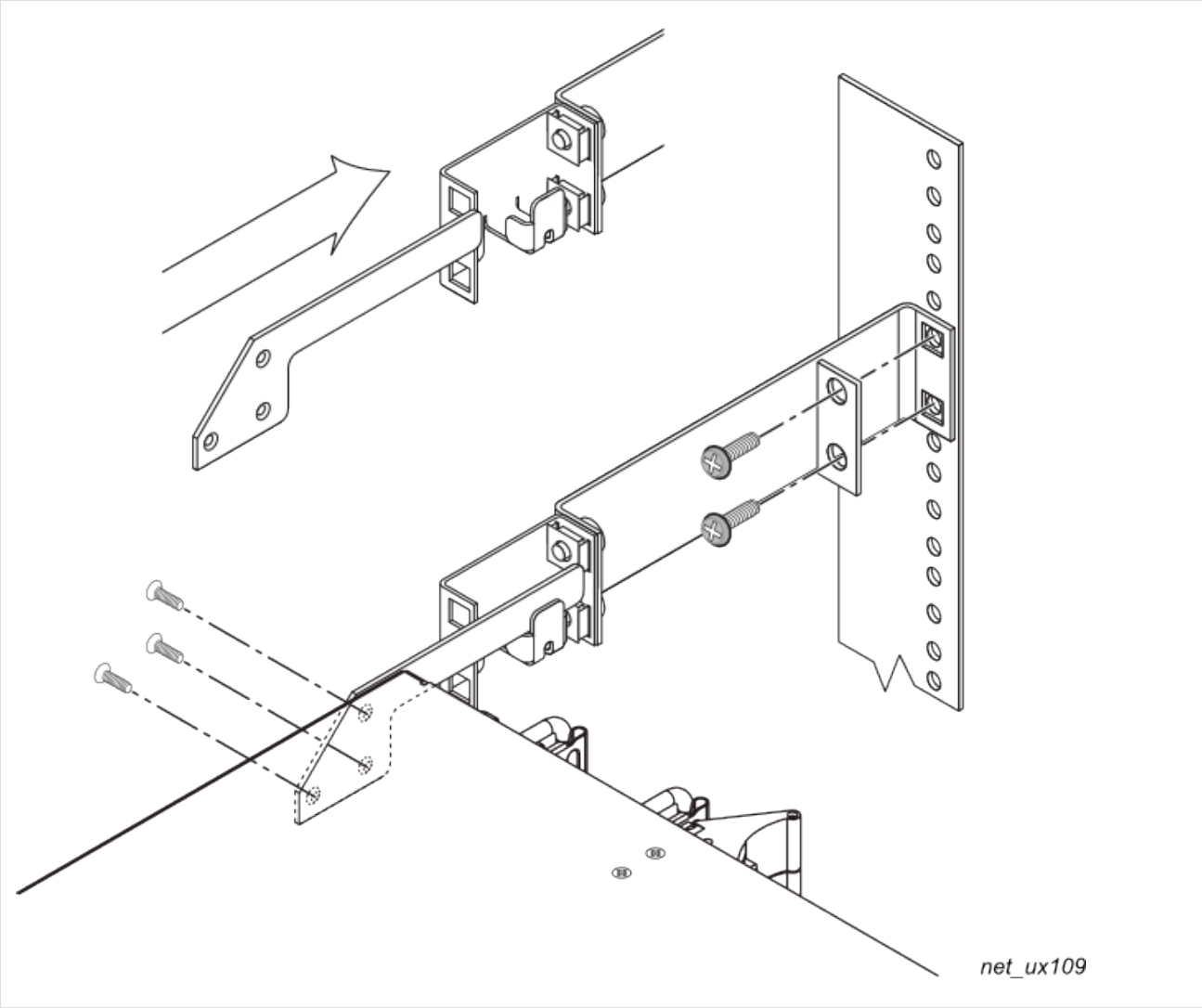
The Sonus SBC 2000 chassis can be installed in a standard 19-inch, 4-post equipment racks. Mounting hardware is provided for racks with 24-inch and 30-inch depths.

Before installing the Sonus SBC 2000 chassis in a 4-post equipment rack, you must first assemble and attach the 2 rear support brackets to the two rear rack posts.

To Assemble and Install the Sonus SBC 2000 Rear Support Brackets

1. In the mounting hardware bag provided with the Sonus SBC 2000 system, find the rear support brackets (2) and 9-inch extension arms (2).
2. If you are installing the Sonus SBC 2000 system into a 30-inch depth rack, attach the extension arms to the support brackets.
3. Attach the support brackets securely to the two rear posts of your equipment rack. Refer to the illustration below for visual details of the assembly:

Copyright © 2015 Sonus Networks. All rights reserved.

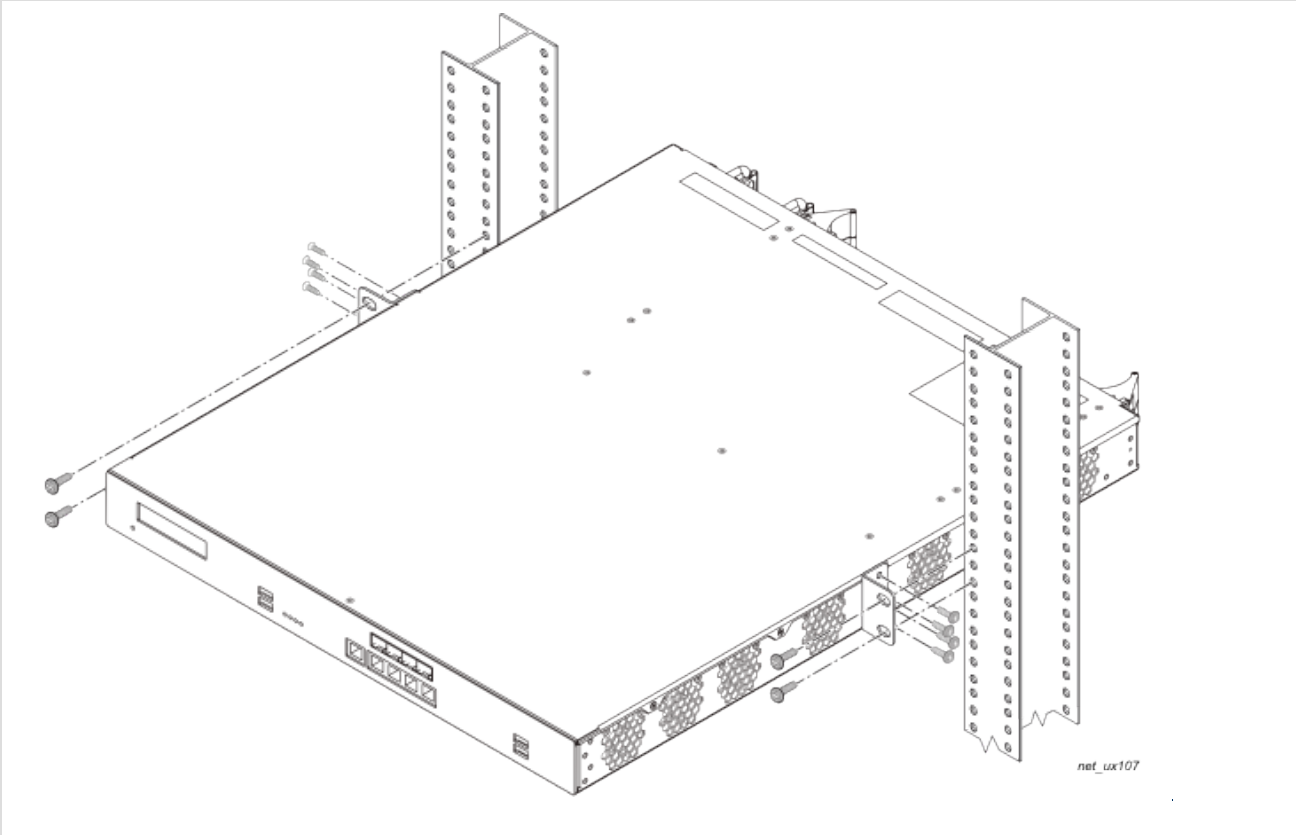


The illustration above shows the rear bracket assembly for a rack with a 30-inch depth. For racks with a 24-inch depth, do not use the 9-inch extension arm and attach each support bracket directly to the rear rack posts.

To Install Sonus SBC 2000 in a 4-Post Equipment Rack

1. Attach the 2 rack mounting ears securely to the front corners of the Sonus SBC 2000 chassis.
2. Attach the 2 pan handle plates securely to the rear corners of the Sonus SBC 2000 chassis.
3. Working with a partner, lift the Sonus SBC 2000 chassis and slide it into the equipment rack, making sure to seat each pan handle plate into the support brackets mounted on the rear support posts.
4. Attach the 2 rack mounting ears securely to the front mounting posts of the equipment rack. Refer to the illustration below for visual details of the installation (click to enlarge).

Copyright © 2015 Sonus Networks. All rights reserved.



Do not block the air vents on either side of the Sonus SBC 2000 chassis. Both sides of the unit must clear to ensure proper cooling of the unit.

Installing the Sonus SBC 2000 Chassis in a 2-Post Equipment Rack

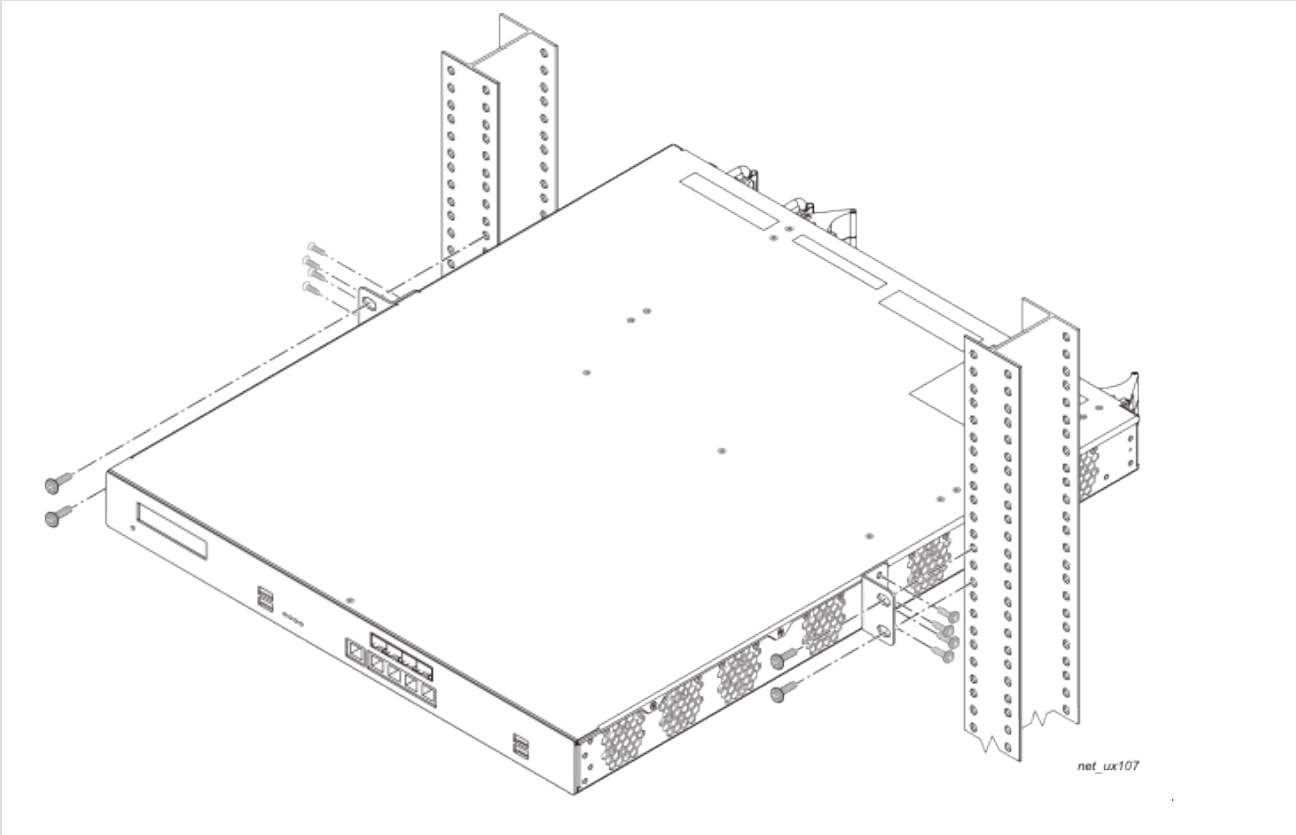
The Sonus SBC 2000 chassis can be installed in a standard 19-inch, 2-post equipment racks by attaching the rack mounting ears to the middle attachment points on both sides of the chassis.

DO NOT mount the Sonus SBC 2000 chassis using only the rack ears attached to the front corners on a 2-post equipment rack. Mounting the chassis using only the front mount rack ears will not provide adequate mechanical support and can cause damage the Sonus SBC 2000 chassis and other equipment in the rack.

To Install Sonus SBC 2000 in a 2-Post Equipment Rack

1. Attach the 2 rack mounting ears securely to the center mounting points on both sides of the Sonus SBC 2000 chassis.
2. Attach the 2 rack mounting ears securely to the mounting posts of the equipment rack. Refer to the illustration below for visual details of the installation (click to enlarge).

Copyright © 2015 Sonus Networks. All rights reserved.



Installing Interface Cards

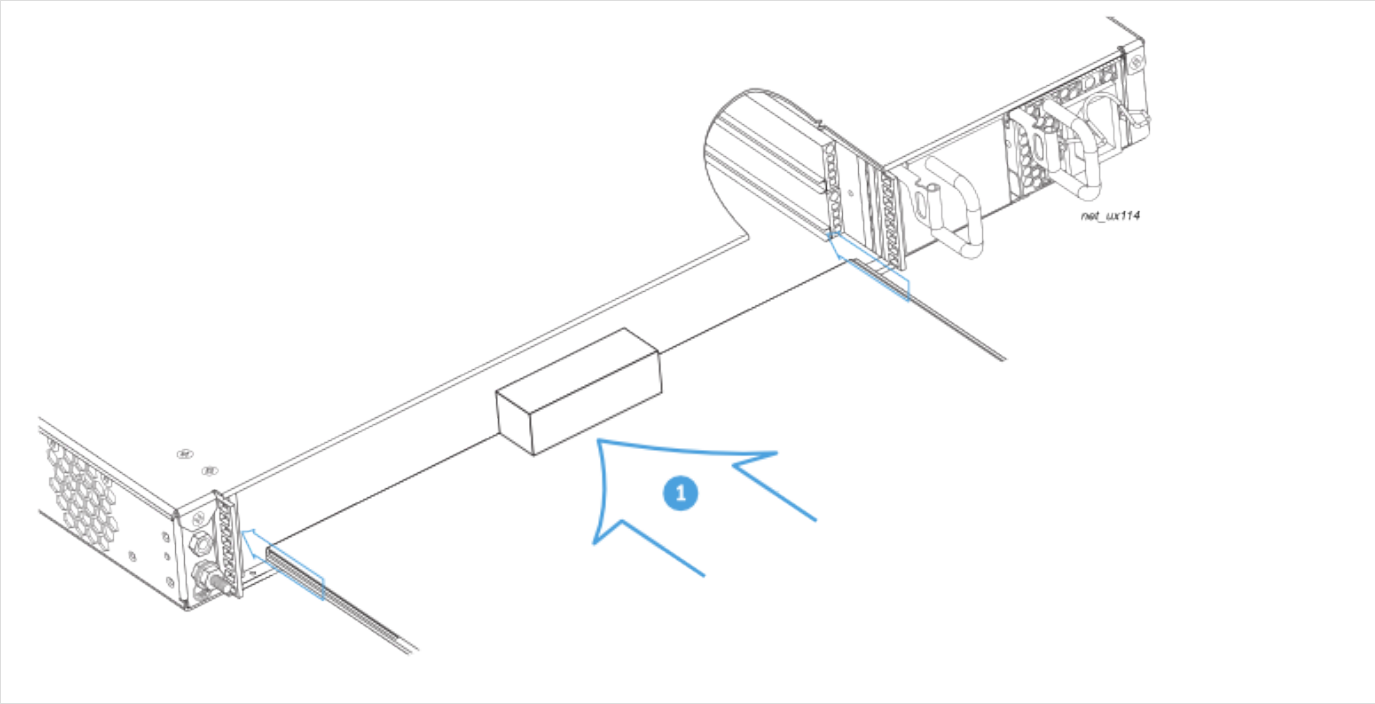
Sonus SBC 2000 interface cards are delivered separately from the Sonus SBC 2000 chassis. Install the cards in the Sonus SBC 2000 chassis before powering on the unit. For more information about Sonus SBC 2000 interface cards, see Sonus SBC 2000 Interface Cards. For more information about installing and removing interface cards, see Inserting and Removing Interface Cards.

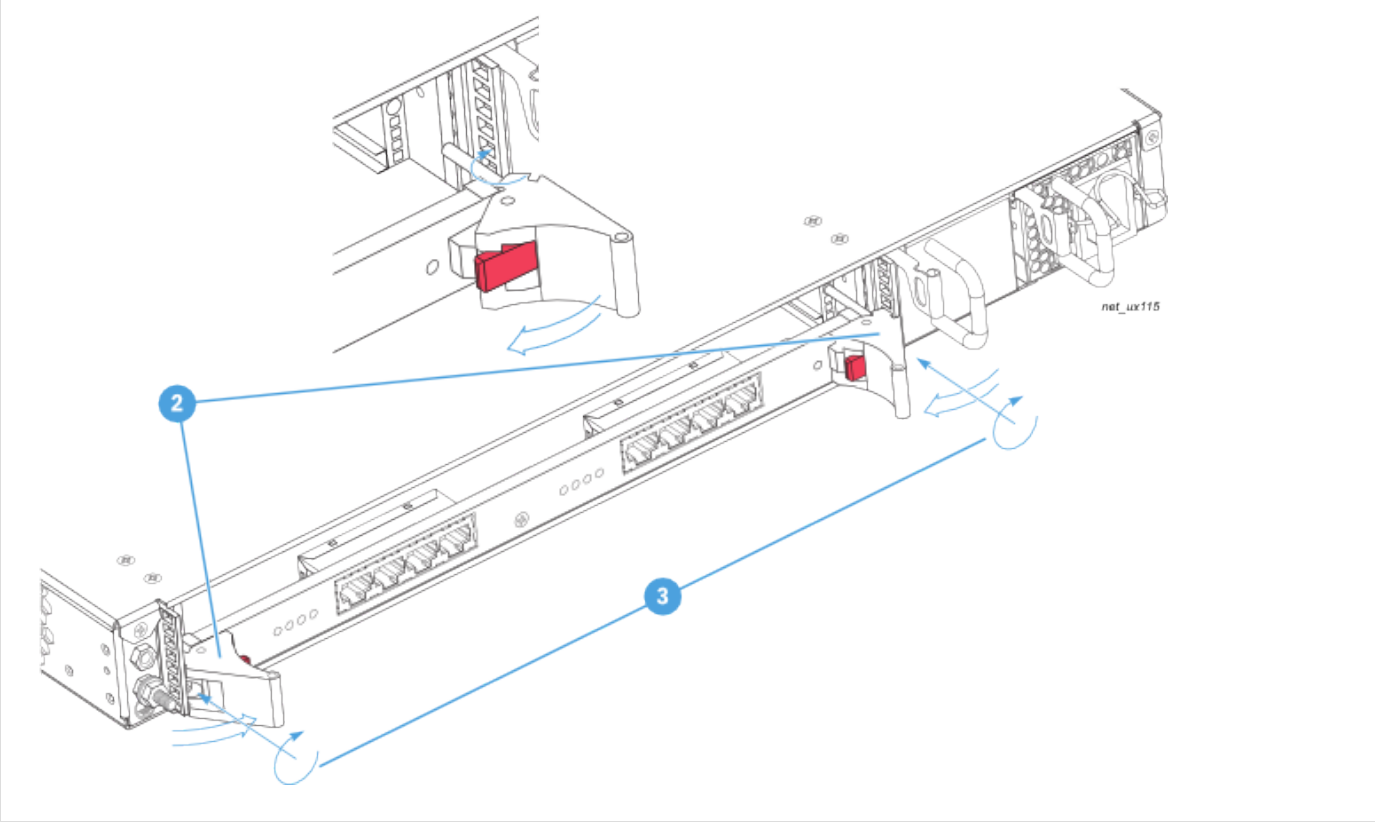
You must power down the Sonus SBC 2000 system before installing or removing Interface Cards. Hot swapping of Interface Cards is not supported in **Sonus SBC 2000 4.0.x**.

To Insert an Interface Card

1. Carefully insert the card so that the left and right edges slide into the mounting slots.
2. Grip the outside of the attachment levers and push toward the inside of the card until the card locks into place.
   The red buttons click and pop out when the card is properly locked into place.
3. Tighten the screws on the right and left side of the interface card.

Copyright © 2015 Sonus Networks. All rights reserved.





Installing Ground Wire, Power Cables and Connect Power

After you have completed the physical installation of the Sonus SBC 2000 chassis, connect the grounding wire and power cables

To Install the Grounding Wire and Power Cables

1. Connect a grounding wire to the grounding bolt on the left side of the rear panel, in accordance with System

Copyright © 2015 Sonus Networks. All rights reserved.

Grounding Requirements.

2. Connect power cords to the power supply and electrical sockets.

> If your equipment rack provides dual power circuits and your unit is equipped with a dual power supply, make sure to plug each power supply into a separate power circuit.

DO NOT INSTALL EITHER Sonus or TELECOM CABLES. You must complete the Initial Configuration *before* connecting the Sonus SBC 2000 system to your network.

Installing the Cable Management Bracket

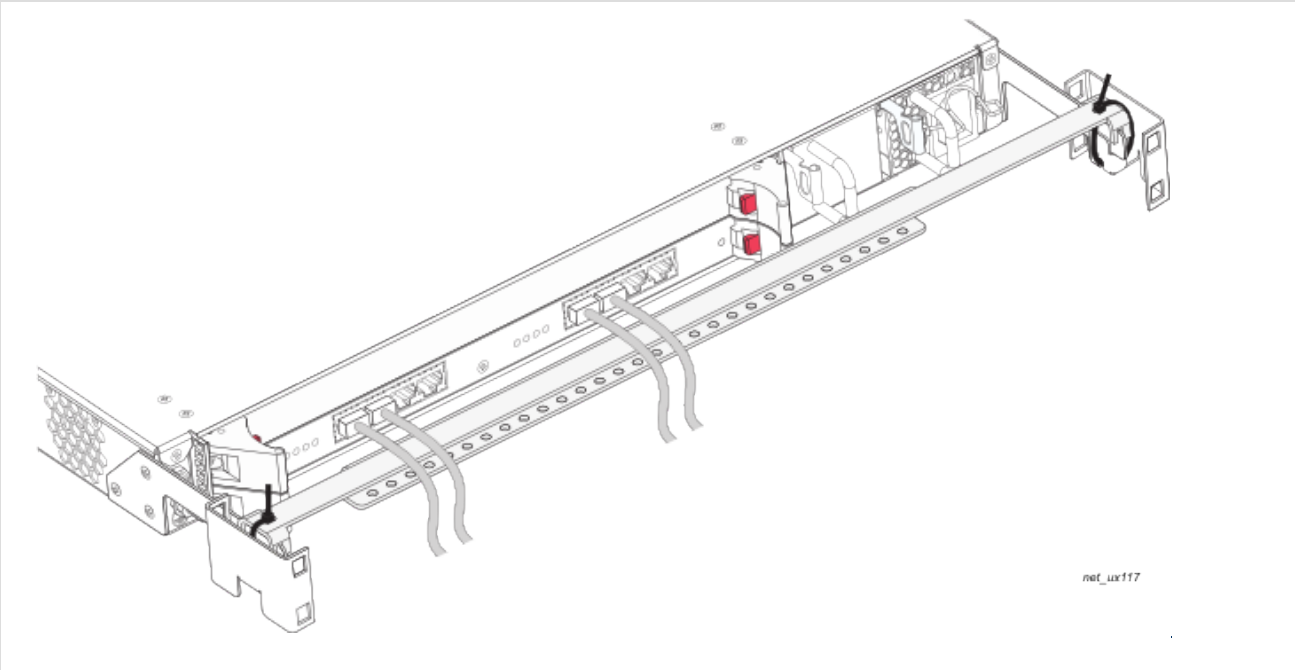
In order to provide cable strain relief for cables connected to Sonus SBC 2000 interface cards, a cable management bracket is provided.

To Install the Cable Management Bracket

1. Place the cable management bracket on top of the pan handle plates.

> If you have installed the Sonus SBC 2000 chassis in a 2-post configuration, you must install the pan handle plates on the rear corners of the chassis.

2. Use the provided cable ties to secure the cable management bracket to the pan handle plates. Refer to the illustration below for visual details of the installation (click to enlarge).



DO NOT INSTALL EITHER Sonus or TELECOM CABLES. You must complete the Initial Configuration *before* connecting the Sonus SBC 2000 system to your network.

Next Steps

You are now ready to complete the initial configuration of the Sonus SBC 2000 system. Proceed to Running Initial Setup.

Copyright © 2015 Sonus Networks. All rights reserved.

Running Initial Setup

If you have installed the Sonus SBC 1000/2000 for the first time, or have reset the Sonus SBC 1000/2000 to factory defaults, then you will need to run the **Initial Setup** to configure the Sonus SBC 1000/2000 System.

When a system is in Factory Default mode, the DHCP client is enabled on **Ethernet 1** and the DHCP server is enabled on **Ethernet 2**. This allows you to connect to the Sonus SBC without having to assign your computer a static IP.

Before you begin

1. Assemble the following equipment:
   - Laptop or other portable computer running a compatible web browser equipped with an Ethernet port.
   - Ethernet patch cord with standard straight-through wiring or crossover wiring.
   - Optional: DHCP server and DNS server (with dynamic DNS enabled). Dynamic DNS is required for initial configuration only if you want to access the system via its serial number/hostname.
2. Verify that the Sonus SBC 1000/2000 system power cable is plugged in and the system is running.

Connect the Sonus SBC 1000/2000

For SBC 1000/2000 - Connect through Ethernet 1

Prerequisite: The DHCP server must be linked with the DNS server through dynamic DNS. For more information, see Managing the DHCP Client.

1. Connect the Ethernet 1 port on the SBC to the DHCP/DNS enabled network. For the location of the Ethernet 1 port, see Sonus SBC 1000 Front Panel or Sonus SBC 2000 Front Panel.
   ▼ Click for a note on how DHCP/DNS use the serial number as the hostname

   The DHCP client acquires an IP address from the DHCP server. During DHCP lease acquisition, the SBC provides the DHCP server with its hostname, which is set to the SBC node's serial number. If your network's DHCP and DNS servers have Dynamic DNS configured properly, the DHCP server will inform the DNS server that the SBC is reachable via its default hostname (i.e., the SBC's serial number). For more information, see Managing the DHCP Client.
2. Direct your PC's browser to the node's serial number as the domain name (i.e., *A4025511270005.yourdocaldomain.doc or A4025511270005.yourdocaldomain.com*).
3. Continue with Initial Setup. See #Proceed with the Initial Setup.

For SBC 1000/2000 - Connect through Ethernet 2

1. Connect the Ethernet 2 port on the SBC to your PC. The SBC's DHCP server will assign an IP address to the PC automatically (192.168.129.10). If you prefer, you can statically assign an address to the PC in the 192.168.129.x subnet (i.e.. 192.168.129.8). See Configuring a Static IP on Windows or Configuring a Static IP on a Mac. For the location of the Ethernet 2 port, see Sonus SBC 1000 Front Panel or Sonus SBC 2000 Front Panel.
2. Direct your PC's browser to the SBC at 192.168.129.2 (default IP address).
3. Continue with Initial Setup. See #Proceed with the Initial Setup.

For SBC 2000 - Connect through the Admin Port

1. Directly connect the Ethernet Cable to the Admin Port on the SBC. To see where the Admin port is located, see Sonus SBC 2000 Front Panel.
2. Assign a temporary static IP address of 192.168.128.8 to the PC.

Copyright © 2015 Sonus Networks. All rights reserved.

- Configuring a Static IP on Windows
- Configuring a Static IP on a Mac

3. Connect to the Sonus SBC 2000 at `192.168.128.2`.
4. Continue with Initial Setup. See #Proceed with the Initial Setup.

Proceed with the Initial Setup

Follow the instructions for your Sonus SBC 1000/2000 model:

- Sonus SBC 1000 - Initial Setup
- Sonus SBC 2000 - Initial Setup

> **Initializing more than one Sonus SBC 1000/2000**
>
> If you are deploying multiple Sonus SBC 1000/2000 units using the same laptop, you may need to **flush the ARP cache on your laptop** before initializing the next Sonus SBC 1000/2000 system.

You're done!

Once you complete the Initial Setup, Sonus SBC 1000/2000 should be set up and ready for use.

1. Browse to the **IP address** or **Host Name** of the Sonus SBC 1000/2000 system you assigned during the Initial Setup.
2. You will be presented with the welcome screen.
3. Click **Enter** to proceed to the login screen.
4. Enter the Sonus SBC 1000/2000 Administrator **Username** and **Password** you have configured during the Initial Setup.

For information on getting started with Sonus SBC 1000/2000, please refer to the following guides:

- Sonus SBC 1000-2000 User's Guide
- Sonus SBC 1000/2000 FAQ and Best Practices

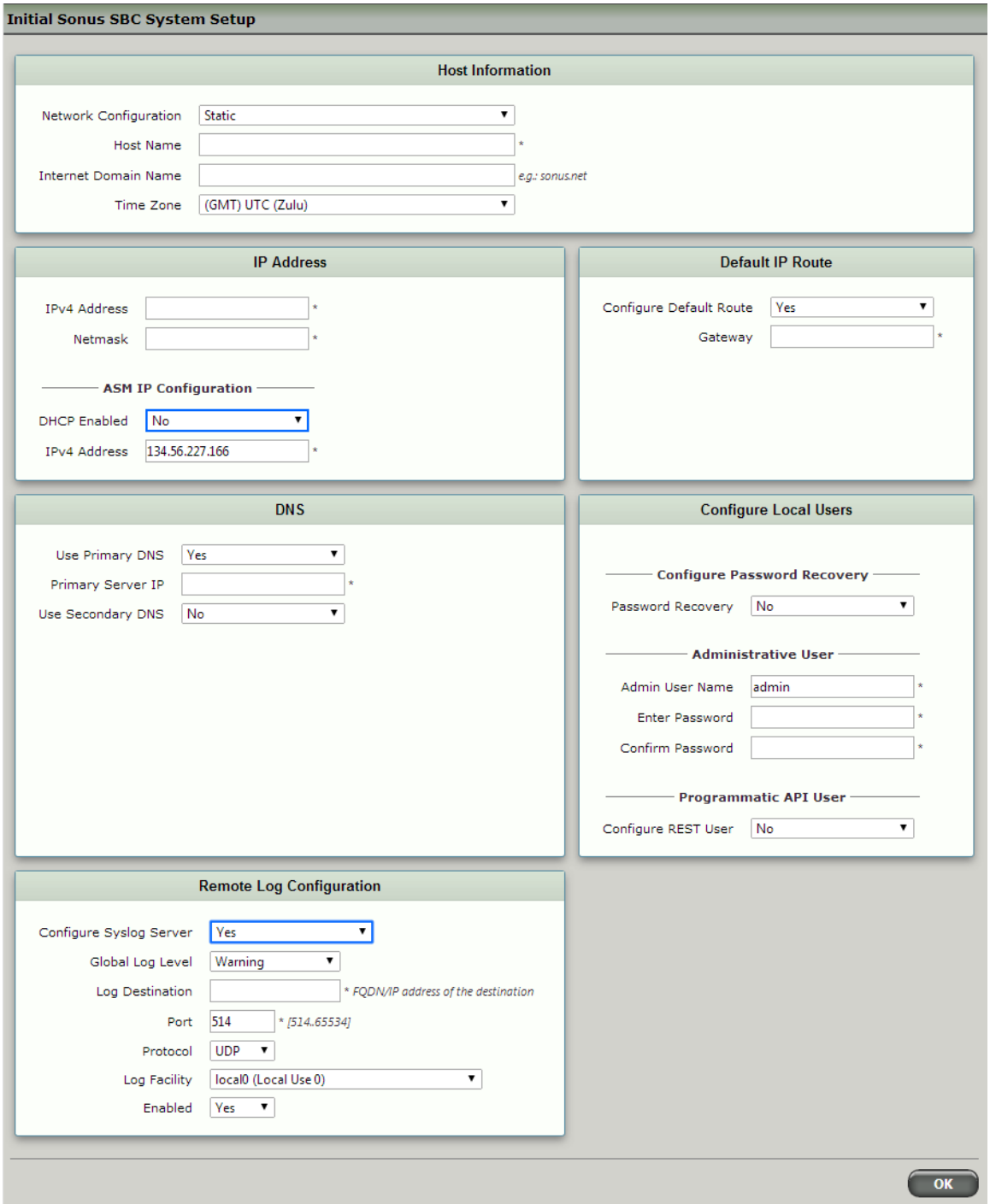
Sonus SBC 1000 - Initial Setup

The Initial Setup process sets the basic configuration for the Sonus SBC 1000/2000 system and is only required the first time you setup the system. After completing this process, you can start using and configuring the system remotely using a web browser.

The Initial Setup screen will present different information depending whether or not your Sonus SBC 1000/2000 is equipped with an Application Solution Module. The screen below is shown for an Sonus SBC 1000/2000 with an installed ASM. If the SBC you are setting up does not have an ASM, certain fields are unavailable. These are noted below.

Initial Setup Screen (Sonus SBC 1000/2000 with built-in ASM)

Copyright © 2015 Sonus Networks. All rights reserved.



Field Definitions - Host Information

Configure Syslog Server

The default value for this field is **No**, and none of the following fields are visible.

Network Configuration

Sets how the SBC acquires the IP address information. Valid entries: Static or Dynamic. Static enables you to enter an IP address manually. Dynamic acquires the interface's IP configuration dynamically from a reachable DHCP server.

Copyright © 2015 Sonus Networks. All rights reserved.

Host Name

Enter the Host Name for the Sonus SBC 1000/2000. This is typically useful when you plan to join Sonus SBC 1000/2000 to a domain.

Internet Domain Name

Typically useful if the Sonus SBC 1000/2000 system resides on a network that uses an internet domain name (such as net.com). This field is displayed only when Static is selected from the **Network Configuration** field.

Time Zone

Use this field to set the local timezone of the SBC1000/2000.

Field Definitions - IP Address

IPV4 Address and Network Mask

Enter an IP address and a Network Mask. The IP address in this field will be configured onto Ethernet Port #1 on the Sonus SBC 2000. This field will not be displayed if the Network Configuration option is set to **Static**.

Field Definitions - ASM IP Configuration

DHCP Enabled

Determines how the ASM configures its network interface. When set to **Yes**, it enables the ASM to automatically configure its network interface from the DHCP server reachable via the Sonus SBC 1000's Ethernet Port #1. Ensure that the IP address is on the same subnet as those provided by your DHCP server. When set to **No**, the IPV4 Address field is displayed and the ASM IP address must be entered manually.

This option is set to **No** by default.

Field Definitions - Default IP Route

Configure Default Route

If you plan to use a gateway to route IP traffic from the Sonus SBC 1000/2000 system, set **Configure Default Route** to **Yes** and specify a **Gateway** IP address. This field is displayed only when Static is selected from the **Network Configuration** field.

Gateway

The IP Address of the default gateway.

Field Definitions - DNS

Use Primary DNS

Copyright © 2015 Sonus Networks. All rights reserved.

If you plan to use host names for routing network traffic from the Sonus SBC 1000/2000 system, set **Use Primary DNS** to **Yes** and provide a **Primary DNS IP** address

Primary Server IP

The IP address of the primary DNS server.

Use Secondary DNS

Optionally, set the **Use Secondary DNS** to**Yes** and provide a **Secondary DNS IP** address.

Field Definitions - Configure Local Users

This section is used to create a local Administrative User and an optional REST User.

Admin User Name

Enter a Admin user name.

Password

Enter a password and then re-enter the same password in the ***Confirm Password*** field.

Configure REST User

Select ***Yes*** if you wish to configure and enable a REST user.

REST User Name

Enter a REST username.

Password

Enter a password and then re-enter the same password in the ***Confirm Password*** field.

Field Definitions - Remote Log Configuration

For detailed information about remote logging see Working with Logging.

Global Log Level

Use this list box to select the desired logging level.

Log Destination

The IP address of the destination log server or its FQDN.

Port

Copyright © 2015 Sonus Networks. All rights reserved.

The logging port on the destination log server.

Protocol

Use this list box to select the transport protocol for the logging information.

Log Facility

Selects a logging facility code to insert in the transmitted log such that the entries can be filtered. For more information see RFC 5424

Once you have clicked **OK**, you may connect the Sonus SBC 2000 to your network using **Ethernet Port 1**. The Sonus SBC 1000/2000 will now be reachable on its new IP address - you may browse to it now.

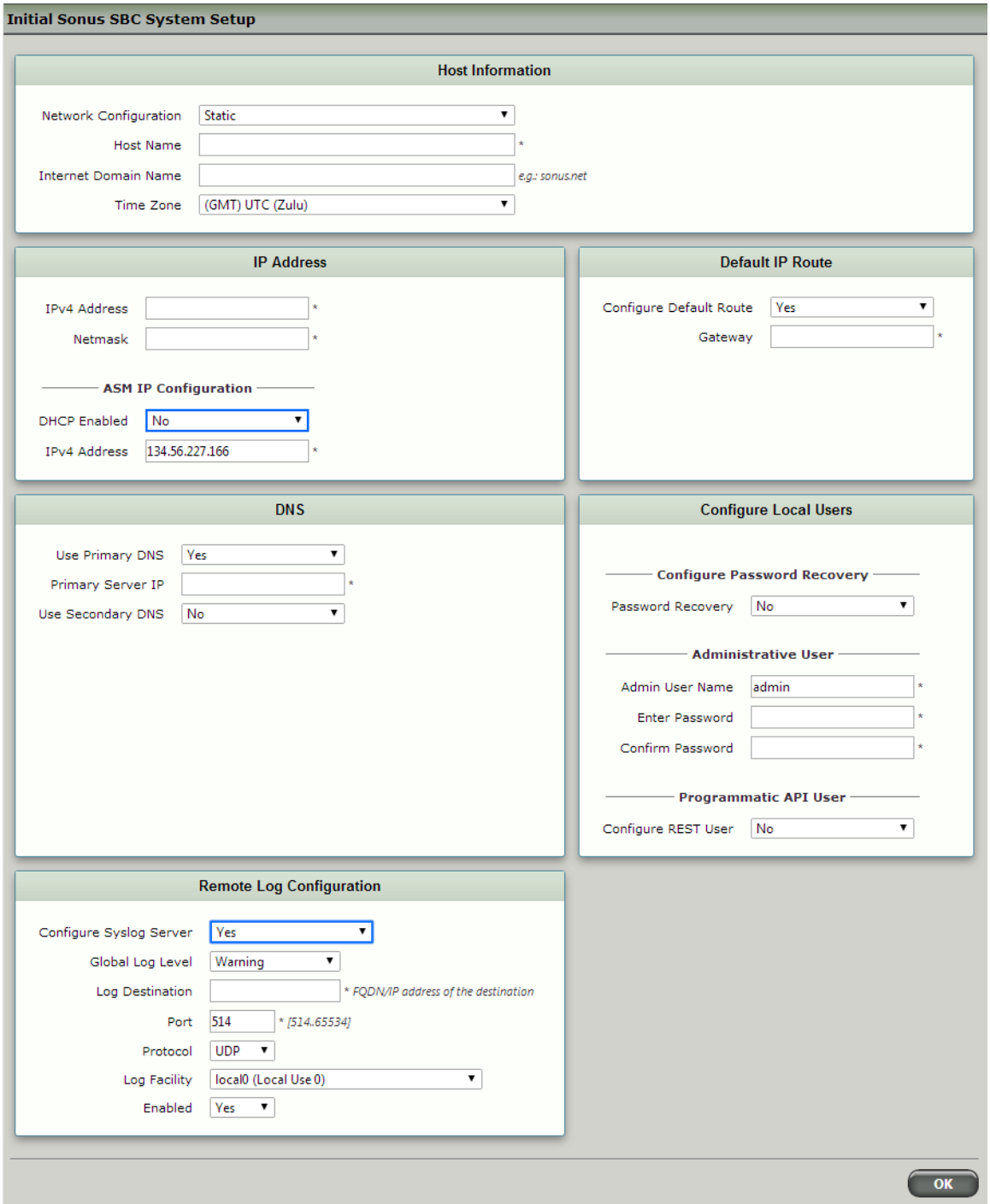
Sonus SBC 2000 - Initial Setup

The Initial Setup process sets the basic configuration for the Sonus SBC 1000/2000 system and is only required the first time you setup the system. After completing this process, you can start using and configuring the system remotely using a web browser.

The Initial Setup screen will present different information depending whether or not your Sonus SBC 1000/2000 is equipped with an Application Solution Module. The screen below is shown for an Sonus SBC 1000/2000 with an installed ASM. If the SBC you are setting up does not have an ASM, certain fields are unavailable. These are noted below.

Initial Setup Screen (Sonus SBC 1000/2000 with built-in ASM)

Copyright © 2015 Sonus Networks. All rights reserved.



Field Definitions - Host Information

Configure Syslog Server

The default value for this field is **No**, and none of the following fields are visible.

Network Configuration

Sets how the SBC acquires the IP address information. Valid entries: Static or Dynamic. Static enables you to enter an IP address manually. Dynamic acquires the interface's IP configuration dynamically from a reachable DHCP server.

Copyright © 2015 Sonus Networks. All rights reserved.

Host Name

Enter the Host Name for the Sonus SBC 1000/2000. This is typically useful when you plan to join Sonus SBC 1000/2000 to a domain.

Internet Domain Name

Typically useful if the Sonus SBC 1000/2000 system resides on a network that uses an internet domain name (such as net.com). This field is displayed only when Static is selected from the **Network Configuration** field.

Time Zone

Use this field to set the local timezone of the SBC1000/2000.

Field Definitions - IP Address

IPV4 Address and Network Mask

Enter an IP address and a Network Mask. The IP address in this field will be configured onto Ethernet Port #1 on the Sonus SBC 2000. This field will not be displayed if the Network Configuration option is set to **Static**.

Field Definitions - ASM IP Configuration

DHCP Enabled

Determines how the ASM configures its network interface. When set to **Yes**, it enables the ASM to automatically configure its network interface from the DHCP server reachable via the Sonus SBC 1000's Ethernet Port #1. Ensure that the IP address is on the same subnet as those provided by your DHCP server. When set to **No**, the IPV4 Address field is displayed and the ASM IP address must be entered manually.

This option is set to **No** by default.

Field Definitions - Default IP Route

Configure Default Route

If you plan to use a gateway to route IP traffic from the Sonus SBC 1000/2000 system, set **Configure Default Route** to **Yes** and specify a **Gateway** IP address. This field is displayed only when Static is selected from the **Network Configuration** field.

Gateway

The IP Address of the default gateway.

Field Definitions - DNS

Use Primary DNS

Copyright © 2015 Sonus Networks. All rights reserved.

If you plan to use host names for routing network traffic from the Sonus SBC 1000/2000 system, set **Use Primary DNS** to **Yes** and provide a **Primary DNS IP** address

Primary Server IP

The IP address of the primary DNS server.

Use Secondary DNS

Optionally, set the **Use Secondary DNS** to**Yes** and provide a **Secondary DNS IP** address.

Field Definitions - Configure Local Users

This section is used to create a local Administrative User and an optional REST User.

Admin User Name

Enter a Admin user name.

Password

Enter a password and then re-enter the same password in the ***Confirm Password*** field.

Configure REST User

Select ***Yes*** if you wish to configure and enable a REST user.

REST User Name

Enter a REST username.

Password

Enter a password and then re-enter the same password in the ***Confirm Password*** field.

Field Definitions - Remote Log Configuration

For detailed information about remote logging see Working with Logging.

Global Log Level

Use this list box to select the desired logging level.

Log Destination

The IP address of the destination log server or its FQDN.

Port

Copyright © 2015 Sonus Networks. All rights reserved.

The logging port on the destination log server.

Protocol

Use this list box to select the transport protocol for the logging information.

Log Facility

Selects a logging facility code to insert in the transmitted log such that the entries can be filtered. For more information see RFC 5424

✅ Once you have clicked **OK**, you may connect the Sonus SBC 2000 to your network using **Ethernet Port 1**. The Sonus SBC 1000/2000 will now be reachable on its new IP address - you may browse to it now.

Upgrading Sonus SBC 1000-2000

This document describes the standard, recommended procedure for upgrading to **Sonus SBC 1000/2000 4.1.x**



Before You Begin

You will need **current software maintenance** to perform the upgrade.

1. Read the release notes for the version of Sonus SBC 1000/2000 you are upgrading to **and the associated upgrade notes**. The upgrade notes (in particular) contain important information that may be relevant to you Sonus SBC 1000/2000 configuration. A newer version of Sonus SBC 1000/2000 may have different requirements than the previous version.
2. Make sure that your environment still complies with the Sonus SBC 1000/2000 requirements and supported platforms.
   ✅ The End of Support Announcements for Sonus SBC 1000-2000 page also has important information regarding platform support for future versions of Sonus SBC 1000/2000.
3. **You must Backup your Sonus SBC 1000/2000 data** in the unlikely event that you encounter an issue with your Sonus SBC 1000/2000 upgrade and need to 'roll back' by downgrading back.
   ✅ We recommend you rename the backup filename to indicate the current software version and build number. For example, rename the backup to `Sonus SBC 1000/2000-1.3.0-b80.tar.gz` if you are currently running a Sonus SBC 1000/2000 version 1.3.0 build 80.
4. In the event of new alarms raised after upgrading the Sonus SBC 1000/2000, ensure you have no outstanding alarms before upgrading the Sonus SBC 1000/2000. To clear alarm(s), follow the instructions outlined in Acting on Displayed Alarms.
5. If you have any problems with your production upgrade which you cannot resolve, create an issue at our support site so that we can assist you.



Performing the Upgrade

Copyright © 2015 Sonus Networks. All rights reserved.

Refer to the appropriate upgrade instructions below for your Sonus SBC 1000/2000 hardware configuration:

- Sonus SBC 1000/2000 with Built-in ASM
- Sonus SBC 1000/2000 without ASM

Upgrading Sonus SBC 1000/2000 with a Built-in ASM

To ensure the Sonus SBC 1000/2000 can communicate with the ASM, you must **always upgrade the SBC Communication Service before upgrading the Sonus SBC 1000/2000 software**.

> The ASM may become unavailable if you upgrade the Sonus SBC 1000/2000 firmware before upgrading the ASM SBC Communication Service.

Follow these steps to upgrade the SBC Communication Service:

1. From the Sonus SBC 1000-2000 Download Center, download the **SBC Communication Service** update — file name `uxcommsvc-release-A.B.C.zip`, where A.B.C refers to the version you are upgrading to.
2. Open the `.zip` file and unpack it to a temporary folder. This will produce a `Setup.msi` file.
3. Apply this SBC Communication Service update by following the instructions outlined in Installing an ASM Package.
4. To ensure the SBC Communication Service was properly updated, verify the Sonus SBC 1000/2000 Communication Service Version has changed to the intended version.

You now may proceed with upgrading the Sonus SBC 1000/2000, follow the instructions below

Upgrading Sonus SBC 1000/2000

1. From the Sonus SBC 1000-2000 Download Center, download the **sw-release-x.y.z**file where x.y.z indicates the version number you are upgrading to:
   - Sonus SBC 1000 Model - the filename will have file extension **`.img`**.
   - Sonus SBC 2000 Model - the filename will have file extension **`.img`**.
2. Select the desired Sonus SBC 1000/2000 upgrade method:
   - Upgrade and activate new version in a single step - use the One-Step Upgrade
   - Upgrade and activate new version during maintenance hours - Upgrading the Inactive Partition
3. Ensure Sonus SBC 1000/2000 has upgraded by verifying the running Sonus SBC 1000/2000 software version.

Congratulations, you have completed upgrading the Sonus SBC 1000/2000! Proceed with the Upgrade Check List



Post-upgrade Check List

1. You must **clear your web browser cache**before you login to Sonus SBC 1000/2000
   - Clearing the browser cache on Internet Explorer
   - Clearing the browser cache on Mozilla Firefox
2. **Perform a backup of your data** on the new Sonus SBC 1000/2000 version. Similarly to the backup preformed in step 3 of the Before You Begin section above, we recommend you rename the backup filenam to indicate the current software version and build number.
3. Ensure there are no new alarms generated after the upgrade. In the event of finding new alarms, address what is causing them.

ASM Roll-up Update

Copyright © 2015 Sonus Networks. All rights reserved.

This article describes the steps necessary to apply ASM Roll-up updates on Sonus SBC 1000/2000 nodes with System Release 2.2.x or higher.

On this Page

- Overview
- Uploading and Installing the ASM Roll-up Files
  - Uploading/Installing the Windows or Cumulative Updates ASM Roll-up File
  - Installing the Windows Update's

Overview

Sonus publishes **Update Packs** on a regular basis through the Sonus Download Center . The Update Packs work with Windows Update and other Non-Windows updates in order to keep the ASM up-to-date. The Update Packs contain a **list** of tested and authorized Windows updates, or specific installation packages such as Lync Cumulative Updates.

> ⚠ The ASM needs to have access to the Internet and specifically to the Microsoft Windows Support website.

Two types of ASM Roll-up Update *.pkg* files are provided and they include the following:

Windows Update		Cumulative Updates
Windows service packs		MS Lync Server Cumulative Updates
Windows Patches		

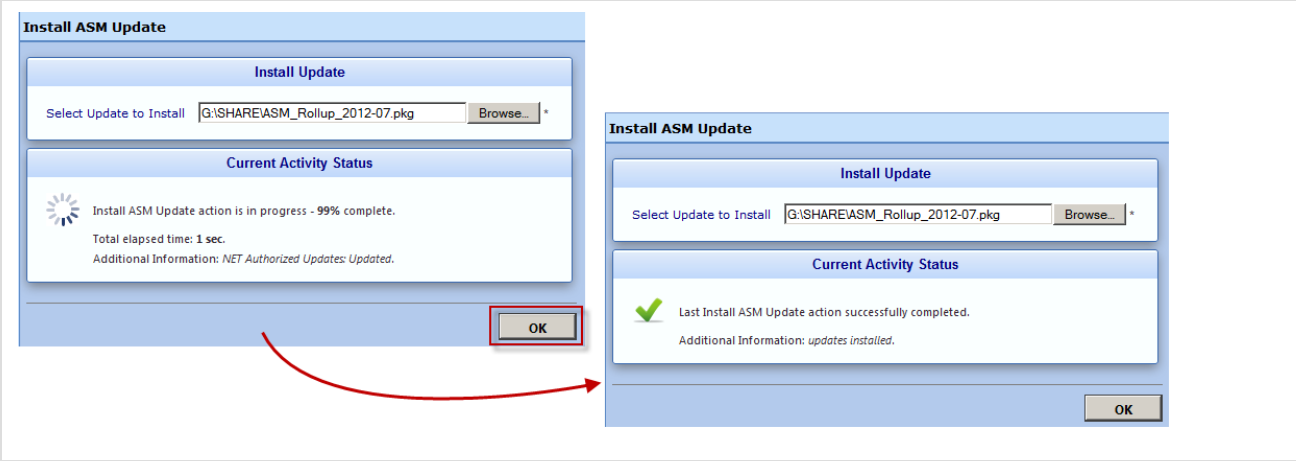
> **NOTE: Windows Update** packs are cumulative (you only need to install the latest release). The update requires the following 2-step process:
>
> - Installation/Uploading the *.pkg* via the Install ASM update task. - This installs the Authorized windows updates list
> - Initiating **Windows Update** installation (via the operational status pane). - This connects to Microsoft support to install the updates listed in the authorization list

Uploading and Installing the ASM Roll-up Files

Uploading/Installing the Windows or Cumulative Updates ASM Roll-up File

1. Download the roll-up file from Sonus Download Center and save it on your desktop or other convenient location.
2. Launch your preferred browser. See Supported Platforms.
3. Login to the Sonus SBC 1000/2000 node through the WebUI.
4. In the WebUI, click the **Tasks** tab.
5. In the left navigation pane, go to **Application Solution Module > Install ASM Update**.

Copyright © 2015 Sonus Networks. All rights reserved.



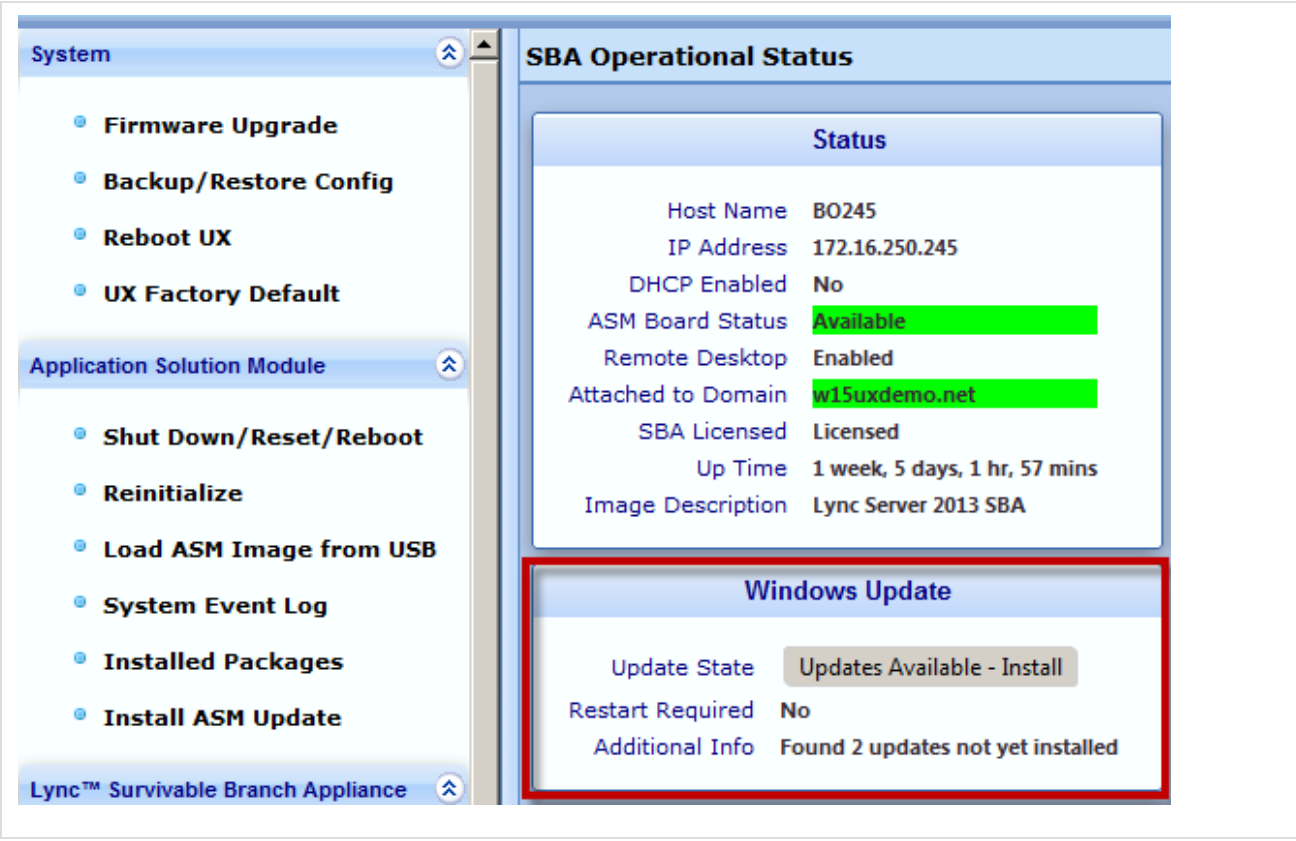
6. Browse to the roll-up (**.pkg**) file.
7. Click **OK**.

Installing the Windows Update's

After a successful upload of a windows update **.pkg** file, the Windows State field in the Windows Update panel changes to **Updates Available - Install**.
Once the **.pkg** file is uploaded to the node, the Operational Status pane, Windows Update, and Update State field will change to **Updates Available - Install**.

To install the updates:

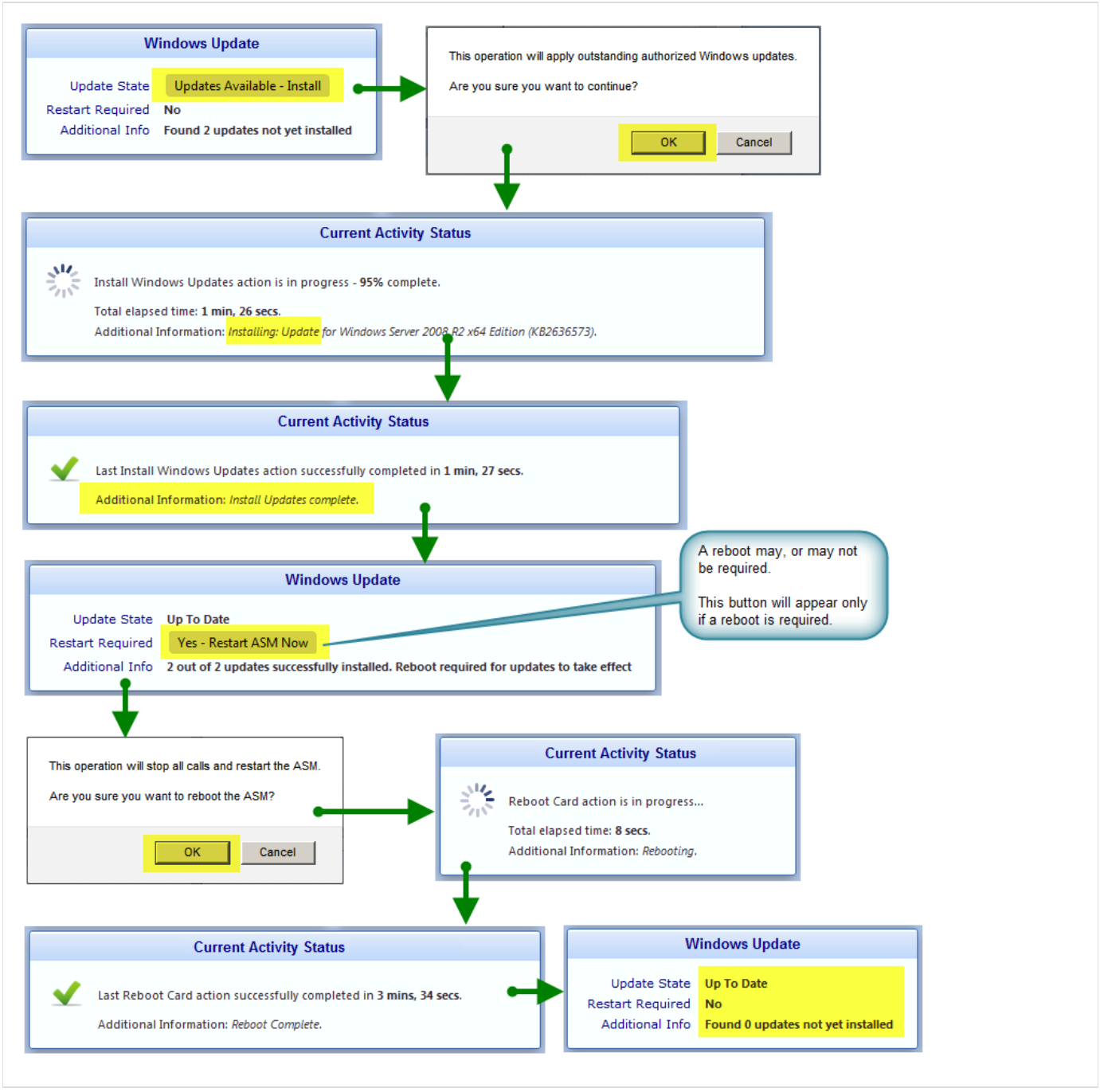
1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, go to **Lync Survivable Branch Appliance > Operational Status**.



Copyright © 2015 Sonus Networks. All rights reserved.

3. Click the **Updates Available - Install** link in the Windows Update panel.
4. Click **OK**.
5. If required, click "Yes - Restart ASM now (this is not always required).

> ⚠ Depending on the size of the update, the reboot may take several minutes.



Downgrading (rolling-back) a Sonus SBC 1000-2000 Upgrade

The 'roll back' procedures on this page describe how to restore your previous version of Sonus SBC 1000/2000 in the unlikely event that you encounter an issue with your Sonus SBC 1000/2000 upgrade.

Copyright © 2015 Sonus Networks. All rights reserved.

Before you begin

Prior to rolling back your Sonus SBC 1000/2000 upgrade, ensure that you have a backup of your Sonus SBC 1000/2000 data for the version you intend to roll back to.

Warning: Restoring From A 3.1 or Higher Configuration Backup

Do not attempt to restore your version 3.0 or earlier SBC 1000/2000 configuration from a backup made us8ing a version 3.1 or higher SBC 1000/2000. Doing so will result in a complete user lockout and the system must be reset to factory default to recover.

Performing the Rollback

Refer to the appropriate upgrade instructions below for your Sonus SBC 1000/2000 hardware configuration:

- Sonus SBC 1000/2000 with Built-in ASM
- Sonus SBC 1000/2000 without ASM

Rollback Sonus SBC 1000/2000 with a Built-in ASM

The instructions in this section may be best coordinated with your Sonus service representative.

Similarly to upgrading, to ensure the Sonus SBC 1000/2000 can communicate with the ASM, you must **downgrade the Sonus SBC 1000/2000 Communication Service before downgrading the Sonus SBC 1000/2000 software**.

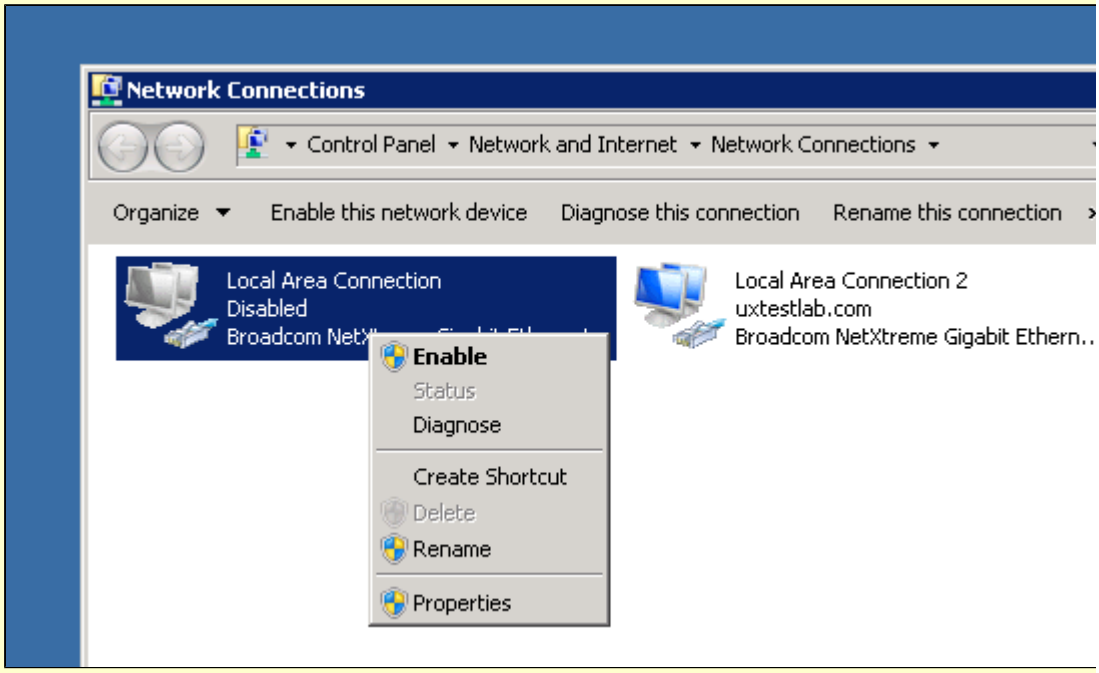
1. Remotely login to the ASM via Remote Desktop.
2. Manually uninstall the current Sonus SBC 1000/2000 Communication Service from the **Programs and Features** via the **Control Panel**.
3. From the Sonus SBC 1000-2000 Download Center, download the **Sonus SBC 1000/2000 Communication Service** `.zip` file for the version that you are downgrading to.
4. Open the `.zip` file and unpack it to a temporary folder. This will produce a `Setup.msi` file.
5. Copy the `Setup.msi` onto a local folder directly onto the ASM.
6. Launch the installer and proceed with the installation wizard.
7. To ensure the Sonus SBC 1000/2000 Communication Service was properly updated, verify the Sonus SBC 1000/2000 Communication Service Version has changed to the intended version.

Important ASM Note

If you are **downgrading from 2.0.x (or later) to 1.3.x (or earlier)**, all disabled Network Adapters on the ASM **mu be enabled**. This is because the 2.0.x (or later) upgrade disables one of the network adapters (by design), and it must be re-enabled if you're downgrading to 1.3.x (or earlier).

Copyright © 2015 Sonus Networks. All rights reserved.

- *Step 1*: Click here to view the instructions for enabling the network adapter
    1. From the **Start** menu - type **View network connections** and select it
    2. You will find at least one disabled network adapter. Enable it as shown below:



Once the network adapter is enabled, you must set the necessary permissions to allow the downgraded Sonus SBC 1000/2000 Communication Service to Install ASM packages via the Sonus SBC 1000/2000 WebUI.

Copyright © 2015 Sonus Networks. All rights reserved.

Step 2: Click here to view the instructions for setting the permissions

1. From the **Start** menu - type **Command Prompt** and select it
2. Enter (or paste in) the following commands - **the order is important**:

```
nfsadmin server deletegroup Sonus SBC 1000/2000
nfsadmin server creategroup Sonus SBC 1000/2000
nfsadmin server addmembers Sonus SBC 1000/2000 169.254.1.1
nfsshare public -o rw=Sonus SBC 1000/2000 root=Sonus SBC 1000/2000
```

3. The results should appear like so:

```
C:\Users\Administrator>nfsadmin server deletegroup Sonus SBC
1000/2000
The settings were successfully updated.

C:\Users\Administrator>nfsadmin server creategroup Sonus SBC
1000/2000
The settings were successfully updated.

C:\Users\Administrator>nfsadmin server addmembers Sonus SBC
1000/2000 169.254.1.1
169.254.1.1 was successfully added to Sonus SBC 1000/2000.
The settings were successfully updated.

C:\Users\Administrator>nfsshare public -o rw=Sonus SBC 1000/2000
root=Sonus SBC 1000/2000
Public was modified successfully
```

You now may proceed with rolling back the Sonus SBC 1000/2000 software version, follow the instructions below

Rollback the Sonus SBC 1000/2000 Software

The Sonus SBC 1000/2000 keeps its system software (firmware) in containers known as "Application Partitions". There are **two** application partitions, one of which is **Active**. When the Sonus SBC 1000/2000 system is operational, it is running off of the **Active Partition**, and the remaining (inactive) partition serves as a spare.

You can rollback to the previous Sonus SBC 1000/2000 version stored in the **inactive** partition:

1. To rollback the Sonus SBC 1000/2000 Software, simply activate the inactive partition.
2. Verify that you are booting from the new partition either by checking the active partition, or by Viewing the Software Version and Hardware ID.
3. Restore the backup configuration data associated with the Sonus SBC 1000/2000 version you have downgraded to.

This completes the rollback procedure.

Supported Platforms

End of Support Announcements

Please read End of Support Announcements for Sonus SBC 1000/2000 for important information regarding the end of support for various platforms and browsers when used with Sonus SBC 1000/2000.

Copyright © 2015 Sonus Networks. All rights reserved.

This page describes the supported platforms for **Sonus SBC 1000/2000 4.1.x**. If a particular platform's version is not mentioned on this page, then we do not support that version of the platform for **Sonus SBC 1000/2000 4.1.x**.

Key: ✅ = Supported; ❌ = Not Supported

Web Browsers	
Microsoft Internet Explorer (#1) (#5)	✅ 10.0 ,11.0 ❌ 6.0, 7.0, 8.0. 9.x
Mozilla Firefox (#1)	✅ Strongly recommend the latest Firefox ESR version, Firefox 24 or higher is required.
Safari	❌ Latest stable version
Chrome	✅ 35 or higher
Communications Servers	
Microsoft	✅ Lync Server 2010, 2013 ✅ Office Communications Server (OCS) 2007 (including R2) ✅ Exchange Server 2007 and 2010 with Unified Messaging
Devices and End-Points	
Polycom	✅ Soundpoint Series (including all Microsoft Certified OCS and Lync devices) ✅ Spectralink 8400
SNOM	✅ 360, 820, 870
NEC	✅ FOMA N900iL/902iL
CounterPath	✅ X-Lite ✅ Eyebeam
Microsoft (#3)	✅ Lync 2010, 2013 ✅ Office Communicator 2007

Microsoft Lync 2010	**Tested SBC 1000/2000 Releases**
Lync 2010 CU4	✅ version 1.3.2 build 89 ✅ version 2.0.1 build 118
Lync 2010 CU5	✅ version 2.0.2 build 132
Lync 2010 CU6	✅ version 2.1.2 build 150
Lync 2010 CU7	✅ version 2.2.0 build 181

Copyright © 2015 Sonus Networks. All rights reserved.

Lync 2010 CU8	✅ version 2.2.1 build 207
Lync 2010 CU9	✅ version 3.0.1 build 254
Lync 2010 CU10	✅ version 3.0.1 build 254
Lync 2010 CU11	✅ version 3.1.0 build 283
Lync 2010 CU12	✅ version 4.0.1 build 353
Lync 2010 CU13	✅ version 4.0.1 build 353
Microsoft Lync 2013	**Tested SBC 1000/2000 Releases**
Lync 2013 CU1	✅ version 2.2.0 build 181
Lync 2013 CU2	✅ version 3.0.0 build 241
Lync 2013 CU3	✅ version 3.0.1 build 254
Lync 2013 CU4	✅ version 3.1.0 build 283
Lync 2013 CU5	✅ version 3.2.0 build 315
Lync 2013 CU6	✅ version 3.2.1 build 322
Lync 2013 CU7	✅ version 4.0.1 build 353
Lync 2013 CU8	✅ version 4.0.1 build 353

Notes:

1. Minimum screen resolution of 1024 x 768 (when these browsers are maximised).
2. Verified using Microsoft certified headphones and handsets such as: Plantronics Audio 110M handset and Plantronics USB Headset
3. Compatibility Mode is unsupported.

End of Support Announcements for Sonus SBC 1000-2000

This page contains announcements of the end of support for various platforms and browsers used with Sonus SBC 1000/2000. These are summarized for upcoming Sonus SBC 1000/2000 releases in the table below. Please see the following sections for the full announcements.

On this page (most recent announcements first):

Copyright © 2015 Sonus Networks. All rights reserved.

Deprecated Web Browsers for Sonus SBC 1000/2000 (14 April 2011)

This section announces the end of Sonus support for certain web browsers for Sonus SBC 1000/2000.

Internet Explorer 9

Internet Explorer 8

Internet Explorer 7

We will **stop supporting older versions of web browsers** as follows:

- Sonus SBC 1000/2000 1.0 will be the last major version of Sonus SBC 1000/2000 to support IE7. This also includes IE 7 in "Compatibility Mode". In "Compatibility Mode", IE 8 and 9 will claim to be IE 7 (or earlier), and will actually run that earlier code.

The details are below. Please refer to the Supported Platforms for more details regarding platform support for Sonus SBC 1000/2000. If you have questions or concerns regarding this announcement, Contact Sonus.

Internet Explorer 7 End of Support Notes

- IE7, now 4+ years after its release, has less than 10% of browser market share. Microsoft has released IE8 and recently IE9.
- Sonus SBC 1000/2000 1.0.3 (due early June 2011) will be the last version of Sonus SBC 1000/2000 to officially support Internet Explorer 7.
- Sonus SBC 1000/2000 1.0.x and earlier versions will continue to work with Internet Explorer 7. However, we will not fix bugs affecting this browser version past the last version of Sonus SBC 1000/2000 1.0.3 to be released.

Internet Explorer Compatibility Mode

Beginning with version 8, Microsoft Internet Explorer (IE) includes a Compatibility View feature which, if enabled for a given web page, causes Internet Explorer to render that page in IE 7 Standards Mode. This allows later versions of the browser to render pages which have not been updated for modern standards support with Internet Explorer. In addition, IE 11 adds support for an Enterprise Mode which causes Internet Explorer to emulate some behaviors of IE 8.

The SBC 1000 and 2000 fully support modern web standards for all supported browsers, and thus neither need nor support Compatibility View or Enterprise Mode.

Enterprise Mode is centrally managed within an IT organization, and is intended to be enabled only for sites for which it is required. Enterprise Mode should not be enabled for the SBC 1000 and 2000.

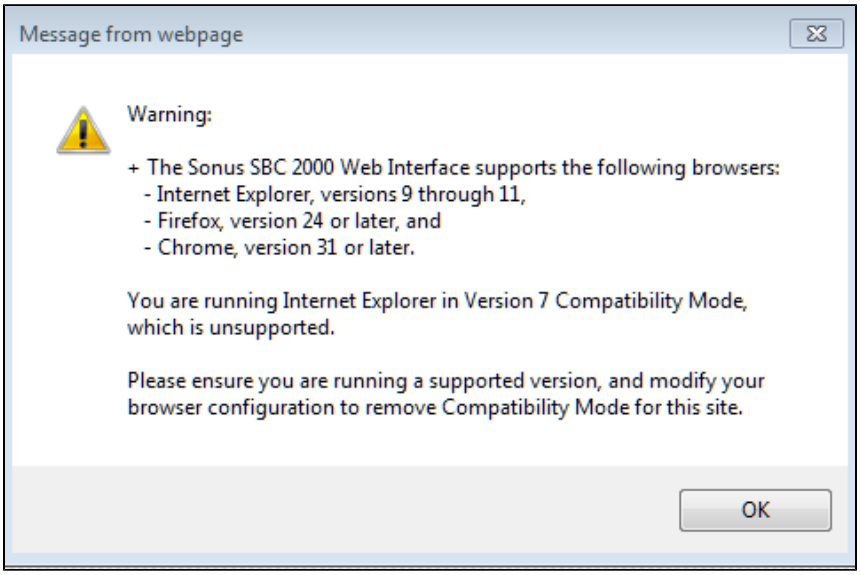
Compatibility View Indication

The Sonus SBC 1000 and 2000 supports modern releases of Internet Explorer, Firefox, and Chrome. Under Compatibility View later versions of IE will display web pages as though they were IE 7. As the SBC 1000 and 2000 do not support IE 7, Compatibility View may cause problems and should not be used. If Compatibility View is

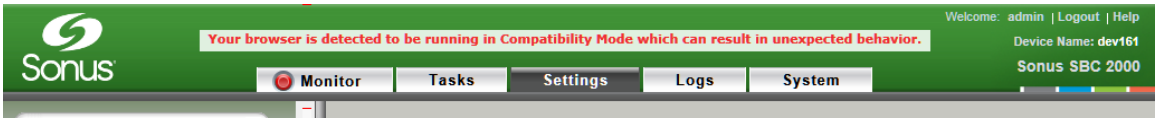
Copyright © 2015 Sonus Networks. All rights reserved.

enabled then the SBC 1000 and 2000 will present the following indications:

Login Page Dialog:



Top Banner Display:



If you see these indications, modify your browser configuration to not use compatibility mode. If necessary, consult your IT organization for assistance on how to do this.

Copyright © 2015 Sonus Networks. All rights reserved.

SBC 1000-2000 FAQ and Best Practices

Solutions to frequently asked questions and queries about Sonus SBC 1000/2000 and commonly encountered issues with the product:

Sonus SBC 1000/2000 FAQ

Administration FAQ

- How do I find a logged in user's IP address?
- What user authentication methods does the Sonus SBC 1000-2000 support?
- How are users authenticated on the Sonus SBC 1000-2000?
- Does the Sonus SBC 1000-2000 support advanced SIP matching?
- How does the Sonus SBC 1000-2000 process network traffic through its Ethernet Interfaces?
- Is there a compiled list of doc pages for viewing all Sonus SBC 1000-2000 related software versions?
- When installing cumulative updates for Lync SBA, can we skip CUs in between?

Best Practices

- Configuring the Sonus SBC 1000-2000 for DNS Load Balancing
- Deploying an F5 Load Balancer in a PBX-SBC-Lync Topology
- Deploying the Survivable Branch Appliance
  - Adding the SBA to Active Directory
  - Adding the SBA to your Lync 2010 Topology
  - Adding the SBA to your Lync 2013 Topology
  - Verifying and Configuring DNS
- Configuring the SBC 1000 for FXS Calling
- Deployment in PSTN - SBC - Microsoft OCS 2007 R2 Topology
- Microsoft Lync Server 2010 Quick Start Guide
  - Configuring the Lync 2010 Server - Dial Plan and Gateway
  - Creating a Lync 2010 User
- Downstream Deployment of a Sonus SBC 1000-2000 in a PBX-SBC-eUM Topology
- Changing SIP Transport from MTLS - SRTP to TCP - RTP
- Call Forking Based on Active Directory User Attributes
- Call Routing Based on Active Directory User Attributes
- Configuring a Nortel PBX v4.5 to connect via TDM to the SBC 1000-2000
- Configuring SBC 1000-2000 with Exchange 2013
- Configuring TDM ports on the SBC 1000-2000
- Configuring the Avaya S8300/8400/8500/8700 v.3.1.x to connect via TDM to the SBC 1000-2000
- Configuring the Mitel 3300 ICP v9.0.0.41 to connect via TDM to the SBC 1000-2000
- Configuring the QoE Feature
- How to enable, collect, and provide log files from SBC and SBA
- SBC 1000/2000 Security Hardening Checklist
- SIP Trunking Between SIP Border Elements
- SIP Trunking with Multiple IP support
- Configuring the Sonus SBC 1000-2000 for Music On Hold
- Configuring the Sonus SBC 1000-2000 for Standard and Mutual TLS Authentication
- Translating SIP Responses in SIP-SIP Calls Using "Pass-thru Peer SIP Response Code"
- Configuring Sonus SBC1000-2000 for Calling Party Category II-8 based Collect Call Blocking
- Use of Calling Extension in Transformation Table for ext=xxxx Input Value
- Changing SIP Transport Protocol from TCP to TLS in a PBX-UX-eUM Topology

Copyright © 2015 Sonus Networks. All rights reserved.

- Configuring a Sonus SBC 1000-2000 with ITSP that requires digest authentication with 401 Unauthorized challenge
- SIP Message Manipulation Document Catalog
  - 6 Steps to Creating Effective SMM Rules
  - Call Routing Based On SDP Media IP Address - SIP Message Manipulation
  - Correcting a FROM Tag using SIP Message Manipulation
  - Correcting letter case using SIP Message Manipulation
  - Modifying the m and a lines in SDP using SIP Message Manipulation
  - Properly canceling forked LYNC calls using SIP Message Manipulation
  - Remove the User Agent or Server Header using SIP Message Manipulation
  - Removing Brackets from a Parameter using SIP Message Manipulation
  - Setting the Calling Number from a SIP Header using Sip Message Manipulation
  - SIP Message Manipulation Overview
  - SIP Message Manipulation - Set the Request URI number from the TO Header
  - SIP Message Manipulation - Setting the P-Asserted Identity
  - Using HISTORY-INFO to set the FROM Number
- Action Set Documents
  - How Action Sets Work
  - SBC AD Integrated Application Solutions using Action Sets
- SBC for Dummies Series
  - Basic AD-based Call Routing for Dummies
  - SBC Basic Call Processing For Dummies - SIP to SIP
  - SBC Call Routing Reference for Dummies
  - SBC ISDN to SIP Routing For Dummies - TCP
  - SBC ISDN To SIP Routing for Dummies - TLS
  - SBC Transformation Tables for Dummies
- Configuring the RBA 3G4G Feature
- Remote Update of ASM Recovery Partition
- Lync Related Best Practices
  - Using SBC to Process Lync to Lync Calls (Replicating an upstream forked call flow in a downstream installation)
  - Configuring the Sonus SBC 1000-2000 and Lync to Support Enhanced Emergency (911) Services
  - Configuring the Sonus SBC 1000-2000 for Lync E911 with PSAP Callback Number
  - LYNC side Gateway Failover Configuration
  - Lync 2013 Call Forwarding Integration to an ITSP
- SIP Registration
  - SIP Phone Registration and SIPph to Sonus SBC 1000-2000 to ISDN call
  - SIP Registration using Authorization Tables
- Deploying the Sonus SBC 1000-2000
  - Upstream Deployment of a Sonus SBC 1000-2000 in a PSTN - SBC - eUM Toplogy
  - Using Tenor as an Analog Device in a Lync SBC SBA Deployment
  - Deploying the Sonus SBC 1000-2000 with OCS2007 R2 using the ASM as a Mediation Server
- How to Enable, Collect, and Provide Log Files From The SBC 1000-2000 SBA
- Configuring The SBC 1000-2000 with ISDN IDA-P Switch Variant
- Upgrading the ASM Image From Windows-Only to Lync SBA
- Configuring SBC 1000-2000 for Broadsoft Compatibility
  - Configuring the SBC 1000-2000 for BroadSoft SUBSCRIBE/NOTIFY
- Configuring SBC 1000-2000 for Multiple Media Streams (Video Call Passthrough)

How Incoming Calls are Handled when Server is Unreachable

Copyright © 2015 Sonus Networks. All rights reserved.

Administration FAQ

This section contains solutions for common issues or queries associated with administering Sonus SBC 1000/2000.

This section focuses on providing instructions to perform administration-level tasks on Sonus SBC 1000/2000 via the User Interface.

View one of the following issues or queries for more information:

- How do I find a logged in user's IP address?
- What user authentication methods does the Sonus SBC 1000-2000 support?
- How are users authenticated on the Sonus SBC 1000-2000?
- Does the Sonus SBC 1000-2000 support advanced SIP matching?
- How does the Sonus SBC 1000-2000 process network traffic through its Ethernet Interfaces?
- Is there a compiled list of doc pages for viewing all Sonus SBC 1000-2000 related software versions?
- When installing cumulative updates for Lync SBA, can we skip CUs in between?

How do I find a logged in user's IP address?

Is there a way to track the IP address of users logging into our Sonus SBC 1000/2000 system?

The IP address of all active sessions on Sonus SBC 1000/2000 are located under the Active User Sessions Table. If you are an administrator, you can terminate their session or delete the user's account, please read Managing Local Users.

What user authentication methods does the Sonus SBC 1000-2000 support?

Other than local authentication, what other user authentication methods does the Sonus SBC 1000/2000 support?

The Sonus SBC 1000/2000 system has three means of authentication:

1. Local Authentication
2. Authentication through Active Directory — does not require a Sonus SBC 1000/2000 license to work
3. Authentication through RADIUS — does not require a Sonus SBC 1000/2000 license to work

Related Articles

- How are users authenticated on the Sonus SBC 1000-2000?
- Managing Remote Authentication

How are users authenticated on the Sonus SBC 1000-2000?

Since Sonus SBC 1000/2000 supports multiple forms of authentication, what method does it use to authenticate them?

See How User Authentication Works.

Does the Sonus SBC 1000-2000 support advanced SIP matching?

I'm trying to match and route on SIP user extension `61292856286;ext=5311` - does Sonus SBC 1000/2000 support type of advanced SIP matching?

Yes - starting with Sonus SBC 1000/2000 version 2.0, SIP URI matching for Extension and Phone Context is now supported in Transformation Tables. For more details, see SIP URI Manipulation.

Copyright © 2015 Sonus Networks. All rights reserved.

How does the Sonus SBC 1000-2000 process network traffic through its Ethernet Interfaces?

I would like to know how the Sonus SBC 1000/2000 system processes (knows) which NIC/Ethernet-interface to use when routing traffic?

See How the Sonus SBC 1000-2000 Routes IP Traffic to a NIC.

Is there a compiled list of doc pages for viewing all Sonus SBC 1000-2000 related software versions?

I have a fully-loaded Sonus SBC 1000/2000 system with a built-in ASM. Can you provide me with a consolidated list of pages in this documentation that helps me track down all software versions installed on Sonus SBC 1000/2000?

Here the compiled list of documentation pages related to software/package version on the Sonus SBC 1000/2000:

Software Component	Documentation Page Link
Sonus SBC 1000/2000 Software version	Viewing the Software Version and Hardware ID
Sonus SBC 1000/2000 Boot Image version	Viewing the Boot Image Version
Sonus SBC 1000/2000 Communication Service version	Viewing the Sonus SBC Communication Service Version
Sonus SBC 1000/2000 Lync SBA version	Viewing the SBA Operational Status
Sonus SBC 1000/2000 Lync SBA installed packages	Viewing the Installed Packages on the ASM
Sonus SBC 1000/2000 Lync SBA Cumulative Updates	Installing Cumulative Updates for Lync SBA

Related Articles:

- Working with System Settings
- Managing the SBC Communication Service
- Managing the Lync SBA
- Checking your System Information

When installing cumulative updates for Lync SBA, can we skip CUs in between?

Our Lync Front End (FE) server is already running Lync CU4, and our Sonus SBC 1000/2000 Lync SBA is still running CU2. Can the Lync SBA be upgraded from Lync CU2 directly to CU4 or does it need to be upgraded to CU3 first then CU4?

Just like matryoshka dolls, the latest latest Cumulative Updates (CU) for Lync Server contains all previous CUs. It is safe to apply the CU directly without having to increment through each one.

Related Articles

- Installing Cumulative Updates for Lync SBA
- Deploying the Survivable Branch Appliance

Best Practices

Copyright © 2015 Sonus Networks. All rights reserved.

This section contains a collection of articles which explore supported ways of configuring and deploying Sonus SBC 1000/2000 using a range of existing and new features.

The intent is to encourage field engineers, customers, and partners to adopt these best practices to help them improve existing techniques used for configuring and deploying Sonus SBC 1000/2000 in their VoIP and networking topology.

In addition to configuration procedures, some of these articles contain in-depth verification steps to help you solve common deployment scenarios using methods that are supported and have been tested by Sonus. These articles are applicable to the latest version of Sonus SBC 1000/2000 and assumes the reader has a solid understanding of Unified Communications concepts in addition to training on Microsoft Unified Communication Applications:

- Configuring the Sonus SBC 1000-2000 for DNS Load Balancing
- Deploying an F5 Load Balancer in a PBX-SBC-Lync Topology
- Deploying the Survivable Branch Appliance
    - Adding the SBA to Active Directory
    - Adding the SBA to your Lync 2010 Topology
    - Adding the SBA to your Lync 2013 Topology
    - Verifying and Configuring DNS
- Configuring the SBC 1000 for FXS Calling
- Deployment in PSTN - SBC - Microsoft OCS 2007 R2 Topology
- Microsoft Lync Server 2010 Quick Start Guide
    - Configuring the Lync 2010 Server - Dial Plan and Gateway
    - Creating a Lync 2010 User
- Downstream Deployment of a Sonus SBC 1000-2000 in a PBX-SBC-eUM Topology
- Changing SIP Transport from MTLS - SRTP to TCP - RTP
- Call Forking Based on Active Directory User Attributes
- Call Routing Based on Active Directory User Attributes
- Configuring a Nortel PBX v4.5 to connect via TDM to the SBC 1000-2000
- Configuring SBC 1000-2000 with Exchange 2013
- Configuring TDM ports on the SBC 1000-2000
- Configuring the Avaya S8300/8400/8500/8700 v.3.1.x to connect via TDM to the SBC 1000-2000
- Configuring the Mitel 3300 ICP v9.0.0.41 to connect via TDM to the SBC 1000-2000
- Configuring the QoE Feature
- How to enable, collect, and provide log files from SBC and SBA
- SBC 1000/2000 Security Hardening Checklist
- SIP Trunking Between SIP Border Elements
- SIP Trunking with Multiple IP support
- Configuring the Sonus SBC 1000-2000 for Music On Hold
- Configuring the Sonus SBC 1000-2000 for Standard and Mutual TLS Authentication
- Translating SIP Responses in SIP-SIP Calls Using "Pass-thru Peer SIP Response Code"
- Configuring Sonus SBC1000-2000 for Calling Party Category II-8 based Collect Call Blocking
- Use of Calling Extension in Transformation Table for ext=xxxx Input Value
- Changing SIP Transport Protocol from TCP to TLS in a PBX-UX-eUM Topology
- Configuring a Sonus SBC 1000-2000 with ITSP that requires digest authentication with 401 Unauthorized challenge
- SIP Message Manipulation Document Catalog
    - 6 Steps to Creating Effective SMM Rules
    - Call Routing Based On SDP Media IP Address - SIP Message Manipulation
    - Correcting a FROM Tag using SIP Message Manipulation
    - Correcting letter case using SIP Message Manipulation
    - Modifying the m and a lines in SDP using SIP Message Manipulation
    - Properly canceling forked LYNC calls using SIP Message Manipulation
    - Remove the User Agent or Server Header using SIP Message Manipulation

Copyright © 2015 Sonus Networks. All rights reserved.

    - Removing Brackets from a Parameter using SIP Message Manipulation
    - Setting the Calling Number from a SIP Header using Sip Message Manipulation
    - SIP Message Manipulation Overview
    - SIP Message Manipulation - Set the Request URI number from the TO Header
    - SIP Message Manipulation - Setting the P-Asserted Identity
    - Using HISTORY-INFO to set the FROM Number
- Action Set Documents
    - How Action Sets Work
    - SBC AD Integrated Application Solutions using Action Sets
        - Blacklisted Numbers
        - Calls to Exchange Subscriber Access (EUM SA)
        - Calls to Lync Users
        - Calls to Lync users with ext=
        - Calls to PBX
        - Get Calling Name
        - Normalizing Numbers
        - Two-number FAX
        - Voicemail for Lync Analog Devices
- SBC for Dummies Series
    - Basic AD-based Call Routing for Dummies
    - SBC Basic Call Processing For Dummies - SIP to SIP
    - SBC Call Routing Reference for Dummies
    - SBC ISDN to SIP Routing For Dummies - TCP
    - SBC ISDN To SIP Routing for Dummies - TLS
    - SBC Transformation Tables for Dummies
- Configuring the RBA 3G4G Feature
- Remote Update of ASM Recovery Partition
- Lync Related Best Practices
    - Using SBC to Process Lync to Lync Calls (Replicating an upstream forked call flow in a downstream installation)
    - Configuring the Sonus SBC 1000-2000 and Lync to Support Enhanced Emergency (911) Services
    - Configuring the Sonus SBC 1000-2000 for Lync E911 with PSAP Callback Number
    - LYNC side Gateway Failover Configuration
    - Lync 2013 Call Forwarding Integration to an ITSP
- SIP Registration
    - SIP Phone Registration and SIPph to Sonus SBC 1000-2000 to ISDN call
    - SIP Registration using Authorization Tables
- Deploying the Sonus SBC 1000-2000
    - Upstream Deployment of a Sonus SBC 1000-2000 in a PSTN - SBC - eUM Toplogy
    - Using Tenor as an Analog Device in a Lync SBC SBA Deployment
        - Configuring Valcom For Use With Tenor
    - Deploying the Sonus SBC 1000-2000 with OCS2007 R2 using the ASM as a Mediation Server
- How to Enable, Collect, and Provide Log Files From The SBC 1000-2000 SBA
- Configuring The SBC 1000-2000 with ISDN IDA-P Switch Variant
- Upgrading the ASM Image From Windows-Only to Lync SBA
- Configuring SBC 1000-2000 for Broadsoft Compatibility
    - Configuring the SBC 1000-2000 for BroadSoft SUBSCRIBE/NOTIFY
- Configuring SBC 1000-2000 for Multiple Media Streams (Video Call Passthrough)

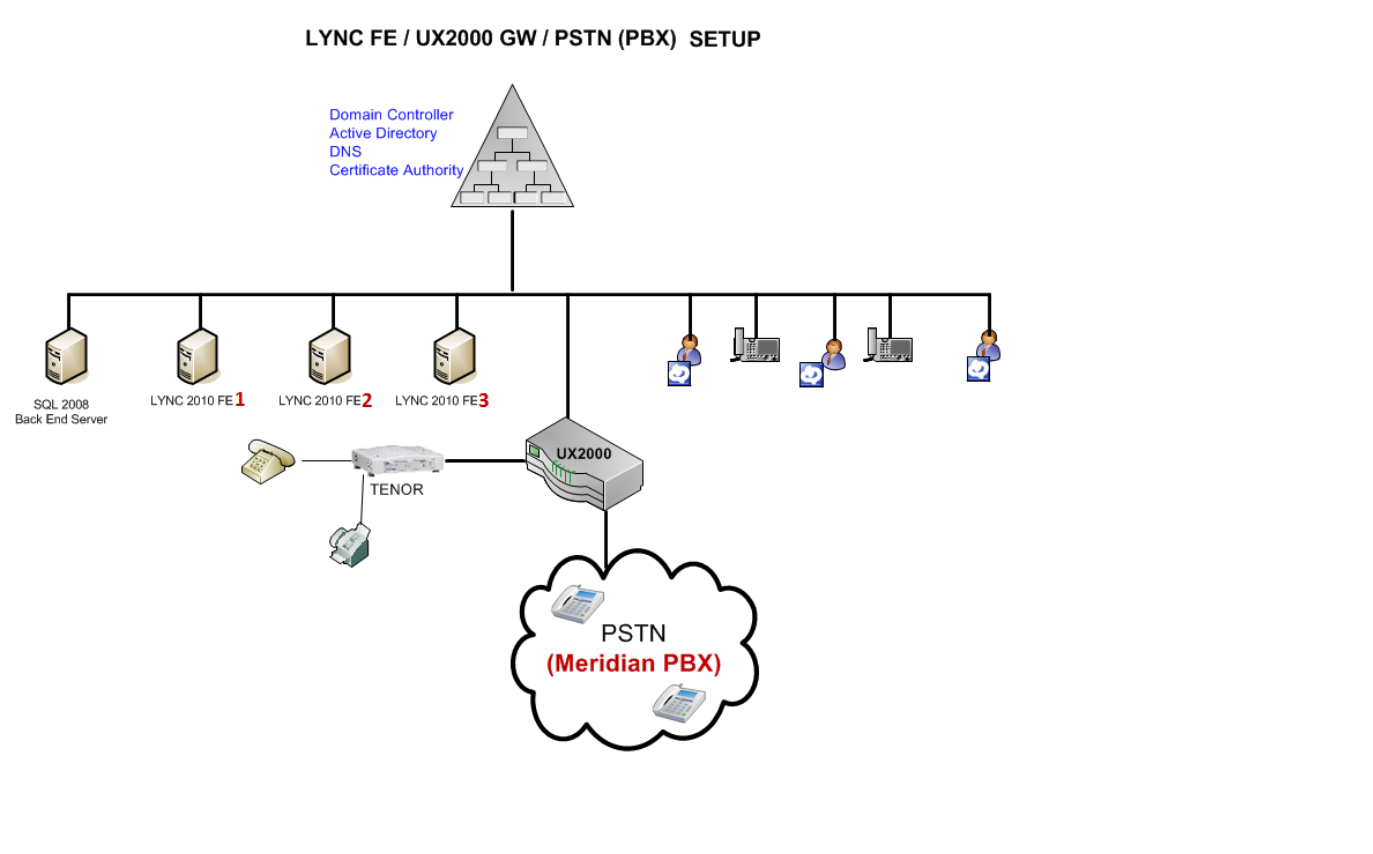
Configuring the Sonus SBC 1000-2000 for DNS Load Balancing

In this article we describe how to configure the Sonus SBC 1000/2000 to use a server pool to accomplish DNS load

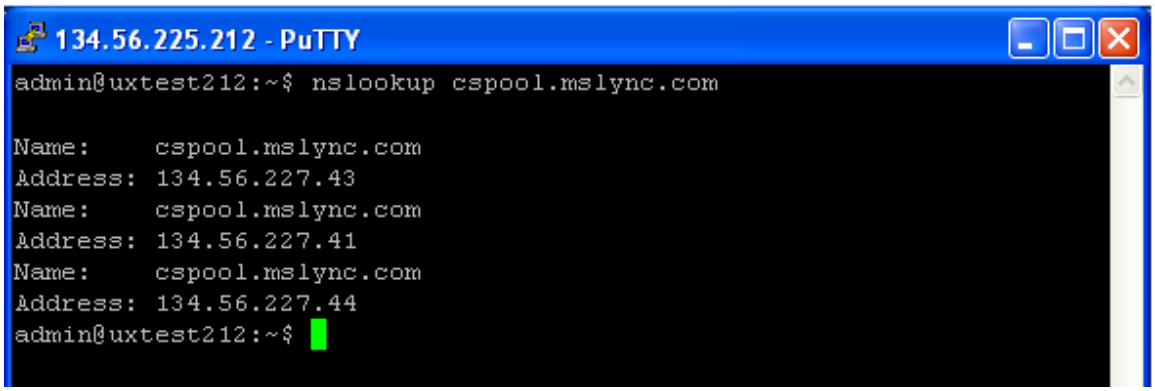
Copyright © 2015 Sonus Networks. All rights reserved.

balancing using a pool of Lync Mediation Servers.

For the purpose of this article, we assume that the the **PBX - Sonus SBC 1000/2000 - Microsoft Lync 2010** topology is in place and employs multiple front end servers, as shown below. For more information about this topology, see Deploying the SBC 1000-2000 and Lync with a PSTN Provider.



Perform a Name Server (NS) Lookup on of the Lync 2010 Pool (cspool.mylync.com) with three front end servers.



The FQDN *cspool.mylync.com* resolves to three separate IP Addresses:

- Front End Server 1: 134.56.227.43
- Front End Server 2: 134.56.227.41
- Front End Server 3: 134.56.227.44

On this page:

Copyright © 2015 Sonus Networks. All rights reserved.

- Configuration
  - SIP Server Table
  - Signaling Group
- Example of Round Robin Load Balancing

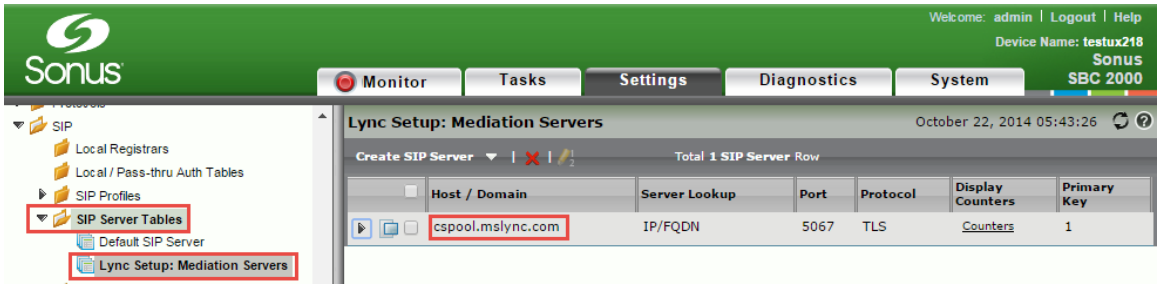
Configuration

Configuration for this functionality is straight-forward and relatively simple. It involves two basic steps"

- Creating SIP Server Table and/or entry.
- Assigning that SIP Server Table and specifying the Load Balancing Method in a Signaling Group.

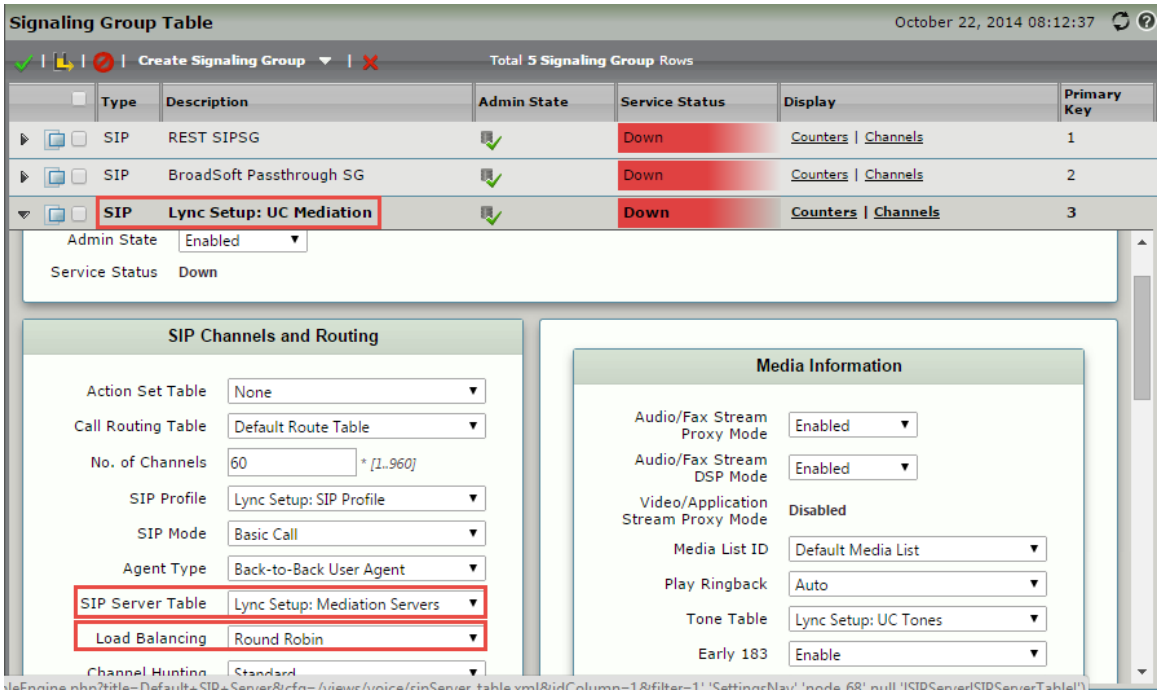
SIP Server Table

Create a new SIP Server Table and entry as shown below.
⚠ Use the **FQDN of the Lync pool** as shown.



Signaling Group

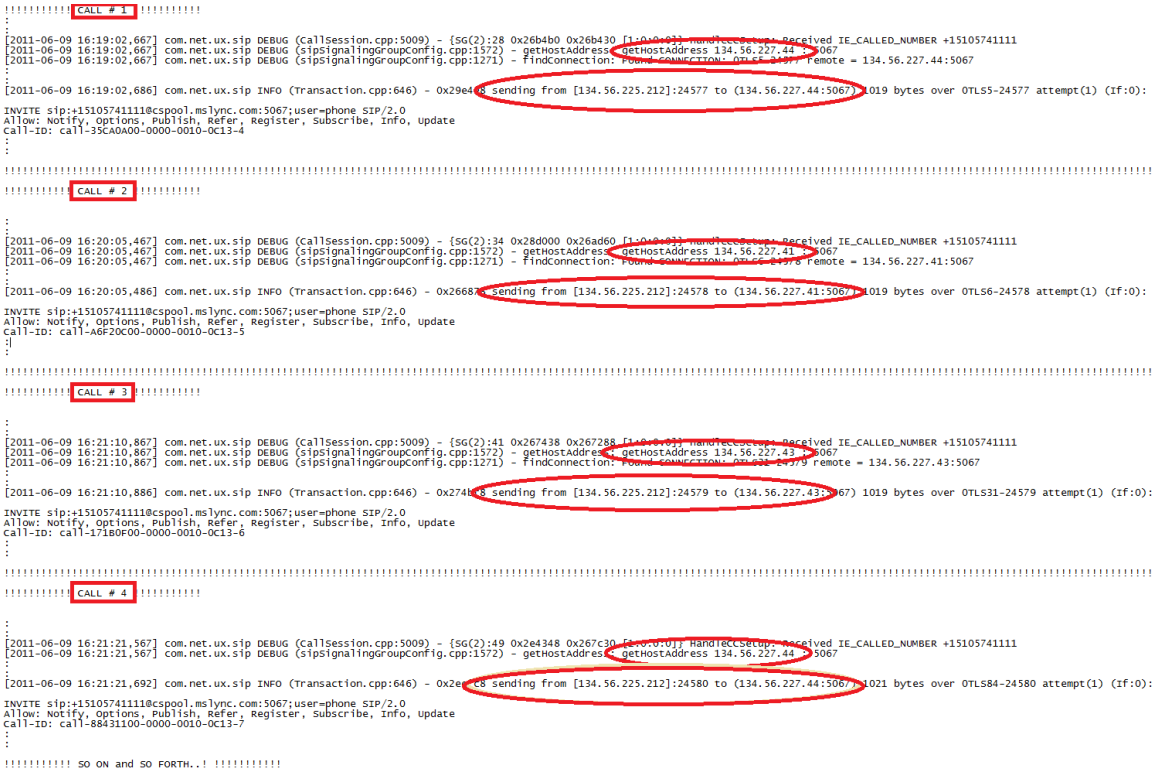
Create a new, or modify an existing, SIP Signaling Group and configure the SIP Server Table and Load Balancing options as shown below.



Copyright © 2015 Sonus Networks. All rights reserved.

Example of Round Robin Load Balancing

In the Sonus SBC 1000/2000 to Lync direction call scenarios in this setup, Sonus SBC 1000/2000 load balances outbound calls among the multiple IP addresses to which the FQDN resolves. The following screenshot depicts the multiple calls received by the Sonus SBC 1000/2000 and how they are sent to different Front End Servers in a round robin fashion.



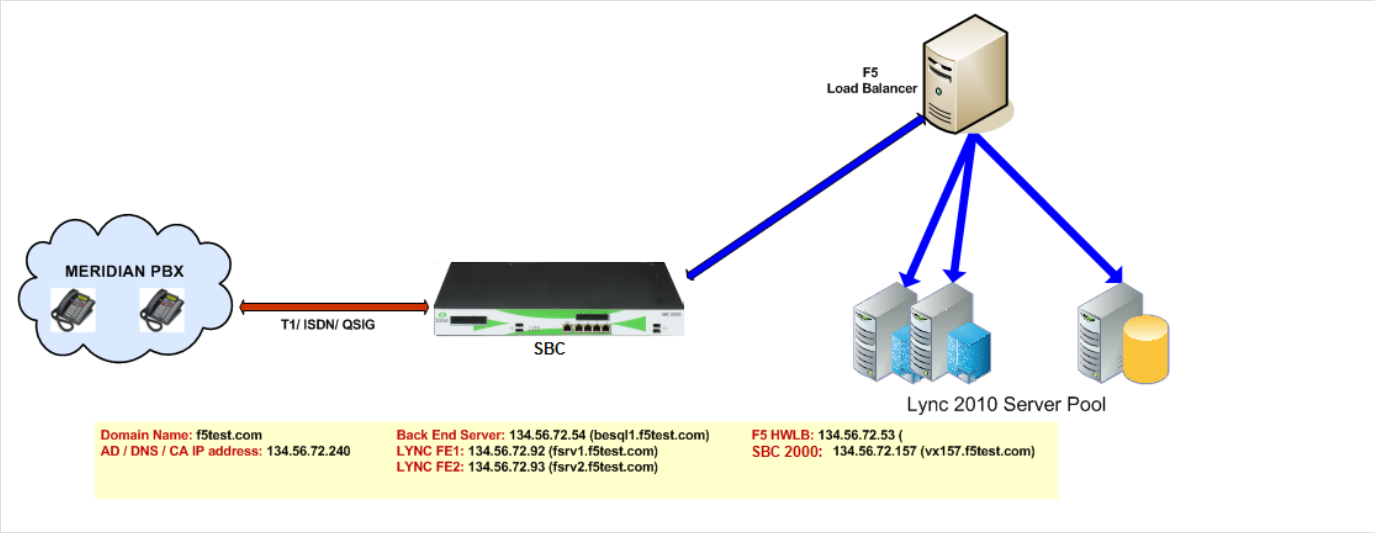
> the load balancing also works if the multiple IP addresses are configured in same SIP Server Table instead of a FQDN. In other words, if IP addresses of 134.56.227.43, 134.56.227.41, and 134.56.227.44 are listed in the server table instead of cspool.mylync.com, the load balancing still occurs in the outbound SIP Signaling Groups that use this server table.

Deploying an F5 Load Balancer in a PBX-SBC-Lync Topology

This article describes the steps necessary to configure the Sonus SBC 1000/2000 with an F5 Networks load balancer in a **PBX-Sonus SBC 1000/2000-Microsoft Lync** topology as illustrated below:

Topology

Copyright © 2015 Sonus Networks. All rights reserved.



The elements used in this topology are as follows:

- 2x Microsoft Lync 2010 front end servers
- 1x F5 Networks hardware load balancer
- 1x Meridian PBX
- 1x Sonus SBC 1000/2000 Gateway

For the purpose of this article we assume that the F5 load balancer is already installed, configured, and successfully integrated with Lync 2010.

For more details regarding the F5 load balancer configuration and Lync integration, please review the F5 Hardware Loadbalancer (HWLB) Configuration section. You may also jump directly to the Sonus SBC 2000 Configuration and Call Flows sections.

F5 Hardware Loadbalancer (HWLB) Configuration

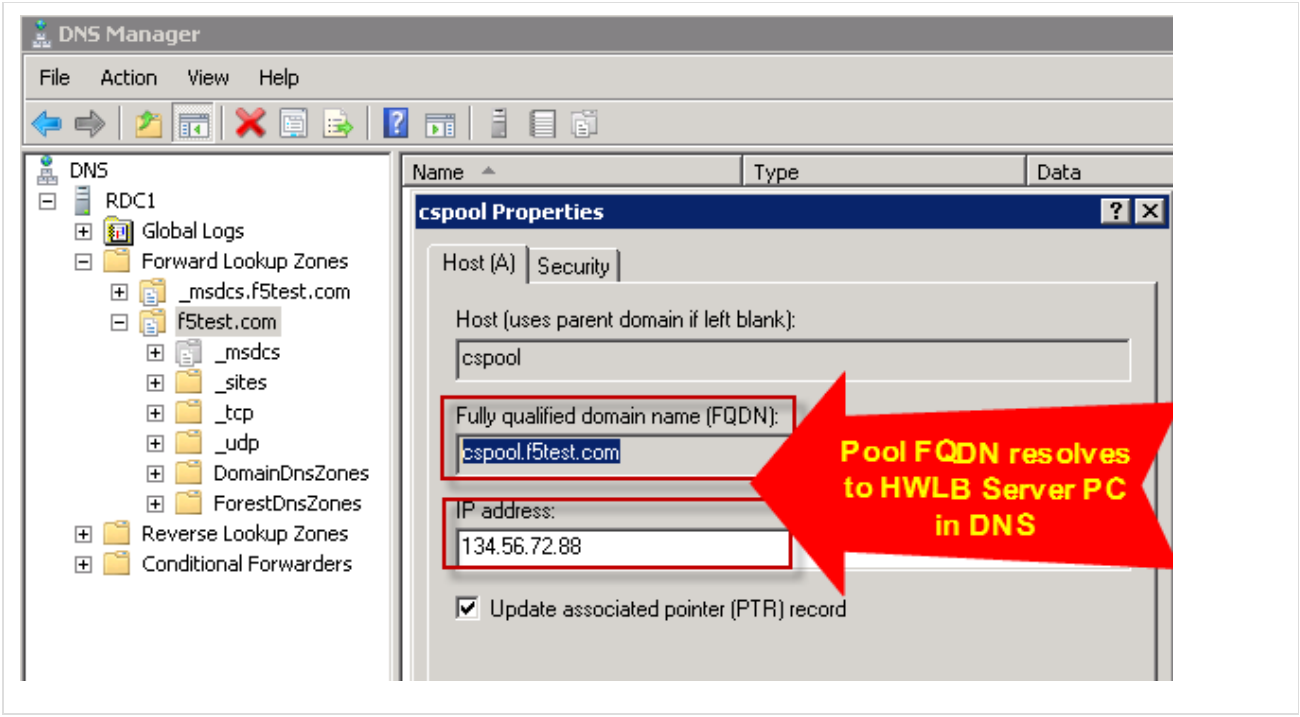
For the purpose of this article we assume that the F5 load balancer is installed and configured such that it is already successfully integrated with Lync 2010. For details regarding the configuration and integration of an F5 load balancer see the following F5 documents:

- BIG-IP Virtual Edition Setup Guide for VMware ESX or ESXi
- Deploying the BIG-IP LTM with Microsoft Lync Server 2010

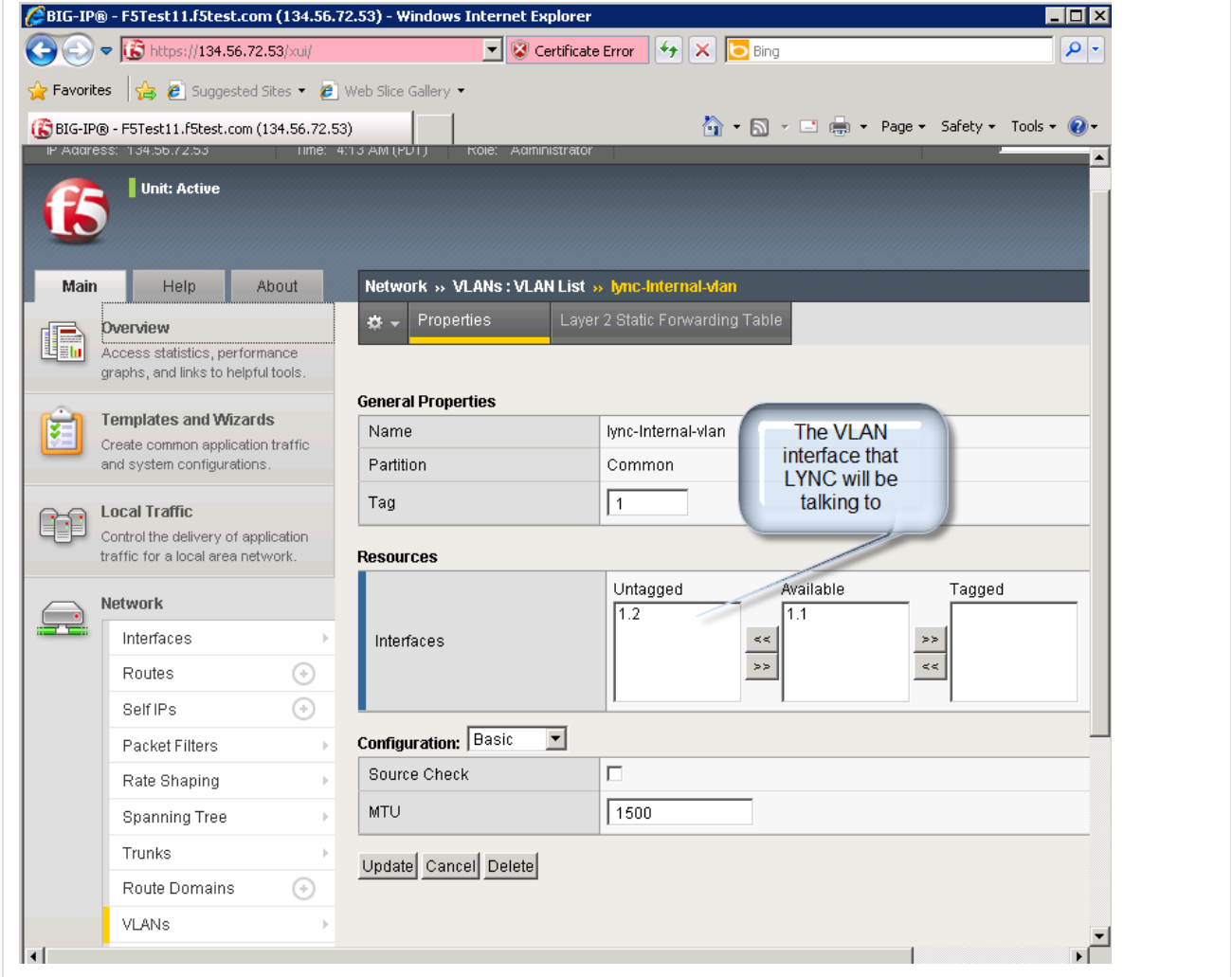
Load Balancer Configuration Hints

1. Using the **DNS Manager**, verify that the Lync 2010 Enterprise Pool Alias is pointing (therefore resolving) to the IP address of the hardware Load balancer machine as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.

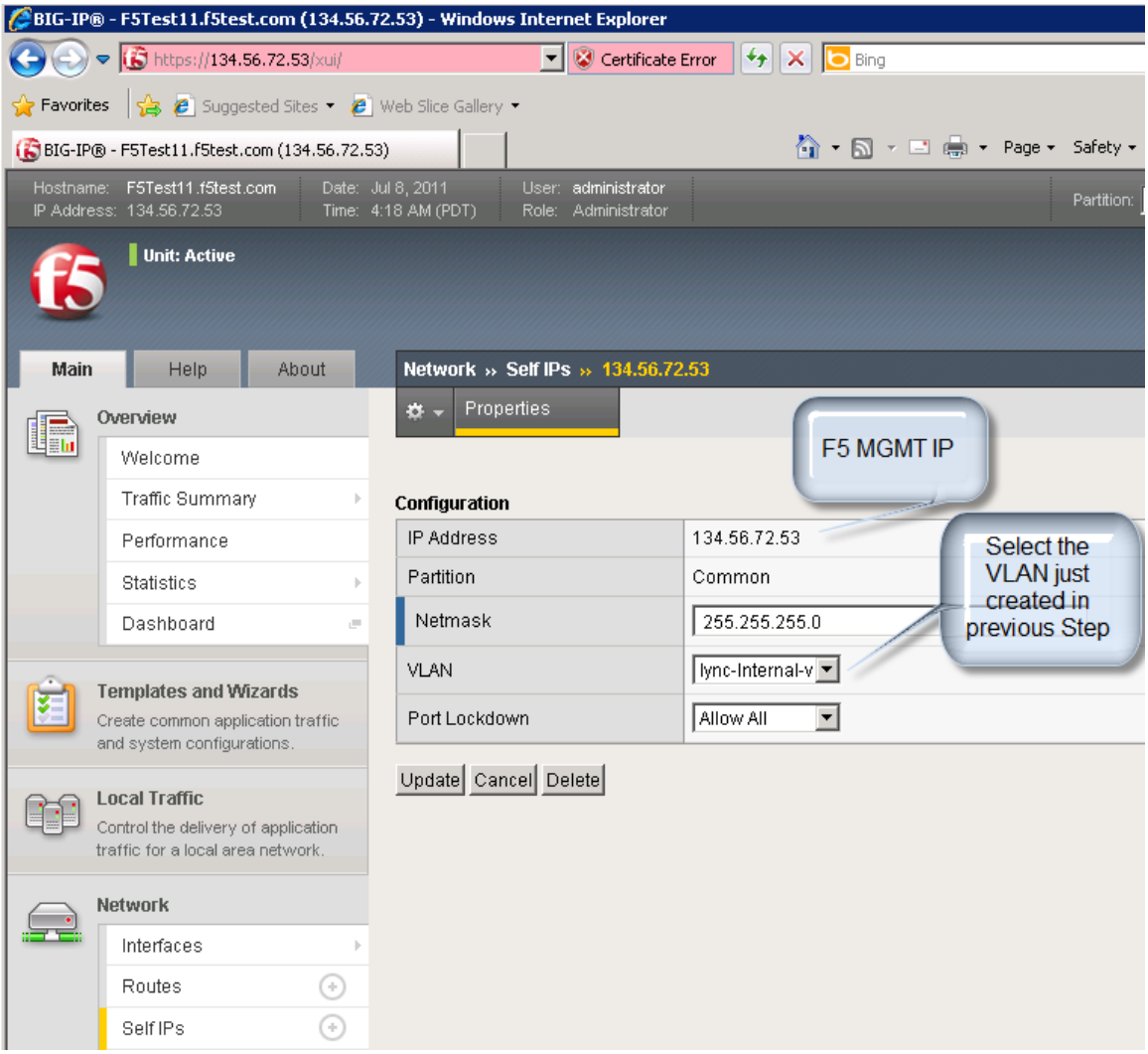


2. Verify that the VLAN interface used to communicate with the Lync server is tagged as indicted below.



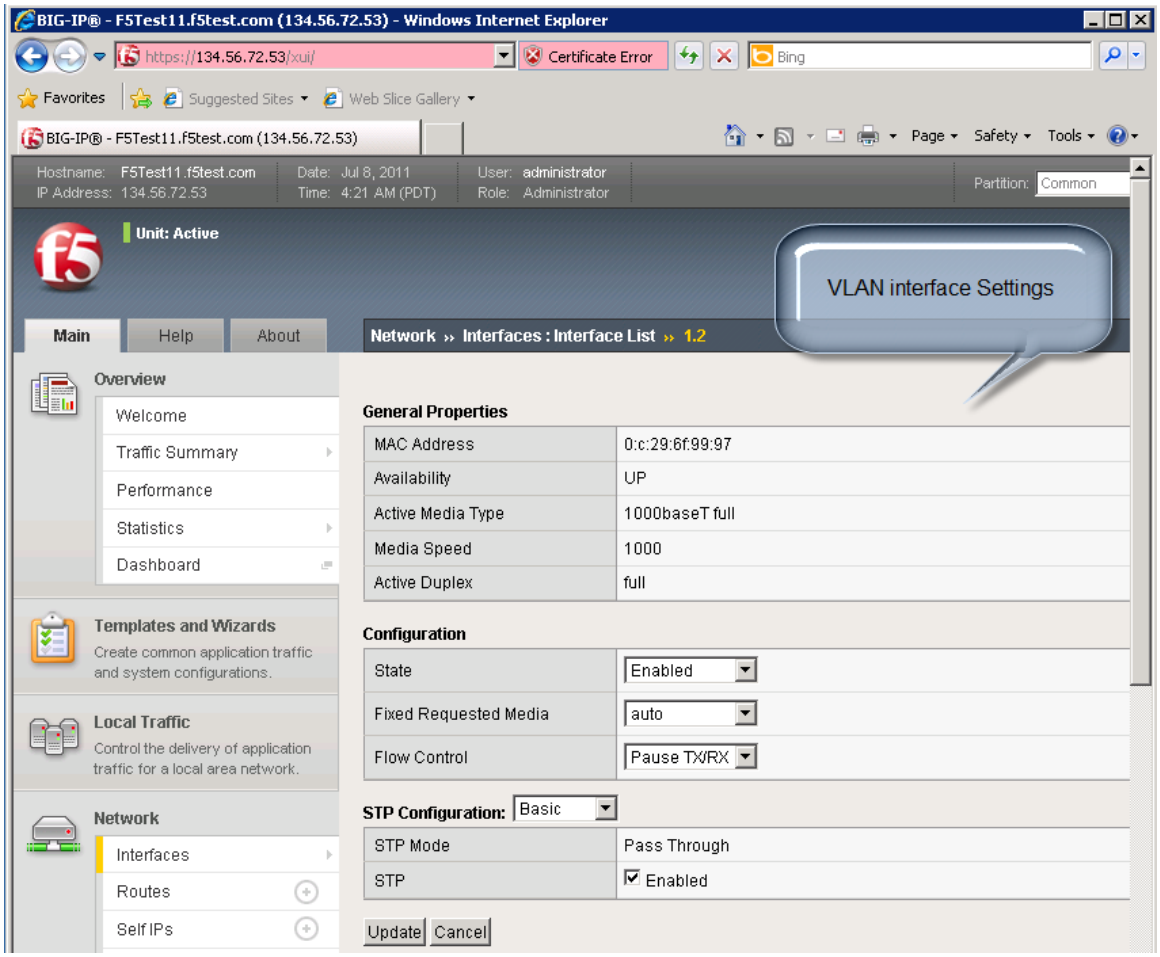
Copyright © 2015 Sonus Networks. All rights reserved.

3. Verify that the F5 MGMT IP address is configured to use the VLAN interface set in the previous step.



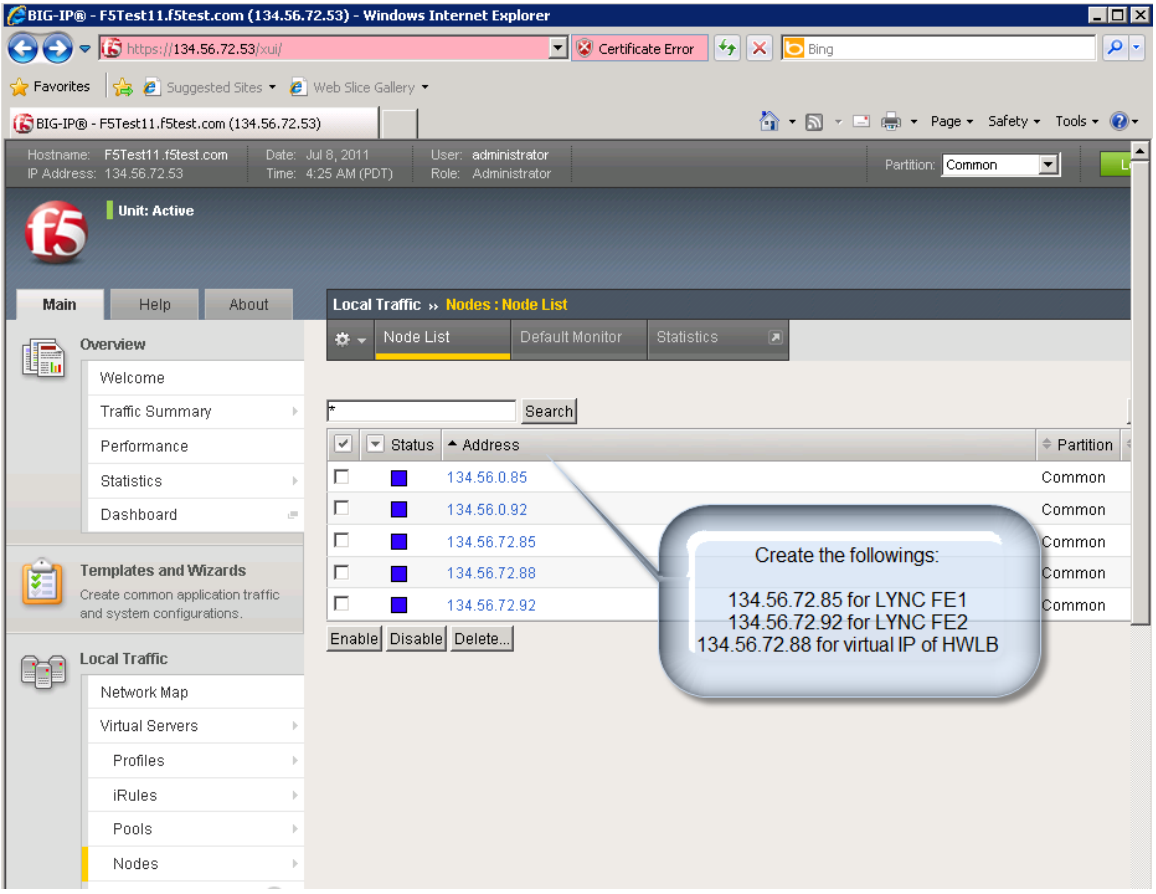
4. Verify that the VLAN interface Settings are configured as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



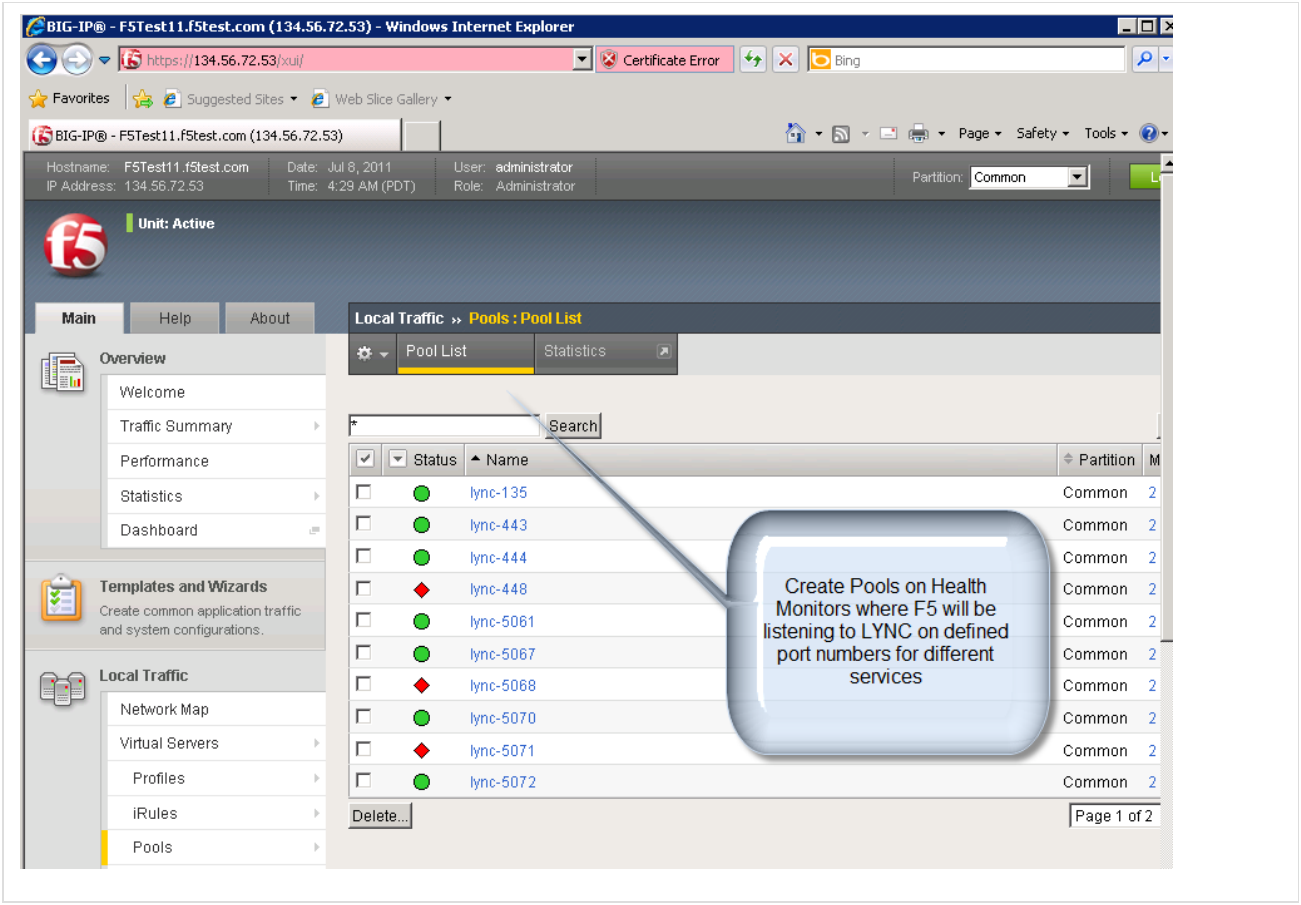
5. Verify that **Local Traffic > Nodes** settings contain the Lync FE1, Lync FE2, and the virtual IP address of hardware load balancer machine as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



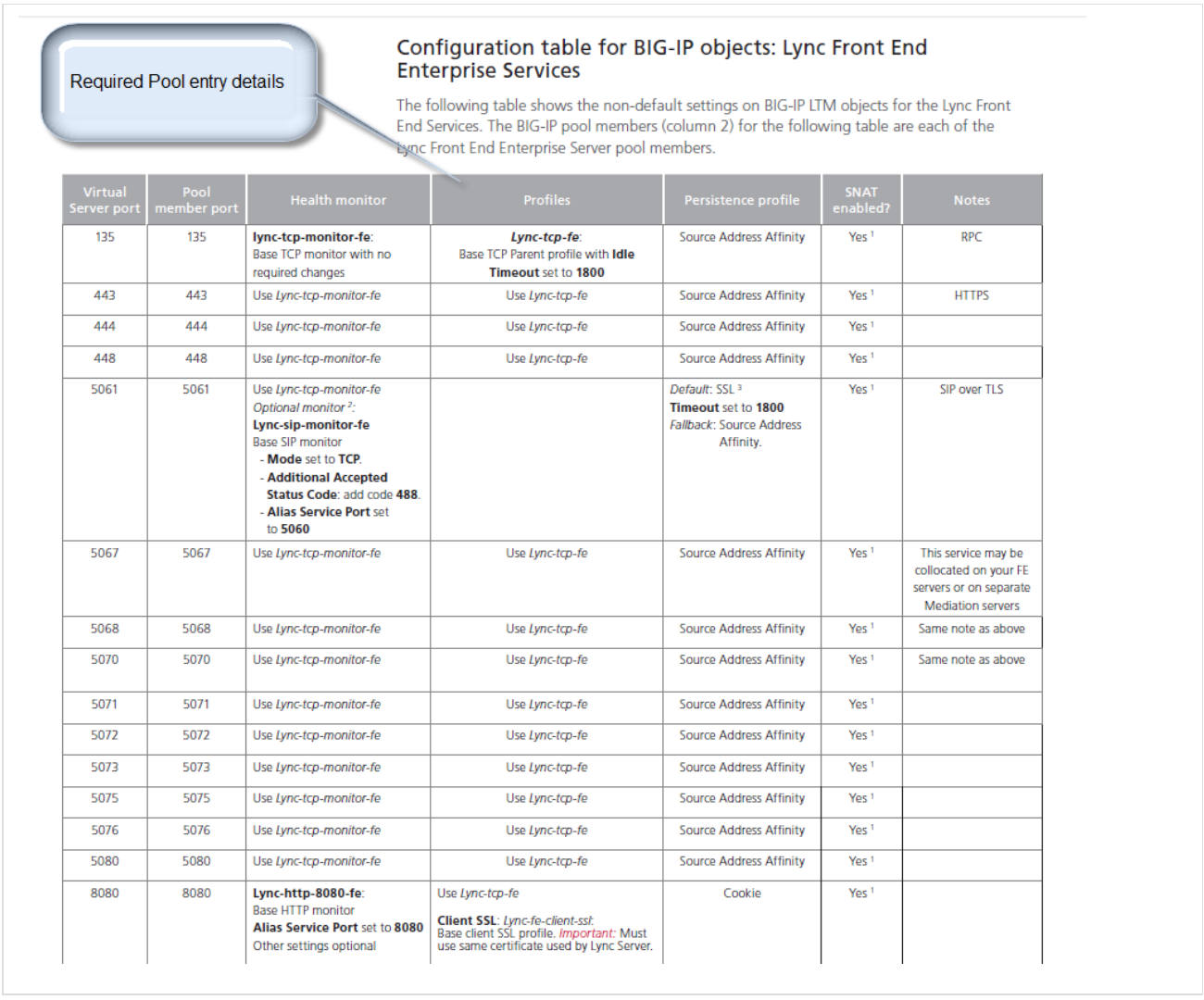
6. Verify that the settings found in **Local Traffic > Pools** contain the pools that the F5 load balancer listens to Lync on defined port numbers for various services as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



NOTE: the details of pool creation is explained in [Deploying the BIG-IP LTM with Microsoft Lync Server 2010] as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



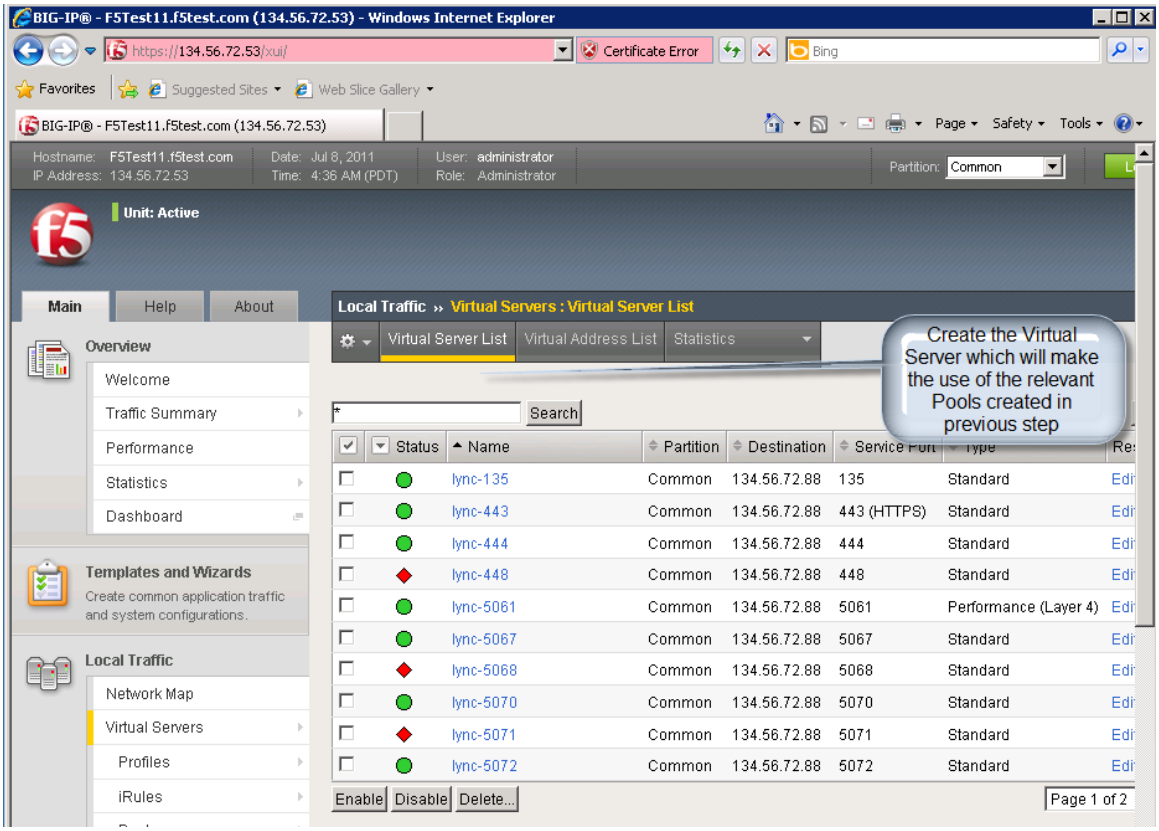
Configuration table for BIG-IP objects: Lync Front End Enterprise Services

The following table shows the non-default settings on BIG-IP LTM objects for the Lync Front End Services. The BIG-IP pool members (column 2) for the following table are each of the Lync Front End Enterprise Server pool members.

Virtual Server port	Pool member port	Health monitor	Profiles	Persistence profile	SNAT enabled?	Notes
135	135	**lync-tcp-monitor-fe**: Base TCP monitor with no required changes	***Lync-tcp-fe***: Base TCP Parent profile with **Idle Timeout** set to **1800**	Source Address Affinity	Yes [1]	RPC
443	443	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	HTTPS
444	444	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	
448	448	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	
5061	5061	Use *Lync-tcp-monitor-fe* *Optional monitor* [2]: **Lync-sip-monitor-fe** Base SIP monitor - **Mode** set to **TCP**. - **Additional Accepted Status Code**: add code **488**. - **Alias Service Port** set to **5060**		*Default*: SSL [3] **Timeout** set to **1800** *Fallback*: Source Address Affinity.	Yes [1]	SIP over TLS
5067	5067	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	This service may be collocated on your FE servers or on separate Mediation servers
5068	5068	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	Same note as above
5070	5070	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	Same note as above
5071	5071	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	
5072	5072	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	
5073	5073	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	
5075	5075	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	
5076	5076	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	
5080	5080	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Source Address Affinity	Yes [1]	
8080	8080	**Lync-http-8080-fe**: Base HTTP monitor **Alias Service Port** set to **8080** Other settings optional	Use *Lync-tcp-fe* **Client SSL**: *Lync-fe-client-ssl*: Base client SSL profile. *Important:* Must use same certificate used by Lync Server.	Cookie	Yes [1]	

7. Verify the virtual server making use of the pools created above has itself been created as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.

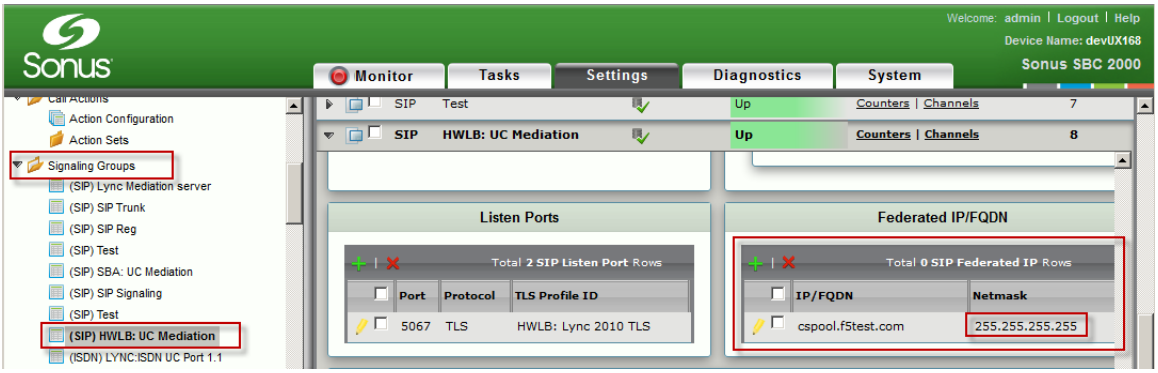


Sonus SBC 2000 Configuration

The Sonus SBC 1000/2000 configuration for deployment in this topology requires the use of the LYNC 2010 wizard in order to correctly configure all the required fields in the Sonus SBC 1000/2000.

Follow the steps described in [Deploying the SBC 1000-2000 and Lync with a PSTN Provider] .

Lync 2010 Wizard configures the **Federated IP/FQDN** with the Pool FQDN in the **IP/FQDN** field and 255.255.255.255 in **Netmask** fields allowing the Sonus SBC 1000/2000 to receive SIP messages from the hardware load balancer HWLB. However, in order to receive/send SIP messages to/from Front End Servers, the **Netmask** field must be configured with a value of **255.255.255.0** as shown below.



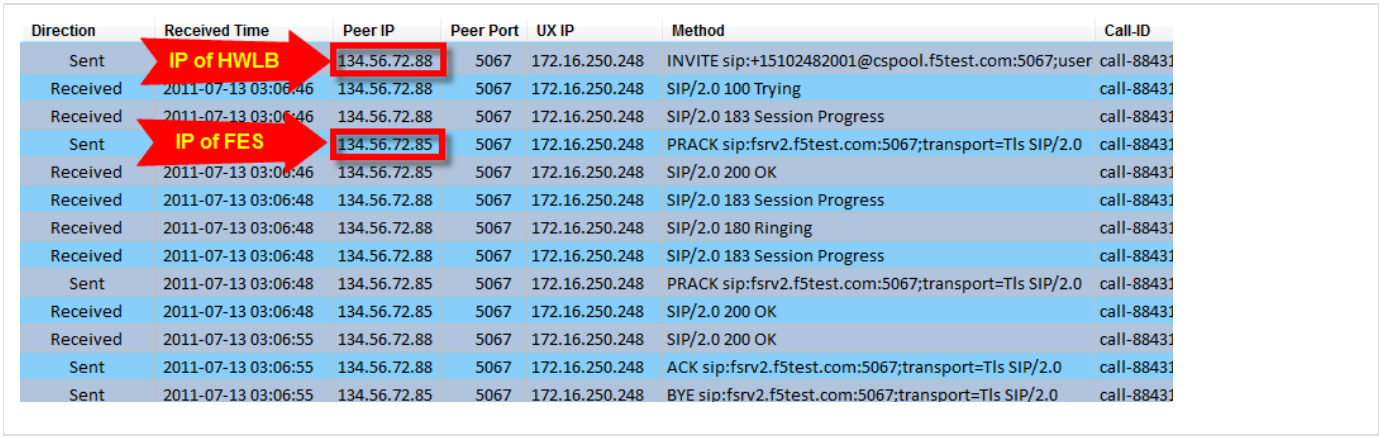
Call Flows

Copyright © 2015 Sonus Networks. All rights reserved.

Using the **Log Exchange** utility, you can verify the F5 Hardware Load Balancer (HWLB) in action —

PSTN ph > Sonus SBC 1000/2000 > Lync client

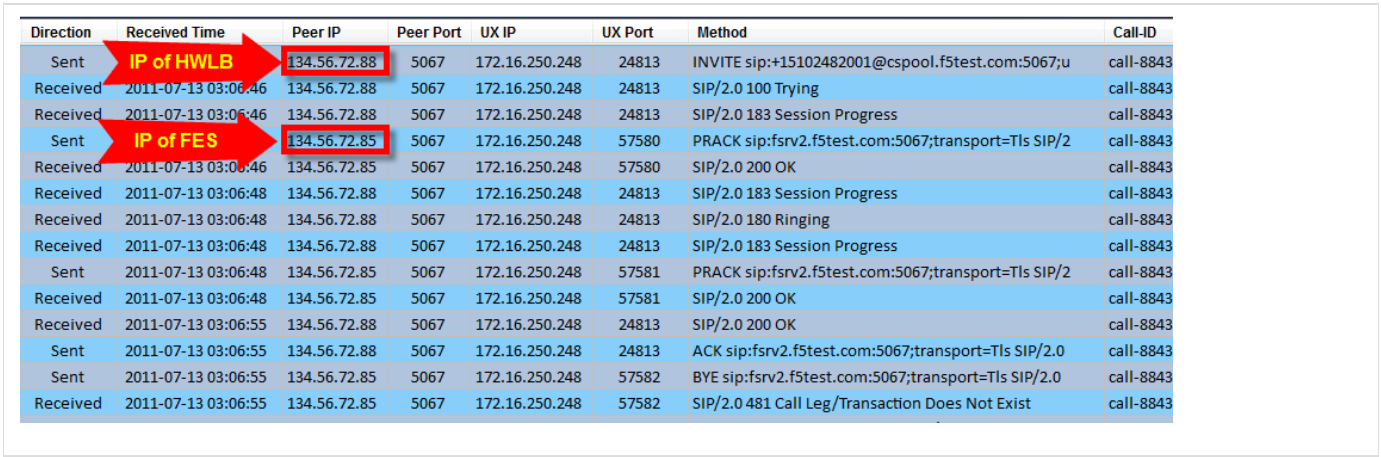
The deployment in this article allows the following call flow in PSTN ph > Sonus SBC 1000/2000 > Lync client call direction.



Direction	Received Time	Peer IP	Peer Port	UX IP	Method	Call-ID
Sent	2011-07-13 03:06:46	134.56.72.88	5067	172.16.250.248	INVITE sip:+15102482001@cspool.f5test.com:5067;user	call-8843
Received	2011-07-13 03:06:46	134.56.72.88	5067	172.16.250.248	SIP/2.0 100 Trying	call-8843
Received	2011-07-13 03:06:46	134.56.72.88	5067	172.16.250.248	SIP/2.0 183 Session Progress	call-8843
Sent	2011-07-13 03:06:46	134.56.72.85	5067	172.16.250.248	PRACK sip:fsrv2.f5test.com:5067;transport=Tls SIP/2.0	call-8843
Received	2011-07-13 03:06:46	134.56.72.85	5067	172.16.250.248	SIP/2.0 200 OK	call-8843
Received	2011-07-13 03:06:48	134.56.72.88	5067	172.16.250.248	SIP/2.0 183 Session Progress	call-8843
Received	2011-07-13 03:06:48	134.56.72.88	5067	172.16.250.248	SIP/2.0 180 Ringing	call-8843
Received	2011-07-13 03:06:48	134.56.72.88	5067	172.16.250.248	SIP/2.0 183 Session Progress	call-8843
Sent	2011-07-13 03:06:48	134.56.72.85	5067	172.16.250.248	PRACK sip:fsrv2.f5test.com:5067;transport=Tls SIP/2.0	call-8843
Received	2011-07-13 03:06:48	134.56.72.85	5067	172.16.250.248	SIP/2.0 200 OK	call-8843
Received	2011-07-13 03:06:55	134.56.72.88	5067	172.16.250.248	SIP/2.0 200 OK	call-8843
Sent	2011-07-13 03:06:55	134.56.72.88	5067	172.16.250.248	ACK sip:fsrv2.f5test.com:5067;transport=Tls SIP/2.0	call-8843
Sent	2011-07-13 03:06:55	134.56.72.85	5067	172.16.250.248	BYE sip:fsrv2.f5test.com:5067;transport=Tls SIP/2.0	call-8843

LYNC client > Sonus SBC 1000/2000 > PSTN ph

The deployment in this article allows the following call flow in **Lync client > Sonus SBC 1000/2000 > PSTN ph** call direction.

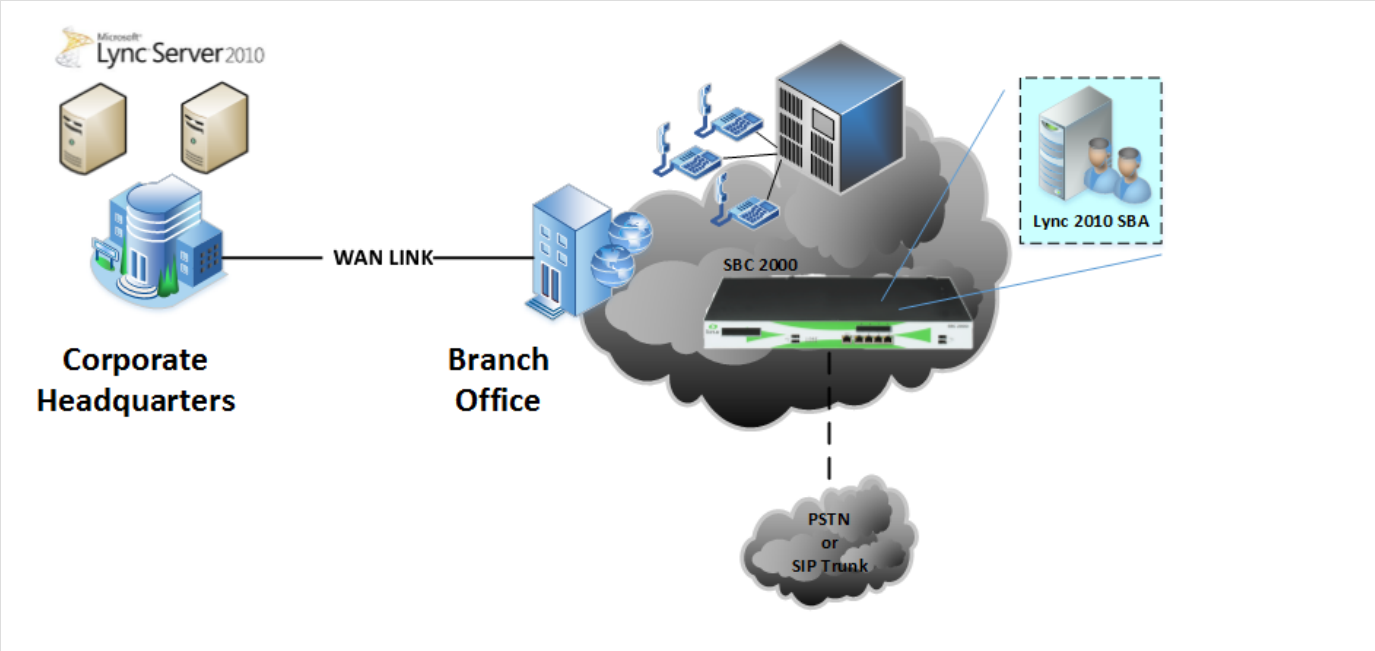


Direction	Received Time	Peer IP	Peer Port	UX IP	UX Port	Method	Call-ID
Sent	2011-07-13 03:06:46	134.56.72.88	5067	172.16.250.248	24813	INVITE sip:+15102482001@cspool.f5test.com:5067;u	call-8843
Received	2011-07-13 03:06:46	134.56.72.88	5067	172.16.250.248	24813	SIP/2.0 100 Trying	call-8843
Received	2011-07-13 03:06:46	134.56.72.88	5067	172.16.250.248	24813	SIP/2.0 183 Session Progress	call-8843
Sent	2011-07-13 03:06:46	134.56.72.85	5067	172.16.250.248	57580	PRACK sip:fsrv2.f5test.com:5067;transport=Tls SIP/2	call-8843
Received	2011-07-13 03:06:46	134.56.72.85	5067	172.16.250.248	57580	SIP/2.0 200 OK	call-8843
Received	2011-07-13 03:06:48	134.56.72.88	5067	172.16.250.248	24813	SIP/2.0 183 Session Progress	call-8843
Received	2011-07-13 03:06:48	134.56.72.88	5067	172.16.250.248	24813	SIP/2.0 180 Ringing	call-8843
Received	2011-07-13 03:06:48	134.56.72.88	5067	172.16.250.248	24813	SIP/2.0 183 Session Progress	call-8843
Sent	2011-07-13 03:06:48	134.56.72.85	5067	172.16.250.248	57581	PRACK sip:fsrv2.f5test.com:5067;transport=Tls SIP/2	call-8843
Received	2011-07-13 03:06:48	134.56.72.85	5067	172.16.250.248	57581	SIP/2.0 200 OK	call-8843
Received	2011-07-13 03:06:55	134.56.72.88	5067	172.16.250.248	24813	SIP/2.0 200 OK	call-8843
Sent	2011-07-13 03:06:55	134.56.72.88	5067	172.16.250.248	24813	ACK sip:fsrv2.f5test.com:5067;transport=Tls SIP/2.0	call-8843
Sent	2011-07-13 03:06:55	134.56.72.85	5067	172.16.250.248	57582	BYE sip:fsrv2.f5test.com:5067;transport=Tls SIP/2.0	call-8843
Received	2011-07-13 03:06:55	134.56.72.85	5067	172.16.250.248	57582	SIP/2.0 481 Call Leg/Transaction Does Not Exist	call-8843

Deploying the Survivable Branch Appliance

Lync 2010 allows enterprises to deploy a Survivable Branch Appliance (SBA) at branch/remote offices that can switch to a stand-alone mode with limited functionality when the WAN link between the branch and the central site (which is usually corporate HQ) goes down. This page lists the steps needed to deploy Lync 2010 SBA at a branch site along with the corresponding configurations needed at the central site.

Copyright © 2015 Sonus Networks. All rights reserved.



Central Site Tasks

The following steps are required when deploying the SBA for the first time.

1. Adding the SBA to Active Directory
2. Adding the SBA to your Lync 2010 Topology or Adding the SBA to your Lync 2013 Topology, as appropriate to your deployment.
3. DNS Verification

> **Re-deploying the SBA?**
>
> If the SBA was previously deployed, and your ASM has been re-initialized, then you may skip over this section and continue starting with the #Branch Site Tasks.

Branch Site Tasks

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under **Lync™ Survivable Branch Appliance**, click **Setup SBA**.
3. Proceed with these steps in order:
    a. Configuring the ASM IP Settings
    b. Joining the ASM to a Domain
    c. Deploying the SBA
    d. Generate and Import an SBA Certificate
    e. Starting the SBA Services
    f. Applying an SBA Security Template (Optional Step)

Install the Latest Lync SBA Cumulative Update (CU)

To ensure the Lync SBA is running the latest Lync Server patches, administrators should install the latest Cumulative Update

Checking the SBA Status

To confirm that all the SBA services are running properly, check the status by Viewing the SBA Operational Status.

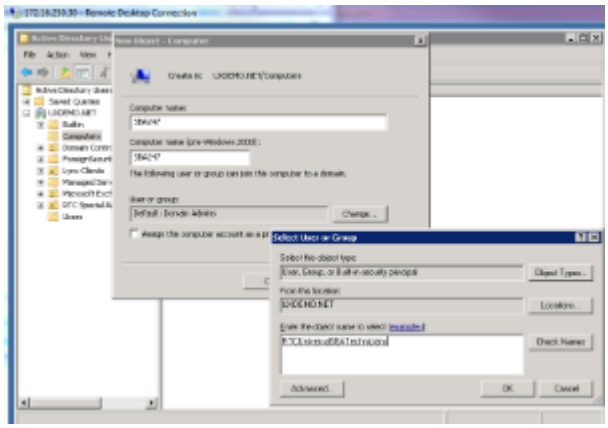
Copyright © 2015 Sonus Networks. All rights reserved.

Adding the SBA to Active Directory

For the latest Microsoft documentation on this step, please refer to Add a Survivable Branch Appliance to Active Directory

Adding the SBA to Active Directory as a Computer

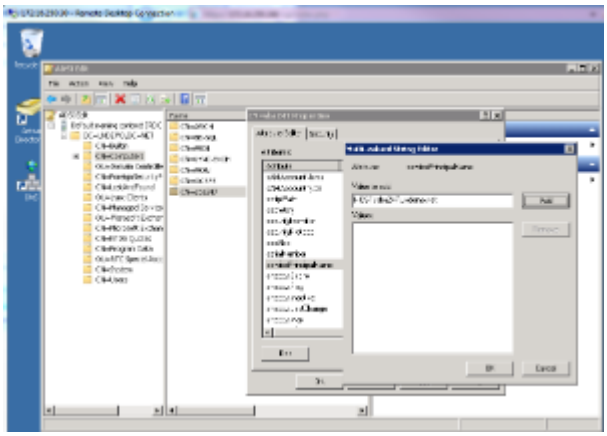
1. Remote Desktop in to AD machine with AD credentials.
2. Launch the Active Directory Users and Computers snap-in
3. Do a right click Computers object > select New > select Computer
4. In the Computer name field, enter the SBA machine name
   ⚠ **Note:** The computer name **must be NetBIOS compliant** with a maximum length of 15 characters.
5. In the Users or Group field, click Change > type "RTCUniversalSBATechnicians" in the Enter the object name to select field > click Check Names > hit OK.
6. Hit OK in the next screen to add the object as shown below:



Setting up the SPN

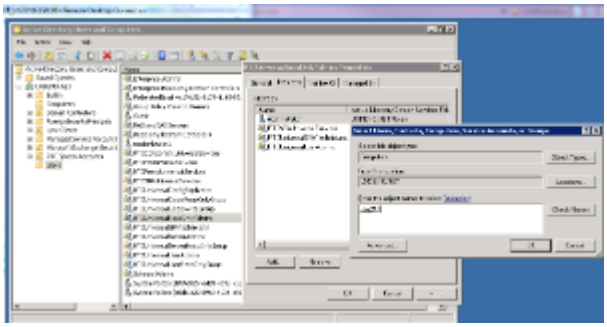
1. Remote Desktop in to Active Directory with AD credentials.
2. Launch the ADSI Edit snap-in
3. In the left pane, browse down to CN=Computers.
4. In the right pane, Do a right click CN=<sba machine name> object > select Properties
5. Scroll down and select the Service Principal Name entry in the list and click Edit button.
6. In Value to add field, enter HOST/<fqdn of the sba machine name> and hit Add button as shown below.
7. Hit OK and exit out from ADSI Edit:

Copyright © 2015 Sonus Networks. All rights reserved.



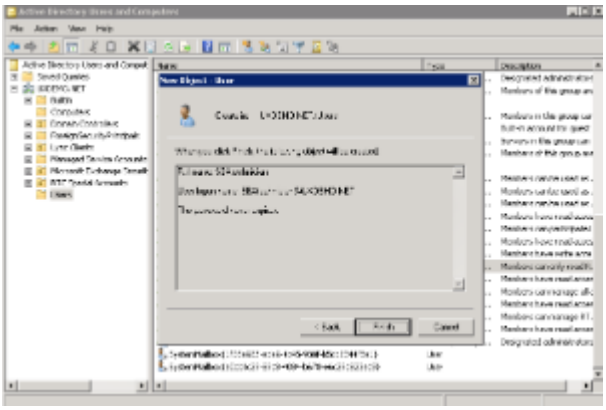
Adding the SBA to the RTCUniversalReadOnlyAdmins Group

1. Remote Desktop in to AD machine with AD credentials.
2. Launch the Active Directory Users and Computers snap-in
3. Browse down to Users object (on the left pane) > do a right click RTCUniversalReadOnlyAdmins group and select Properties
4. In the Members tab click Add button
5. In the new popup enter the sba machine name as shown below, hit on Check Names > hit on OK button
6. Click OK button to close the properties screen.



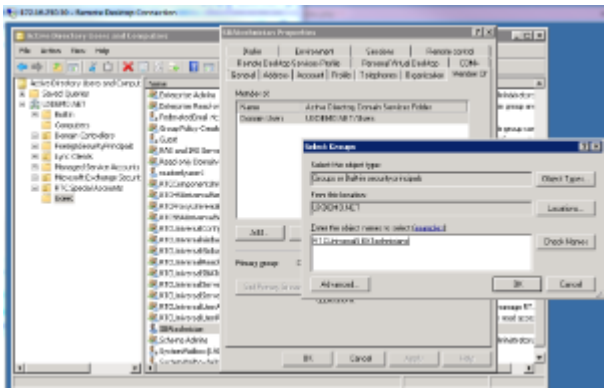
Creating the SBA Installer Account in Active Directory

1. Remote Desktop in to AD machine with AD credentials.
2. Launch the Active Directory Users and Computers snap-in
3. Do a right click Users object > select New > select User
4. Create an SBA installer account as shown below:



Copyright © 2015 Sonus Networks. All rights reserved.

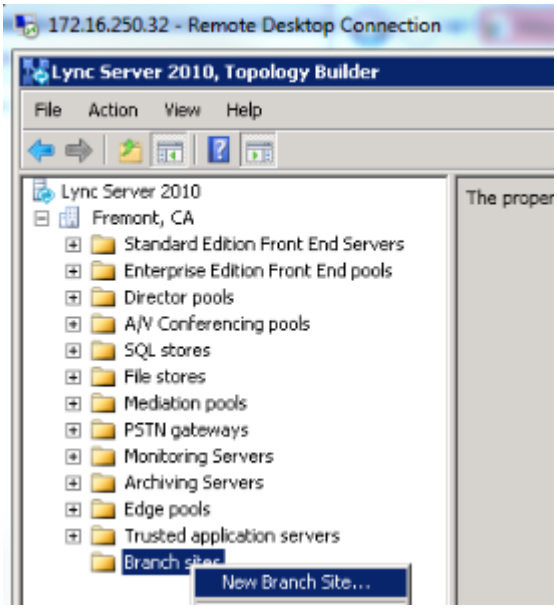
5. In the newly created user's properties, add a membership to RTCUniversalSBATechnicians groups as shown below:



Adding the SBA to your Lync 2010 Topology

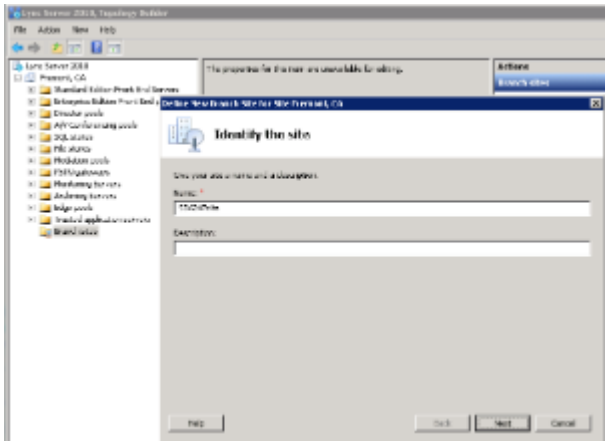
For the latest Microsoft documentation on this step, please refer to Add Branch Sites to Your Topology

1. Remote Desktop into the Lync Front End Server.
2. Launch the Lync Server Topology Builder.
3. In the left pane, right-click on the Branch Site and select New Branch Site as shown below:

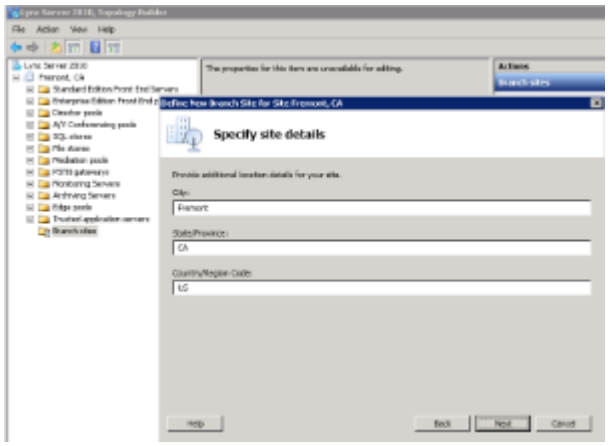


4. Define the site name and click Next.
   Note: The computer name **must be NetBIOS compliant**with a maximum length of 15 characters.

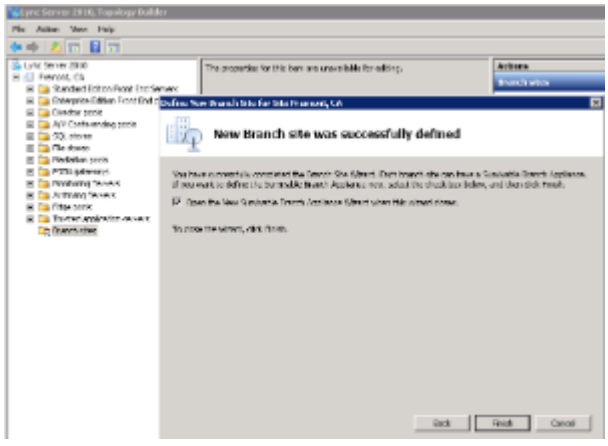
Copyright © 2015 Sonus Networks. All rights reserved.



5. Enter the site details as shown below and click Next.

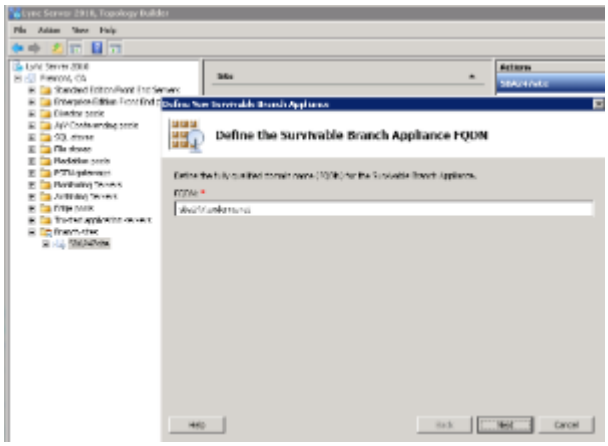


6. Click Finish.

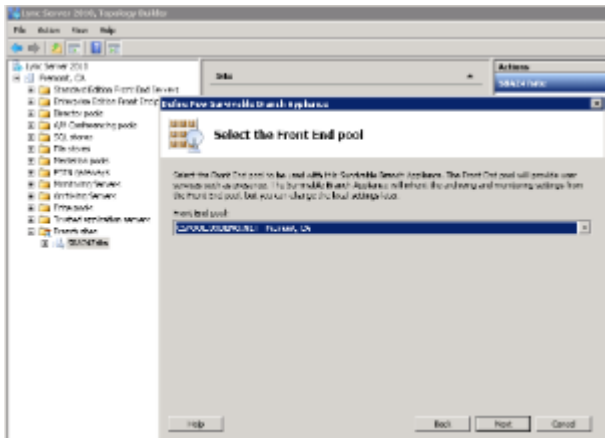


7. Enter the FQDN of the SBA as shown below.

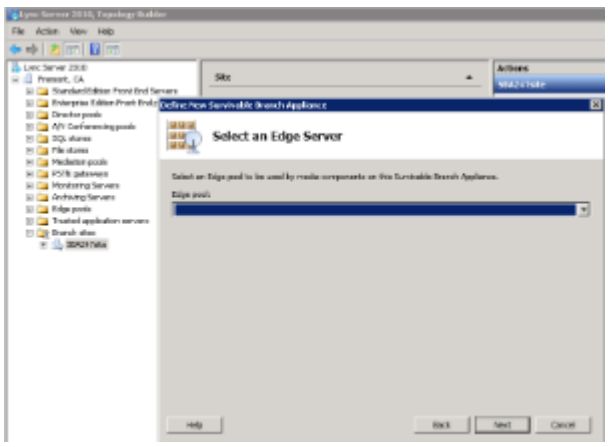
Copyright © 2015 Sonus Networks. All rights reserved.



8. Select the Front End Pool.

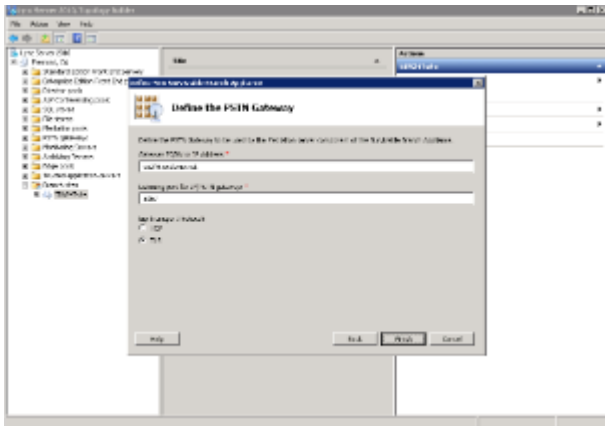


9. If you have an Edge Server, select the Edge pool (or leave it blank) and click Next.

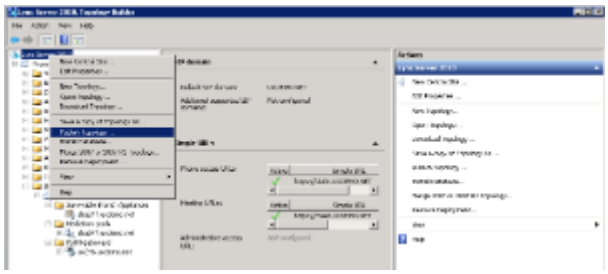


10. Define the PSTN gateway as shown below and click Finish.

Copyright © 2015 Sonus Networks. All rights reserved.



11. In the left pane, Right-click the Lync Server 2010 and select Publish Topology to publish the newly created topology.

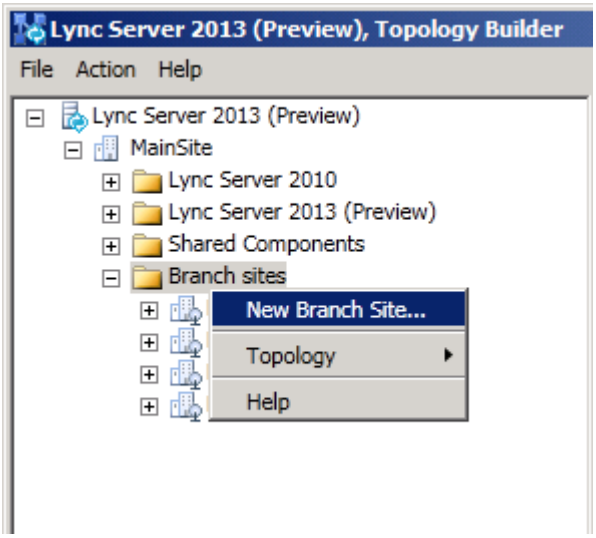


Adding the SBA to your Lync 2013 Topology

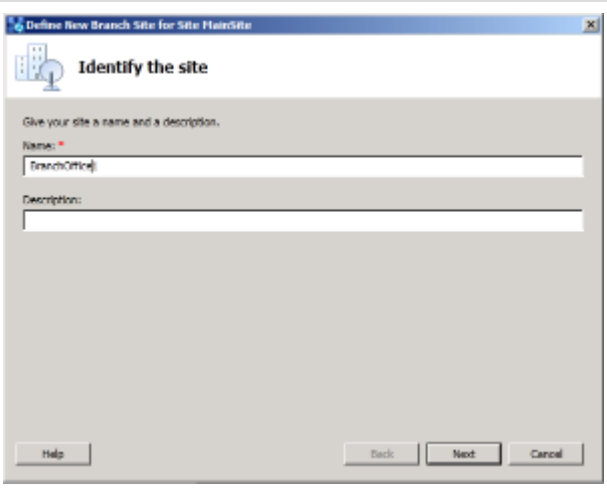
For the latest Microsoft documentation on this step, please refer to Add Branch Sites to Your Topology

1. Remote Desktop into the Lync Front End Server.
2. Launch the Lync Server Topology Builder.
3. In the left pane, right-click on the Branch Site and select New Branch Site as shown below:

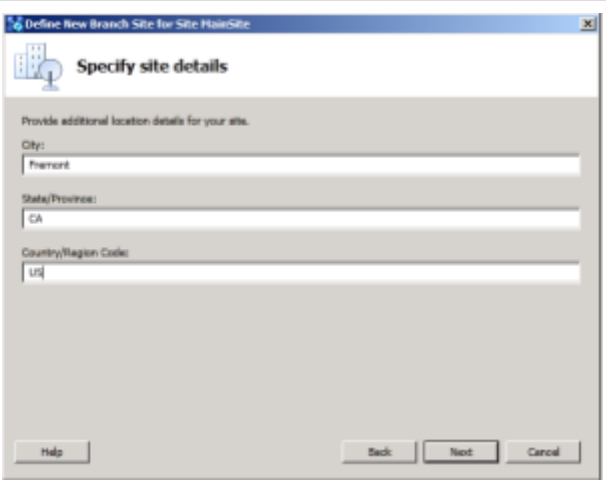
Copyright © 2015 Sonus Networks. All rights reserved.



4. Define the site name and click Next.
   Note: The computer name **must be NetBIOS compliant**with a maximum length of 15 characters.

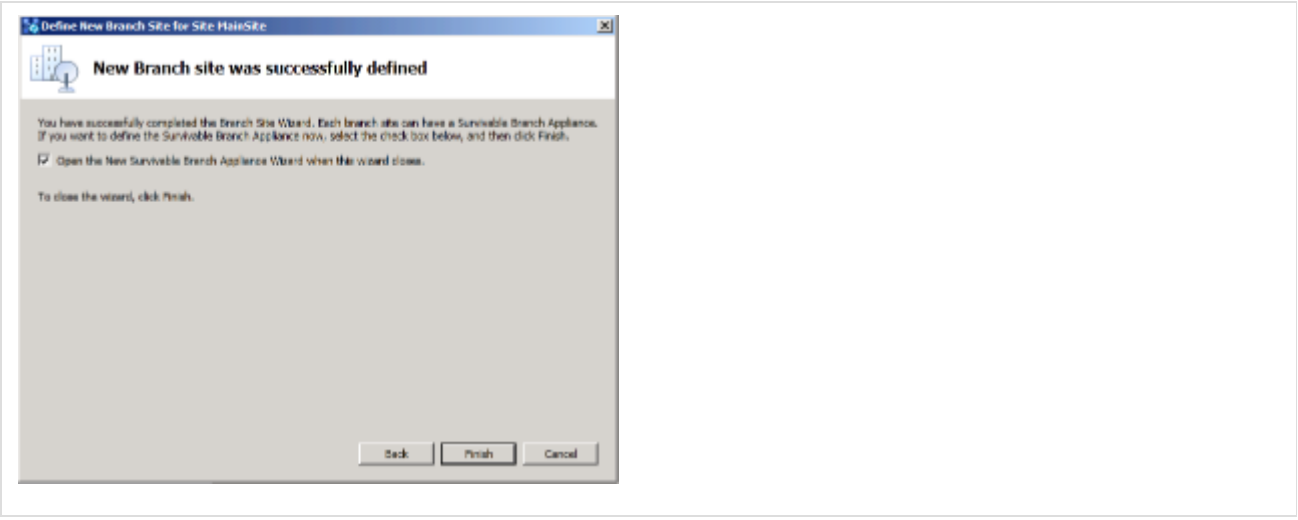


5. Enter the site details as shown below and click Next.

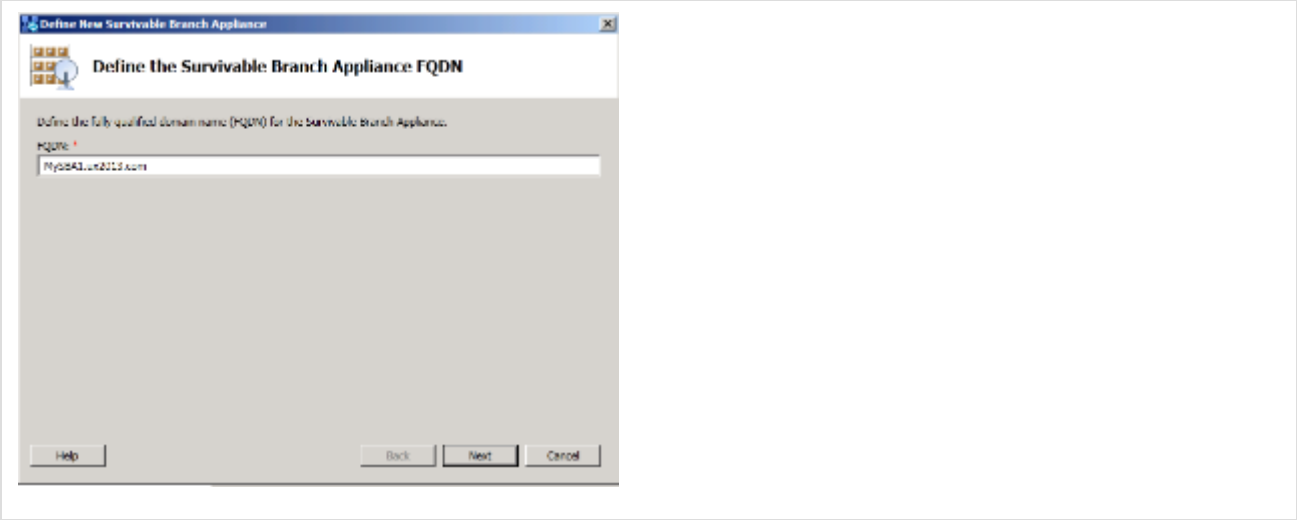


6. Click Finish.

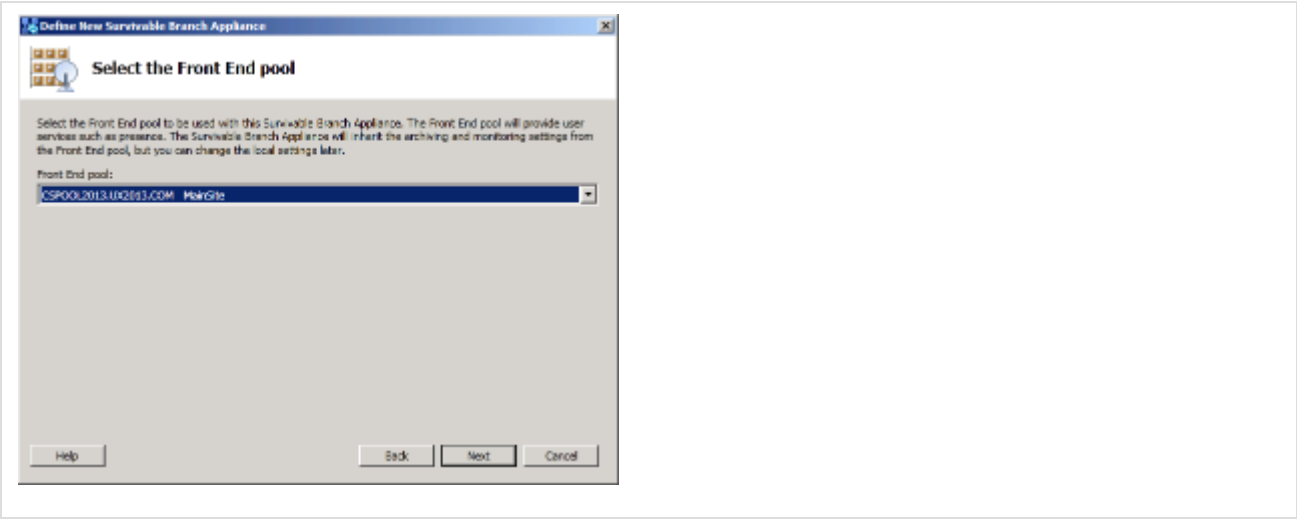
Copyright © 2015 Sonus Networks. All rights reserved.



7. Enter the FQDN of the SBA as shown below.

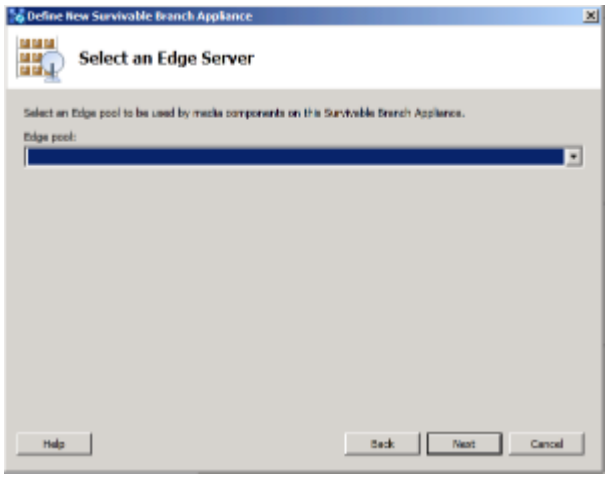


8. Select the Front End Pool.

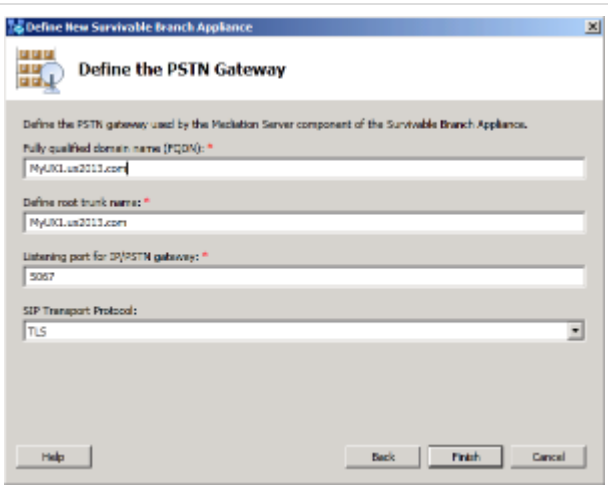


9. If you have an Edge Server, select the Edge pool (or leave it blank) and click Next.

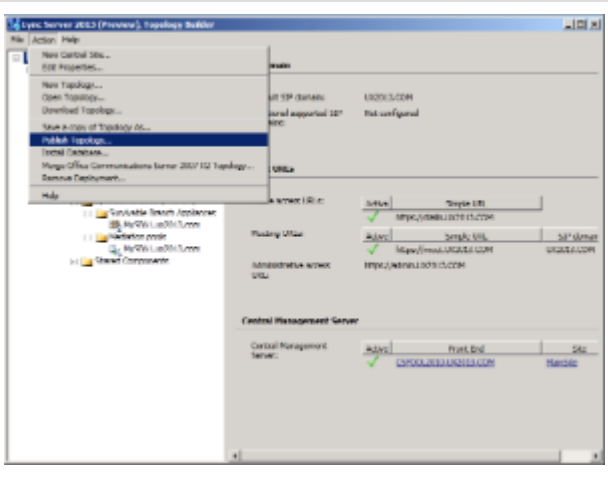
Copyright © 2015 Sonus Networks. All rights reserved.



10. Define the PSTN gateway as shown below and click Finish.



11. In the left pane, Right-click the Lync Server 2013 and select Publish Topology to publish the newly created topology.



Verifying and Configuring DNS

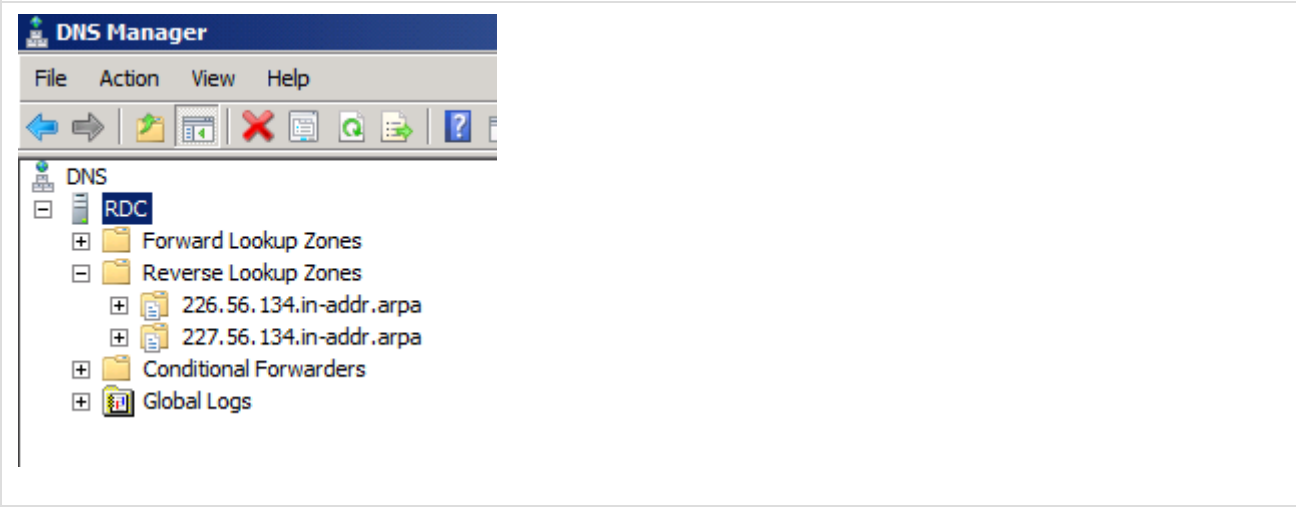
This procedure explains how to configure the DNS Server for use with the Sonus SBC 1000/2000-SBA in a Lync

Copyright © 2015 Sonus Networks. All rights reserved.

Server deployment.

Verifying the DNS Reverse Lookup

1. Connect to the DNS machine using a Remote Desktop Application.
2. Log into the DNS machine using administrator credentials.
3. Launch the DNS snap-in.



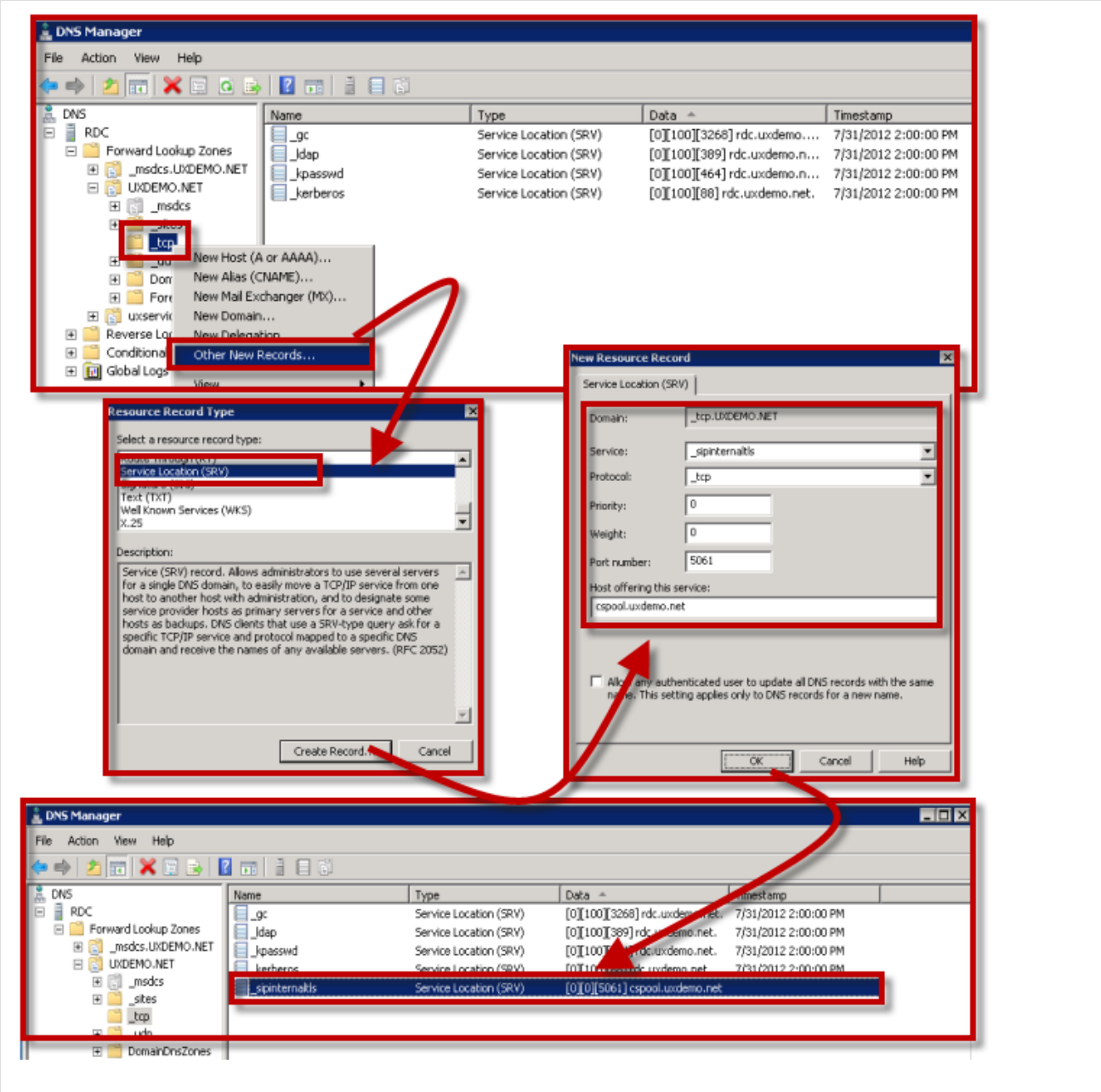
4. Expand the tree until you reach the computer name of the DNS server.
5. Verify that there is one entry for each network in the domain in the **Reverse Lookup Zones** directory.

> **Note:** The name is in reverse order. For example:the network ***134.56.226.0*** appears as ***226.56.134.in-addr.arpa***.

Configuring DNS auto login

1. Connect to the DNS machine using a Remote Desktop Application.
2. Log into the DNS machine using administrator credentials.
3. Launch the DNS snap-in.

Copyright © 2015 Sonus Networks. All rights reserved.

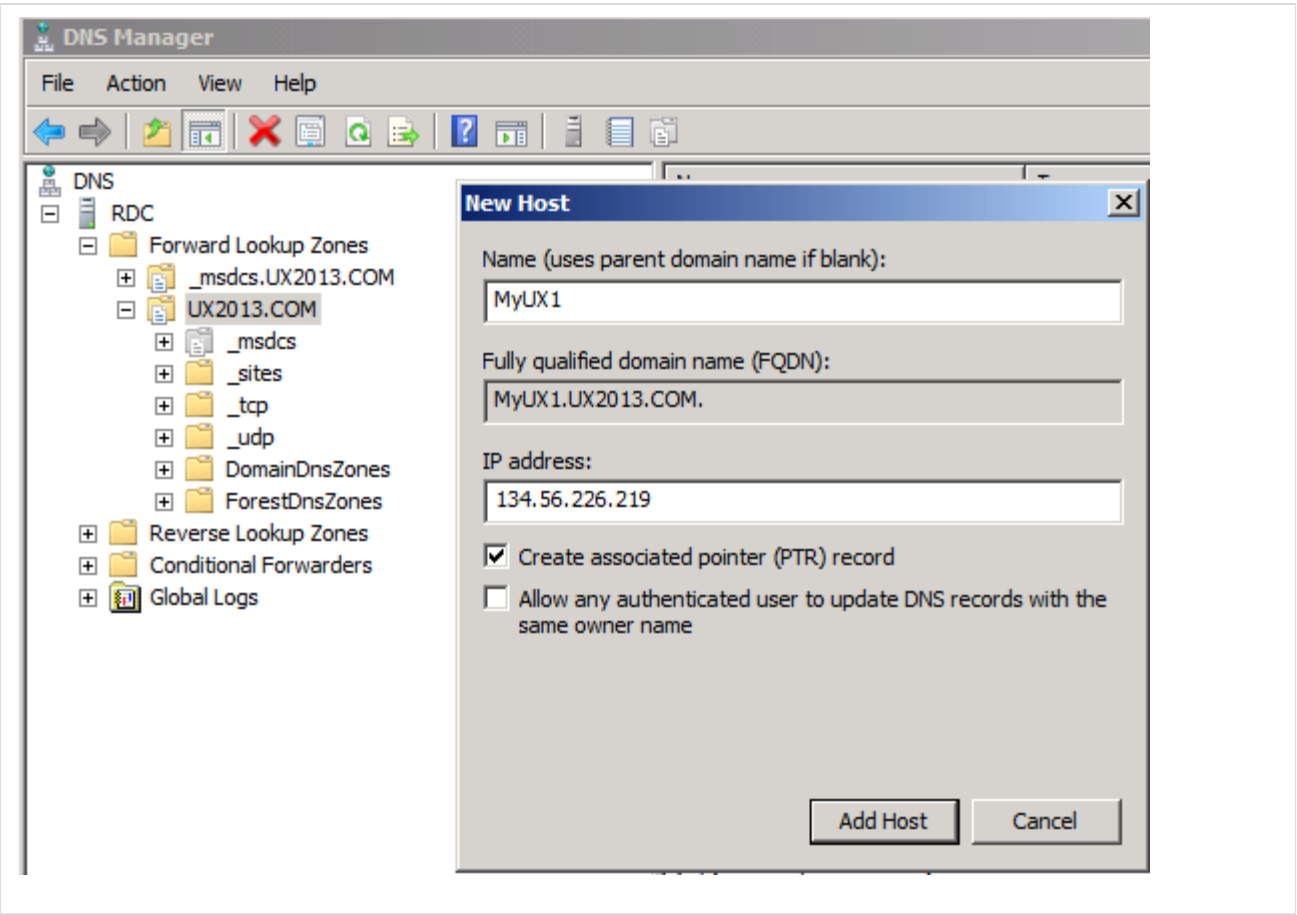


4. Expand the tree until you reach the computer name of the DNS server.
5. Right click the **_TCP** folder.
6. Select **Other New Records...**.
7. Select **Service Location (SRV)**.
8. click "Create Record".
9. In the **Service Location (SRV** tab*, make the following selections:
    a. Enter _sipinternaltls in the **Service** text box.
    b. Enter_TCP in the **Protocol:** text box.
    c. Enter the cspool FQDN in the **Host offering this servide:** text box.
10. Click **OK**.

Adding a DNS record for Sonus SBC 1000/2000

1. Connect to the DNS machine using a Remote Desktop Application.
2. Log into the DNS machine using administrator credentials.
3. Launch the DNS snap-in.

Copyright © 2015 Sonus Networks. All rights reserved.



4. Expand the tree until you reach the computer name of the DNS server.
5. Right click the appropriate domain.
6. Select **New Host (A or AAAA)...**.
7. Enter the command name of the Sonus SBC 1000/2000 in the **Name:** text box.
8. Enter the IP Address of the Sonus SBC 1000/2000 in the **IP address:** text box.
9. Select **Create associated pointer (PTR) record**.
10. Click **OK**.

Configuring the SBC 1000 for FXS Calling

This article describes the steps necessary for configuring the Sonus SBC 1000 to route incoming PSTN calls to an FXS port. In the example below, ISDN/PSTN calls arriving with four digits are routed to an FXS port.

The process comprises four overall steps:

- Creating an FXS Signaling Profile
- Creating and configuring a CAS Signaling Group
- Adding and configuring a Transformation Table and Entry
- Adding a Call Routing Entry and resequencing it

- Prerequisites
  - Software Version
  - System Licenses
  - FXS Card State and Port Status
    - FXS Card State
    - Port Status

Copyright © 2015 Sonus Networks. All rights reserved.

    - Verify the FXS Port Connections
- Configuration
    - CAS Signaling Group and FXS Port configuration
    - Telephony Routing configuration
    - Call Debugging Trace

Prerequisites

Software Version

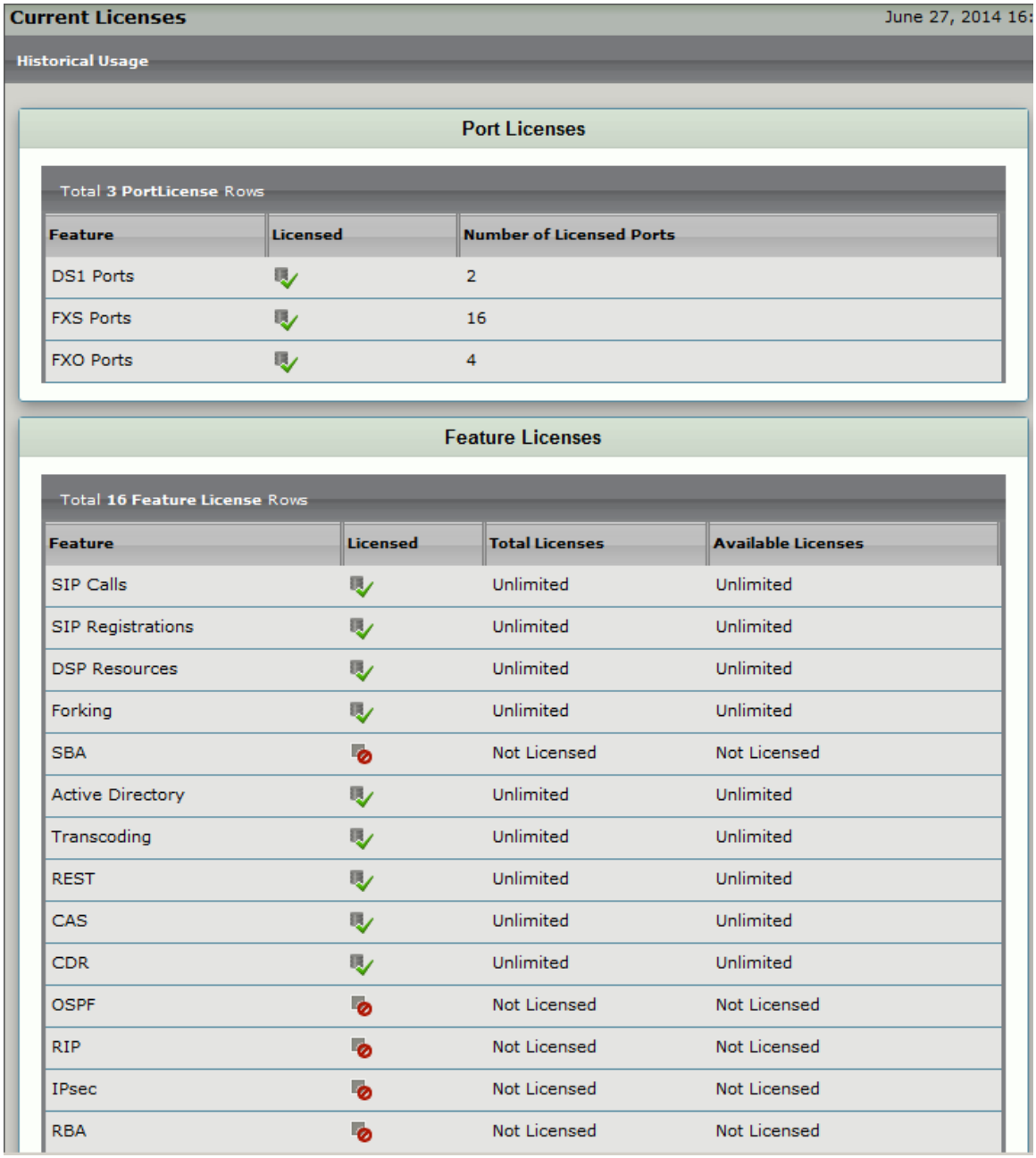
Verify that your Sonus SBC 1000 is loaded with the correct boot image version and that your Sonus SBC 1000 base software version is at least version 2.0.0, build 108.

⚠️ The FXS card does not function with older versions of the Sonus SBC 1000 firmware/software. Should you need to upgrade your Sonus SBC 1000 unit, you must follow the Sonus SBC 1000/2000 Upgrade Guide.

System Licenses

The Sonus SBC 1000 system must have the necessary licenses to make calls. In addition to **CAS** and **DSP channels**, and depending upon the types of calls, the **Transcoding** and **SIP calls** licenses may also be necessary as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



Current Licenses June 27, 2014 16:

Historical Usage

Port Licenses

Total **3 PortLicense** Rows

Feature	Licensed	Number of Licensed Ports
DS1 Ports	✓	2
FXS Ports	✓	16
FXO Ports	✓	4

Feature Licenses

Total **16 Feature License** Rows

Feature	Licensed	Total Licenses	Available Licenses
SIP Calls	✓	Unlimited	Unlimited
SIP Registrations	✓	Unlimited	Unlimited
DSP Resources	✓	Unlimited	Unlimited
Forking	✓	Unlimited	Unlimited
SBA	⊘	Not Licensed	Not Licensed
Active Directory	✓	Unlimited	Unlimited
Transcoding	✓	Unlimited	Unlimited
REST	✓	Unlimited	Unlimited
CAS	✓	Unlimited	Unlimited
CDR	✓	Unlimited	Unlimited
OSPF	⊘	Not Licensed	Not Licensed
RIP	⊘	Not Licensed	Not Licensed
IPsec	⊘	Not Licensed	Not Licensed
RBA	⊘	Not Licensed	Not Licensed

FXS Card State and Port Status

FXS Card State

- Check the state of the FXS card.
  - Verify that the state for the Telco Module(s) indicated in the **Cards/Modules Status** pane is **Activated**.

Copyright © 2015 Sonus Networks. All rights reserved.

Cards/Modules Status

Total **9 Module** Rows

Location	Type	Module Service Status	Module State
Main Board	Main Board	Up	Activated
DSP Module 1	MSPD C300 DSP	Up	Activated
DSP Module 2	MSPD C300 DSP	Up	Activated
Telco Module 2	FXS w/ 4 Ports (Licensed 4 Ports)	Up	Activated
Telco Module 4	FXS w/ 4 Ports (Licensed 4 Ports)	Up	Activated
Telco Module 5	FXO w/ 4 Ports (Licensed 4 Ports)	Up	Activated
Telco Module 7	DS1 w/ 2 Spans (Licensed 2 Ports)	Up	Activated
Telco Module 1	FXS w/ 4 Ports (Licensed 4 Ports)	Up	Activated
Telco Module 3	FXS w/ 4 Ports (Licensed 4 Ports)	Up	Activated

Port Status

- Check the Port Status to verify that the FXS ports are functional.
  - Verify that the **Admin State** and **Service Status** for each port indicates **Up** as shown below.

Ports Status

Total **24 Port** Rows

Port ID	Port Type	Admin State	Service Status
Port 1:1	FXS	Up	Up
Port 1:2	FXS	Up	Up
Port 1:3	FXS	Up	Up
Port 1:4	FXS	Up	Up
Port 2:1	FXS	Up	Up
Port 2:2	FXS	Up	Up
Port 2:3	FXS	Up	Up
Port 2:4	FXS	Up	Up

✅ **FXS not Activated and Up?** Did you upgrade the boot image and Sonus SBC 1000 base software versions as outlined above.

Verify the FXS Port Connections

Copyright © 2015 Sonus Networks. All rights reserved.

Verify that your FXS devices are connected to the ports you plan to configure.
Later in this article, you will create a CAS Signaling Group and assign channels and ports, they must match the physical ports to which the FXS devices are connected. See the figure below.



The FXS Ports and Channels in a CAS Signaling Group

Assigned Channels

Total **4 CAS Channel** Rows

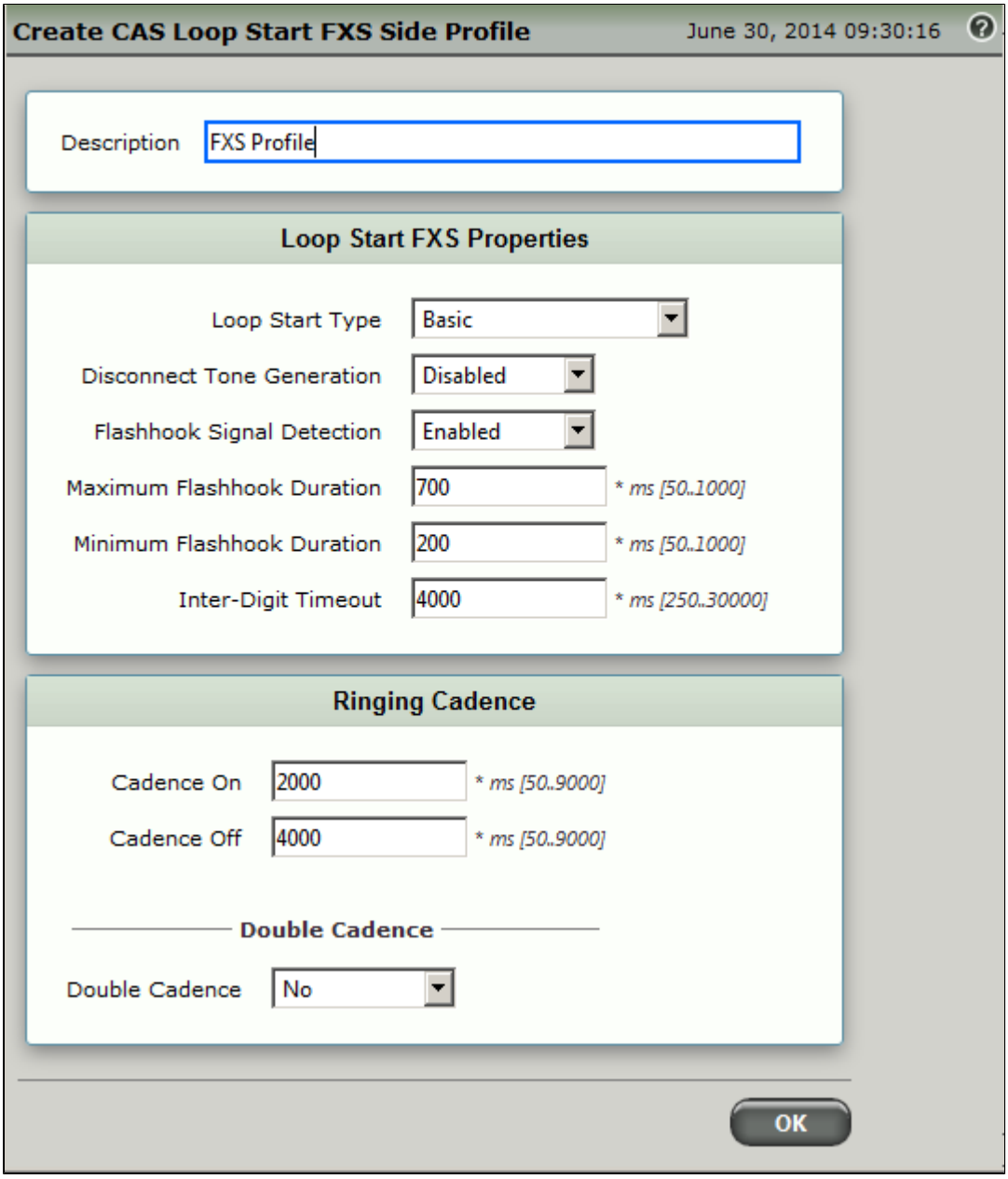
Port Name	Channel Phone Number	Hotline Enabled	Hotline Number	Call Forwarding Activated	Call Forwarding Number
1:1	5401	No		No	
1:2	5402	No		No	
1:3	5403	No		No	
1:4	5404	No		No	

Configuration

CAS Signaling Group and FXS Port configuration

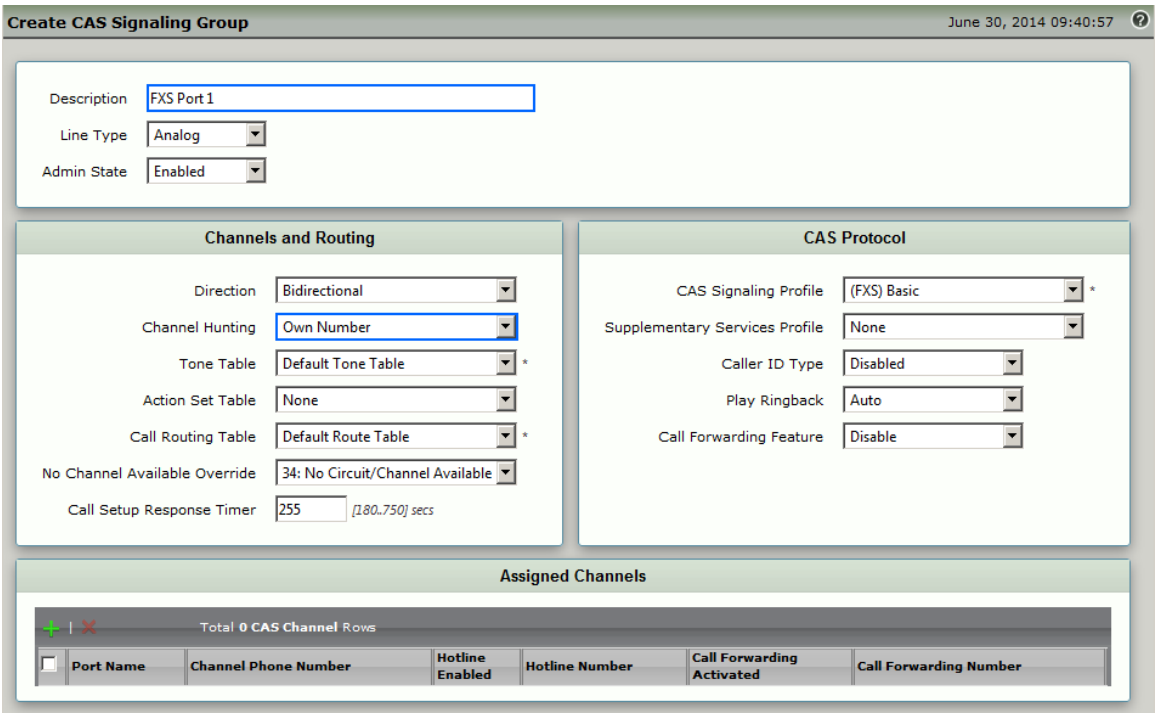
1. Create an FXS Signaling Profile for CAS.

Copyright © 2015 Sonus Networks. All rights reserved.

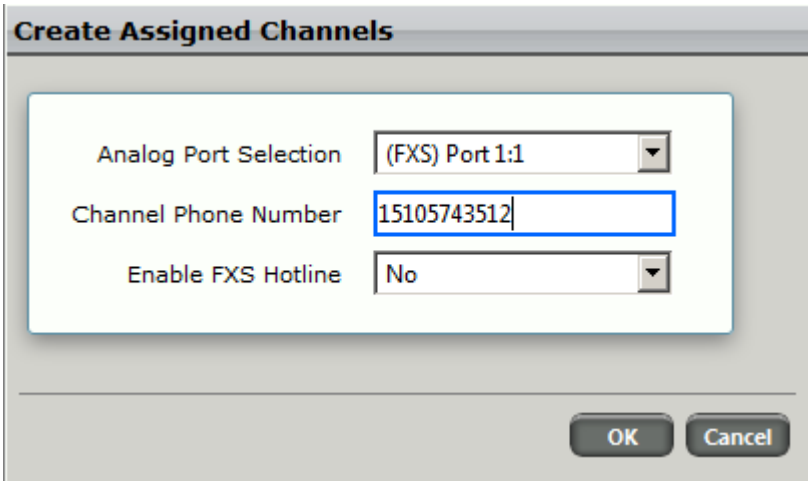


2. Create a CAS Signaling Group.
   ⚠ Make sure to set the Channel Hunting to **Own Number**, otherwise the first free channel will answer every call (regardless of any other configuration settings).

Copyright © 2015 Sonus Networks. All rights reserved.

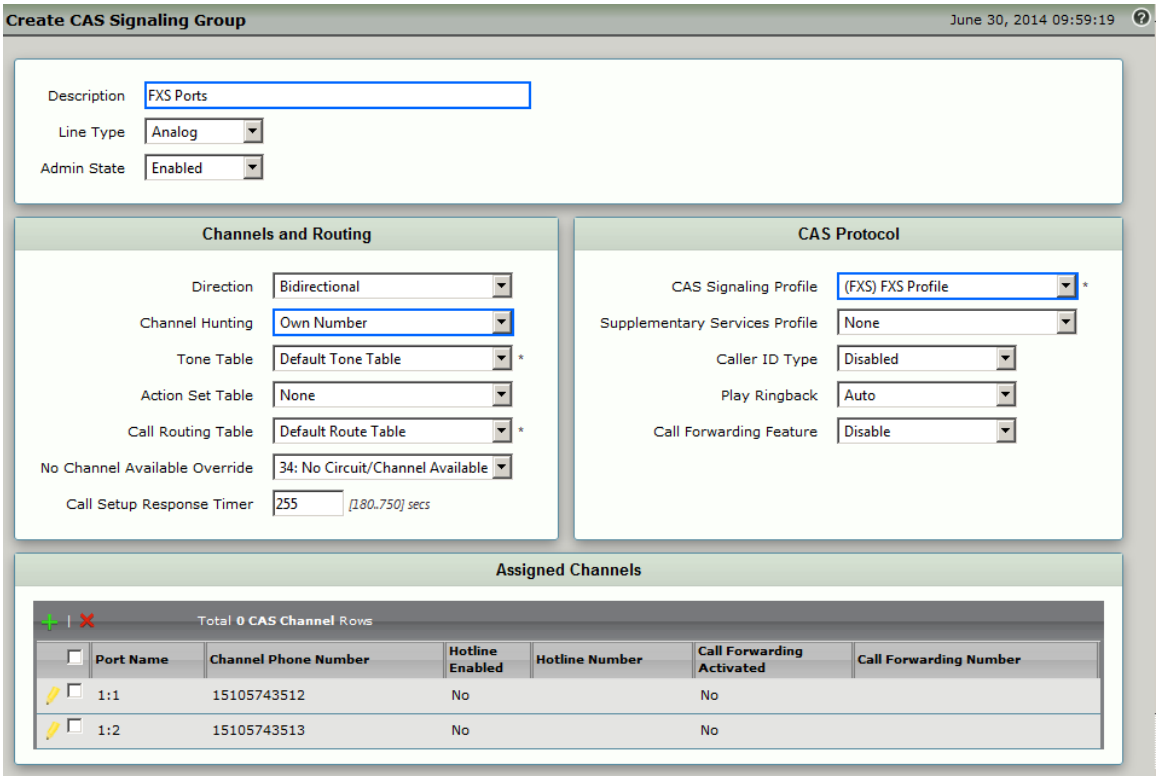


3. Create an **Assigned Channel** and apply the desired phone number to the corresponding FXS port.
   ✅You may add all of the port/number combinations for FXS in a single Signaling Group.



4. Verify that the CAS Signaling group is configured as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



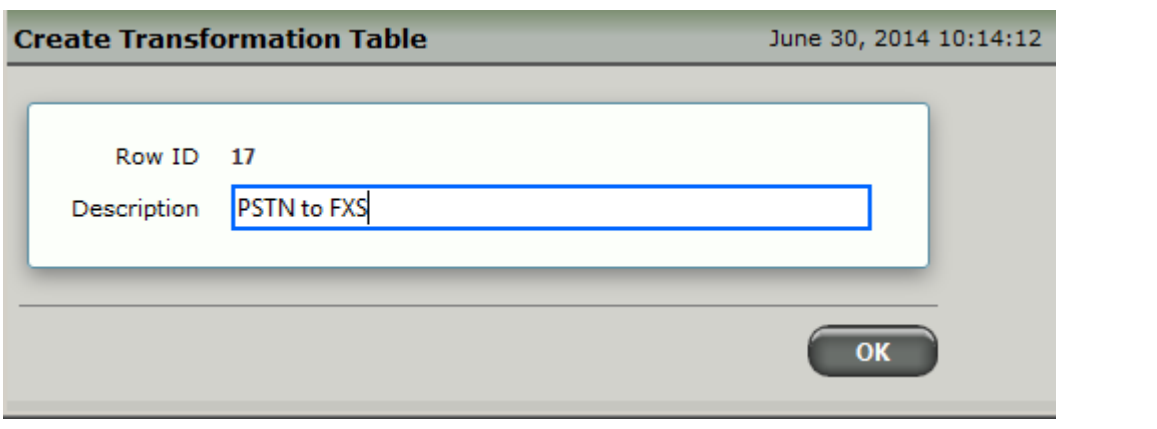
5. Verify that the FXS-attached phone(s) now have dial-tone.

> **No dial-tone?**
>
> Are you certain your boot image and Sonus SBC 1000/2000 software versions are up to date as noted in the Prerequisites?

Telephony Routing configuration

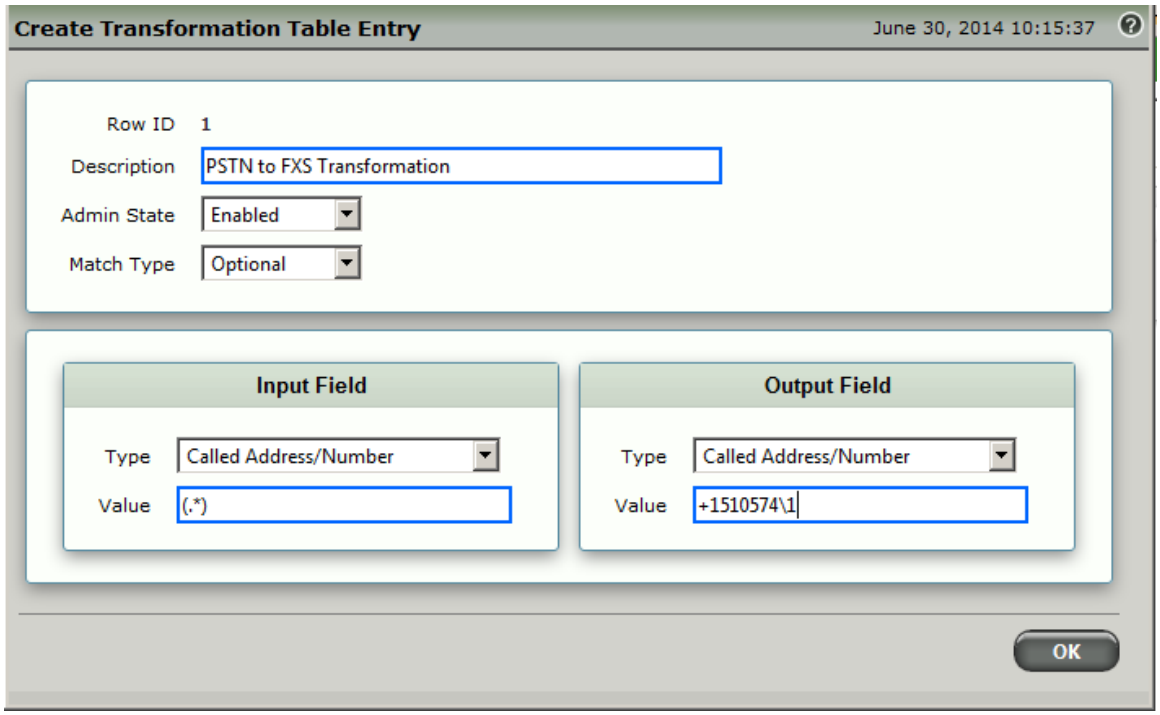
In order to route incoming ISDN calls with 4 digits to FXS ports, you must create a Transformation table whose entry prepends +1510574. The resulting called number, *+1510574xxxx*, then matches the Channel Phone Numbers configured in the previous section.

1. Create a Transformation Table for the FXS calls called **PSTN to FXS**:

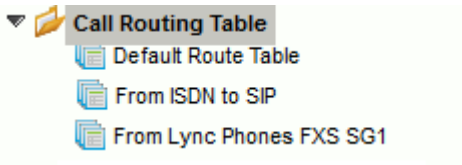


2. Create a Transformation entry to that table called **PSTN to FXS Transformation**.

Copyright © 2015 Sonus Networks. All rights reserved.

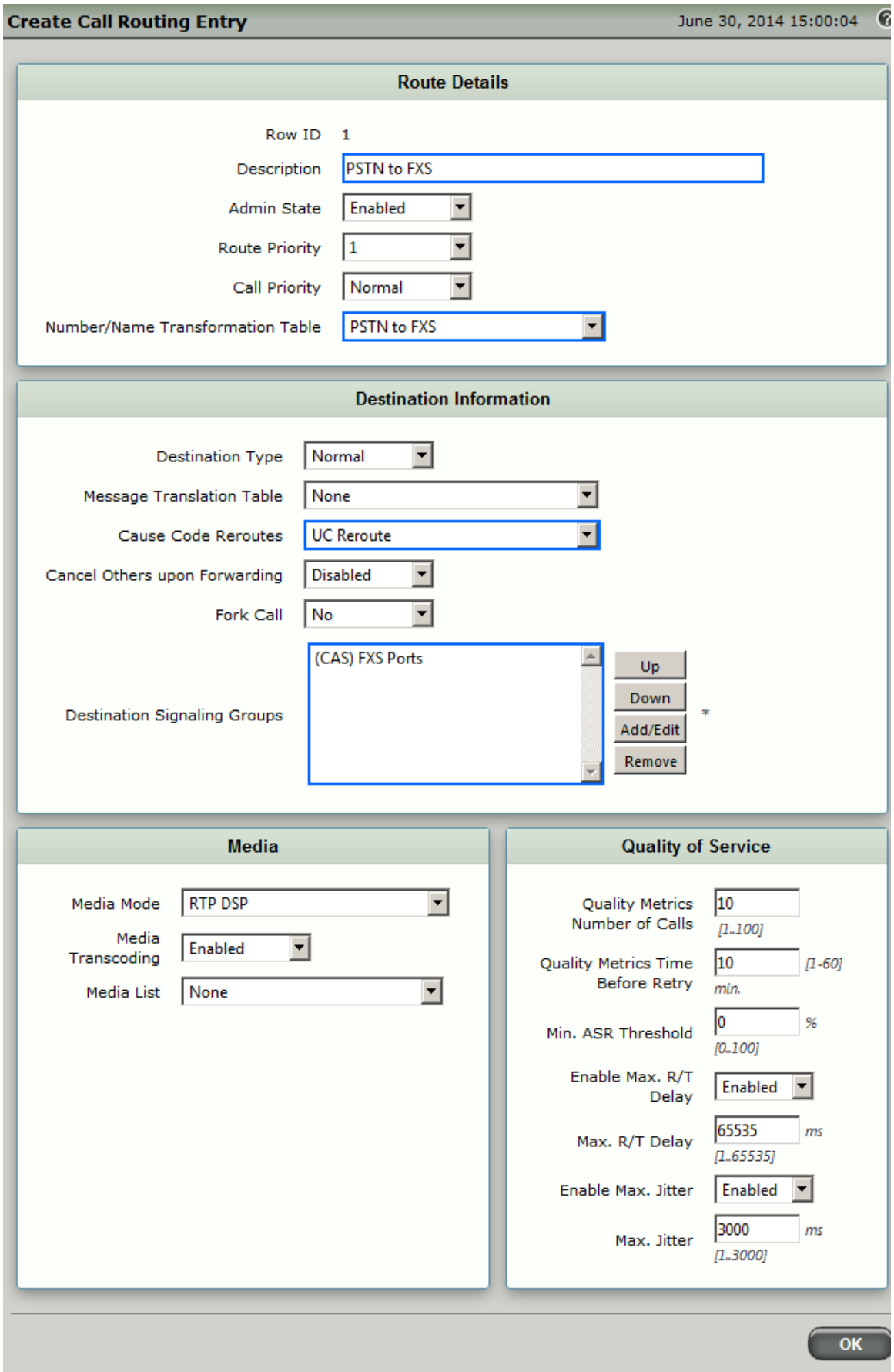


3. Add a call route table called **From ISDN to SIP**.



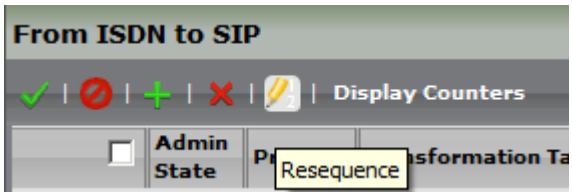
Add a call route entry to that table which employs the transformation created in the previous step called **PSTN to FXS**.

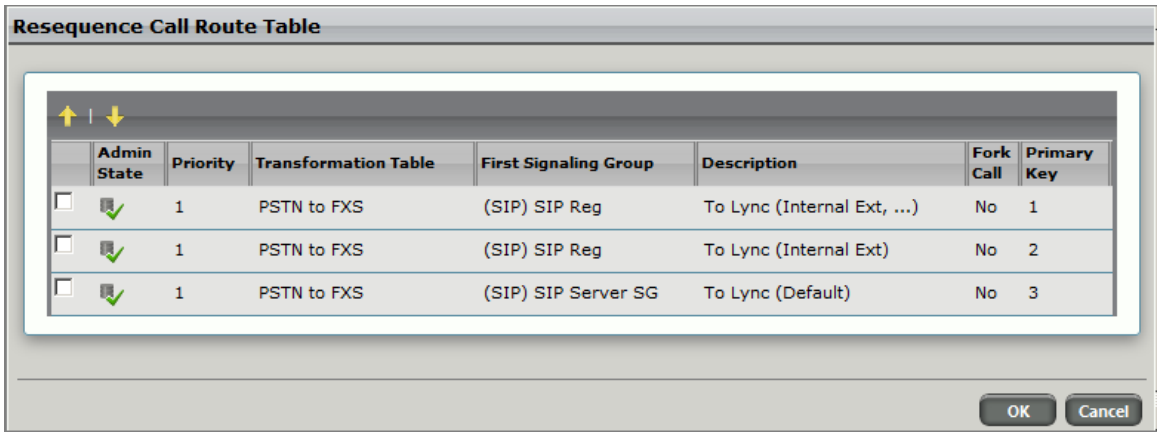
Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.

4. Resequence the FXS call route.





Calls should now work from ISDN to FXS.

> **No audio or dial-tone, but calls complete?**
>
> Try reseating the DSP cards and telephony feature cards. Also, re-verify your licenses.

Call Debugging Trace

The Sonus SBC 1000 logging trace produced was saved when making the FXS call - you can download it here.

Deployment in PSTN - SBC - Microsoft OCS 2007 R2 Topology

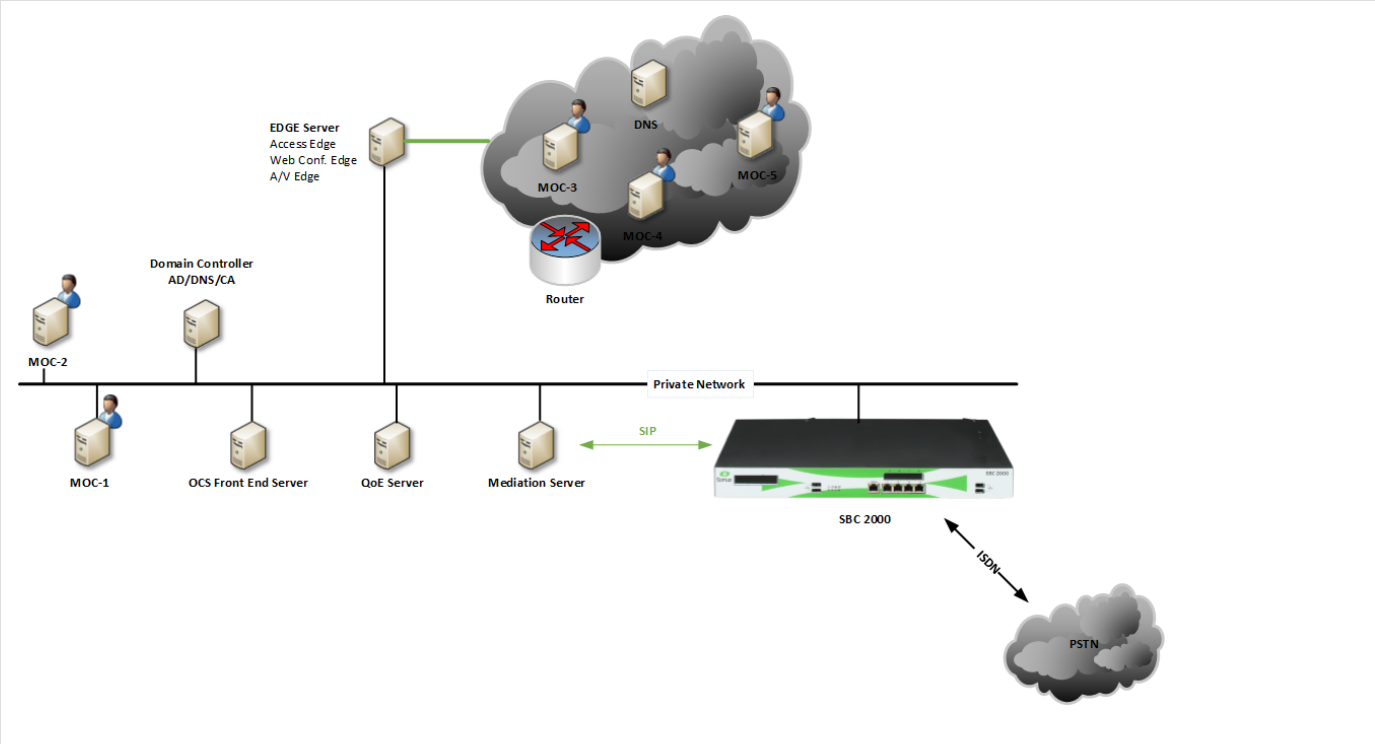
This article describes the process of configuring a Sonus SBC 1000/2000 for deployment in an ISDN environment using Microsoft Office Communication Server (OCS) 2007 R2 to support connectivity between OCS 2007 R2 and PSTN.

The OCS 2007 Setup configuration Wizard allows you to rapidly configure the Sonus SBC 1000/2000 for integration with OCS 2007. Although you can manually configure the Sonus SBC 1000/2000 for integration with OCS, it is highly recommended that you use the wizard:

- Accessing the Sonus SBC 1000/2000 OCS 2007 Setup Wizard
- Wizard Created Configuration
- Sonus SBC 1000/2000 Verification Steps

Topology

Copyright © 2015 Sonus Networks. All rights reserved.

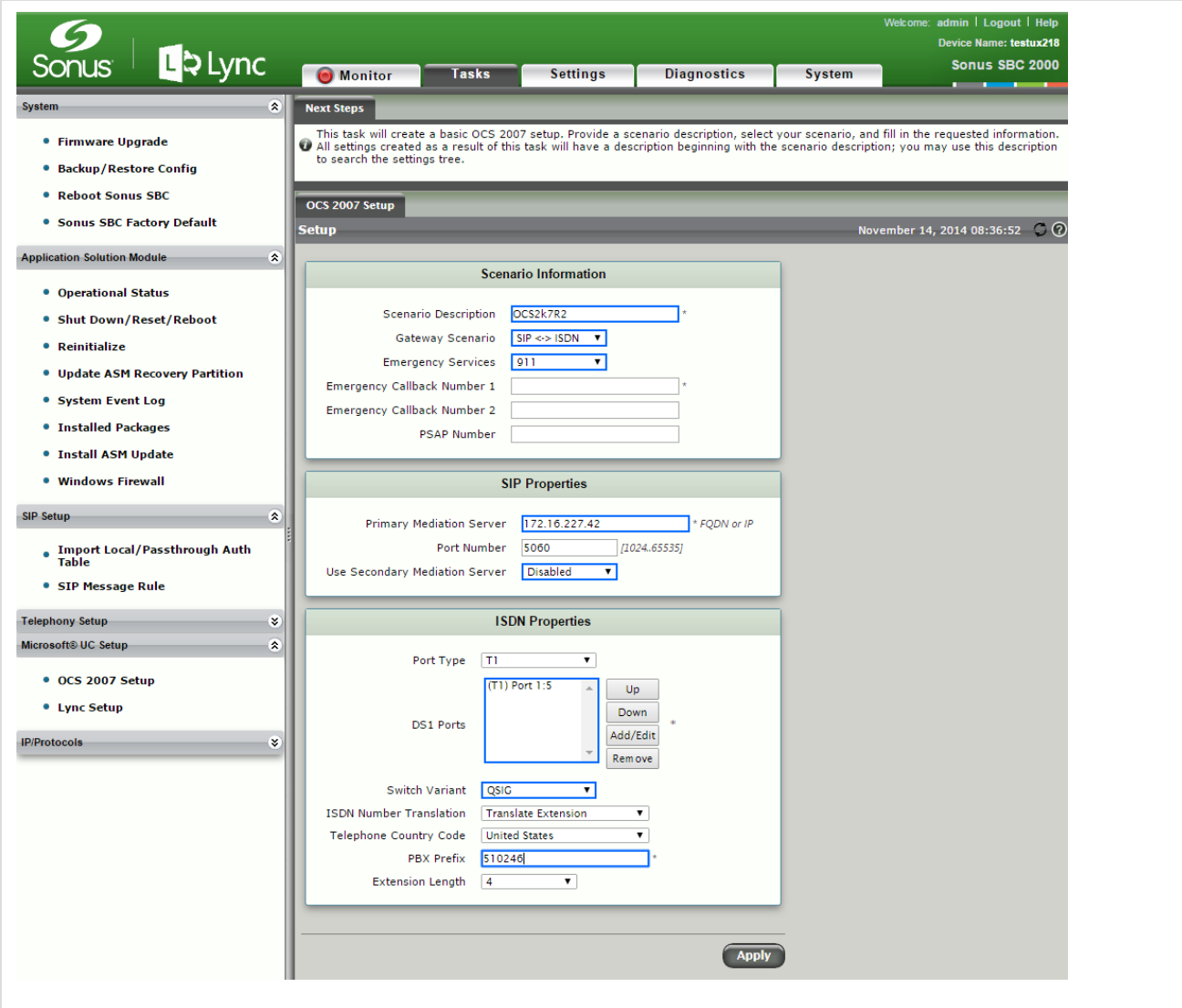


Accessing the Sonus SBC 1000/2000 OCS 2007 Setup Wizard

> The OCS 2007 Setup Wizard **does not** overwrite nor replace existing Sonus SBC 1000/2000 configuration. Wizard resources are created on top of existing Sonus SBC 1000/2000 configuration items.

1. In the WebUI, navigate to the **Tasks** tab.
2. Click **OCS 2007 Setup** in the left pane.
3. Fill in the desired information for a PSTN – Sonus SBC 1000/2000 – MS OCS 2007 R2 deployment.
   ✅ For a SIP Trunking deployment, please refer to Deploying the Sonus SBC 1000-2000 and OCS 2007 with a SIP Trunk Provider
4. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.



Wizard Created Configuration

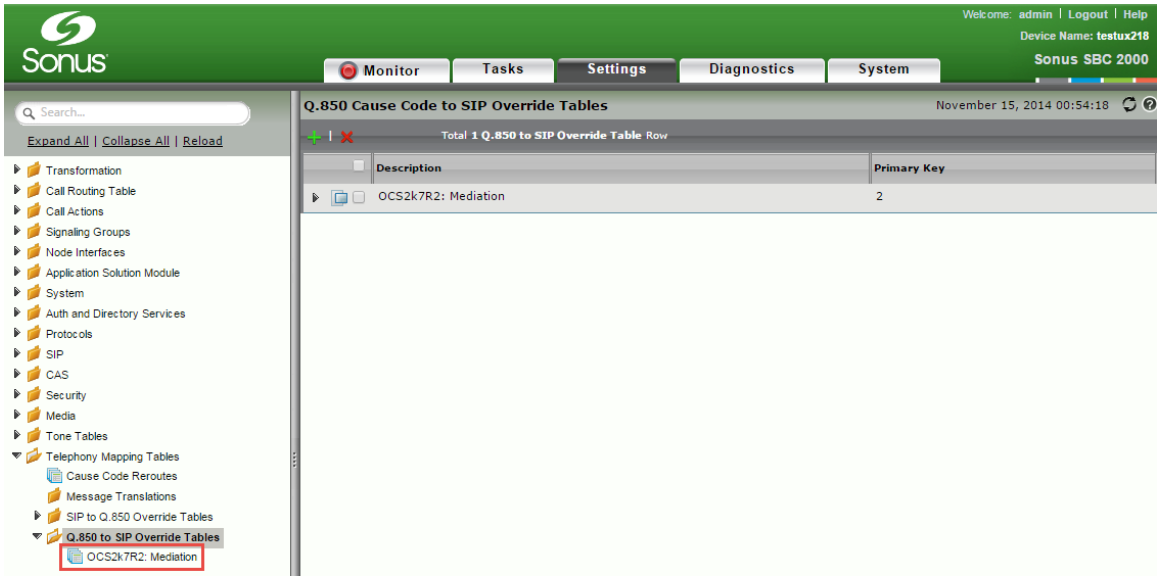
Upon the wizard's successful setup completion, the Sonus SBC 1000/2000's configuration gets populated with the following attributes:

1. #Q.50 to SIP Cause Code Mapping
2. #Tone Table
3. #Media Profiles
4. #Media List
5. #SIP Server Table
6. #SIP Profile
7. #SIP Signaling Groups
8. #ISDN Signaling Groups
9. ISDN_SIP Routing Tables
10. ISDN_SIP Translation Tables

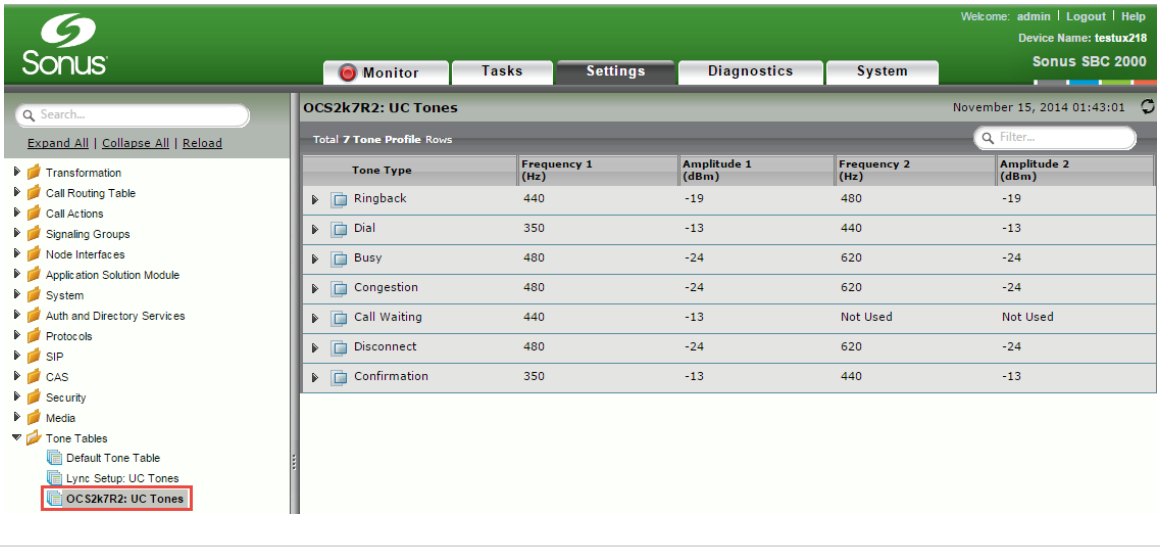
The following images depict the various configuration resources and attributes created by the wizard

Q.850 to SIP Cause Code Mapping

Copyright © 2015 Sonus Networks. All rights reserved.

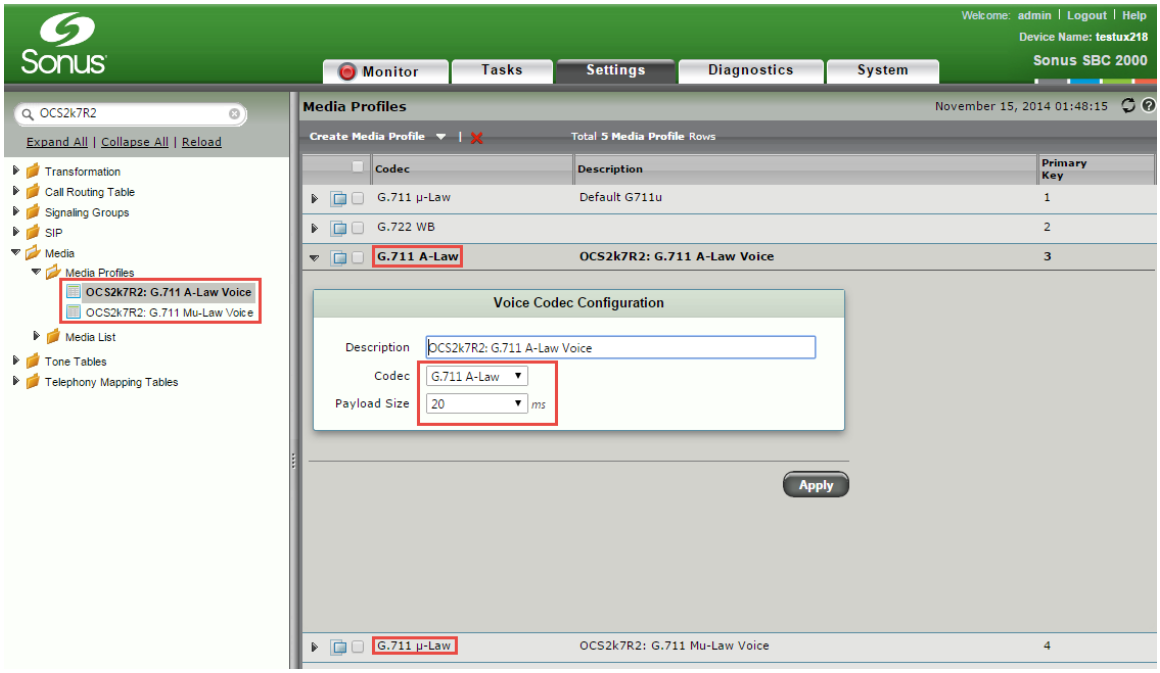


Tone Table

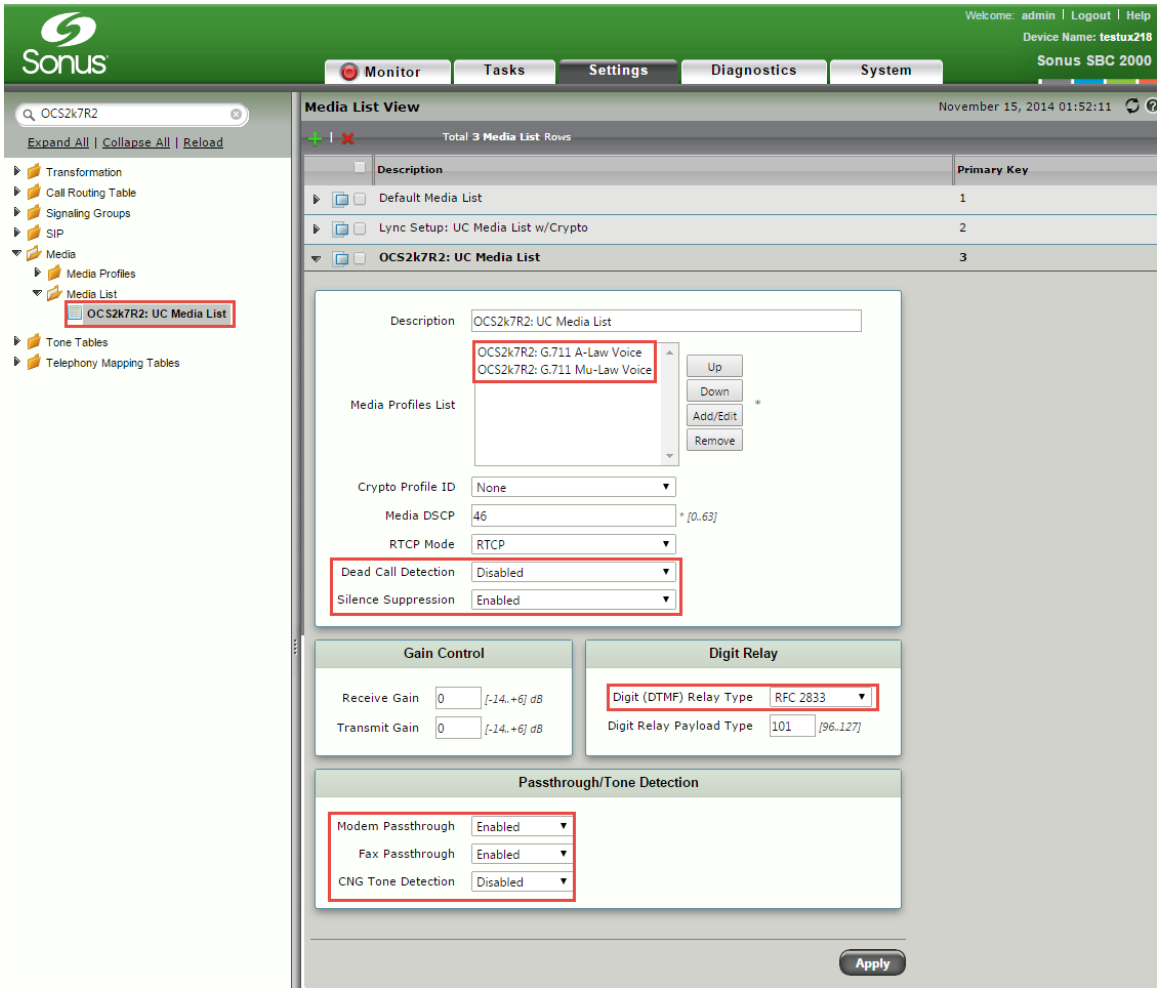


Media Profiles

Copyright © 2015 Sonus Networks. All rights reserved.

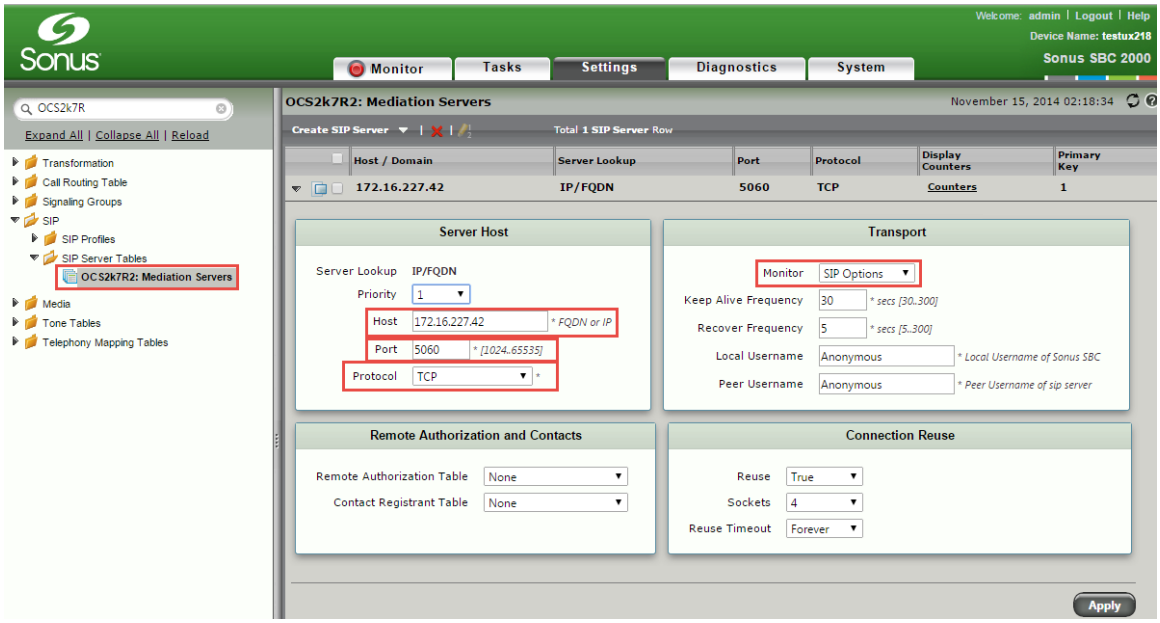


Media List

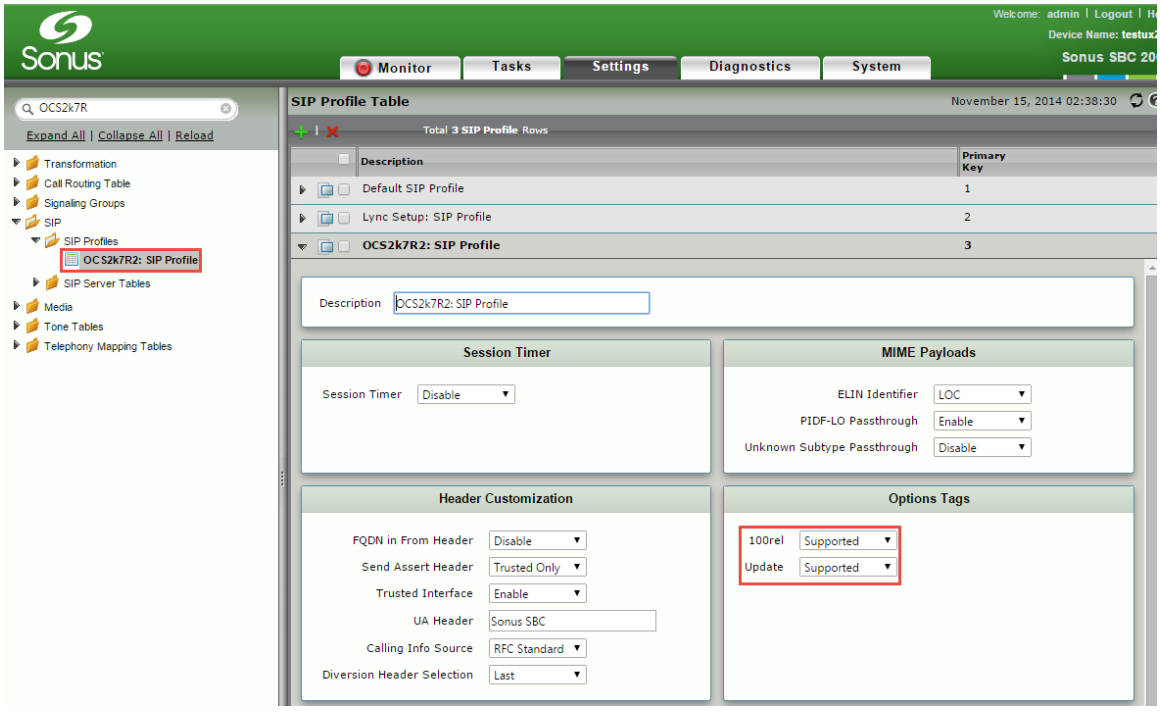


Copyright © 2015 Sonus Networks. All rights reserved.

SIP Server Table

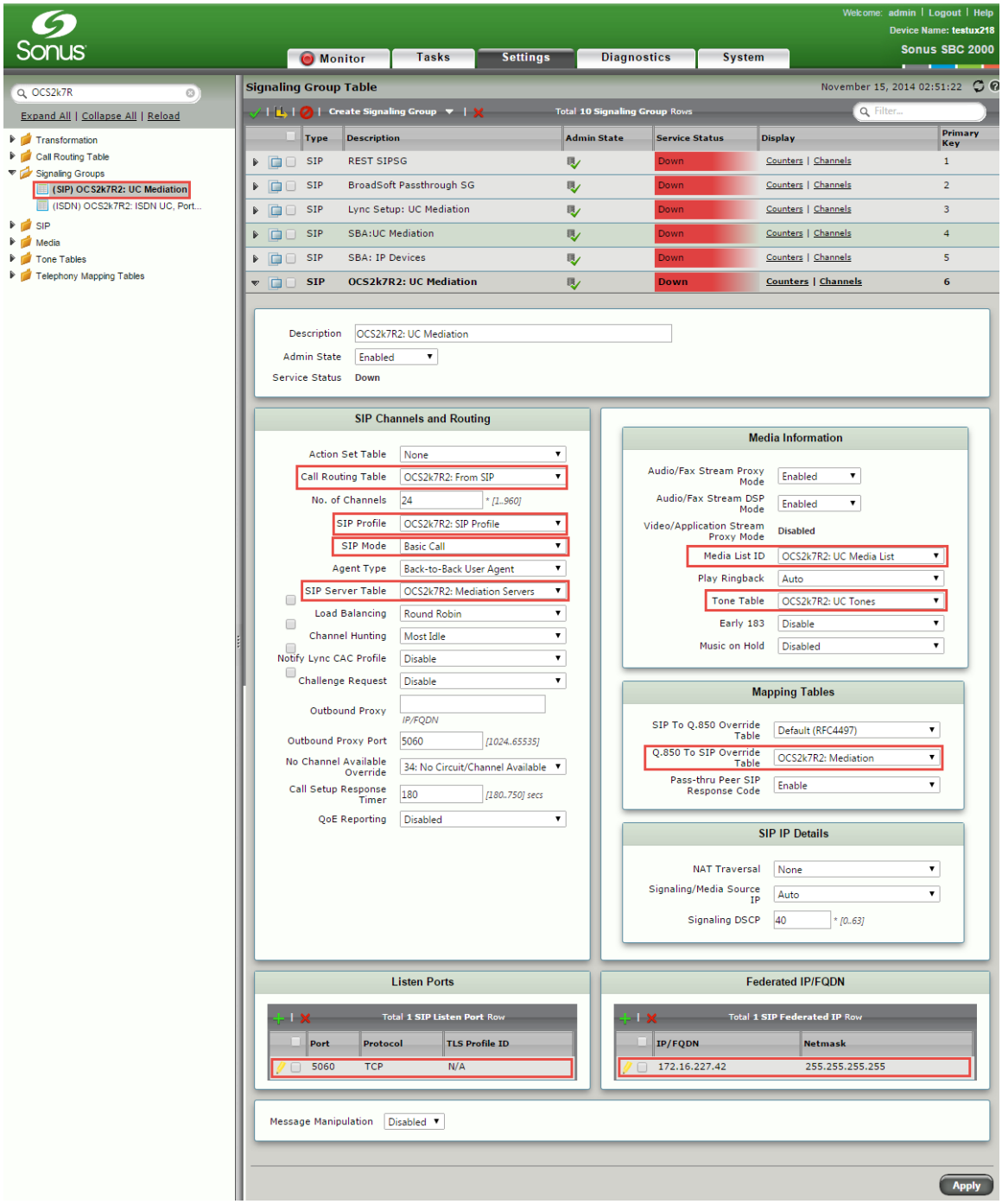


SIP Profile



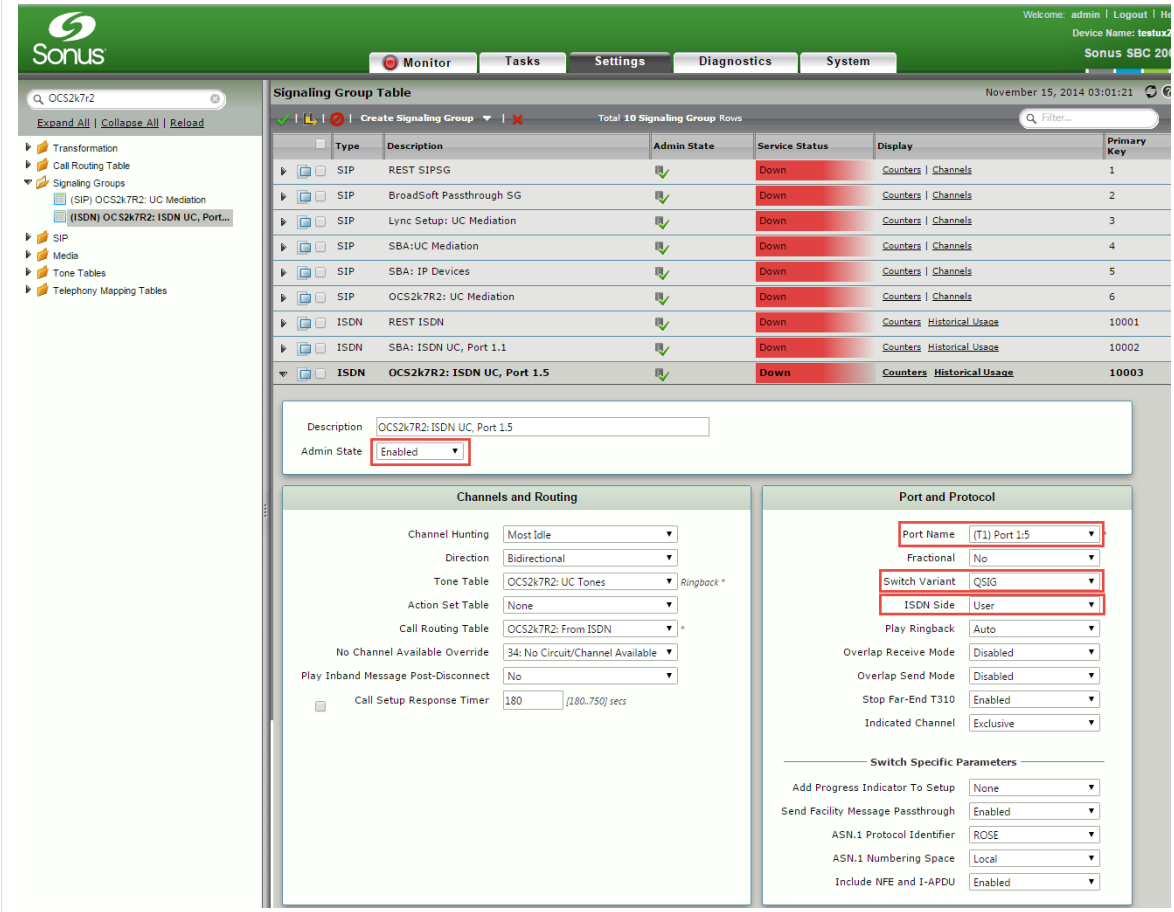
SIP Signaling Groups

Copyright © 2015 Sonus Networks. All rights reserved.



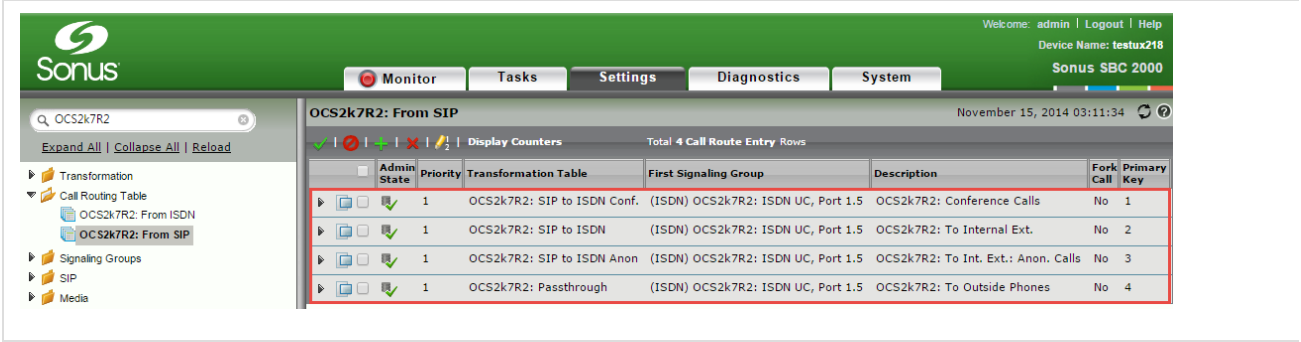
ISDN Signaling Group

Copyright © 2015 Sonus Networks. All rights reserved.



Call Routing Tables

- **SIP to ISDN Call Routing Table**



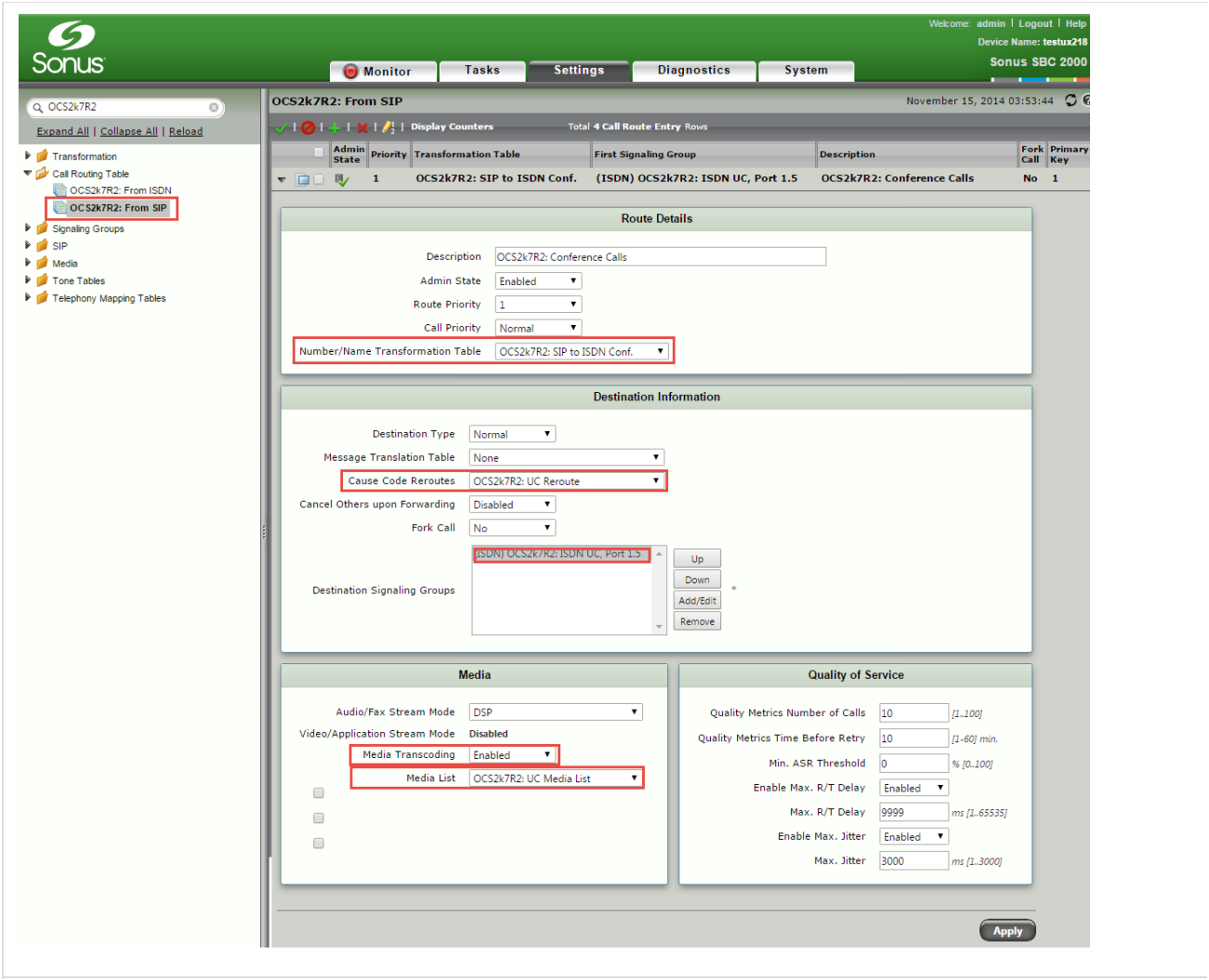
The **OCS2k7R2: SIP to ISDN** Routing Table contains the following four entries:

- OCS2k7R2: SIP to ISDN Conf.
- OCS2k7R2: SIP to ISDN
- OCS2k7R2: SIP to ISDN Anon
- OCS2k7R2: To Outside Phones

The details of each entry are shown below:

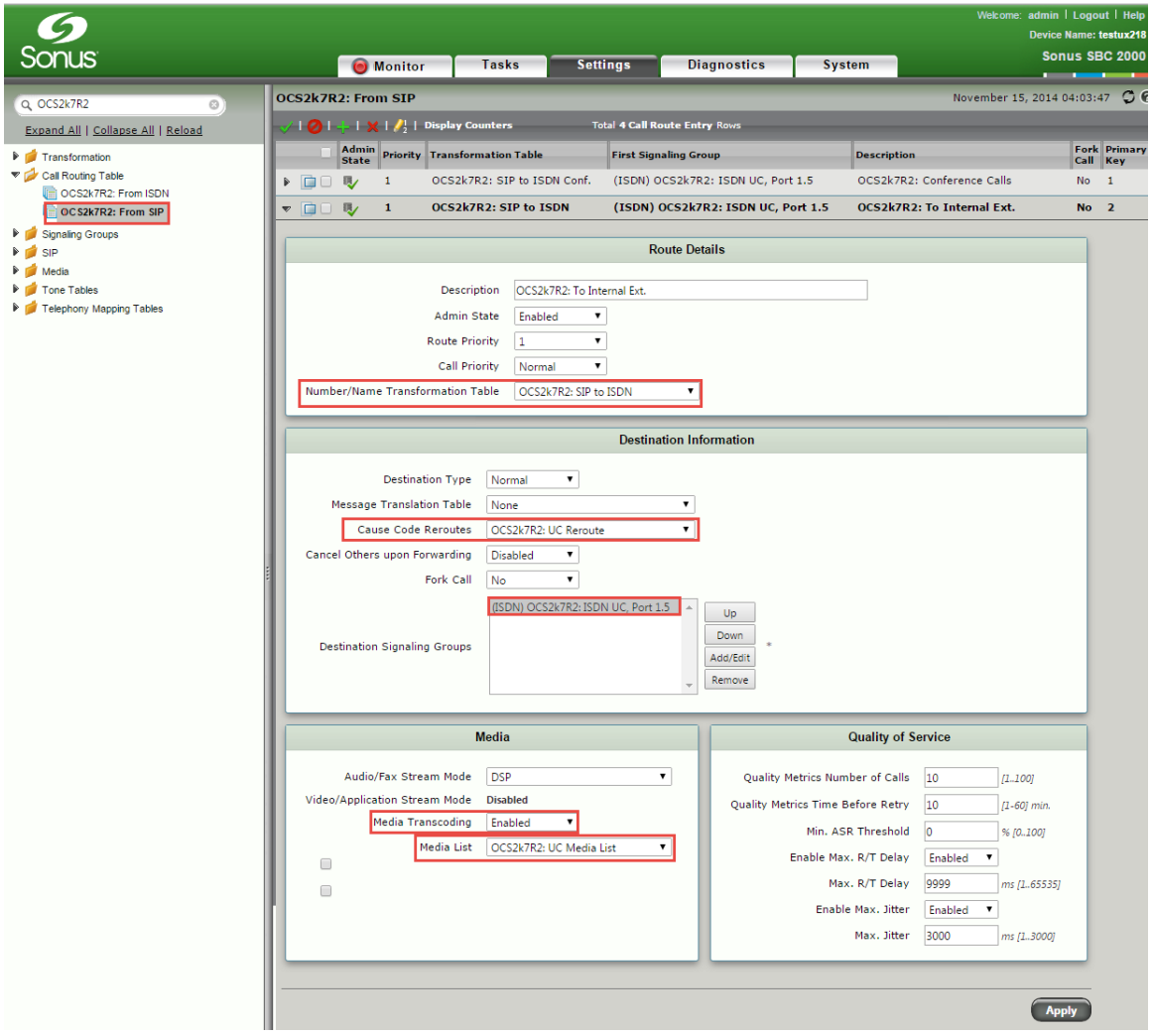
- OCS2k7R2:Conference Calls

Copyright © 2015 Sonus Networks. All rights reserved.



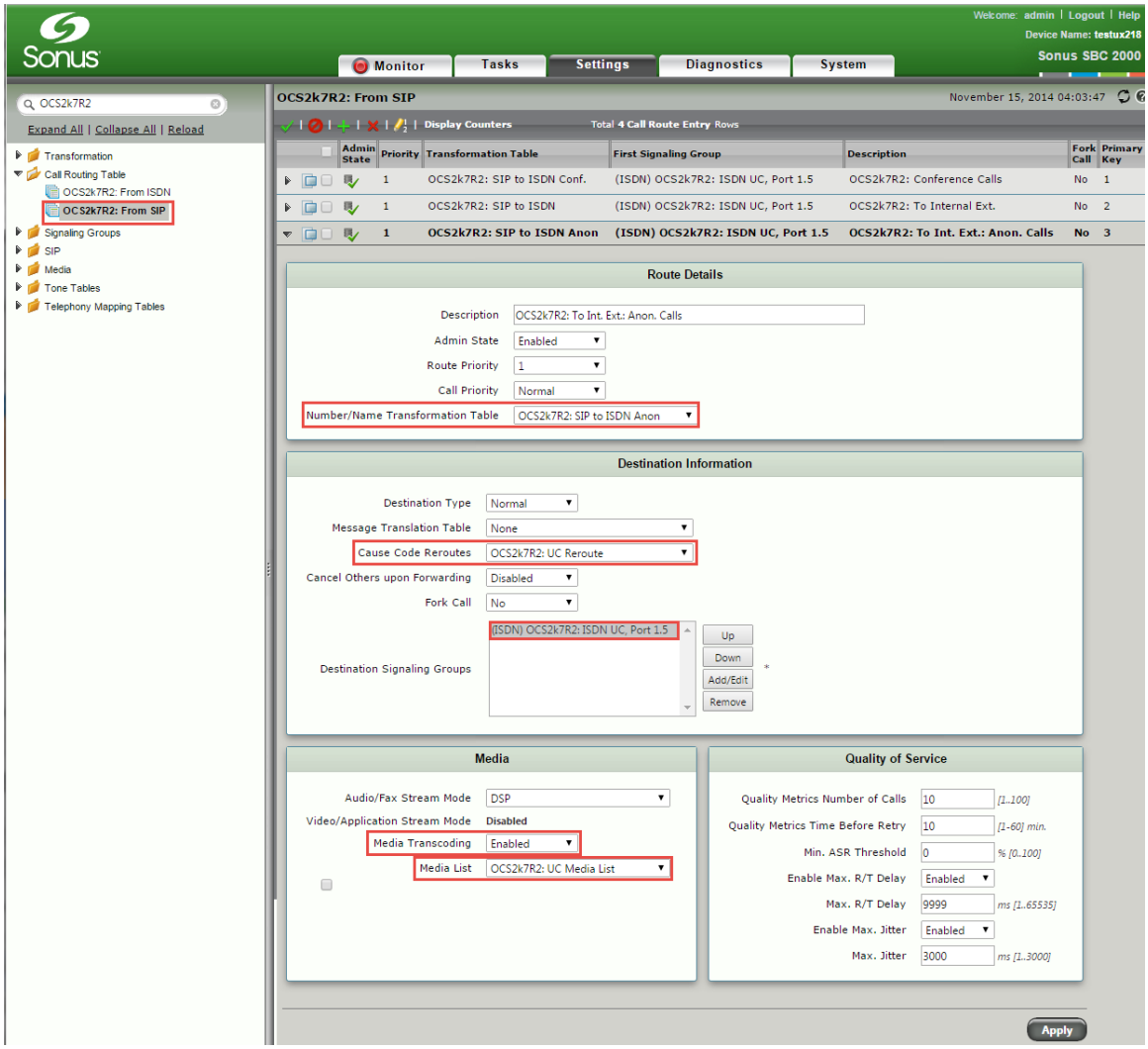
- OCS2k7R2: To Internal Ext.

Copyright © 2015 Sonus Networks. All rights reserved.



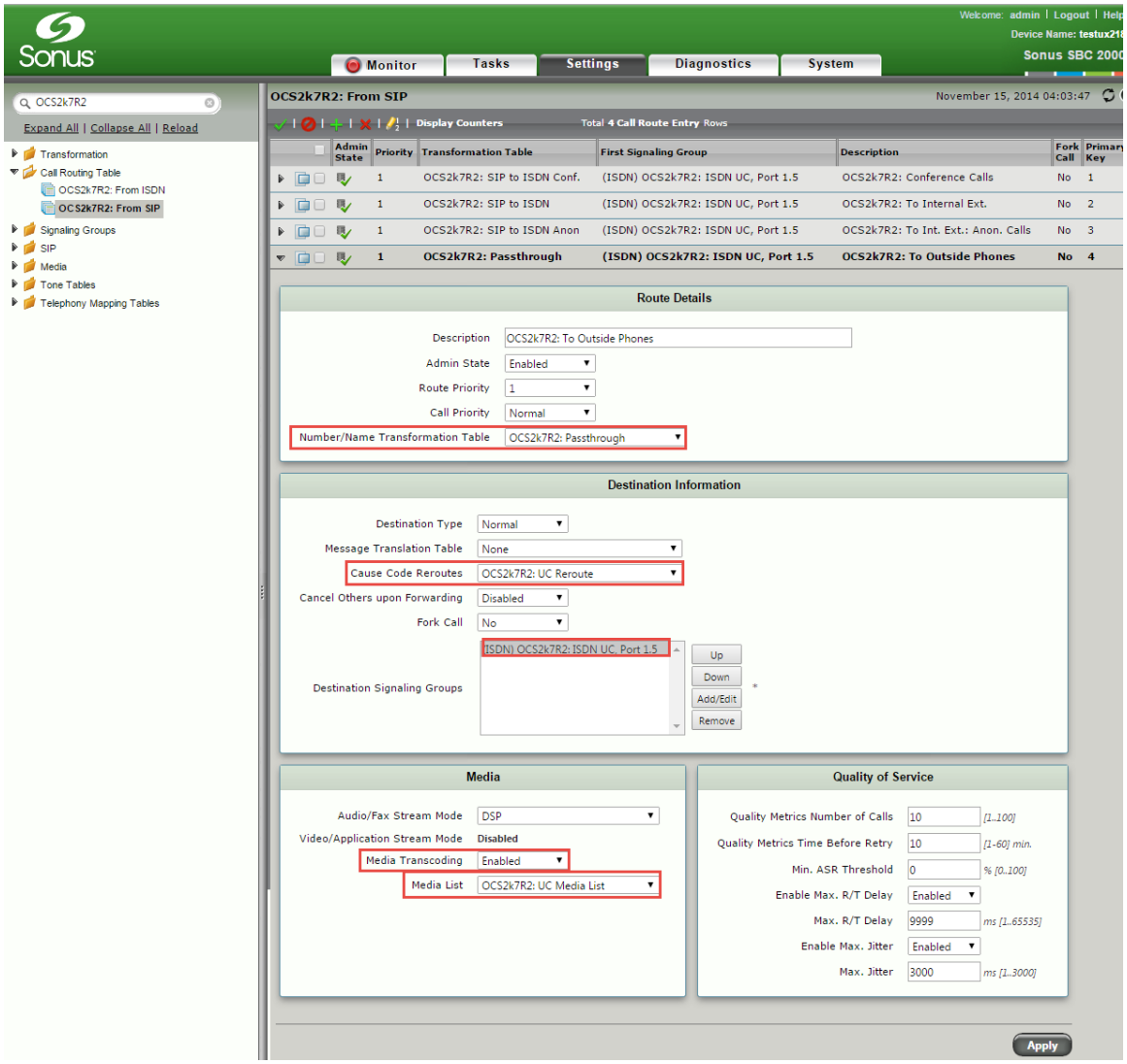
- OCS2k7R2: To Int.Ext.:Anon Calls

Copyright © 2015 Sonus Networks. All rights reserved.

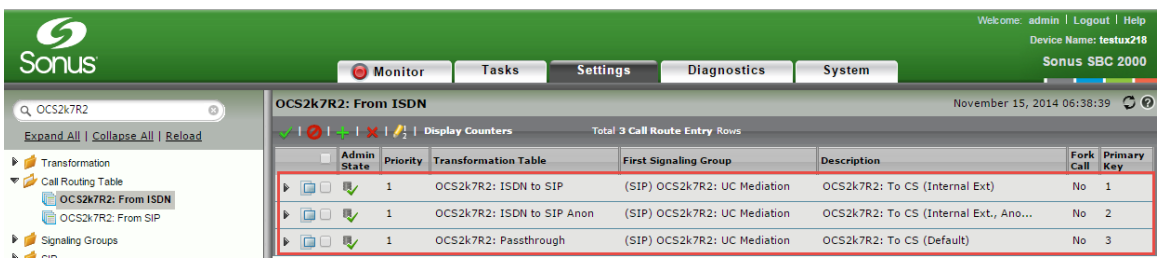


- OCS2k7R2: To Outside Phones

Copyright © 2015 Sonus Networks. All rights reserved.



- **ISDN to SIP Call Routing Table**



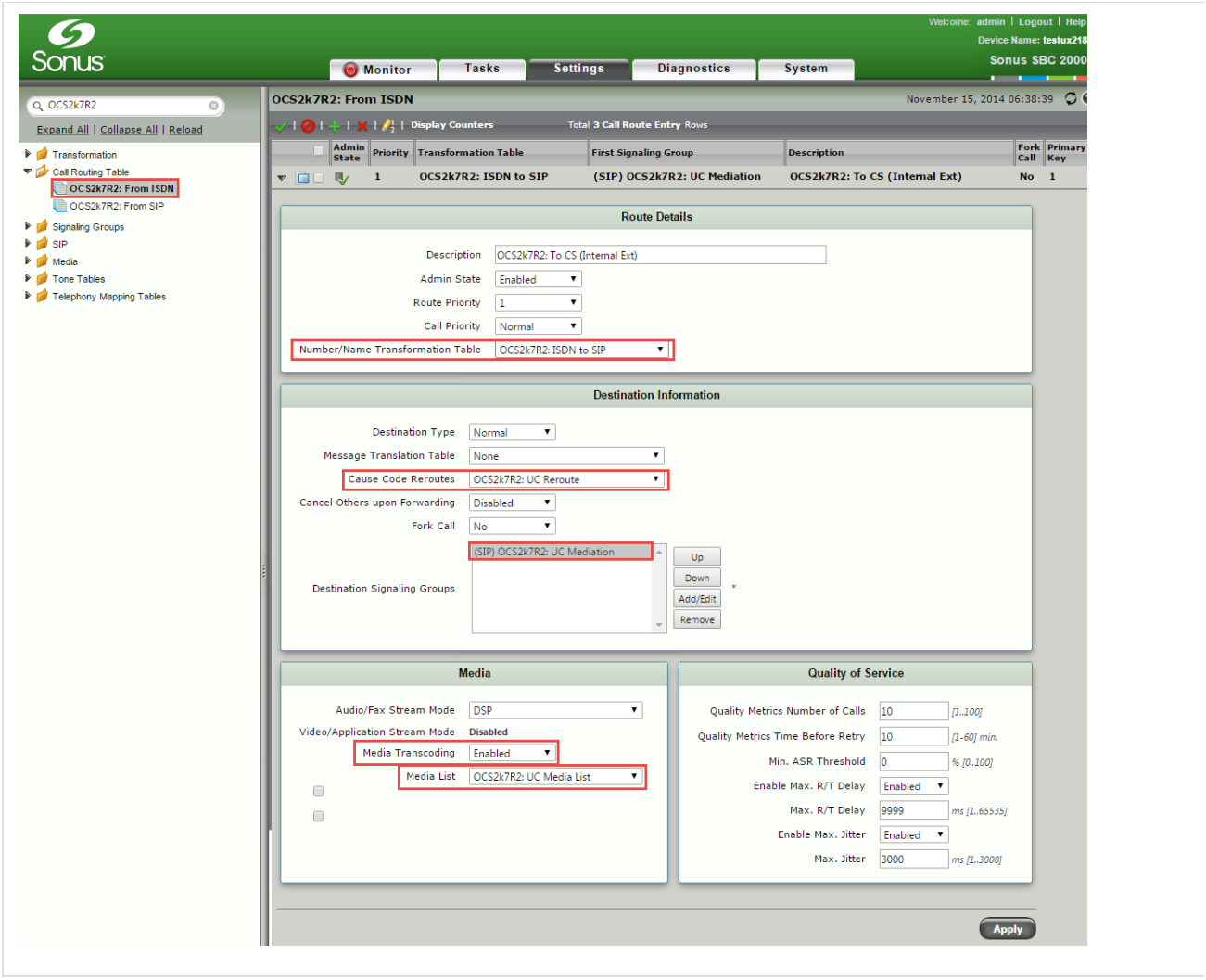
The **OCS2k7R2: ISDN to SIP** Routing Table contains the following three entries:

- OCS2k7R2: To CS (Internal Ext.)
- OCS2k7R2: To CS (Internal Ext., Anon.)
- OCS2k7R2: To CS (Default)

The details of each entry are shown below

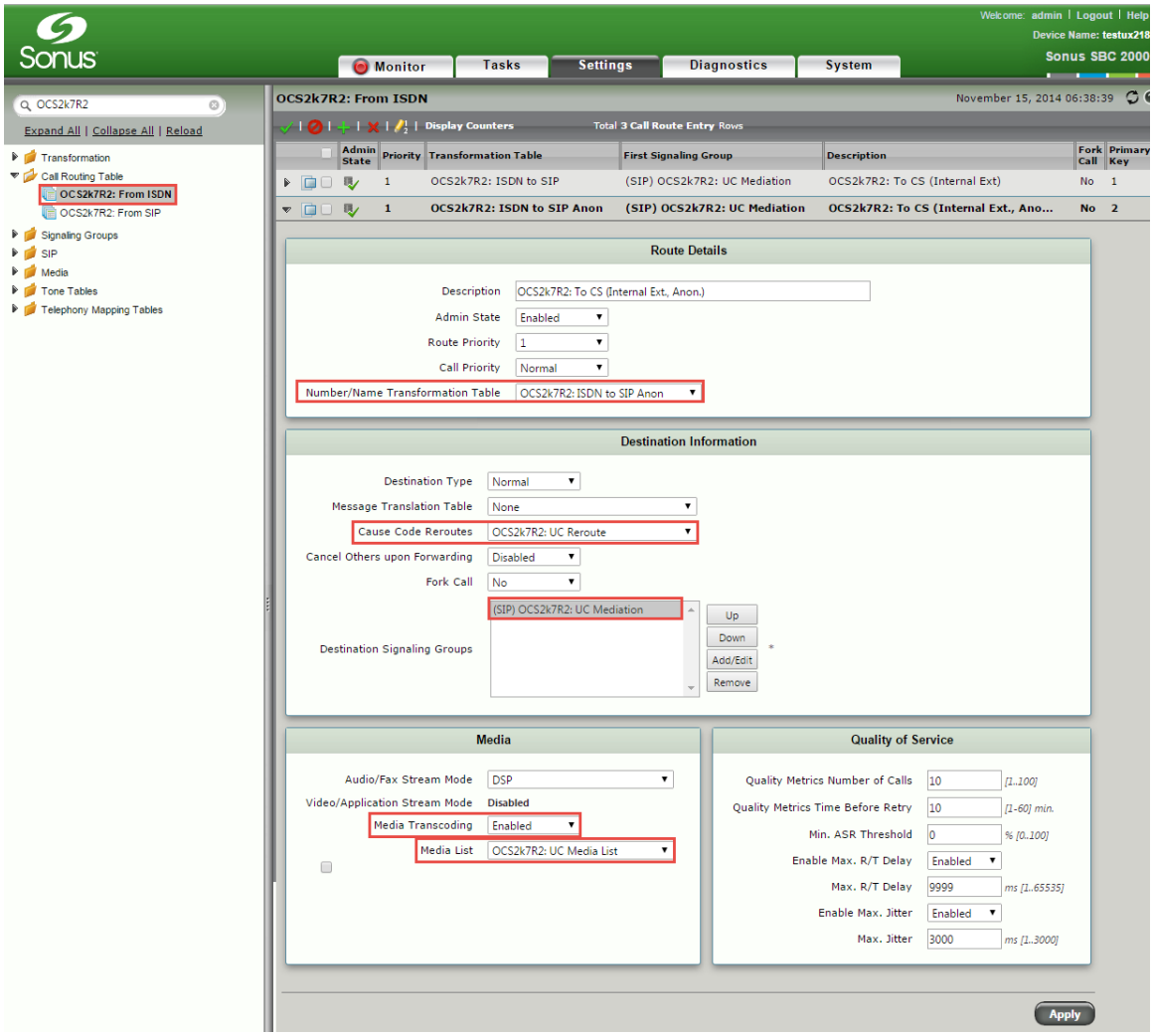
- OCS2k7R2: To CS (Internal Ext.)

Copyright © 2015 Sonus Networks. All rights reserved.



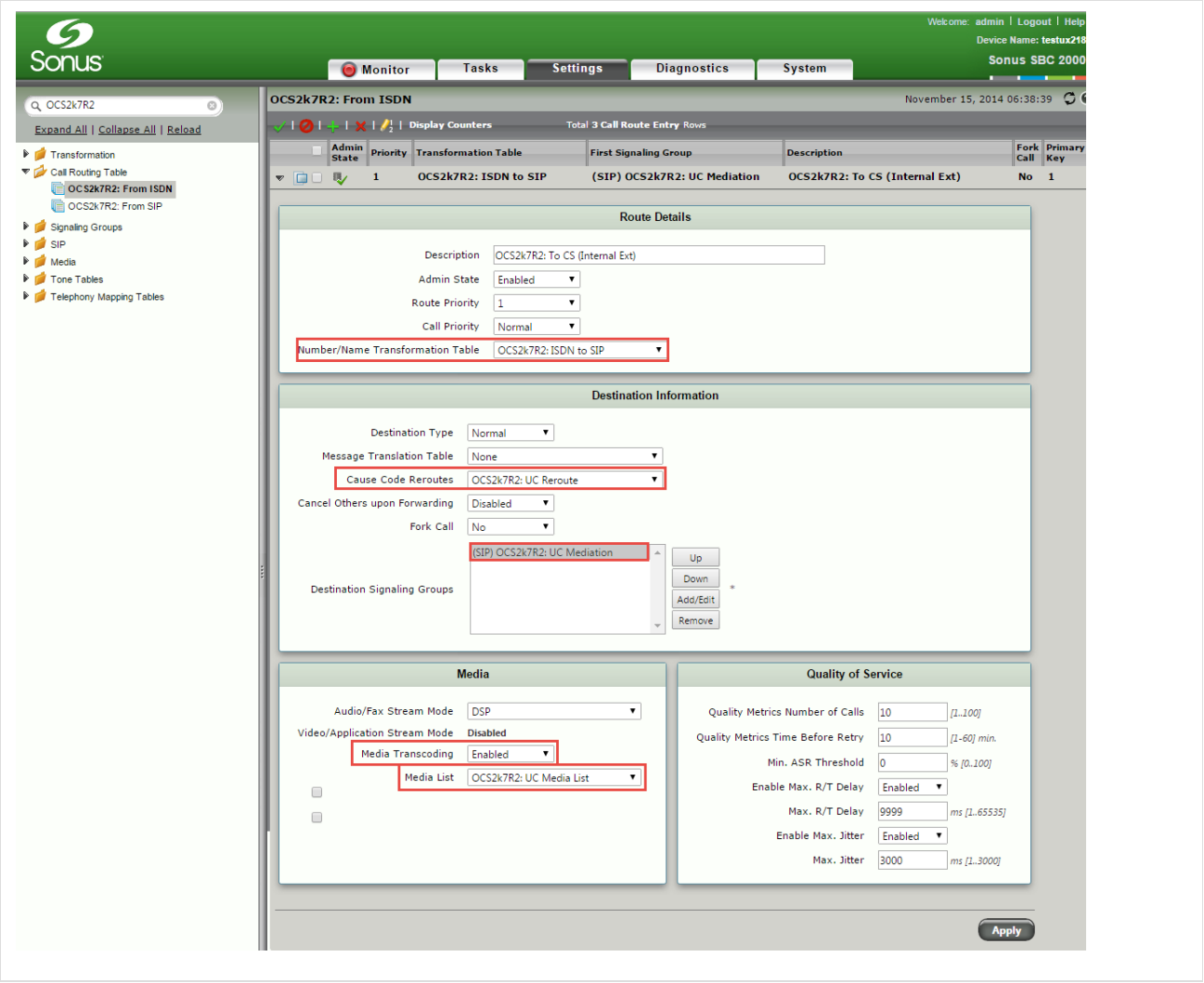
- OCS2k7R2: To CS (Internal Ext., Anon.)

Copyright © 2015 Sonus Networks. All rights reserved.

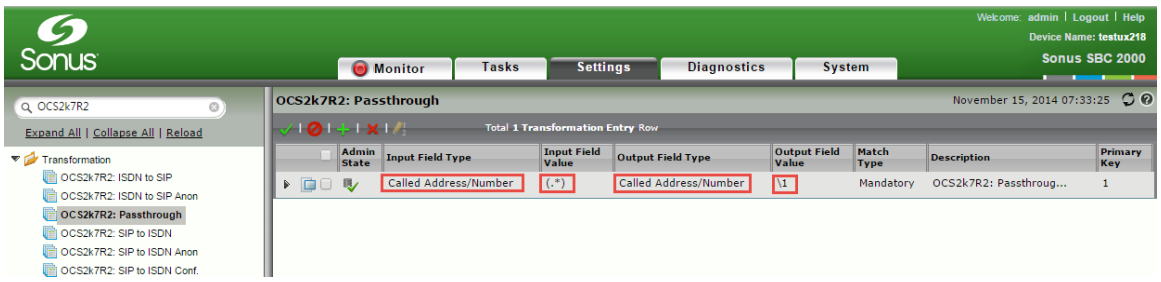


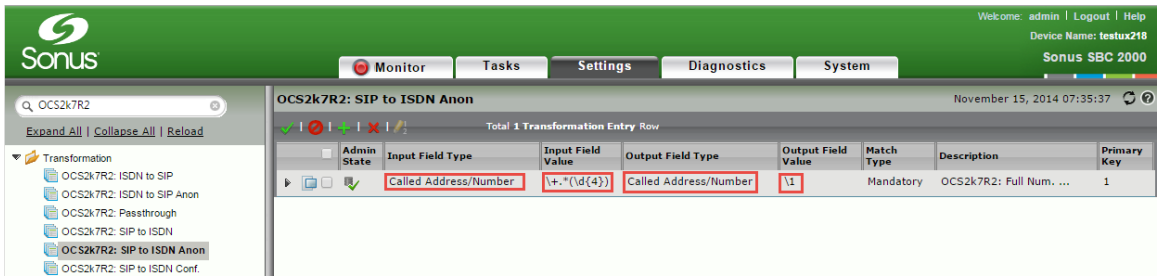
- OCS2k7R2: To CS (Default)

Copyright © 2015 Sonus Networks. All rights reserved.

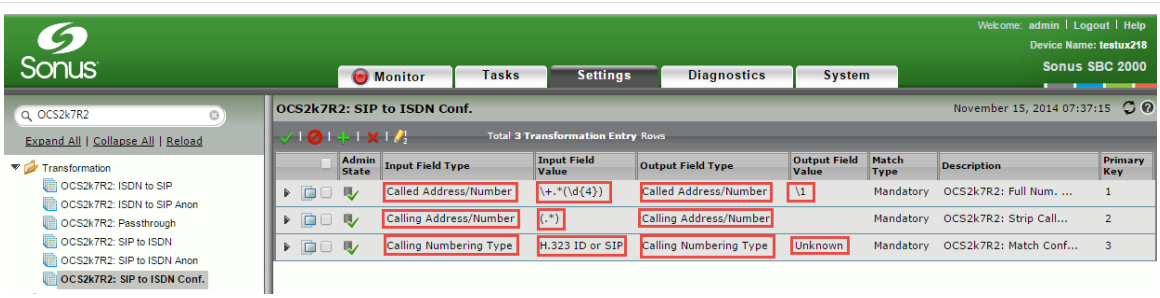


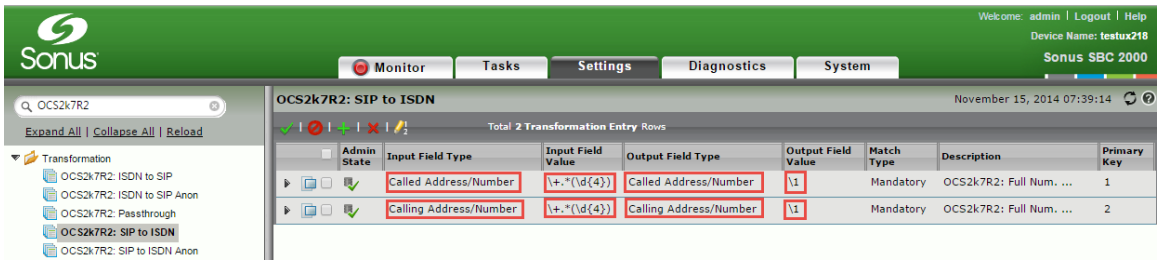
SIP to ISDN and ISDN to SIP Number Transformation Tables

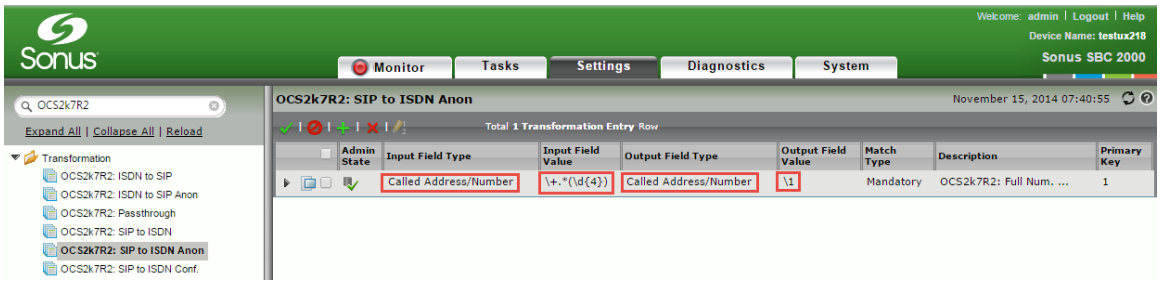


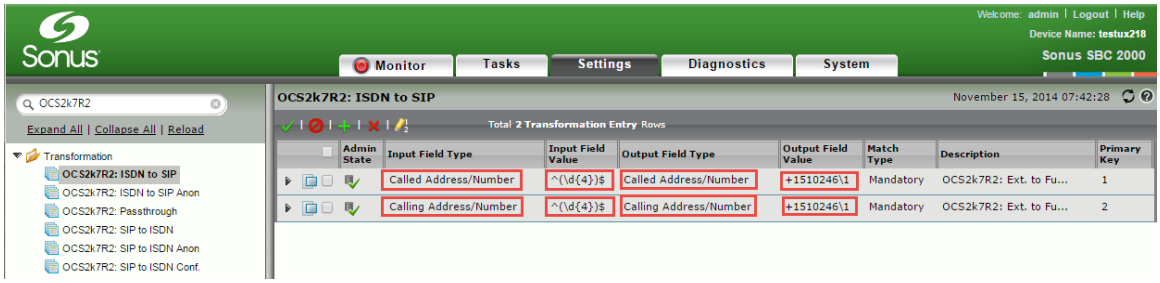


Copyright © 2015 Sonus Networks. All rights reserved.







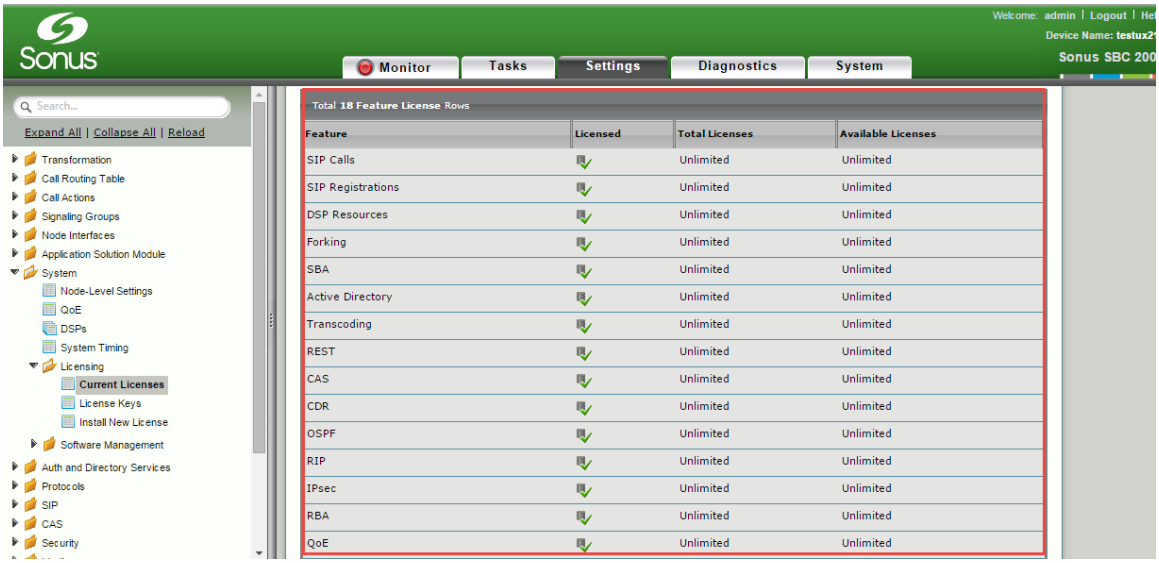


Sonus SBC 1000/2000 Verification Steps

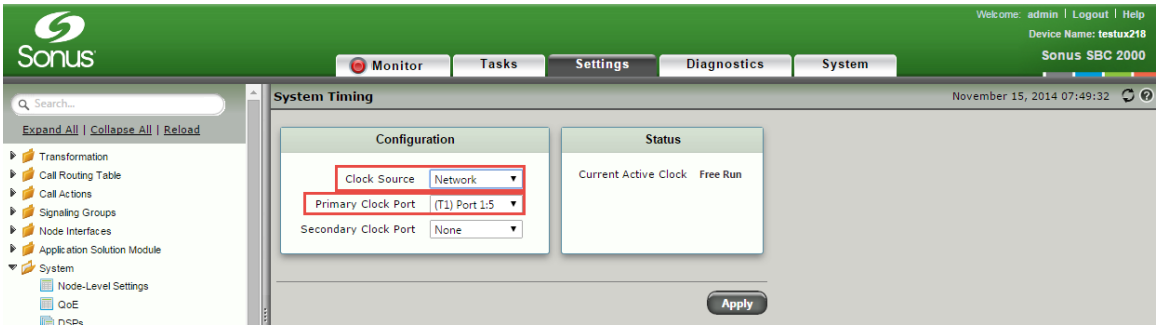
Before attempting to establish calls, it is good practice to check the available Sonus SBC 1000/2000 licenses, PSTN connectivity, and the System Clock Source:

- **Licensing**

Copyright © 2015 Sonus Networks. All rights reserved.

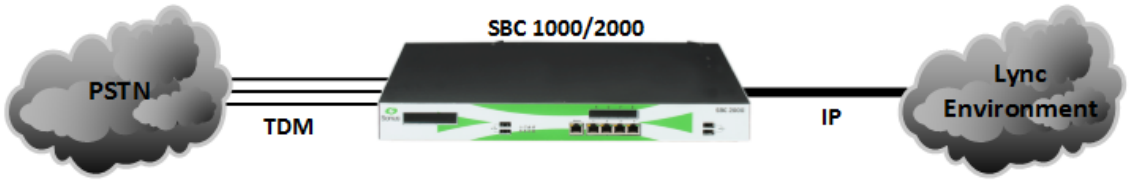


- **System Timing**(System Clock Source)



Microsoft Lync Server 2010 Quick Start Guide

UX acts as a Survivable Branch Appliance (SBA) and a gateway for Microsoft Lync 2010 Server to Public Switched Telephone Networks (PSTN), Private Branch Exchanges (PBX), and to ITSP, while improving resiliency and providing the ability for Microsoft Unified Communications users to collaborate with people outside the Unified Communications network.



This guide explains how to configure UX as Microsoft Lync Server 2010 Survivable Branch Appliance.

On this Page

- Before you Begin
- Procedure
  - Configuring the Lync 2010 Server - Dial Plan and Gateway
  - Creating a Lync 2010 User

Copyright © 2015 Sonus Networks. All rights reserved.

Related Articles

- Lync Setup
- Working with the ASM and SBA

Before you Begin

The following information should be gathered prior to performing this procedure.

- The IP Address or FQDN of the Active Directory machine.
- The IP Address or FQDN of the ASM.
- The computer name of the ASM module.
- Valid login credentials for the AD machine.
- A name for the SBA Installer account you are creating.
- The IP Address or FQDN of the Lync Server.
- A name for the branch site.
- The site details (City, State, Country/Region Code).
- The FQDN of Front End Pool assigned to the SBA.
- The FQDN of Edge Pool assigned to the SBA (If you have an Edge Server).
- The IP Address or FQDN of the PSTN Gateway to be used by the mediation Server.
- The listening port on the IP/PSTN gateway.
- The SIP Transport Protocol used (TCL or TLS).

Procedure

The following steps comprise the general procedure for configuration and deployment.

1. Verify the DNS Server has been configured and that there is an entry for the UX.
2. Running the Initial Setup on your UX, if you have not already done so.
3. Upgrade your SBC software. Before you proceed with the next steps be sure that you have installed the latest version of the UX softwares.
4. Deploy the SBA. This procedure guides you through the both Central Site and Branch Site tasks.
5. Use the Lync Setup Wizard in the UI to configure the Lync&#8482 Server.
6. Create a user in Lync 2010.
7. Configure Lync 2010. This procedure guides you through the voice routing configuration of your SBA.
8. Make a Lync test call.

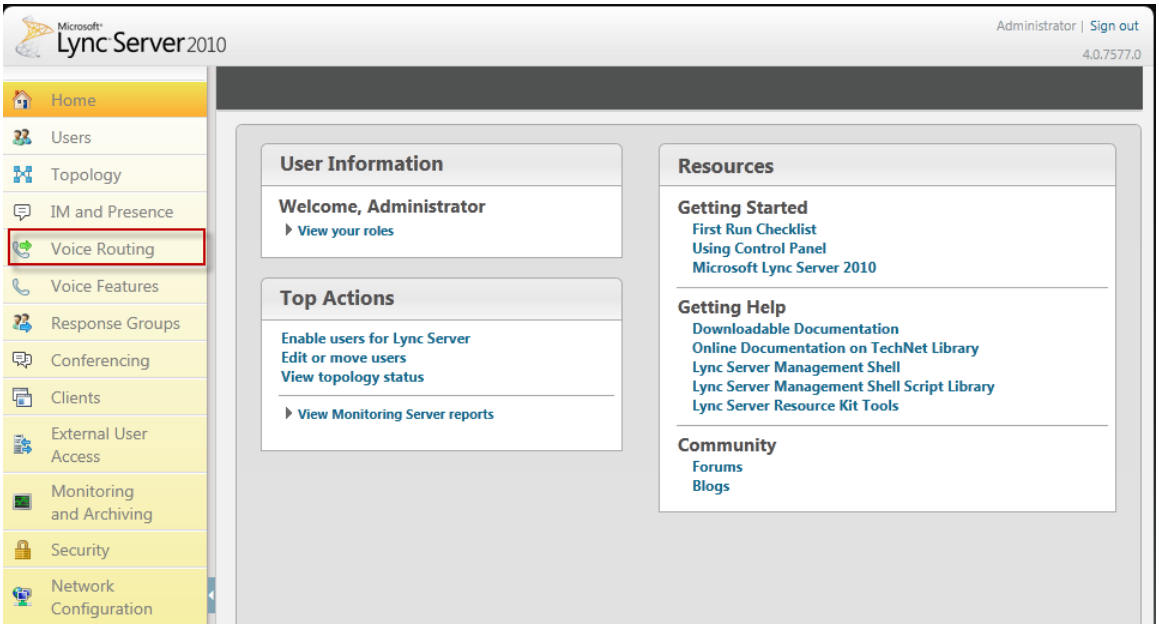
Configuring the Lync 2010 Server - Dial Plan and Gateway

Creating a Lync 2010 User

Configuring the Lync 2010 Server - Dial Plan and Gateway

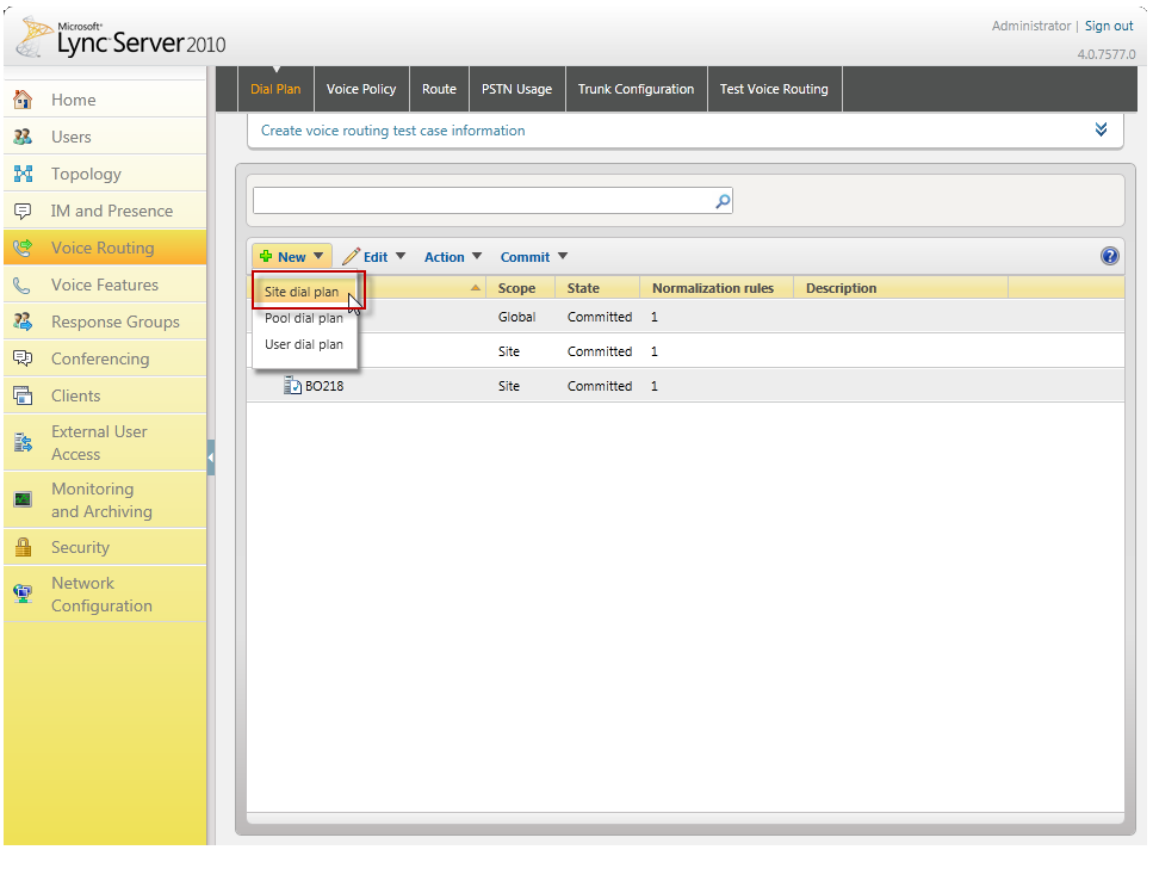
1. Connect to the Microsoft Lync 2010 Front End Server.
   There are two methods:
   a. Connect via Remote Desktop, or
   b. Connect via your web browser (https:\\<Server FQDN>\CSCP)
2. Launch the Lync Server Control panel.

Copyright © 2015 Sonus Networks. All rights reserved.



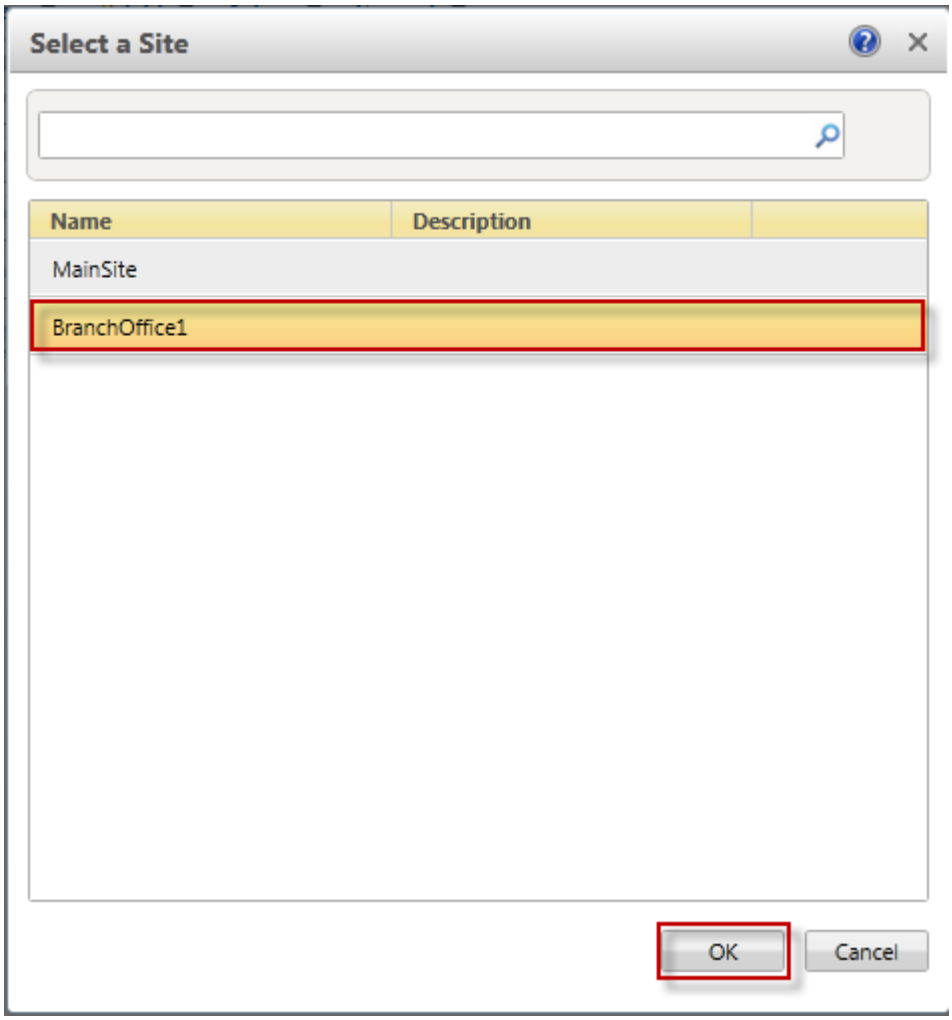
Adding a Dial Plan

1. Select **Voice Routing**



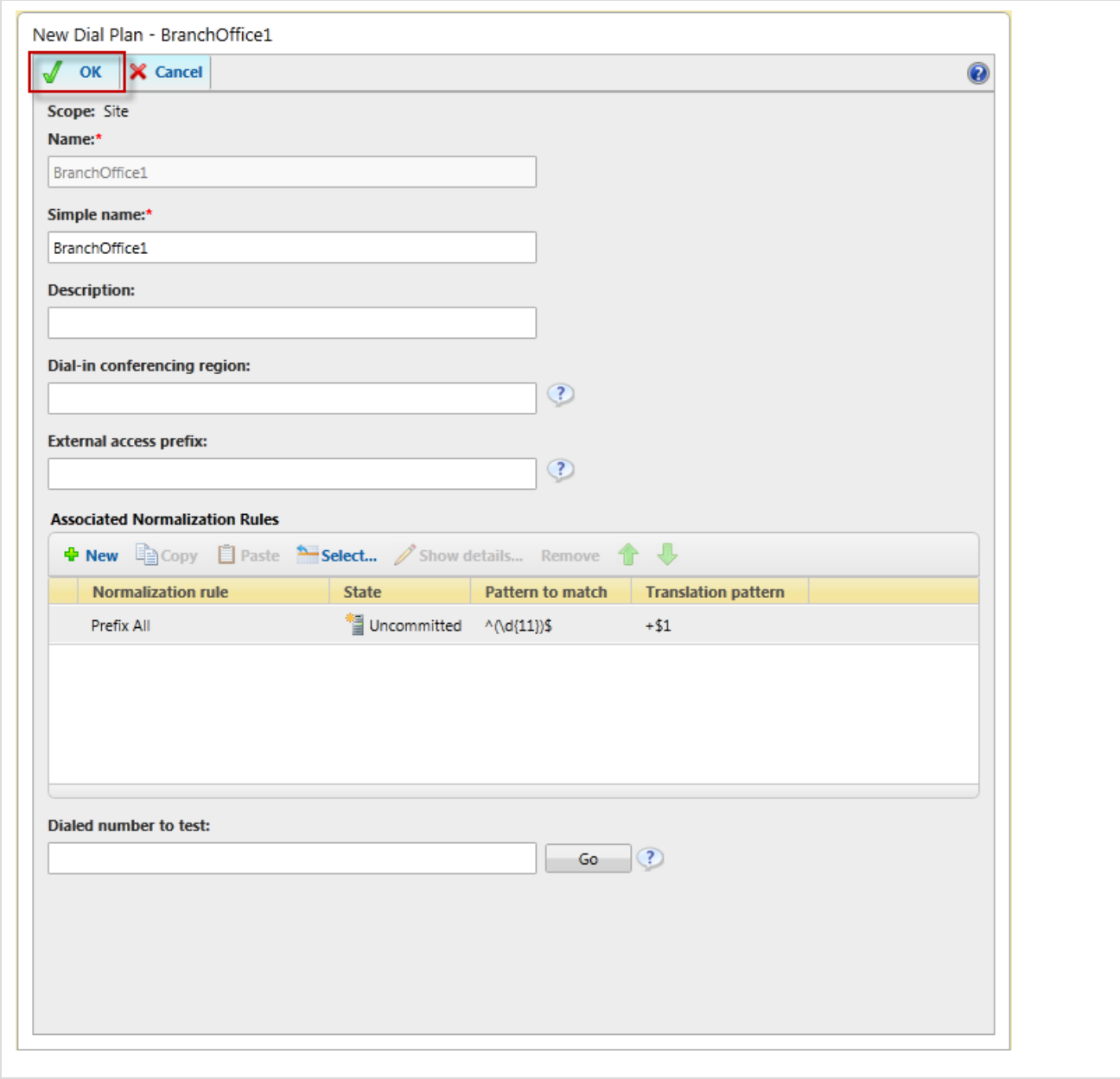
2. In the **New** menu, click **Site dial plan**.

Copyright © 2015 Sonus Networks. All rights reserved.



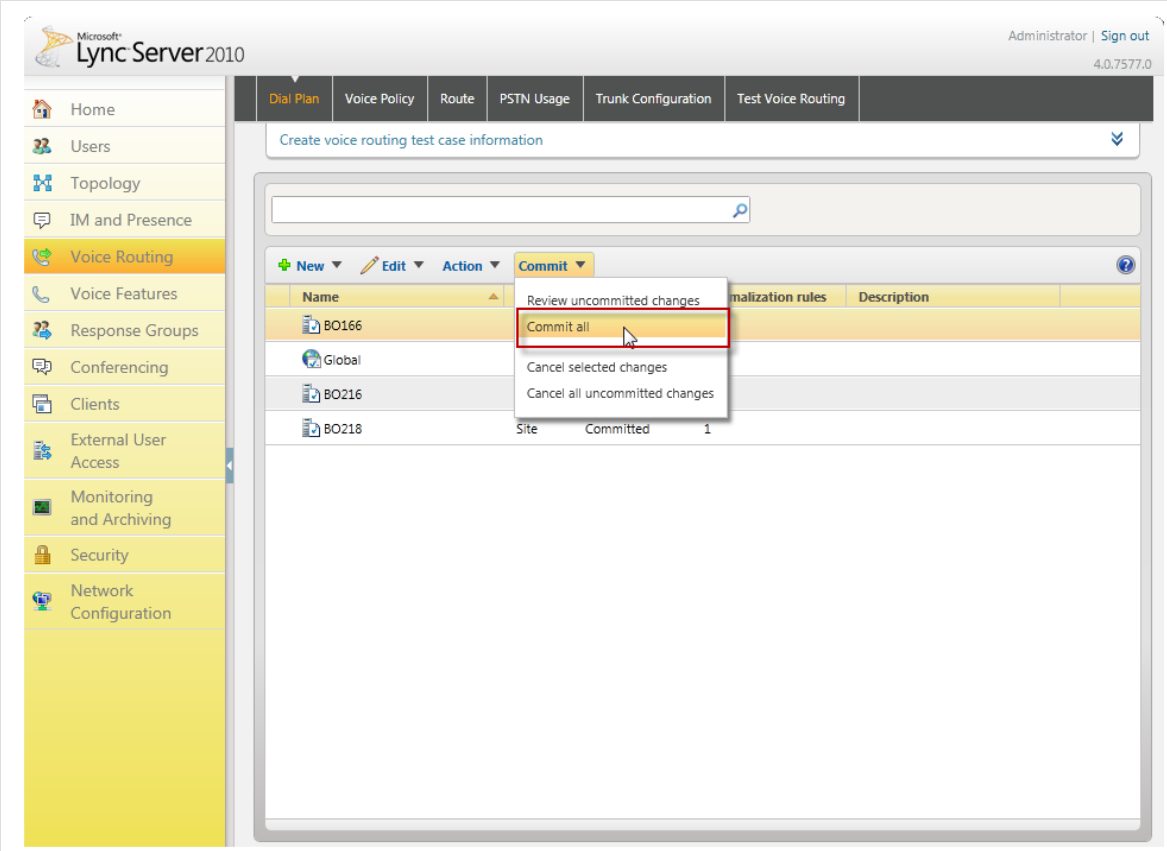
3. Select your Site location.
4. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.



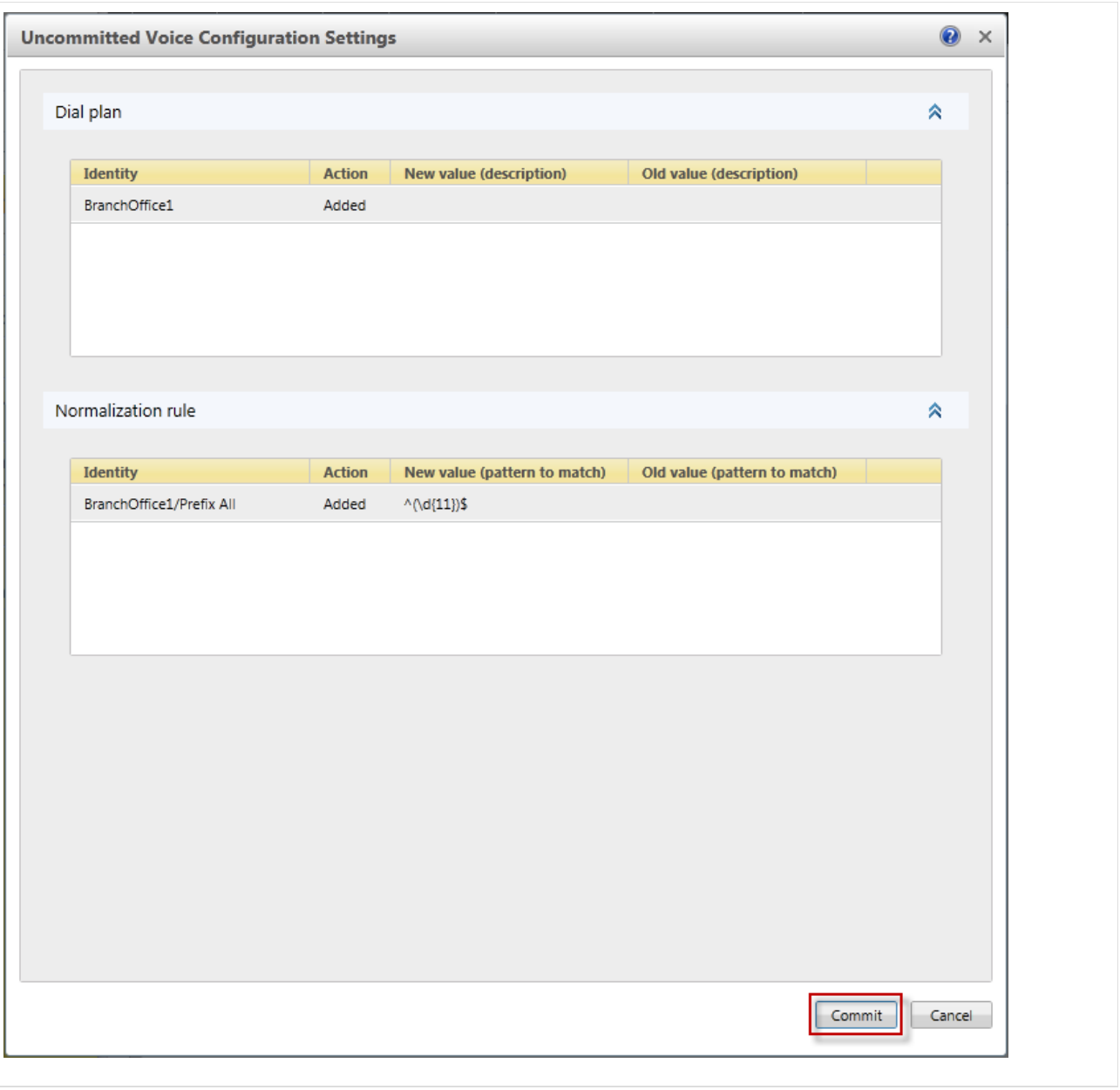
5. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.



6. In the **Commit** menu, click **Commit all**

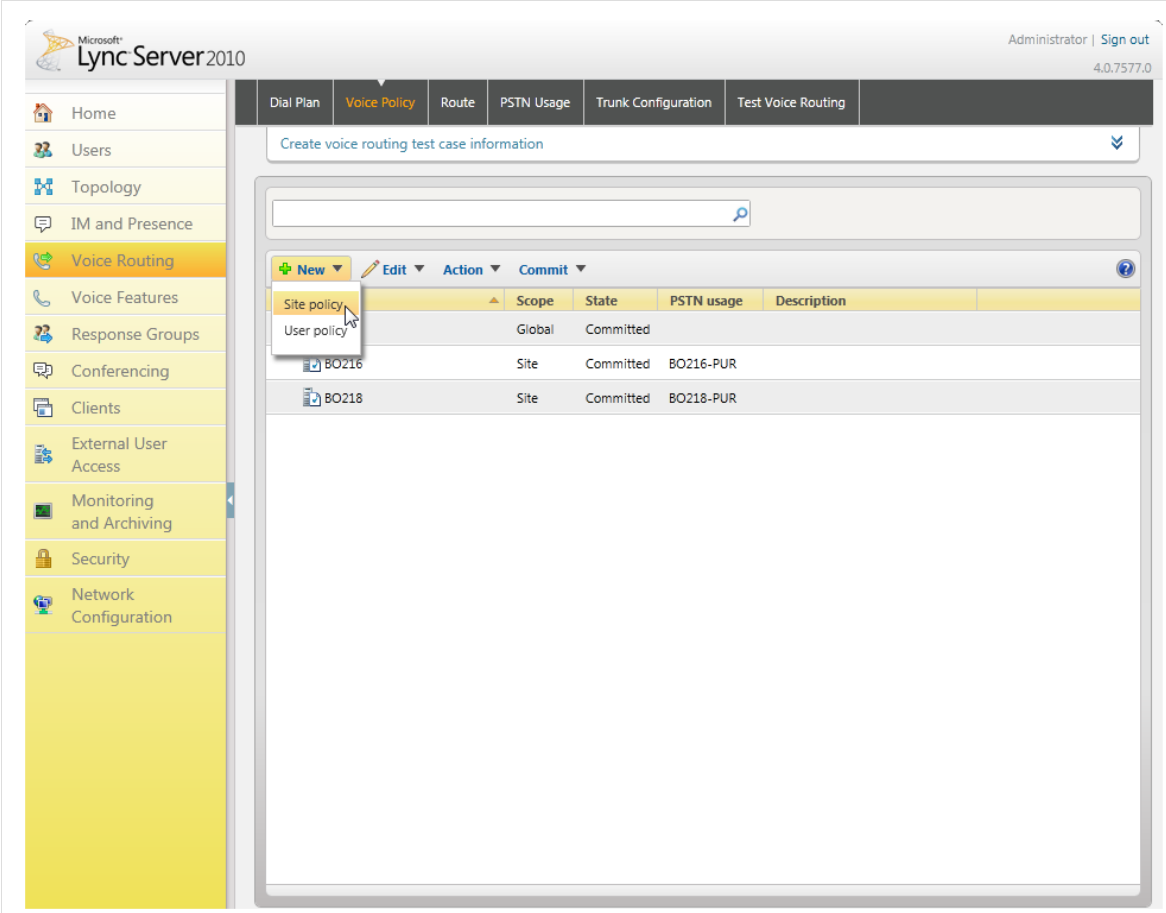
Copyright © 2015 Sonus Networks. All rights reserved.



7. Click **Commit**.
8. Click **Close**.

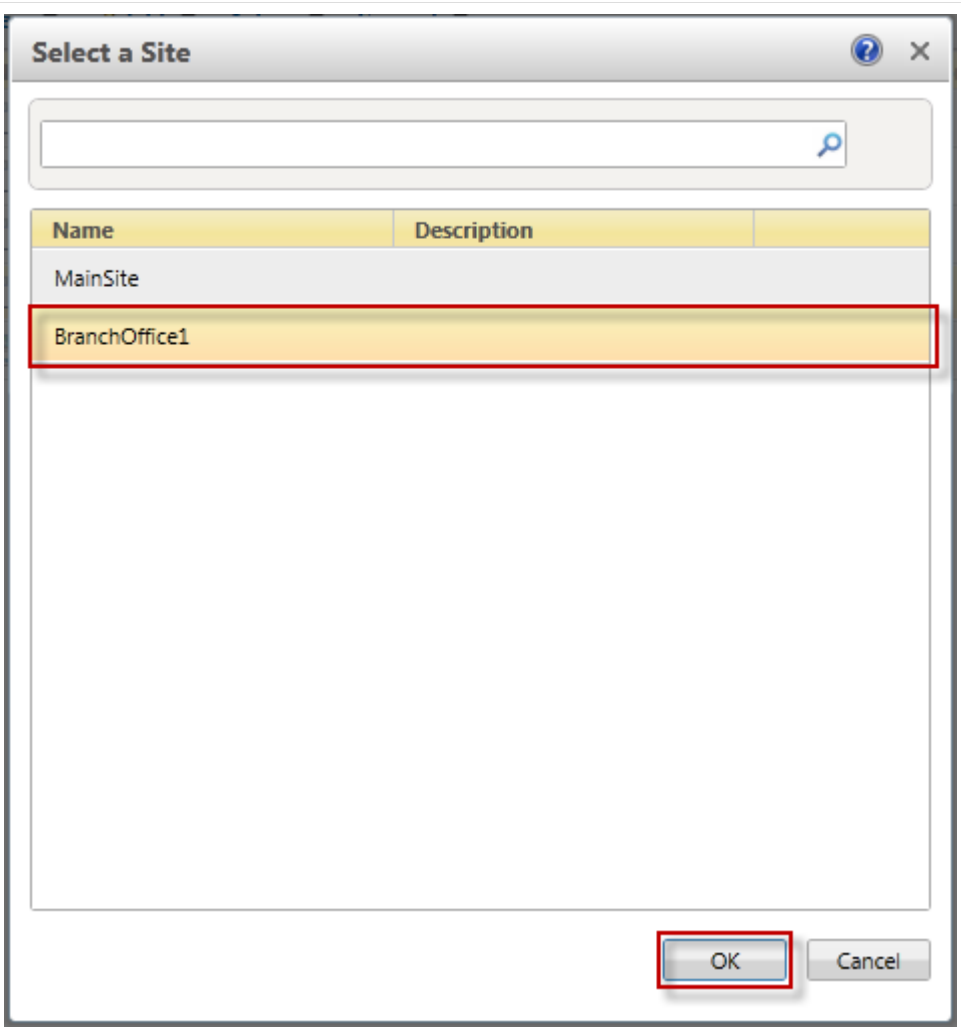
Adding a Voice Policy

Copyright © 2015 Sonus Networks. All rights reserved.



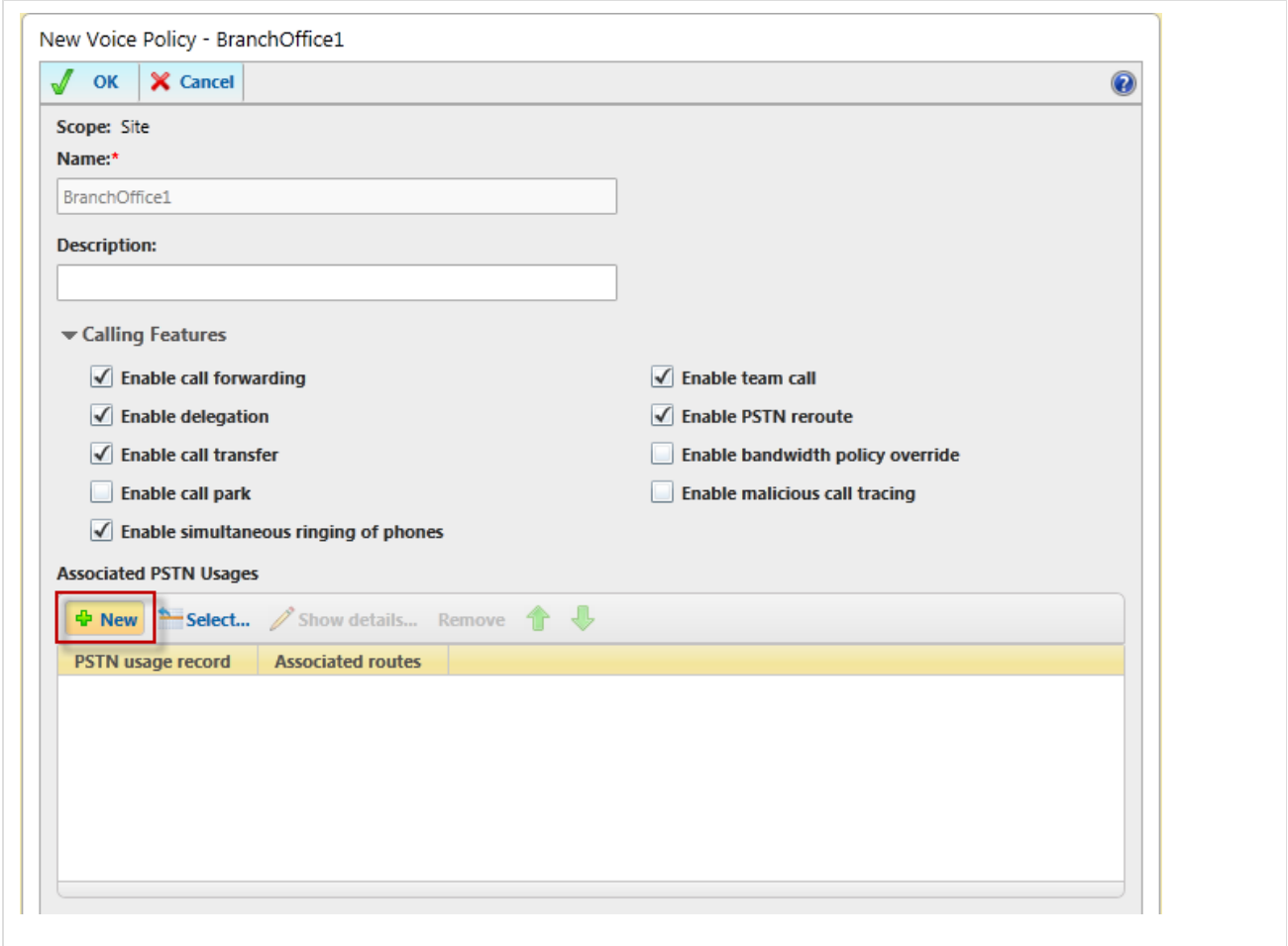
1. Click the voice Policy Tab
2. In the **New** menu, click **Site policy**.

Copyright © 2015 Sonus Networks. All rights reserved.

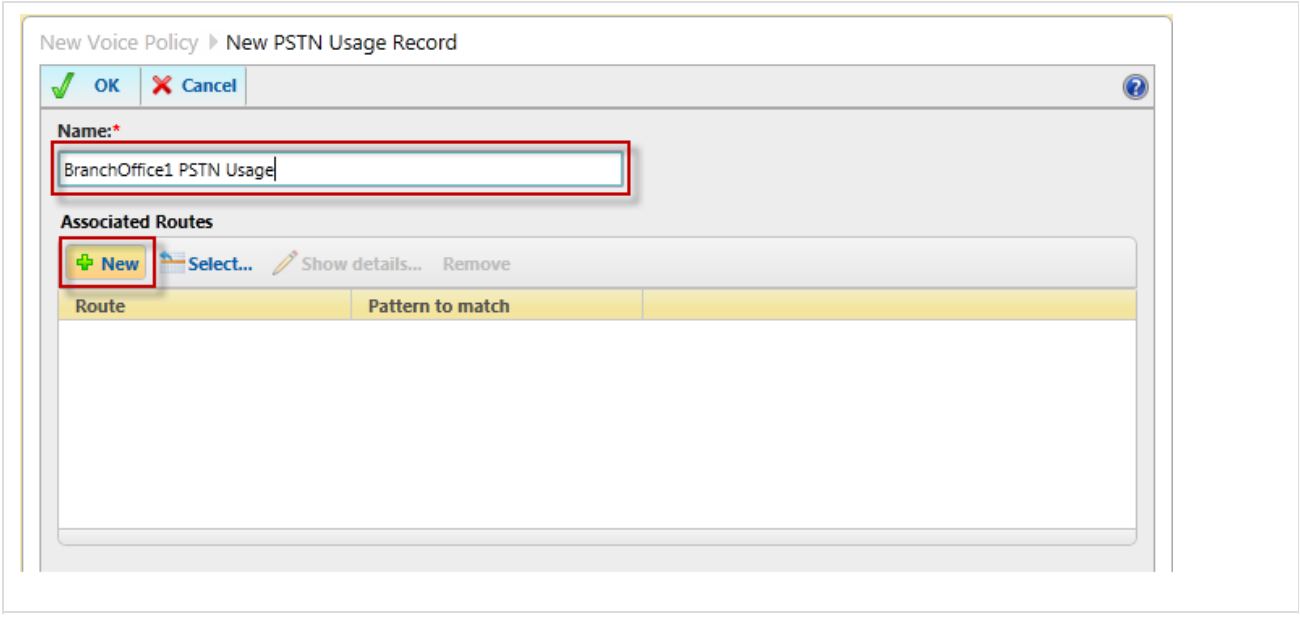


3. Select the Site location.
4. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.

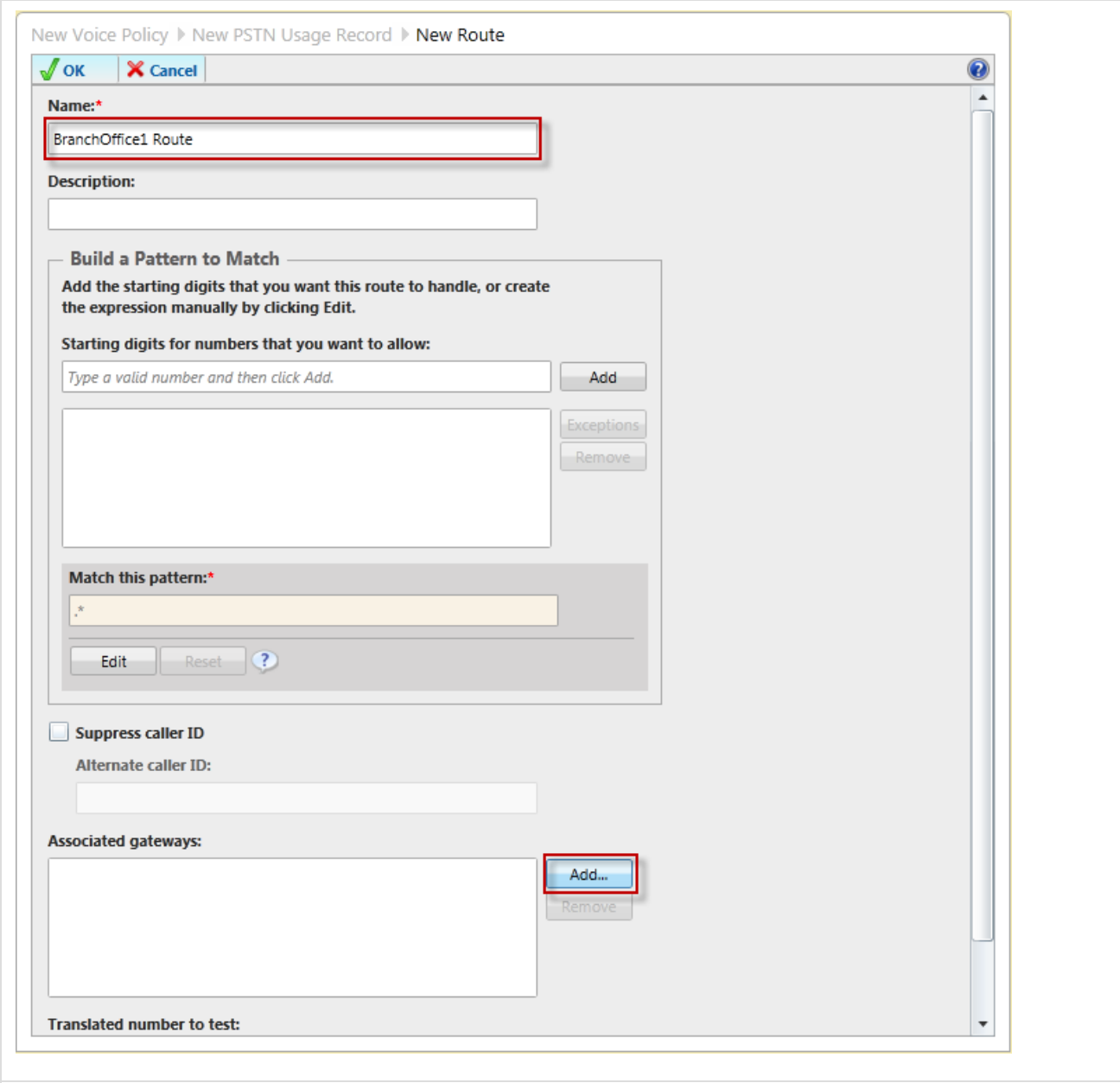


5. Under **Associated PSTN Usages**, click **New**.



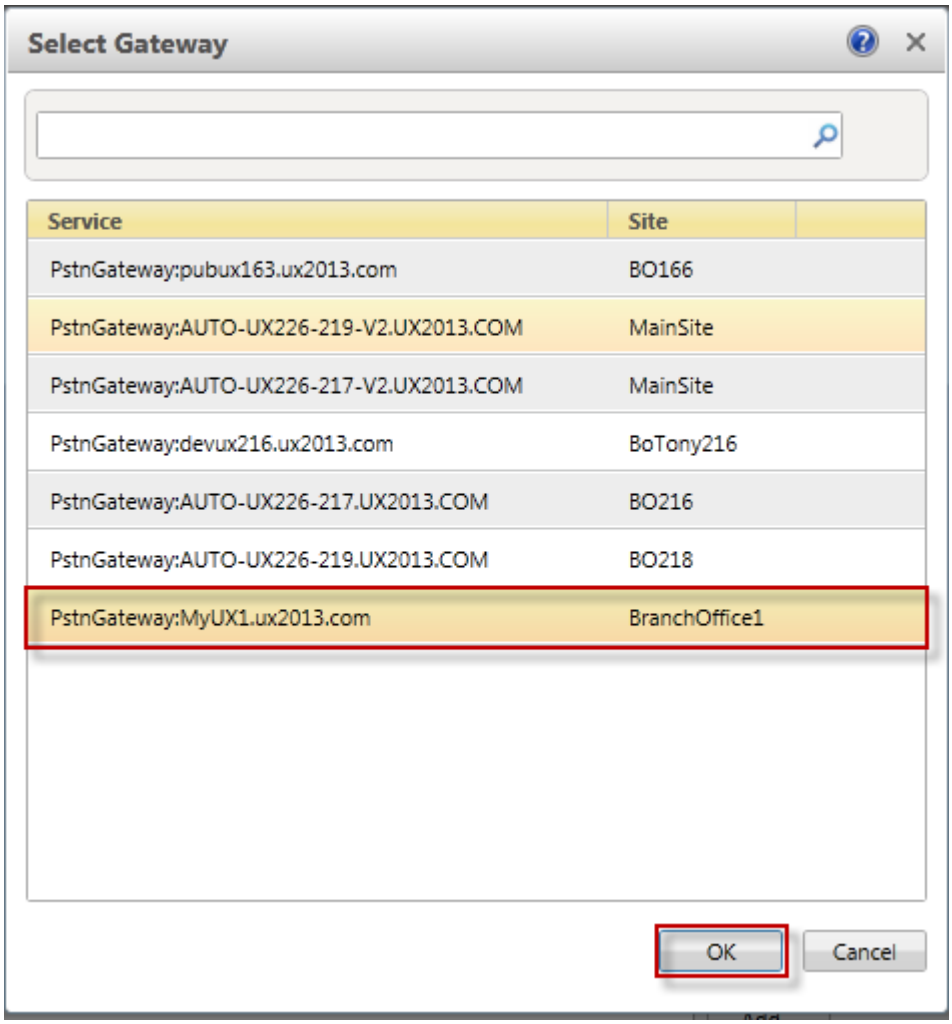
6. In the **Name** text box, enter a name for the usage record.
7. Click **New**.

Copyright © 2015 Sonus Networks. All rights reserved.



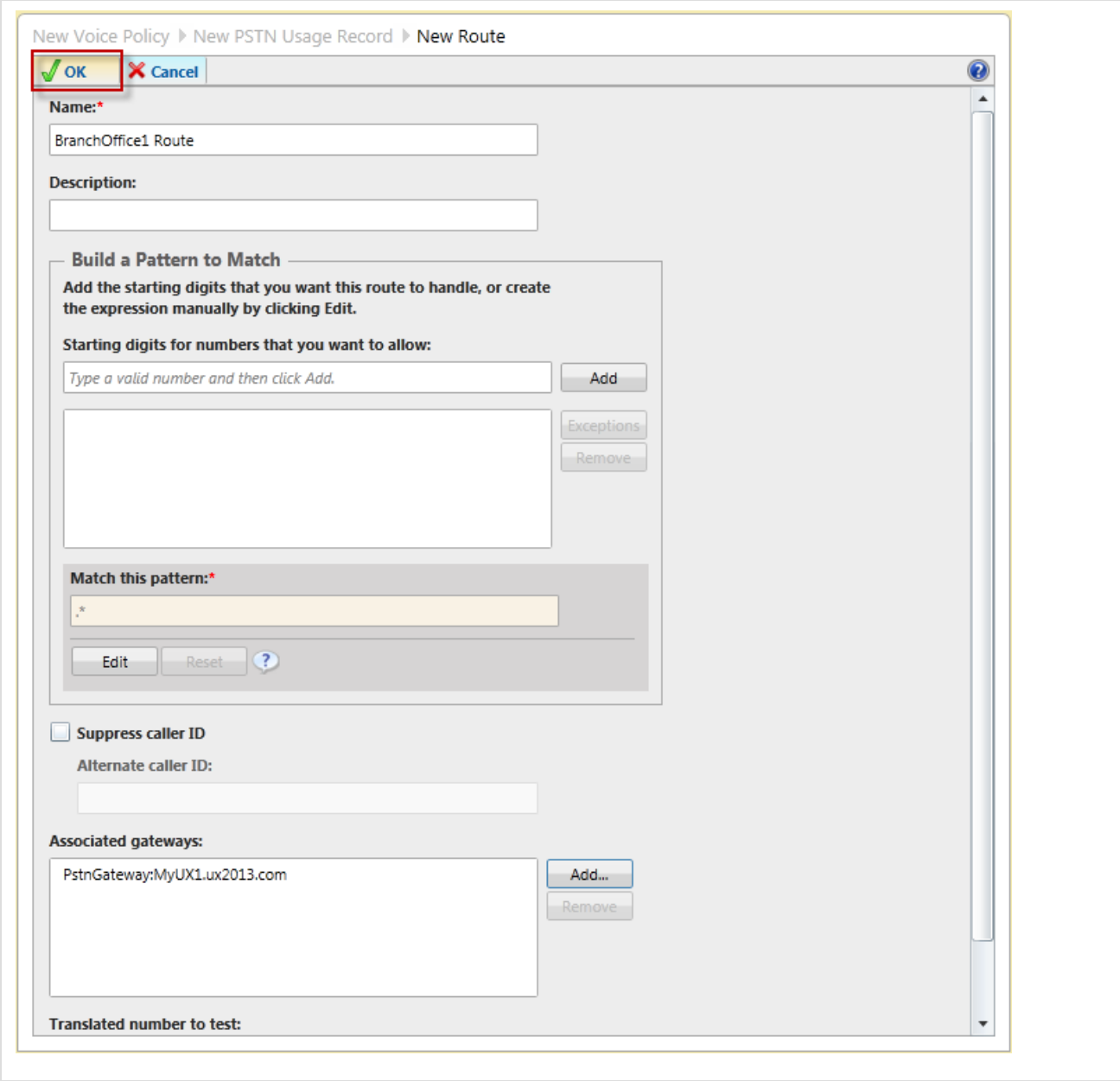
8. In the **Name** text box, enter a name for the route.
9. Next to the **Associated gateways** text box, click **Add**.

Copyright © 2015 Sonus Networks. All rights reserved.



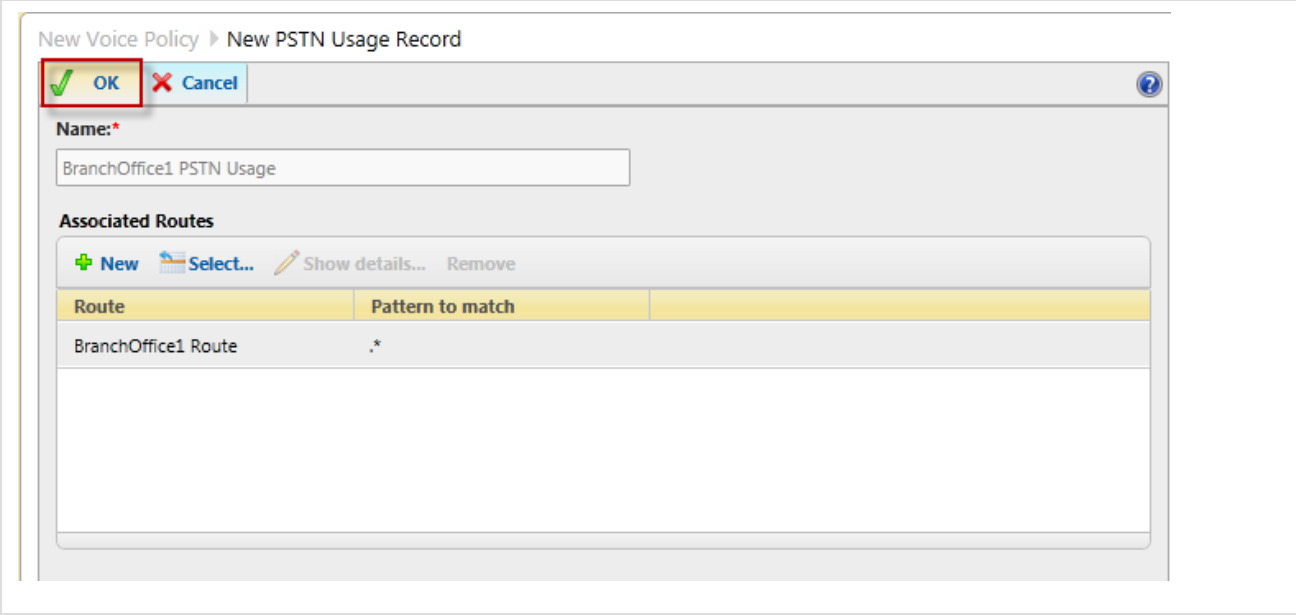
10. Select the gateway to associate with the site.
11. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.



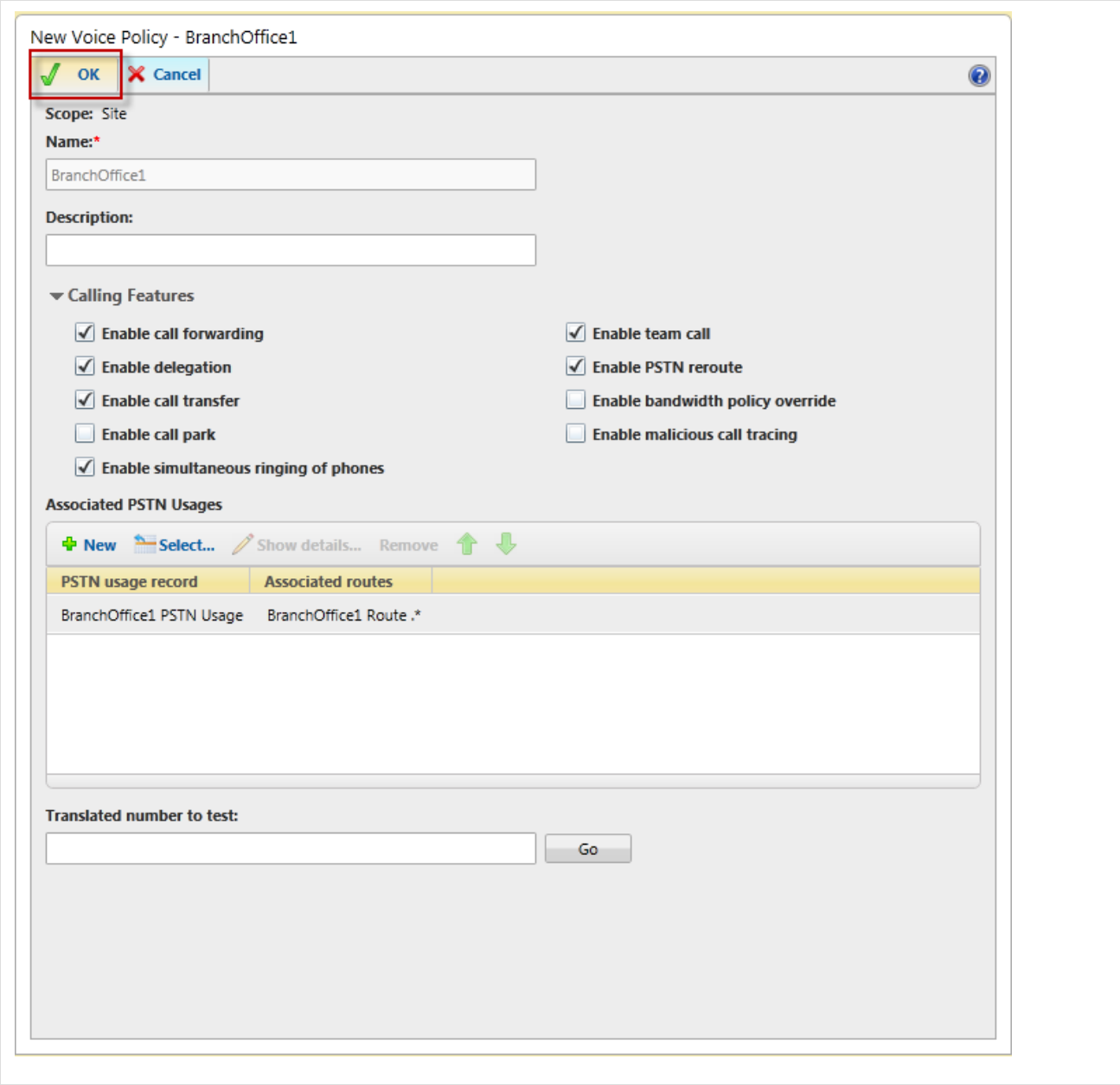
12. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.



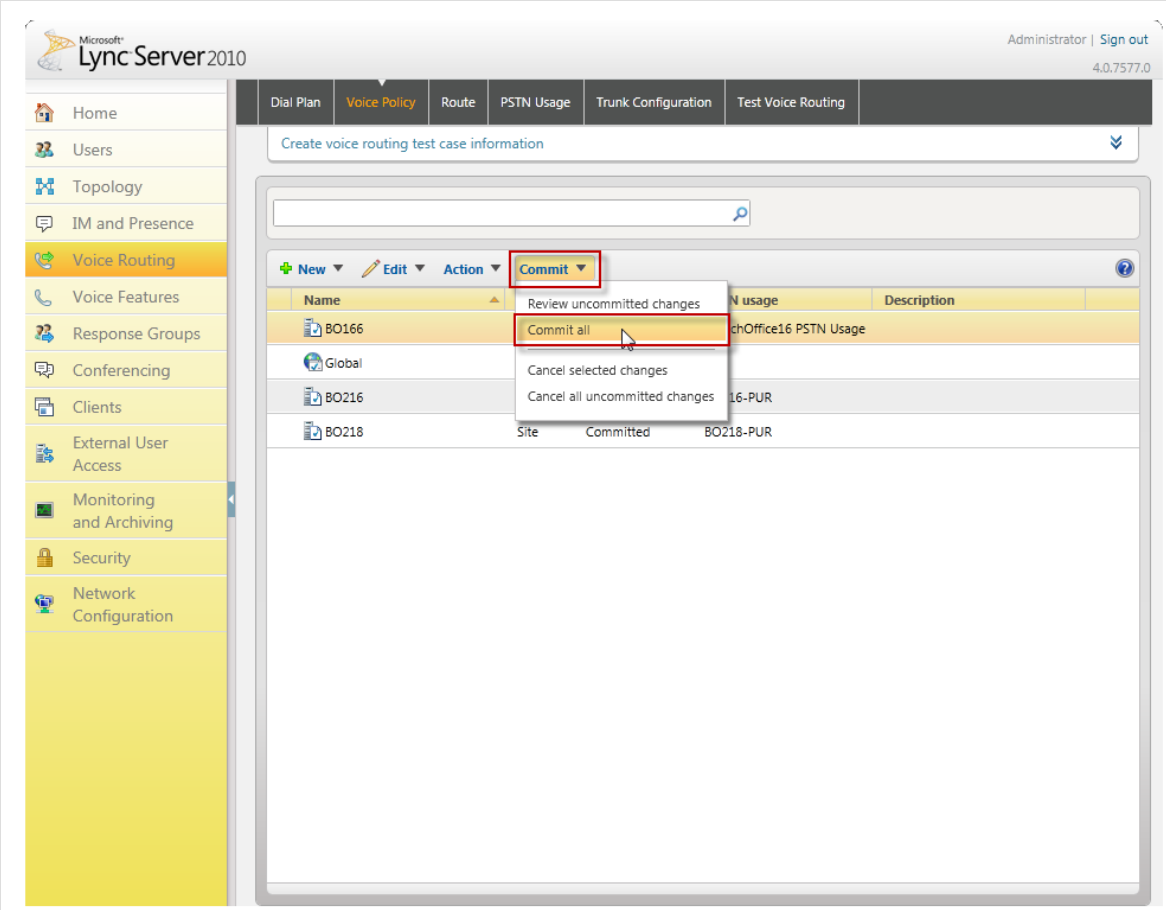
13. Click **OK** to save your PSTN Usage record

Copyright © 2015 Sonus Networks. All rights reserved.



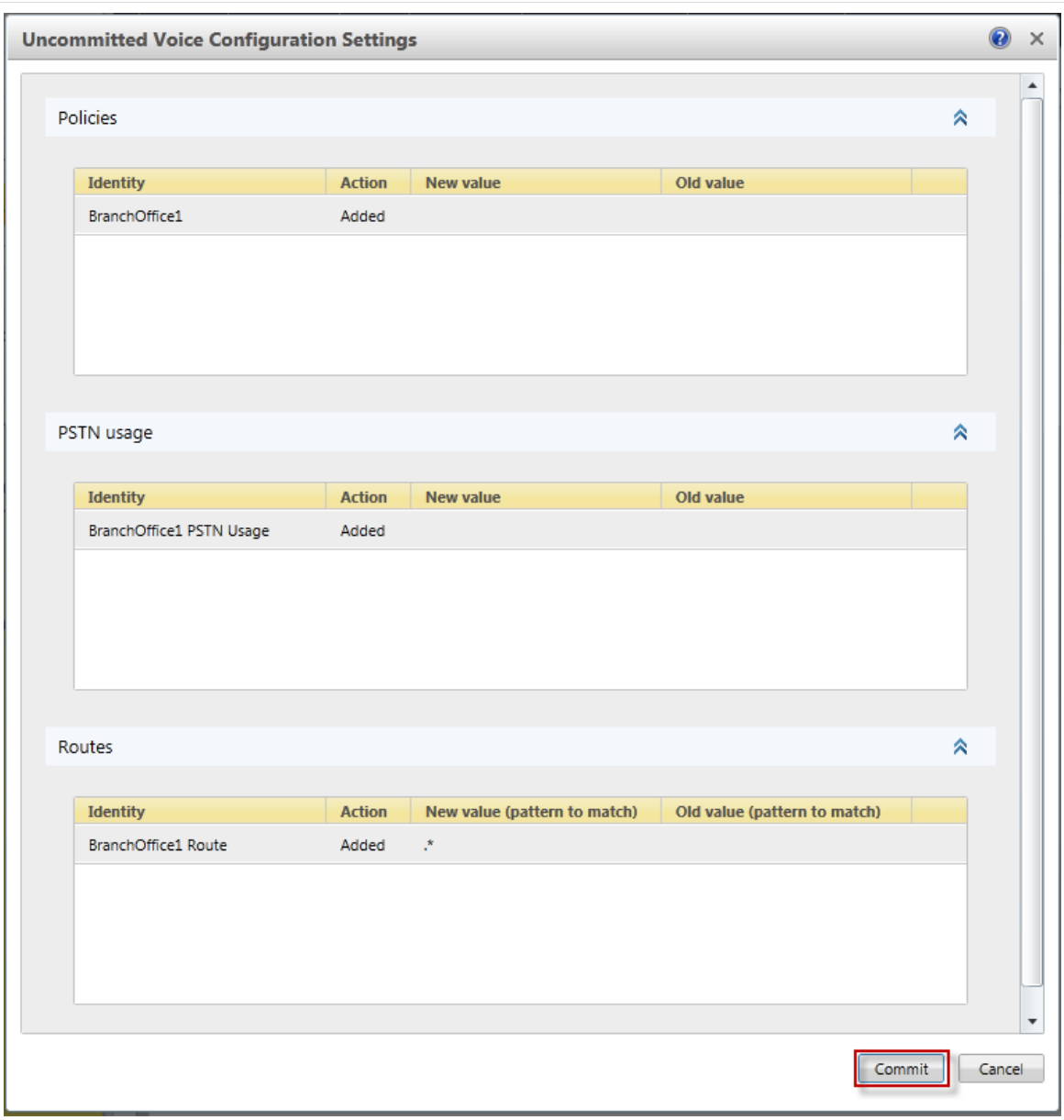
14. Click **OK** to save the voice policy.

Copyright © 2015 Sonus Networks. All rights reserved.



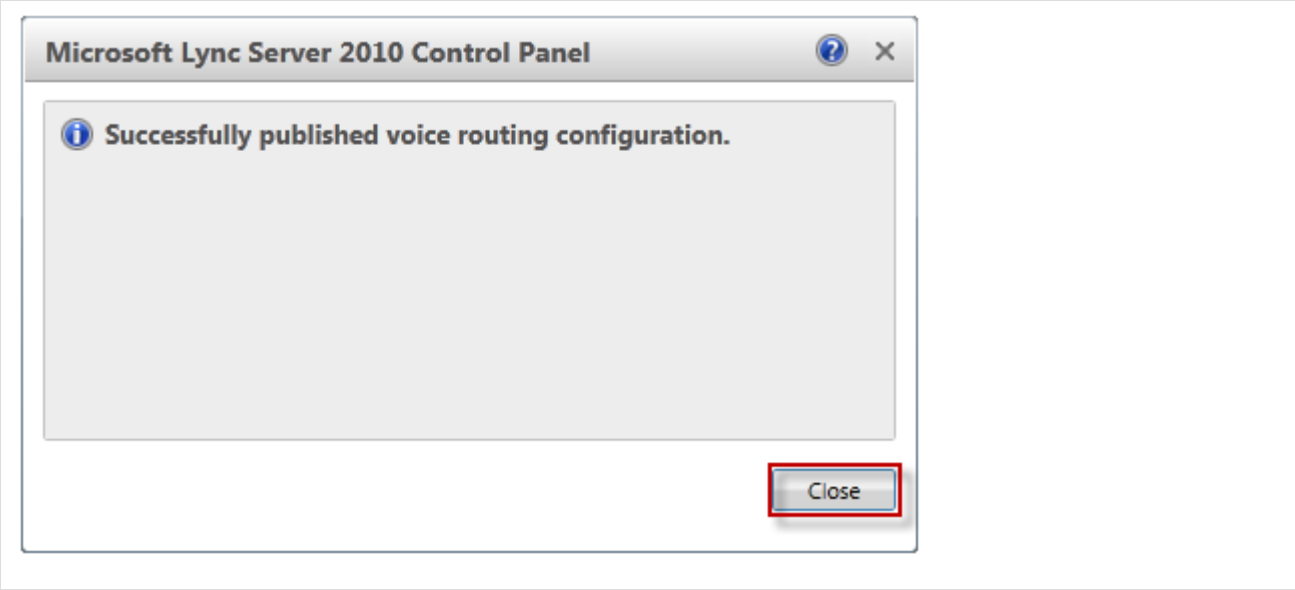
15. In the **Commit** menu, select **Commit all**.

Copyright © 2015 Sonus Networks. All rights reserved.



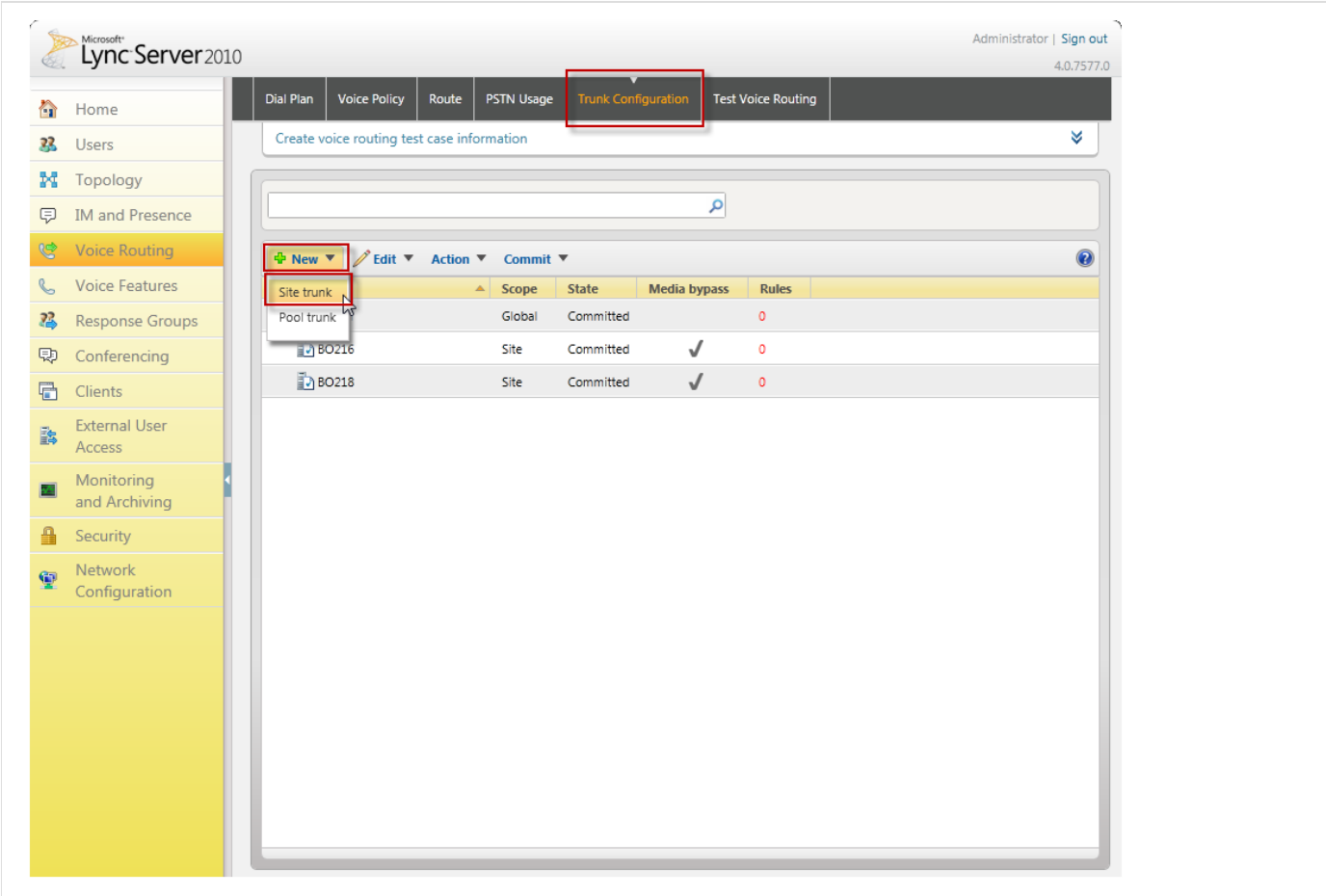
16. Click **Commit**.

Copyright © 2015 Sonus Networks. All rights reserved.



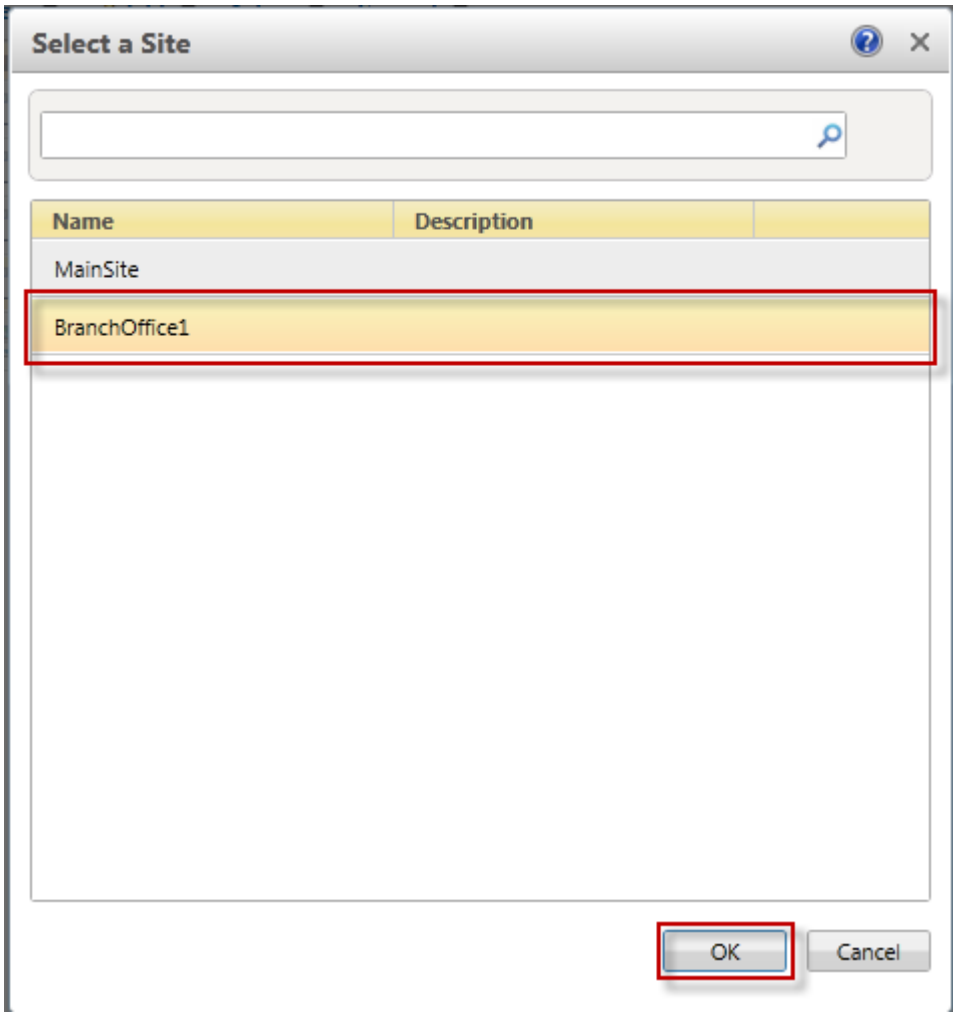
17. Click **Close**.

Adding a Trunk Configuration



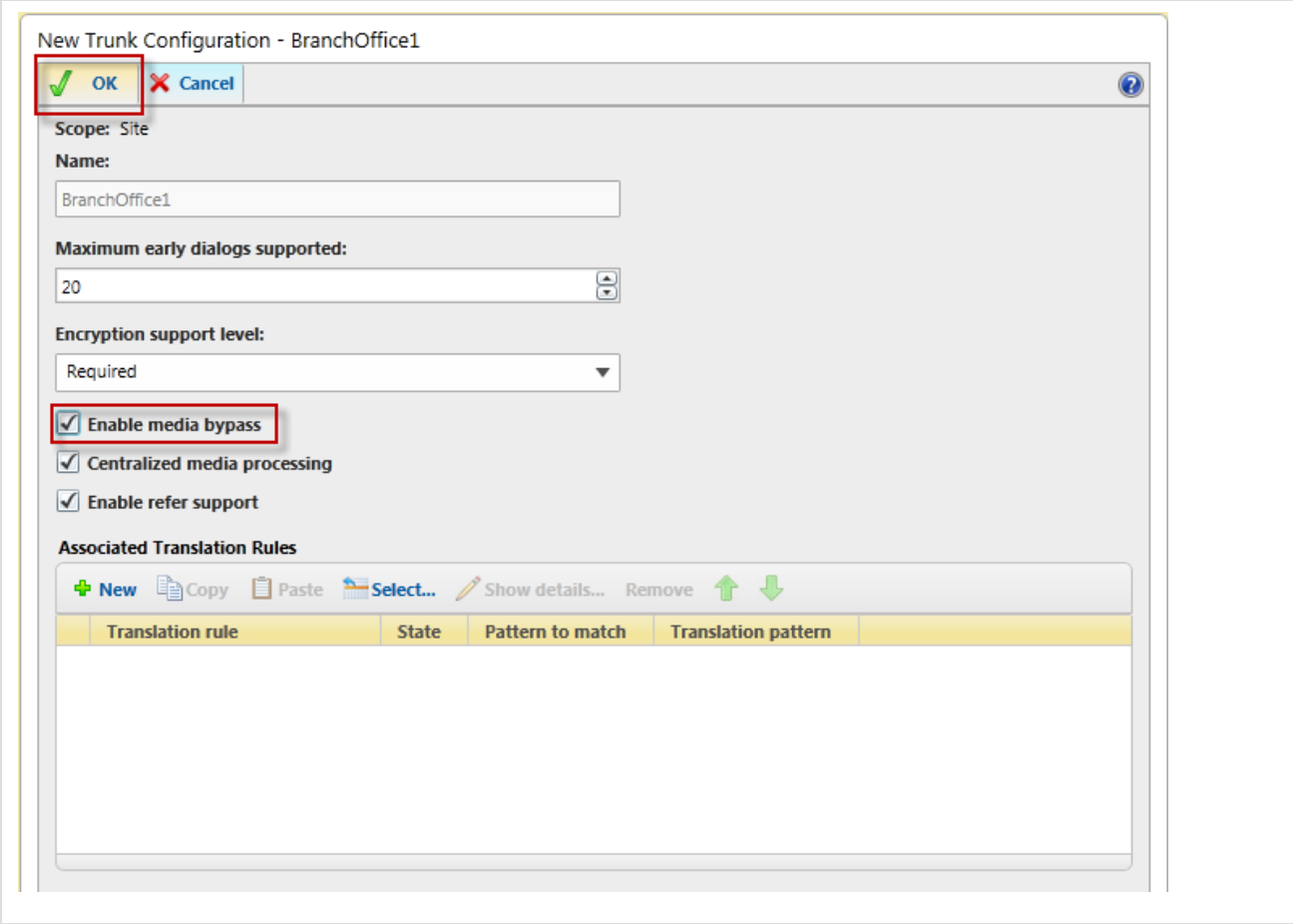
1. Click the **Trunk Configuration** tab.
2. In the **New** menu, select **Site trunk**.

Copyright © 2015 Sonus Networks. All rights reserved.



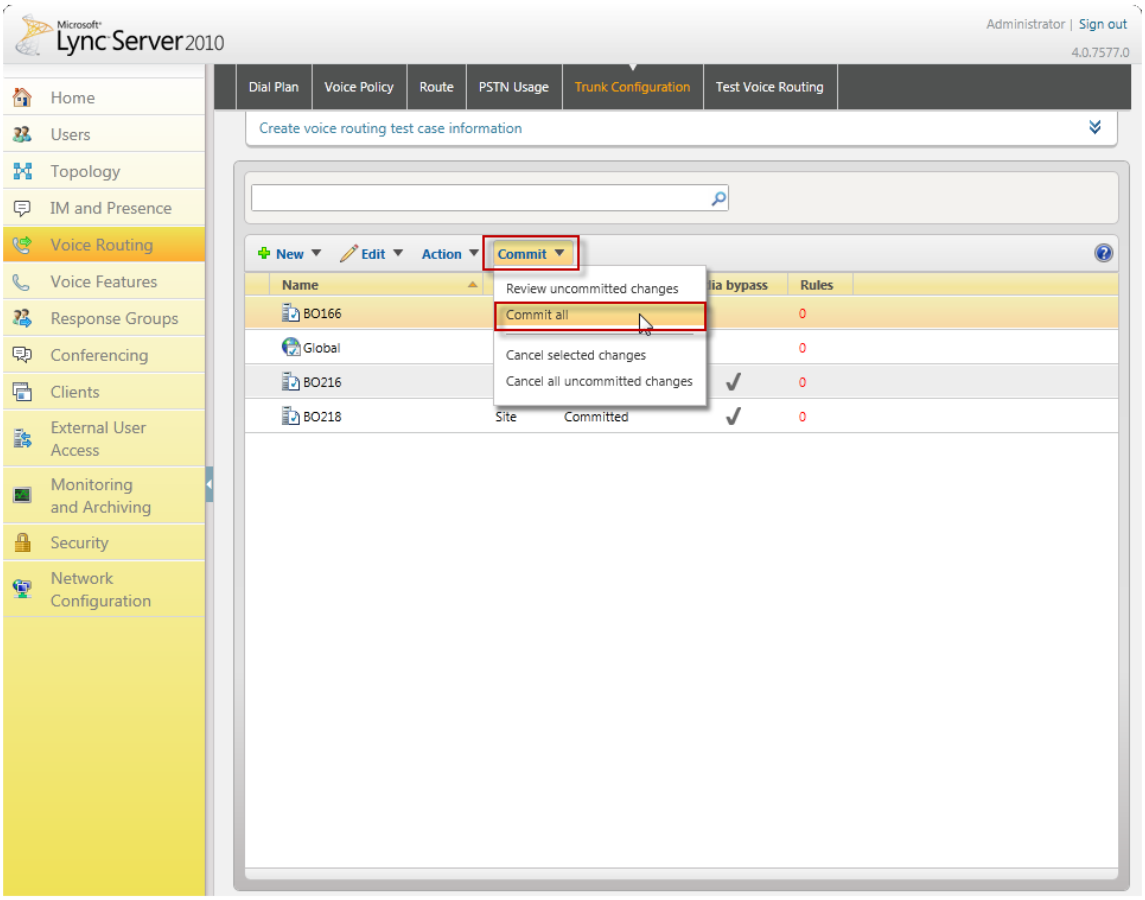
3. Select the appropriate site location.
4. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.



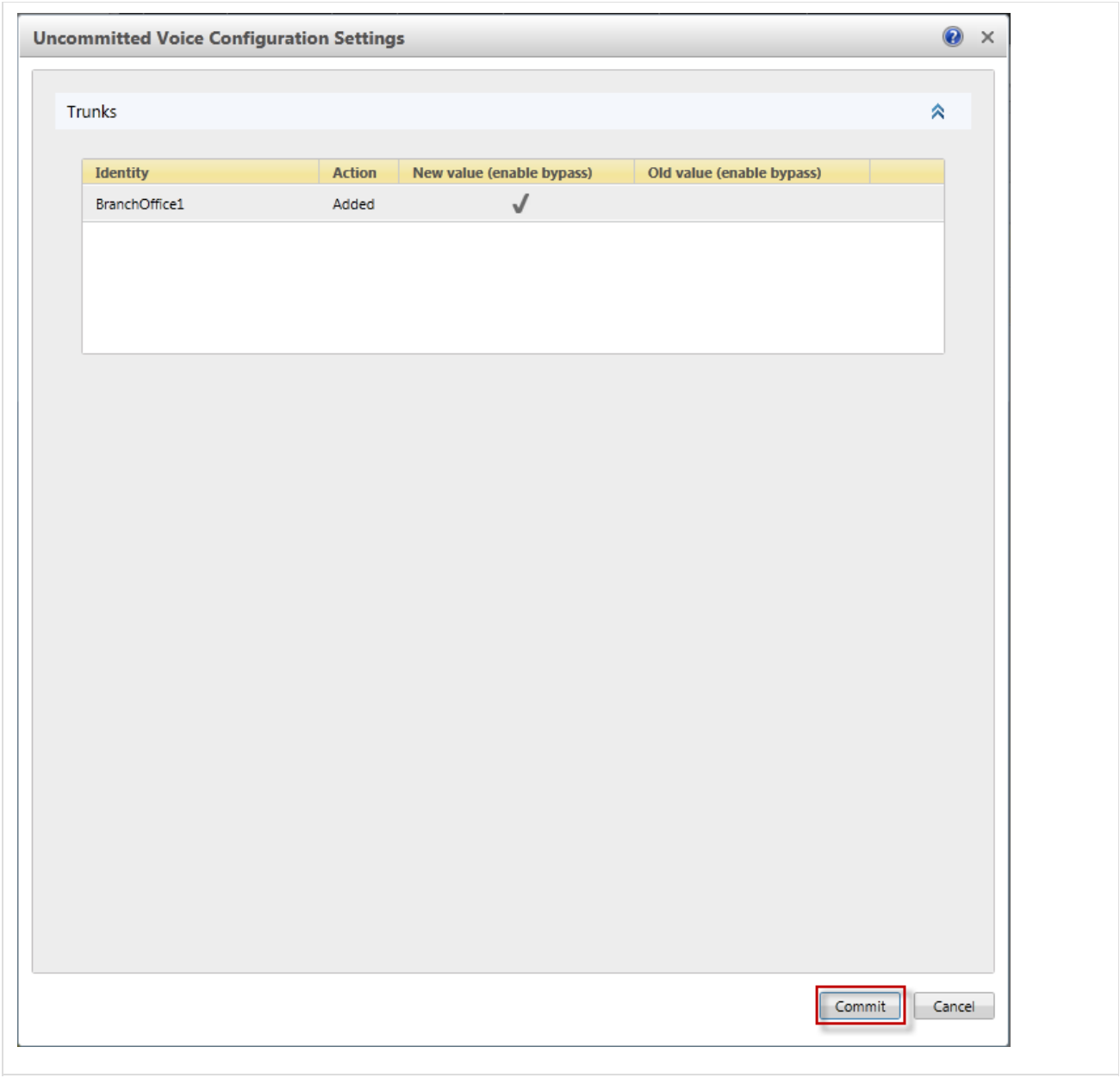
5. Select **Enable media bypass**.
6. Click **OK** to save your selections.

Copyright © 2015 Sonus Networks. All rights reserved.



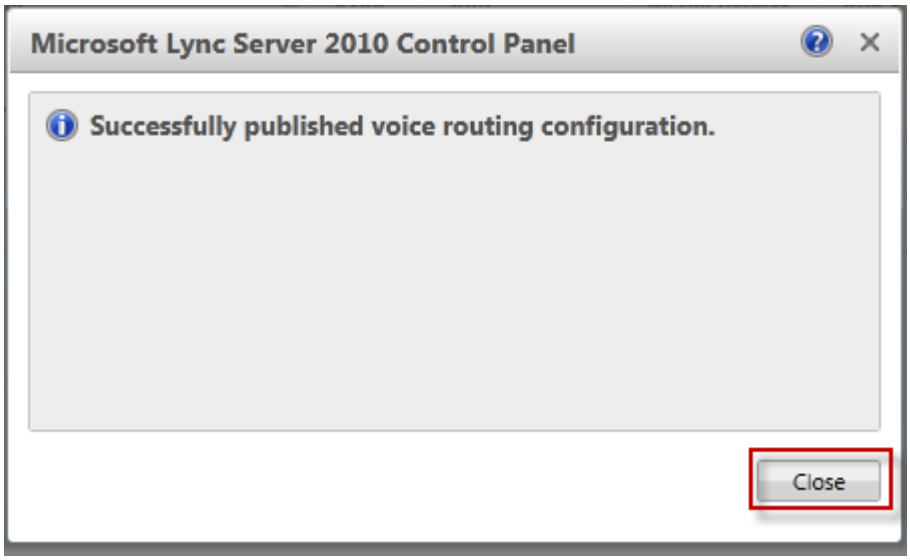
7. In the **Commit** manu, select **Commit all**

Copyright © 2015 Sonus Networks. All rights reserved.



8. Click **Commit** to published the voice routing configuration.

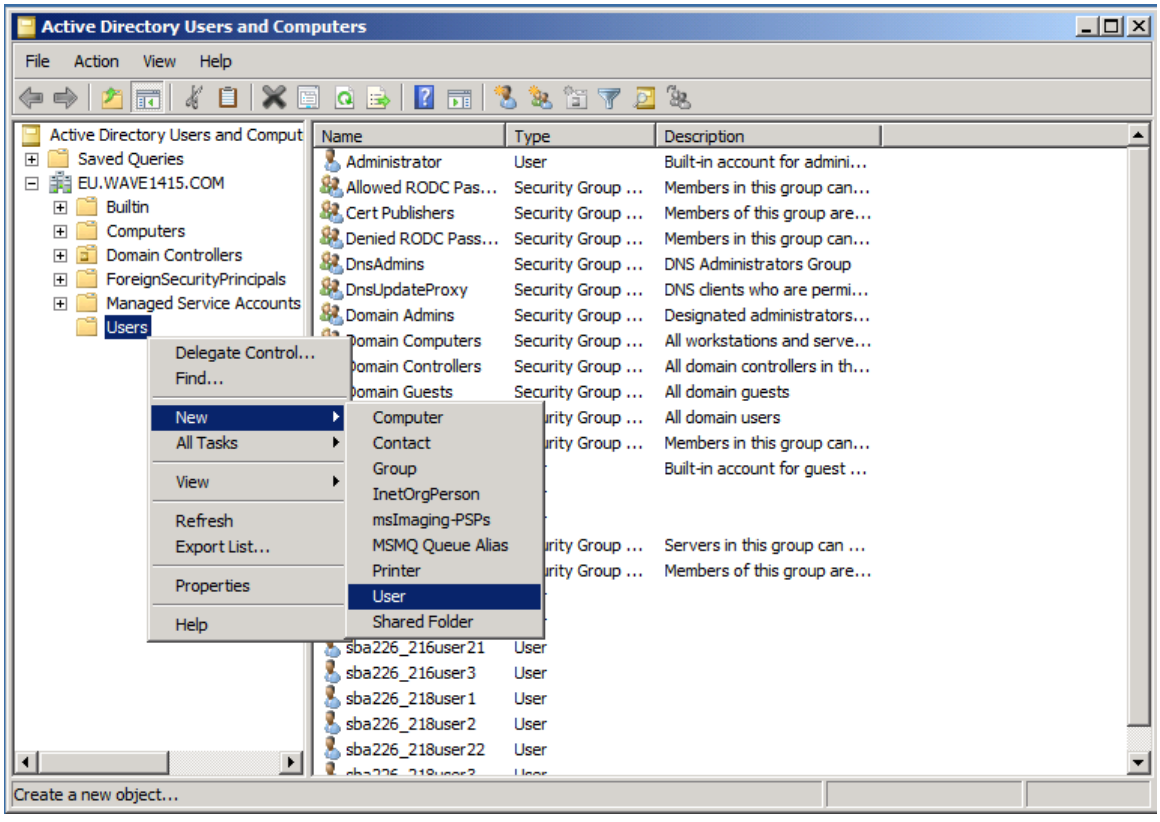
Copyright © 2015 Sonus Networks. All rights reserved.



Creating a Lync 2010 User

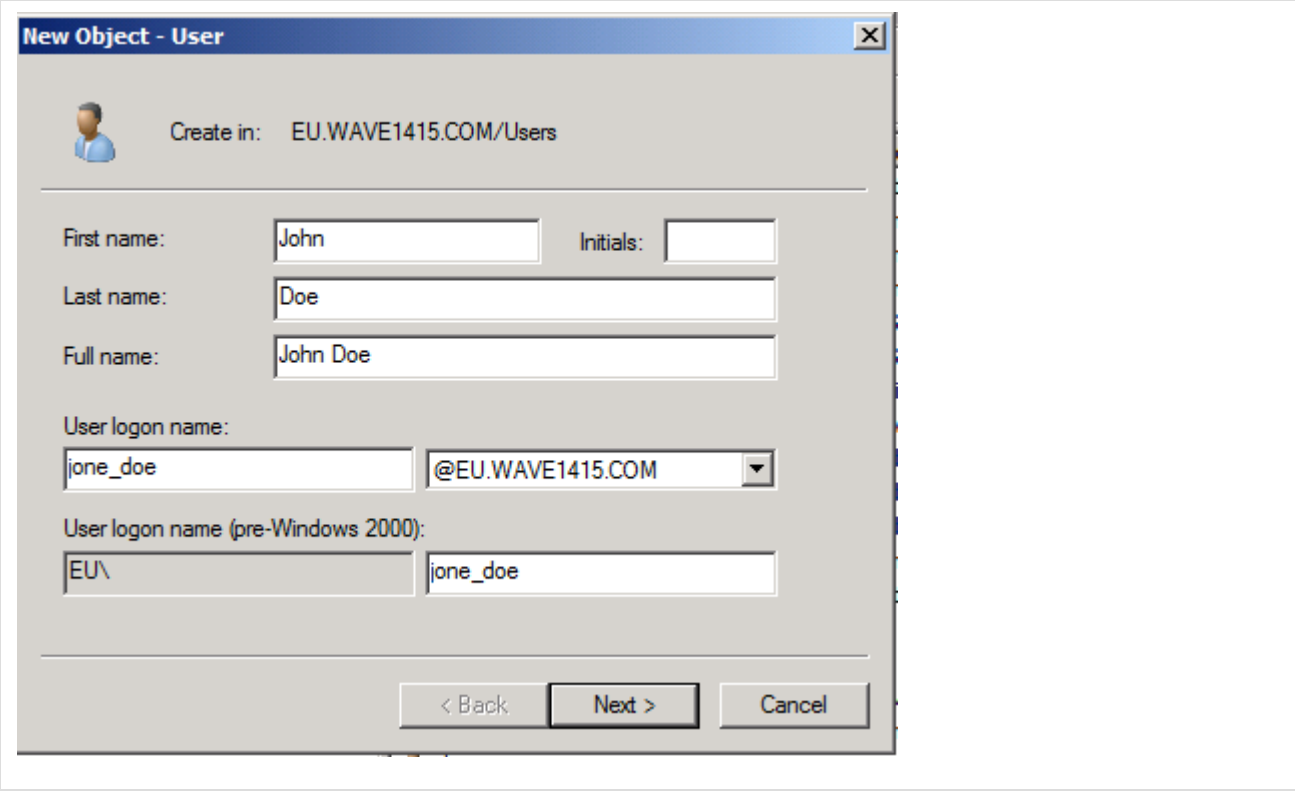
Adding the User in Active Directory

1. Establish a Remote Desktop connection to the domain controller (DC).
2. On the DC, launch the Active Directory Users and Computers Snap-in.

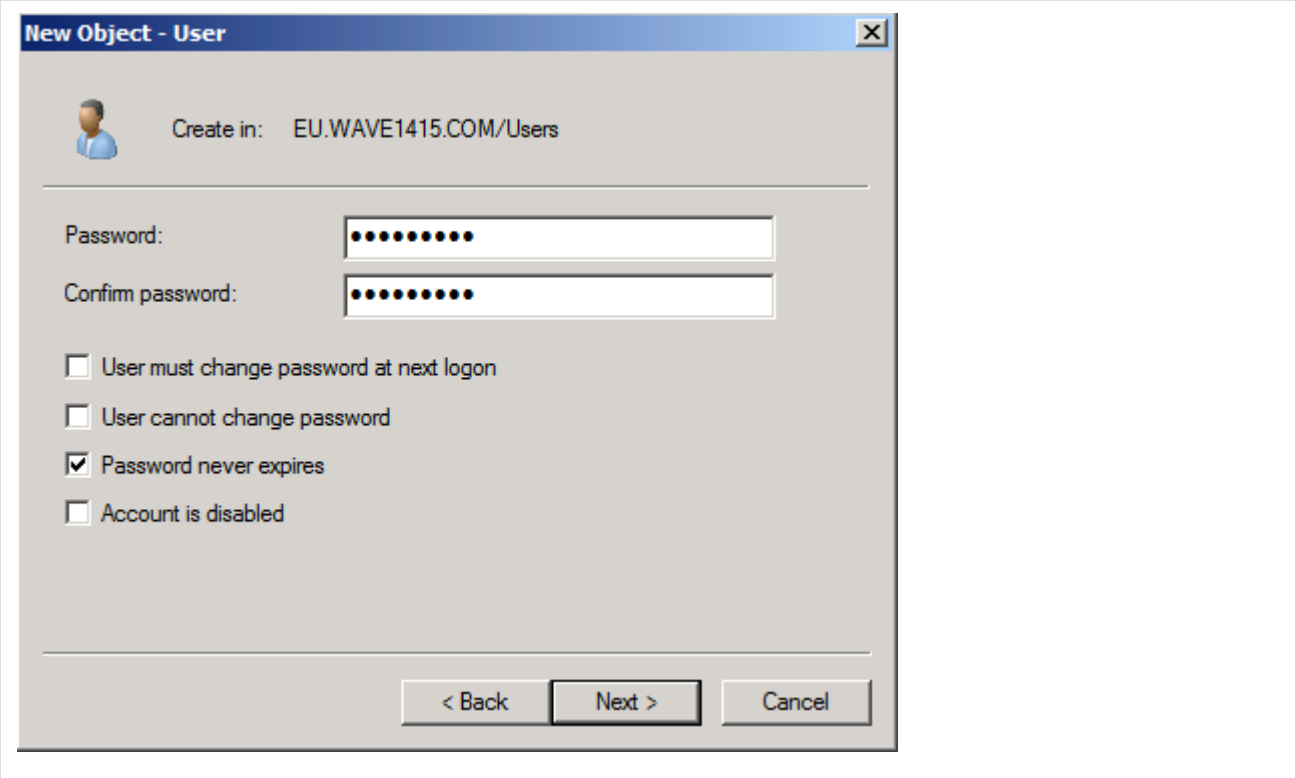


3. In the navigation tree on the left side of the screen, right-click Users, then select **New > User**.

Copyright © 2015 Sonus Networks. All rights reserved.

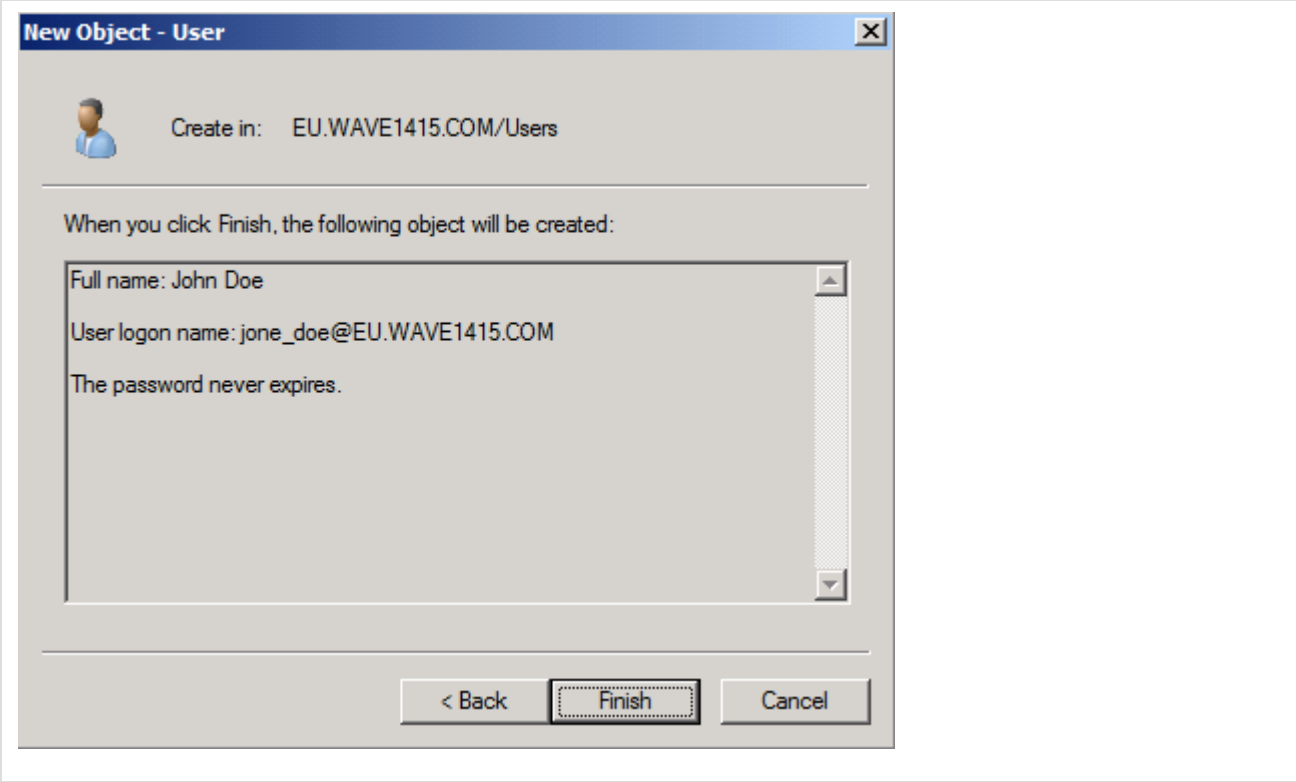


4. Enter the user's name and logon information in the **New Object - User dialog**.
5. Click **Next**.



6. Enter the user's password in the **New Object - User dialog**.
7. Select a password expiry option.
8. Click **Next**.

Copyright © 2015 Sonus Networks. All rights reserved.



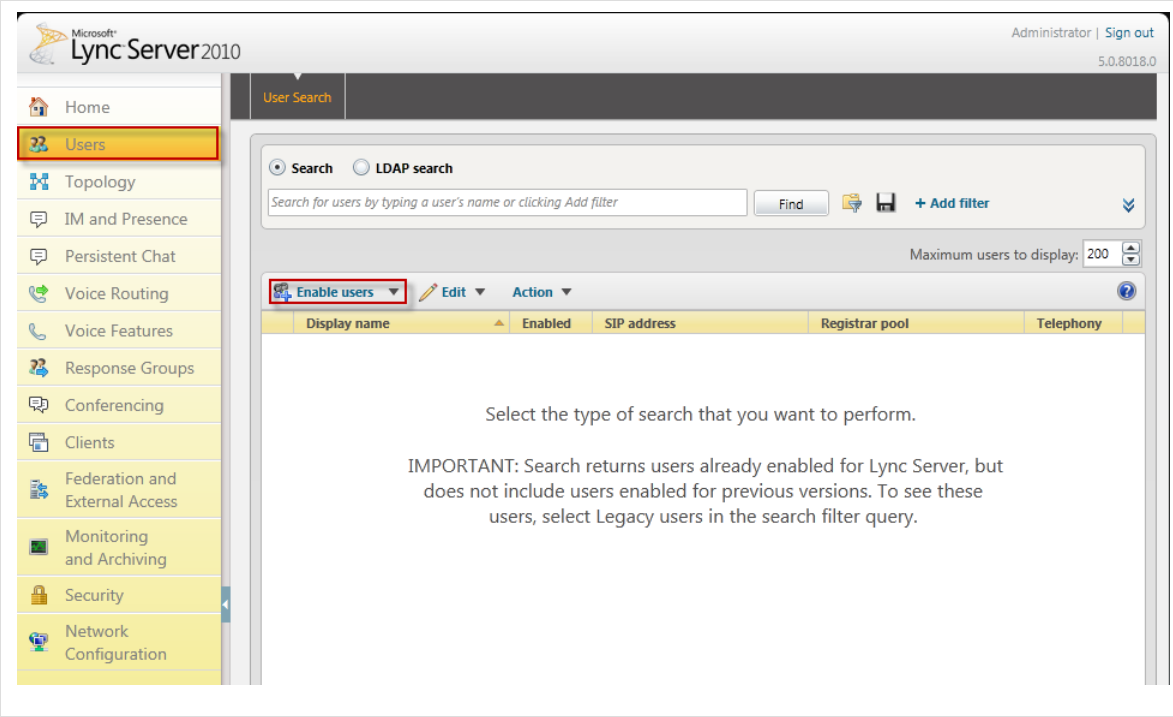
9. Review the user's information.
10. Click **Finish** if it is correct, or click **Back** to back up to the place where it must be corrected.

Adding the User in Lync

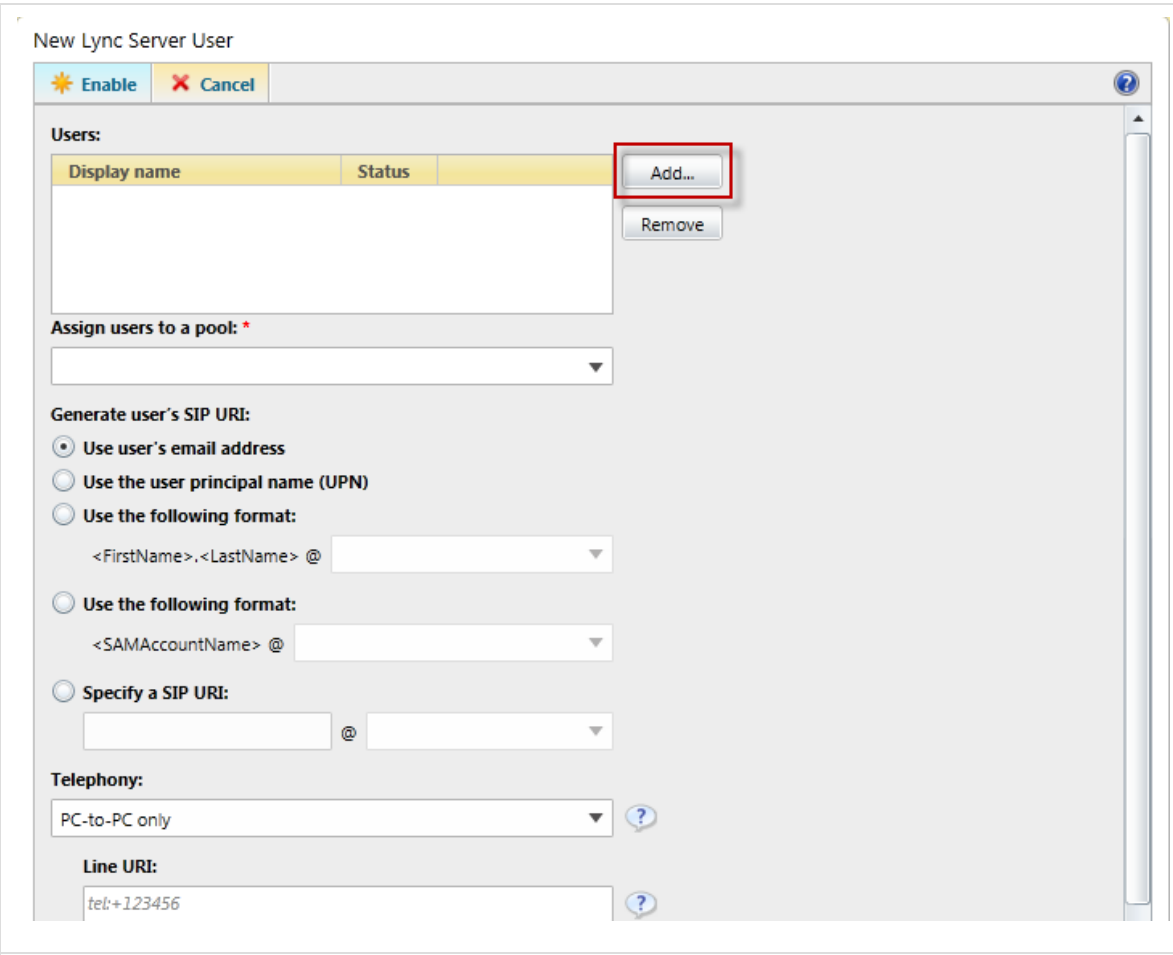
This process creates a new Lync user and maps that user to an existing Active Directory user.

1. Connect to the Front End Server.
   There are two methods:
   a. Connect via Remote Desktop, or
   b. Connect via your web browser (https:\\<Server FQDN>\CSCP)
2. Launch the Lync Server Control panel.
3. Select the Users Tab on the left panel.

Copyright © 2015 Sonus Networks. All rights reserved.

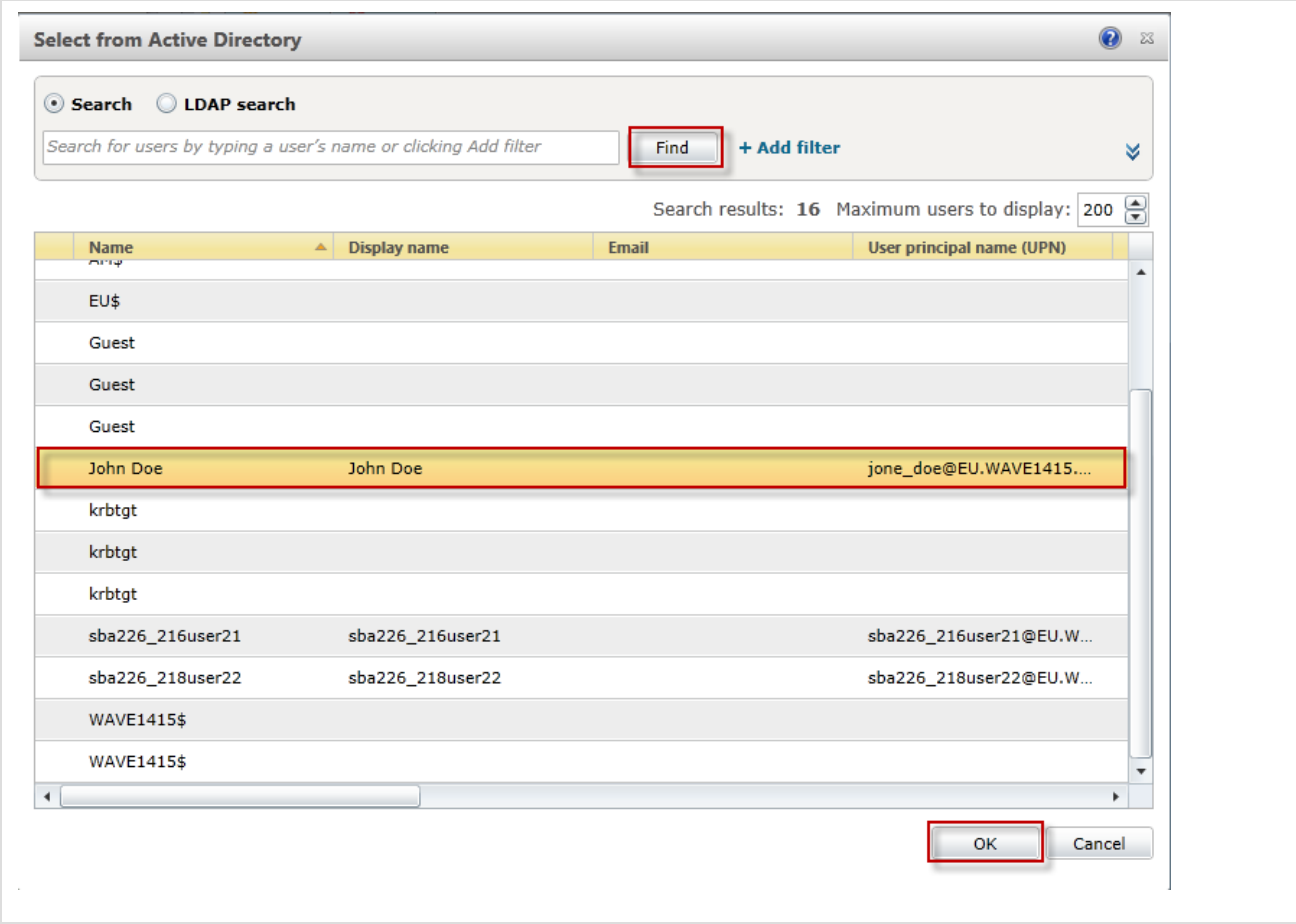


4. Select **Enable Users**



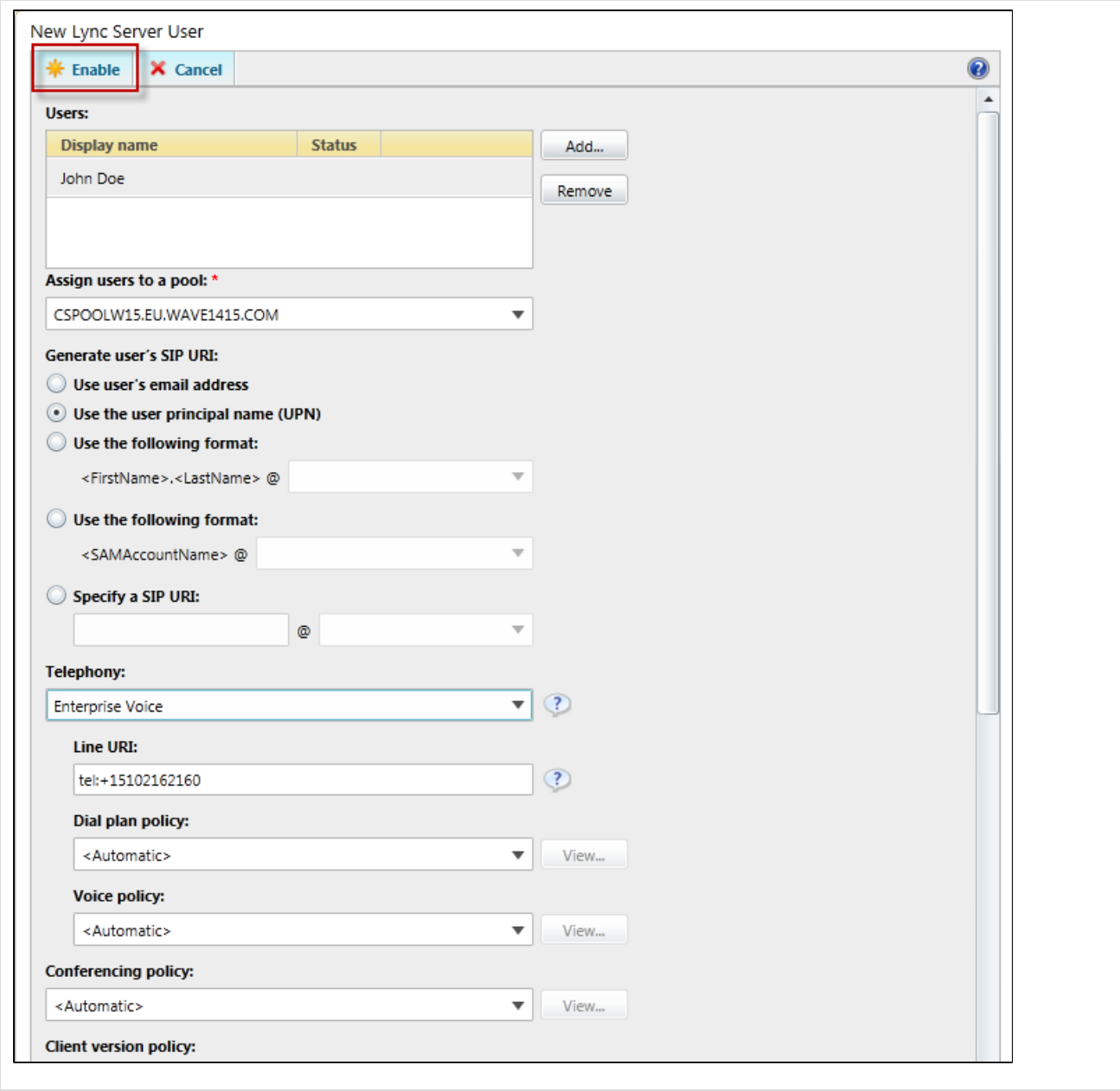
5. Click **Add**.

Copyright © 2015 Sonus Networks. All rights reserved.



6. Click **Find**.
7. Select the Active Directory user.
8. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.



9. Assign the user to a pool.
    a. Select a pool from the **Assign users to a pool** list box.
10. Select **Use the user principal name (UPN)** option.
11. Select **Enterprise Voice** from the **Telephony** list box.
12. Enter a phone number in the **Line URI** text box. Prefix the number with `tel:`.
13. Click **Enable**.

Downstream Deployment of a Sonus SBC 1000-2000 in a PBX-SBC-eUM Topology

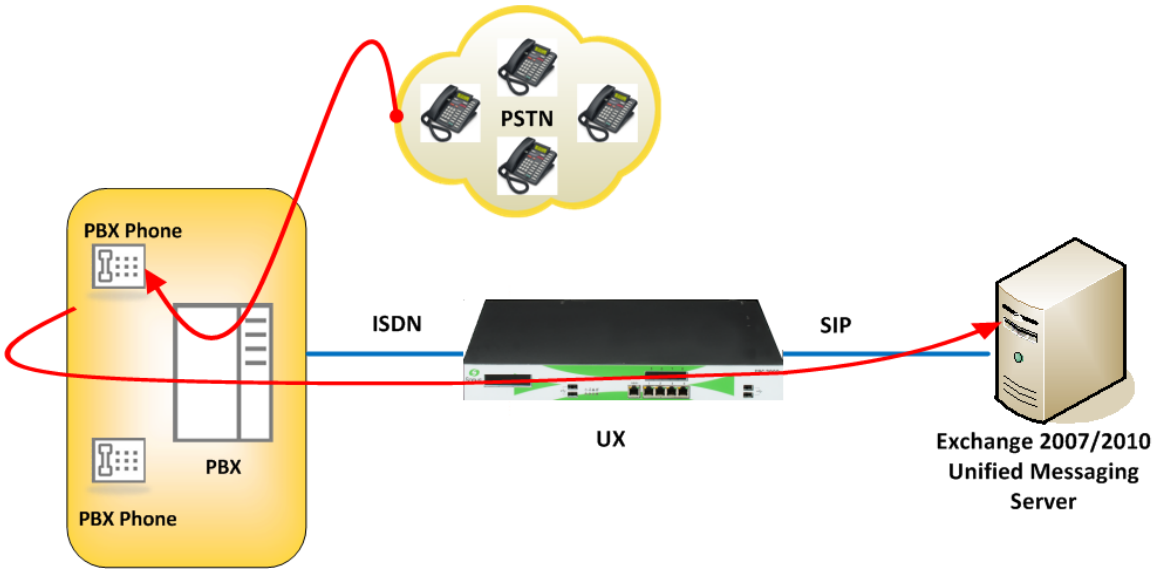
This article describes how to configure the Sonus SBC 1000/2000 such that it can be deployed downstream in a **PBX - Sonus SBC 1000/2000 - MS Exchange 2007/2010 Unified Messaging Server** topology.

Configuring the Sonus SBC 1000/2000 for this type of deployment requires specific configuration steps to be completed in the following order:

Copyright © 2015 Sonus Networks. All rights reserved.

- Configuration Overview
- Configuring the Sonus SBC 1000/2000
  - SIP WebUI Login and verification of the Node Level Settings:
  - SIP Server Table
  - Transformation Table
  - Call Routing Table
  - Port Configuration
  - Signaling Groups
  - Call Routing Table Entries
  - System Timing Configuration
- Exchange 20xx UM Server Configuration Steps:
  - Dial Plan Configuration
  - Associating Dial Plan to UM Server
- Sonus SBC 1000/2000 Signaling Group Status Verification
- Common Use Case

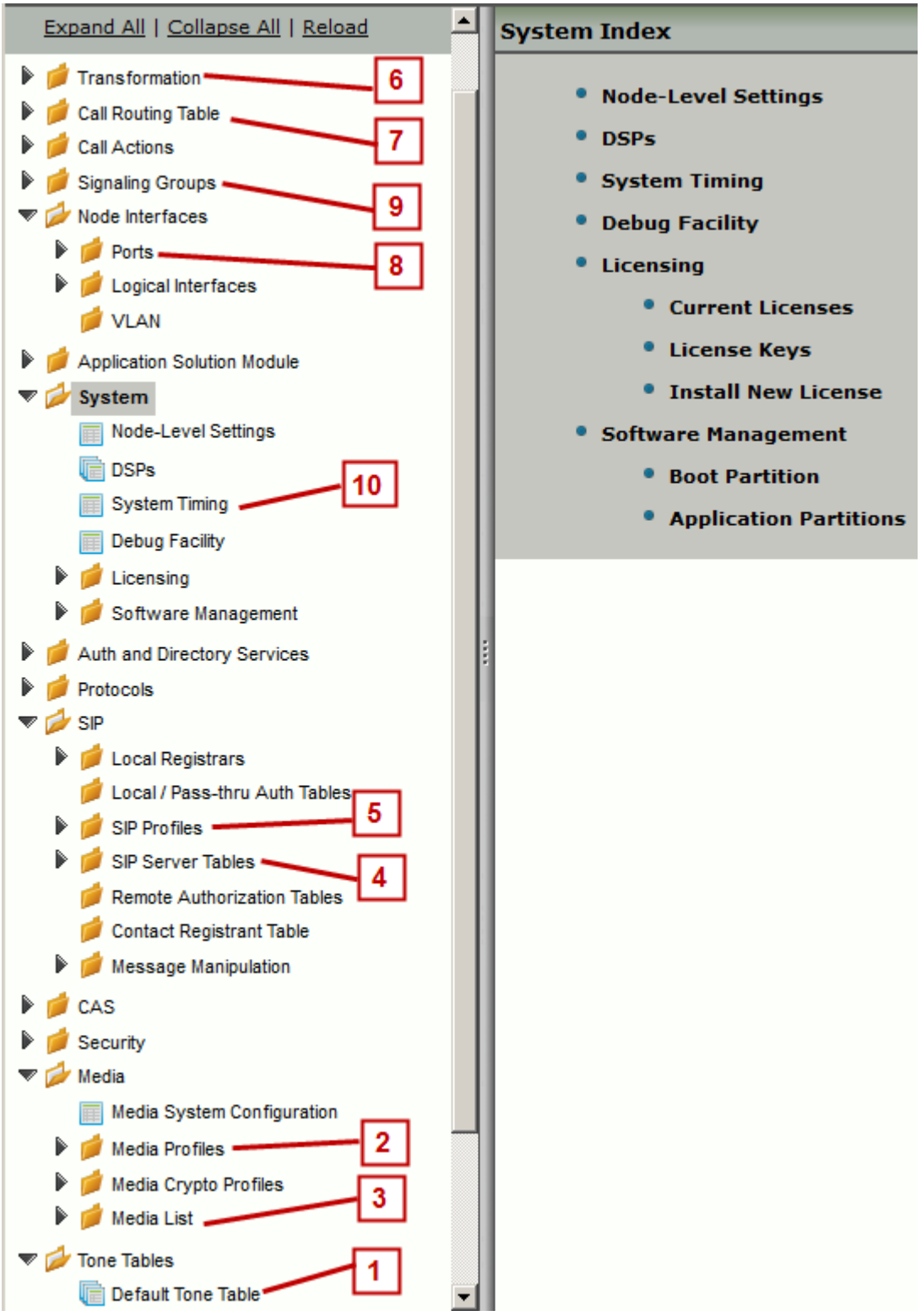
Topology



Configuration Overview

The configuration process comprises the following 10 steps, each of which is explained in detail in the body of this article.

Copyright © 2015 Sonus Networks. All rights reserved.



1. **Default Tone Table**: A factory default Sonus SBC 1000/2000 configuration contains the "Default Tone Tabl entry. This article's configuration requires it, ensure its presence in your configuration.
2. **Default Media Profile(s)**: the default G.711A/Mu-Law profile is used in this example.
3. **Default Media List**: the Default Media List is used in this example.
4. **Create a SIP Server Table**: In this example we add a SIP Server table entry for the Exchange 2007/2010 Server.

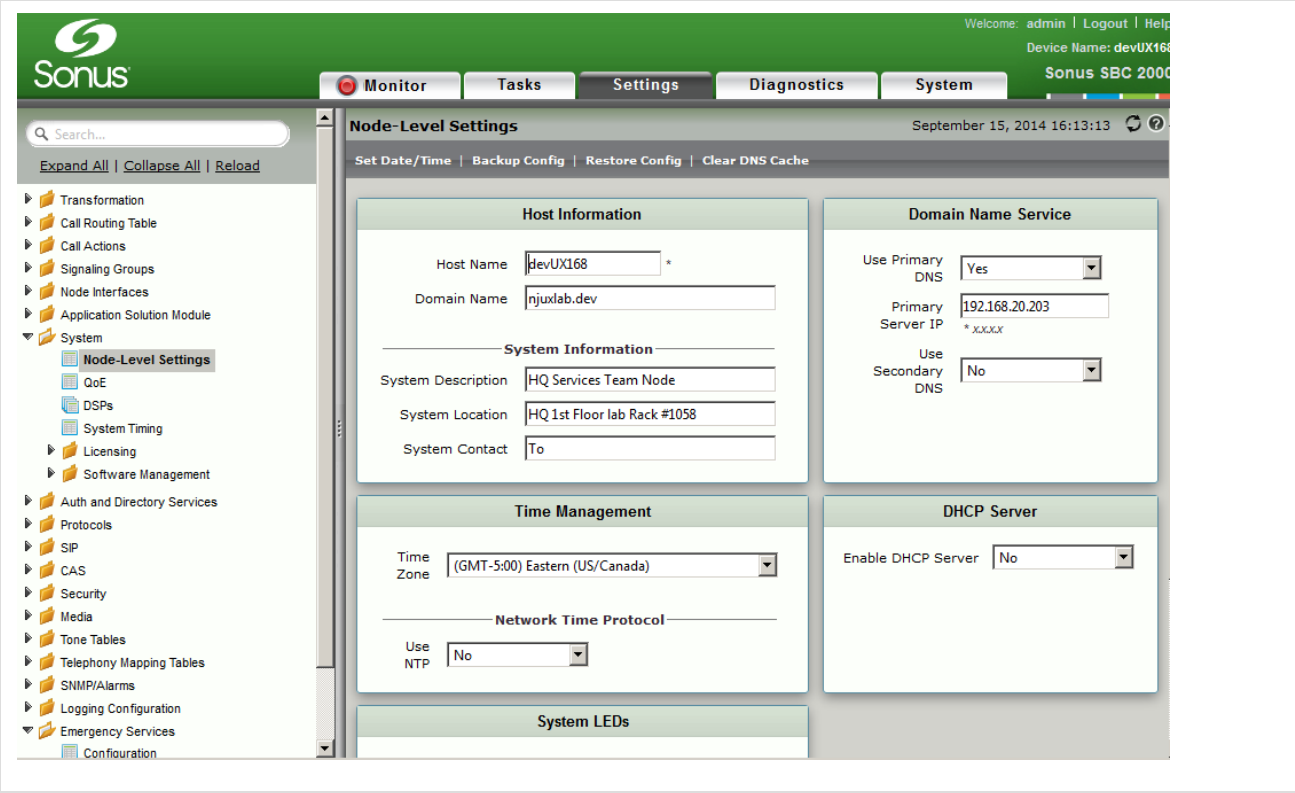
Copyright © 2015 Sonus Networks. All rights reserved.

5. **Create a SIP Profile**: you can create a custom SIP Profile or use the default. The default is used in this example.
6. **Create a Transformation Table**: this table is used in the relate Call Routing tables and for Called/Calling Number transformations.
7. **Create a Call Routing Table**: in this example we create two table entries, one for ISDN and another for SIF They are required in the relevant Signaling Groups.
8. **Configure a DS1 Port**: this port is associated with the Physical PRI (T1/E1) connection.
9. **Create two Signaling Groups**: One Signaling Group will be designated for for SIP and the other is for ISDN
10. **Set the System Timing**: you can configure the Clock Source to use the Sonus SBC 1000/2000 system cloc or a network source, depending on your PBX.

Configuring the Sonus SBC 1000/2000

SIP WebUI Login and verification of the Node Level Settings:

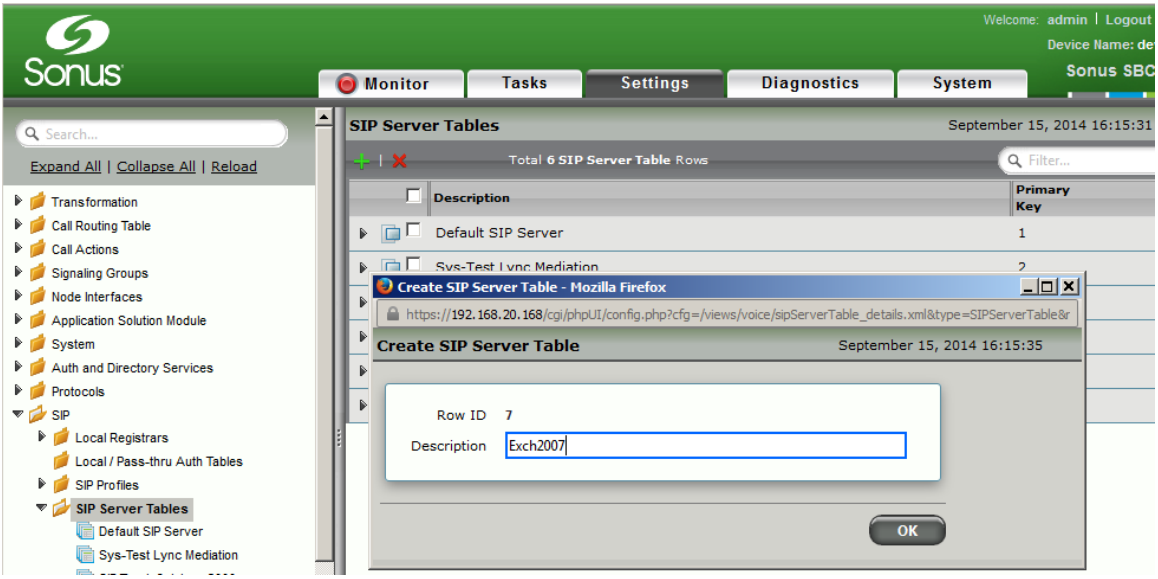
1. In the WebUI, click on **Settings**.
2. In the left navigation pane, go to **System > Node-Level Settings**.
3. Verify that the settings are configured correctly as indicated below.



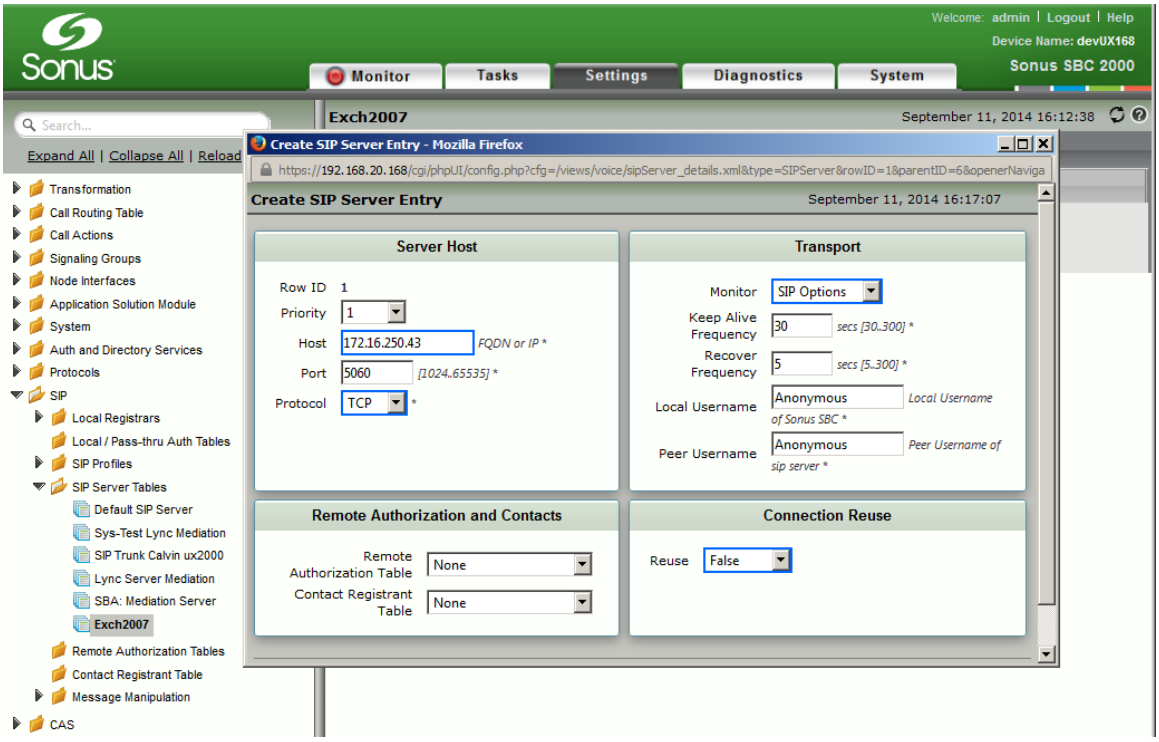
SIP Server Table

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Server Tables**.
3. Create a new **IP Server Table**. Click on the Create (+) icon.
   The SIP Server Tables page is a table of SIP Server Tables.
4. Configure the new SIP Server Table as shown in the illustration below.

Copyright © 2015 Sonus Networks. All rights reserved.



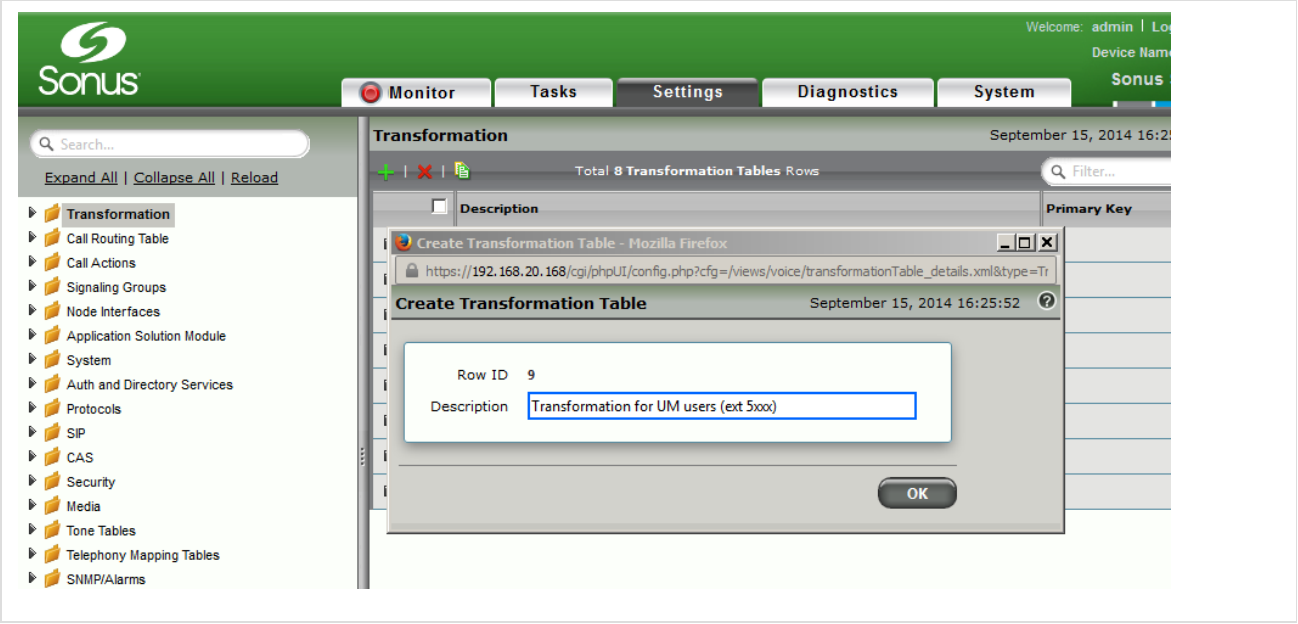
5. In the left navigation pane, go to **SIP > SIP Server Tables > (The table you created in the previous step)**.
6. Click the **Create SIP Server > IP/FQDN.**
7. Enter the IP address of the eUM Server in the **Host** as shown below.
8. Click **OK**.



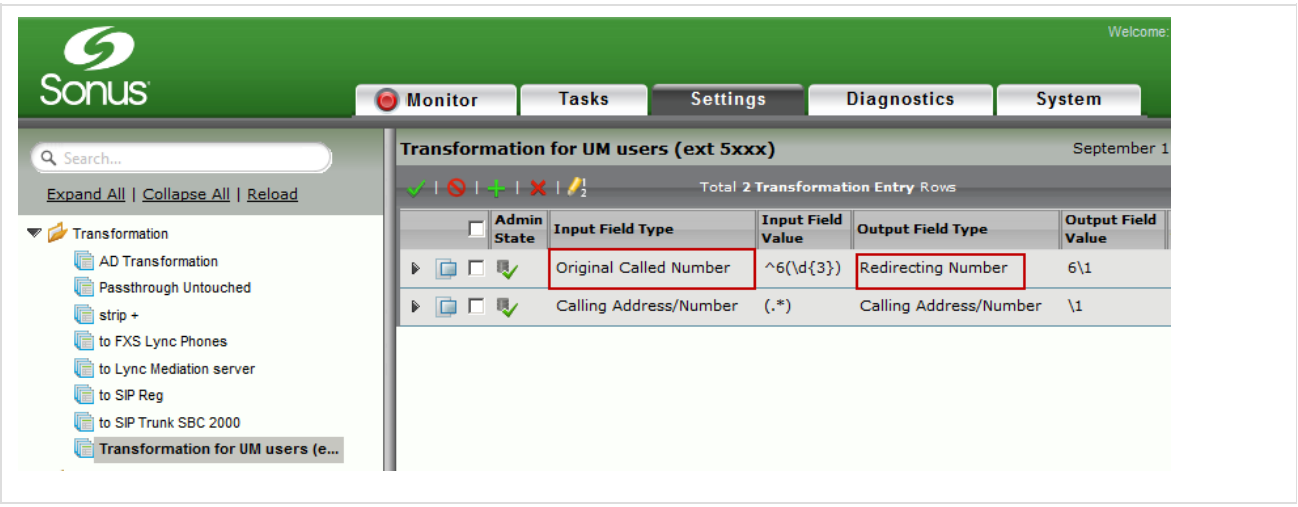
Transformation Table

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Transformation**.
3. Click the Create (+) icon.
4. Create a new Transformation Table.

Copyright © 2015 Sonus Networks. All rights reserved.



5. In the left navigation pane, go to **Transformation >(the table created in the previous step)**.
6. Add an entry as shown below.



Call Routing Table

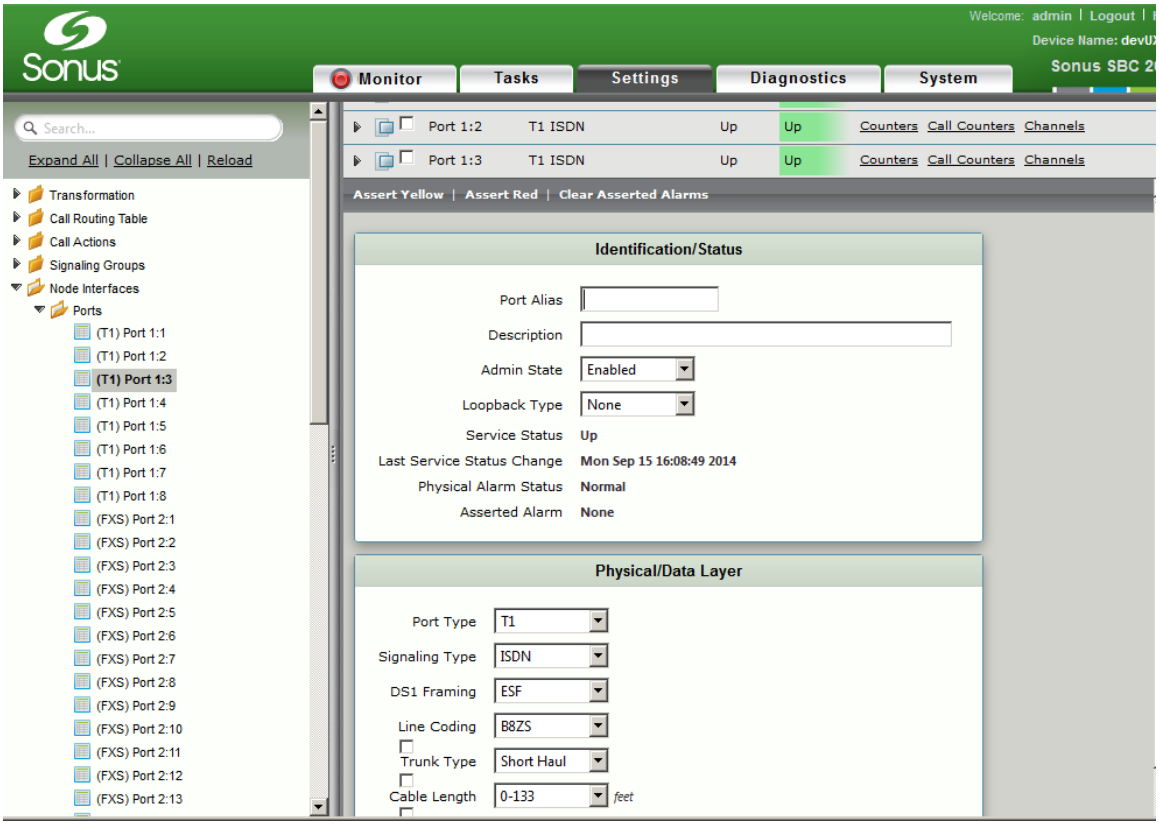
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table**.
3. Create two entries (Calls from ISDN, Calls to ISDN) as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



Port Configuration

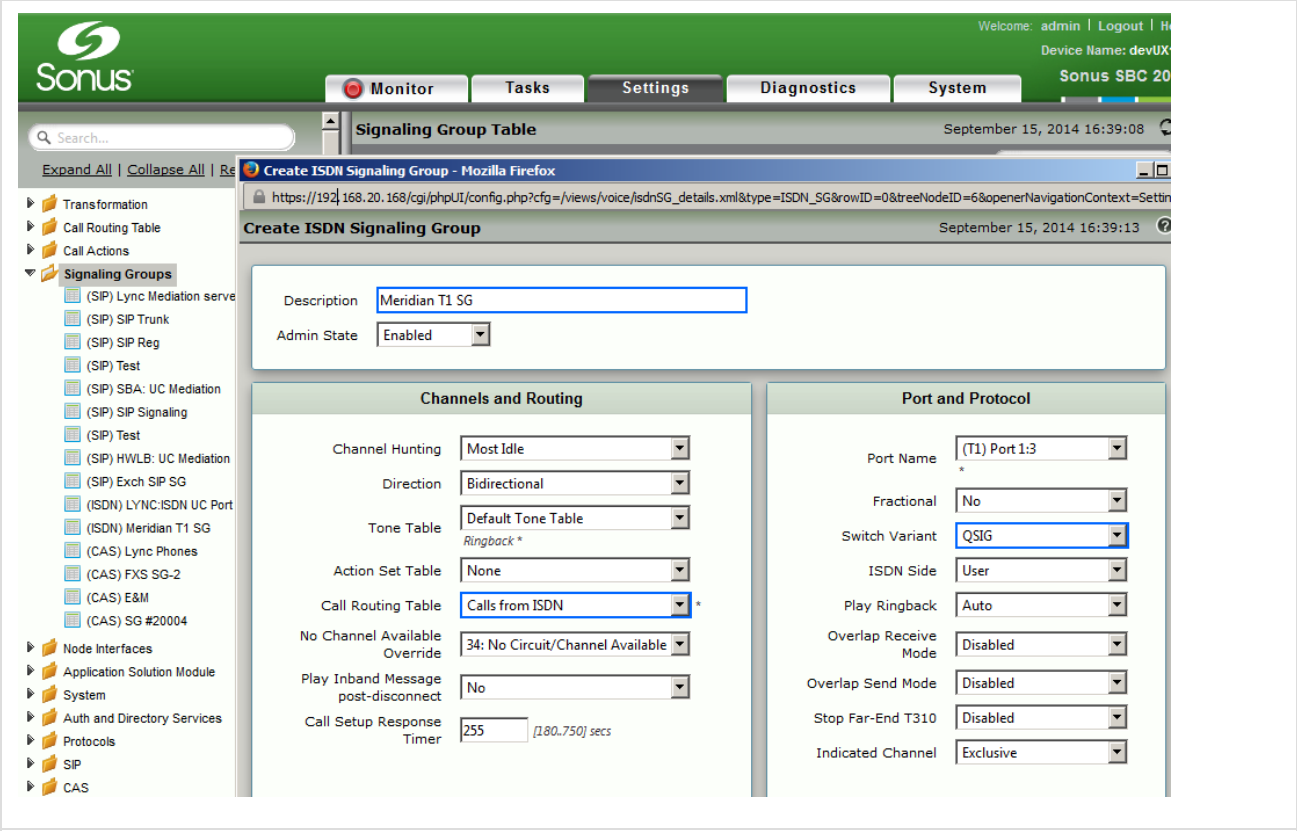
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.
3. Click the port that you wish to connect to the physical PRI line.
4. Fill in the fields as shown below.



Signaling Groups

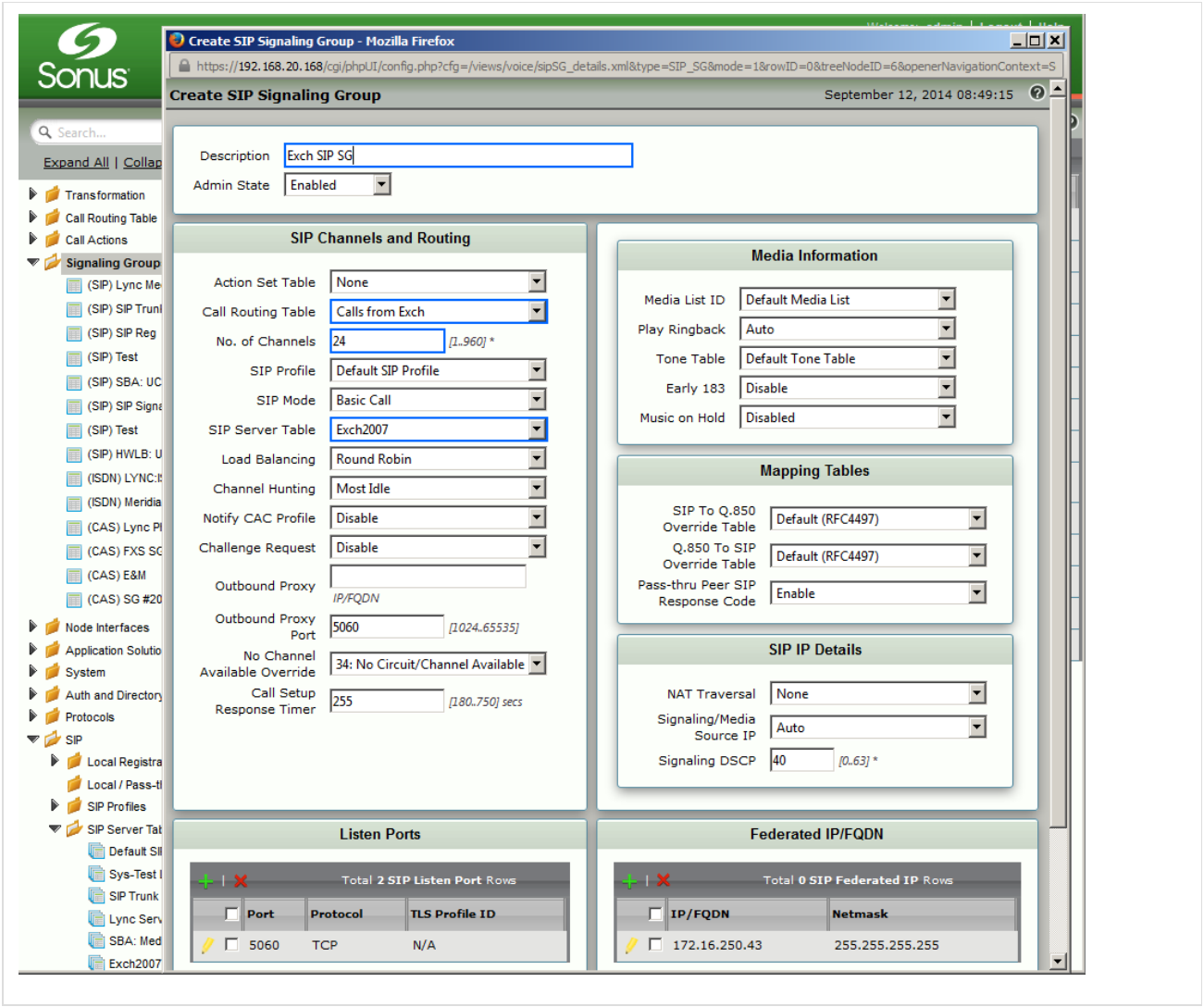
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
   Click **Create Signaling Group** and select **ISDN Signaling Group** text at the top of the table.
3. Fill in the fields as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.

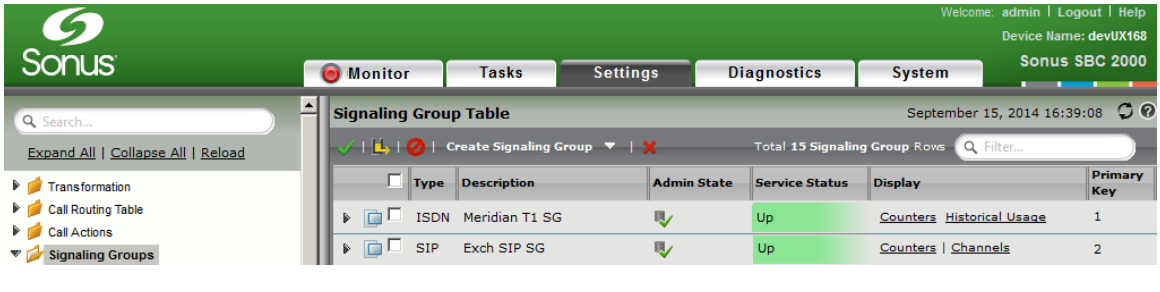


1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click **Create Signaling Group** and select **SIP Signaling Group**.
4. Fill in the fields as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



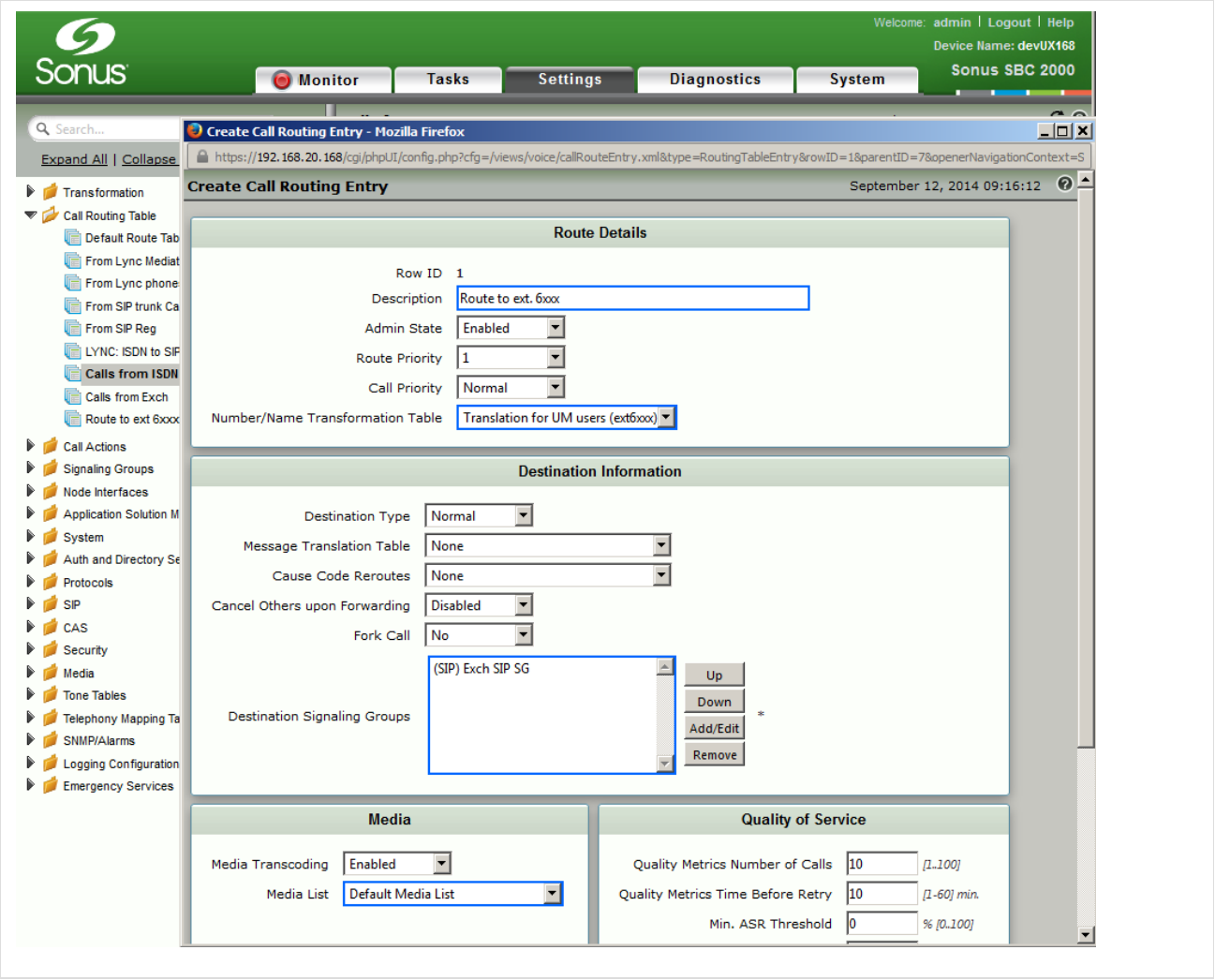
The Signaling Groups should appear like the following after adding the ISDN and SIP Signaling Groups:



Call Routing Table Entries

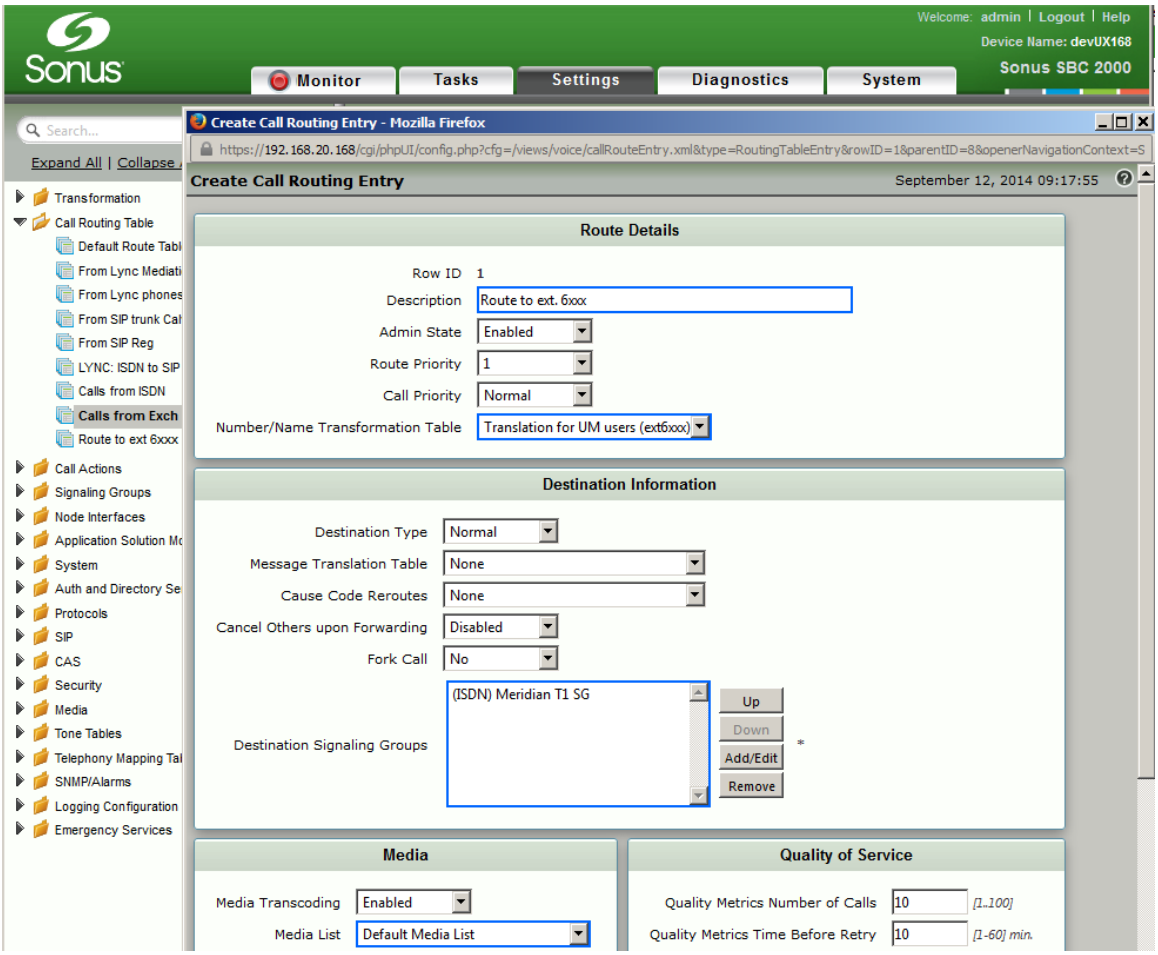
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table > (call route entry for ISDN)**.
3. Fill in the fields as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



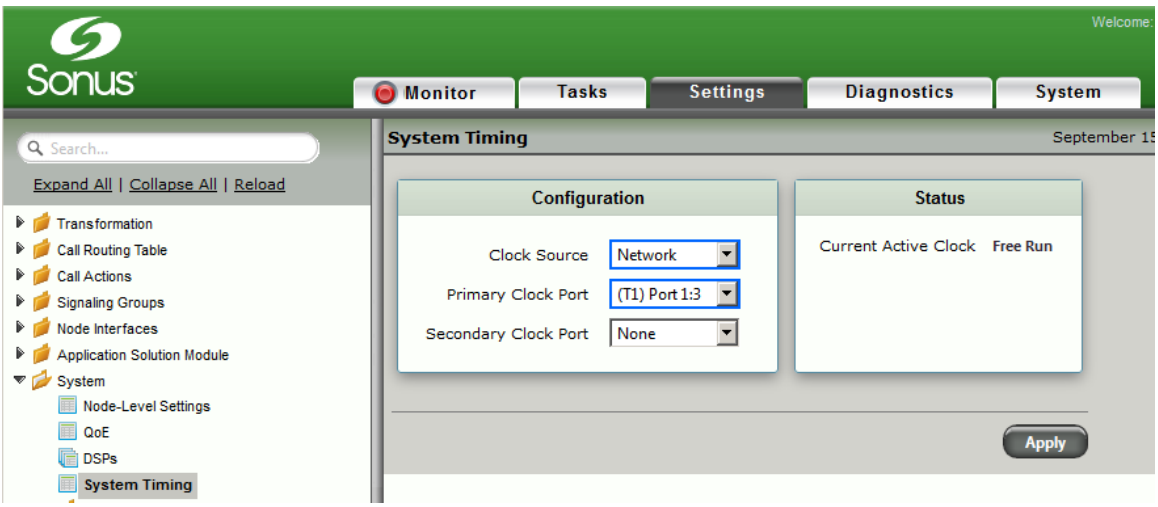
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table > (call route entry for SIP)**
3. Fill in the fields as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



System Timing Configuration

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > System Timing**.
3. Configure the Clock Source either as System or the Network, depending on your PBX timing settings.
   In this exercise, the Sonus SBC 1000/2000 node is reading the system time from the network therefore the configuration is done as shown below:
   For more information about system timing see, Configuring the System Clock Source.



Copyright © 2015 Sonus Networks. All rights reserved.

Exchange 20xx UM Server Configuration Steps:

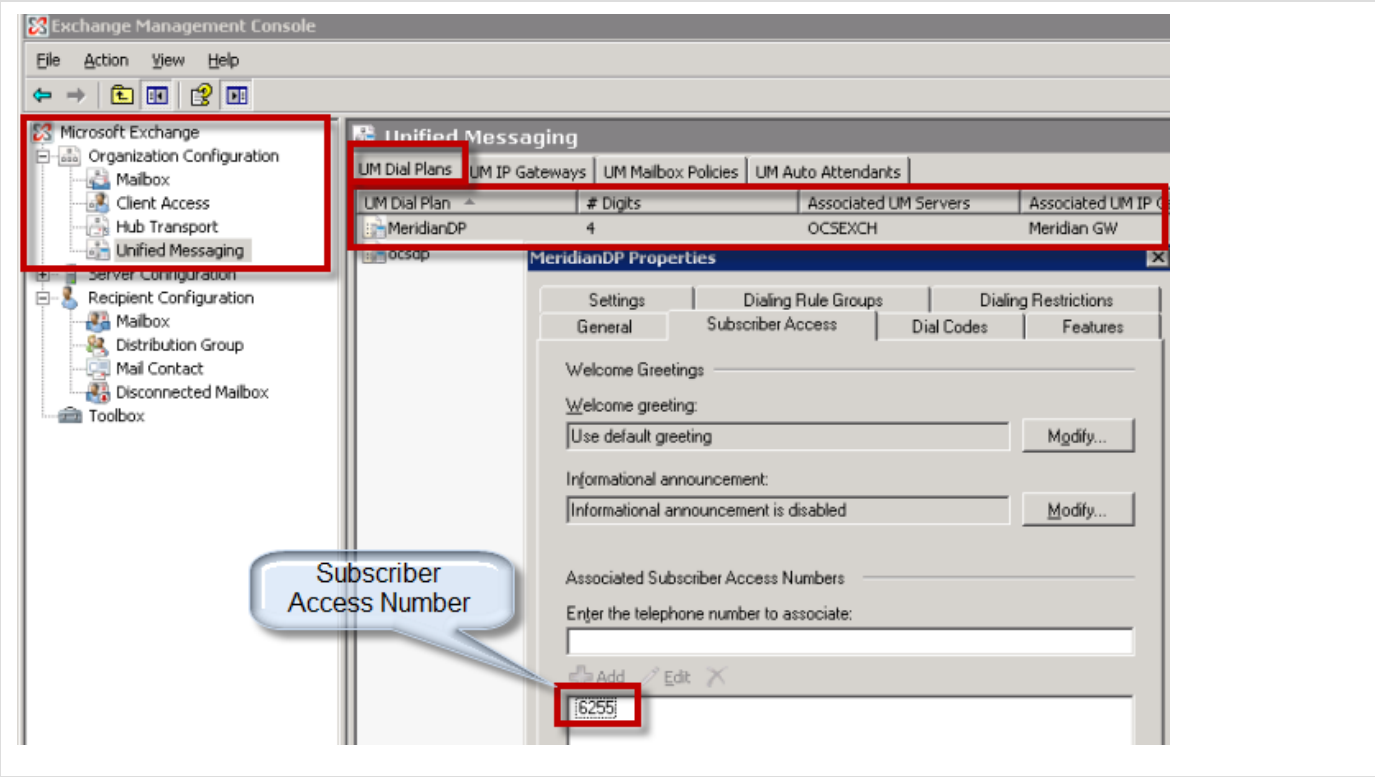
Exchange 20xx UM Server and Sonus SBC 2000 Gateway integration requires the following items to be configured on **Exchange Management Console**:

1. A Dial Plan configuration with:
    - Subscriber Access Number
    - UM Mailbox Policy
    - UM IP Gateway
    - UM Auto Attendant
2. UM Dial Plan association

Dial Plan Configuration

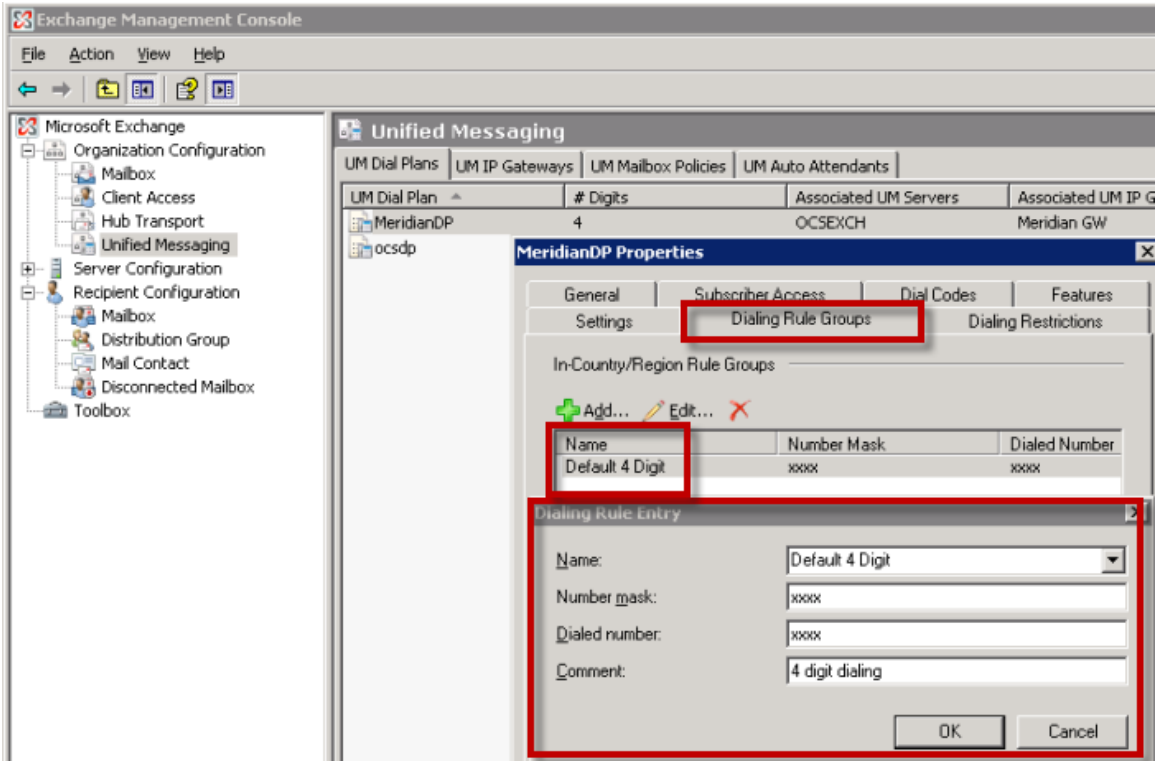
- Logon to Exchange / UM Server PC
- Launch **Exchange Management Console**
- Create a New Dial Plan using the following information:

Subscriber Access Number

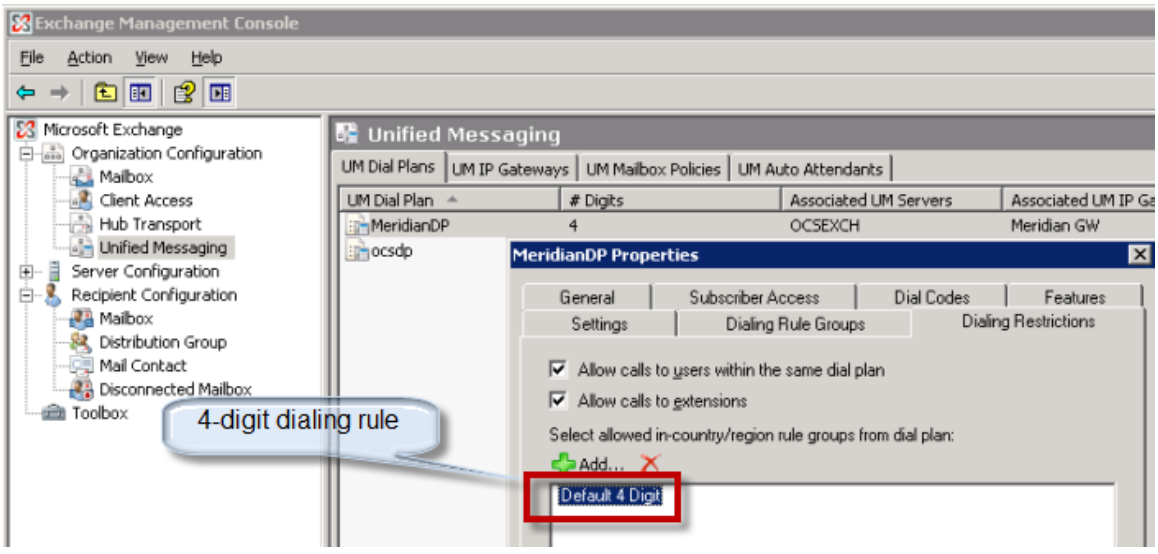


Dialing Rule Group for 4 digit dialing used in this example:

Copyright © 2015 Sonus Networks. All rights reserved.

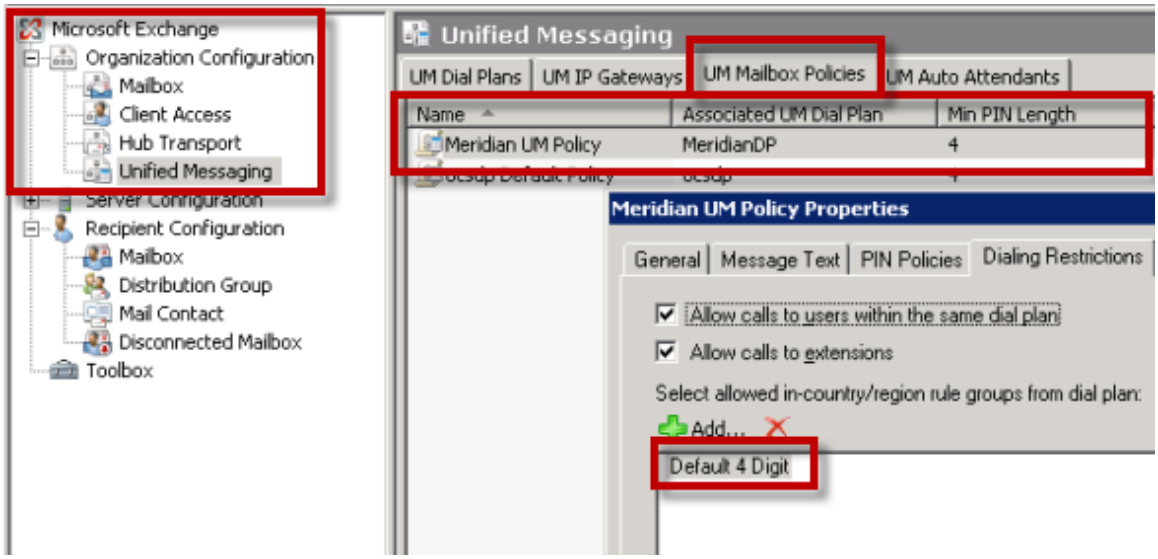


Dialing Restriction

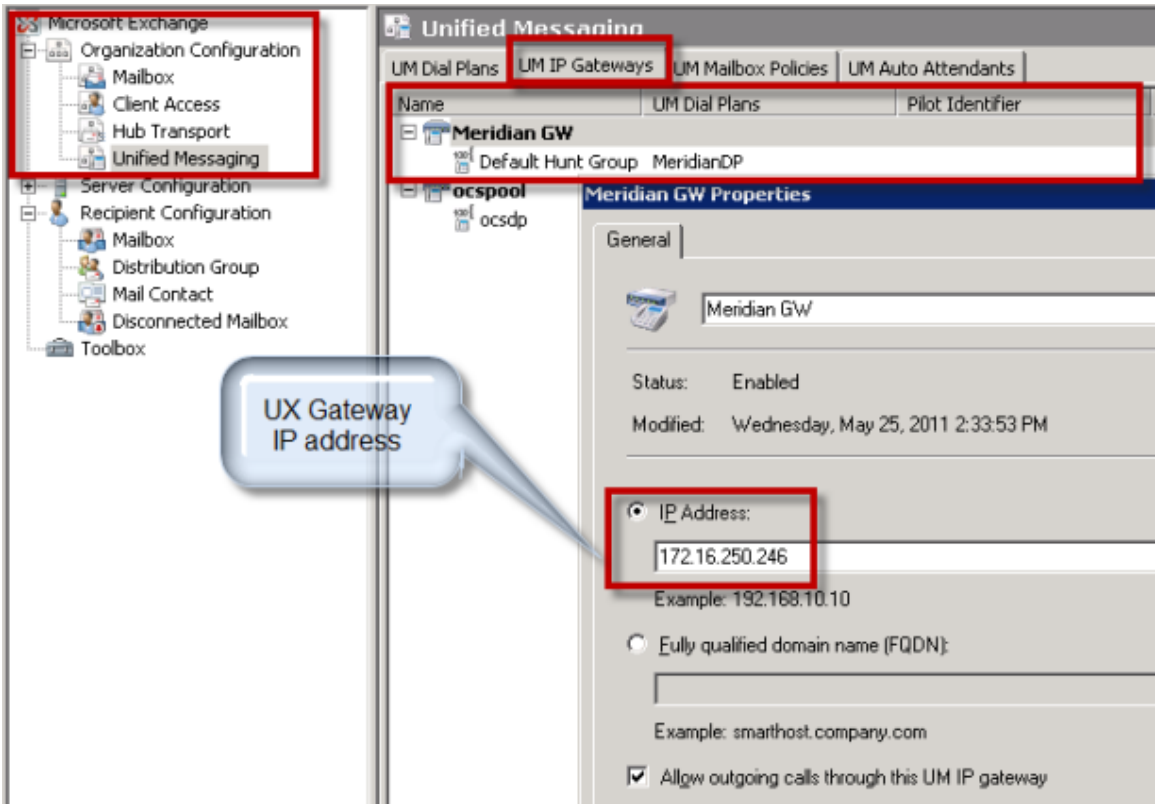


UM Mailbox Policy

Copyright © 2015 Sonus Networks. All rights reserved.

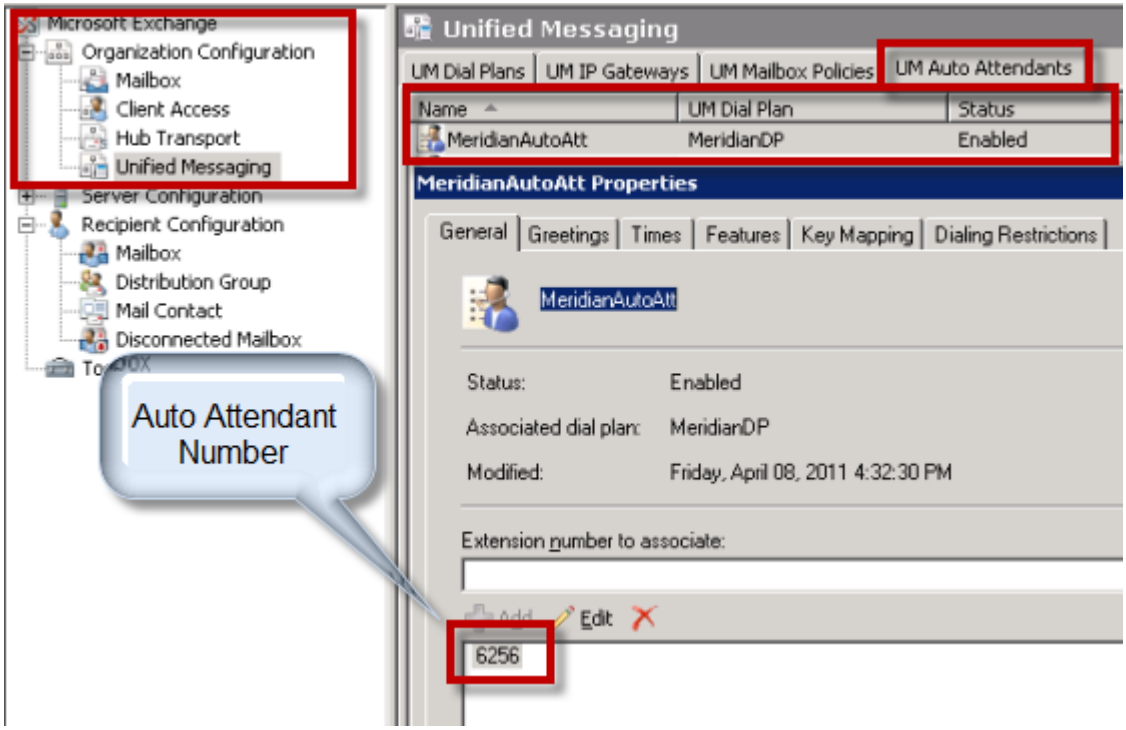


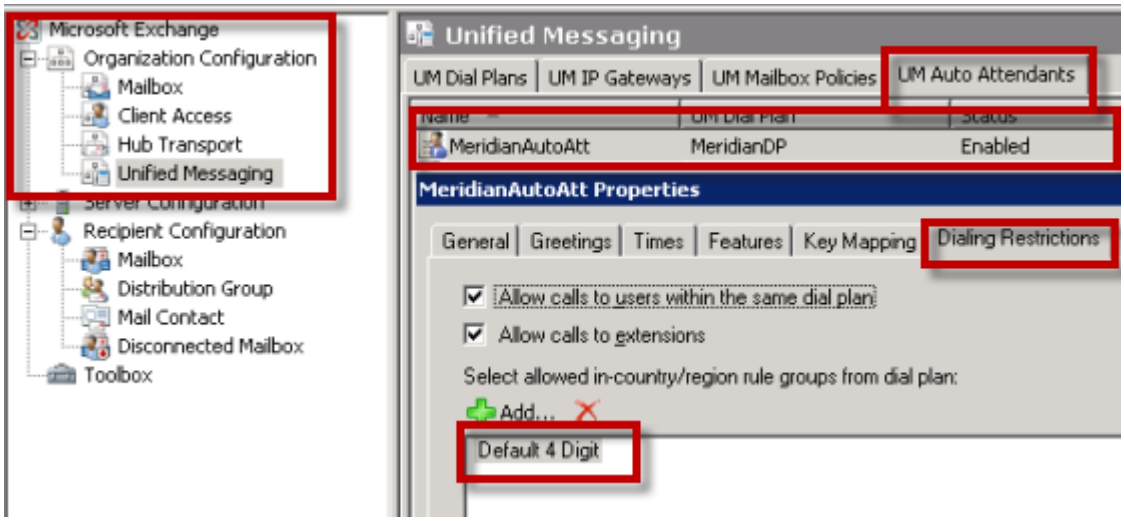
UM IP Gateway



UM Auto Attendants

Copyright © 2015 Sonus Networks. All rights reserved.

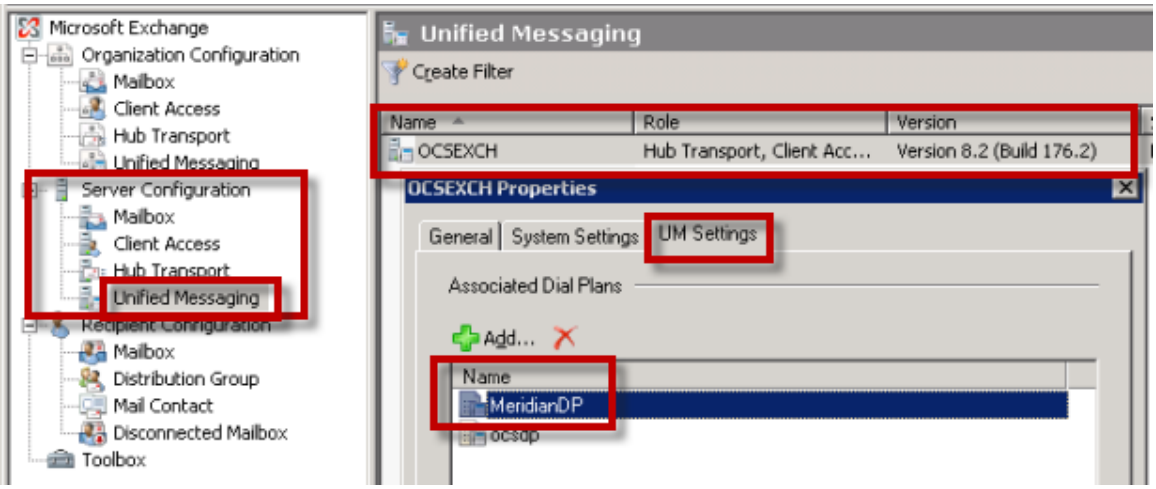




Associating Dial Plan to UM Server

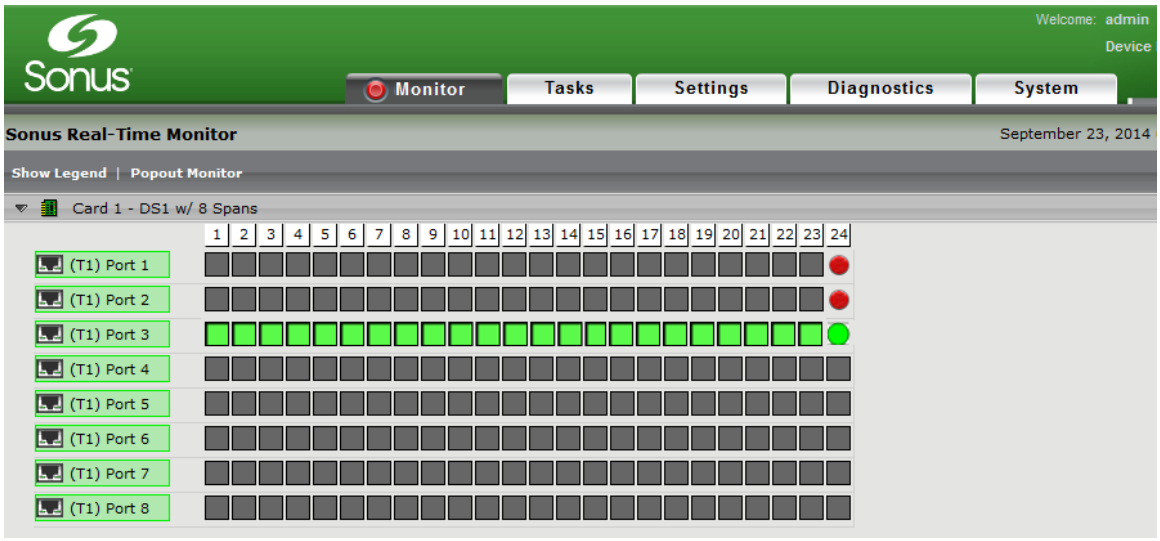
- Logon to Exchange / UM Server PC.
- Launch **Exchange Management Console**.
- Associate the relevant dial plan with the UM Server as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



Sonus SBC 1000/2000 Signaling Group Status Verification

After having completed both Sonus SBC 1000/2000 and Exchange 20xx Unified Messaging Server configuration steps, using the monitor view, ensure both PRI and SIP ports are up and in idle as shown below:

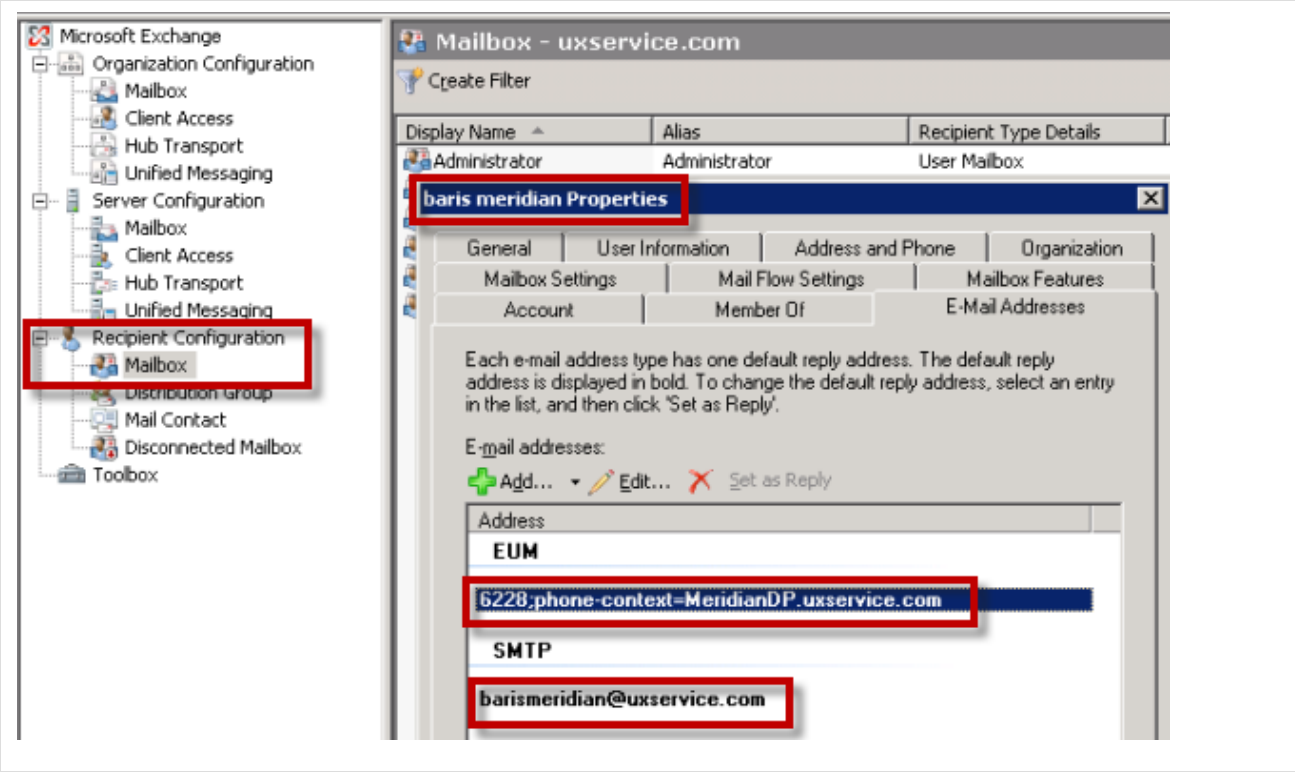


Common Use Case

In a **PBX – Sonus SBC 1000/2000 – eUM Server** scenario the following configuration steps allow PBX users to have UM voice mail boxes:

1. On the **PBX**, a user must be configured with a diversion number as the **Subscriber Access Number** (i.e: **6255**).
   This number is configured in the ***Exchange Management Console >> Organization Configuration >> Unified Messaging >> UM Dial Plan >> Subscriber Access tab***.
2. On the **eUM**, the relevant user entry must be enabled for **Unified Messaging**as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



3. When a PBX user-1 receives a call (i.e., from PBX user-2) and does not answer, the call is diverted by the PBX to the diversion number (6225). The call arrives at the Sonus SBC 1000/2000, and the Sonus SBC 1000/2000 sends an INVITE to the UM Server. Once the call reaches the UM Server, the Calling Party can leave a message in PBX user-1's voice mail box.
4. In addition, PBX user(s) can call a Subscriber Access (SA) Number (**6255**) and an Auto Attendant (AA) Number (**6256**) via 4 digit dialing in above setup to navigate UM prompts via DTMF or voice commands

Changing SIP Transport from MTLS - SRTP to TCP - RTP

This article describes the steps necessary to modify the Sonus SBC 1000/2000 configuration such that the SIP Transport is changed from TLS/SRTP (MTLS/SRTP) to TCP/RTP.

For the purposes of this article it is assumed that **PBX – Sonus SBC 1000/2000 – Microsoft Lync 2010** configuration is in place already with MTLS/SRTP as SIP Transport. This particular Sonus SBC 2000 configuration is explained in Sonus SBC 1000/2000 configuration for Deployment in PSTN - Sonus SBC 1000/2000 - Microsoft LYNC 2010 Setup.

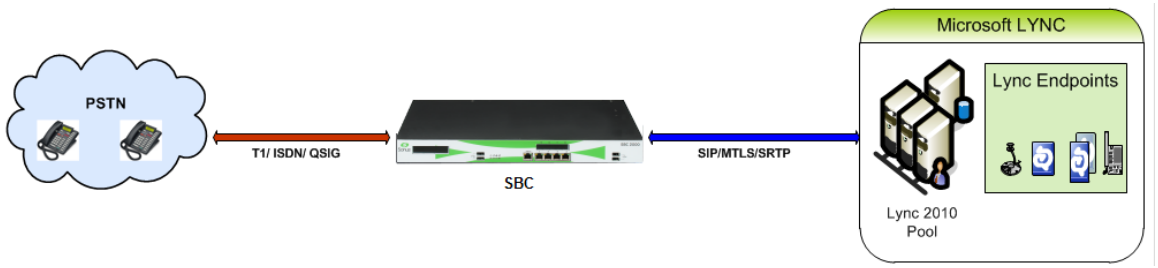
The process requires changes on both the Sonus SBC 1000/2000 and on the Lync Server. The six steps to accomplish the change are:

1. Edit the appropriate Signal Group on the Sonus SBC 1000/2000.
2. Edit the appropriate Media List on the Sonus SBC 1000/2000.
3. Edit the appropriate SIP Server Table on the Sonus SBC 1000/2000.
4. Edit the port and protocol settings on the Lync Server.
5. Publish the altered topology
6. Stop/Restart the Lync Mediation Server service.

Topology Before

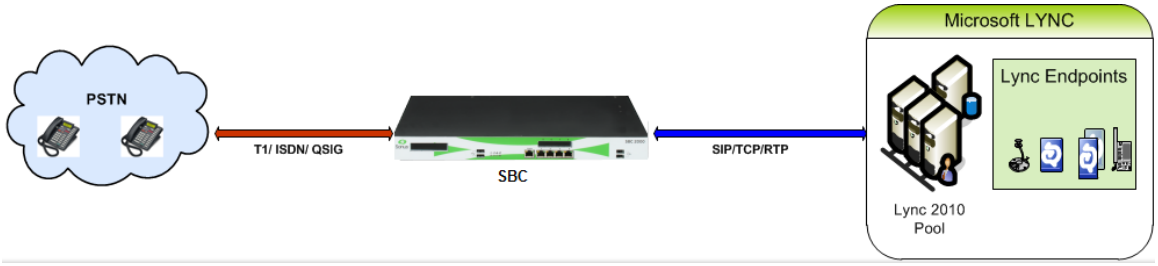
Copyright © 2015 Sonus Networks. All rights reserved.

PBX – Sonus SBC 1000/2000 – Microsoft Lync 2010 configuration in place with MTLS/SRTP as SIP Transport



Topology After

PBX – Sonus SBC 1000/2000 – Microsoft Lync 2010 configuration in place with TCP/RTP as SIP Transport



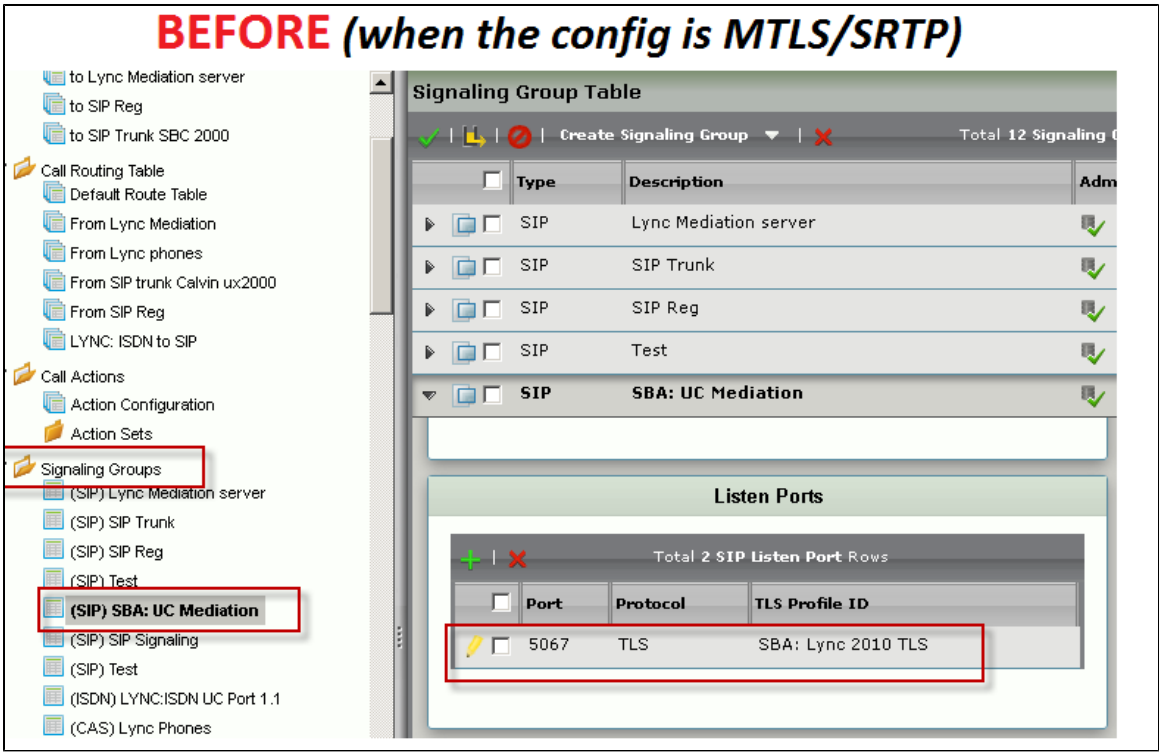
- Sonus SBC 1000/2000 Configuration Changes
  - SIP Signaling Group
  - Media List
  - SIP Server Table
- Lync Changes (Topology Builder)
  - PSTN Gateway Properties Change
  - Publish Topology
- Lync Mediation Server Service Restart

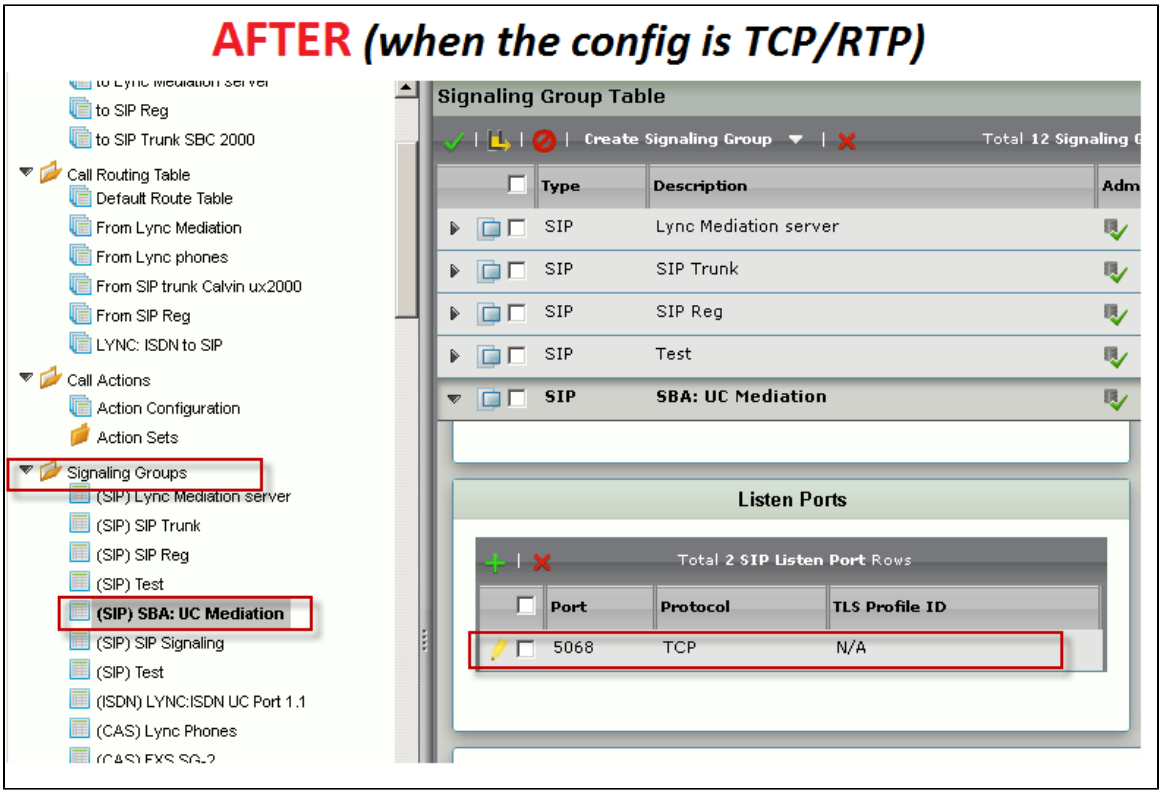
Sonus SBC 1000/2000 Configuration Changes

SIP Signaling Group

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups > (relevant SIP Signaling Group)**.
3. Change the Listening Ports configuration to 5068, as shown below.
4. Change the **TLS Profile ID** to N/A.

Copyright © 2015 Sonus Networks. All rights reserved.

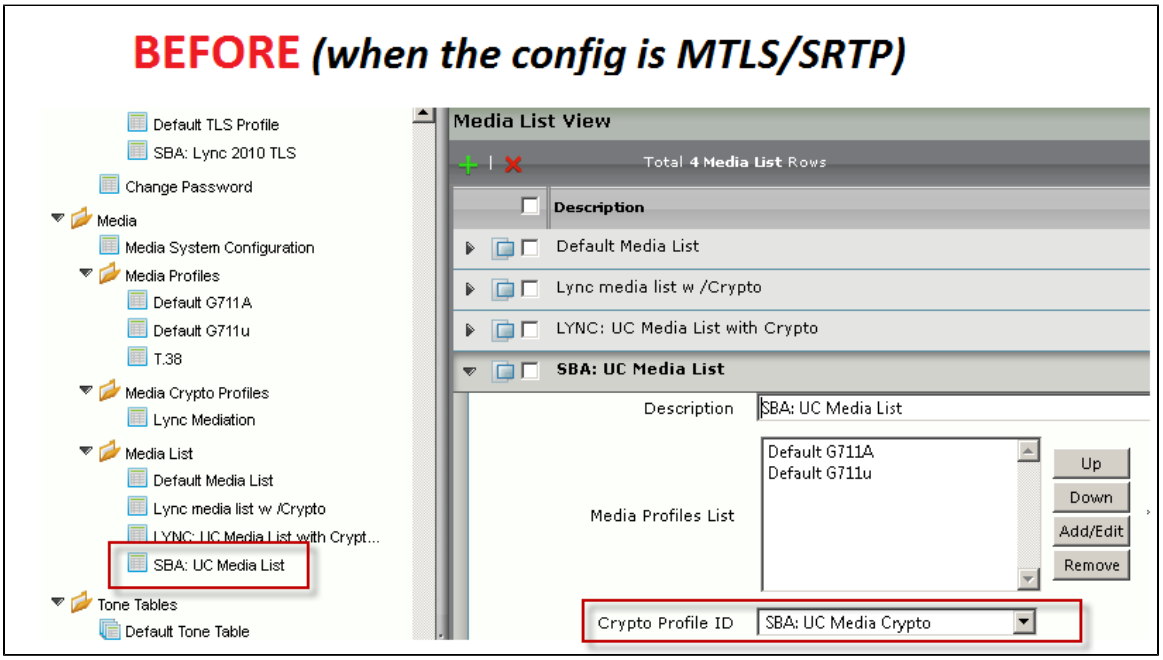


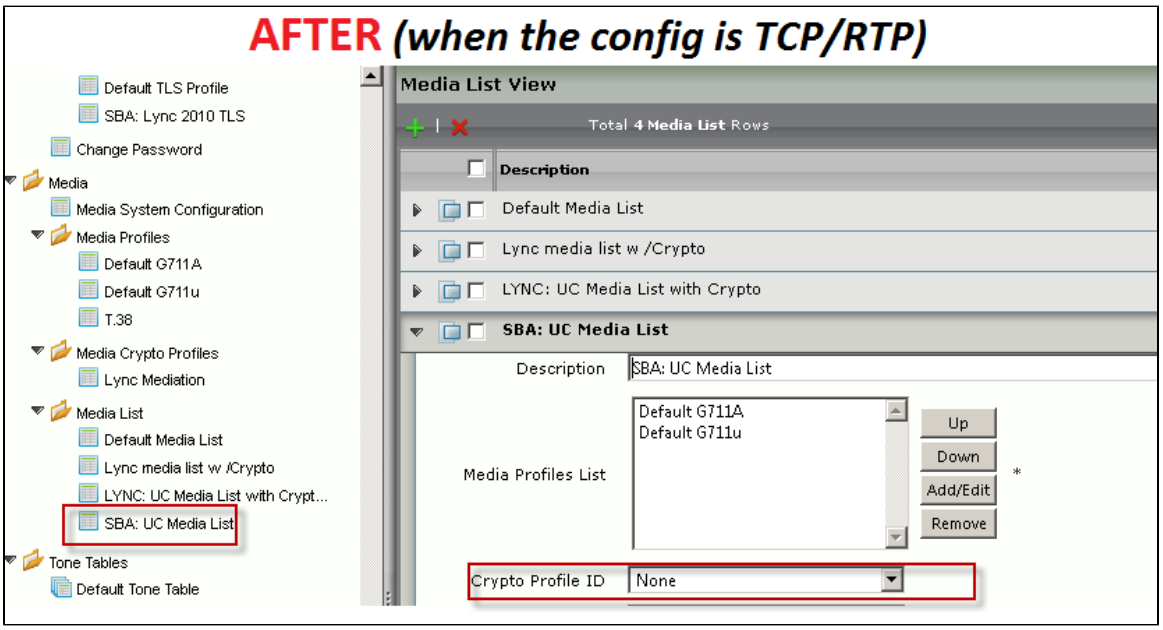


Media List

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Media > Media List > (relevant media list entry)**.
   This is the Media List specified in the SIP Signaling Group above.
3. Change the **Crypto Profile ID** value to **None** as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.

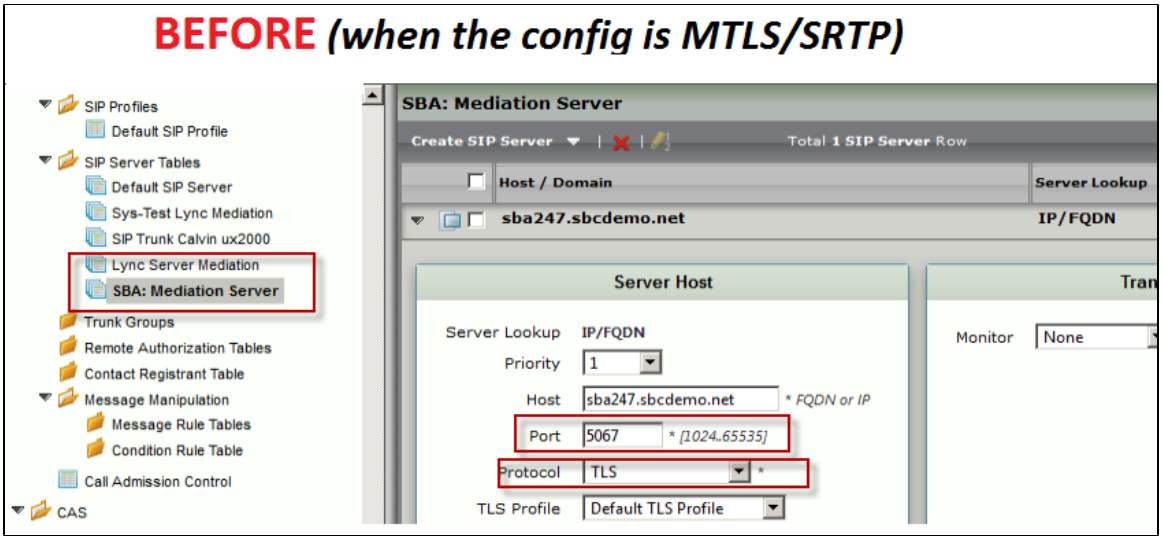


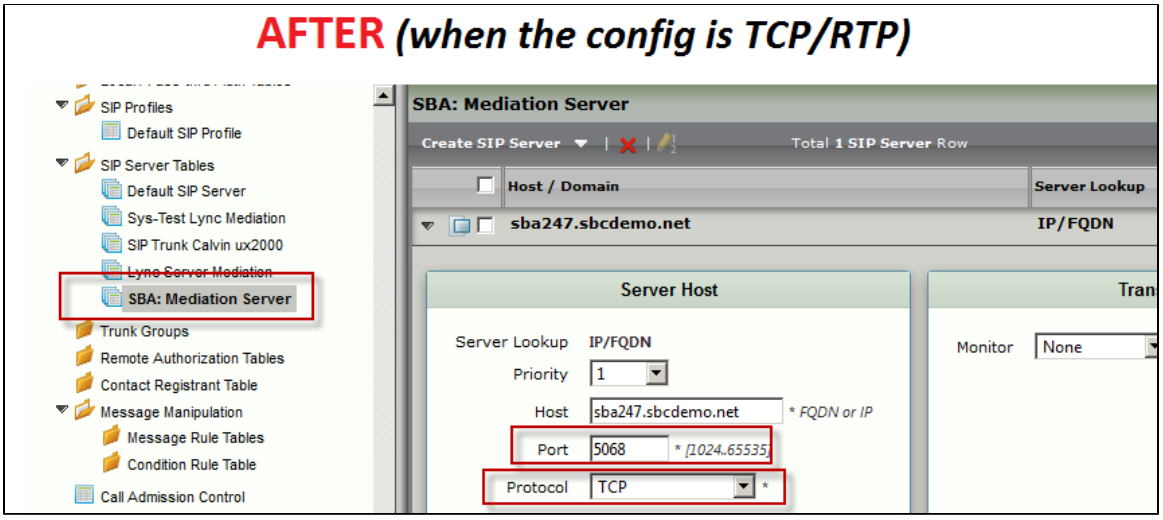


SIP Server Table

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Server Tables >(relevant SIP Server Table Entry)**.
3. Change the **Port** value to 5068, as shown below.
4. Change the **Protocol** value to TCP, as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.





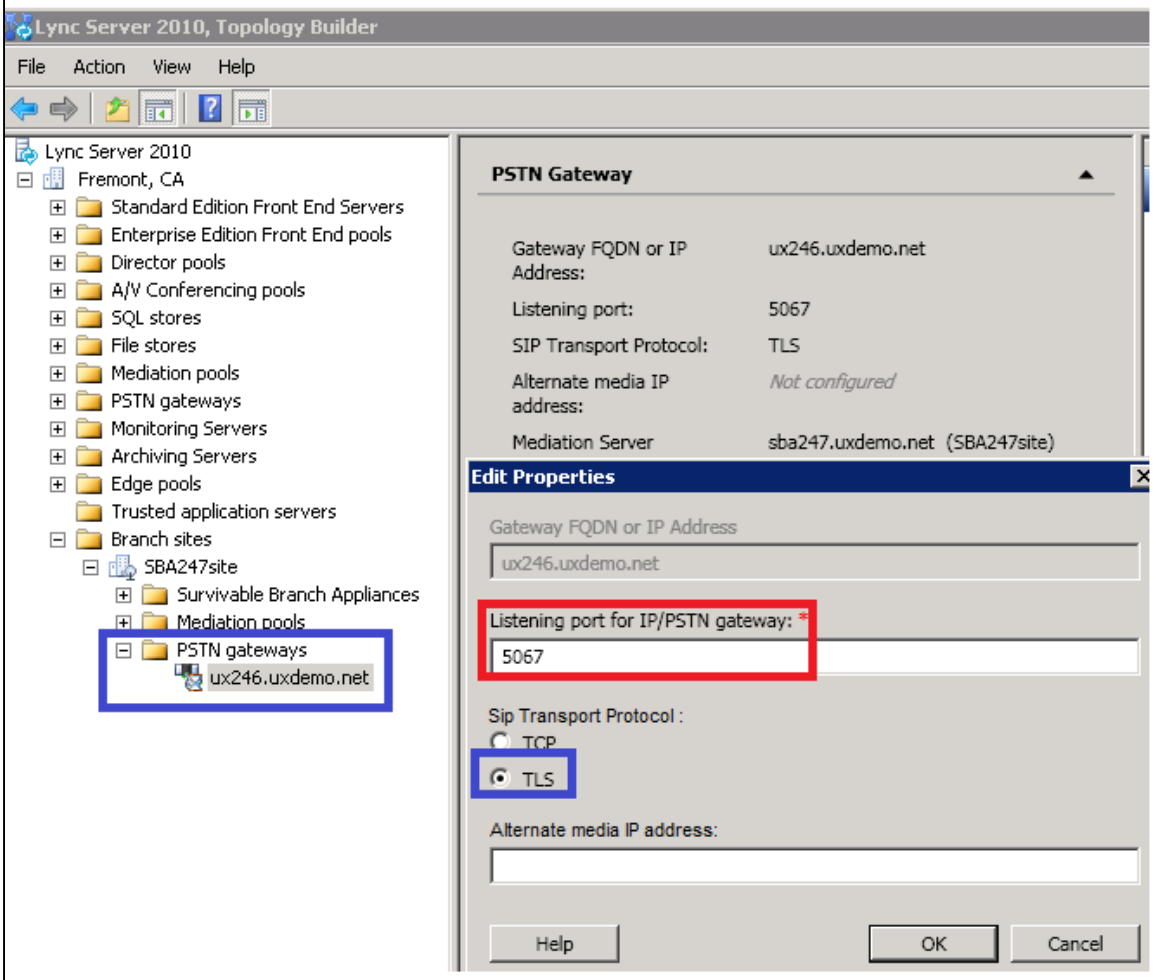
Lync Changes (Topology Builder)

PSTN Gateway Properties Change

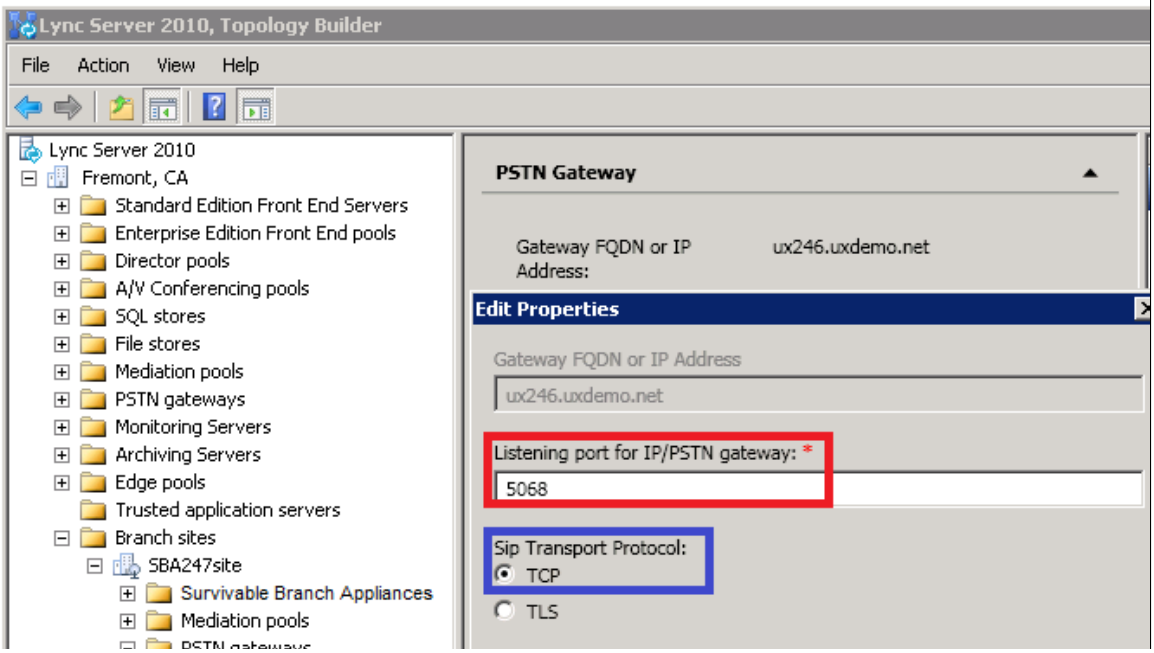
1. Log into the Lync front end server PC.
2. Launch the **Lync Server 2010 Topology Builder**.
3. In the Navigation Tree, go to **Branch Sites > PSTN gateways > (relevant Sonus SBC 1000/2000 entry)**.
4. Right-click the relevant Sonus SBC 1000/2000.
5. Select **Edit Properties...**
6. Change the **Listening Port for IP/PSTN gateway** to 5068, as shown below.
7. Change the **SIP Transport Protocol** to TCP, as shown below.
8. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.

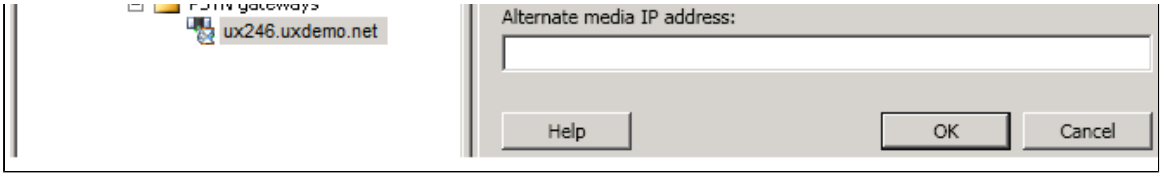
BEFORE ***(when the config is MTLS/SRTP)***



AFTER ***(when the config is TCP/RTP)***



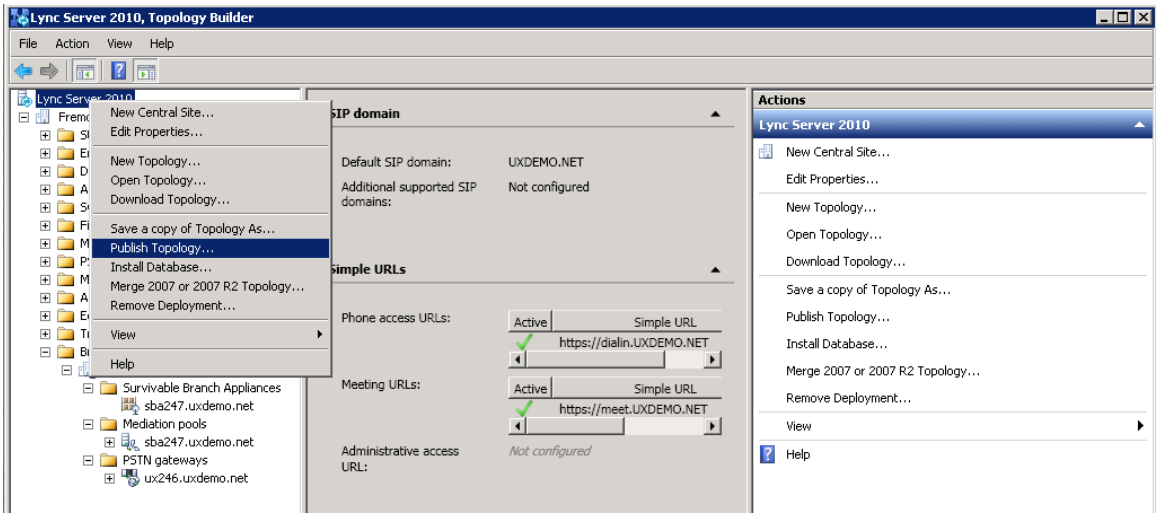
Copyright © 2015 Sonus Networks. All rights reserved.



Publish Topology

To publish the topology:

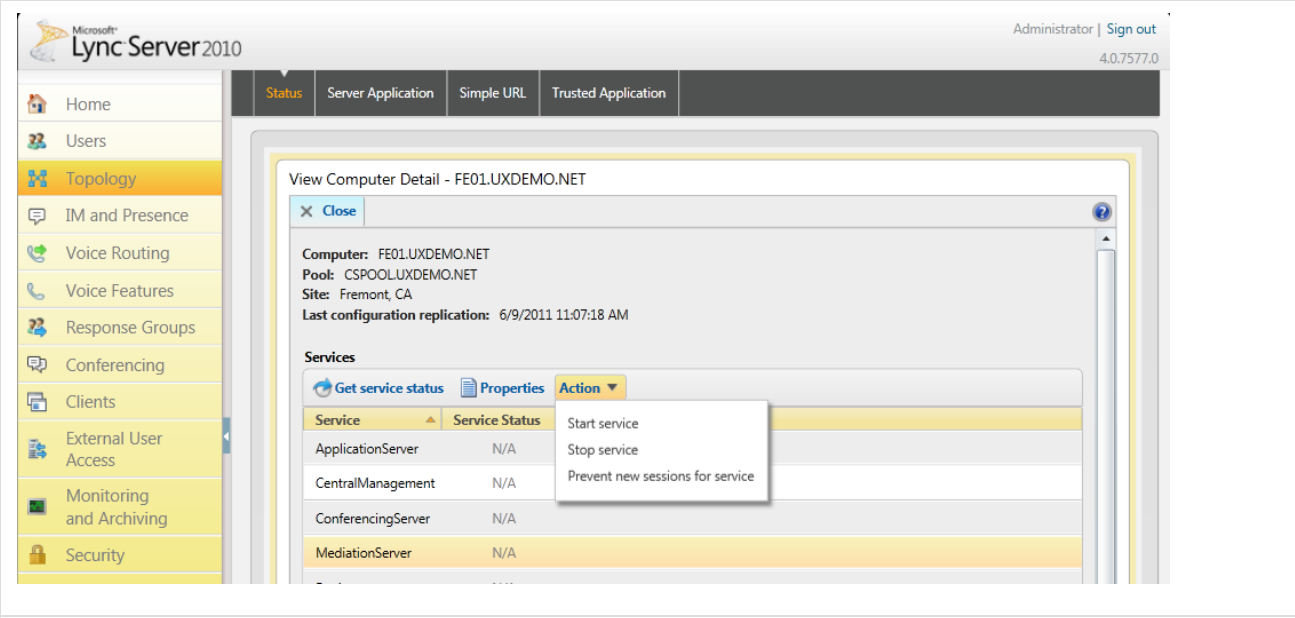
1. In the Topology Builder navigation tree, right-click **Lync Server 2010**.
2. Select **Publish Topology...**.



Lync Mediation Server Service Restart

1. Launch the **Lync Server 2010 Configuration**page
    a. In your brorwser, go to (the FQDN of the front end pool//cscp).
2. Select the *Mediation Server in the Service list.
3. Select **Stop service** from the **Action** drop-down list, as shown below.
4. Select **Start service** from the **Action**drop-down list, as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



Call Forking Based on Active Directory User Attributes

This article describes the steps necessary to configure the Sonus SBC 1000/2000 to fork calls using User attributes stored in Active Directory by employing Sonus SBC 1000/2000's **Transformation** and **Call Forking** features.

In this example we use a **PSTN - Sonus SBC 2000 - Lync/SBA** environment, and we want to route all calls from PSTN to Lync clients to a Lync user, and we want them forked to the same Lync user's mobile and IP phone numbers using attributes from the user's AD record.

On this Page

- Call Forking Logic Overview
- Before You Begin
  - Verify the Call Forking License
  - Verify Lync/SBA Configuration and AD Integration
  - Related Information
- Sonus SBC 1000/2000 Configuration
  - Transformation Table Configuration
  - Call Routing Table
  - Inbound ISDN Signaling Group

Related Articles

- Working with Microsoft Unified Communications
- Call Routing Based on Active Directory User Attributes

Call Forking Logic Overview

Copyright © 2015 Sonus Networks. All rights reserved.

A PBX phone 6222 dials the Lync/SBA user's extension number 1005, resulting in the call landing on the inbound ISDN Signaling Group on Sonus SBC 1000/2000. The call is then routed using the relevant Call Route Table triggering the relevant sequence of events:

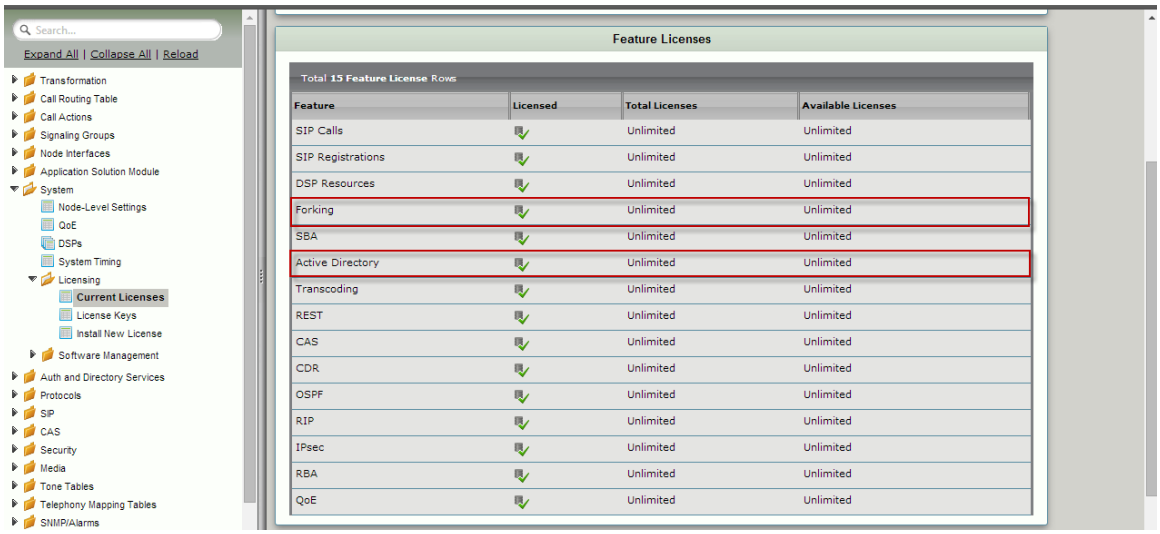
1. In the Call Route Entry, where the call forking option is enabled, the number is normalized first using the relevant call Transformation Table, and then gets routed to the relevant outbound Signaling Group (in this exercise, the call goes to a Lync user using by a SIP SG).
2. The call continues with the next Call Route Entry, where the call forking option is also enabled. The number is normalized using the relevant Transformation Table using the **cached Active Directory user attributes**, resulting in the call to get routed to the relevant outbound signaling group (in this exercise, the call goes to outbound SIP signaling group to reach out to Lync/SBA user's IP phone).
3. Lastly, the routing continues with the next Call Route Entry (where the call forking option is **disabled**, denoting the last forked call leg). The number is normalized using the relevant Transformation Table using the cached Active Directory user attributes, and the call is routed to the relevant outbound signaling group (in this exercise call goes to outbound ISDN signaling group to reach out to Lync/SBA user's mobile device).

Before You Begin

Before you begin, you'll need to verify the following:

Verify the Call Forking License

1. In Sonus SBC 1000/2000 WebUI, click the **Settings** Tab.
2. In the left navigation pane, go to **System > Licensing > Current Licenses**.
3. Verify that Call Forking Feature is licensed as shown below.



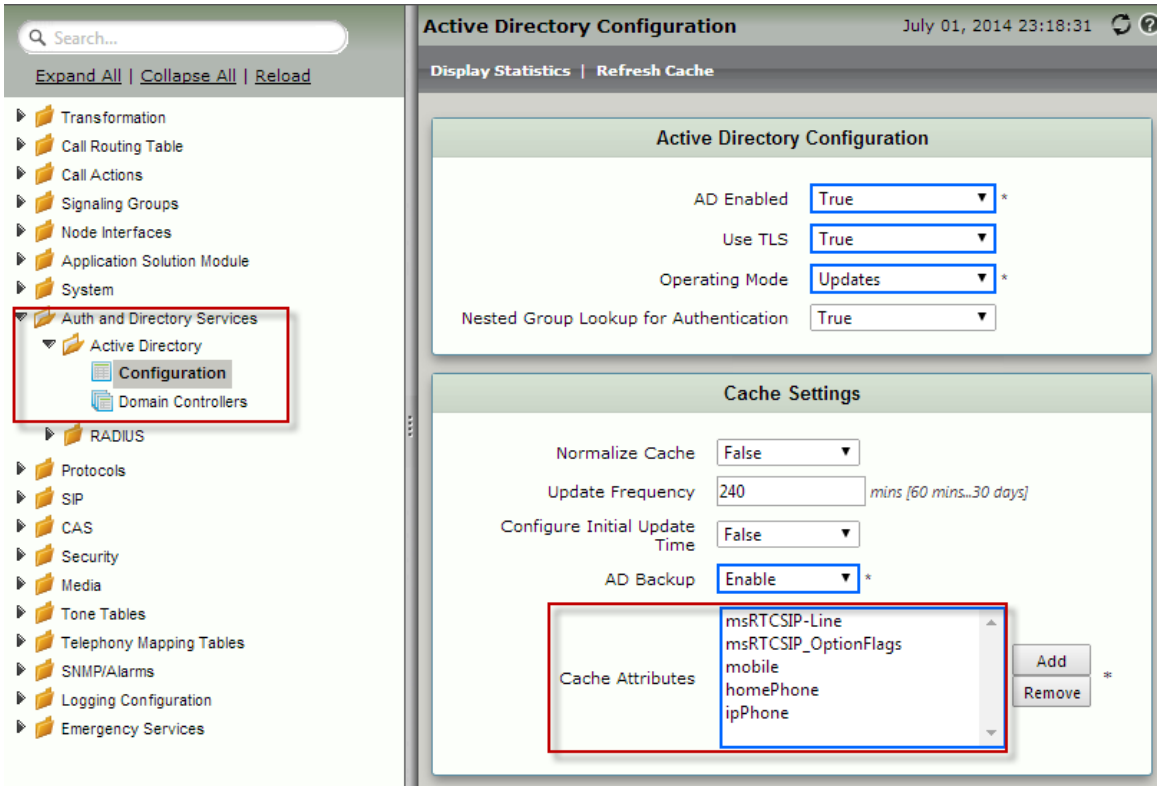
Verify Lync/SBA Configuration and AD Integration

Before you begin, make sure the Sonus SBC 1000/2000 is configured and integrated with Lync/SBA as described in Call Routing Based on Active Directory User Attributes. In addition to this, verify the Sonus SBC 1000/2000 Active Directory settings:

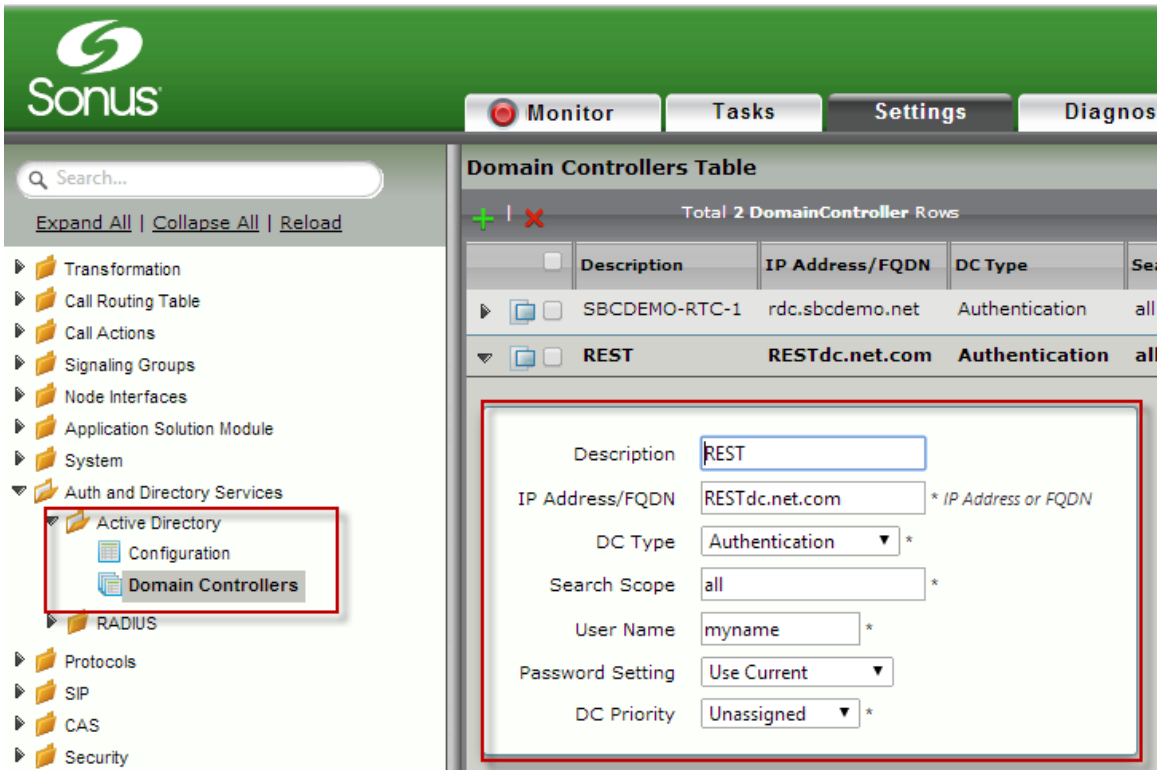
Please note: this article ONLY describes the steps necessary to configure the call forking feature.

Active Directory Configuration

Copyright © 2015 Sonus Networks. All rights reserved.



Active Directory Domain Controller Configuration



Related Information

- Calling Party: PSTN phone 6222

Copyright © 2015 Sonus Networks. All rights reserved.

- Called Party: Lync client with following AD profile:
  - userPrincipalName: `SBAagent1@Sonus SBC 1000/2000DEMO.Sonus`
  - ipPhone: 9911
  - mobile: 6228
  - msRTCSIP-Line: `tel:+15102461005`

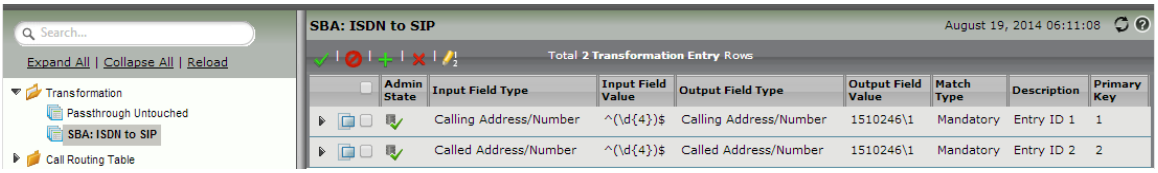
Sonus SBC 1000/2000 Configuration

In this section, we provide a step-by-step configuration walk through enabling the use of Call Forking on the Sonus SBC 1000/2000:

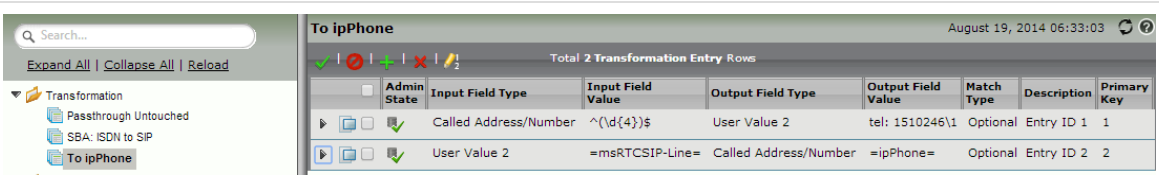
Transformation Table Configuration

We will need three Transformation Tables created as shown below:

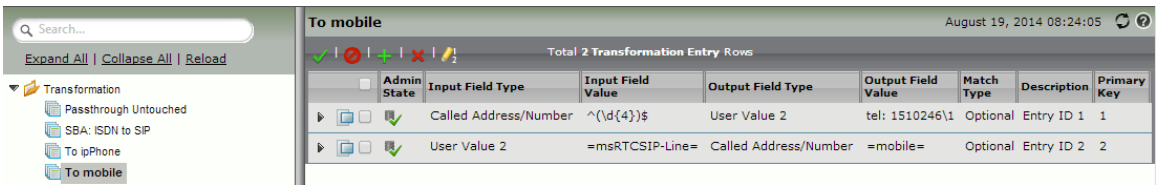
1. **To SIP (Lync) transformation**
   - Configure the "Calling Address/Number" and "Called Address/Number" translations



2. **To ipPhone attribute transformation:**
   - Configure the "Called Address/Number" translations to normalize it to a "User Value" of AD attribute format (`msRTCSIP-Line`)
   - Configure the "User Value" translation to another AD attribute format "ipPhone"



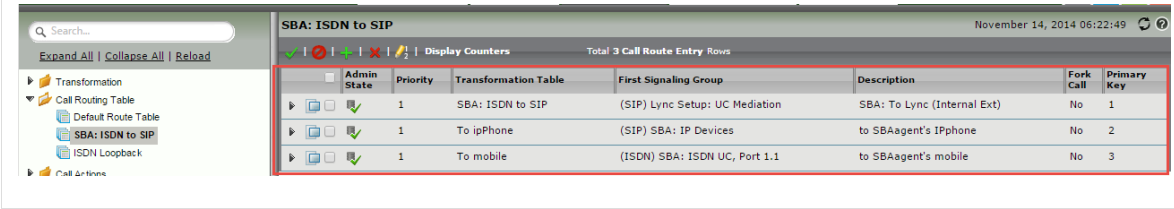
3. **To mobile attribute transformation:**
   - Configure the "Called Address/Number" translations to normalize it to a "User Value" of AD attribute format (`msRTCSIP-Line`)
   - Configure the "User Value" translation to another AD attribute format "mobile"



Call Routing Table

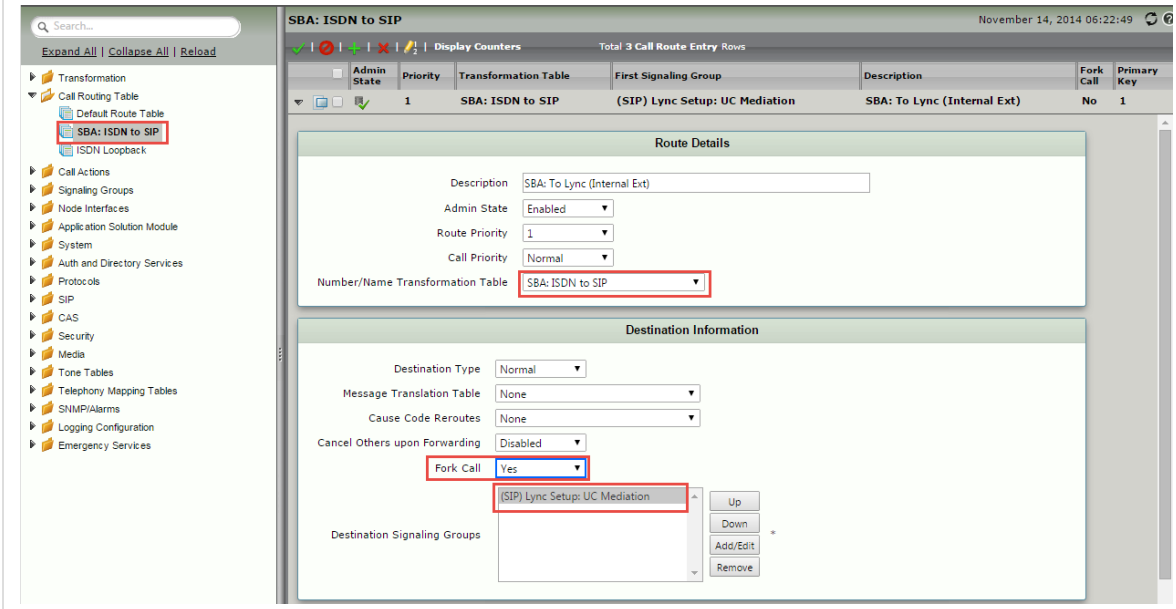
We create three entries in a Call Route used for ISDN to Lync calls, as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



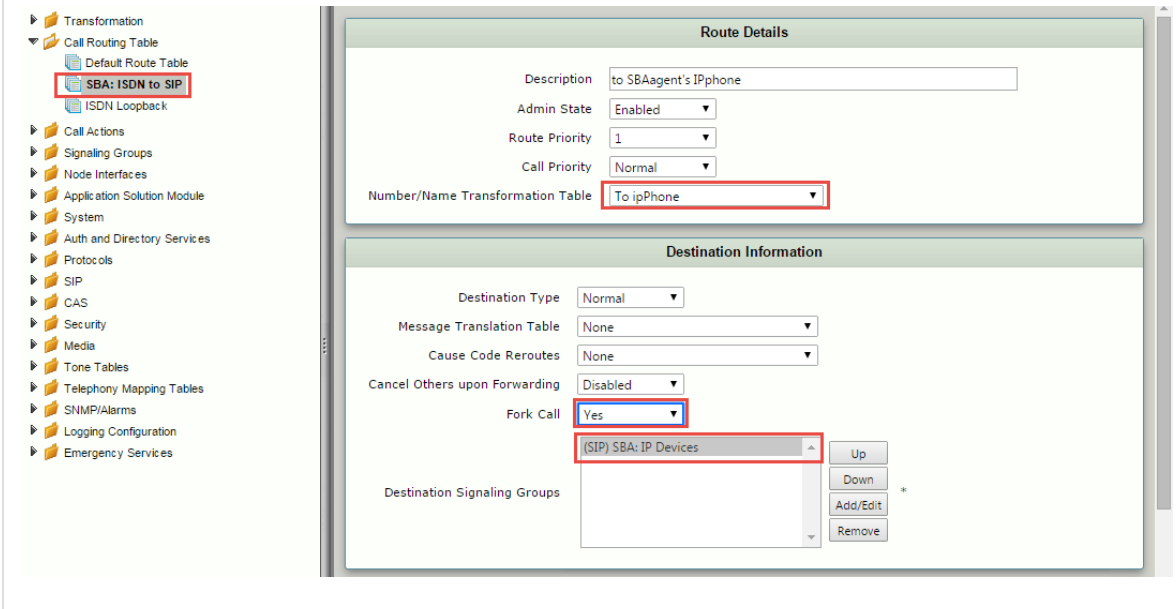
1. **ISDN to Lync/SBA client route entry**

   Note that **Fork Call** is set to **Enabled**, so for a particular call will continue.



2. **ISDN to Lync/SBA client's ipPhone route entry**

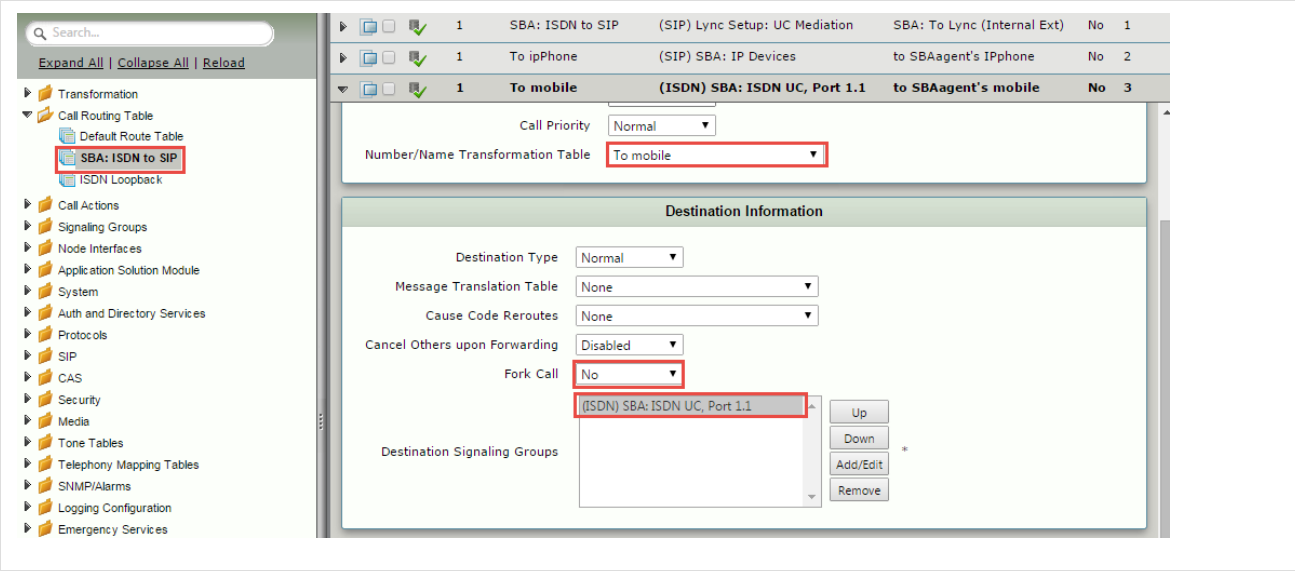
   Note that **Fork Call** is set to **Enabled**, so routing for a particular call will continue.



3. **ISDN to Lync/SBA client's mobile device route entry**

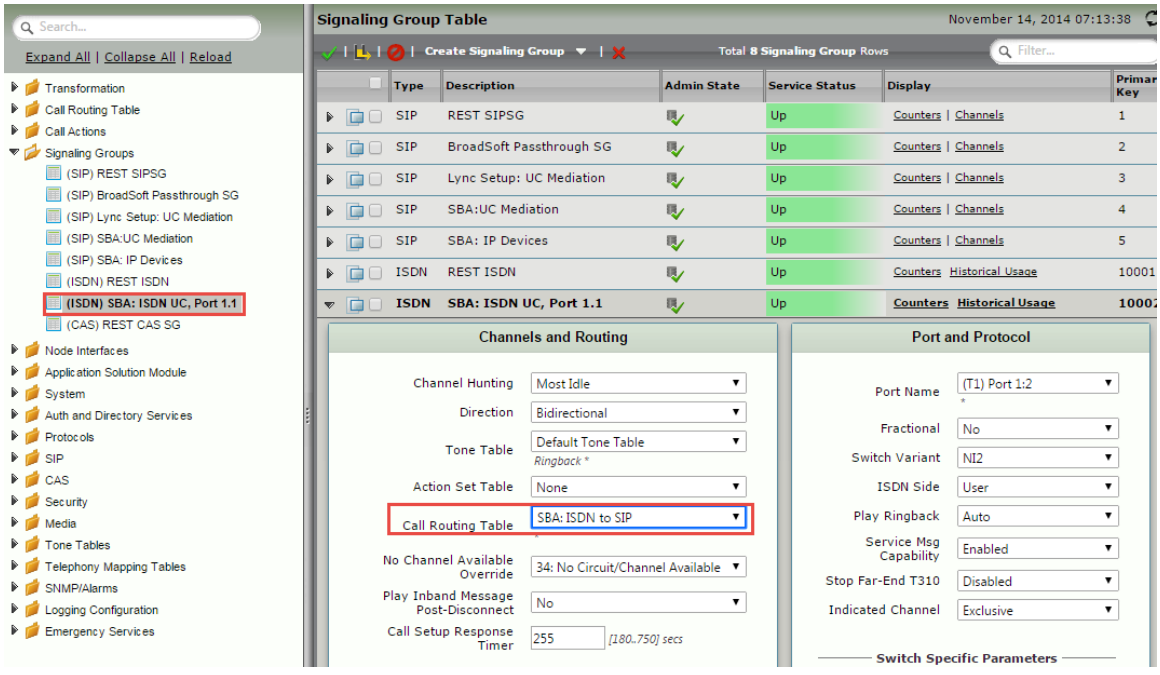
   Note that **Fork Call** is set to **Disabled**, so routing for a particular call will stop at this entry.

Copyright © 2015 Sonus Networks. All rights reserved.



Inbound ISDN Signaling Group

The ISDN signaling group for inbound calls is configured to use the relevant Call Routing Table (configured in the previous section):



> See Call Routing Based on Active Directory User Attributes for more information on call routing via Active Directory.

Call Routing Based on Active Directory User Attributes

In this article, we illustrate how to configure the Sonus SBC 1000/2000 to query the User attributes stored in the Sonus SBC 1000/2000's Active Directory Cache in order to route calls to a user's mobile phone:

- Call Routing Logic Overview

Copyright © 2015 Sonus Networks. All rights reserved.

- Active Directory Related Setup
  - AD Query User
  - Verification of Active Directory License
  - Domain Controller Settings
  - Active Directory Configuration
  - AD Query Functionality Verification
- Telephony Routing Setup
  - Transformation Table Configuration
  - Call Routing Table
- Verification of Call Routing using AD attributes

Call Routing Logic Overview

In this example, a call arrives from PSTN on a TDM port associated with an ISDN Signaling Group (SG), the SG points to a Call Routing Table which in turn specifies a Transformation Table.

The Transformation Table contains two entries, the first transformation strips the last four digits from the **Called Number** and appends them to a string `tel:+1510774` for which the first part constitutes of a valid AD `msRTCSIP-Line` Active Directory user attribute entry. The second entry takes an `msRTCSIP-Line` entry and outputs the corresponding mobile phone number to the Destination Signaling Group.

For the purpose of this example the parties to the call and their relevant attributes are:

- Calling Party: PSTN phone 6228
- Called Party: Lync client with following AD profile:
  - userPrincipalName: `baris@Sonus SBC 1000/2000DEMO.Sonus`
  - homePhone: 3633
  - mobile: 6223
  - msRTCSIP-Line: `tel:+15105743633;ext=3633`
  - mail: `Baris@uxdemo.net`



To see how Sonus SBC 1000/2000 call routing works in general, refer to Working with Telephony Routing.

Active Directory Related Setup

AD Query User

In order to perform a successful query of either the AD cache or to query AD directly, a valid domain user must be specified in the Active Directory Configuration panel (see AD config section below. **User Name** field).

The AD query user must be a domain user. For this exercise, the following user is created in Sonus SBC 1000/2000DEMO.Sonus domain where Lync is deployed.

- userPrincipalName: `queryUser@Sonus SBC 1000/2000DEMO.Sonus`
- dn: `CN=queryUser,OU=Lync Clients,DC=Sonus SBC 1000/2000DEMO,DC=Sonus`

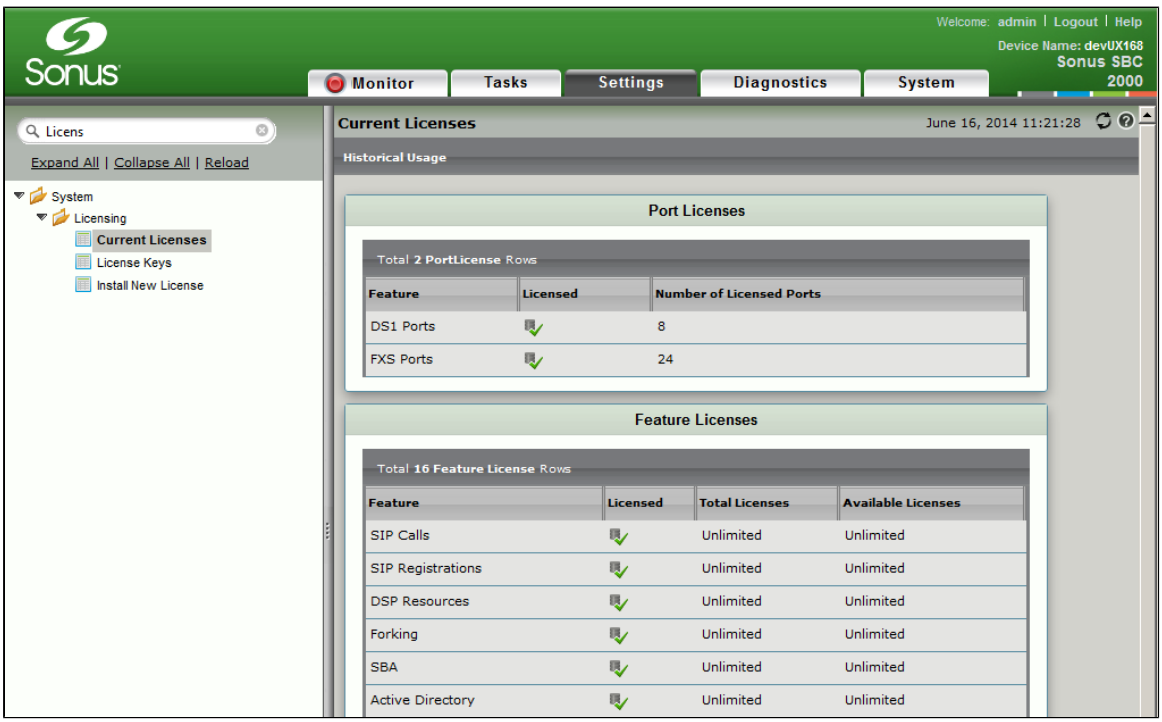
Verification of Active Directory License

Active Directory based call routing can only be preformed with an AD feature license - ensure you have this license installed:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Licensing > Current Licenses**.

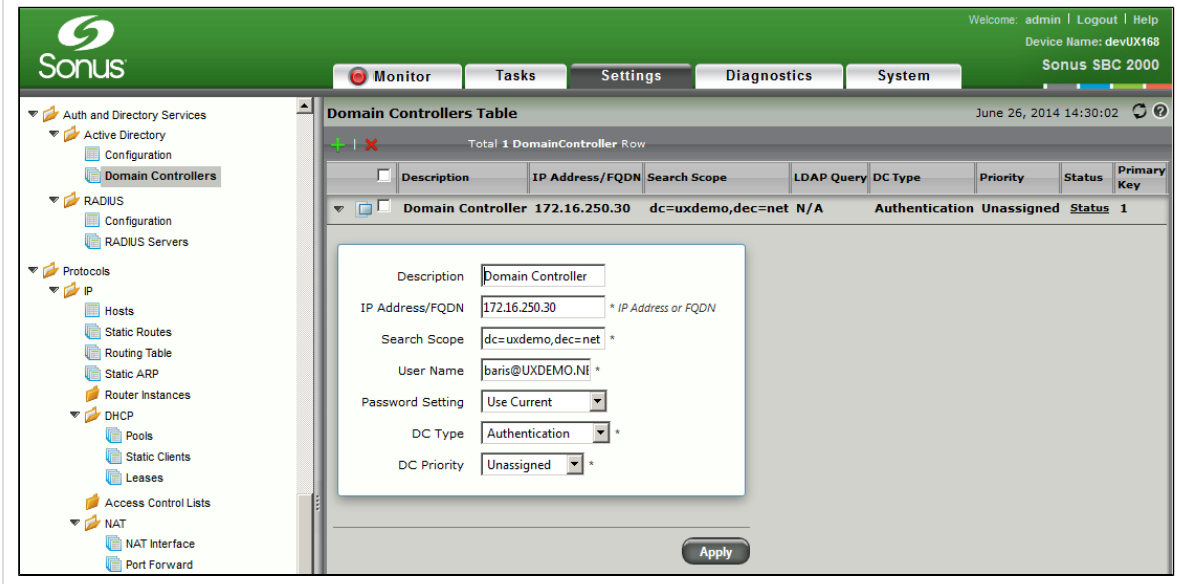
Copyright © 2015 Sonus Networks. All rights reserved.

3. Verify that the Active Directory feature is licensed as shown below.



Domain Controller Settings

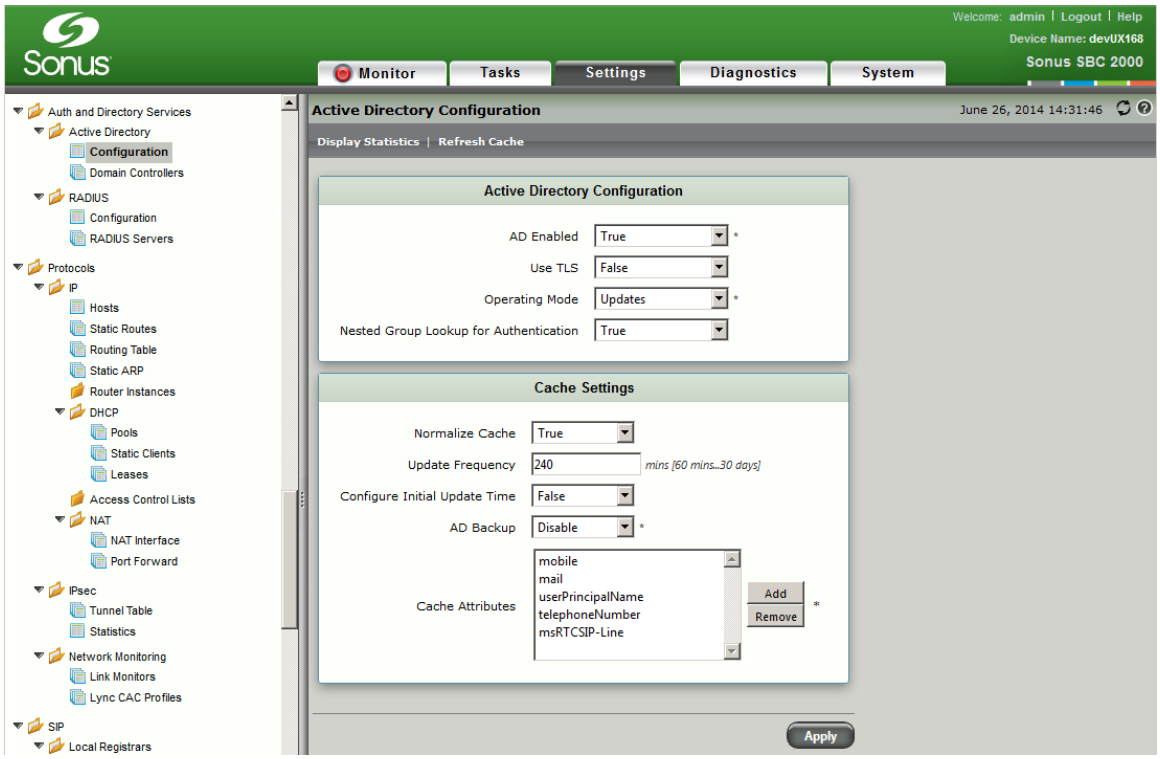
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Active Directory > Domain Controllers**.
3. Add a domain controller.
    a. Configure the domain controller configuration items as shown below.



Active Directory Configuration

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Active Directory > Configuration**.
3. Configure the relevant settings as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



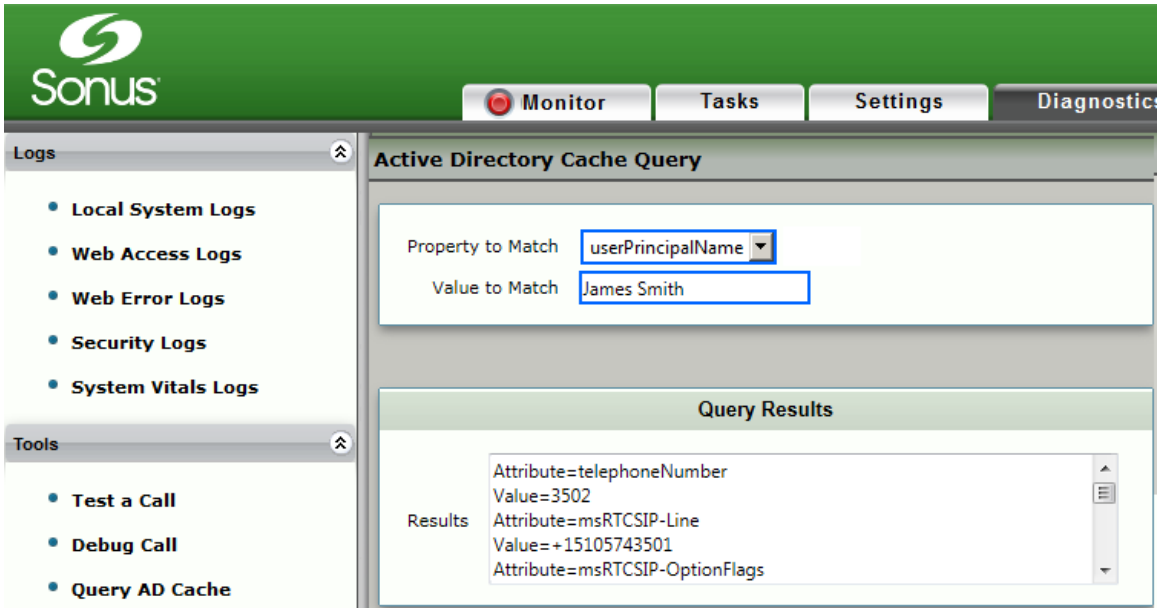
The username is **case sensitive** and must match the username in Active Directory.

AD Query Functionality Verification

1. In the WebUI, click the **Diagnostics** tab.
2. In the left navigation pane, go to **Tools > Query AD Cache**.
   In the Active Directory Cache Query page:
3. Select **userPrincipalName** from the **Property to Match** list box.
4. Enter the Lync user's **userPrincipalName** (i.e:James Smith) in the Value to Match field.
5. Click **OK**.

The query should return results similar to those shown below.

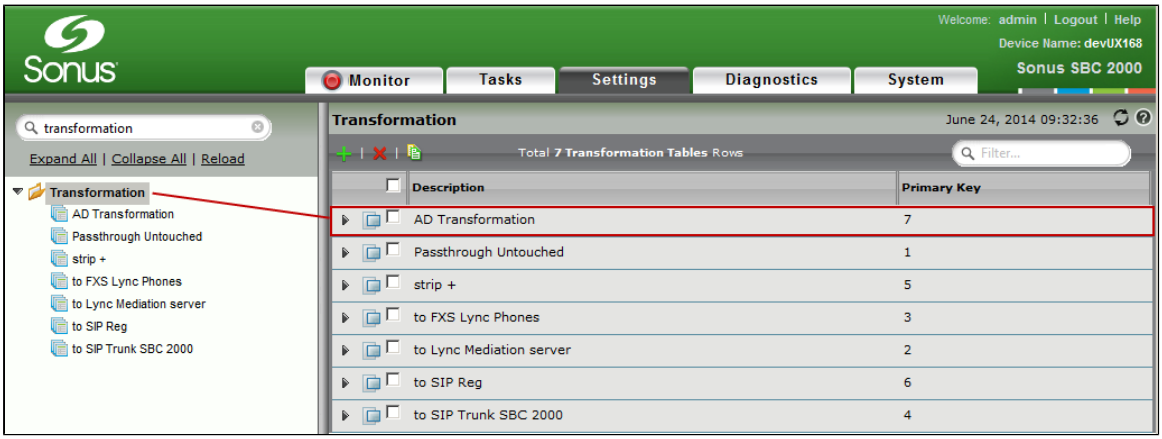
Copyright © 2015 Sonus Networks. All rights reserved.



Telephony Routing Setup

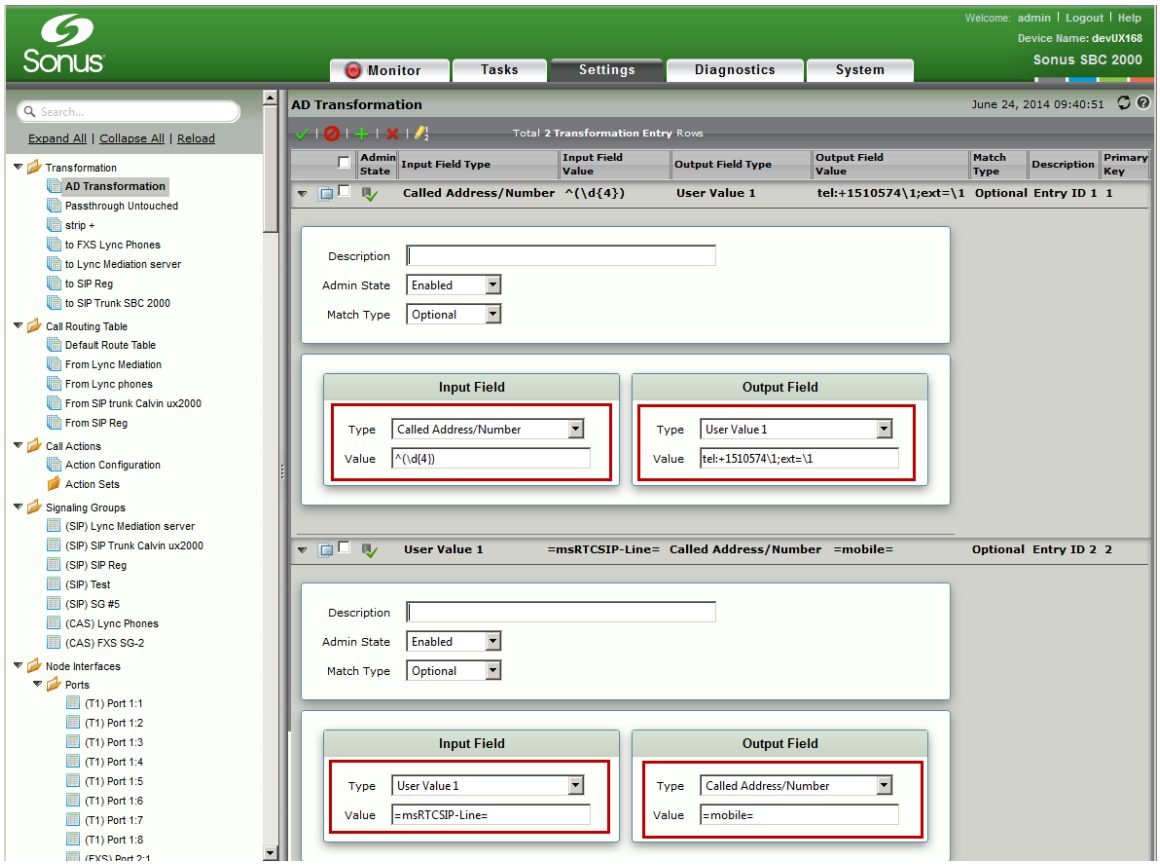
Transformation Table Configuration

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Transformation**.
3. Add an entry to the Transformation Table.



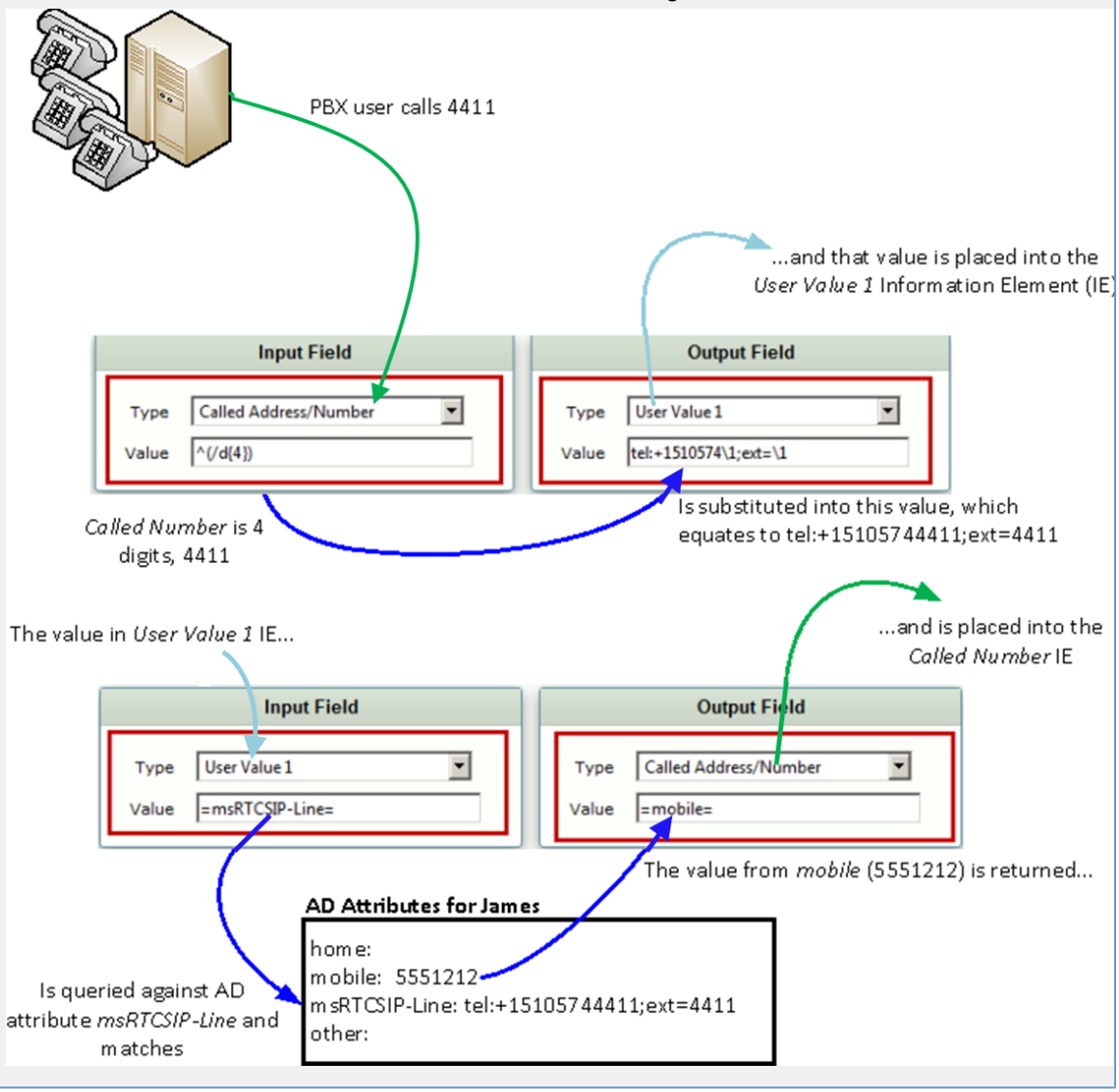
4. In the left navigation pane, select the Transformation Table created in the previous step.
5. Add two entries as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.

Click here to see detailed information on AD-based routing via the transformation table



Include tel: in a msRTCSIP-Line AD search if the Sonus SBC 1000/2000's Active Directory Configuration *Operating Mode* is configured to either Online, or Updates with the *Normalization Cache* set to False. Do not include tel: if the *Normalization Cache* is set to True. See Configuring Sonus SBC 1000/2000 for Active Directory for more information.

Copyright © 2015 Sonus Networks. All rights reserved.

AD Wild Cards

Sonus SBC 1000/2000 supports the use of wild cards. This means that you can do partial matching in AD fields. The following is an example of how the ***=telephoneNumber=*** field is used to forward an inbound call to the user's new extension.

AD Transformation June 24, 2014 13:53:17

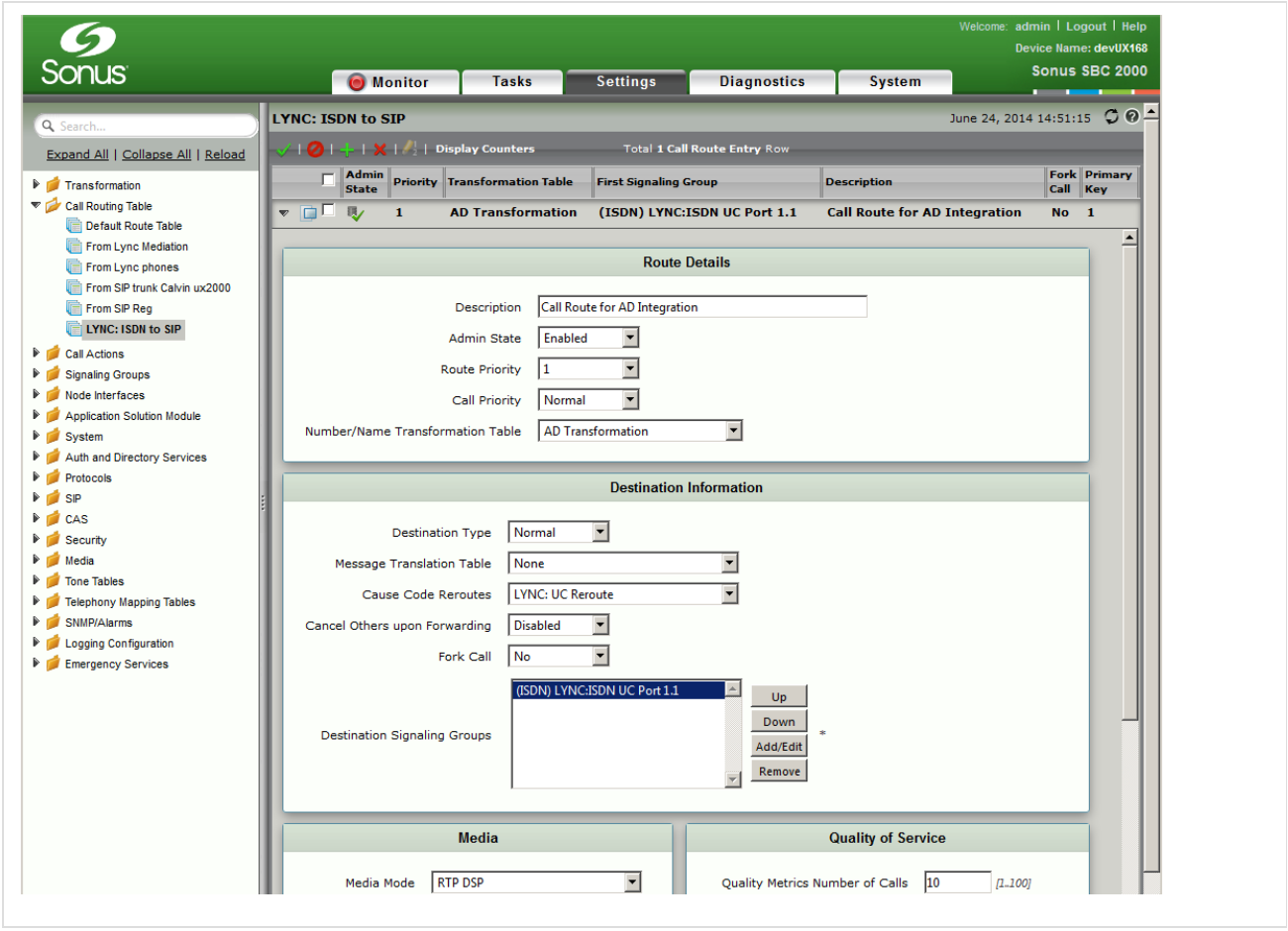
Total **3 Transformation Entry** Rows

	Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description	Primary Key
		Called Address/Number	^(/d{4})	User Value 1	tel:+1510284\1*	Mandatory	Entry ID 1	1
		User Value 1	=telephonenumber=	Called Address/Number	=telephonenumber=	Mandatory	Entry ID 2	2
		Called Address/Number	.*(\d{4})$	Called Address/Number	\1	Mandatory	Entry ID 3	3

Scenario
Someone dials extension *3633*, the four digits are added to the Area Code and prefix as well as the wildcard character, the result (User Value 1) is used in an AD query against the *=telephoneNumber=* field. The contents of the first =telephoneNumber= field containing the match string is then parsed for the last four digits, which are output from the transformation.

Call Routing Table

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table > (relevant entry)**.
3. Select the appropriate Transformation Table in the **Number/Name Transformation Table** list box as shown below.



Copyright © 2015 Sonus Networks. All rights reserved.

Verification of Call Routing using AD attributes

In order to properly verify the Sonus SBC 1000/2000 configuration, please follow these steps:

1. A PBX phone (6228) dials the Lync user's number (3633).
2. The call lands on the ISDN inbound Signaling Group on the Sonus SBC 1000/2000.
3. The call is then sent to the relevant Call Route Table Entry.
4. In the Call Route Entry, the incoming number is first transformed using the relevant call route entry (using the cached Active Directory user attributes) and is then routed to the relevant outbound Signaling Group.

You can see the AD usage in action via the WebUI log as shown below:

```
[2011-05-27 10:40:05,336] com.sonus.sbc.ccc INFO (sg.cpp:139) - [15424] Received MSG_CC_SETUP message with called#[3633]
:
[2011-05-27 10:40:05,424] com.sonus.sbc.ccc INFO (fsmco.cpp:1428) - [15493] Requesting call route for route table 4, called# [3633]
:
[2011-05-27 10:40:05,426] com.sonus.sbc.route INFO (callrouter.cpp:1771) - Handling route request.
[2011-05-27 10:40:05,426] com.sonus.sbc.route DEBUG (translation.cpp:1143) - Performing translation using entry 10.1.
[2011-05-27 10:40:05,426] com.sonus.sbc.route DEBUG (translation.cpp:555) - Successful regex match for "^(\d{4})" (updated "^(\d{4})") with input of "3633"
[2011-05-27 10:40:05,426] com.sonus.sbc.route DEBUG (translation.cpp:599) - Regex replacement output is "tel:+15105743633;ext=3633"
[2011-05-27 10:40:05,427] com.sonus.sbc.route INFO (translation.cpp:1010) - Doing AD lookup for field 'msRTCSIP-Line' with value 'tel:+15105743633;ext=3633'
[2011-05-27 10:40:05,427] com.sonus.sbc.route.libcommon TRACE (AFSessionManagementLayer.cpp:1286) - SMSession: creating session=0xf3f78 level=2 session id=2.
[2011-05-27 10:40:05,427] com.sonus.sbc.route.libcommon TRACE (AFSessionManagementLayer.cpp:1306) - SMSession: new session=0xf3f78 id=0 subsession id=32770 pCBO=0x9b8b8.
[2011-05-27 10:40:05,427] com.sonus.sbc.route.libcommon DEBUG (AFSessionManagementLayer.cpp:1596) - Sending REQ: transaction id=10:0/32770/0 message=MSG_ADS_AD_QUERY msg len=75 end session=0 session=0xf3f78(0xd71d8).
[2011-05-27 10:40:05,427] com.sonus.sbc.route.libcommon TRACE (AFEventLoop.cpp:92) - AFEventLoop::Monitor: Adding fd=13 for events=0x1.
[2011-05-27 10:40:05,429] com.sonus.sbc.route.libcommon DEBUG (AFSessionManagementLayer.cpp:758) - SMConnection: Received RESP: session id=10:0/32770/0 message=MSG_ADS_AD_QUERY len=267 end sesion=0, moredata=0
[2011-05-27 10:40:05,429] com.sonus.sbc.route.libcommon TRACE (AFSessionManagementLayer.cpp:831) - SMconnection: transaction=0xf3f78(0xd71d8) pCBO=(nil), pCBOFunction=0x9b8b8.
[2011-05-27 10:40:05,429] com.sonus.sbc.route.libcommon TRACE (AFSessionManagementLayer.cpp:1314) - SMSession: destructing session=0xf3f78 id=32770 state=4 level=2.
[2011-05-27 10:40:05,429] com.sonus.sbc.route DEBUG (callrouter.cpp:3235) - Got AD lookup response with 4 field/value pairs.
[2011-05-27 10:40:05,429] com.sonus.sbc.route INFO (callrouter.cpp:1771) - Handling route request.
[2011-05-27 10:40:05,429] com.sonus.sbc.route DEBUG (callrouter.cpp:1774) - Using AD lookup response in request.
[2011-05-27 10:40:05,430] com.sonus.sbc.route DEBUG (translation.cpp:1143) - Performing translation using entry 10.2.
[2011-05-27 10:40:05,430] com.sonus.sbc.route DEBUG (translation.cpp:555) - Successful regex match for "msRTCSIP-Line=" (updated "tel:\+15105743633;ext=3633") with input of "tel:+15105743633;ext=3633"
[2011-05-27 10:40:05,430] com.sonus.sbc.route DEBUG (translation.cpp:599) - Regex replacement output is "6223"
[2011-05-27 10:40:05,430] com.sonus.sbc.route.libcommon TRACE (AFSessionManagementLayer.cpp:1286) - SMSession: creating session=0xf55c8 level=2 session id=86.
[2011-05-27 10:40:05,430] com.sonus.sbc.route.libcommon TRACE (AFSessionManagementLayer.cpp:1306) - SMSession: new session=0xf55c8 id=0 subsession id=32854 pCBO=0x9b858.
[2011-05-27 10:40:05,431] com.sonus.sbc.route INFO (callrouter.cpp:1924) - Successful route request with entry 4.1
:
[2011-05-27 10:40:05,448] com.sonus.sbc.route INFO channel.cpp:568) - [15550] Sending out setup message with called#[6223]
```

Configuring a Nortel PBX v4.5 to connect via TDM to the SBC 1000-2000

Table of Contents

- Prerequistes
- Interoperation Notes
- PBX Configuration

About this Page

- This Interoperability Note describes how to configure a TDM port on a Nortel Meridian PBX to integrate with the Sonus SBC 1k/2k. Also included is configuration information for integrating Exchange Unified Messaging to the Nortel PBX via the Sonus SBC.

Related Articles

- Managing Telephony Ports

Prerequistes

Requires Sonus SBC1000/2000 Version 3.0 or later

Copyright © 2015 Sonus Networks. All rights reserved.

☑ Nortel Meridian Option 11C, version 4.5, T1, QSIG

QSIG Option Packages: PKG 305 (Generic QSIG), PKG 316 (QSIG Supplemental services), PKG 263 (QSIG Basic Call / Name display), PKG 175 (Network Message Service

Interoperation Notes

The following extension numbers are used within this document:

- UMS Pilot Extension: 2562
- Extensions enabled for Microsoft Exchange Server UM: 5100 - 5199

PBX Configuration

Use the following configurations to interconnect the Avaya to the SBC1k/2k.

1. D-channel Configuration:
   ADAN DCH 15
   CTYP MSDL
   CARD 05
   PORT 1
   DES dch5
   USR PRI
   DCHL 5
   OTBF 32
   PARM RS422 DTE
   DRAT 64KC
   CLOK EXT
   IFC ISGF
   PINX_CUST 0
   ISDN_MCNT 300
   CLID OPT0
   CO_TYPE STD
   SIDE NET
   CNEG 1
   RLS ID **
   RCAP COLP NDI CCBI CCNI PRI DV3I CTI QMWI
   PR_TRIGS DIV 2 3
   CNG 2 3
   PR_RTN NO
   MBGA NO
   OVLR NO
   OVLS NO
   T310 120
   T200 3
   T203 10
   N200 3
   N201 260
   K 7

2. Route Configuration:
   TYPE RDB
   CUST 00

Copyright © 2015 Sonus Networks. All rights reserved.

DMOD
ROUT 5
DES UMDEV
TKTP TIE
NPID_TBL_NUM 0
ESN NO
CNVT NO
SAT NO
RCLS EXT
VTRK NO
NODE
DTRK YES
BRIP NO
DGTP PRI
ISDN YES
MODE PRA
IFC ISGF
SBN NO
PNI 00000
NCNA NO
NCRD NO
CHTY BCH
CTYP UKWN
INAC NO
ISAR NO
CPFXS YES
DAPC NO
INTC NO
DSEL VOD
PTYP PRI
AUTO NO
DNIS NO
DCDR NO
ICOG IAO
PREM NO
SRCH LIN
TRMB YES
STEP
ACOD 6005
TCPP NO
TARG
CLEN 1
BILN NO
OABS
INST
ANTK
SIGO STD
MFC NO
ICIS YES
OGIS YES
TIMR ICF 512
OGF 512
EOD 512

Copyright © 2015 Sonus Networks. All rights reserved.

NRD 10112
DDL 70
ODT 4096
RGV 640
GRD 896
SFB 3
NBS 2048
NBL 256
IENB 5
TFD 0
VSS 0
VGD 6
DRNG NO
CDR NO
VRAT NO
MUS NO
OHQ NO
OHQT 00
CBQ NO
AUTH NO
TTBL 0
ATAN NO
PLEV 2
ALRM NO
ART 0
SGRP 0
ARDN NO
AACR NO

3. B-channel Configuration:
   DES UMDEV
   TN 005 01
   TYPE TIE
   CDEN SD
   CUST 0
   TRK PRI
   PDCA 1
   PCML MU
   NCOS 0
   RTMB 5 1
   B-CHANNEL SIGNALING
   TGAR 1
   AST NO
   IAPG 0
   CLS CTD DIP WTA LPR APN THFD HKD
   P10 VNL
   TKID
   AACR NO

4. Use the TDM document to configure the SBC 1k/2k.

   - Configuring TDM ports on the SBC 1000/2000

Copyright © 2015 Sonus Networks. All rights reserved.

5. Use the EUM integration document to finished the voicemail integration.

- Configuring SBC 1000-2000 with Exchange 2013

Configuring SBC 1000-2000 with Exchange 2013

Table of Contents

- Prerequistes
- Interoperation Notes
- Exchange 2013 Configuration
- Configure the SBC 1k/2k

About this Page

- This Interoperability Note describes how to integrate a SBC 1k/2k directly to Exchange 2013
- This document presumes the reader is familiar with configuring Exchange and the SBC 1k/2k

Related Articles

- Managing Telephony Ports
- Managing Signaling Groups

Prerequistes

Requires Sonus SBC1000/2000 Version 3.0

Exchange 2013

Interoperation Notes

The following instructions detail configuring both Exchange 2013 and Sonus SBC 1k/2k to interoperate via TCP. It is suggested that any integration attempt begin with TCP and move to TLS, if required, only after ensuring the Exchange <> SBC connection is fully functional.

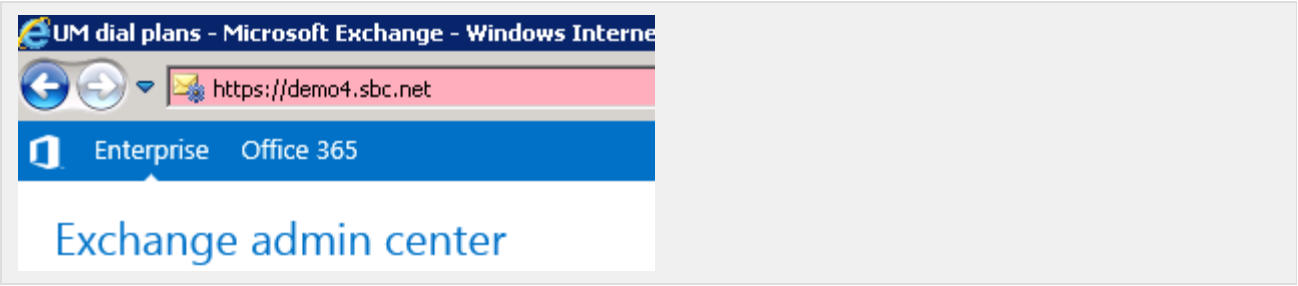
- Exchange = demo4.sbc.net (10.1.1.4)
- SBC = sbc2000.sbc.net (10.1.1.74)

Exchange 2013 Configuration

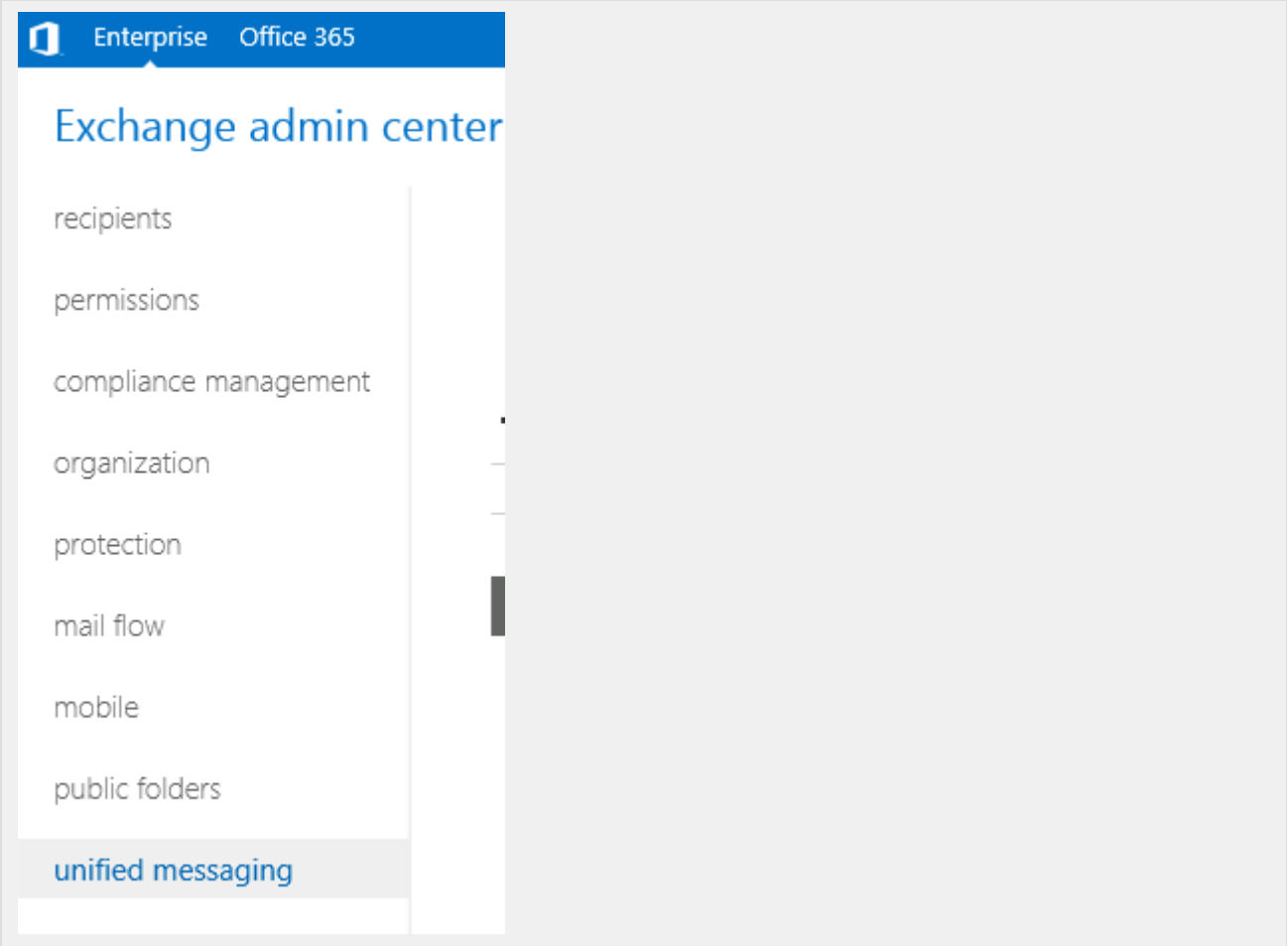
Use the following to configure Exchange 2013 to accept and process calls sent directly from the SBC.

Copyright © 2015 Sonus Networks. All rights reserved.

1. Connect to the Exchange Admin interface via your web browser.

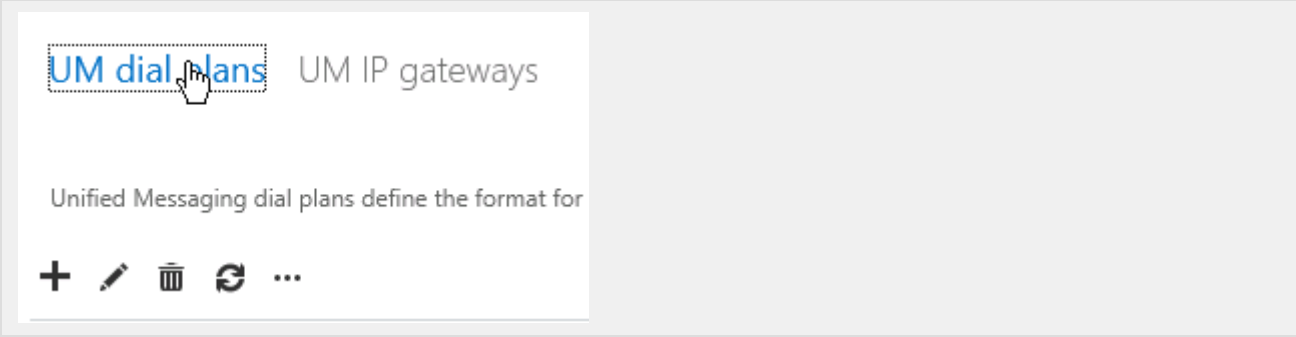


2. Select *Unified Messaging*.



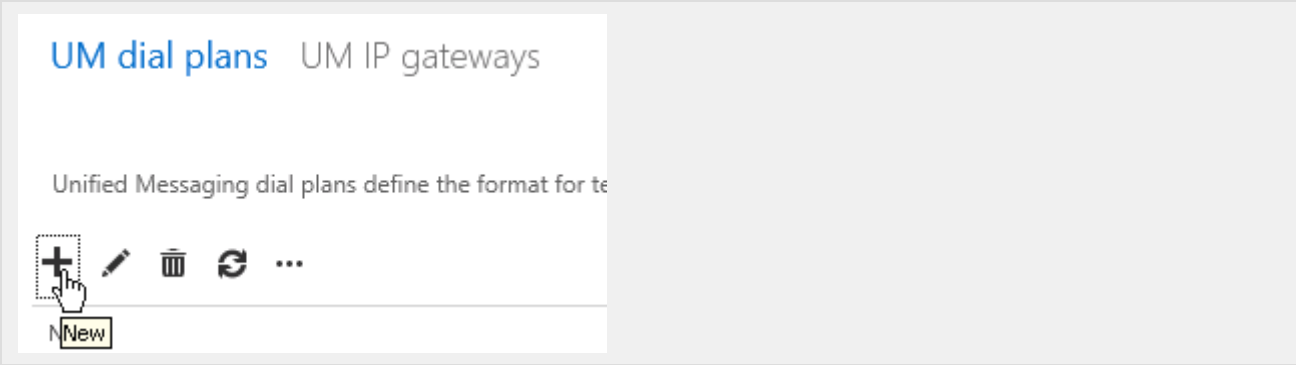
3. Select *UM dial plans*.

Copyright © 2015 Sonus Networks. All rights reserved.

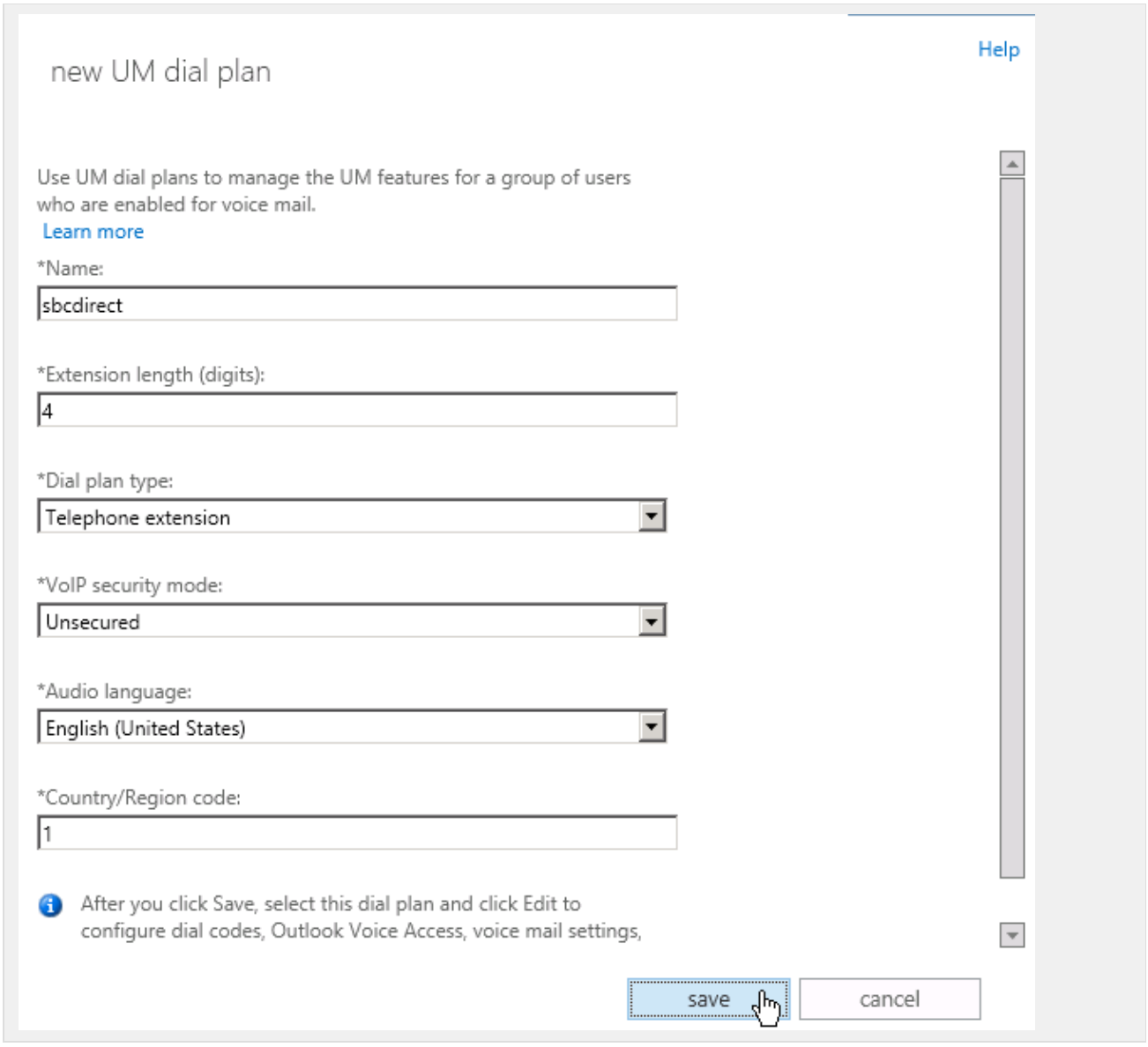


4. Add a new UM dial plan. Add a dia plan to support the Exchange <> SBC connection.

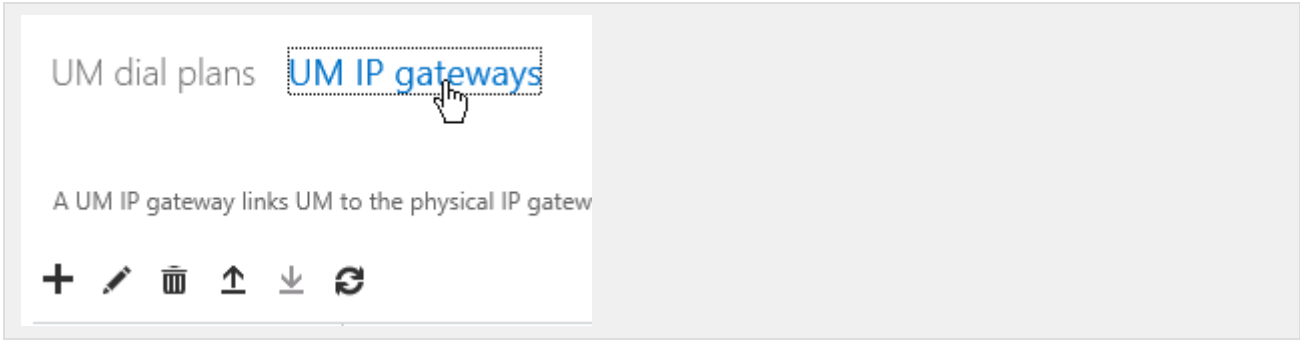
> Lync and PBX dial plans are different. You should not attempt to use a Lync dial plan to support the Exchange <> SBC connection.



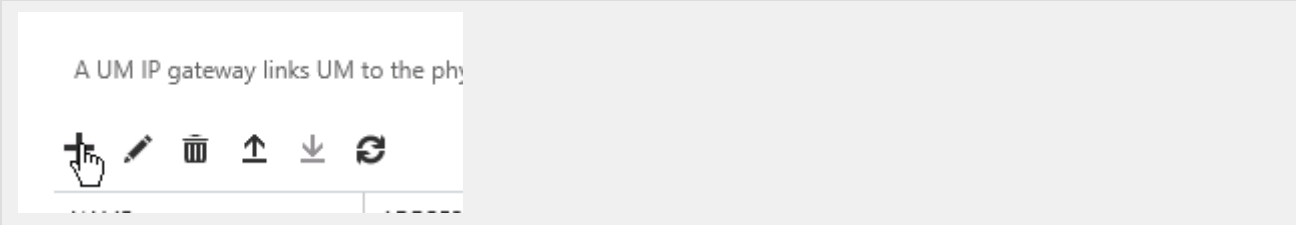
Copyright © 2015 Sonus Networks. All rights reserved.

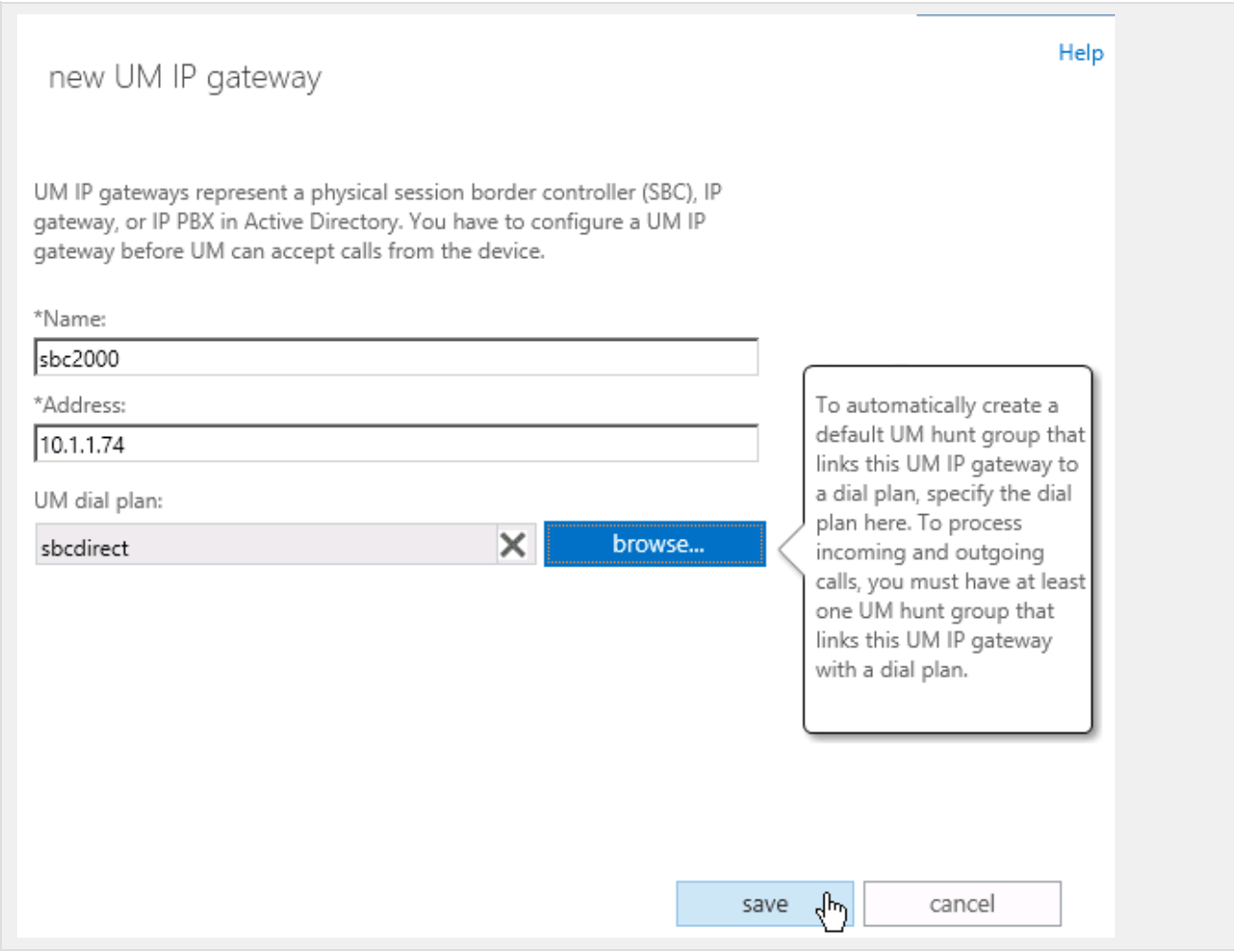


5. Create a *UM IP gateway*. Create an entry in Exchange for the SBC gateway.

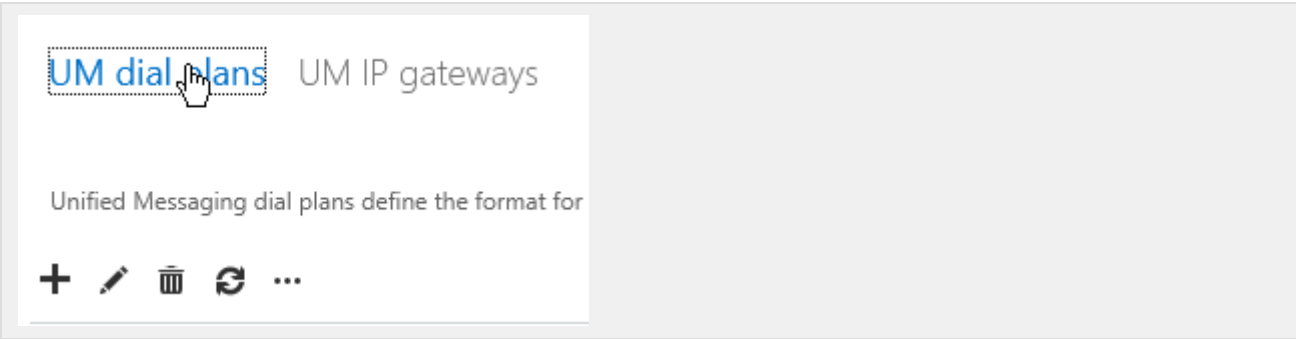


Copyright © 2015 Sonus Networks. All rights reserved.

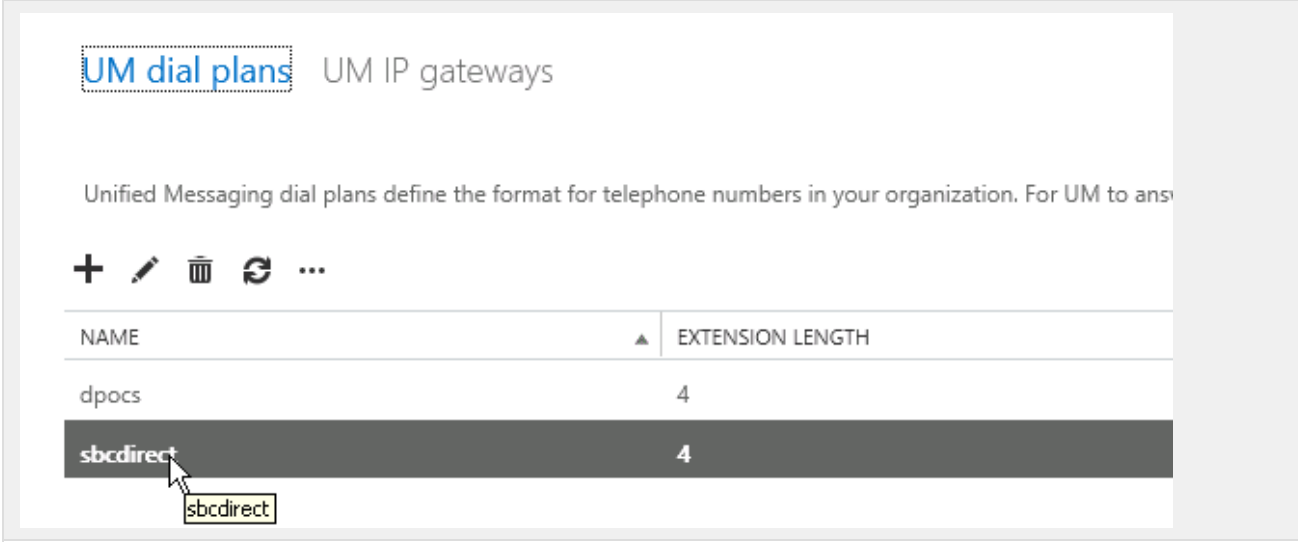




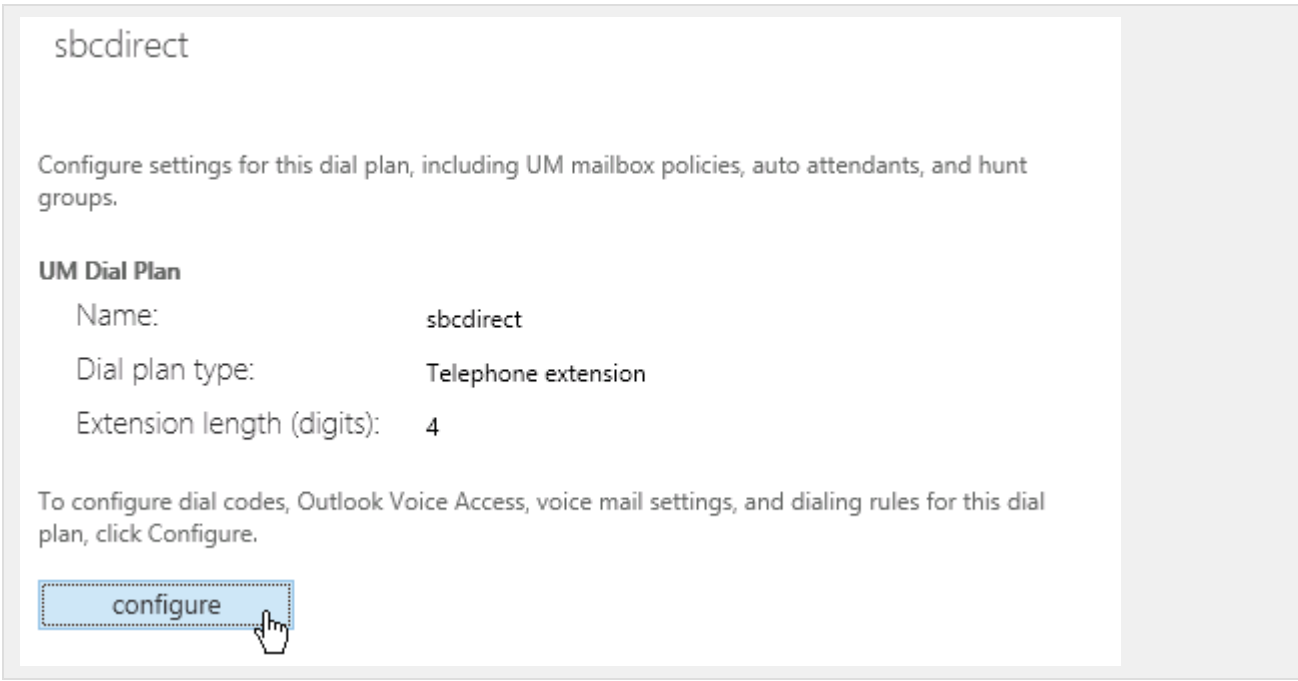
6. Modify the newly created UM dial plan.



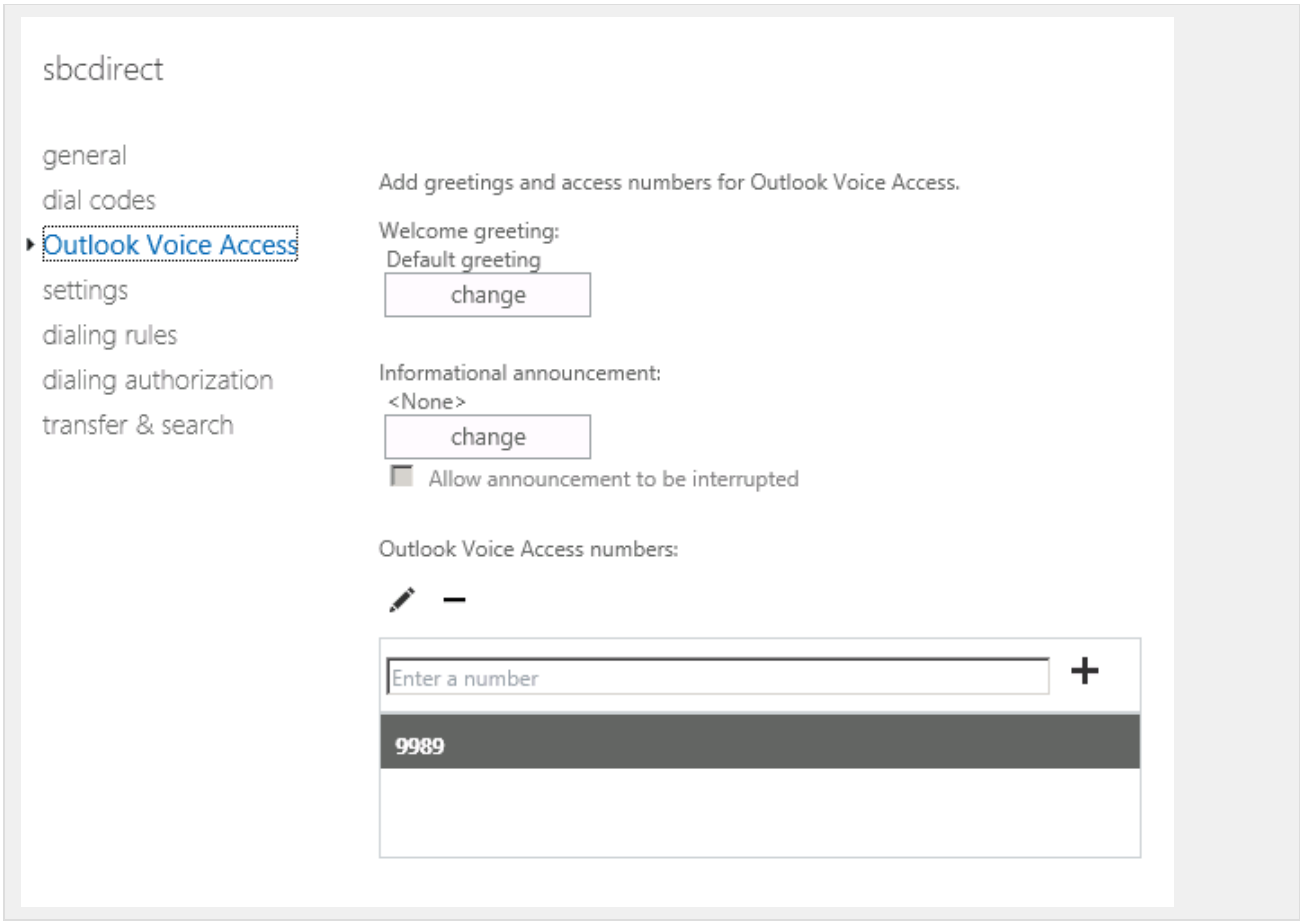
Copyright © 2015 Sonus Networks. All rights reserved.



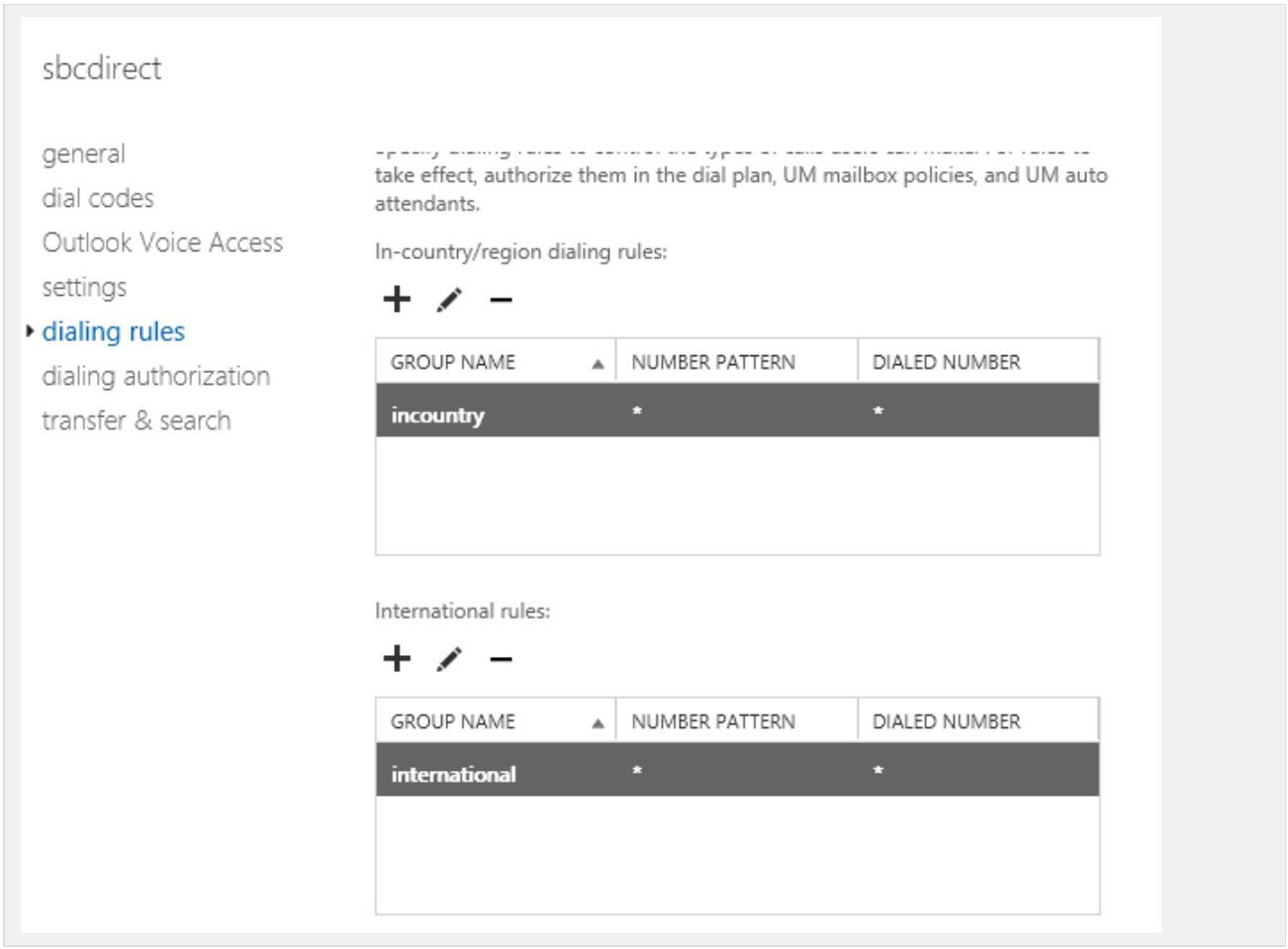
7. Configure/verify Outlook Voice Access.



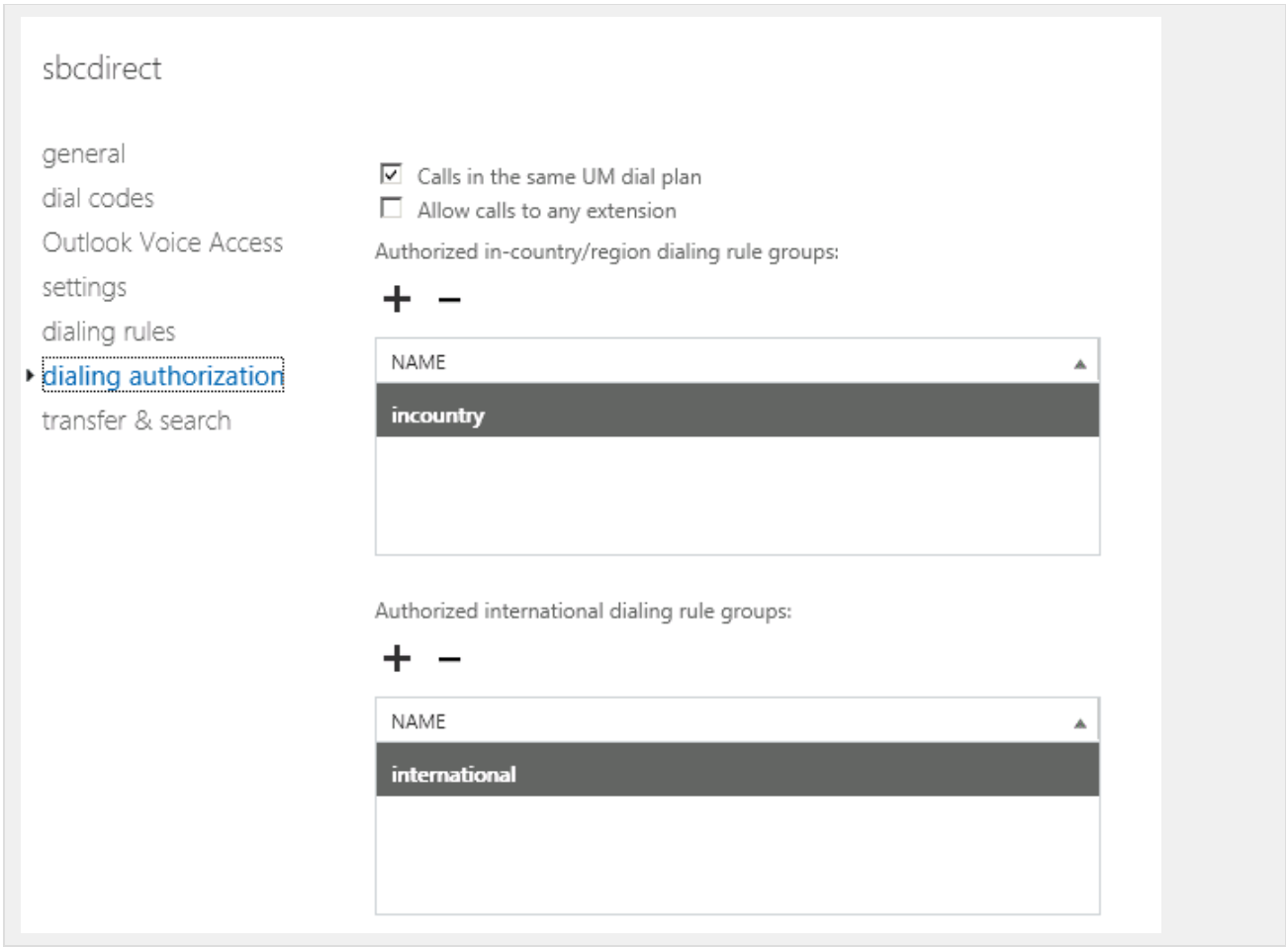
Copyright © 2015 Sonus Networks. All rights reserved.



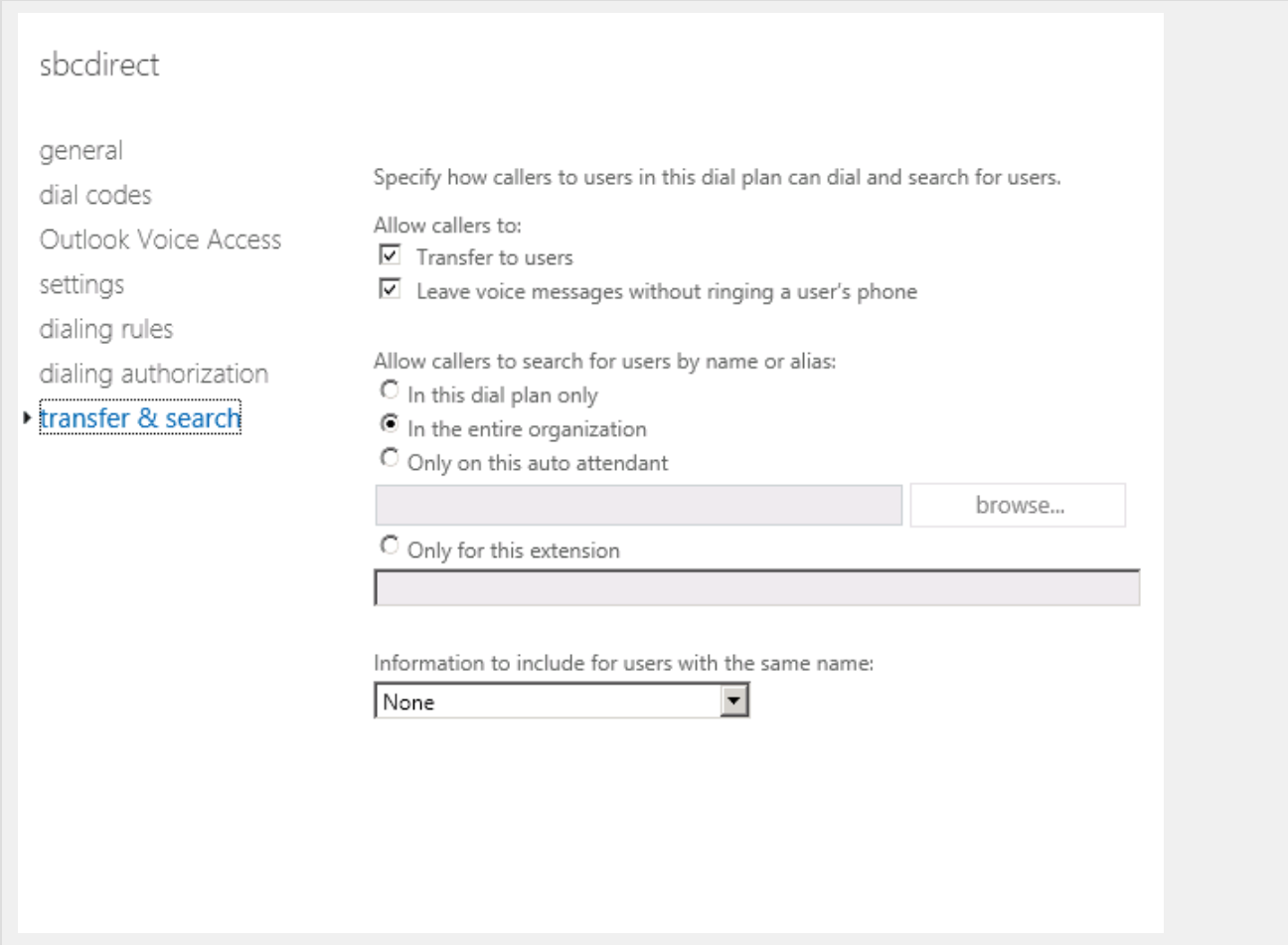
Copyright © 2015 Sonus Networks. All rights reserved.



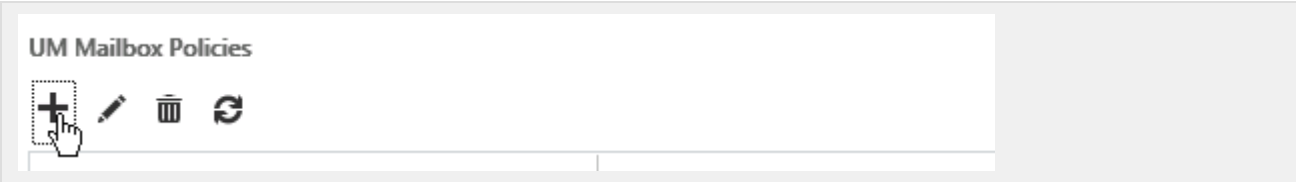
Copyright © 2015 Sonus Networks. All rights reserved.



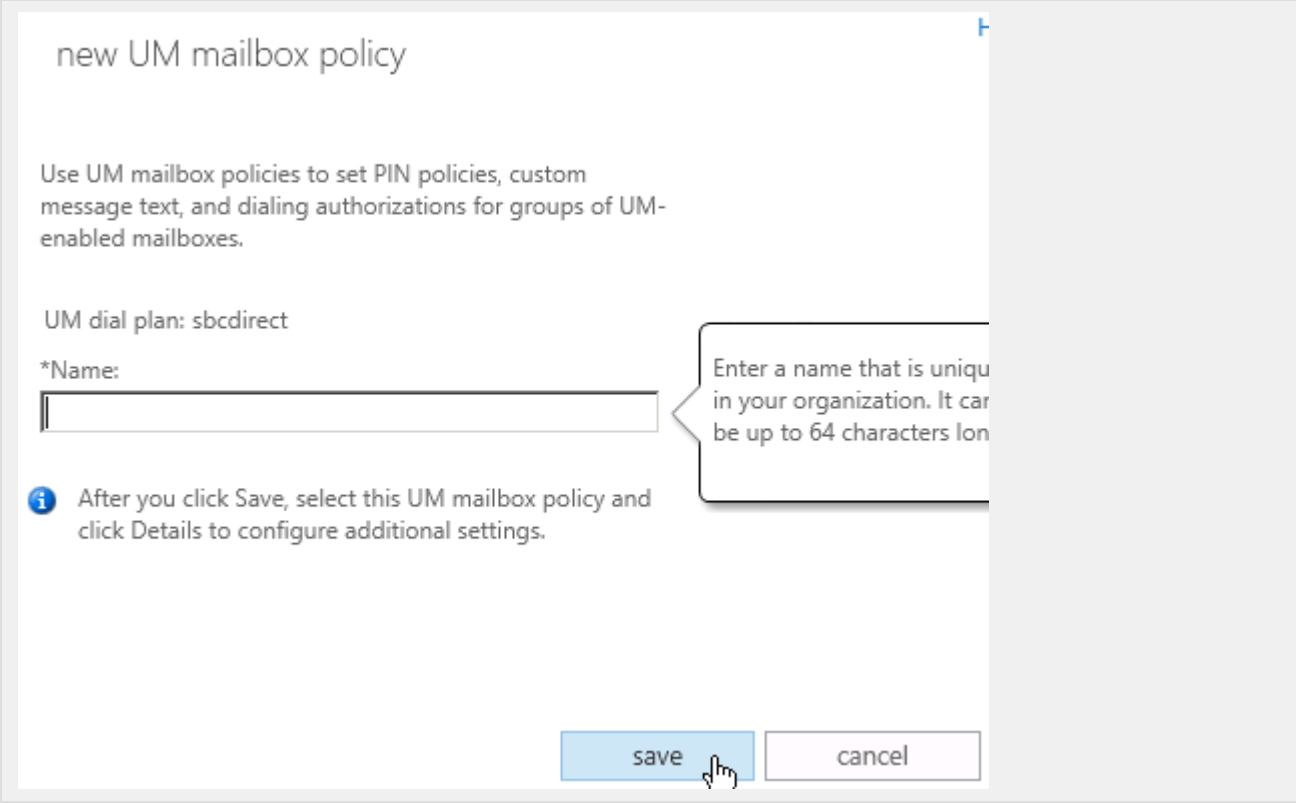
Copyright © 2015 Sonus Networks. All rights reserved.



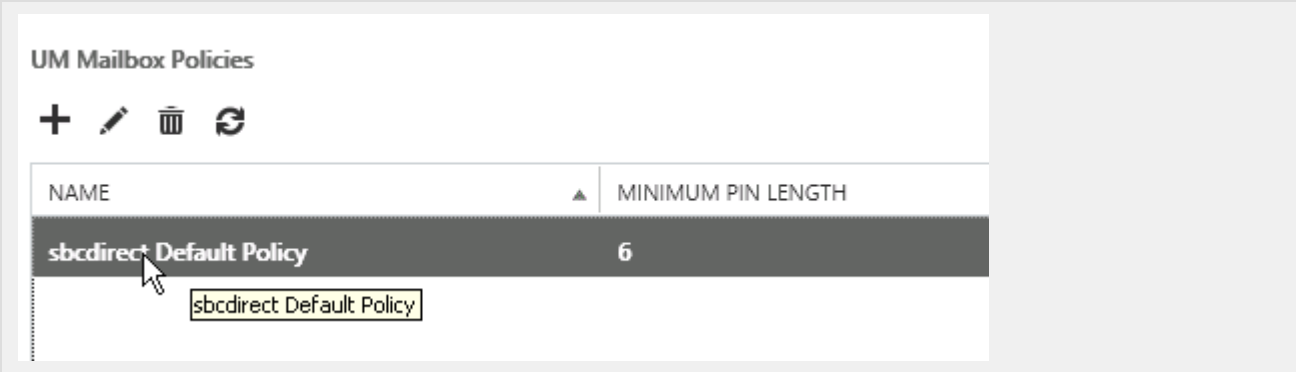
8. Add a UM Mailbox Policy to the dial plan.



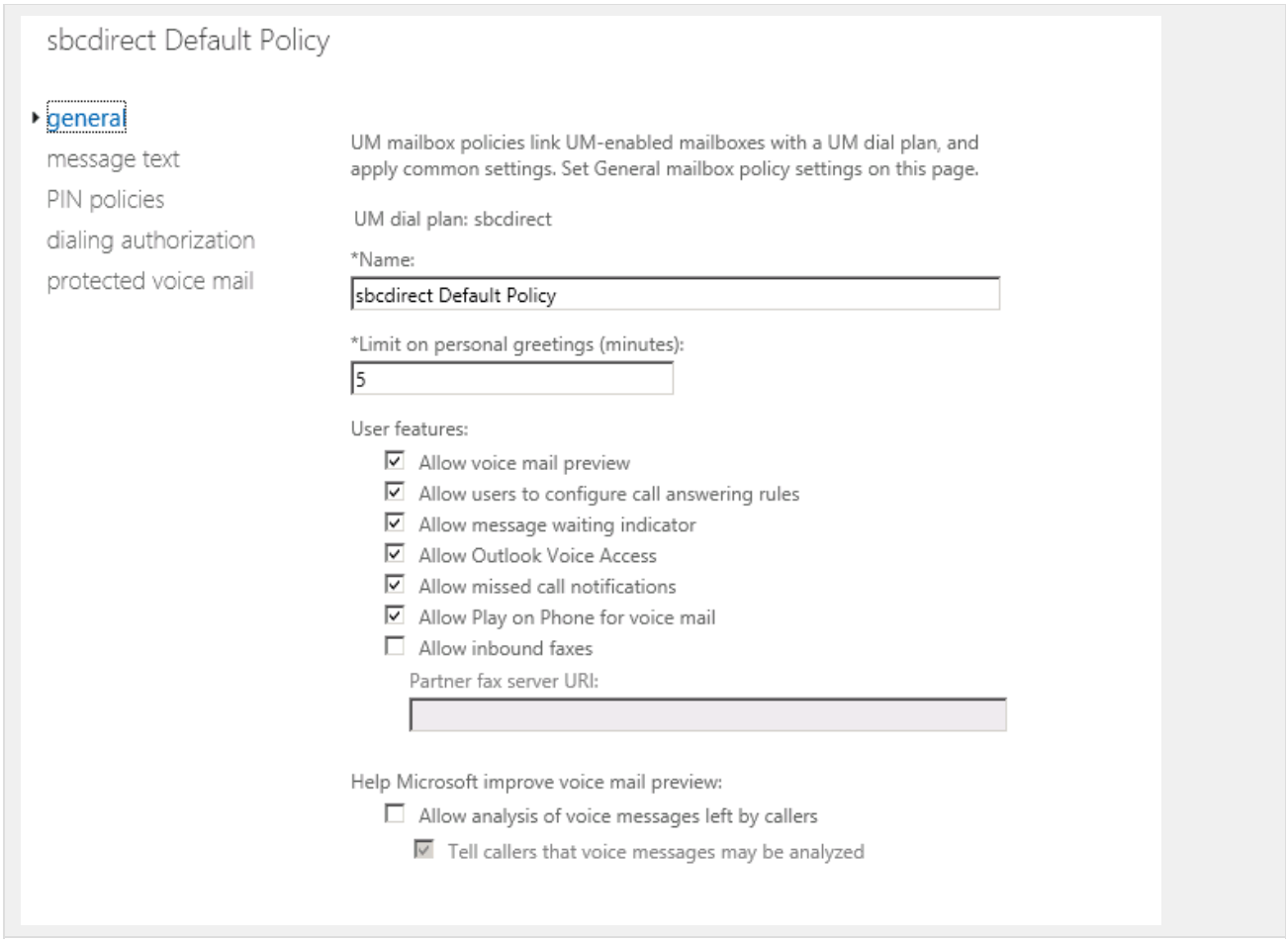
Copyright © 2015 Sonus Networks. All rights reserved.



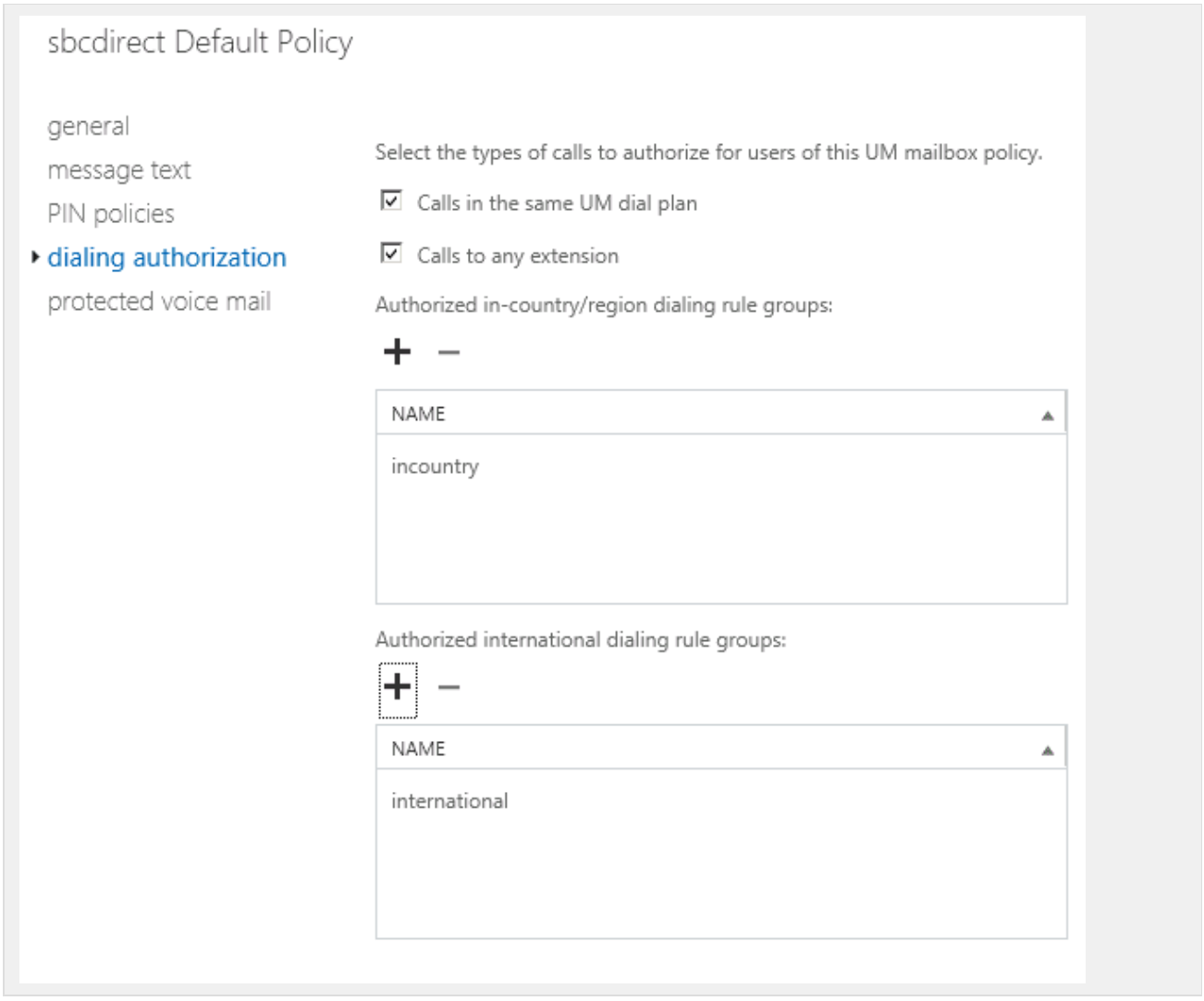
9. Modify/verify the newly created UM Mailbox Policy.



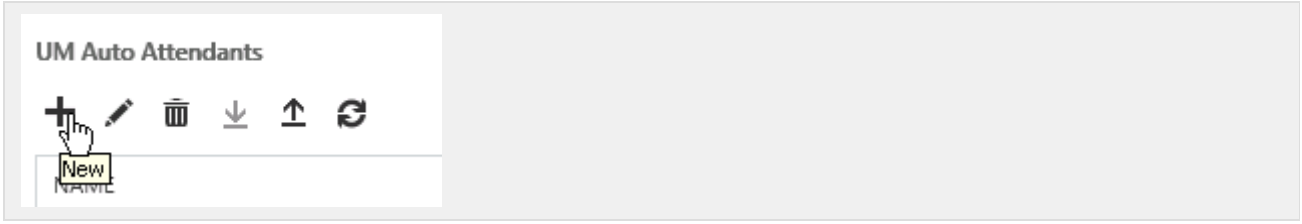
Copyright © 2015 Sonus Networks. All rights reserved.



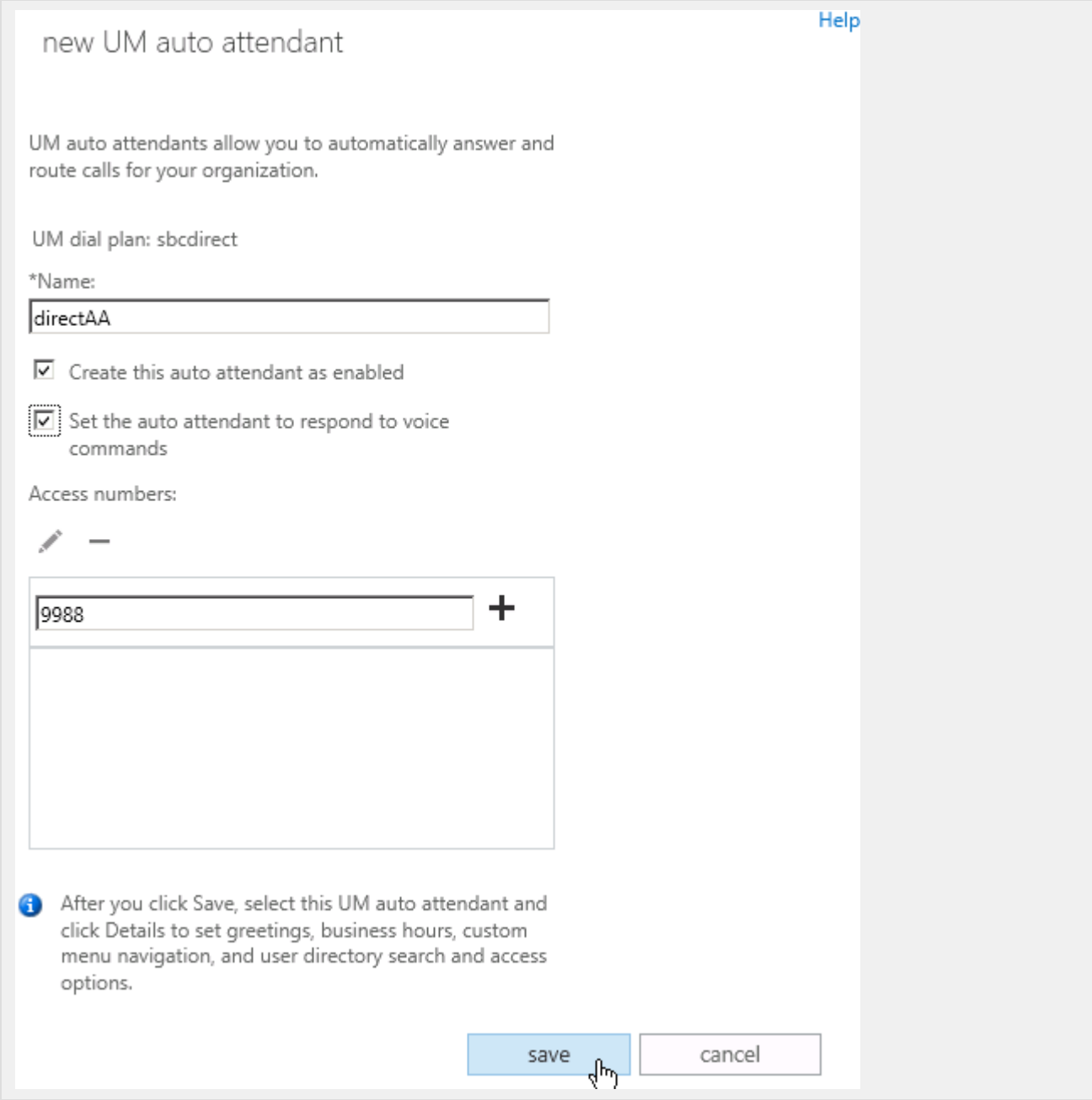
Copyright © 2015 Sonus Networks. All rights reserved.



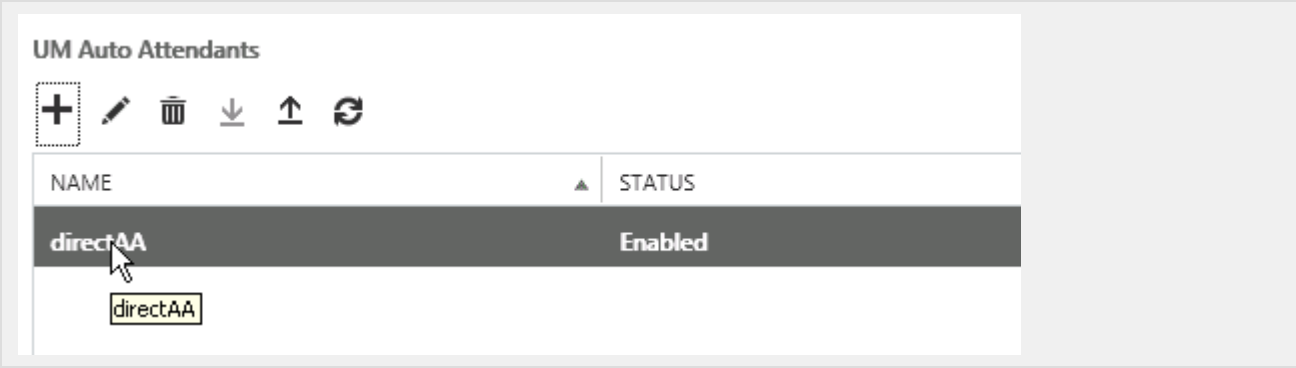
10. Add a UM Auto Attendant.



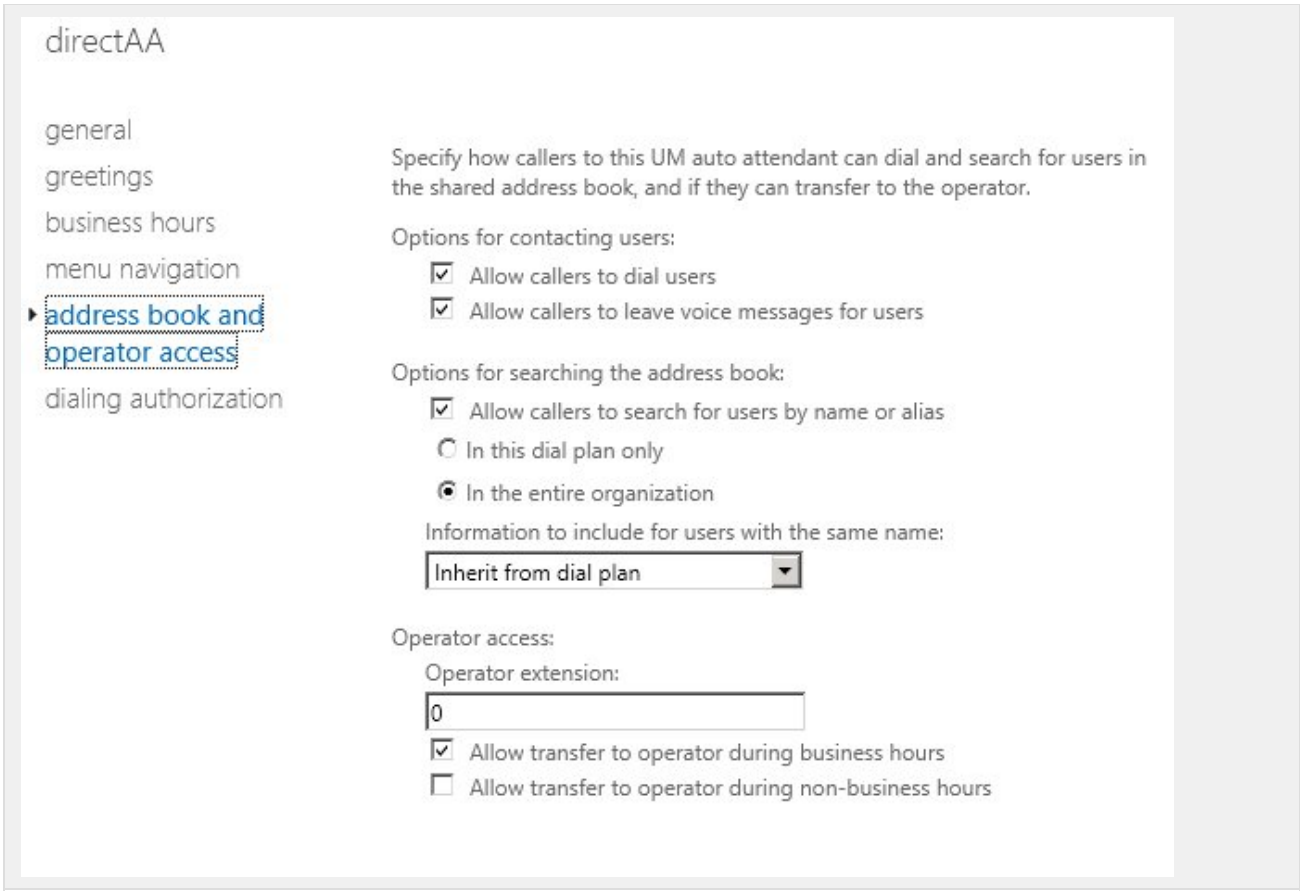
Copyright © 2015 Sonus Networks. All rights reserved.

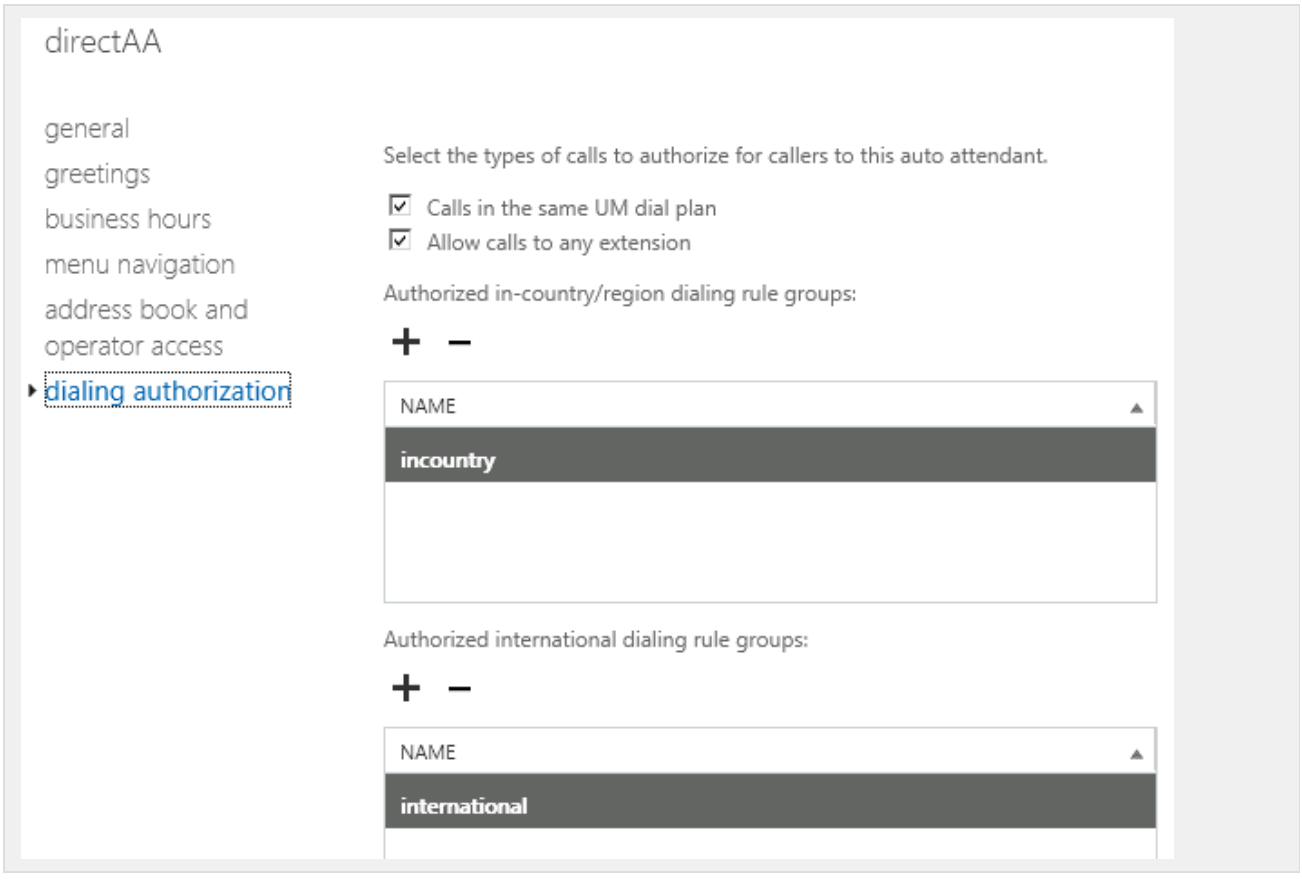


11. Modify/verify the newly created UM Auto Attendant.



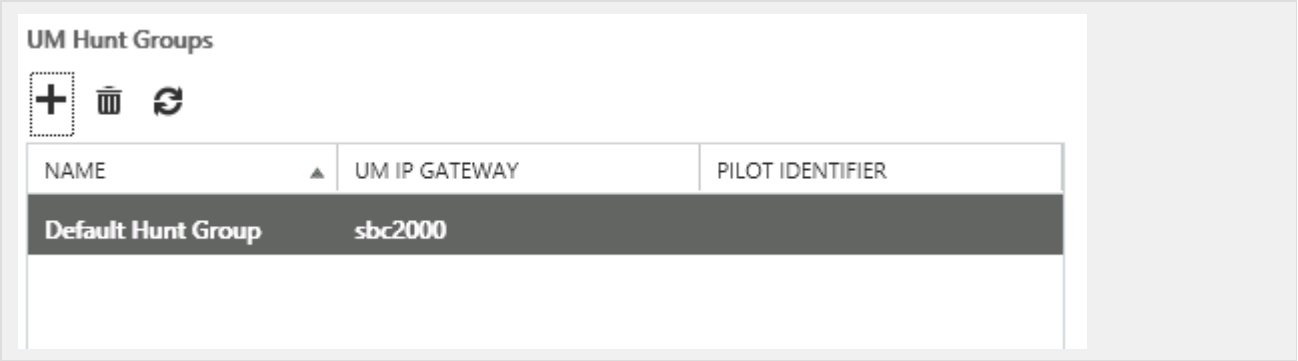
Copyright © 2015 Sonus Networks. All rights reserved.



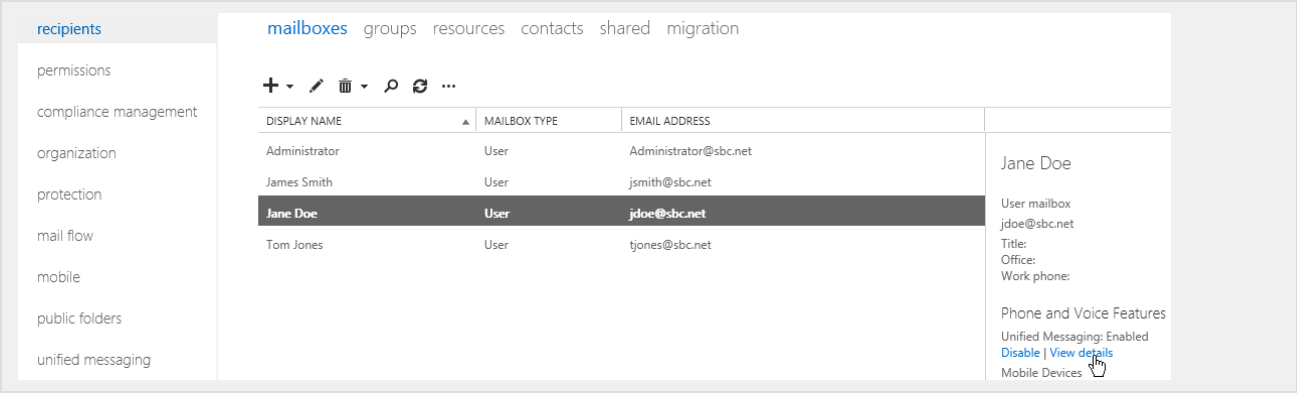


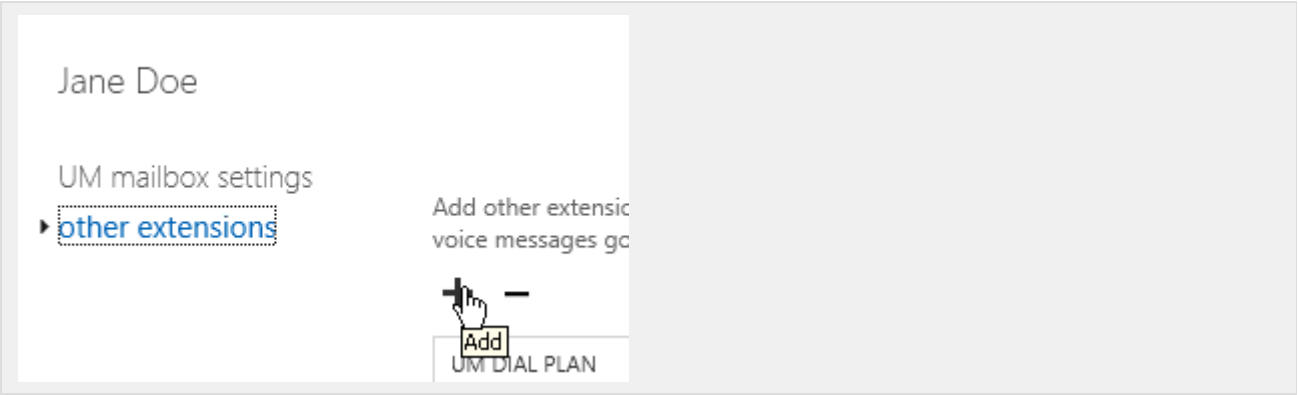
Copyright © 2015 Sonus Networks. All rights reserved.

12. If a UM Hunt Group if a default does not already exist.

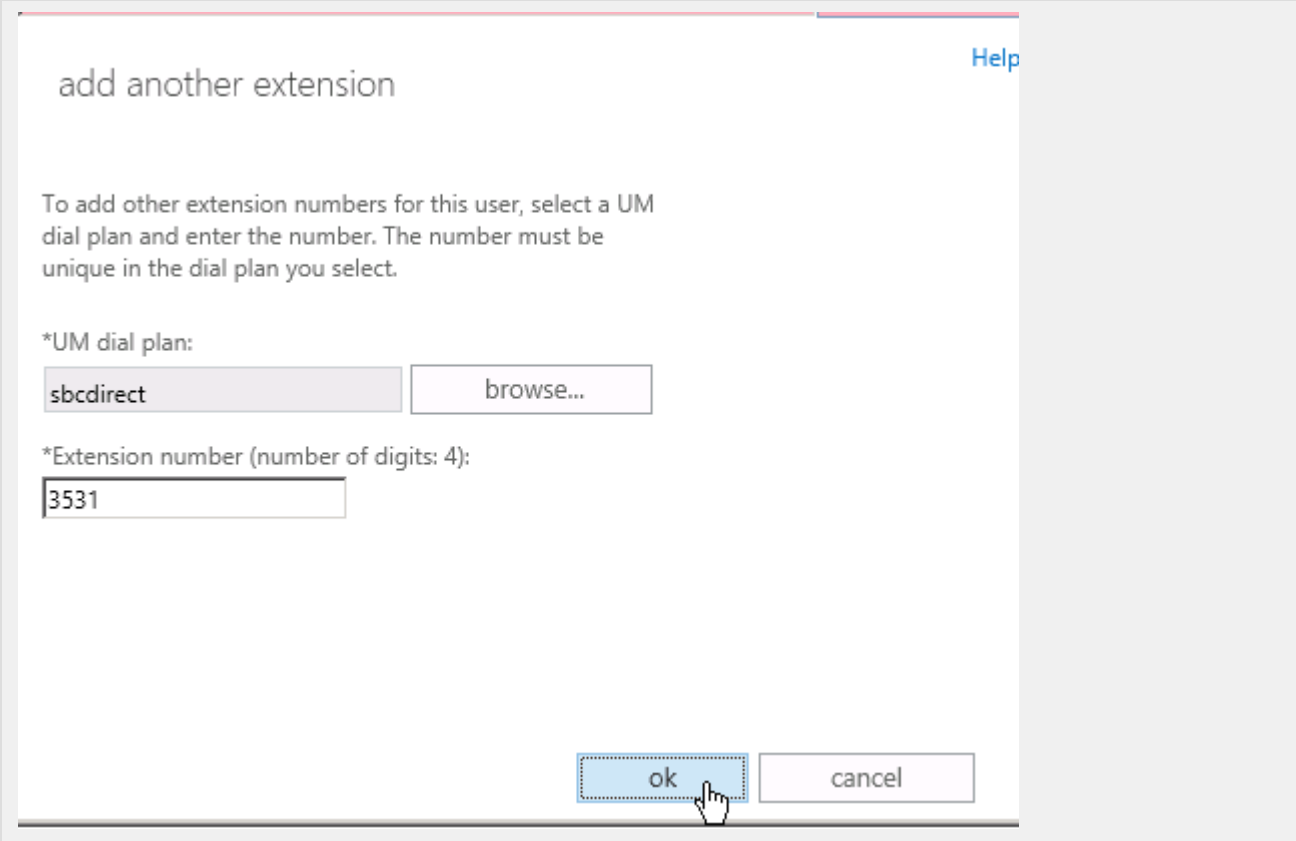


13. Add users to the newly created SBC dial plan. Adding extensions is accomplished via a user's Unified Messaging configuration.





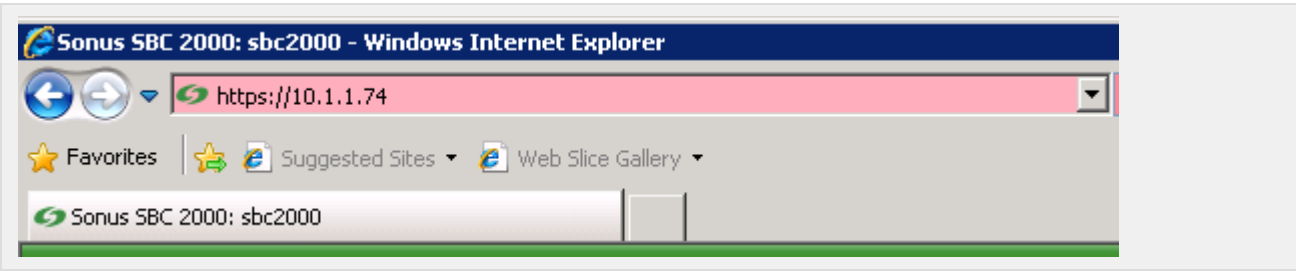
Copyright © 2015 Sonus Networks. All rights reserved.



Configure the SBC 1k/2k

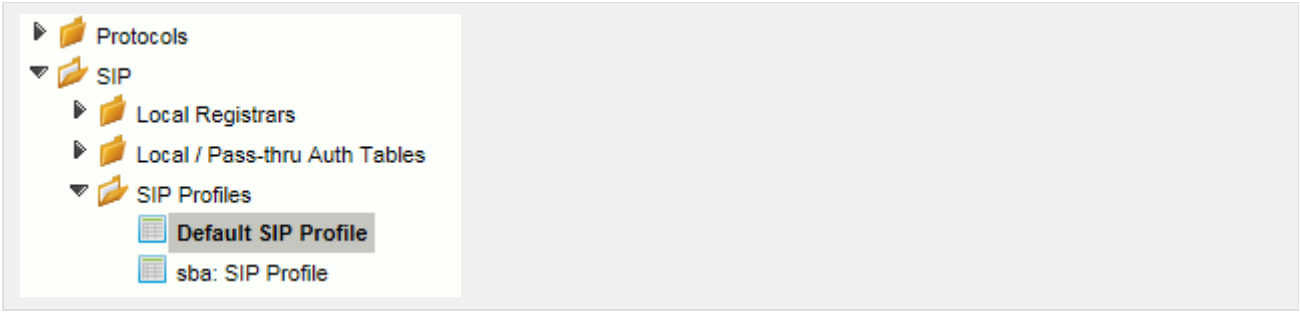
The next section covers configuring the SBC 1k/2k to interface to the Exchange server.

1. Browse to the Sonus SBC 1k/2k.



2. Create/verify SIP Profile.

Copyright © 2015 Sonus Networks. All rights reserved.



SIP Profile Entry: Default SIP Profile

Description **Default SIP Profile**

Session Timer

Session Timer	**Disable**

MIME Payloads

ELIN Identifier	**LOC**
PIDF-LO Passthrough	**Enable**
Unknown Subtype Passthrough	**Disable**

Header Customization

UA Header	**UX**
Subscription State Passthrough	**Enable**
FQDN in From Header	**Sonus SBC FQDN**
Send Assert Header	**Trusted Only**
Trusted Interface	**Enable**
Calling Info Source	**RFC Standard**
Diversion Header Selection	**First**

Options Tags

100rel	**Supported**
Update	**Supported**

Timers

Transport Timeout Timer	**5000**
Maximum Retransmissions	**RFC Standard**

RFC timers

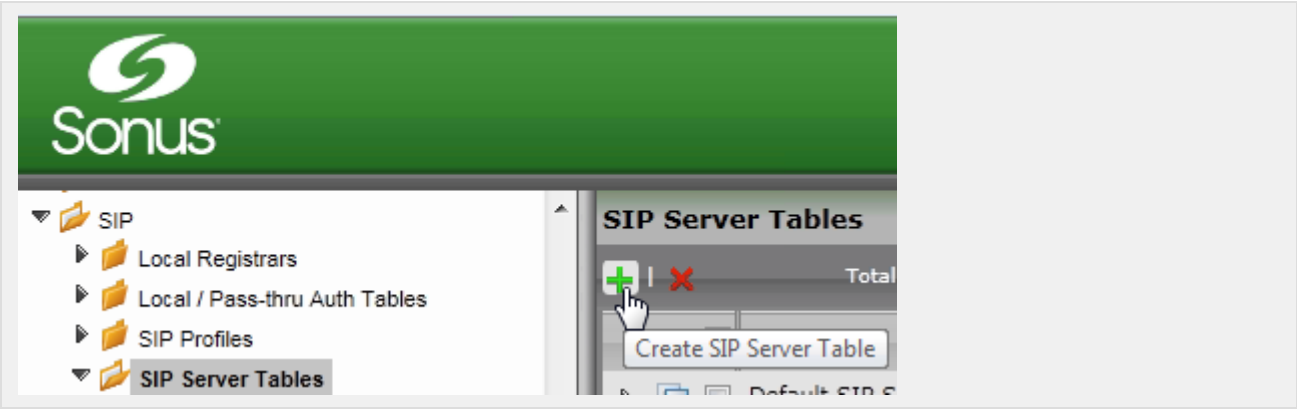
Timer T1	**500**
Timer T2	**4000**
Timer T4	**5000**
Timer D	**32000**
Timer B	**32000** *ms*
Timer F	**32000** *ms*
Timer H	**32000** *ms* *(64*TimerT1)*
Timer J	**32000** *ms* *(64*TimerT1)*

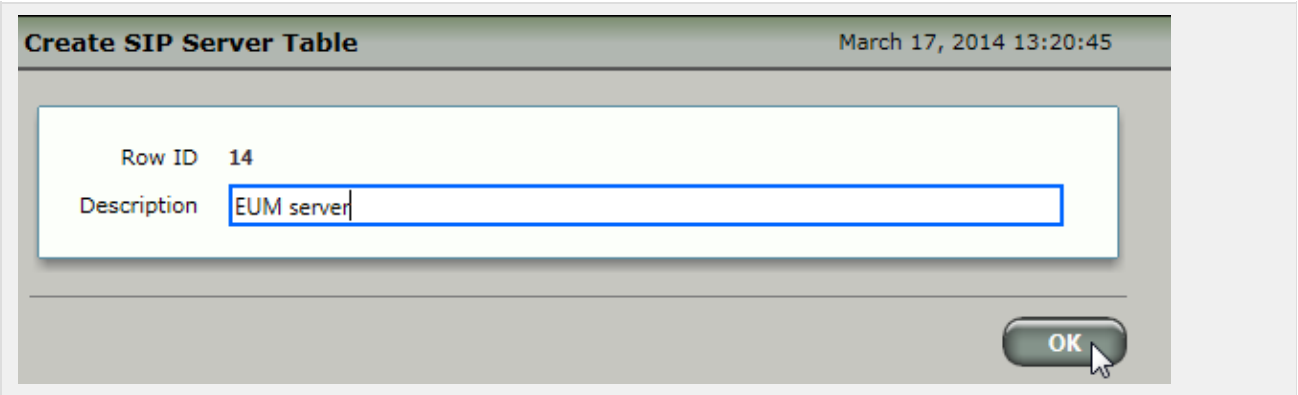
SDP Customization

Send Number of Audio Channels	**True**
Connection Info in Media Section	**True**
Origin Field Username	**SBC**
Session Name	**VoipCall**

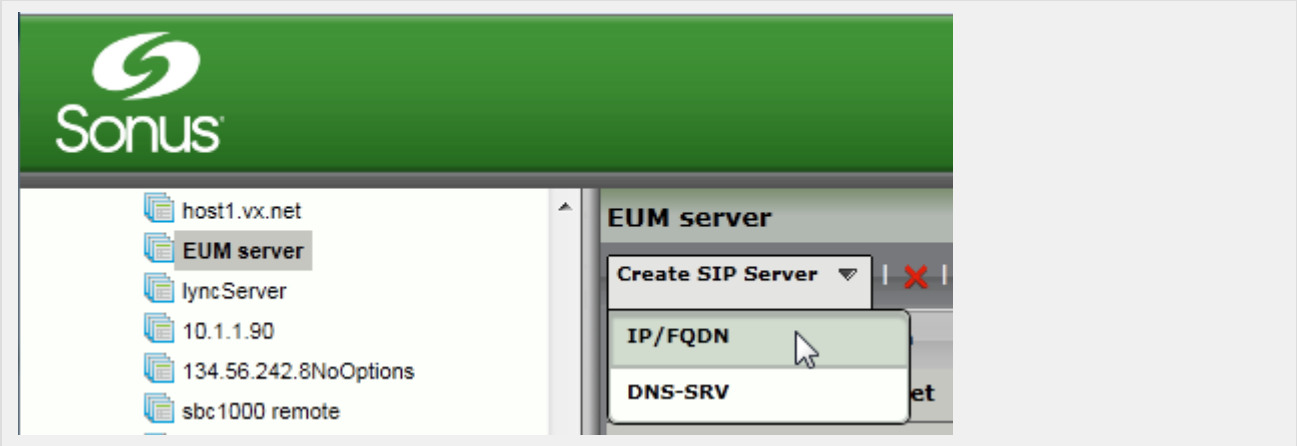
Copyright © 2015 Sonus Networks. All rights reserved.

3. Create a SIP Server Table for the Exchange Server.

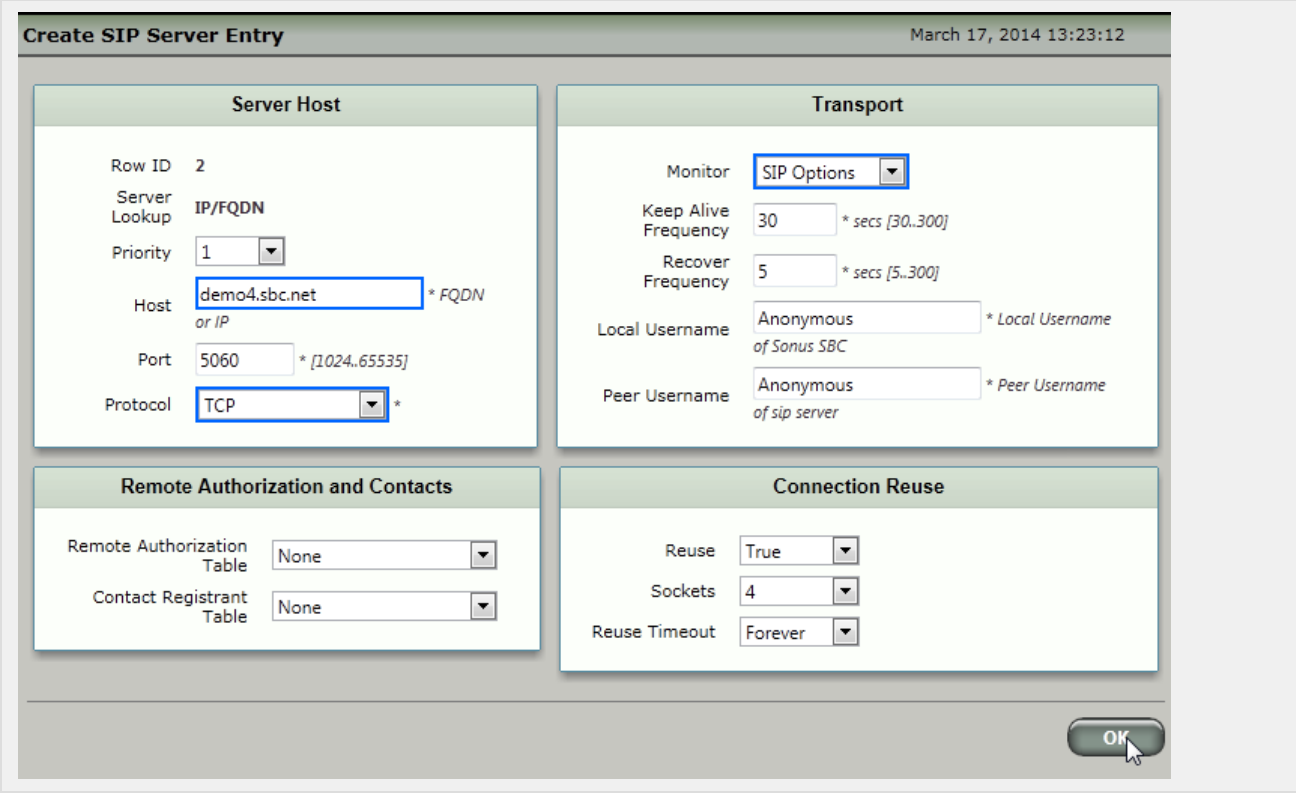




4. Add the Exchange Server to the newly created SIP Server Table.



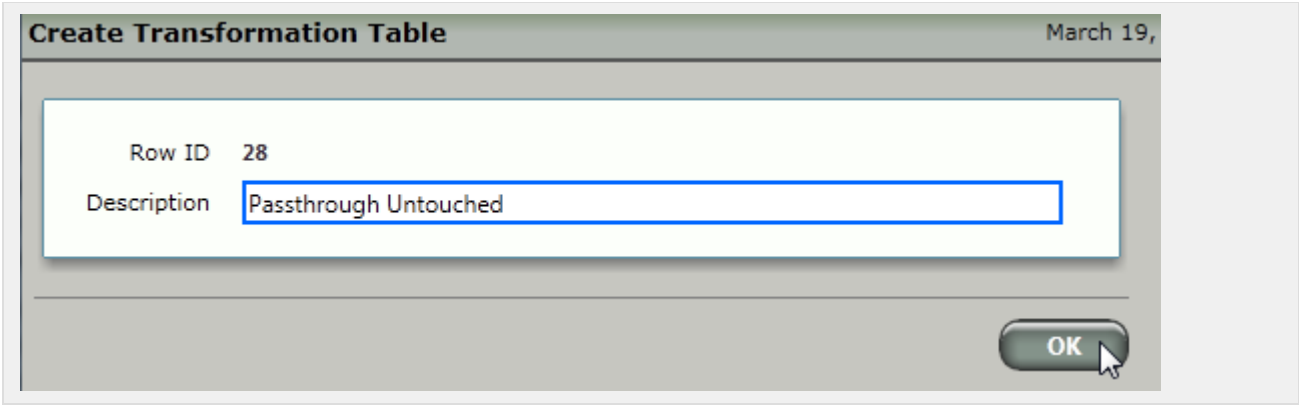
Copyright © 2015 Sonus Networks. All rights reserved.

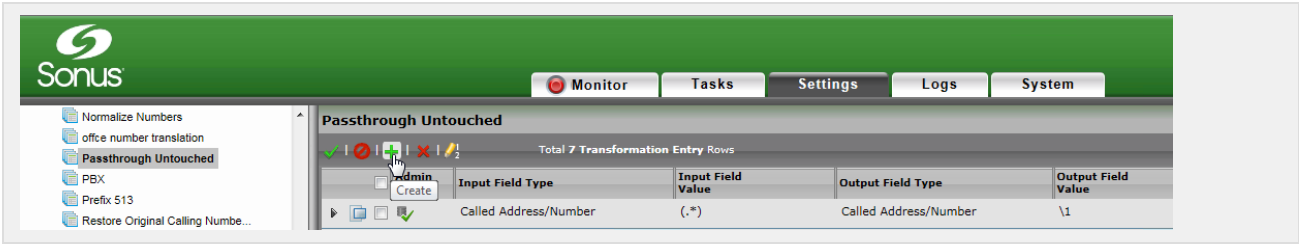


5. Create a Transformation Table and Transformation Entries to be used to process calls sent from Exchange's Subscriber Access (SA) and Automated Attendant (AA) to the SBC. In the example below, no manipulation is performed on the calls received from Exchange. Adjust your configuration according to your specific needs.

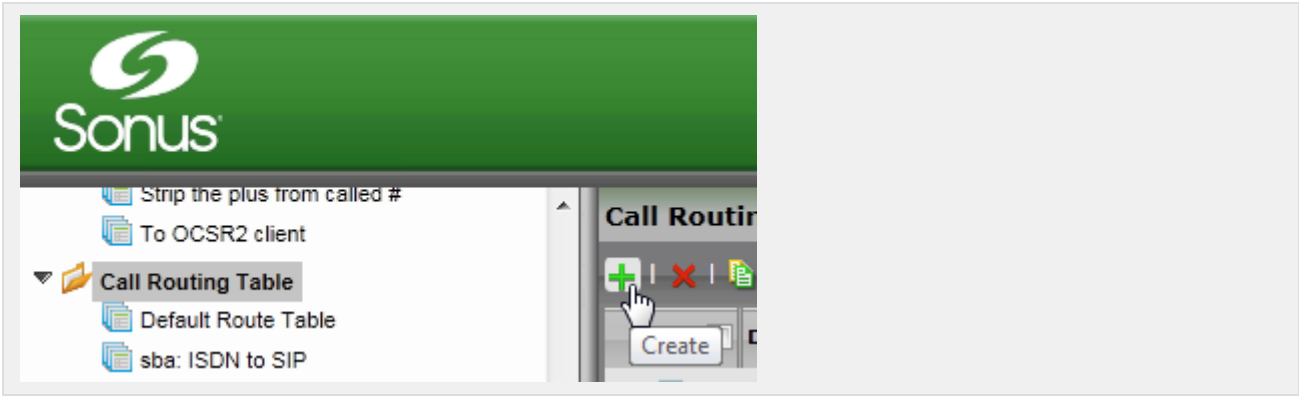


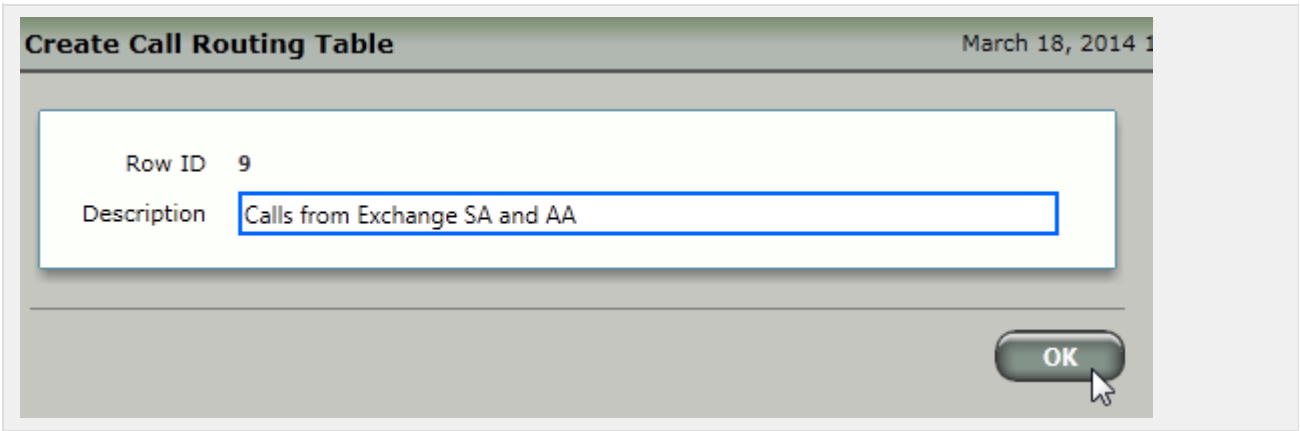
Copyright © 2015 Sonus Networks. All rights reserved.





6. Create a Call Routing Table to process incoming calls from the Exchange SA and AA.

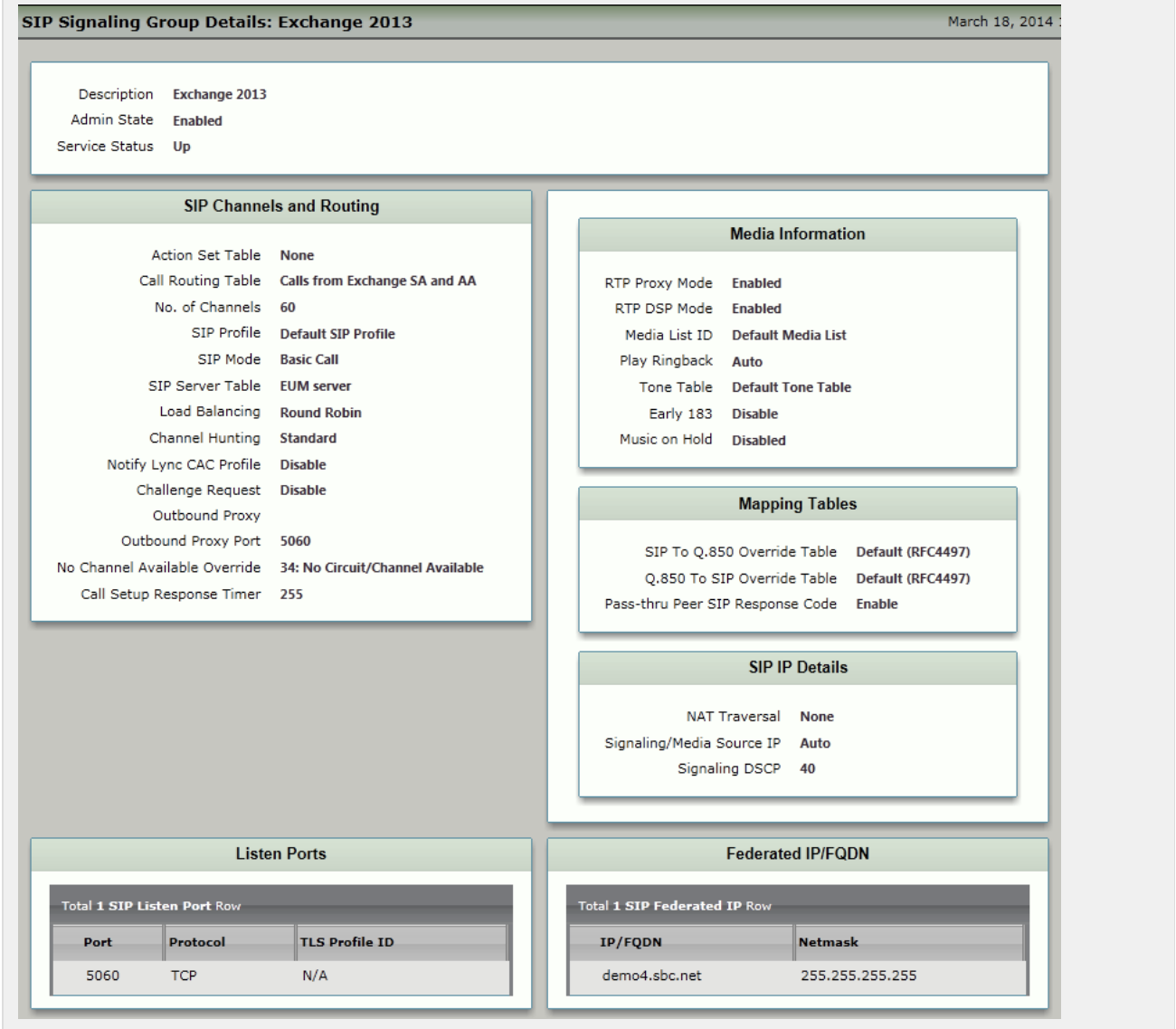




7. Create a SIP Signaling Group to process incoming SIP calls from the Exchange Subscriber Access and Automated Attendant.

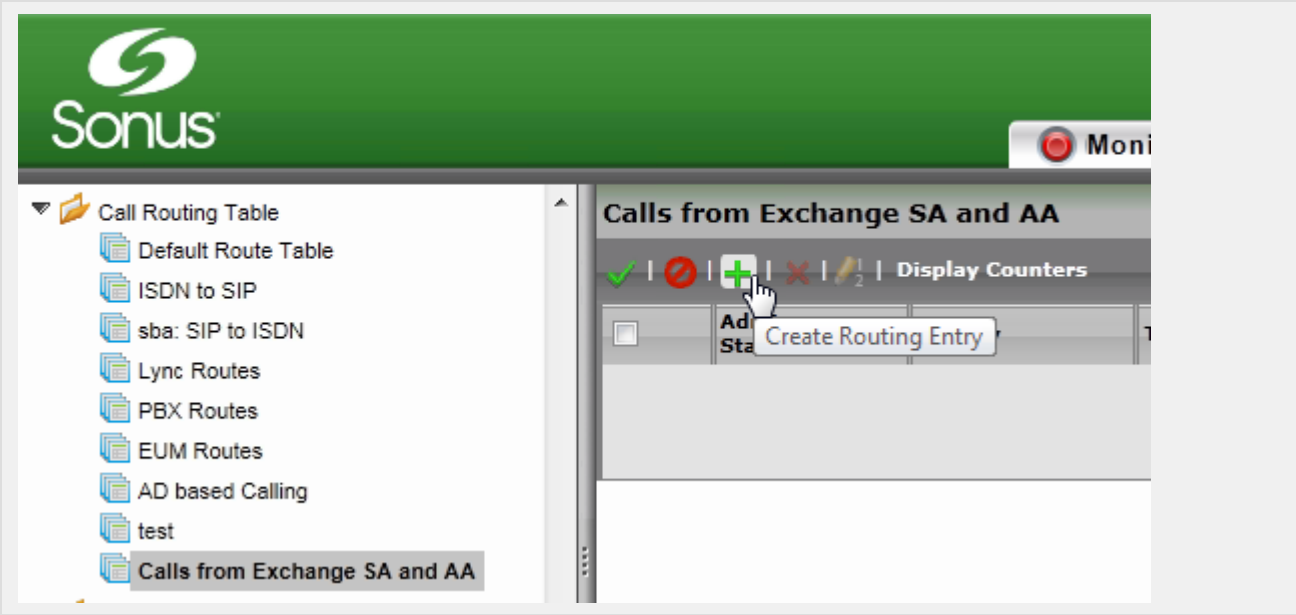
Copyright © 2015 Sonus Networks. All rights reserved.



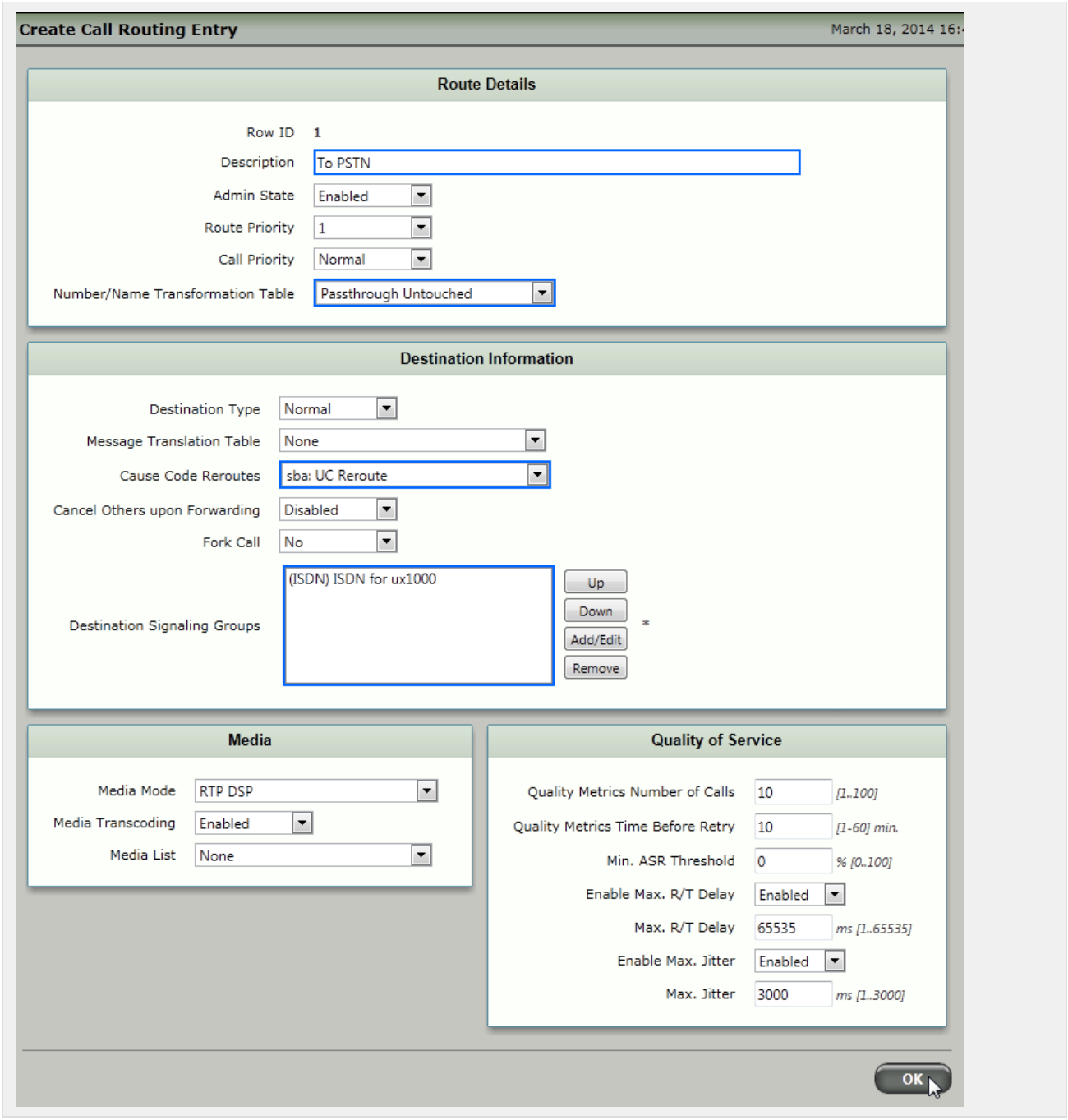


Copyright © 2015 Sonus Networks. All rights reserved.

8. Create entries in the Call Route Table. These call route entries process incoming calls from the Exchange Subscriber Access and Auto Attendant. Create a call route for every possible destination for Exchange SA/AA calls.



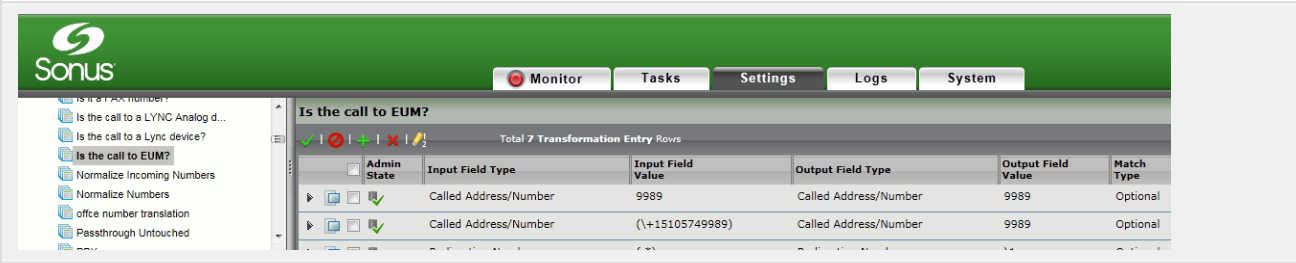
Copyright © 2015 Sonus Networks. All rights reserved.



9. In addition to the above configuration that supports incoming calls from Exchange, you will need to create corresponding configurations to route calls *to* Exchange from other sources (such as PSTN and PBXs). It is strongly recommended that transformations for Exchange SA/AA appear at the top any transformation table. These entries not only handle the initial calls to Exchange, but also the 302 from Exchange (used during the call setup).

> Not placing the Exchange transformations at the top of the transformation table may cause the 302 to fail, which will cause the calls to Exchange to fail.

Copyright © 2015 Sonus Networks. All rights reserved.



When configuring for TLS, in Exchange Configuration, Step 5, change the SBC *address* to the SBC's FQDN rather than IP.

It has been reported that when a Exchange user has extensions for both Lync and direct-to-SBC dial plans that Exchange will send Message Waiting Indicator status only to the Lync extension. Exchange will not send MWI to a user's telephone extension when that user also has a Lync extension.

Configuring TDM ports on the SBC 1000-2000

Table of Contents

- Prerequistes
- SBC 1000/2000 TDM port configuration
- Additional Information

About this Page

- This document details how to configure a Sonus 1000/2000 TDM port
- This document presumes the reader is familiar with configuring the SBC 1000/2000

Related Articles

- Managing Telephony Ports
- Managing ISDN Signaling Groups

Prerequistes

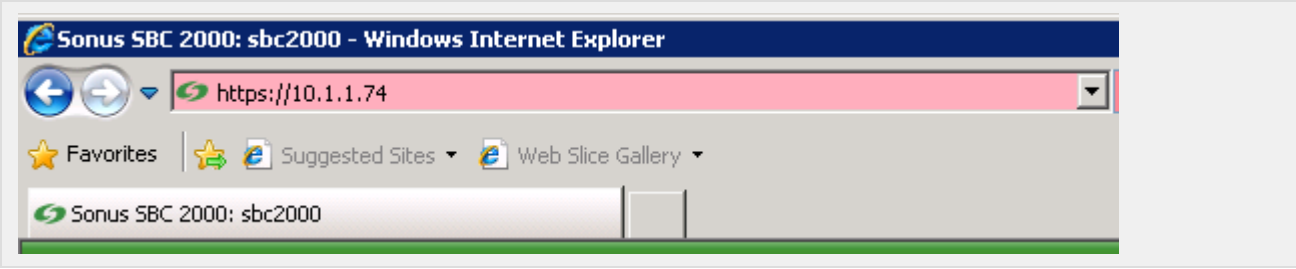
Requires Sonus SBC1000/2000 Version 3.0

Copyright © 2015 Sonus Networks. All rights reserved.

SBC 1000/2000 TDM port configuration

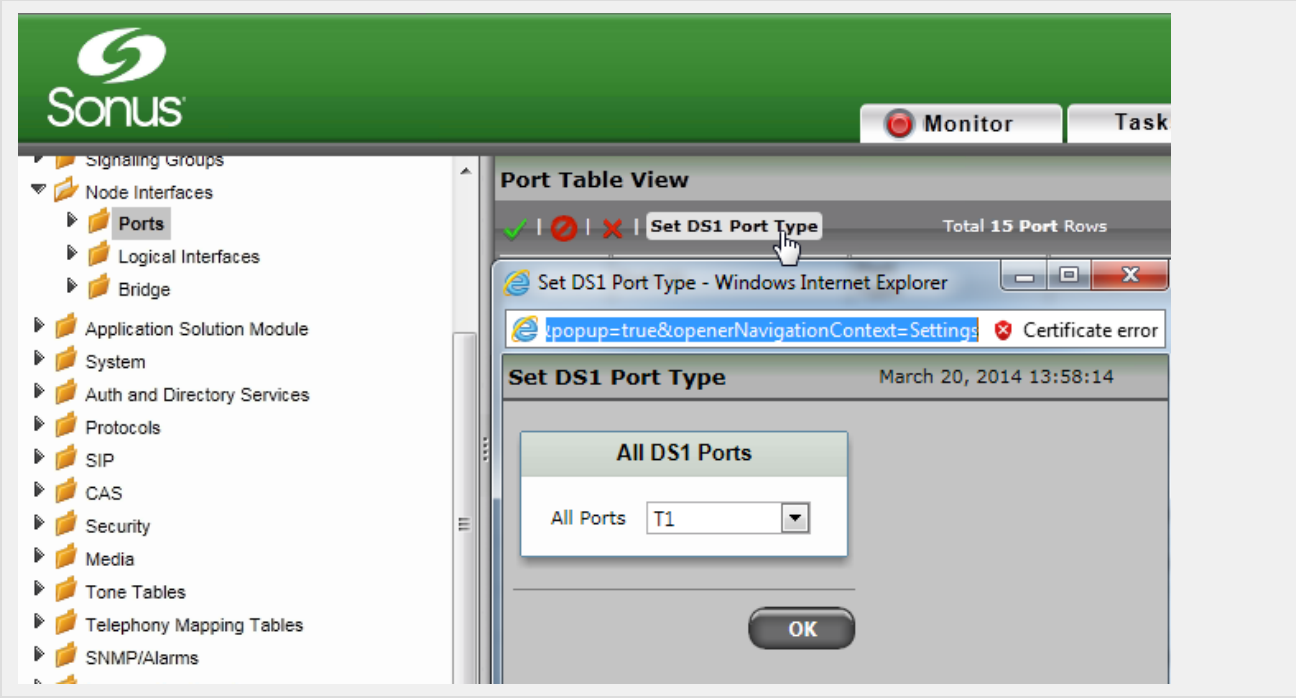
Use the following to configure a SBC 1k/2k TDM port to interconnect to another TDM port/device.

1. Connect to the SBC interface via your web browser.



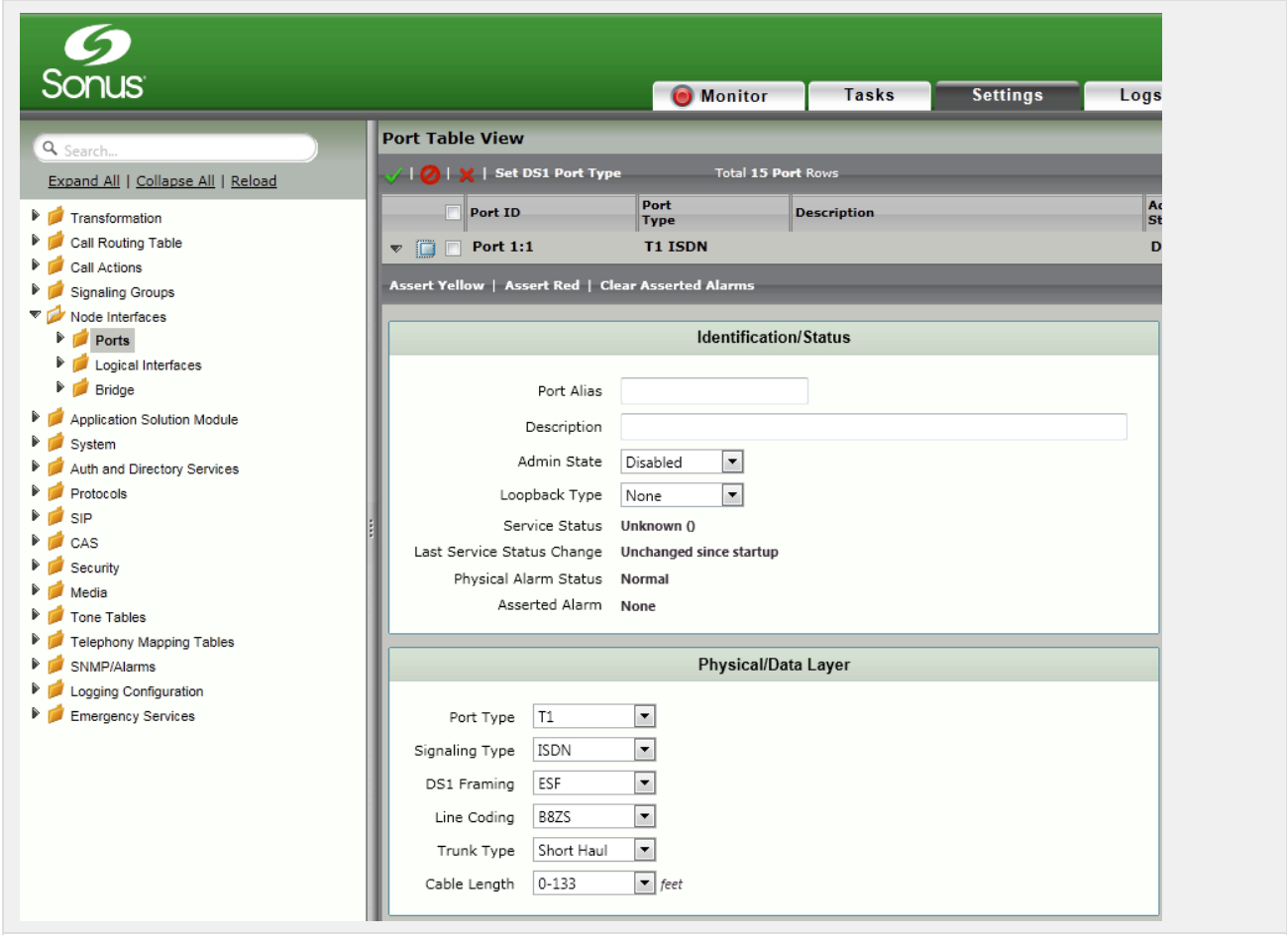
2. Set the DS1 Type of the ports on your TDM card, either T1 or E1 depending upon your installation situation.

> More information on the TDM port configuration parameters can be found at Managing Telephony Ports.



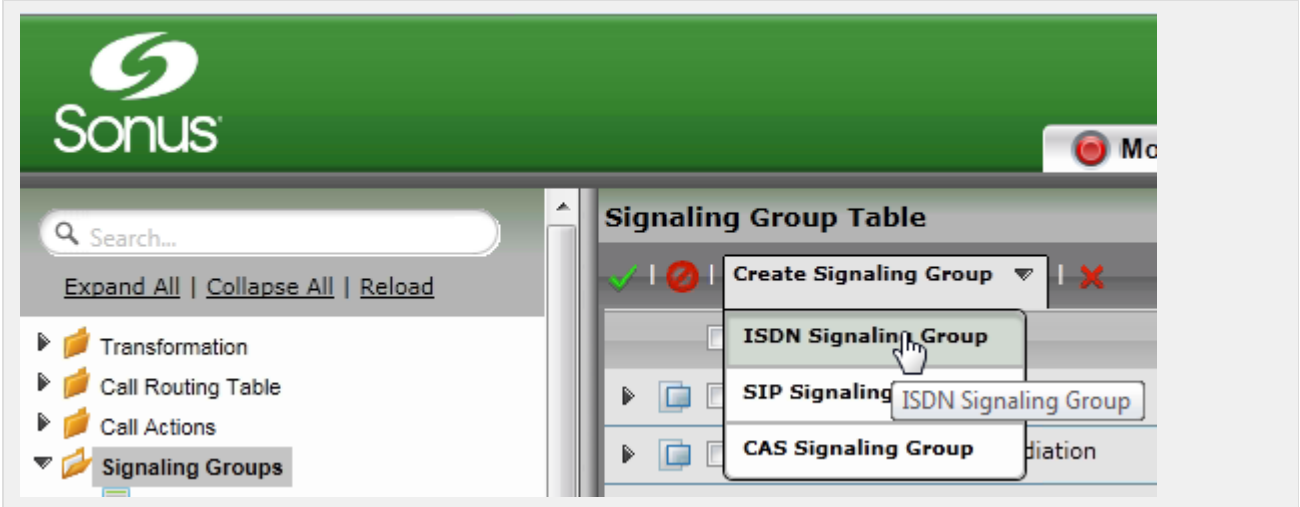
3. Configure the TDM port parameters to match with your installation.

Copyright © 2015 Sonus Networks. All rights reserved.



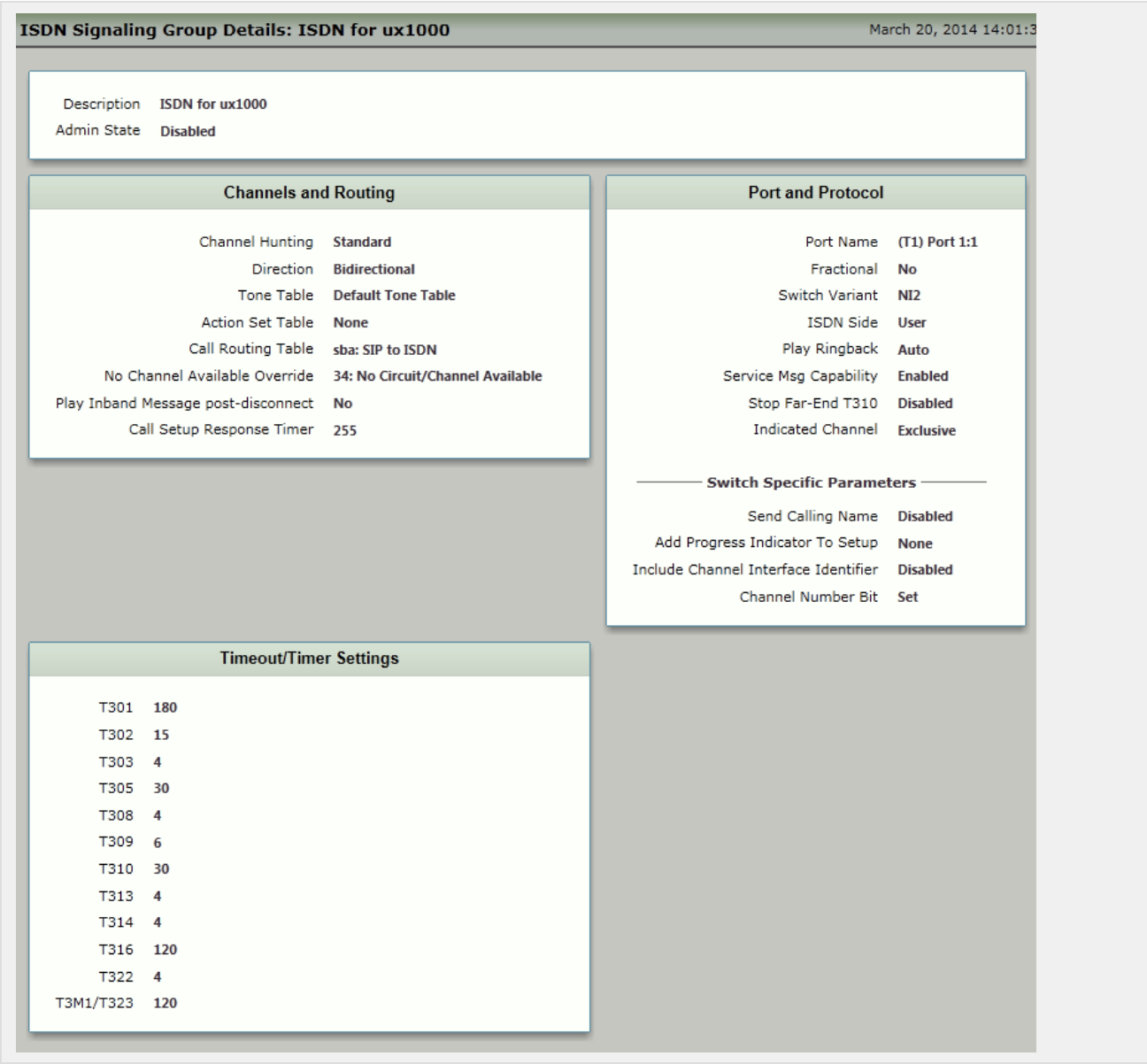
4. Create a ISDN Signaling Group to process inbound calls from the TDM port.

> More information on the TDM Signaling Group configuration parameters can be found at Managing ISDN Signaling Groups.



Copyright © 2015 Sonus Networks. All rights reserved.

5. Configure the ISDN Signaling Group to match the requirements of the incoming TDM signaling.

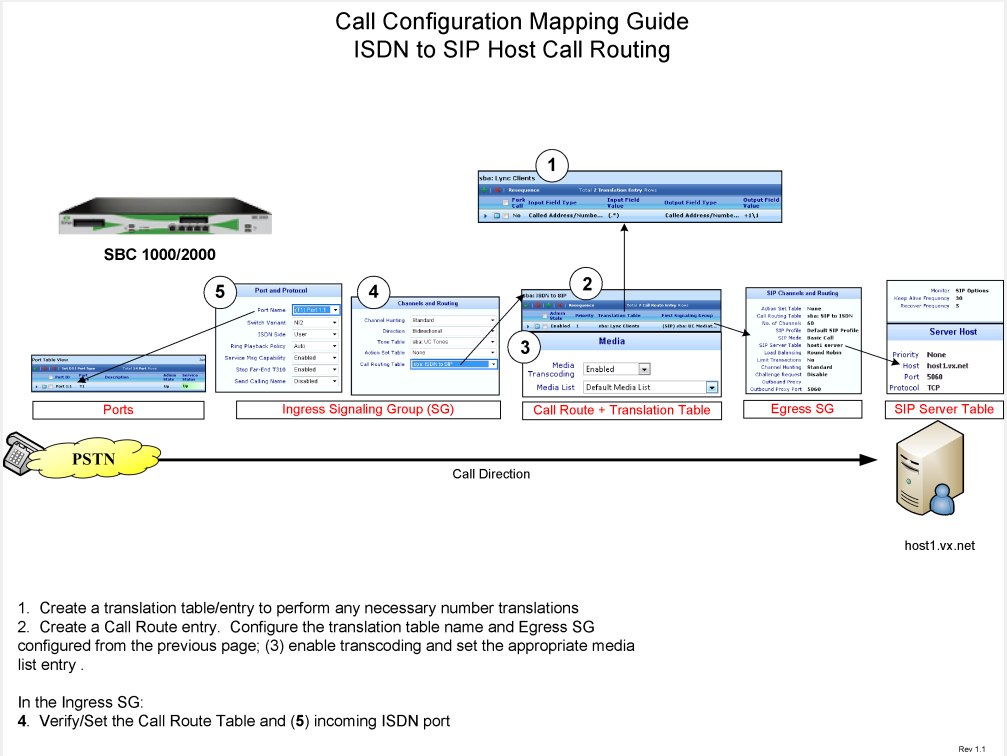


6. You will need to create and configure call routing tables/entries, transformation tables/entries and destination Signaling Groups in order to successfully route calls from a ISDN port to any given destination.

Additional Information

Below is a diagram for configuring a TDM port to route to a SIP destination

Copyright © 2015 Sonus Networks. All rights reserved.



- Download TDM Routing Diagram

Configuring the Avaya S8300/8400/8500/8700 v.3.1.x to connect via TDM to the SBC 1000-2000

Table of Contents

- Prerequistes
- Interoperation Notes
- PBX Configuration

About this Page

- This Interoperability Note describes how to configure a TDM port on a Avaya S8300/8400/8500/8700 PBX to integrate with the Sonus SBC 1k/2k. Also included is configuration information for integrating Exchange Unified Messaging to the Avaya PBX via the Sonus SBC.

Related Articles

- Managing Telephony Ports

Prerequistes

- Requires Sonus SBC1000/2000 Version 3.0

- Avaya S8x00 PBX, Version 3.1.x, T1, QSIG

Copyright © 2015 Sonus Networks. All rights reserved.

Interoperation Notes

The following extension numbers are used within this document:

- UMS Pilot Extension: 2562
- Extensions enabled for Microsoft Exchange Server UM: 5100 - 5199

PBX Configuration

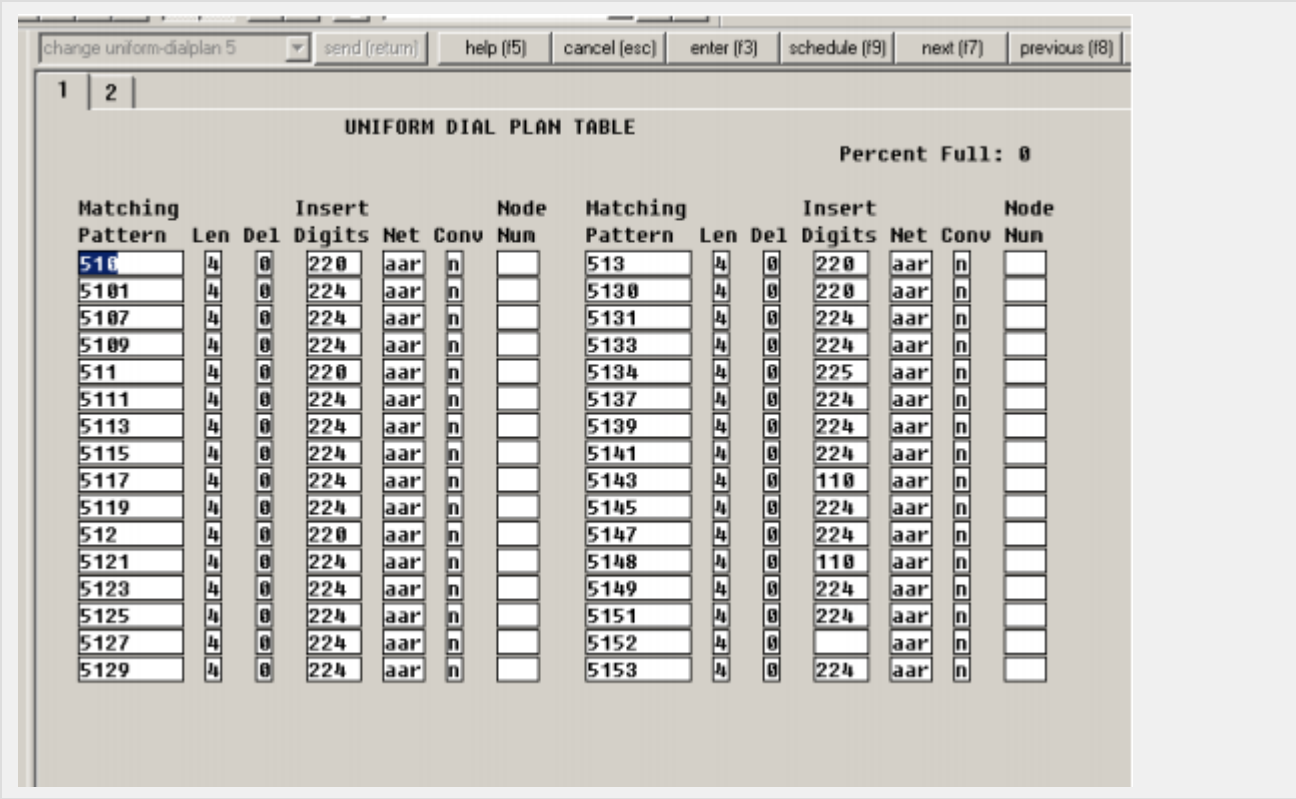
Use the following configurations to interconnect the Avaya to the SBC1k/2k.

1. Change Uniform Dialplan

   Destinations on the SBC must be identified in the Uniform Dial Plan.

   In this example extensions are individually identified but there is no reason a block of numbers could be used (matching 51 for 4 = 5100-5199).

   For all individual stations or groups:
   - Length = 4 (number of digits in the number)
   - Deleted = zero (No digits to be deleted)
   - Inserted Digits = 110 (used to route calls in AAR)
   - Net = AAR
   - Conv = N
   - Node Num = blank



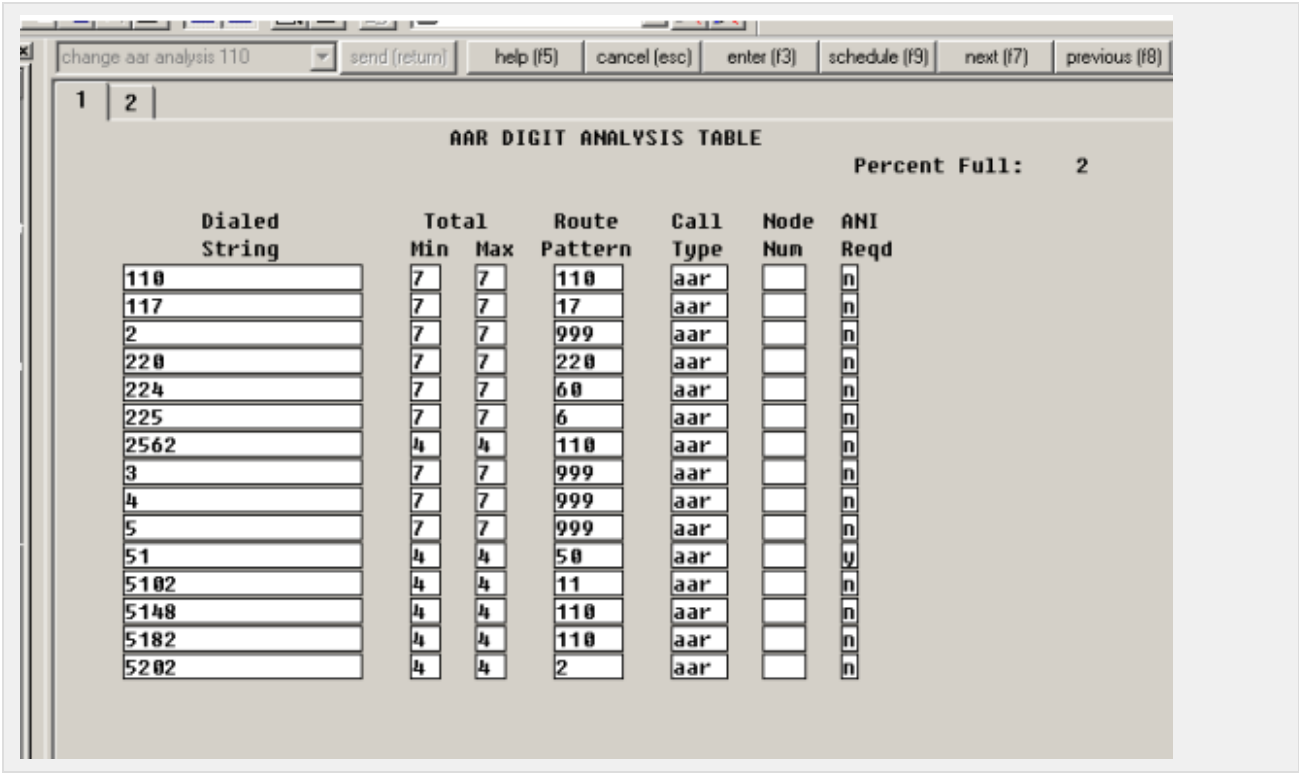
Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num	Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num
516	4	0	220	aar	n		513	4	0	220	aar	n	
5101	4	0	224	aar	n		5130	4	0	220	aar	n	
5107	4	0	224	aar	n		5131	4	0	224	aar	n	
5109	4	0	224	aar	n		5133	4	0	224	aar	n	
511	4	0	220	aar	n		5134	4	0	225	aar	n	
5111	4	0	224	aar	n		5137	4	0	224	aar	n	
5113	4	0	224	aar	n		5139	4	0	224	aar	n	
5115	4	0	224	aar	n		5141	4	0	224	aar	n	
5117	4	0	224	aar	n		5143	4	0	110	aar	n	
5119	4	0	224	aar	n		5145	4	0	224	aar	n	
512	4	0	220	aar	n		5147	4	0	224	aar	n	
5121	4	0	224	aar	n		5148	4	0	110	aar	n	
5123	4	0	224	aar	n		5149	4	0	224	aar	n	
5125	4	0	224	aar	n		5151	4	0	224	aar	n	
5127	4	0	224	aar	n		5152	4	0		aar	n	
5129	4	0	224	aar	n		5153	4	0	224	aar	n	

2. Change AAR Digit Analysis

Copyright © 2015 Sonus Networks. All rights reserved.

All calls starting with 110 and 7 digits in length are forwarded to AAR for distribution

- Dialed String = 110 [digits inserted in uniform dial plan]
- Min = 7 [110xxxx]
- Max = 7 [110xxxx]
- Route Pattern = 110 [SBC 1k/2k Route Pattern]

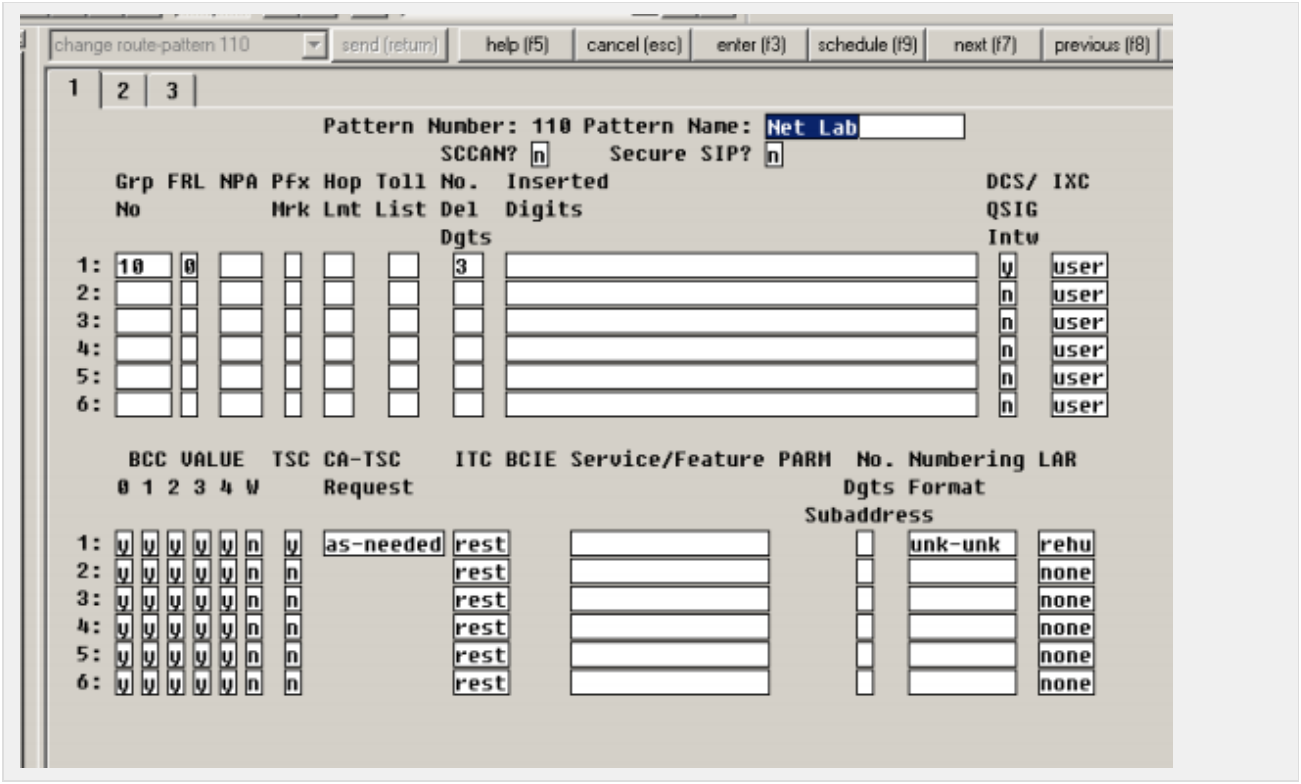


3. Change Route Pattern

   Calls directed to route pattern 110 from the AAR digit analysis are forwarded to trunk group 10 in this operation. The first three digits [110] are dropped from the number so the call hits the Sonus SBC 1k/2k as a 4-digit extension.

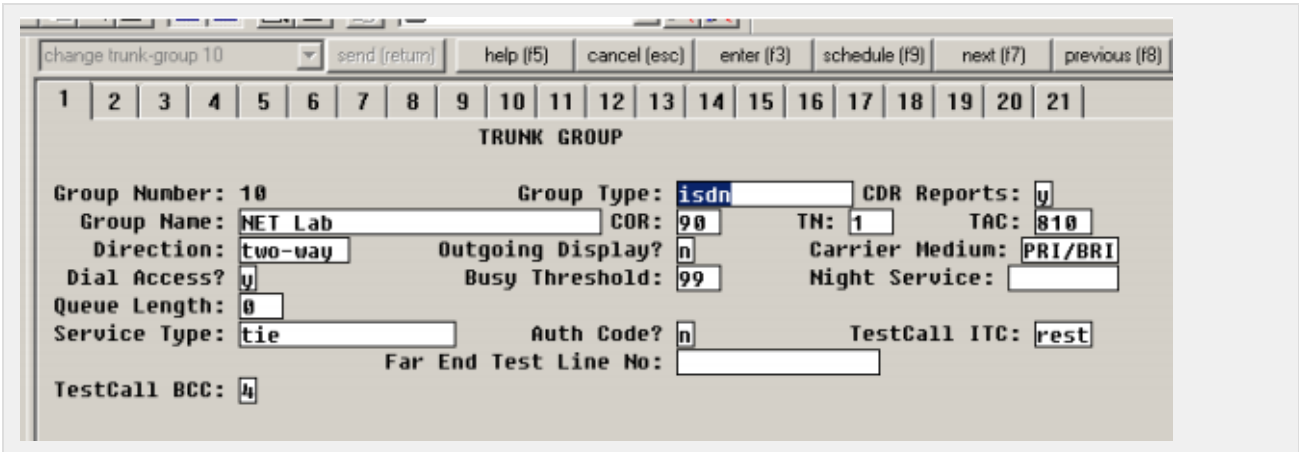
   - Grp No = 10 [trunk group 10]
   - Del Dgts = 3 [deleted 110 from the number]

Copyright © 2015 Sonus Networks. All rights reserved.

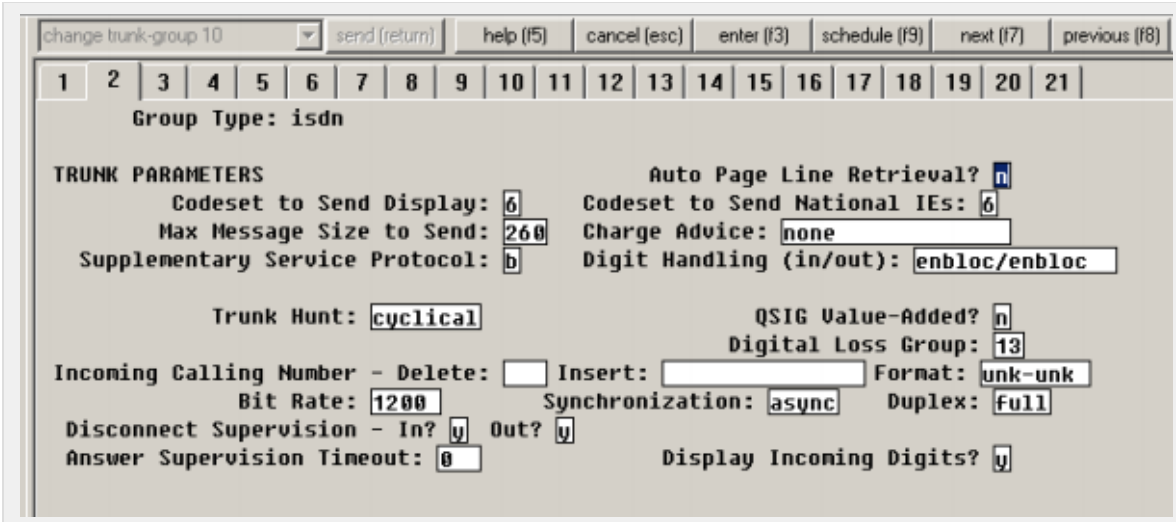


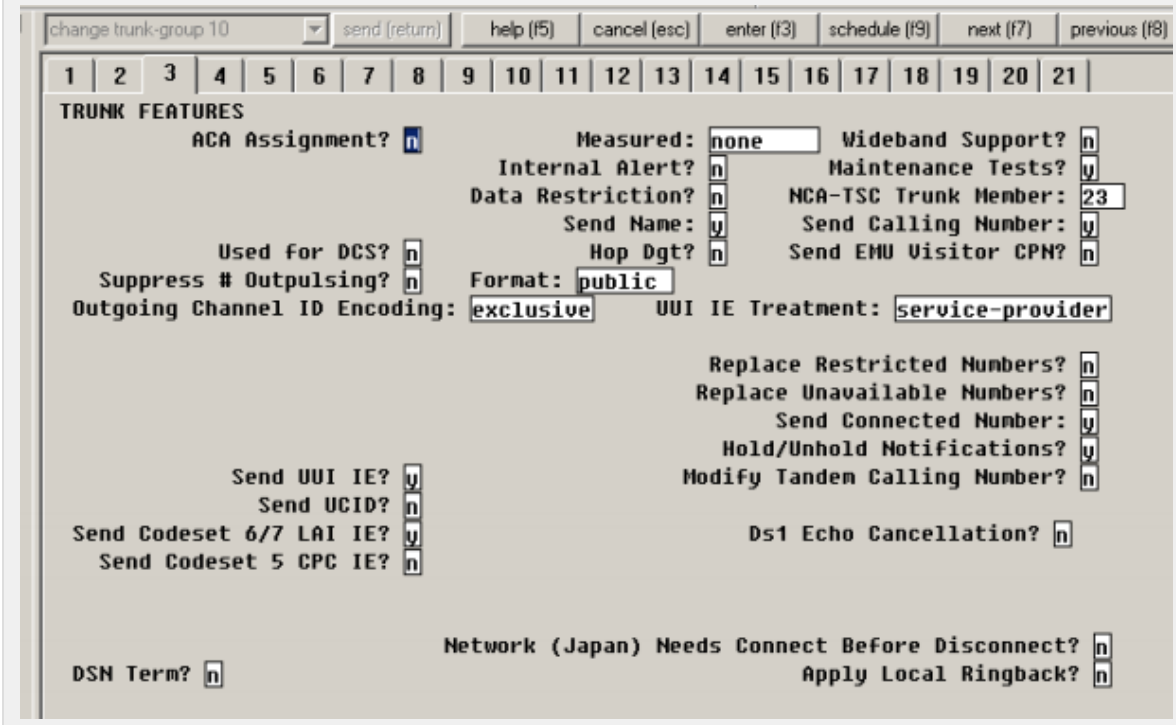
4. Change Trunk Group

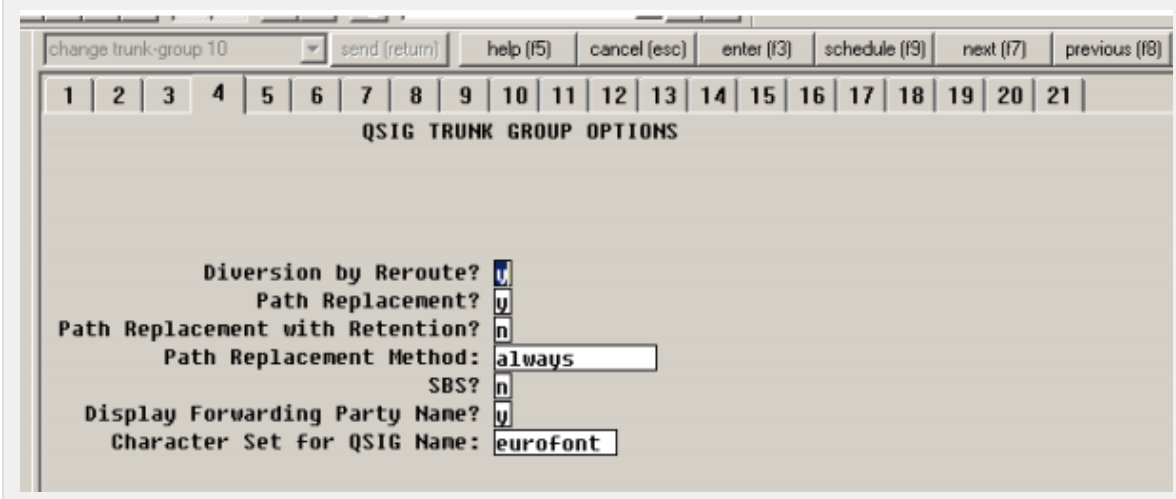
   Trunk group 10 is a standard 23 channel QSIG T1 trunk used in UM integrations.



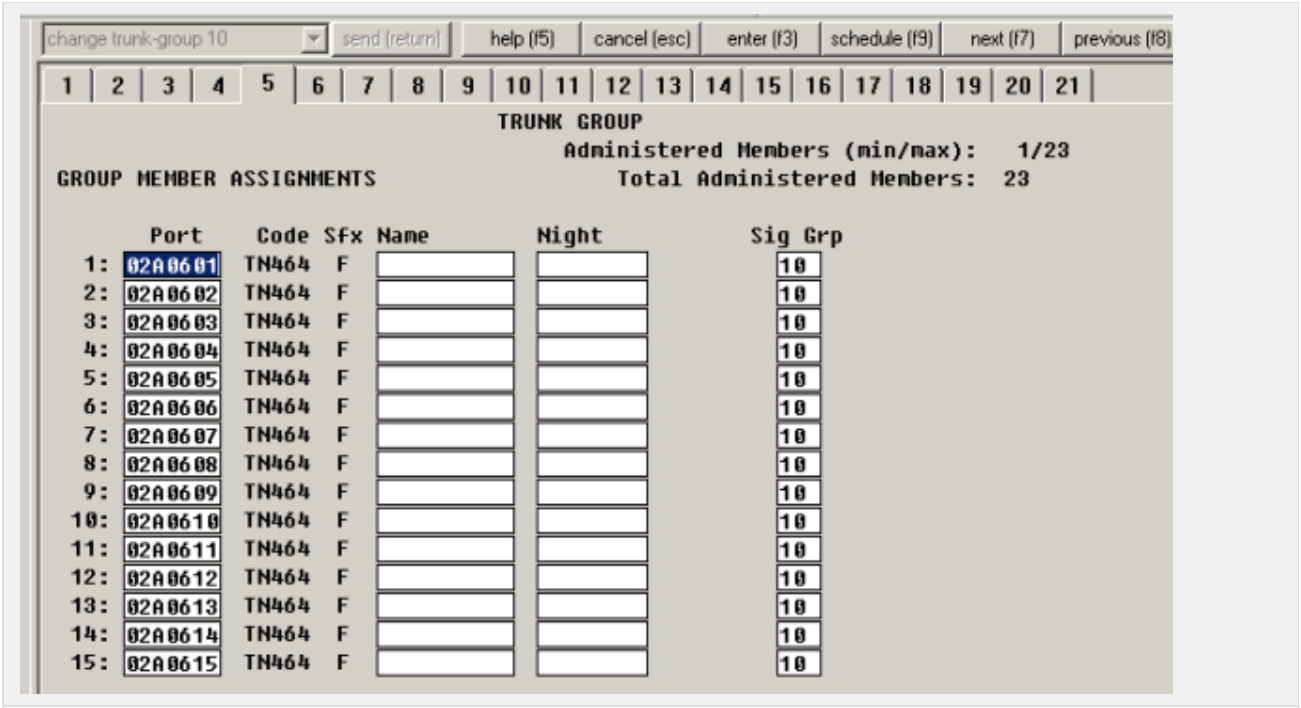
Copyright © 2015 Sonus Networks. All rights reserved.

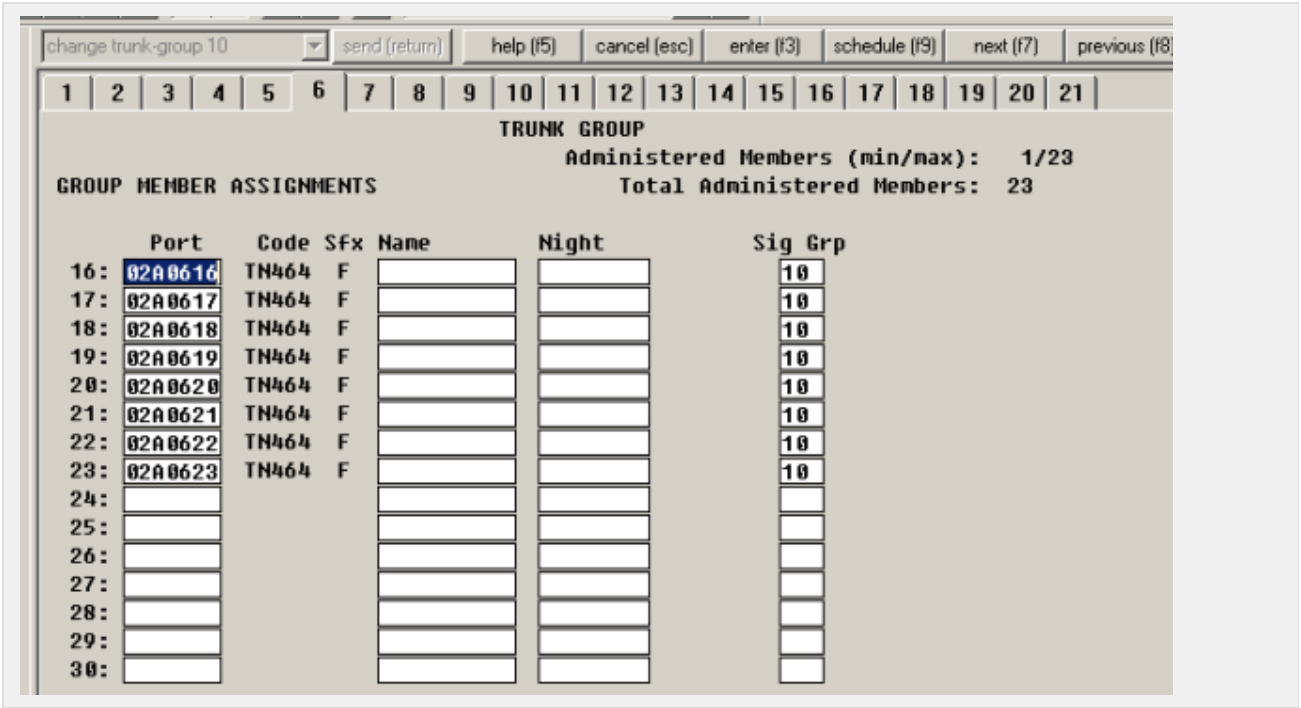






Copyright © 2015 Sonus Networks. All rights reserved.

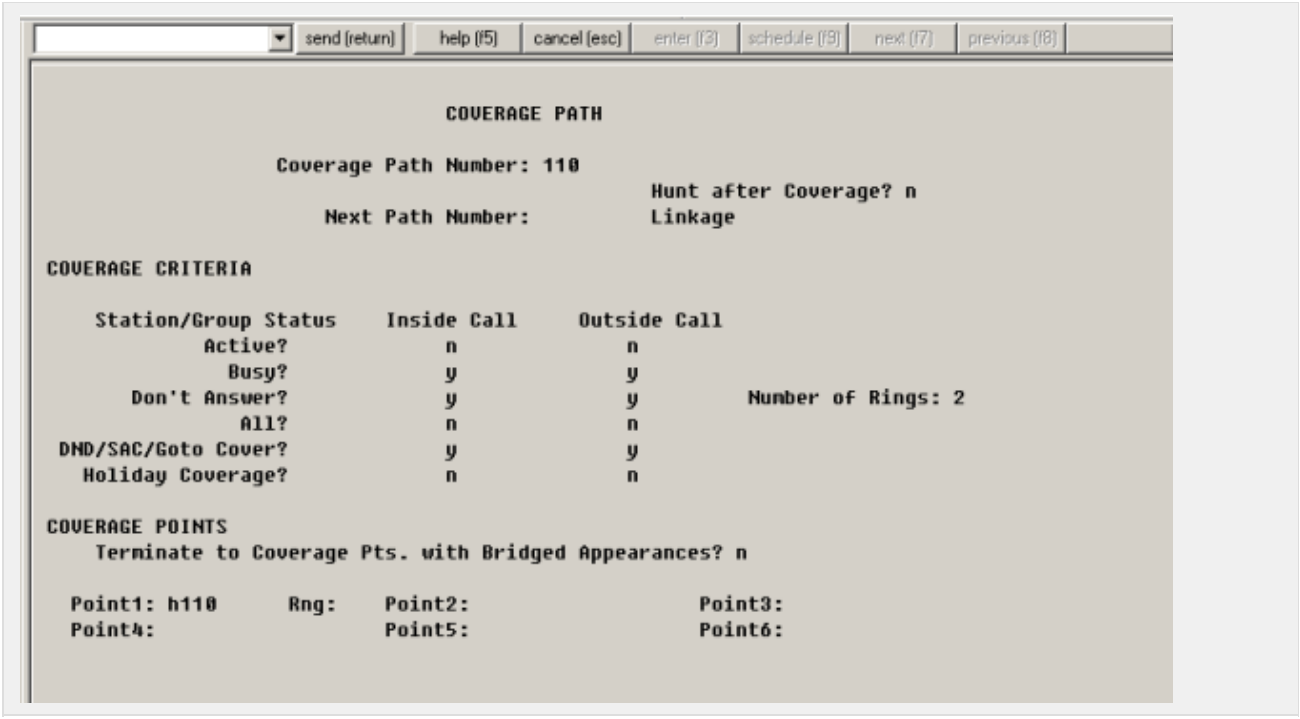




5. Change Coverage Path

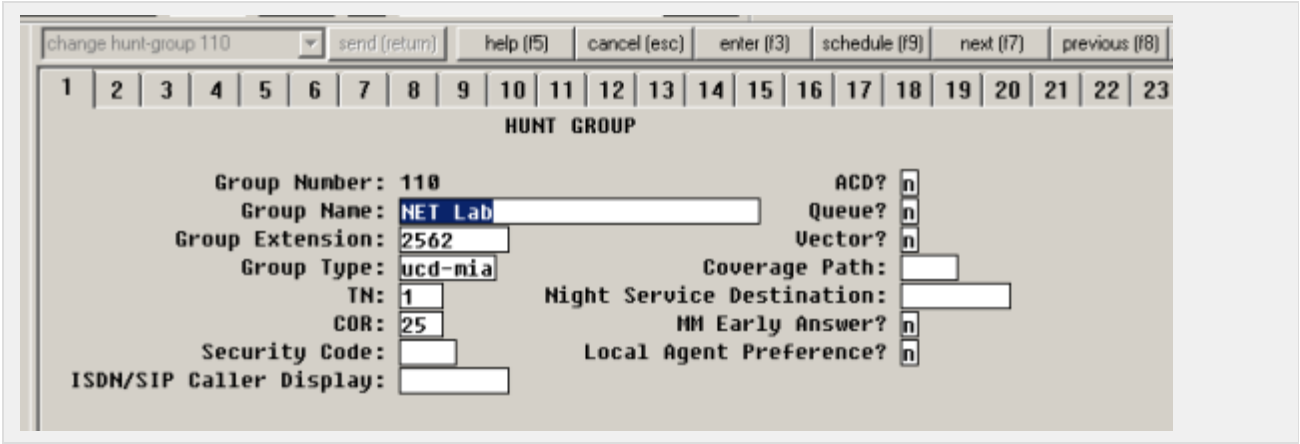
   Coverage path is available for routing unanswered calls on PBX extensions to Unified Messaging over the Sonus SBC 1k/2k. This configuration directs the unanswered call to hunt group 110.

Copyright © 2015 Sonus Networks. All rights reserved.

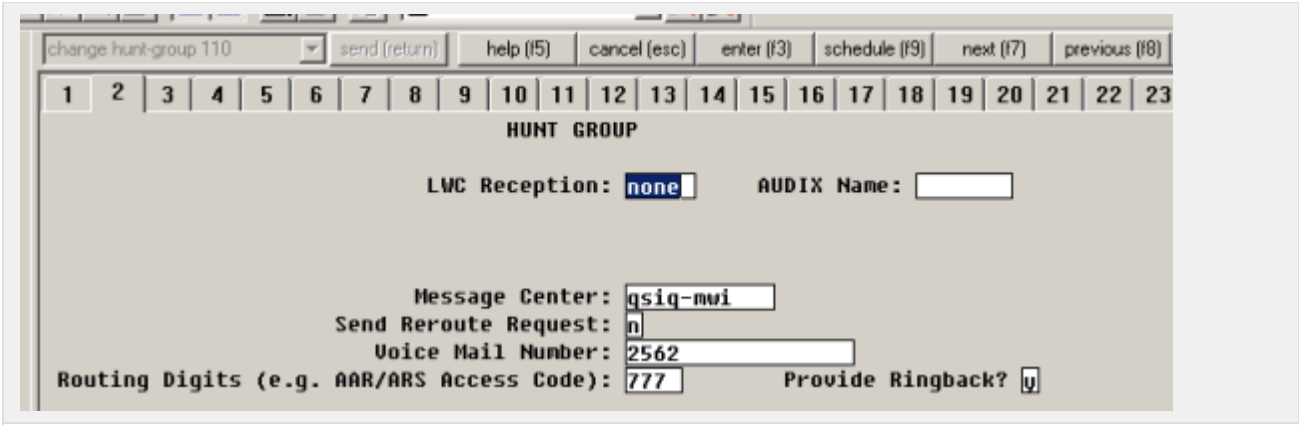


6. Change Hunt Group

   All calls forwarded to this hunt group are redirected to 7772562. The original called party and calling party are retained and sent in the data stream to voicemail so the call hits the correct mailbox.

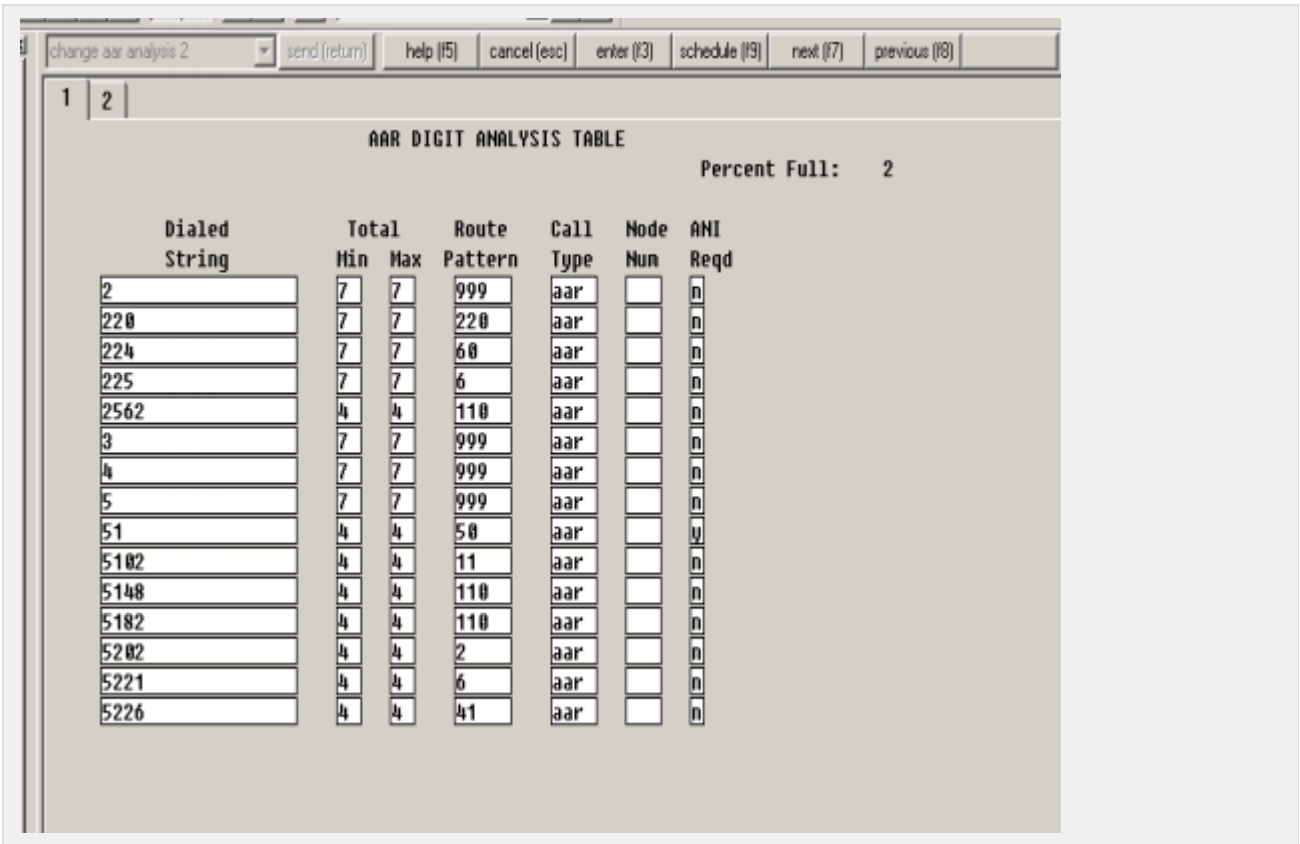


Copyright © 2015 Sonus Networks. All rights reserved.



7. Change AAR Digit Analysis

   All calls for 7772562 are handled via dialed string 2562. The (forward calls) feature access code 777 is ignored and the 4 digits behind it are used to determine the path of the call.

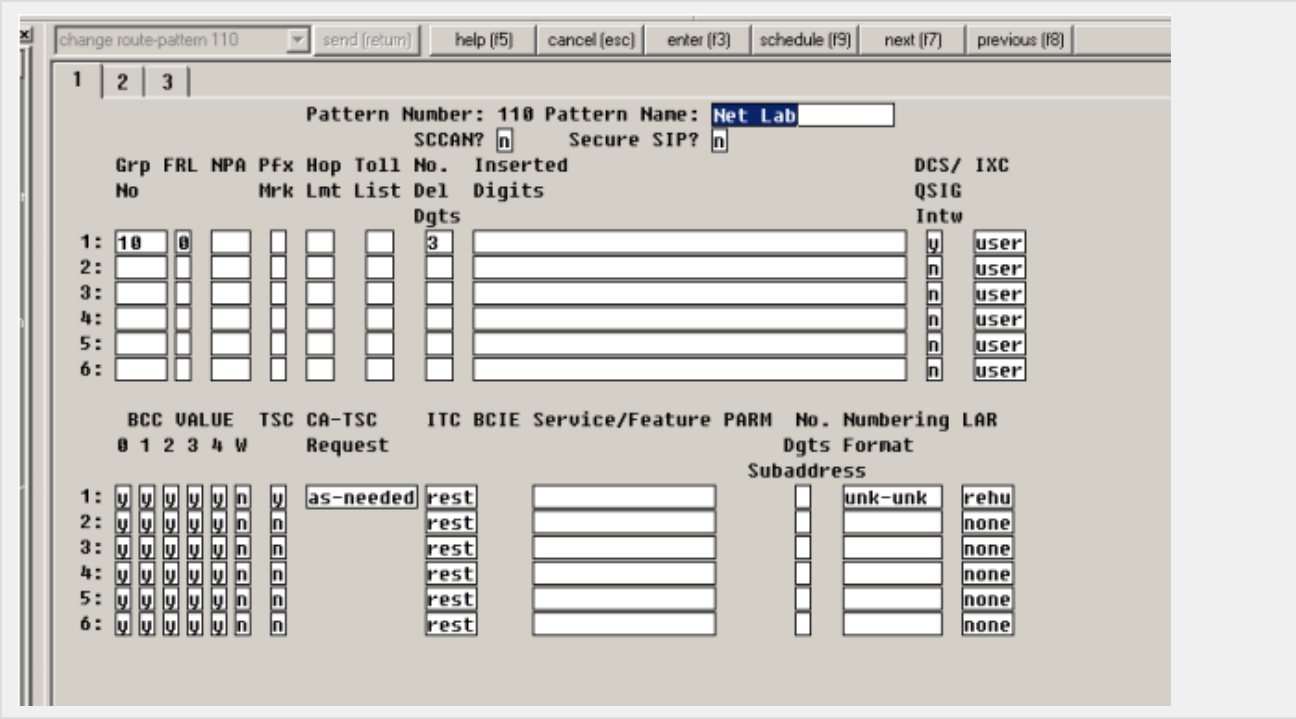


8. Change Route Pattern

   Calls directed to route pattern 110 from the AAR digit analysis are forwarded to trunk group 10 in this operation. The first three digits [777] are dropped from the number so the call hits the gateway as 2562.

Copyright © 2015 Sonus Networks. All rights reserved.

- Grp No = 10 [trunk group 10]
- Del Dgts = 3 [deleted 777 from the number]



9. Use the TDM document to configure the SBC 1k/2k.

   - Configuring TDM ports on the SBC 1k/2k

10. Use the EUM integration document to finished the voicemail integration.

    - Configuring SBC 1000/2000 with Exchange 2013

Configuring the Mitel 3300 ICP v9.0.0.41 to connect via TDM to the SBC 1000-2000

Table of Contents

- Prerequistes
- Interoperation Notes
- PBX Configuration

Copyright © 2015 Sonus Networks. All rights reserved.

About this Page

- This Interoperability Note describes how to configure a TDM port on a Mitel 3000 ICP PBX to integrate with the Sonus SBC 1k/2k. Also included is configuration information for integrating Exchange Unified Messaging to the Mitel PBX via the Sonus SBC.

Related Articles

- Managing Telephony Ports

Prerequistes

Requires Sonus SBC1000/2000 Version 3.0

Mitel 3300 ICP PBX, Version 9.0.0.41, T1, QSIG

Interoperation Notes

The following extension numbers are used within this document:

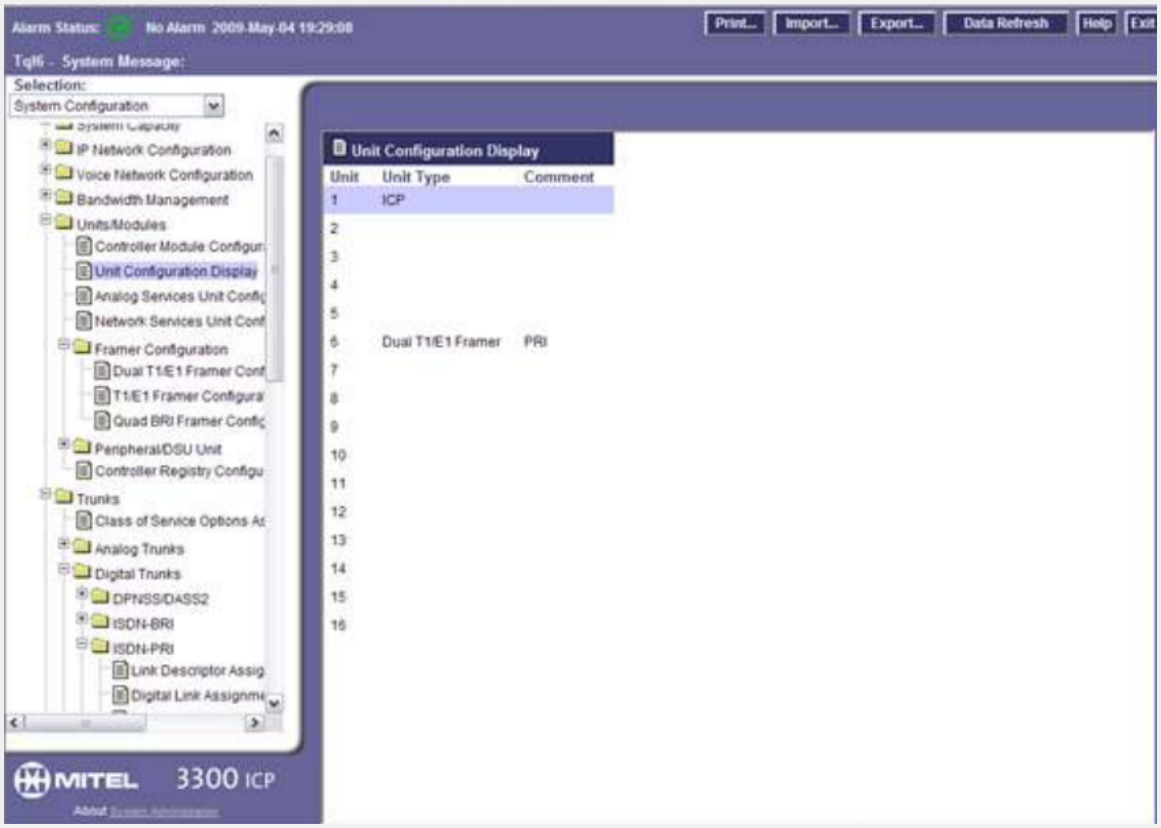
- UMS Pilot Extension: 2562
- Extensions enabled for Microsoft Exchange Server UM: 5100 - 5199

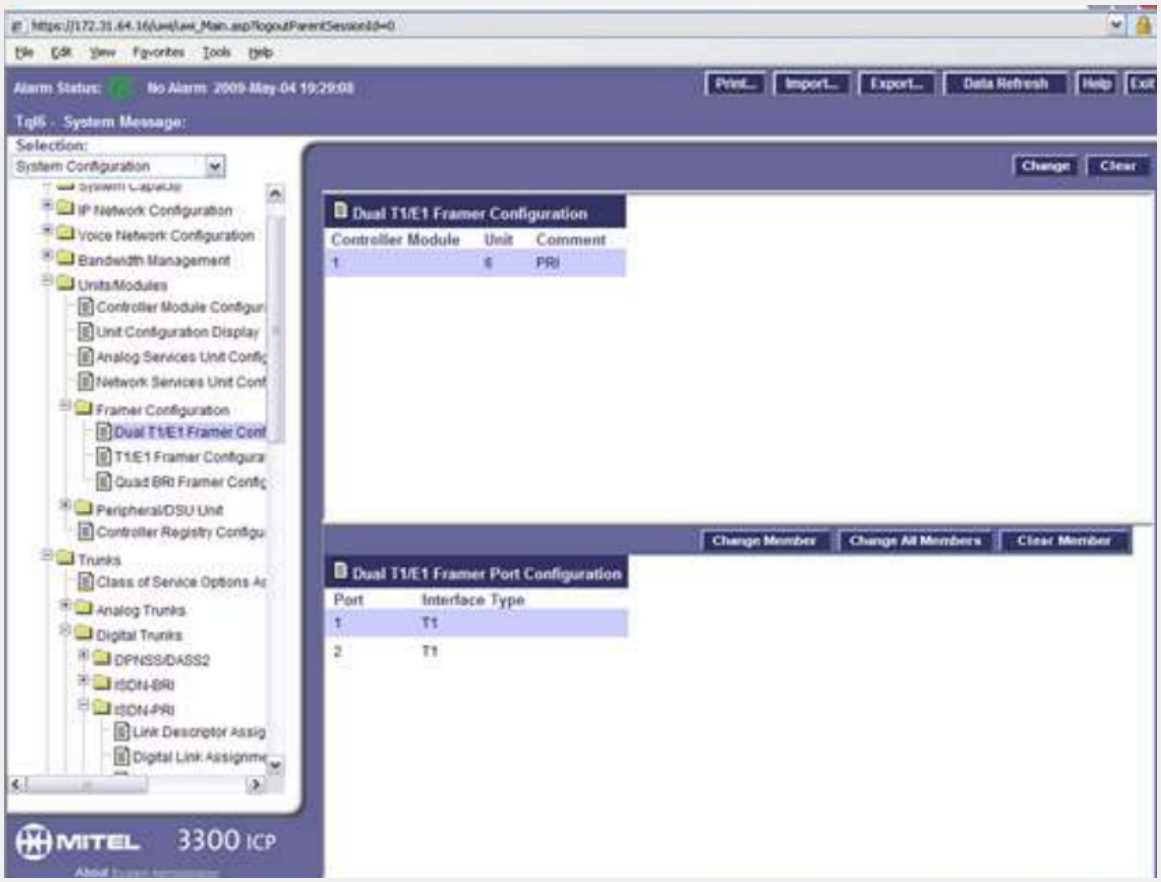
PBX Configuration

Use the following configurations to interconnect the Mitel to the SBC1k/2k.

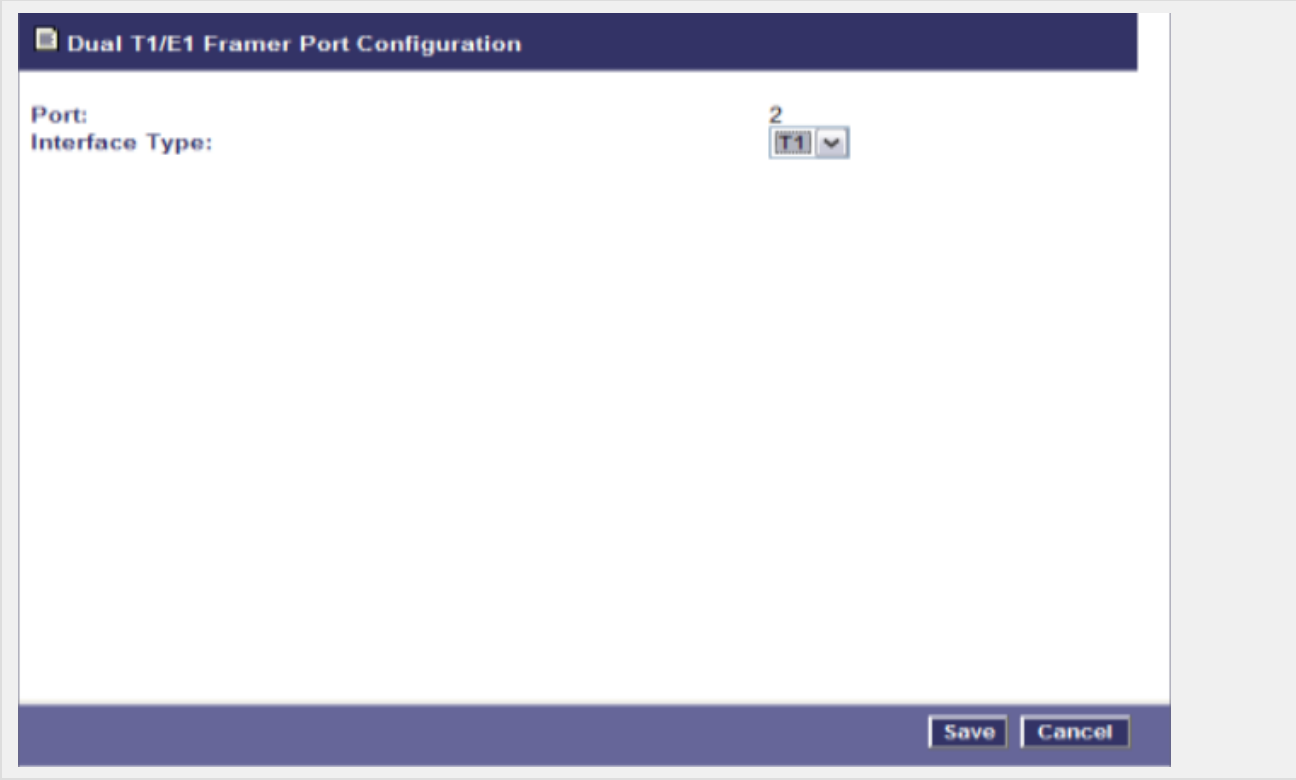
1. Ensure that your Mitel 3300 ICP PBX has the necessary T1 PRI Module to Support T1 QSIG by navigating to: System Configuration / Units/Modules / Units Configuration Display.

Copyright © 2015 Sonus Networks. All rights reserved.



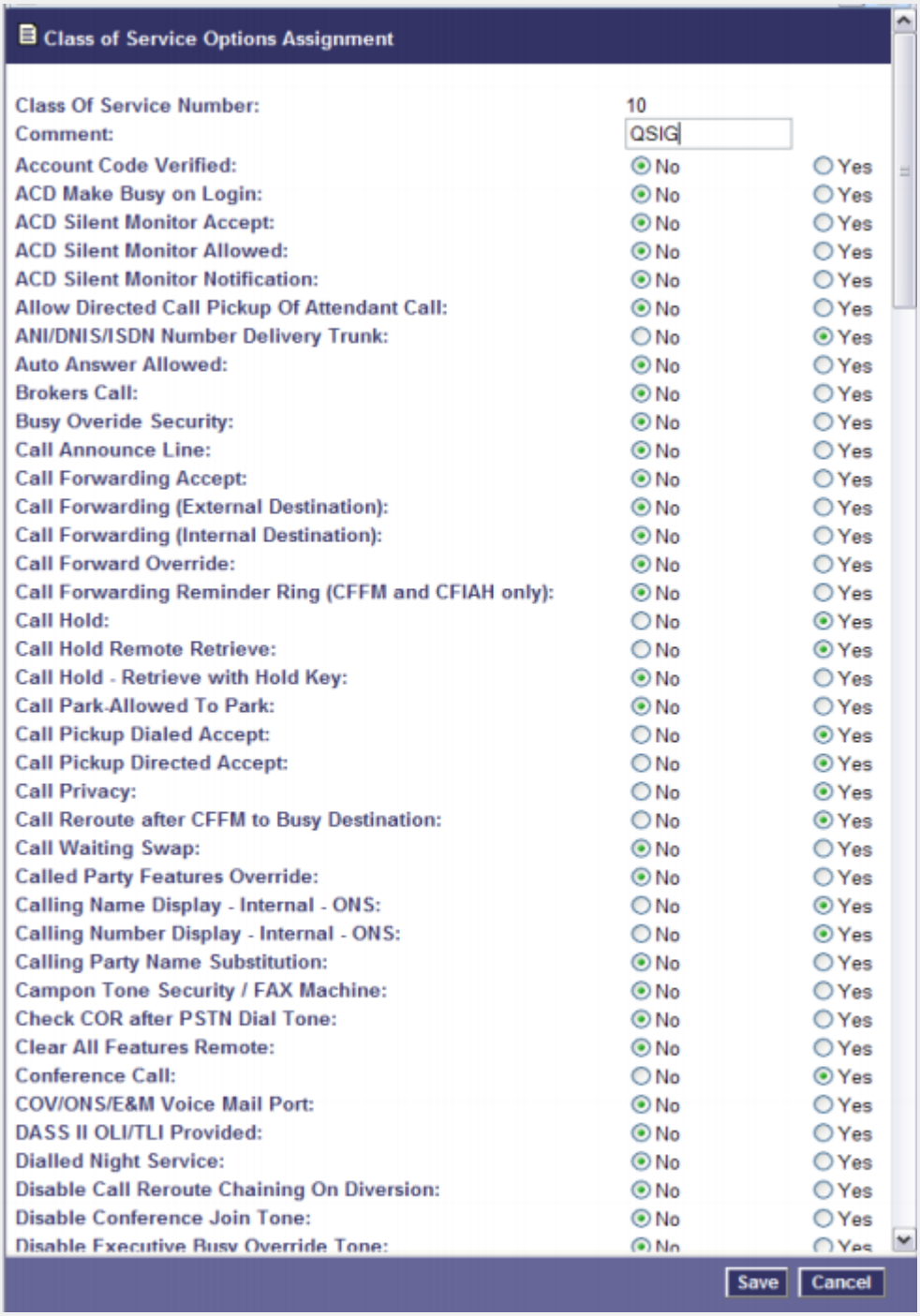


Copyright © 2015 Sonus Networks. All rights reserved.



2. Create Class of Service for your QSIG trunk by using the following path to create a Class of Service for the QSIG trunk: System Configuration / Trunks / Class of Service Options Assignment.

Copyright © 2015 Sonus Networks. All rights reserved.



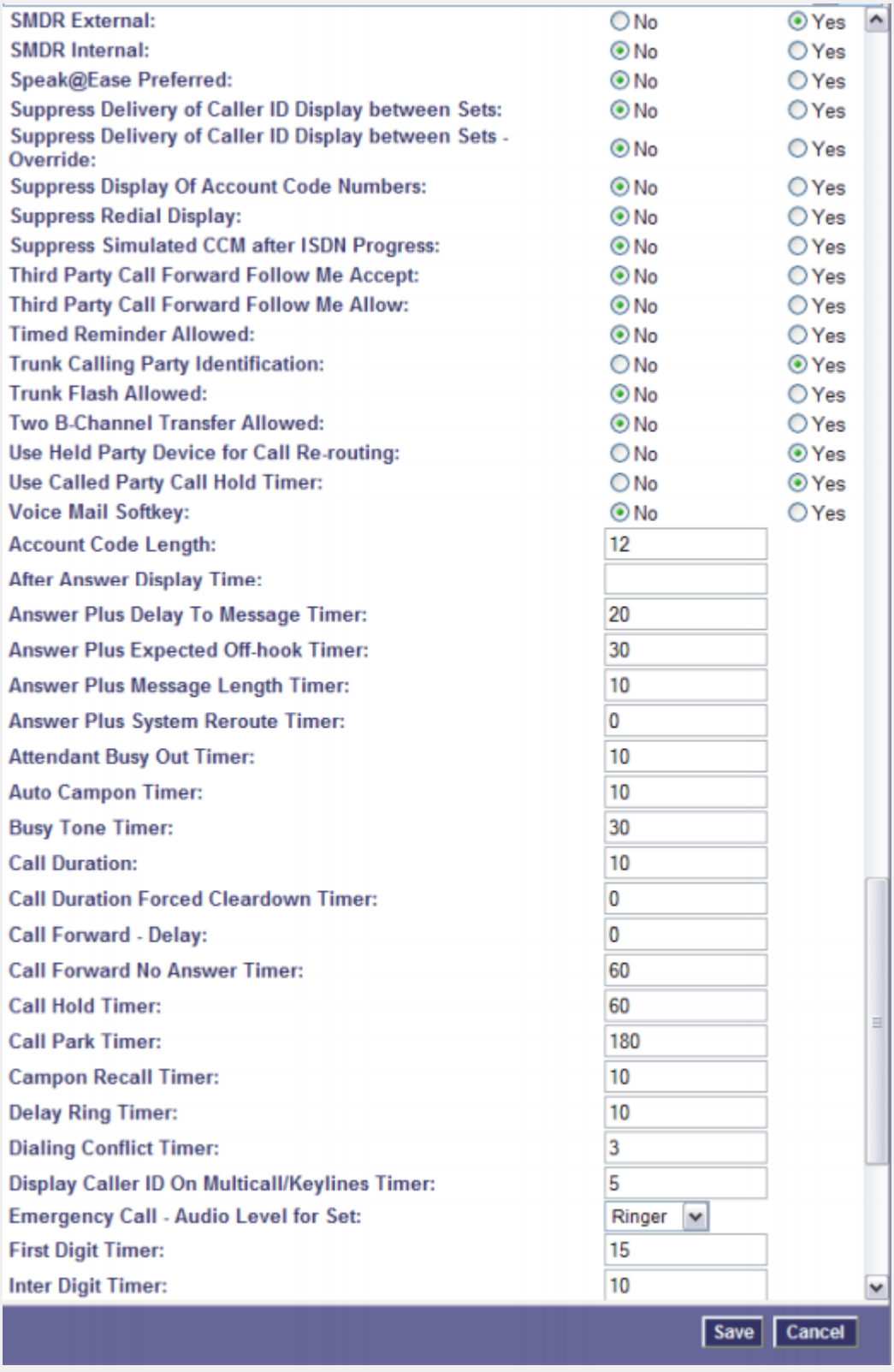
Copyright © 2015 Sonus Networks. All rights reserved.



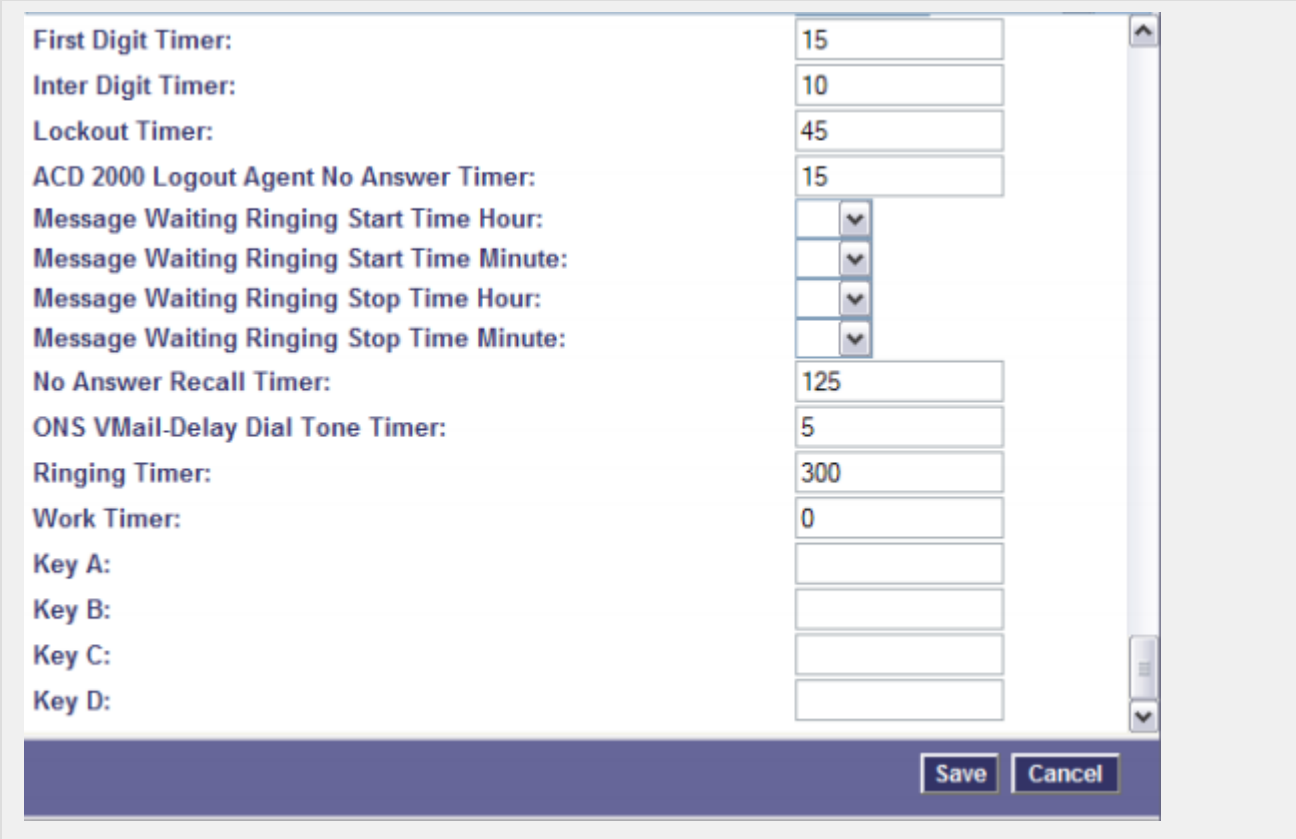
Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.

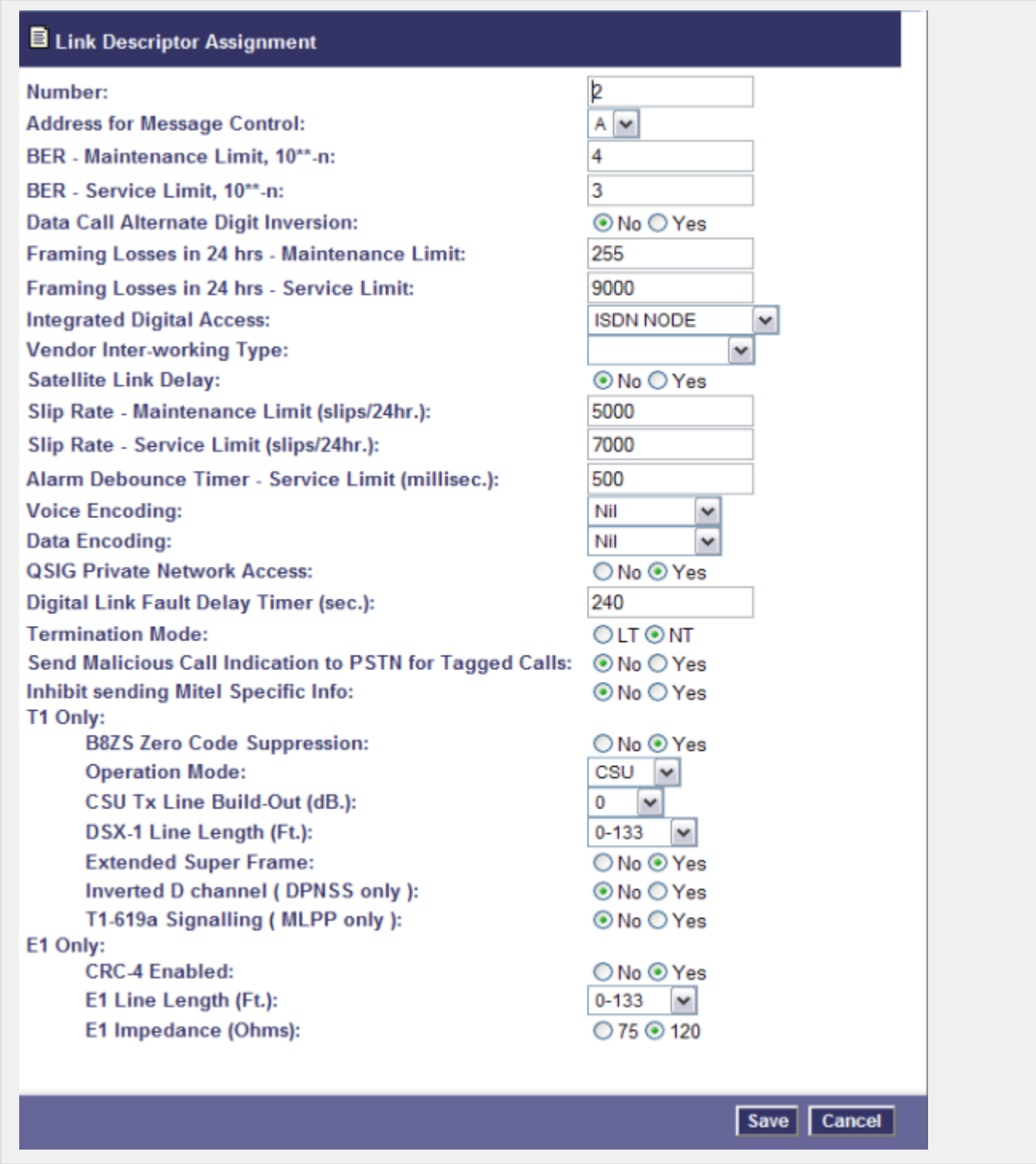


Copyright © 2015 Sonus Networks. All rights reserved.



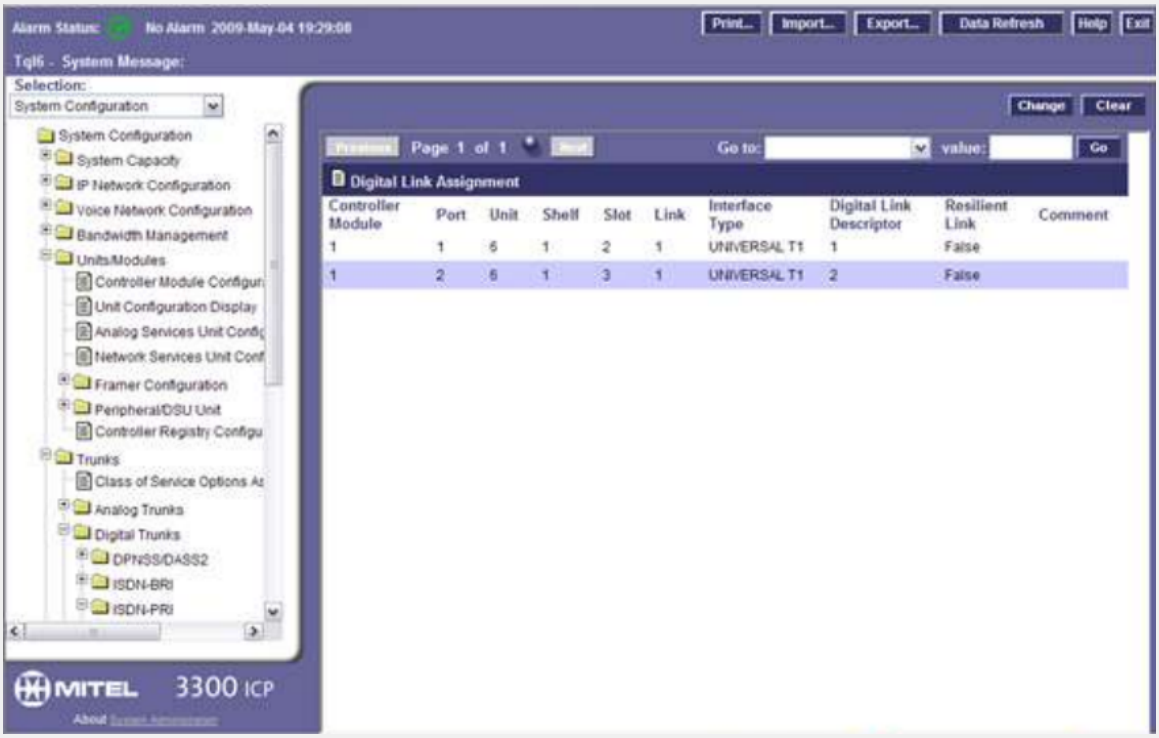
3. Create a Link Descriptor Assignment by using the following path: System Configuration / Trunks / Digital Trunks / ISDN-PRI / Link Descriptor Assignment.

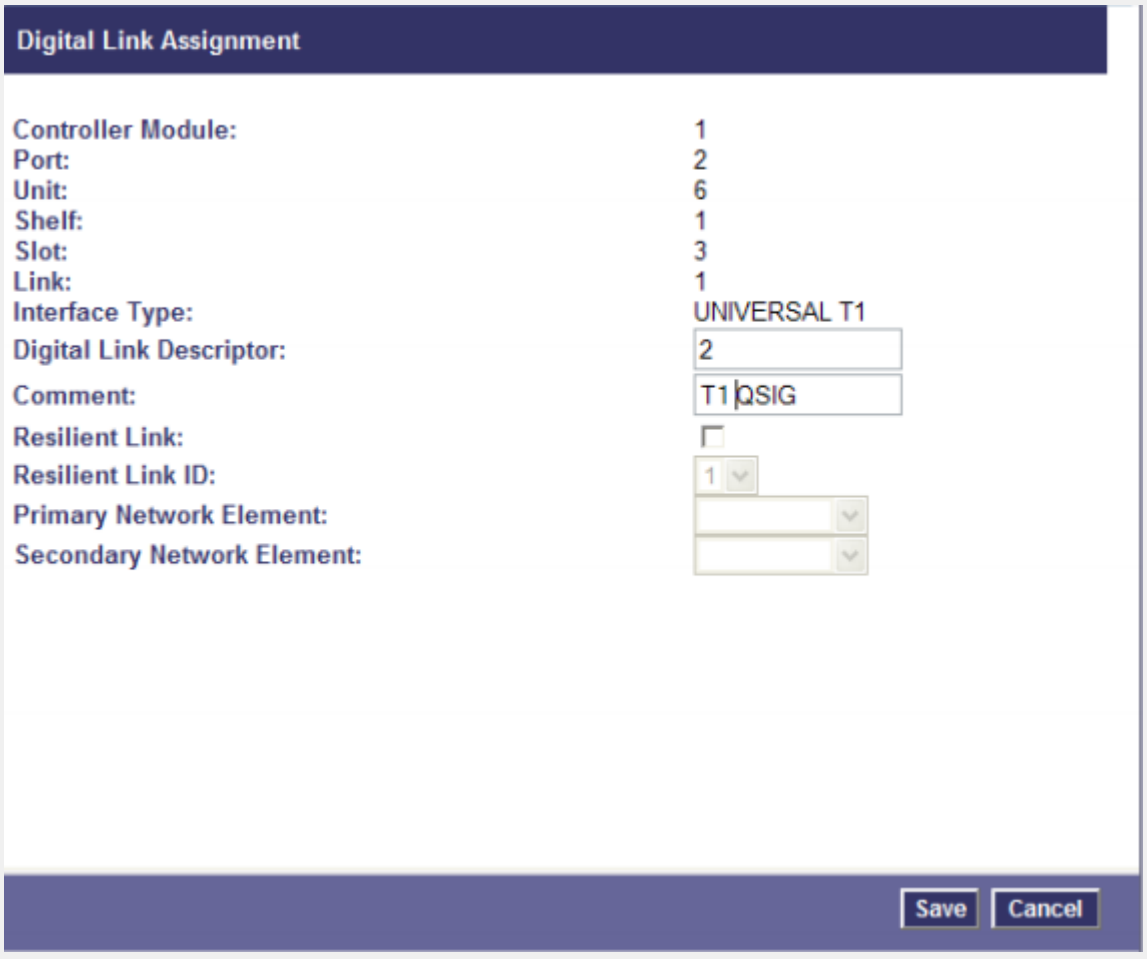
Copyright © 2015 Sonus Networks. All rights reserved.



4. Create a Digital Link Assignment by using the following path: System Configuration / Trunks / Digital Trunks / ISDN-PRI / Digital Link Assignment.

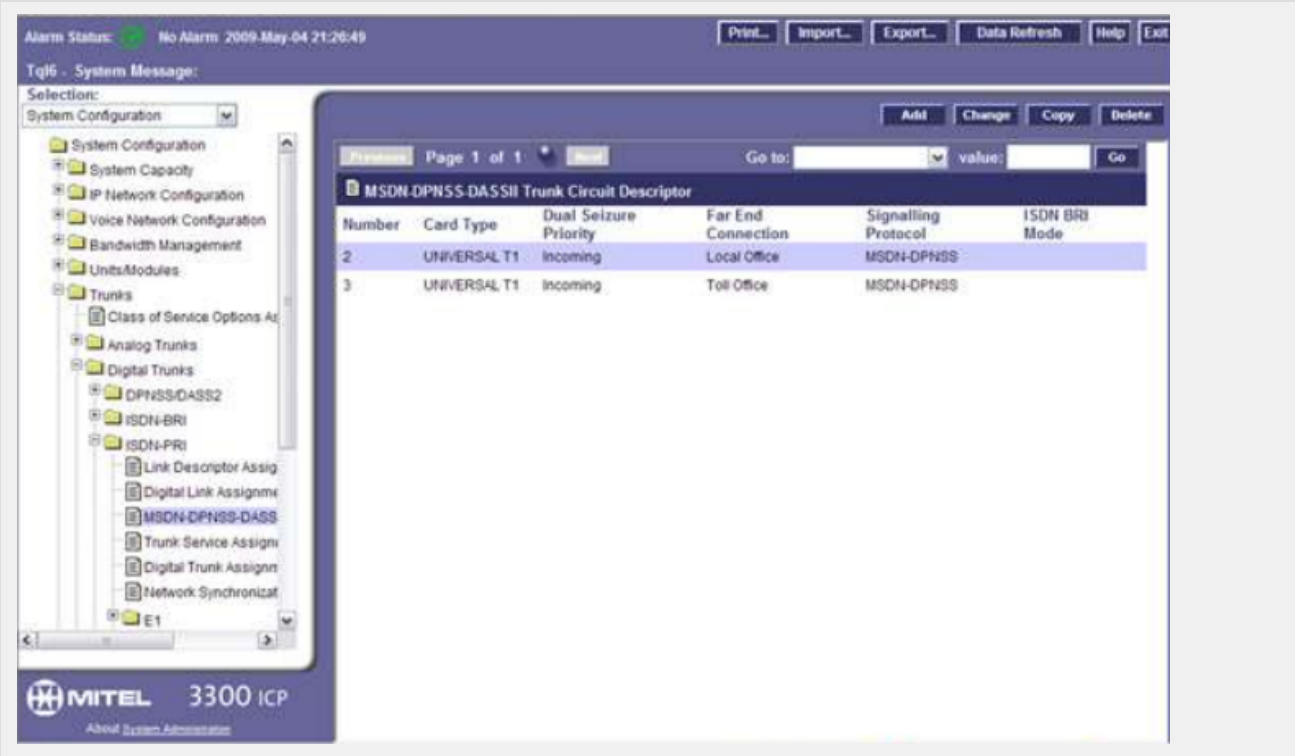
Copyright © 2015 Sonus Networks. All rights reserved.



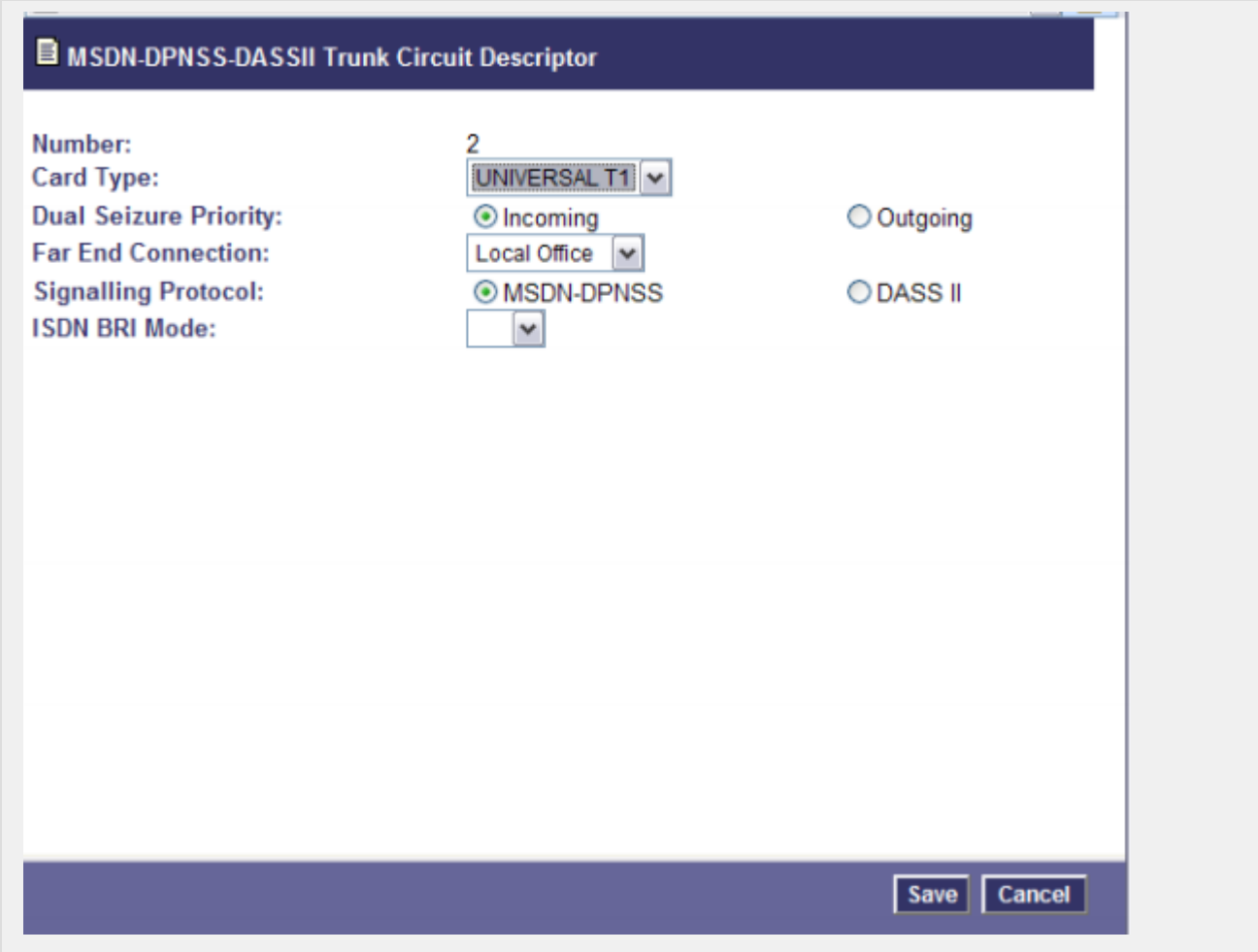


Copyright © 2015 Sonus Networks. All rights reserved.

5. Add a MSDN-DPNSS-DASSII Trunk Circuit Descriptor by using the following path: System Configuration / Trunks / Digital Trunks / ISDN-PRI/MSDN-DPNSS-DASSII Trunk Circuit Descriptor.

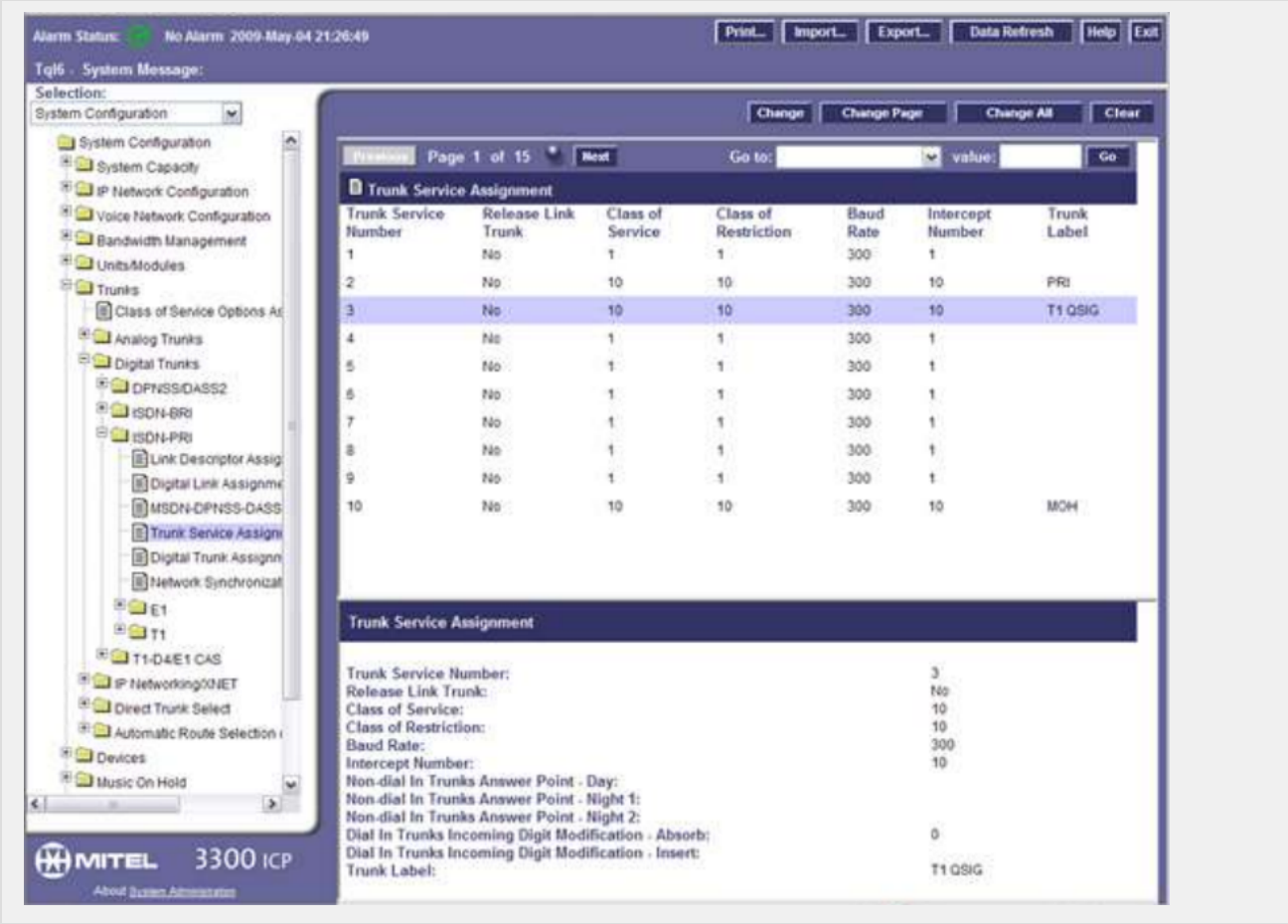


Copyright © 2015 Sonus Networks. All rights reserved.



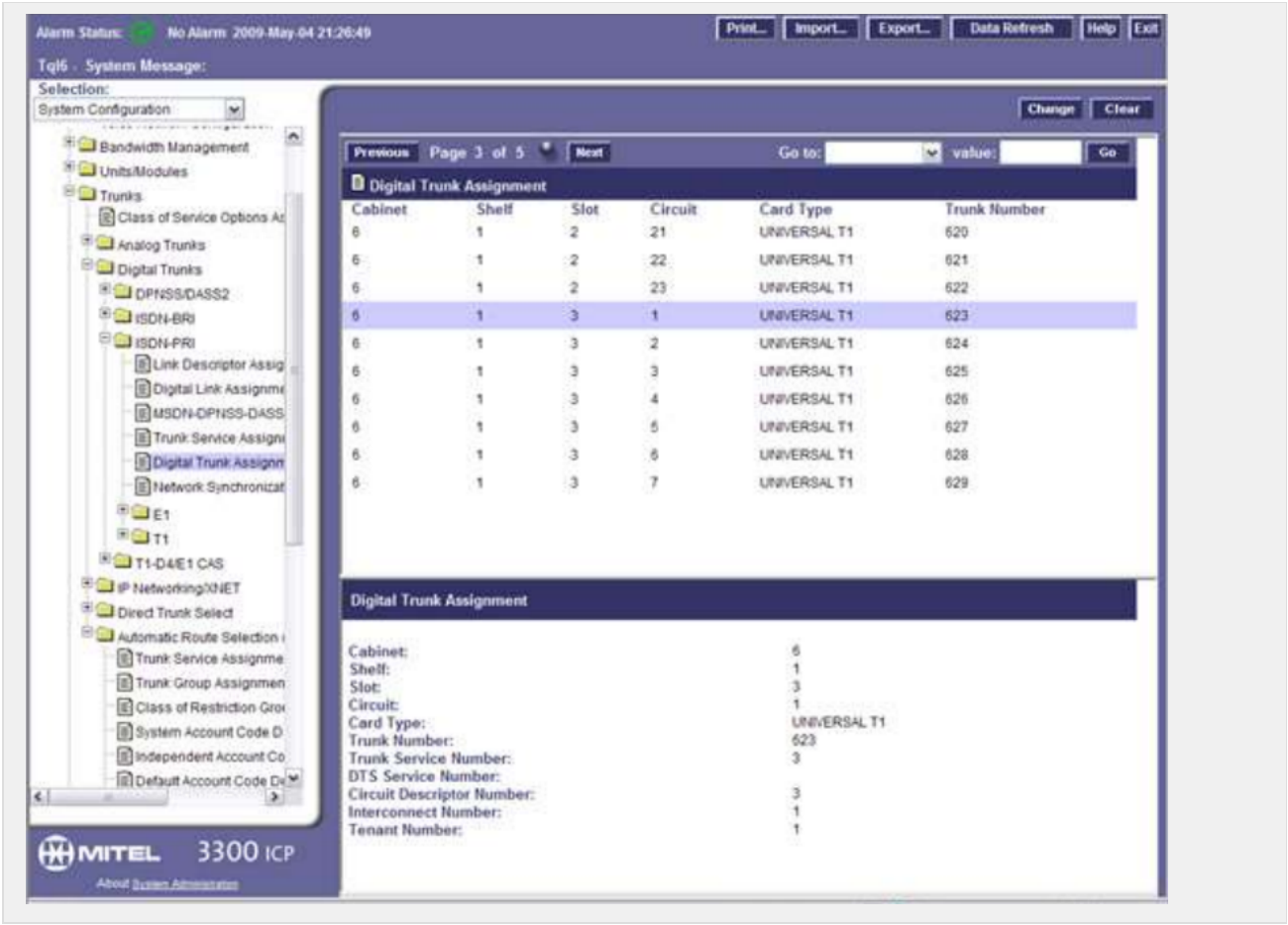
6. Create a Trunk Service Assignment by using the following path to create a Trunk Service Assignment: System Configuration / Trunks / Digital Trunks / ISDN-PRI / Trunk Service Assignment.

Copyright © 2015 Sonus Networks. All rights reserved.

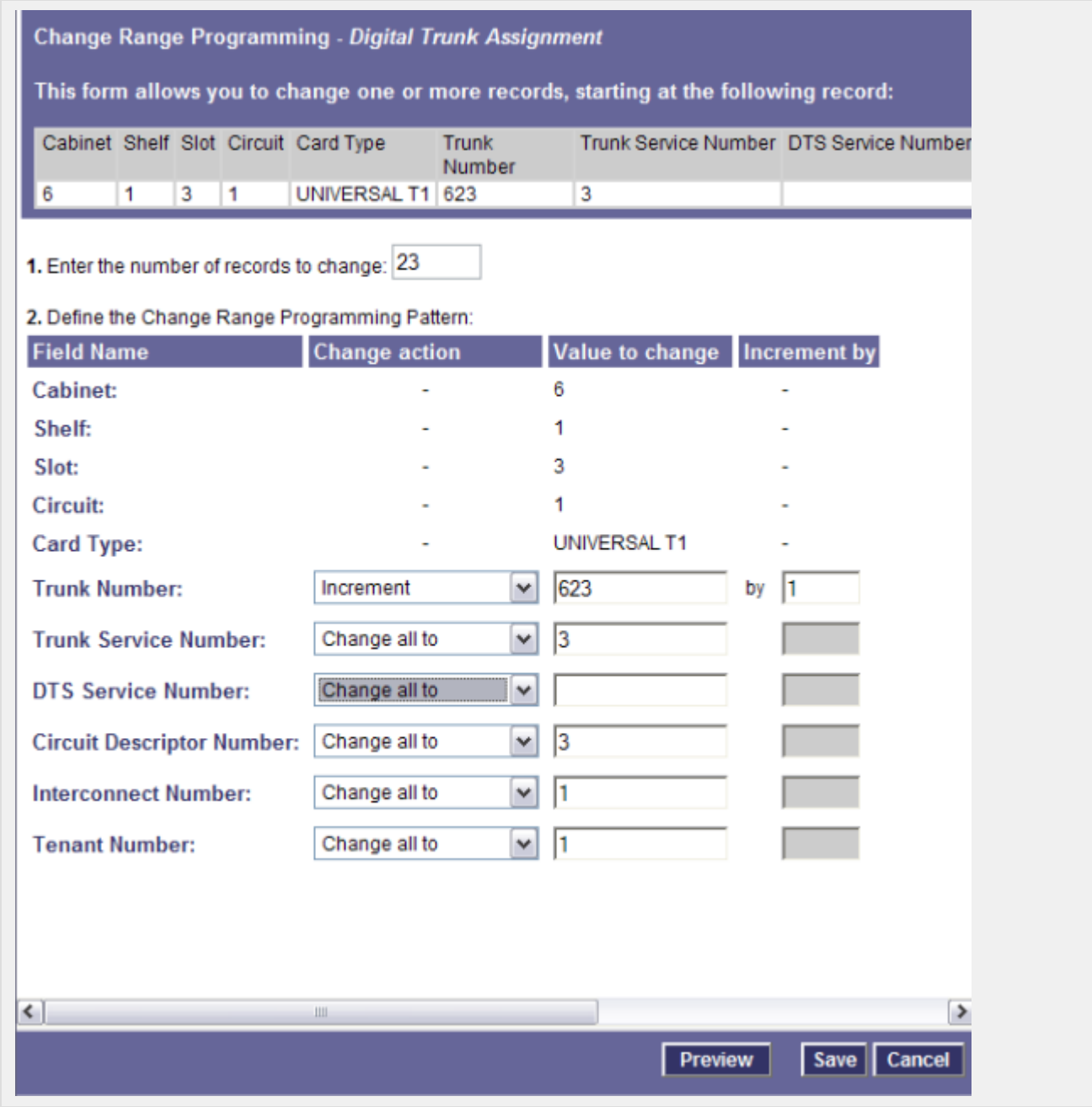


7. Assign Digital Trunks by using the following path to assign Digital Trunks: System Configuration / Trunks / Digital Trunks / ISDN-PRI / Digital Trunk Assignment.

Copyright © 2015 Sonus Networks. All rights reserved.

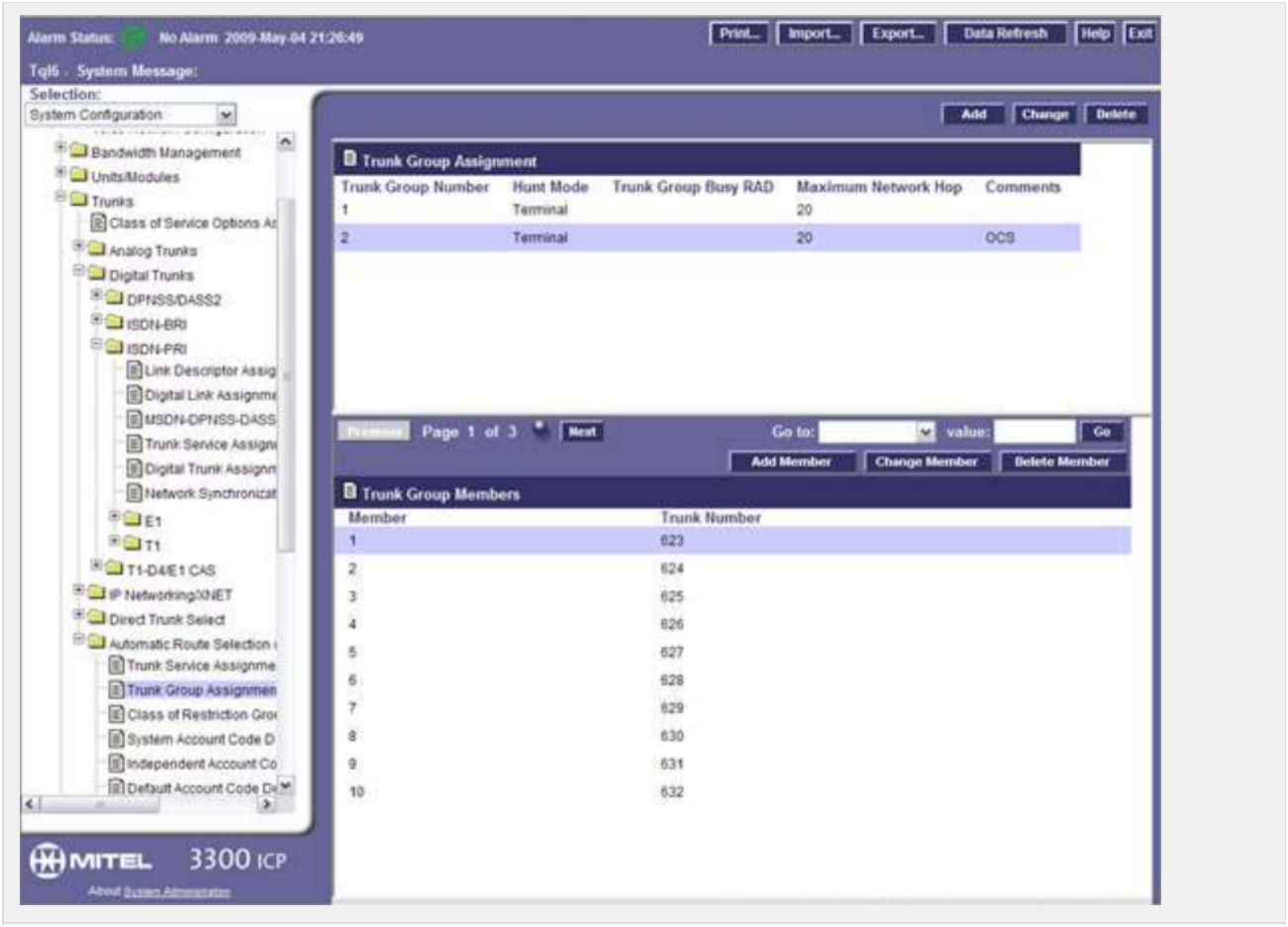


Copyright © 2015 Sonus Networks. All rights reserved.

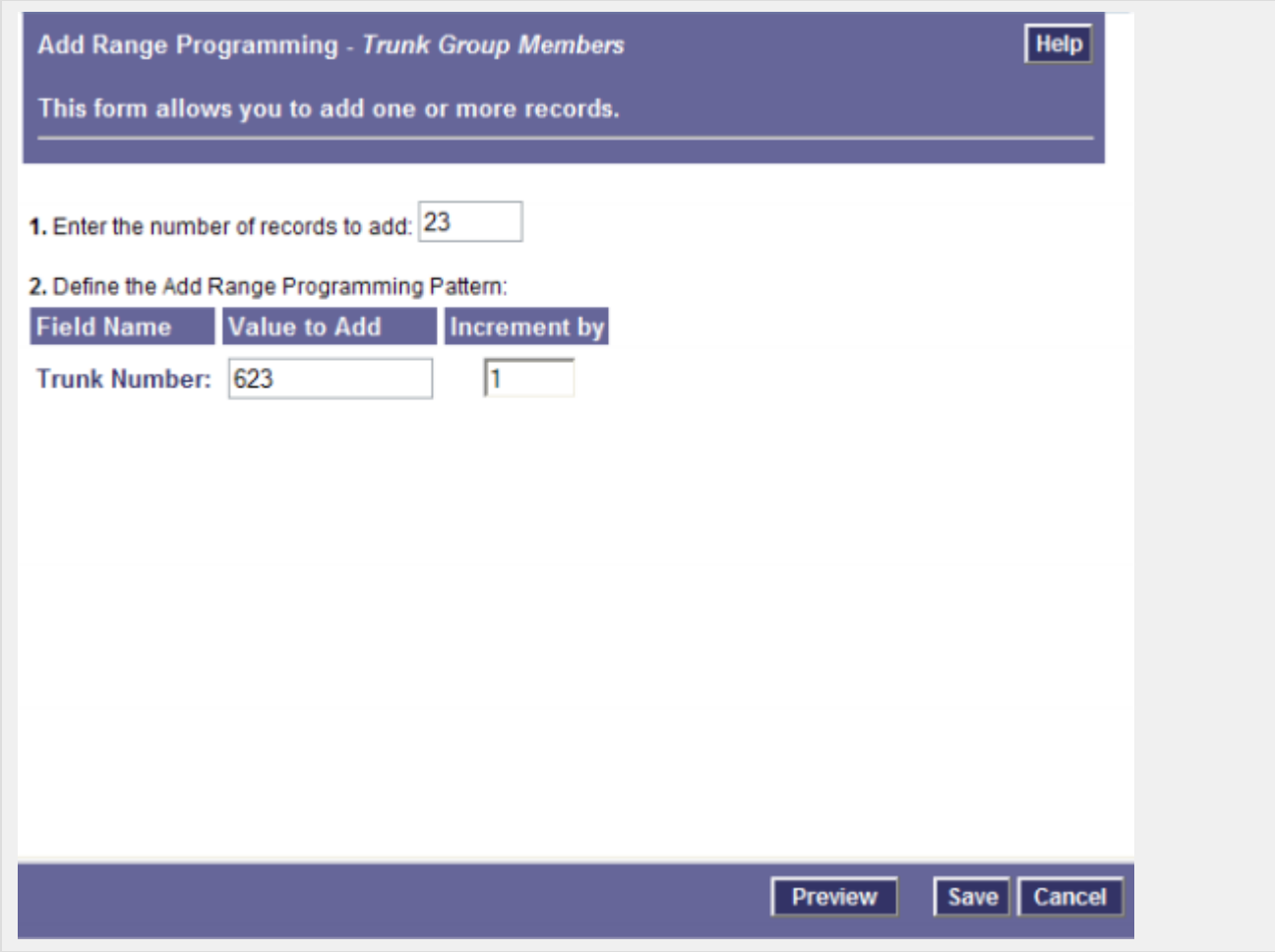


8. Add a Trunk Group for QSIG Using the following path: System Administration / Automatic Route Selection / Trunk Group Assignment. Next, create a new trunk group for QSIG and add trunk group members.

Copyright © 2015 Sonus Networks. All rights reserved.

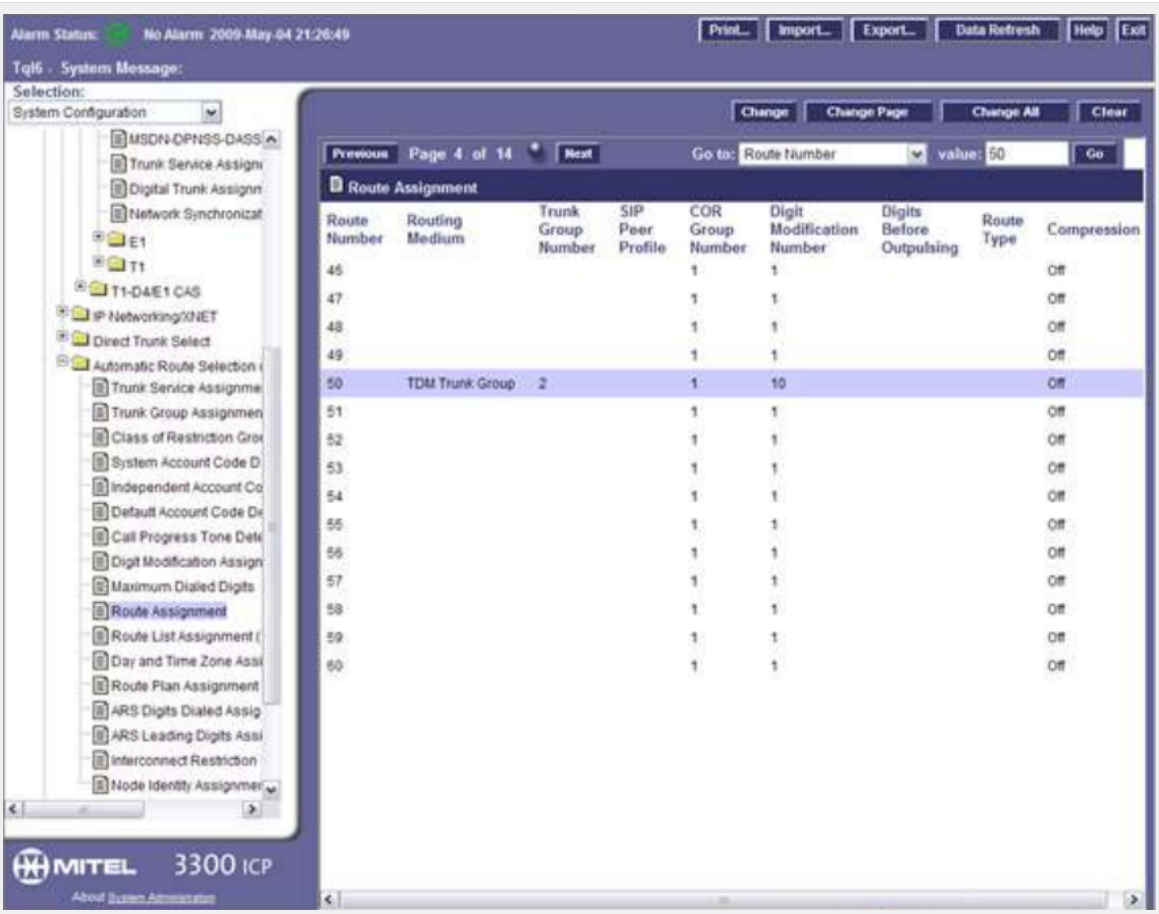


Copyright © 2015 Sonus Networks. All rights reserved.

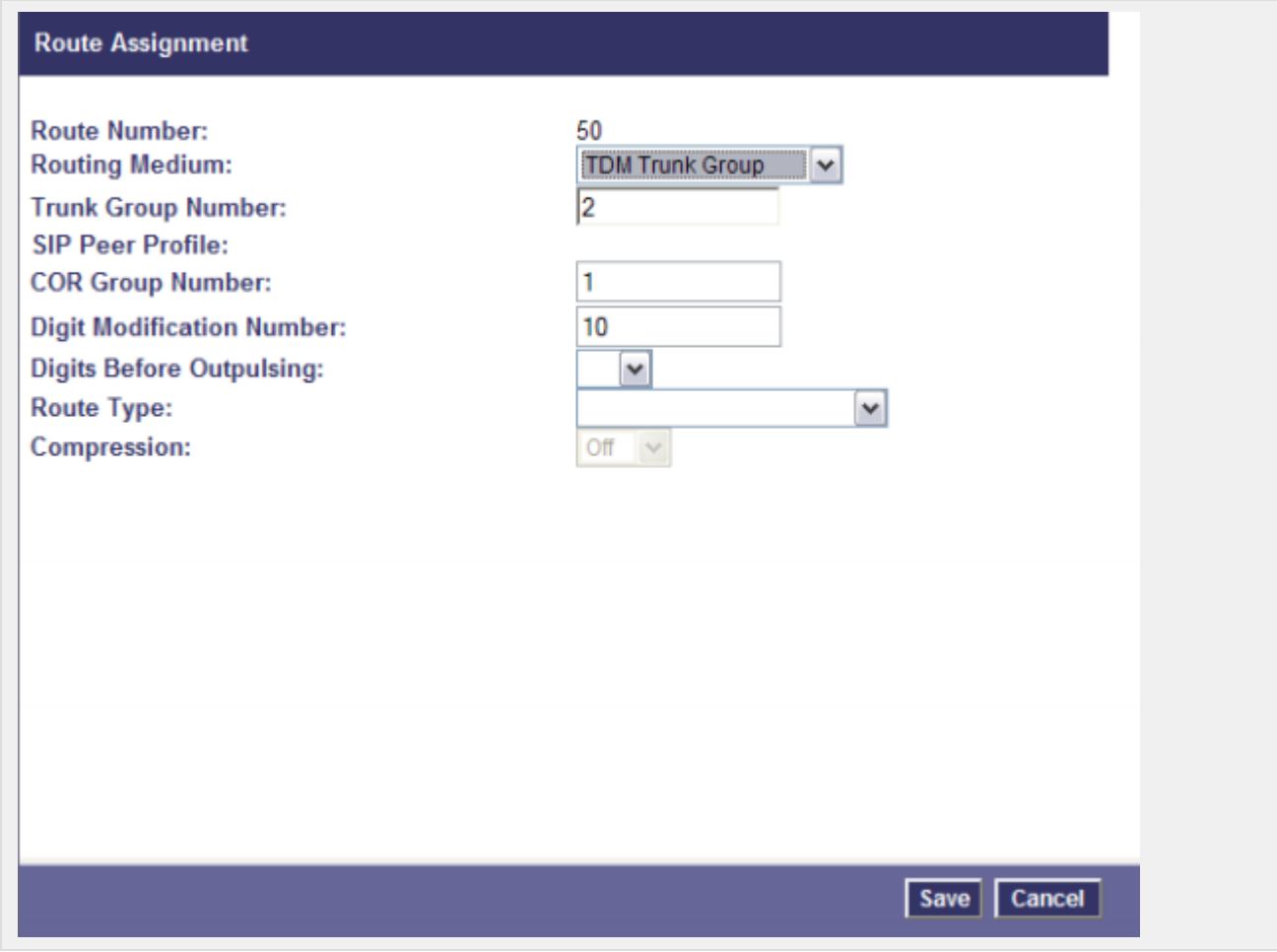


9. Add a Route Assignment by using the following path: System Administration / Automatic Route Selection / Route Assignment.

Copyright © 2015 Sonus Networks. All rights reserved.

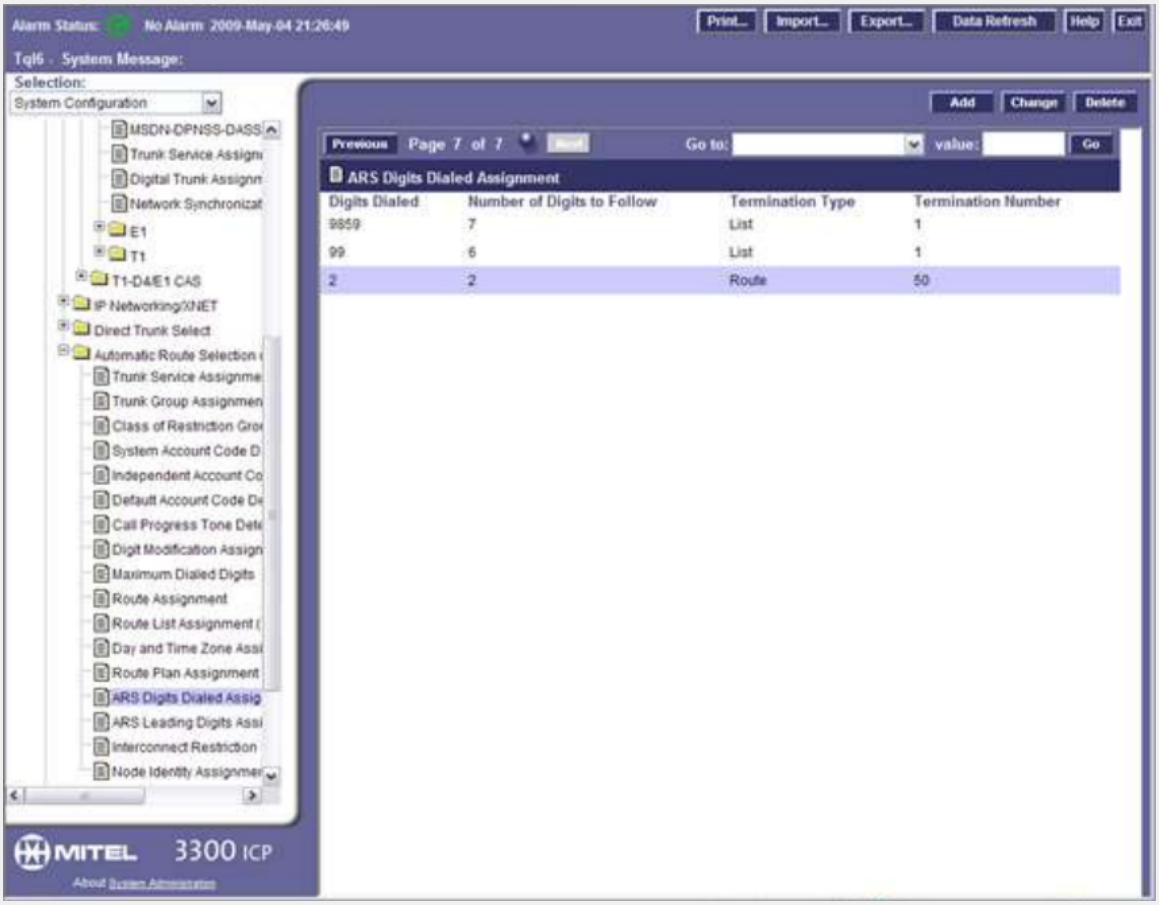


Copyright © 2015 Sonus Networks. All rights reserved.

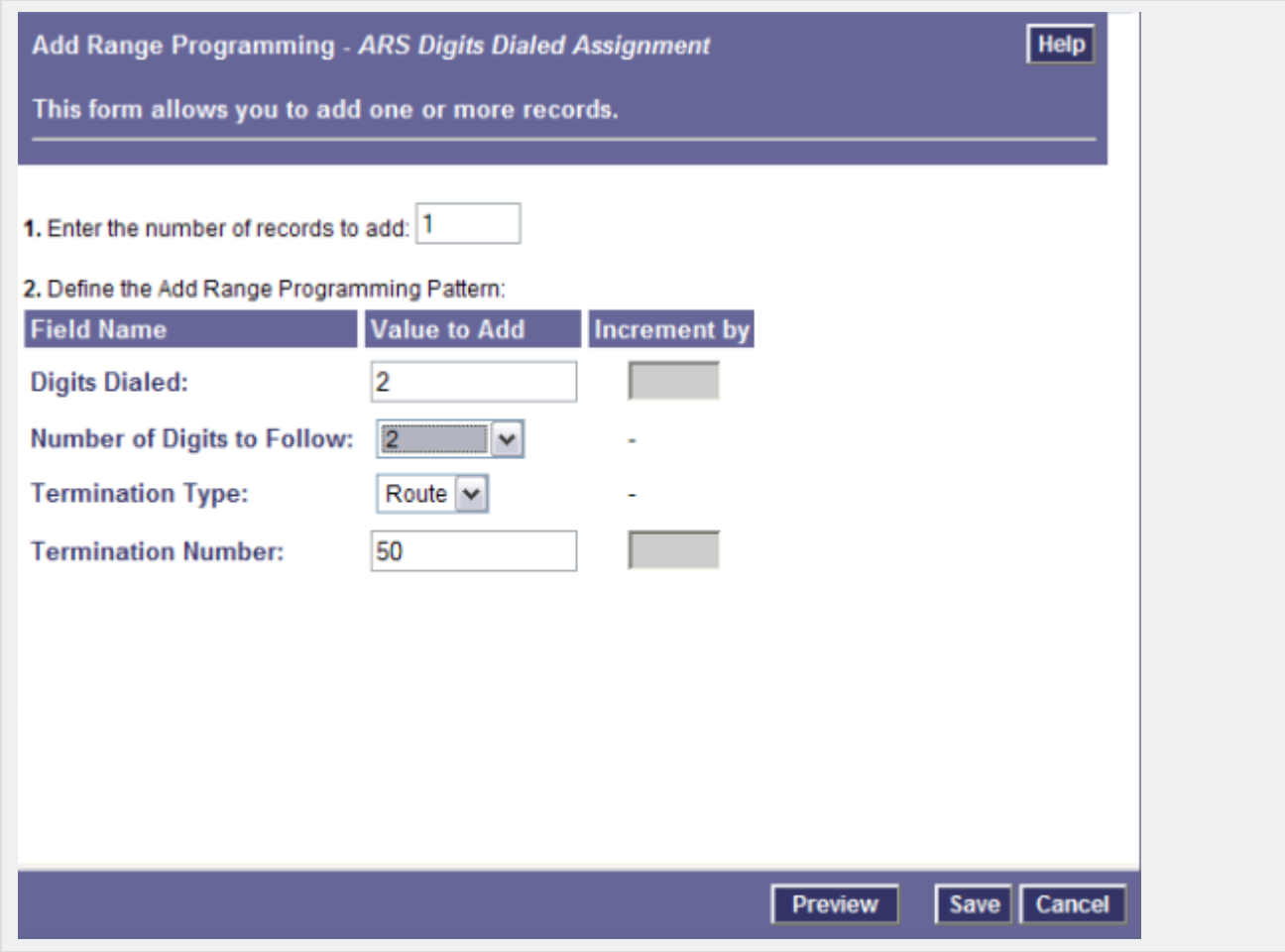


10. Add a ARS Digits Dialed Assignment by using the following path to add ARS Digits Dialed Assignment: System Administration / Automatic Route Selection / ARS Digits Dialed Assignment.

Copyright © 2015 Sonus Networks. All rights reserved.



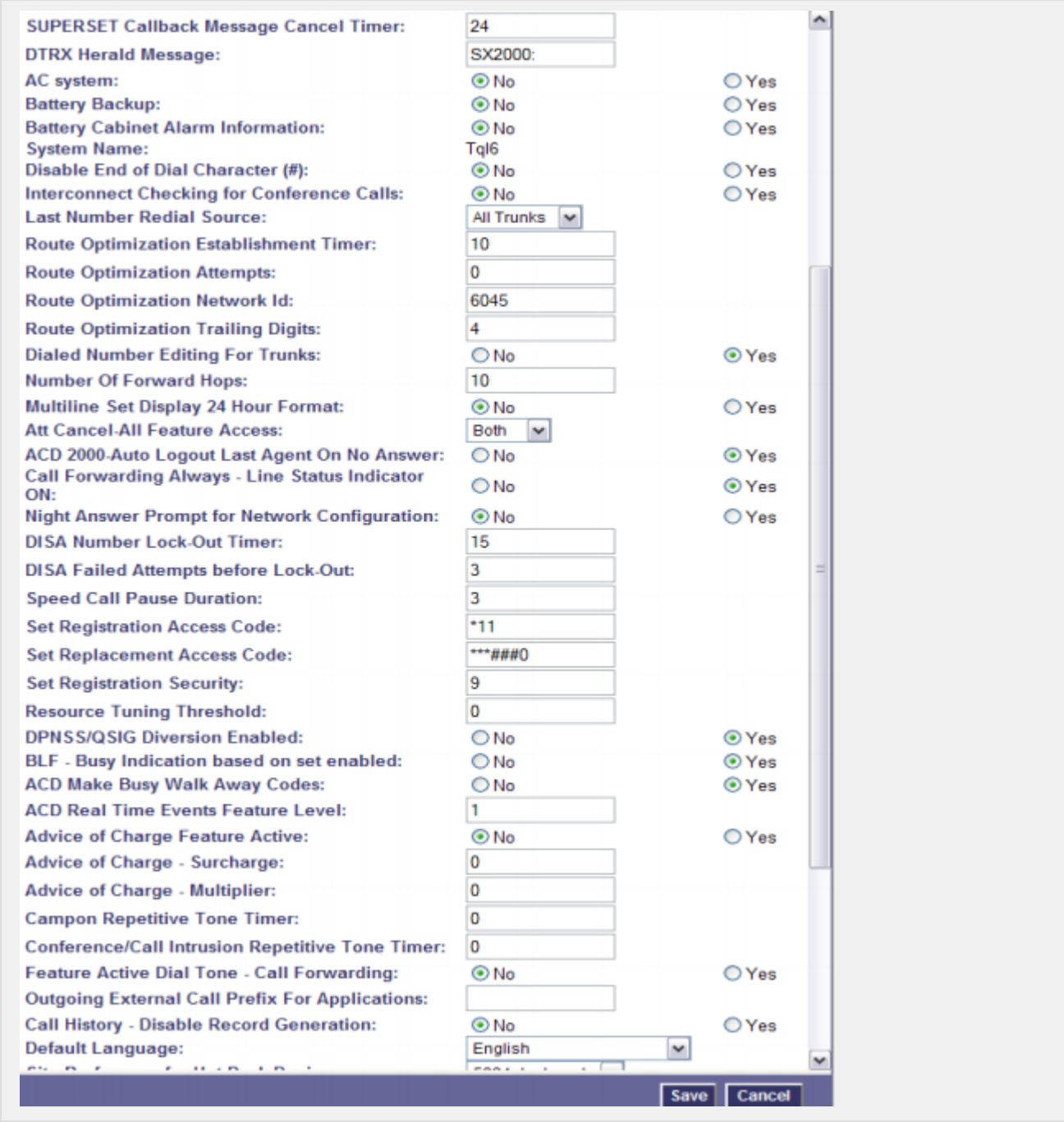
Copyright © 2015 Sonus Networks. All rights reserved.



11. Under System Option Assignment, set the following fields as follows:

    1) Route Optimization Network ID: Select a unique number.
    2) DPNSS/QSIG Diversion Enabled: Select 'Yes'.

Copyright © 2015 Sonus Networks. All rights reserved.



12. Use the TDM document to configure the SBC 1k/2k.

    - Configuring TDM ports on the SBC 1000/2000

13. Use the EUM integration document to finished the voicemail integration.

    - Configuring SBC 1000/2000 with Exchange 2013

Copyright © 2015 Sonus Networks. All rights reserved.

Configuring the QoE Feature

Table of Contents

- Overview
- Prerequisites
- Step 1: Update your SQL database rights
- Step 2: Update the QoE Agent Server ASM AD Rights
  - Adding the ASM QoE Agent Server Machine Account to the RTCComponentUniversalServices Group
  - Adding the ASM QoE Agent ServerMachine Account to the RTCUniversalReadOnlyAdmins Group
- Step 3: Configure the QoE Agent Server Gateway
- Step 4: Configure the QoE Agent Client Gateway

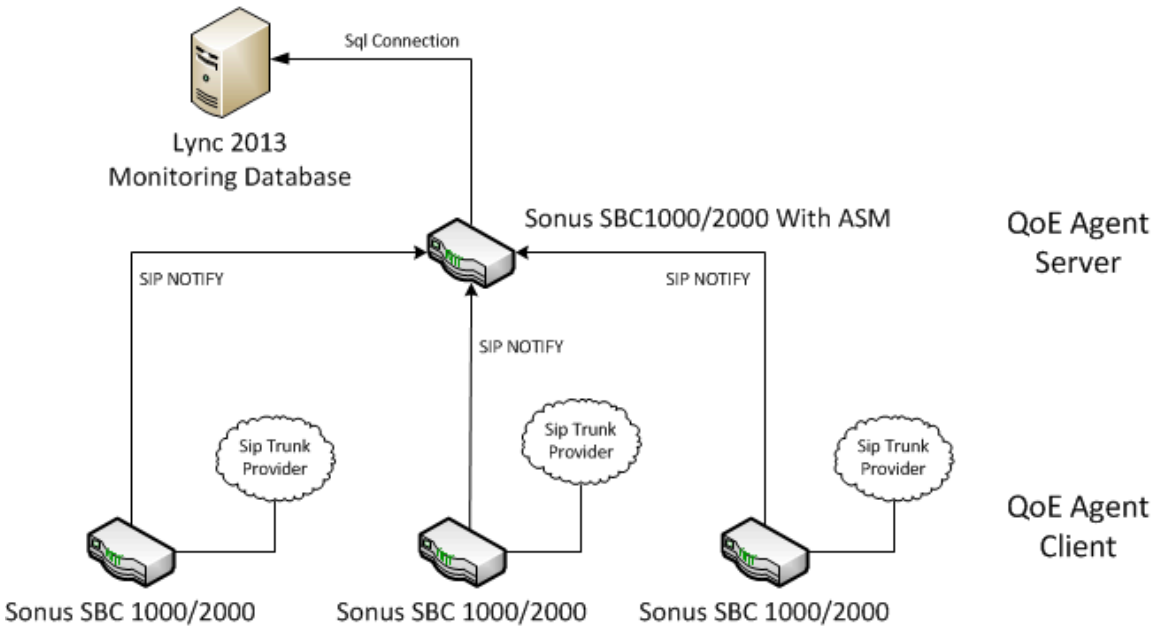
Troubleshooting
- QoE Report Verification on the QoE Agent Client Gateway
- QoE Report Verification on the QoE Agent Server Gateway

Additional Resources

- Microsoft Lync Server 2013: http://technet.microsoft.com/en-us/library/gg398616.aspx
- Deploy Monitoring: http://technet.microsoft.com/en-us/library/gg398199.aspx
- Using Monitoring Reports: http://technet.microsoft.com/en-us/library/gg558662.aspx
- Promote your customized QoE Reports: http://windowspbx.blogspot.fr/2013/09/lync-community-reports-repository-free.html

Overview

Copyright © 2015 Sonus Networks. All rights reserved.



The Quality of Experience (QoE) feature enables statistics reporting to a QoE Server in order to provide quality monitoring. The information collected helps administrators better understand the media quality that users experience. With QoE monitoring, the administrators can:-

- Gather statistics on media quality at individual locations or based on a grouping of subnets.
- Proactively monitor and troubleshoot media quality of experience issues.
- Perform diagnostics in response to VoIP user complaints.
- View trends that can help them with post-deployment growth and measure results against the service level agreement.

By introducing this feature to the SBC1000 and SBC2000, all IP legs of a call can now report QoE information. Currently, QoE statistics do not get reported on the SBC1000/2000 to SIP Carrier leg of a call. Statistics such as delay, jitter and packet loss will be reported for the SIP Trunk Leg. This will be a feature unique in the product space.

The SBC1000/2000 with ASM (QoE Agent Server Gateway) will use the SQL server to modify the data used by the Microsoft QoE Services for quality monitoring. The QoE Agent Client gateways (SBC with or without ASM) will notify the QoE Agent Server Gateway with QoE stats for each call in order to update the database of the QoE server. Exchange between QoE Agent Server Gateway and QoE Agent Client Gateway will be handle using SIP NOTIFY.

Prerequisites

- A Lync 2013 deployment with Monitoring Reports fully implemented.
- A Sonus SBC 1000 or SBC 2000 with an ASM and QoE license.
- All additional Sonus SBC 1000/2000 nodes which the system administrator wants to receive QoE reports must have QoE feature licensed.

> **ASM Info**
>
> An ASM module is only required on the SBC node functioning as the QoE Agent Server Gateway.

Step 1: Update your SQL database rights

The goal of this step is to allow an AD group to access and add information inside the Monitoring Server database.

1. 1.Log on a computer of your domain with your **MS Lync Database Administrator** account.

Copyright © 2015 Sonus Networks. All rights reserved.

2. Start Windows Powershell.
3. Update the Database SQL rights using the following commands:

```
Invoke-Sqlcmd -ServerInstance {Fqdn of your Sql Server}\{Instance of the Monitoring
Database} -Database QoEMetrics -Query "GRANT UPDATE ON Session TO ServerRole; GRANT
EXECUTE ON QoeInsertAudioStreamReport TO ServerRole; GRANT UPDATE ON Session TO
ServerRole; EXEC QoEMetrics..sp_addrolemember ReportsReadOnlyRole, '{Your
domain}\RTCComponentUniversalServices';"

Replace {Fqdn of your Sql Server} by your SQL Server FQDN
Replace {Instance of the Monitoring Database} by your Monitoring Database Instance
Replace {Your Domain} by your domain FQDN in cap

Eg:
Invoke-Sqlcmd -ServerInstance BE-SQL2.UX2013.COM\RTC2013REPORTS -Database QoEMetrics
-Query "GRANT UPDATE ON Session TO ServerRole; GRANT EXECUTE ON
QoeInsertAudioStreamReport TO ServerRole; EXEC QoEMetrics..sp_addrolemember
ReportsReadOnlyRole, 'UX2013\RTCComponentUniversalServices';"
```

If you don't know your SQL server FQDN and/or your monitoring database instance, execute the following Powershell commands on the Lync Front End Server machine

```
Get-CsService -MonitoringDatabase
```

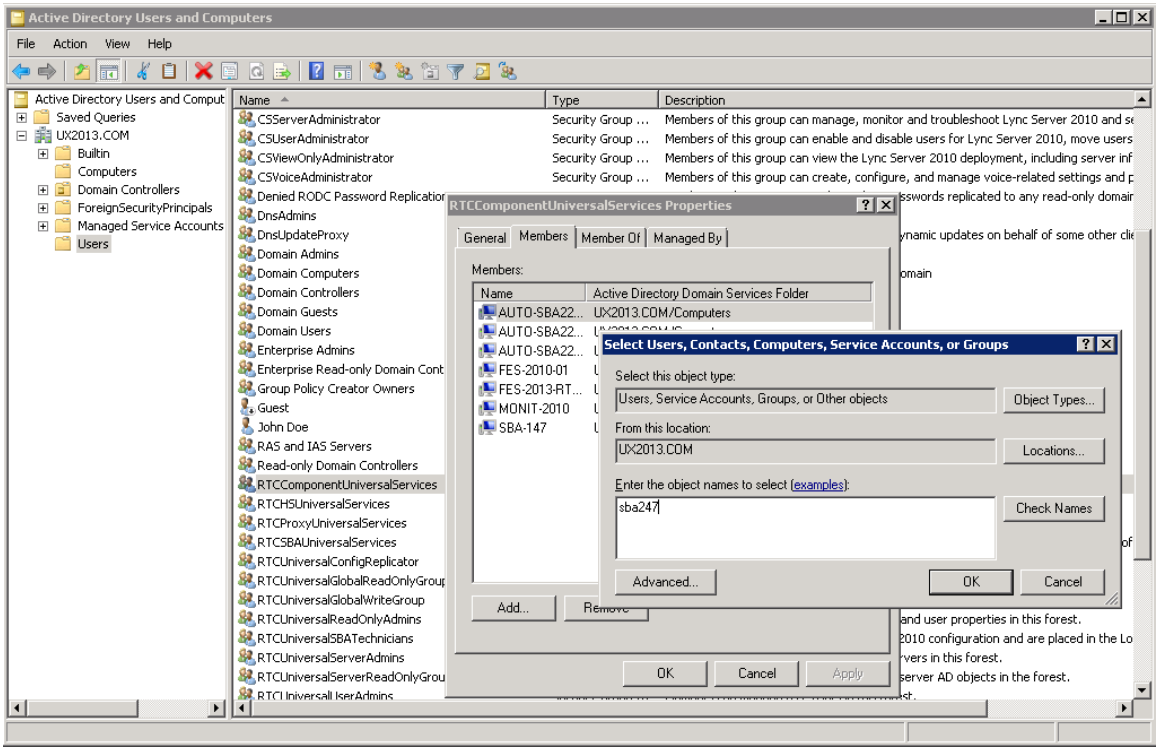
Step 2: Update the QoE Agent Server ASM AD Rights

Adding the ASM QoE Agent Server Machine Account to the RTCComponentUniversalServices Group

The goal of this step is to add the ASM into the group that we previously increase the database access.

1. Connect to the Domain Controler through Remote Desktop (RDP) using your regular AD credentials.
2. Launch the Active Directory Users and Computers snap-in.
3. Browse down to Users object (on the left pane).
4. Right-click *RTCComponentUniveralServices* group and select Properties
5. Click **ADD** in the the Members tab.
6. In the popup, enter the ASM machine name.
7. Click **Check Names**.

Copyright © 2015 Sonus Networks. All rights reserved.



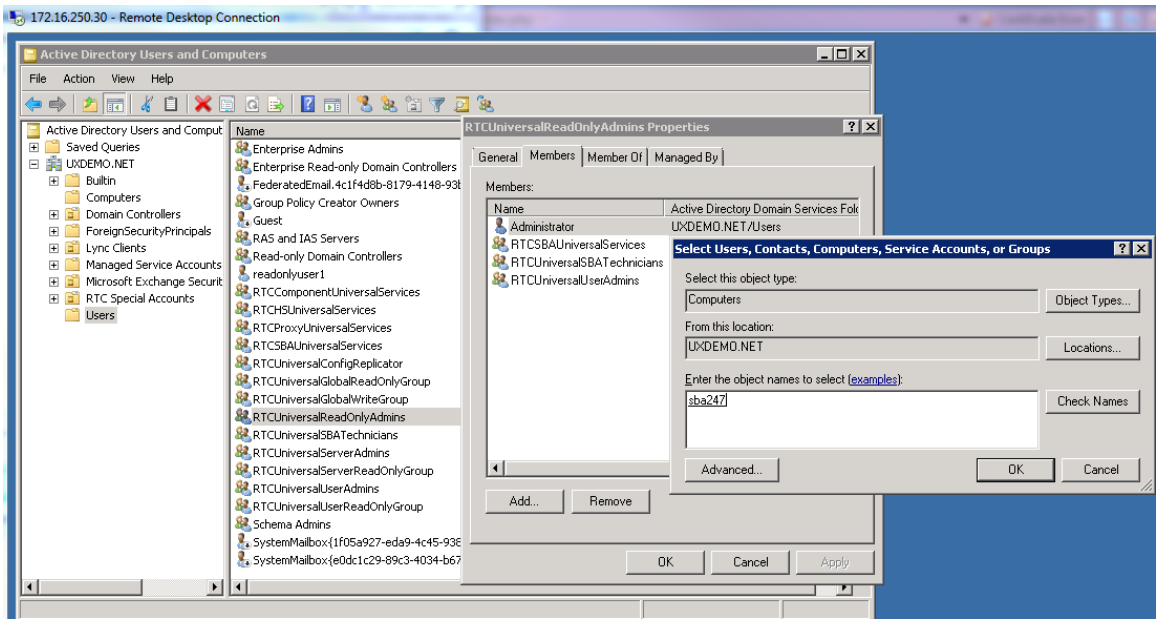
8. Click **OK**.
9. Click **OK** to close the properties screen.

Adding the ASM QoE Agent ServerMachine Account to the RTCUniversalReadOnlyAdmins Group

The goal of this step is to add the ASM into the group wich is allow to read the topology in order to locate the monitoring database.

1. Connect to the Domain Controler through Remote Desktop (RDP) using your regular AD credentials.
2. Launch the Active Directory Users and Computers snap-in.
3. Browse down to Users object (on the left pane).
4. Right-click *RTCUniversalReadOnlyAdmins* group and select Properties
5. Click **ADD** in the the Members tab.
6. In the popup, enter the ASM machine name.
7. Click **Check Names**.

Copyright © 2015 Sonus Networks. All rights reserved.



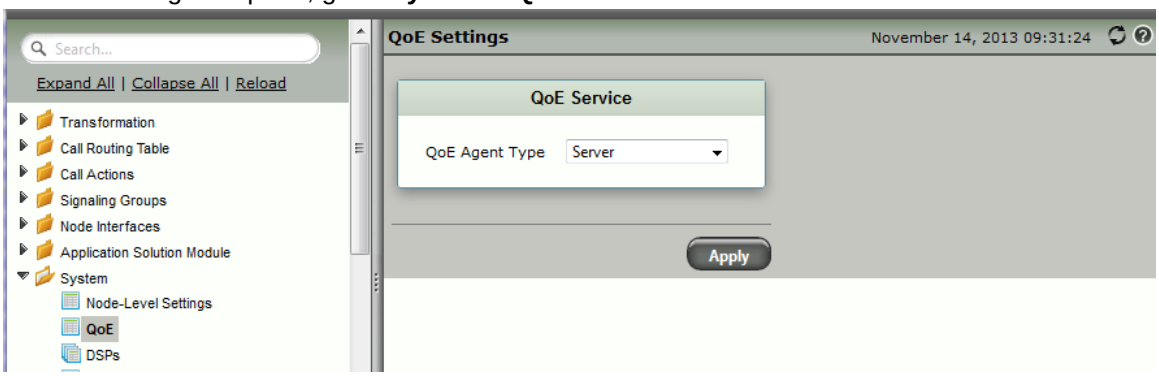
8. Click **OK**.
9. Click **OK** to close the properties screen.

Step 3: Configure the QoE Agent Server Gateway

ASM should have a Lync 2013 SBA image or a Lync 2013 RBA image loaded

1. Configure the ASM IP Settings
2. Join the ASM to a Domain
3. Perform Step 1 (Prepare the SBA) of the Deploying the SBA Best Practice article.
4. You need to accept the SIP NOTIFY traffic from the QoE Agent Client Gateway by creating or reusing a signaling group to accept SIP traffic from Client. The listening port will be the port provide in the System tab of the QoE Agent Client Gateways.
5. **To configure the QoE service as a Server:**

    a. In the WebUI, click the **Settings** tab.
    b. In the left navigation pane, go to **System > QoE**.



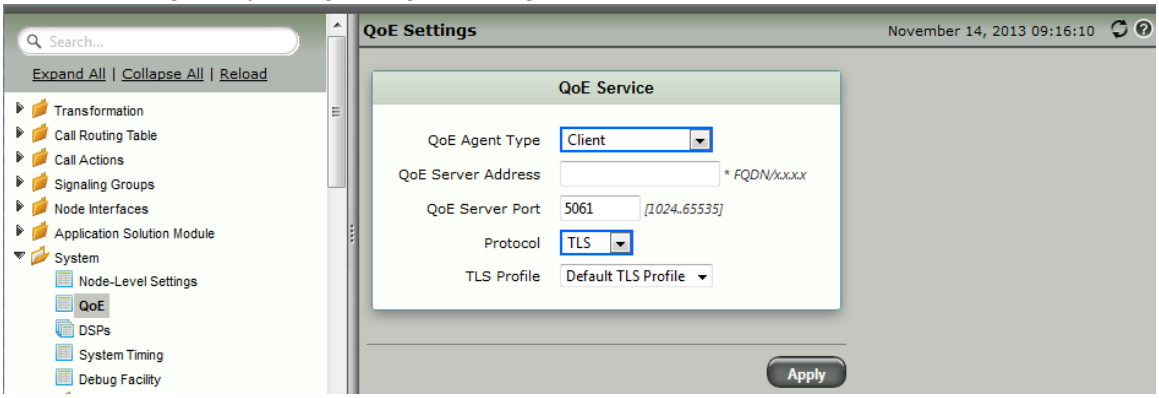
    c. In the QoE Service panel, select **Server** from the **QoE Agent Type** list box.
    d. Click **Apply**.

Step 4: Configure the QoE Agent Client Gateway

Copyright © 2015 Sonus Networks. All rights reserved.

To configure the QoE service as a client:

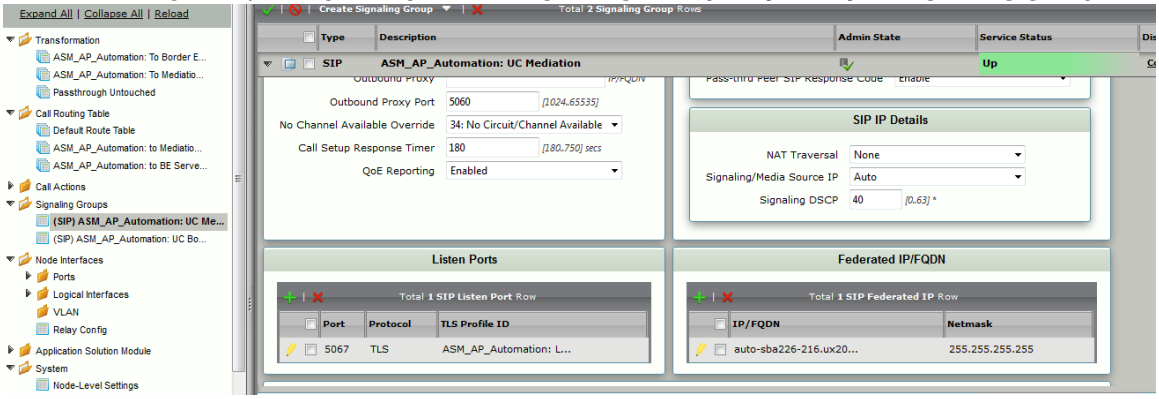
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > QoE**.



3. In the QoE Service panel:
   a. Select **Client** in the **QoE Agent Type** list box.
   b. Enter the FQDN or IP address of the QoE Agent Server gateway in the **QoE Server Address** text field.
   c. Enter the port number for the Sip Signaling Group in the **QoE Agent Server Gateway Port** text field.
   d. Select the transport protocol from the **Protocol** list box. If the transport protocol selected is TLS, make sure the QoE Server Address is FQDN (certificate common name is FQDN).
4. Click **Apply**.

To enable QoE reporting in the Lync SIP Signaling Group:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Signaling Groups > *your Lync signaling group*.**



3. In the SIP Channels and Routing Panel, select **Enabled** from the **QoE Reporting** list box.
4. Click **Apply**.

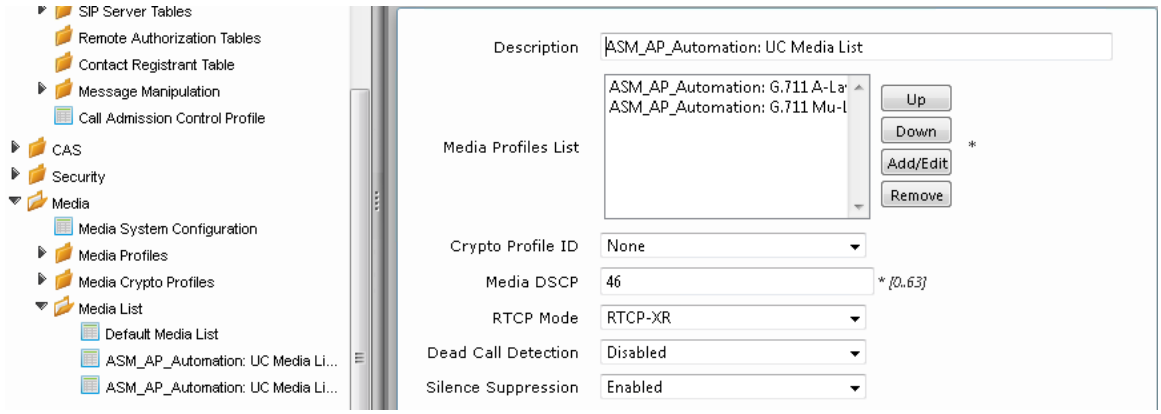
> This SIP Signaling Group is used to send QoE Information to the server. You can track the statistic by looking at the counter.

To enable RTCP-XR:

RTCP-XR must be enabled in each Media List through which the system administrator wants to receive QoE reports from the SBC 1000/2000.

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Media > *Media List > your SIP Trunk Media List***

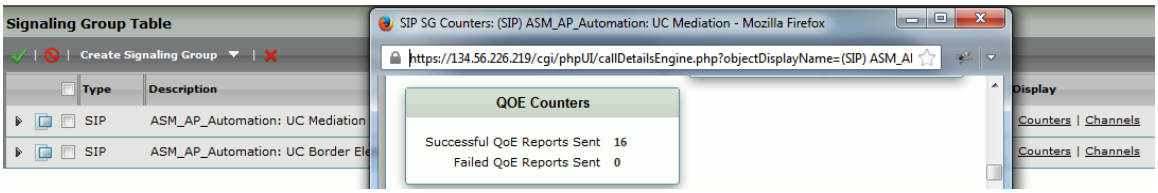


3. Select **RTCP-XR** in the **RTCP Mode** list box
4. Click **Apply**.

Troubleshooting

QoE Report Verification on the QoE Agent Client Gateway

You can track the status of a QoE message sent from the client using the SIP Signaling Group counter.



> If more than one signaling are reporting QoE reports, The counters will update on a signaling where the call came in the Gateway.

QoE Report Verification on the QoE Agent Server Gateway

You can track the status of the QoE messages stored in the database by viewing the **Operational Status** page in the Application Solution Module section of the Tasks tab.



How to enable, collect, and provide log files from SBC and SBA

Copyright © 2015 Sonus Networks. All rights reserved.

Table of Contents

- Overview
- Use Case
  - Setup
  - Scenario
- Files to be provided
  - SBC Configuration Backup File
  - Logs
    - Enabling Logging
      - SBC Logs
      - Lync (SBA) Logs
    - Executing the Scenario in Question
    - Collecting the Logs
      - SBC Logs
      - Lync (SBA) Logs
      - SBCSBA/ASM Logs
  - Provide the Logs

About this Page

This is a best practice on how to enable, collect, and provide traces and logs from a Sonus SBC 1000/2000 and from ASM.

Overview

In the process of troubleshooting issues in your voice SONUSwork, you may need to collect logs from SBC or from Application Solution Module (ASM) yourself, or you may be asked by SONUS TAC to do it. In most cases, when a CRM case is opened, SONUS TAC will request the relevant logs and configuration backup. In most cases, SONUS TAC engineers will need the following files as the minimum requirement to start their analysis:

1. SBC 1000/2000 configuration backup file
2. WebUI log with following subsystems enabled:
   - Call Routing Service
   - Common Call Control
   - Media Stream Control Service
   - SIP Stack Service
   - ISDN Protocol
3. Brief description of the scenario in question with the calling and called party numbers
4. Peer IP addresses
5. The Lync Server 2010 Log
6. ASM (SBA) logs from ASM machine

Use Case

Setup

Copyright © 2015 Sonus Networks. All rights reserved.

SBC 1k/2k is configured in following setup:

```
PSTN -- [SBC 1000/2000 gateway] -- [SBA] -- [Lync SBA client]
```

Scenario

1. Lync SBA client calls a PSTN number
2. Call in question is reproduced, and SBA event log states that the gateway is marked as down

Once the issue is addressed with a CRM case, be sure to include the following files for a quicker resolution:

Files to be provided

SBC Configuration Backup File

1. Procedure to backup SBC 1k/2k configuration file is explained in Backing Up Data

Logs

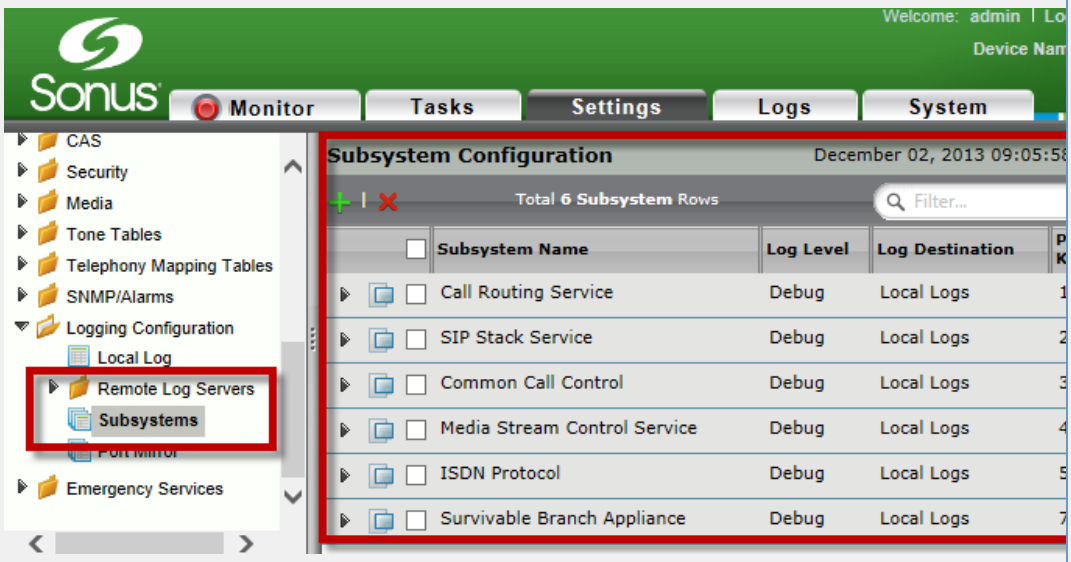
Enabling Logging

SBC Logs

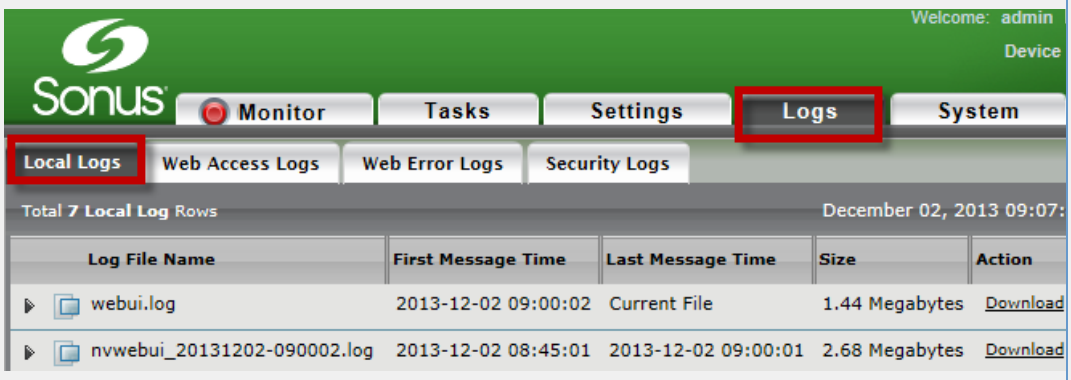
SBC2000

Copyright © 2015 Sonus Networks. All rights reserved.

1. Launch your preferred browser and log into WebUI
2. Navigate to SETTINGS (tab) > Logging Configuration / Subsystems (in navigation pane)
3. Add the following subsystems with the log level of **Debug** as shown on following screenshot



4. Rotate the log as shown on the following screenshot:

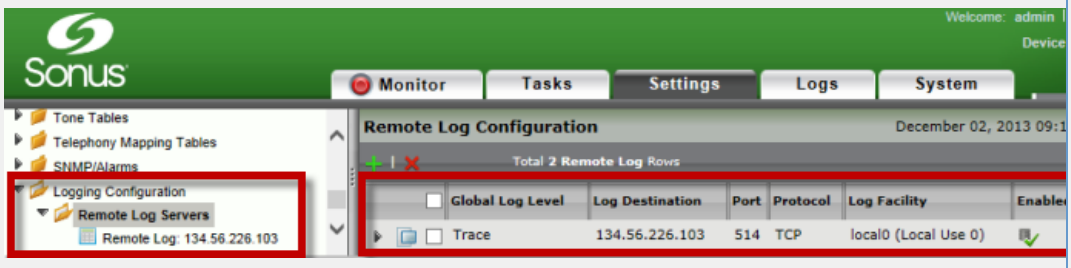


SBC1000

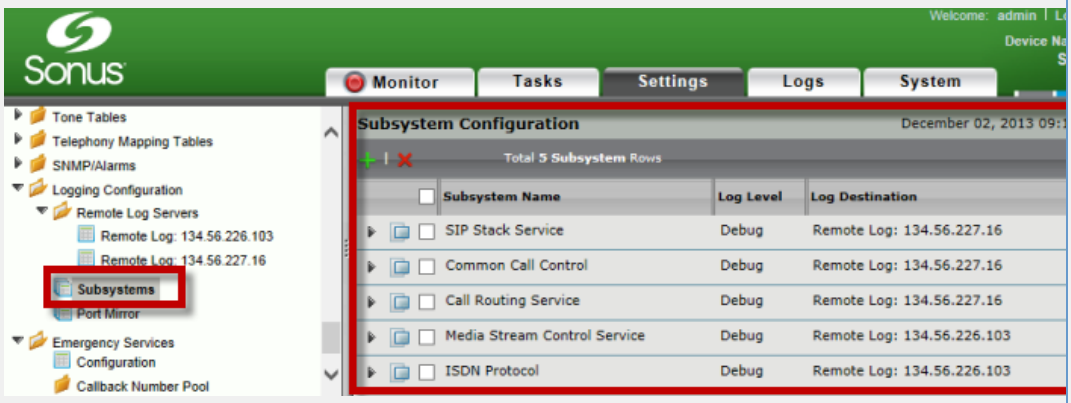
1. Make sure to have a syslog server installed in your SONUSwork; preferably Log Exchange (LX), which you can download from SONUS downloads.
2. In the WebUI, click the Settings tab.
3. In the left navigation pane, go to Logging Configuration > Remote Log Servers.

Copyright © 2015 Sonus Networks. All rights reserved.

4. Add Remote Log Server as show on the following screenshot (Log Destination is where the SONUS Log Exchange (LX) is installed)



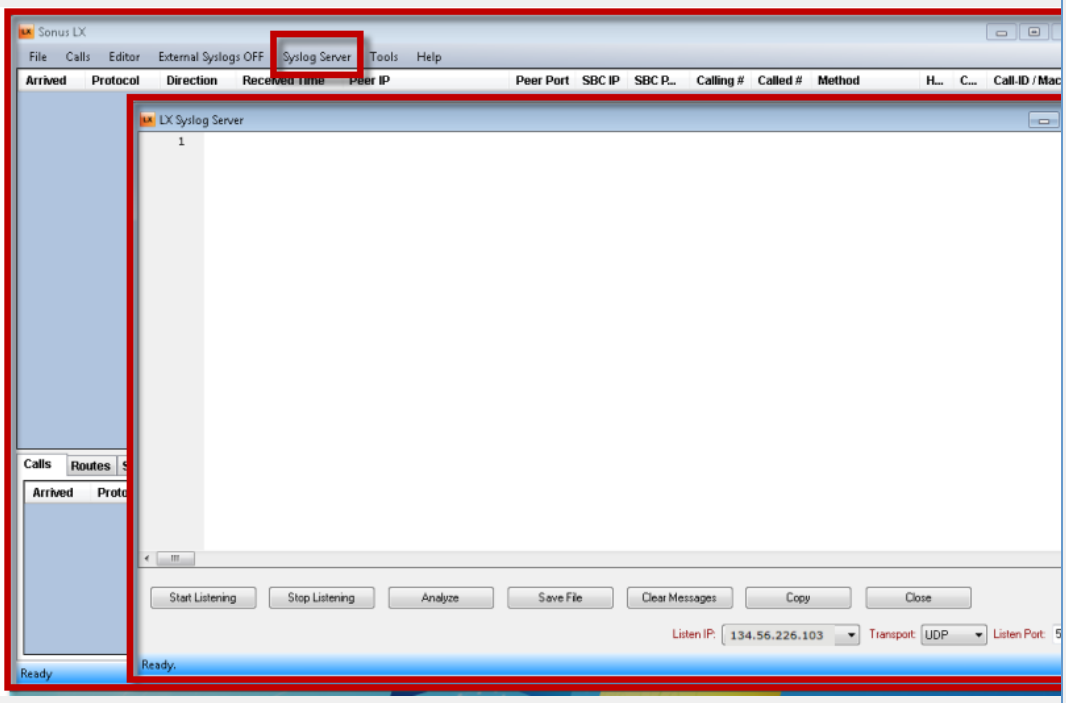
5. In the WebUI, click the Settings tab.
6. In the left navigation pane, go to Logging Configuration > Subsystems and add the following subsystems as show on the following screenshot.



7. Launch the Log Exchange (LX) on the Syslog Server Machine
8. Click **Syslog Server**

Copyright © 2015 Sonus Networks. All rights reserved.

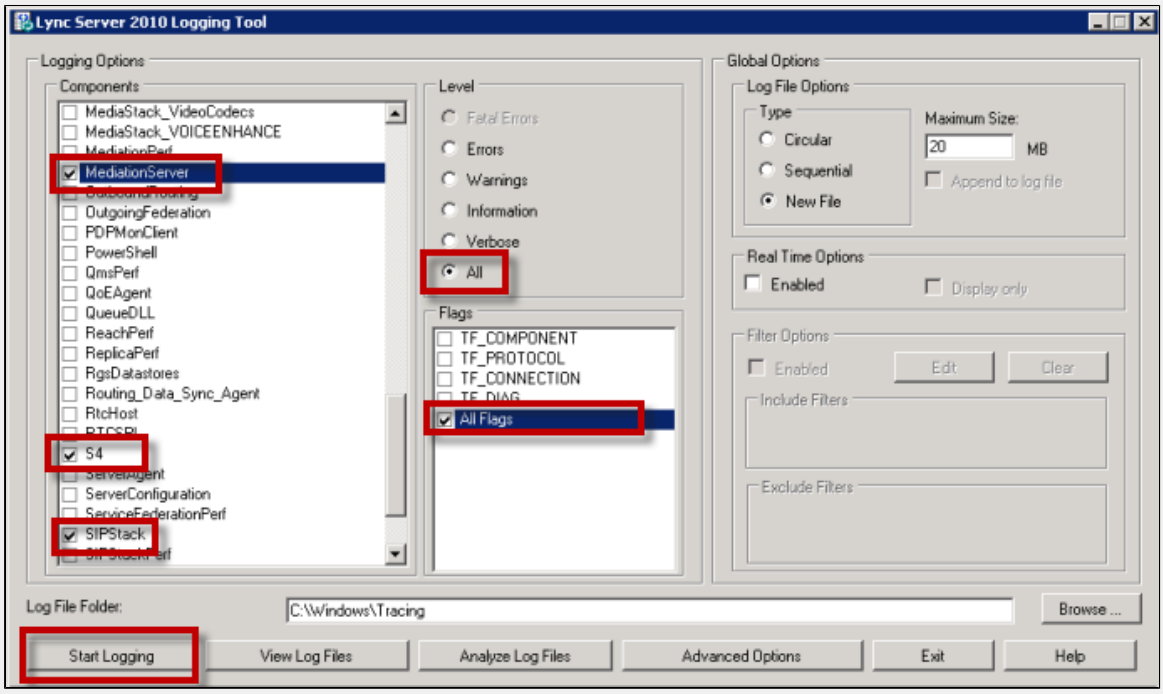
9. Click **Start Listening** as shown on the following screenshot.



Lync (SBA) Logs

Copyright © 2015 Sonus Networks. All rights reserved.

1. Remote Desktop into SBA machine (ASM)
2. Launch the Lync Server 2010 Logging Tool
3. Enable **Mediation Server**, **S4**, and **SIPStack** components with Level **All**, and Flags **All** for each component
4. Hit **Start Logging** as shown on the following screenshot:



Executing the Scenario in Question

Now execute the scenario (i.e: Lync client calls to PSTN number, call is reproduced.)

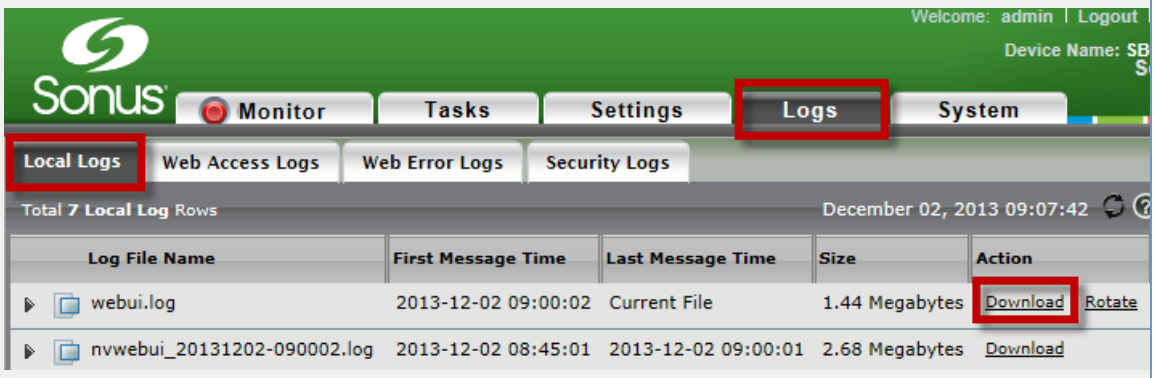
Collecting the Logs

SBC Logs

SBC2000

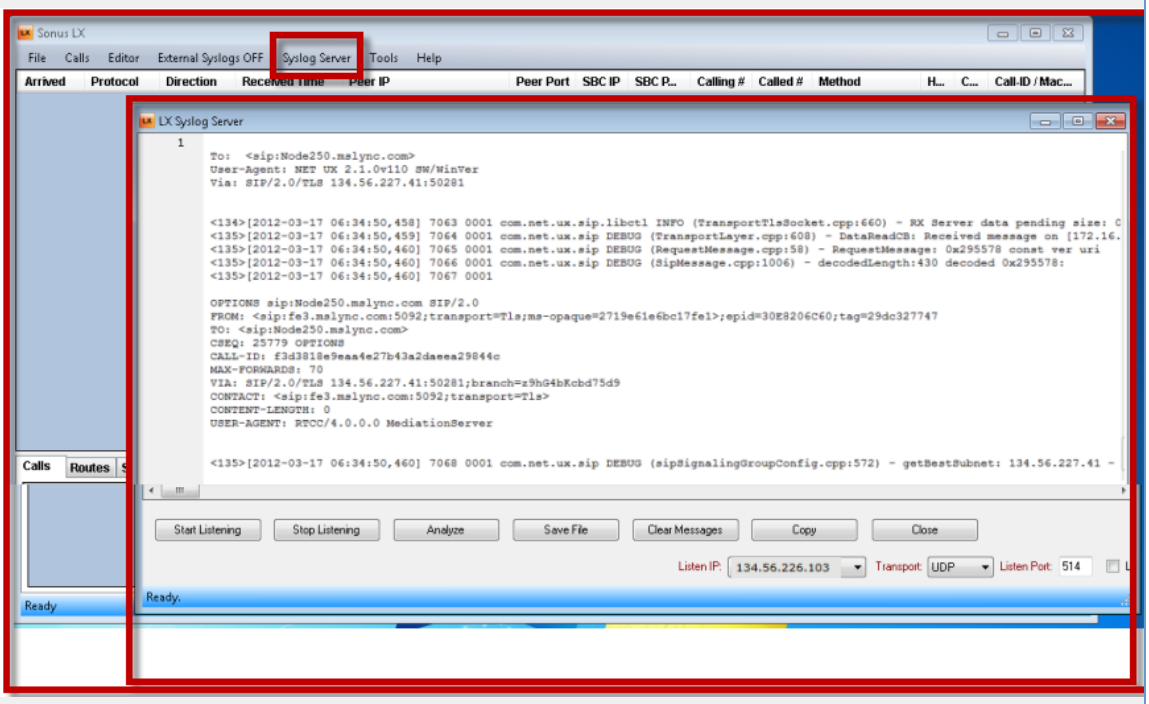
Copyright © 2015 Sonus Networks. All rights reserved.

1. Launch a supported browser and log into WebUI
2. Navigate to SETTINGS (tab) > Logging Configuration / Subsystems (in navigation pane)
3. Download the log as shown on the following screenshot:



SBC1000

1. On Syslog Server machine, click **Stop Listening** on LX Syslog Server as shown on the following screenshot:



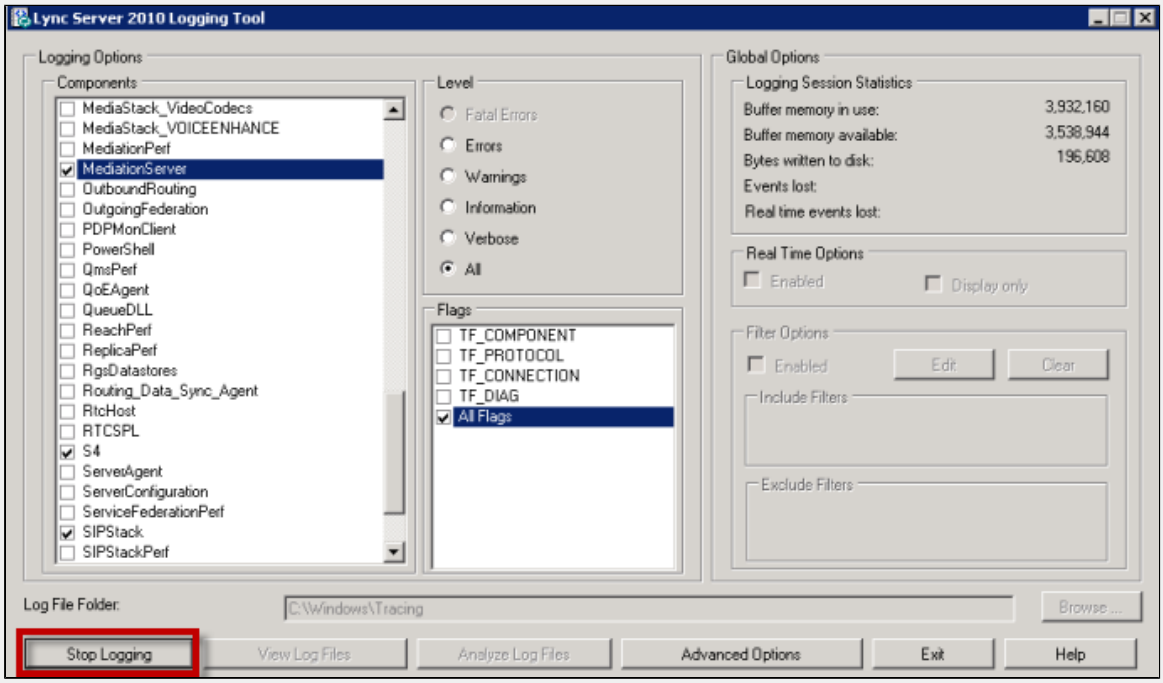
2. Click **Save File** button and save it as **.log** or **.txt** file.

Lync (SBA) Logs

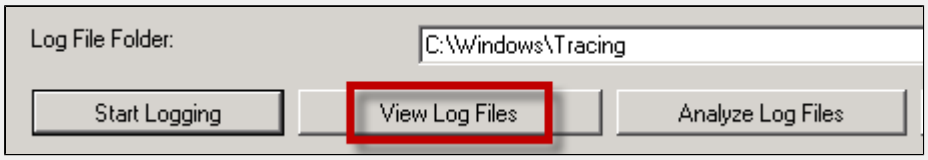
1. Remote Desktop into SBA machine (ASM)
2. In the Lync Server 2010 Logging Tool

Copyright © 2015 Sonus Networks. All rights reserved.

3. Hit **Stop Logging** as shown on the following screenshot:

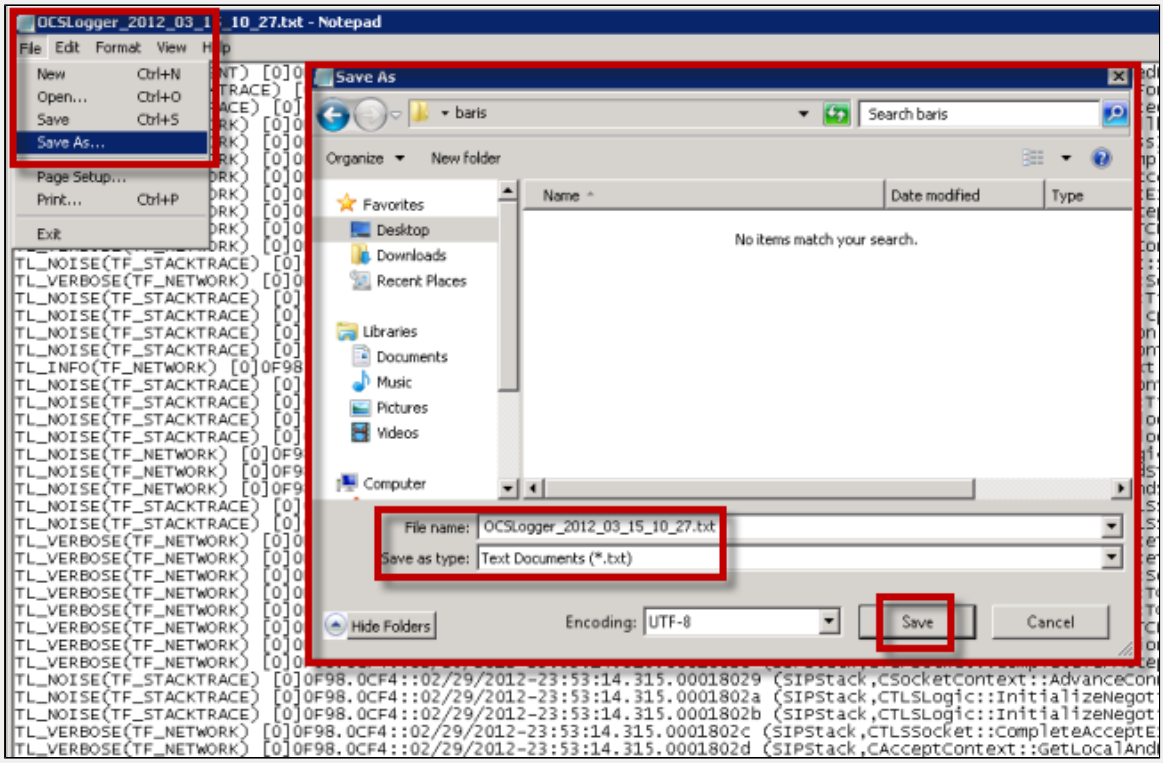


4. Hit **View Log Files** on Lync Server 2010 Logging Tool as shown on the following screenshot



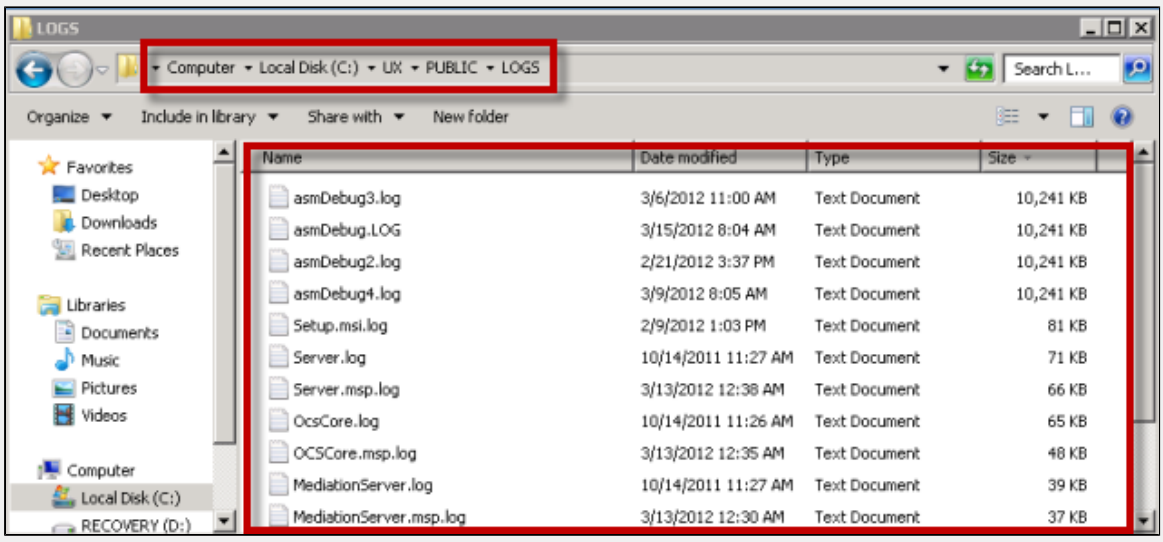
Copyright © 2015 Sonus Networks. All rights reserved.

5. Save the log as txt file as shown on the following screenshot



SBCSBA/ASM Logs

1. Remote Desktop into SBA machine (ASM)
2. Use Windows Explorer to navigate to the **C:\SBC\PUBLIC\LOGS** directory as shown below and collect/copy all files in this directory as shown on the following screenshot



Provide the Logs

Copyright © 2015 Sonus Networks. All rights reserved.

Once you have the necessary logs compress all files into ZIP or RAR format and provide them to SONUS TAC engineer. Depending on the size of the files, you could either email them or upload them onto our FTP site: supportftp.sonusnet.com Instructions about uploading the files will be provided with your case.

SBC 1000/2000 Security Hardening Checklist

On This Page

- Purpose
- Security Hardening Checklist
- Monitoring Security

Related Articles

Purpose

This document provides a checklist to help with hardening the SBC1000/2000 against malicious network-based attacks.

Security Hardening Checklist

The following checklist provides a security hardening guide.

1. Use latest versions of Sonus SBC1000/2000 software. When new security vulnerabilities are reported in operating systems and common third-party software, Sonus produces maintenance releases incorporating the fixes.
2. Configure Access Control Lists.
    - Configure access lists to prevent excessive amounts of unwanted traffic (Dos attacks) on the SBC 1000/2000.
    - Documentation Links:
        - Managing Access Control Lists
        - Creating and Modifying Rules in Access Control Lists
3. Use TLS/SRTP for SIP/Media.
    - Use TLS for signaling and SRTP for media. Do not use UDP/RTP for signaling and media because they are not encrypted.
    - Some documentation links:
        - Managing TLS Profiles
        - SBC ISDN To SIP Routing for Dummies - TLS
        - Configuring the Sonus SBC 1000-2000 for Standard and Mutual TLS Authentication
        - Managing Media Crypto Profiles
4. Only use Certificates from Trusted CA. Do not use self-signed certificates (unless the systems with self-signed certificates are within your trusted network).
    - Always use certificates from a trusted certificate authority, do not use self-signed certificates.
    - Documentation Links:
        - Working with Certificates
        - Common Troubleshooting Issues with Certificates in Sonus SBC 1000-2000
5. Enable enhanced password security for SBC operator accounts.

Copyright © 2015 Sonus Networks. All rights reserved.

- By default, when new SBC operator accounts are created, enhanced security such as complex passwords, limited account duration, limiting the number of login sessions, etc., are not enforced. This must be enabled by the administrator to limit the number of malicious/unauthorized login attacks on the system.
- Documentation:
  - Managing Global Security Options
  - Monitoring User Activity
  - How do I find a logged in user's IP address

6. If Active Directory is used, use TLS with Active Directory.
   - Use TLS when configuring Active Directory services on SBC1000/2000.
   - Documentation:
     - Configuring the Sonus SBC 1000-2000 for Active Directory
     - How User Authentication Works
7. Check if RADIUS is used for user authentication.
   - Passwords are encrypted during RADIUS authentication process. However, RADIUS works on UDP and fields other than the user's credentials are not encrypted. RADIUS servers and the SBC1000/2000 are usually within the same trusted domain (inside corporate LAN protected by firewall or over VPN) and so this is not an issue at all. However, if confidentiality is important even inside the trusted domain, RADIUS should not be used.
   - Documentation links:
     - How User Authentication Works
     - Configuring the Sonus SBC 1000-2000 for RADIUS
     - RADIUS User Authentication Tips Using FreeRADIUS
8. Check if RADIUS CDR confidentiality is required
   - RADIUS CDR transport is based on UDP and this data is not encrypted. In all cases however, RADIUS servers and the SBC1000/2000 are usually within the same trusted domain (inside corporate LAN protected by firewall or over VPN), consequently this is not an issue. However, if confidentiality is important inside the trusted domain, RADIUS should not be used.
   - Documentation link:
     - Configuring the Sonus SBC 1000-2000 for CDR
9. If the ASM module is present, configure the ASM Firewall.
   - Documentation link:
     - Configuring the ASM Firewall
10. If the ASM module is present, configure the ASM security template
     - Documentation link:
       - Applying an SBA Security Template

Monitoring Security

Once the system is fully configured,the operator should periodically monitor the system. Many alarms supported by the system are triggered upon security events.

1. Review system security logs and user-login activity.
   - Monitoring User Activity
2. .Review web-access logs:
   - Managing Local Logs
3. Review alarms.
   - Viewing Alarms and Events

Copyright © 2015 Sonus Networks. All rights reserved.

SIP Trunking Between SIP Border Elements

This article explains the configuration steps necessary to allow SIP calls in an **IP.PBX(1) – Sonus SBC 1000/2000 – IP.PBX(2)** topology as illustrated in the diagram below. For the purpose of this article, it is assumed that the IP.PBX - Border Elements - are configured to send/receive SIP calls:

- Sonus SBC 1000/2000 Configuration
- Call verification

Topology



Sonus SBC 1000/2000 Configuration

Configuration Overview

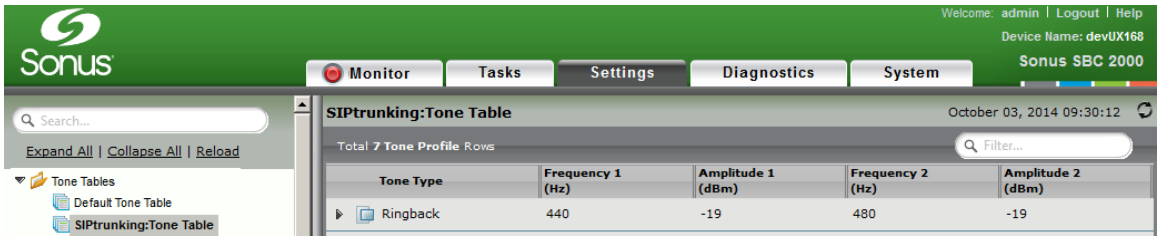
The following configuration steps must be accomplished in the order presented as shown below.

1. Tone Table — You may use the default Tone Table or create a custom table.
2. Media Profiles — In this configuration, G.711A/Mu-law profiles are configured and used.
3. Media List — You may use the default Media List or create a custom list.
4. SIP Server Tables — Add an entry for border elements (i.e., the IP_PBX's used in this example).
5. SIP Profile — You may use the default SIP Profile or create a custom profile.
6. Transformation Table — Create a transformation table to be used in the relevant Call Routing Table(s) for Called/Calling Number transformations.
7. Call Routing Table — Create two Call Routing Tables (one for ISDN and another for SIP) to be used in the relevant Signaling Groups.
8. Signaling Groups — Create two SIP Signaling Groups (one for each border element).
9. Call Routing Table Entries — Create two Call Routing Table Entries to route the calls.

Tone Table

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Tone Tables**.
3. Add a Tone Profile Table (*SIPtrunking: Tone Table*) as shown below.

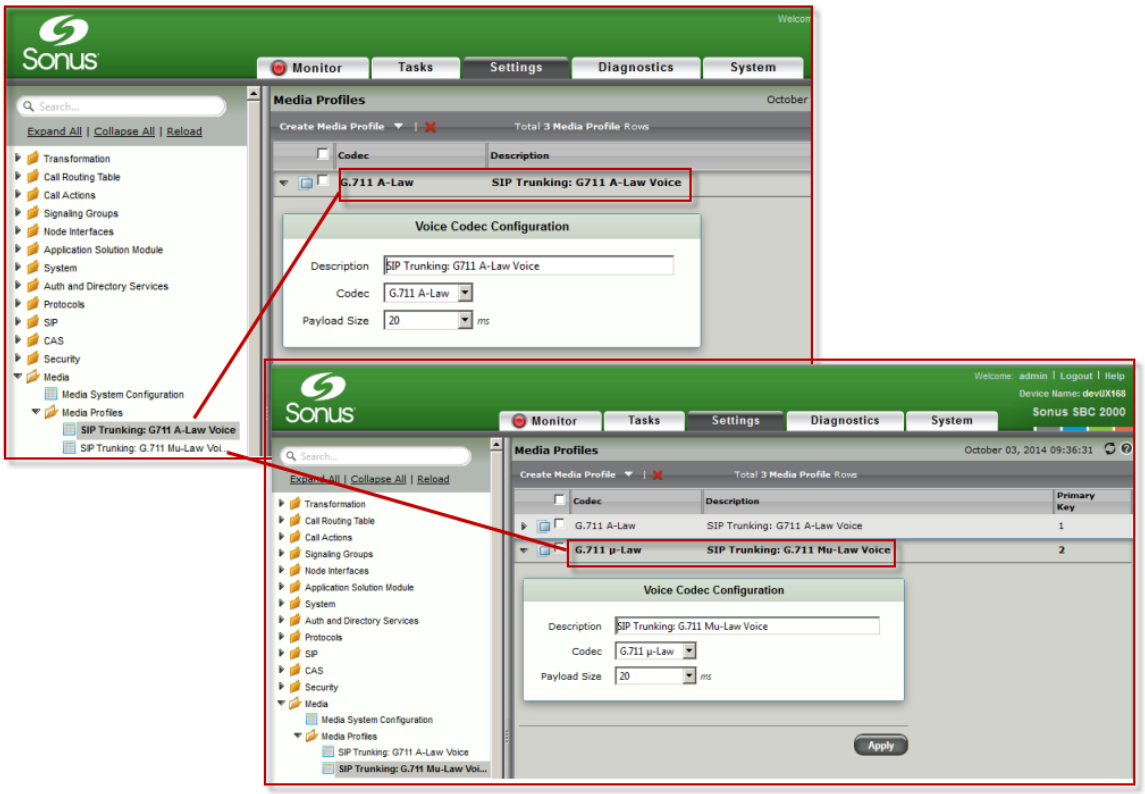
Copyright © 2015 Sonus Networks. All rights reserved.



Media Profiles

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Media > Media Profiles**.
3. Add two new Voice Codec Profiles, as shown below.
    a. Name them *SIPtrunking: G.711 A-Law Voice* and *SIPtrunking: G.711 Mu-Law Voice*.
    b. Select the G.711 A-Law Codec.

This example illustrates the usage of G.711 A-Law Voice and G.711 Mu-Law Voice Codec profiles. G.723.1, G.726, and G.729 codecs are also available in Sonus SBC 1000/2000, and can be created if necessary.

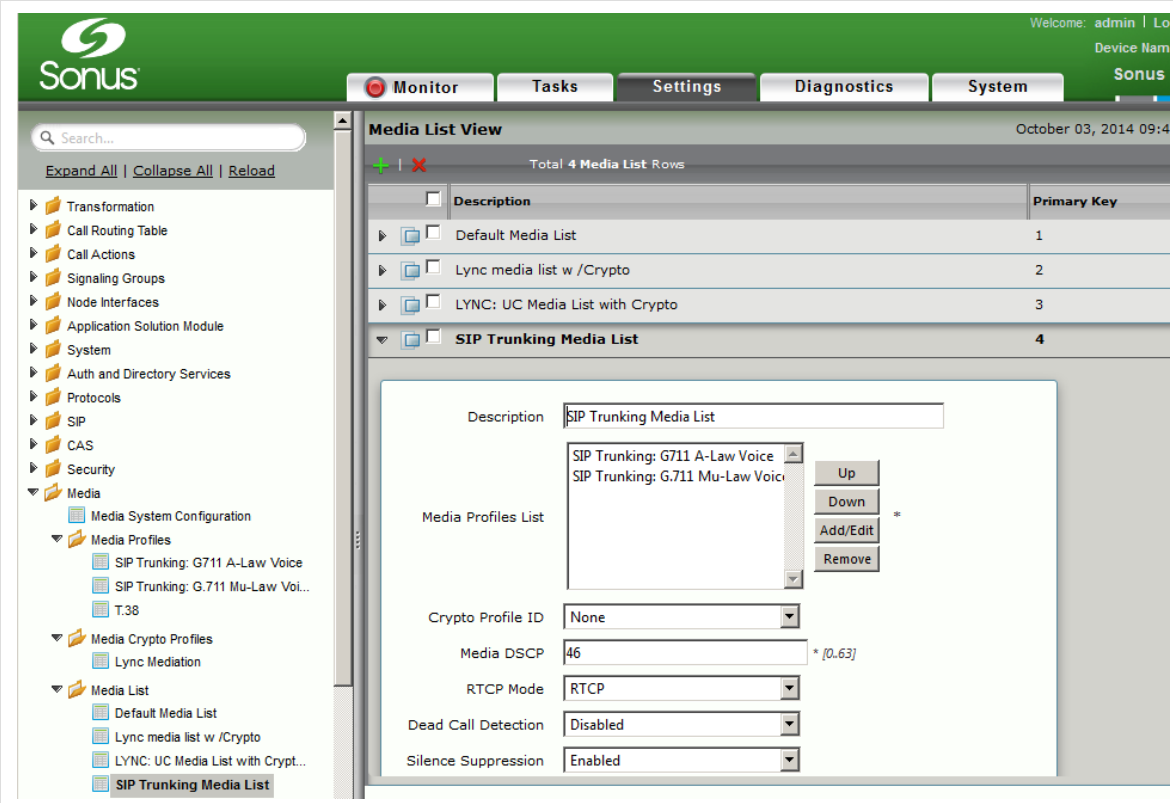


Media List

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Media > Media List**.
3. Add a new Media List.
    a. Specify the Media Profiles created in the previous section in the **Media Profiles List** text box.

Note that in this example, the other variants in the Media List entry are left with their default settings (i.e: Crypto as NONE, Dead Call Detection as Disabled, Silence Suppression as Enabled,...etc.)

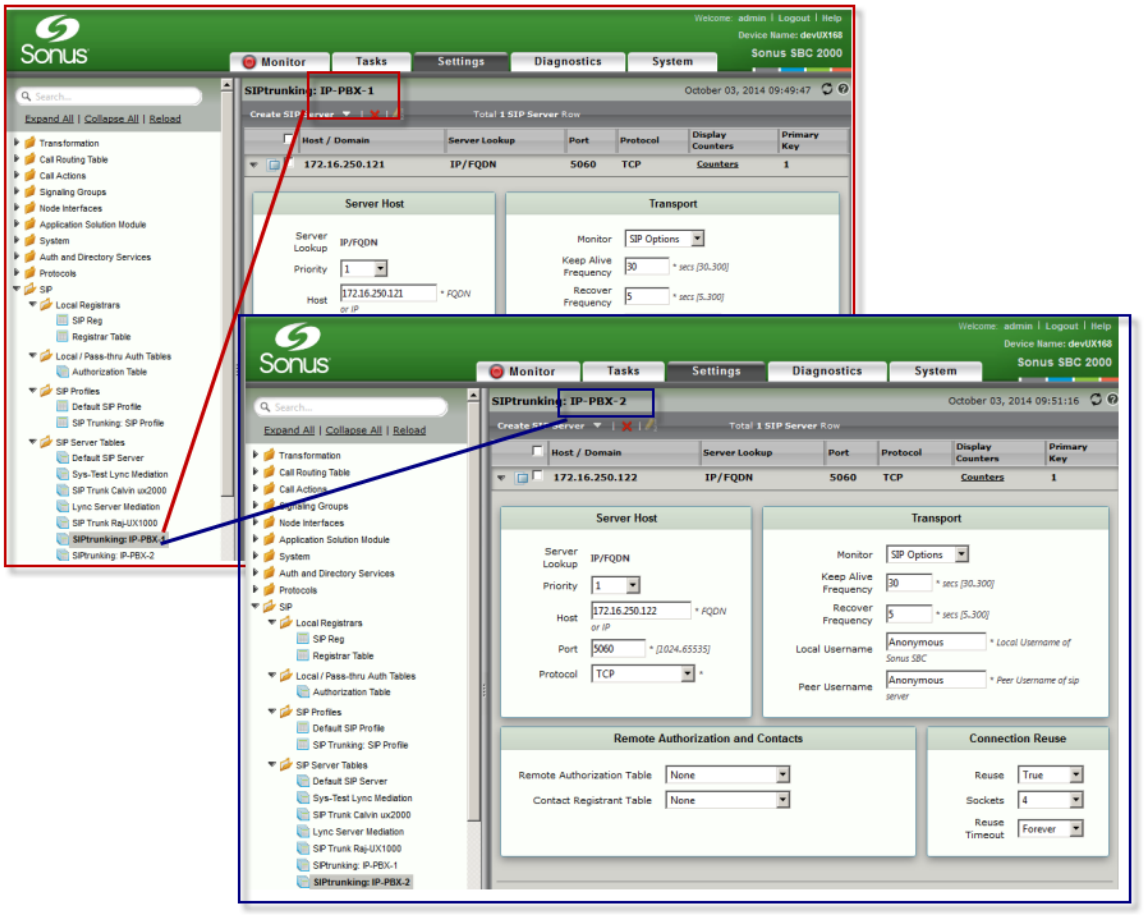
Copyright © 2015 Sonus Networks. All rights reserved.



SIP Server Tables

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Server Tables**.
3. Add two new SIP Server Table entries(one for each border element).
    a. Name them *SIPtrunking: IP-PBX-1* and *SIPtrunking: IP-PBX-2*.
4. Configure the new entries from the previous step as shown below.

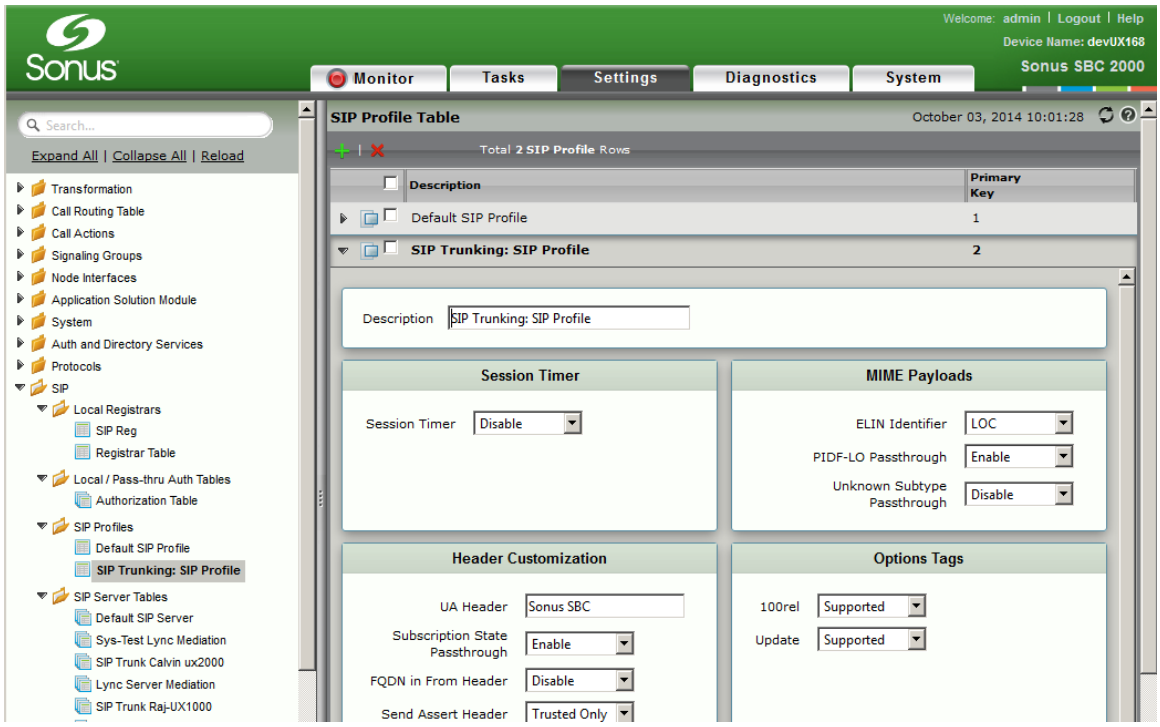
Copyright © 2015 Sonus Networks. All rights reserved.



SIP Profile

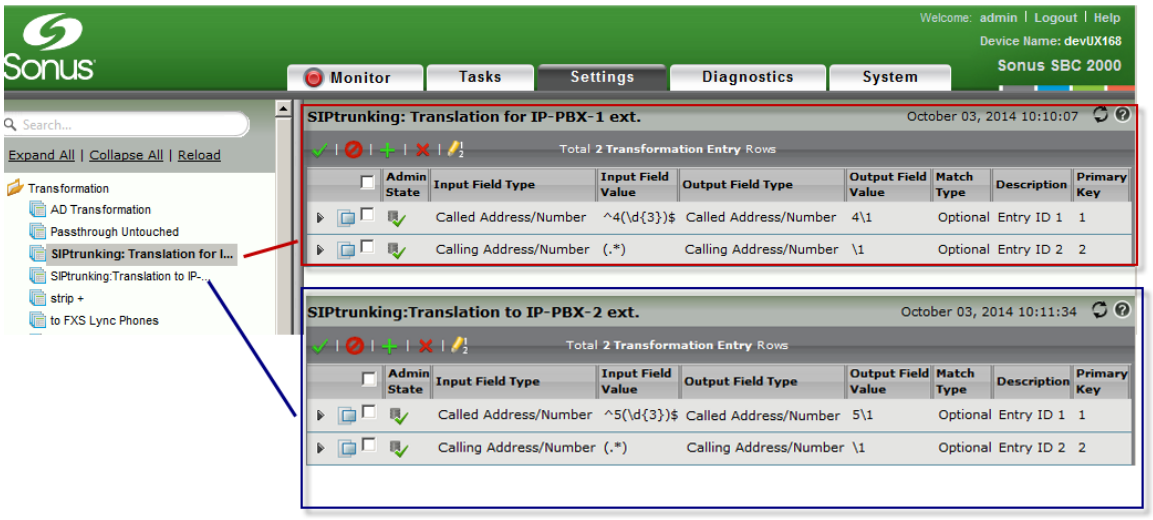
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Profiles**.
3. Add a new SIP Profile as shown below.
4. Name it *SIPtrunking: SIP Profile*.

Copyright © 2015 Sonus Networks. All rights reserved.



Transformation Table

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Transformation**.
3. Add two new entries and name them *SIPtrunking: Translation for IP-PBX-1 ext.* and *SIPtrunking: Translation for IP-PBX-2 ext.*.
4. Configure the entries created in the previous step as shown below.



Call Routing Table

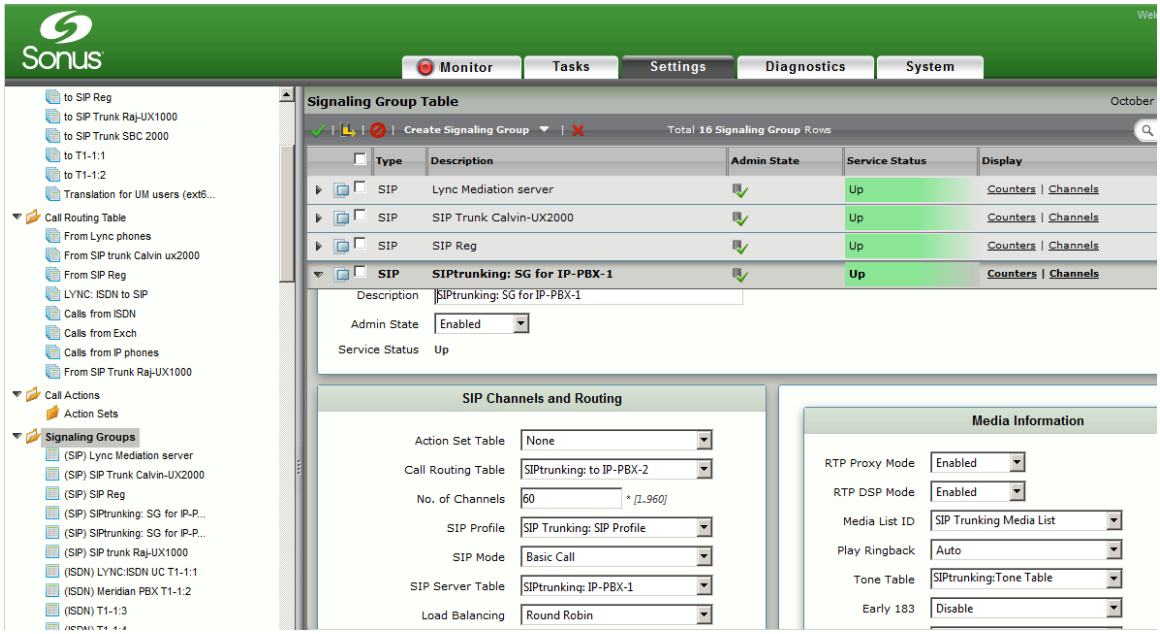
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table**.
3. Add two new Call Routing Tables, and name them *SIPtrunking: to IP-PBX-1* and *SIPtrunking: to IP-PBX-2*.

Copyright © 2015 Sonus Networks. All rights reserved.

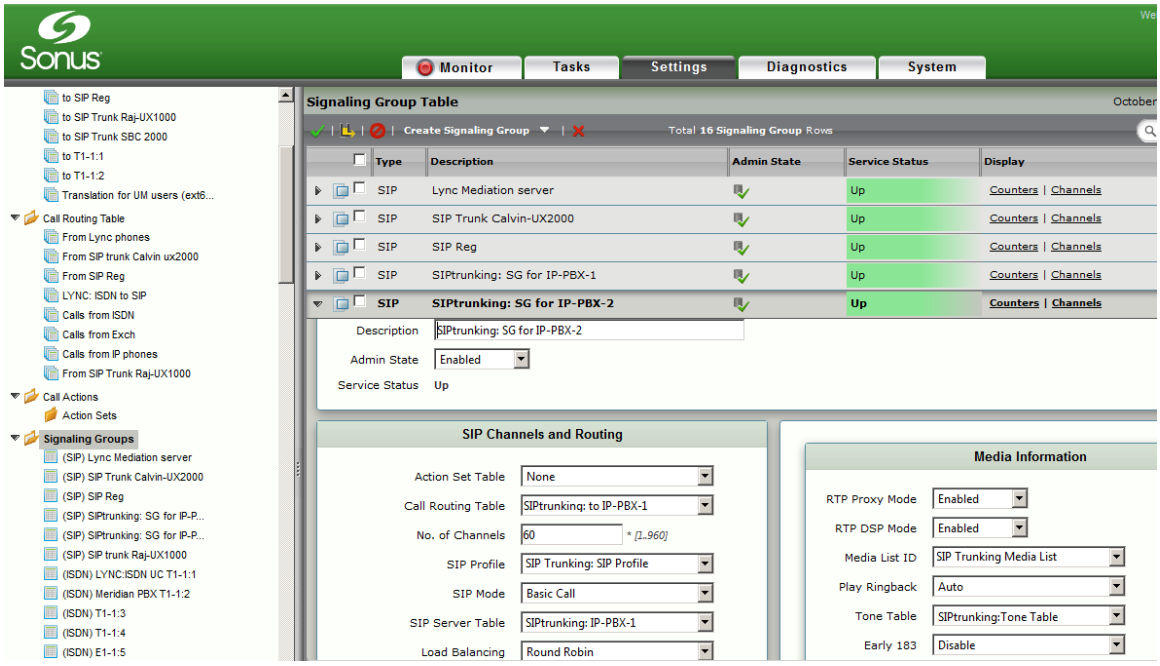
Signaling Groups

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**
3. Add two new SIP Signaling Groups, and configure them as show below.

SIP Signaling Group #1



SIP Signaling Group #2



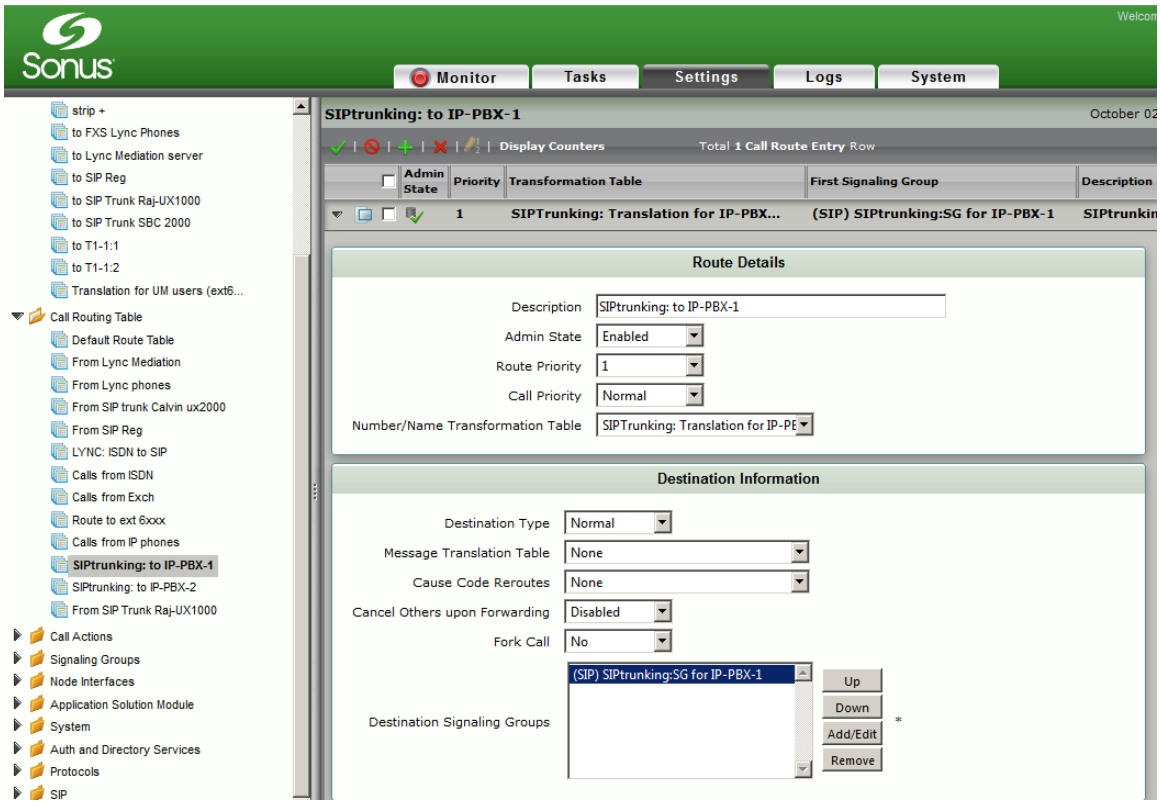
Call Routing Table Entries

1. In the WebUI, click the **Settings** tab.

Copyright © 2015 Sonus Networks. All rights reserved.

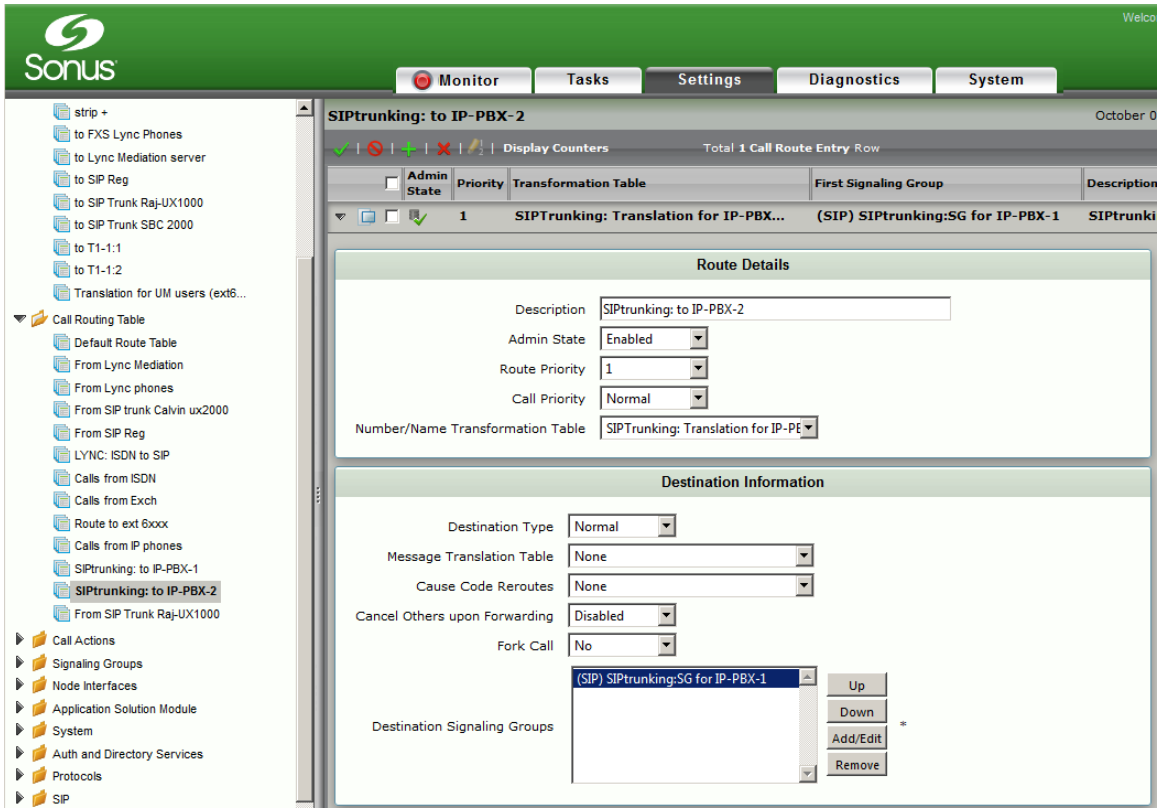
2. In the left navigation pane, go to **Call Routing Table > (relevant entry)**.
3. Configure each of Call Routing entries that you created earlier in this article as shown below.

Call Routing Entry #1 for Table #1



Call Routing Entry #1 for Table #2

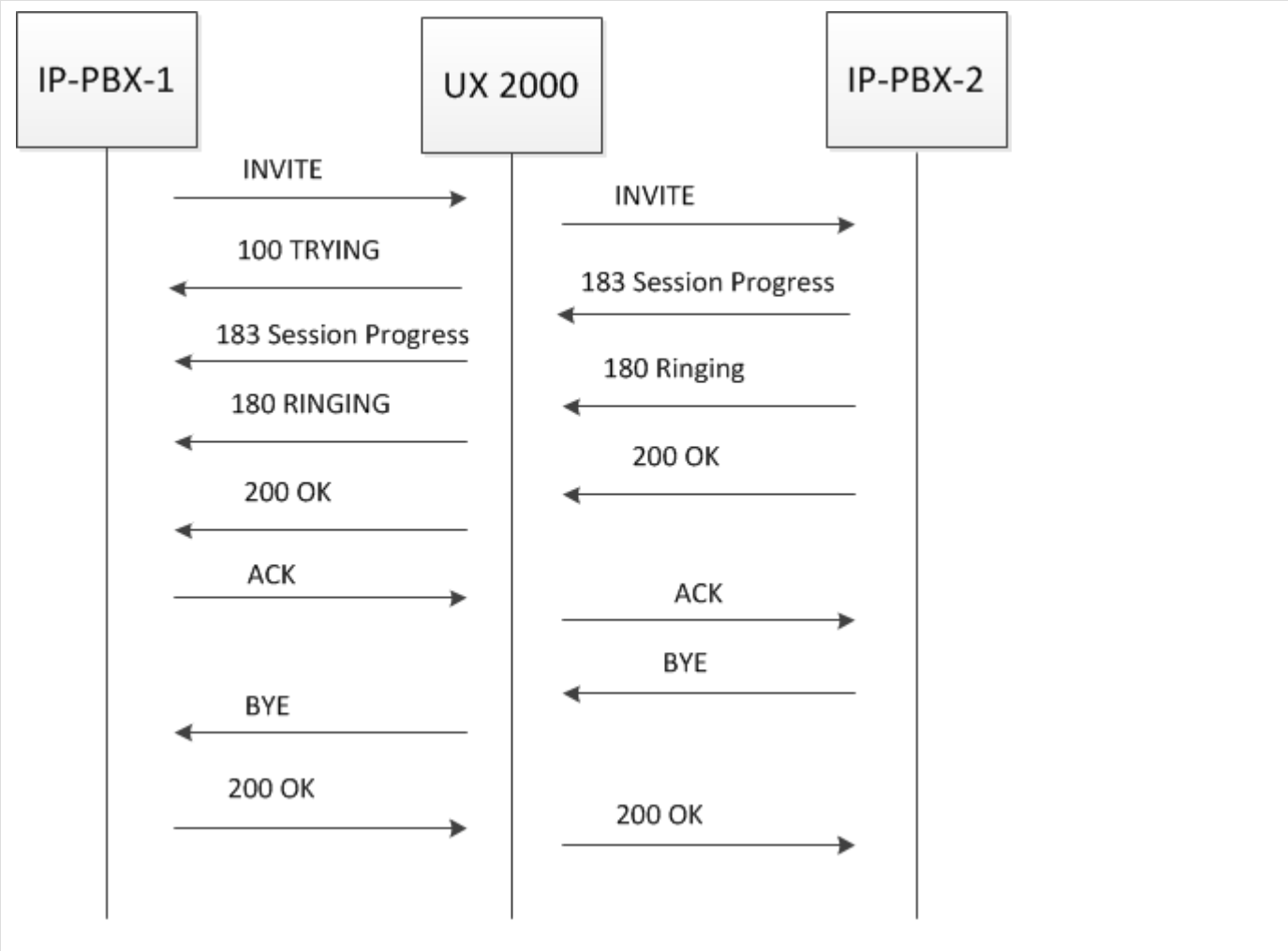
Copyright © 2015 Sonus Networks. All rights reserved.



Call verification

Once the above configuration steps have been completed, a SIP call from Border Element 1 (IP-PBX-1) to Border Element 2 (IP-PBX-2) using Sonus SBC 1000/2000 SIP Trunking will have the following call flow:

Copyright © 2015 Sonus Networks. All rights reserved.



SIP Trunking with Multiple IP support

This article describes the steps necessary to configure the Sonus SBC 1000/2000 for SIP Trunking using **Multiple IP Interface** support – available in since UX Release 1.0.2:

- Use Case Scenario
- Sonus SBC 1000/2000 Configuration
  - LAN Port 2/Ethernet 2 IP
  - Transformation Table
  - Call Routing Tables
  - Signaling Groups

Use Case Scenario

A typical use case scenario for the Multiple IP Interface support is as follows: — also illustrated in the diagram below

Sonus SBC 1000/2000 is connected to both a public network and a private (Enterprise) network, acting as a Session Border Controller (SBC) which effectively hides the topologies, IP addressing, signaling attributes and policies established between these two networks from each other. Calls from one network to the other are terminated on Sonus SBC 1000/2000 (i.e. at the network border) and Sonus SBC 1000/2000 establishes a different call on the other network, and enables end-to-end conversation.

In this example, the SIP trunking provider and the Sonus SBC 1000/2000 are connected using the `10.51.100.X`

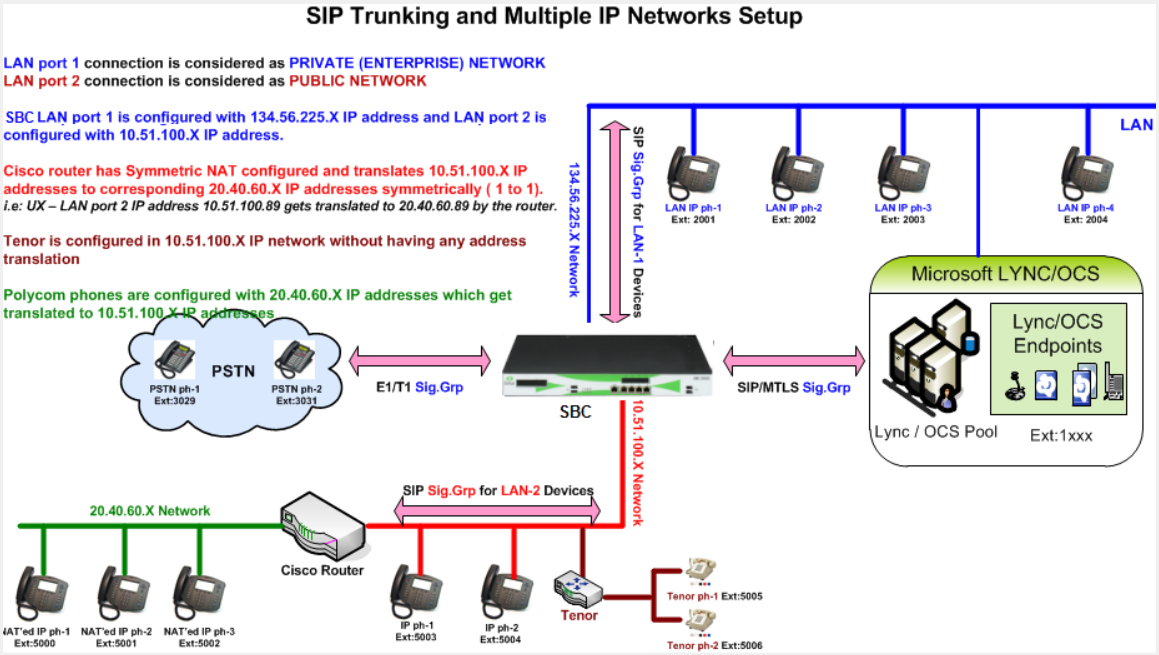
Copyright © 2015 Sonus Networks. All rights reserved.

network. The enterprise has a IP range of `134.56.225.X`. The Sonus SBC 1000/2000's main application bridge is configured to `134.56.225.202` which is the default interface and has the default IP route pointing to it. The signaling and media packets for calls to and from OCS and LAN-1 endpoints will use 134.56.225.202 as the IP address of Sonus SBC 1000/2000.

When calls are established over the SIP trunk, LAN-2 interface is used. In this case the SIP calls must use the interface IP of `10.51.100.89` for the SIP messaging, SIP source IP address and RTP source IP address. This allows Sonus SBC 1000/2000 to bridge the networks for calls and not simply route the IP packets.

The cleanest solution is to configure a single SIP Signaling Group for each network. The SIP SG pointing towards the ISP network should refer to LAN-2 interface. LAN-2 should be placed in ROUTED mode with an IP address in the `10.51.100.89/24` range. The SIP SG pointing to the Enterprise network should use the Application-IP interface, which is the default.

Topology



Sonus SBC 1000/2000 Configuration

This article assumes that a **PSTN - Sonus SBC 1000/2000 - OCS 2007 R2** configuration is already in place, therefore it is unnecessary to configure Media Profiles, Media List, SIP Profiles, SIP Server Tables, Tone Table, Telephony Mapping Table in this exercise.

The relevant configuration steps for these items are already covered in the Deployment in PSTN - SBC - Microsoft OCS 2007 R2 Topology page.

From the SIP Trunking with Multiple IP configuration point of view, the following items must be configured in the Sonus SBC 1000/2000:

- LAN Port 2/Ethernet 2 IP
- Translation Table
- Call Routing Table

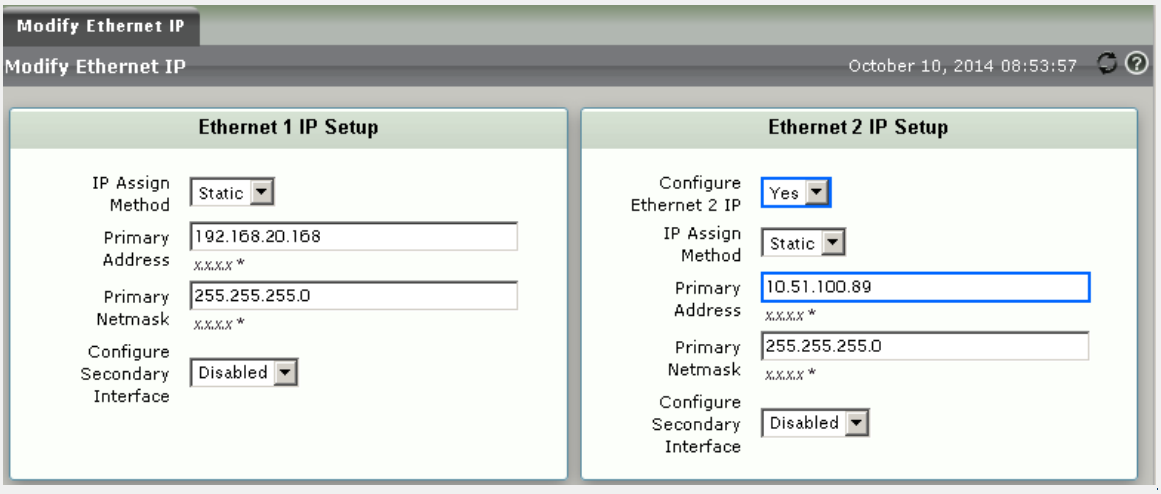
Copyright © 2015 Sonus Networks. All rights reserved.

- Signaling Group

LAN Port 2/Ethernet 2 IP

Sonus SBC 2000

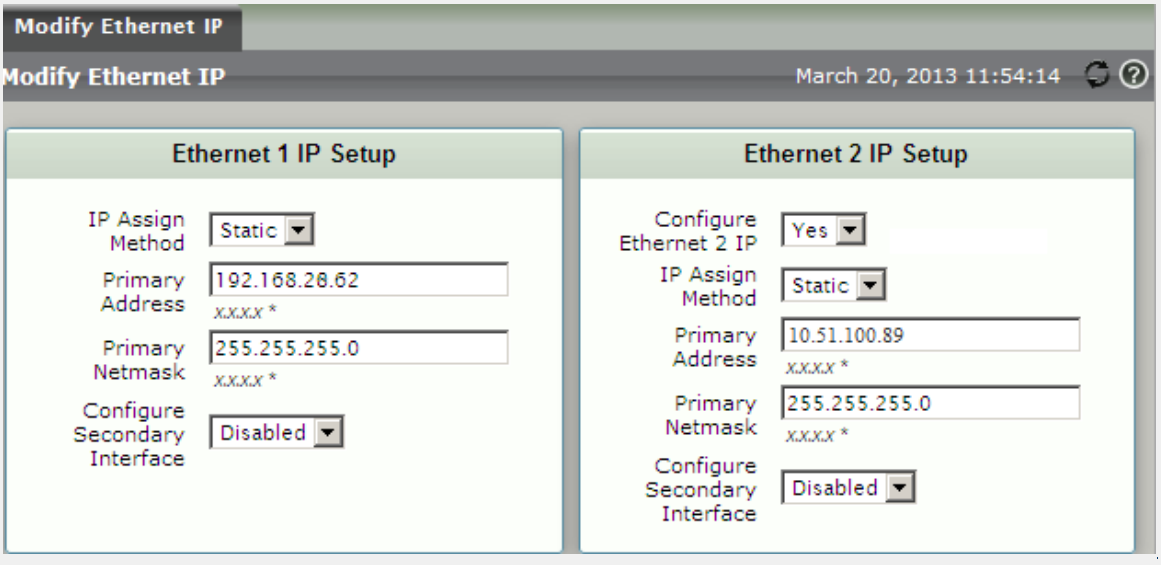
Configure the public IP address **`10.51.100.89`** in the Sonus SBC 1000/2000. In the WebUI, access **Tasks** and select **Modify Ethernet IP Address.**



Note that LAN Port 1 **`134.56.225.202`** is already configured on the node which you'd be using to URL into WebUI. Following screenshot depicts the verification of LAN 1 configuration:

Sonus SBC 1000

Configure the public IP address of **`10.51.100.89`** in theSonus SBC 1000/2000. In the WebUI, access **Tasks** and select **Modify Ethernet IP Address.**

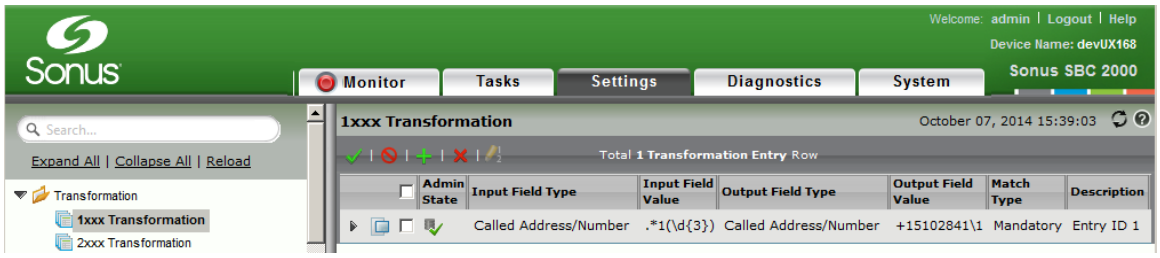


Transformation Table

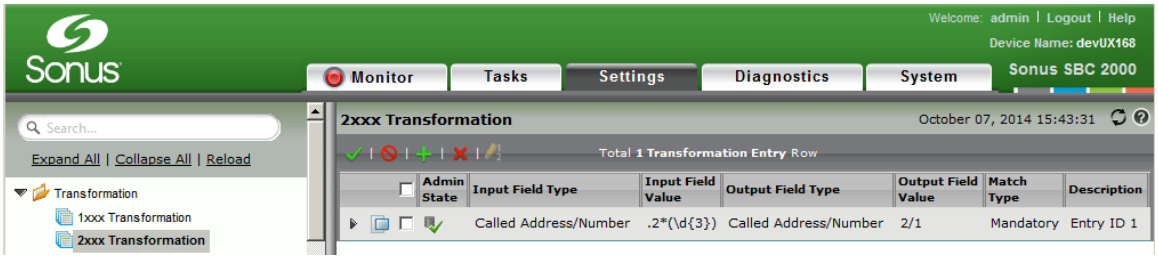
Copyright © 2015 Sonus Networks. All rights reserved.

There are 4 different transformations used in this exercise:

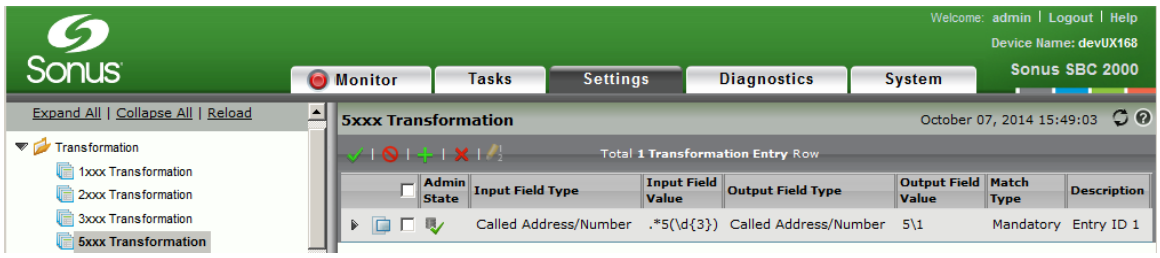
Translation table for OCS (1xxx) extensions



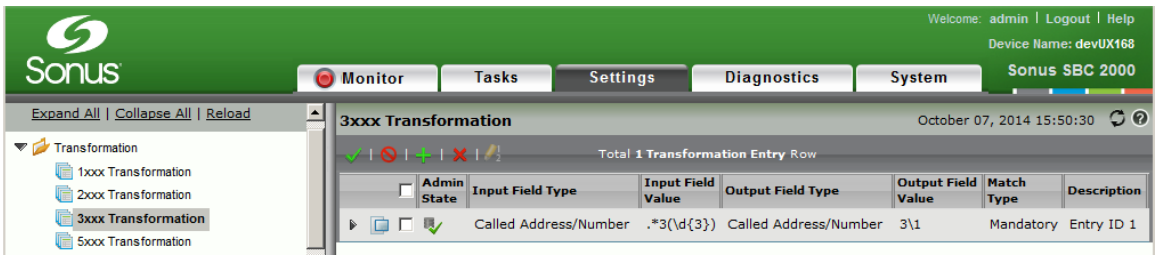
Translation table for LAN-1 (2xxx) extensions



Translation table for LAN-2 (5xxx) extensions



Translation table for PSTN (3xxx) extensions

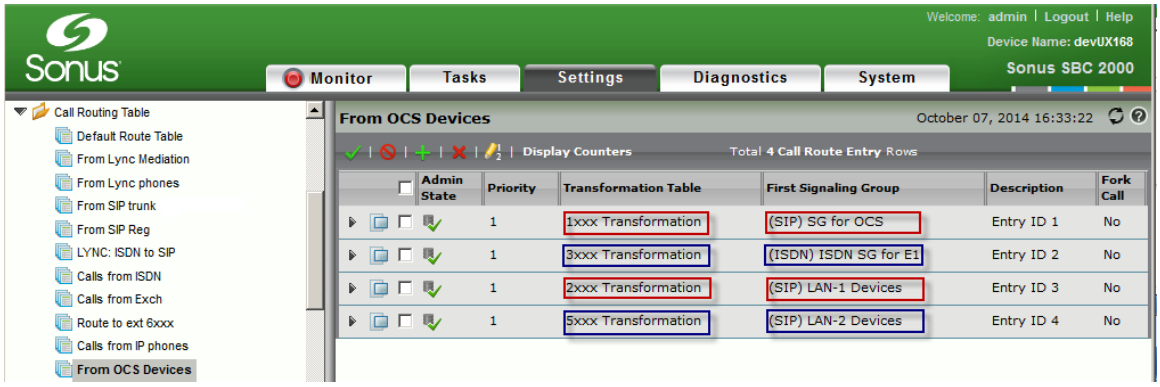


Call Routing Tables

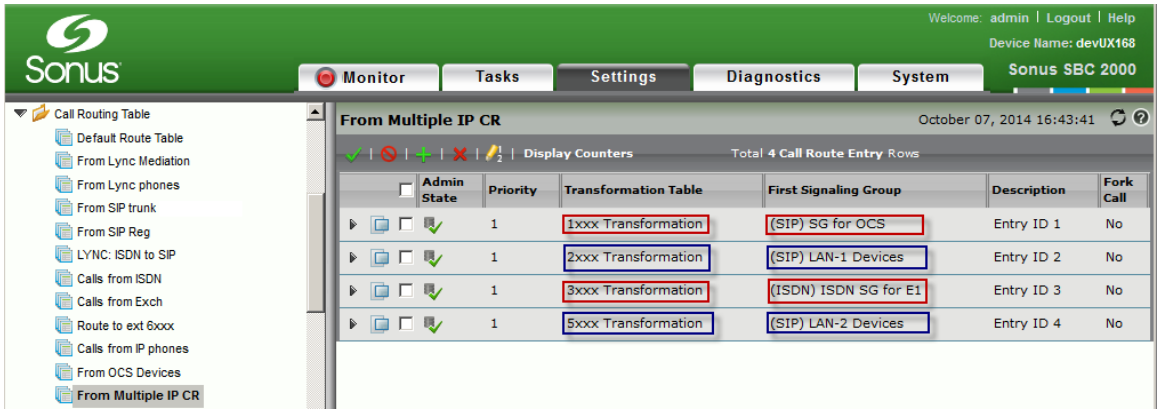
There are 3 different Call Routing Table entries used in this exercise:

Routing Calls from OCS Endpoints

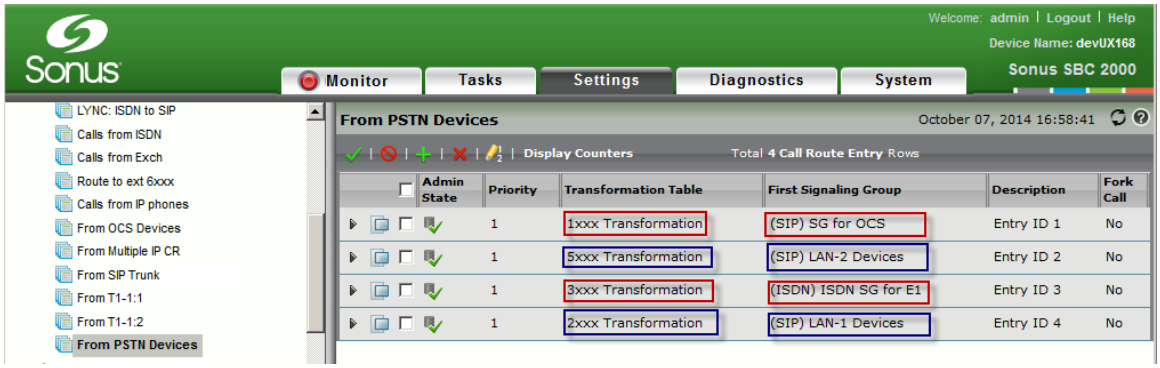
Copyright © 2015 Sonus Networks. All rights reserved.



Routing Calls from Multiple IP Endpoints (LAN-1 and LAN-2 endpoints)



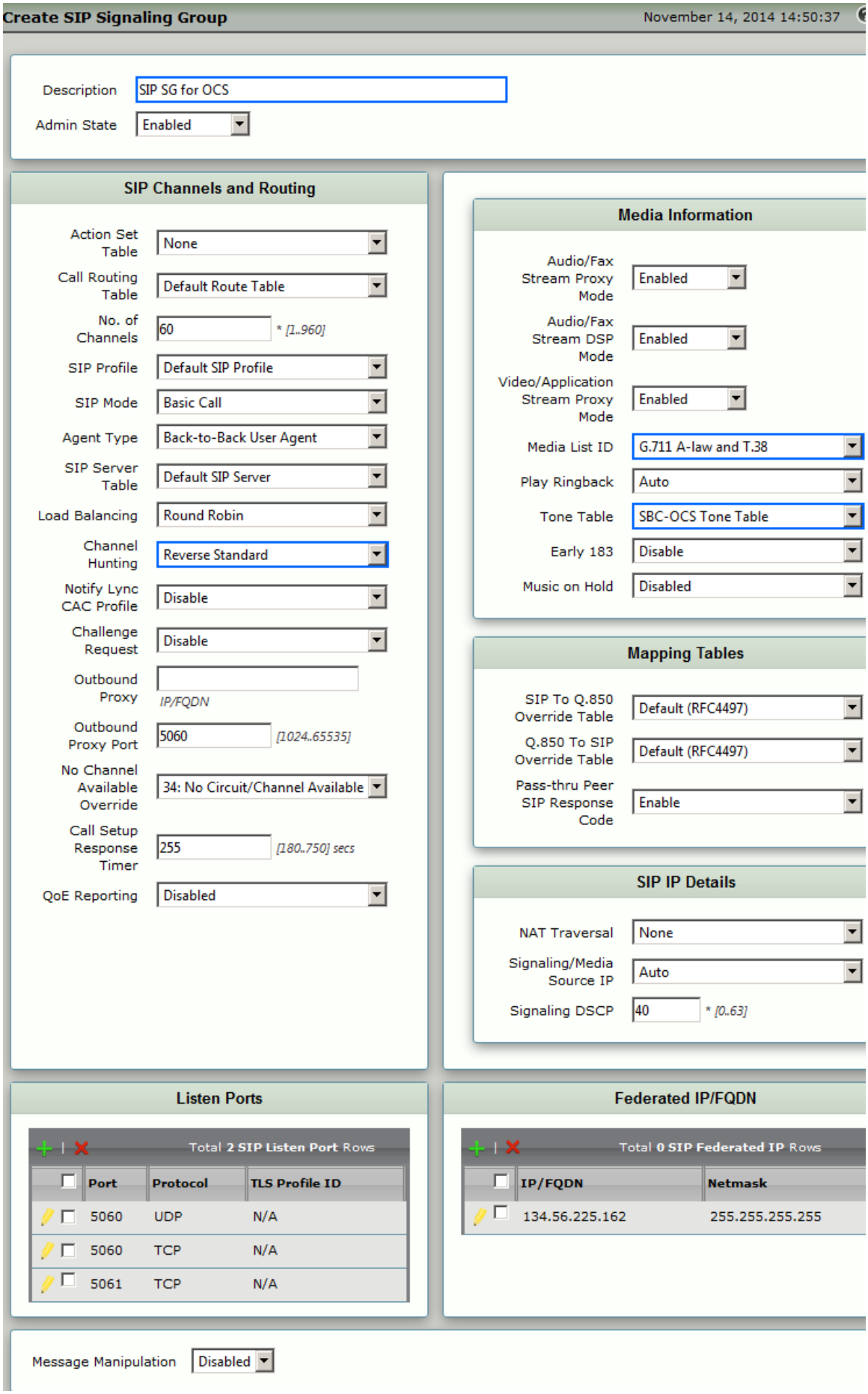
Routing Calls from PSTN Endpoints



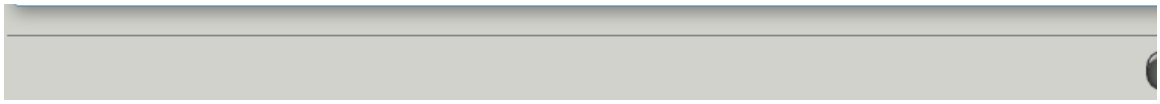
Signaling Groups

Signaling Groups for OCS

Copyright © 2015 Sonus Networks. All rights reserved.

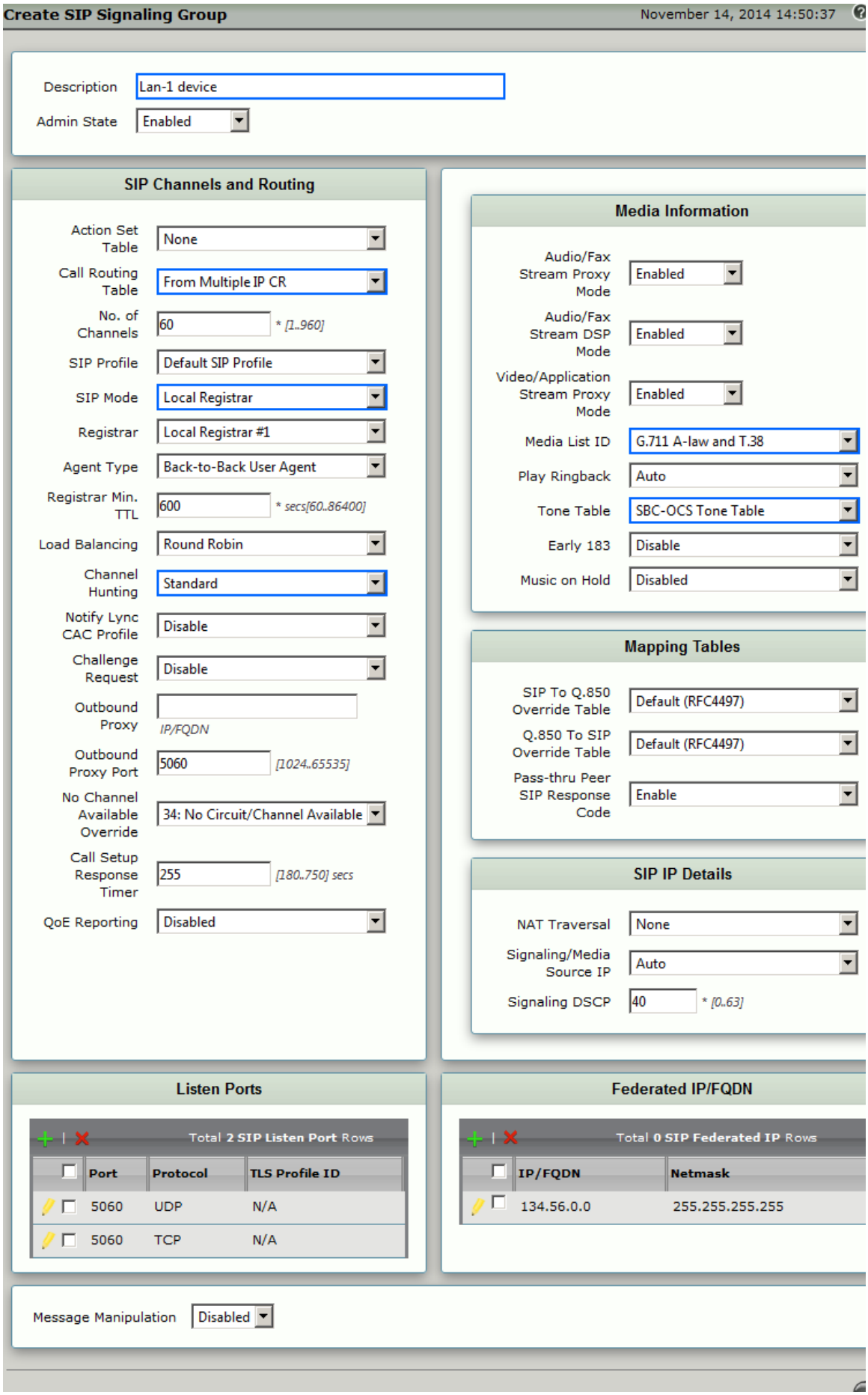


Copyright © 2015 Sonus Networks. All rights reserved.



Signaling Groups for LAN-1 endpoints

Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.

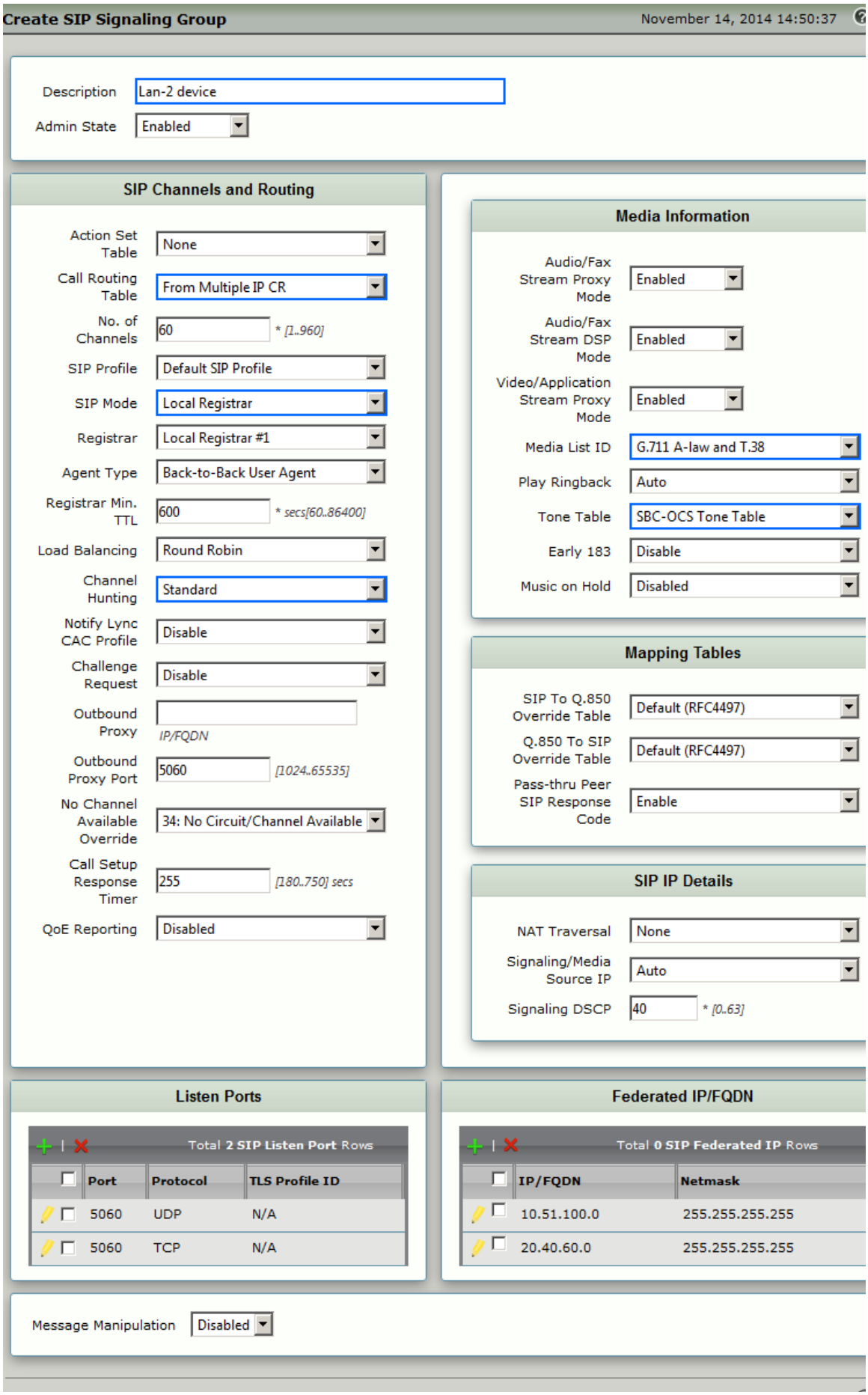
Signaling Groups for LAN-2 endpoints

This signaling group refers to the IP subnet used between Sonus SBC 1000/2000 and the SIP trunking provider. There are two subcases here.

If there is a NAT device between Sonus SBC 1000/2000 and the SIP-trunking peer, then **NAT Traversal** must be set to **STATIC NAT** and the public IP address of the NAT `20.40.60.89` must be specified as the **Application IP**. In addition, the NAT device should be configured such that it translates between the private address of `10.51.100.89` and the public address of `20.40.60.89`.

If there is no NAT device between Sonus SBC 1000/2000 and the SIP-trunking peer, then **NAT Traversal** must be set to **NONE** as shown below:

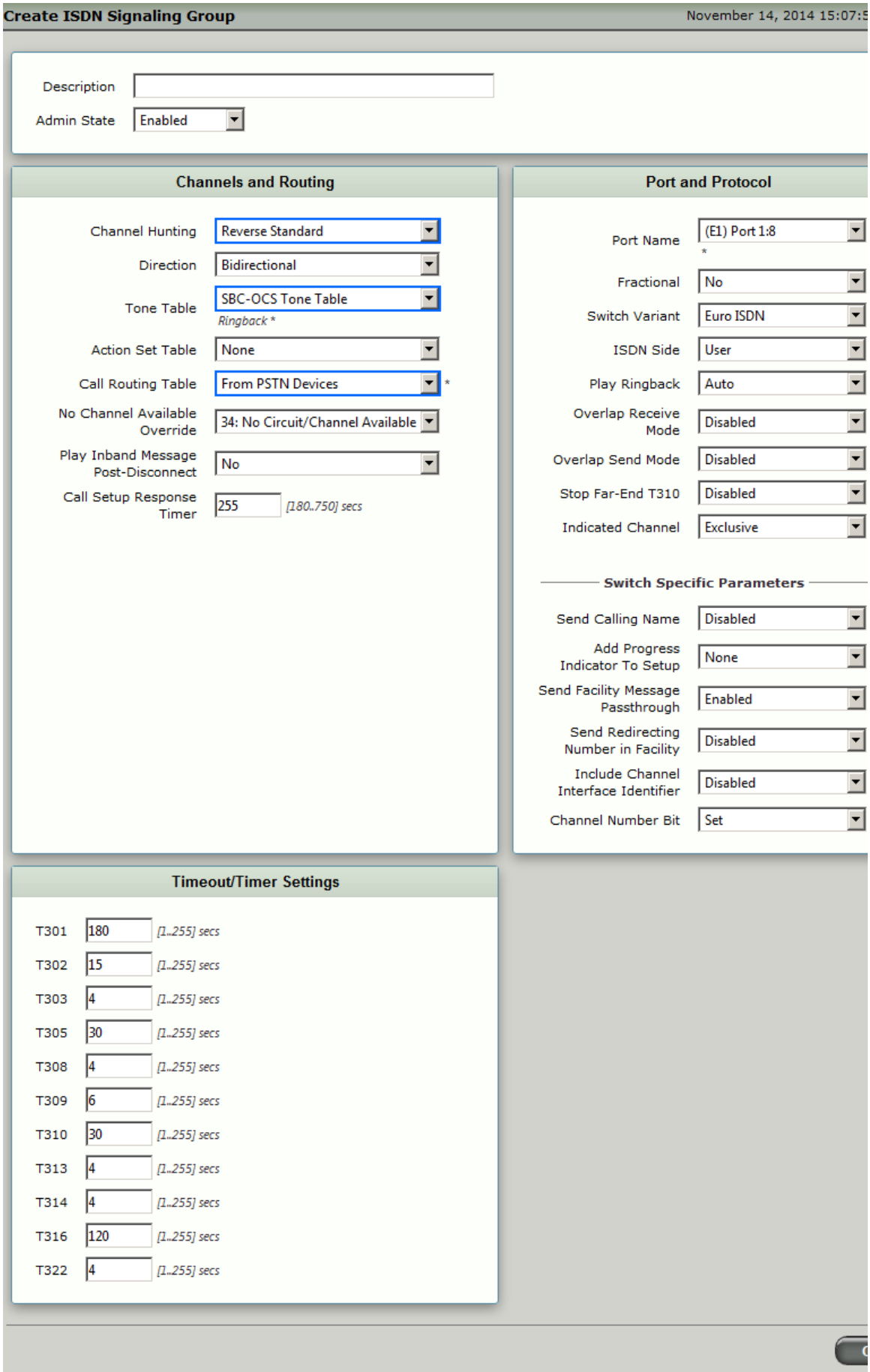
Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.

Signaling Group for PSTN endpoints

Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.

Configuring the Sonus SBC 1000-2000 for Music On Hold

This article shows you how to setup the Sonus SBC 1000/2000 to use the Music-on-Hold feature. Configuring the Music-on-Hold feature is a relatively straight-forward process that involves the following overall steps:

1. Providing a sound source by either uploading a sound file to the Sonus SBC 1000/2000 or by connecting a *live* audio source through an FXS port.
2. Specify the source.
3. Enable the Music-on-Hold Service.

System and Music File Requirements

- The Sonus SBC 1000/2000 must be running version 2.1 or later.
- Music files must be one of the following formats:
  - WAV
  - PCMA
  - PCMU
  - PCM
  - G726

Platform	Max. File Size
Sonus SBC 1000	1MB
Sonus SBC 2000	4MB

Providing The Audio Source

To upload a music (sound) file :
Upload the file using the **Uploading a Sound File** procedure in Configuring the Media System.

To connect a live audio source through an FXS port:

- Specify the live audio source using the **Specifying a Live Audio Source** procedure in Configuring the Media System.

Connecting an audio source for Music On Hold requires the use of an adapter between the Sonus SBC 1000/2000 RJ11 port and the source device (CD player, radio, iPod. MP3 player, personal computer, etc.). Common adapters include a 3.5mm connector on one end and an RJ11 on the other with an isolation transformer between the two.

Music On Hold volume is controlled from the audio source device (iPod, MP3 Player, etc.). The preferred volume level can be adjusted by listening to the stream, or by examining the RTP trace captured from the SIP call leg of the call. Use the receive gain settings on the FXS port to make any additional fine-tuning volume adjustments.

Selecting the Music-on-Hold Mode

To use Music on Hold, you must specify a source in the Media System Configuration page of the UI and then Enable Music on Hold in the applicable SIP Signaling Group.

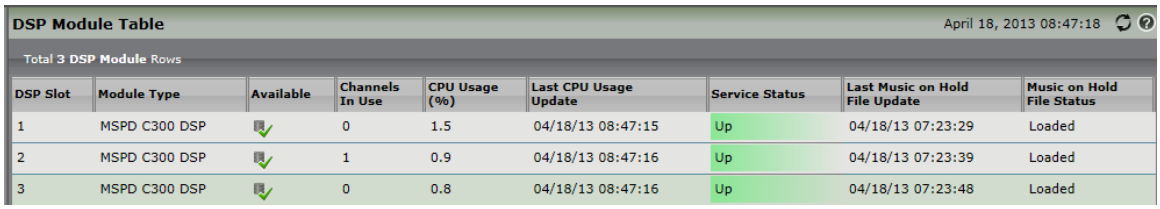
Verifying Music Upload Status and FXS Music-on-Hold source.

To verify that the file has been successfully uploaded:

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > DSPs**

The Music on Hold status will be ***Loaded*** if the file was successfully uploaded.



DSP Module Table — April 18, 2013 08:47:18

Total 3 DSP Module Rows

DSP Slot	Module Type	Available	Channels In Use	CPU Usage (%)	Last CPU Usage Update	Service Status	Last Music on Hold File Update	Music on Hold File Status
1	MSPD C300 DSP		0	1.5	04/18/13 08:47:15	Up	04/18/13 07:23:29	Loaded
2	MSPD C300 DSP		1	0.9	04/18/13 08:47:16	Up	04/18/13 07:23:39	Loaded
3	MSPD C300 DSP		0	0.8	04/18/13 08:47:16	Up	04/18/13 07:23:48	Loaded

Other status' are:

- Not Loaded
- Load Fail

> **Note:**
>
> If your system does not have transcoding licenses, be sure your MOH file is encoded in the same Law as your calls use. For instance, if you're using A-Law for your calls, be sure to use an A-law encoded MOH file.
>
> If your system has transcoding licenses, then the system will automatically transcode between different types of codec compressions.

Configuring the Sonus SBC 1000-2000 for Standard and Mutual TLS Authentication

This article describes the steps necessary to configure the Sonus SBC 1000/2000 for Standard and Mutual TLS (MTLS).

On this Page

- Standard TLS
  - Overview
  - Standard TLS handshake
  - Sonus SBC 1000/2000 Configuration for Standard TLS
- Mutual TLS (MTLS)
  - MTLS Overview
  - MTLS Illustration Notes
  - Sonus SBC 1000/2000 Configuration for MTLS

Related Articles

- Creating and Modifying TLS Profiles

Standard TLS

Overview

Transport Layer Security (TLS) is a cryptographic protocol providing communication security over the Internet which

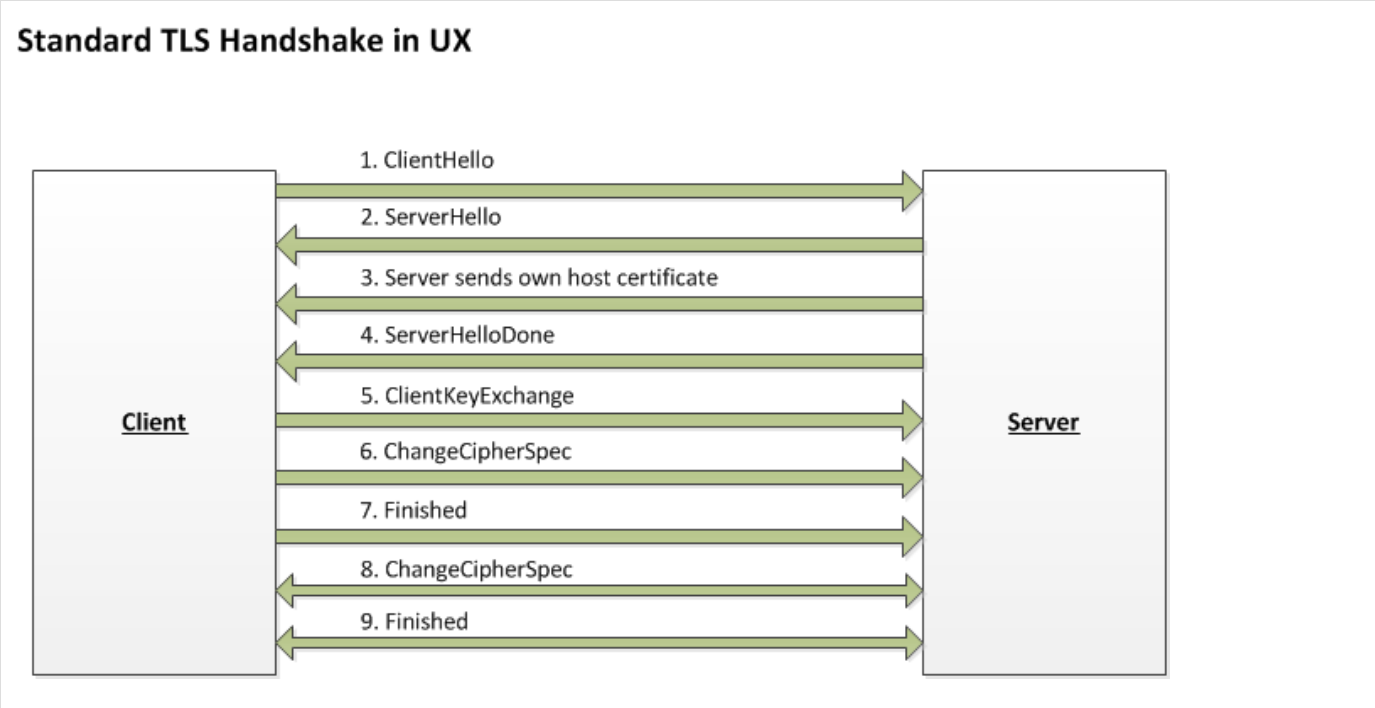
Copyright © 2015 Sonus Networks. All rights reserved.

is designed to prevent eavesdropping and tampering. In TLS, the server proves its identity to the client.

Standard TLS handshake

1. The client sends a ClientHello message with a list of the supported cipher suites, random number, the supported TLS versions and the compression methods.
2. The server sends a ServerHello message with the TLS version, a random number, the strongest cipher suite, and a compression method from the client's list.
3. The server sends its own certificate.
4. The server sends a ServerHelloDone message.
5. The client sends a key depending on the cipher selected, and then begins computing the master secret.
6. The client sends the ChangeCipherSpec message - authentication and encryption starts.
7. The client sends its Finished message, which the server decrypts and verifies.
8. The server sends a ChangeCipherSpec message, which the client decrypts and verifies.
9. The server sends a Finished message.

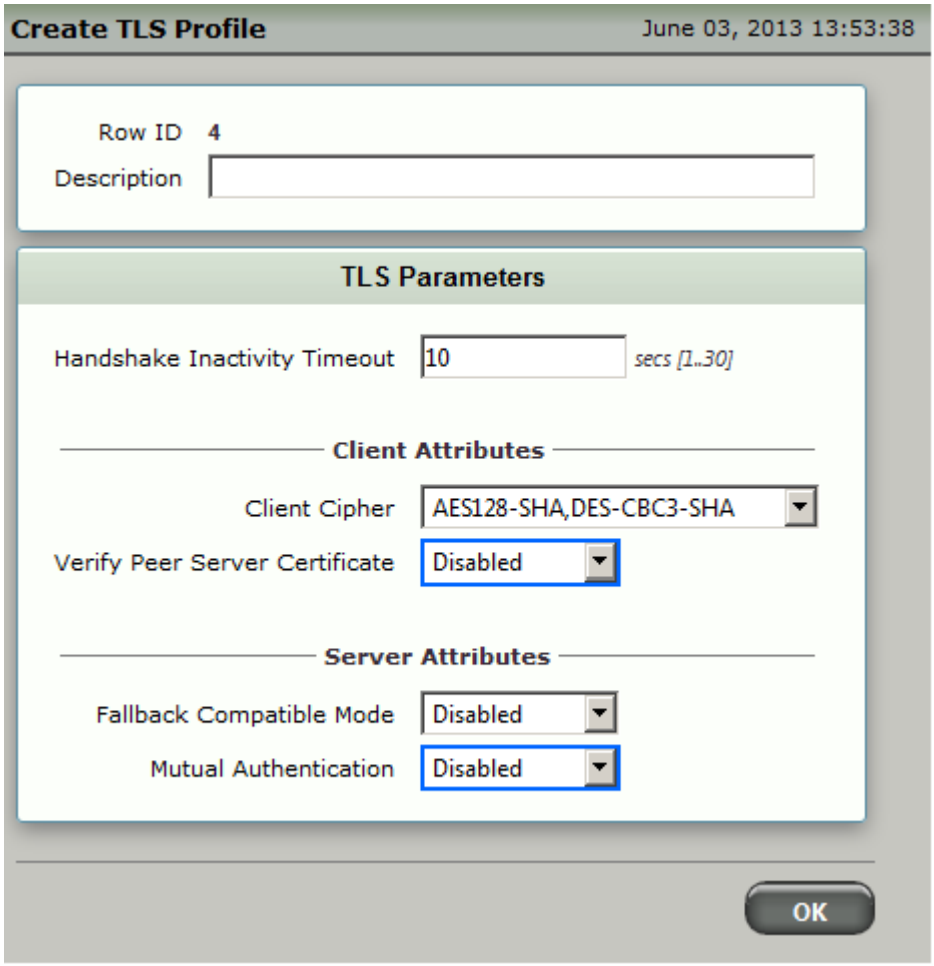
The encrypted application messages then start flowing until the session ends.



Sonus SBC 1000/2000 Configuration for Standard TLS

In order to configure Sonus SBC 1000/2000 for standard TLS, both **Mutual Authentication** and **Verify Peer Server Certificate** fields in the TLS Profile must be set to **Disabled**.

Copyright © 2015 Sonus Networks. All rights reserved.



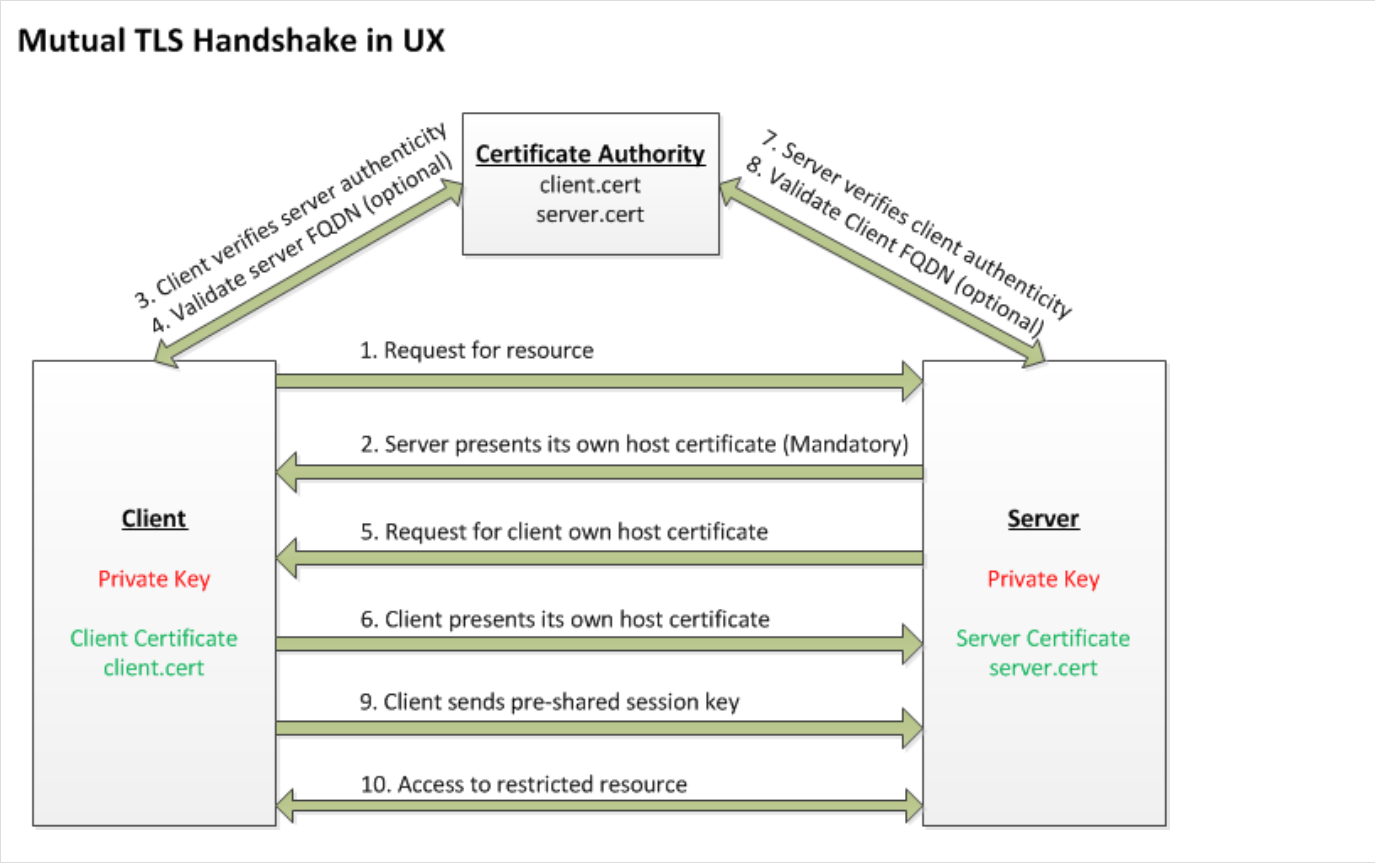
Note that enabling **Fallback Compatibility Mode** will allow reversion of the connection to an earlier, less secure, version of TLS (for example to SSLv3), thus weakening the security level. For more information, refer to Creating and Modifying TLS Profiles.

Mutual TLS (MTLS)

MTLS Overview

Mutual TLS provides mutual identity authentication of the server and the client through the exchange and verification of their digital certificates.

Copyright © 2015 Sonus Networks. All rights reserved.



Verify Peer Server Certificate can only be disabled if MTLS is disabled.

MTLS Illustration Notes

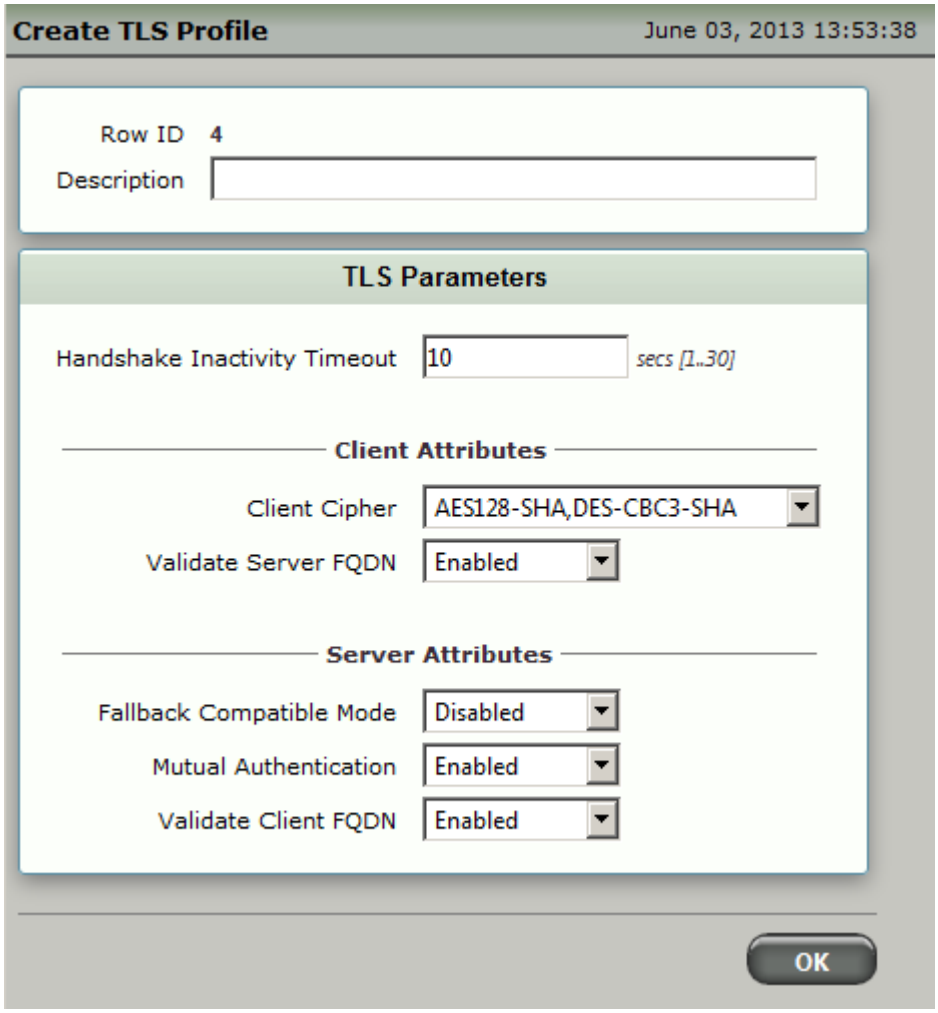
Step 3 - Always takes place when Mutual Authentication is enabled. If MTLS is disabled, then **Verify Peer Server Certificate** can be disabled.
Step 4 - This action takes place when MTLS is enabled and **Validate Server FQDN** is enabled. If **Verify Peer Server Certificate** is disabled, the **Validate Server FQDN** is also disabled. **Validate Server FQDN** is an enhanced security feature of Sonus SBC 1000/2000, which can be disabled if the common name in the certificate is an IP address (some ITSP's do that). The **Validate Server FQDN Enabled** option allows Sonus SBC 1000/2000 to perform an FQDN match of an incoming peer certificate CN or SAN against the host configured in the SIP Server table of Sonus SBC 1000/2000 (protocol must be TLS and the Host FQDN).
Steps 5, 6, 7 and 8 - If MTLS is enabled, steps 5, 6, and 7 are mandatory and point 8 could be made optional but the steps 5 through 8 are performed by default. If MTLS is disabled, steps 5 through 8 will not be performed.
Step 8 - This action takes place when MTLS is enabled and **Validate Client FQDN** is enabled. If MTLS is disabled, the **Validate Client FQDN** is also disabled. **Validate Client FQDN** is an enhanced security feature of Sonus SBC 1000/2000, which can be disabled if the common name in the certificate is an IP address (some ITSP's do that). The **Validate Client FQDN Enabled** option allows Sonus SBC 1000/2000 to perform an FQDN match of an incoming peer certificate CN or SAN against a reverse DNS lookup of the IP address to an FQDN.

Sonus SBC 1000/2000 Configuration for MTLS

In order to configure Sonus SBC 1000/2000 for MTLS, you must enable Mutual Authentication.

If you want to validate the client FQDN, you must enable **Validate Client FQDN**.

Copyright © 2015 Sonus Networks. All rights reserved.



If you want to check and verify the TLS profile that was used, you must capture a debug log of the SIP subsystem at DEBUG level and search for the **TLS Profile** string. The example log below is when MTLS is enabled and client and server FQDN validation is disabled, for example when ITSP uses an IP address instead of a FQDN in the CN of the certificate:

```
Dump: TLS Client socket uses TLS Profile #1 'ITSP TLS Profile' {ver=TLS1,
mutual=Yes, validate client:server FQDN=No:No, verify peer=Yes, cipher=AES128 &
3DES Sha, selfsigned=No
```

Translating SIP Responses in SIP-SIP Calls Using "Pass-thru Peer SIP Response Code"

In this article, we describe how to translate SIP response in SIP to SIP calls using "Pass-thru Peer SIP Response Code".

On this Page:

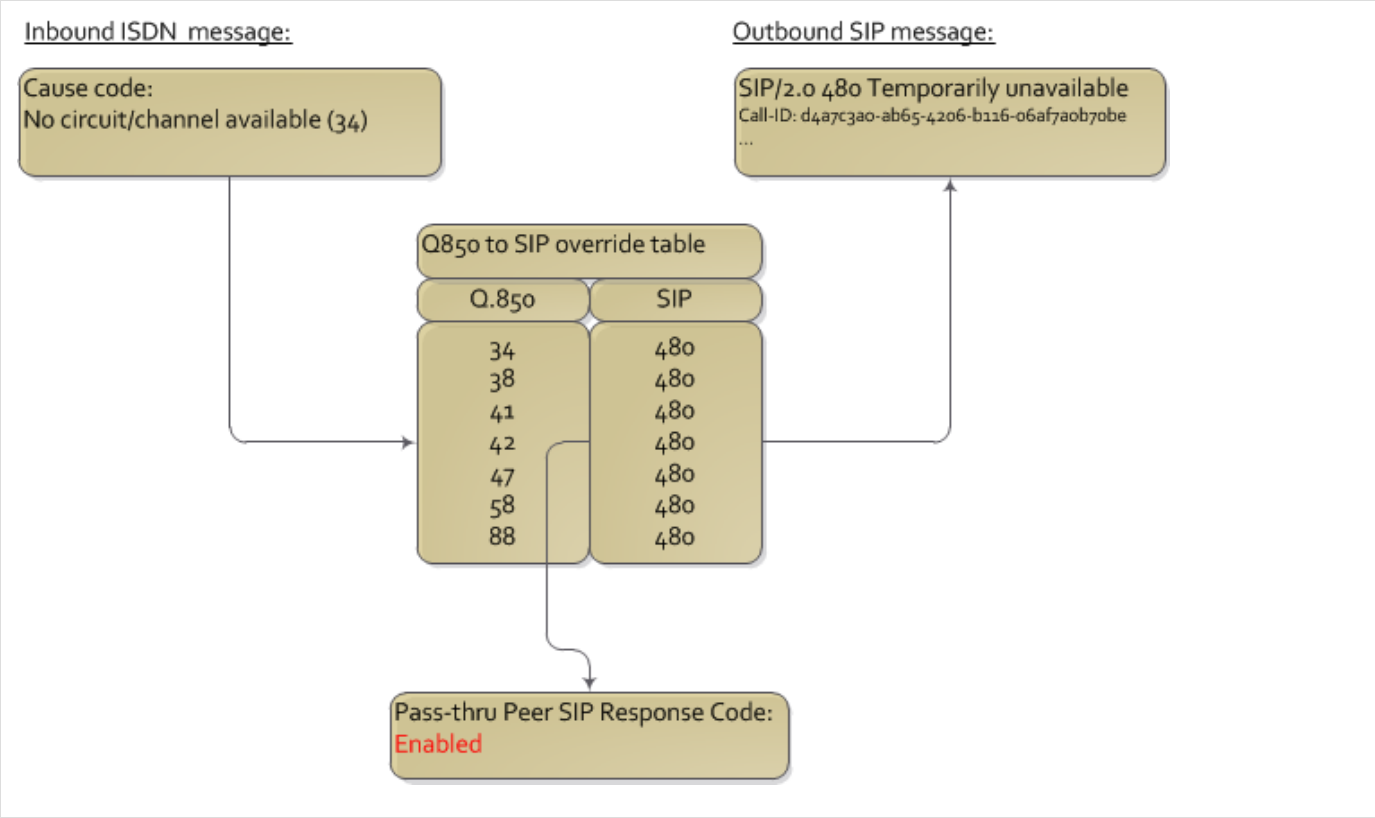
- Background and Overview
- Sonus SBC 1000/2000 Configuration
  - General Overview of the Configuration
  - Default Q.850 to SIP and SIP to Q.850 Mapping Tables in Sonus SBC 1000/2000
  - Sonus SBC 1000/2000 Configuration

Copyright © 2015 Sonus Networks. All rights reserved.

Background and Overview

By default, SIP responses received are passed through from one SIP peer to another by the Sonus SBC 1000/2000. The default Q.850 to SIP and SIP to Q.850 mapping tables fully conform with RFC4497. With the help of these two override tables, you can change the default mapping for any SIP response to and from any Q.850 cause.

For example, in the default Q.850 to SIP override table, QSIG Cause Codes 34, 38, 41, 42, 47, 58, and 88 map to 503 Service Unavailable. A problem occurs when the Sonus SBC 1000/2000 receives Cause Code 34 from the PSTN. The Sonus SBC 1000/2000 maps it to 503 Service Unavailable, which causes Lync to declare the Sonus SBC 1000/2000 gateway unavailable with Event ID 46046. In this case, the Sonus SBC 1000/2000 administrator may want to override the default mapping in order to prevent Lync from flagging the whole gateway as unavailable. Consider the following illustration.



This article expands more on this practice, and describes how to configure the Sonus SBC 1000/2000 to perform custom SIP response mapping for SIP to SIP calls.

Related Articles

- RFC4497
- Calls to PSTN numbers fail. Lync declares the gateway unavailable with Event ID 46046
- Managing Q.850 to SIP Override Tables
- Managing SIP to Q.850 Override Tables

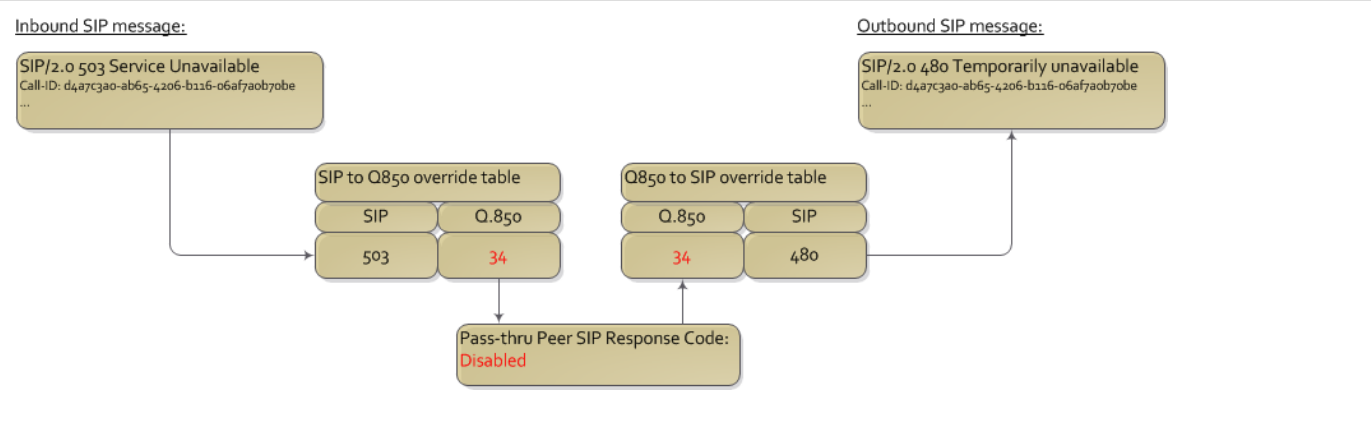
Sonus SBC 1000/2000 Configuration

General Overview of the Configuration

In this example we use the SIP to Q850 and Q850 to SIP Override Tables. Upon receiving a SIP response, the

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000/2000 uses the SIP to Q850 Override Table to map the SIP response to a Q850 Cause Code. Once the Q850 Cause Code is found, the Sonus SBC 1000/2000 uses the Q850 Cause Code, via the Q850 to SIP mapping table, to map it to a SIP response. This behavior is achieved when the default Pass-through SIP Response Code feature is disabled.



Default Q.850 to SIP and SIP to Q.850 Mapping Tables in Sonus SBC 1000/2000

SIP response	Q.850 Cause value
400 Bad Request	41 Temporary Failure
401 Unauthorized	21 Call rejected
402 Payment required	21 Call rejected
403 Forbidden	21 Call rejected
404 Not found	1 Unallocated number
405 Method not allowed	63 Service or option unavailable
406 Not acceptable	79 Service/option not implemented
407 Proxy authentication required	21 Call rejected
408 Request timeout	102 Recovery on timer expiry
410 Gone	22 Number changed (w/o diagnostic)
413 Request Entity too long	127 Interworking
414 Request-URI too long	127 Interworking
415 Unsupported media type	79 Service/option not implemented
416 Unsupported URI Scheme	127 Interworking
420 Bad extension	127 Interworking

Copyright © 2015 Sonus Networks. All rights reserved.

421 Extension Required	127 Interworking
423 Interval Too Brief	127 Interworking
480 Temporarily unavailable	18 No user responding
481 Call/Transaction Does not Exist	41 Temporary Failure
482 Loop Detected	25 Exchange - routing error
483 Too many hops	25 Exchange - routing error
484 Address incomplete	28 Invalid Number Format
485 Ambiguous	1 Unallocated number
486 Busy here	17 User busy
487 Request Terminated	127 Interworking
488 Not Acceptable Here	65 Bearer capability not implemented
500 Server internal error	41 Temporary failure
501 Not implemented	79 Not implemented, unspecified
502 Bad gateway	38 Network out of order
503 Service unavailable	41 Temporary failure
504 Server time-out	102 Recovery on timer expiry
505 Version Not Supported	127 Interworking
513 Message Too Large	127 Interworking
600 Busy everywhere	17 User busy
603 Decline	21 Call rejected
604 Does not exist anywhere	1 Unallocated number
606 Not acceptable	31 Normal, unspecified

Q.850 Cause value	**SIP response**
1 Unallocated number	404 Not Found
2 No route to network	404 Not found

Copyright © 2015 Sonus Networks. All rights reserved.

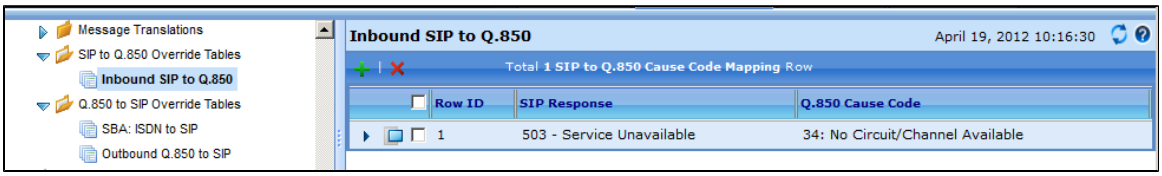
3 No route to destination	404 Not found
16 Normal call clearing	result in a BYE or CANCEL
17 User busy	486 Busy here
18 No user responding	408 Request Timeout
19 No answer from the user	480 Temporarily unavailable
20 Subscriber absent	480 Temporarily unavailable
21 Call rejected (location - user)	603 Forbidden
21 Call rejected (location - nonuser)	403 Forbidden
22 Number changed (w/o diagnostic)	410 Gone
22 Number changed (w/ diagnostic)	301 Moved Permanently
23 Redirection to new destination	410 Gone
26 Non-selected user clearing	404 Not Found
27 Destination out of order	502 Bad Gateway
28 Address incomplete	484 Address incomplete
29 Facility rejected	501 Not implemented
31 Normal unspecified	480 Temporarily unavailable
34 No circuit available	503 Service unavailable
38 Network out of order	503 Service unavailable
41 Temporary failure	503 Service unavailable
42 Switching equipment congestion	503 Service unavailable
46 Precedence call blocked	480 Temporarily unavailable
47 Resource unavailable	503 Service unavailable
55 Incoming calls barred within CUG	403 Forbidden
57 Bearer capability not authorized	403 Forbidden
58 Bearer capability not presently	503 Service unavailable available
65 Bearer capability not implemented	488 Not Acceptable Here

Copyright © 2015 Sonus Networks. All rights reserved.

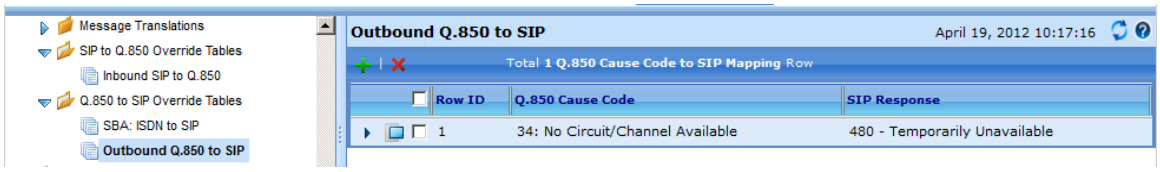
69 Requested facility not implemented	501 Not implemented
70 Only restricted digital avail	488 Not Acceptable Here
79 Service or option not implemented	501 Not implemented
87 User not member of CUG	403 Forbidden
88 Incompatible destination	503 Service unavailable
102 Recovery of timer expiry	504 Gateway timeout
111 Protocol error	500 Server internal error
127 Interworking unspecified	500 Server internal error

Sonus SBC 1000/2000 Configuration

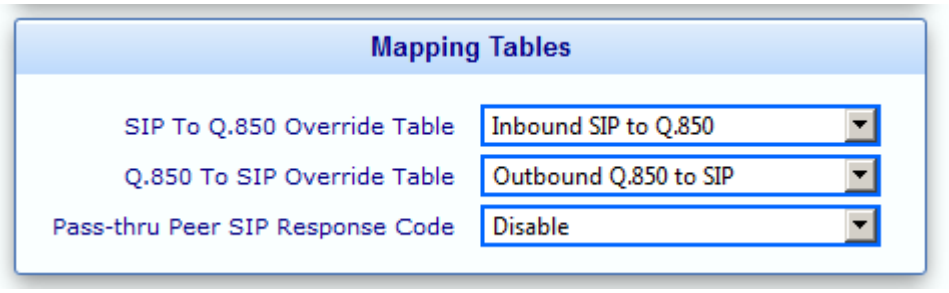
- Create a SIP to Q.850 mapping table, which will be used to match the SIP Response to a Q.850 Cause Code for **inbound** calls.



- Create a Q.850 to SIP mapping table, which will be used to match the Q.850 Cause Code to SIP Response for **outbound** calls.



- Disable Pass-through Peer SIP Response Code and select the two mapping tables.



Configuring Sonus SBC1000-2000 for Calling Party Category II-8 based Collect Call Blocking

Copyright © 2015 Sonus Networks. All rights reserved.

This article describes the steps necessary to configure the Sonus SBC 1000/2000 to block collect incoming R2 calls. At the time this article was written, Brazil is the only country using this methodology for blocking collect calls.

Collect call blocking uses the R2 **_Calling Party Category**- to accomplish the block. For an incoming R2 call to the Sonus SBC 1000/2000, the switch sends a called number and a Calling Party Category (CPC) of II-8. To accomplish the block, the Sonus SBC 1000/2000 must reject the called number that was received. Therefore, in advance, the Sonus SBC 1000/2000 is configured to reject certain number(s), and does so with a specific cause code. Instead of responding with a B-4 for call rejection, the Sonus SBC 1000/2000 responds with a B-7 to indicate collect call blocking.

On this Page

- Before You Begin
- Sonus SBC 1000/2000 Configuration
  - Transformation Table
  - Action Configuration
  - Action Sets
  - R2 incoming Signaling Group

Related Articles

None

Before You Begin

Verify the following:

- Confirm that the switch is configured to use CPC of II-8 to indicate collect calling.
- Identify the number(s) on which the Sonus SBC 1000/2000 will receive a collect call.
- Follow the configuration steps below.

Sonus SBC 1000/2000 Configuration

This section assumes that the user is familiar with basic R2 call setup and routing in the Sonus SBC 1000/2000.

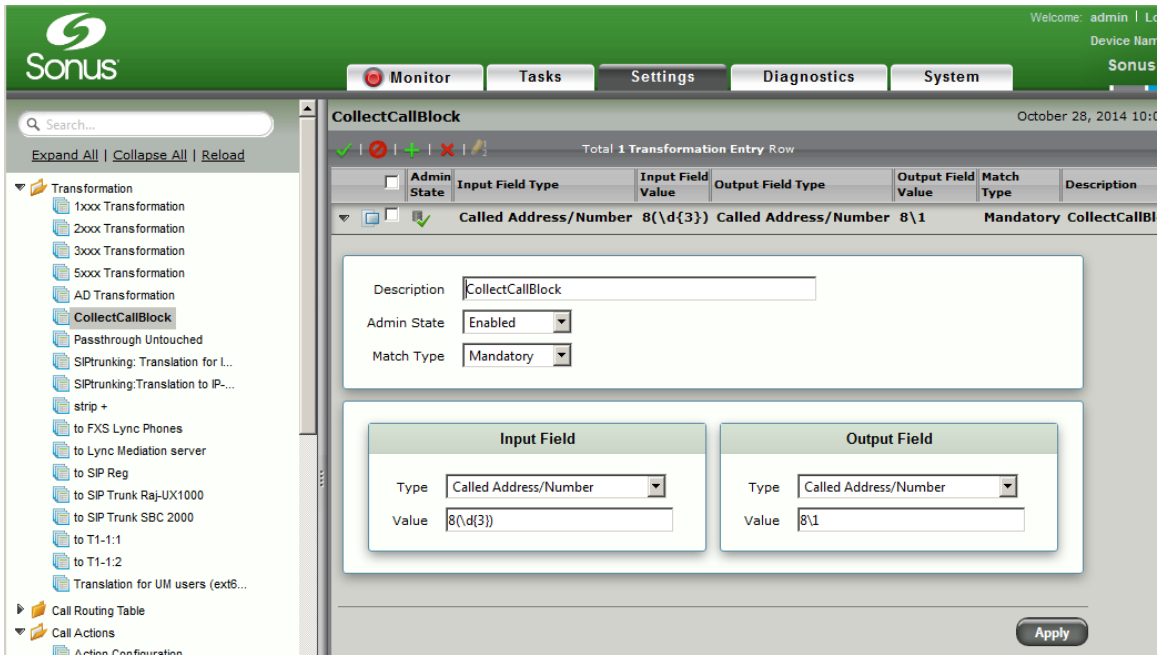
The configuration process comprises four major actions:

- Create and configure a transformation table and transformation table entry for collect call blocking.
- Create a call action.
- Create and configure an action set.
- Create and configure a signaling group.

Transformation Table

Define, using regular expressions, the called number(s) that the Sonus SBC 1000/2000 receives collect calls on. In the following example, any four digit number beginning with 8 (e.g., 8888) is matched to the regular expression defined in the Input Value Field (this number will be rejected by Sonus SBC 1000/2000). The Input and Output Fields have the same value.

Copyright © 2015 Sonus Networks. All rights reserved.

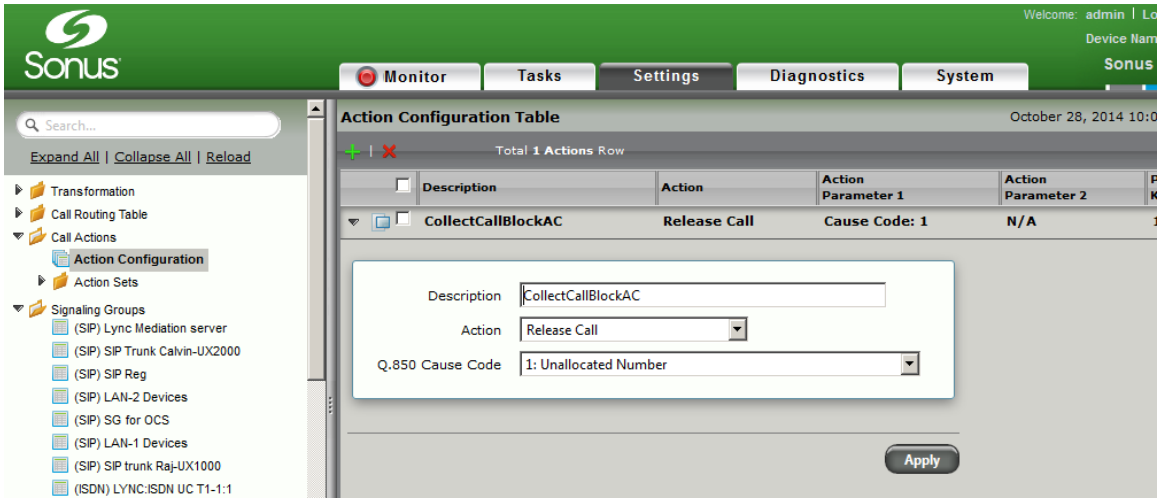


To create and configure the transformation:

1. Add a transformation.
2. Name the table ***CollectCallBlock***.
3. Add an entry to the transformation table using the following information:
    a. **Admin State:** Enabled.
    b. **Match Type:** Mandatory.
    c. **Input Field - Type:** Called Address/Number.
    d. **Input Field - Value:** 8(\d{3})
    e. **Output Field - Type:** Called Address/Number.
    f. **Output Field - Value:** 8\1

Action Configuration

Define an action configuration which, if matched, acts as defined. In this case, the action configuration releases the call with a cause code of **1: Unallocated Number**. This cause code MUST be defined.



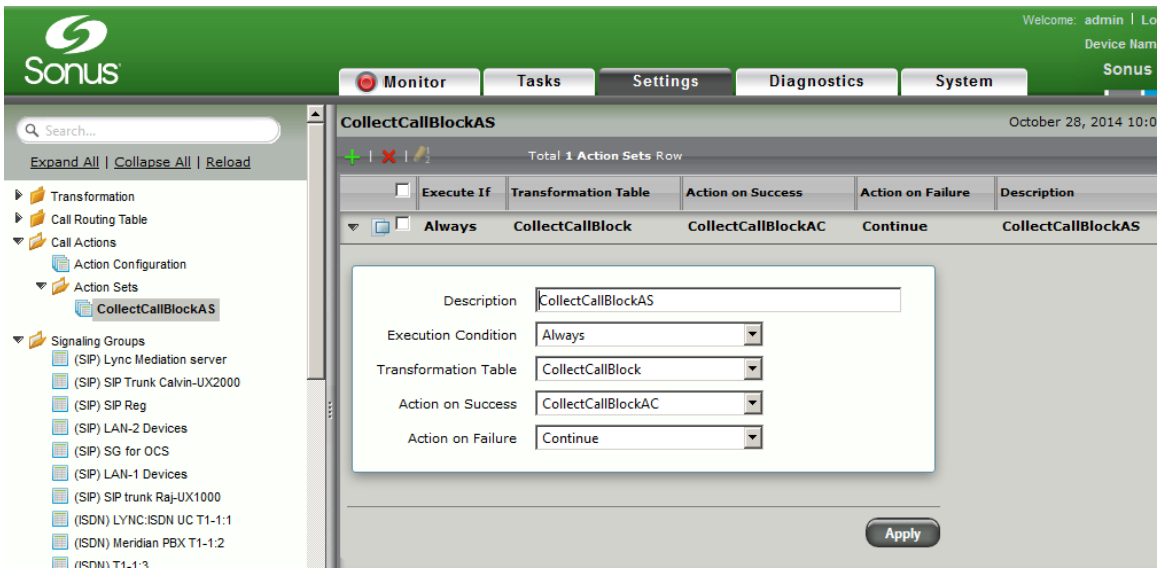
Copyright © 2015 Sonus Networks. All rights reserved.

To create the action configuration:

1. Add an action configuration using the following information:
    a. **Description:** CollectCallBlockAC.
    b. **Action:** Release Call.
    c. **Q.850 Cause Code:** 1. Unallocated Number.

Action Sets

Create an action set and define an entry to that action set which ties the transformation number(s) to the action configuration. Using this action set, if the Sonus SBC 1000/2000 receives any of the numbers defined in the transformation table above, it rejects the call with the cause code of 1: Unallocated Number.



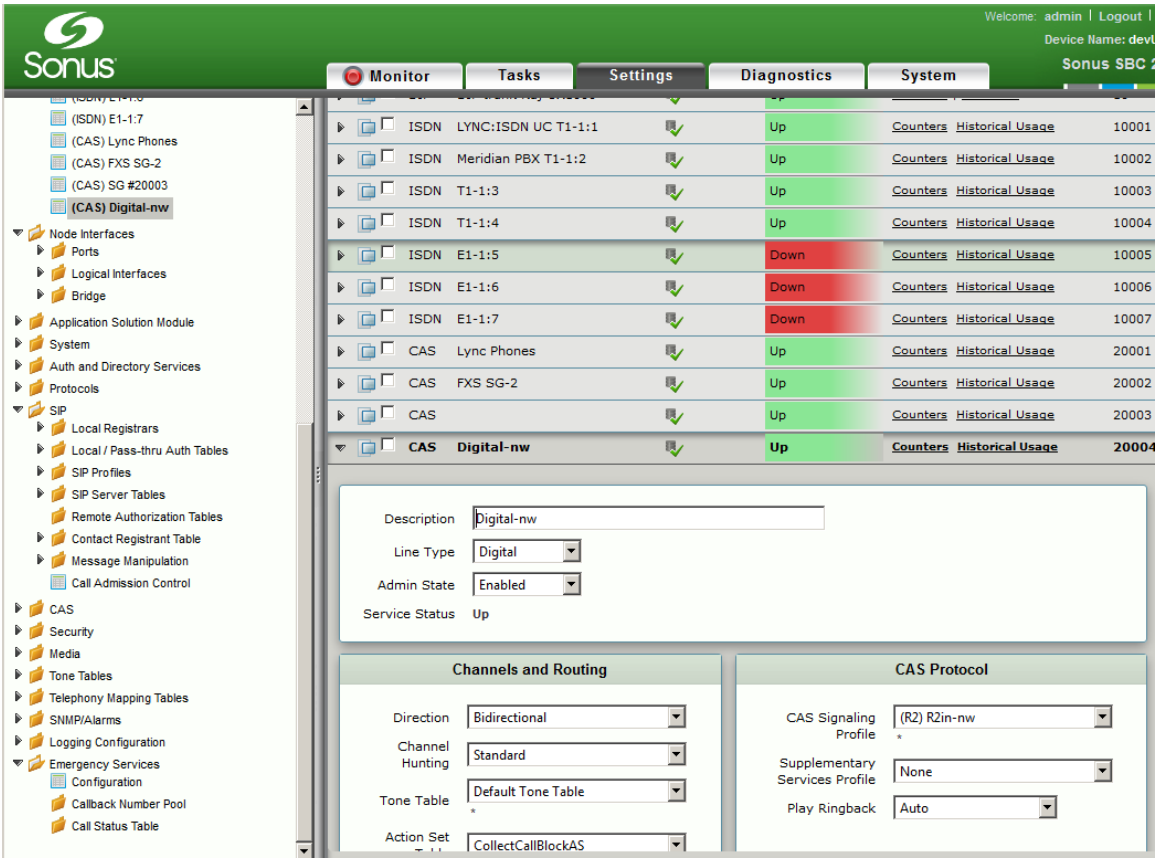
To create the action set and add the entry:

1. Create an action set table using the following information:
    a. **Description:** CollectCallBlockAS.
2. Add an entry to the table using the following information:
    a. **Description:** CollectCallBlock - action set.
    b. **Execution Condition:** Always.
    c. **Transformation Table:** CollectCallBlock.
    d. **Action on Success:** CollectCallBlockAC.
    e. **Action on Failure:** Continue.

R2 incoming Signaling Group

Assign the above action set in the incoming R2 Signaling Group definition for Action Set Table. This procedure assumes that the signaling group and the CAS signaling profile have already been created and configured. This procedure only adds the Action set to this pre-defined signaling group.

Copyright © 2015 Sonus Networks. All rights reserved.



To add the action set to the signaling group:

1. Modify the existing incoming CAS-R2 inbound signaling group using the following information:
    a. **Channels and Routing - Action Set Table:** CollectCallBlockAS.

Use of Calling Extension in Transformation Table for ext=xxxx Input Value

On This Page

- Overview
- Topology
    - Use Case
- Scenario
- Resolving the Issue

Related Articles

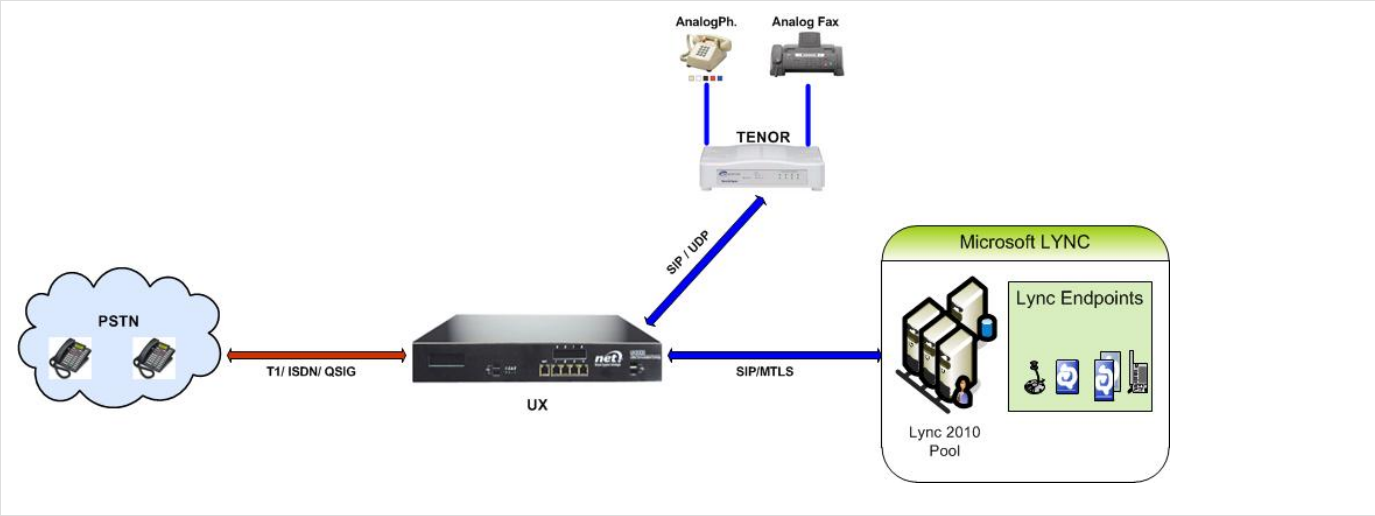
- Deploying the SBC 1000-2000 and Lync with a PSTN Provider
- Using Tenor as an Analog Device in a Lync SBC SBA Deployment
- Creating and Modifying Entries to Transformation Tables
- Creating Call Routing Logic with Regular Expressions

Overview

Copyright © 2015 Sonus Networks. All rights reserved.

- This article describes the configuration and settings necessary for removing Calling Extension/Called Extension in a Transformation Table for ext=xxxx input value.
- This document assumes that **PSTN - Sonus SBC 1000/2000 - Microsoft Lync 20XX** setting is completed in following topology. For these settings, refer to Deploying the SBC 1000-2000 and Lync with a PSTN Provider.

Topology



Use Case

In some cases, Lync users may be created with a Line URI with **tel:+XXXXXXXXXXX;ext=XXXX** format as shown below:



In such situations, when a call is received from the Lync Mediation Server, the INVITE message contains **;ext=xxxx** in the Request URI. However, in a LYNC >> Sonus SBC 1000/2000 >> Tenor call setup, TENOR expects the REQUEST URI without **ext=xxxx**, therefore Sonus SBC 1000/2000 will have to remove from the **TO HEADER** by using a Transformation Table.

To do so, please follow the steps below:

Scenario

- Lync sends an INVITE to the Sonus SBC 1000/2000:

Copyright © 2015 Sonus Networks. All rights reserved.

```
INVITE sip:+15102039002;ext=9002@testux203.vxtestlab.com;user=phone SIP/2.0
FROM:
"ux227-203-user2"<sip:+15102031002;ext=1002@FES1-W14.vxtestlab.com;user=phone>;epid=B2F0A127

TO: <sip:+15102039002;ext=9002@testux203.vxtestlab.com;user=phone>


CSEQ: 197589 INVITE
CALL-ID: e60f1373-93a3-44e8-985f-b1f0c03ebb69
```

- SIP Registered Tenor endpoint expects the INVITE from the Sonus SBC 1000/2000:

```
INVITE sip:9002@134.56.227.217:5085;user=phone SIP/2.0
From: "ux227-203-user2" <sip:+15102031002@134.56.227.203:5060;user=phone>;tag=8638e3cb-5f

TO:<sip:9002@134.56.227.217;user=phone>


CSEQ: 197589 INVITE
Call-ID: call-BD0D1C00-0000-0010-0C13-C@134.56.227.203
```

However, if **ext=xxxx** is not removed from the TO HEADER, the Sonus SBC 1000/2000 sends out an INVITE to the Tenor with:

```
INVITE sip:9002;ext=9002@134.56.227.217:5085;user=phone SIP/2.0


From: "ux227-203-user2"
<sip:+15102031002;ext=1002@134.56.227.203:5060;user=phone>;tag=8638e3cb-12b

To: <sip:9002;ext=9002@134.56.227.217;user=phone>


CSEQ: 1 INVITE
Call-ID: call-F96B1300-0000-0010-0C13-8@134.56.227.203
```

... and the call fails with:

```
SIP/2.0 503 Service Unavailable


Call-ID: call-F96B1300-0000-0010-0C13-8@134.56.227.203
Content-Length: 0
CSeq: 1 INVITE
From:
"ux227-203-user2"<sip:+15102031002;ext=1002@134.56.227.203:5060;user=phone>;tag=8638e3cb-12b

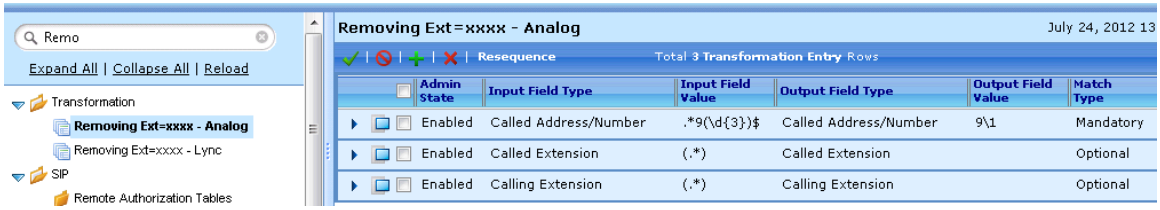
To: <sip:9002;ext=9002@134.56.227.217;user=phone>;tag=8638e3d9-18
User-Agent: Quintum/1.0.0 SN/0030E1209173 SW/P108-09-14-Lync
Via: SIP/2.0/TCP 134.56.227.203:5060;branch=z9hG4bK-Sonus SBC 1000/2000-8638-e3cb-00d0
```

Resolving the Issue

To resolve the issue:

Copyright © 2015 Sonus Networks. All rights reserved.

Remove the Extension Number in the relevant Transformation Table *(in this example we are showing how to remove Calling as well as Called Extension Numbers)* as shown below:



Subsequently if the above call is placed again, the transformation table will modify the TO header and remove **ext=xxxx** which then allow call to be successful as shown below:

Inbound INVITE

INVITE sip:+15102039002;ext=9002@testux203.vxtestlab.com;user=phone SIP/2.0

FROM:
"ux227-203-user2"<sip:+15102031002;ext=1002@FES1-W14.vxtestlab.com;user=phone>;epid=B2F0A127

TO: <sip:+15102039002;ext=9002@testux203.vxtestlab.com;user=phone>

CSEQ: 197673 INVITE
CALL-ID: 6a8e8f94-b0c7-4bfe-83b9-e03e638ef1fd

Sonus SBC 1000/2000 Removes the ext=xxxx, using the Transformation Table and Routes the Call

```
com.net.ux.route DEBUG (translation.cpp:1171) - Performing MANDATORY transformation
using entry  (19.1(1)).
com.net.ux.route DEBUG (translation.cpp:583) - Successful regex match of
"tfCalledNumber" field for ".*9(\d{3})$" (updated ".*9(\d{3})$") with input of
"+15102039002"
com.net.ux.route DEBUG (translation.cpp:627) - Regex replacement output of
"tfCalledNumber" field is "9002"
com.net.ux.route DEBUG (translation.cpp:1171) - Performing OPTIONAL transformation
using entry  (19.2(2)).
com.net.ux.route DEBUG (translation.cpp:583) - Successful regex match of
"tfCalledExt" field for "(.*)" (updated "(.*)") with input of "9002"
com.net.ux.route DEBUG (translation.cpp:1171) - Performing OPTIONAL transformation
using entry  (19.3(3)).
com.net.ux.route DEBUG (translation.cpp:583) - Successful regex match of
"tfCallingExt" field for "(.*)" (updated "(.*)") with input of "1002"
com.net.ux.route INFO (callrouter.cpp:2059) - Successful route request with entry
(1.5(10))
```

Outbound INVITE

Copyright © 2015 Sonus Networks. All rights reserved.

INVITE sip:9002@134.56.227.217:5085;user=phone SIP/2.0

From: "ux227-203-user2" <sip:+15102031002@134.56.227.203:5060;user=phone>;tag=8638e3cb-5f

TO: <sip:9002@134.56.227.217;user=phone>

CSEQ: 1 INVITE
Call-ID: call-BD0D1C00-0000-0010-0C13-C@134.56.227.203

200 OK RESPONSE from Tenor

SIP/2.0 200 OK

Call-ID: call-BD0D1C00-0000-0010-0C13-C@134.56.227.203
Contact: <sip:9002@134.56.227.217:5085;user=phone>
Content-Length: 253
Content-Type: application/sdp
CSeq: 1 INVITE
From: "ux227-203-user2"<sip:+15102031002@134.56.227.203:5060;user=phone>;tag=8638e3cb-5f
To: <sip:9002@134.56.227.217;user=phone>;tag=8638e3d9-26

Changing SIP Transport Protocol from TCP to TLS in a PBX-UX-eUM Topology

This article describes how to change the SIP transport protocol from TCP to TLS in a **PBX - Sonus SBC 1000/2000 - MS Exchange 2007/2010 Unified Messaging Server** topology.

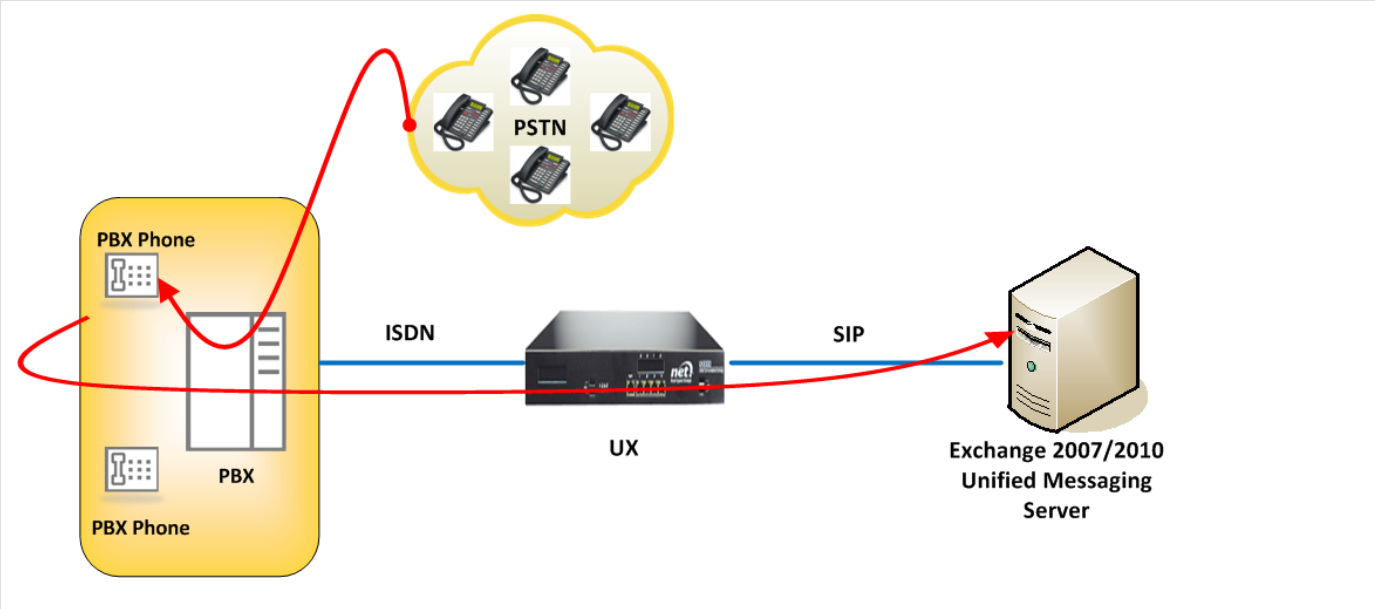
- Overview
- Configuring the Sonus SBC 1000/2000
- Configuring the Exchange Server
  - VoIP Security
  - Port Settings

Overview

Previously, we covered the configuration steps for **PBX - Sonus SBC 1000/2000 - MS Exchange 2007/2010 Unified Messaging Server** in Downstream Deployment of a Sonus SBC 1000-2000 in a PBX-SBC-eUM Topology. That configuration allows connectivity using TCP as the SIP Transport Protocol in the topology shown below.

Topology

Copyright © 2015 Sonus Networks. All rights reserved.



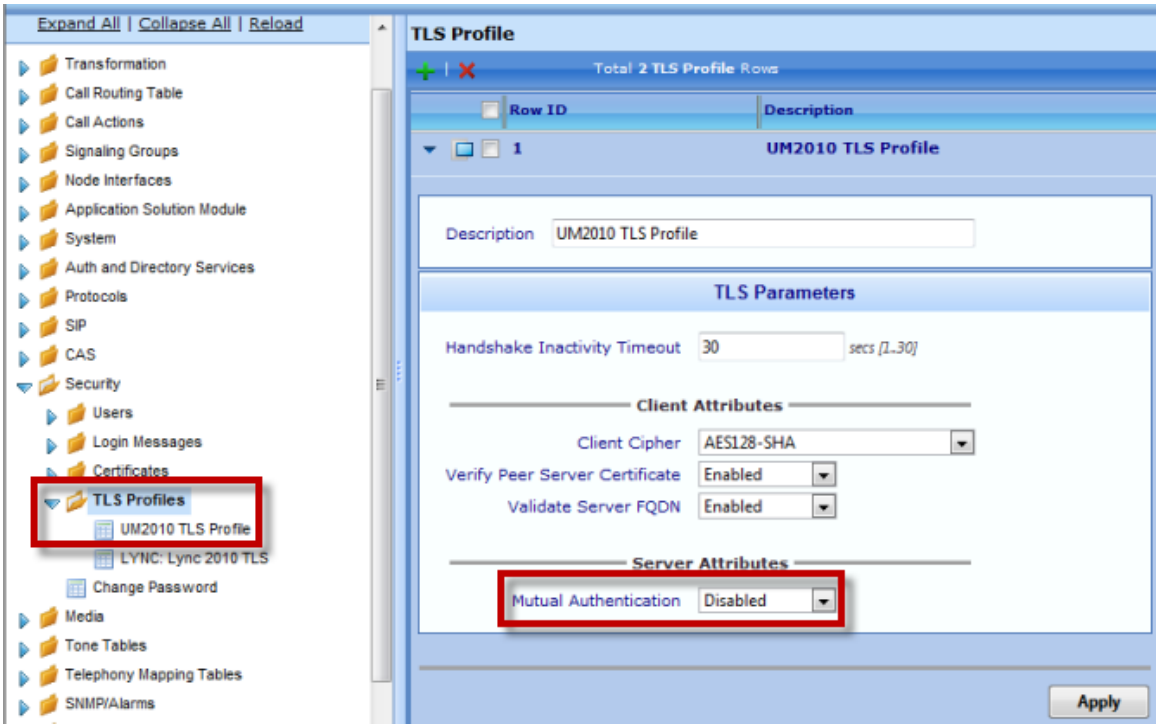
In this article, we change the transport protocol from TCP to TLS in order to secure the voice calls. Follow the steps below to make the necessary additional adjustments to your existing configuration.

Configuring the Sonus SBC 1000/2000

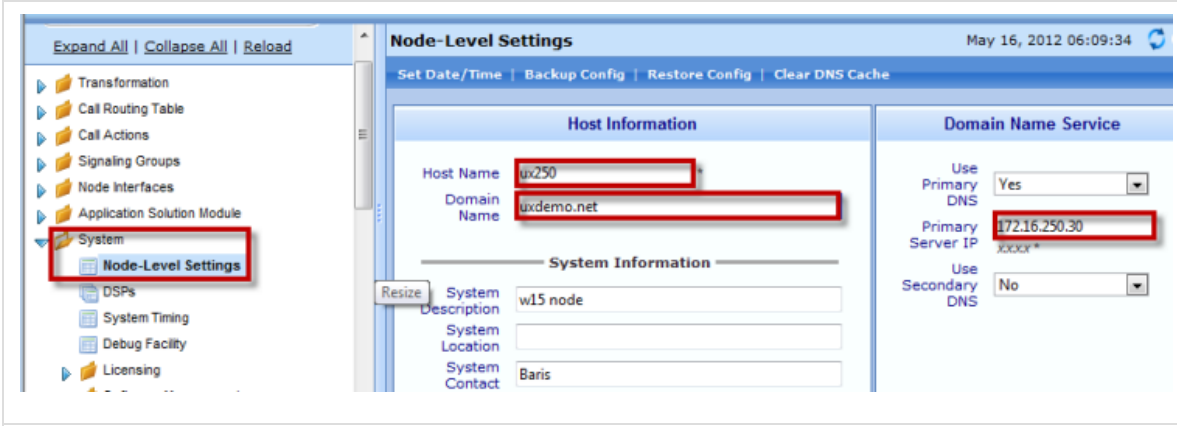
> **Note:**
>
> Please note that this document assumes that **PBX - Sonus SBC 1000/2000 - MS Exchange 2007/2010 Unified Messaging Server** settings are already completed as described in Downstream Deployment of a Sonus SBC 1000-2000 in a PBX-SBC-eUM Topology

1. Create a new TLS profile.
   If you only want to have TLS transport protocol between Sonus SBC 1000/2000 and UMS:
   a. Disable Mutual Authentication from the drop-down menu.
   b. Click Apply.

Copyright © 2015 Sonus Networks. All rights reserved.

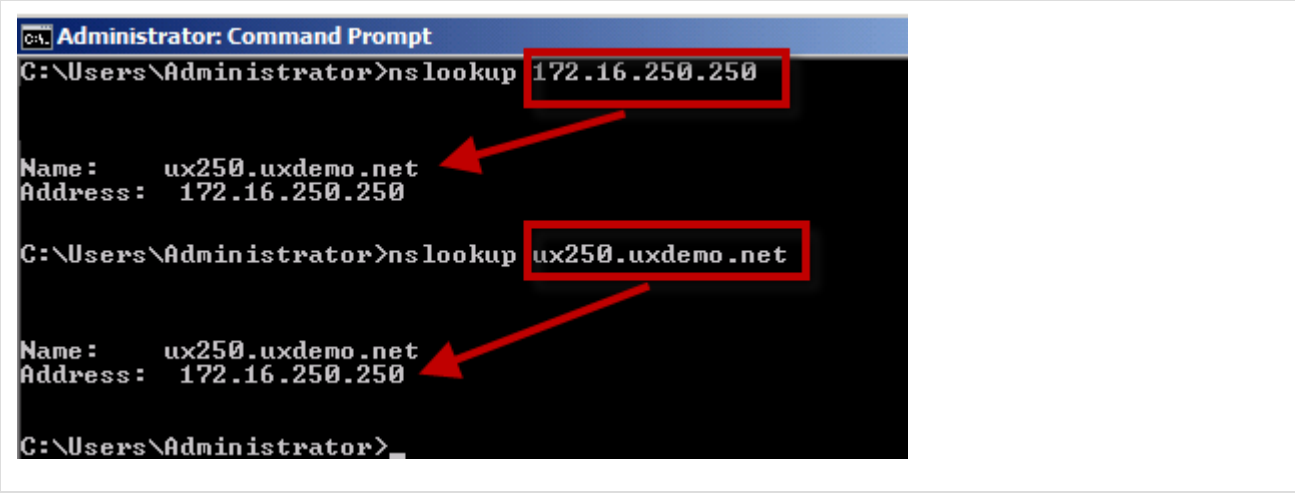


2. In the left navigation pane, go to **System > Node-Level Settings**.
3. Verify that Sonus SBC 1000/2000 host name, domain name, and relevant DNS IP address are correctly configured.

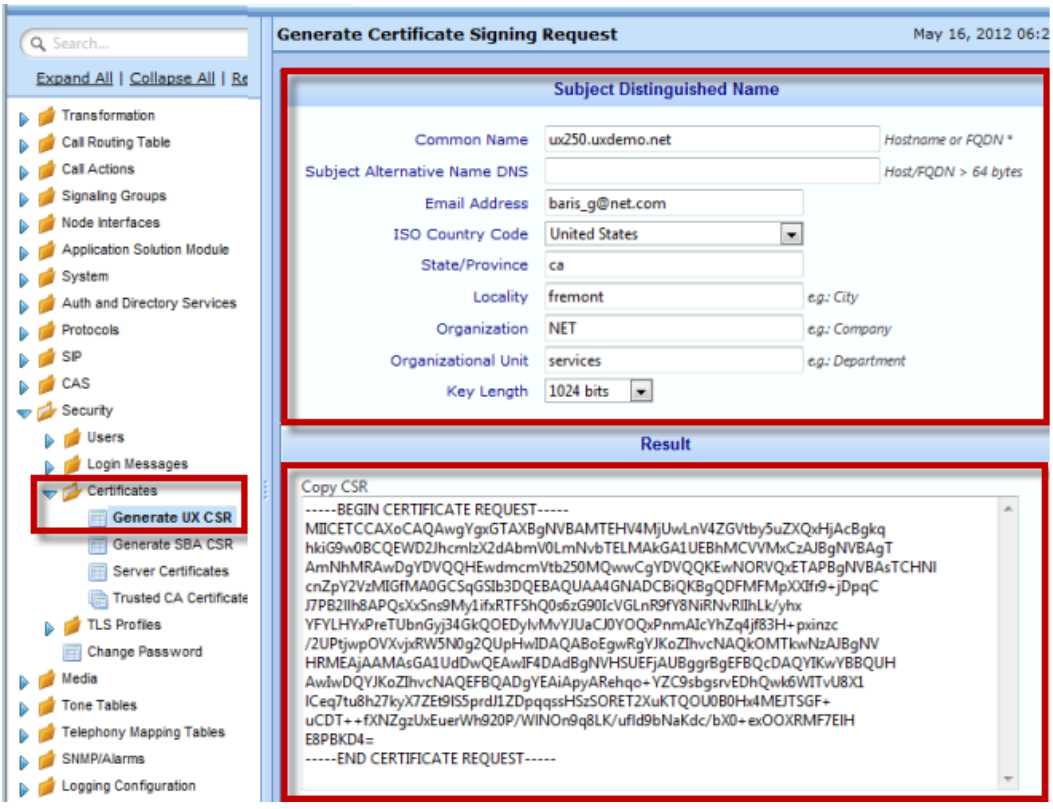


4. Verify that the Sonus SBC 1000/2000 gateway FQDN resolves to the correct IP address in DNS level.
   If not, request that your domain administrator to allow the relevant name resolution in DNS level. (e.g., FQDN should resolve to IP address and IP address resolves to FQDN correctly).

Copyright © 2015 Sonus Networks. All rights reserved.



5. Generate a Sonus SBC 1000/2000 CSR.
   a. In the left navigation pane, go to **Security > Certificates > Generate Sonus SBC 1000/2000 CSR**. For more information see, Working with Certificates in the User's Guide.
   b. Verify that the FQDN of the gateway appears in the **Common Name** field.
   c. After clicking the **OK** button, the Sonus SBC 1000/2000 certificate request is generated and is displayed in the lower pane of **Generate Certificate Signing Request** page.
   d. Copy the content of the request and save it as a text file (e.g., certRequest.txt).
   e. Email the text file (Sonus SBC 1000/2000 certificate request file) to your Root Certificate Authority and get it signed by CA.

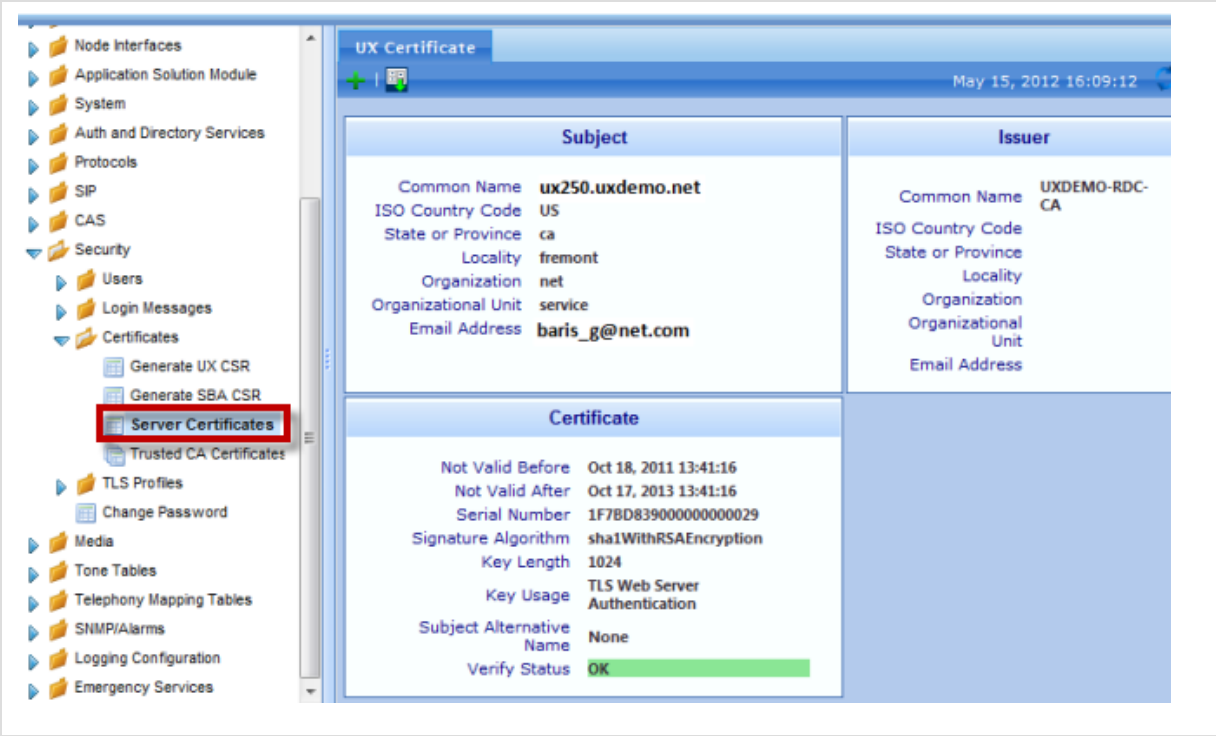


After the certificate request is signed, CA administrator will provide you a signed certificate (e.g., Sonus SBC 1000/2000cert.p7b) file.

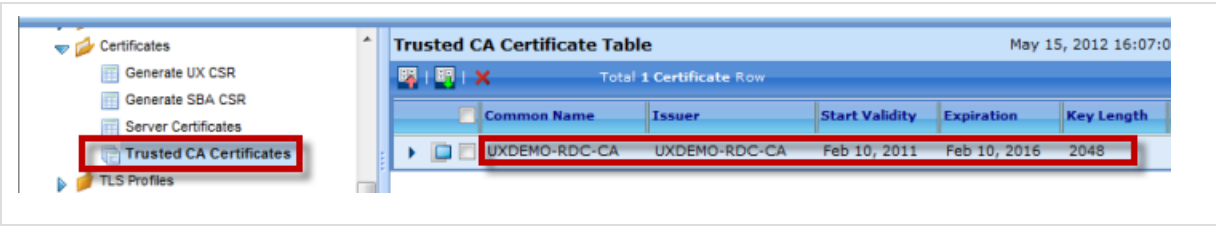
6. Import this file to the Sonus SBC 1000/2000.
   a. In the left navigation pane, go to **Security / Certificates / Server Certificates**.

Copyright © 2015 Sonus Networks. All rights reserved.

b. Confirm on the screen that status of the certificate is **OK**.
For more information see, Importing a Sonus SBC 1000-2000 Server Certificate in the User's Guide.

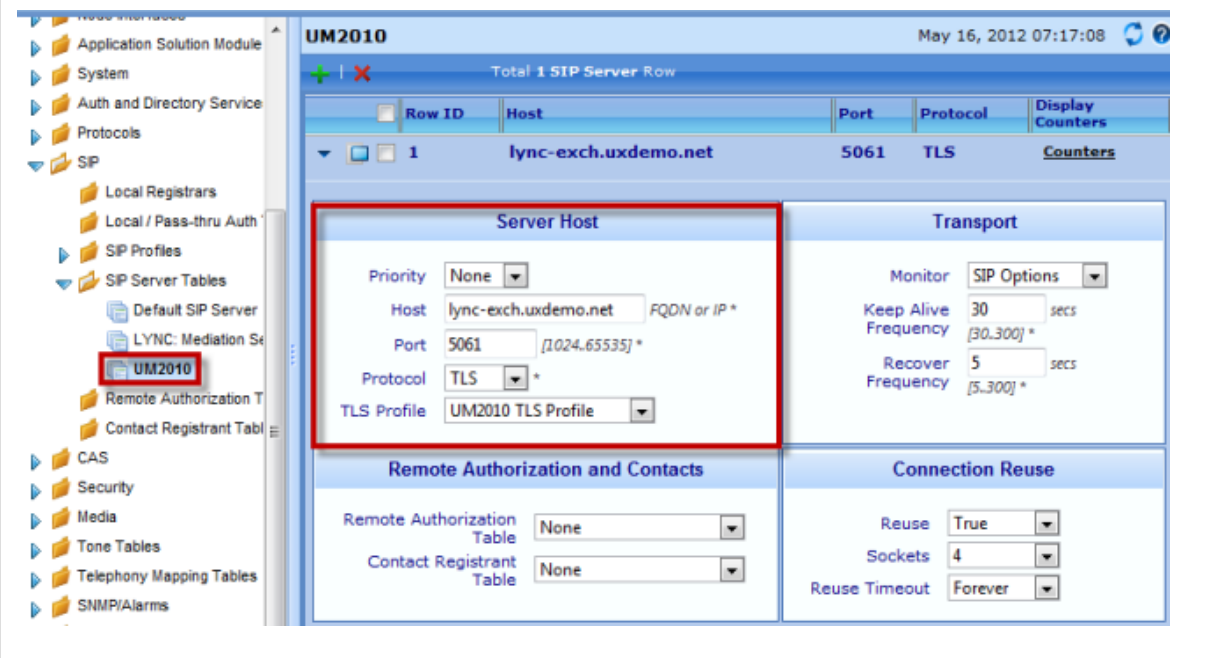


7. Verify that Trusted CA Certificate is imported.
   a. In the left navigation pane, go to **Security / Certificates / Server Certificates**.
   b. Verify that today's date is in the date range between the **Start Validity** and **Expiration** dates.

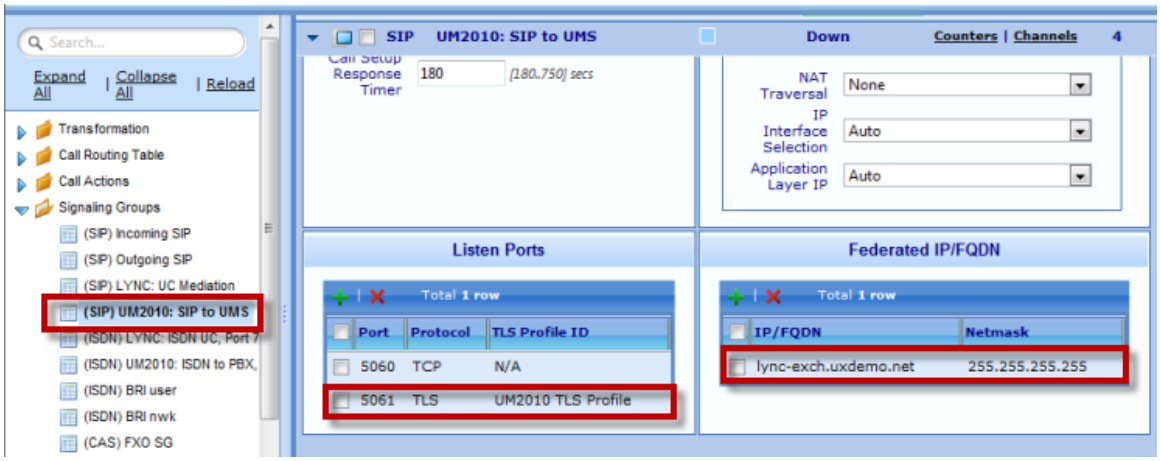


8. In the left navigation pane, go to **Signaling Groups > *Relevant Signaling Group for the Exchange 2010 Server***.
9. Add port **5061** for TLS in the **Listening Ports** pane.
10. Add the FQDN of the Exchange server in the *Federated IP/FQDN pane.
    For more information, see Creating and Modifying SIP Signaling Groups in the User's guide.
11. In the left navigation pane, go to **Security > Certificates > *Exchange server entry***.
12. Verify that the following are present:
    a. FQDN of the Exchange server is entered in **HOST** field.
    b. Desired port number is set (e.g., 5061).
    c. TLS is selected in the **PROTOCOL** field.

Copyright © 2015 Sonus Networks. All rights reserved.



13. In the left navigation pane, go to **Signaling Groups > *Relevant Signaling Group for the Exchange 2010 Server***.
14. Add port **5061** for TLS in the **Listening Ports** pane.
15. Add the FQDN of the Exchange 2010 server in the *Federated IP/FQDN pane.
16. In the left navigation pane, go to **Security > Certificates > *Exchange 2010 server entry***.
    For more information, see Creating and Modifying SIP Signaling Groups in the User's guide.

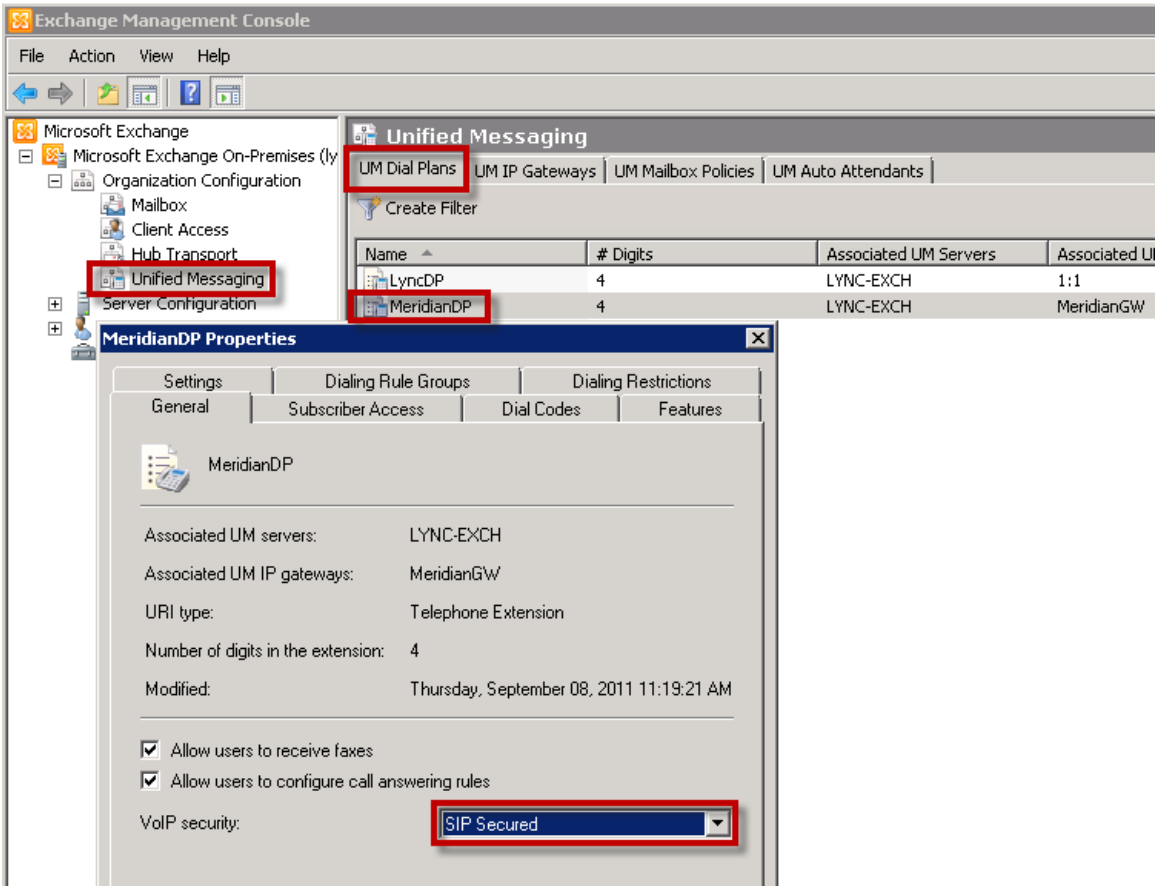


Configuring the Exchange Server

VoIP Security

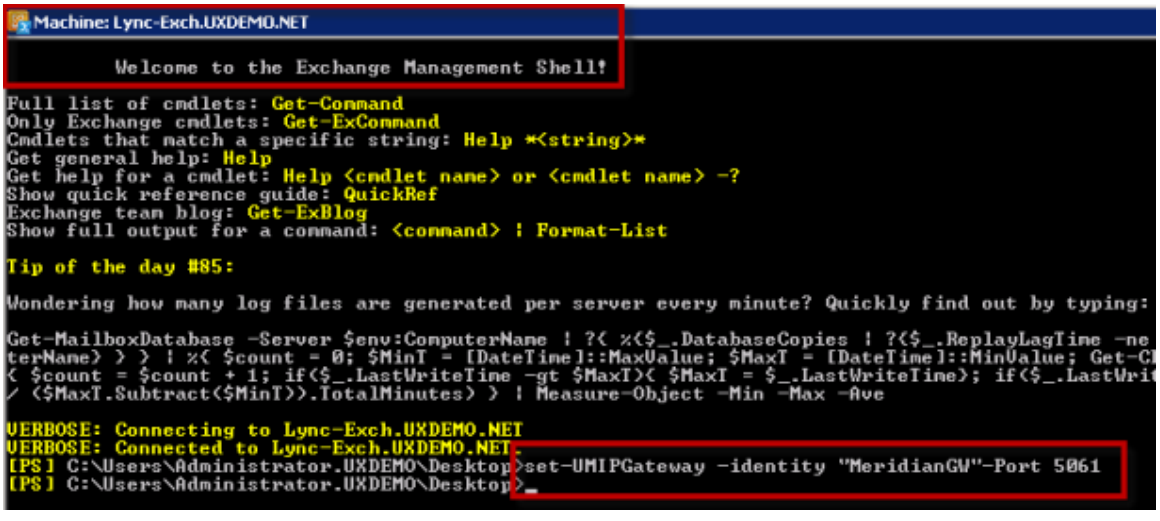
1. Launch ***Exchange Management Console*** on Exchange Server and navigate to ***Organization Configuration > Unified Messaging (in navigation pane)***.
2. Open the properties of the relevant **UM Dial Plan**.
3. Configure the VoIP security settings as *SIP Secured* in the drop-down menu.
4. Click **OK** (this is necessary for TLS).

Copyright © 2015 Sonus Networks. All rights reserved.



Port Settings

1. Launch ***Exchange Management Shell*** on Exchange Server.
2. Execute the `set-UMIPgateway -identity "<Your UM IP GW ID>" -Port 5061` command to set the communication port between Sonus SBC 1000/2000 and the Exchange Server to 5061.



Upon successful completion of the steps in this procedure you should be able to make Sonus SBC 1000/2000 <--> Exchange UMS calls over TLS transport protocol without any issues.

Configuring a Sonus SBC 1000-2000 with ITSP that requires digest authentication with 401

Copyright © 2015 Sonus Networks. All rights reserved.

Unauthorized challenge

This article describes the steps necessary to configure the Sonus SBC 1000 or Sonus SBC 2000 with a SIP peer or with an Internet Telephony Service Provider (ITSP) that requires digest authentication with 401 Unauthorized challenge.

On this Page

- Prerequisites
  - General
  - Software Version
  - System Licenses
- Configuration Steps
- Additional Information
  - Call Flow
  - Call Debugging Trace

Related Articles

- Managing Remote Authorization Tables
- Creating and Modifying Entries to Remote Authorization Tables
- Creating and Modifying Entries in SIP Server Tables

Prerequisites

General

This document assumes that you have already created a Signaling Group and a SIP Server table for the ITSP.

Software Version

Verify that your Sonus SBC 1000 is loaded with the correct boot image version and that your Sonus SBC 1000/2000 base software version is at least version 2.0.0, build 108.

System Licenses

The Sonus SBC 1000/2000 system must have the necessary licenses to make calls.

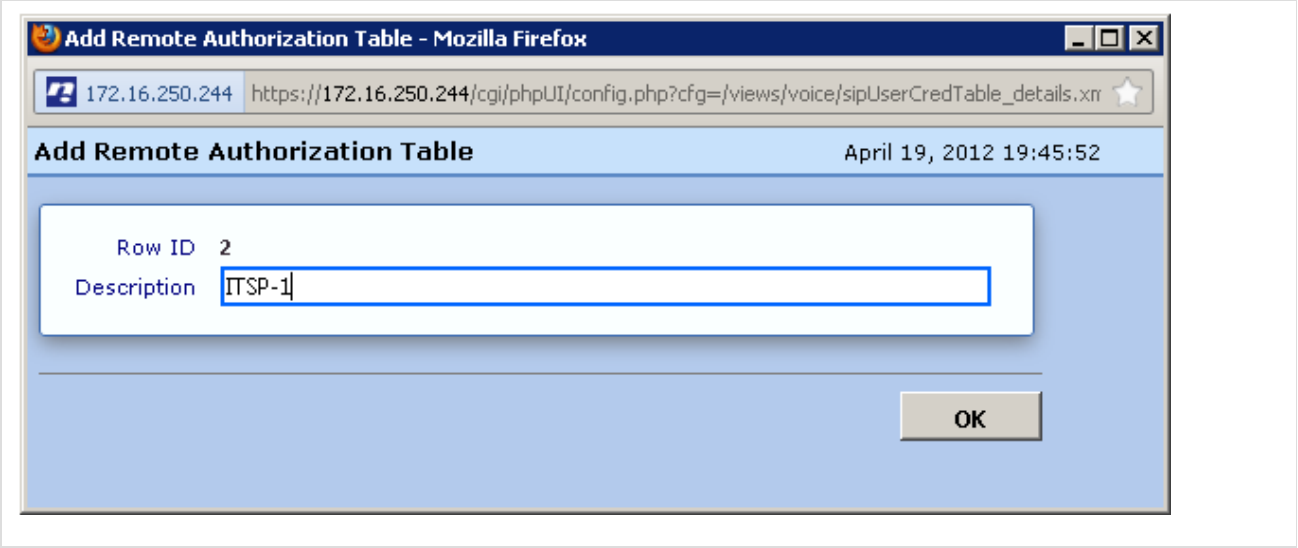
Configuration Steps

The configuration is comprised of three overall steps:

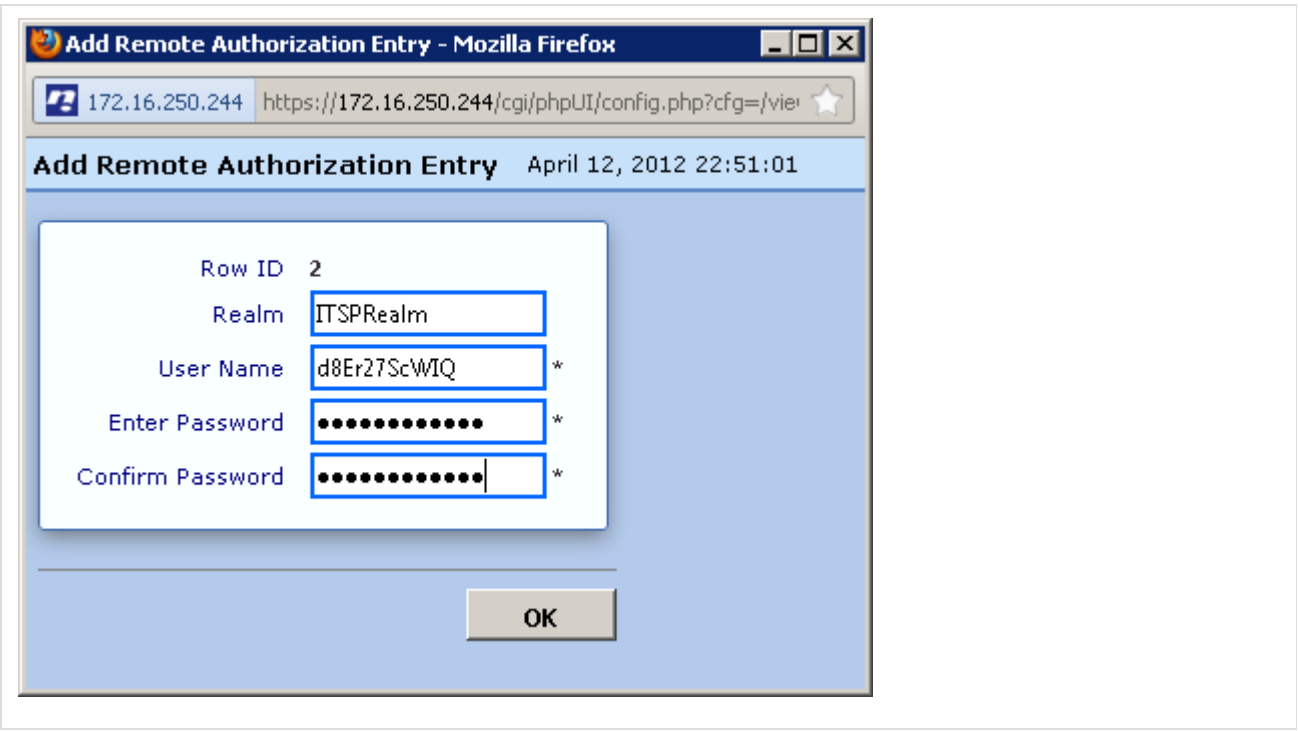
- Creating a Remote Authorization Table
- Assigning the Remote Authorization Table to the SIP Server Table
- Assigning the SIP Server Table to the Signaling Group for the ITSP

1. Add a Remote Authorization Table

Copyright © 2015 Sonus Networks. All rights reserved.

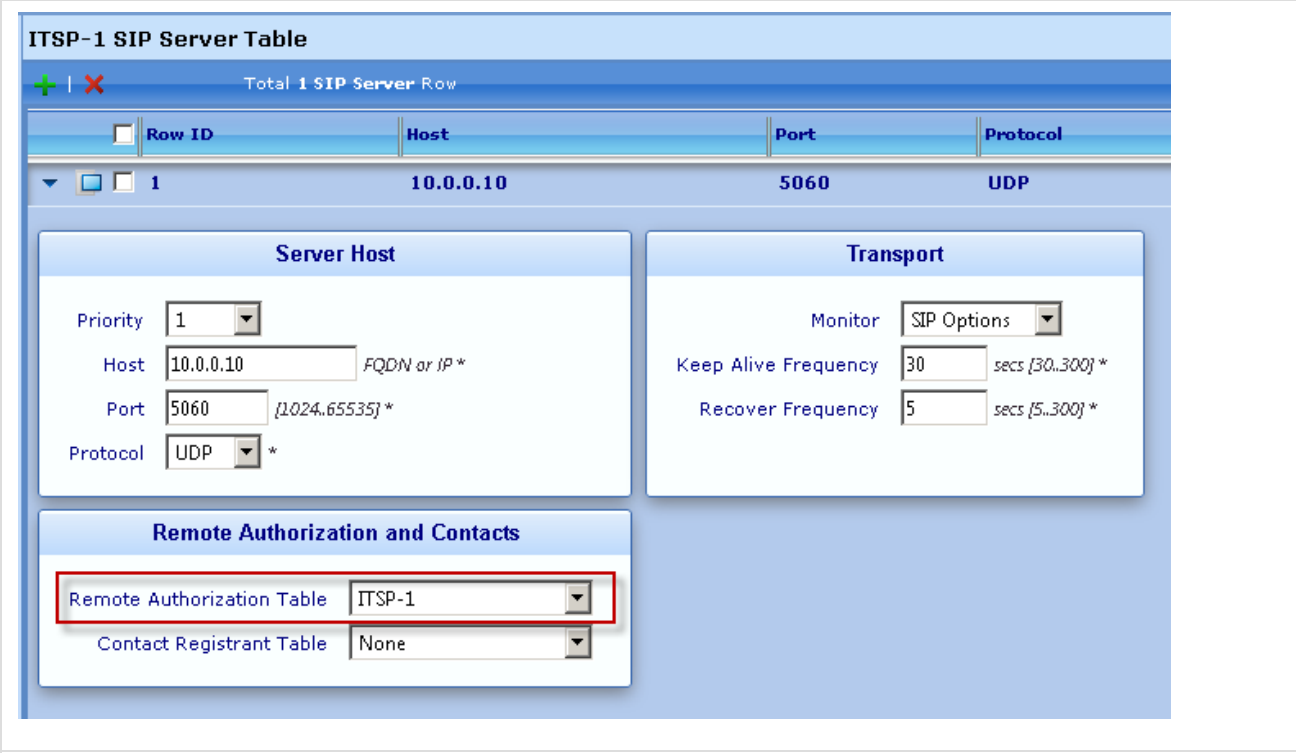


2. Add a Remote Authorization entry



3. Assign the Remote Authorization Table to the SIP Server Table

Copyright © 2015 Sonus Networks. All rights reserved.



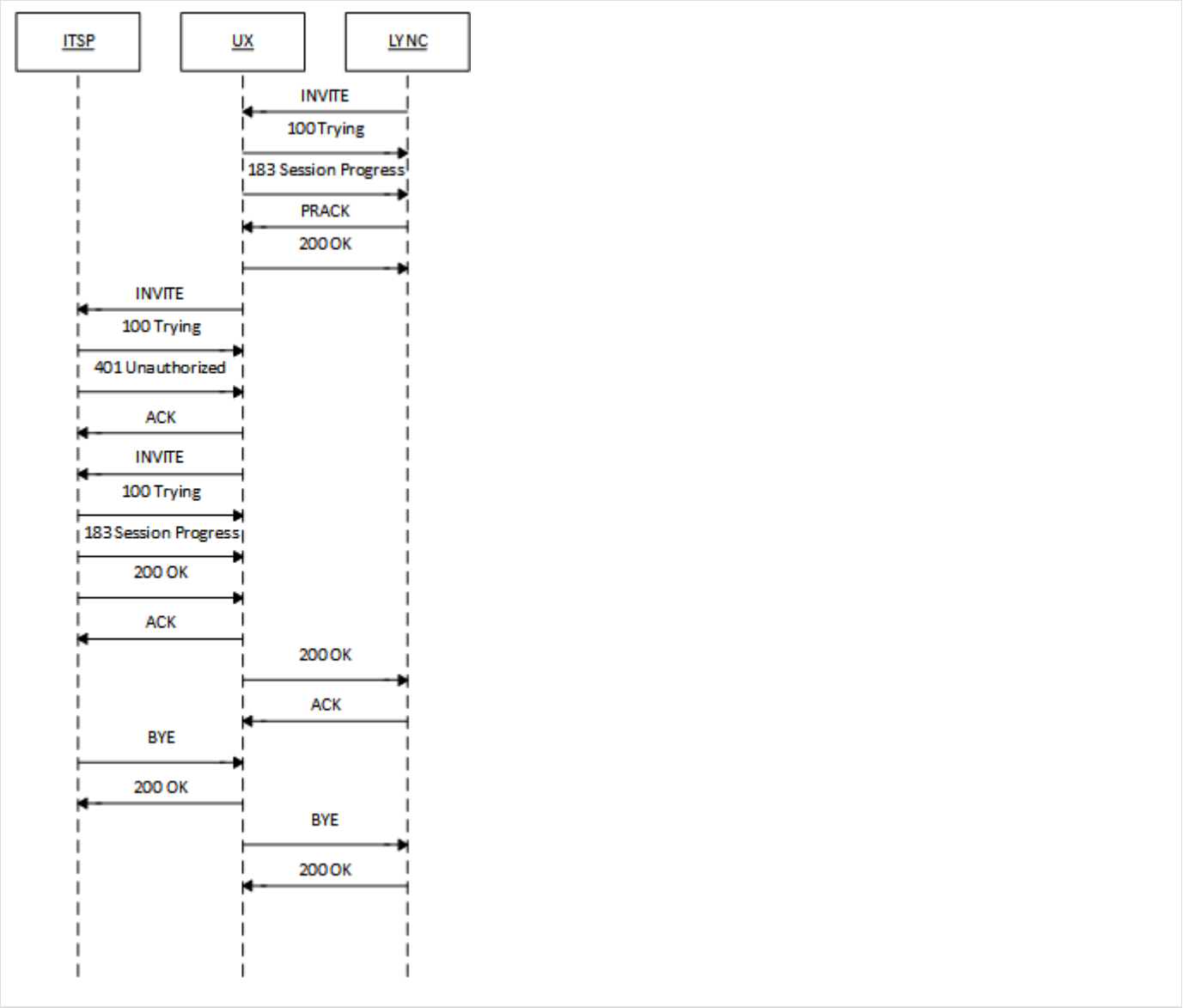
Additional Information

Call Flow

The call flow below depicts an outbound call from Lync to ITSP via Sonus SBC 1000/2000.

- After the initial INVITE from the Mediation server, Sonus SBC 1000/2000 (UA) sends an INVITE request to the ITSP proxy server (UAS).
- Sonus SBC 1000/2000 then receives 100 Trying and then 401 Unauthorized request from the ITSP proxy server.
- Sonus SBC 1000/2000, acting as a UA, then re-sends the request and authenticates itself by including an Authorization header field with the request.
- The Authorization field value consists of credentials containing the authentication information of the UA for the realm of the resource being requested as well as parameters required in support of authentication and replay protection.
- The Realm, Username and Password information are taken from the Remote Authorization Table entry based on the username that is provided by the realm provided by the UAS.

Copyright © 2015 Sonus Networks. All rights reserved.



Call Debugging Trace

The Sonus SBC 1000/2000 debug log produced at Trace level will show the information that is used to compute the MD5 string used in the Authorization header:

```
[2012-04-12 16:17:40,303] 5688 0001 com.net.ux.sip TRACE (Credentials.cpp:451) -
computeResponse: creating credentials:
   algorithm : "MD5"
   userName  : "d8Er27ScWIQ"
   passWord  : "uw83i29BeY3x"
   realm     : "ITSPRealm"
   nonce     : "ITSPRealmDe98wSj8euJdU8SHs8"
   cNonce    : "baea32a3"
   nonceCount: "00000001"
   qop       : "auth"
   method    : "INVITE"
   uri       : "sip:15105742474@10.0.0.10:5070;user=phone"
```

Copyright © 2015 Sonus Networks. All rights reserved.

SIP Message Manipulation Document Catalog

Table of Contents

- Prerequistes
- Document Catalog
  - Configuration Documents
  - Educational/Reference Documents
  - Troubleshooting Documents
  - More Information

About this Page

This catalog lists SIP Message Manipulation documents by feature. It is intended to guide and educate the user about the various SMM features by providing example configurations

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups
- SIP Message Manipulation Overview
- 6 Steps to Creating Effective SMM Rules

Prerequistes

Assumes the user is familiar with configuring the SBCx000's WebUI

Requires Sonus SBC1000/2000 Version 2.2

Document Catalog

This catalog lists SIP Message Manipulation documents by feature. It is intended to guide and educate the user about the various SMM features by providing example configurations.

Configuration Documents

SMM Feature	Document Name
Complete step-by-step SMM configuration	• **Set the Request URI number from the TO Header** • **Setting the P-Asserted Identity**
Changes to SIP Headers (The *Add Header* feature)	• **Setting the P-Asserted Identity** • **Properly canceling forked LYNC calls using SIP Message Manipulation** • **Correcting a FROM Tag using SIP Message Manipulation** • **Call Routing Based On SDP Media IP Address** • **Removing Brackets from a Parameter using SIP Message Manipulation**

Copyright © 2015 Sonus Networks. All rights reserved.

Changes to the Request URI (The *Add Request* feature)	• **Set the Request URI number from the TO Header** • **Call Routing Based On SDP Media IP Address**
Changes to other portions of a SIP Message (The *Add Raw* feature)	• **Modifying the m and a lines in SDP using SIP Message Manipulation** • **Call Routing Based On SDP Media IP Address**
Removing a SIP Header	• **Remove the User Agent or Server Header using SIP Message Manipulation**
Uses a Token	• **Set the Request URI number from the TO Header** • **Correcting a FROM Tag using SIP Message Manipulation** • **Call Routing Based On SDP Media IP Address**
Uses a Regex	• **Removing Brackets from a Parameter using SIP Message Manipulation** • **Modifying the m and a lines in SDP using SIP Message Manipulation** • **Call Routing Based On SDP Media IP Address**
SIP Headers that aren't pre-programmed tokens	• **Properly canceling forked LYNC calls using SIP Message Manipulation** • **Setting the Calling Number from a SIP Header using Sip Message Manipulation** • **Removing Brackets from a Parameter using SIP Message Manipulation**
Using Literal Values	• **Setting the P-Asserted Identity**
URI and Header Parameter manipulation	• **Correcting a FROM Tag using SIP Message Manipulation** • **Call Routing Based On SDP Media IP Address**
Header Pass-through	• **Properly canceling forked LYNC calls using SIP Message Manipulation**
Selection of specific SIP Message Types	• **Properly canceling forked LYNC calls using SIP Message Manipulation** • **Setting the Calling Number from a SIP Header using Sip Message Manipulation**
Using the Conditional Rules feature to restrict Message Manipulation	• **Setting the P-Asserted Identity**
SMM Solutions that use a Transformation Table	• **Setting the Calling Number from a SIP Header using Sip Message Manipulation** • **Using HISTORY-INFO to set the FROM Number**
SMM Solutions that use a Header Ordinals	• **Using HISTORY-INFO to set the FROM Number**

Copyright © 2015 Sonus Networks. All rights reserved.

Changing headers from lower-case to upper-case	• **Correcting letter case using SIP Message Manipulation**

Educational/Reference Documents

Document Name	Description
SIP Message Manipulation Overview	Overview of the SMM fundamentals.
6 Steps to Creating Effective SMM Rules	How to create useful SMM Rules.

Troubleshooting Documents

Document Name	Description
The Test Message function doesn't return proper Result	Must remove ^M characters or Test Message features malfunctions.

More Information

6 Steps to Creating Effective SMM Rules

Table of Contents

- Prerequistes
- Steps to Creating an Effective SMM Translation
- Important Notes

About this Page

- This document details the steps required to produce an effective SIP Message Manipulation.

Related Articles

- SIP Message Manipulation Overview
- SIP Message Manipulation
- Managing Signaling Groups
- SIP Message Manipulation Document Catalog
- Optional Matching Overview

Prerequistes

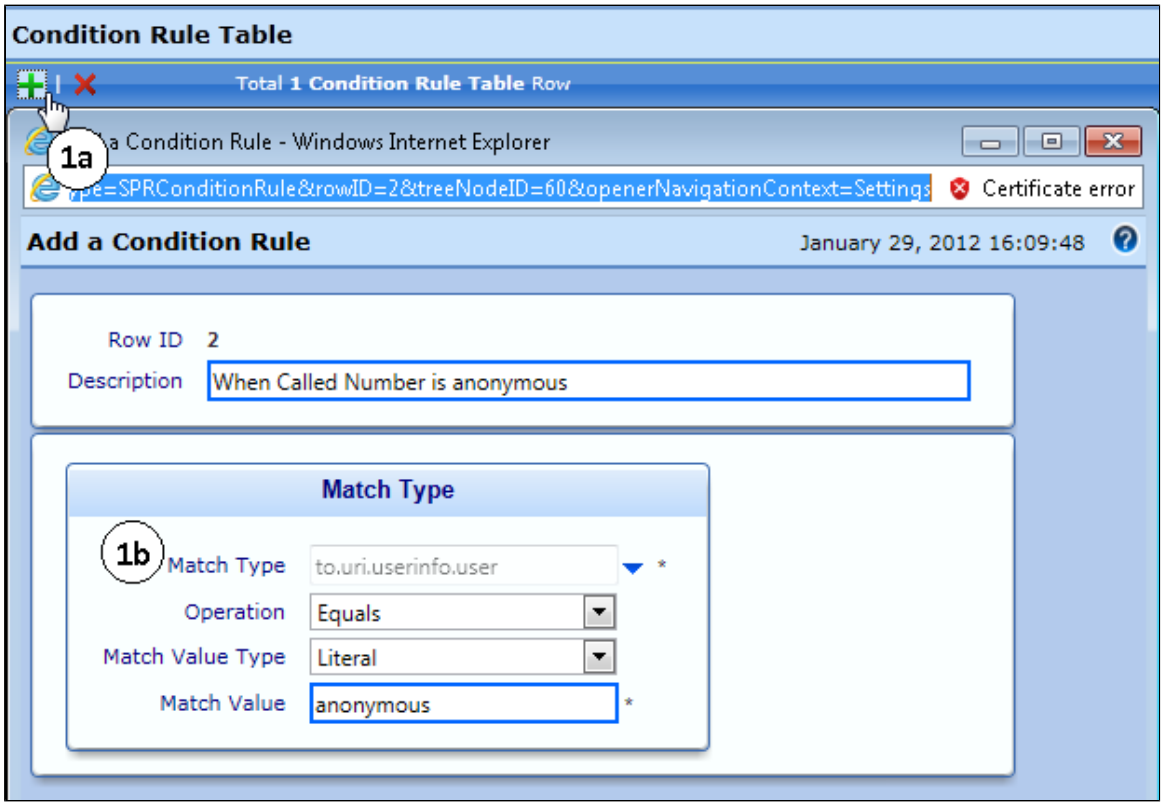
Copyright © 2015 Sonus Networks. All rights reserved.

Read the SIP Message Manipulation Overview
Requires Sonus SBC2000/1000 Version 2.2 or later
This document assumes the reader is familiar with the Transformation Table's *Optional/Mandatory* and *User Value* features.

Steps to Creating an Effective SMM Translation

1. **If there are any conditions for the SMM Rule, add a Condition Rule.**
   Some example conditions might be:
   - Only on a particular phone number
   - Only a specific header (name)

   In the example below, the Called Number must be 'anonymous'. This condition will be applied later in the SIP Message Rule.

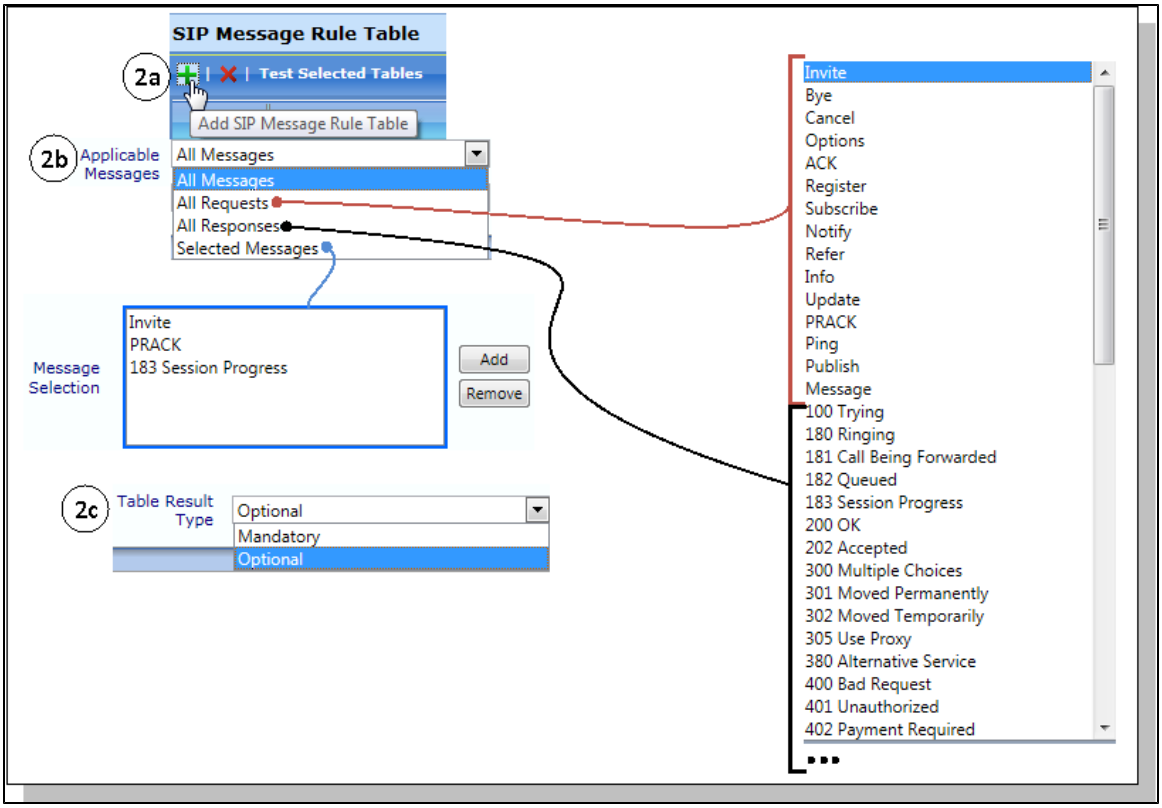


Condition: When the Called Number is 'anonymous'

   - 1a: Add a Condition Rule
   - 1b: Select a *Match Type* Token value; this states the SIP Packet element (diversion number, IP address, etc.) for the match. Then, complete of the remainder which provides the **value** you desire to match.

2. **Decide which type of SIP packets are to be changed. The types of SIP packets to be changed is selected when the *SMM Message Rule Table* is created.**

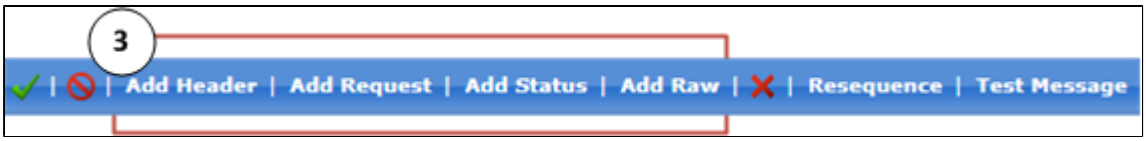
Copyright © 2015 Sonus Networks. All rights reserved.



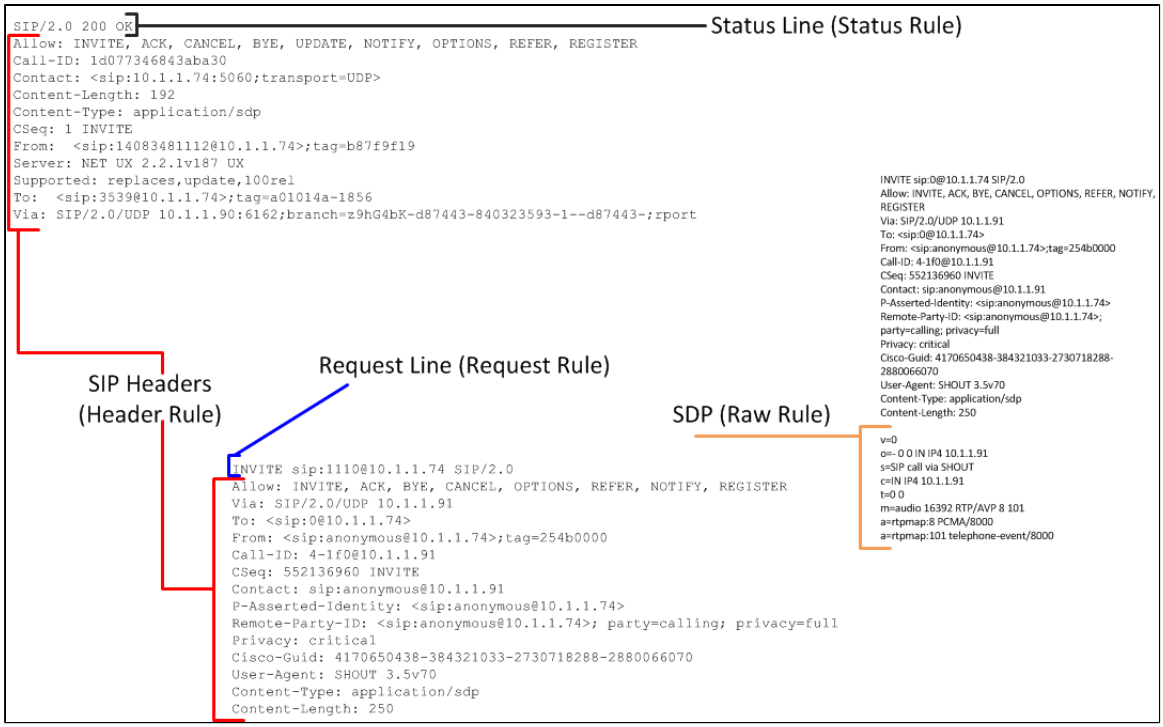
Creating an SMM Rule Table

- 2a: Add a SIP Message Rule Table
- 2b: Select which SIP Messages will be examined by this Rule Table
- 2c: Will this SMM Table be *Mandatory* or *Optional* within the Signaling Group?

3. **What SIP Packet element needs to be changed?**
   - Click the name of the newly created SMM Table in the left-hand navigation tree, then add an SMM Rule entry.
   - Which type of Rule? Use the diagram below!



Copyright © 2015 Sonus Networks. All rights reserved.

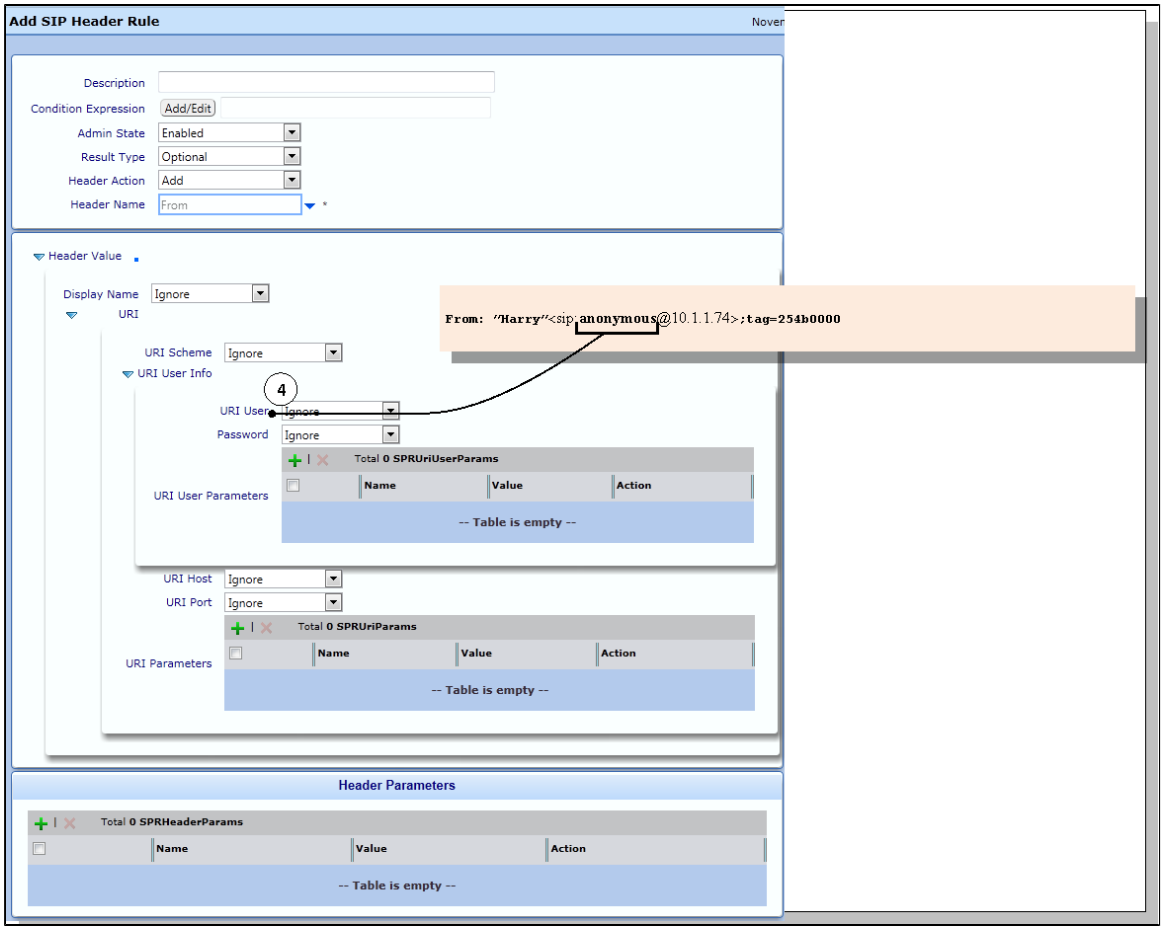


Be sure to select the appropiate SMM Rule type!

- 3: Add one of the Rule Types: Header, Request, Status, or Raw

4. **Identify which rule section corresponds to the SIP element you want to change.**
   - Example: If you wanted to change the FROM number to something other than **anonymous**
     From: <sip:**anonymous**@10.1.1.74>;tag=254b0000

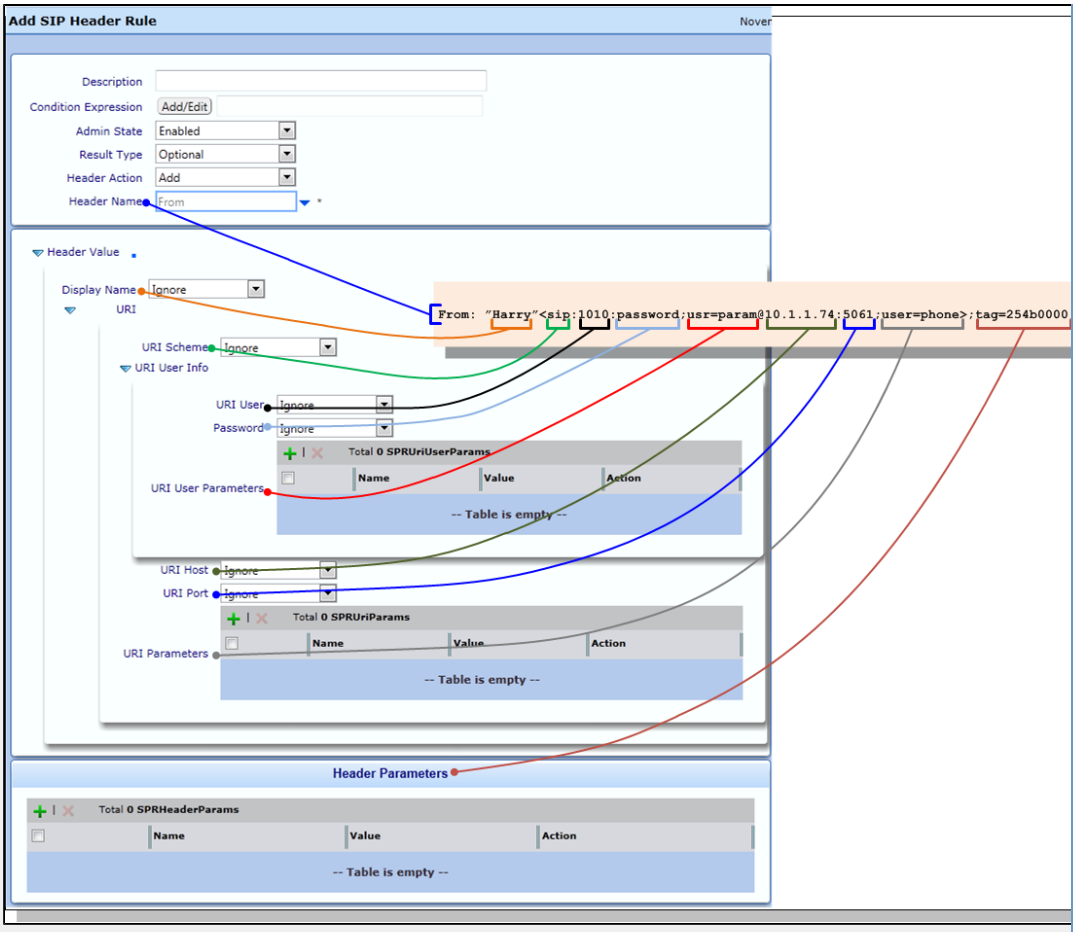
Copyright © 2015 Sonus Networks. All rights reserved.



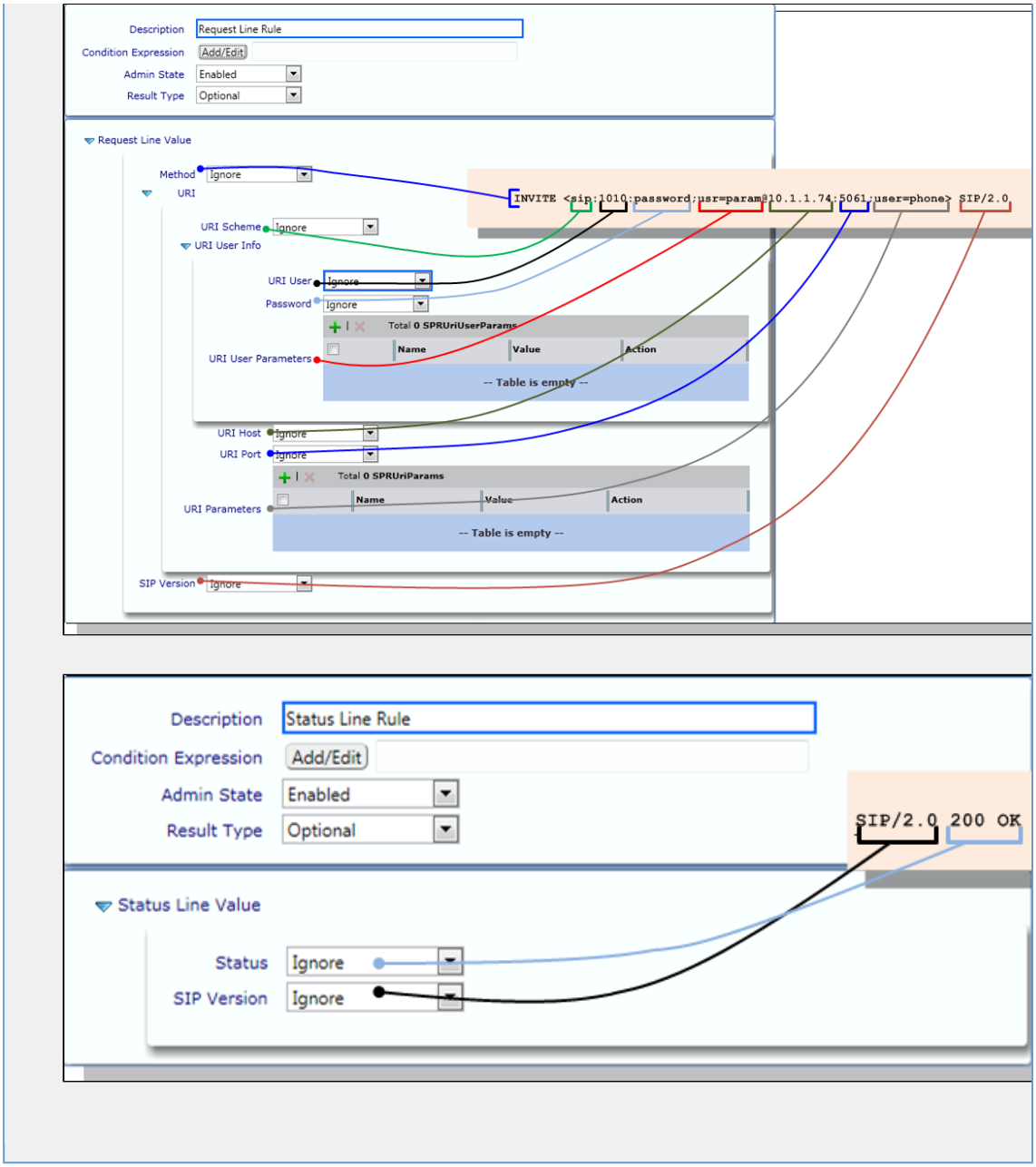
Use the references below if you're uncertain about which configuration to use

▼ Click here to see the mapping between SIP packet elements and their corrsponding SMM configurations

Copyright © 2015 Sonus Networks. All rights reserved.

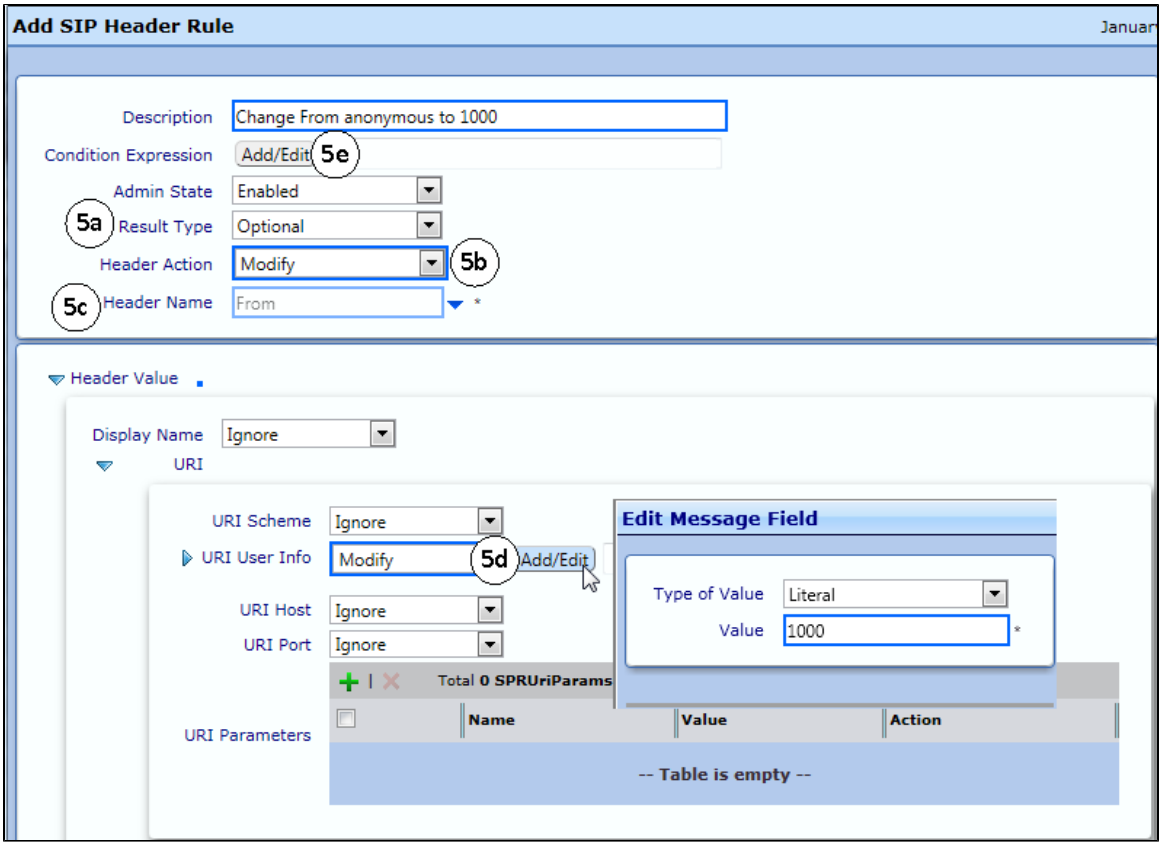


Copyright © 2015 Sonus Networks. All rights reserved.



5. **Select the appropriate type of change to be made**
   Configure the rule to correspond with the manipulation you require.

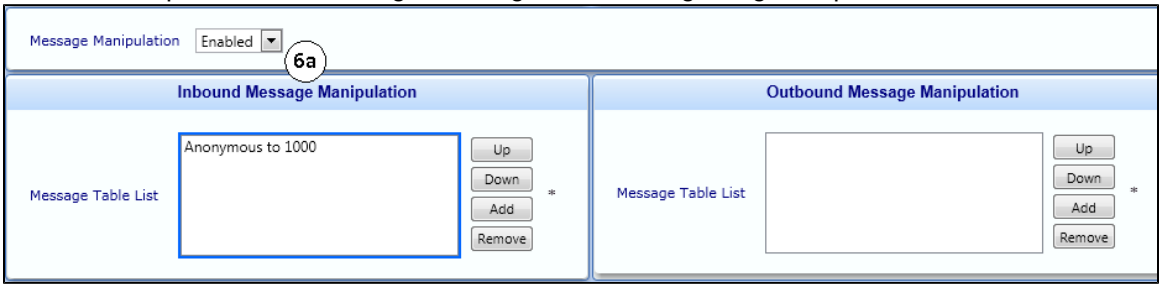
Copyright © 2015 Sonus Networks. All rights reserved.



Steps to create a SMM Rule

- 5a: Select the *Result Type*. This setting operates exactly the same as the Translational Table optional/mandatory.
- 5b: Set the *Action* to *Add, Remove, Copy, or Modify. The available options will vary based upon the type of rule you're adding. If you think about it, you can't _add* a Request URI or Status Line; the SIP packet already has one, right?
- 5c: For a Header Rule, you'll need supply a Header Name either from the pre-progammed list or by simply typing the name of the header if it doesn't appear in the list. **Request and Status Rules address only the Request and Status headers, so those rules don't require the user to pick a header.**
- 5d: Configure the target rule setting. In the case of the example for changing any calling number of *anonymous* to 1000, set the User URI info to *Modify* and add the configuration/value you want the SIP element changed to.
- 5e: If you created a Condition in Step 1, add it to the Rule entry now. In this example, the SMM will only execute if the Calling Number is 'anonymous'.

6. **Configure your new rule into either a Signaling Group or Call Route.**
   SMM Rules can be processed either ingress or egress at the Signaling Group.



Copyright © 2015 Sonus Networks. All rights reserved.

Important Notes

Like the Transformation Table's *User Values*, the SMM feature supports a method to copy values into user-controlled, generic tokens, *SG User Values*. The *SG User Values* can be transported from ingress to egress SG, or be utilized in a Transformation Table (e.g. to move a P-Asserted number to the Calling Number at the Call Route level rather than the Signaling Group level). See this SMM Document for an example of the *SG User Value* used with a Translation Table.

Call Routing Based On SDP Media IP Address - SIP Message Manipulation

Table of Contents

- Prerequistes
- Summary
  - Configure the SBC1000/2000 Header Manipulation
  - Debugging Output
  - Important Notes

About this Page

- This document details setting the RURI number and TO number based upon information in the SDP body.
- This document features the *Add Raw* function. In this example, *Add Raw* is used to search for (and possibly replace) text in the SDP body.
- This document features a SMM entry that is configured as *Mandatory*.
- This document details the configuration to change the Request URI Line in a SIP Request (INVITE, ACK, REGISTER, CANCEL, etc.) using the *Add Request* selection.
- This document details the configuration to change the TO Header using the *Add Header* selection.
- This Header Manipulation document utilizes the *Token* manipulation function.

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups

Prerequistes

Requires Sonus SBC1000/2000 Version 2.2

Summary

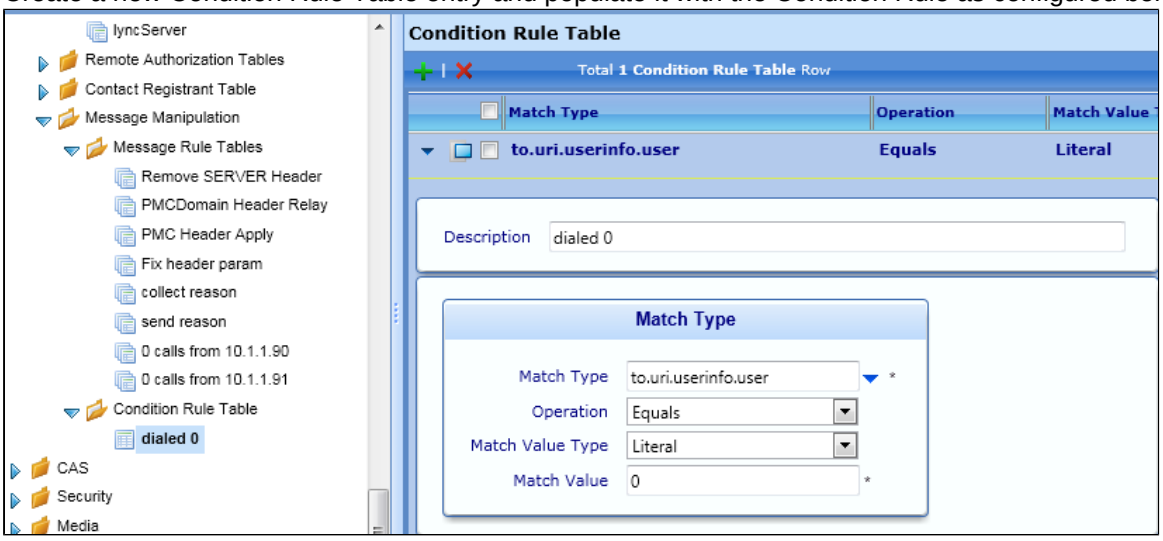
This document describes how the contents of and SDP might be utilized to make call routing decision. In this highly unlikely scenario, a call placed to the Operator is routed to a specific building's Operator based upon the source

Copyright © 2015 Sonus Networks. All rights reserved.

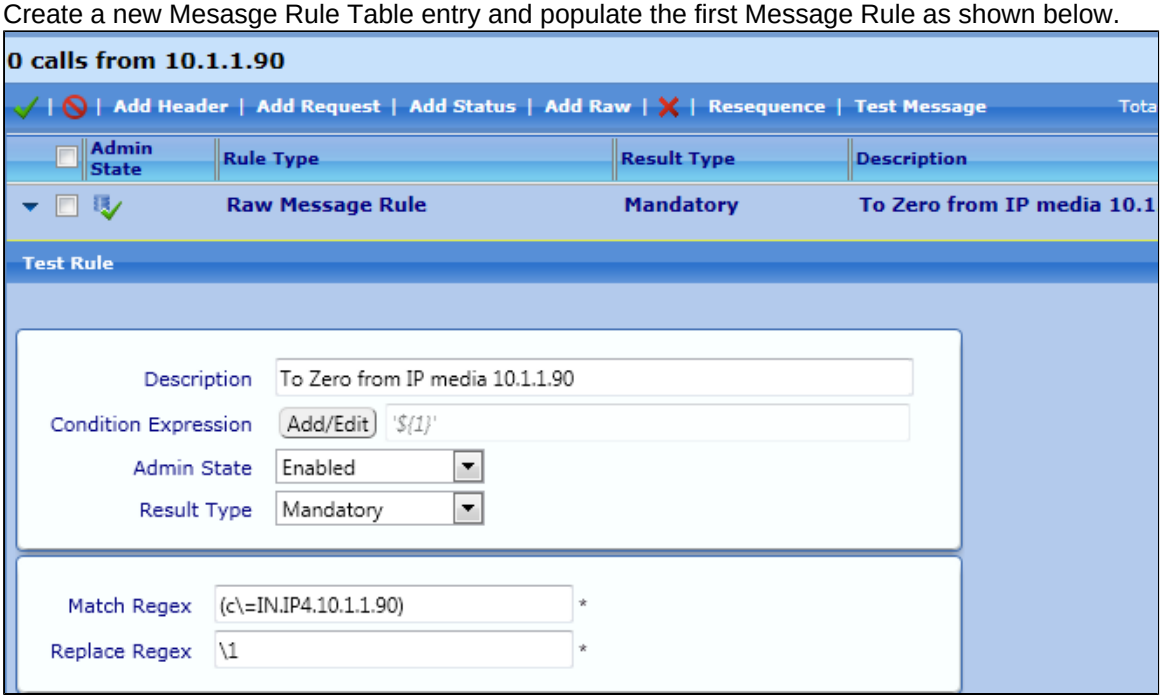
subnet of the call (presuming that each building employs a different subnet). **This configuration note does not detailed a supported configuration as changing the RURI number of a call may lead to numerous interoperability issues.** Rather, this configuraton note is intended as SMM education. Several SMM features are employed within this scenario, thus it provides an excellent learning example.

Configure the SBC1000/2000 Header Manipulation

1. Create a new Condition Rule Table entry and populate it with the Condition Rule as configured below.

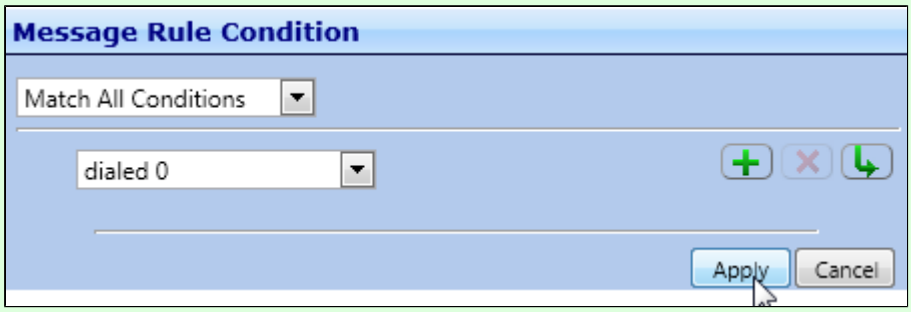


2. Create a new Mesasge Rule Table entry and populate the first Message Rule as shown below.



Copyright © 2015 Sonus Networks. All rights reserved.

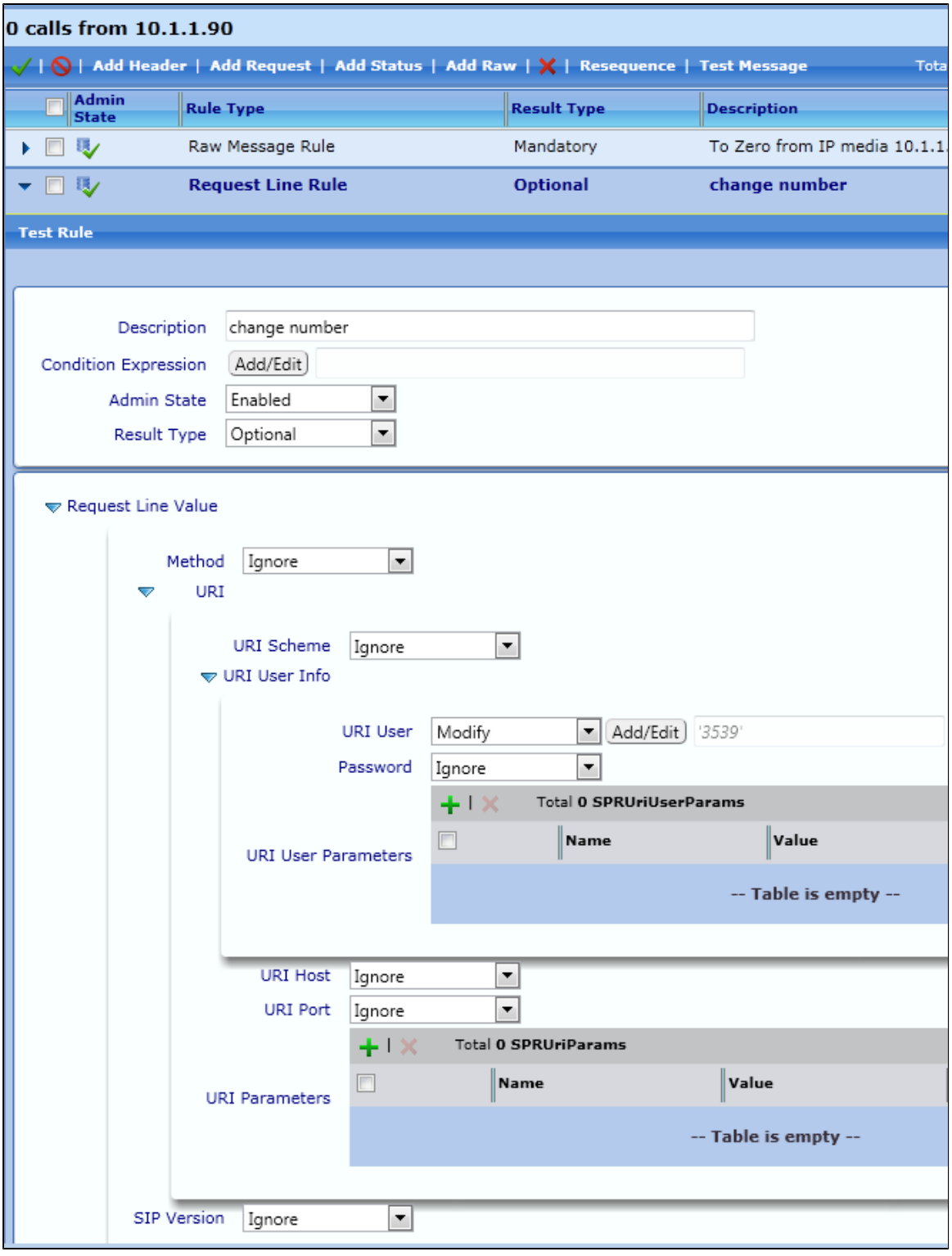
Be sure to add the Condition Expression by clicking the Condition Expression *Add/Edit* button and configuring as shown. This Condition Expression will cause this particular SMM entry to be run only when the condition is met--when the called number is '0'.



As this entry's *Result Type* is configured to *Mandatory*, this entry, and all the subsequent entries, will only execute if a Regex match is found in the SIP Message. Being an *Add Raw* entry, the entire SIP packet, including SDP, will be searched for the pattern configured in the in the *Match Regex* box.

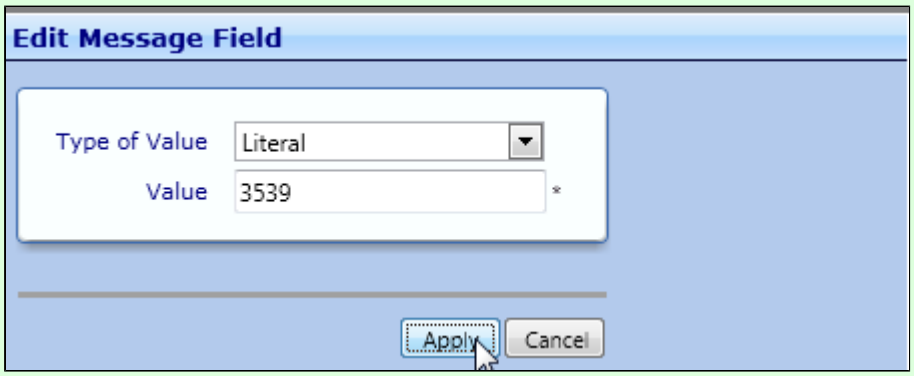
3. If the dialed number is 0 and the SIP Message contains *c=IN IP4 10.1.1.90*, then we want to change the Request URI number (URI User) to a different number. The only method for changing the Request URI header is via the *Add Request* feature. Use the *Add Request* selection to create this SMM entry.

Copyright © 2015 Sonus Networks. All rights reserved.



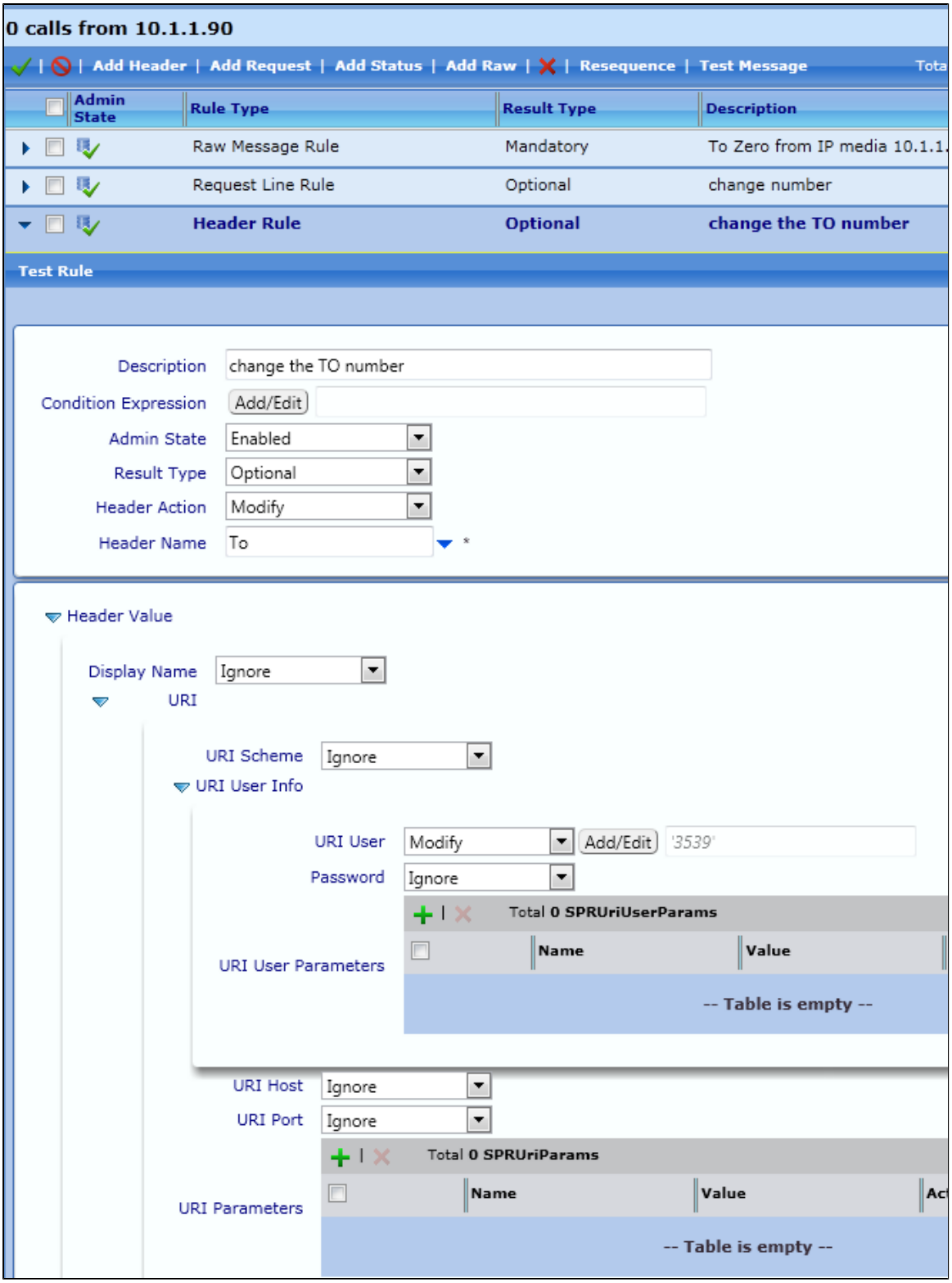
Copyright © 2015 Sonus Networks. All rights reserved.

- [x] Use the User URI *Add/Edit* button to set the new RURI number



4. Since the RURI number is being changed, it's probably a good idea to change the TO header number as well. TO headers are configured using the *Add Header* feature. Use the *Add Header* feature to create this SMM entry to change the TO Header User URI (number).

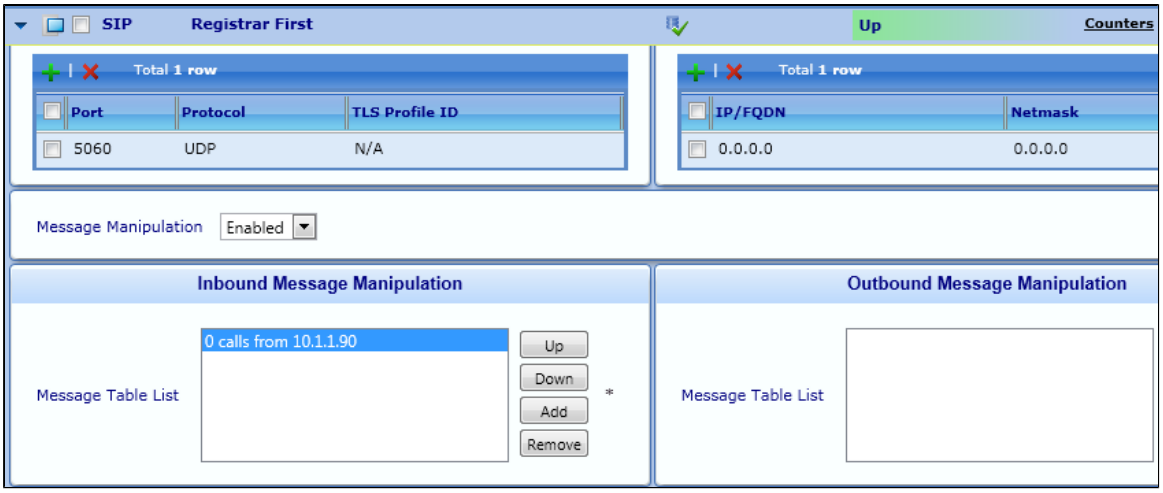
Copyright © 2015 Sonus Networks. All rights reserved.



Don't forget the User URI *Add/Edit* button!

5. Add the SMM Table to the desired Signaling Group.

Copyright © 2015 Sonus Networks. All rights reserved.



Debugging Output

```
[2012-11-08 14:12:04,413] 2159 002b com.net.ux.sip DEBUG (SipMessage.cpp:1137) -
decodedLength:1009 decoded 0x228268:
[2012-11-08 14:12:04,413] 2160 002a

INVITE sip:0@10.1.1.74 SIP/2.0
Via: SIP/2.0/UDP
10.1.1.90:6336;branch=z9hG4bK-d87543-28224e612861dc20-1--d87543-;rport
Max-Forwards: 70
Contact: <sip:444@10.1.1.90:6336>
To: "0"<sip:0@10.1.1.74>
From: "test"<sip:444@10.1.1.74>;tag=3f31e106
Call-ID: MTAzZGZhY2ZlMDkwZjE1N2M5MTdkYzdmMWE4MzcyOWE.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: eyeBeam release 1011w stamp 41324
Content-Length: 508

v=0
o=- 5 2 IN IP4 10.1.1.90
s=CounterPath eyeBeam 1.5
c=IN IP4 10.1.1.90
t=0 0
m=audio 7092 RTP/AVP 107 100 106 6 0 105 8 18 3 5 101
a=alt:1 2 : 4memZGA5 jvFXZUL/ 10.1.1.90 7092
a=alt:2 1 : fRF9Sxzc EyUo4lyB 192.168.128.5 7092
a=fmtp:18 annexb=yes
a=fmtp:101 0-15
a=rtpmap:107 BV32/16000
a=rtpmap:100 SPEEX/16000
a=rtpmap:106 SPEEX-FEC/16000
a=rtpmap:105 SPEEX-FEC/8000
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/8000
a=sendrecv
a=x-rtp-session-id:DAE5D[2012-11-08 14:12:04,413] 2161 0029
666CB8E4F1E991072554573C185
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-11-08 14:12:04,414] 2162 0028 com.net.ux.sip DEBUG
(sipSignalingGroupConfig.cpp:672) - getBestSubnet: 10.1.1.90 - 10.1.1.6
[2012-11-08 14:12:04,414] 2163 0027 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(1) 0x273a60} CanAccept: Reject msg: call=1,
transport=1, filter=0 localPort=1
[2012-11-08 14:12:04,414] 2164 0026 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(9) 0x278560} CanAccept: Reject msg: call=1,
transport=0, filter=0 localPort=0
[2012-11-08 14:12:04,414] 2165 0025 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(8) 0x27b1f8} CanAccept: Reject msg: call=1,
transport=0, filter=0 localPort=0
[2012-11-08 14:12:04,414] 2166 0024 com.net.ux.sip DEBUG
(sipSignalingGroupConfig.cpp:672) - getBestSubnet: 10.1.1.90 - 10.1.1.76
[2012-11-08 14:12:04,414] 2167 0023 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(7) 0x27e328} CanAccept: Reject msg: call=1,
transport=1, filter=0 localPort=1
[2012-11-08 14:12:04,414] 2168 0022 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(6) 0x281018} CanAccept: Reject msg: call=1,
transport=0, filter=0 localPort=0
[2012-11-08 14:12:04,414] 2169 0021 com.net.ux.sip DEBUG
(sipSignalingGroupConfig.cpp:672) - getBestSubnet: 10.1.1.90 - 10.1.1.76
[2012-11-08 14:12:04,414] 2170 0020 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(4) 0x288528} CanAccept: Reject msg: call=1,
transport=1, filter=0 localPort=1
[2012-11-08 14:12:04,415] 2171 001f com.net.ux.sip DEBUG
(sipSignalingGroupConfig.cpp:672) - getBestSubnet: 10.1.1.90 - 0.0.0.0
[2012-11-08 14:12:04,415] 2172 001e com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(2) 0x28dfe8} CanAccept: Reject msg: call=1,
transport=0, filter=0 localPort=0
[2012-11-08 14:12:04,415] 2173 001d com.net.ux.sip DEBUG (sipSignalingGroup.cpp:792)
- {SG(3) 0x28b360} ProcessTransportMessage: Protocol Repair,calling Ingress
executive(2 item(s) on list)
[2012-11-08 14:12:04,415] 2174 001c com.net.ux.sip DEBUG (Executive.cpp:52) - Run:
Protocol Engine::Executive running 2 rules
[2012-11-08 14:12:04,415] 2175 001b com.net.ux.sip TRACE (Executive.cpp:58) - Run:
Protocol Engine::getting ruleid (7)
[2012-11-08 14:12:04,415] 2176 001a com.net.ux.sip TRACE (Executive.cpp:75) - Run:
Processing Message Rule (0 calls from 10.1.1.90)
[2012-11-08 14:12:04,415] 2177 0019 com.net.ux.sip TRACE (Executive.cpp:127) -
processMessageRule: Processing Message Rule (7)
[2012-11-08 14:12:04,415] 2178 0018 com.net.ux.sip TRACE (Executive.cpp:1252) -
MatchSipMessageRule: StartLine from configuration (*)From Msg (INVITE
sip:0@10.1.1.74 SIP/2.0)
[2012-11-08 14:12:04,415] 2179 0017 com.net.ux.sip DEBUG (RegexRule.h:74) -
debugInfo: RegexRule:: RuleType(0), Expression((c\=IN.IP4.10.1.1.90))

[2012-11-08 14:12:04,415] 2180 0016 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(\1)
[2012-11-08 14:12:04,415] 2181 0015 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(\1)
[2012-11-08 14:12:04,415] 2182 0014 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(0)  Result(0) Description(To Zero from IP media
10.1.1.90) valid(true), Condition Expression(${1})
[2012-11-08 14:12:04,415] 2183 0013 com.net.ux.sip TRACE (Executive.cpp:186) -
processMessageRule: Processing Regex rule
[2012-11-08 14:12:04,415] 2184 0012 com.net.ux.sip TRACE (Executive.cpp:263) -
processRegexMessage: Processing Regex Conditions Count=1
[2012-11-08 14:12:04,415] 2185 0011 com.net.ux.sip TRACE (Executive.cpp:640) -
processConditionRules: Condition Rule value=1
[2012-11-08 14:12:04,415] 2186 0010 com.net.ux.sip TRACE (Executive.cpp:652) -
evaluateConditionRuleTruth: CREId=1
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-11-08 14:12:04,415] 2187 000f com.net.ux.sip DEBUG (ConditionRule.h:121) -
debugInfo: ConditionRule:: Description: dialed 0 AdminState(0) Result(0) Operand(1)
valid(true)
[2012-11-08 14:12:04,415] 2188 000e com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(header["to",1].uri[1].userinfo.user)
[2012-11-08 14:12:04,415] 2189 000d com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-08 14:12:04,415] 2190 000c com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(0)
[2012-11-08 14:12:04,415] 2191 000b com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(0)
[2012-11-08 14:12:04,415] 2192 000a com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-11-08 14:12:04,415] 2193 0009 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-11-08 14:12:04,415] 2194 0008 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(3:Header) value:
[2012-11-08 14:12:04,416] 2195 0007 com.net.ux.sip TRACE (Executive.cpp:706) -
evaluateConditionRuleTruth: Full CR match=1. oObj=0, oMatch=0, oObjLen=1,
oMatchLen=1
[2012-11-08 14:12:04,416] 2196 0006 com.net.ux.sip TRACE (Executive.cpp:270) -
processRegexMessage: Condition matched
[2012-11-08 14:12:04,416] 2197 0005 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-11-08 14:12:04,416] 2198 0004 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-11-08 14:12:04,416] 2199 0003 com.net.ux.sip TRACE (Executive.cpp:295) -
processRegexMessage: RuleRegex replacement=\1, exp=(c\=IN.IP4.10.1.1.90)
[2012-11-08 14:12:04,416] 2200 0002 com.net.ux.sip TRACE (Executive.cpp:785) -
messageRegex: Executing Message Regex
[2012-11-08 14:12:04,416] 2201 0001 com.net.ux.sip WARN
(GenericUriListHeader.cpp:41) - encode: encode error hdr:Contact uri-count:0
this:0x263d88
[2012-11-08 14:12:04,418] 2202 0001 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(0:Message) value:
[2012-11-08 14:12:04,419] 2203 0001 com.net.ux.sip TRACE (SipMessage.cpp:1392) -
setObjectValue: name:(0:Message) value:INVITE sip:0@10.1.1.74 SIP/2.0
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Call-ID: MTAzZGZhY2ZlMDkwZjE1N2M5MTdkYzdmMWE4MzcyOWE.
Contact: <sip:444@10.1.1.90:6336>
Content-Length: 508
Content-Type: application/sdp
CSeq: 1 INVITE
From: "test" <sip:444@10.1.1.74>;tag=3f31e106
Max-Forwards: 70
To: "0" <sip:0@10.1.1.74>
User-Agent: eyeBeam release 1011w stamp 41324
Via: SIP/2.0/UDP
10.1.1.90:6336;branch=z9hG4bK-d87543-28224e612861dc20-1--d87543-;rport

v=0
o=- 5 2 IN IP4 10.1.1.90
s=CounterPath eyeBeam 1.5
c=IN IP4 10.1.1.90
t=0 0
m=audio 7092 RTP/AVP 107 100 106 6 0 105 8 18 3 5 101
a=alt:1 2 : 4memZGA5 jvFXZUL/ 10.1.1.90 7092
a=alt:2 1 : fRF9Sxzc EyUo4lyB 192.168.128.5 7092
a=fmtp:18 annexb=yes
a=fmtp:101 0-15
a=rtpmap:107 BV32/16000
a=rtpmap:100 SPEEX/16000
a=rtpmap:106 SPEEX-FEC/16000
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
a=rtpmap:105 SPEEX-FEC/8000
a=rtpmap:1Ä-PÑ+L[2012-11-08 14:10:12,994] 6300 0001 com.net.ux.sip DEBUG
(StatusCode.cpp:601) - lookup: [2012-11-08 14:12:04,420] 2204 0001 com.net.ux.sip
TRACE (SipMessage.cpp:569) - decodeHeaders: SIP message Header type Allow
[2012-11-08 14:12:04,420] 2205 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Call-ID
[2012-11-08 14:12:04,420] 2206 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Contact
[2012-11-08 14:12:04,420] 2207 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Content-Length
[2012-11-08 14:12:04,420] 2208 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Content-Type
[2012-11-08 14:12:04,420] 2209 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type CSeq
[2012-11-08 14:12:04,420] 2210 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type From
[2012-11-08 14:12:04,420] 2211 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Max-Forwards
[2012-11-08 14:12:04,420] 2212 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type To
[2012-11-08 14:12:04,421] 2213 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type User-Agent
[2012-11-08 14:12:04,421] 2214 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Via
[2012-11-08 14:12:04,422] 2215 0001 com.net.ux.sip TRACE (Executive.cpp:297) -
processRegexMessage: RuleRegex return:(1)n
[2012-11-08 14:12:04,422] 2216 0001 com.net.ux.sip DEBUG (HeaderRule.h:912) -
debugInfo: HeaderRuleFieldModify
[2012-11-08 14:12:04,422] 2217 0001 com.net.ux.sip DEBUG (HeaderRule.h:798) -
debugInfo: HeaderRuleFieldChange mReplacement
[2012-11-08 14:12:04,422] 2218 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(3539)
[2012-11-08 14:12:04,422] 2219 0001 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(3539)
[2012-11-08 14:12:04,423] 2220 0001 com.net.ux.sip DEBUG (HeaderRule.h:679) -
debugInfo: HeaderRuleField:: Element
[2012-11-08 14:12:04,423] 2221 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(requestline.uri.userinfo.user)
[2012-11-08 14:12:04,423] 2222 0001 com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-08 14:12:04,423] 2223 0001 com.net.ux.sip DEBUG (HeaderRule.h:115) -
debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-11-08 14:12:04,423] 2224 0001 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(1)  Result(1) Description(change number)
valid(true), Condition Expression(No conditions for this header rule)
[2012-11-08 14:12:04,423] 2225 0001 com.net.ux.sip TRACE (Executive.cpp:211) -
processMessageRule: Processing Header rule
[2012-11-08 14:12:04,423] 2226 0001 com.net.ux.sip DEBUG (Executive.cpp:316) -
processHeaderRule: Processing header Rule (change number)
[2012-11-08 14:12:04,423] 2227 0001 com.net.ux.sip TRACE (Executive.cpp:489) -
processHeaderRule: Processing Rule Field Modify
[2012-11-08 14:12:04,423] 2228 0001 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-11-08 14:12:04,423] 2229 0001 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-11-08 14:12:04,423] 2230 0001 com.net.ux.sip TRACE (Executive.cpp:1161) -
headerFieldModify: Executing header field modify, replacement=3539
[2012-11-08 14:12:04,423] 2231 0001 com.net.ux.sip TRACE (Executive.cpp:1165) -
headerFieldModify: Header field modify single ordinal
[2012-11-08 14:12:04,424] 2232 0001 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(1:RequestLine) value:
[2012-11-08 14:12:04,424] 2233 0001 com.net.ux.sip TRACE (SipMessage.cpp:1392) -
setObjectValue: name:(1:RequestLine) value:3539
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-11-08 14:12:04,424] 2234 0001 com.net.ux.sip TRACE (Executive.cpp:218) -
processMessageRule: HeaderRule executed
[2012-11-08 14:12:04,424] 2235 0001 com.net.ux.sip DEBUG (HeaderRule.h:912) -
debugInfo: HeaderRuleFieldModify
[2012-11-08 14:12:04,424] 2236 0001 com.net.ux.sip DEBUG (HeaderRule.h:798) -
debugInfo: HeaderRuleFieldChange mReplacement
[2012-11-08 14:12:04,424] 2237 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(3539)
[2012-11-08 14:12:04,424] 2238 0001 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(3539)
[2012-11-08 14:12:04,424] 2239 0001 com.net.ux.sip DEBUG (HeaderRule.h:679) -
debugInfo: HeaderRuleField:: Element
[2012-11-08 14:12:04,424] 2240 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(header["to",1].uri.userinfo.user)
[2012-11-08 14:12:04,424] 2241 0001 com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-08 14:12:04,424] 2242 0001 com.net.ux.sip DEBUG (HeaderRule.h:115) -
debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-11-08 14:12:04,425] 2243 0001 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(1)  Result(1) Description(change the TO number)
valid(true), Condition Expression(No conditions for this header rule)
[2012-11-08 14:12:04,425] 2244 0001 com.net.ux.sip TRACE (Executive.cpp:211) -
processMessageRule: Processing Header rule
[2012-11-08 14:12:04,425] 2245 0001 com.net.ux.sip DEBUG (Executive.cpp:316) -
processHeaderRule: Processing header Rule (change the TO number)
[2012-11-08 14:12:04,425] 2246 0001 com.net.ux.sip TRACE (Executive.cpp:489) -
processHeaderRule: Processing Rule Field Modify
[2012-11-08 14:12:04,425] 2247 0001 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-11-08 14:12:04,425] 2248 0001 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-11-08 14:12:04,425] 2249 0001 com.net.ux.sip TRACE (Executive.cpp:1161) -
headerFieldModify: Executing header field modify, replacement=3539
[2012-11-08 14:12:04,425] 2250 0001 com.net.ux.sip TRACE (Executive.cpp:1297) -
checkOrdinalAll: ObjectToken:: StringIndex(to) Ordinal(1)
[2012-11-08 14:12:04,425] 2251 0001 com.net.ux.sip TRACE (Executive.cpp:1165) -
headerFieldModify: Header field modify single ordinal
[2012-11-08 14:12:04,425] 2252 0001 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(3:Header) value:
[2012-11-08 14:12:04,425] 2253 0001 com.net.ux.sip TRACE (SipMessage.cpp:1392) -
setObjectValue: name:(3:Header) value:3539
[2012-11-08 14:12:04,426] 2254 0001 com.net.ux.sip TRACE (Executive.cpp:218) -
processMessageRule: HeaderRule executed
[2012-11-08 14:12:04,426] 2255 0001 com.net.ux.sip TRACE (Executive.cpp:81) - Run:
Message Rule (7) matched at least one message rule
[2012-11-08 14:12:04,426] 2256 0001 com.net.ux.sip TRACE (Executive.cpp:58) - Run:
Protocol Engine::getting ruleid (8)
[2012-11-08 14:12:04,426] 2257 0001 com.net.ux.sip TRACE (Executive.cpp:75) - Run:
Processing Message Rule (0 calls from 10.1.1.91)
[2012-11-08 14:12:04,426] 2258 0001 com.net.ux.sip TRACE (Executive.cpp:127) -
processMessageRule: Processing Message Rule (8)
[2012-11-08 14:12:04,426] 2259 0001 com.net.ux.sip TRACE (Executive.cpp:1252) -
MatchSipMessageRule: StartLine from configuration (*)From Msg (INVITE
sip:0@10.1.1.74 SIP/2.0)
[2012-11-08 14:12:04,426] 2260 0001 com.net.ux.sip DEBUG (RegexRule.h:74) -
debugInfo: RegexRule:: RuleType(0), Expression((c\=IN.IP4.10.1.1.91))

[2012-11-08 14:12:04,426] 2261 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(\1)
[2012-11-08 14:12:04,426] 2262 0001 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(\1)
[2012-11-08 14:12:04,427] 2263 0001 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(0)  Result(0) Description(Call to Zero from
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
10.1.1.91) valid(true), Condition Expression(${1})
[2012-11-08 14:12:04,427] 2264 0001 com.net.ux.sip TRACE (Executive.cpp:186) -
processMessageRule: Processing Regex rule
[2012-11-08 14:12:04,427] 2265 0001 com.net.ux.sip TRACE (Executive.cpp:263) -
processRegexMessage: Processing Regex Conditions Count=1
[2012-11-08 14:12:04,427] 2266 0001 com.net.ux.sip TRACE (Executive.cpp:640) -
processConditionRules: Condition Rule value=1
[2012-11-08 14:12:04,427] 2267 0001 com.net.ux.sip TRACE (Executive.cpp:652) -
evaluateConditionRuleTruth: CREId=1
[2012-11-08 14:12:04,427] 2268 0001 com.net.ux.sip DEBUG (ConditionRule.h:121) -
debugInfo: ConditionRule:: Description: dialed 0 AdminState(0) Result(0) Operand(1)
valid(true)
[2012-11-08 14:12:04,427] 2269 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(header["to",1].uri[1].userinfo.user)
[2012-11-08 14:12:04,427] 2270 0001 com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-08 14:12:04,427] 2271 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(0)
[2012-11-08 14:12:04,427] 2272 0001 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(0)
[2012-11-08 14:12:04,428] 2273 0001 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-11-08 14:12:04,428] 2274 0001 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-11-08 14:12:04,428] 2275 0001 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(3:Header) value:
[2012-11-08 14:12:04,428] 2276 0001 com.net.ux.sip TRACE (Executive.cpp:706) -
evaluateConditionRuleTruth: Full CR match=0. oObj=3539, oMatch=0, oObjLen=4,
oMatchLen=1
[2012-11-08 14:12:04,428] 2277 0001 com.net.ux.sip TRACE (Executive.cpp:273) -
processRegexMessage: Condition did not match
[2012-11-08 14:12:04,428] 2278 0001 com.net.ux.sip TRACE (Executive.cpp:86) - Run:
Message Rule (8) no message rules matched
[2012-11-08 14:12:04,428] 2279 0001 com.net.ux.sip DEBUG (sipSignalingGroup.cpp:794)
- {SG(3) 0x28b360} ProcessTransportMessage: Protocol Repair, out of Ingress
executive

....
[2012-11-08 14:12:04,454] 2488 0071 com.net.ux.sip DEBUG (TransportLayer.cpp:538) -
0x2af8f0 sending from [0.0.0.0]:5060 to [10.1.1.90]:6336 403 bytes over 10UDP1-5060
attempt(1) (If:0) ln(1323):
[2012-11-08 14:12:04,454] 2489 0070

SIP/2.0 100 Trying
Call-ID: MTAzZGZhY2ZlMDkwZjE1N2M5MTdkYzdmMWE4MzcyOWE.
Contact: <sip:10.1.1.74:5060;transport=UDP>
Content-Length: 0
CSeq: 1 INVITE
From: "test" <sip:444@10.1.1.74>;tag=3f31e106
Server: NET UX 2.2.1v999 UX
Supported: replaces,update,100rel
To: "0" <sip:3539@10.1.1.74>;tag=a01014a-45c
Via: SIP/2.0/UDP
10.1.1.90:6336;branch=z9hG4bK-d87543-28224e612861dc20-1--d87543-;rport

.....

2-11-08 14:12:04,533] 2753 001a com.net.ux.route INFO (callrouter.cpp:2280) - Using
table EUM Routes (6) to route call.
[2012-11-08 14:12:04,534] 2754 0019 com.net.ux.route DEBUG (translation.cpp:1295) -
Performing OPTIONAL transformation using entry Subscriber Access # from PSTN
(5.1(1)).
[2012-11-08 14:12:04,534] 2755 0018 com.net.ux.route DEBUG (translation.cpp:634) -
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
Failed regex match of "tfCalledNumber" field for "(\+14083483539)" (updated
"(\+14083483539)") with input of "3539"
[2012-11-08 14:12:04,534] 2756 0017 com.net.ux.route DEBUG (translation.cpp:1295) -
Performing OPTIONAL transformation using entry EUM SA 302 route (5.2(2)).
[2012-11-08 14:12:04,534] 2757 0016 com.net.ux.route DEBUG (translation.cpp:638) -
Successful regex match of "tfCalledNumber" field for "3539" (updated "3539") with
input of "3539"
[2012-11-08 14:12:04,534] 2758 0015 com.net.ux.route DEBUG (translation.cpp:683) -
Regex replacement output of "tfCalledNumber" field is "3539"
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-11-08 14:12:04,534] 2759 0014 com.net.ux.route INFO (callrouter.cpp:2403) -
Successful route request with entry Call to Exchange (6.1(9))
```

Important Notes

The SIP Header feature cannot **generate** a new SIP packet. Only arriving or leaving SIP packets changed via the SIP Header function.

Care must be exercised when modifying incoming SIP packets, especially with respects to the TO, FROM and RURI headers. Modifying tags, IDs or any other items that define the dialogue or transactions, will likely cause calls to not complete.

This configuration note does not detailed a supported configuration as changing the RURI number of a call may lead to numerous interoperability issues.

rev 0.4

Correcting a FROM Tag using SIP Message Manipulation

Table of Contents

- Prerequistes
- Summary
- Repairing the FROM Tag
  - Configure the SBC1000/2000 for Header Manipulation
  - Debugging Output
  - Important Notes

About this Page

- This document details how to configure the SBC to repair the Tag in a FROM header.
- This document deatils the manipulation of SIP URI and Header parameters.
- This document features SMM's URI and Header Parameter options.
- This document employs the *SG User Value* token

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups

Prerequistes

Copyright © 2015 Sonus Networks. All rights reserved.

Requires Sonus SBC1000/2000 Version 2.2

Summary

Some implementations do not place < > (brackets) around the URI portion of the FROM header. Without the brackets, UX parses the Tag as a URI parameter rather than a header parameter.

The following SMM configuration can be used to repair the issue.

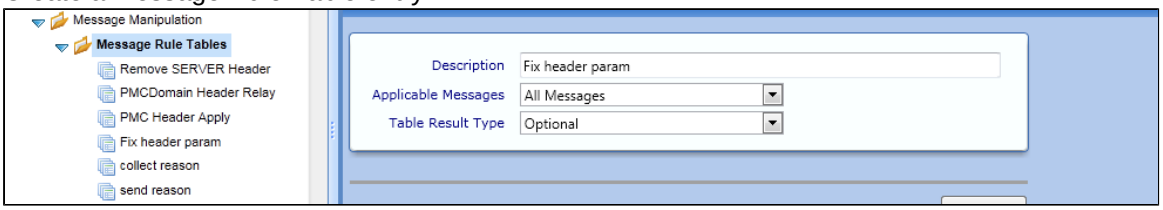
Repairing the FROM Tag

Notice that the FROM header below is missing the brackets that are present in the TO header. Follow the SMM steps below as the tag is copied, removed, then re-added to reform the FROM to a more standard syntax.

INVITE sip:3539@10.1.1.74 SIP/2.0
To: <sip:3539@10.1.1.74>
From: sip:14083481112@10.1.1.74;tag=b87f9f19
Via: SIP/2.0/UDP 10.1.1.90:6162;branch=z9hG4bK-d87443-840323593-1-~~d87443~~;rport
Call-ID: 1d077346843aba30
CSeq: 1 INVITE
Contact: <sip:14083481112@10.1.1.90:6162>
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: eyeBeam release 3007n stamp 90816
P-MC-Domain: aginc.com
Content-Length: 0

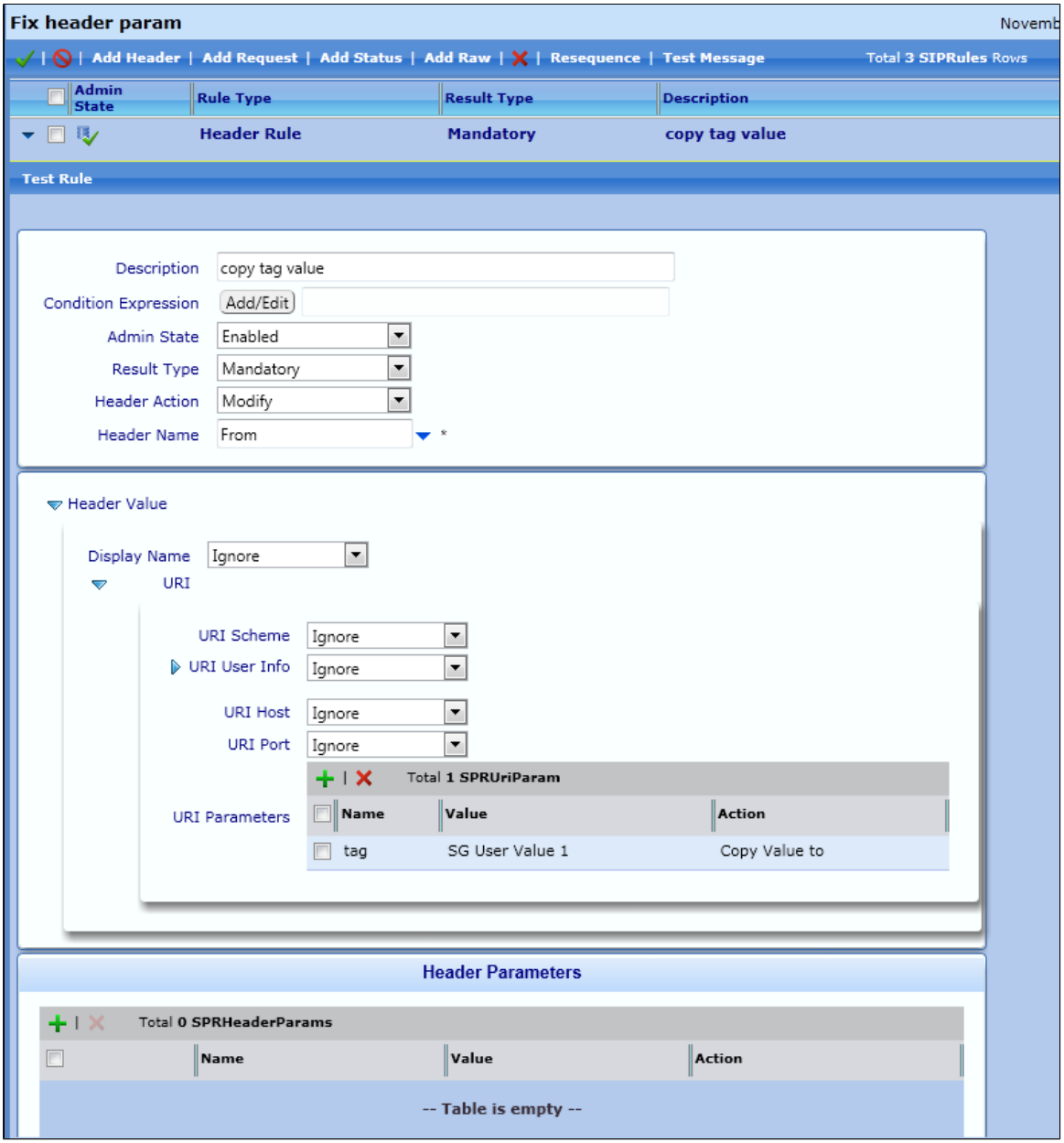
Configure the SBC1000/2000 for Header Manipulation

1. Create a Message Rule Table entry



2. Add the first SMM Rule using the *Add Header* selection. This rule copies the tag value into the *SG User Value 1* token.

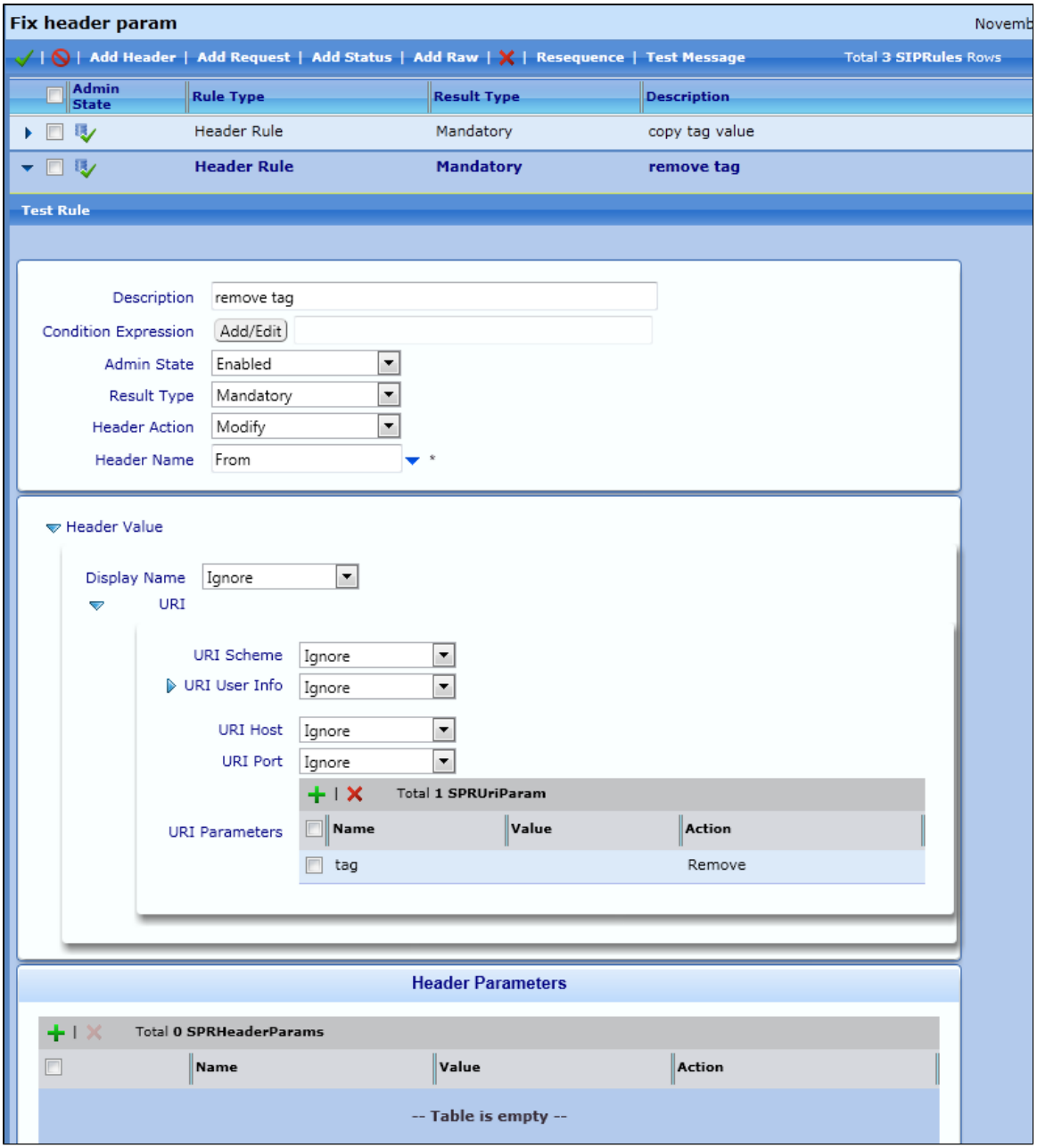
Copyright © 2015 Sonus Networks. All rights reserved.



SIP/2.0 100 Trying
Call-ID: 1d077346843aba30
Contact: <sip:10.1.1.74:5060;transport=UDP>
Content-Length: 0
CSeq: 1 INVITE
From: sip:14083481112@10.1.1.74;tag=b87f9f19 (URI parameter *tag* b87f9f19 copied to SG User Value 1)
Server: NET UX 2.2.1v187 UX
Supported: replaces,update,100rel
To: <sip:3539@10.1.1.74>;tag=a01014a-47
Via: SIP/2.0/UDP 10.1.1.90:6162;branch=z9hG4bK-d87443-840323593-1-~~d87443~~;rport

3. The second SMM Rule removes the Tag. Again, use the *Add Header* selection when creating the SMM entry.

Copyright © 2015 Sonus Networks. All rights reserved.

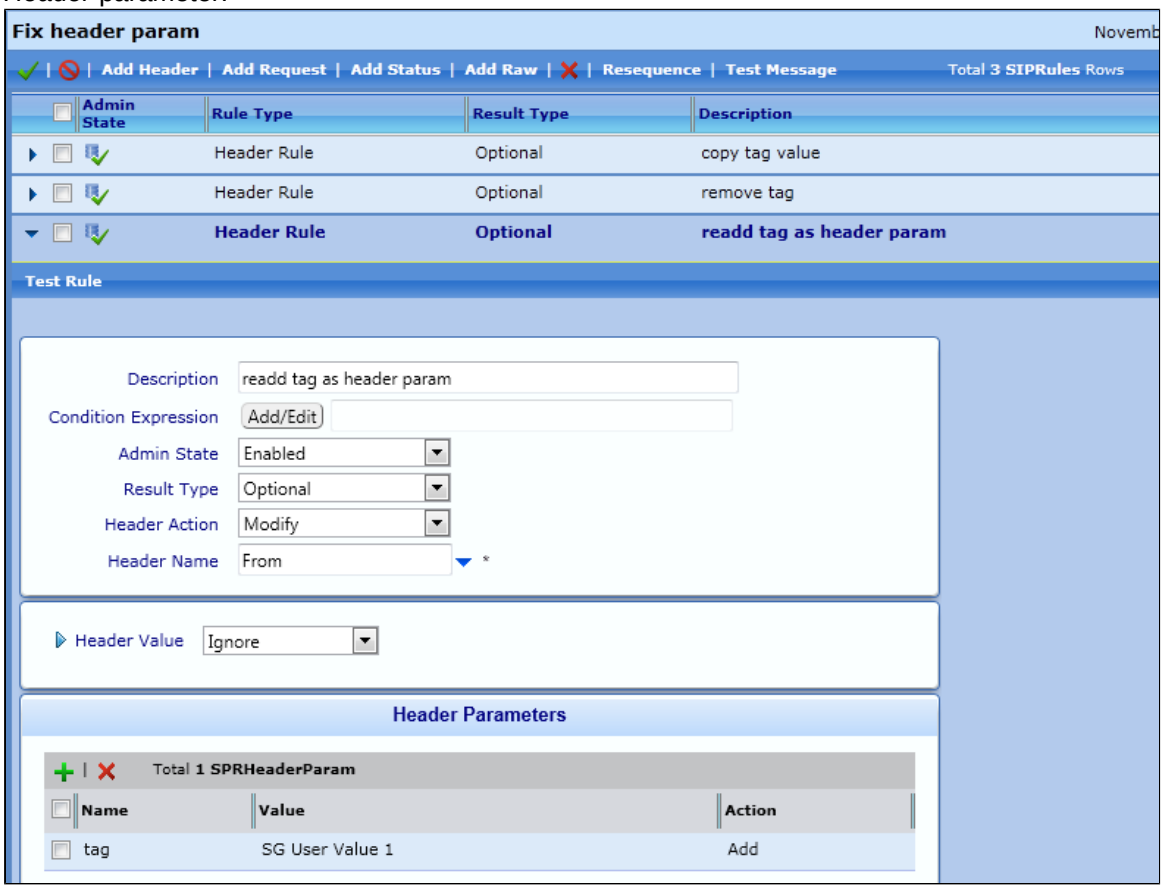


SIP/2.0 100 Trying
Call-ID: 1d077346843aba30
Contact: <sip:10.1.1.74:5060;transport=UDP>
Content-Length: 0
CSeq: 1 INVITE
From: <sip:14083481112@10.1.1.74> (URI parameter *tag* removed)
Server: NET UX 2.2.1v187 UX
Supported: replaces,update,100rel
To: <sip:3539@10.1.1.74>;tag=a01014a-47
Via: SIP/2.0/UDP 10.1.1.90:6162;branch=z9hG4bK-d87443-840323593-1-~~d87443~~;rport

4. The last SMM Rule adds a Header Parameter to the FROM header. Be sure to continue to select the *Add*

Copyright © 2015 Sonus Networks. All rights reserved.

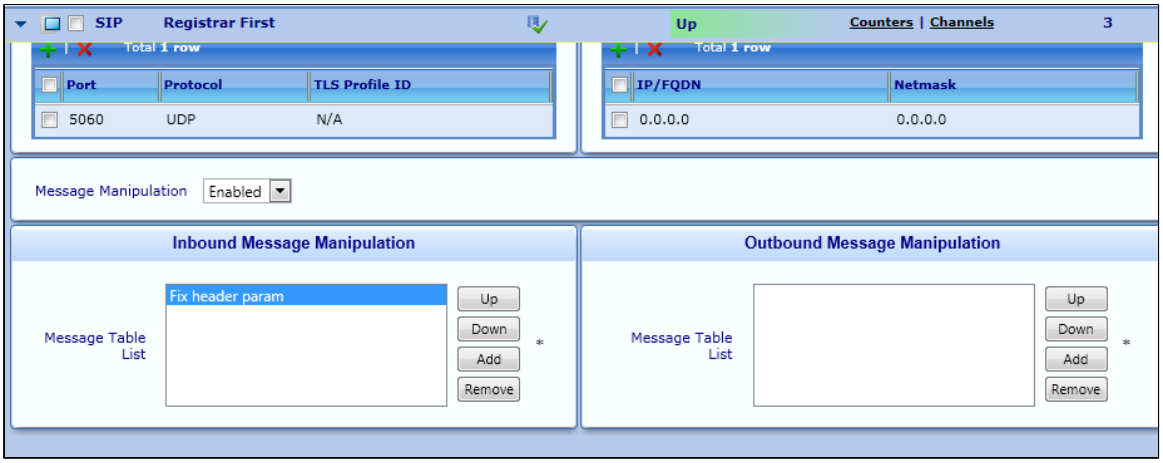
Header parameter.



SIP/2.0 100 Trying
Call-ID: 1d077346843aba30
Contact: <sip:10.1.1.74:5060;transport=UDP>
Content-Length: 0
CSeq: 1 INVITE
From: <sip:14083481112@10.1.1.74>;tag=b87f9f19 (User Value 1 added as a header parameter *tag*)
Server: NET UX 2.2.1v187 UX
Supported: replaces,update,100rel
To: <sip:3539@10.1.1.74>;tag=a01014a-47
Via: SIP/2.0/UDP 10.1.1.90:6162;branch=z9hG4bK-d87443-840323593-1-~~d87443~~;rport

5. Finally, the SMM Table Entry is added to the incoming SG.

Copyright © 2015 Sonus Networks. All rights reserved.



Debugging Output

```
INVITE sip:3539@10.1.1.74 SIP/2.0
To: <sip:3539@10.1.1.74>
From: sip:14083481112@10.1.1.74;tag=b87f9f19
Via: SIP/2.0/UDP 10.1.1.90:6162;branch=z9hG4bK-d87443-840323593-1--d87443-;rport
Call-ID: 1d077346843aba30
CSeq: 1 INVITE
Contact: <sip:14083481112@10.1.1.90:6162>
Max-Forwards: 70
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: eyeBeam release 3007n stamp 90816
P-MC-Domain: aginc.com
Content-Length: 0

[2012-11-07 16:43:38,389] 7276 002d com.net.ux.sip DEBUG
(sipSignalingGroupConfig.cpp:672) - getBestSubnet: 10.1.1.90 - 10.1.1.6
[2012-11-07 16:43:38,389] 7277 002c com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(1) 0x299190} CanAccept: Reject msg: call=1,
transport=1, filter=0 localPort=1
[2012-11-07 16:43:38,389] 7278 002b com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(9) 0x2281e0} CanAccept: Reject msg: call=1,
transport=0, filter=0 localPort=0
[2012-11-07 16:43:38,389] 7279 002a com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(8) 0x253350} CanAccept: Reject msg: call=1,
transport=0, filter=0 localPort=0
[2012-11-07 16:43:38,389] 7280 0029 com.net.ux.sip DEBUG
(sipSignalingGroupConfig.cpp:672) - getBestSubnet: 10.1.1.90 - 10.1.1.76
[2012-11-07 16:43:38,389] 7281 0028 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(7) 0x241198} CanAccept: Reject msg: call=1,
transport=1, filter=0 localPort=1
[2012-11-07 16:43:38,390] 7282 0027 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(6) 0x27b0e8} CanAccept: Reject msg: call=1,
transport=0, filter=0 localPort=0
[2012-11-07 16:43:38,390] 7283 0026 com.net.ux.sip DEBUG
(sipSignalingGroupConfig.cpp:672) - getBestSubnet: 10.1.1.90 - 10.1.1.76
[2012-11-07 16:43:38,390] 7284 0025 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(4) 0x279750} CanAccept: Reject msg: call=1,
transport=1, filter=0 localPort=1
[2012-11-07 16:43:38,390] 7285 0024 com.net.ux.sip DEBUG
(sipSignalingGroupConfig.cpp:672) - getBestSubnet: 10.1.1.90 - 0.0.0.0
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-11-07 16:43:38,390] 7286 0023 com.net.ux.sip TRACE
(sipSignalingGroup.cpp:1480) - {SG(2) 0x29b718} CanAccept: Reject msg: call=1,
transport=0, filter=0 localPort=0
[2012-11-07 16:43:38,390] 7287 0022 com.net.ux.sip DEBUG (sipSignalingGroup.cpp:792)
- {SG(3) 0x277be8} ProcessTransportMessage: Protocol Repair,calling Ingress
executive(1 item(s) on list)
[2012-11-07 16:43:38,390] 7288 0021 com.net.ux.sip DEBUG (Executive.cpp:52) - Run:
Protocol Engine::Executive running 1 rules
[2012-11-07 16:43:38,390] 7289 0020 com.net.ux.sip TRACE (Executive.cpp:58) - Run:
Protocol Engine::getting ruleid (4)
[2012-11-07 16:43:38,390] 7290 001f com.net.ux.sip TRACE (Executive.cpp:75) - Run:
Processing Message Rule (Fix header param)
[2012-11-07 16:43:38,390] 7291 001e com.net.ux.sip TRACE (Executive.cpp:127) -
processMessageRule: Processing Message Rule (4)
[2012-11-07 16:43:38,390] 7292 001d com.net.ux.sip TRACE (Executive.cpp:1252) -
MatchSipMessageRule: StartLine from configuration (*)From Msg (INVITE
sip:3539@10.1.1.74 SIP/2.0)
[2012-11-07 16:43:38,390] 7293 001c com.net.ux.sip DEBUG (HeaderRule.h:1069) -
debugInfo: HeaderRuleFieldCopy
[2012-11-07 16:43:38,390] 7294 001b com.net.ux.sip DEBUG (HeaderRule.h:798) -
debugInfo: HeaderRuleFieldChange mReplacement
[2012-11-07 16:43:38,390] 7295 001a com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(sguser[1])
[2012-11-07 16:43:38,390] 7296 0019 com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-07 16:43:38,390] 7297 0018 com.net.ux.sip DEBUG (HeaderRule.h:679) -
debugInfo: HeaderRuleField:: Element
[2012-11-07 16:43:38,390] 7298 0017 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(header["from",1].uri.param["tag"])
[2012-11-07 16:43:38,390] 7299 0016 com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-07 16:43:38,390] 7300 0015 com.net.ux.sip DEBUG (HeaderRule.h:115) -
debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-11-07 16:43:38,390] 7301 0014 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(1)  Result(1) Description(copy tag value)
valid(true), Condition Expression(No conditions for this header rule)
[2012-11-07 16:43:38,390] 7302 0013 com.net.ux.sip TRACE (Executive.cpp:211) -
processMessageRule: Processing Header rule
[2012-11-07 16:43:38,390] 7303 0012 com.net.ux.sip DEBUG (Executive.cpp:316) -
processHeaderRule: Processing header Rule (copy tag value)
[2012-11-07 16:43:38,391] 7304 0011 com.net.ux.sip TRACE (Executive.cpp:546) -
processHeaderRule: Processing Rule Field Copy
[2012-11-07 16:43:38,391] 7305 0010 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(3:Header) value:
[2012-11-07 16:43:38,391] 7306 000f com.net.ux.sip TRACE (SipMessage.cpp:1392) -
setObjectValue: name:(19:SGUser) value:b87f9f19
[2012-11-07 16:43:38,391] 7307 000e com.net.ux.sip TRACE (Executive.cpp:218) -
processMessageRule: HeaderRule executed
[2012-11-07 16:43:38,391] 7308 000d com.net.ux.sip DEBUG (HeaderRule.h:730) -
debugInfo: HeaderRuleFieldRemove
[2012-11-07 16:43:38,391] 7309 000c com.net.ux.sip DEBUG (HeaderRule.h:679) -
debugInfo: HeaderRuleField:: Element
[2012-11-07 16:43:38,391] 7310 000b com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(header["from",1].uri.param["tag"])
[2012-11-07 16:43:38,391] 7311 000a com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-07 16:43:38,391] 7312 0009 com.net.ux.sip DEBUG (HeaderRule.h:115) -
debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-11-07 16:43:38,391] 7313 0008 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(1)  Result(1) Description(remove tag)
valid(true), Condition Expression(No conditions for this header rule)
[2012-11-07 16:43:38,391] 7314 0007 com.net.ux.sip TRACE (Executive.cpp:211) -
processMessageRule: Processing Header rule
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-11-07 16:43:38,391] 7315 0006 com.net.ux.sip DEBUG (Executive.cpp:316) -
processHeaderRule: Processing header Rule (remove tag)
[2012-11-07 16:43:38,391] 7316 0005 com.net.ux.sip TRACE (Executive.cpp:462) -
processHeaderRule: Processing Rule Field Remove
[2012-11-07 16:43:38,391] 7317 0004 com.net.ux.sip TRACE (Executive.cpp:1203) -
headerFieldRemove: Executing header field remove
[2012-11-07 16:43:38,391] 7318 0003 com.net.ux.sip TRACE (Executive.cpp:1297) -
checkOrdinalAll: ObjectToken:: StringIndex(from) Ordinal(1)
[2012-11-07 16:43:38,391] 7319 0002 com.net.ux.sip TRACE (Executive.cpp:1208) -
headerFieldRemove: Header field remove single ordinal
[2012-11-07 16:43:38,391] 7320 0001 com.net.ux.sip TRACE (SipMessage.cpp:1573) -
removeObjectValue: name:(3:Header) value:
[2012-11-07 16:43:38,404] 7321 0001 com.net.ux.sip TRACE (Executive.cpp:218) -
processMessageRule: HeaderRule executed
[2012-11-07 16:43:38,404] 7322 0001 com.net.ux.sip DEBUG (HeaderRule.h:963) -
debugInfo: HeaderRuleFieldAdd
[2012-11-07 16:43:38,404] 7323 0001 com.net.ux.sip DEBUG (HeaderRule.h:798) -
debugInfo: HeaderRuleFieldChange mReplacement
[2012-11-07 16:43:38,404] 7324 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(sguser[1])
[2012-11-07 16:43:38,404] 7325 0001 com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-07 16:43:38,404] 7326 0001 com.net.ux.sip DEBUG (HeaderRule.h:679) -
debugInfo: HeaderRuleField:: Element
[2012-11-07 16:43:38,404] 7327 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(header["from",1].param["tag"])
[2012-11-07 16:43:38,404] 7328 0001 com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-07 16:43:38,405] 7329 0001 com.net.ux.sip DEBUG (HeaderRule.h:115) -
debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-11-07 16:43:38,405] 7330 0001 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(1)  Result(1) Description(readd tag as header
param) valid(true), Condition Expression(No conditions for this header rule)
[2012-11-07 16:43:38,405] 7331 0001 com.net.ux.sip TRACE (Executive.cpp:211) -
processMessageRule: Processing Header rule
[2012-11-07 16:43:38,405] 7332 0001 com.net.ux.sip DEBUG (Executive.cpp:316) -
processHeaderRule: Processing header Rule (readd tag as header param)
[2012-11-07 16:43:38,405] 7333 0001 com.net.ux.sip TRACE (Executive.cpp:508) -
processHeaderRule: Processing Rule Field Add
[2012-11-07 16:43:38,405] 7334 0001 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-11-07 16:43:38,405] 7335 0001 com.net.ux.sip TRACE (Executive.cpp:736) -
buildField: Building field object
[2012-11-07 16:43:38,406] 7336 0001 com.net.ux.msc DEBUG (MscAppBL.c:150) -
MODIFY_RESP_CB connID=0x01020004 cmdlvl = 0x00 result=0 reqid=0x00219d90
CmdId=0xff0d resBufLen 12 and UserDataU16Len 2 SizeofHdr 8
[2012-11-07 16:43:38,406] 7337 0001 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(19:SGUser) value:
[2012-11-07 16:43:38,406] 7338 0001 com.net.ux.msc TRACE (MscResponseMainBL.c:1792)
- connID=0x01020004,CONF_DTMFOPT respBufLen 12,B4:Aft setting DTMF realy Fifo4
0x0001:0x0006
[2012-11-07 16:43:38,406] 7339 0001 com.net.ux.sip TRACE (Executive.cpp:1131) -
headerFieldAdd: Executing header field add, replacement=b87f9f19
[2012-11-07 16:43:38,406] 7340 0001 com.net.ux.sip TRACE (Executive.cpp:1297) -
checkOrdinalAll: ObjectToken:: StringIndex(from) Ordinal(1)
[2012-11-07 16:43:38,406] 7341 0001 com.net.ux.sip TRACE (Executive.cpp:1134) -
headerFieldAdd: Header field add single ordinal
[2012-11-07 16:43:38,407] 7342 0001 com.net.ux.sip TRACE (SipMessage.cpp:1474) -
addObjectValue: name:(3:Header) value:b87f9f19
[2012-11-07 16:43:38,407] 7343 0001 com.net.ux.sip TRACE (Executive.cpp:218) -
processMessageRule: HeaderRule executed
[2012-11-07 16:43:38,407] 7344 0001 com.net.ux.sip TRACE (Executive.cpp:81) - Run:
Message Rule (4) matched at least one message rule
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-11-07 16:43:38,407] 7345 0001 com.net.ux.sip DEBUG (sipSignalingGroup.cpp:794)
- {SG(3) 0x277be8} ProcessTransportMessage: Protocol Repair, out of Ingress
executive
[2012-11-07 16:43:38,407] 7346 0001 com.net.ux.sip DEBUG
(sipSignalingGroup.cpp:1148) - {SG(3) 0x277be8} searchSessions: processing session
id 1d077346843aba30. Total 2 sessions.
[2012-11-07 16:43:38,407] 7347 0001 com.net.ux.sip DEBUG
(sipSignalingGroup.cpp:1163) - {SG(3) 0x277be8} searchSessions: searchSessions:
Session Matched
[2012-11-07 16:43:38,407] 7348 0001 com.net.ux.sip DEBUG (CallSession.cpp:1363) -
{SG(3):48 0x24bed0 0x24d398 [CID:5][1:0:3:1]} ProcessMessage: CallSession, from
Transport. No client tran match; try server 0x2f9438
[2012-11-07 16:43:38,408] 7349 0001 com.net.ux.sip DEBUG (ServerTransaction.cpp:581)
- ProcessRequest: ServerTransaction 24d170 called
[2012-11-07 16:43:38,408] 7350 0001 com.net.ux.sip DEBUG
(ServerInviteTransaction.cpp:547) - stateMachine: ServerInviteTransaction 24d170
state(1) event(4)
[2012-11-07 16:43:38,408] 7351 0001 com.net.ux.sip DEBUG
(ServerInviteTransaction.cpp:413) - stateRetransmitResponse: ServerInviteTransaction
24d170 called
[2012-11-07 16:43:38,408] 7352 0001 com.net.ux.sip.libcommon TRACE
(AFEventLoop.cpp:107) - AFEventLoop::Monitor: Adding event info fd=72 for
events=0x1, info=0x2ad9a8, pCBO=0x27e220
[2012-11-07 16:43:38,408] 7353 0001 com.net.ux.sip DEBUG (TransportLayer.cpp:1319) -
startTransaction: Sending data if=0.
[2012-11-07 16:43:38,408] 7354 0001 com.net.ux.sip.libctl DEBUG (Socket.cpp:666) -
Transmitting a packet on Socket: 14 DSCP: 40 TOS: 160 (a0)
[2012-11-07 16:43:38,410] 7355 0001 com.net.ux.msc TRACE (MscResponseMainBL.c:1087)
- connID=0x01020004 CONFERENCEId=0xffffffff Async VAPI Response came for DTMFOPT
[2012-11-07 16:43:38,410] 7356 0001 com.net.ux.sip DEBUG (TransportLayer.cpp:538) -
0x24d170 sending from [0.0.0.0]:5060 to [10.1.1.90]:6162 366 bytes over 10UDP1-5060
attempt(2) (If:0) ln(1323):
[2012-11-07 16:43:38,410] 7357 0001

SIP/2.0 100 Trying
Call-ID: 1d077346843aba30
Contact: <sip:10.1.1.74:5060;transport=UDP>
Content-Length: 0
CSeq: 1 INVITE
From:  <sip:14083481112@10.1.1.74>;tag=b87f9f19
Server: NET UX 2.2.1v187 UX
Supported: replaces,update,100rel
To:  <sip:3539@10.1.1.74>;tag=a01014a-47
```

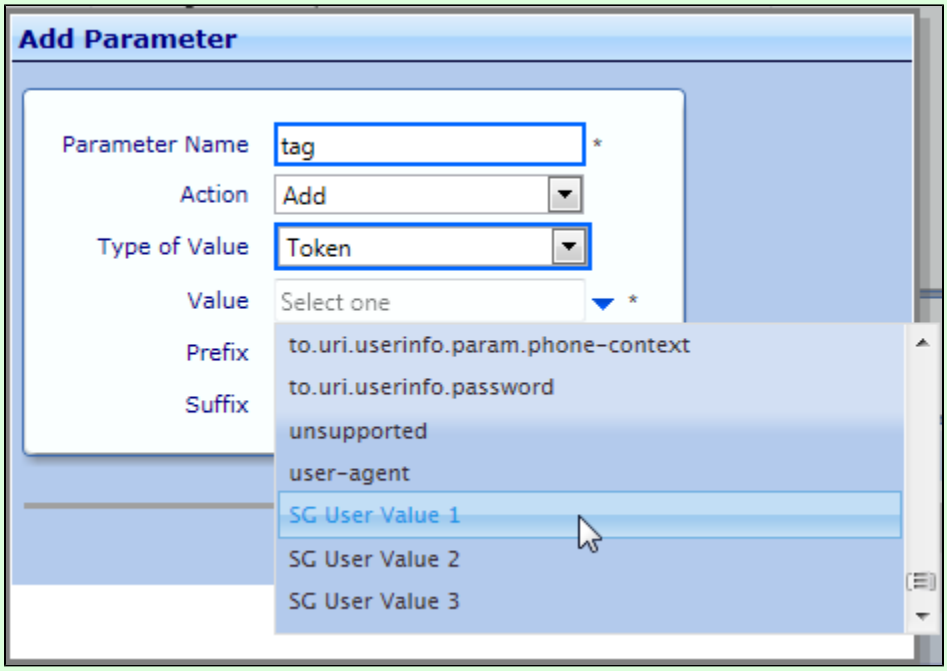
Copyright © 2015 Sonus Networks. All rights reserved.

```
Via: SIP/2.0/UDP 10.1.1.90:6162;branch=z9hG4bK-d87443-840323593-1--d87443-;rport
```

Important Notes

When you add, modify, or remove a URI or Header Parameter, type the actual parameter name you wish to effect. In this case, the *tag* parameter was the desired target.

From: <sip:14083481112@10.1.1.74>;**tag**=b87f9f19



The SIP Header feature cannot **generate** a new SIP packet. Only arriving or leaving SIP packets changed via the SIP Header function.

Care must be exercised when modifying incoming SIP packets, especially with respects to the TO, FROM and RURI headers. Modifying tags, IDs or any other items that define the dialogue or transactions, will likely cause calls to not complete.

rev 0.4

Correcting letter case using SIP Message Manipulation

Copyright © 2015 Sonus Networks. All rights reserved.

Table of Contents

- Prerequisites
- Summary
- Input Invite
- Configuring SMM to Restore Upper-Case Letters
- Output Invite

About this Page

- This document details how to configure SMM Rules to restore upper-case letters in a customer SIP header.

Related Articles

- SIP Message Manipulation Overview
- SIP Message Manipulation
- Managing Signaling Groups
- SIP Message Manipulation Document Catalog
- Optional Matching Overview

Prerequisites

Requires Sonus SBC1000/2000 Version 2.2 or later

This document assumes the user has a working knowledge of the SBC, its WebUI and the SMM function.

Summary

When adding a custom SIP header, the case of letters in the added header is not preserved. To restore the proper case, a second SMM entry, using the Raw Rule, is needed.

Input Invite

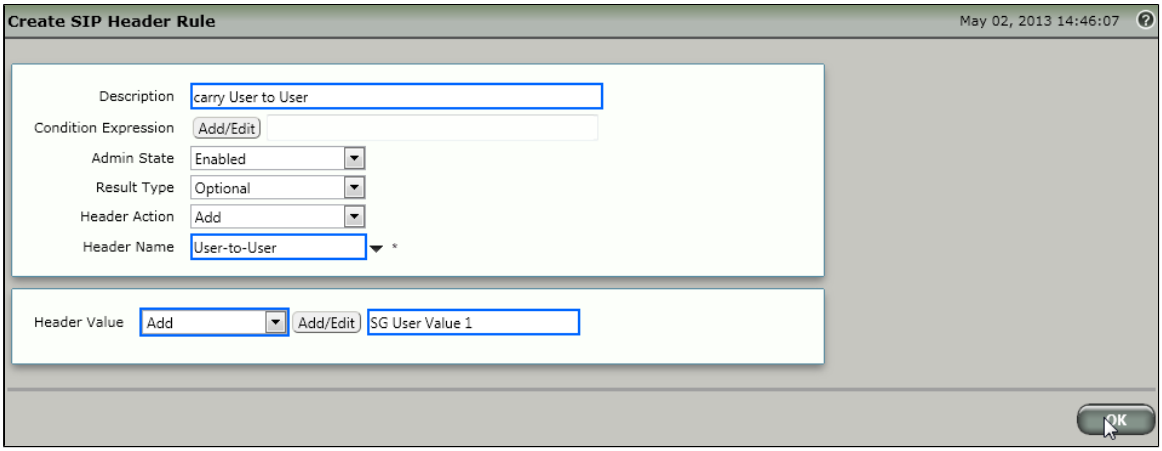
INVITE sip:6001@10.1.24.57:5060;user=phone SIP/2.0
user-to-user:
04412C312C49412C696476313130302C49445F552C41522C2C2C2C4E2C4E2C4E6F6E652C;encoding=hex
Allow: INVITE, ACK, CANCEL, BYE, UPDATE, NOTIFY, OPTIONS, REFER, REGISTER
Call-ID: call-8AA25A00-0000-0010-0C13-29@10.1.24.37
Contact: <sip:07768200610@10.1.24.37:5060;transport=UDP>
Content-Length: 263
Content-Type: application/sdp
CSeq: 1 INVITE
From: <sip:07768200610@10.1.24.37:5060>;tag=c0a8e61b-61
Max-Forwards: 70
P-Asserted-Identity: <sip:07768200610@10.1.24.37:5060>
Referred-By: <sip:33333@10.1.24.80;transport=tcp>
Supported: replaces,update,100rel

Copyright © 2015 Sonus Networks. All rights reserved.

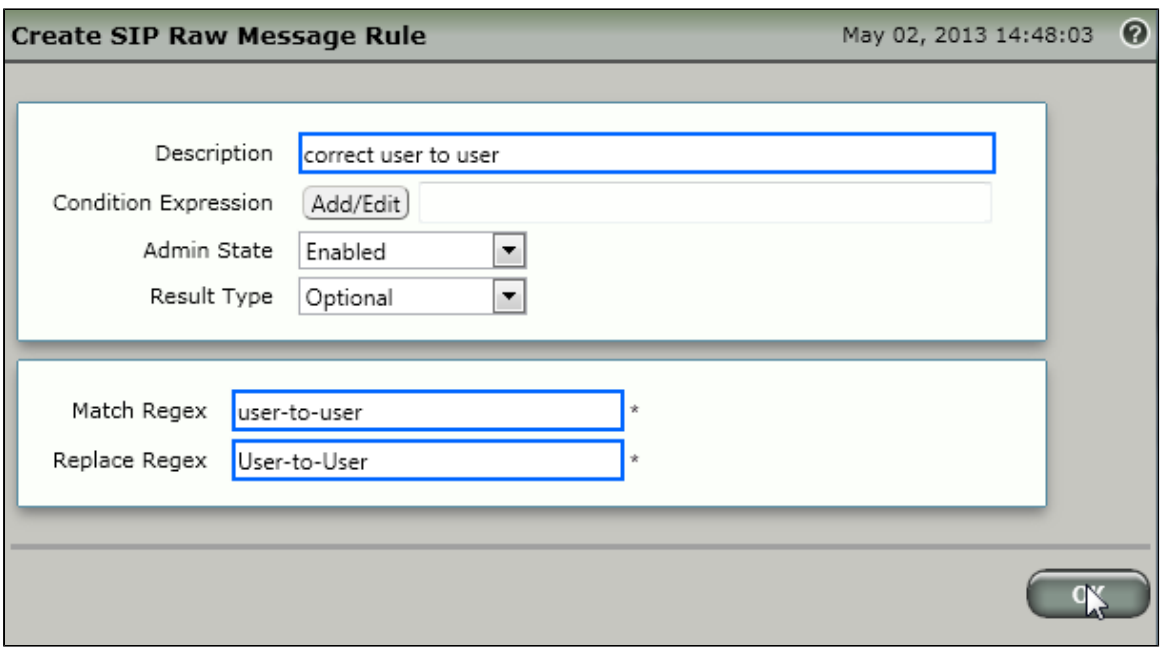
To: <sip:6001@10.1.24.57:5060;user=phone>
User-Agent: NET UX 2.2.1v195 UX
Via: SIP/2.0/UDP 10.1.24.37:5060;branch=z9hG4bK-UX-c0a8-e61b-0439

Configuring SMM to Restore Upper-Case Letters

1. Create a Header Rule that adds the User-to-User header and populates it with the value stored in *SG User Value 1*. *SG User Value 1* would have been populated using a different SMM rule at the ingress SG.

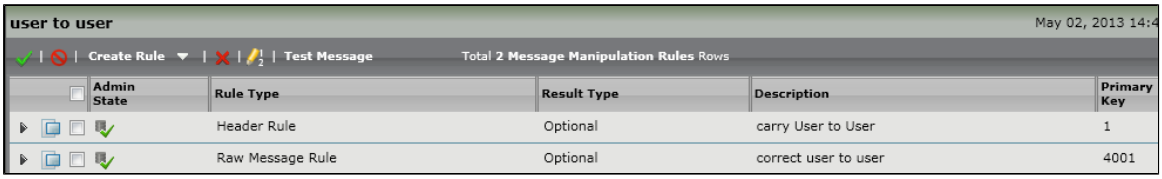


2. When the SBC creates the new header, the case of the letters is not preserved (all the upper-case letters are sent as lower-case). To re-establish the proper case, make a second entry in the SMM table - a Raw Rule. Set the regex input to the lower-case and the regex output to the desired case. The Raw Rule will restore the desired case.



Copyright © 2015 Sonus Networks. All rights reserved.

3. The resulting SMM table. Make sure to apply the SMM Table to the egress Signaling Group.



Output Invite

INVITE sip:6001@10.1.24.57:5060;user=phone SIP/2.0
User-to-User:
04412C312C49412C696476313130302C49445F552C41522C2C2C2C4E2C4E2C4E6F6E652C;encoding=hex
Allow: INVITE, ACK, CANCEL, BYE, UPDATE, NOTIFY, OPTIONS, REFER, REGISTER
Call-ID: call-8AA25A00-0000-0010-0C13-29@10.1.24.37
Contact: <sip:07768200610@10.1.24.37:5060;transport=UDP>
Content-Length: 0
Content-Type: application/sdp
CSeq: 1 INVITE
From: <sip:07768200610@10.1.24.37:5060>;tag=c0a8e61b-61
Max-Forwards: 70
P-Asserted-Identity: <sip:07768200610@10.1.24.37:5060>
Referred-By: <sip:33333@10.1.24.80;transport=tcp>
Supported: replaces,update,100rel
To: <sip:6001@10.1.24.57:5060;user=phone>
User-Agent: NET UX 2.2.1v195 UX
Via: SIP/2.0/UDP 10.1.24.37:5060;branch=z9hG4bK-UX-c0a8-e61b-0439

Modifying the m and a lines in SDP using SIP Message Manipulation

Table of Contents

- Prerequistes
- Summary
- Changing the DTMF event number
  - Configure the SBC1000/2000 Header Manipulation
  - Debugging Output
  - Important Notes

Copyright © 2015 Sonus Networks. All rights reserved.

About this Page

- This document details changing the DTMF event number in the SDP body.
- This document features the *Add Raw* function. In this example, *Add Raw* is used to search for (and possibly replace) text in the SDP body.
- **This document is only an example of how SMM might be used. An incoming media/rtpmap cannot be successfully changed because the opposing SIP device will still expect events to arrive at the original mapping. If the mapping for 2833 digits is changed by an ingress SMM from 116 to 101, the opposing device will still expect to receive 2833 digits as RTP event 116. Changing the incoming SIP SDP does not change anything in the opposing SIP device.**

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups

Prerequistes

Requires Sonus SBC1000/2000 Version 2.2 or later

Summary

This document describes how to change the DTMF event number in an incoming SDP.

Changing the DTMF event number

In this particular instance, an incoming SDP used 116 for the DTMF event instead of the standard 101. The SMM configuration below repairs both the media (m line) and the attributes (a line) to modify 116 to 101.

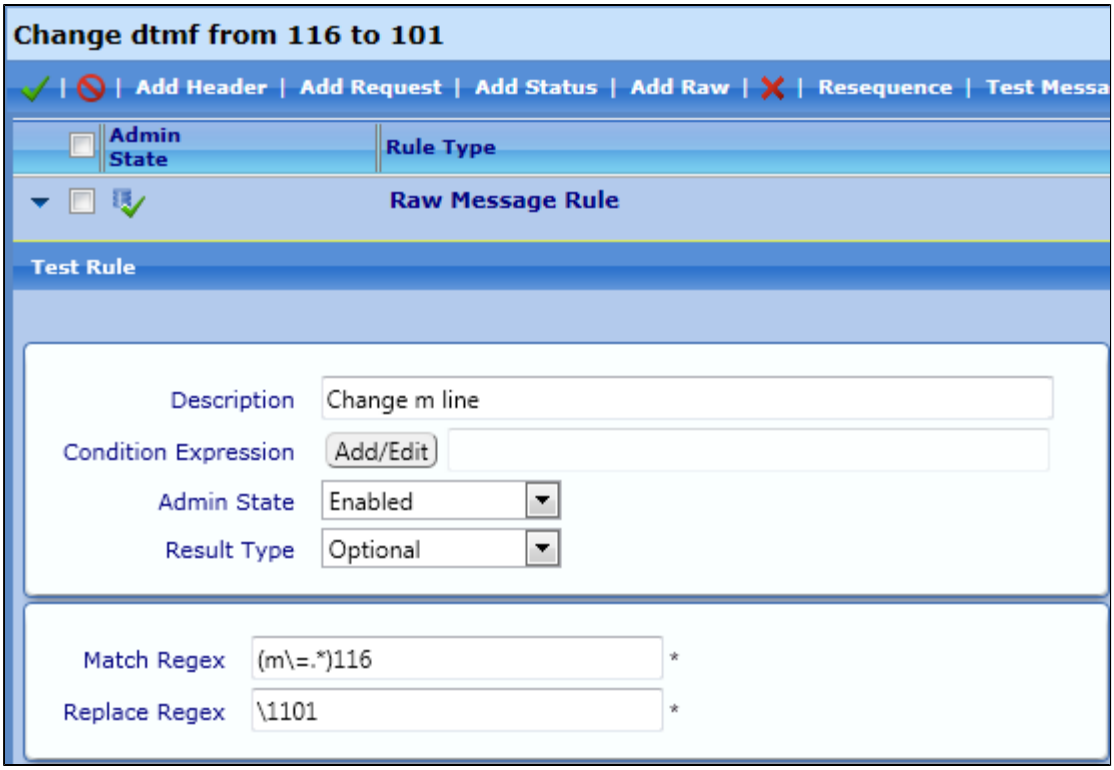
m=audio 28048 RTP/AVP 18 **116**
c=IN IP4 41.87.234.68
a=rtpmap:18 G729/8000
a=rtpmap:**116** telephone-event/8000

As mentioned in the *About This Page*, the device that originated the above SDP will still expect to receive telephone-events as RTP event 116. Changing the incoming SDP will cause the SBC to send events on 101, but the receiving device's RTP processor will still expect events to arrive at 116; DTMF digits will not function. This document is both an example of how to use the SMM Raw and Regex options, and is also a reminder that one must consider the actual protocols in order to successfully employ the SMM feature.

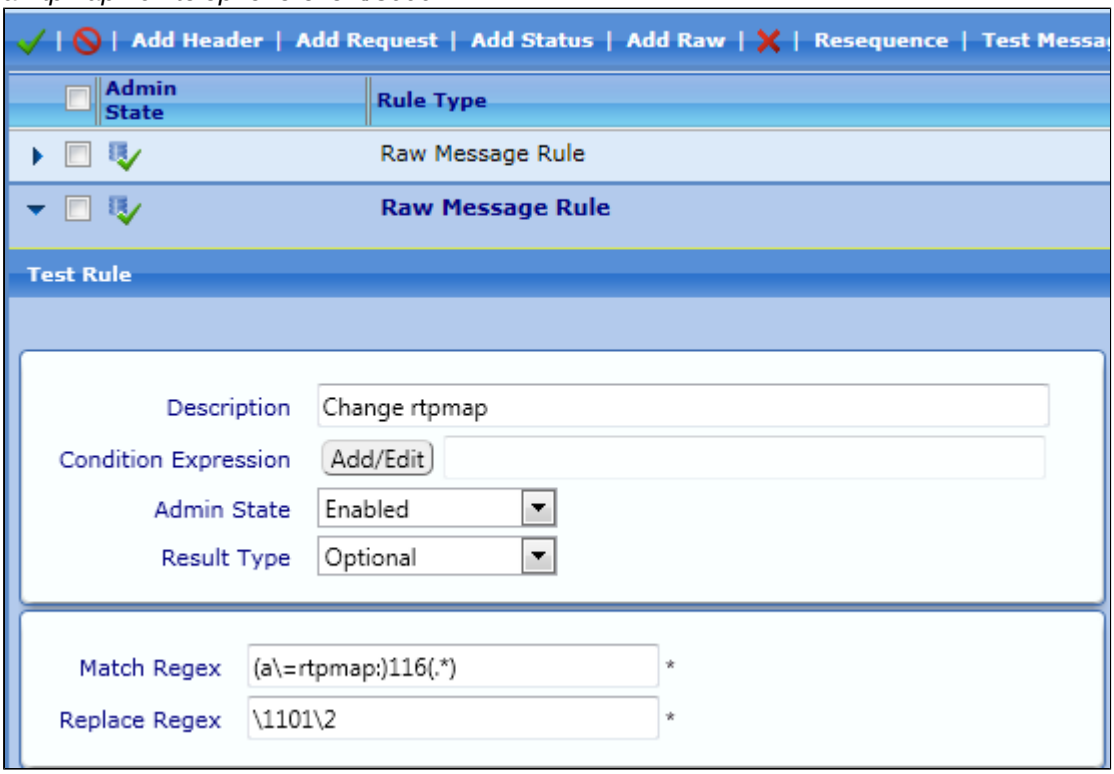
Configure the SBC1000/2000 Header Manipulation

1. Create a new Mesasge Rule Table entry and populate the first Message Rule as shown below. This entry will modify the m line from
   m=audio 28048 RTP/AVP 18 ***116*** to
   m=audio 28048 RTP/AVP 18 ***101***.

Copyright © 2015 Sonus Networks. All rights reserved.



2. Create a second Message Rule entry in the table. This entry will modify the a line from *a=rtpmap:**116** telephone-event/8000* to *a=rtpmap:**101** telephone-event/8000*



3. Add the SMM Table to the incoming Signaling Group.

Copyright © 2015 Sonus Networks. All rights reserved.



Debugging Output

```
2012-01-22 13:31:58,610] 1420 0001 com.net.ux.sip TRACE (Executive.cpp:58) - Run:
Protocol Engine::getting ruleid (19)
[2012-01-22 13:31:58,610] 1421 0001 com.net.ux.sip TRACE (Executive.cpp:75) - Run:
Processing Message Rule (Change dtmf from 116 to 101)
[2012-01-22 13:31:58,610] 1422 0001 com.net.ux.sip TRACE (Executive.cpp:127) -
processMessageRule: Processing Message Rule (19)
[2012-01-22 13:31:58,610] 1423 0001 com.net.ux.sip TRACE (Executive.cpp:1252) -
MatchSipMessageRule: StartLine from configuration (*)From Msg (INVITE
sip:3539@10.1.1.74 SIP/2.0)
[2012-01-22 13:31:58,610] 1424 0001 com.net.ux.sip DEBUG (RegexRule.h:74) -
debugInfo: RegexRule:: RuleType(0), Expression((m\=.*)116)

[2012-01-22 13:31:58,610] 1425 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(\1101)
[2012-01-22 13:31:58,611] 1426 0001 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(\1101)
[2012-01-22 13:31:58,611] 1427 0001 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(0)  Result(1) Description(Change m line)
valid(true), Condition Expression(No conditions for this header rule)
[2012-01-22 13:31:58,611] 1428 0001 com.net.ux.sip TRACE (Executive.cpp:186) -
processMessageRule: Processing Regex rule
[2012-01-22 13:31:58,611] 1429 0001 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-01-22 13:31:58,611] 1430 0001 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-01-22 13:31:58,611] 1431 0001 com.net.ux.sip TRACE (Executive.cpp:295) -
processRegexMessage: RuleRegex replacement=\1101, exp=(m\=.*)116
[2012-01-22 13:31:58,611] 1432 0001 com.net.ux.sip TRACE (Executive.cpp:785) -
messageRegex: Executing Message Regex
[2012-01-22 13:31:58,612] 1433 0001 com.net.ux.sip WARN
(GenericUriListHeader.cpp:41) - encode: encode error hdr:Contact uri-count:0
this:0x61fd58
[2012-01-22 13:31:58,612] 1434 0001 com.net.ux.sip WARN (GenericUriHeader.cpp:69) -
encode: Error in Encoding uri:0x0 type:0 this:0x309bb0
[2012-01-22 13:31:58,612] 1435 0001 com.net.ux.sip WARN (GenericUriHeader.cpp:69) -
encode: Error in Encoding uri:0x0 type:0 this:0x309c48
[2012-01-22 13:31:58,612] 1436 0001 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(0:Message) value:
[2012-01-22 13:31:58,613] 1437 0001 com.net.ux.sip TRACE (SipMessage.cpp:1392) -
setObjectValue: name:(0:Message) value:INVITE sip:3539@10.1.1.74 SIP/2.0
Cisco-Guid: 4170650438-384321033-2730718288-2880066070
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, REFER, NOTIFY, REGISTER
Call-ID: 4-1f0@10.1.1.91
Contact: sip:anonymous@10.1.1.91
Content-Length: 177
Content-Type: application/sdp
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
CSeq: 552136960 INVITE
From:  <sip:anonymous@10.1.1.74>;tag=254b0000
P-Asserted-Identity: <sip:anonymous@10.1.1.74>
Privacy:
Remote-Party-Id: <sip:anonymous@10.1.1.74>; party=calling; privacy=full
To:  <sip:3539@10.1.1.74>
User-Agent: SHOUT 3.5v70
Via: SIP/2.0/UDP 10.1.1.91

v=0
o=- 0 0 IN IP4 10.1.1.91
s=SIP call via SHOUT
c=IN IP4 10.1.1.91
b=CT:1000
t=0 0
m=audio 16392 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:116 telephone-event/8000

[2012-01-22 13:31:58,613] 1438 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Unknown
[2012-01-22 13:31:58,614] 1439 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Allow
[2012-01-22 13:31:58,614] 1440 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Call-ID
[2012-01-22 13:31:58,614] 1441 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Contact
[2012-01-22 13:31:58,614] 1442 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Content-Length
[2012-01-22 13:31:58,614] 1443 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Content-Type
[2012-01-22 13:31:58,614] 1444 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type CSeq
[2012-01-22 13:31:58,614] 1445 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type From
[2012-01-22 13:31:58,614] 1446 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type P-Asserted-Identity
[2012-01-22 13:31:58,614] 1447 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Privacy
[2012-01-22 13:31:58,614] 1448 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Remote-Party-Id
[2012-01-22 13:31:58,614] 1449 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type To
[2012-01-22 13:31:58,615] 1450 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type User-Agent
[2012-01-22 13:31:58,615] 1451 0001 com.net.ux.sip TRACE (SipMessage.cpp:569) -
decodeHeaders: SIP message Header type Via
[2012-01-22 13:31:58,616] 1452 0001 com.net.ux.sip TRACE (Executive.cpp:297) -
processRegexMessage: RuleRegex return:(1)n
[2012-01-22 13:31:58,616] 1453 0001 com.net.ux.sip DEBUG (RegexRule.h:74) -
debugInfo: RegexRule:: RuleType(0), Expression((a\=rtpmap:)116(.*))

[2012-01-22 13:31:58,616] 1454 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(\1101\2)
[2012-01-22 13:31:58,616] 1455 0001 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(\1101\2)
[2012-01-22 13:31:58,616] 1456 0001 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(0)  Result(1) Description(Change rtpmap)
valid(true), Condition Expression(No conditions for this header rule)
[2012-01-22 13:31:58,616] 1457 0001 com.net.ux.sip TRACE (Executive.cpp:186) -
processMessageRule: Processing Regex rule
[2012-01-22 13:31:58,616] 1458 0001 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-01-22 13:31:58,616] 1459 0001 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-01-22 13:31:58,617] 1460 0001 com.net.ux.sip TRACE (Executive.cpp:295) -
processRegexMessage: RuleRegex replacement=\1101\2, exp=(a\=rtpmap:)116(.*)
[2012-01-22 13:31:58,617] 1461 0001 com.net.ux.sip TRACE (Executive.cpp:785) -
messageRegex: Executing Message Regex
[2012-01-22 13:31:58,617] 1462 0001 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(0:Message) value:
[2012-01-22 13:31:58,618] 1463 0001 com.net.ux.sip TRACE (SipMessage.cpp:1392) -
setObjectValue: name:(0:Message) value:INVITE sip:3539@10.1.1.74 SIP/2.0
Cisco-Guid: 4170650438-384321033-2730718288-2880066070
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, REFER, NOTIFY, REGISTER
Call-ID: 4-1f0@10.1.1.91
Contact: <sip:anonymous@10.1.1.91>
Content-Length: 177
Content-Type: application/sdp
CSeq: 552136960 INVITE
From:  <sip:anonymous@10.1.1.74>;tag=254b0000
P-Asserted-Identity:  <sip:anonymous@10.1.1.74>
Privacy:
Remote-Party-Id:  <sip:anonymous@10.1.1.74>;party=calling;privacy=full
To:  <sip:3539@10.1.1.74>
User-Agent: SHOUT 3.5v70
Via: SIP/2.0/UDP 10.1.1.91

v=0
o=- 0 0 IN IP4 10.1.1.91
s=SIP call via SHOUT
c=IN IP4 10.1.1.91
b=CT:1000
t=0 0
m=audio 16392 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
a=rtpmap:101 telephone-event/8000
```

Important Notes

The SIP Header feature cannot **generate** a new SIP packet. Only arriving or leaving SIP packets changed via the SIP Header function.

Care must be exercised when modifying incoming SIP packets, especially with respects to the TO, FROM and RURI headers. Modifying tags, IDs or any other items that define the dialogue or transactions, will likely cause calls to not complete.

This configuration note does not detailed a supported configuration as changing the rtpmap on an incoming SDP does not change the sending device's internal rtpmaping.

rev 0.4

Properly canceling forked LYNC calls using SIP Message Manipulation

Table of Contents

- Prerequistes
- Summary
- Passing-through a CANCEL's Reason Header
  - Configure the SBC1000/2000 for Header Manipulation
  - Debugging Output
  - Important Notes

About this Page

- This document details how to configure the SBC to pass through the Reason header from LYNC's CANCEL message to any other leg that is forked by LYNC.
- This document shows the creation of a SMM Rule Table that selects only certain SIP Messages for modification. In this case, only CANCEL packets will be modified.
- This document details how to use the SMM feature to pass-through a SIP Header that is normally removed by the SBC.
- This document features the use of a Header Name that isn't included in the pre-programmed token list.

Copyright © 2015 Sonus Networks. All rights reserved.

Related Articles

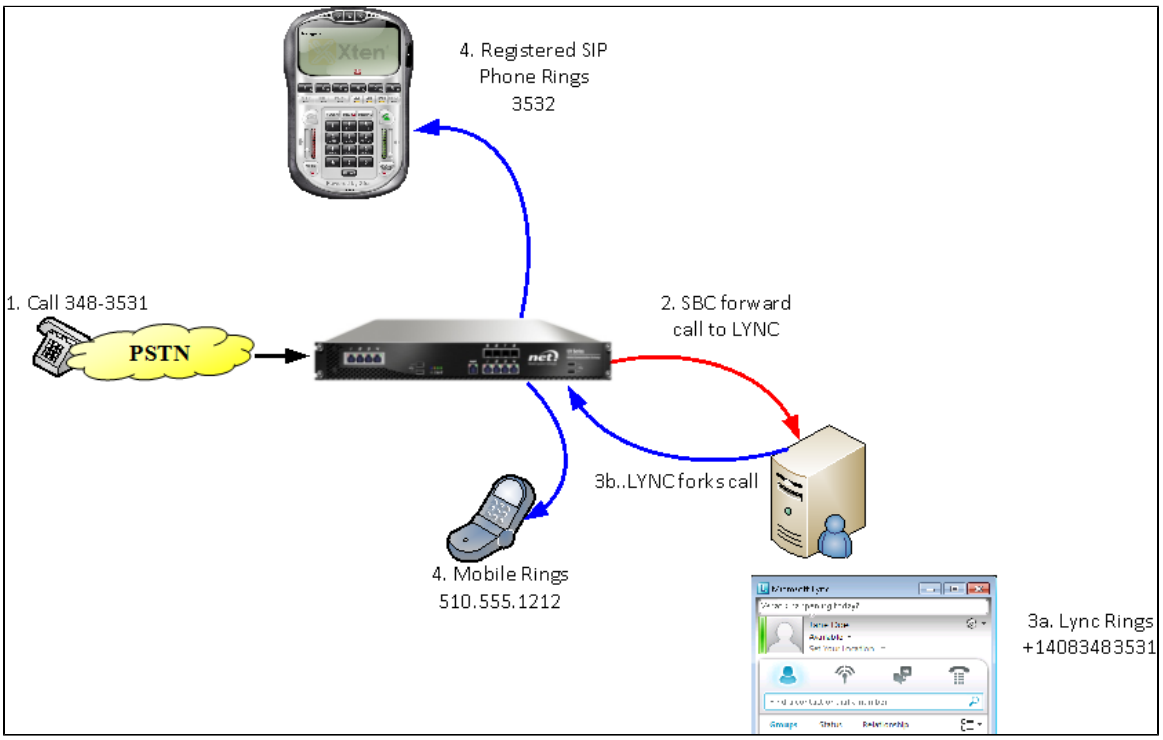
- SIP Message Manipulation
- Managing Signaling Groups

Prerequistes

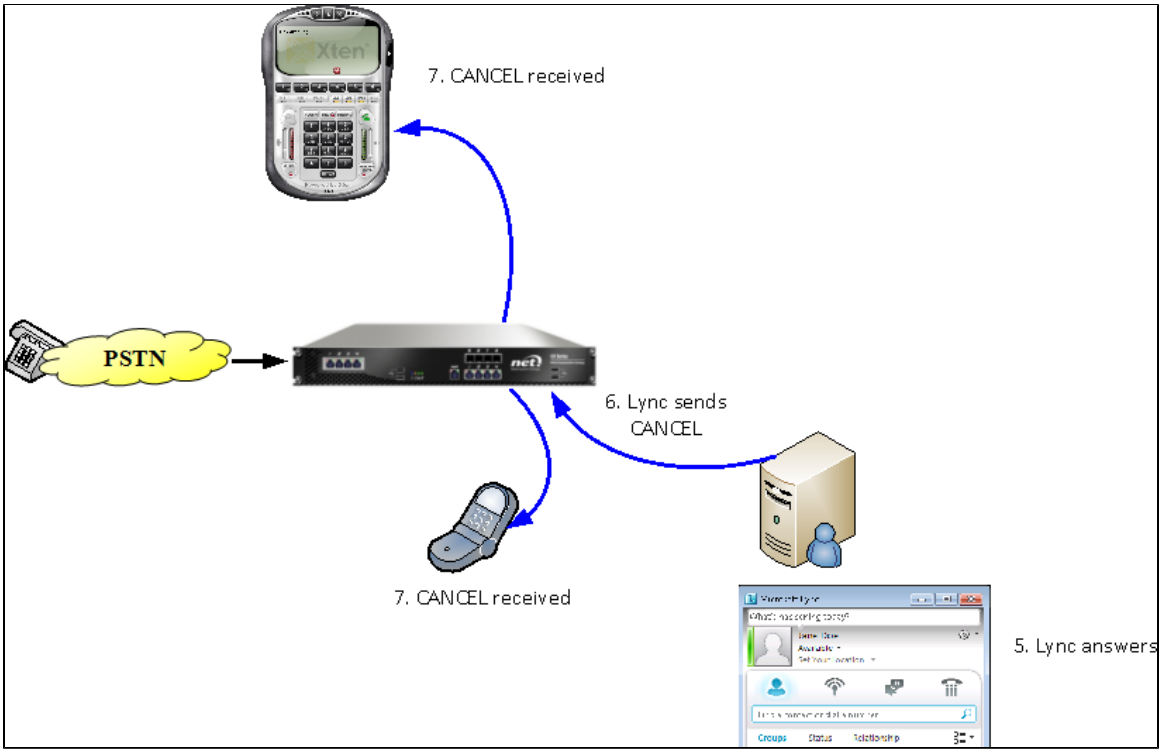
Requires Sonus SBC1000/2000 Version 2.2

Summary

When LYNC forks a call and that call is answered by one of the forked devices, LYNC will CANCEL the other forked legs. The CANCEL includes a Reason header which should stop the other forked devices from displaying a missed call notifcation.



Copyright © 2015 Sonus Networks. All rights reserved.



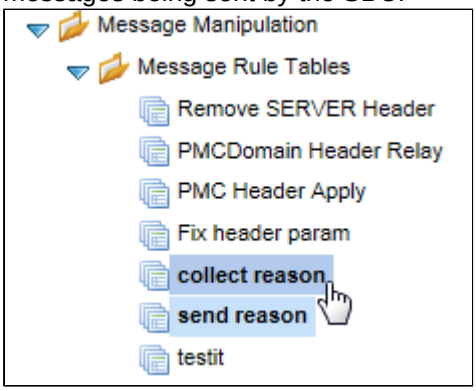
The SBC does not natively transport the received Reason header, so, using the configuration below, the SBC can pass-through the Reason header to other call legs.

Passing-through a CANCEL's Reason Header

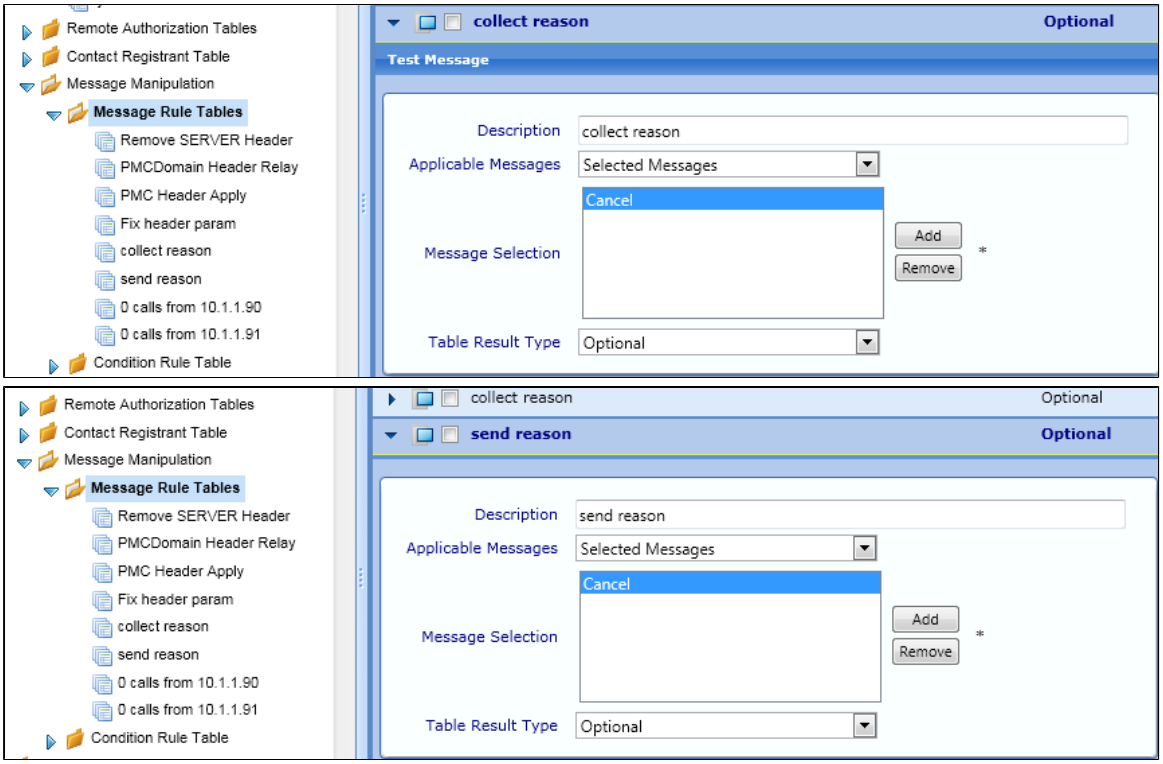
This document details how to pass a Reason Header from the incoming SIP leg to the outgoing SIP leg.

Configure the SBC1000/2000 for Header Manipulation

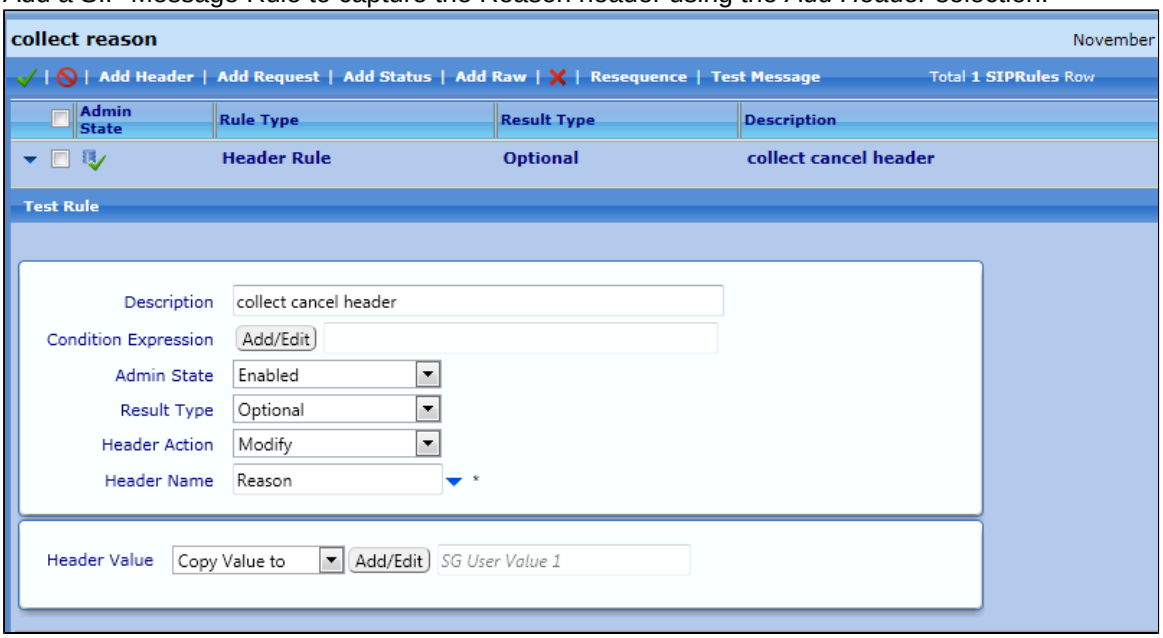
1. Create two new SIP Message Rule Tables. The first will be used to capture the SIP Reason header from SIP CANCEL messages delivered by LYNC. The second will be used to add the Reason header to CANCEL messages being sent by the SBC.



Copyright © 2015 Sonus Networks. All rights reserved.



2. Add a SIP Message Rule to capture the Reason header using the *Add Header* selection.



The Header Name *Reason* isn't included in the token drop-down list. It must be typed in by hand!

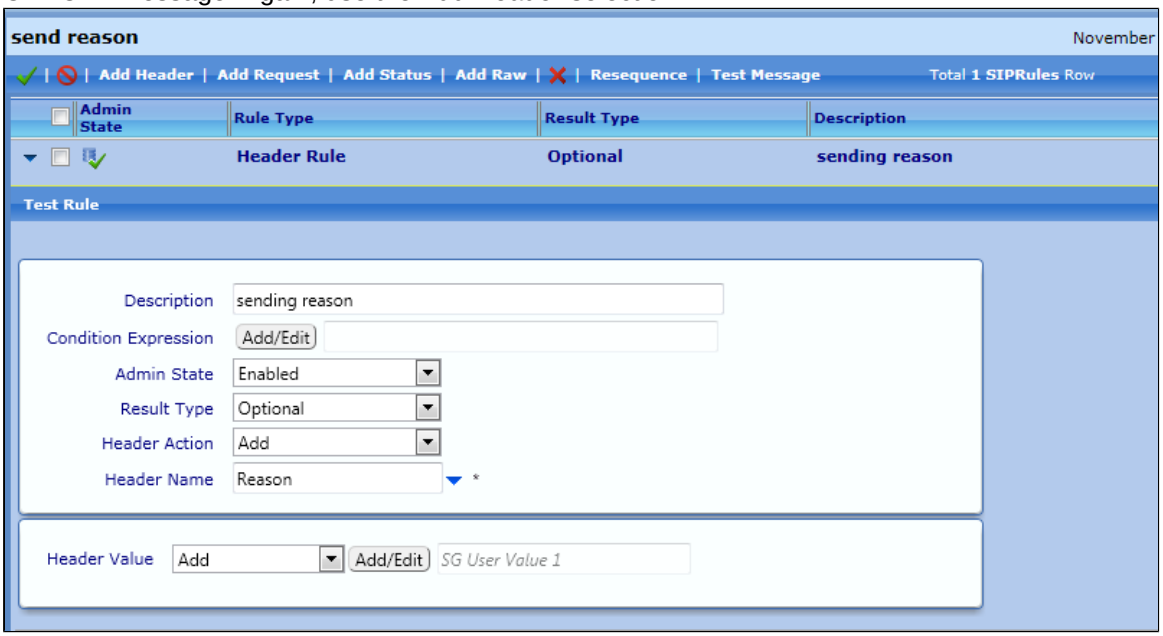
CANCEL sip:+15103644064@ux.vx.net;user=phone SIP/2.0
FROM: <sip:+14083489775@vx.net;user=phone>;tag=6186a5308f;epid=03FE79405B
TO: <sip:+15103644064@ux.vx.net;user=phone>
CSEQ: 34 CANCEL
CALL-ID: e2cb98ce-038e-442b-be0c-f82c1265e0d3
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 10.1.1.73:49399;branch=z9hG4bKbbacc69a

Copyright © 2015 Sonus Networks. All rights reserved.

CONTACT: <sip:SBA1.vx.net:5067;transport=Tls>
CONTENT-LENGTH: 0
USER-AGENT: RTCC/4.0.0.0 MediationServer
Reason: SIP;cause=200;text="Call completed elsewhere";ms-acceptedby="sip:jdoe@vx.net" (reason header from LYNC)

---

3. In a separate SIP Message Table, add a SIP Message Rule to add the Reason header to the outgoing SIP CANCEL message. Again, use the *Add Header* selection.

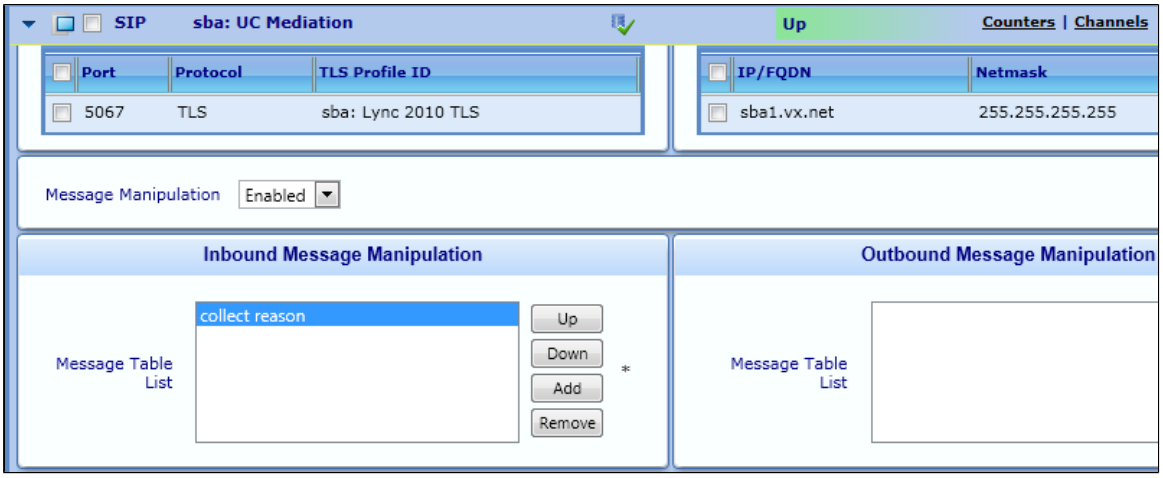


CANCEL sip:15103644064@vxgw2.vx.net:5060;user=phone SIP/2.0
reason: SIP;cause=200;text="Call completed elsewhere";ms-acceptedby="sip:jdoe@vx.net" (SBC-added reason header)
Allow: INVITE, ACK, CANCEL, BYE, UPDATE, NOTIFY, OPTIONS, REFER, REGISTER
Call-ID: call-F96B1300-0000-0010-0C13-8@10.1.1.74
Content-Length: 0
CSeq: 1 CANCEL
From: <sip:+14083489775@10.1.1.74:5060;user=phone>;tag=a01014a-d
Max-Forwards: 70
To: <sip:15103644064@vxgw2.vx.net:5060;user=phone>
User-Agent: NET UX 2.2.1v999 UX
Via: SIP/2.0/TCP 10.1.1.74:5060;branch=z9hG4bK-UX-0a01-014a-0038

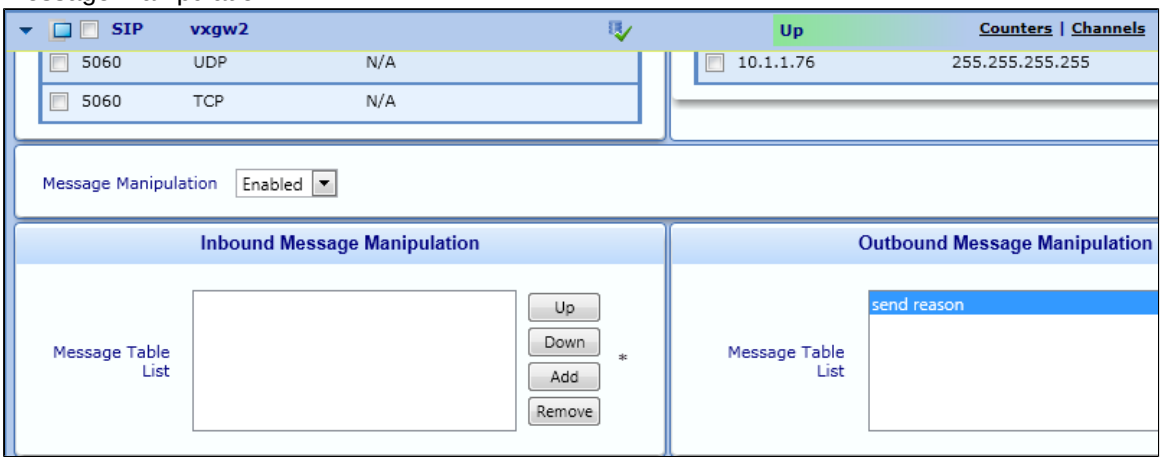
---

4. On the LYNC or SBA Signaling Group, add the capture SIP Message Rule to the Inbound Message Manipulation.

Copyright © 2015 Sonus Networks. All rights reserved.



5. On any Signaling Group which would send a forked call, add the sending SIP Message Rule to the Outbound Message Manipulation.



Debugging Output

```
CANCEL sip:+15103644064@ux.vx.net;user=phone SIP/2.0
FROM: <sip:+14083489775@vx.net;user=phone>;tag=6186a5308f;epid=03FE79405B
TO: <sip:+15103644064@ux.vx.net;user=phone>
CSEQ: 34 CANCEL
CALL-ID: e2cb98ce-038e-442b-be0c-f82c1265e0d3
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 10.1.1.73:49399;branch=z9hG4bKbbacc69a
CONTACT: <sip:SBA1.vx.net:5067;transport=Tls>
CONTENT-LENGTH: 0
USER-AGENT: RTCC/4.0.0.0 MediationServer
Reason: SIP;cause=200;text="Call completed
elsewhere";ms-acceptedby="sip:jdoe@vx.net"

...

012-11-07 20:22:27,202] 3723 0039 com.net.ux.sip DEBUG (sipSignalingGroup.cpp:792) -
{SG(2) 0x28dfe8} ProcessTransportMessage: Protocol Repair,calling Ingress
executive(1 item(s) on list)
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-11-07 20:22:27,202] 3724 0038 com.net.ux.sip DEBUG (Executive.cpp:52) - Run:
Protocol Engine::Executive running 1 rules
[2012-11-07 20:22:27,202] 3725 0037 com.net.ux.sip TRACE (Executive.cpp:58) - Run:
Protocol Engine::getting ruleid (5)
[2012-11-07 20:22:27,202] 3726 0036 com.net.ux.sip TRACE (Executive.cpp:75) - Run:
Processing Message Rule (collect reason)
[2012-11-07 20:22:27,202] 3727 0035 com.net.ux.sip TRACE (Executive.cpp:127) -
processMessageRule: Processing Message Rule (5)
[2012-11-07 20:22:27,202] 3728 0034 com.net.ux.sip TRACE (Executive.cpp:1252) -
MatchSipMessageRule: StartLine from configuration (cancel)From Msg (CANCEL
sip:+15103644064@ux.vx.net;user=phone SIP/2.0)
[2012-11-07 20:22:27,202] 3729 0033 com.net.ux.sip TRACE (Executive.cpp:1262) -
MatchSipMessageRule: Request configuration (cancel)From Msg (cancel)
[2012-11-07 20:22:27,202] 3730 0032 com.net.ux.sip DEBUG (HeaderRule.h:1069) -
debugInfo: HeaderRuleFieldCopy
[2012-11-07 20:22:27,202] 3731 0031 com.net.ux.sip DEBUG (HeaderRule.h:798) -
debugInfo: HeaderRuleFieldChange mReplacement
[2012-11-07 20:22:27,202] 3732 0030 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(sguser[1])
[2012-11-07 20:22:27,202] 3733 002f com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-07 20:22:27,203] 3734 002e com.net.ux.sip DEBUG (HeaderRule.h:679) -
debugInfo: HeaderRuleField:: Element
[2012-11-07 20:22:27,203] 3735 002d com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(header["reason",1])
[2012-11-07 20:22:27,203] 3736 002c com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-07 20:22:27,203] 3737 002b com.net.ux.sip DEBUG (HeaderRule.h:115) -
debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-11-07 20:22:27,203] 3738 002a com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(1)  Result(1) Description(collect cancel header)
valid(true), Condition Expression(No conditions for this header rule)
[2012-11-07 20:22:27,203] 3739 0029 com.net.ux.sip TRACE (Executive.cpp:211) -
processMessageRule: Processing Header rule
[2012-11-07 20:22:27,203] 3740 0028 com.net.ux.sip DEBUG (Executive.cpp:316) -
processHeaderRule: Processing header Rule (collect cancel header)
[2012-11-07 20:22:27,203] 3741 0027 com.net.ux.sip TRACE (Executive.cpp:546) -
processHeaderRule: Processing Rule Field Copy
[2012-11-07 20:22:27,203] 3742 0026 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(3:Header) value:
[2012-11-07 20:22:27,203] 3743 0025 com.net.ux.sip TRACE (SipMessage.cpp:1392) -
setObjectValue: name:(19:SGUser) value:SIP;cause=200;text="Call completed
elsewhere";ms-acceptedby="sip:jdoe@vx.net"
[2012-11-07 20:22:27,203] 3744 0024 com.net.ux.sip TRACE (Executive.cpp:218) -
processMessageRule: HeaderRule executed
[2012-11-07 20:22:27,203] 3745 0023 com.net.ux.sip TRACE (Executive.cpp:81) - Run:
Message Rule (5) matched at least one message rule
[2012-11-07 20:22:27,203] 3746 0022 com.net.ux.sip DEBUG (sipSignalingGroup.cpp:794)
- {SG(2) 0x28dfe8} ProcessTransportMessage: Protocol Repair, out of Ingress
executive


...
[2012-11-07 20:22:27,402] 4645 0021 com.net.ux.sip DEBUG (Transaction.cpp:698) -
egressProtocolRepair: Transaction Protocol Repair (Transaction),calling Egress
executive(1 item(s) on list)
[2012-11-07 20:22:27,402] 4646 0020 com.net.ux.sip DEBUG (Executive.cpp:52) - Run:
Protocol Engine::Executive running 1 rules
[2012-11-07 20:22:27,402] 4647 001f com.net.ux.sip TRACE (Executive.cpp:58) - Run:
Protocol Engine::getting ruleid (6)
[2012-11-07 20:22:27,402] 4648 001e com.net.ux.sip TRACE (Executive.cpp:75) - Run:
Processing Message Rule (send reason)
[2012-11-07 20:22:27,402] 4649 001d com.net.ux.sip TRACE (Executive.cpp:127) -
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
processMessageRule: Processing Message Rule (6)
[2012-11-07 20:22:27,402] 4650 001c com.net.ux.sip TRACE (Executive.cpp:1252) -
MatchSipMessageRule: StartLine from configuration (cancel)From Msg (CANCEL
sip:15103644064@vxgw2.vx.net:5060;user=phone SIP/2.0
)
[2012-11-07 20:22:27,402] 4651 001b com.net.ux.sip TRACE (Executive.cpp:1262) -
MatchSipMessageRule: Request configuration (cancel)From Msg (cancel)
[2012-11-07 20:22:27,402] 4652 001a com.net.ux.sip DEBUG (HeaderRule.h:281) -
debugInfo: HeaderRuleAdd
[2012-11-07 20:22:27,402] 4653 0019 com.net.ux.sip DEBUG (HeaderRule.h:176) -
debugInfo: HeaderRulePayload:: FieldList
[2012-11-07 20:22:27,402] 4654 0018 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(sguser[1])
[2012-11-07 20:22:27,402] 4655 0017 com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-11-07 20:22:27,402] 4656 0016 com.net.ux.sip DEBUG (HeaderRule.h:115) -
debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-11-07 20:22:27,402] 4657 0015 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(1)  Result(1) Description(sending reason)
valid(true), Condition Expression(No conditions for this header rule)
[2012-11-07 20:22:27,402] 4658 0014 com.net.ux.sip TRACE (Executive.cpp:211) -
processMessageRule: Processing Header rule
[2012-11-07 20:22:27,402] 4659 0013 com.net.ux.sip DEBUG (Executive.cpp:316) -
processHeaderRule: Processing header Rule (sending reason)
[2012-11-07 20:22:27,402] 4660 0012 com.net.ux.sip TRACE (Executive.cpp:358) -
processHeaderRule: Processing Rule Add
[2012-11-07 20:22:27,402] 4661 0011 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-11-07 20:22:27,402] 4662 0010 com.net.ux.sip TRACE (Executive.cpp:736) -
buildField: Building field object
[2012-11-07 20:22:27,402] 4663 00e9 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(19:SGUser) value:
[2012-11-07 20:22:27,402] 4664 00e8 com.net.ux.sip TRACE (Executive.cpp:948) -
headerAdd: Executing header add
[2012-11-07 20:22:27,403] 4665 00e7 com.net.ux.sip TRACE (SipMessage.cpp:1474) -
addObjectValue: name:(3:Header) value:SIP;cause=200;text="Call completed
elsewhere";ms-acceptedby="sip:jdoe@vx.net"
[2012-11-07 20:22:27,403] 4666 00e6 com.net.ux.sip TRACE (Executive.cpp:218) -
processMessageRule: HeaderRule executed
[2012-11-07 20:22:27,403] 4667 00e5 com.net.ux.sip TRACE (Executive.cpp:81) - Run:
Message Rule (6) matched at least one message rule
[2012-11-07 20:22:27,403] 4668 00e4 com.net.ux.sip DEBUG (Transaction.cpp:700) -
egressProtocolRepair: Transaction Protocol Repair, out of Egress executive

...

CANCEL sip:15103644064@vxgw2.vx.net:5060;user=phone SIP/2.0
reason: SIP;cause=200;text="Call completed
elsewhere";ms-acceptedby="sip:jdoe@vx.net"
Allow: INVITE, ACK, CANCEL, BYE, UPDATE, NOTIFY, OPTIONS, REFER, REGISTER
Call-ID: call-F96B1300-0000-0010-0C13-8@10.1.1.74
Content-Length: 0
CSeq: 1 CANCEL
From:  <sip:+14083489775@10.1.1.74:5060;user=phone>;tag=a01014a-d
Max-Forwards: 70
To:  <sip:15103644064@vxgw2.vx.net:5060;user=phone>
User-Agent: NET UX 2.2.1v999 UX
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
Via: SIP/2.0/TCP 10.1.1.74:5060;branch=z9hG4bK-UX-0a01-014a-0038
```

Important Notes

The SIP Header feature cannot **generate** a new SIP packet. Only arriving or leaving SIP packets changed via the SIP Header function.

Care must be exercised when modifying incoming SIP packets, especially with respects to the TO, FROM and RURI headers. Modifying tags, IDs or any other items that define the dialogue or transactions, will likely cause calls to not complete.

rev 0.5

Remove the User Agent or Server Header using SIP Message Manipulation

Table of Contents

- Prerequistes
- Summary
  - Configure the SBC1000/2000 Header Manipulation
  - Debugging Output
  - Important Notes

About this Page

- This document details removing the SBC's User Agent or Server Header before transmitting a SIP Message.
- This document details the removal of a header using the *Add Header* selection.
- This Header Manipulation document utilizes the *Token* function.

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups

Prerequistes

Requires Sonus SBC1000/2000 Version 2.2

Copyright © 2015 Sonus Networks. All rights reserved.

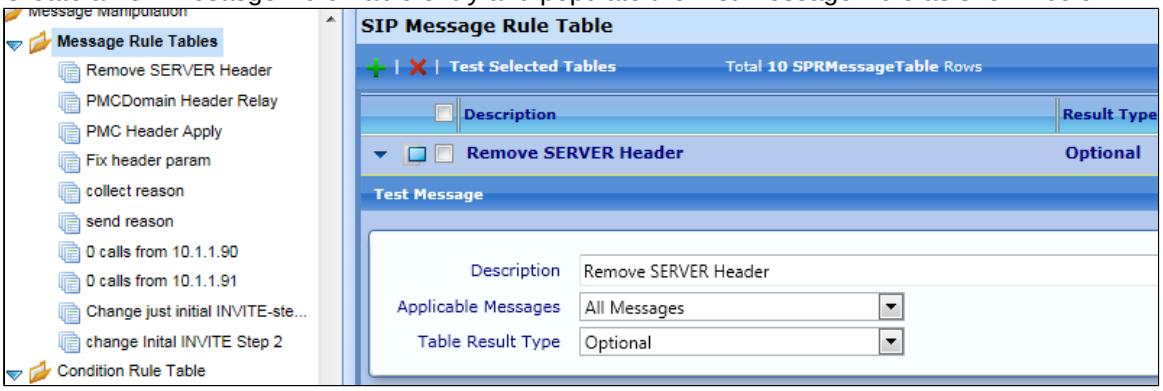
Summary

In certain circumstances, in order to increase network security it may be desirable to remove the UX's User Agent/Server Header before transmitting SIP packets to a downstream peer.

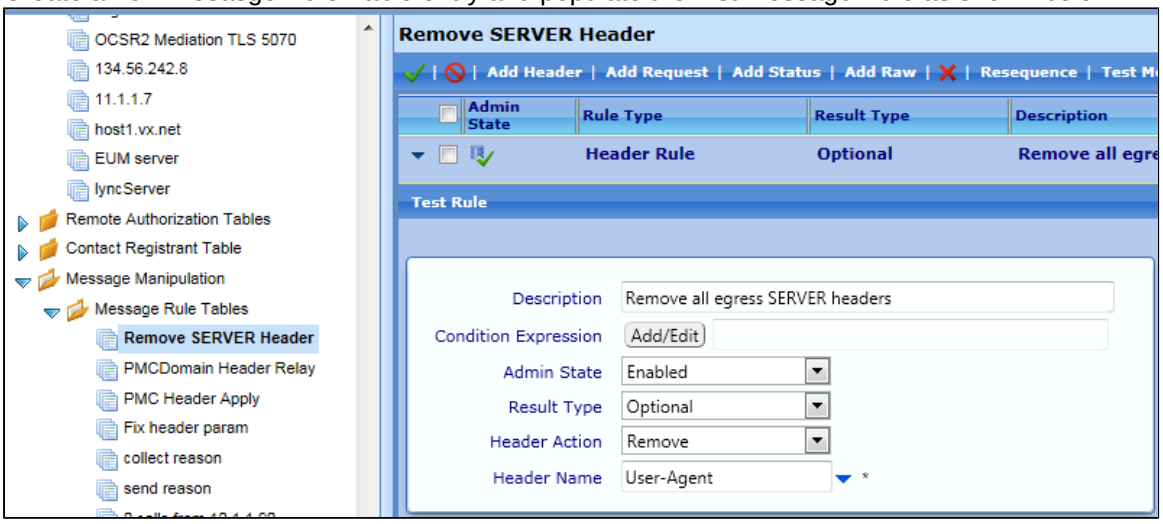
This document detail using the SIP Message Manipulation feature to remove the User Agent/Server header from SIP packets before they are transmitted.

Configure the SBC1000/2000 Header Manipulation

1. Create a new Mesasge Rule Table entry and populate the first Message Rule as shown below.



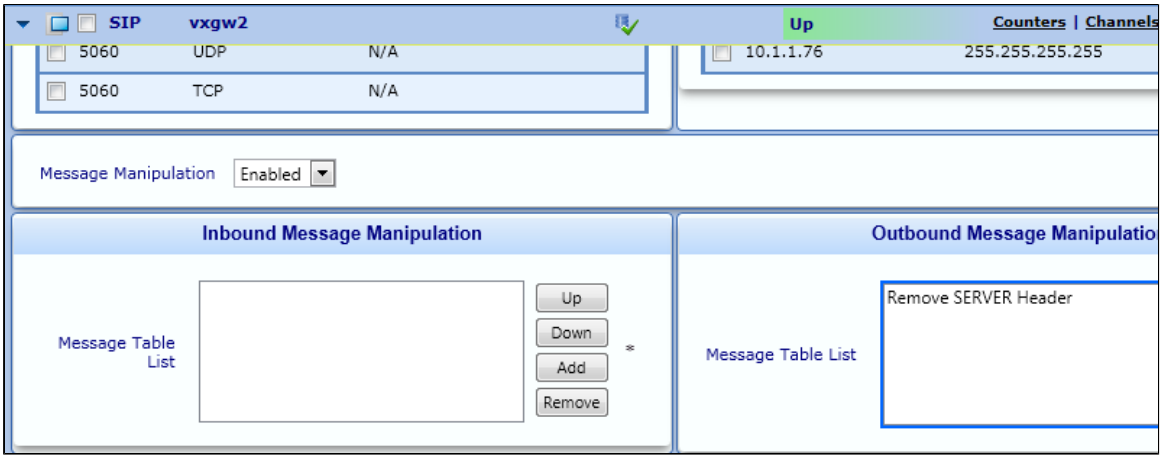
2. Create a new Mesasge Rule Table entry and populate the first Message Rule as shown below.



> If you wish to also remove any packets with the *Server* header, create an additional Message Rule entry and select *Server* from the *Header Name* pulldown.

3. Add the SMM Table to the desired Signaling Group.

Copyright © 2015 Sonus Networks. All rights reserved.



Debugging Output

TBD

Important Notes

The SIP Header feature cannot **generate** a new SIP packet. Only arriving or leaving SIP packets changed via the SIP Header function.

Care must be exercised when modifying incoming SIP packets, especially with respects to the TO, FROM and RURI headers. Modifying tags, IDs or any other items that define the dialogue or transactions, will likely cause calls to not complete.

rev 0.4

Removing Brackets from a Parameter using SIP Message Manipulation

Table of Contents

- Prerequistes
- Summary
  - Configure the SBC1000/2000 for Header Manipulation
- Debugging Output

Copyright © 2015 Sonus Networks. All rights reserved.

About this Page

- This document details how to configure the SBC to remove brackets from a the uri parameter in a Proxy-Authentication header.
- This document shows the creation of a SMM Rule Table that selects only certain SIP Messages for modification. In this case, only INVITE packets will be modified.
- This document features the use of a Header Name that isn't included in the pre-programmed token list.

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups

Prerequistes

Requires Sonus SBC1000/2000 Version 2.2

Summary

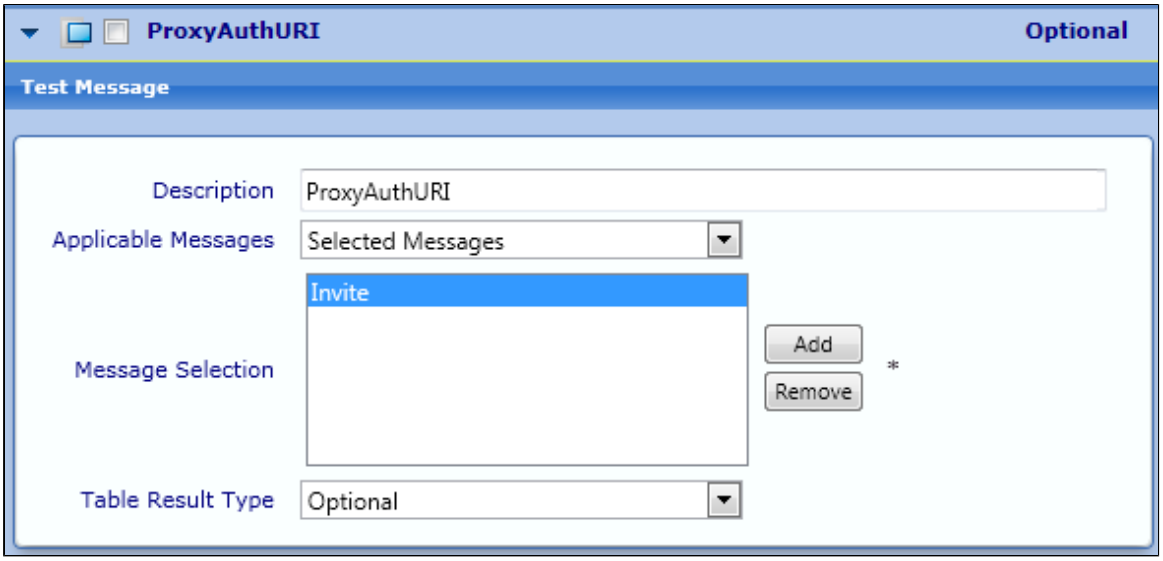
This document shows how to configure the UX to remove <> characters from a parameter within a header. In this specific example, the <> characters are removed from the uri parameter of a Proxy-Authentication header from an INVITE sent by the SBC x000.

SIP Header	**Proxy-Authorization: Digest realm="Realm", nonce="MTM1NTMxMTYwNjE0N2NhYWRhYWZkZjY0NzVkYmNmMTRmZGY3ZjVlMjVhZWJl",alg username="tech01_1723207030", uri="<sip:01274662967@80.193.254.193:5060;user=phone>", response="c3aec7cea80019ca04a9bb064383fb9d", cnonce="bef5a3cc", nc=00000001**
Parameter to Match	**uri="<sip:01274662967@80.193.254.193:5060;user=phone>"**
Regex Match	**(.*)(uri..).(.*)(phone).(.*)**
Desired Output	**uri="sip:01274662967@80.193.254.193:5060;user=phone"**

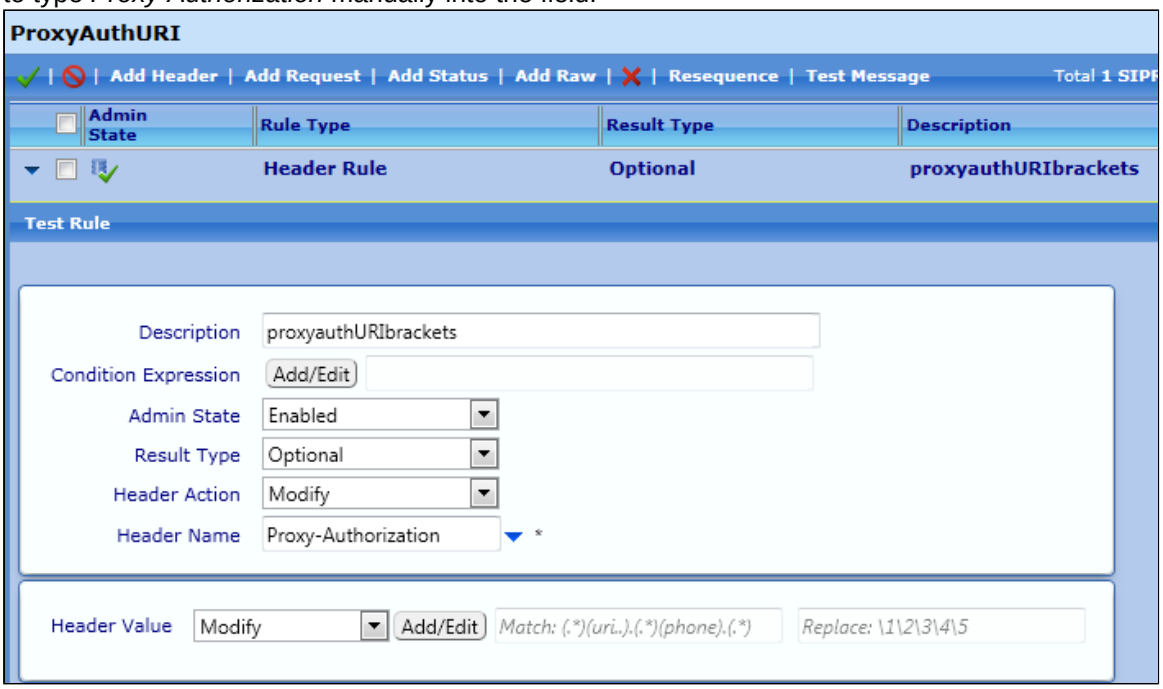
Configure the SBC1000/2000 for Header Manipulation

1. Create a new SIP Message Rule Tables. This entry will only activate on INVITE messages.

Copyright © 2015 Sonus Networks. All rights reserved.

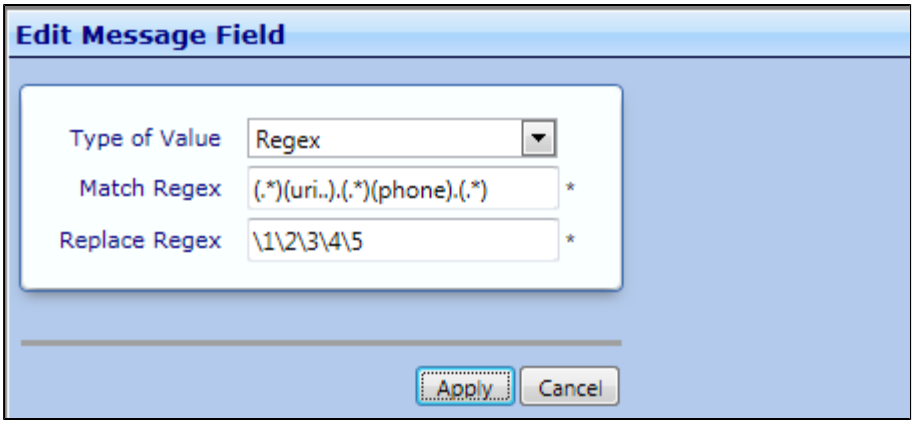


2. Create a Message Rule Table entry. As Proxy-Authorization is not a pre-defined Header Name, you will need to type *Proxy-Authorization* manually into the field.

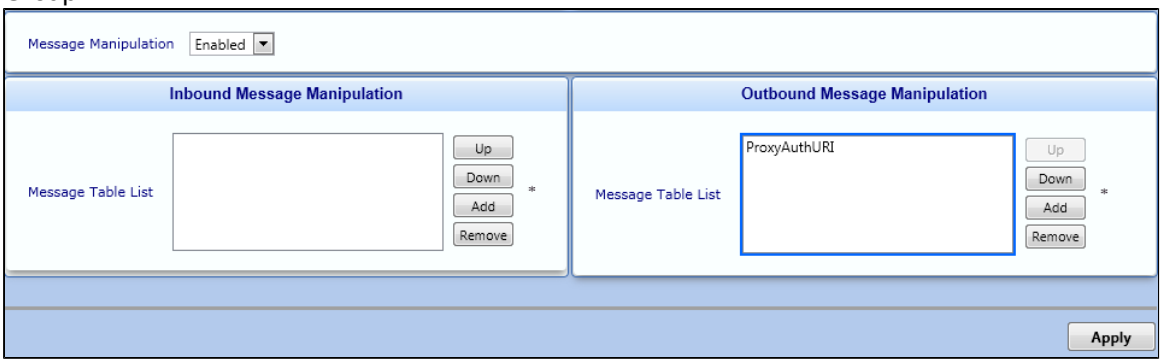


3. In the Message Rule Table entry, click the *Add/Edit* button and enter the Message Field values as shown. This regex will match the Proxy-Authorization header and remove the <> (brackets) from the uri parameter.

Copyright © 2015 Sonus Networks. All rights reserved.



4. Apply the SIP Message Manipulation to the Output Message Manipulation on the desired egress Signaling Group.



Debugging Output

```
[2012-01-10 13:16:53,774] 2641 0001 com.net.ux.sip TRACE (Executive.cpp:81) - Run:
Message Rule (17) matched at least one message rule
[2012-01-10 13:16:53,774] 2642 0001 com.net.ux.sip TRACE (Executive.cpp:58) - Run:
Protocol Engine::getting ruleid (15)
[2012-01-10 13:16:53,775] 2643 0001 com.net.ux.sip TRACE (Executive.cpp:75) - Run:
Processing Message Rule (ProxyAuthURI)
[2012-01-10 13:16:53,775] 2644 0001 com.net.ux.sip TRACE (Executive.cpp:127) -
processMessageRule: Processing Message Rule (15)
[2012-01-10 13:16:53,775] 2645 0001 com.net.ux.sip TRACE (Executive.cpp:1252) -
MatchSipMessageRule: StartLine from configuration (invite)From Msg (INVITE
sip:3539@demo6.vx.net:5060 SIP/2.0
)
[2012-01-10 13:16:53,775] 2646 0001 com.net.ux.sip TRACE (Executive.cpp:1262) -
MatchSipMessageRule: Request configuration (invite)From Msg (invite)
[2012-01-10 13:16:53,775] 2647 0001 com.net.ux.sip DEBUG (HeaderRule.h:549) -
debugInfo: ReaderRuleRegexModify: HeaderRulePayload:: mReplacement
[2012-01-10 13:16:53,775] 2648 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(\1\2\3\4\5)
[2012-01-10 13:16:53,775] 2649 0001 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(\1\2\3\4\5)
[2012-01-10 13:16:53,775] 2650 0001 com.net.ux.sip DEBUG (HeaderRule.h:486) -
debugInfo: HeaderRuleRegex:: Expression((.*)(uri..).(.*)(phone).(.*))
[2012-01-10 13:16:53,775] 2651 0001 com.net.ux.sip DEBUG (HeaderRule.h:115) -
debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-01-10 13:16:53,775] 2652 0001 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(1)  Result(1) Description(proxyauthURIbrackets)
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
valid(true), Condition Expression(No conditions for this header rule)
[2012-01-10 13:16:53,775] 2653 0001 com.net.ux.sip TRACE (Executive.cpp:211) -
processMessageRule: Processing Header rule
[2012-01-10 13:16:53,776] 2654 0001 com.net.ux.sip DEBUG (Executive.cpp:316) -
processHeaderRule: Processing header Rule (proxyauthURIbrackets)
[2012-01-10 13:16:53,776] 2655 0001 com.net.ux.sip TRACE (Executive.cpp:428) -
processHeaderRule: Processing Rule Regex Modify
[2012-01-10 13:16:53,776] 2656 0001 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-01-10 13:16:53,776] 2657 0001 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-01-10 13:16:53,776] 2658 0001 com.net.ux.sip TRACE (Executive.cpp:1297) -
checkOrdinalAll: ObjectToken:: StringIndex(proxy-authorization) Ordinal(1)
[2012-01-10 13:16:53,776] 2659 0001 com.net.ux.sip TRACE (Executive.cpp:823) -
headerRegexModify: Header regex single ordinal
[2012-01-10 13:16:53,776] 2660 0001 com.net.ux.sip TRACE (SipMessage.cpp:1312) -
getObjectValue: name:(3:Header) value:
[2012-01-10 13:16:53,776] 2661 0001 com.net.ux.sip TRACE (Executive.cpp:859) -
doHeaderRegexModify: Executing headerRegex modify, Header to change: Digest
realm="Realm",
nonce="MTM1NTMxMTYwNjE0N2NhYWRhYWZkZjY0NzVkYmNmMTRmZGY3ZjVlMjVhZWJl",algorithm=MD5,qop=
username="tech_1723207030", uri="<sip:01274662967@80.193.254.193:5060;user=phone>",
response="c3aec7cea80019ca04a9bb064383fb9d", cnonce="bef5a3cc", nc=00000001
[2012-01-10 13:16:53,777] 2662 0001 com.net.ux.sip TRACE (Executive.cpp:872) -
doHeaderRegexModify: Header after Regex change: Digest realm="Realm",
nonce="MTM1NTMxMTYwNjE0N2NhYWRhYWZkZjY0NzVkYmNmMTRmZGY3ZjVlMjVhZWJl",algorithm=MD5,qop=
username="tech_1723207030", uri="sip:01274662967@80.193.254.193:5060;user=phone",
response="c3aec7cea80019ca04a9bb064383fb9d", cnonce="bef5a3cc", nc=00000001
[2012-01-10 13:16:53,777] 2663 0001 com.net.ux.sip TRACE (SipMessage.cpp:1392) -
setObjectValue: name:(3:Header) value:Digest realm="Realm",
nonce="MTM1NTMxMTYwNjE0N2NhYWRhYWZkZjY0NzVkYmNmMTRmZGY3ZjVlMjVhZWJl",algorithm=MD5,qop=
username="tech_1723207030", uri="sip:01274662967@80.193.254.193:5060;user=phone",
response="c3aec7cea80019ca04a9bb064383fb9d", cnonce="bef5a3cc", nc=00000001
[2012-01-10 13:16:53,777] 2664 0001 com.net.ux.sip TRACE (Executive.cpp:218) -
processMessageRule: HeaderRule executed
[2012-01-10 13:16:53,778] 2665 0001 com.net.ux.sip TRACE (Executive.cpp:81) - Run:
Message Rule (15) matched at least one message rule
[2012-01-10 13:16:53,778] 2666 0001 com.net.ux.sip DEBUG (Transaction.cpp:699) -
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
egressProtocolRepair: Transaction Protocol Repair, out of Egress executive
[201
```

```
INVITE sip:3539@demo6.vx.net:5060 SIP/2.0
Allow: INVITE, ACK, CANCEL, BYE, UPDATE, NOTIFY, OPTIONS, REFER, REGISTER
Call-ID: call-F2D72600-0000-0010-0C13-11@10.1.1.74
Contact: <sip:anonymous@10.1.1.74:5060;transport=TCP>
Content-Length: 256
Content-Type: application/sdp
CSeq: 1 INVITE
From:  <sip:anonymous@10.1.1.74:5060>;tag=a01014a-636
Max-Forwards: 70
P-Asserted-Identity:  <sip:anonymous@10.1.1.74:5060>
Privacy: critical
Proxy-Authorization: Digest realm="Realm",
nonce="MTM1NTMxMTYwNjE0N2NhYWRhYWZkZjY0NzVkYmNmMTRmZGY3ZjVlMjVhZWJl",algorithm=MD5,qop=
username="tech_1723207030", uri="sip:01274662967@80.193.254.193:5060;user=phone",
response="c3aec7cea80019ca04a9bb064383fb9d", cnonce="bef5a3cc", nc=00000001
Supported: replaces,update,100rel
To:  <sip:3539@demo6.vx.net:5060>
User-Agent: NET UX 2.2.1v187 UX
Via: SIP/2.0/TCP 10.1.1.74:5060;branch=z9hG4bK-UX-0a01-014a-3e87
```

Setting the Calling Number from a SIP Header using Sip Message Manipulation

Table of Contents

- Prerequistes
- Moving the Number from the X-Genesys-CTIKey into the Calling Number
  - Target REFER Message
  - Configuring the SIP Message Manipulation
  - Important Notes

About this Page

- This document details how to configure the SBC to copy a value from REFER's SIP header into the Calling Number.
- This document shows the creation of a SMM Rule Table that selects only certain SIP Messages for modification. In this case, only REFER packets will be inspected.
- This document details how to use the SMM feature copy a header value into one of the user-controlled IEs (SG User Value 1).
- This document details how to copy a user-controlled IE value into the Calling Name IE using the Transformation Table.
- This document features the use of a Header Name that isn't included in the pre-programmed token list.

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups

Copyright © 2015 Sonus Networks. All rights reserved.

Prerequistes

Requires Sonus SBC2000/1000 Version 2.2 or later

Moving the Number from the X-Genesys-CTIKey into the Calling Number

In this instance, the implementation called for setting the Calling Number on a REFER-initiated INVITE to the number contained in the X-Genesys-CTIKey. To perform this function:

- The contents of the X-Genesys-CTIKey header are copied to generic IE, *SG User Value 1*, using the SMM function.
- A translation table copies the value from *SG User Value 1* to the *Calling Number* IE.

Target REFER Message

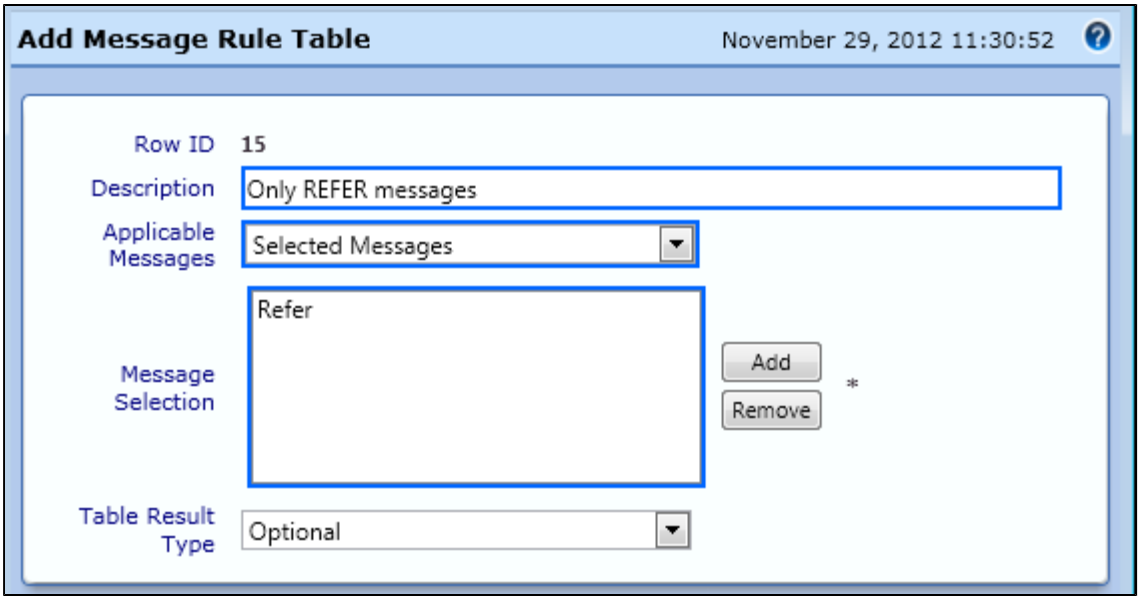
REFER sip:6363575933@172.16.16.9:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 172.16.78.171.22:5060;branch=z9hG4bK0cBde579611ace4c4c0
From: <sip:2522103487@172.16.171.22:5060;user=phone>;tag=gK0cf2c42e
To: <sip:6363575933@172.16.16.9:5060;user=phone>;tag=ac151009-4898
Call-ID: call-39889D00-0000-0010-0C13-48@172.16.16.9
CSeq: 346182208 REFER
Max-Forwards: 70
Allow:
INVITE,ACK,CANCEL,BYE,REGISTER,REFER,INFO,SUBSCRIBE,NOTIFY,PRACK,UPDATE,OPTIONS,MESSAGE

Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay, multipart/mixed
Contact: <sip:2522103487@172.16.171.22:5060>
Refer-To: <sip:5811111@172.16.16.9:5060>
Referred-By: sip:4910131@172.16.16.9:5060
X-Genesys-CallUUID: 01V9PK7IFK8BP1IR95LHQ2LAES05D0QH
X-Genesys-CTIKey: **2144380553**
X-Genesys-GVP-Session-ID:
B2565000-5300-8BFC-585A-C62BB00F862D;gvp.rm.datdes=2|1;gvp.rm.tenant-id=1.101.107_Refer_POC
Supported: 100rel
Content-Length: 0

Configuring the SIP Message Manipulation

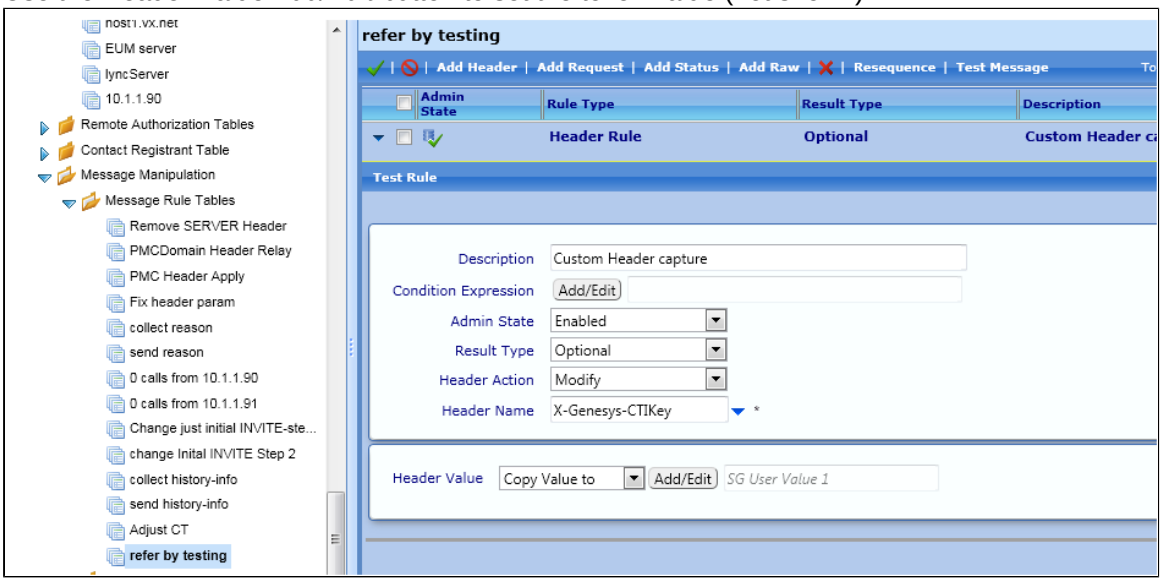
1. Select a new Message Manipulation Table. Configure the *Message Selection* to *Refer*. The SMM Table will only effect REFER messages.

Copyright © 2015 Sonus Networks. All rights reserved.



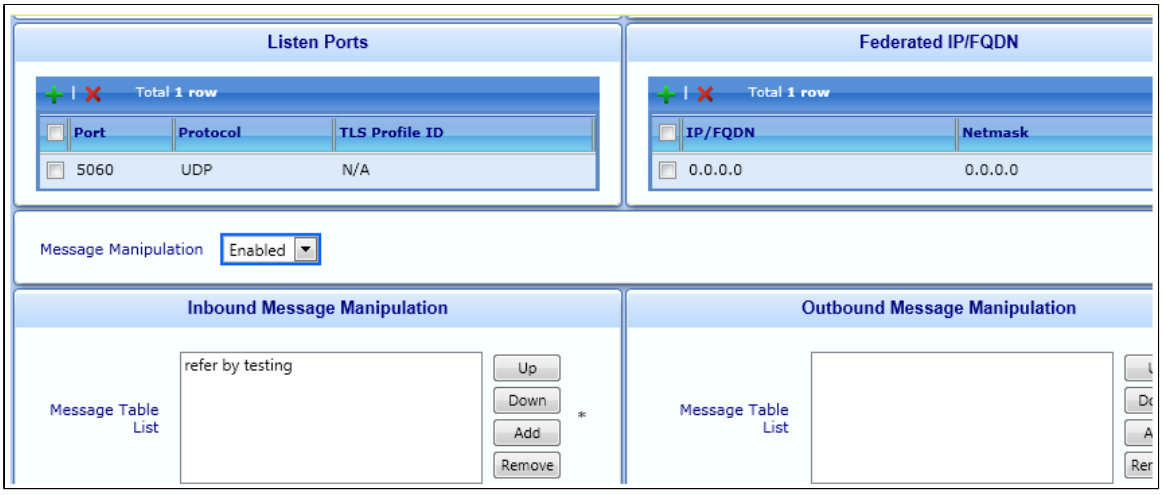
2. Add an entry to the table. As the X-Genesys-CTIKey header is not a pre-programmed *Header Name*, you must manually enter the header name.

   The entry below searches for the SIP header *X-Genesys-CTIKey* and copies the value of the header into the token *SG User Value 1*.
   Use the Header Value *Add/Edit* button to set the token value (not shown).

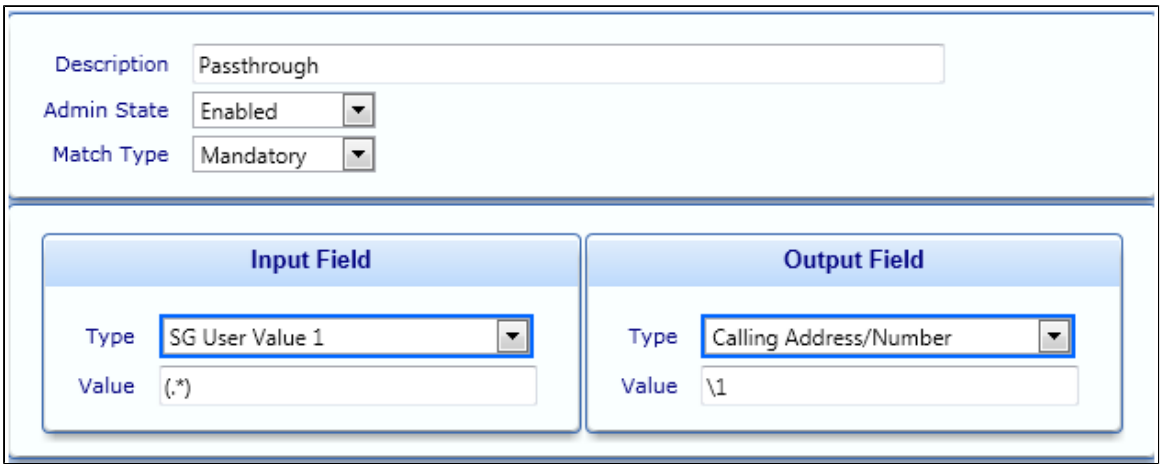


3. Add the new Message Manipulation to the Outbound Message Manipulation Table

Copyright © 2015 Sonus Networks. All rights reserved.



4. Add a translation in the appropriate Translation Table to copy the value from *SG User Value 1* into the *Calling Number*.



Important Notes

> The SIP Header feature cannot **generate** a new SIP packet. Only arriving or leaving SIP packets changed via the SIP Header function.

rev 0.3

SIP Message Manipulation Overview

Copyright © 2015 Sonus Networks. All rights reserved.

Table of Contents

- Prerequistes
- SMM Overview
- A SIP Refresher
  - Packet Types
  - Anatomy of a SIP Packet
- The 4 SIP Message Rules
- Mapping Sections of the SMM Rule to the SIP Packet
  - Request Rule Mapping
  - Status Rule Mapping
  - Header Rule Mapping
  - The Raw Rule
- Tokens
  - Token Mapping
- Conditions
- More Information

About this Page

This document outlines the SIP Message Manipulation feature.

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups
- SIP Message Manipulation Document Catalog
- 6 Steps to Creating Effective SMM Rules

Prerequistes

Assumes the user is familiar with configuring the SBCx000's WebUI

Requires Sonus SBC1000/2000 Version 2.2 or later

SMM Overview

Because you can never tell just what the other side of a SIP connection might send or need, the SBC1000/2000 version 2.2 includes a feature to manipulate any SIP header.

- SIP Headers can be added, deleted, or modified.
- Manipulation can be done for every SIP message, or separately for SIP Requests or SIP Responses.
- Manipulations can set to occur based upon user specified matching criteria.
- Manipulations can be executed at the ingress or egress SG.
  - At the ingress, inbound SIP messages are modified to permit proper handling by the SBC's routing function.
  - At the egress, SIP messages (already processed by the SBC) are modified to meet the SIP requirements of the upstream device.

The SMM feature is enabled on a Signaling Group. That means you can configure a SMM to change an incoming or outgoing SIP Message. It is important to note that SMM feature is separate from the SBC's SIP engine. SMM changes SIP Message either before they are processed, or after they are processed, by the SIP engine. In essence,

Copyright © 2015 Sonus Networks. All rights reserved.

SMM is not state aware.

For instance, if you were to change a FROM Tag on a 180 Ringing Message, the SIP engine would discard that 180 Ringing because it had a differernt Tag than all the previous SIP Messages. To the SIP engine, it would appear as if that 180 Ringing belonged to a different dialogue.

So, SMM changes must be made carefully to ensure that the SIP engine can still recognize that the messages are part of an ongoing dialogue.

What you will learn from this document...
• A SIP Refresher - the Anatomy of SIP Packets • The 4 SIP Message Rules • Mapping SIP Packet elements to their corresponding SMM configuration items • Tokens - SMM's version of the Transformation Table

A SIP Refresher

In order to properly employ the SMM function, you need to understand the SIP protocol and packet syntax. With SMM its possible to change any portion of the SIP packet, so you best understand what's being changed!

Below is a brief SIP referesher, including:

- SIP Packet Types (requests vs. responses)
- Headers
- Parameters

Packet Types

SIP Requests are different than SIP Responses. In order to employ the SIP Manipulation function, you must know the difference between a Request and Response.

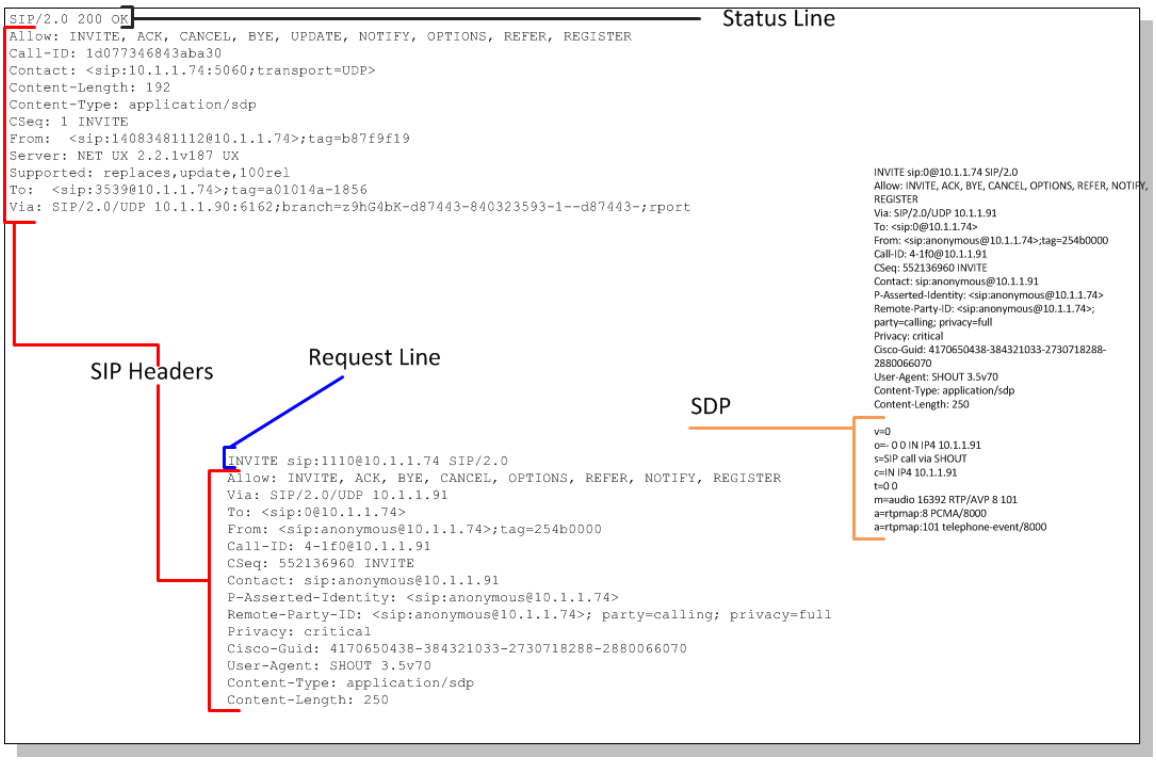
SIP Requests		SIP Responses (partial list)
INVITE		100 Trying
ACK		180 Ringing
BYE		183 Session Progressing
CANCEL		200 OK
OPTIONS		202 Accepted
REGISTER		302 Moved Temporarily
PRACK		400 Bad Request

Copyright © 2015 Sonus Networks. All rights reserved.

SUBSCRIBE		401 Unauthorized
NOTIFY		403 Forbidden
PUBLISH		500 Server Internal Error
INFO		503 Service Unavailable
REFER		504 Server Timeout
MESSAGE		603 Decline
UPDATE		606 Message Too Large

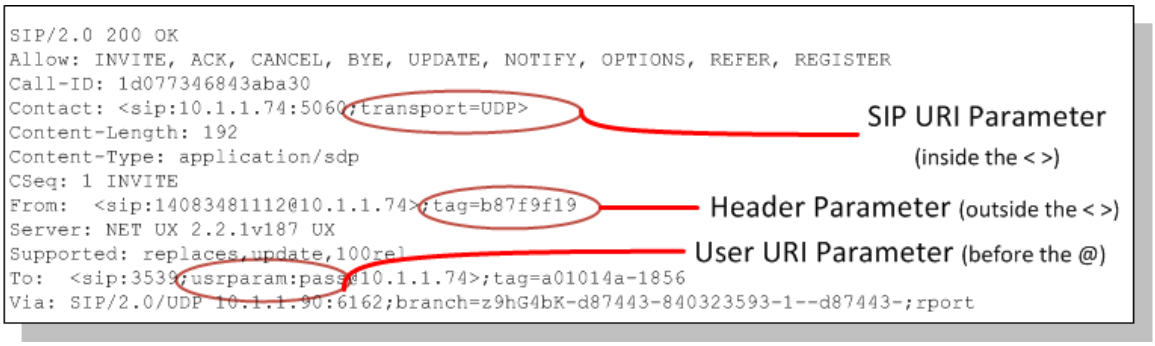
Anatomy of a SIP Packet

Knowing the seperate parts of the SIP packet will help you use the correct section of the SMM Web UI. Request Line, Status Line, Headers, Header Parameters, URI and URI parameters are all portions of a SIP packet.



SIP Lines and Headers

Copyright © 2015 Sonus Networks. All rights reserved.

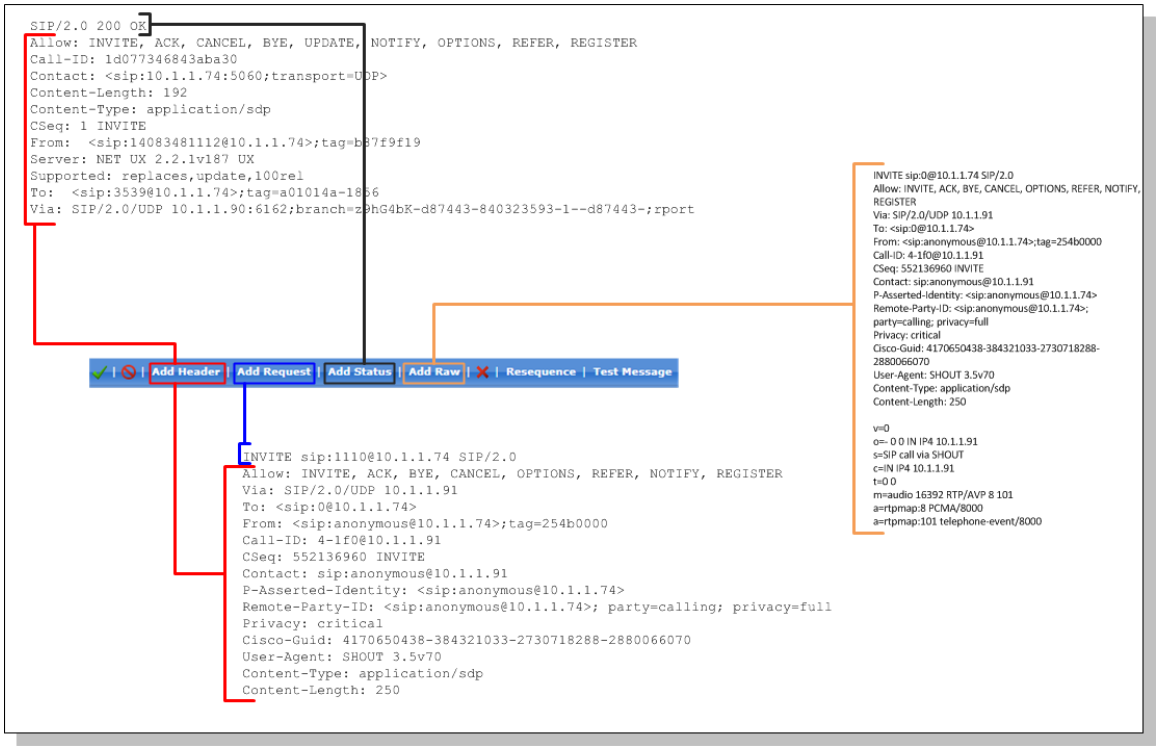


SIP Packet Parameters

The 4 SIP Message Rules

Now that we're familiar with the anatomy of a SIP packet, let's examine the SMM Rules.

This diagram shows each type of SMM Rule and what portion of the SIP packet that type of rule affects.



A mapping of SMM Rule types to portions of SIP messages

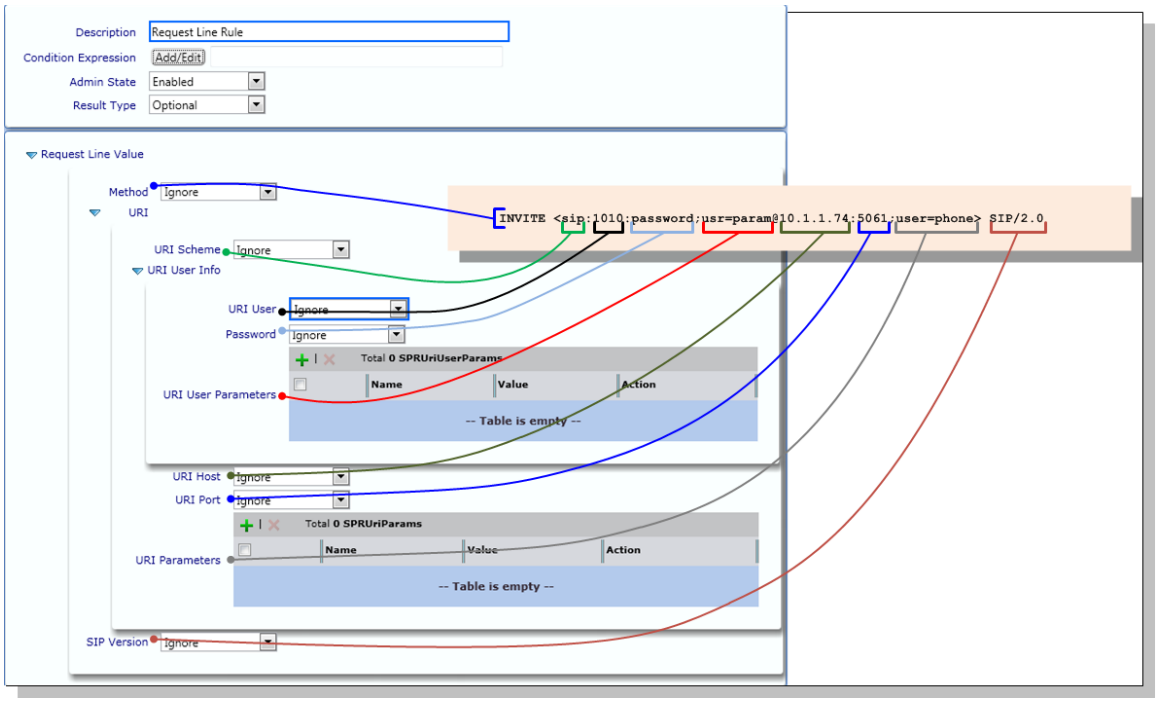
- Use **Request Rules** to change the Request URI Line
- **Status Rules** to change the Status Line
- **Header Rules** to change SIP headers
- **Raw Rules** to change SDP, or any portion of the SIP message not affected by other rules.

Copyright © 2015 Sonus Networks. All rights reserved.

Mapping Sections of the SMM Rule to the SIP Packet

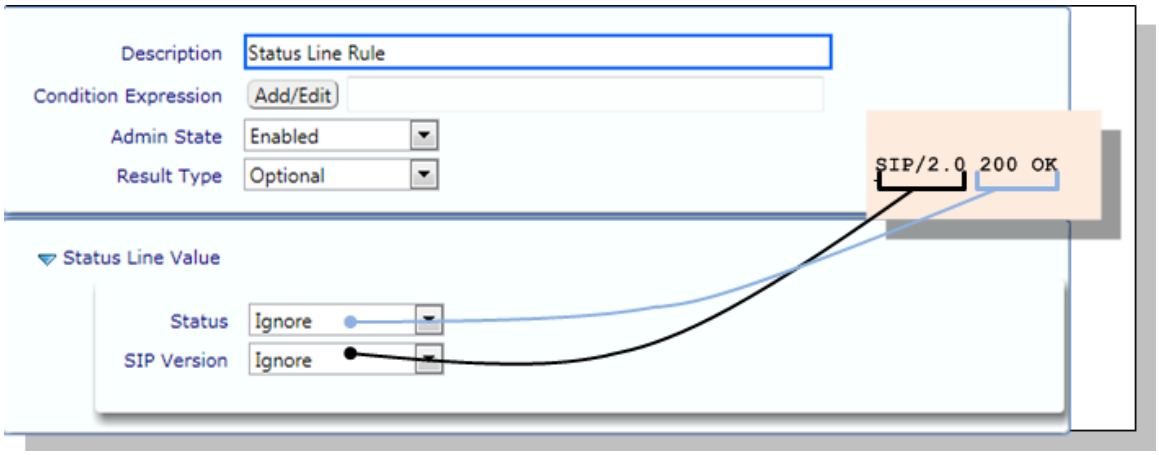
After selecting the appropriate Rule type, the Rule itself must be configured. Using the diagrams below, you can see which section of each rule corresponds with portions of a SIP message. Once you've identified what needs to be changed, consult the diagrams below to determine which configuration entry to employ to create the desired change.

Request Rule Mapping



Request Rule Configuration Options

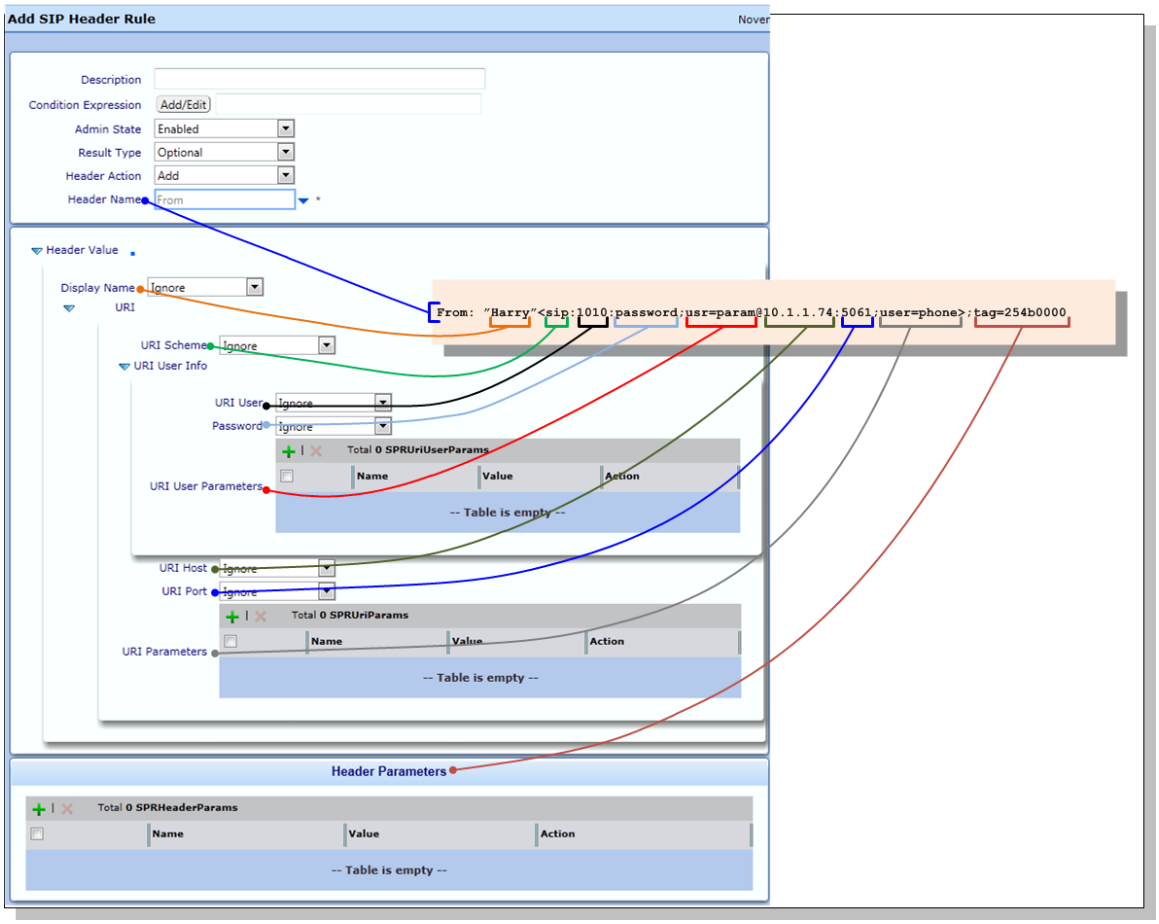
Status Rule Mapping



Status Rule Configuration Options

Copyright © 2015 Sonus Networks. All rights reserved.

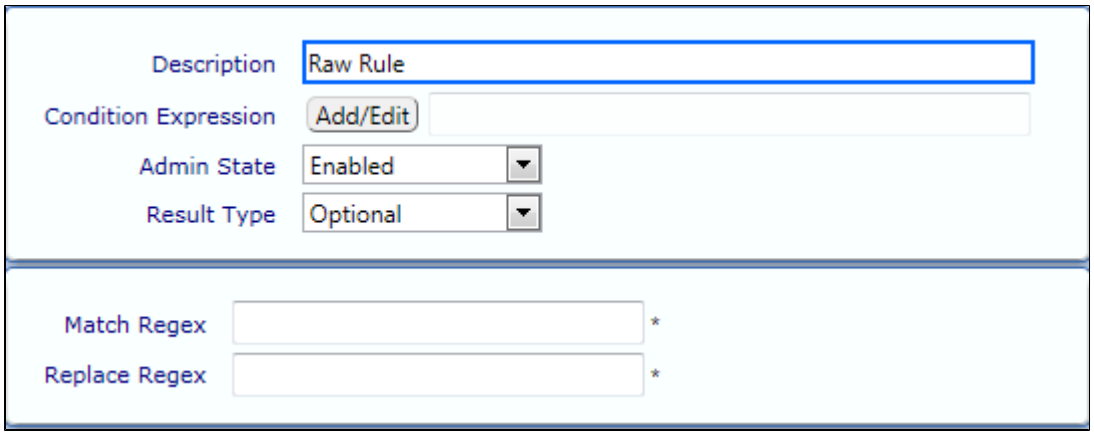
Header Rule Mapping



SIP Header Rule Configuration Options

The Raw Rule

Normally used to change the SDP, the Raw Rule will change *any* regex match found within the entire SIP packet. If a Raw Rule was created to match on *sip:* and change it to *sips:*, then **every** *sip:* that appears in a packet would be changed to *sips:* using a single Raw Rule.



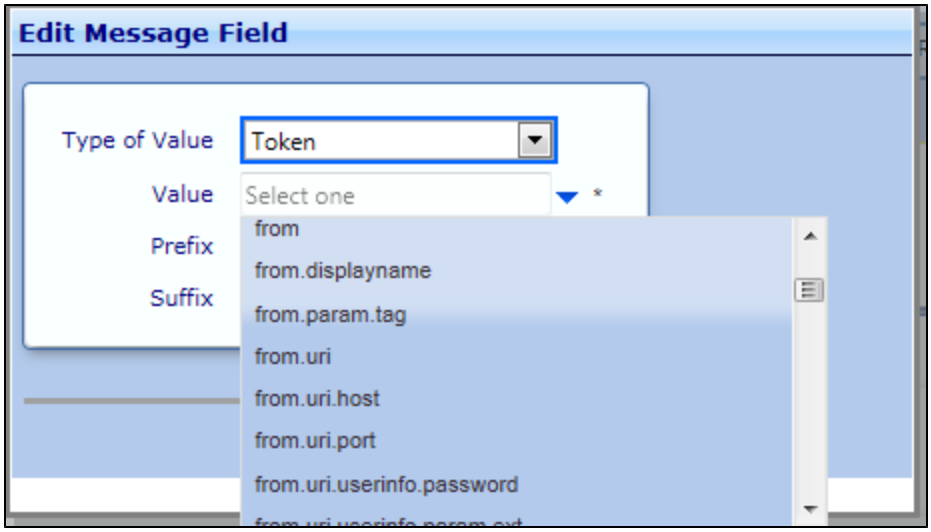
Copyright © 2015 Sonus Networks. All rights reserved.

The Raw Rule performs a straight regex replacment

Tokens

Tokens are basically variable names which have been pre-assigned to different portions of a SIP Message. Just like the numbers in an incoming SIP packet are mapped into Tranformation Table IEs (Called Number, Calling Number, etc.), various portions of a SIP Packet are mapped into SMM Tokens.

Tokens make it easier for you to know what's being changed. For instance, if you're making a SMM Rule to change the diversion number to be the same as the the calling number, you would use the SMM Rules menu to change the diversion value from the token *from.user.userinfo.user* (as that is the token that contains the calling number).



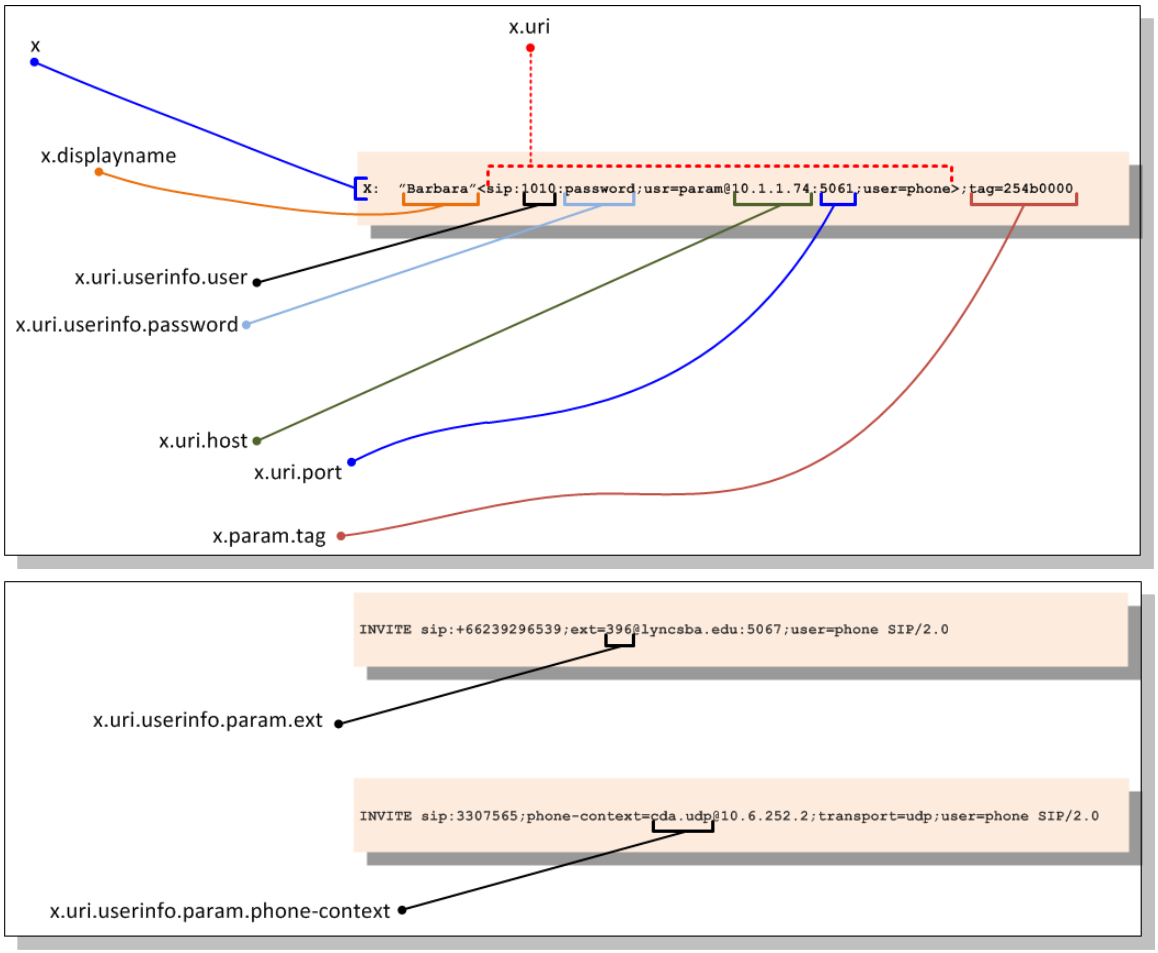
Tokens are selected from various SMM configuration items

Token Mapping

Below find a sample mapping of SIP messages sections to their corresponding tokens; **x** represents a *SIP Request Line, Status Line or Header* name. For example:

- The Display Name in a FROM header would be recorded in the ***from.displayname*** token.
- The TO number would be recorded in the ***to.uri.userinfo.user*** token.

Copyright © 2015 Sonus Networks. All rights reserved.



Tokens mapped to their corresponding SIP packet elements

Some of the available tokens are listed below.

Request URI Header Tokens	Value
request-line	sip:+15103644064@ux.vx.net;user=phone SIP/2.0
request-line.uri	sip:+15103644064@ux.vx.net
request-line.uri.host	ux.vx.net
request-line.uri.port	5061
request-line.uri.userinfo.user	+15103644064
request-line.sipversion	2.0

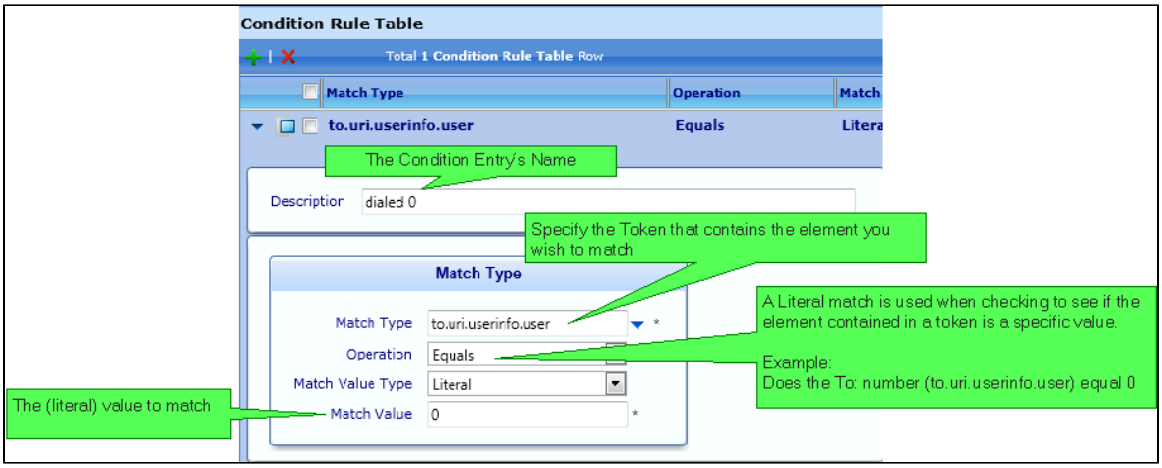
TO/FROM/P-headers Tokens	Value

Copyright © 2015 Sonus Networks. All rights reserved.

from	"Jane Doe"<sip:+14083483531:passwrd;usr=param:test@sba1.vx.net:5061;user=phone>;e "J Smith"<sip:3307565;ext=7565;phone-context=cda.udp@10.6.252.2;transport=udp;us
from.displayname	"Jane Doe"
from.param.tag	d953c6165d
from.uri	sip:+14083483531@sba1.vx.net;user=phone
from.uri.host	sba1.vx.net
from.user.port	5061
from.user.userinfo.password	passwrd
from.user.userinfo.param.ext	7565
from.user.userinfo.param.phone-context	cda.udp
from.user.userinfo.user	+14083483531

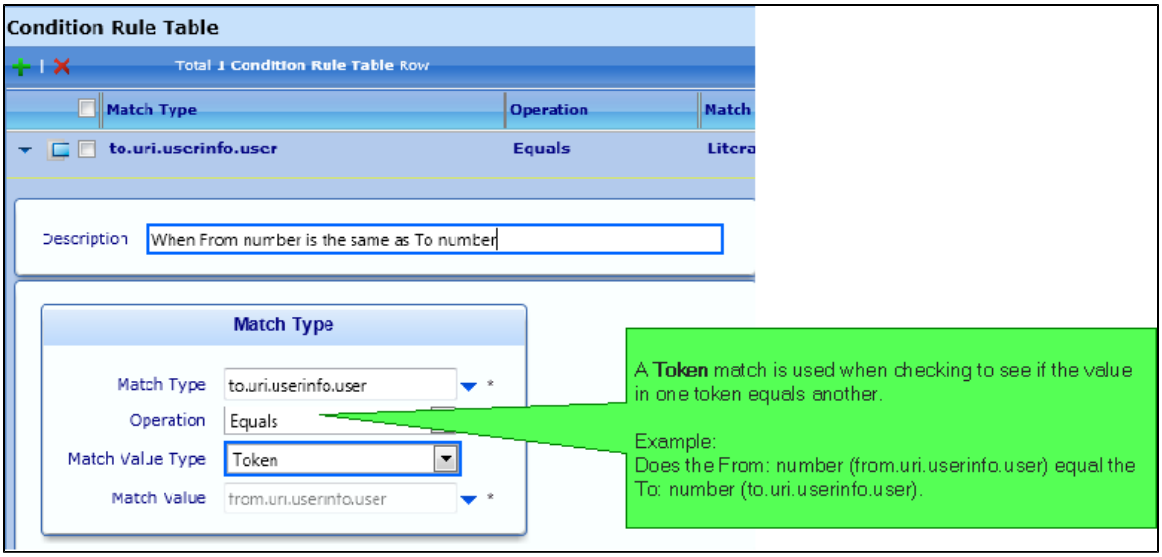
Conditions

When you want an SMM to operate only if something specific occurs, then you create a Condition Rule. Condition Rules, which are applied with the Message Rule, can be configured to match specific numbers, tokens, or by regex.

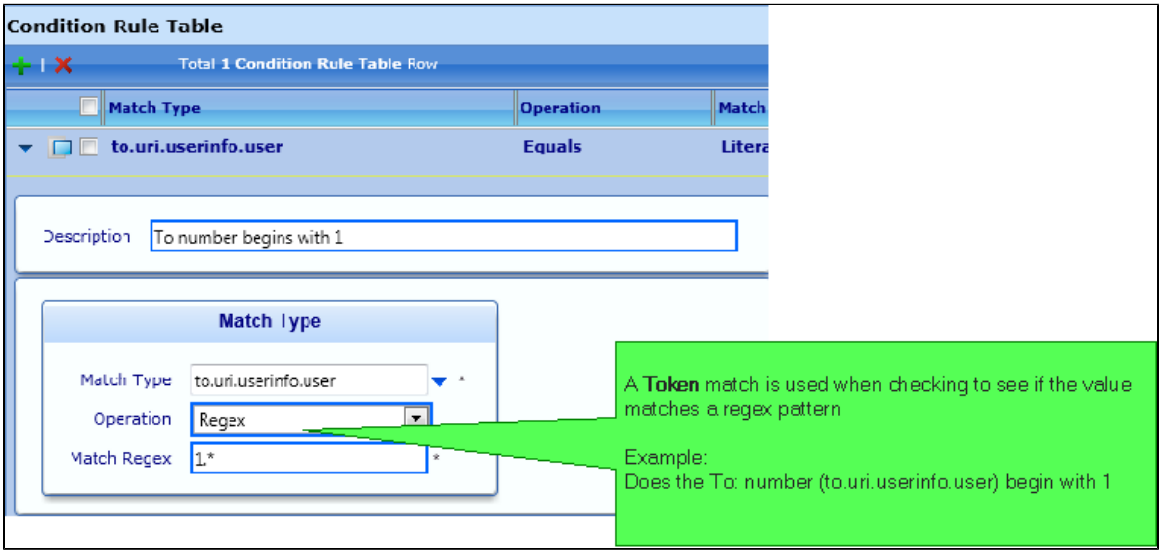


Literal Condition Match

Copyright © 2015 Sonus Networks. All rights reserved.



Token Condition Match



Regex Condition Match

More Information

The SMM feature cannot be used to create a SIP packet. As indicated above, the SMM feature handles a SIP packet either just before or just after the SIP Engine. In either case, an already-existing SIP packet is presented to the SMM function. The SMM function only works on packet it receives--it cannot create a packet.

SIP Message Manipulation - Set the Request URI number from the TO Header

Copyright © 2015 Sonus Networks. All rights reserved.

Table of Contents

- Prerequistes
- Summary
- Setting the number listed in the Request URI (RURI) from the number in the TO header.
  - Configure the SBC1000/2000 for Header Manipulation
  - Debugging Output
  - Important Notes

About this Page

- This document details setting the RURI number from the number listed in the TO Header.
- This document details the configuration to change the Request URI Line in a SIP Request (INVITE, ACK, REGISTER, CANCEL, etc.) using the *Add Request* selection.
- This Header Manipulation document utilizes the *Token* manipulation function.

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups

Prerequistes

Requires Sonus SBC2000/1000 Version 2.2

Summary

Because you can never tell just what the other side might send or need, the SBC1000/2000 version 2.2 will include a feature to manipulate any SIP header.

- SIP Headers can be added, deleted, or modified.
- Manipulation can be done for every SIP message, or separately for SIP Requests or SIP Responses.
- Manipulations can set to occur based upon user specified matching criteria.
- Manipulations can be executed at the ingress or egress SG. At the ingress, inbound SIP messages are modified to permit proper handling by the SBC's routing function. At the egress, SIP messages already processed by the SBC are modified to meet the SIP requirements of the upstream device.

Setting the number listed in the Request URI (RURI) from the number in the TO header.

This document details how to change the incoming RURI number using the TO header number. This solution was originally generated to eliminate a problem from an incoming INVITE.

Copyright © 2015 Sonus Networks. All rights reserved.

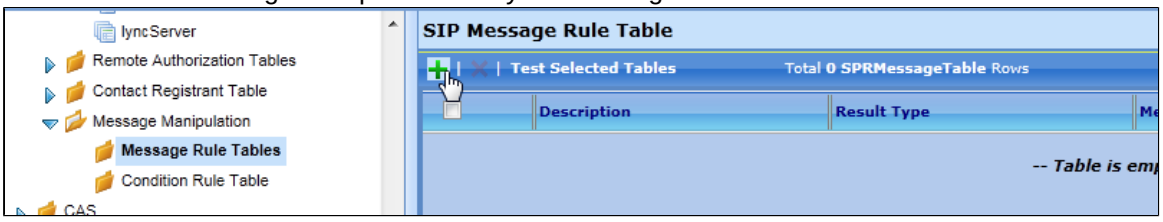


You can see that the number on the RURI is not a number at all, but an IP address.

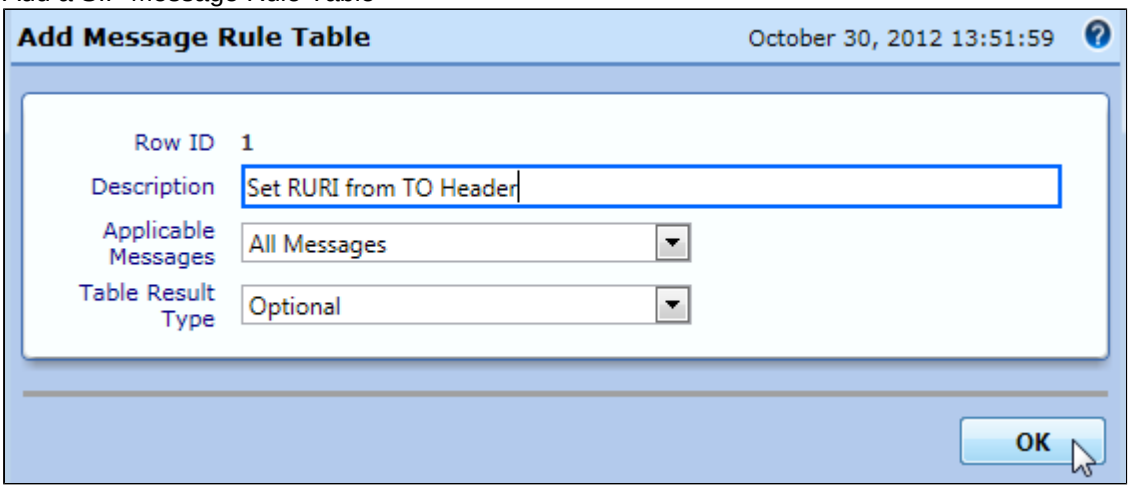
Below is the process for changing the user (e.g. number) portion of the RURI.

Configure the SBC1000/2000 for Header Manipulation

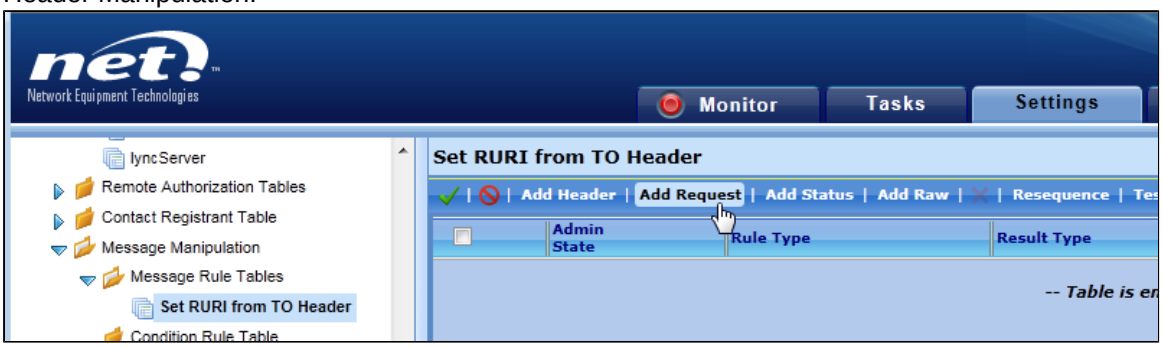
1. Select the new Message Manipulation entry in the navigation tree



2. Add a SIP Message Rule Table

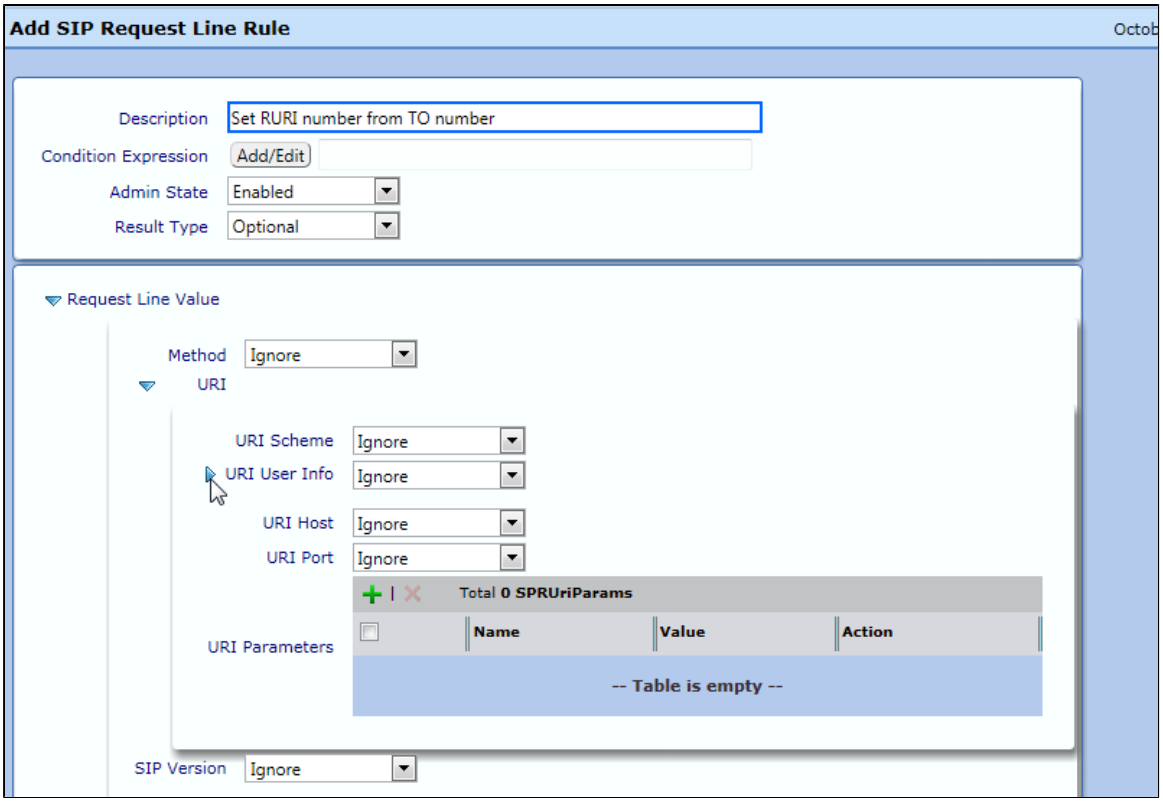


3. Set how the rule will be applied. It can be applied to All SIP Messages, only Requests, only Responses, or Selected Messages. Since the Request URI only appears in a SIP Request, select *Add Requests* type of Header Manipulation.

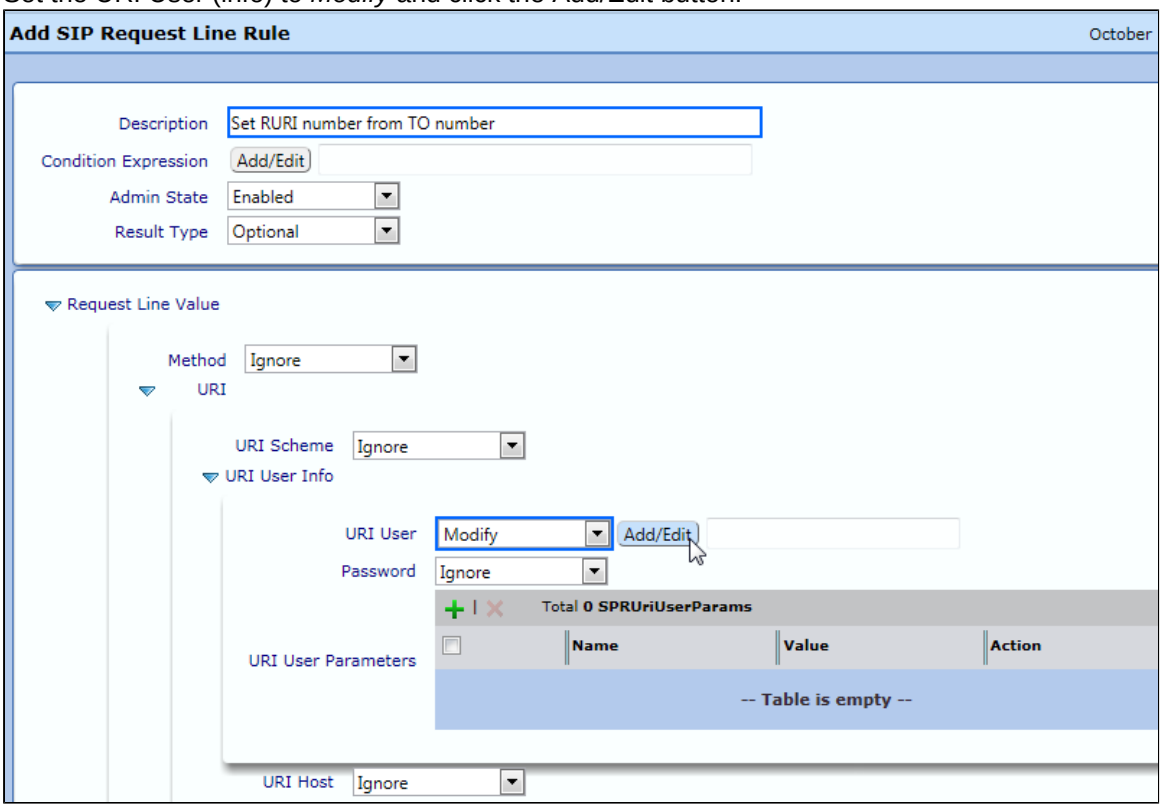


4. Add an entry to the new table. Expand the arrows as shown to reach the lower levels of header matching.

Copyright © 2015 Sonus Networks. All rights reserved.

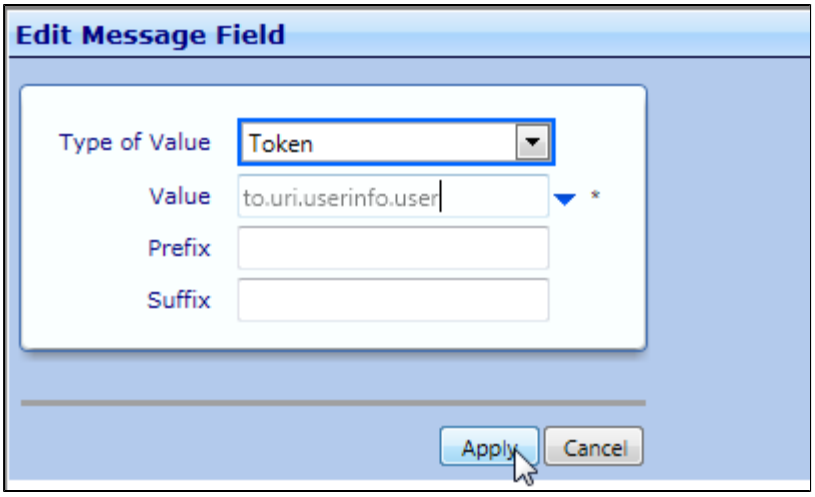


5. Set the URI User (info) to *Modify* and click the Add/Edit button.

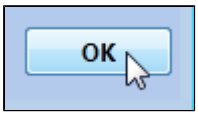


6. Set the Type of Value to *Token* and the *Value* to *to.uri.userinfo.user* (selected from the pop-up box generated by clicking the arrow to the right of the field). This setting says to set the Request URI from the number listed in the TO header (userinfo.user=number).

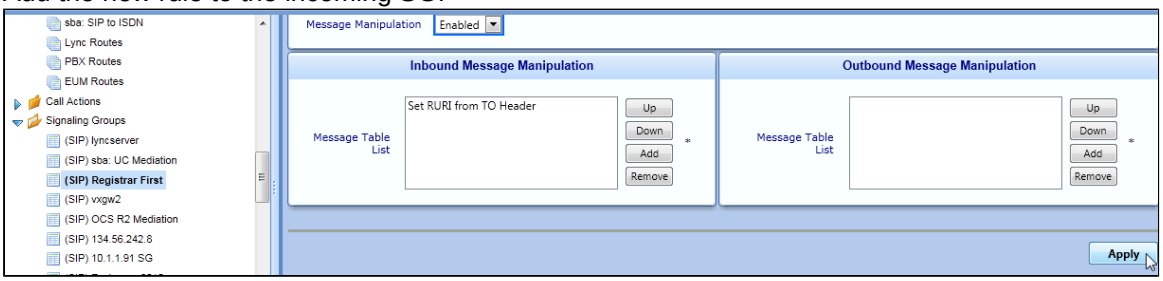
Copyright © 2015 Sonus Networks. All rights reserved.



7. Click the OK button.



8. Add the new rule to the incoming SG.



Debugging Output

> In the debugging output below, the RURI Header Manipulation rule was modified to take the number from the FROM header, not the TO header so that it would be easier to follow the header manipulation function in the debug.

```
INVITE sip:14083489775@10.1.1.74 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.90:53770;branch=z9hG4bK-d87543-a30cd0225701a76e-1--d87543-;rport
Max-Forwards: 70
Contact: <sip:444@10.1.1.90:53770>
To: "14083489775"<sip:14083489775@10.1.1.74>
From: "test"<sip:444@10.1.1.74>;tag=f80e8e32
Call-ID: YmM2NWZkNTA5ZTcwYWE5NzQyYTZiMDE4NTk1NmU5NWI.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
User-Agent: eyeBeam release 1011w stamp 41324
Content-Length: 511

...

[2012-10-30 10:56:47,158] 4563 000d com.net.ux.sip DEBUG (Executive.cpp:52) - Run: Protocol
```

Copyright © 2015 Sonus Networks. All rights reserved.

Engine::Executive running 1 rules
[2012-10-30 10:56:47,158] 4564 000c com.net.ux.sip TRACE (Executive.cpp:58) - Run: Protocol Engine::getting ruleid (1)
[2012-10-30 10:56:47,158] 4565 000b com.net.ux.sip TRACE (Executive.cpp:75) - Run: Processing Message Rule (test1)
[2012-10-30 10:56:47,158] 4566 000a com.net.ux.sip TRACE (Executive.cpp:127) - processMessageRule: Processing Message Rule (1)
[2012-10-30 10:56:47,158] 4567 0009 com.net.ux.sip TRACE (Executive.cpp:1252) - MatchSipMessageRule: StartLine from configuration (*)From Msg (INVITE sip:14083489775@10.1.1.74 SIP/2.0)
[2012-10-30 10:56:47,158] 4568 0008 com.net.ux.sip DEBUG (HeaderRule.h:912) - debugInfo: HeaderRuleFieldModify
[2012-10-30 10:56:47,158] 4569 0007 com.net.ux.sip DEBUG (HeaderRule.h:798) - debugInfo: HeaderRuleFieldChange mReplacement
[2012-10-30 10:56:47,158] 4570 0006 com.net.ux.sip DEBUG (ProtocolField.h:93) - debugInfo: FieldElement:: FieldType(0) Source(header["from",1].uri[1].userinfo.user)
[2012-10-30 10:56:47,158] 4571 0005 com.net.ux.sip DEBUG (ProtocolField.h:272) - debugInfo: FieldElementObject:: Valid Object Tokens
[2012-10-30 10:56:47,158] 4572 0004 com.net.ux.sip DEBUG (HeaderRule.h:679) - debugInfo: HeaderRuleField:: Element
[2012-10-30 10:56:47,158] 4573 0003 com.net.ux.sip DEBUG (ProtocolField.h:93) - debugInfo: FieldElement:: FieldType(0) Source(requestline.uri.userinfo.user)
[2012-10-30 10:56:47,159] 4574 0002 com.net.ux.sip DEBUG (ProtocolField.h:272) - debugInfo: FieldElementObject:: Valid Object Tokens
[2012-10-30 10:56:47,159] 4575 0001 com.net.ux.sip DEBUG (HeaderRule.h:115) - debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-10-30 10:56:47,160] 4576 0001 com.net.ux.sip DEBUG (RuleBase.h:123) - debugInfo: RuleBase:: RuleBaseType(1) Result(1) Description(testruri) valid(true), Condition Expression(No conditions for this header rule)
[2012-10-30 10:56:47,160] 4577 0001 com.net.ux.sip TRACE (Executive.cpp:211) - processMessageRule: Processing Header rule
[2012-10-30 10:56:47,160] 4578 0001 com.net.ux.sip DEBUG (Executive.cpp:316) - processHeaderRule: Processing header Rule (testruri)
[2012-10-30 10:56:47,160] 4579 0001 com.net.ux.sip TRACE (Executive.cpp:489) - processHeaderRule: Processing Rule Field Modify
[2012-10-30 10:56:47,160] 4580 0001 com.net.ux.sip TRACE (Executive.cpp:727) - buildField: Building fields with element count=1
[2012-10-30 10:56:47,160] 4581 0001 com.net.ux.sip TRACE (Executive.cpp:736) - buildField: Building field object
[2012-10-30 10:56:47,160] 4582 0001 com.net.ux.sip TRACE (SipMessage.cpp:1311) - getObjectValue: name:(3:Header) value:
[2012-10-30 10:56:47,161] 4583 0001 com.net.ux.sip TRACE (Executive.cpp:1161) - **headerFieldModify: Executing header field modify, replacement=444**
[2012-10-30 10:56:47,161] 4584 0001 com.net.ux.sip TRACE (Executive.cpp:1165) - headerFieldModify: Header field modify single ordinal
[2012-10-30 10:56:47,161] 4585 0001 com.net.ux.sip TRACE (SipMessage.cpp:1311) - getObjectValue: name:(1:RequestLine) value:
[2012-10-30 10:56:47,161] 4586 0001 com.net.ux.sip TRACE (SipMessage.cpp:1391) - **setObjectValue: name:(1:RequestLine) value:444**
[2012-10-30 10:56:47,161] 4587 0001 com.net.ux.sip TRACE (Executive.cpp:218) - processMessageRule: HeaderRule executed
[2012-10-30 10:56:47,161] 4588 0001 com.net.ux.sip TRACE (Executive.cpp:81) - Run: Message Rule (1) matched at least one message rule

Copyright © 2015 Sonus Networks. All rights reserved.

[2012-10-30 10:56:47,161] 4589 0001 com.net.ux.sip DEBUG (sipSignalingGroup.cpp:794) - {SG(3) 0x2476b8} ProcessTransportMessage: Protocol Repair, out of Ingress executive

...

[2012-10-30 10:56:47,237] 4966 000d com.net.ux.route INFO (callrouter.cpp:2280) - Using table sba: SIP to ISDN (3) to route call.
[2012-10-30 10:56:47,237] 4967 000c com.net.ux.route INFO (callrouter.cpp:2458) - Rule sba: To Internal Ext. (3.1(2)) skipped due to route disabled.
[2012-10-30 10:56:47,237] 4968 000b com.net.ux.route DEBUG (translation.cpp:1295) - Performing OPTIONAL transformation using entry Subscriber Access # from PSTN (5.1(1)).
[2012-10-30 10:56:47,237] 4969 000a com.net.ux.route DEBUG (translation.cpp:634) - **Failed regex match of "tfCalledNumber" field for "(+14083483539)" (updated "(+14083483539)") with input of "444"**
[2012-10-30 10:56:47,237] 4970 0009 com.net.ux.route DEBUG (translation.cpp:1295) - Performing OPTIONAL transformation using entry EUM SA 302 route (5.2(2)).
[2012-10-30 10:56:47,237] 4971 0008 com.net.ux.route DEBUG (translation.cpp:634) - **Failed regex match of "tfCalledNumber" field for "3539" (updated "3539") with input of "444"**
[2012-10-30 10:56:47,238] 4972 0007 com.net.ux.route INFO (callrouter.cpp:2458) - Rule Static Routing (3.3(12)) skipped due to route disabled.
[2012-10-30 10:56:47,238] 4973 0006 com.net.ux.route DEBUG (translation.cpp:1295) - Performing MANDATORY transformation using entry sba: Full Num. to Ext. (Called) (23.1(1)).
[2012-10-30 10:56:47,238] 4974 0005 com.net.ux.route DEBUG (translation.cpp:634) - **Failed regex match of "tfCalledNumber" field for "+.**(\d{4})" (updated "+.**(\d{4})") with input of "444"**

Important Notes

The SIP Header feature cannot **generate** a new SIP packet. Only arriving or leaving SIP packets changed via the SIP Header function.

Care must be exercised when modifying incoming SIP packets, especially with respects to the TO, FROM and RURI headers. Modifying tags, IDs or any other items that define the dialogue or transactions, will likely cause calls to not complete.

rev 0.4

SIP Message Manipulation - Setting the P-Asserted Identity

Copyright © 2015 Sonus Networks. All rights reserved.

Table of Contents

- Prerequistes
- Summary
- PAI Static Modification
  - Configure the SBC1000/2000
  - Debugging Output
  - Conditional PAI Modification
  - Important Notes

About this Page

- A sneak peek into the SBC 1000/2000's new SIP Header Manipulation Feature. This new feature permits any SIP header to be added, deleted, or modified.
- This SIP Header Manipulation example uses the *Literal* manipulation option and shows how perform Header Manipulation only when certain criteria are met.
- This document uses the *Conditional Rules* feature to limit Message Manipulation to very specific instances.

Related Articles

- Managing Signaling Groups

Prerequistes

Requires Sonus SBC2000/1000 Version 2.2

Summary

Because you can never tell just what the other side might send or need, the SBC1000/2000 version 2.2 will include a feature to manipulate any SIP header.

- SIP Headers can be added, deleted, or modified.
- Manipulation can be done for every SIP message, or separately for SIP Requests or SIP Responses.
- Manipulations can set to occur based upon user specified matching criteria.
- Manipulations can be executed at the ingress or egress SG. At the ingress, inbound SIP messages are modified to permit proper handling by the SBC's routing function. At the egress, SIP messages already processed by the SBC are modified to meet the SIP requirements of the upstream device.

PAI Static Modification

In today's sneak peek, we modifiy the PAI at the egress SG for a PSTN > SBC > Lync call. This is an example of a static replacement--a replacement that will take place on every SIP packet that leaves the SBC bound for Lync.

Near the end of the document, we'll add a configuration that will make the PAI modification conditional, only changing the PAI when certain criteria is met.

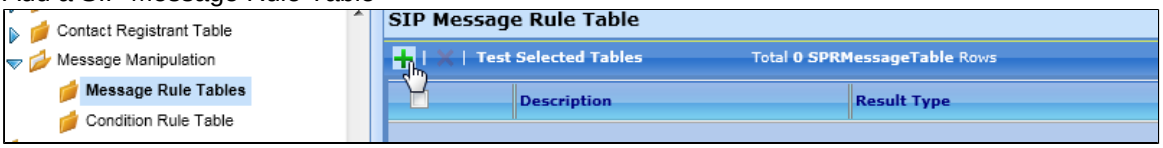
Configure the SBC1000/2000

Copyright © 2015 Sonus Networks. All rights reserved.

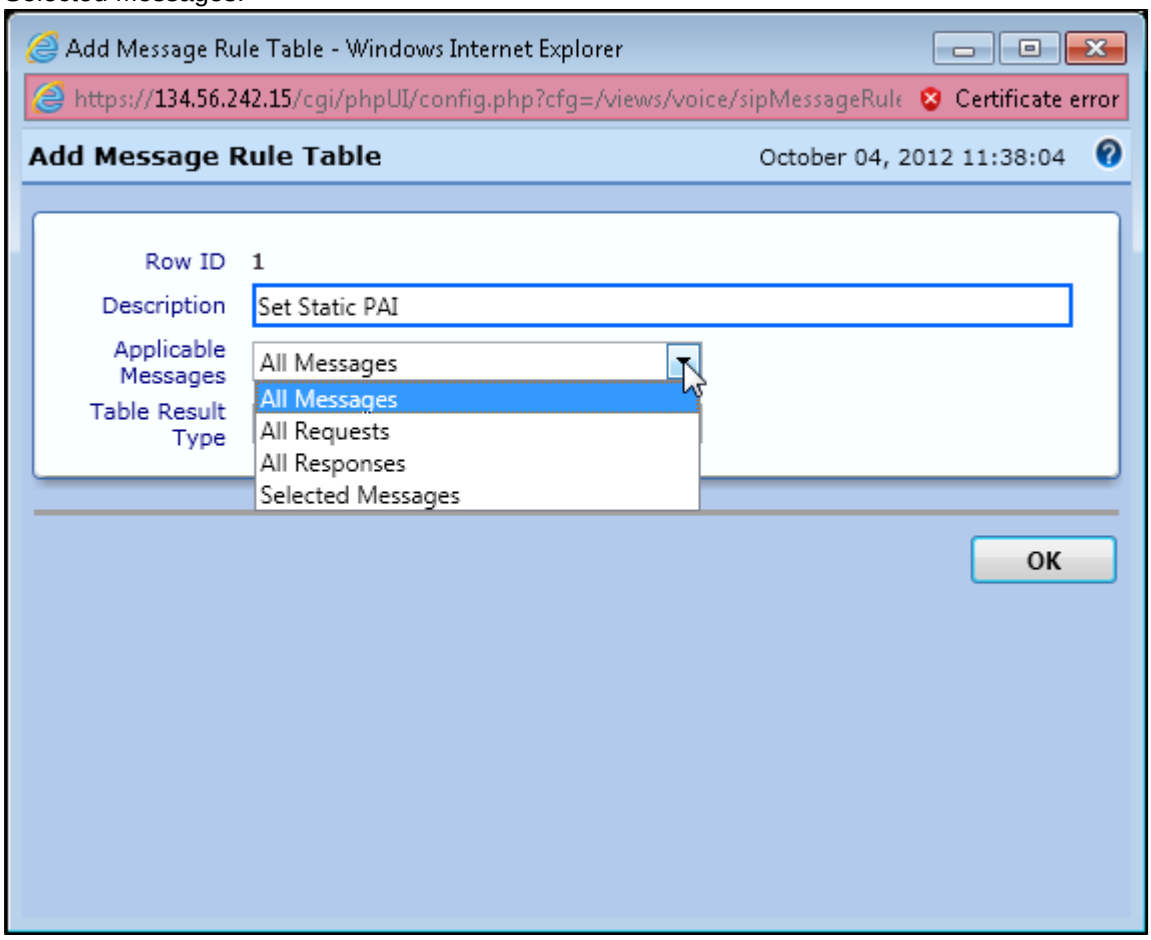
1. Select the new Message Manipulation entry in the navigation tree



2. Add a SIP Message Rule Table



3. Set how the rule will be applied. It can be applied to All SIP Messages, only Requests, only Responses, or Selected Messages.

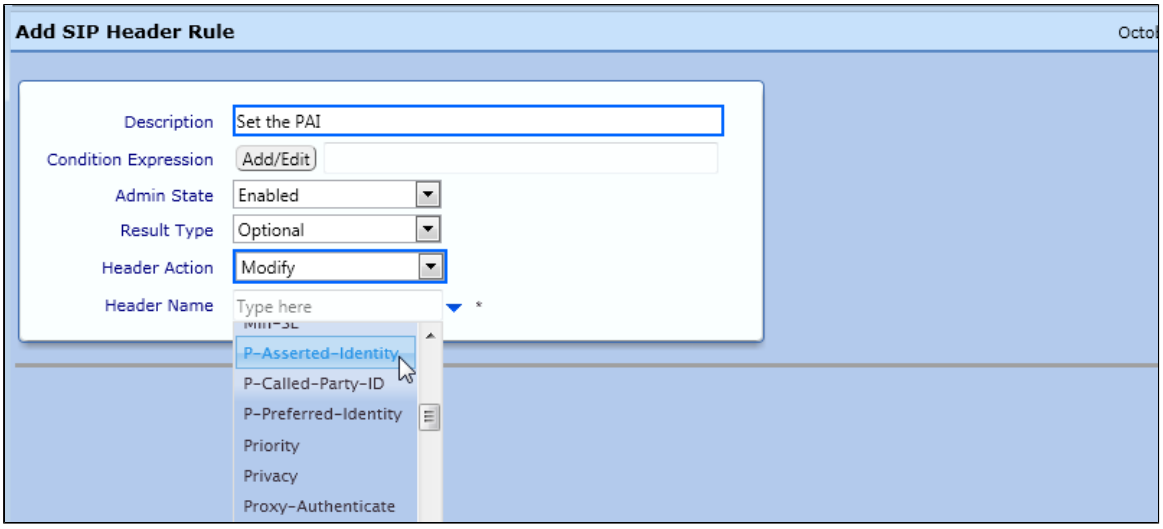


4. Add an entry to the new table.

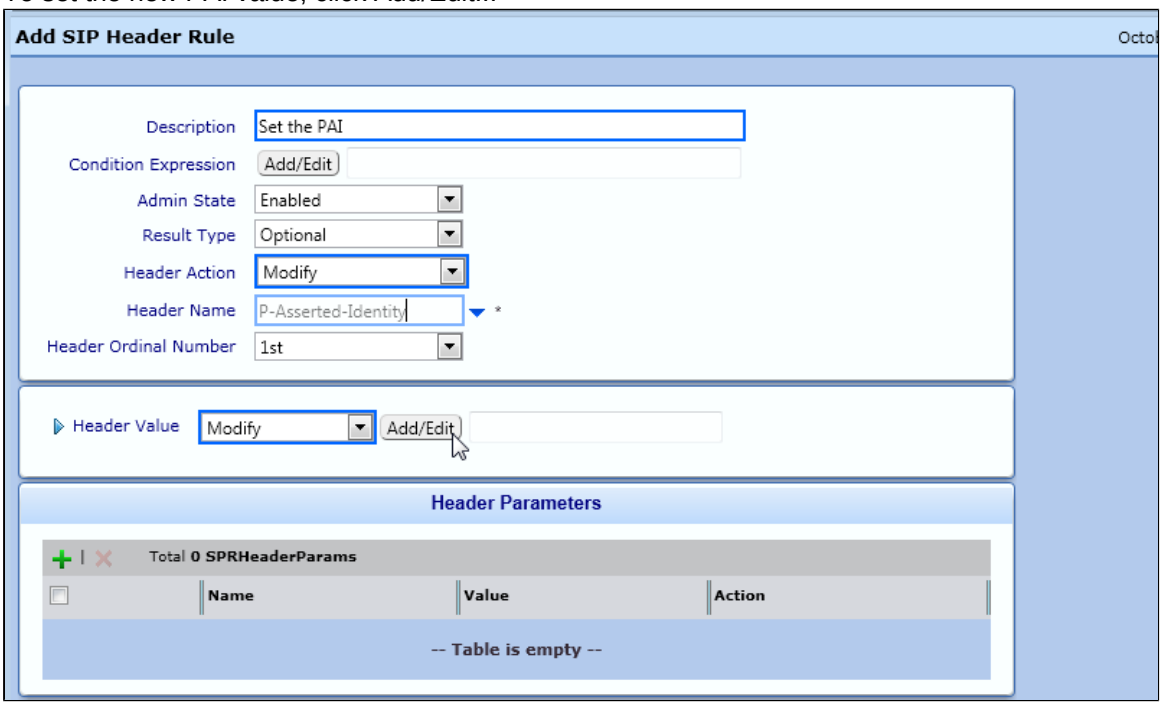


5. Set the Header Action to *Modify* and the Header Name to *P-Asserted-Identity*. As you can see, any SIP Header can be manipulated.

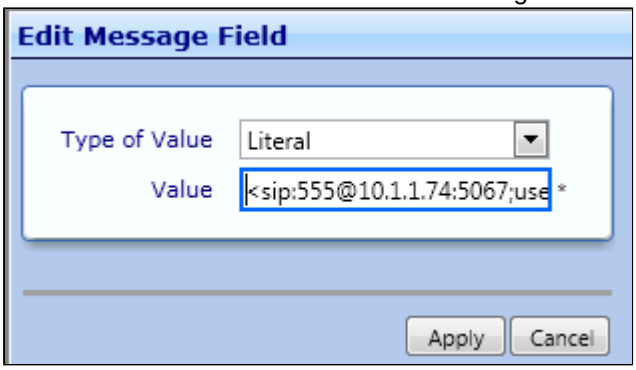
Copyright © 2015 Sonus Networks. All rights reserved.



6. To set the new PAI value, click Add/Edit...

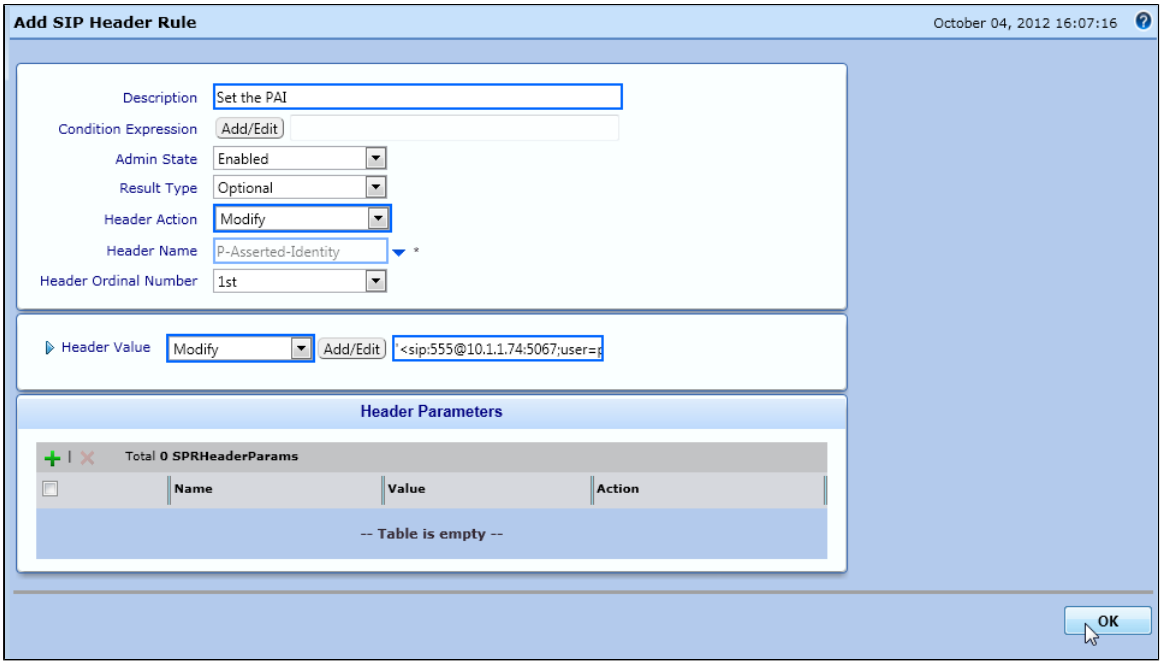


7. ... and add the new value in the Edit Message Field

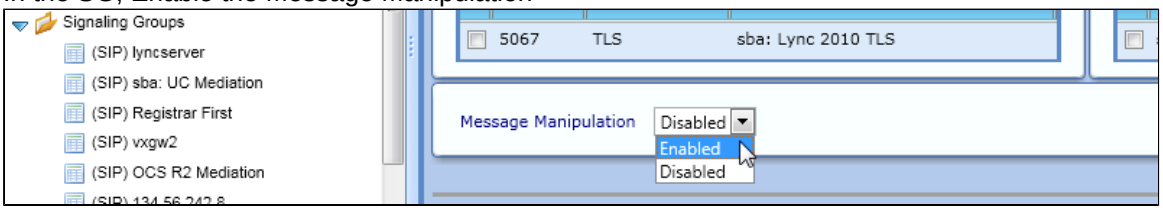


8. Click OK to complete adding the entry to the table.

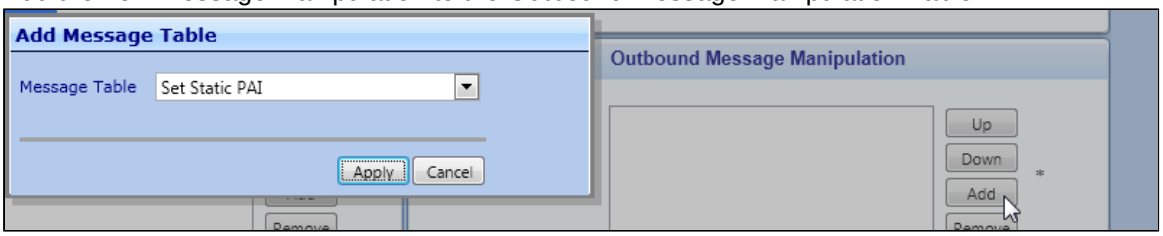
Copyright © 2015 Sonus Networks. All rights reserved.



9. In the SG, Enable the Message Manipulation



10. Add the new Message Manipulation to the Outbound Message Manipulation Table



Debugging Output

In the debugging output below, you can see the PAI change from +15103644064 to 555

```
[2012-10-03 18:20:32,198] 5392 0001 com.net.ux.sip DEBUG (Transaction.cpp:685) -
egressProtocolRepair: Transaction Protocol Repair (Transaction),calling Egress
executive(1 item(s) on list)
[2012-10-03 18:20:32,198] 5393 0001 com.net.ux.sip DEBUG (Executive.cpp:52) - Run:
Protocol Engine::Executive running 1 rules
[2012-10-03 18:20:32,198] 5394 0001 com.net.ux.sip TRACE (Executive.cpp:58) - Run:
Protocol Engine::getting ruleid (1)
[2012-10-03 18:20:32,198] 5395 0001 com.net.ux.sip TRACE (Executive.cpp:75) - Run:
Processing Message Rule (PAI fix)
[2012-10-03 18:20:32,198] 5396 0001 com.net.ux.sip TRACE (Executive.cpp:127) -
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
processMessageRule: Processing Message Rule (1)
[2012-10-03 18:20:32,198] 5397 0001 com.net.ux.sip TRACE (Executive.cpp:1252) -
MatchSipMessageRule: StartLine from configuration (*)From Msg (INVITE
sip:+14083483531@sba1.vx.net:5067;user=phone SIP/2.0
)
[2012-10-03 18:20:32,198] 5398 0001 com.net.ux.sip DEBUG (HeaderRule.h:231) -
debugInfo: HeaderRuleModify
[2012-10-03 18:20:32,198] 5399 0001 com.net.ux.sip DEBUG (HeaderRule.h:176) -
debugInfo: HeaderRulePayload:: FieldList
[2012-10-03 18:20:32,198] 5400 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(<sip:555@10.1.1.74:5067;user=phone>)
[2012-10-03 18:20:32,199] 5401 0001 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(<sip:555@10.1.1.74:5067;user=phone>)
[2012-10-03 18:20:32,199] 5402 0001 com.net.ux.sip DEBUG (HeaderRule.h:115) -
debugInfo: HeaderRule:: HeaderRuleType(1)
[2012-10-03 18:20:32,199] 5403 0001 com.net.ux.sip DEBUG (RuleBase.h:123) -
debugInfo: RuleBase:: RuleBaseType(1)  Result(0) Description(test pai) valid(true),
Condition Expression(${1})
[2012-10-03 18:20:32,199] 5404 0001 com.net.ux.sip TRACE (Executive.cpp:211) -
processMessageRule: Processing Header rule
[2012-10-03 18:20:32,199] 5405 0001 com.net.ux.sip DEBUG (Executive.cpp:316) -
processHeaderRule: Processing header Rule (test pai)
[2012-10-03 18:20:32,199] 5406 0001 com.net.ux.sip TRACE (Executive.cpp:328) -
processHeaderRule: Processing header Conditions Count=1
[2012-10-03 18:20:32,199] 5407 0001 com.net.ux.sip TRACE (Executive.cpp:640) -
processConditionRules: Condition Rule value=1
[2012-10-03 18:20:32,199] 5408 0001 com.net.ux.sip TRACE (Executive.cpp:652) -
evaluateConditionRuleTruth: CREId=1
[2012-10-03 18:20:32,199] 5409 0001 com.net.ux.sip DEBUG (ConditionRule.h:121) -
debugInfo: ConditionRule:: Description: test rule AdminState(0) Result(0) Operand(1)
valid(true)
[2012-10-03 18:20:32,199] 5410 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(0) Source(header["from",1].uri[1].userinfo.user)
[2012-10-03 18:20:32,200] 5411 0001 com.net.ux.sip DEBUG (ProtocolField.h:272) -
debugInfo: FieldElementObject:: Valid Object Tokens
[2012-10-03 18:20:32,200] 5412 0001 com.net.ux.sip DEBUG (ProtocolField.h:93) -
debugInfo: FieldElement:: FieldType(1) Source(+15103644064)
[2012-10-03 18:20:32,200] 5413 0001 com.net.ux.sip DEBUG (ProtocolField.h:211) -
debugInfo: FieldElementLiteral:: stringLiteral(+15103644064)
[2012-10-03 18:20:32,200] 5414 0001 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-10-03 18:20:32,200] 5415 0001 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-10-03 18:20:32,200] 5416 0001 com.net.ux.sip TRACE (SipMessage.cpp:1311) -
getObjectValue: name:(3:Header) value:
[2012-10-03 18:20:32,200] 5417 0001 com.net.ux.sip TRACE (Executive.cpp:706) -
evaluateConditionRuleTruth: Full CR match=1. oObj=+15103644064, oMatch=+15103644064,
oObjLen=12, oMatchLen=12
[2012-10-03 18:20:32,200] 5418 0001 com.net.ux.sip TRACE (Executive.cpp:336) -
processHeaderRule: Condition matched
[2012-10-03 18:20:32,200] 5419 0001 com.net.ux.sip TRACE (Executive.cpp:374) -
processHeaderRule: Processing Rule Modify
[2012-10-03 18:20:32,200] 5420 0001 com.net.ux.sip TRACE (Executive.cpp:727) -
buildField: Building fields with element count=1
[2012-10-03 18:20:32,200] 5421 0001 com.net.ux.sip TRACE (Executive.cpp:755) -
buildField: Building field literal
[2012-10-03 18:20:32,201] 5422 0001 com.net.ux.sip TRACE (Executive.cpp:963) -
headerModify: Executing header modify
[2012-10-03 18:20:32,201] 5423 0001 com.net.ux.sip TRACE (Executive.cpp:1297) -
checkOrdinalAll: ObjectToken:: StringIndex(p-asserted-identity) Ordinal(1)
[2012-10-03 18:20:32,201] 5424 0001 com.net.ux.sip TRACE (Executive.cpp:967) -
headerModify: Header modify single ordinal
[2012-10-03 18:20:32,201] 5425 0001 com.net.ux.sip TRACE (SipMessage.cpp:1311) -
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
getObjectValue: name:(3:Header) value:
[2012-10-03 18:20:32,201] 5426 0001 com.net.ux.sip TRACE (SipMessage.cpp:1391) -
setObjectValue: name:(3:Header) value:<sip:555@10.1.1.74:5067;user=phone>
[2012-10-03 18:20:32,201] 5427 0001 com.net.ux.sip TRACE (Executive.cpp:218) -
processMessageRule: HeaderRule executed
[2012-10-03 18:20:32,201] 5428 0001 com.net.ux.sip TRACE (Executive.cpp:81) - Run:
Message Rule (1) matched at least one message rule
[2012-10-03 18:20:32,201] 5429 0001 com.net.ux.sip DEBUG (Transaction.cpp:687) -
egressProtocolRepair: Transaction Protocol Repair, out of Egress executive
[2012-10-03 18:20:32,202] 5430 0001 com.net.ux.sip DEBUG (TransportLayer.cpp:1316) -
startTransaction: Sending data if=0.
[2012-10-03 18:20:32,203] 5431 0001 com.net.ux.sip.libctl TRACE
(TransportTlsSocket.cpp:2278) - TX application data size: 990 for conn_id: 427 on
handle: 0x2200b8, retry: 0, retry attempts: 0
[2012-10-03 18:20:32,204] 5432 0001 com.net.ux.sip DEBUG (TransportLayer.cpp:538) -
0x293a30 sending from [10.1.1.74]:25174 to [10.1.1.73]:5067 990 bytes over
00TLS722-25174 attempt(1) (If:0) ln(1320):
[2012-10-03 18:20:32,204] 5433 0001

INVITE sip:+14083483531@sba1.vx.net:5067;user=phone SIP/2.0
Allow: INVITE, ACK, CANCEL, BYE, UPDATE, NOTIFY, OPTIONS, REFER, REGISTER
Call-ID: call-4CE51900-0000-0010-0C13-B
Contact: <sip:+15103644064@ux.vx.net:5067;transport=TLS>
Content-Length: 353
Content-Type: application/sdp
CSeq: 1 INVITE
From:  <sip:+15103644064@10.1.1.74:5067;user=phone>;tag=a01014a-85
Max-Forwards: 70
P-Asserted-Identity:  <sip:555@10.1.1.74:5067;user=phone>
Supported: replaces,update,100rel
To:  <sip:+14083483531@sba1.vx.net:5067;user=phone>
User-Agent: NET UX 2.2.0v177 UX
Via: SIP/2.0/TLS 10.1.1.74:5067;branch=z9hG4bK-UX-0a01-014a-02fa

v=0
o=UX 1007 1007 IN IP4 10.1.1.74
s=VoipCall
c=IN IP4 10.1.1.74
t=0 0
m=audio 16432 RTP/SAVP 8 0 101 13
c=IN IP4 10.1.1.74
a=rtpmap:8 PCMA/8000/1
a=rtpmap:0 PCMU/8000/1
a=rtpmap:101 telephone-event/8000
a=rtpmap:13 CN/8000
a=ptime:20
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:oovkXPxgygyKXpZrX9W4gx9s6z1KQnRnIrk/mNcT|2^31|1:1
```

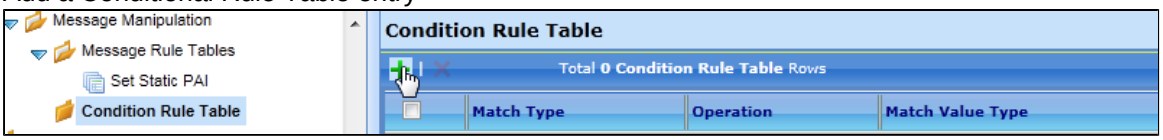
Copyright © 2015 Sonus Networks. All rights reserved.

```
a=[2012-10-03 18:20:32,204] 5434 0001
sendrecv
```

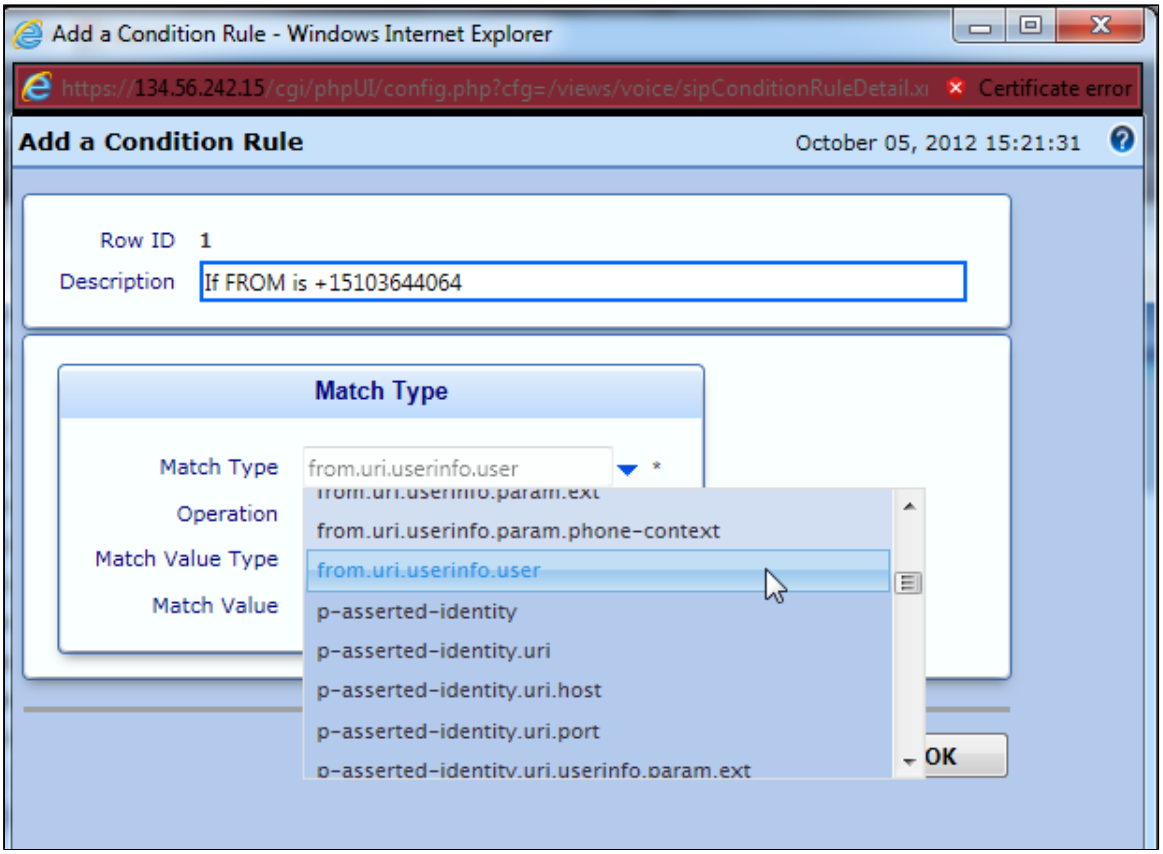
Conditional PAI Modification

By adding a Conditional Rule to the Message Rule, you can perform the manipulation only when it matches a particular condition. In the example below, the PAI would only be modified if the call is from +15103644064.

1. Add a Conditional Rule Table entry

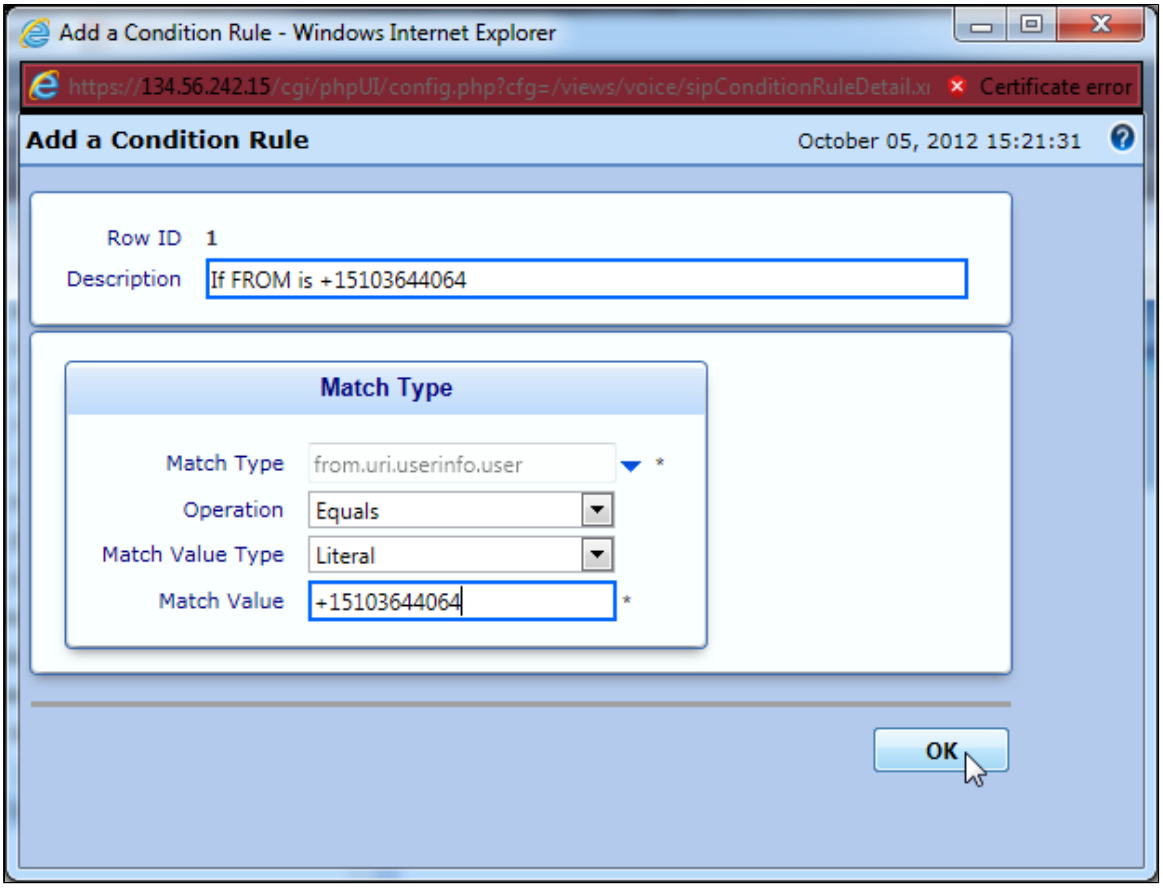


2. Add the Description and set the *Match Type* from the pulldown. In this case, we're looking to match the calling number, which is represented by the *from.uri.userinfo.user* token.

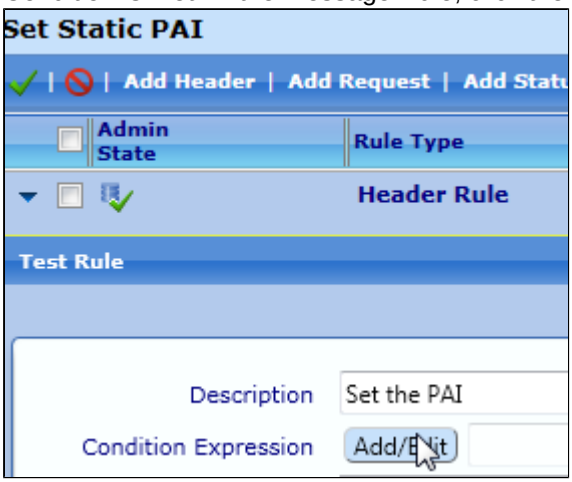


3. Set the *Operation* to *Equals*. Set the *Match Value Type* to *Literal* and put the number to be matched into the *Match Value*.

Copyright © 2015 Sonus Networks. All rights reserved.

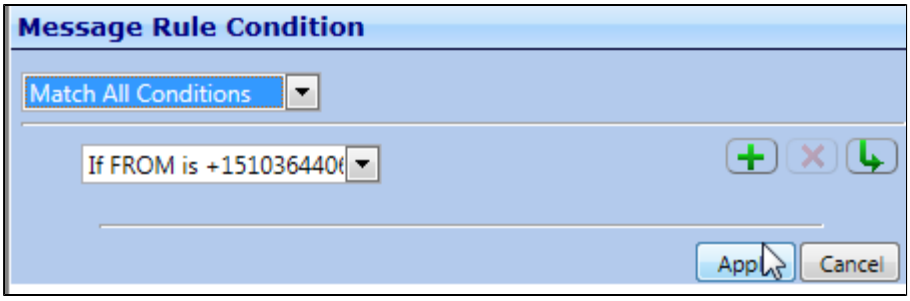


4. With the Match information configured, it's time to modify the Message Rule so that it only runs when the Condition is met. In the Message Rule, click the *Condition Expression Add/Edit* button.

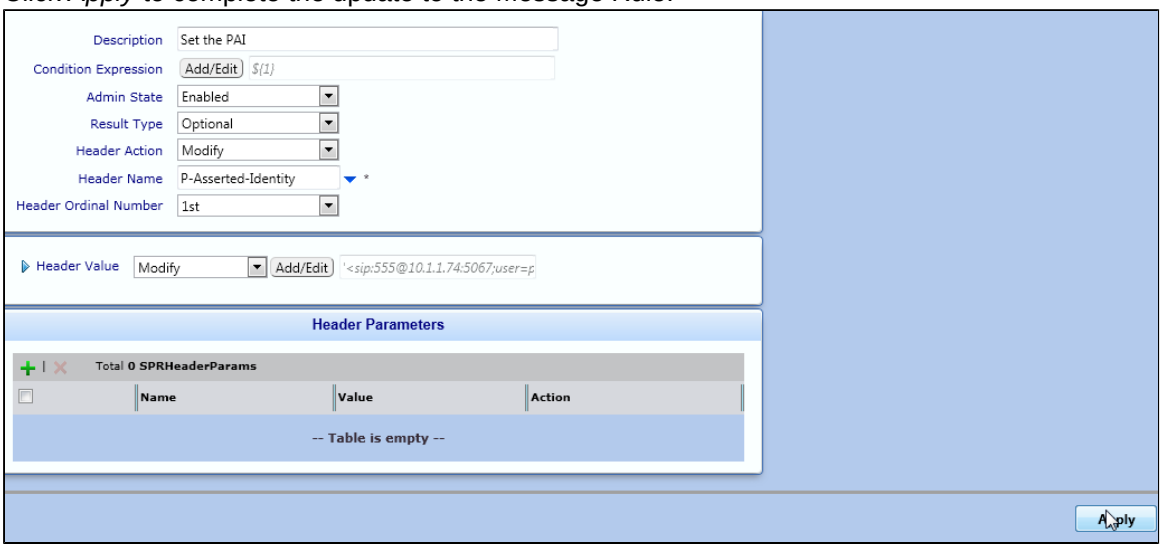


5. Set it for *Match All Conditions* and select the Conditional Rule you just finished programming in the previous steps. Click *Apply*.

Copyright © 2015 Sonus Networks. All rights reserved.



6. Click *Apply* to complete the update to the Message Rule.



Important Notes

The SIP Header feature cannot **generate** a new SIP packet. Only arriving or leaving SIP packets changed via the SIP Header function.

rev 0.3

Using HISTORY-INFO to set the FROM Number

Table of Contents

- Prerequistes
- Moving the History-Info Number to the FROM Number
  - Configure the SBC1000/2000 for Header Manipulation

Copyright © 2015 Sonus Networks. All rights reserved.

About this Page

- This document details how to configure the SBC to copy a value from the HISTORY-INFO SIP header into the Calling Number.
- This document shows the creation of a SMM Rule Table that selects only certain SIP Messages for modification. In this case, only INVITE packets will be inspected.
- This document details how to use the SMM feature copy a header value into one of the user-controlled IEs (SG User Value 1).
- This document details how to copy a user-controlled IE value into the Calling Name IE using the Transformation Table.

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups

Prerequistes

Requires Sonus SBC2000/1000 Version 2.2 or later

Moving the History-Info Number to the FROM Number

Normally, the SBC automatically maps History-Info into Redirecting Number; however, the automated mapping function works for specific *reasons* encoded in the History-Info header. In some cases, like Lync's forwarding feature, a *reason* is not present.

SMM may be used to map the History-Info to the FROM (or Redirecting) as detailed in this document.

The process entails:

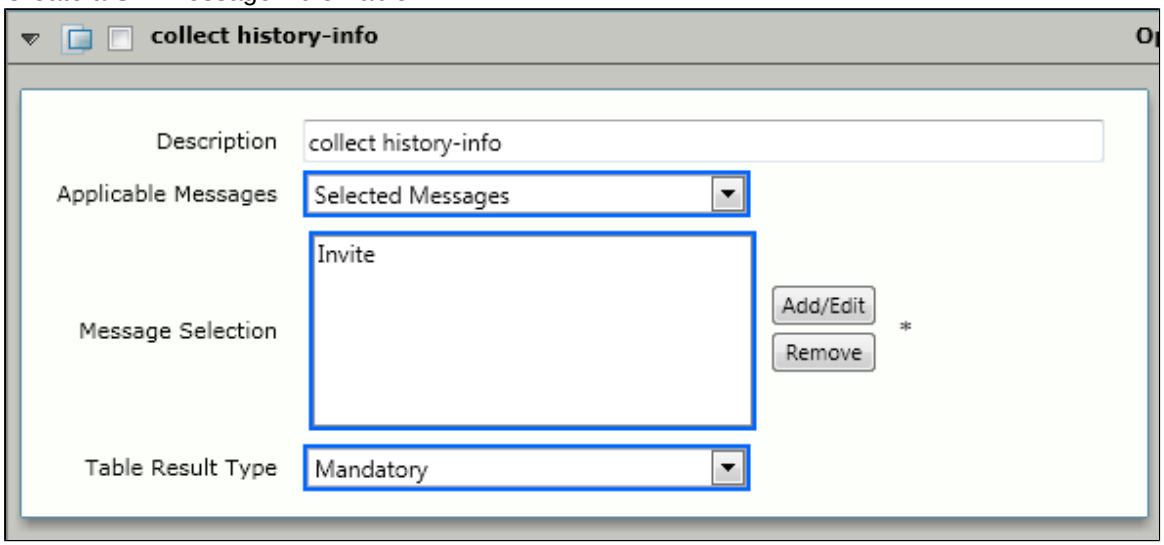
- Copy the contents of the first ordinal in the History-Info header to *SG User Value 1*. The *first ordinal* (in italics below) is considered anything before the comma which is used to separate the lineage (history) of the call.
- A translation table copies a modified value from *SG User Value 1* to the *Calling Number* IE.

INVITE sip:3539@10.1.1.74 SIP/2.0
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, REFER, NOTIFY, REGISTER
Via: SIP/2.0/UDP 10.1.1.91
To: <sip:3539@10.1.1.74>
From: <sip:13790060529@10.1.1.74>;tag=254b0000
Call-ID: 4-1f0@10.1.1.91
CSeq: 552136960 INVITE
Contact: sip:test@10.1.1.91
HISTORY-INFO: <*sip:**+39975379***@*bcc-lyncFE-01.com;user=phone>;index=1;ms-retarget-reason=forwarding* **,**
<sip:+13790060529@bcc-lyncFE-01.com;user=phone>;index=1.2
Cisco-Guid: 4170650438-384321033-2730718288-2880066070
Content-Type: application/sdp
Content-Length: 250

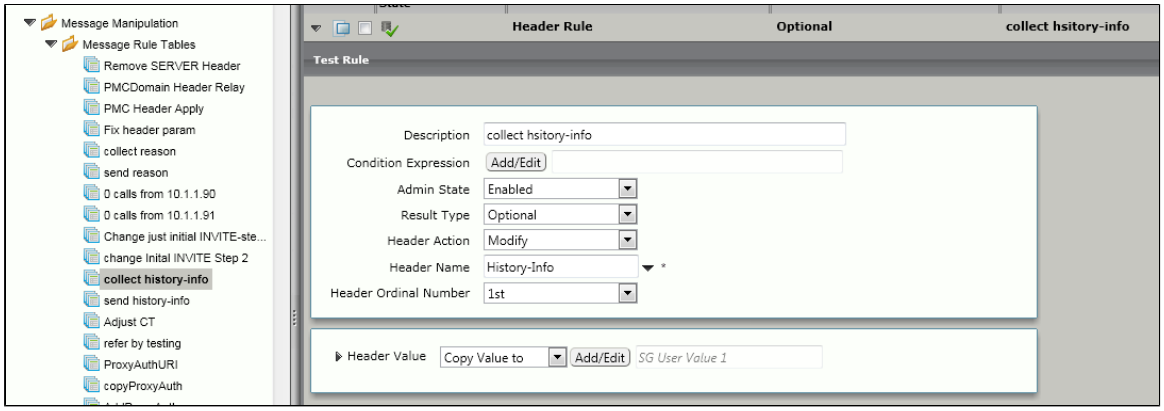
Copyright © 2015 Sonus Networks. All rights reserved.

Configure the SBC1000/2000 for Header Manipulation

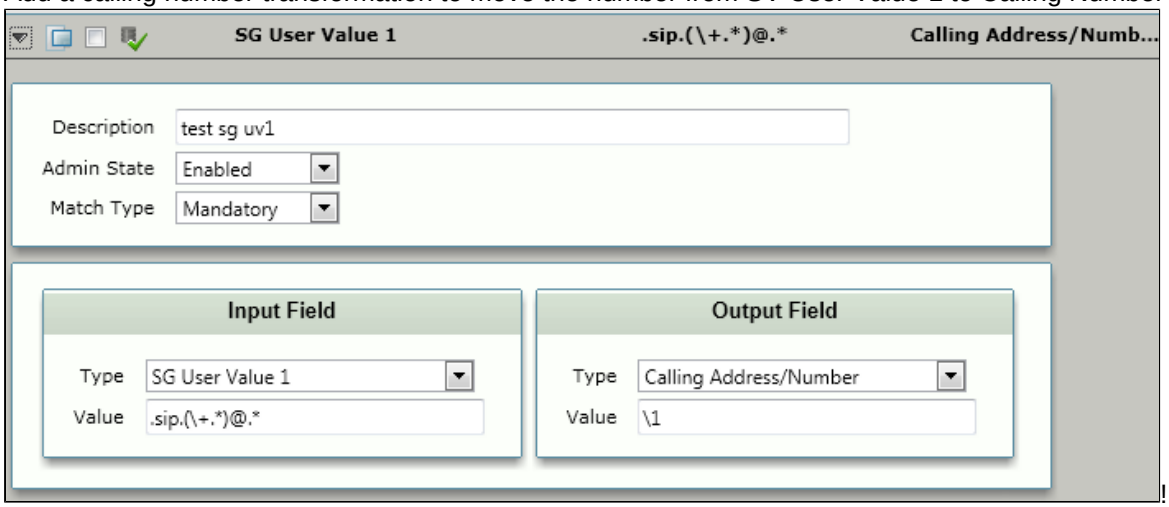
1. Create a SIP Message Rule Table.



2. Add a SIP Message Rule to capture the first ordinarl of the History-infoheader using the *Add Header* selection.



3. Add a calling number transformation to move the number from SV User Value 1 to Calling Number



Copyright © 2015 Sonus Networks. All rights reserved.

```
INVITE sip:+13539@lyncserver.sbc.net:5068 SIP/2.0
Allow: INVITE, ACK, CANCEL, BYE, UPDATE, NOTIFY, OPTIONS, REFER, REGISTER
Call-ID: call-63002900-0000-0010-0C13-12@10.1.1.74
Contact: <sip:+39975379@10.1.1.74:5066;transport=TCP>
Content-Length: 231
Content-Type: application/sdp
CSeq: 2 INVITE
From: <sip:+39975379@sbc2000.sbc.net>;tag=a01014a-2977
Max-Forwards: 70
Supported: replaces,update,100rel
To: <sip:+13539@lyncserver.sbc.net:5068>
User-Agent: SONUS SBC1000/2000 3.0.0v222 UX
Via: SIP/2.0/TCP 10.1.1.74:5066;branch=z9hG4bK-UX-0a01-014a-3821
```

Action Set Documents

- How Action Sets Work
- SBC AD Integrated Application Solutions using Action Sets, Rev 0.3

How Action Sets Work

Introduction

The purpose for a UX is to route calls – matching and modifying telephone numbers, adding diversions, applying calling names. Call Routes and Transformation Tables are the tools typically selected to perform these functions, but they are not the only, nor the most powerful, manipulation tools available in the UX.

Action Sets operate similarly to Call Routes, but because Action Sets are performed before call routing, Action Sets provide the capability to perform a high degree of number normalization before engaging the call router. Even more importantly, Action Sets incorporate a powerful set of programatic functionality that permits the construction of calling applications.

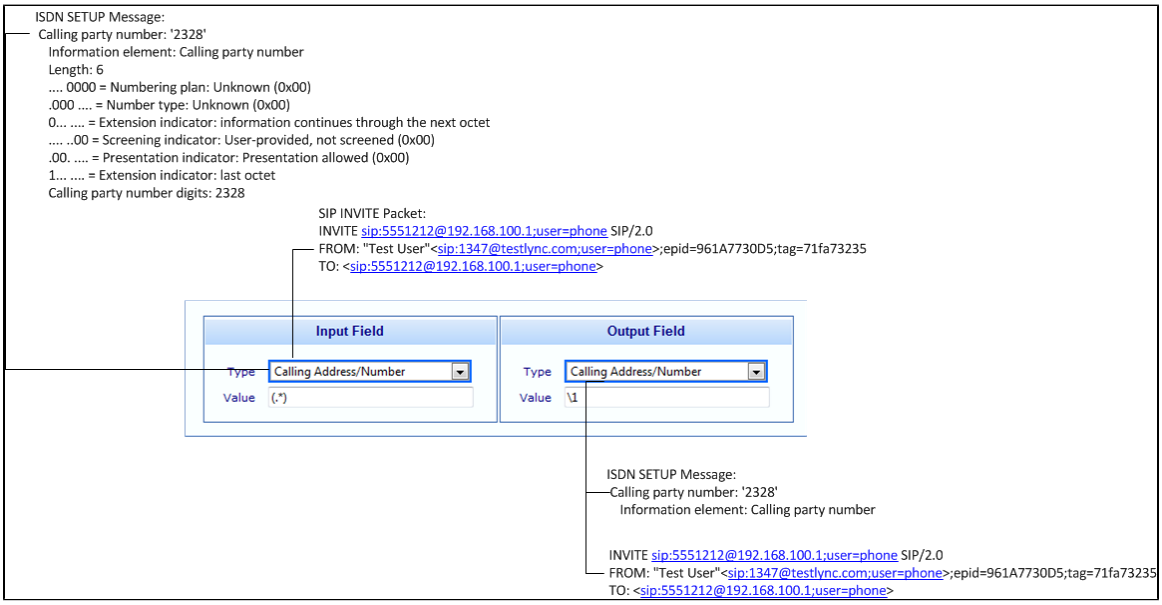
In this article you will learn the basics of Action Sets and their capabilities. We'll begin with a quick review of basic call routing, look at the Action Set components, reveal the steps to create an Action Set, and finally follow the Action Set processing step-by-step.

Basic UX Call Routing

Stored Information Elements (IEs)

Copyright © 2015 Sonus Networks. All rights reserved.

Figure 1: Mapping SIP and ISDN Calling Numbers into UX Information Elements



When a call arrives at UX, the information contained in the incoming message (called number, calling number, name, etc.) is stored into variables within UX. These variables are called Information Elements, a nomenclature lifted from ISDN definitions. So, for example, when a SIP call arrives, the number in the FROM header is stored in UX's Calling Number IE. All arriving SIP headers or ISDN messages are similarly stored.

Transformation Tables

With the IEs stored, we need a way to compare and manipulate those IEs as a function of routing calls. Within the UX, Transformation Tables provide this functionality. For instance, in a Tranformation Table, called numbers can be matched and changed, caller's names can be looked up in AD and recorded in the Calling Name IE, or diversion headers can be added. This Transformation Table functionality works the same regardless of whether it is called from a Call Route or Action Set. However, there is a difference in Actions Sets and the Call Router when it comes to the **persistance** of manipulations. We'll talk about that in a second.

The Call Router

With basic call routing, Transformation Tables are tied to Call Routes. As a call route is executed, the associated Transformation Table is used to match, and possibly, manipulate the data within the IEs. For example, a Call Route to Lync can be associated with a Transformation Table that checks the called number IE against Active Directory's msRTCSIP-Line attribute. If a match is found, the call is routed to Lync. **If the Transformation Table fails, all the IEs are restored to their original values before the next Call Route Entry is executed.**

Call Routes (group into Call Route Tables) are executed in order from top to bottom. This processing path is immutable--every entry in a call Route Table is processed one at a time from top to bottom (unless the call route entry is disabled).

This fixed top-to-bottom processing works perfectly well for the vast majority of circumstances. But what if we wanted to do further processing based upon success or failure of the msRTCSIP lookup? Maybe the circumstances are such that we want to send the call to a different Call Route Table if the msRTCSIP succeeds, possibly to a shared Transformation Table that performs all the static transformations. This can't be done from a Call Route. From a Call Route, when the Transformation Table succeeds, the call is automatically routed.

Copyright © 2015 Sonus Networks. All rights reserved.

In order to perform additional processing, we need a funciton that permits *programatic* call processing. Action Sets are the answer. They perform a similar function as the Call Route Table, but with a completely different approach to processing.

UX Action Sets

Action Sets are called from the ingress Signaling Group and bypass the Call Route Table setting (if one is configured in the SG). Action Sets provide the opportunity to process transformations **before** sending the call to the call router. Think of it as a chance to normalize all the IEs before routing a call.

And not only do Action Sets provide normalization, but they also provide **two** levels of if/then logic: *Actions* and *Execute If*. These two features are the foundation for creating UX calling application solutions.

Let's start by looking at *Actions*.

Actions

Actions are configured from the *Action Configuration* menu. The available Actions are:

Action	Usage
Route Call	Route a call to the specific call route table
Send Alert	Send Alert/Ring. To be implemented in the future with the One Number Fax function
Send Connect	Send Connect/200 OK. To be implemented in the future with the One Number Fax function
Route Call, Await Connect Timer	Routes the call and starts a timer. Automatically continues execution of the Action Set if the call is not answered before the timer expires. Can be used to create applications to send unanswered calls to a local voicemail store.
Generic Timer	Provides a delay function in processing entries in the Action Set
Invoke Action Set	Invoke a different Action Set. Provides the ability to continue execution with a different Action Set.

Using these Actions, we can do things like:

- Route a call using a specific call route table
- Disconnect a call if a transformation table fails
- Continue processing a call using a different Action Set
- Set an Action to occur if a routed call Rings with No Answer

Once some Actions are created, you need a way to use them. That's where *Action Sets* come into play.

Action Set Table

An Action Set Table contains the list of entries that are executed when that particular Action Set is called (from the ingress SG). Unlike a Call Route Table, the entries in an Action Set are not necessarily processed in sequential order. Instead, by using *Action On Success*, *Action on Failure*, or *Execute If* (in any combination), you can control which Action Set entries are processed.

Copyright © 2015 Sonus Networks. All rights reserved.

Execute If	Transformation Table	Action on Success	Action on Failure
Always	Normalize Incoming Numbers	Continue	Failure - Disconnect Call
Always	Get Calling Name - concat	Continue	Continue
Always	Is the call to EUM SA?	Continue	Continue
Prior Success	AutoID Caller to EUM SA	Action, Route to EUM	Continue
Prior Failure	Is it a FAX number?	Action, Route to EUM	Continue
Always	Is the call to a LYNC Analog device?	Action, RNA Timer, Route to Lync	Continue
Prior Timeout	EUM Leave voicemail, get callee's umbox number	Action, Route to EUM	Failure - Disconnect Call
Always	Is the call to a Lync device?	Action, Route to Lync	Continue
Always	Restore Original Calling Number	Action, Route to PBX	Failure - Disconnect Call

Action Set with various Actions and Execute Ifs

Actions within Action Sets

When an Action Set Entry is executed, the associated Transformation Table is evaluated to be either TRUE or FALSE (the result of whether the Transformation Table succeeded or failed in its matching). So far, exactly the same as an entry in a Call Route Table.

One difference between a Call Route and Action Set is that each entry in a Action Set contains an *Action on Success* and *Action on Failure* setting. These two settings provide control over the next step in processing based upon the outcome of the associated Transformation Set:

- If the Transformation Set succeeds, the Action configured in the *Action on Success* is performed.
- If the Transformation Set fails, the Action configured in the *Action on Failure* is performed.

Transformation Table	Action on Success	Action on Failure
Normalize Incoming Numbers	Continue	Failure - Disconnect Call

In the Action Set Entry above, processing will *Continue* with the next entry (if any) if the transformation is TRUE; but, it will disconnect the call if the transformation is FALSE.

So, unlike the Call Routes, we can control what happens when a Transformation Table succeeds or fails.

> ✅ Using Actions, you can control how the processing proceeds: Route the call; disconnect the call; continue with the current or a different Action Set, etc.

Execute If:

When an Action Set is executed, the execution of individual Action Set entries is controlled by the *Execute If*. Whereas Call Route entries can only be Enabled or Disabled, the execution of Action Set entries can be controlled **based on success or failure of the previous entry**.

Looking at the configuration below, we can see that the first three Action Set entries are *Always* executed. You can also see that the Actions for the third entry's *Success* and *Failure* are configured to *Continue*. Regardless of the outcome of the third entry's Transformation Table, processing will continue. The question is with which entry?

Copyright © 2015 Sonus Networks. All rights reserved.

Execute If	Transformation Table	Action on Success	Action on Failure
Always	Normalize Incoming Numbers	Continue	Failure - Disconnect Call
Always	Get Calling Name - concat	Continue	Continue
Always	Is the call to EUM SA?	Continue	Continue
Prior Success	AutoID Caller to EUM SA	Action, Route to EUM	Continue
Prior Failure	Is it a FAX number?	Action, Route to EUM	Continue

Notice that the fourth entry's *Execute If* is configured to *Prior Success*. This means that the fourth entry will run *only if* the third entry is successful. Alternatively, if the third entry is *not* successful, the fourth entry will be skipped and the fifth entry will run.

You can see that using *Execute If* the order of entry execution can be controlled.

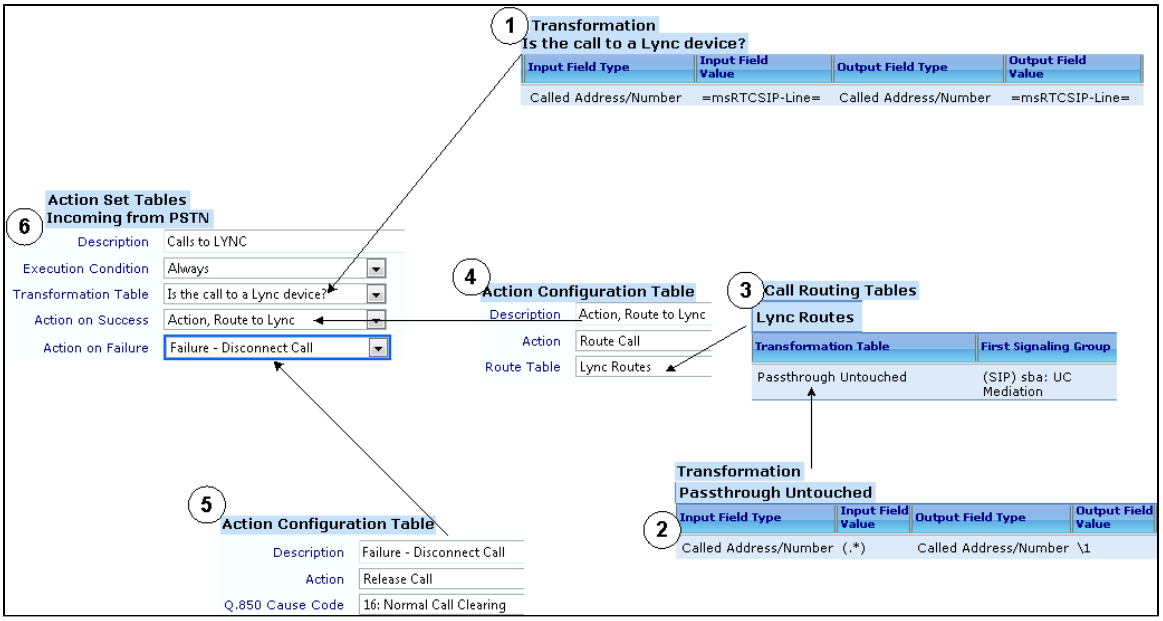
- If an Action Set entry succeeds, the next entry that processes will be set for either *Always* or *Prior Success*.
- If an Action Set entry fails, the next entry that processes will be set for either *Always* or *Prior Failure*.

With *Execute If*, you can control which Action Set entries are executed based upon the success or failure of the previous entry.

Unlike Call Route entries, the IEs are **not** restored for each different Action Set Entry. Each change to an IE (in a successful Transformation Table) is carried **throughout the entire Action Set Table**. In this way, the IEs can be normalized over several entries before the call is routed. If you wish to retain a particular value, place it into one of the user-defined IEs (UserValue1-UserValue5).

Configuring an Action Set

Much like the configuration of Call Routes, there are a number of inter-dependecies in configuring Action Sets. The diagram (below) will help guide you through the process.

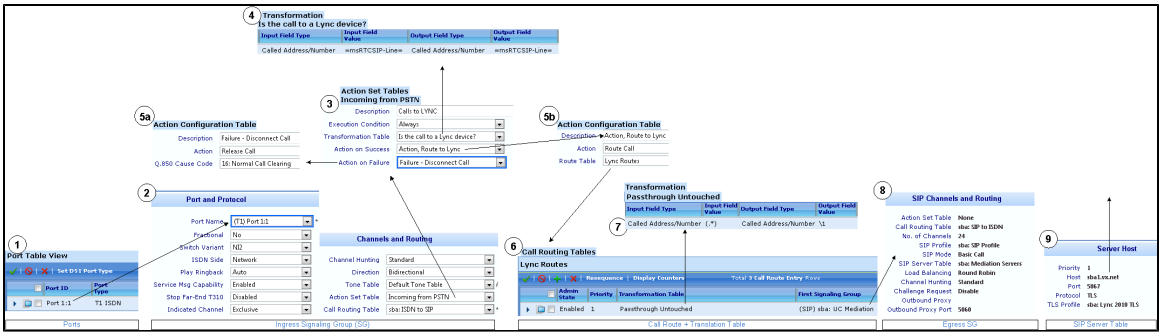


1. Create a Transformation Table to be used by the Action Set
2. Create a Transformation Table to be used by the Call Route.
3. Create a Call Route Table and add any Call Route entries required to complete the calls.
4 and 5. Add any desired Actions in the *Action Configuration* table.
6. Add an Action Set table and populate it with whatever entries are required to complete the desired IE processing.

Copyright © 2015 Sonus Networks. All rights reserved.

How Action Sets Process a Call

Let's put it all together and see what an Action Set call looks like.



1. Call arrives at ingress port
2. Ingress Signaling Group sends the call to the configured Action Set. Note that the Call Routing Table configuration is ignored when an Action Set Table is defined.
3. The first entry in the Action Set Table executes and
4. Processes the associated Transformation Table.
5. If the Tranformation Table fails, the call is disconnected per the *Action on Failure* configuration. If the transformation succeeds, the call is sent to the *Lync Routes* Call Route Table.
6. The *Lync Routes* Call Route Table executes and
7. Processes the associated translation table.
8. Finally, the call is sent to the egress Signaling Group and
9. To the destination SIP Server.

Next Steps

UX AD Integrated Application Solutions using Action Sets details a real-world applcation of Actions Sets to:

- Normalize Numbers
- Blacklisted Numbers
- Find a Calling Name
- Send calls to Exchange for voicemail retreival
- Calls to Fax Numbers
- Permit voicemail for analog Lync devices
- Send calls to Lync Users
- Use the PBX as the route of last resort

This application employs the Action Set's full capabilities. Reviewing this document should help solidfy your understanding of Action Sets and put you on the path to creating your own.

rev 0.2

SBC AD Integrated Application Solutions using Action Sets

Copyright © 2015 Sonus Networks. All rights reserved.

Table of Contents

- Prerequistes
- Summary
- Overview of the Applications
  - More Information

About this Page

This page describes how to employ SBC's Action Sets to create AD-integrated call applications for LYNC, LYNC analog, Exchange, PBX, and FAX devices. The functionality described below is very similar to VX's AD-integrated scripting.

Related Articles

- Managing Action Configurations
- Managing Action Sets
- Managing Call Routing Tables
- Managing Transformation Tables
- Managing Signaling Groups
- Integrating with Active Directory
- How Action Sets Work

Prerequistes

- Requires AD integration
- Some features require a direct connection (SIP trunk) between the SBC and Exchange
- Assumes the user is familiar with configuring the SBC's WebUI
- Assumes SBC version 2.2 or better
- Assumes that a wizard has been executed
- Assumes that the SIP destinations and signaling groups are already configured

Summary

Action Sets permit a programatic-like ability to manipulate a call before it is processed by the SBC's call router. The programtic capabilities include:

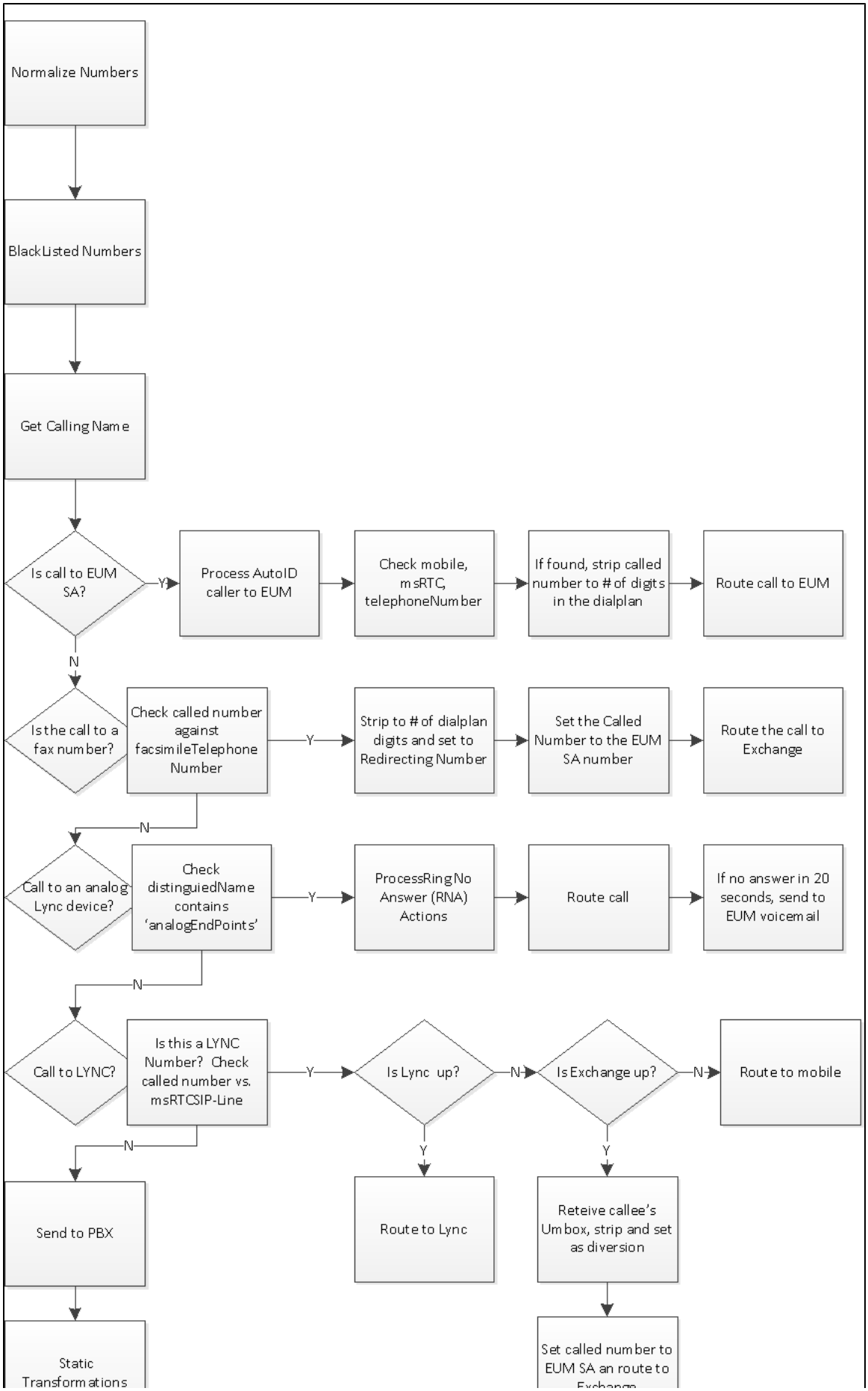
- The ability of control whether an entry is executed based upon the failure or success of a previous entry. Unlike the immuatble sequential execution of the entries in the Call Routing Table, Action Set entries can be skipped or executed based upon the failure or success of the previous entries in the table.
- Once an Action Set entry is executed, you can control what happens based upon whether the associated Transformation Table was successful.

Copyright © 2015 Sonus Networks. All rights reserved.

Overview of the Applications

Figure 2: SBC AD-Integrated Call Application Flow chart

Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.



Operational Modules	Description
Normalize Numbers	Normalizes the called and calling numbers. Includes functions to strip digits, as well as to prepend digits. Also assigns the Exchange Subscriber Access (EUM SA) number.
Blacklisted Numbers	Automatically disconnects calls listed in the Blacklisted Numbers tranformation table.
Get Calling Name	Searches AD attribute mobile, msRTCSIP-Line, and telephoneNumber using the calling number and returns the Calling Name, if found.
Calls to the EUM SA to Retrieve Voicemail	Processes calls for retrieving voicemail via the EUM SA. Attempts to automatically identify the caller to Exchange by searching AD attributes mobile, msRTCSIP-Line, and telephoneNumber for the calling number and returning the caller's UMbox number.
Calls to FAX numbers	A two-number fax solution, searches AD attribute facsimileTelephoneNumber for the called number. If found, sets the diversion header to the destination UMbox number. The call is then routed to the EUMS SA.
Voicemail for Lync Analog Devices	Uses the Ring No Answer (RNA) Action Set feature to provide the ability for callers to leave voicemail for Lync analog devices.
Calls to Lync users	Verifies the called number against the AD msRTCSIP-Line attribute and sends the calls to Lync. Backup routes provide rollover to Exchange and mobile (respectively) if Lync is unavailable.
Calls to Lync users with ext=	Verifies the called number;ext= against the AD msRTCSIP-Line attribute and sends the calls to Lync. Backup routes provide rollover to Exchange and mobile (respectively) if Lync is unavailable.
Calls to PBX	The route of last resort, the original called and calling numbers are restored before sending the call to the PBX.

More Information

- How Action Sets Work

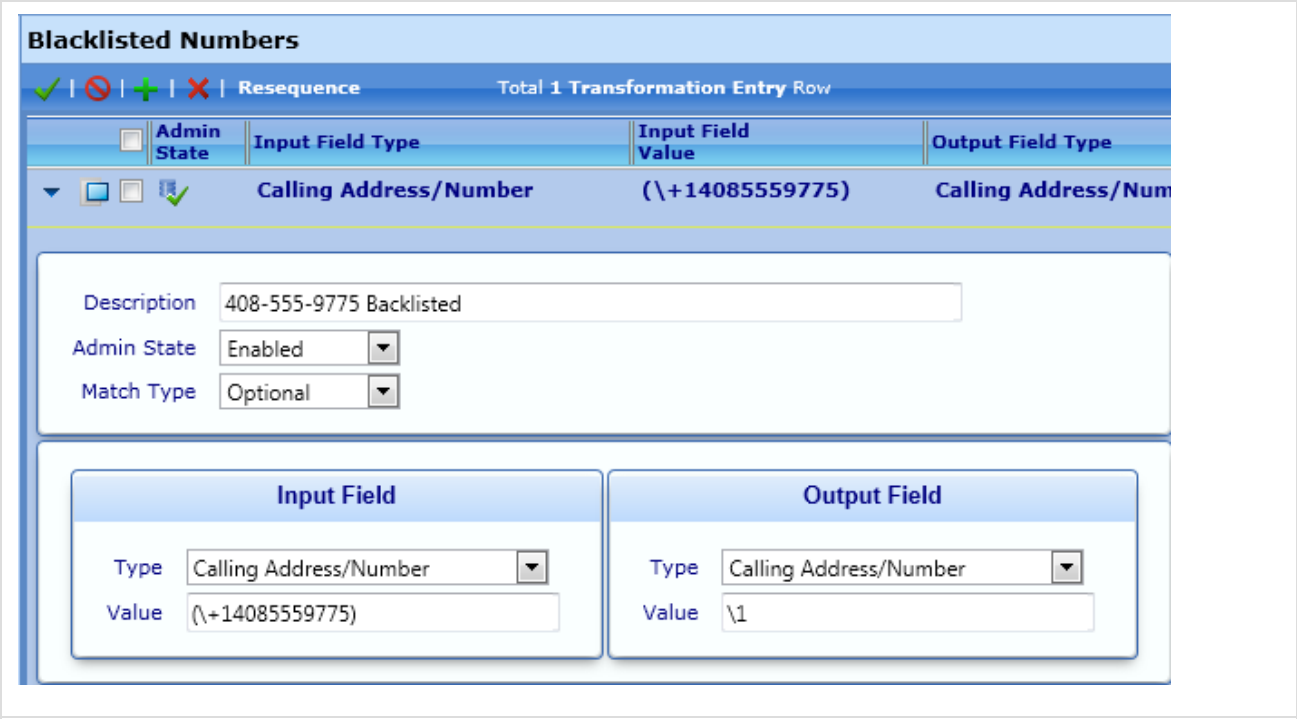
Copyright © 2015 Sonus Networks. All rights reserved.

Blacklisted Numbers

Disconnect Blacklisted Numbers

The Blacklisted Number function disconnects calls for any number that appears in the Blacklist transformation table.

1. Add a Transformation Table.

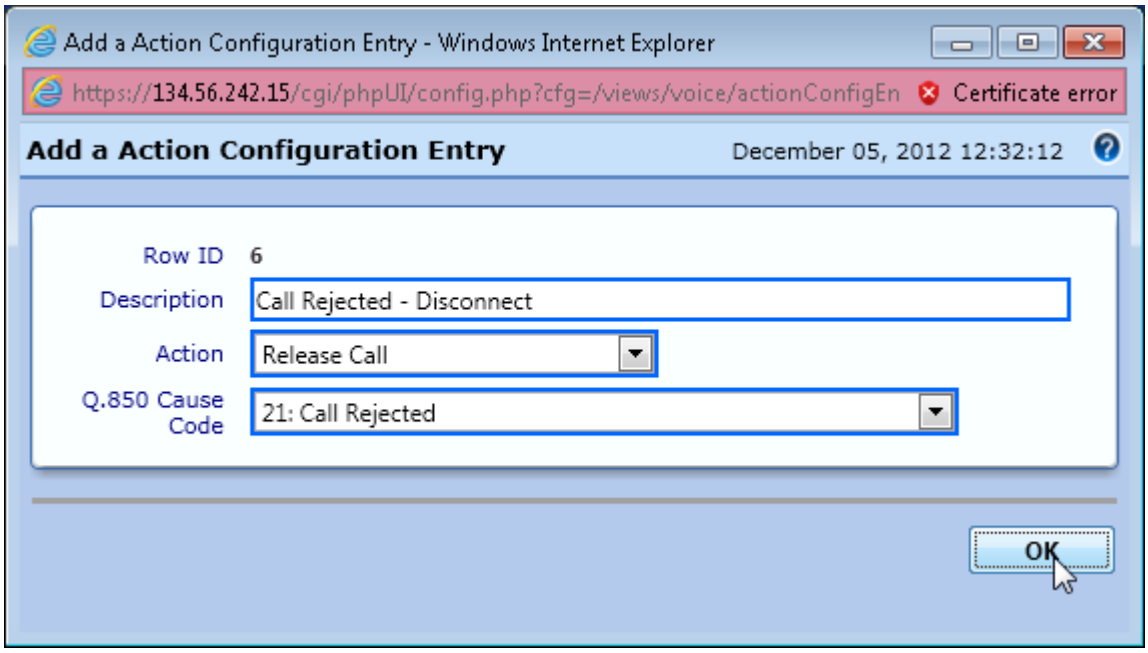


Transformation Table: Blacklisted Numbers

Add a Transformation Table as above. In the example, a call from number 408-555-9775 will be automatically disconnected. You may add any number, or type of number, to the Blacklist Transformation table. The Blacklist is processed following the Number Normalization script, so normalized numbers should be entered into the Blacklist.

2. Create an Action

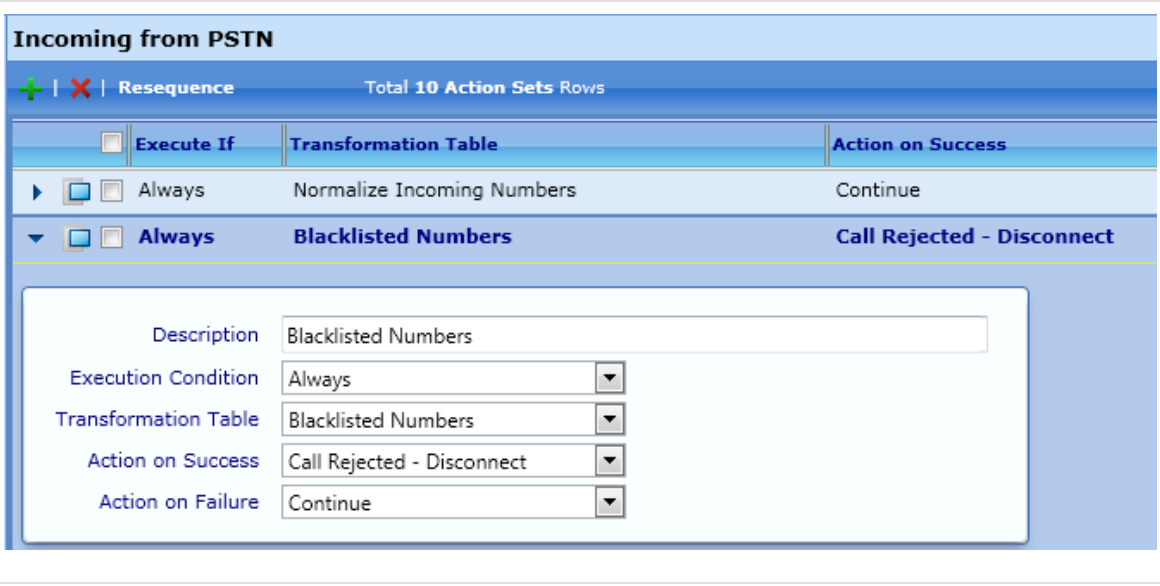
Copyright © 2015 Sonus Networks. All rights reserved.



Reject Call Action Entry

Create an Action to Disconnect Calls that are included in the Blacklist Transformation Table.

3. Create an Entry in the Action Set Table



Calling Name Action Set Entry

Add an entry to the main Action Set using the Calling Name Translation Table you just created.

Important Notes

None.

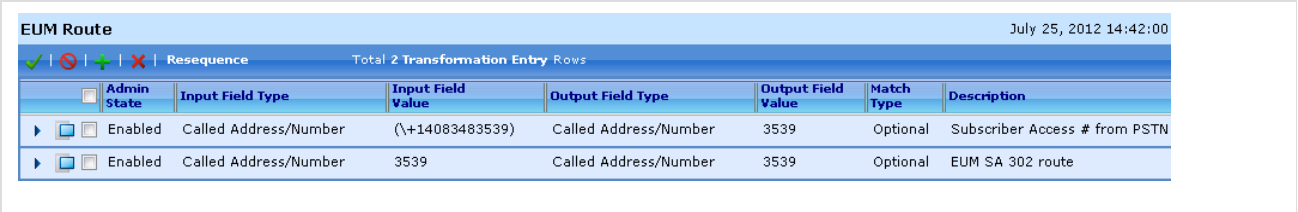
Calls to Exchange Subscriber Access (EUM SA)

Copyright © 2015 Sonus Networks. All rights reserved.

Calls to Exchange Subscriber Access (EUM SA)

This module processes calls to Exchange for voicemail retreival. It verifies the call is to the Exchange SA number.

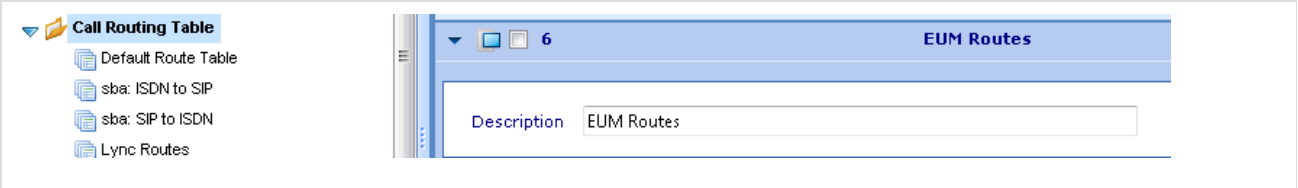
1. Add a EUM SA Transformation Table.



Transformation Table: Is the call to EUM SA?

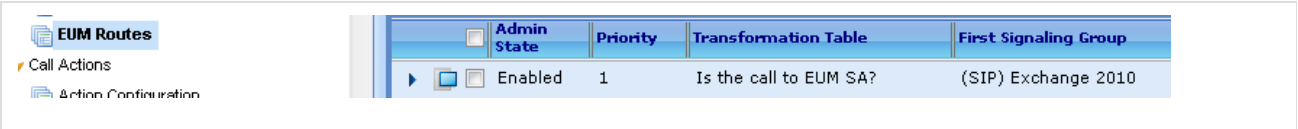
Add any combination of transformations that would be employed to call the Exchange Subscriber's Access number.

2. Create a Route Table for Exchange.



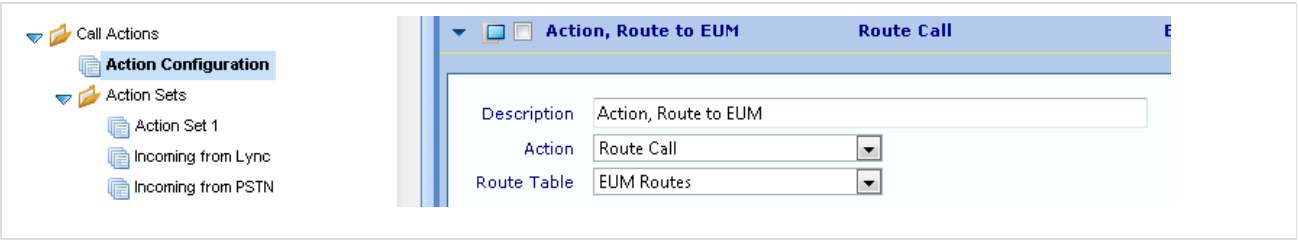
Route Table: EUM Routes

3. Create a Call Route Entry to Exchange.



Call Route Entry to Exchange

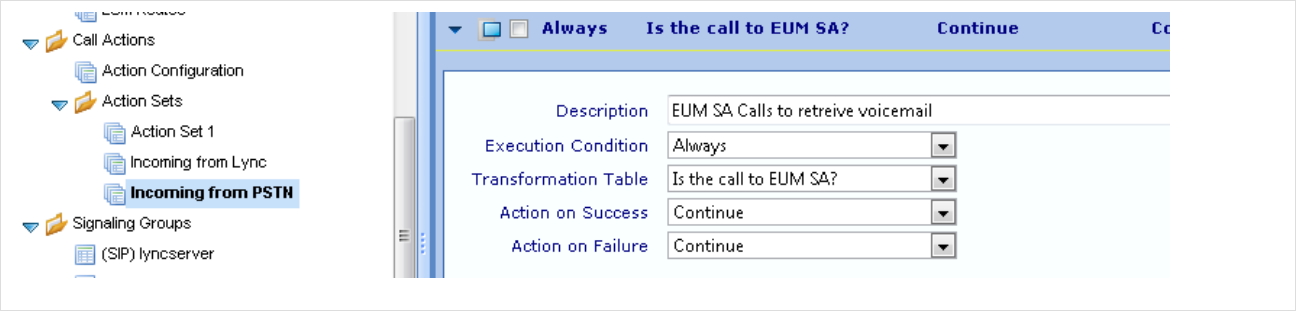
4. Create an Action for Routing to EUM.



Action Configuration: Action, Route to EUM

5. Create an Entry in the Action Set.

Copyright © 2015 Sonus Networks. All rights reserved.

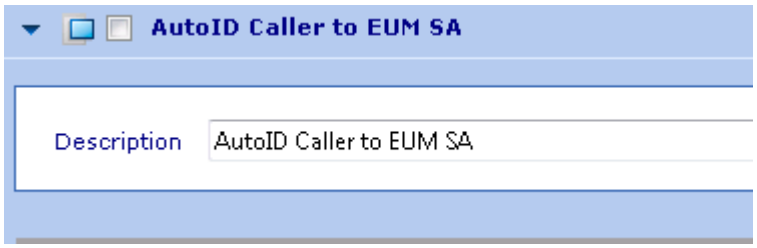


Action Set Entry

AutoID Caller to EUM

This module attempts to change the calling number to the caller's UMbox number (so that the caller is not queried for a UMbox number). The module queries AD for the calling number.

1. Create a Transformation Table.



Transformation Table: AutoID Caller to EUM SA

2. Create the Transformation Table entries.

Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
Calling Address/Number	(.*)	User Value 5	\1	Mandatory	Ensure Table validates as T
Calling Address/Number	==msRTCSIP-Line==	User Value 5	=msRTCSIP-Line=	Optional	Check caller's msRTC to se
Calling Address/Number	==mobile==	User Value 5	=msRTCSIP-Line=	Optional	Check caller's mobile to see
Calling Address/Number	==telephoneNumber==	User Value 5	=msRTCSIP-Line=	Optional	Check caller's telephoneNur
User Value 5	\+.*(\d{4})	Calling Address/Number	\1	Optional	Set Calling UMbox number
User Value 1	(.*)	Called Address/Number	\1	Mandatory	Route to EUM SA

Transformation Table Entries to AutoID caller to EUM

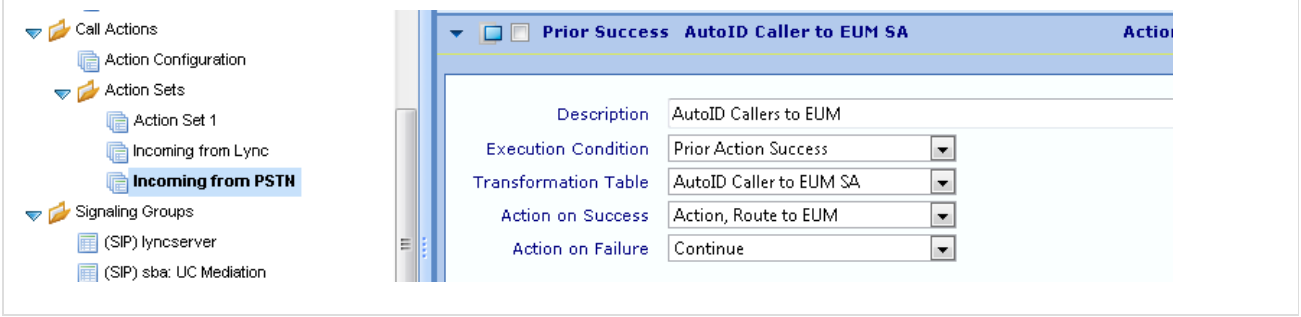
Settings	Descrip
Input Field Type: Calling Address/Number; Input Field Value: (.*); Output Field Type: User Value 5; Output Field Value: \1; Match Type: Mandatory	Store the number i UserValu

Copyright © 2015 Sonus Networks. All rights reserved.

Calling Address/Number	==msRTCSIP-Line==	User Value 5	=msRTCSIP-Line=	Optional	Check UserValu against A msRTCS attribute
Calling Address/Number	==mobile==	User Value 5	=msRTCSIP-Line=	Optional	Check UserValu against A mobile at
Calling Address/Number	==telephoneNumber==	User Value 5	=msRTCSIP-Line=	Optional	Check UserValu against A telephon attribute
User Value 5	\+.*(\d{4})	Calling Address/Number	\1	Optional	Trim the in UserV the numb digits in t dialplan (4)
User Value 1	(.*)	Called Address/Number	\1	Mandatory	Copy the Exchang number i UserValu the Callir Number

If you change the value of an IE in a successful Transformation Table, that value will persist for remainder of the Action Set. Unlike a Call Route, the initial values of the IEs will not be restored when the next Action Set Entry is processed.

3. Create Action Set Entry



Action Set Entry: EUM AutoID Caller to Exchange

Copyright © 2015 Sonus Networks. All rights reserved.

Important Notes

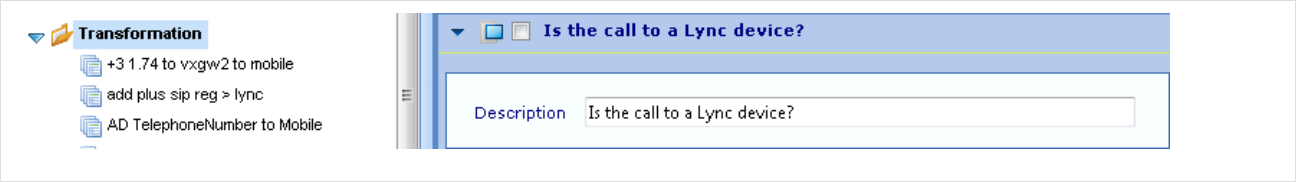
> Beginning in UX Version 2.2, a new double-equal AD lookup function is supported (e.g. ==msRTCSIP-Line==). A new request to the AD server is made for each double-equal AD lookup contain in a Transformation Table. Avoid using this functionality liberally. Requests to the AD server are time-consuming. A heavy load of AD queries will negatively impact call processing time. You should only use this function if, within a Translation Table, you need to perform an AD lookup of two or more user's AD records.

Calls to Lync Users

Calls to Lync Users

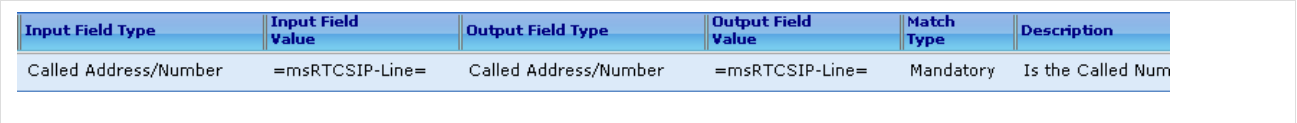
This module routes calls to Lync users. It checks the called number against the msRTCSIP-Line AD attribute to determine if the callee has a Lync number.

1. Create the Lync Transformation Table.



Tranformation Table: Is the Call to a Lync Device?

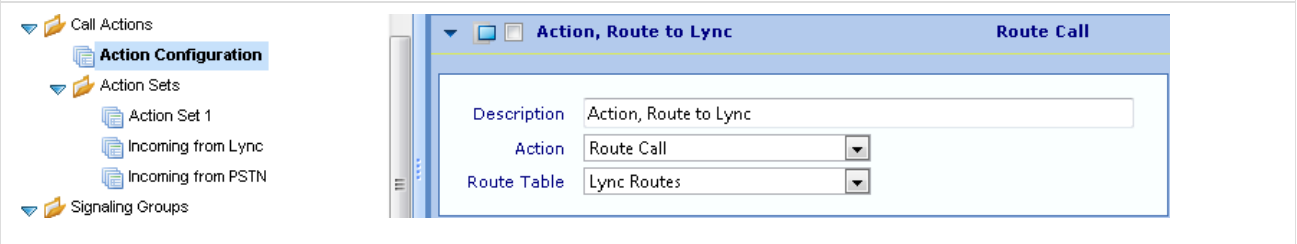
2. Create the Lync Transformation Table entry.
   This entry performs the AD lookup.



Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
Called Address/Number	=msRTCSIP-Line=	Called Address/Number	=msRTCSIP-Line=	Mandatory	Is the Called Num

Tranformation Confirms Lync User

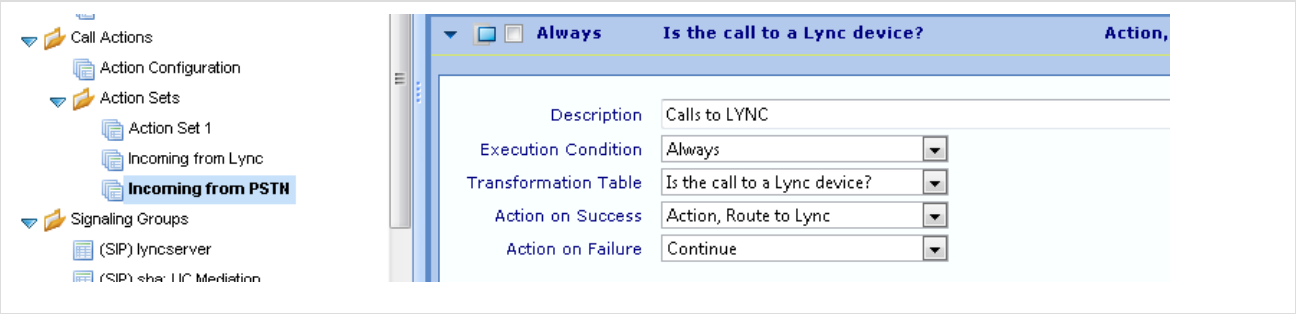
3. Create a Lync Action in the Action Configuration menu.



Action Configuration: Action, Route to Lync

4. Add an entry to the main Action Set.

Copyright © 2015 Sonus Networks. All rights reserved.



Add the Action Set Entry: Calls to Lync

Failover Functionality

From the Lync Route Table, it is possible to add additional Call Route Entries to provide additional call processing should Lync be down.

Failover to Exchange

To add failover functionality to Exchange, use the following:

- Add an entry to the Lync Routing Table that points to Exchange.

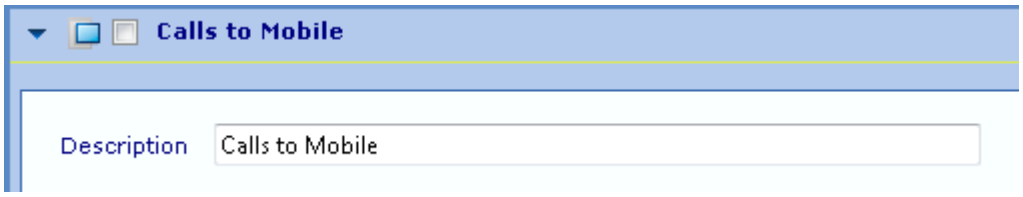
Enabled	1	EUM Leave voicemail, get callee's umbox number	(SIP) Exchange 2010

Lync Route Table Entry That Failsover to Exchange

Failover to Mobile

Add an entry to the Lync Routing Table that points to the callee's mobile phone.

1. Add a Transformation Table to call the mobile.



Tranformation Table: Calls to Mobile

2. Add the Transformation Table entries.

Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value
Enabled	Called Address/Number	=msRTCSIP-Line=	Called Address/Number	=mobile=

Find the Callee's Mobile Number

3. Add an entry to the Lync Call Route Table.

Copyright © 2015 Sonus Networks. All rights reserved.

Enabled	1	Calls to Mobile	(ISDN) ISDN

Call Route Entry Sends Call to Mobile

Summary

Your Lync Call Route Table should now have a route entry to send the call to the Lync server. If the Lync server is down, the call will be re-routed to Exchange to leave voicemail. If Exchange is offline, the calls will be forwarded to the callee's mobile number.

Admin State	Priority	Transformation Table	First Signaling Group
Enabled	1	Passthrough Untouched	(SIP) sba: UC Mediation
Enabled	1	EUM Leave voicemail, get callee's umbox number	(SIP) Exchange 2010
Enabled	1	Calls to Mobile	(ISDN) ISDN to 242.6 vxgw

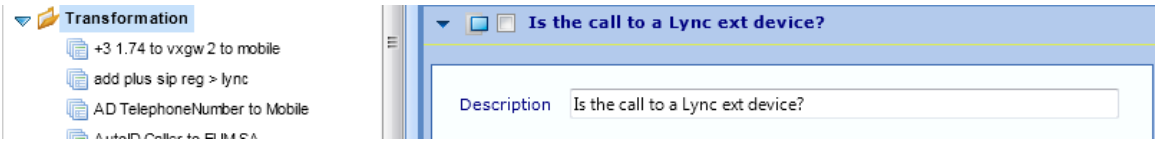
rev 0.1

Calls to Lync users with ext=

Calls to Lync Users

This module routes calls to Lync users. It checks the called number against the msRTCSIP-Line AD attribute to determine if the callee has a Lync number.

1. Create the Lync Transformation Table



Tranformation Table: Is the Call to a Lync Device?

2. Create the Lync Transformation Table entry.

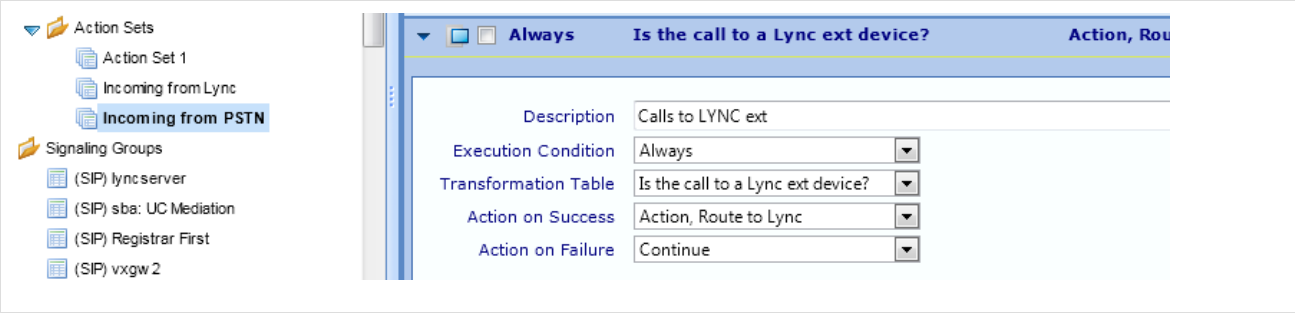
   These entries build a called number+ext, then queries AD.

Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	De
Called Address/Number	^(.*)(\d{4})$	Called Extension	\1\2;ext=\2	Mandatory	te
Called Extension	=msRTCSIP-Line=	Called Address/Number	=msRTCSIP-Line=	Mandatory	ch
Called Extension	(.*)	Called Extension		Mandatory	Cl

Tranformation Confirms Lync User

Copyright © 2015 Sonus Networks. All rights reserved.

3. Add an entry to the main Action Set.



Add the Action Set Entry: Calls to Lync

Calls to PBX

Calls to PBX, the Route of Last Resort

The last module routes call to the PBX as a last resort.

1. Create a PBX Transformation Table



Transformation Table: Restore Original Calling Number

2. Create the PBX Transformation Table Entry.
Notice that *UserValue2* is employed to restore the original calling number to the Calling Number IE.

Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
User Value 2	(.*)	Called Address/Number	\1	Mandatory	Last Resort calls to PBX using originally

Restore Calling Number Before Sending to the PBX

3. Create a PBX Route Table.



Route Table: PBX Routes

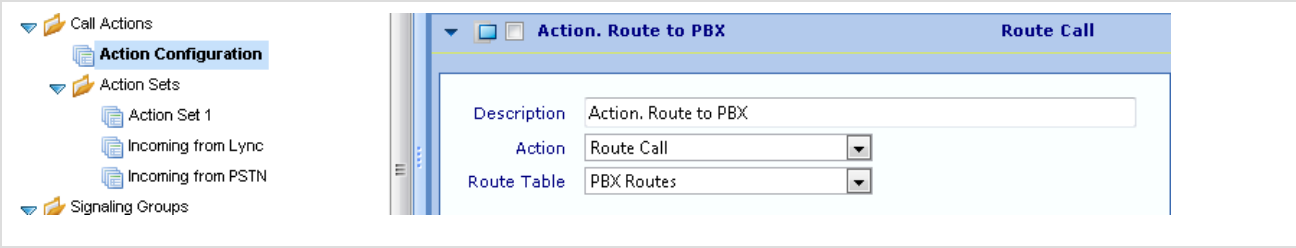
4. Create a PBX Route Table entry that points to the PBX.

Admin State	Priority	Transformation Table	First Signaling Group
Enabled	1	Static Routings	(SIP) sba: UC Mediation
Enabled	1	Passthrough Untouched	(SIP) 10.1.1.91 SG

Copyright © 2015 Sonus Networks. All rights reserved.

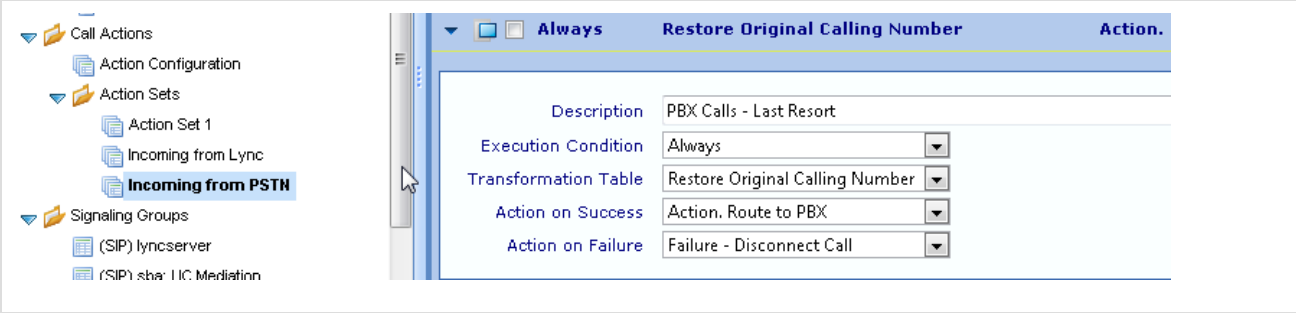
Translations for Any Static or PBX Translations

5. Create an Action that sends calls to the PBX Route Table.



Action: _Route to PBX

6. Add an entry to the main Action Set.



Action Set Entry: PBX Calls - Last Resort

Summary

Configuration complete, your main Action Set should look like the following figure.



Execute If	Transformation Table	Action on Success	Action on Failure	Description
Always	Normalize Incoming Numbers	Continue	Failure - Disconnect Call	Normalize Incoming Numbers
Always	Get Calling Name	Continue	Continue	Get Calling Name
Always	Is the call to EUM SA?	Continue	Continue	EUM SA Calls to retreive voicem
Prior Success	AutoID Caller to EUM SA	Action, Route to EUM	Continue	AutoID Callers to EUM
Prior Failure	Is it a FAX number?	Action, Route to EUM	Continue	Calls to FAX numbers (not one
Always	Is the call to a LYNC Analog device?	Action, RNA Timer, Route to Lync	Continue	Voicemail for Lync Analog Devic
Prior Timeout	EUM Leave voicemail, get callee's umbox number	Action, Route to EUM	Failure - Disconnect Call	Lync analog RNA to voicemail
Always	Is the call to a Lync device?	Action, Route to Lync	Continue	Calls to LYNC
Always	Is the call to a Lync ext device?	Action, Route to Lync	Continue	Calls to LYNC ext
Always	Restore Original Calling Number	Action. Route to PBX	Failure - Disconnect Call	PBX Calls - Last Resort

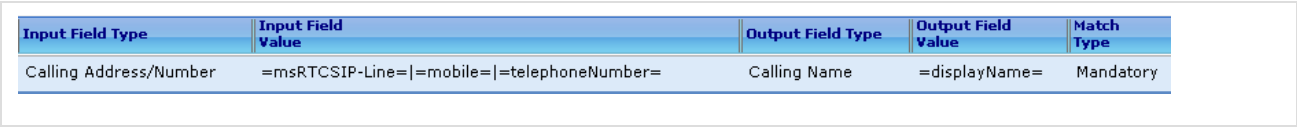
Get Calling Name

Get Calling Name

The Get Calling Name function attempts to retreive a name for the caller. The calling number is searched using the AD attributes of msRTCSIP-Line, mobile, and telephoneNumber. Of course, you may modify this search to suit your requirements.

Copyright © 2015 Sonus Networks. All rights reserved.

1. Add a Transformation Table.

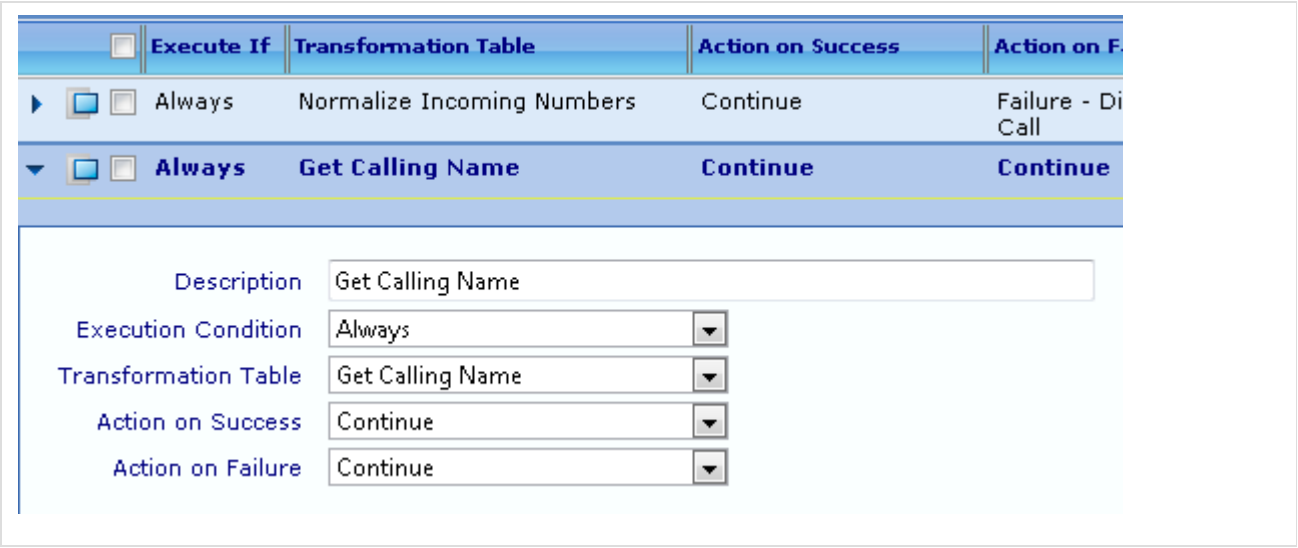


Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type
Calling Address/Number	=msRTCSIP-Line=|=mobile=|=telephoneNumber=	Calling Name	=displayName=	Mandatory

Transformation Table: Get Calling Name

Add a Transformation Table as above. In the example, AD attributes *mobile*, *msRTCSIP-Line*, and *telephoneNumber* are searched using the calling number. If a match is found, the displayName is retrieved and stored in the Calling Name IE.

2. Create an Entry in the Action Set Table.



Calling Name Action Set Entry

Add an entry to the main Action Set using the Calling Name Translation Table you just created.

Important Notes

There are several methods which can be utilized to perform this AD search:

- A simple lookup (=msRTCSIP-Line=) will work well if you want to search a single AD attribute.
- A complex lookup using regex, like the lookup in Step 1, can search multiple entries simultaneously.
- Beginning in UX Version 2.2, a new double-equal AD lookup function is supported (e.g. ==msRTCSIP-Line==). A new request to the AD server is made for each double-equal AD lookup contain in a Transformation Table.

Copyright © 2015 Sonus Networks. All rights reserved.

For single-equal AD Lookups: Remember that the first valid AD lookup in a Translation Table returns all the AD attributes for that user. Any subsequent AD lookup within that same Translation Table will internally query the attributes returned in the first lookup--it will not make another request to the AD itself.

For double-equal AD Lookups: Avoid using this functionality liberally. Requests to the AD server are time-consuming. A heavy load of AD queries will negatively impact call processing time. You should only use this function if, within a Translation Table, you need to perform an AD lookup of two or more user's AD records.

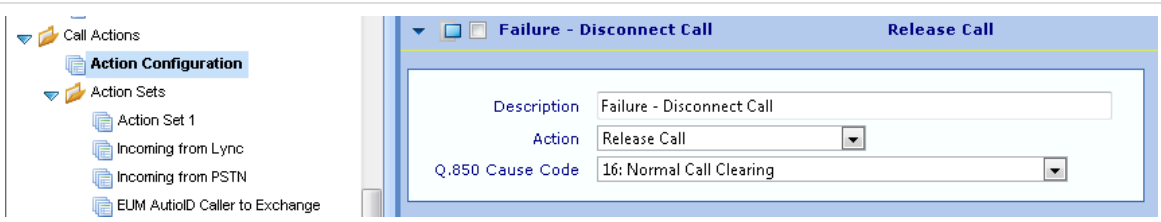
Normalizing Numbers

Normalizing Numbers

The first phase of the process is to normalize the incoming numbers and set the Exchange Subscriber's Access (EUM SA) phone number.

1. Create an Action for releasing calls using the Action Configuration menu.

   This is used for calls that have completed processing, but are still not routed.



Action Configuration: Failure - Disconnect Call

2. Create a Transformation Table for normalizing numbers.

Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
Enabled	Called Address/Number	(.*)	User Value 2	\1	Mandatory	Store Original Called Number
Enabled	Calling Address/Number	(.*)	User Value 3	\1	Mandatory	Store Original Calling Number
Enabled	Called Address/Number	^\d{1}(.*)$	Called Address/Number	\1	Mandatory	Strip X digits from Called Number (default 0)
Enabled	Calling Address/Number	^\d{0}(.*)$	Calling Address/Number	\1	Mandatory	Strip X digits from Calling Number (default 0)
Enabled	Called Address/Number	(.*)	Called Address/Number	+1\1	Mandatory	Normalize Called Number - DNIS
Enabled	Calling Address/Number	(.*)	Calling Address/Number	+1\1	Mandatory	Normalize Calling Number - ANI
Enabled	User Value 1	(.*)	User Value 1	+14083483539	Mandatory	EUM Subscriber Access #
Enabled	Calling Address/Number	(.*)	User Value 4	\1	Mandatory	Save Normalized Calling Number

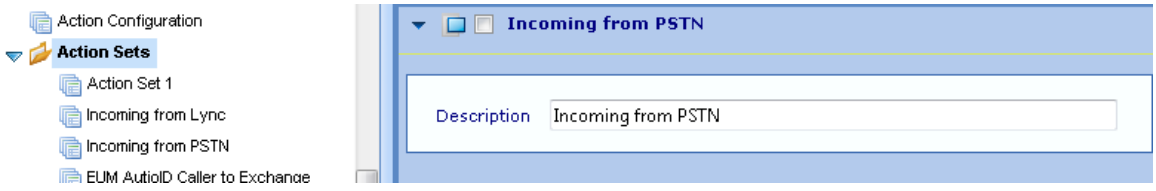
Transformation Table: _Normalize Incoming Numbers

Settings	Description
Input Field Type: Called Address/Number; Input Field Value: (.*); Output Field Type: User Value 2; Output Field Value: \1; Match Type: Mandatory	Saves the originally called number in the User Value #2 IE
Calling Address/Number (.*) User Value 3 \1 Mandatory	Saves the original calling number in the User Value #3 IE

Copyright © 2015 Sonus Networks. All rights reserved.

Called Address/Number	^\d{1}(.*)$	Called Address/Number	\1	Mandatory	Strips the number of digits noted in d{x} from the beginning of the called number. In the example, d{1} digits, or one digit, is stripped from the incoming called number. If the original called number was 15105551212, the output of this translation would be 5105551212.
Calling Address/Number	^\d{0}(.*)$	Calling Address/Number	\1	Mandatory	Strips the number of digits noted in d{x} from the beginning of the calling number. In the example, d{0} digits, or zero digits, are stripped from the incoming calling number. If the original calling number was 15105551212, the output of this translation would be 15105551212.
Called Address/Number	(.*)	Called Address/Number	+1\1	Mandatory	Prepends the digits in the Output Field to the called number. In the example, if the called number was 5105551212, +1 is added to the called number rendering +15105551212.
Calling Address/Number	(.*)	Calling Address/Number	+1\1	Mandatory	Prepends the digits in the Output Field to the calling number. In the example, if the calling number was 5105551212, +1 is added to the calling number rendering +15105551212.
User Value 1	(.*)	User Value 1	+14083483539	Mandatory	Defines the Exchange Subscriber's Access Number. Above, the EUM SA number is configured to +14083483539.
Calling Address/Number	(.*)	User Value 4	\1	Mandatory	Records the normalized calling number into the User Value 4 IE.

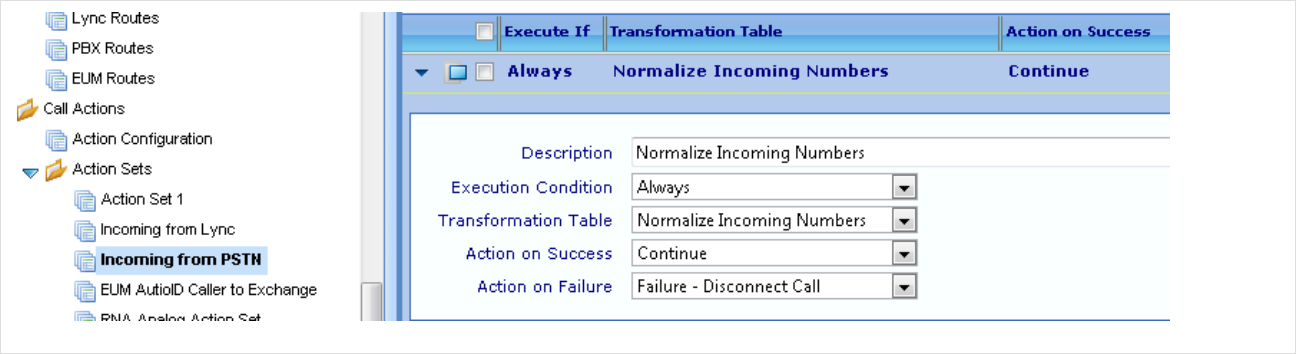
3. Create the main Action Set Table.



Action Set Table: Incoming from PSTN

4. Create an entry in the Action Set Table.

Copyright © 2015 Sonus Networks. All rights reserved.



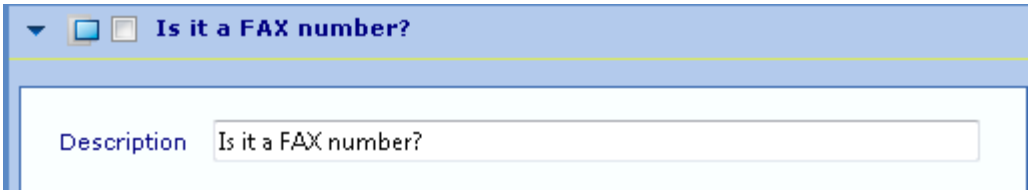
Action Set Entry: Normalize Incoming Numbers

Two-number FAX

Two-Number FAX

This module queries the AD attribute *facsimileTelephoneNumber* for the called number. If a match is found, the callee's UMbox number is retrieved and set as the diversion header. The called number is set to the EUM SA number and the call is forwarded to Exchange.

1. Create a Transformation Table.



Transformation Table: _Is it a FAX number?

2. Create the FAX Transformation entries.

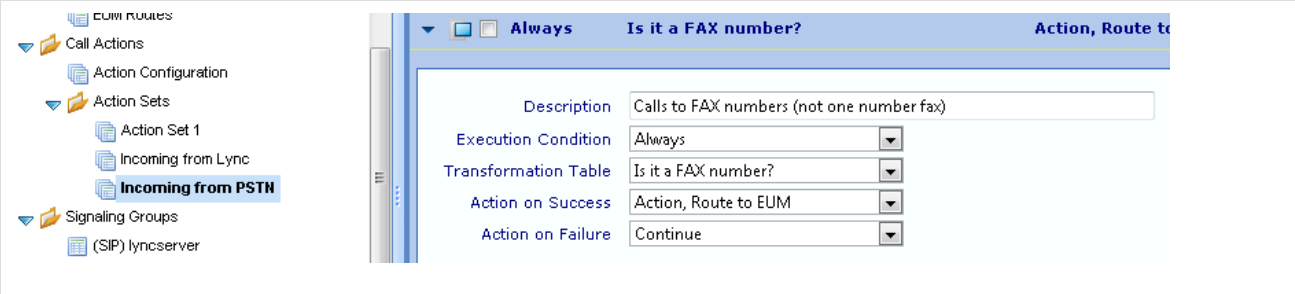
Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
Called Address/Number	=facsimileTelephoneNumber=	Called Address/Number	=msRTCSIP-Line=	Mandatory	FAX calls to UMbox
Called Address/Number	\+.*(\d{4})	Redirecting Number	\1	Mandatory	Strip to UMbox size
User Value 1	(.*)	Called Address/Number	\1	Mandatory	Send call to EUM SA

Fax Transformation Entries}

Settings	Description
Input Field Type: Called Address/Number; Input Field Value: =facsimileTelephoneNumber=; Output Field Type: Called Address/Number; Output Field Value: =msRTCSIP-Line=; Match Type: Mandatory	Search the facsimileTelephoneNumber. If found, return msRTCSIP-Line. Place into the Called Number IE.
Called Address/Number; \+.*(\d{4}); Redirecting Number; \1; Mandatory	Trim the Called Number IE to 4 digits and set it as the Diversion IE.
User Value 1; (.*); Called Address/Number; \1; Mandatory	Set the Called Number IE to the value in the UserValue1 IE (the EUM SA number)

Copyright © 2015 Sonus Networks. All rights reserved.

3. Add the Fax Action Set entry to the Main Action Set.



Fax Action Set Entry

Voicemail for Lync Analog Devices

Calls to Lync analog devices

This module employs the Ring No Answer (RNA) action to send unanswered calls to a Lync analog device to Exchange. In effect, this module supplies the ability to leave voicemail for a Lync analog device.

Is the call to an analog Lync Device?

1. Create a Analog Lync Transformation Table.
   This will be used by the Action Set.

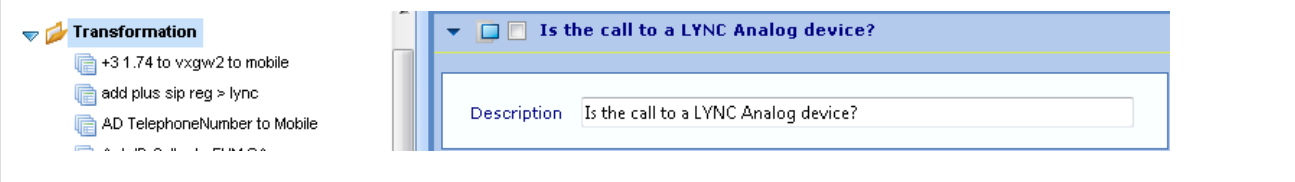


Table: _Is the Call to a Lync Analog Device?

2. Create the Analog Lync Transformation Table entries.

Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Descrip
Called Address/Number	=msRTCSIP-Line=	User Value 5	=distinguishedName=	Mandatory	Is this
User Value 5	^.*analogEndPoints.*$	User Value 5	^.*analogEndPoints.*$	Mandatory	AND A

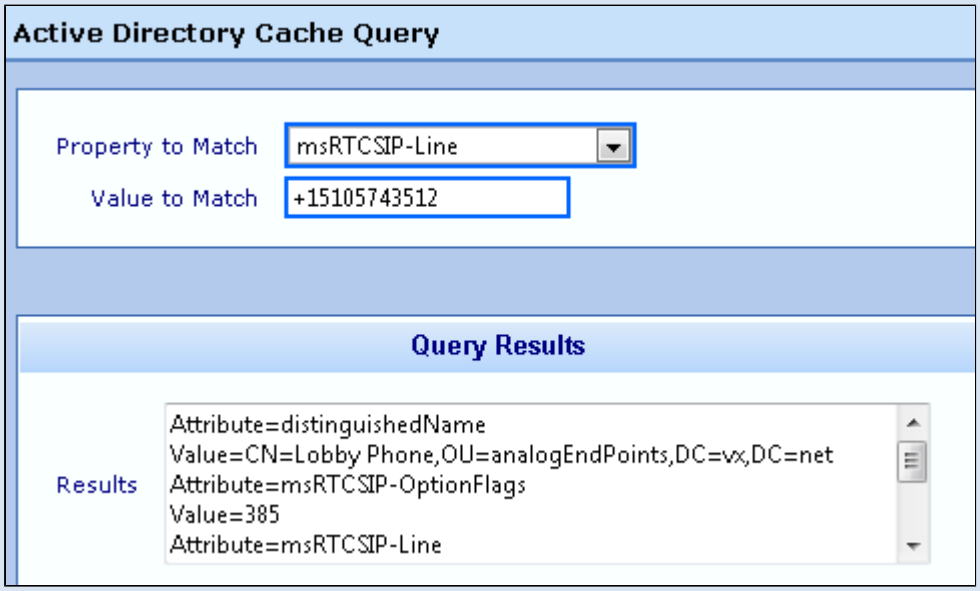
Tranformation Table Identifies Lync Analog Devices

Copyright © 2015 Sonus Networks. All rights reserved.

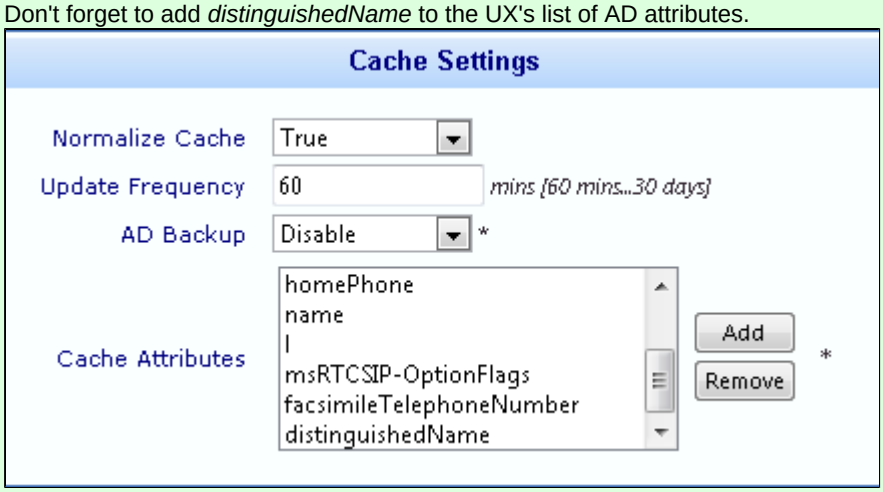
The search in the Transformation Table Entry is the result of the command you entered to enable the analog device, specifically, the OU. Note the corresponding *analogEndPoints* between the Lync command below and the translation entry above.

New-CsAnalogDevice -LineUri tel:+15102462001 -DisplayName "Analogph1" -RegistrarPool cspool.uxdemo.net -AnalogFax $false -Gateway ux246.uxdemo.net -OU "ou=**analogEndPoints**,dc=uxdemo,dc=net"

You can also run a Query Active Directory Cache test from the UX's Task Tab > Diagnostics Section in order to determine the OU name.



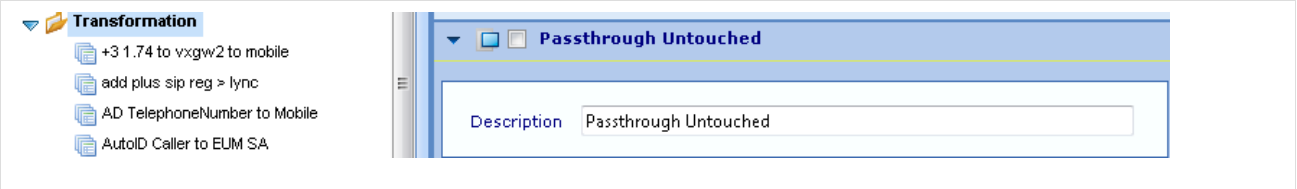
Don't forget to add *distinguishedName* to the UX's list of AD attributes.



Create a Route to Lync

1. Create a Transformation Table for Routing to Lync.
   This will be used by the Call Router.

Copyright © 2015 Sonus Networks. All rights reserved.



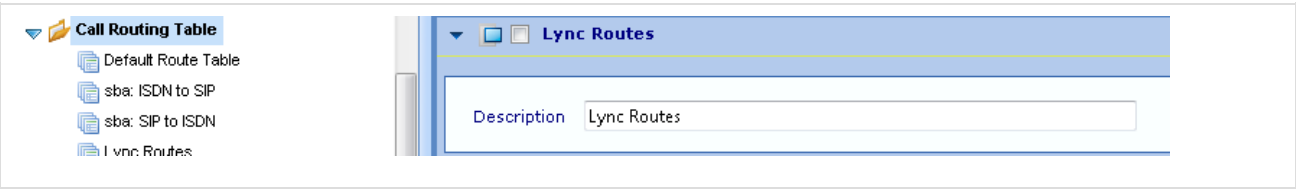
The Preprogrammed Passthrough Untouched Transformation Table

2. Create a Transformation Table Entry to route the call to Lync.
   If all the numbers have been processed and normalized correctly, you should be able to use the *Passthrough Untouched*transformation that is created when the Lync Task (wizard) is run.

Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type
Called Address/Number	(.*)	Called Address/Number	\1	Mandatory

The Passthrough Tranformation

3. Create a Lync Call Routing Table



Call Routing Table: *Lync Routes*

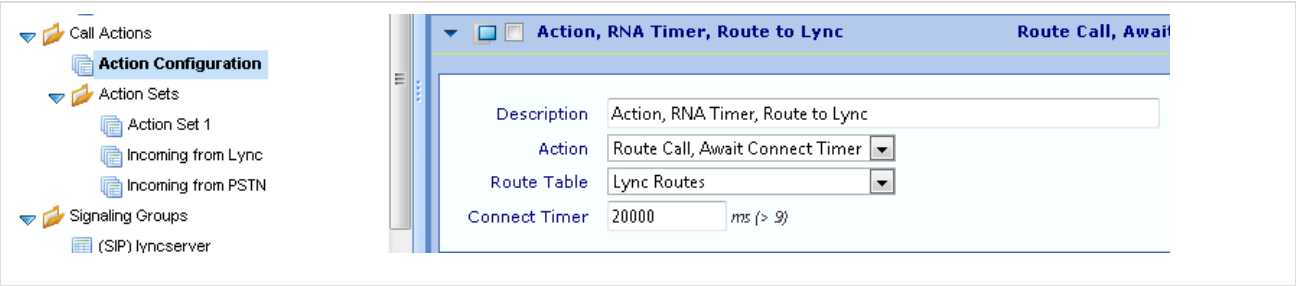
4. Create a Lync Call Routing entry to point the call to the Lync server.

Transformation Table	First Signaling Group	Description
Passthrough Untouched	(SIP) sba: UC Mediation	Passthru to Lync

A Route to the Lync Server

Create the Ring No Answer (RNA) Action Set

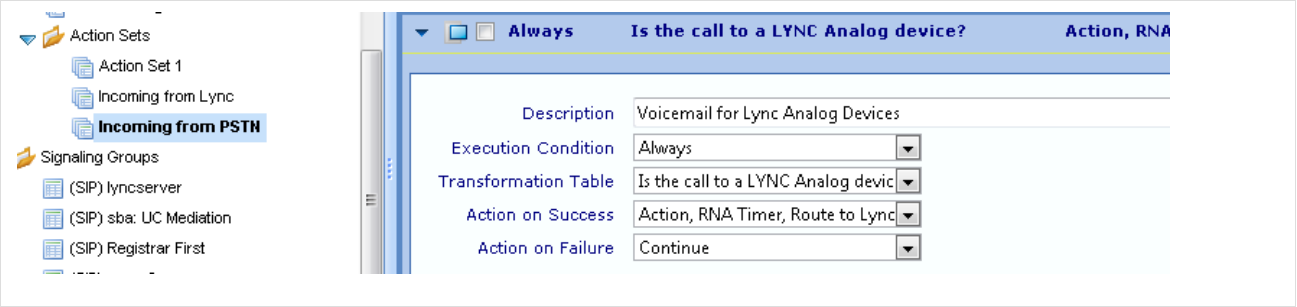
1. Create the Ring No Answer Action in the Action Configuration menu.



Ring No Answer Action

2. Add an entry to the main Action Set.

Copyright © 2015 Sonus Networks. All rights reserved.



Action Set Entry to Route to Lync

Send Unanswered Calls to Exchange

If the prior entry exits with a RNA Timeout, then this entry is executed.

1. Create a Transformation Table route to voicemail transformation.This transformation retreives the callee's UMbox, sets the diversion, and sends the call to Exchange.



EUM Leave Voicemail

2. Create the voicemail Transformation Table Entries as below.

Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
Called Address/Number	==telephoneNumber==	Called Address/Number	=msRTCSIP-Line=	Optional	check telephoneNumbe
Called Address/Number	==mobile==	Called Address/Number	=msRTCSIP-Line=	Optional	check mobile, retrieve
Called Address/Number	==msRTCSIP-Line==	Called Address/Number	=msRTCSIP-Line=	Optional	check msRTC, get umb
Called Address/Number	\+.*(\d{4})	Redirecting Number	\1	Optional	strip called number to t
User Value 1	(.*)	Called Address/Number	\1	Mandatory	Send call to EUM

Transformation Table Creates Diversion to Exchange

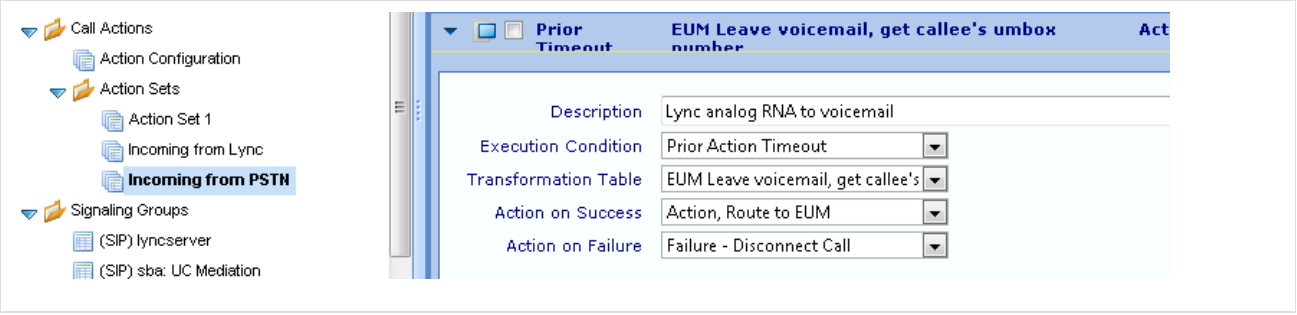
Setting	Description
Input Field Type: Called Address/Number; Input Field Value: ==telephoneNumber==; Output Field Type: Called Address/Number; Output Field Value: =msRTCSIP-Line=; Match Type: Optional	Query the called number against the AD attribute mobile
Called Address/Number ==mobile== Called Address/Number =msRTCSIP-Line= Optional	Query the called number against the AD attribute telephoneNumber
Called Address/Number ==msRTCSIP-Line== Called Address/Number =msRTCSIP-Line= Optional	Query the called number against the AD attribute msRTCSIP-Line
Called Address/Number \+.*(\d{4}) Redirecting Number \1 Optional	Trim the returned value to length of the EUM dialplan digits (default 4), place in the Diversion IE.

Copyright © 2015 Sonus Networks. All rights reserved.

User Value 1	(.*)	Called Address/Number	\1	Mandatory

Set the Called Number IE to the EUM SA number (store in UserValue1)

3. Add an entry to the main Action Set to route unanswered Lync analog calls to Exchange voicemail.



Exchange Action Set Entry

Summary

We are now at the mid-point of configuring the UX AD calling applications. Your Action Set should look like the Action Set below.

Incoming from PSTN

Resequence — Total 9 Action Sets Rows

Execute If	Transformation Table	Action on Success	Action on Failure
Always	Normalize Incoming Numbers	Continue	Failure - Disconnect Call
Always	Get Calling Name	Continue	Continue
Always	Is the call to EUM SA?	Continue	Continue
Prior Success	AutoID Caller to EUM SA	Action, Route to EUM	Continue
Prior Failure	Is it a FAX number?	Action, Route to EUM	Continue
Always	Is the call to a LYNC Analog device?	Action, RNA Timer, Route to Lync	Continue
Prior Timeout	**EUM Leave voicemail, get callee's umbox number**	**Action, Route to EUM**	**Failure - Disconnect Call**

SBC for Dummies Series

- Basic AD-based Call Routing for Dummies
- SBC Basic Call Processing For Dummies - SIP to SIP
- SBC Call Routing Reference for Dummies
- SBC ISDN to SIP Routing For Dummies - TCP
- SBC ISDN To SIP Routing for Dummies - TLS
- SBC Transformation Tables for Dummies

Basic AD-based Call Routing for Dummies

Copyright © 2015 Sonus Networks. All rights reserved.

Table of Contents

- Prerequisites
- Summary
- Before Beginning...
- SBC Active Directory Reference
- SBC AD Configuration
  - Active Directory Integration for Call Routing
  - Active Directory Verification
  - SBC AD-based Call Routing
- Additional Notes

About this Page

- This document details how to configure the SBC for Active Directory-based call routing.
- This document explains how the SBC handles AD caching and repetative AD lookups.

Related Articles

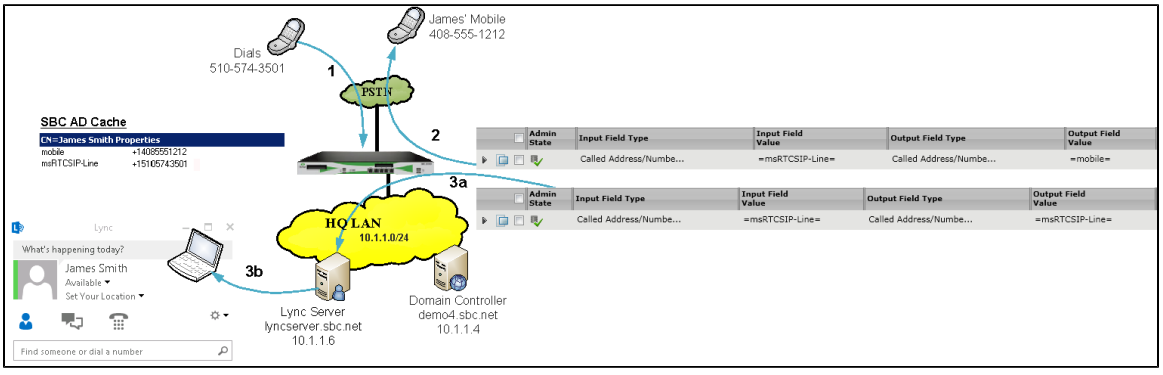
- Configuring Active Directory
- Configuring Domain Controllers
- Querying the Active Directory Cache
- Configuring Call Routing Tables
- Configuring Transformation Tables

Prerequisites

- Requires Sonus SBC1000/2000 Version 2.2 or later
- This document assumes the user has a working knowledge of the SBC and its WebUI.
- This document assumes the user has a working knowledge of Microsoft's Active Directory

Summary

Below is the call diagram example used as a configuration reference for the remainder of this document.



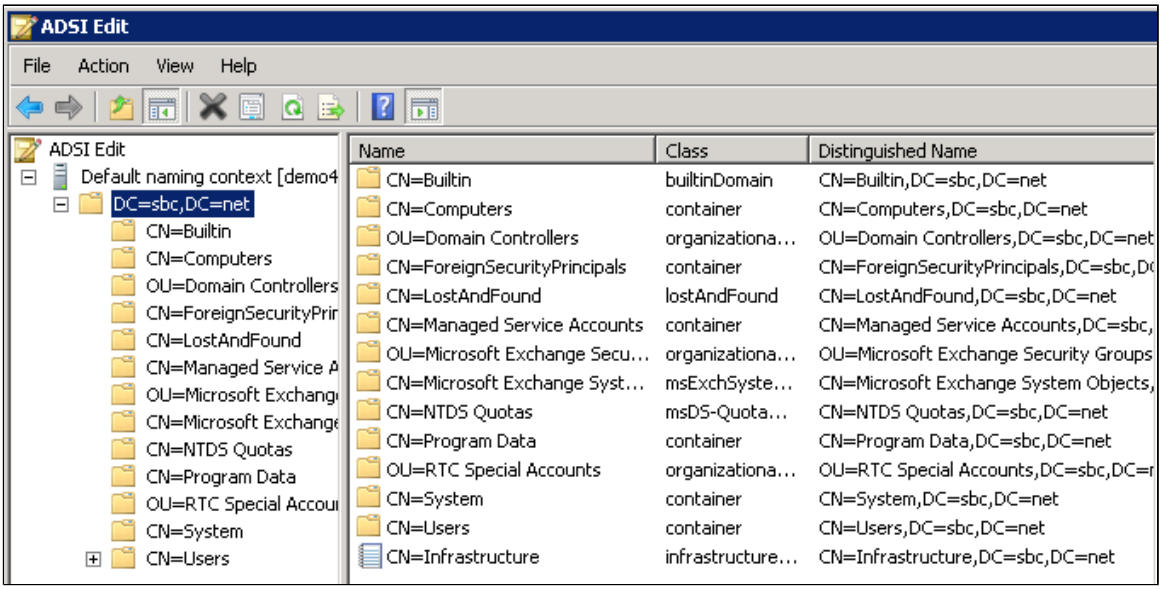
Copyright © 2015 Sonus Networks. All rights reserved.

Step	Action
1	PSTN call arrives at SBC. SBC processes corresponding SG, Call Route & Transformation Table
	Call Route/Transformation Table queries the AD cache. The called number is checked against all msRTCSIP-Line records per the Input portion of the transformation entry.
2	James' msRTCSIP-Line entry matches the called number, +15105743501. James' mobile number is returned from the AD cache. A call is placed to James' mobile, +14085551212.
	All of James' AD records are recorded into a record set. *This record set is used for all subsequent AD queries for this call*.
3a	In forking the call to Lync, the next Call Route entry/Transformation Table is executed. The *record set* (not the AD cache) is searched to see if the called number matches the msRTCSIP-Line. This type of check is performed simply to ascertain if the called number belongs to a Lync user. If it matches, the same number that was searched is returned and the call request is forwarded to the Lync Server.
3b	The Lync Server processes the INVITE, sending it out to James' Lync client

Before Beginning...

Before beginning the AD configuration, investigate and answer the following:

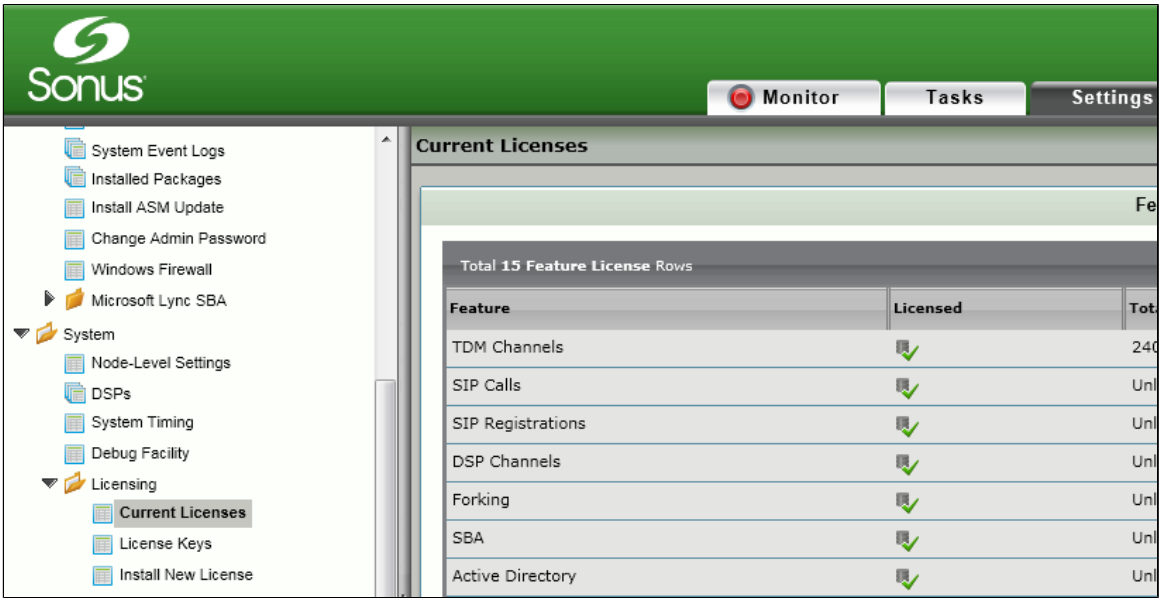
- The FQDN/IP of the Domain Controller
- What AD attribute will be used as key to retrieve records? msRTCSIP-Line, name, or mail are common AD attribute to set as the LDAP search criteria.
- What area of the Active Directory should be searched?



ADSIedit showing a typical location for an AD search

- Does the SBC have a license for Active Directory?

Copyright © 2015 Sonus Networks. All rights reserved.

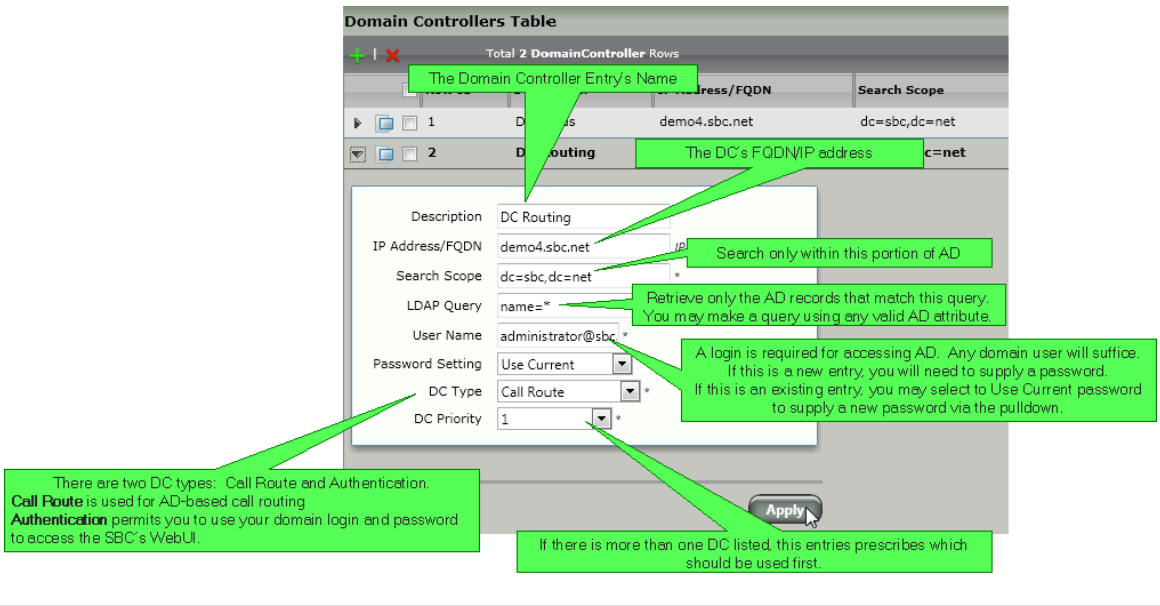


Active Directory is part of the SBC base license. The latest base licenses are available at Sonus Download Center.

SBC Active Directory Reference

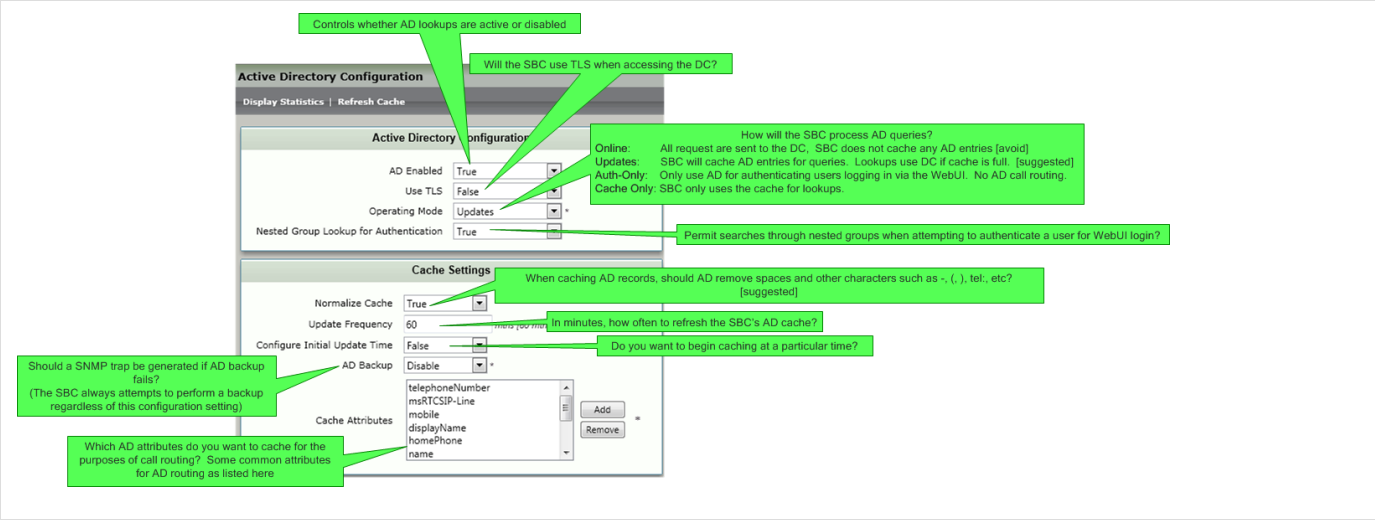
The following diagrams depict the SBC's Active Directory settings for:

- Configuring a *Domain Controller*
- Setting the *Configuration* parameters the SBC will use to interoperate with the domain controller



Configuration for Individual Domain Controllers

Copyright © 2015 Sonus Networks. All rights reserved.



Global Configuration for SBC-to-DC Interactions

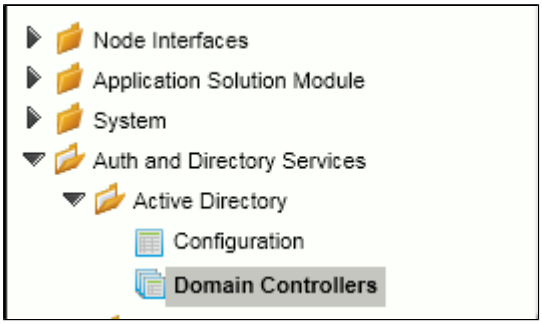
SBC AD Configuration

The SBC must be configured for:

- Active Directory Integration
- Forked Calling
- AD-based Call Routing

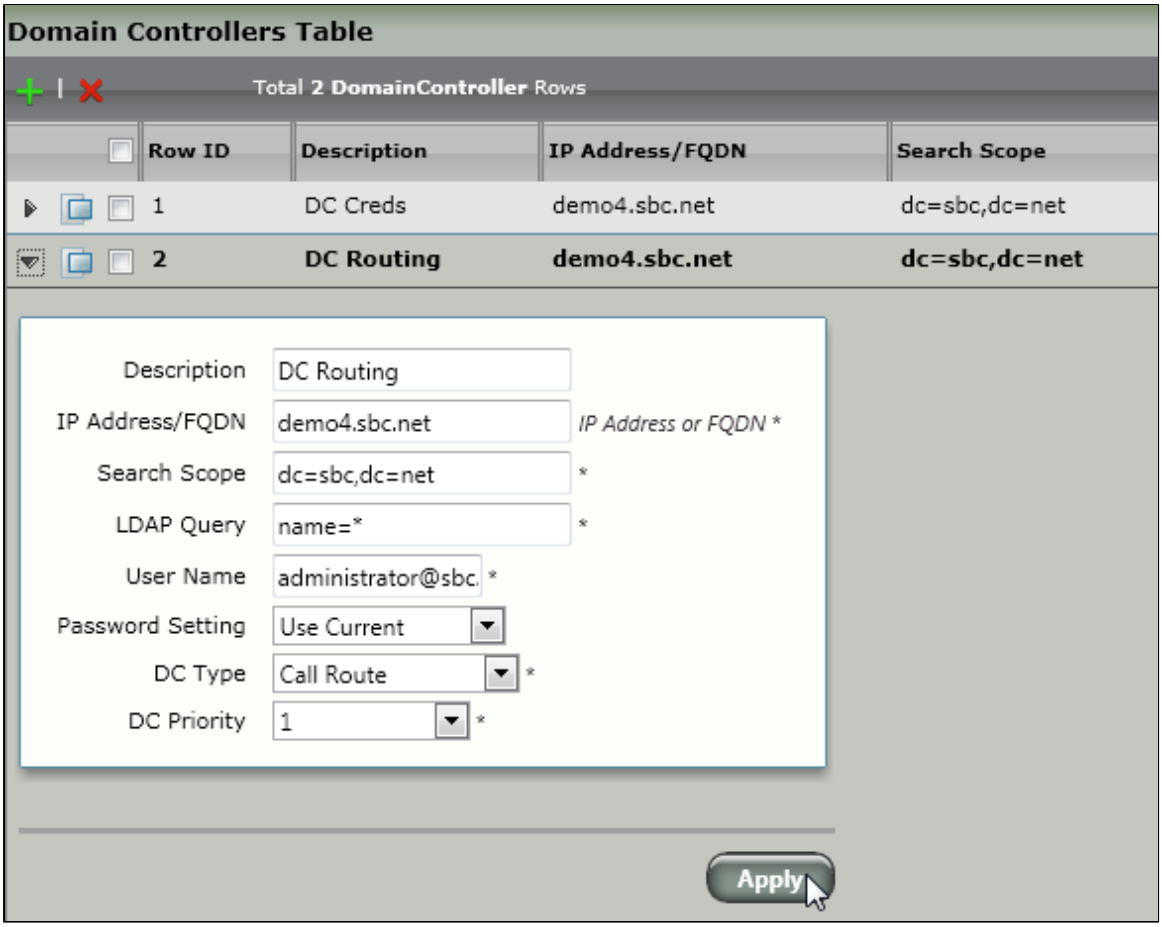
Active Directory Integration for Call Routing

1. Click the *Settings* tab in the top nagivation, then select *Domain Controllers*in the left-hand navigation

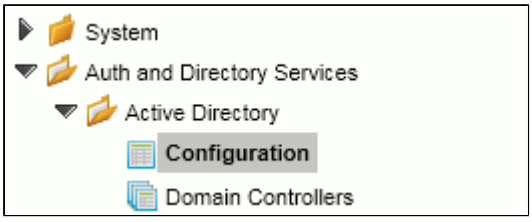


2. Enter the AD information for your network

Copyright © 2015 Sonus Networks. All rights reserved.



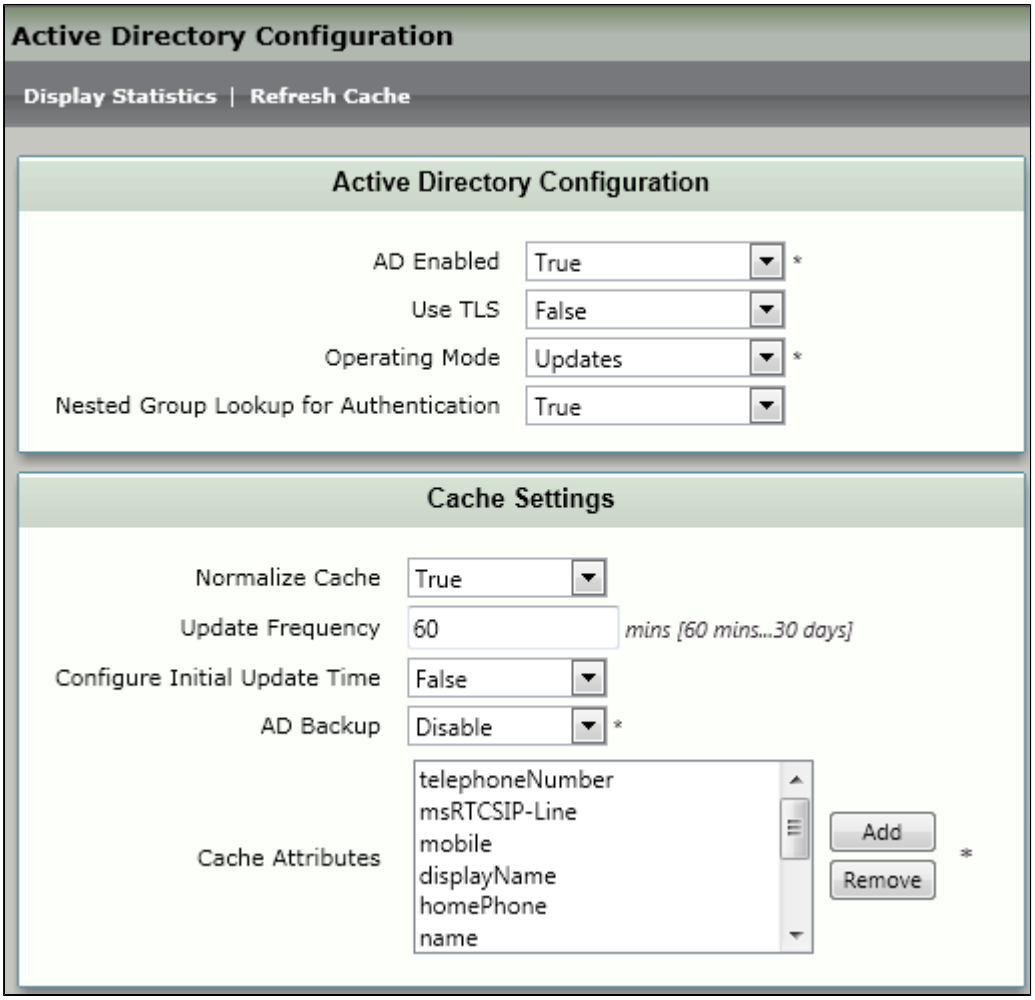
3. Click *Configuration*in the left-hand navigation.



4. Configure the *Active Directory Configuration* as shown. Add whatever *Cache Attributes*you plan to use.

> The minimum configuration for this example document should include the attributes: msRTCSIP-Line, name, displayName, mail, telephoneNumber

Copyright © 2015 Sonus Networks. All rights reserved.



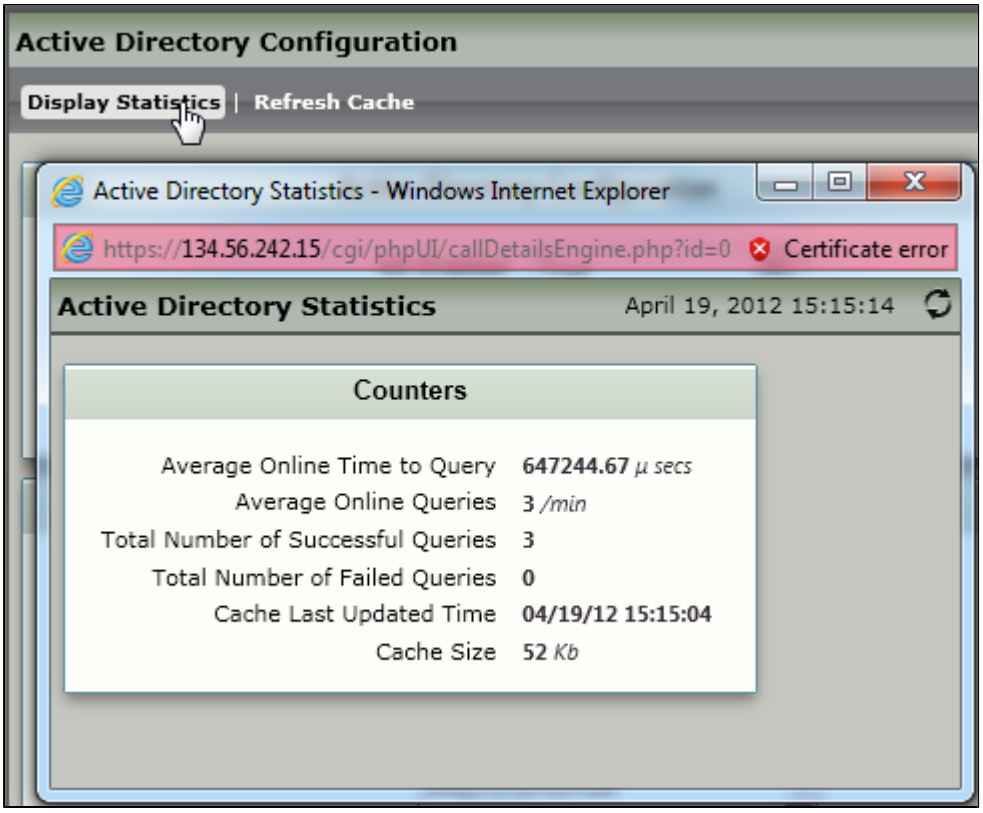
Active Directory Verification

1. With the AD configuration completed, click *Refresh Cache*.

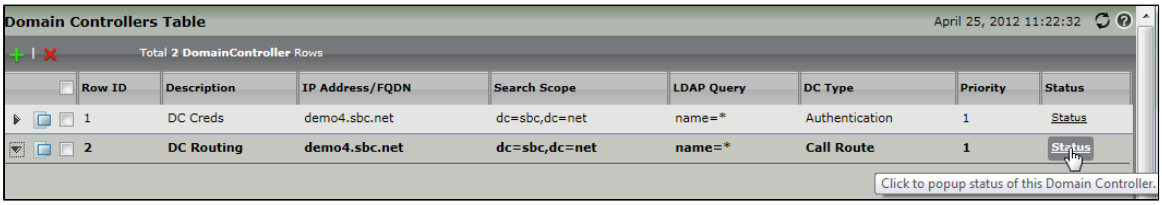


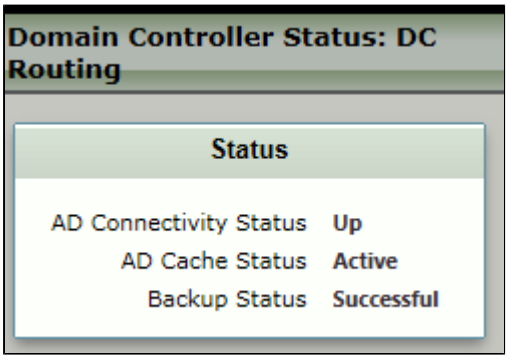
2. Click *Display Statistics*and verify that the AD queries are succeeding.

Copyright © 2015 Sonus Networks. All rights reserved.



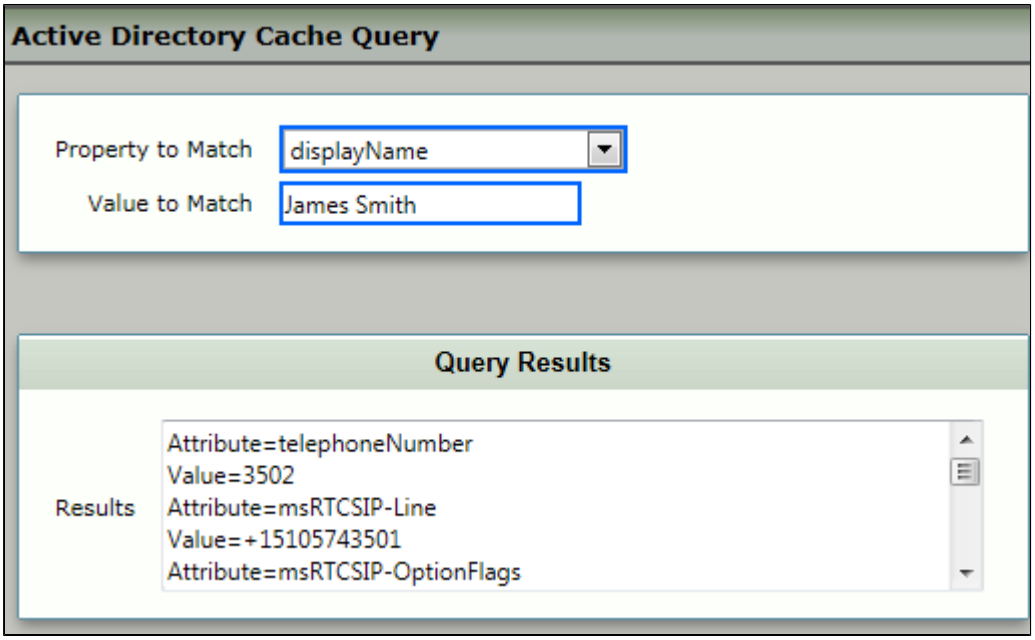
3. In the Domain Controller configuration, check the DC Status





4. Select the *Tasks* tab in the top navigation and click *Active Directory Cache Query*. In the form, pick an AD attribute from the pulldown and supply a corresponding value.

Copyright © 2015 Sonus Networks. All rights reserved.

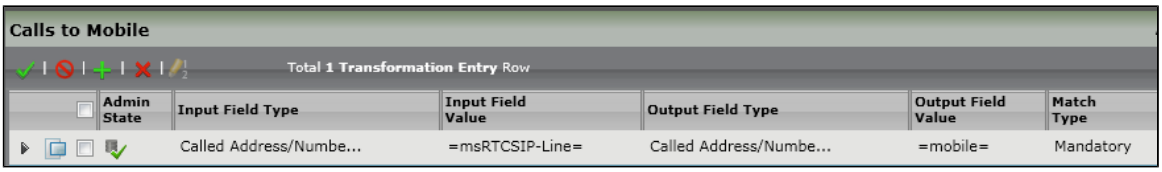


> Queries of the msRTCSIP-Line must match precisely what appears in the Lync *Line URI* for the desired user, unless *Normalized Cache* is configured to *True*. If the cache is normalized, the tel: will be removed from the Lync *User Line URI*.

SBC AD-based Call Routing

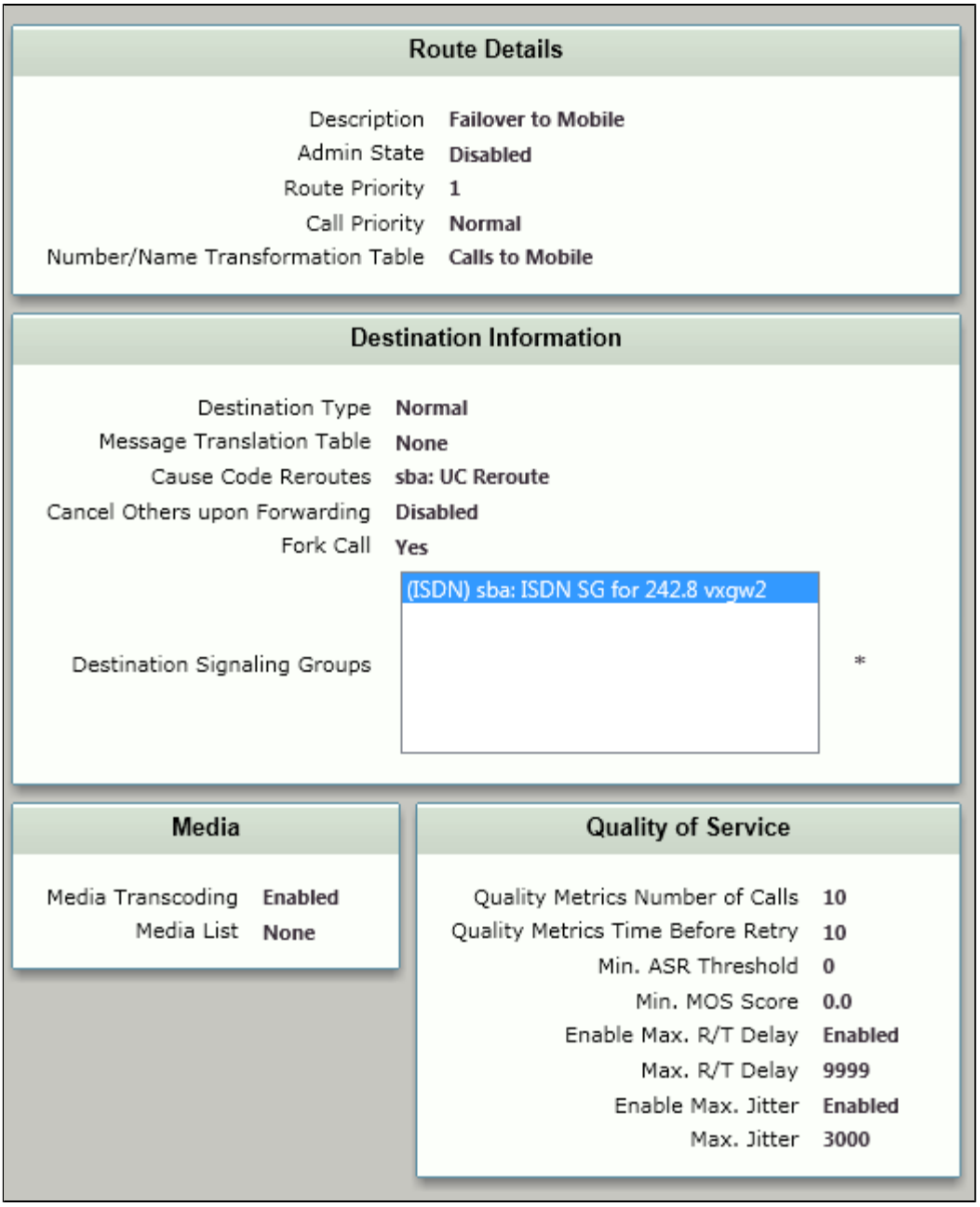
Use the following instructions to create Call Routes and Transformation Tables that perform the call routing noted detail in the Summary section diagram.

1. Create a transformation table with an entry to search for a msRTCSIP-Line entry that matches the called number and returns the mobile number.

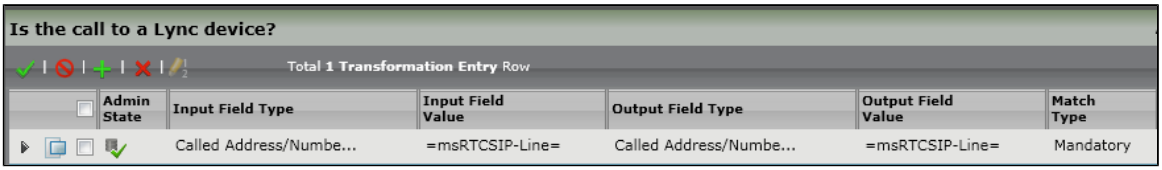


2. Create a new call route table, then a call route entry to the table. In the example, the *Calls to Mobile* transformation table (above) is added to the call route (below).

Copyright © 2015 Sonus Networks. All rights reserved.

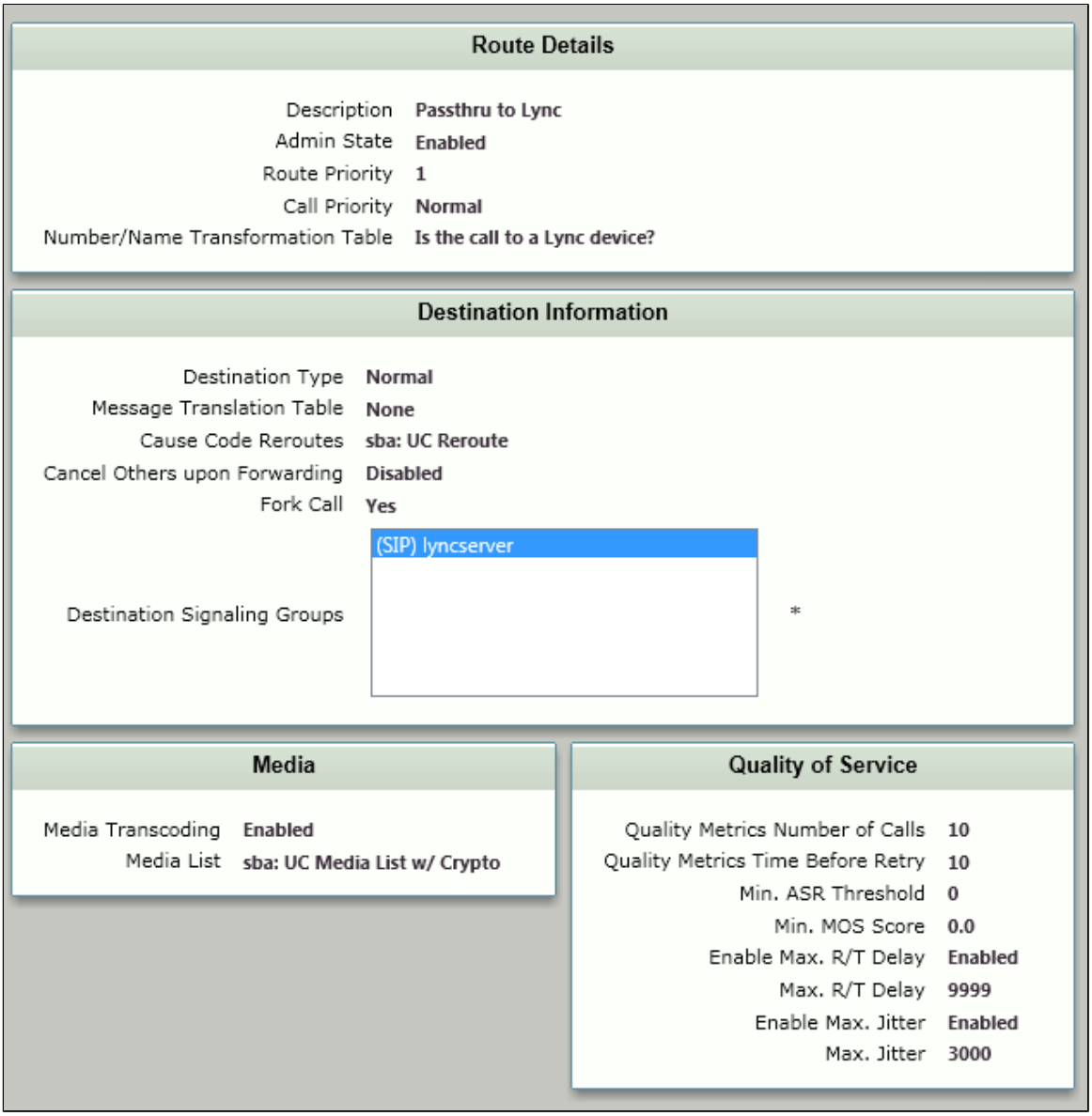


3. Create a second transformation table with an entry to search for a msRTCSIP-Line entry that matches the called number.

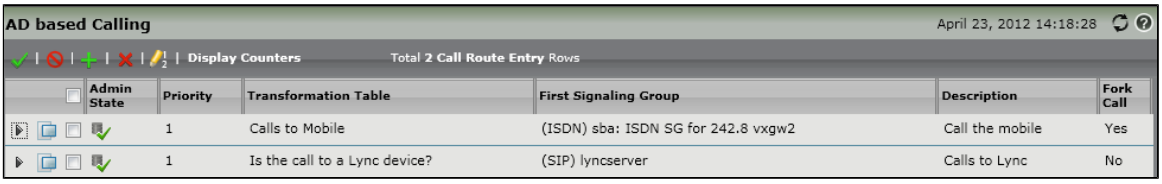


4. Add a second entry to your Call Route table to send the call to the Lync Server. As before, add the transformation table above to the call route below.

Copyright © 2015 Sonus Networks. All rights reserved.



5. Your call route table should look like this:



If you are planning to employ AD lookups for Lync Line URI (msRTCSIP-Line), your searches will likely require additional number translations. Click here to view some common number normalizations for msRTCSIP-Line AD lookups.

It is often necessary to change (normalize) a number before performing an AD lookup. The vast majority of lookups require just the addition of +countrycode (i.e. +1 for the US) for a number that is already 10 digits (areacode+number).

The Lync Line URI (msRTCSIP-Line) is different as it is always prepended with *tel:* and often postpended with *;ext=number*. Since AD searches must be exact matches, the number must be corrected before the search. Below are some common normalization transformations.

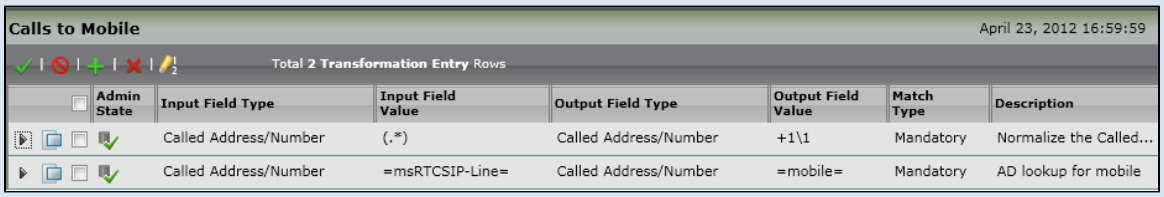
Copyright © 2015 Sonus Networks. All rights reserved.

If *Normalize Cache* is configured to *True*, the tel: will automatically be removed from msRTCSIP-Line before the SBC caches the number. Setting *Normalize Cache* to *True* is recommended.

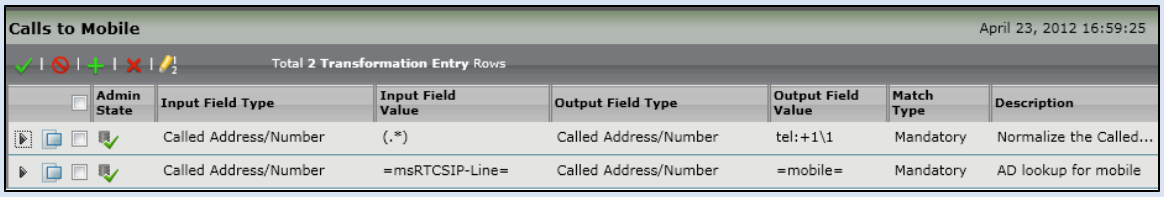
If your Lync Line URI: looks like this:



These are two common normalizations:



with Normalize Cache set to True

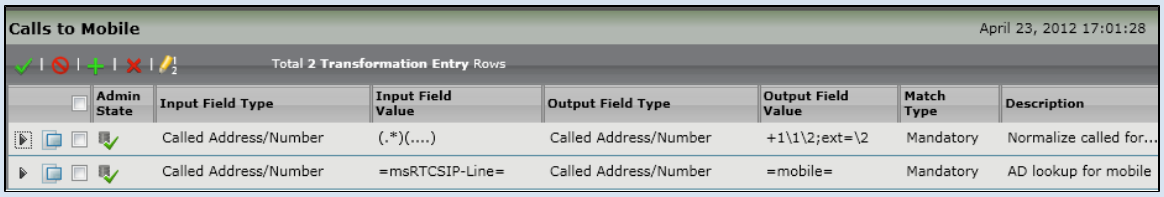


with Normalize Cache set to False

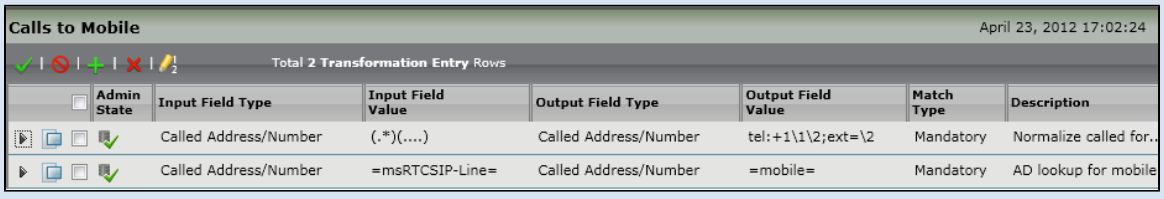
If your Lync Line URI: looks like this:



These are two common normalizations for a 4 digit extension:



with Normalize Cache set to True



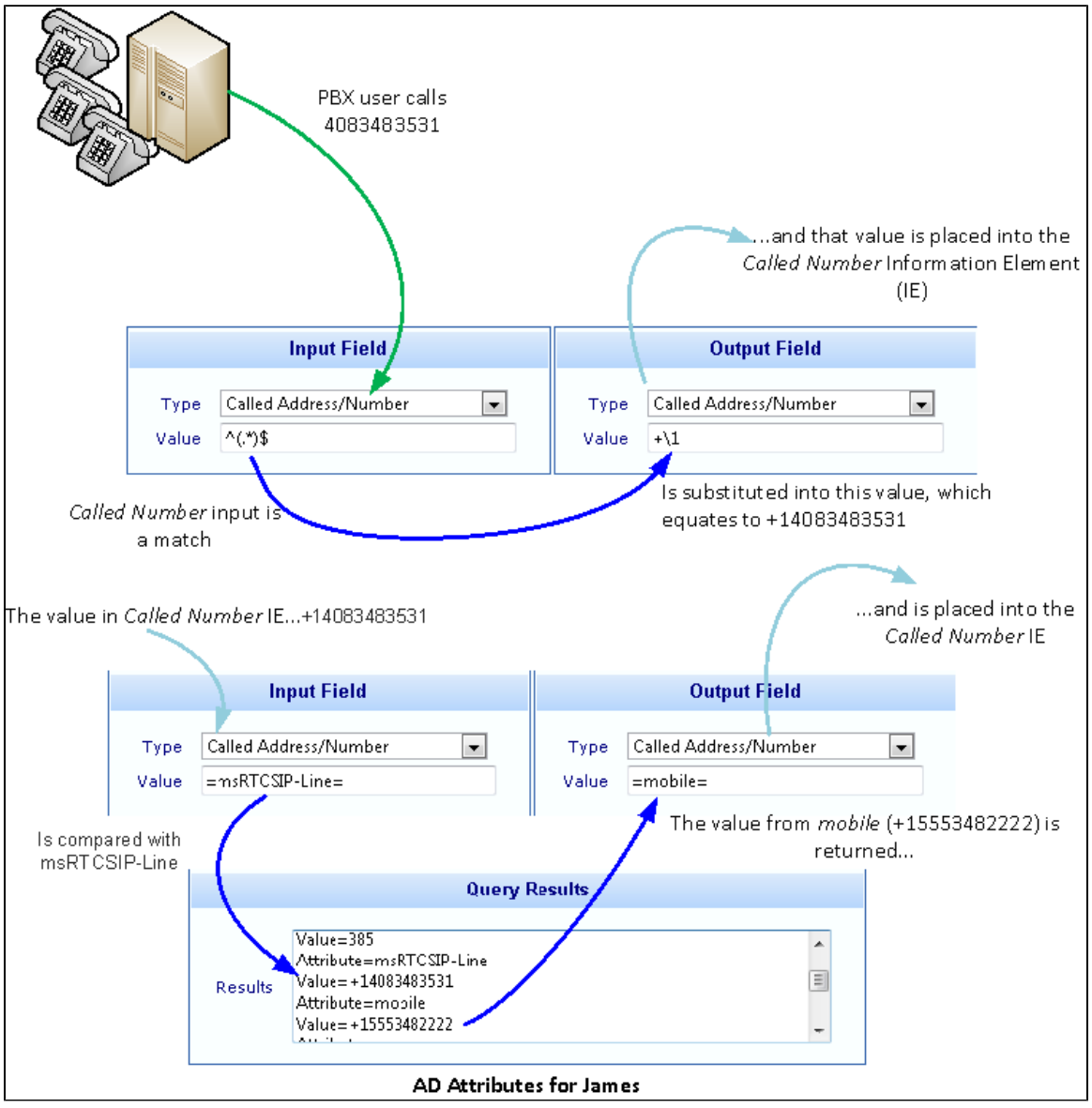
with Normalize Cache set to False

Copyright © 2015 Sonus Networks. All rights reserved.

If your *Operating Mode* is configured to *Online*, normalization should always include tel: as *Normalize Cache* is not available in Online mode. As stated before, *Online* mode is **not** recommended.

Additional Notes

The diagram below provides a pictorial representation for conceptualizing how data is processed through Transformation Table entries.



SBC Basic Call Processing For Dummies - SIP to SIP

Copyright © 2015 Sonus Networks. All rights reserved.

Table of Contents

- Prerequistes
- SBC SIP-to-SIP Basic Call Processing Flow
- Other Important Information

About this Page

This document details the basic flow of a SIP to SIP call through the SBC.

Related Articles

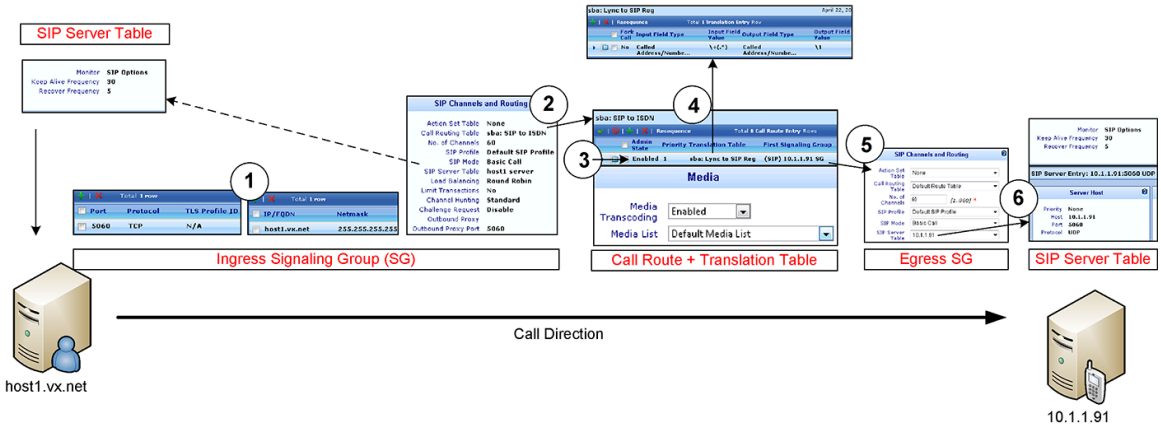
- Managing Signaling Groups
- Managing Call Routing Tables
- Managing Transformation Tables
- Managing SIP Server Tables
- Working with Media

Prerequistes

None

SBC SIP-to-SIP Basic Call Processing Flow

The followoing diagram illustrates the SBC 1000/2000 basic SIP-to-SIP call processing.



SBC Basic Call Processing Flow

1. The call is received by the SBC. The Source IP addresses is matched against the Federated IP addresses contained in all the Signaling Groups (SG).
    a. The SG with the closest matching Federated IP is selected to process the incoming call.?
    b. In the case above, the Federated IP, *host1.vx.net/32*, exactly matches the sending host's source IP as resolved via DNS (*host1.vx.net*).?
    c. Of course, the transport type and incoming port must also match.

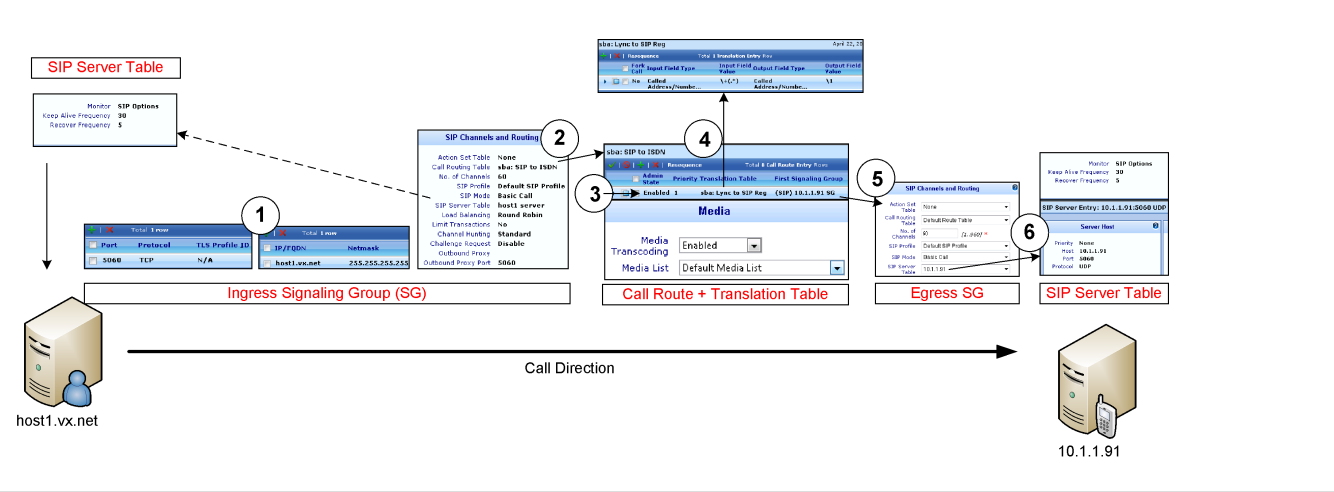
Copyright © 2015 Sonus Networks. All rights reserved.

2. The SG defines the Call Routing Table to use for processing the call, *sba: SIP to ISDN* in this case.
3. The Call Routing Table contains a list of call routing entries.?
4. Those call route entries define which Transformation Table (*sba:Lync to SIP Reg*) to use in manipulating the call's numbers, names, etc.
5. If the transformation is valid, the call is passed to the the Destination Signaling Group (*10.1.1.91 SG*) defined in the call route entry.
6. The Egress Signaling Group contains the configuration for the (egress) SIP Server Table (*10.1.1.91*)

The call is then sent to destination based upon the configuration of the SIP Server Table entry.

Other Important Information

Click here to view the diagram fully-sized



Click here to download a formatted PDF version of this article

SBC Call Routing Reference for Dummies

Table of Contents

- Prerequistes
- Call Route Entry Reference

About this Page

This document provides a brief decription of each element within a Call Route.

Related Articles

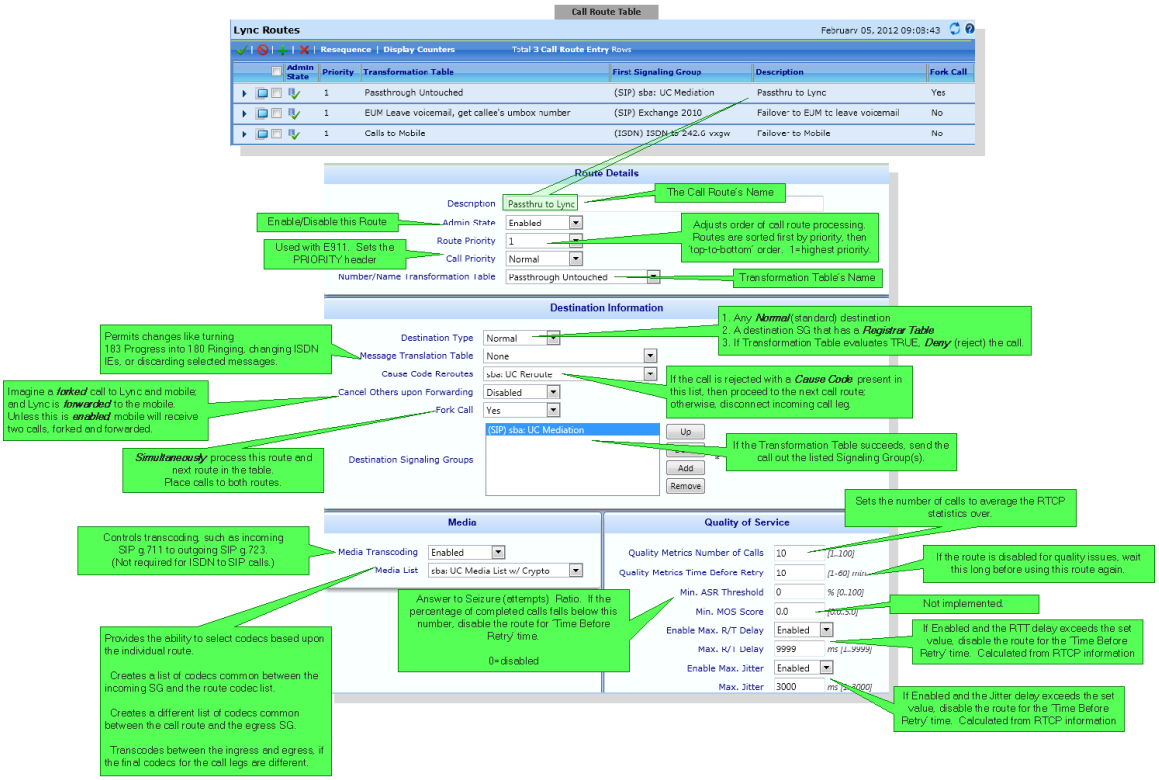
- Managing Signaling Groups
- Managing Call Routing Tables
- Managing Transformation Tables
- Managing SIP Server Tables
- Working with Media

Prerequistes

Copyright © 2015 Sonus Networks. All rights reserved.

Assumes the user is familiar with navigating the SBCx000's WebUI

Call Route Entry Reference



SBC ISDN to SIP Routing For Dummies - TCP

Table of Contents

- Prerequistes
- SBC Network Configuration Summary - ISDN to TCP SIP Server
- Configuration Steps
  - The Lync Wizard Task
  - Configure Media for TCP/RTP
    - Media Configuration Steps
  - Call Routing Configuration
    - Configure ISDN to SIP Call Routing
      - ISDN to SIP Call Configuration Steps
    - Configure SIP to ISDN Call Routing
      - SIP to ISDN Call Configuration Steps
- Important Notes

About this Page

This document details the steps and inter-related parameters to establish an ISDN to SIP Server configuration using TCP transport.

Copyright © 2015 Sonus Networks. All rights reserved.

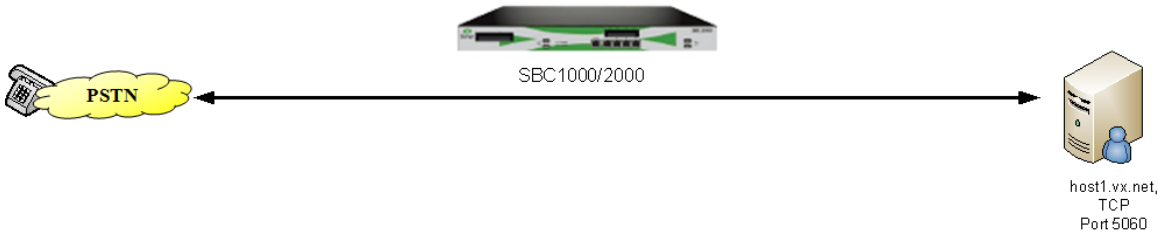
Related Articles

- Managing Signaling Groups
- Managing Call Routing Tables
- Managing Transformation Tables
- Managing SIP Server Tables
- Working with Media

Prerequistes

Assumes the user is familiar with navigating the SBCx000's WebUI

SBC Network Configuration Summary - ISDN to TCP SIP Server



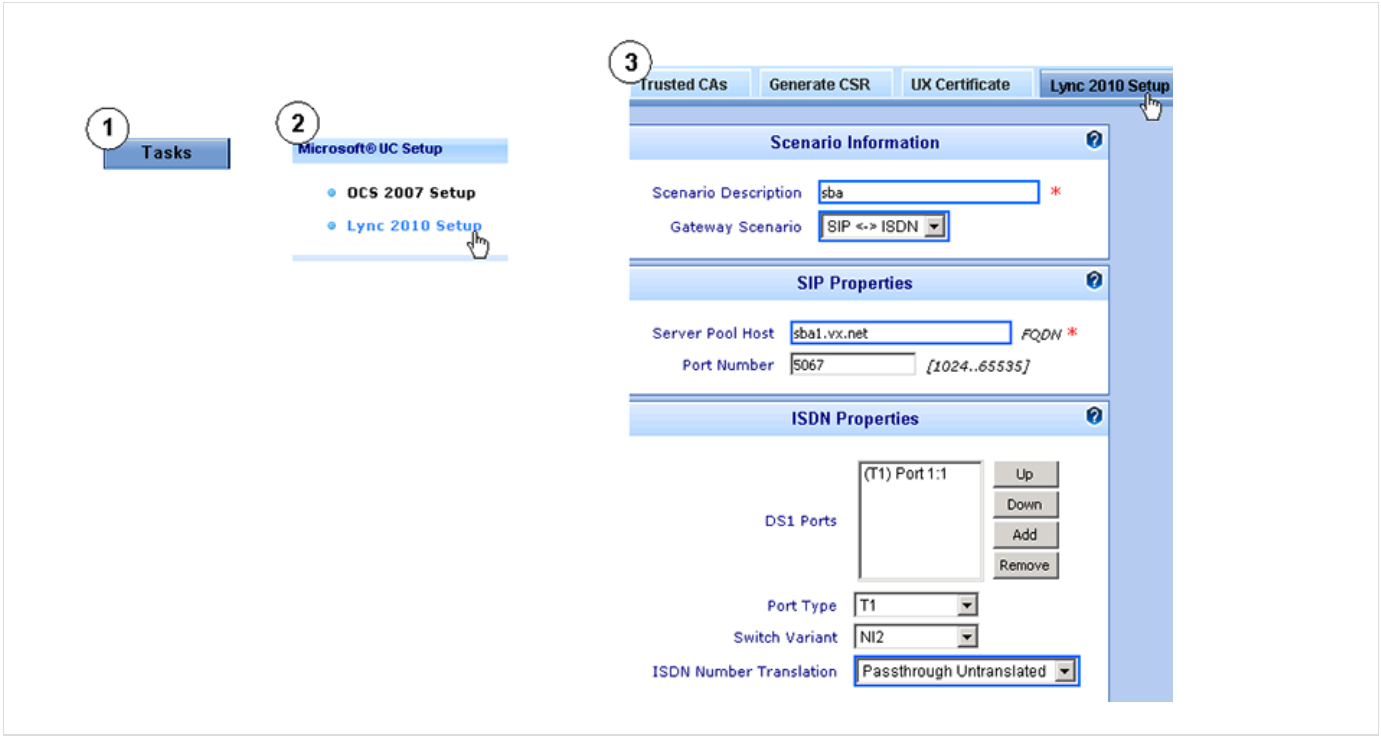
ISDN to SIP (TCP) Network

Configuration Steps

The Lync Wizard Task

The configuration process of a SBC should always begin with running a wizard; however, the wizard only needs to be run for the very first configuration.

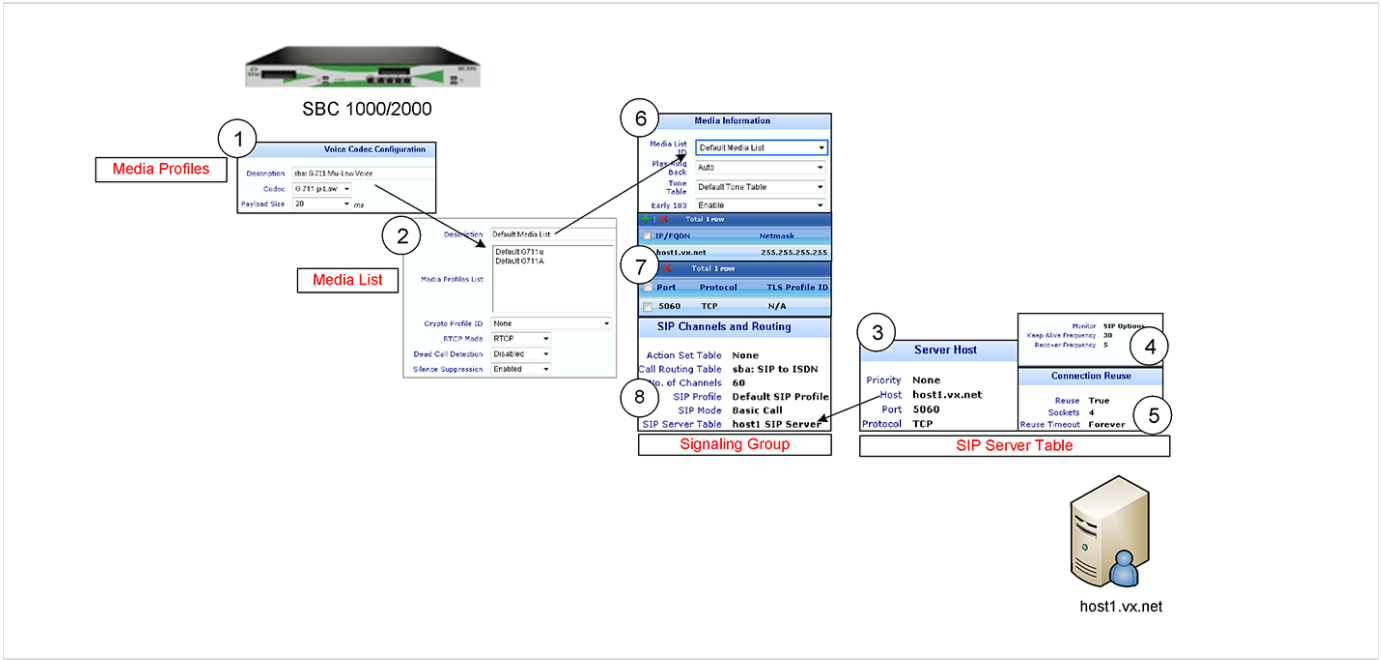
Copyright © 2015 Sonus Networks. All rights reserved.



Lync Wizard Task

Configure Media for TCP/RTP

Use the following diagram and the steps to configure the Media and Profiles for the ISDN to (TCP) SIP Server call.



TCP/RTP Media Configuration Flow

Copyright © 2015 Sonus Networks. All rights reserved.

Media Configuration Steps

1. Ensure there is a media profile for your preferred codec
2. Verify the Media list for Media.

Verify each setting.
In the SIP Server Table:
3. Add a SIP Server Host for the destination server (IP or FQDN), host1.vx.net in the example.
4. Set the SIP Options and the (5) TCP Reuse Parameters

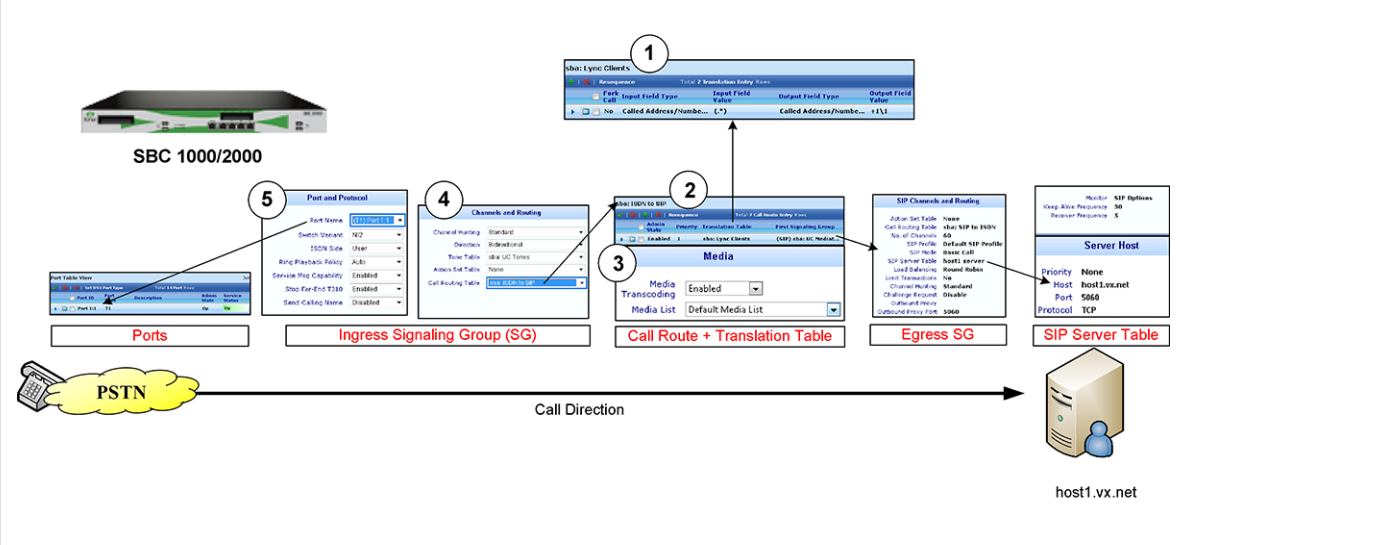
Create a Signaling Group for host1.vx.net:
6. Set the Media List entry
7. Set the Federated IP/FQDN, port and protocol
8. Set the SIP Server Table entry

> ☑ The fully-sized diagrams in this article are available by download at the bottom of the page

Call Routing Configuration

Configure ISDN to SIP Call Routing

Use the following diagram and steps to configure a call route from ISDN to SIP.



ISDN to SIP Call Routing Configuration

ISDN to SIP Call Configuration Steps

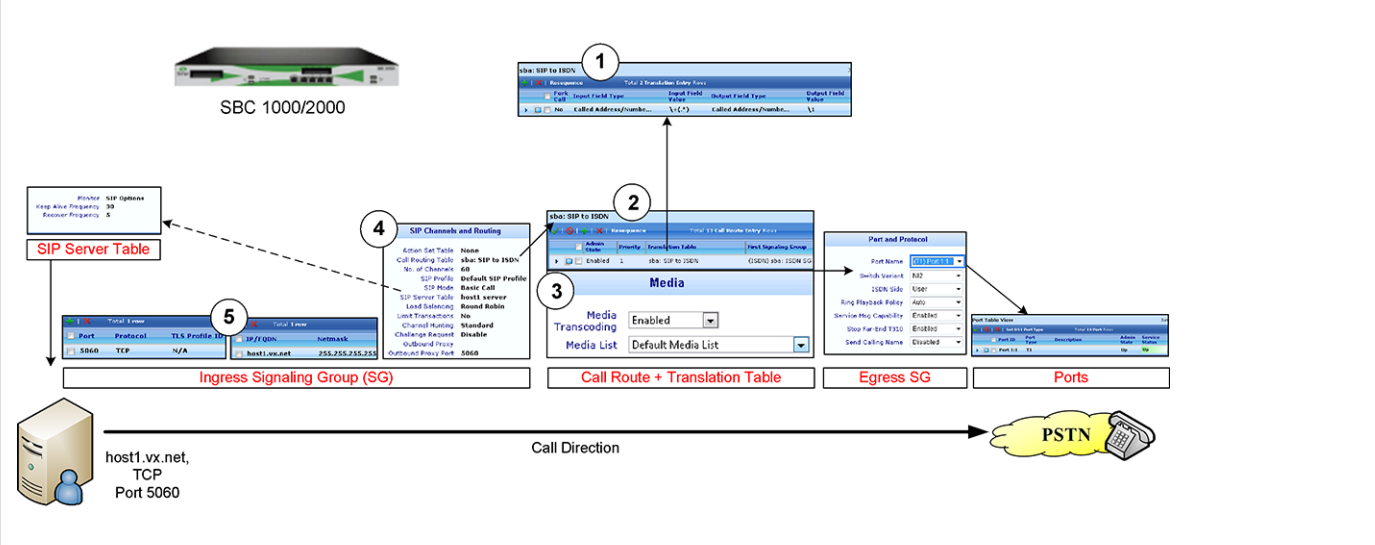
- Create a translation table/entry to perform any necessary number translations.
- Use the automatically created *ISDN to SIP* Call Routing Table, or create a new one of your own. In the Call Routing Table, create a Call Route entry. Configure the translation table name to perform any desired number translations.
- Configure the Egress SG as shown above, setting the *Destination Type* and *Destination Signaling Groups* as shown in the diagram.
- Enable transcoding.

In the Inbound ISDN SG:
- Verify/Set the Call Route Table and incoming ISDN port

Copyright © 2015 Sonus Networks. All rights reserved.

Configure SIP to ISDN Call Routing

Use the following diagram and steps to configure a call route from SIP to ISDN.



SIP to ISDN Call Routing Configuration

SIP to ISDN Call Configuration Steps

- The *Default Route* routing table should have been created automatically as a result of running the Lync Wizard.
- Create (or modify) a Call Route entry in the *Default Route* table. Select a translation table to perform whatever number translation is desired. Also, configure the *Destination Signaling Group* for the ISDN SG.
- Enable transcoding.

In the Ingress SG:

- Verify/Set the Call Route Table and the Federated IP, transport, and port, as shown in #1 Inbound SIP SG (above).

Important Notes

Click here to download the fully-sized diagrams from this article

Click here to download a formatted PDF of this article

SBC ISDN To SIP Routing for Dummies - TLS

Copyright © 2015 Sonus Networks. All rights reserved.

Table of Contents

- Prerequistes
- SBC Network Configuration Summary - ISDN to TLS SIP Server
- Configuration Steps
  - The Lync Wizard Task
  - Media Configuration for TCP/RTP
    - Media Configuration Steps
  - Call Routing Configuration
    - Call Configuration Steps
- Other Important Information

About this Page

This document details the steps and inter-related parameters to establish an ISDN to SIP Server configuration using TLS transport.

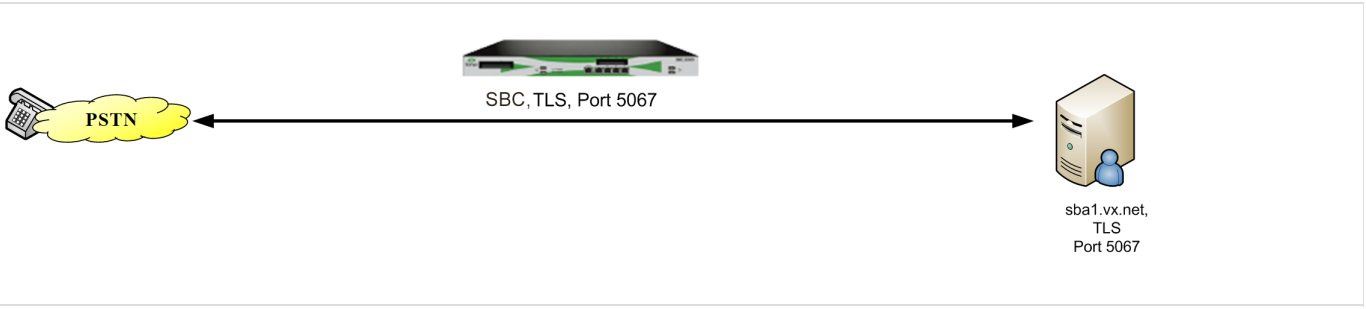
Related Articles

- Managing Signaling Groups
- Managing Call Routing Tables
- Managing Transformation Tables
- Managing SIP Server Tables
- Working with Media

Prerequistes

Assumes the user is familiar with navigating the SBC 1000/2000's WebUI

SBC Network Configuration Summary - ISDN to TLS SIP Server



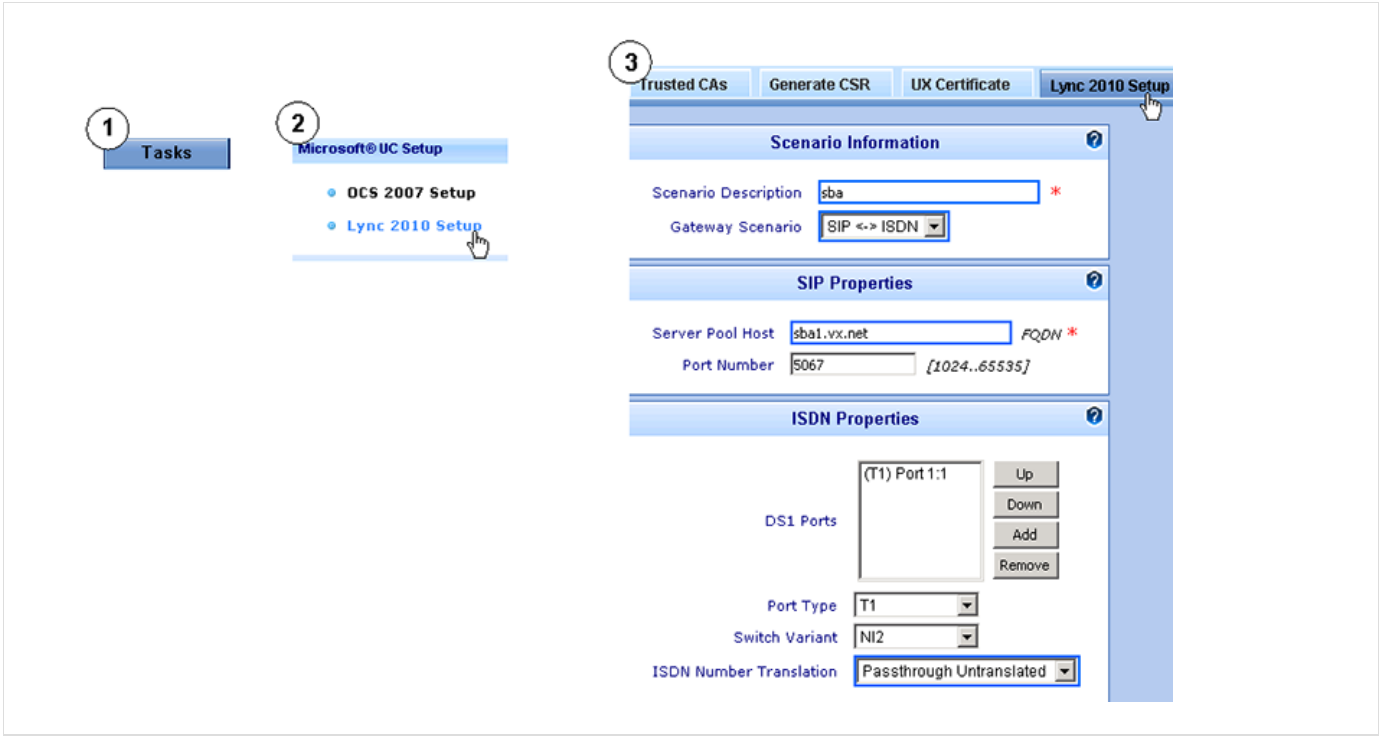
ISDN to TLS SIP Server

Configuration Steps

The Lync Wizard Task

The configuration process of an SBC should always begin with running a wizard. However, the wizard only needs to be run for the very first configuration.

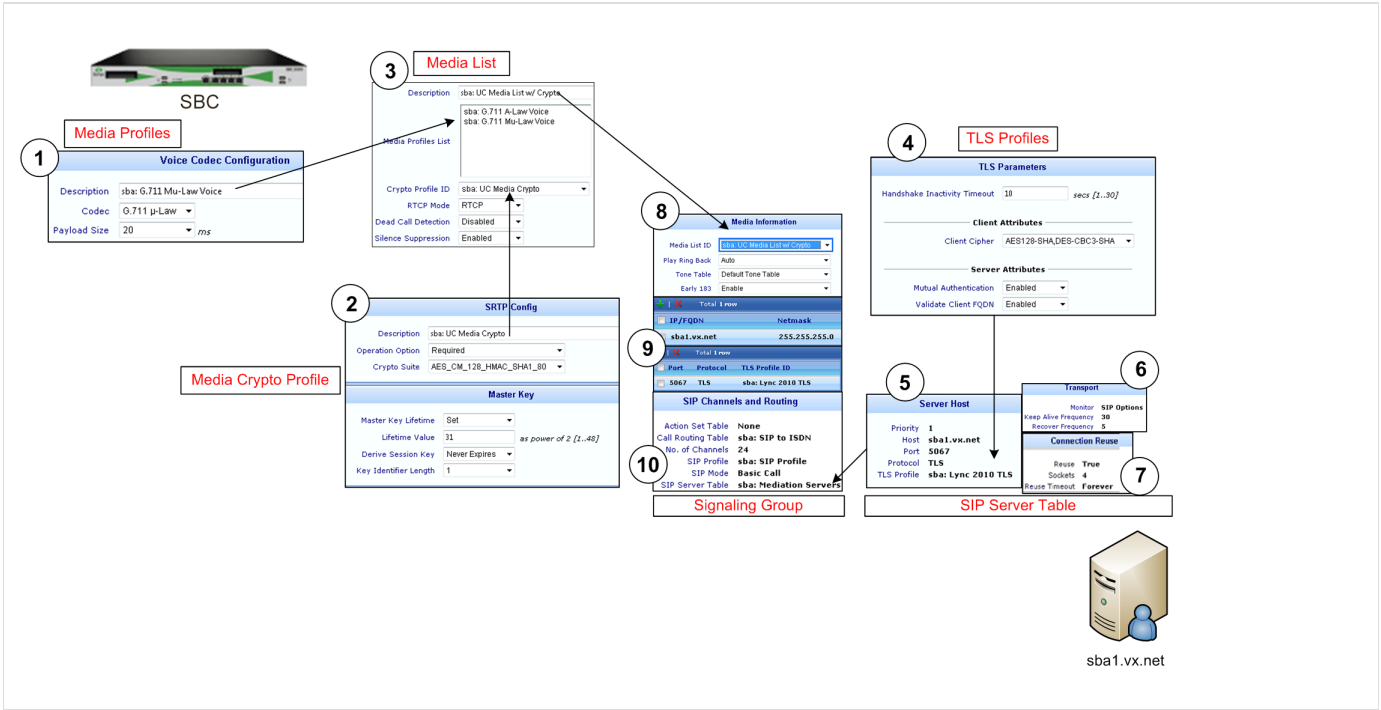
Copyright © 2015 Sonus Networks. All rights reserved.



Lync Wizard Task

Media Configuration for TCP/RTP

Use the following diagram and the steps to configure the Media and TLS profile for the ISDN to TLS SIP Server call.



TLS Media Configuration Flow

Media Configuration Steps

Copyright © 2015 Sonus Networks. All rights reserved.

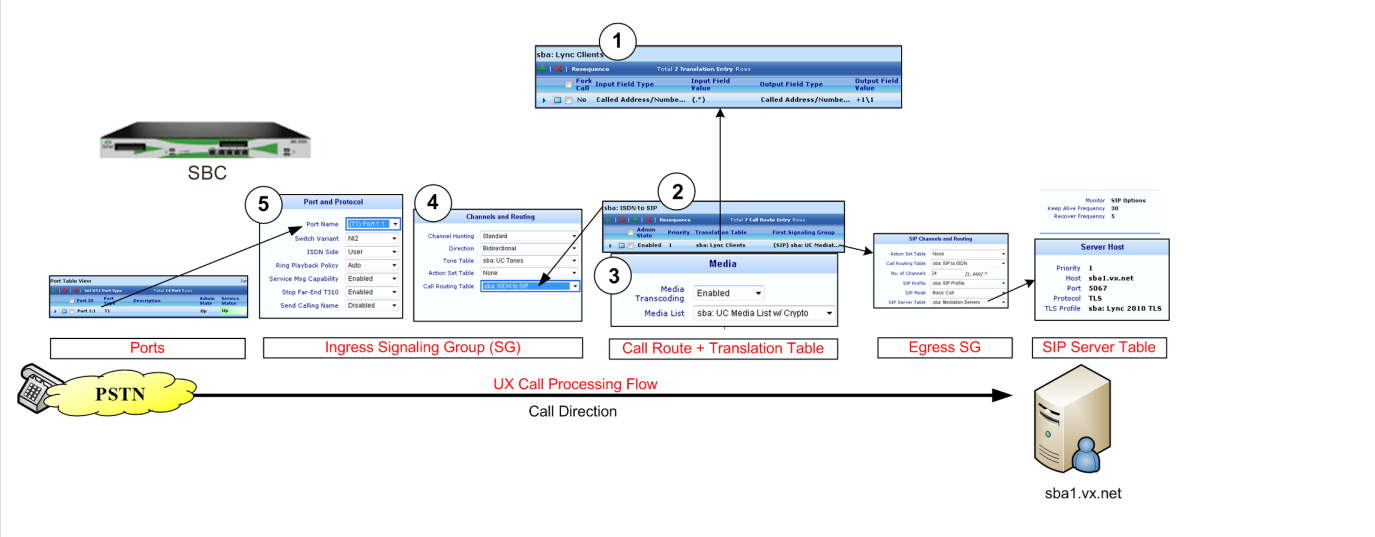
1. Ensure there is a media profile for your preferred codec
2. Review the Crypto Profile
3. Verify the Media list for Media and Crypto Profiles
4. Verify the TLS Profile

In the SIP Server Table:
5. Add a SIP Server Host for the FE/SBA FQDN and set the TLS profile
6. Set the SIP Options and the (7) TLS Reuse Parameters

In the destination Signaling Group:
8. Set the Media List entry
9. Set the Federated FE/SBA FQDN and port:5067/protocol:TLS/TLS Profile
10. Set the SIP Server Table entry

Call Routing Configuration

Use the diagram and steps to configure a call route from ISDN to the TLS SIP Server.



ISDN to Lycn Call Routing Configuration Flow

Call Configuration Steps

1. Create a translation table/entry to perform any necessary number translations
2. Create a Call Route entry. Configure the translation table name and Egress SG configured from the previous page; (3) enable transcoding and set the appropriate media list entry .

In the Ingress SG:
4. Verify/Set the Call Route Table and (5) incoming ISDN port

Other Important Information

> You will still need to configure the SBC for the appropriate certificates in order to complete TLS calls. See Lync Setup documentation for information on certificates and Deploying the Survivable Branch Appliance for further information on deploying a SBA.

> Click here to download the full size diagrams from this article

Copyright © 2015 Sonus Networks. All rights reserved.

Click here to download a formatted PDF of this article

SBC Transformation Tables for Dummies

Table of Contents

- Prerequistes
- Translation Table Reference
- How IE Values Are Processed
- Sample Translations
- Transformation Table IE Definitions

About this Page

This document details a ISDN to SIP UX configuration using either TCP transport.

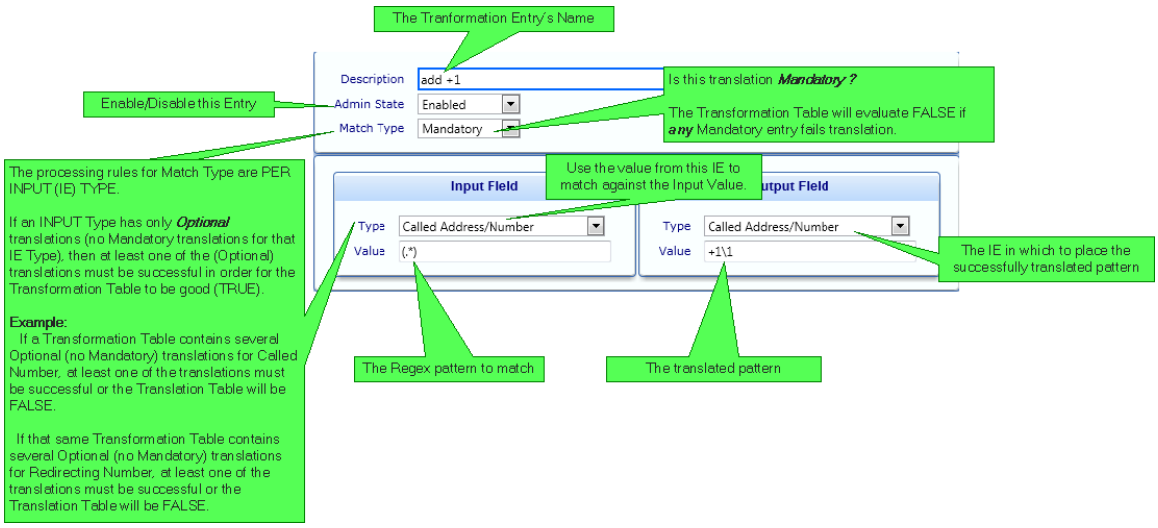
Related Articles

- Managing Signaling Groups
- Managing Call Routing Tables
- Managing Transformation Tables
- Managing SIP Server Tables
- Working with Media

Prerequistes

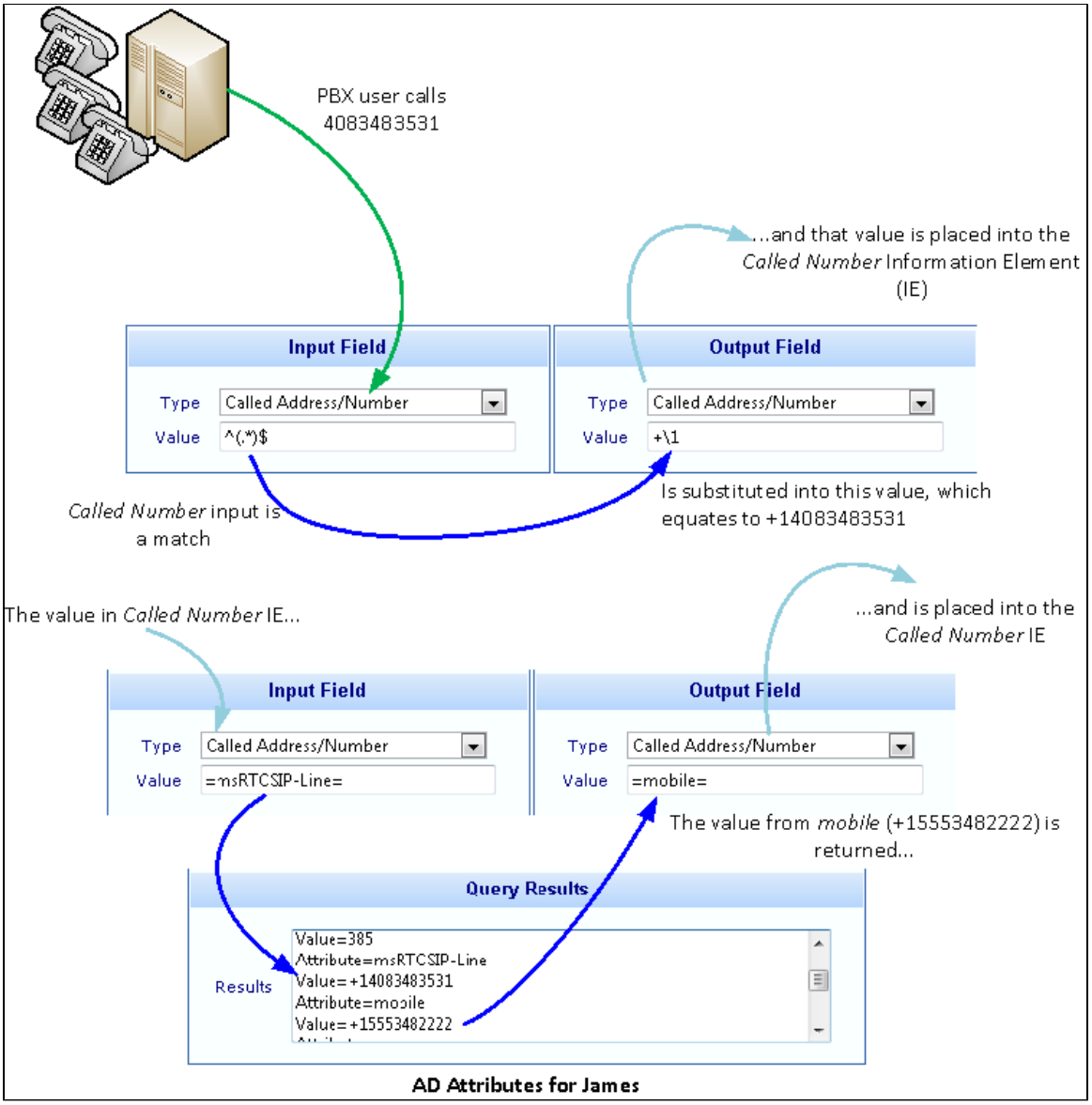
Assumes the user is familiar with navigating the SBCx000's WebUI

Translation Table Reference



How IE Values Are Processed

Copyright © 2015 Sonus Networks. All rights reserved.



Sample Translations

Input Number	Input Field Value	Output Field Value	Resulting Number
14085551212	(\ +14085551212)	\1	+14085551212
5551212	(.*)	\1	5551212
+14085551212	\ +.*(\d{4})	\1	1212
4085551212	^\d{3}(.*)$	\1	5551212
14085551212 15105551212	(1510|1408)(\d{7})	\2	5551212
1212	^(\d{4})$	\1	1212

Copyright © 2015 Sonus Networks. All rights reserved.

Transformation Table IE Definitions

Click here to view the detailed description for the Transformation Table IEs

Input /Output Fields are currently as follows

Field	ISDN Type	SIP Type	Description	Options	Special Notes
Callback Pool Identifier	None	None	Sets the Emergency Callback Numbers Table to be used for calls destined to 911.	None	The Input Field would be set to the public emergency number (like 911) or any other emergency number.
Called Address/Number	DNIS (ISDN IE 0x70)	Request URI	The called number	None	
Called Extension	None	Request URI	Sets the ;ext=	None	To: tel:2222<sip:2222;ext=2222@192.168.1.20>
Called Numbering Type	ISDN IE 0x70		Describes the *format* of the called number. Aids the receiving switch in understanding if this is a SIP or ISDN National formatted number, as an example.	Unknown Subscriber National National-specific Abbreviated International Subscriber (oper.req) National (oper.req) International (oper.req) Not Present (oper.req) Not present (cut through) 950 call Test Line Test Code h323/SIP	Setting to *ISDN* includes user=phone in the Request URI *H323/SIP* removes user=phone from the Request URI
Called Phone Context	None	Request URI	Sets the phone context for tel uri calls	None	To: tel:2222<sip:2222;phone-context=example.com@192.168.1.20>
Called Numbering Plan	ISDN IE 0x70		Describes the called number's numbering scheme or standard.	Any/Untranslated: For Input, any type is accepted. For Output, the plan will remain unchanged. Unknown: The type is unknown. ISDN: E.164 format Data: ITU X.121 format Telex: ITU F.69 format National: The standard national numbering plan Private: A private numbering plan Telephony: same as ISDN	
Calling Address/Number	ANI (ISDN IE 0x6C)	FROM header	The Calling Number	None	
Calling Extension	None	Request URI	Sets the ;ext=	None	From: 5551234<sip:5551234;ext=1234@192.168.1.10>

Copyright © 2015 Sonus Networks. All rights reserved.

Calling Address/Number, User Specified	ANI (ISDN IE 0x6c)	None?	Calling Number supplied by the user in addition to the one supplied by the telephony network	None	
Calling Numbering Type	ISDN Numbering Type, IE 0x6C		Describes the format of the calling number; aids the receiving switch in properly processing the number based upon the configured number type.	Unknown Subscriber National National-specific Abbreviated International Subscriber (oper.req) National (oper.req) International (oper.req) Not Present (oper.req) Not present (cut through) 950 call Test Line Test Code h323/SIP	Setting to *ISDN* includes user=phone in the Request URI *H323/SIP* removes user=phone from the Request URI
Calling Numbering Plan	ISDN Numbering Plan, IE 0x6C		Describes the calling number's numbering plan.	Any/Untranslated: For Input, any type is accepted. For Output, the plan will remain unchanged. Unknown: The type is unknown. ISDN: E.164 format Data: ITU X.121 format Telex: ITU F.69 format National: The standard national numbering plan Private: A private numbering plan Telephony: same as ISDN	
Calling Number Presentation	ISDN Pres. Indicator, IE 0x6C		Controls how the downstream device displays/processes the Calling Number.	Allowed: Display the calling number Restricted: Do not display the calling number Not Available Reserved	May also affect how the downstream device processes the P-Asserted ID or the P-Preferred ID
Calling Number Screening	ISDN Screening Indicator, IE 0x6C		Denotes how/if the calling number has been verified	User - Not Screened: Set by the client, not checked by the sending switch User - Verified: Set by client, verified by the sending switch User - Failed: The sending switch confirms this number as invalid Network: The previous switch provided the calling number	May also affect how the downstream device processes the P-Asserted ID or the P-Preferred ID

Copyright © 2015 Sonus Networks. All rights reserved.

Calling Name	ISDN IE 0x1C or IE 0x28	FROM header	The calling name	None	
Calling Phone Context	None	FROM header	Sets the phone context for tel uri calls	None	To: tel:2222<sip:2222;phone-context=example.com@192.168.1.20>
ELIN Identifier	ISDN IE 0x6c, Calling Number	FROM header	Sets the Emergency Line Identifer that the PSAP will use to lookup the location in the location database.	None	
Original Called Number	ISDN IE 0x1C	DIVERSION header	Specifies the original number when a call has been redirected	None	The redirecting number is the number the call was last redirected from. The original called number is just that, the very first called number, which in the case of multiple redirections can be different.
Original Destination Number	None	TO Header	Specifies the number in the TO header	None	This differs from the Called Number which is set from the SIP Request URI
Redirecting Number	ISDN 0x74	None	Specifies the number to which a call should be redirected to	None	
Redirecting Numbering Type	ISDN 0x74		Same as Types above	Same as Types above	
Redirecting Numbering Plan	ISDN 0x74		Same as Plans above	Same as Plans above	
Transfer Capability			Used for permanent circuits. Not presently supported by UX		

Configuring the RBA 3G4G Feature

Table of Contents

- Prerequistes
- SBC Configuration
- Network Diagram
- Before Beginning
  - STUN Setting
  - RBA Image
  - Check the RBA License
  - DNS Configuration
- Lync Server Topology Configuration
  - Open the Lync Topology Builder
  - New Branch Site
  - New PSTN Gateway
  - Publish

Copyright © 2015 Sonus Networks. All rights reserved.

- Lync Server Configuration
  - Create a new Site Voice Policy
  - Commit New Site Voice Policy
  - Verify Route and PSTN Usage
  - Create a User New Dial Plan
  - Create A New User Voice Policy
  - Create a New PSTN Usage
  - Commit Changes
  - Add or Move a User into the new remote location
  - Configure the Network Configuration
  - Create a new Bandwidth Policy
  - Create a new Region
  - Create a new Site
  - Create new Subnets
  - Create a Region Link
  - Create a new Region Route
- Domain Controller Configuration
- Configuring the RBA
- IP Routing
  - SBC 1000 Static Routes
  - SBC 2000 Static Routes
- SIP Server Tables and Signaling Groups
  - SBC 1000 SIP Server Table
  - SBC 1000 Signaling Groups
  - SBC 2000 SIP Server Table
  - SCB 2000 Signaling Groups
- Verification
  - Verifying Routing
  - Testing Connectivity over the WAN Link
    - From a PC on the HQ side of the network
    - Test a Lync to Lync Call

Copyright © 2015 Sonus Networks. All rights reserved.

- Creating the IPSec Tunnel
  - SBC1000 IPSec Configuration
  - SBC2000 IPSec Tunnel Configuration
  - Verification
    - Preparing for Verification
    - Verifying PC Connectivity
    - Re-add the HQ SBC WAN Route
  - Configuring for Automated Switchover
  - SBC 1000 CAC Profiles
    - Create the CAC Profiles on the Remote SBC
    - SBC 1000 Link Monitor Configuration
    - Verification
    - SBC 2000 Link Monitor Configuration
  - Verification
    - WAN Link Up
      - HQ SBC
      - Remote SBC
      - Lync Server
      - Lync Clients
    - WAN Link Down
      - HQ SBC Status
      - Remote SBC Status
      - Lync Server
      - Lync Clients
- Setting the Remote SBC to TLS
    - Certificate for the SBC
  - Setting the SIP Server and Signaling Group for TLS/SRTP
- RBA Data Flows
  - WAN Up Flow
  - WAN Down Instant Message Flow
  - WAN Down Lync-to-Lync Call Flow
- Troubleshooting
  - Prepare SBA not run
  - RBA computer not a member of RTCUniversalServerAdmins group
  - Service Status Stays Yellow
  - OPTIONS with Carrier's IP address
  - RBA Command Working Properly

About this Page

This document details a complete implmentation of the SBC's RBA Feature

Related Articles

- Managing Signaling Groups
- Managing Call Routing Tables
- Managing Transformation Tables
- Managing SIP Server Tables
- Working with Media

Copyright © 2015 Sonus Networks. All rights reserved.

Prerequistes

- Assumes the user is familiar with navigating the SBCx000's WebUI
- The RBA feature requires the latest ASM image. Be sure that the HQ ASM is upgraded to the latest image version.
- Install the Lync Server Resource Kit on the Lync Server. You will want the Bandwidth Policy Server Monitor Application to verify the dynamic CAC Profile changes. See the Microsoft Lync Server site to obtain the Resource Kit and installation instructions.
- The RBA Feature is only supported between two Sonus SBC nodes
- The RBA Feature requires an ASM installed on the HQ SBC
- The RBA Feature is included only in SBC version 3.0 or better

SBC Configuration

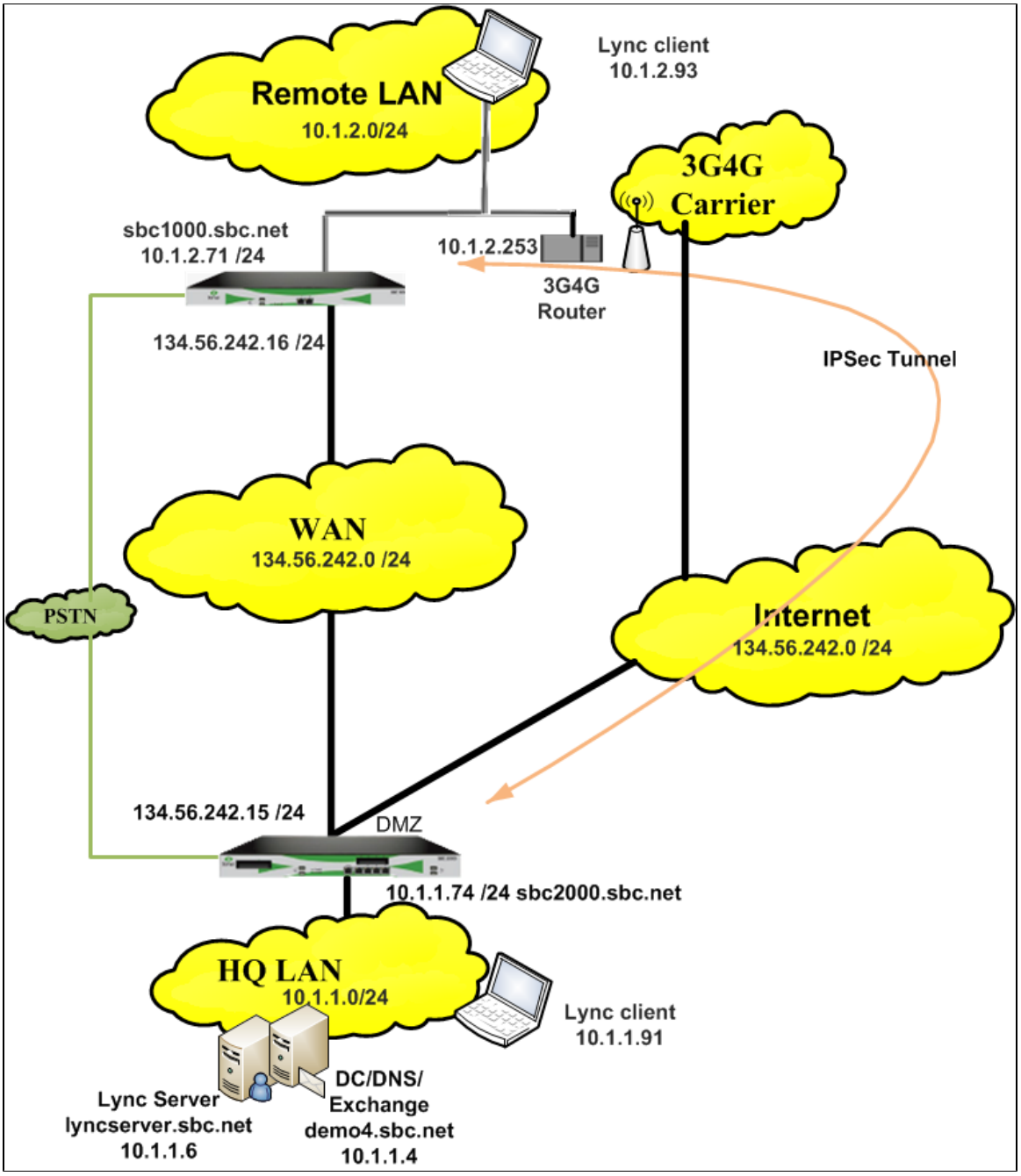
This quick start document shows the steps and interlational parameters required to configure a UX to successfully route calls. The configuration process of a UX should always begin with running a wizard; however, the wizard only needs to be run for the very first configuration.

- There are many different architectures which might be used for connecting remote sites to a main site. The manual pages for this 3G4G feature specify a VLAN switch with the 3G4G and WAN networks sharing a single port of the UX.

  The implementation below uses a 3G4G router connected to the remote LAN segment, thus dedicating the WAN connection to a SBC port. This configuration elminates then need for a VLAN-capable switch.

Network Diagram

Copyright © 2015 Sonus Networks. All rights reserved.



Before Beginning

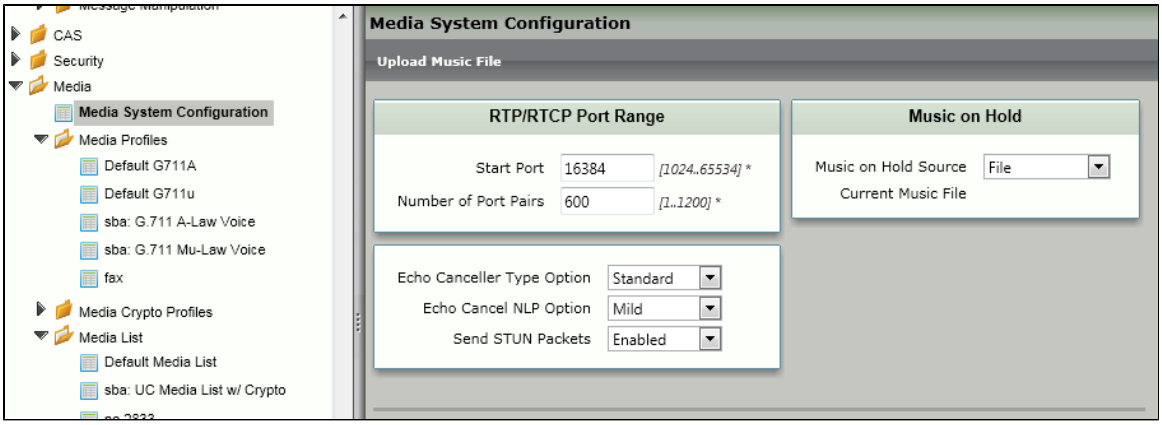
As a prerequisite to installing the RBA feature, check the following items:

- STUN Setting on the SBC
- Installed ASM Image
- RBA License
- DNS Configuration

STUN Setting

Configure *Send STUN Packets* to *Enabled* in the *Media* | *Media System Configuration*.

Copyright © 2015 Sonus Networks. All rights reserved.



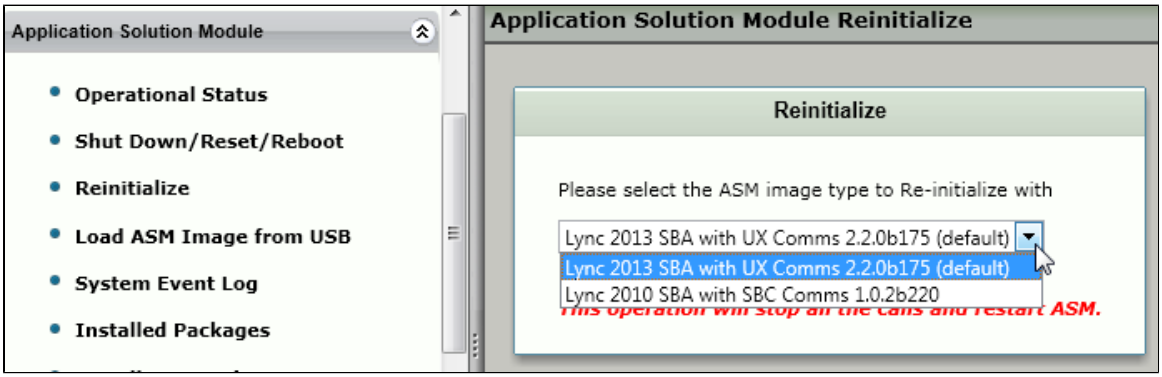
RBA Image

If your HQ-side SBC was running version 2.2, you will need upgrade both the ASM image as well as the SBC firmware. The latest ASM image is available at support.net.com.

These instructions detail the use of an SBA image rather than the RBA image. Both images perform equivalent functions for the RBA implementations. In fact, a future SBC version will use a single image for both SBA and RBA. For now, you may use either the RBA or SBA image when installing the 3G4G Backnet feature.

Is your ASM running an SBA image compatible with your Lync Server? If you're running Lync 2013, be sure your ASM image is the Lync 2013 SBA image. The Lync 2013 SBA image is available from downloads.net.com.

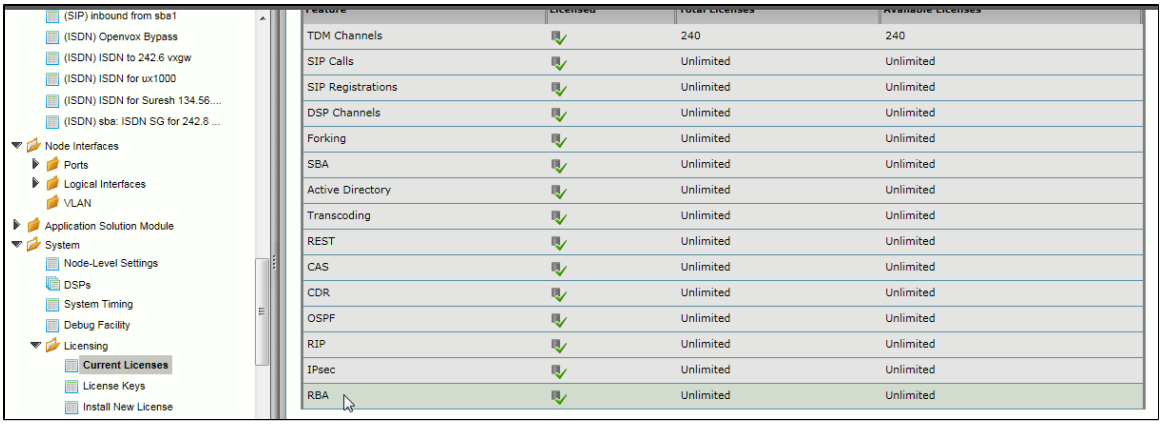
Under the *Tasks Tab* | *Application Solution Module* | *Reinitialize* the pull-down selection will supply the possible images currently available on your ASM. Update your ASM images if you are implementing Lync Server 2013 and there is no Lync 2013 image available on your ASM.



Check the RBA License

Verify that your SBC is licensed for the RBA feature.

Copyright © 2015 Sonus Networks. All rights reserved.

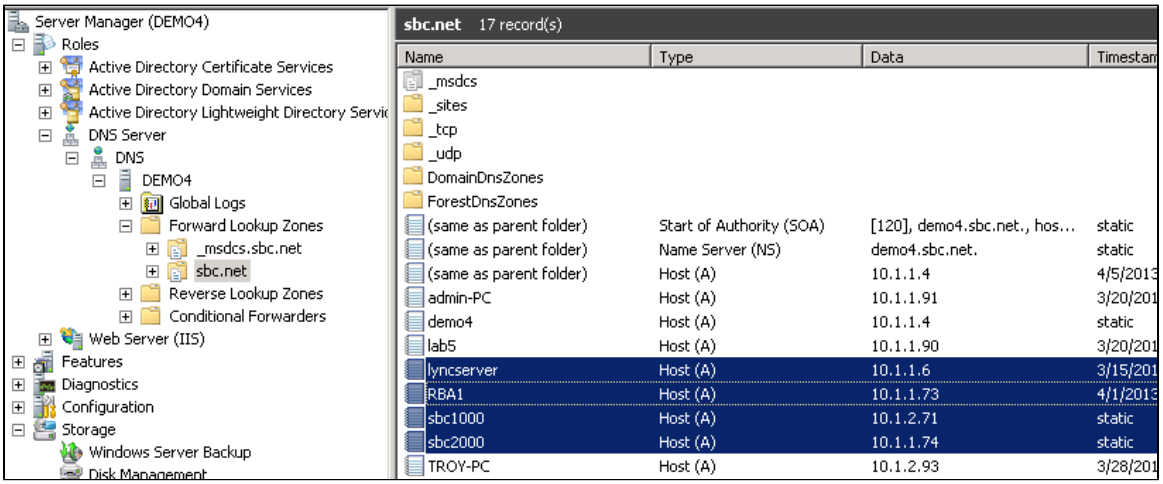


DNS Configuration

Add both SBCs to the DNS server. In the example, SBC2000 is the HQ SBC and SBC1000 is the remote network SBC. The DNS server is configured only with the LAN-side IP addresses of these nodes, 10.1.1.74 and 10.1.2.71, respectively.

Add the FQDNs and IP addresses for nodes that are part of the RBA feature:

- Remote-network SBC
- HQ SBC
- HQ ASM
- Lync Server



Lync Server Topology Configuration

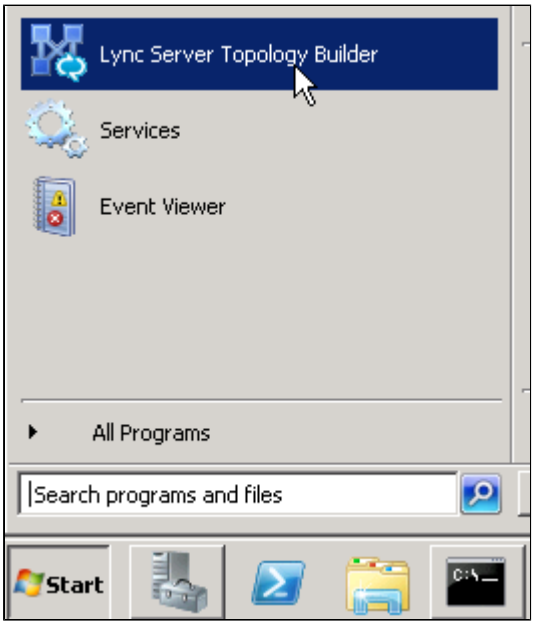
The remote-network SBC must be added to the Lync Topology. Follow these steps:

- Open the Topology Builder
- Add a new Branch Site
- Add the SBC as a PSTN Gateway

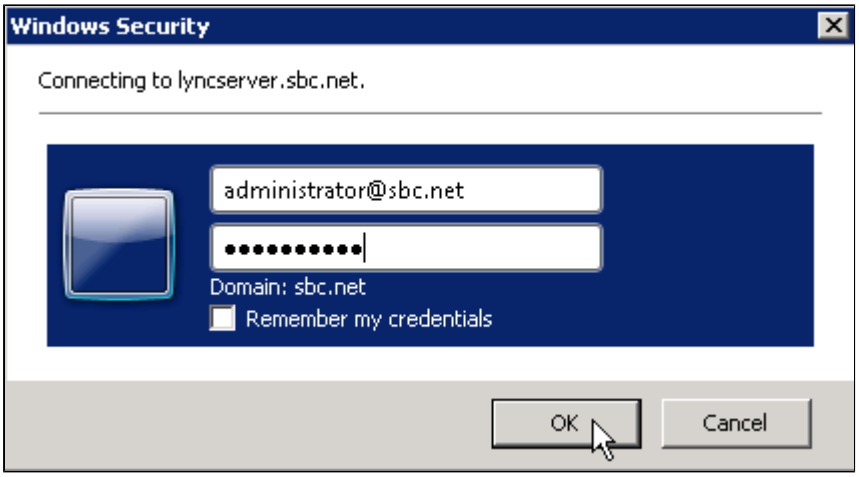
Open the Lync Topology Builder

Copyright © 2015 Sonus Networks. All rights reserved.

1. **Start the Topo Builder**

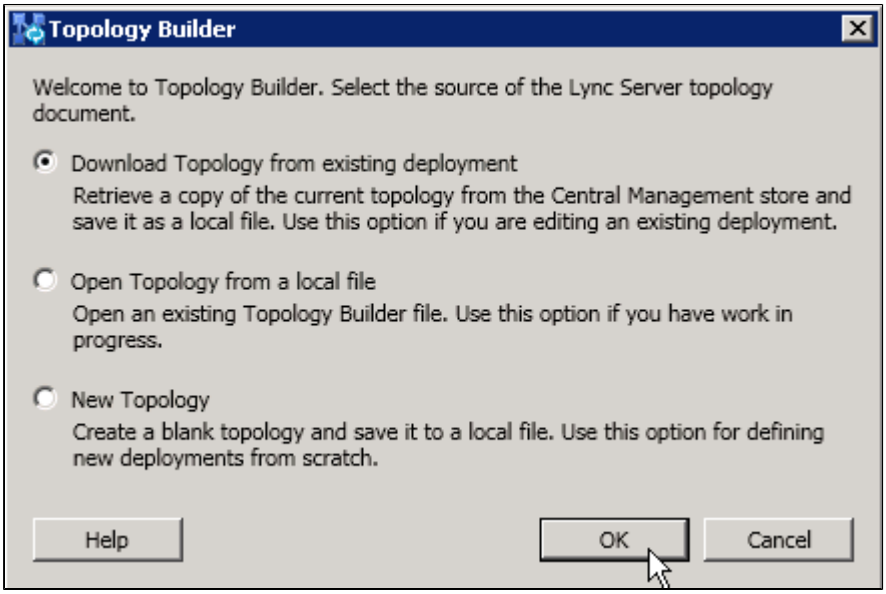


2. **Enter Login Credentials**

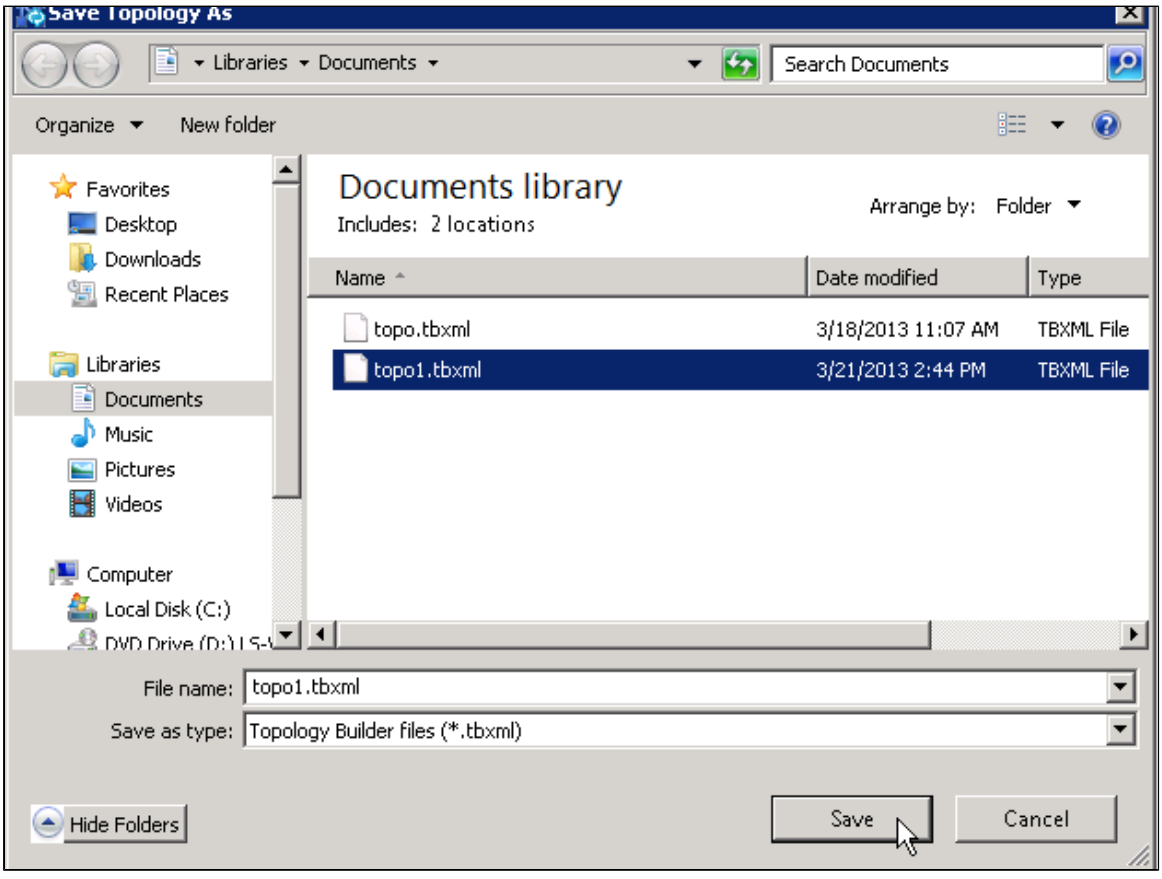


3. **Download the Topology**

Copyright © 2015 Sonus Networks. All rights reserved.

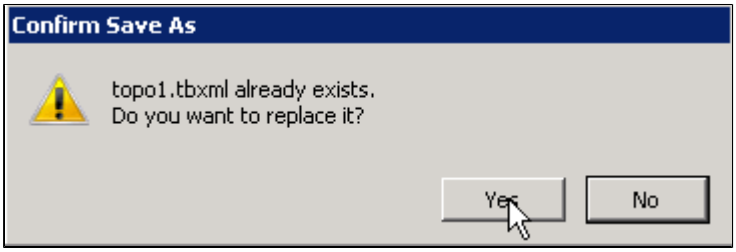


4. **Specify a Filename**



5. **Confirm Changes**

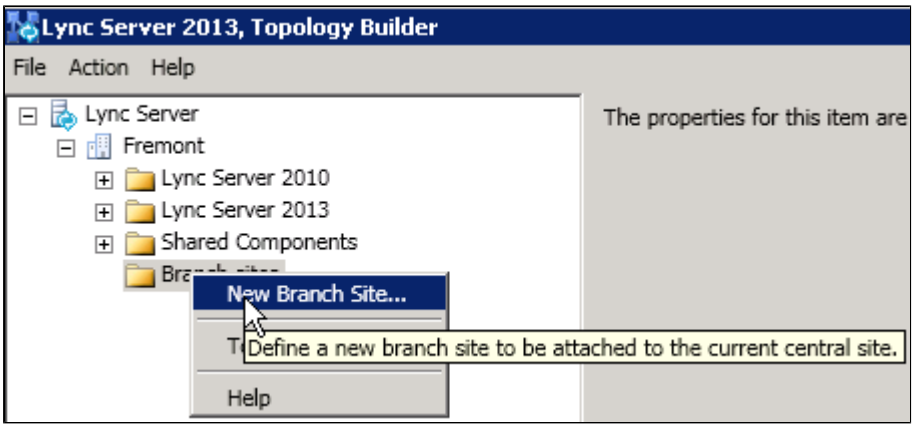
Copyright © 2015 Sonus Networks. All rights reserved.



New Branch Site

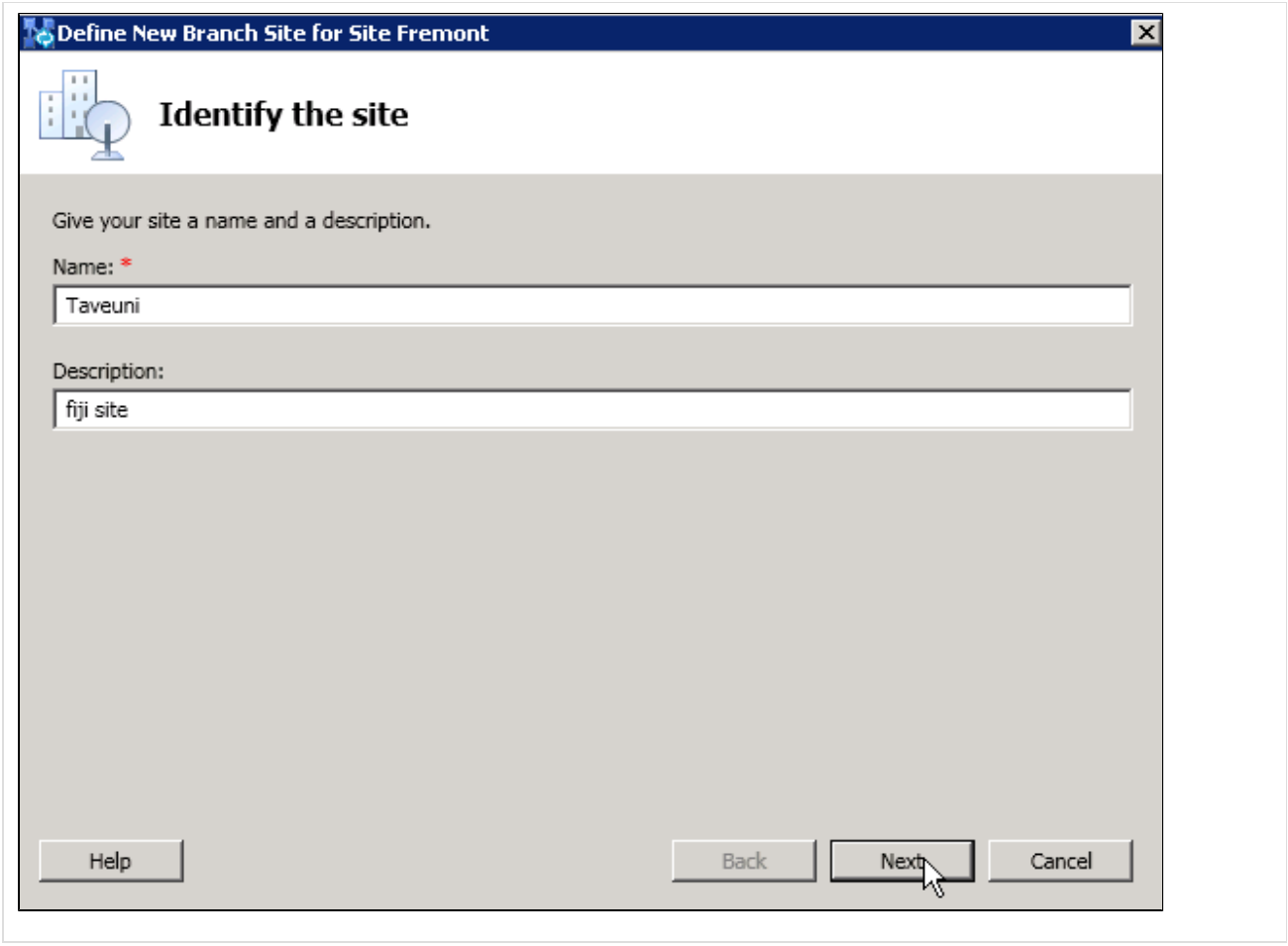
Add a new Branch Site. In the example, *Taveuni* is the new remote branch.

1. **Right-click on *Branch Sites* and select *New Branch Site***



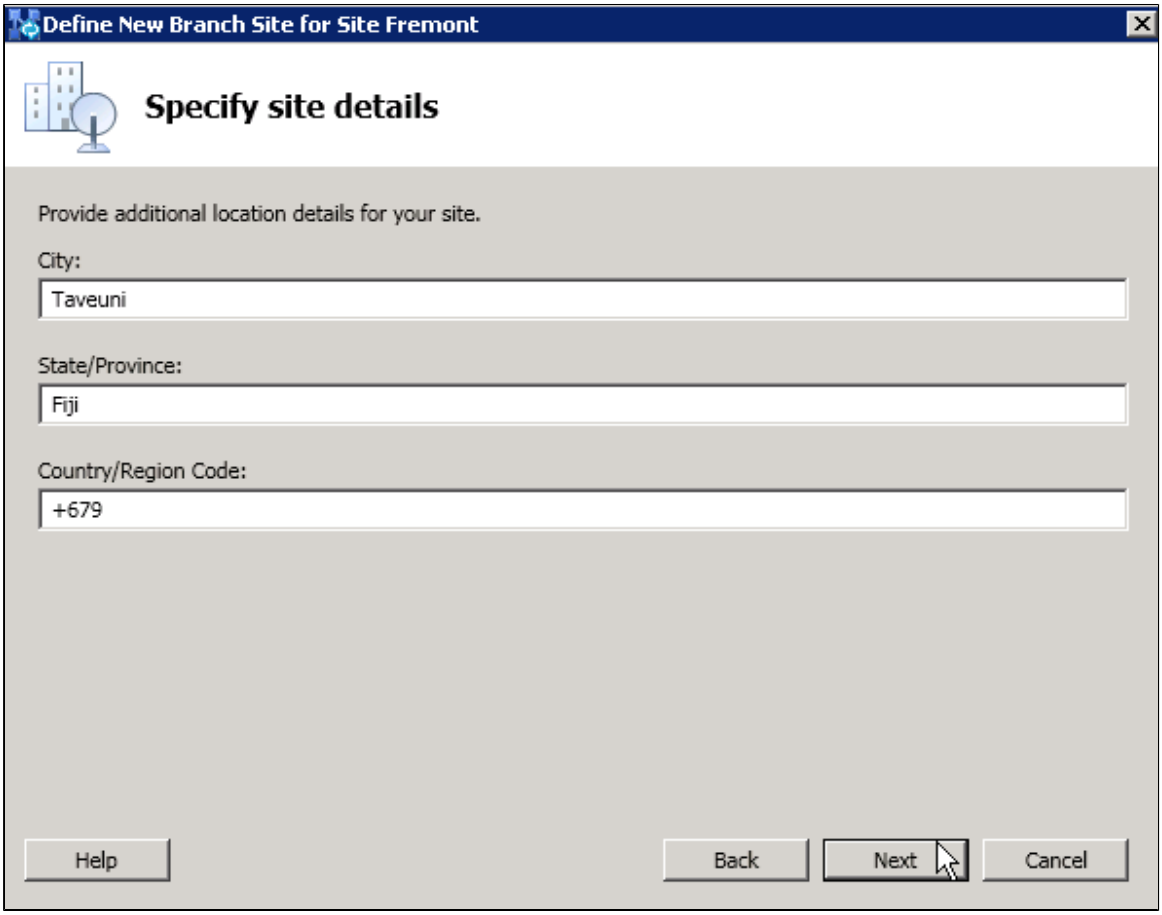
2. **Enter the remote site identity**

Copyright © 2015 Sonus Networks. All rights reserved.



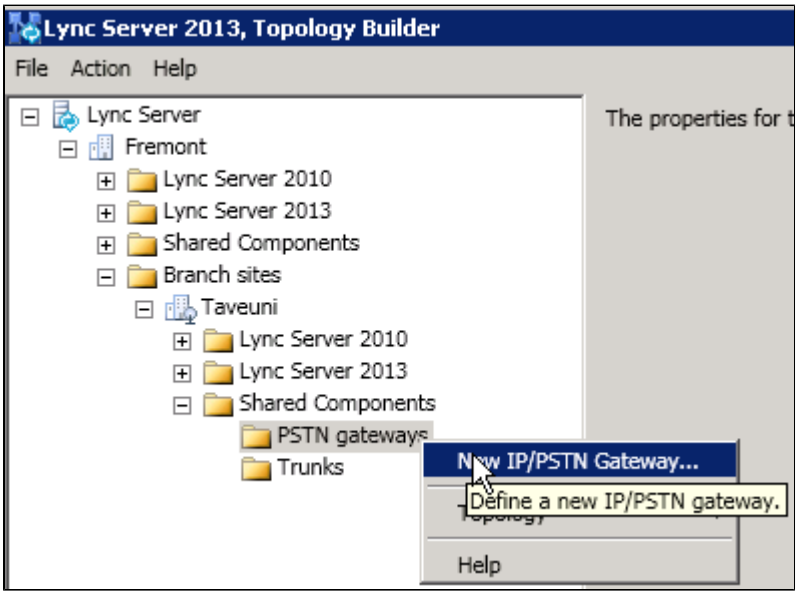
3. Configure the site details

Copyright © 2015 Sonus Networks. All rights reserved.

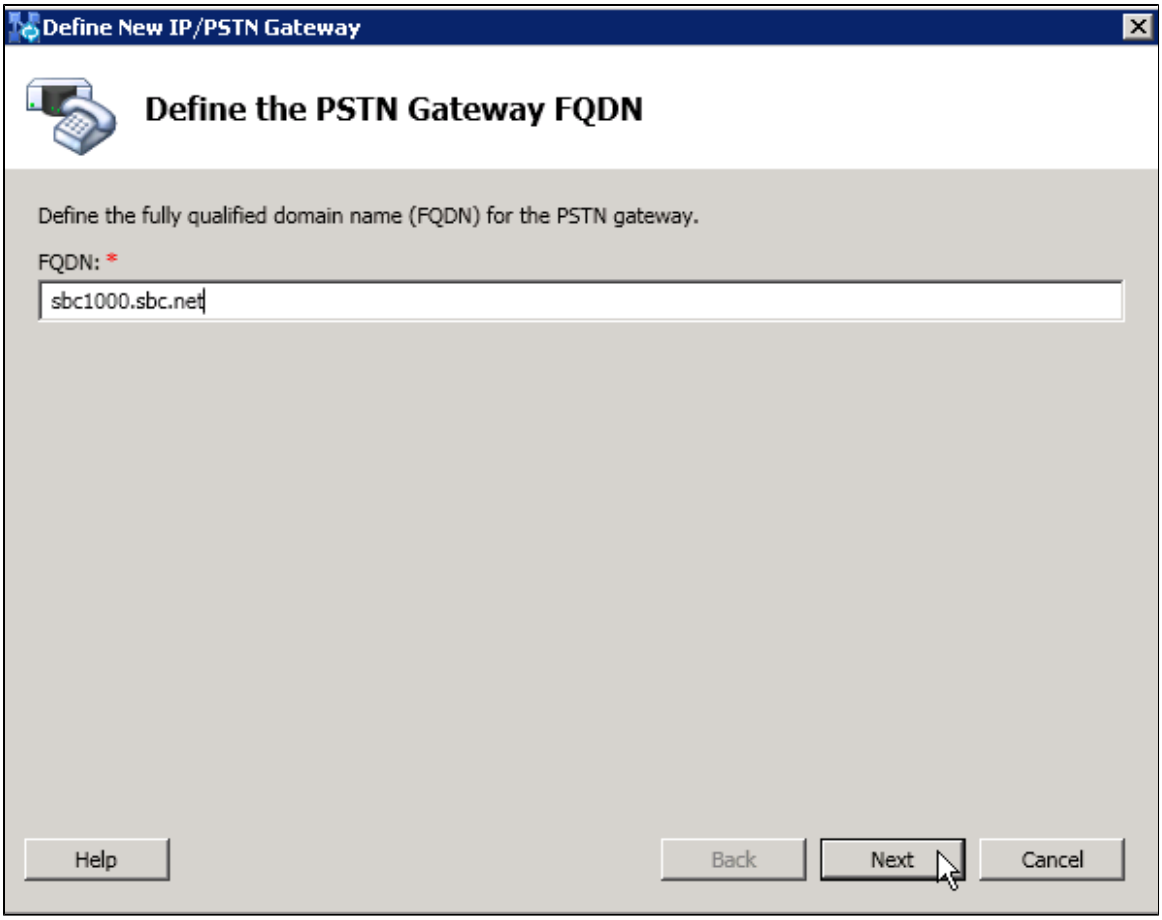


New PSTN Gateway

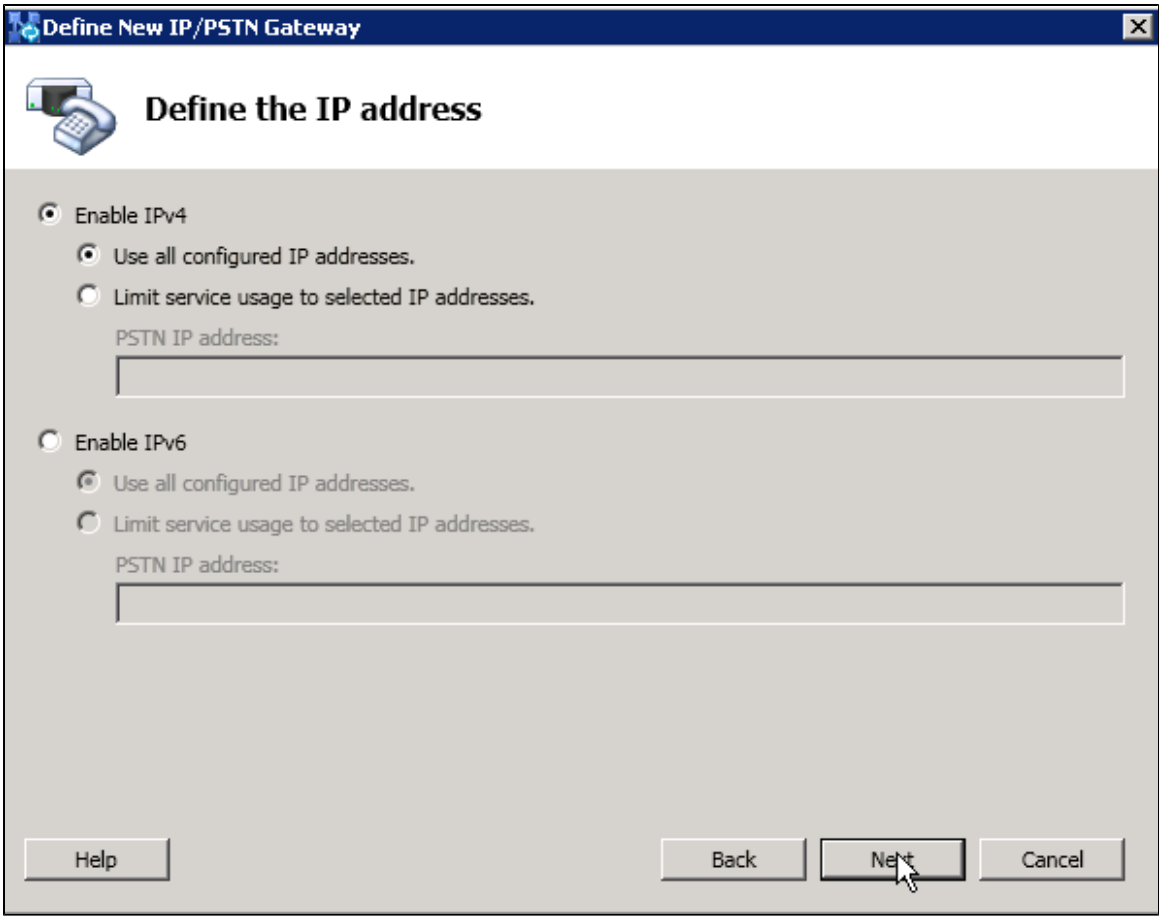
Add *sbc1000.sbc.net* as Taveuni's PSTN Gateway.



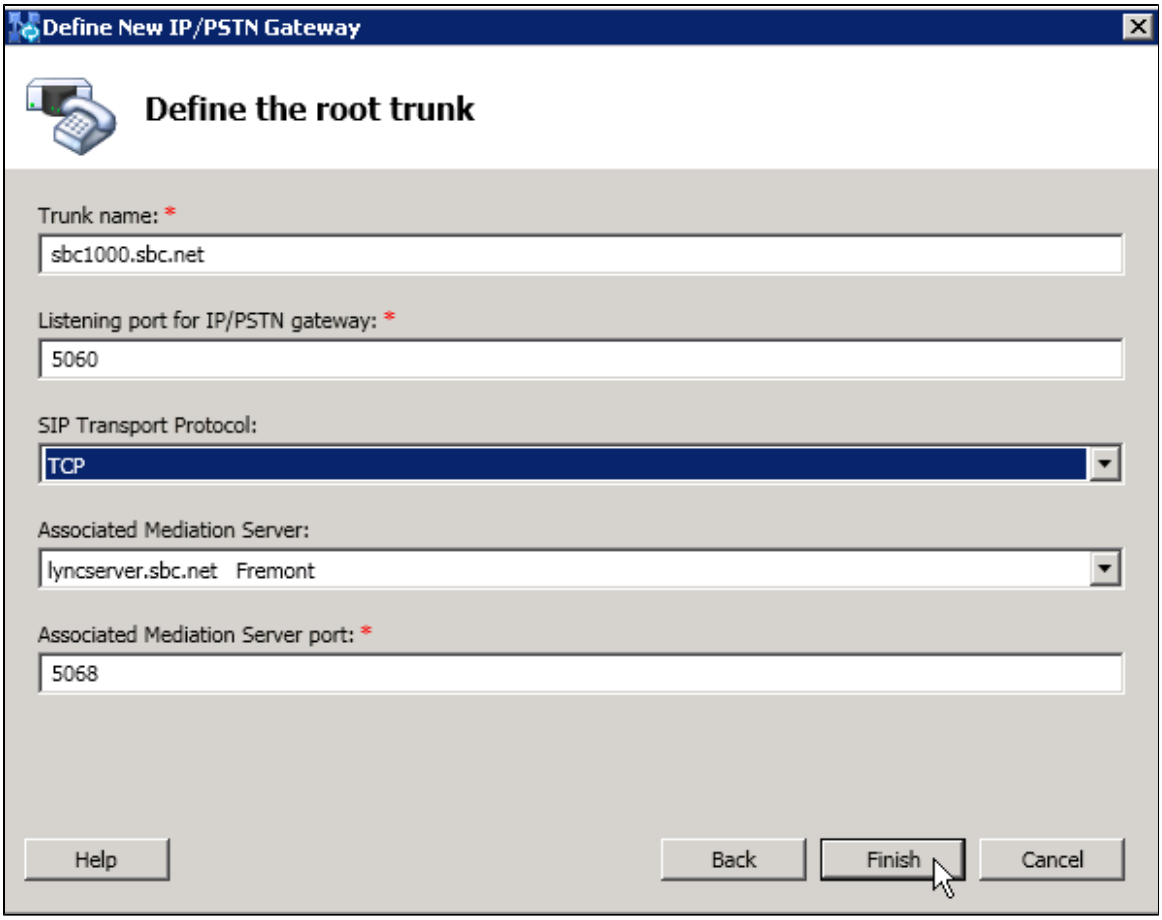
Copyright © 2015 Sonus Networks. All rights reserved.



Copyright © 2015 Sonus Networks. All rights reserved.



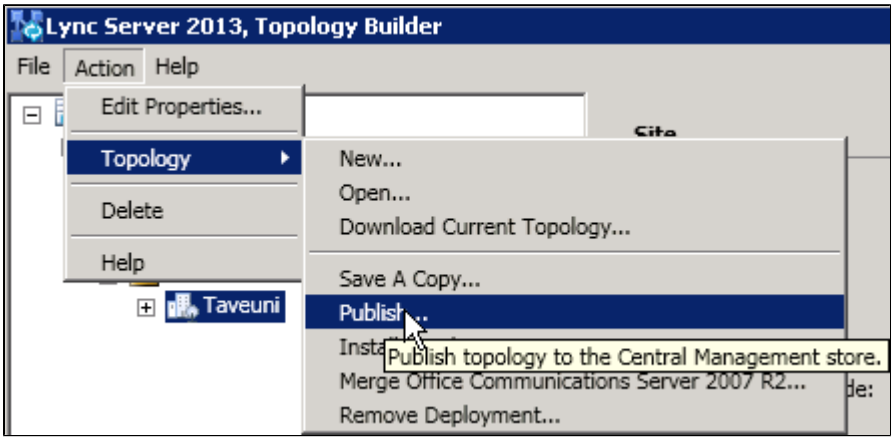
Copyright © 2015 Sonus Networks. All rights reserved.



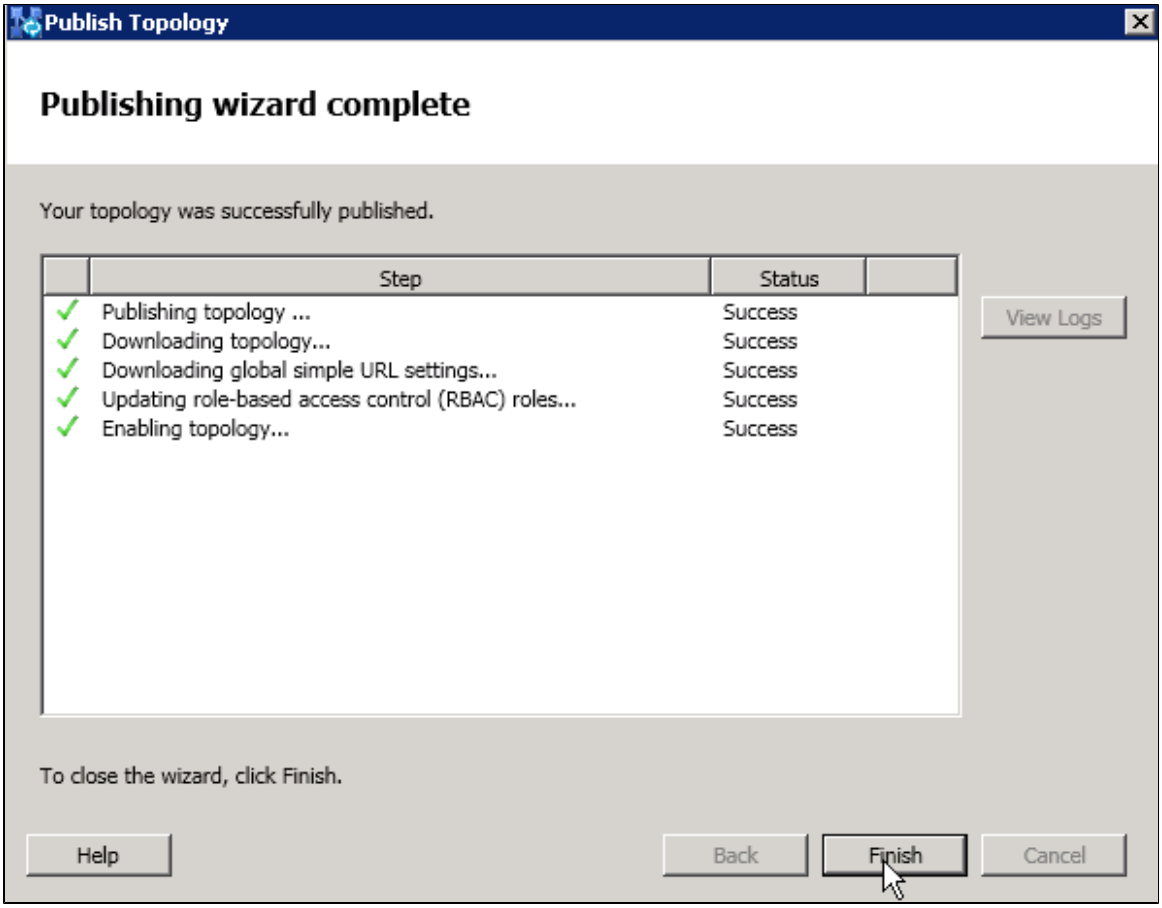
The RBA function requires media bypass, which, in turn requires TLS/SRTP. Later this document, the remote PSTN gateway will be re-configured from TCP/RTP to TLS/SRTP. Employing the simplier TCP/RTP model will help ease the implementation by providing a phased approach to the implementation.

Publish

Finally, Publish the newly configured topology.



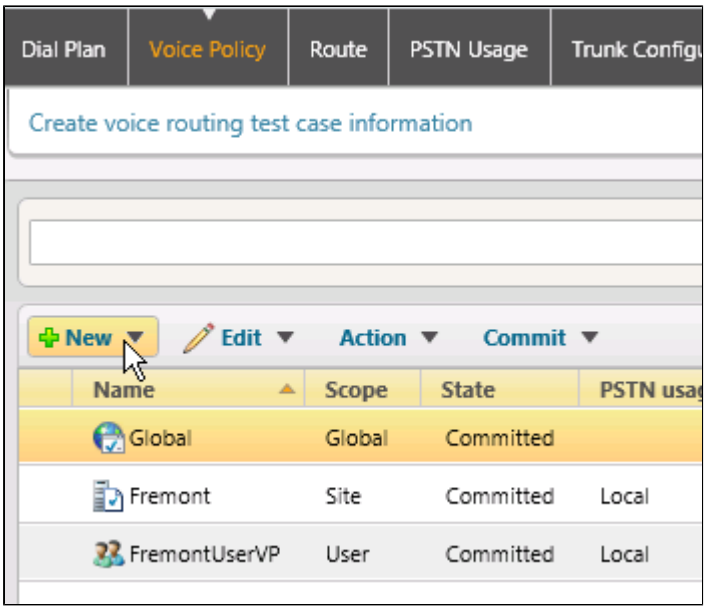
Copyright © 2015 Sonus Networks. All rights reserved.



Lync Server Configuration

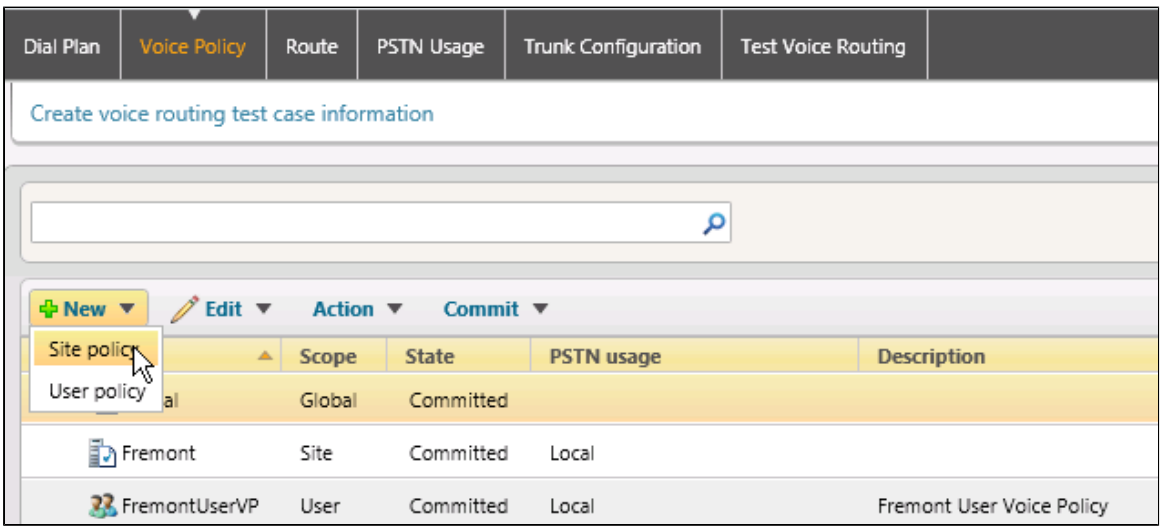
Create a new Site Voice Policy

1. Click *New*

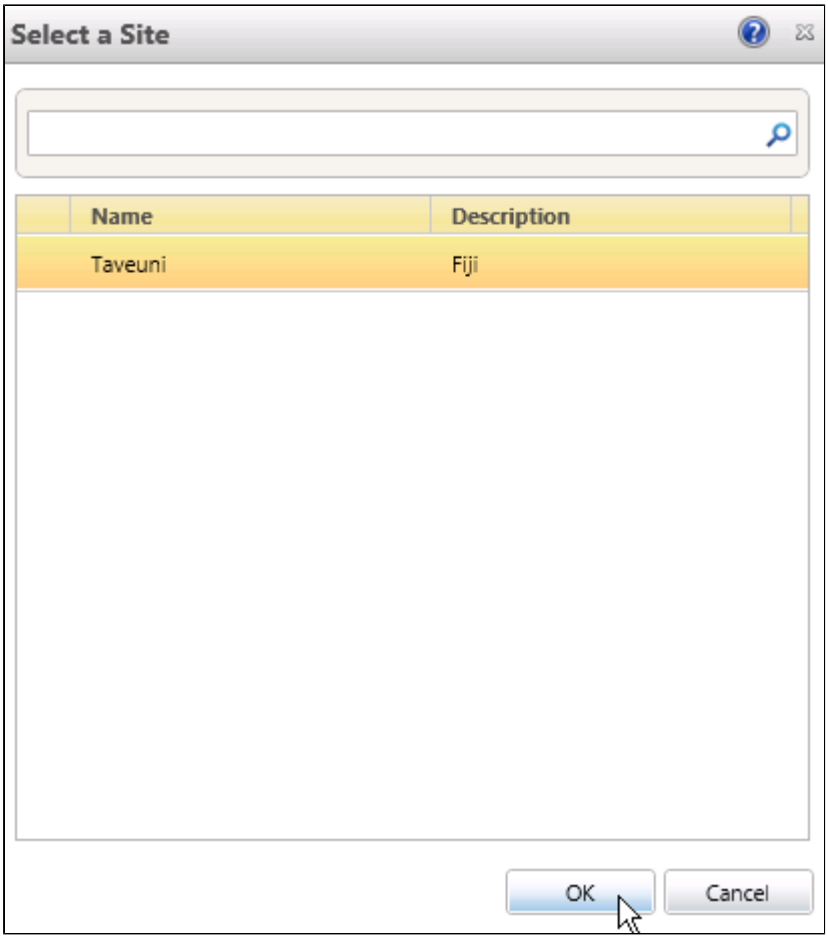


Copyright © 2015 Sonus Networks. All rights reserved.

2. Add a *Site Policy*

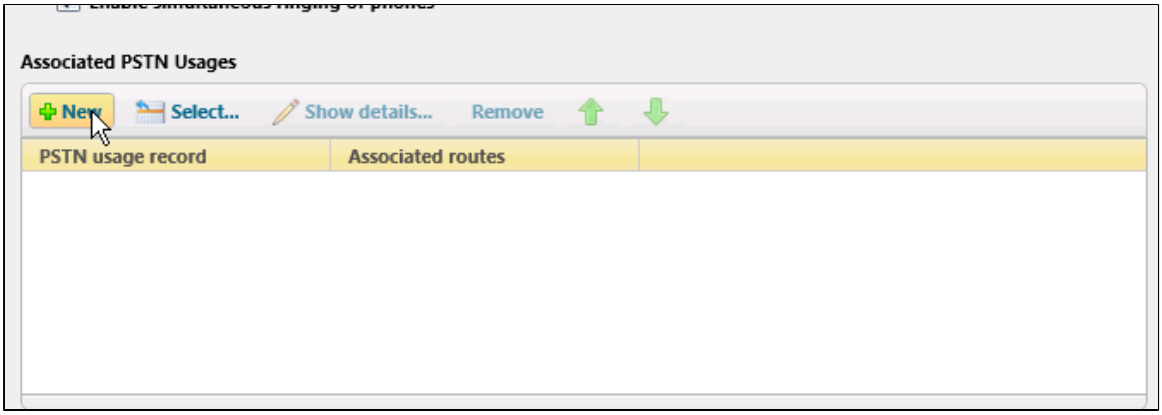


3. Select the remote site you just added to the Lync topology.

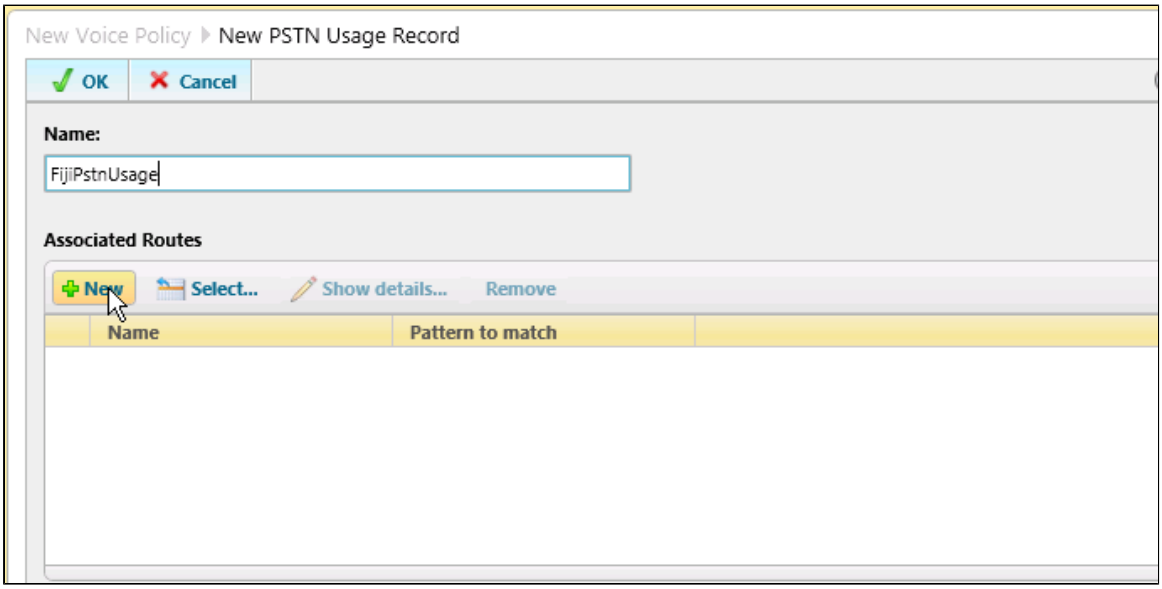


4. Add a new PSTN Usage

Copyright © 2015 Sonus Networks. All rights reserved.

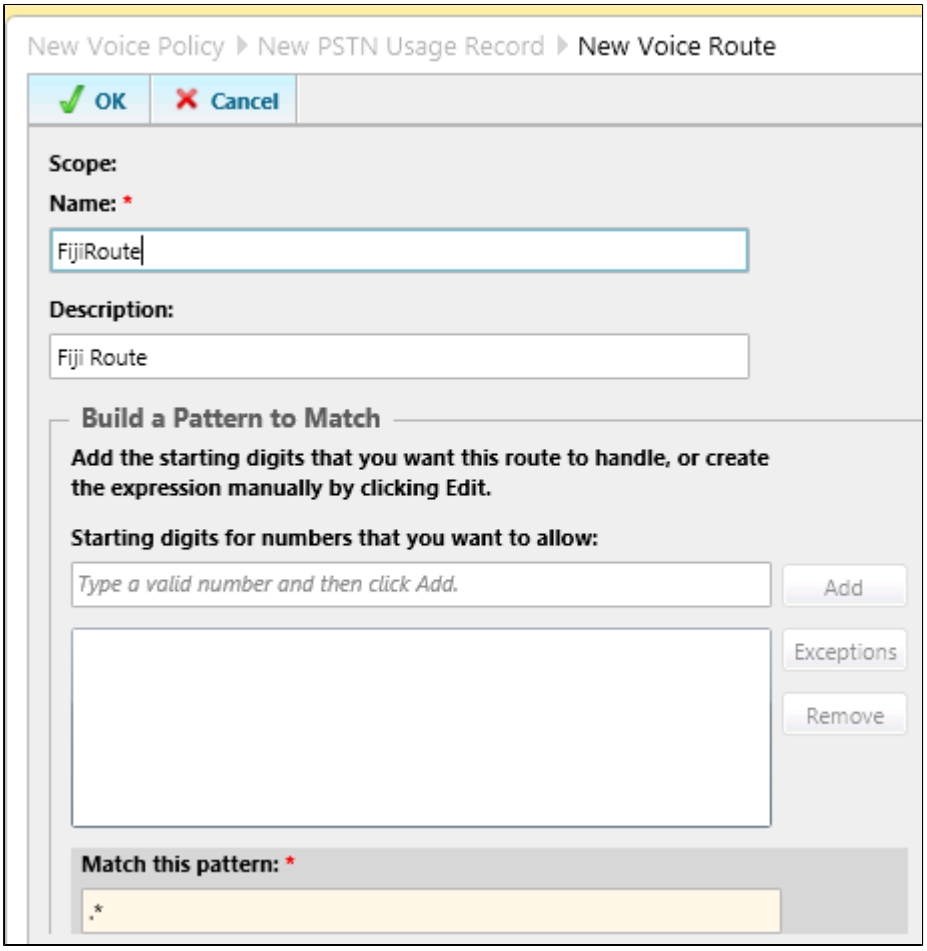


5. Supply a Name and Add a Route

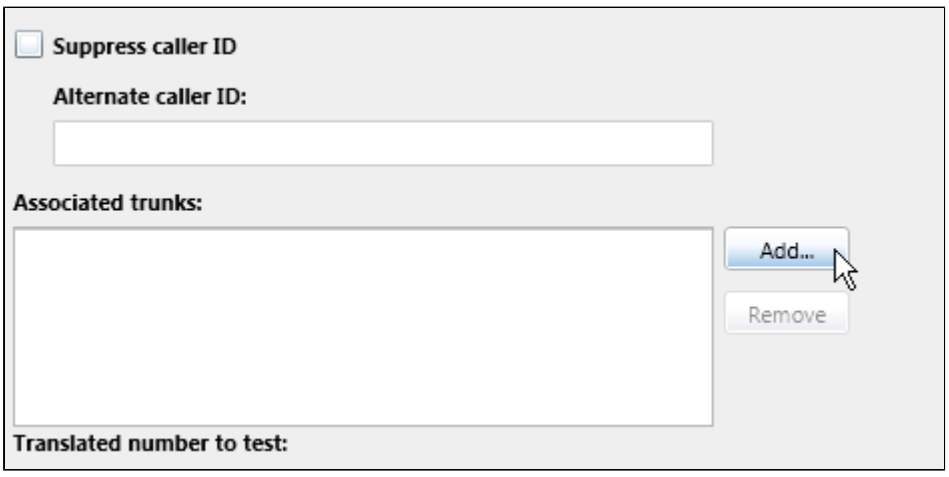


6. Configure a call route pattern

Copyright © 2015 Sonus Networks. All rights reserved.

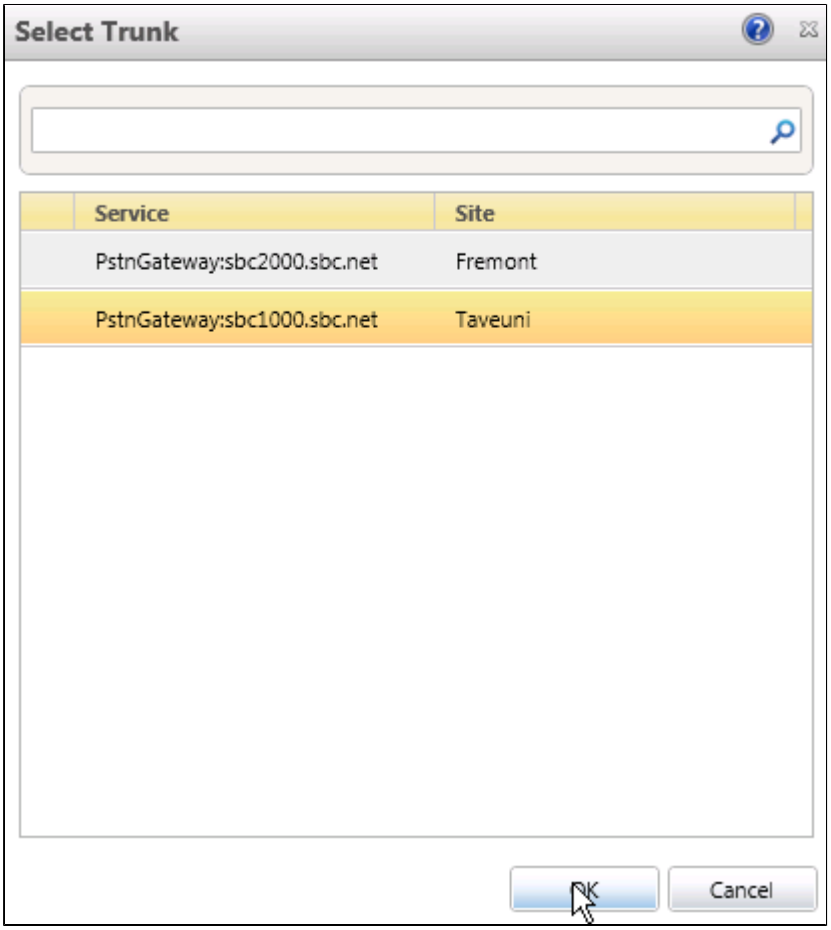


7. Add a Trunk



8. Choose the newly added remote-network SBC

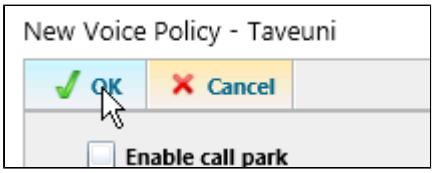
Copyright © 2015 Sonus Networks. All rights reserved.



9. Click *OK*at each of the configuration layers





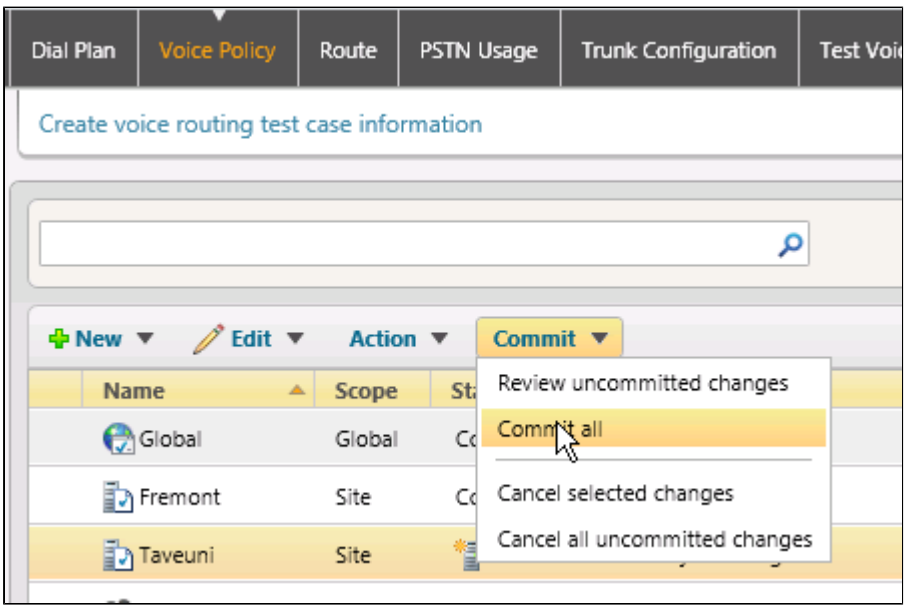


Commit New Site Voice Policy

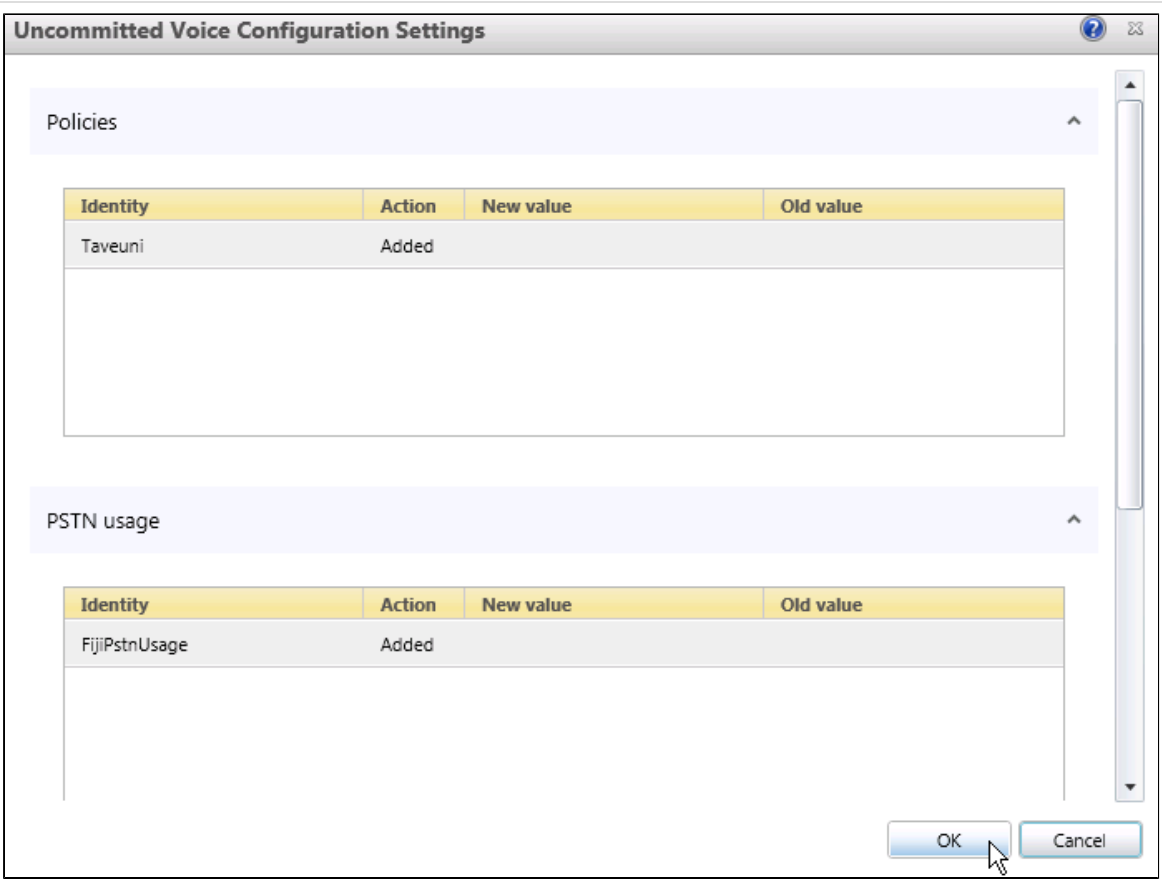
Commit the changes to the Voice Policy

Copyright © 2015 Sonus Networks. All rights reserved.

1. Click the *Commit* pulldown and *Commit All*



2. Click *OK*

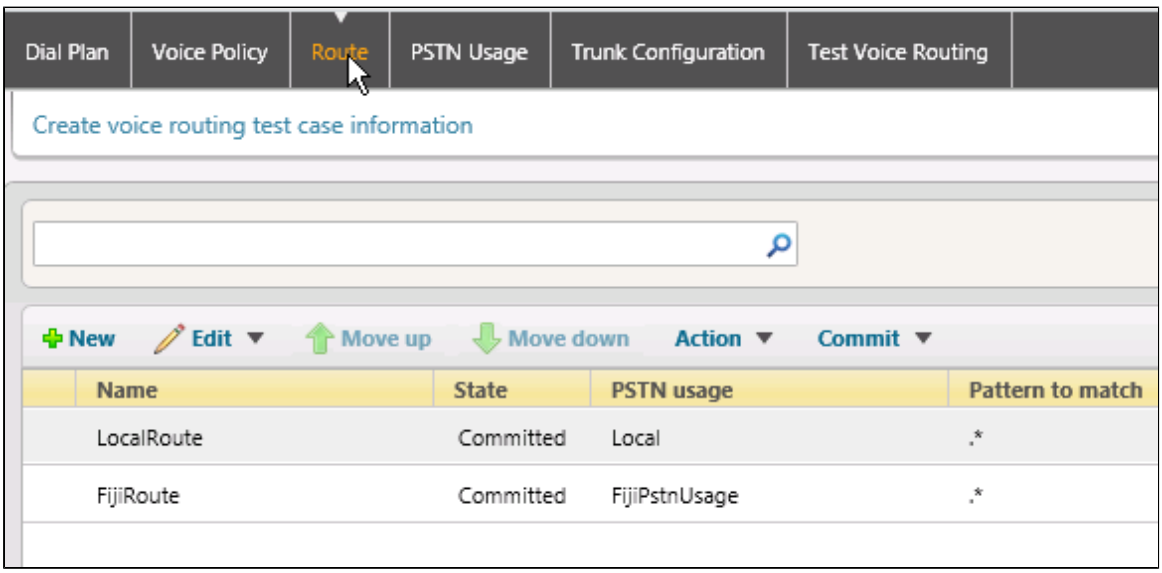


Verify Route and PSTN Usage

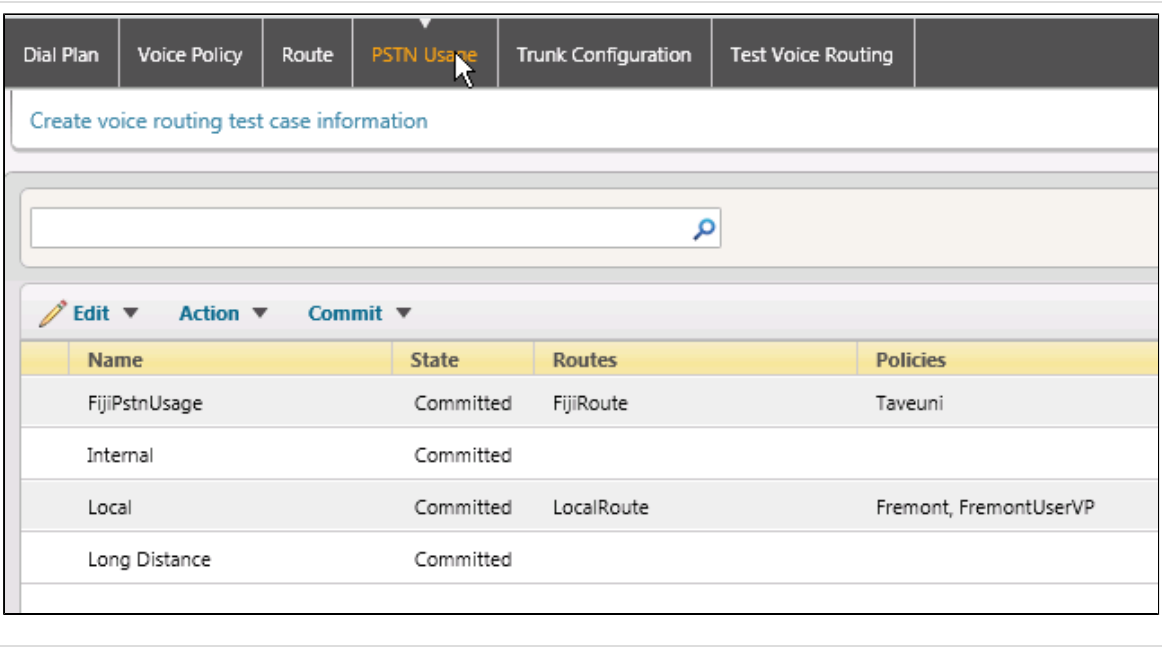
Verify the Route and PSTN Usages were added properly in the previous steps.

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the top navigation bar, click *Route*. Ensure that the route was added.



2. In the top navigation bar, click *PSTN Usage*. Ensure that the PSTN Usage was added.

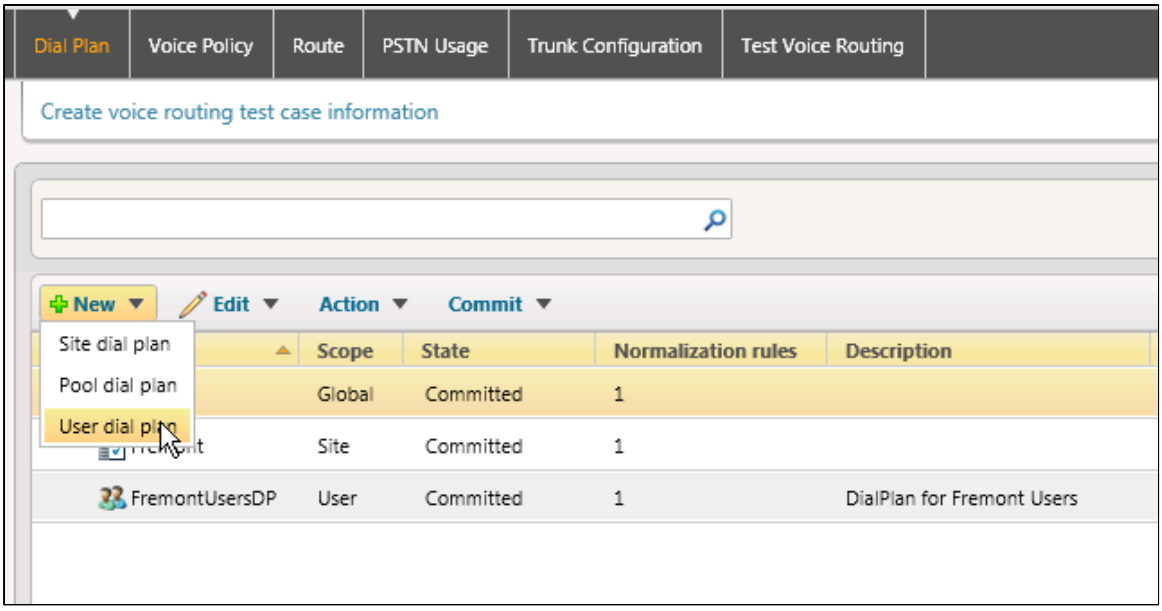


Create a User New Dial Plan

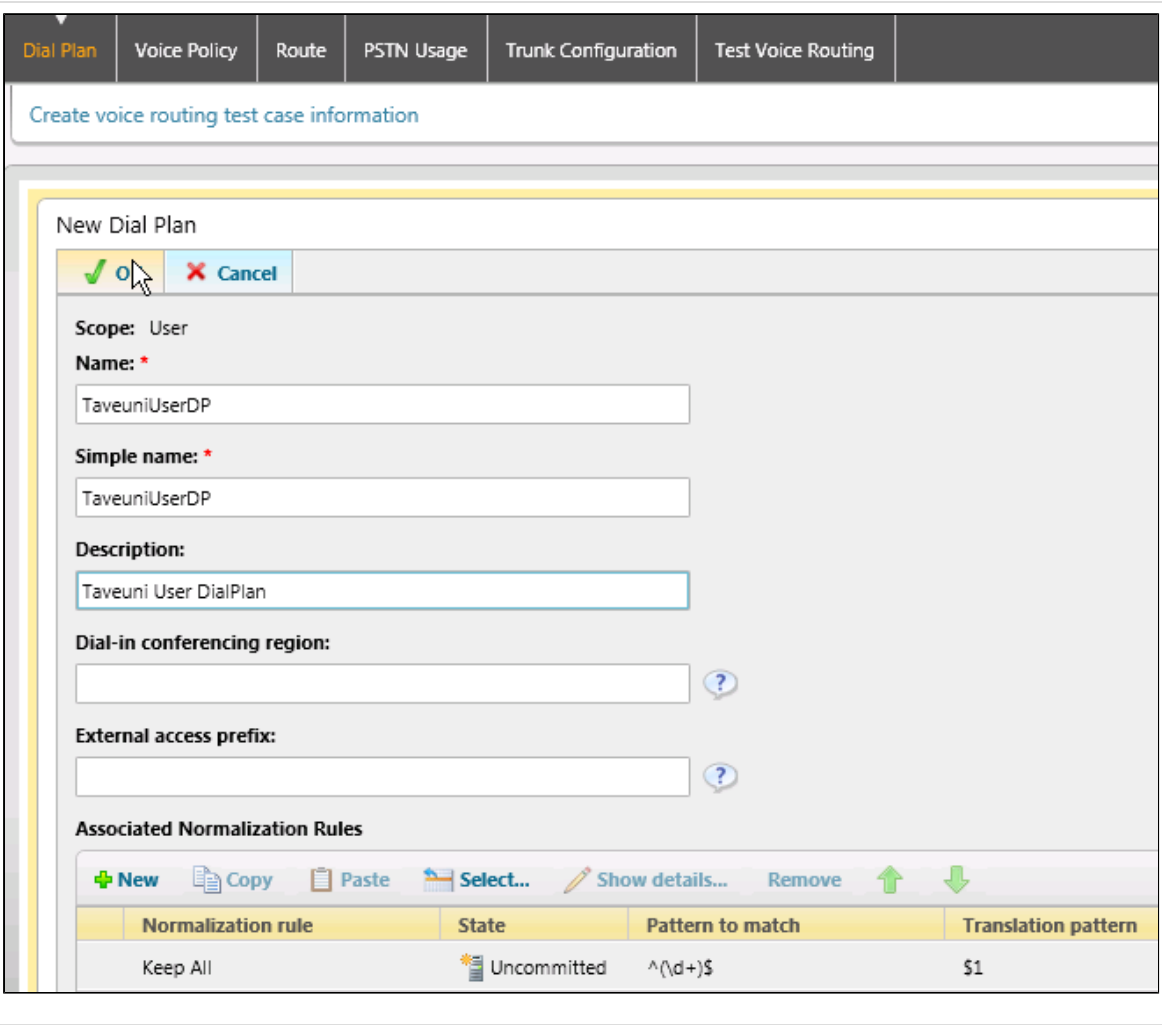
Similar to the previous steps, the following configuration adds User templates as opposed to Site templates.
To enable the RBA function, Lync users will have User-level Dial Plans and Voice Policies. The next steps create those policies.

1. Click *Dial Plan* in the top navigation. Click *New_and select _New User Plan*.

Copyright © 2015 Sonus Networks. All rights reserved.



2. Enter the information for your site and click *OK*.

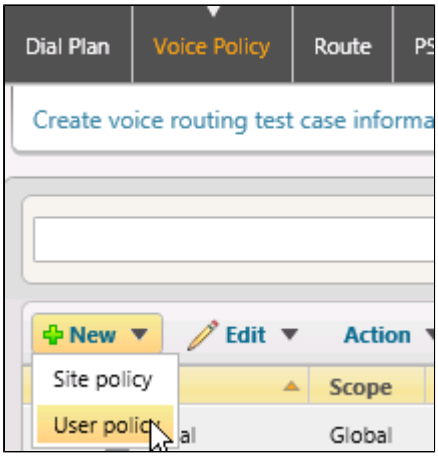


Create A New User Voice Policy

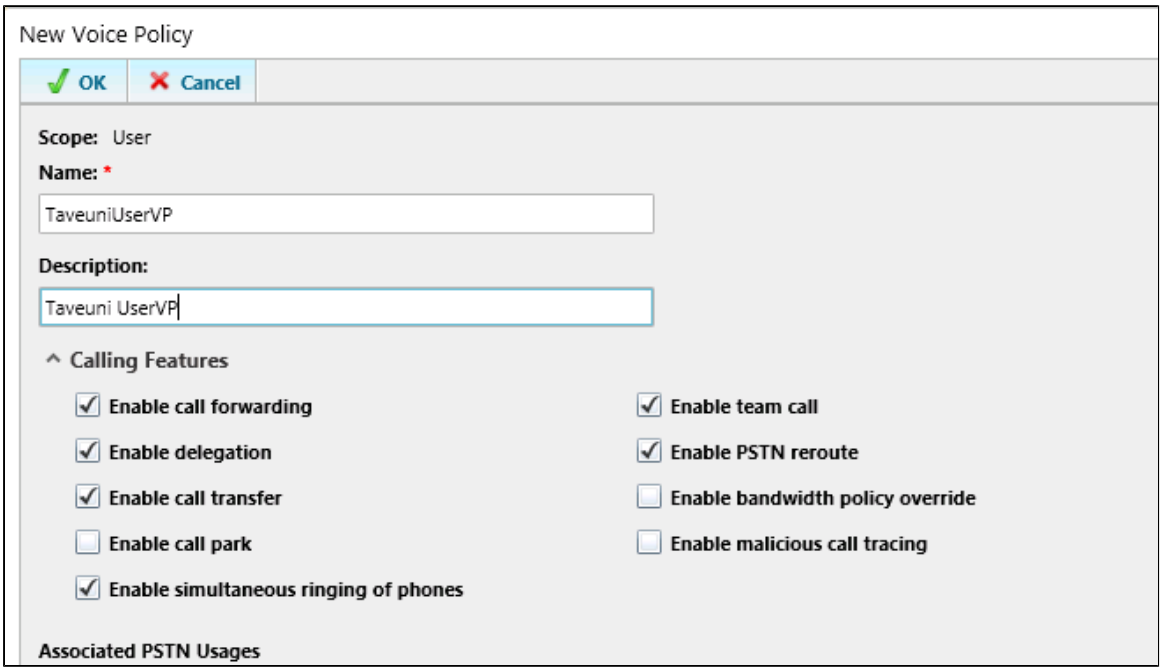
Copyright © 2015 Sonus Networks. All rights reserved.

Create the Voice Policy that will be used with for the remote-network users.

1. Click *Voice Policy* in the top navigation. Click *New* and select *User Policy*.

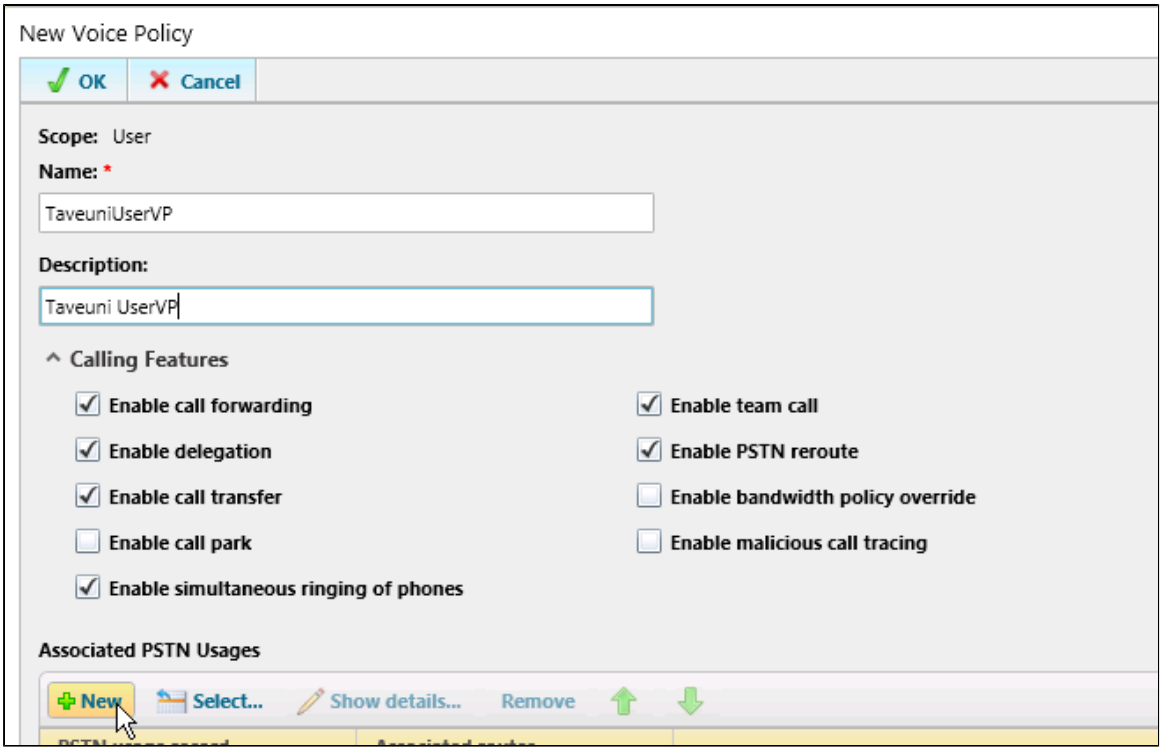


2. Fill in the form as shown using information for your particular installation.



3. Click *New* under *Associated PSTN Usages*.

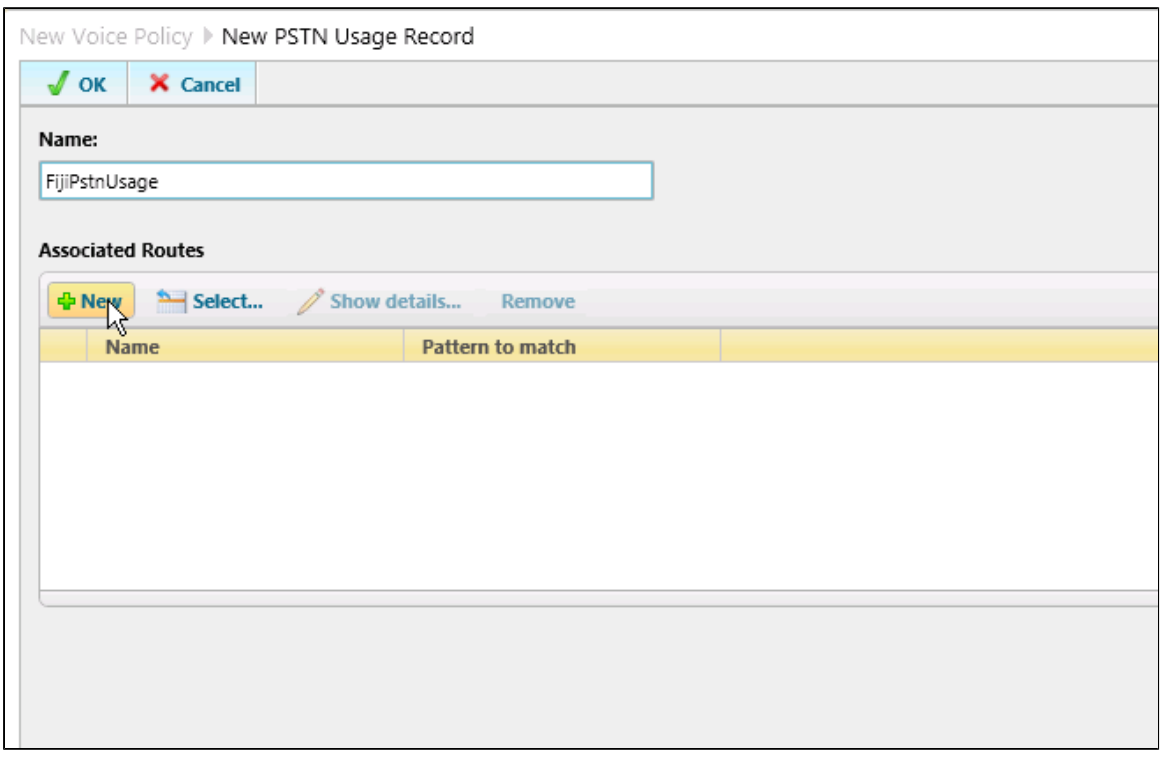
Copyright © 2015 Sonus Networks. All rights reserved.



Create a New PSTN Usage

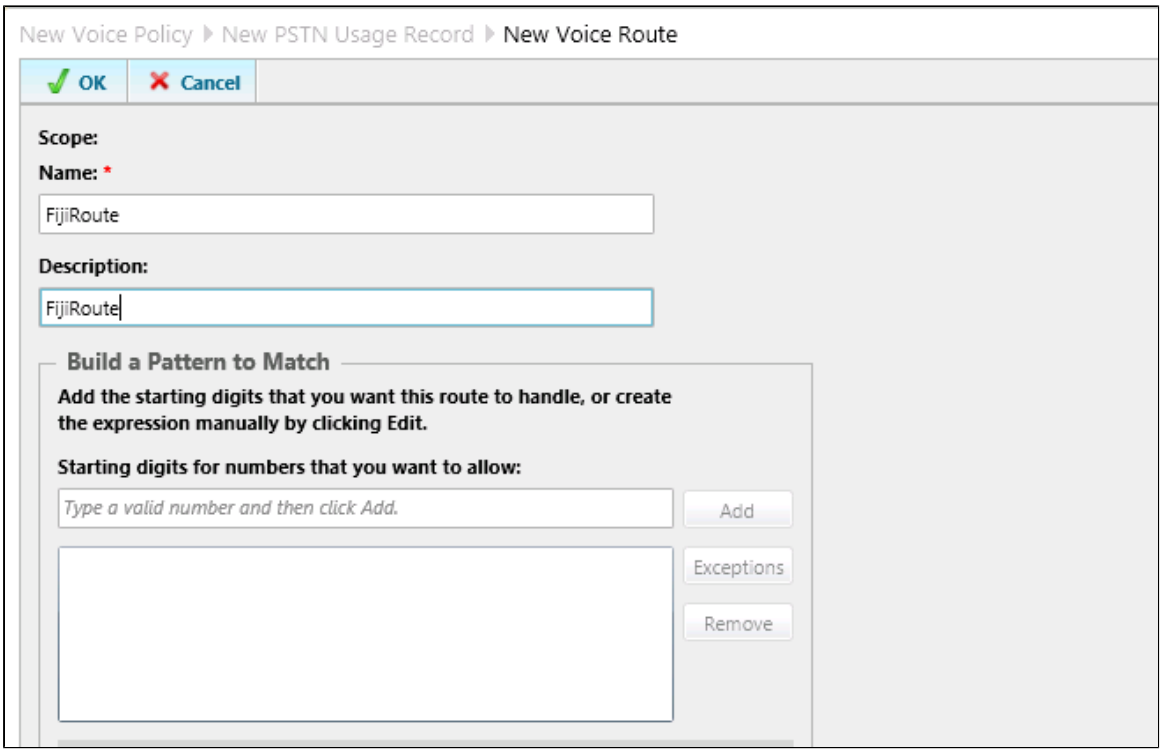
Create a PSTN Usage to be used with the User-level policies.

1. Create a New PSTN Usage record.

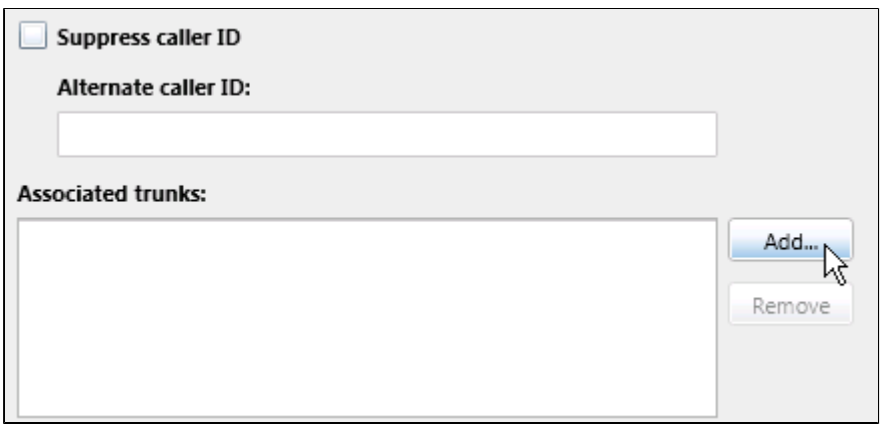


2. Enter your site-specific configuration information.

Copyright © 2015 Sonus Networks. All rights reserved.

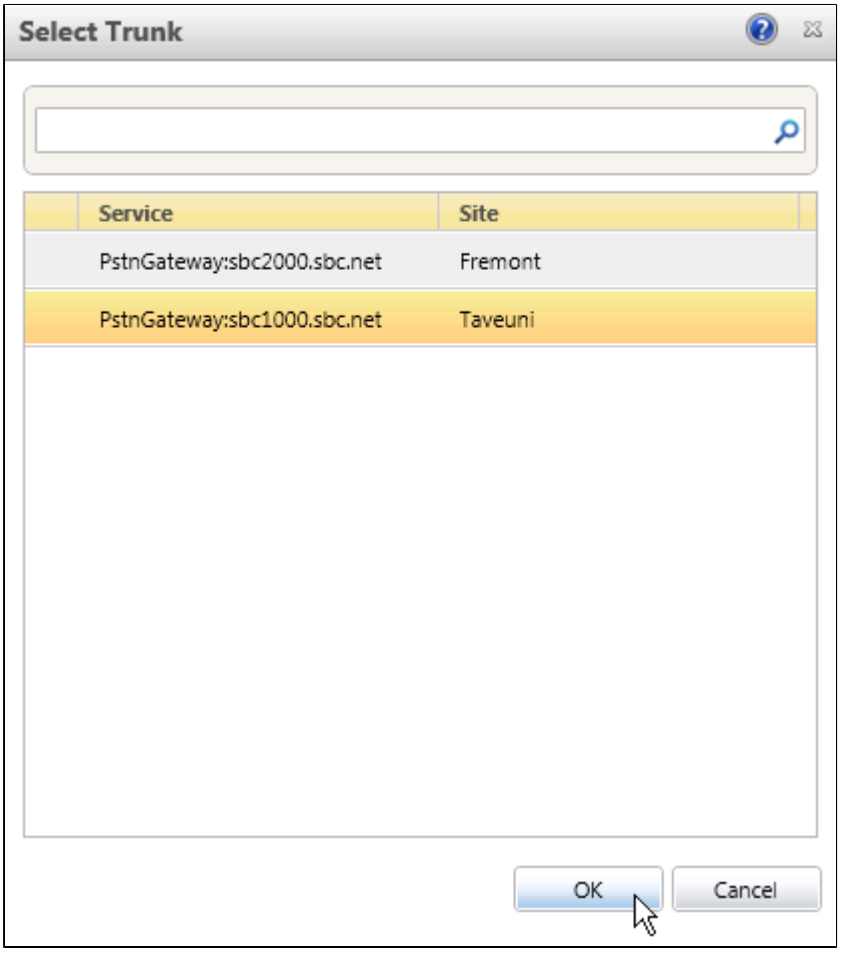


3. Click *Add* for *Associated Trunk*

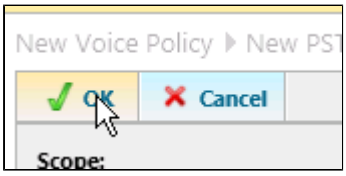


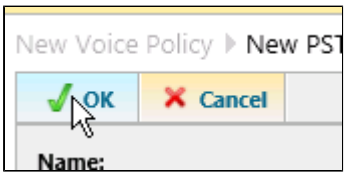
4. Select the remote-network SBC gateway

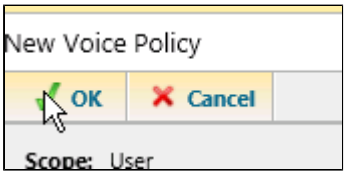
Copyright © 2015 Sonus Networks. All rights reserved.



5. Click *OK*for all the configuration layers.





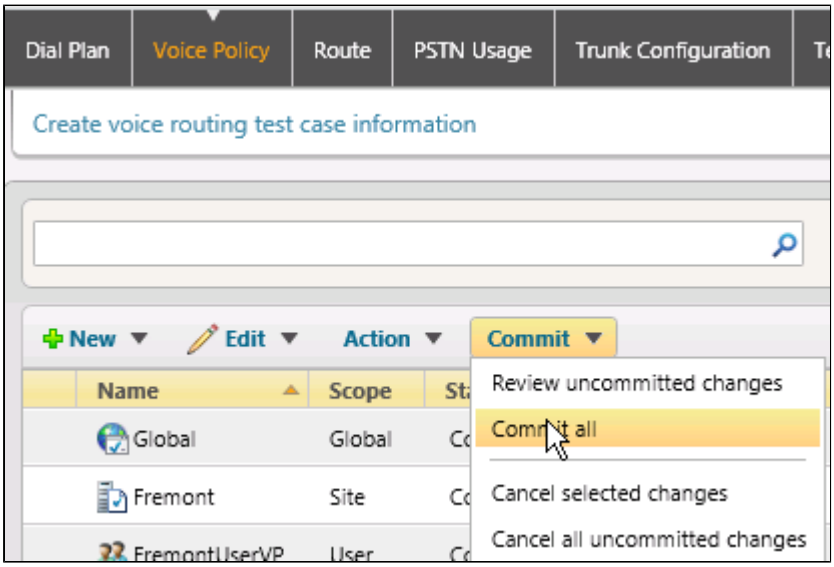


Commit Changes

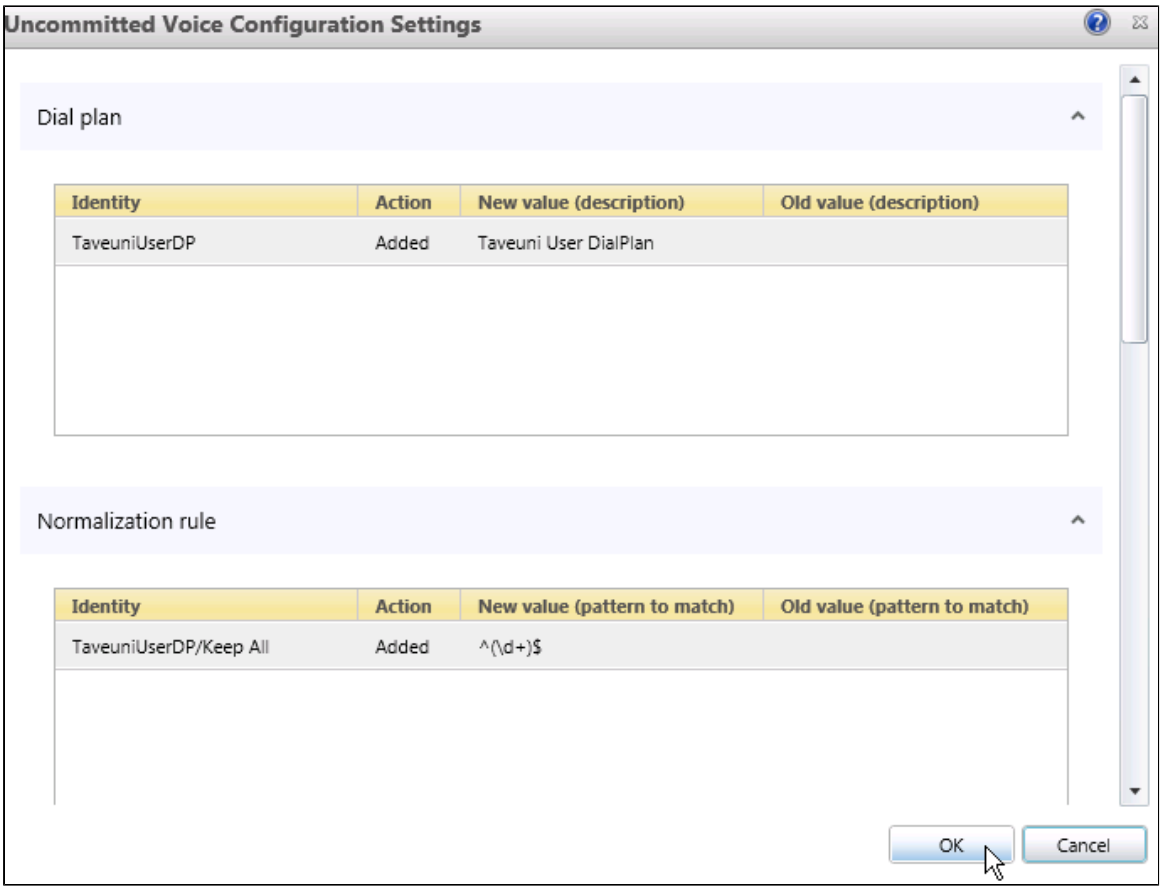
Commit the additions to your Lync configuration.

Copyright © 2015 Sonus Networks. All rights reserved.

1. Click the *Commit* pulldown, then select *Commit All*.

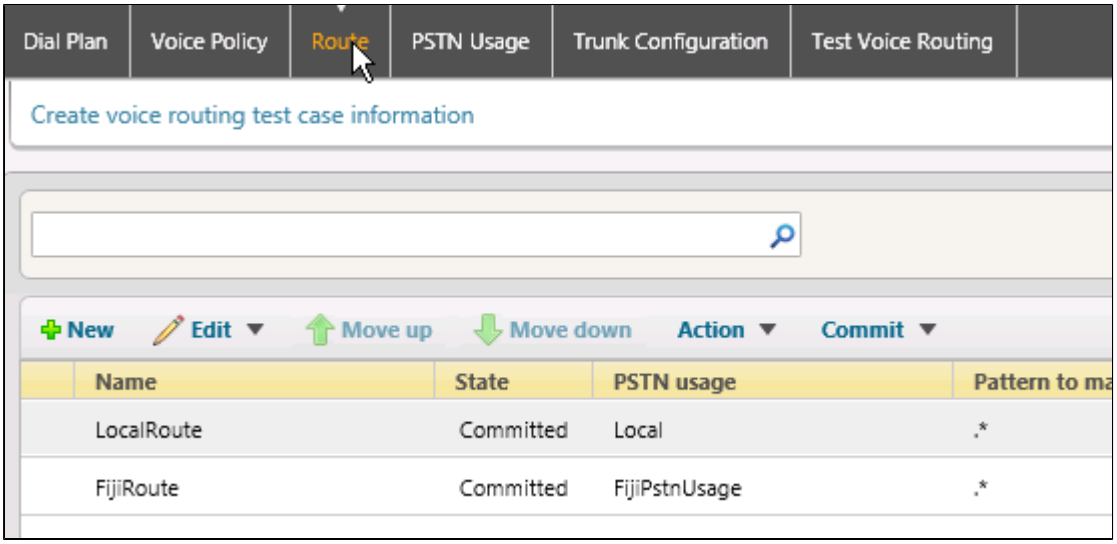


2. Click *OK*.

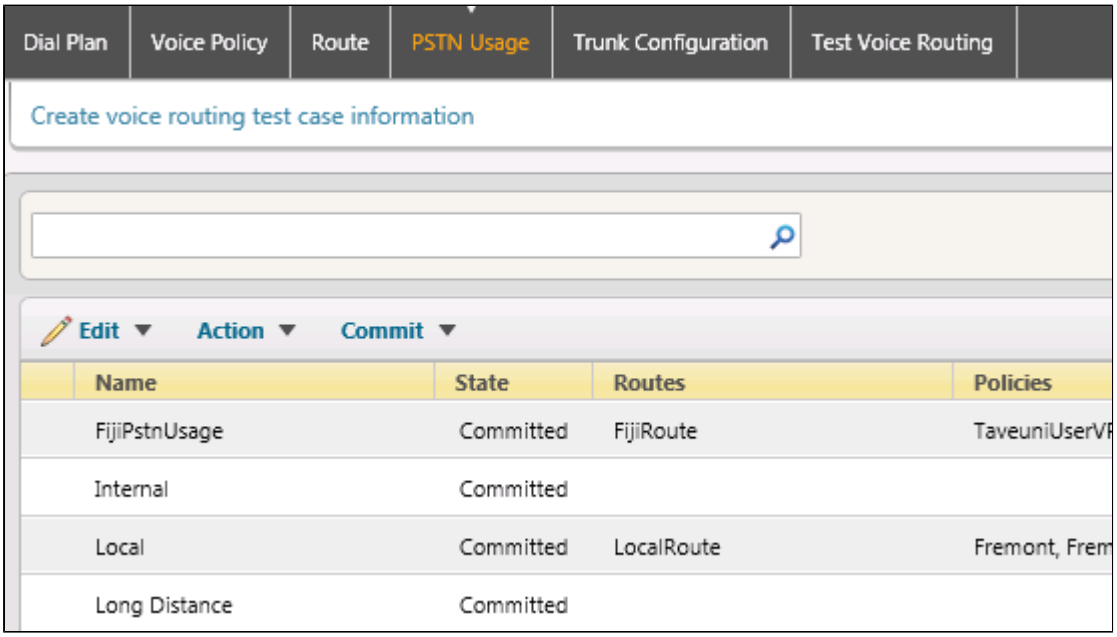


3. Verify the *Route*was added.

Copyright © 2015 Sonus Networks. All rights reserved.



4. Verify the *PSTN Usage*was added.

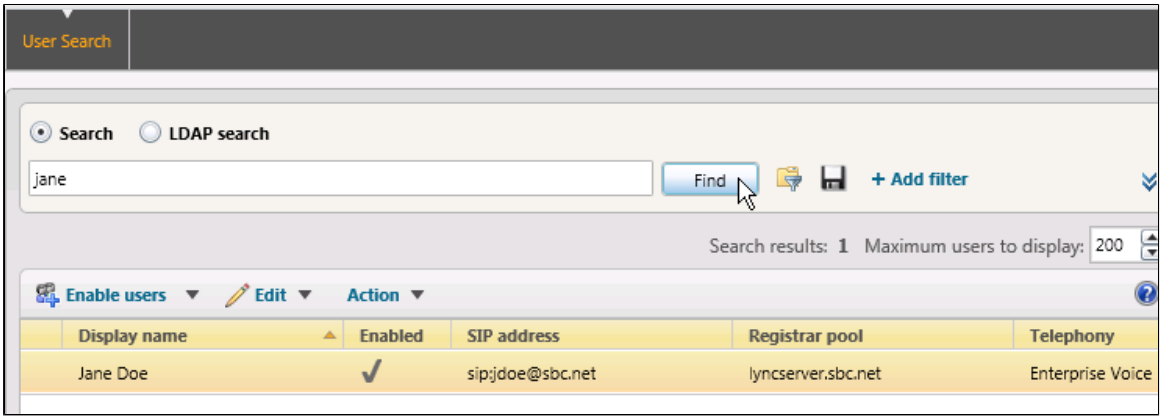


Add or Move a User into the new remote location

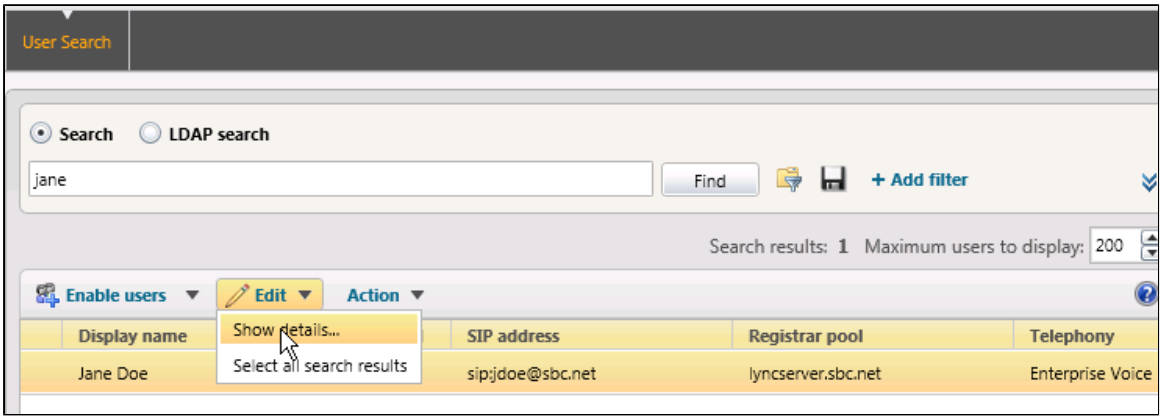
You will need to have a user homed to the remote-network location.

1. Click *Users* in the left-hand navigation. Enter the name of the user to move to the remote network and click *Find*.

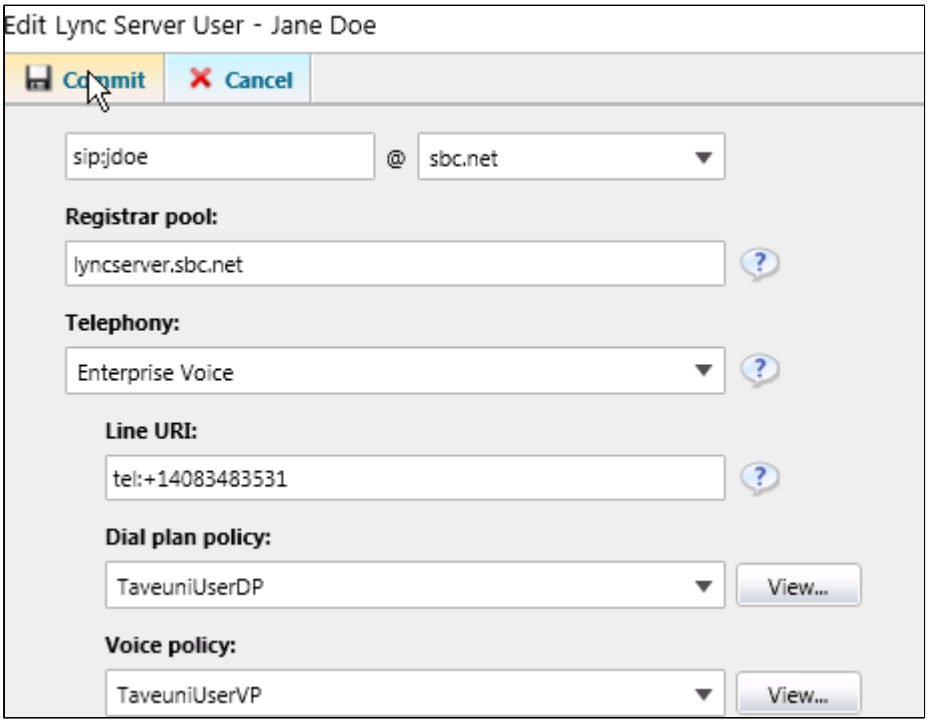
Copyright © 2015 Sonus Networks. All rights reserved.



2. In the *Edit* pulldown, select *Show Details*.



3. Set the Dial Plan and Voice Policy of the user to thos of the remote network **User**policies.

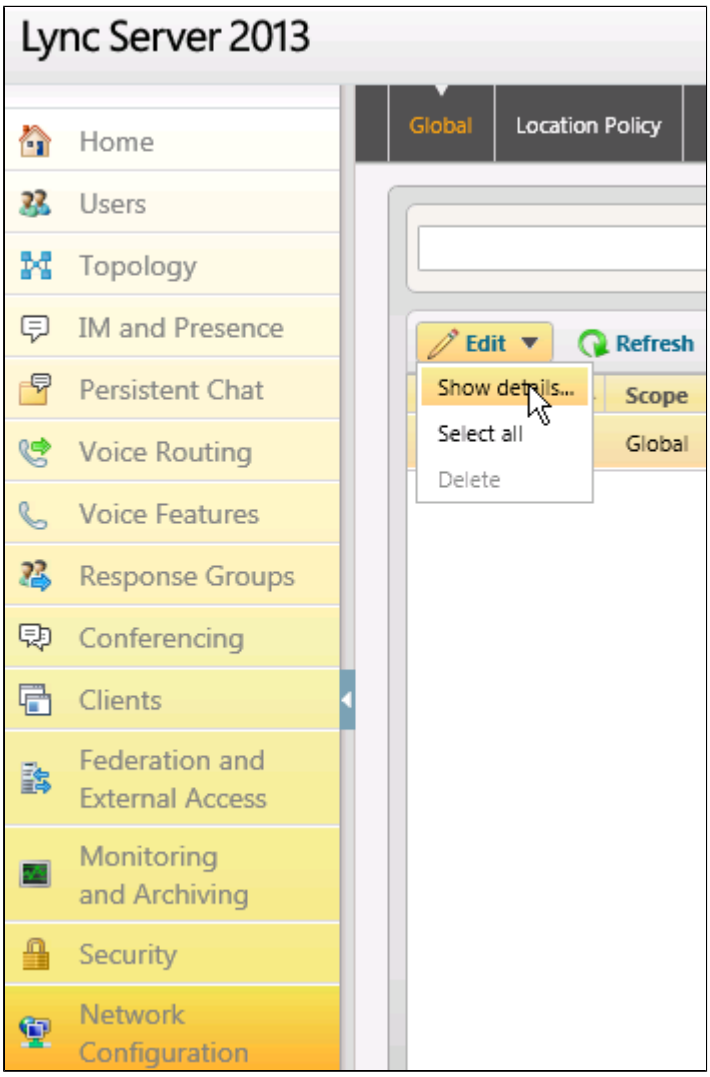


Copyright © 2015 Sonus Networks. All rights reserved.

Configure the Network Configuration

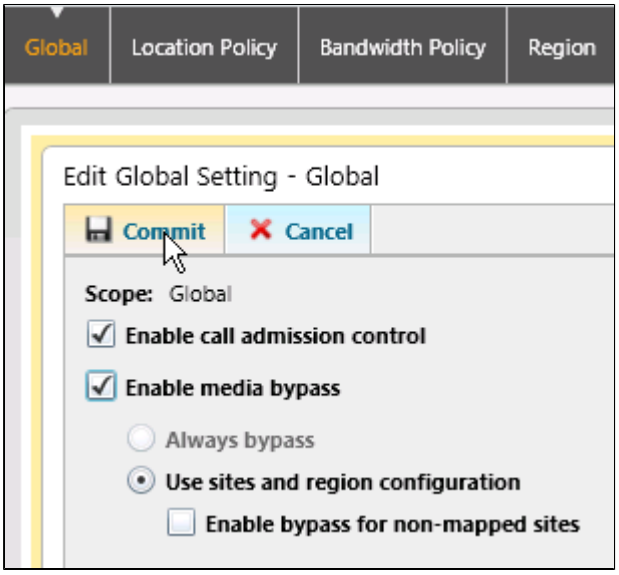
The Network Configuration controls how the CAC policies are applied. Follow the instructions to properly configure the Lync Network Configuration to interoperate with the RBA 3G4G link changes.

1. Click *Network Configuration* in the left-hand navigation. Click *Global* in the top navigation, click the *Edit* pulldown, and select *Show Details*.



2. Ensure that the CAC and Bypass options are selected. Change the settings and commit, if necessary.

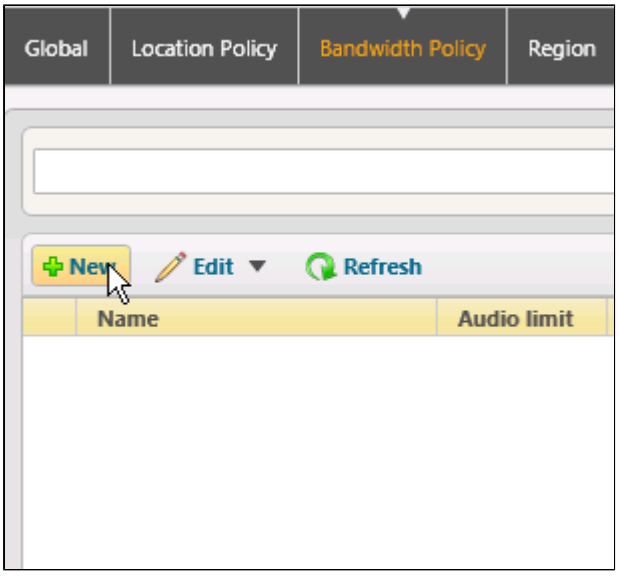
Copyright © 2015 Sonus Networks. All rights reserved.



Create a new Bandwidth Policy

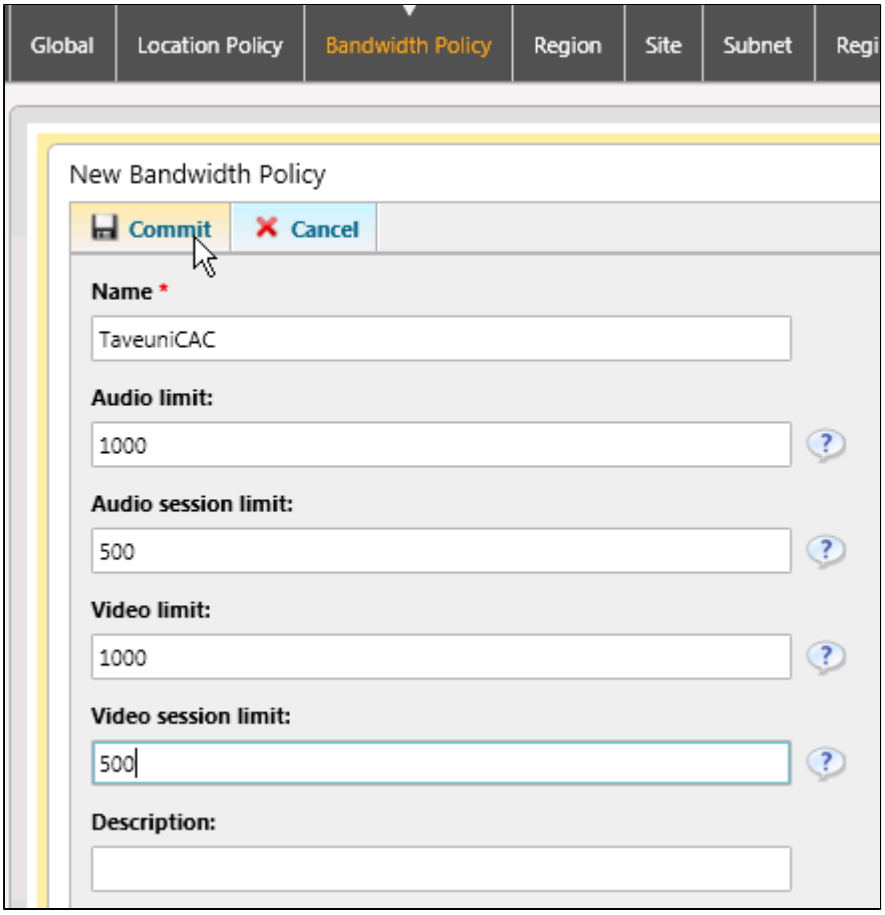
Create a Bandwidth Policy to be used to control the CAC from the RBA function.

1. Click *Bandwidth Policy* in the top navigation and select *New*.



2. Enter the bandwidth specification for your remote network link, then click *Commit*.

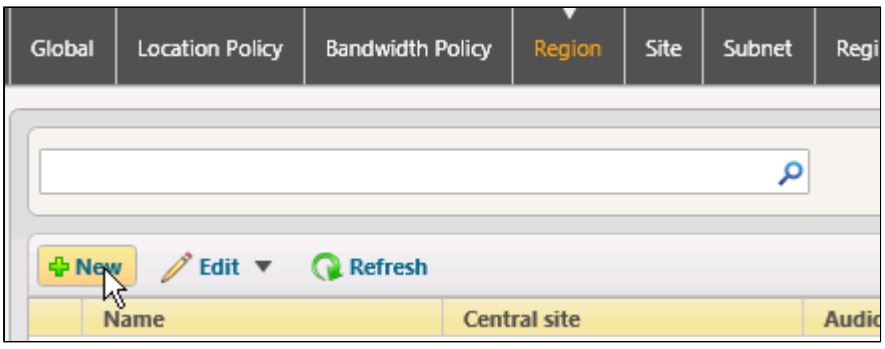
Copyright © 2015 Sonus Networks. All rights reserved.



Create a new Region

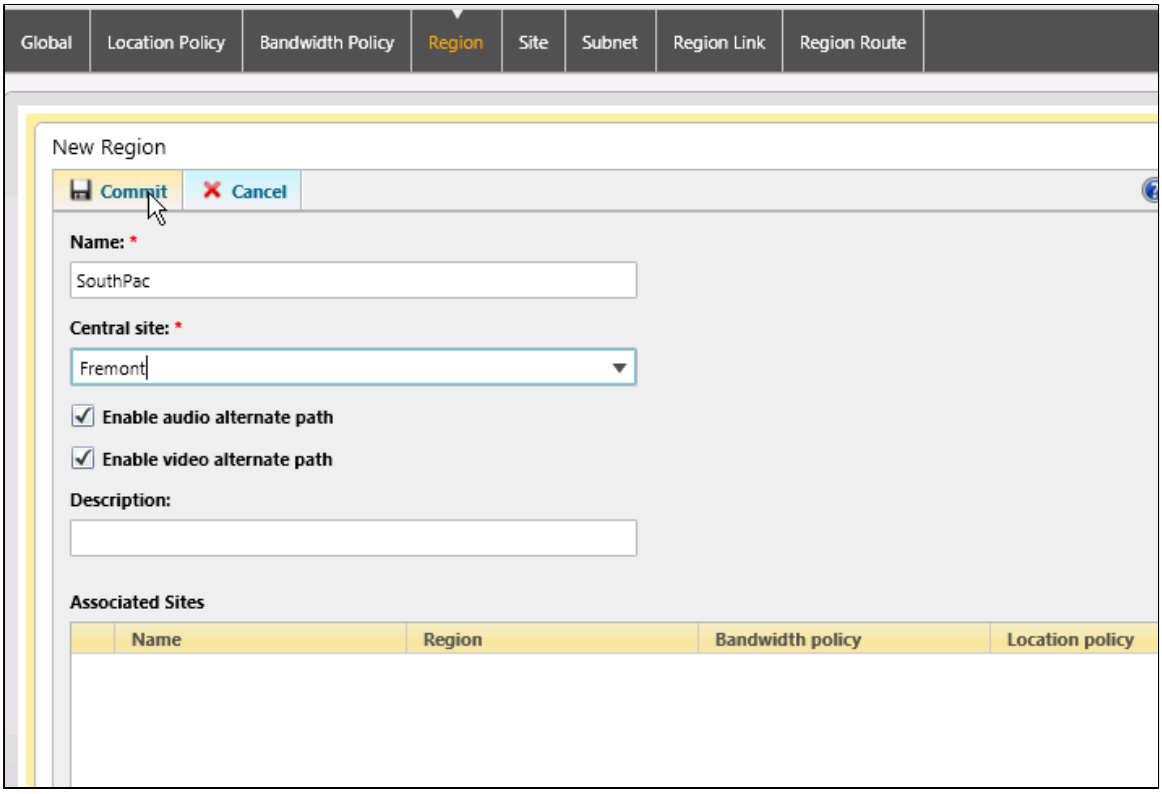
Create regions to be used with the RBA feature. There will be a region for the HQ, as well as the remote-network.

1. Click *Region* in the top navigation and select *New*.

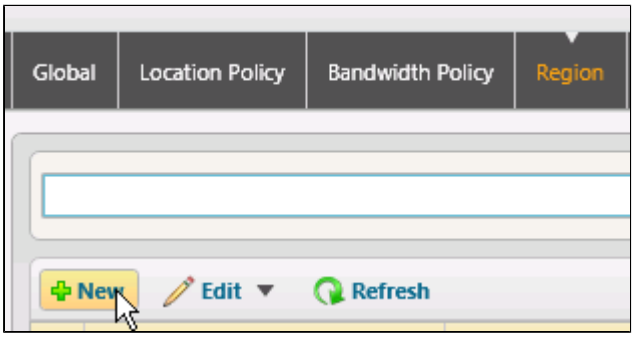


2. Add a record for the remote region and *Commit*.

Copyright © 2015 Sonus Networks. All rights reserved.

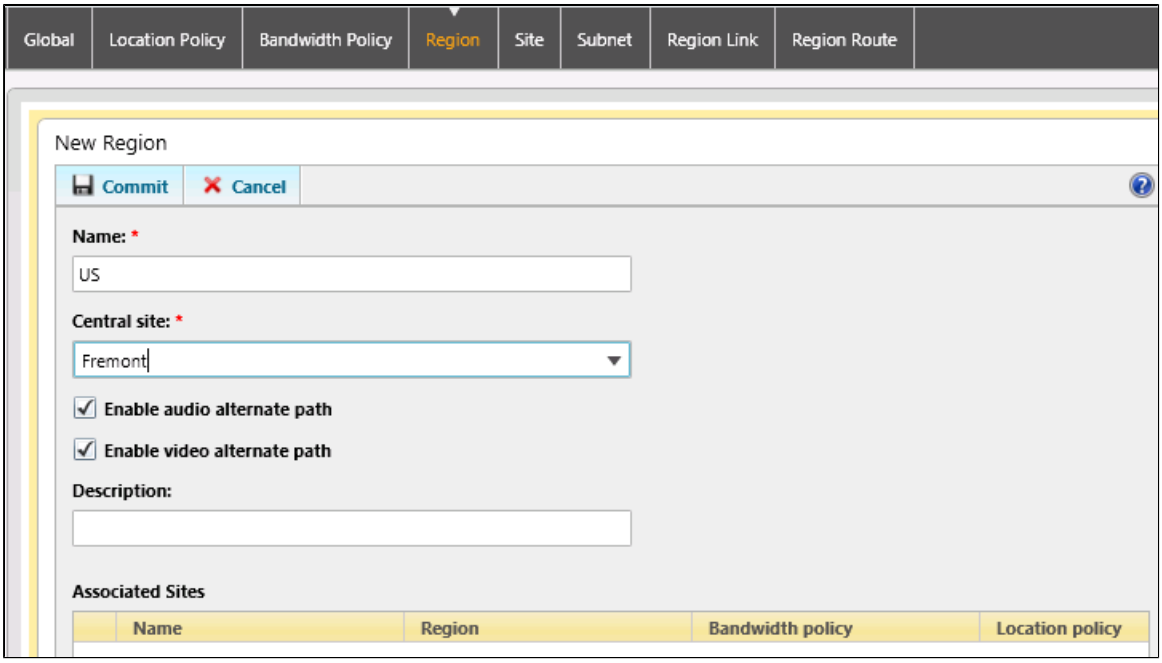


3. Click *New*to add the second region.



4. Add a record for the HQ site and *Commit*.

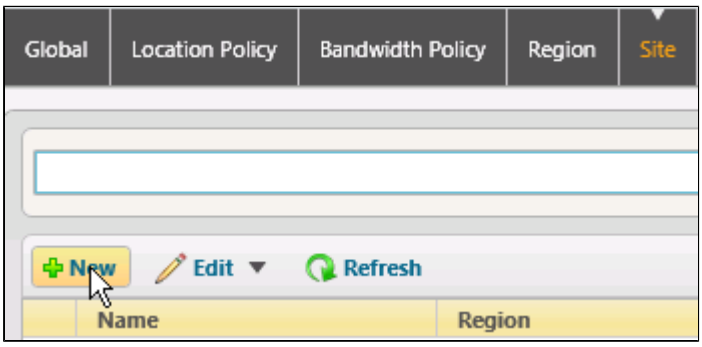
Copyright © 2015 Sonus Networks. All rights reserved.



Create a new Site

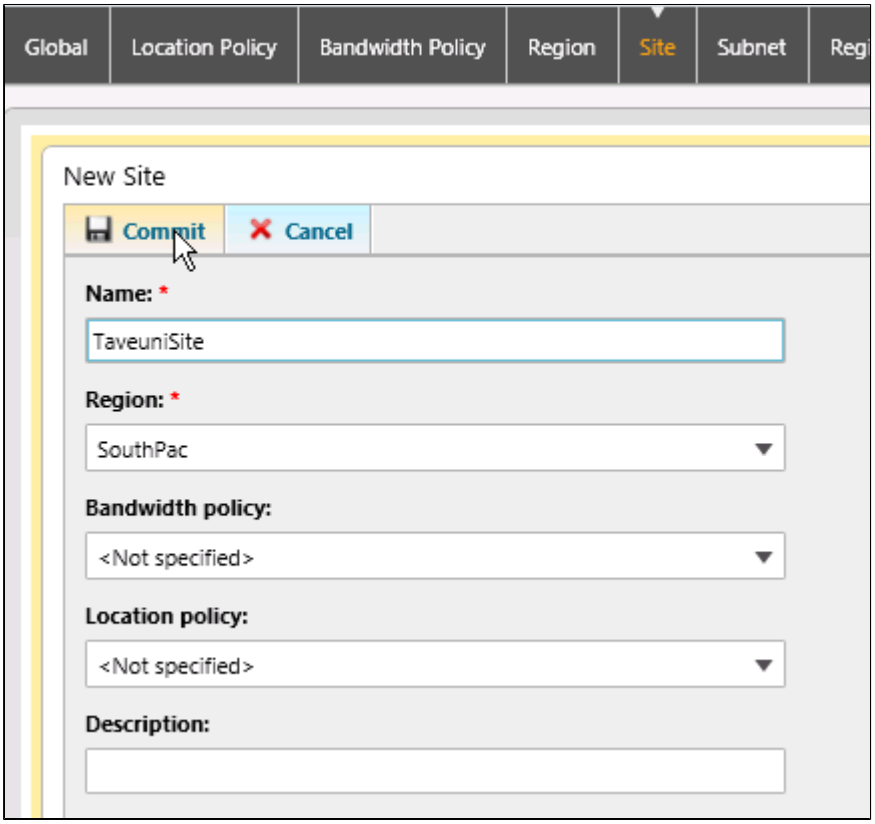
Create sites to be used for the RBA function. Again, there will be a HQ site, as well as a remote site.

1. Click *Site* in the top navigation and select *New*.

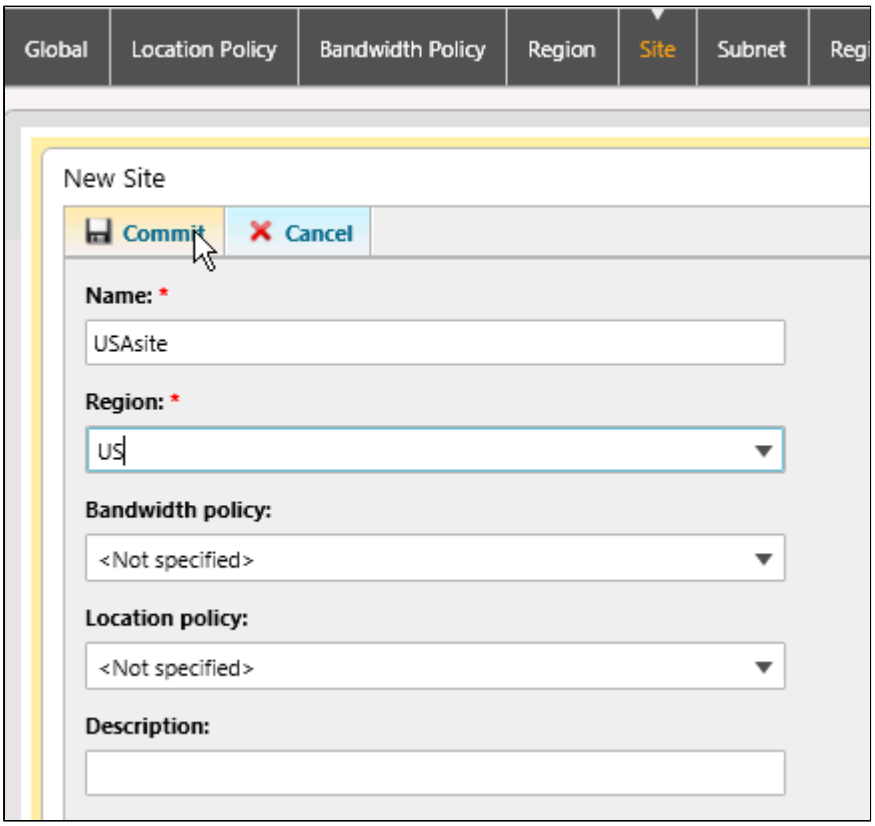


2. Enter the information for your remote site. Click *Commit*.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Click *New* and enter the information for your HQ site. Click *Commit*.

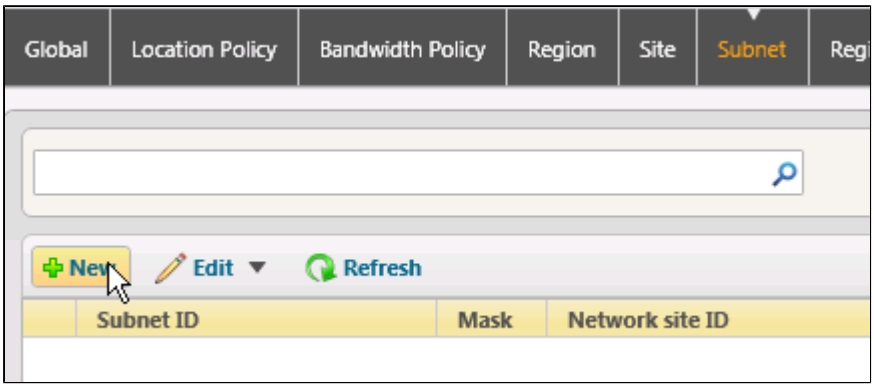


Copyright © 2015 Sonus Networks. All rights reserved.

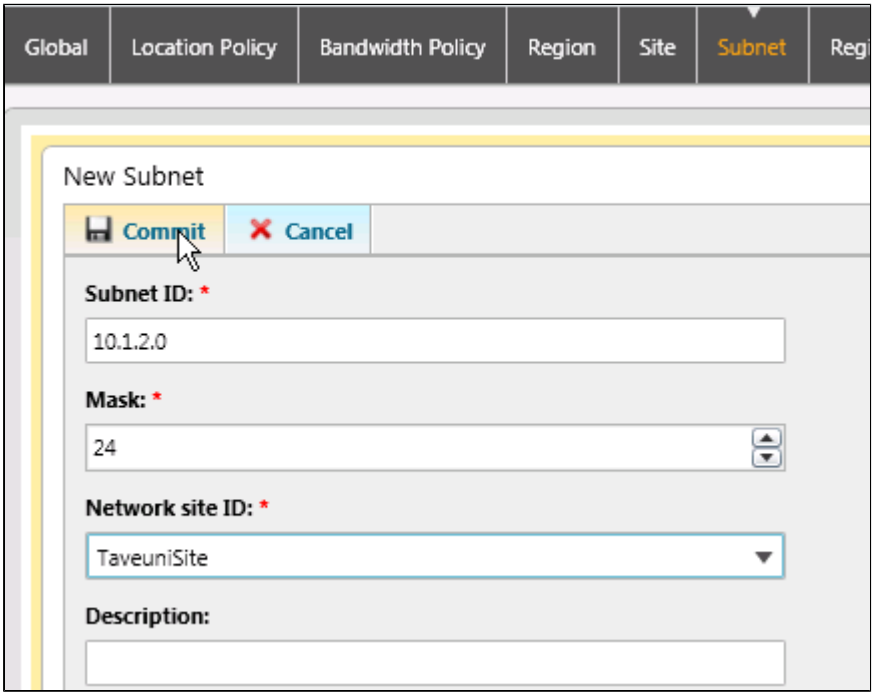
Create new Subnets

IP addresses are used by the Lync Server to identify the origin of a Lync client. Create subnet records for both the HQ and remote network sites.

1. Click *Subnet* in the top navigation and select *New*.

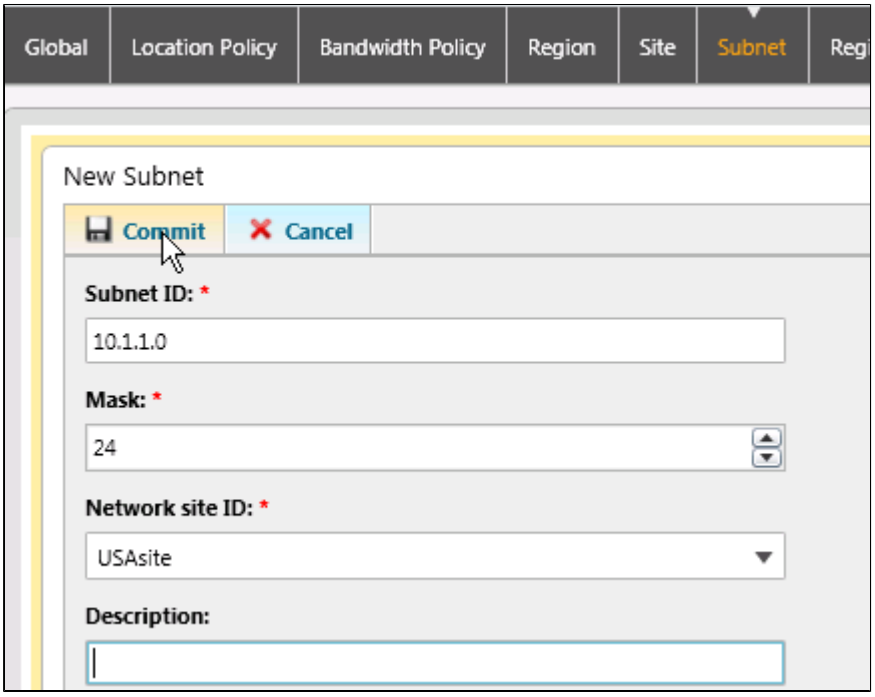


2. Enter the IP network information for the remote network.



3. Click *New*and enter the IP network information for the HQ network.

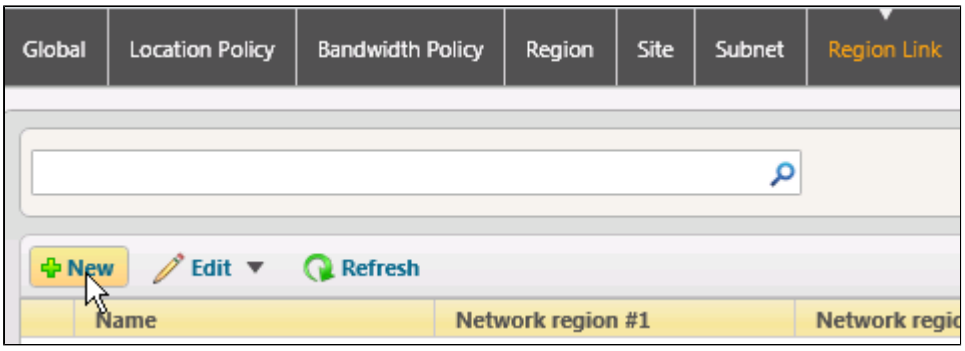
Copyright © 2015 Sonus Networks. All rights reserved.



Create a Region Link

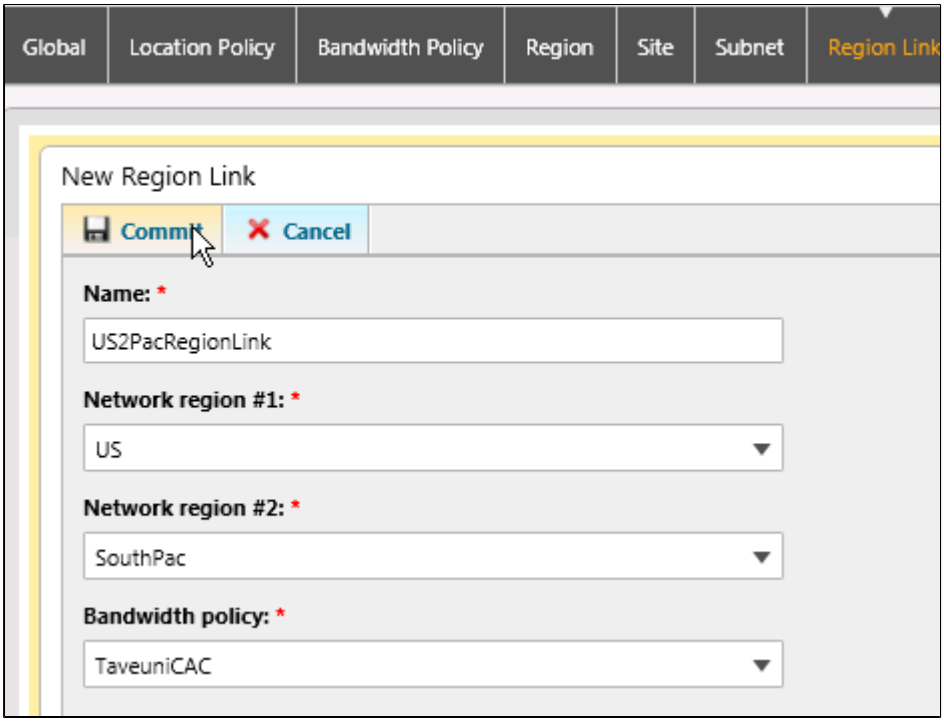
Create a Region Link between the sites.

1. Click *Region Link* in the top navigation and select *New*.



2. Using the pulldowns, select the HQ Region, the Remote Region and the Bandwidth Policy profile you previously created.

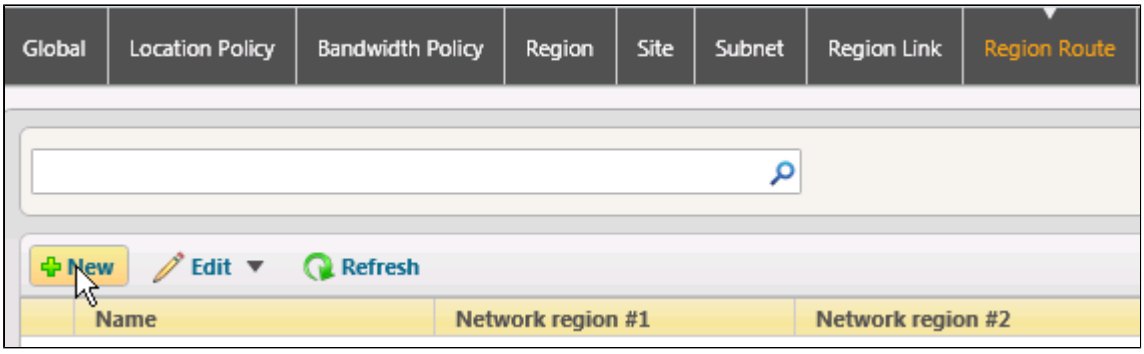
Copyright © 2015 Sonus Networks. All rights reserved.



Create a new Region Route

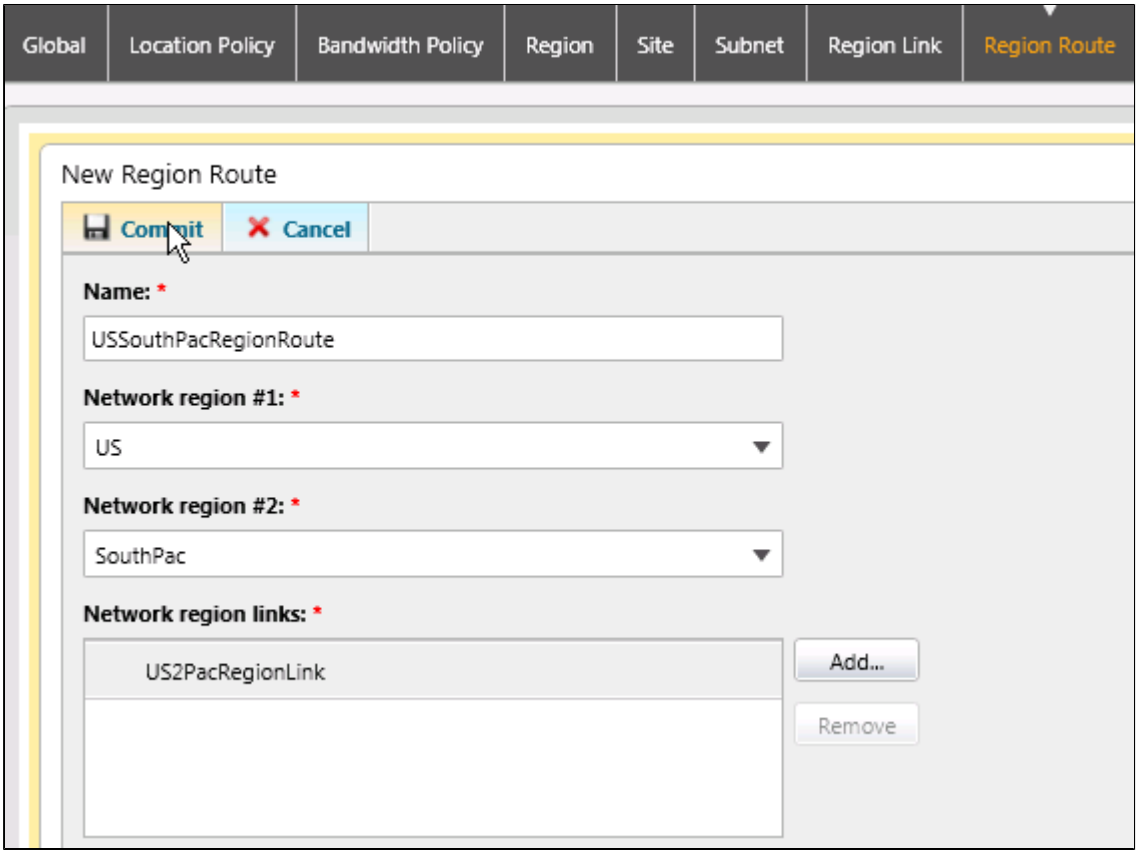
Create a Region Route for the Region Link.

1. Click *Region Route* in the top navigation and select *New*.



2. Add the Network Regions as shown and add the newly created Region Link.

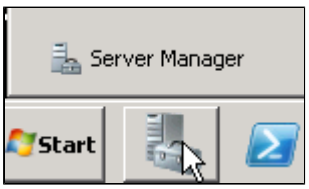
Copyright © 2015 Sonus Networks. All rights reserved.



Domain Controller Configuration

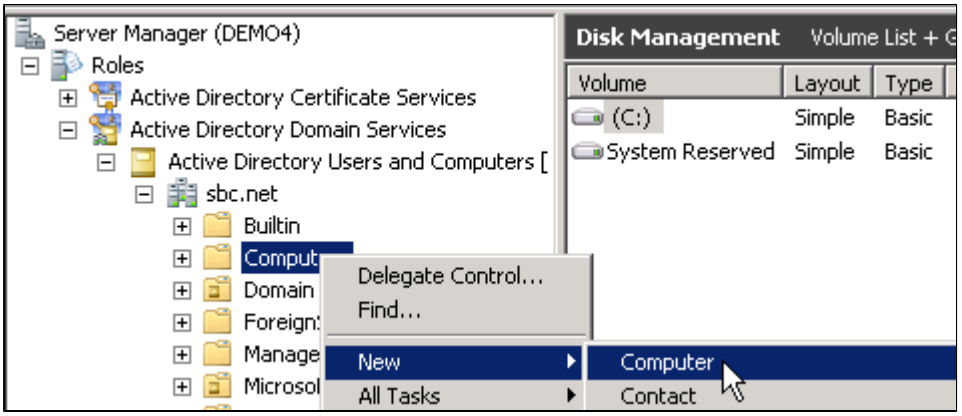
The RBA ASM computer must be added to the Domain Controller as noted below. The computer must also be added to the RTCUniversalServerAdmins group.

1. On the Domain Controller, open the *Server Manager*

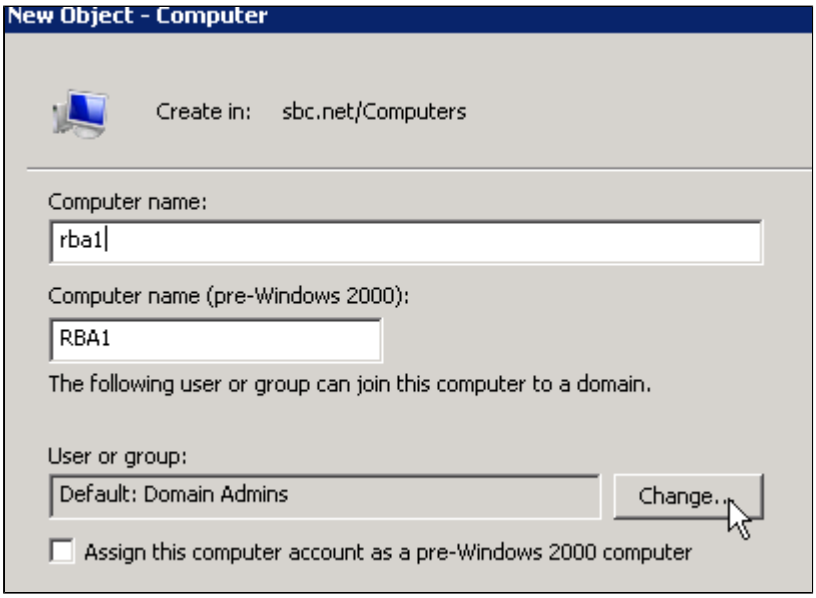


2. Add a new computer to Active Directory. You should have already selected a FQDN for the ASM module during the DNS Configuration section.

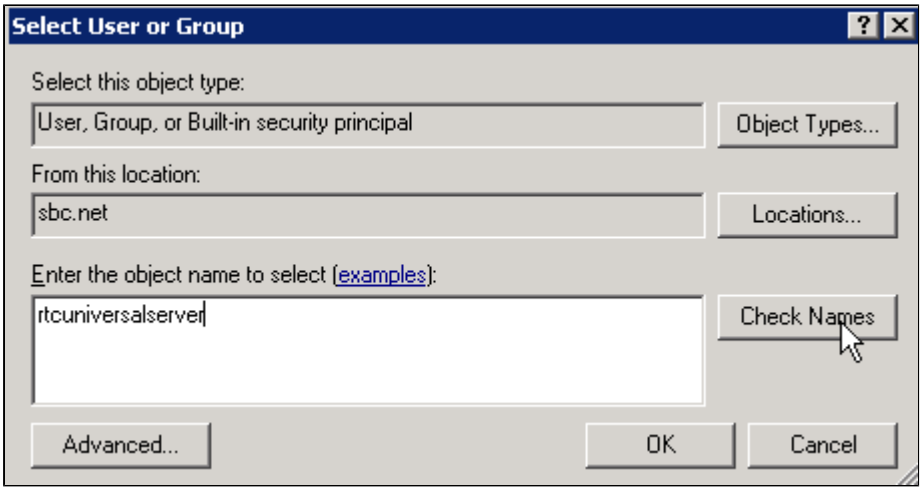
Copyright © 2015 Sonus Networks. All rights reserved.



3. Input the name of the ASM computer

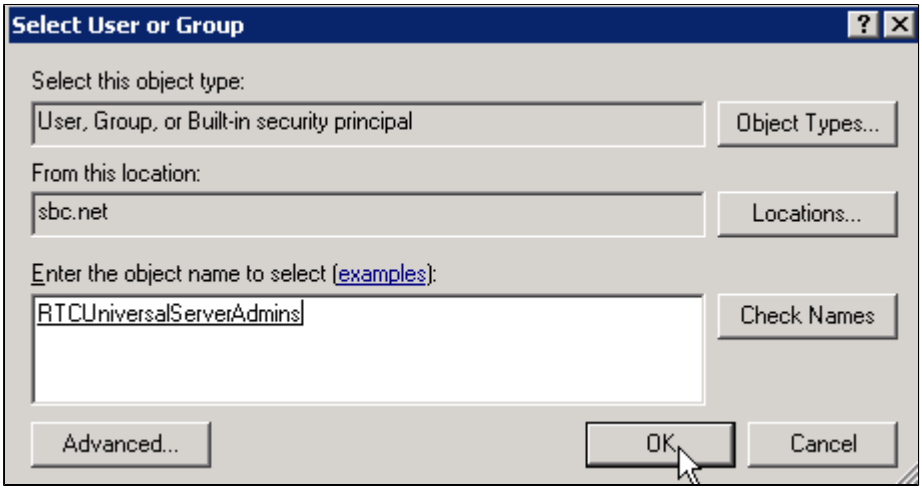


4. Add the computer to the *RTCUniversalServerAdmins*group

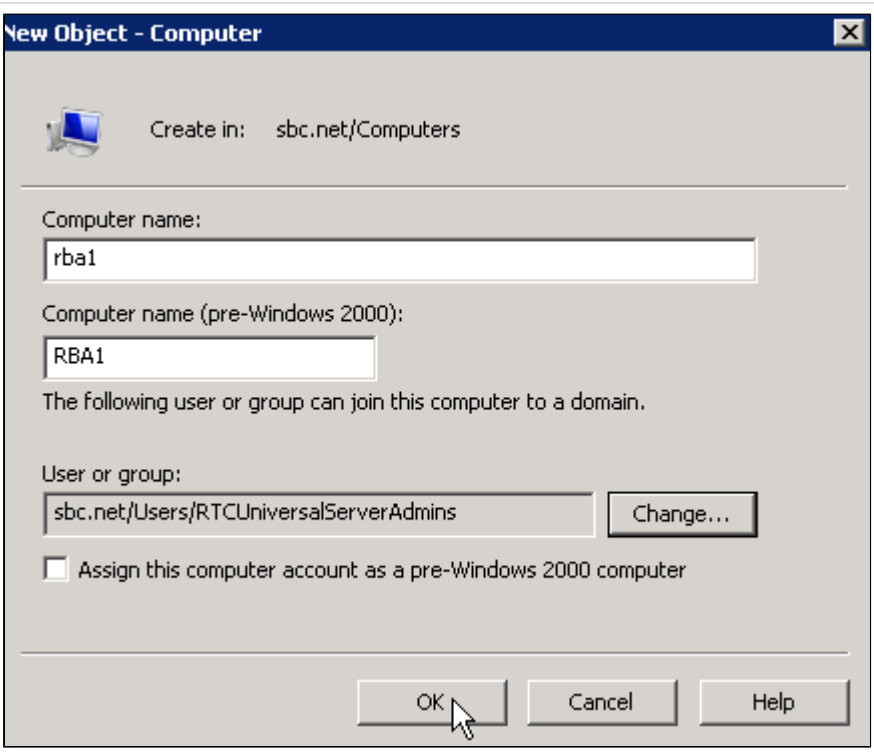


5. Click *OK*

Copyright © 2015 Sonus Networks. All rights reserved.



6. Click *OK*

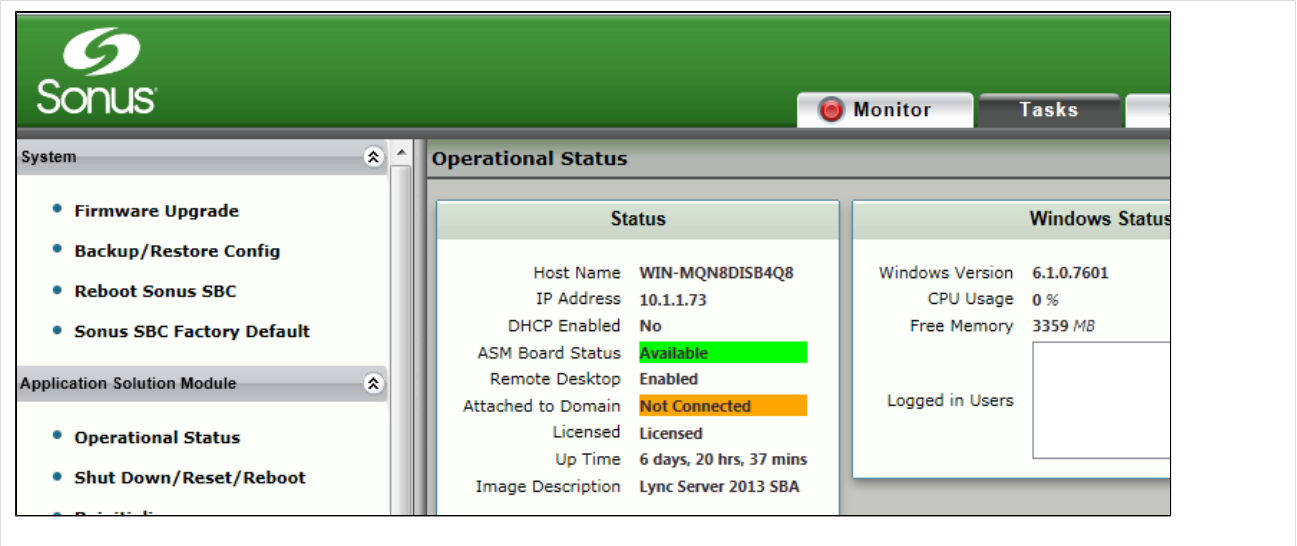


Configuring the RBA

☑ Have you added the RBA as a computer in the Domain Controller and made it part of the RTCUniversalServerAdmins group?

1. Verify the *ASM Board* is *Available* using the *Tasks Tab* | *Operational Status*selection

Copyright © 2015 Sonus Networks. All rights reserved.

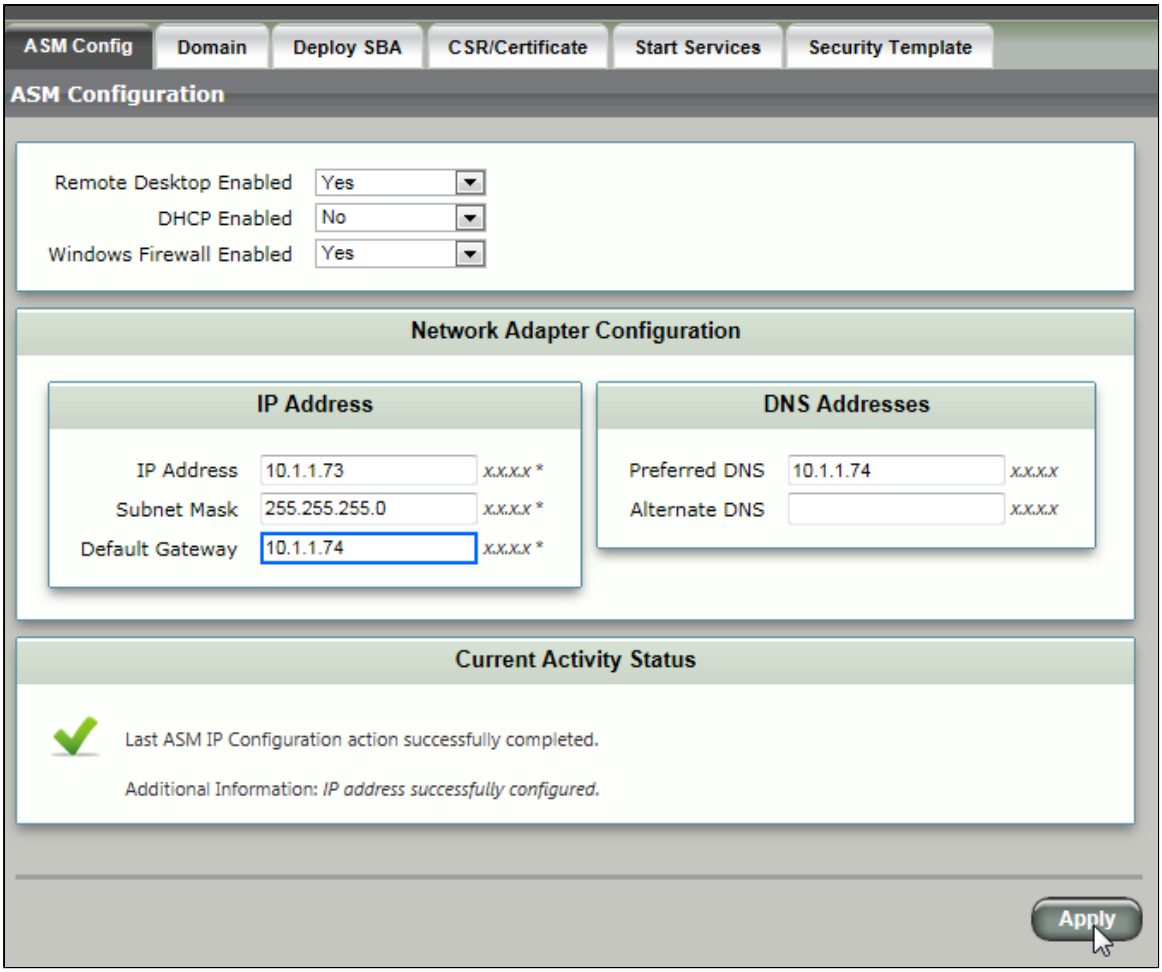


2. Click *Setup SBA* in the left-hand navigation



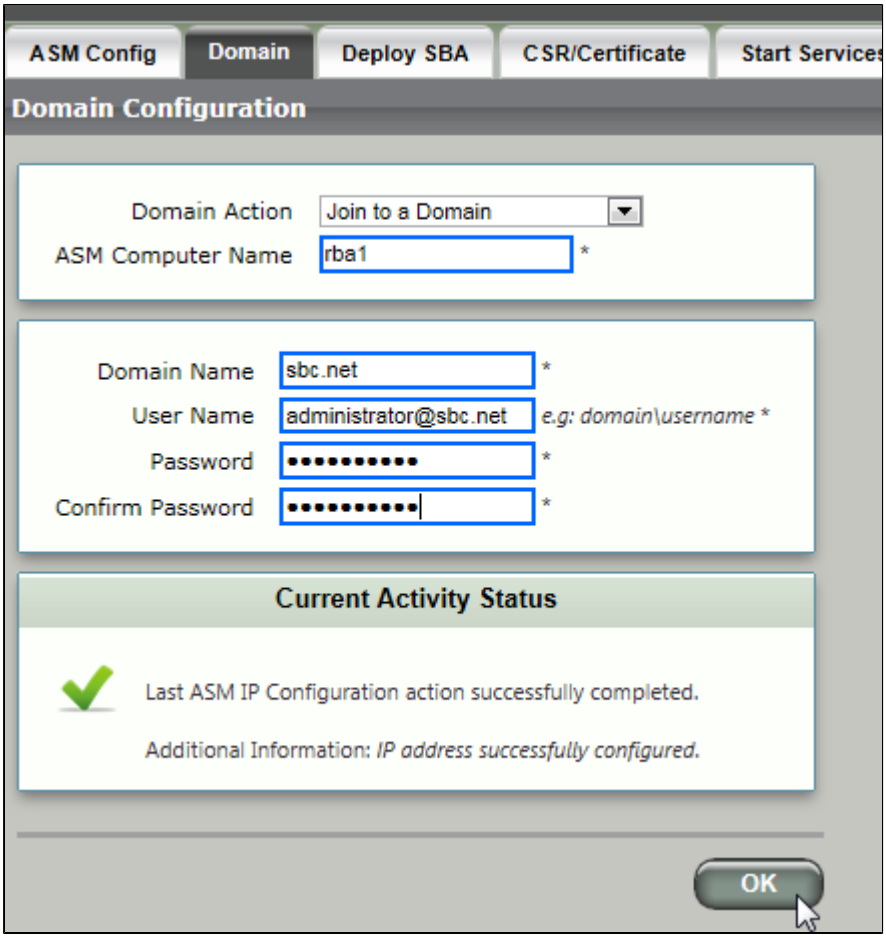
3. Click the *ASM Config* Tab and supply the information for your ASM. Click *Apply*.

Copyright © 2015 Sonus Networks. All rights reserved.



4. Click the *Domain* tab and supply the domain information for your network. Click *OK*. It will take a minutes to add the ASM to the domain and reboot.

Copyright © 2015 Sonus Networks. All rights reserved.

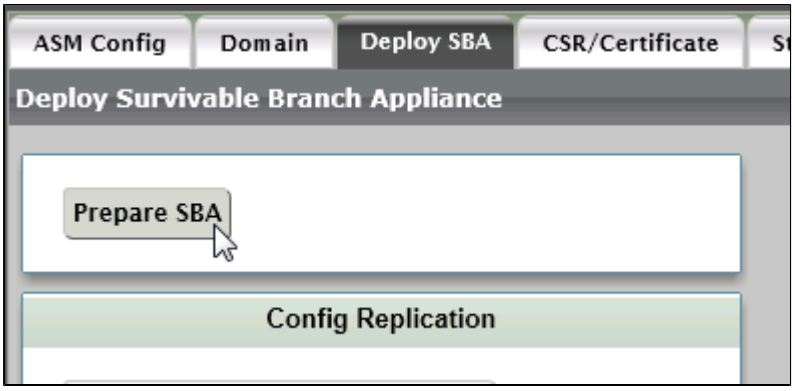


5. The Current Activity Panel will show when the domain join and rebooting processes are complete



6. Click the *Deploy SBA* tab and select *Prepare SBA*. This will install the necessary components for the ASM to process the CAC changes supplied by the remote-network SBC. It will take approximately 30 minutes for the installation to complete.

Copyright © 2015 Sonus Networks. All rights reserved.



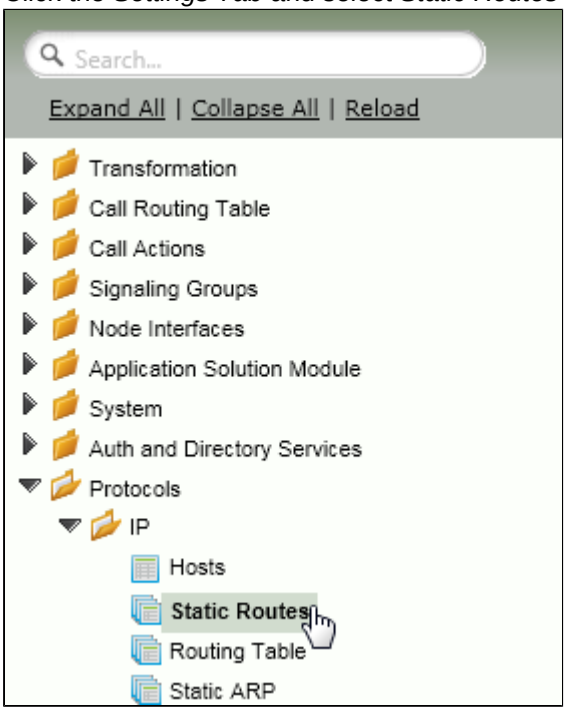
The RBA requires only the *Prep SBA* step. The other SBA deployment steps are not required.

IP Routing

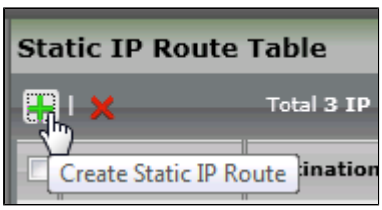
Ensuring the WAN and IPsec traffic use the appropriate routes is crucial to successful RBA failover.

SBC 1000 Static Routes

1. Click the *Settings Tab* and select *Static Routes* as shown in the diagram

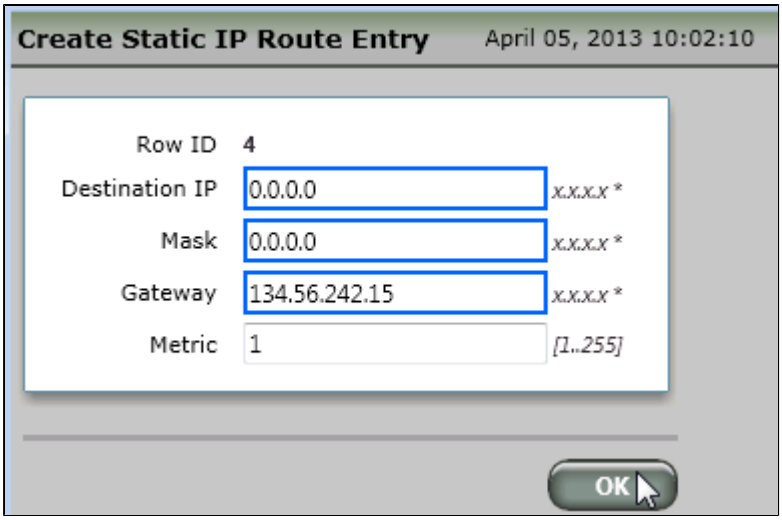


2. On the remote-network SBC, add a *Static IP Route*



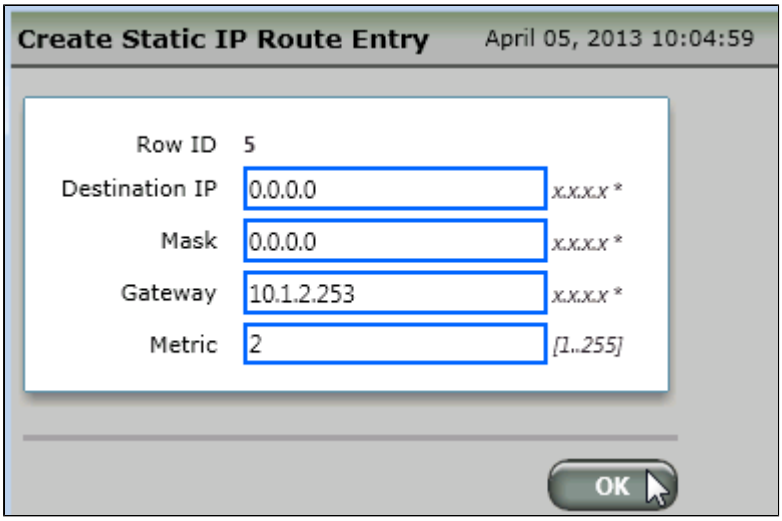
Copyright © 2015 Sonus Networks. All rights reserved.

3. Create a default route that points to the WAN interface on the HQ SBC. Set the *Metric* to *1*.

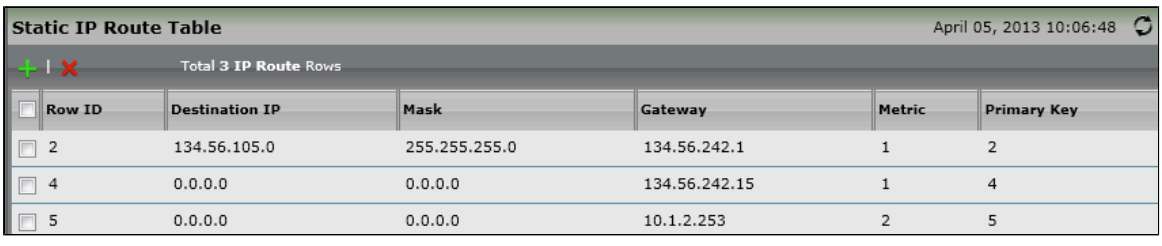


4. Create another default route that points to the IPSec interface on the HQ SBC. Set the *Metric* to *2*.

> ☑ Default routes are **required** for the automated routing failover to function. Only use default routes.



5. Verify the newly added static routes



SBC 2000 Static Routes

On the HQ SBC, add specific subnet routes that point to the remote-network. One route should use the

Copyright © 2015 Sonus Networks. All rights reserved.

remote-network SBC's WAN connection (metric 1), the other should point to the Internet gateway (metric 2).

- When the WAN is up, the WAN-specific route to the remote-network will be used.
- When the WAN is down, the default Internet router will be used to send the traffic via the 3G4G carrier network.

Static IP Route Table

Total 3 IP Route Rows

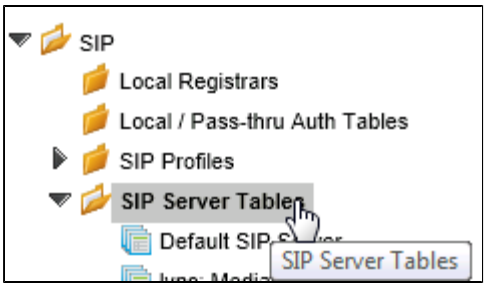
Row ID	Destination IP	Mask	Gateway	Metric
1	10.1.2.0	255.255.255.0	134.56.242.16	1
2	0.0.0.0	0.0.0.0	134.56.242.1	1
4	10.1.2.0	255.255.255.0	134.56.242.1	4

SIP Server Tables and Signaling Groups

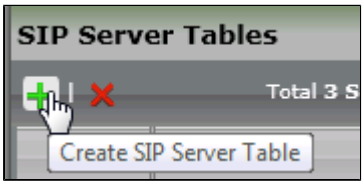
Configure the SIP Servers and Signaling Groups for both HQ and remote-network SBCs.

SBC 1000 SIP Server Table

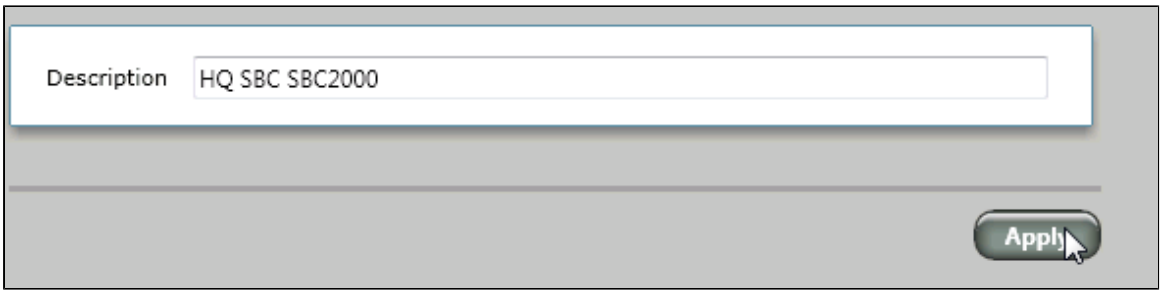
1. Click *SIP Server Tables*in the left-hand navigation



2. Add a SIP Server Table

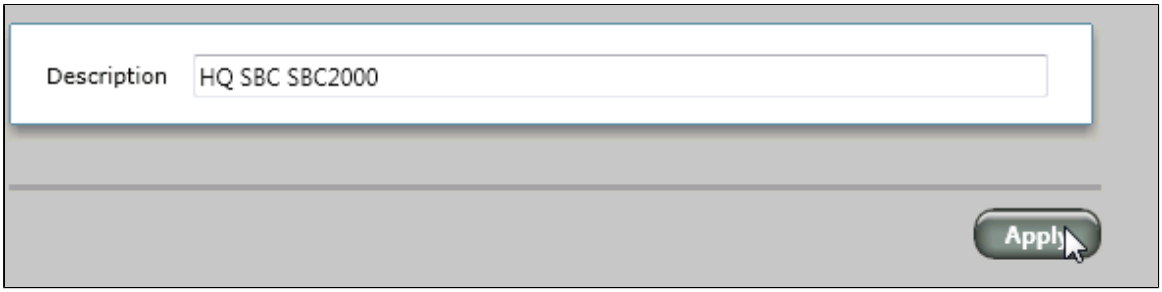


3. Enter a description and click *Apply*.

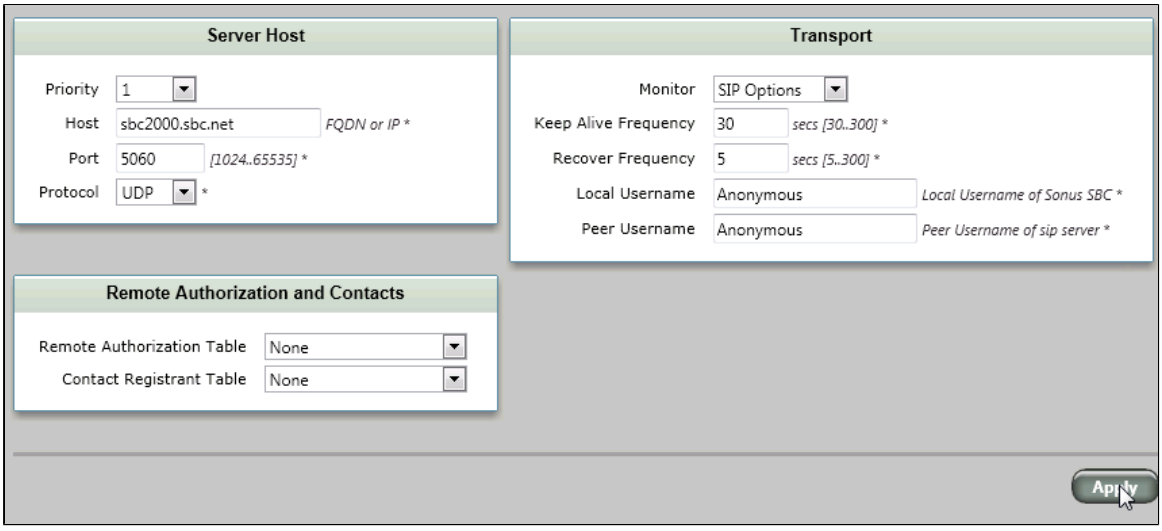


4. Click the newly added SIP Server Table

Copyright © 2015 Sonus Networks. All rights reserved.



5. Enter the information for the HQ SBC



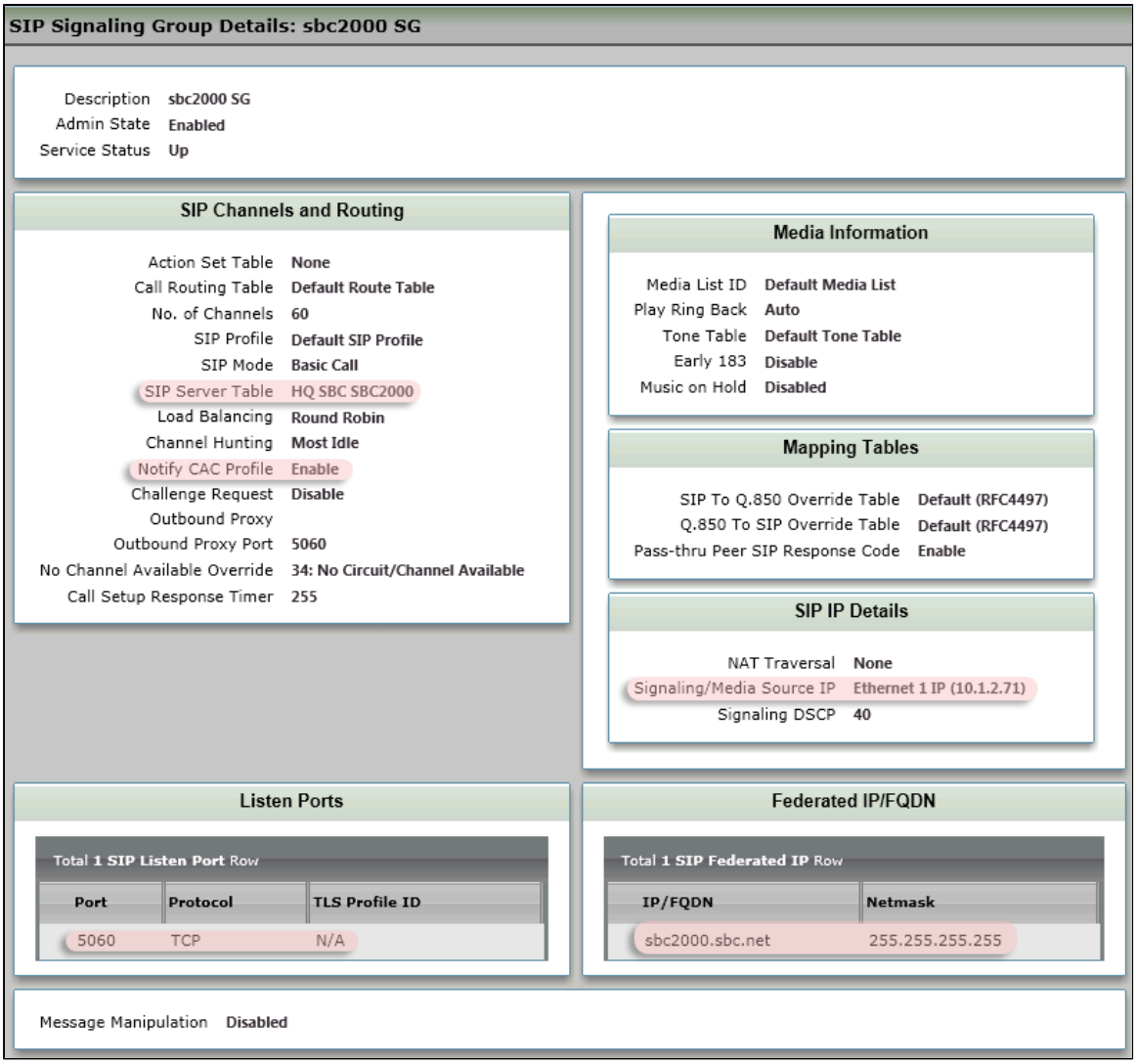
SBC 1000 Signaling Groups

1. Click *Signaling Groups*in the left-hand navigation. Add a Signaling Group for the HQ SBC.



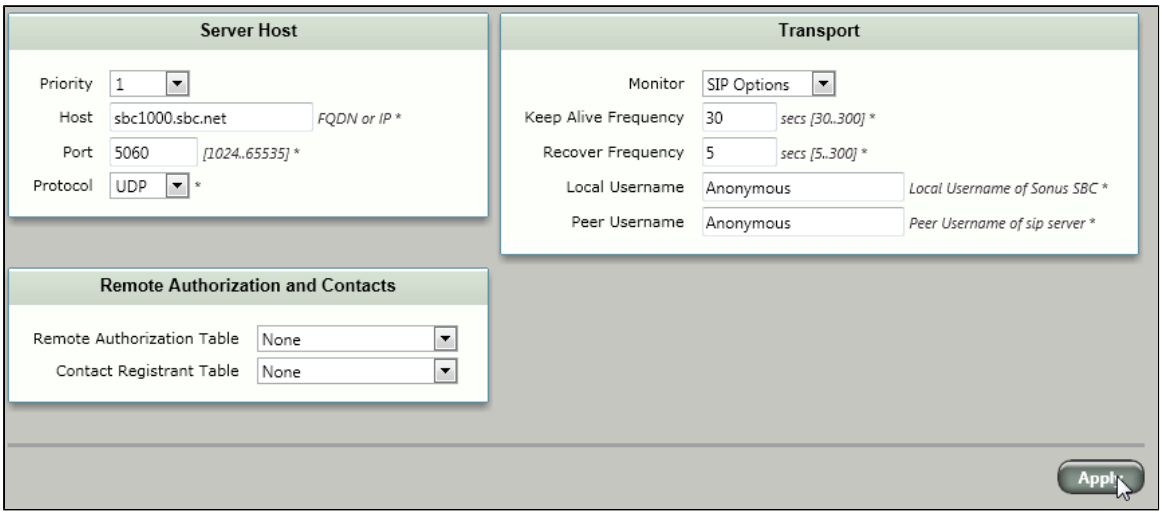
2. Add the information to the newly added SG.

Copyright © 2015 Sonus Networks. All rights reserved.



SBC 2000 SIP Server Table

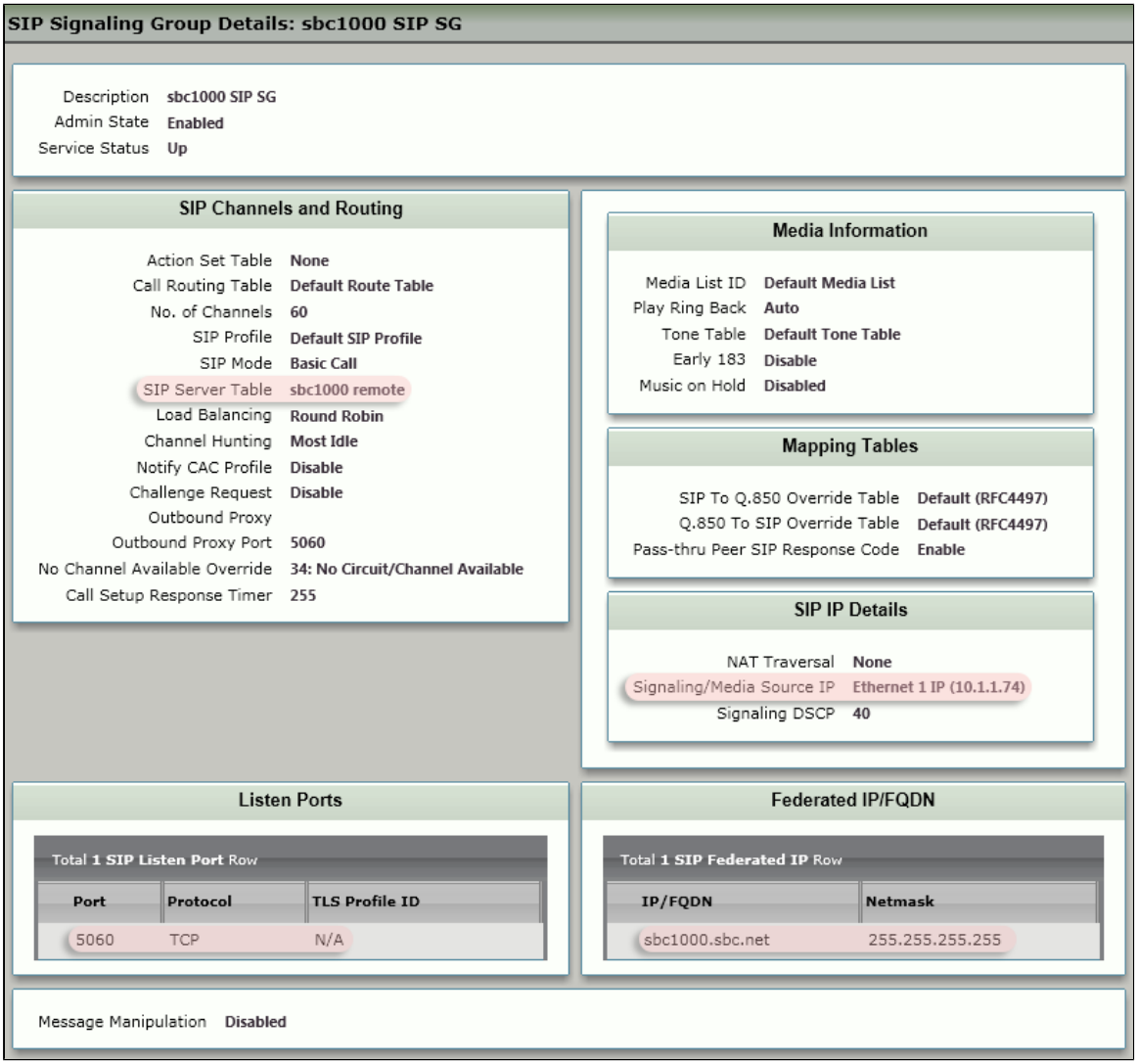
1. On the HQ SBC, add a SIP Server Table that points to the remote-network SBC



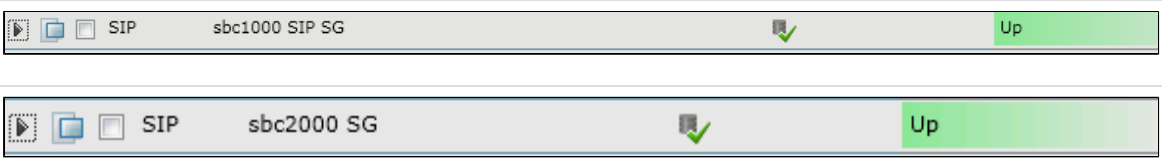
Copyright © 2015 Sonus Networks. All rights reserved.

SCB 2000 Signaling Groups

1. On the HQ SBC, add a Signaling Group that points to the remote-network SBC



2. On both SBCs, ensure that the Signaling Groups come *Up*



Verification

Verifying Routing

On the HQ SBC, verify that the Routing Table shows the route to the remote network using the WAN IP address of the remote SBC. In this case, the route to 10.1.2.0 (remote network) uses the remote SBC's 134.56.242.16 as the gateway.

Copyright © 2015 Sonus Networks. All rights reserved.

Routing Table

Total **7 IP Routing Table** Rows

Network Address	Gateway	Next Hop Interface	Type	Metric
0.0.0.0/0	134.56.242.1	Ethernet 3 IP	Static	1
10.1.1.0/24		Ethernet 1 IP	Connected	0
10.1.2.0/24	134.56.242.16	Ethernet 3 IP	Static	1
134.56.242.0/24		Ethernet 3 IP	Connected	0
169.254.10.0/24		VLAN 4028 IP	Connected	0
169.254.51.0/24		VLAN 4051 IP	Connected	0
169.254.100.0/24		eth2.4050	Connected	0

Testing Connectivity over the WAN Link

Using a Command Prompt window from a PC on the **remote** network.

- Ping the FQDN of the remote SBC. It should return remote-side private IP address (10.1.2.71 in this example).

```
C:\Users\Administrator.SBC>ping sbc1000.sbc.net

Pinging sbc1000.sbc.net [10.1.2.71] with 32 bytes of data:
Reply from 10.1.2.71: bytes=32 time<1ms TTL=64
Reply from 10.1.2.71: bytes=32 time<1ms TTL=64

Ping statistics for 10.1.2.71:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Then ping the FQDN of the HQ SBC. It should return the IP address on the private side of the HQ network (10.1.1.74 in the example, **not**134.56.242.15)

```
C:\Users\Administrator.SBC>ping sbc2000.sbc.net

Pinging sbc2000.sbc.net [10.1.1.74] with 32 bytes of data:
Reply from 10.1.1.74: bytes=32 time=1ms TTL=63
Reply from 10.1.1.74: bytes=32 time<1ms TTL=63
```

- Ping the FQDN of the Lync Server
- Ping the FQDN of the Domain Controller
- Ping the FQDN of the DNS Server
- Ping the FDQN of the RBA

All the returned IP addresses must be on the private-side of the HQ network (e.g. 10.1.1.x)

From a PC on the HQ side of the network

- Ping the FQDN of the Remote SBC. It should return a remote LAN IP address.

Copyright © 2015 Sonus Networks. All rights reserved.

```
C:\Users\Administrator>ping sbc1000.sbc.net

Pinging sbc1000.sbc.net [10.1.2.71] with 32 bytes of data:
Reply from 10.1.2.71: bytes=32 time=5ms TTL=63
Reply from 10.1.2.71: bytes=32 time=3ms TTL=63
Reply from 10.1.2.71: bytes=32 time=3ms TTL=63
Reply from 10.1.2.71: bytes=32 time=3ms TTL=63

Ping statistics for 10.1.2.71:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

- Ping a PC on the remote LAN. Check that the default router on the remote LAN PC is set to the (remote) SBC's LAN interface address (10.1.2.71 in the example).

Test a Lync to Lync Call

At this point you should be able to call Lync-to-Lync over the WAN.

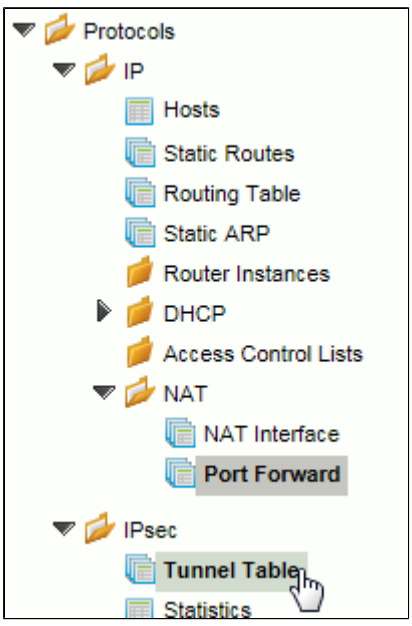
Creating the IPSec Tunnel

Use the following steps to configure an IPsec tunnel between the remote and HQ SBCs.

SBC1000 IPSec Configuration

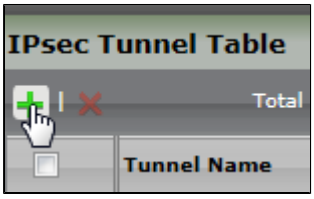
The following steps configure the remote SBC to generate an IPsec tunnel to the HQ SBC when the WAN is down.

1. Click *IPSec* | *Tunnel Table*in the left-hand navigation.



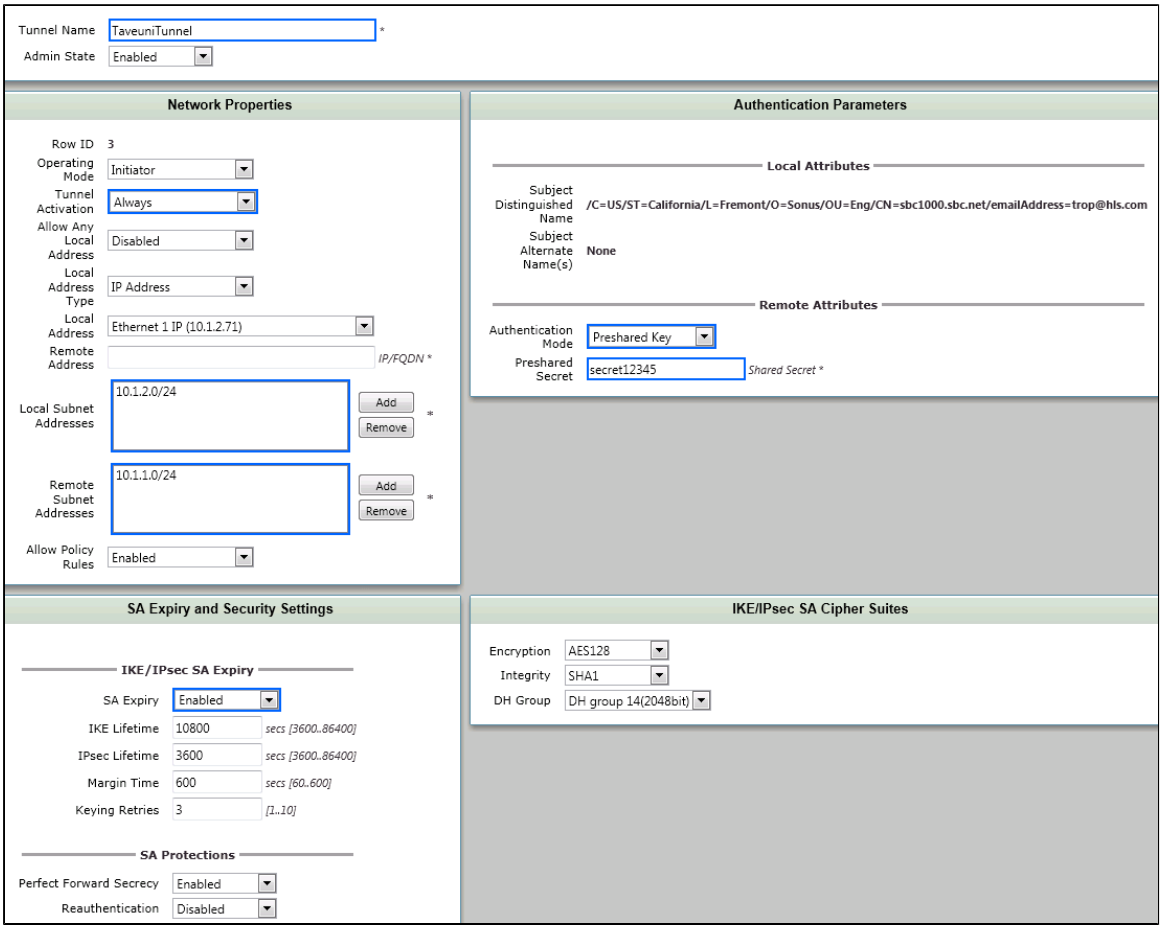
2. Add a Tunnel Table

Copyright © 2015 Sonus Networks. All rights reserved.



3. Enter the configuraton information for your IPsec tunnel.

- The *Local Subnet Address* must be programmed with IP information for the remote network.
- The *Remote Subnet Address*must be programmed with IP information for the HQ network.

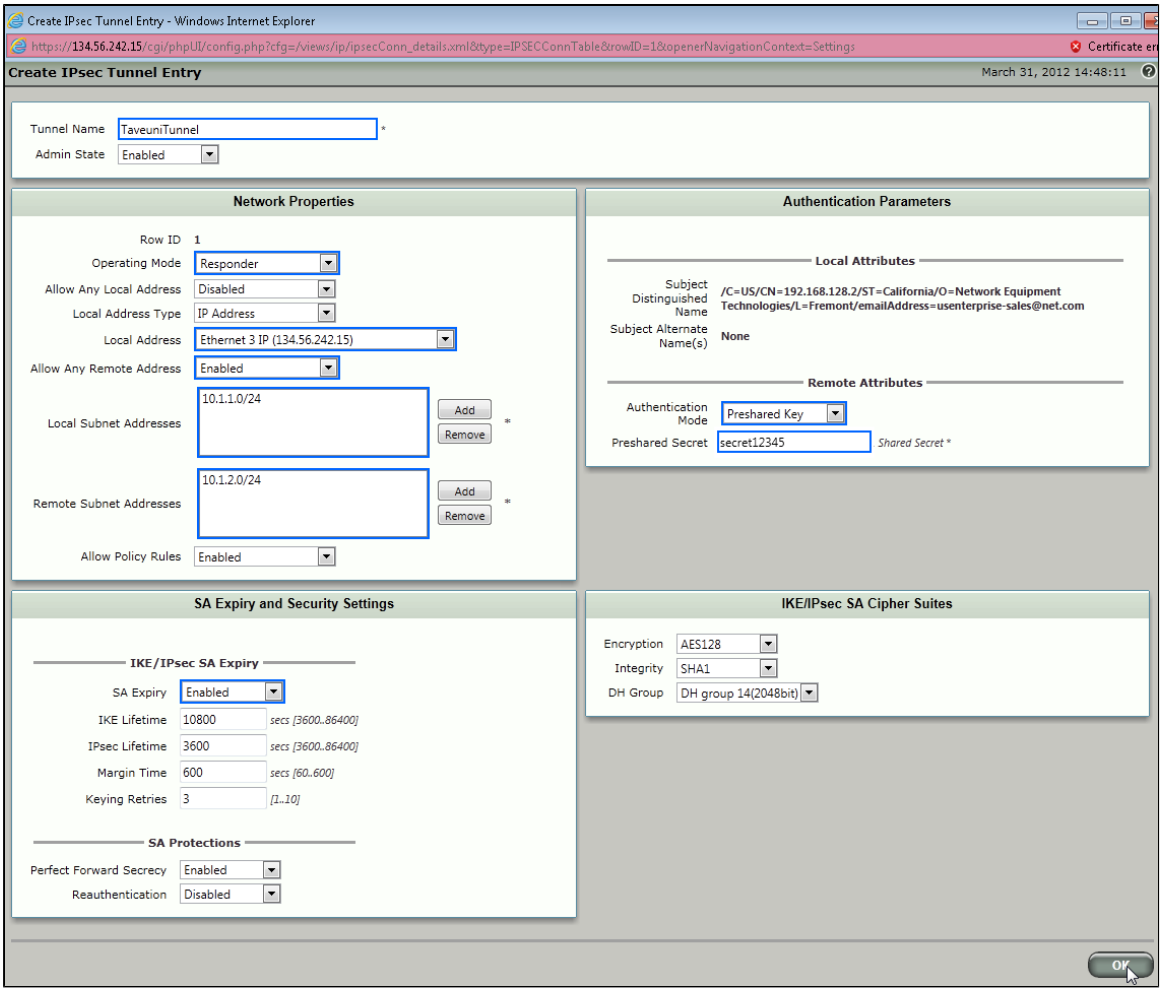


SBC2000 IPSec Tunnel Configuration

The following steps configure the HQ SBC to receive an IPsec tunnel from the remote SBC when the WAN is down.

1. Configure an IPsec tunnel on the HQ SBC with information appropriate to your network. On the HQ SBC, the *Local Subnet Address* is the HQ network, the *Remote Subnet Address*is the remote network subnet(s).

Copyright © 2015 Sonus Networks. All rights reserved.

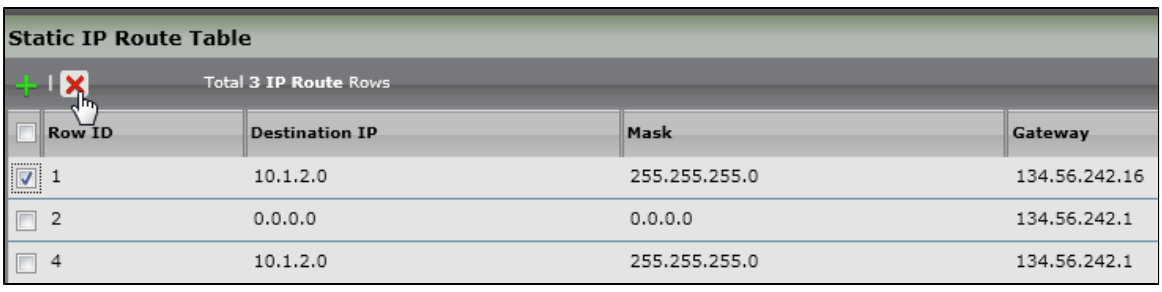


Verification

In this section you will test the IPsec tunnel to ensure connectivity exists when the WAN link is down.

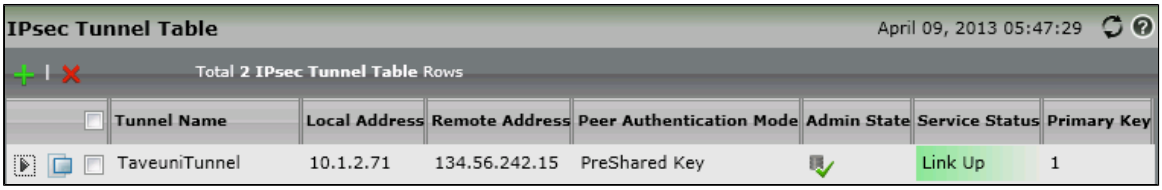
Preparing for Verification

1. Pull the cable from the WAN port on the Remote SBC. You must pull the cable from the WAN port on the Remote SBC for this verification step. Downing the WAN port results in automatically disabling the WAN IP route.
2. Manually remove the WAN Route from the HQ SBC

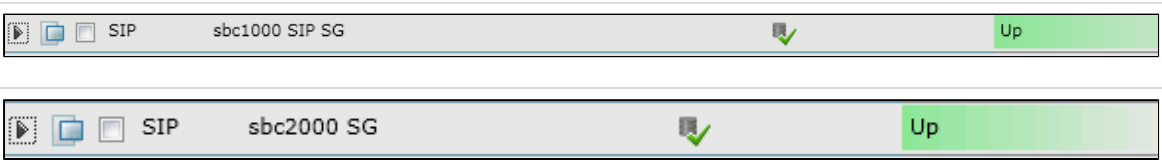


3. On the Remote SBC, use the refresh button to verify the Service Status is *Link Up*.

Copyright © 2015 Sonus Networks. All rights reserved.



4. The Signaling Groups should come back up after the IPsec tunnel is esablished.



Verifying PC Connectivity

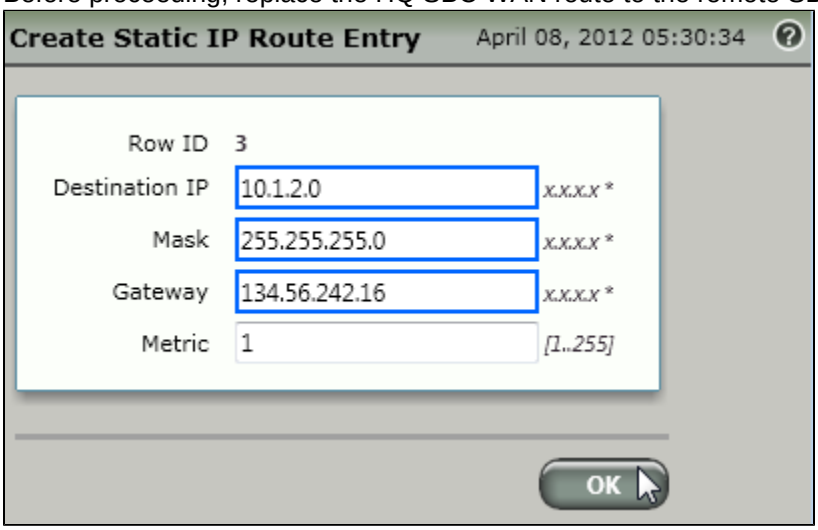
1. From a remote LAN PC, ping the FQDN of the HQ SBC. Note that the Round Trip Time (time) is much longer than that for the ping over the WAN link.

```
root@sbc1000:~# ping sbc2000.sbc.net
PING sbc2000.sbc.net (10.1.1.74) 56(84) bytes of data.
64 bytes from 10.1.1.74: icmp_req=1 ttl=64 time=76.2 ms
64 bytes from 10.1.1.74: icmp_req=2 ttl=64 time=75.4 ms
^C
--- sbc2000.sbc.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
```

1. Make a Lync call from between remote and HQ lync clients. The clients should ring and answer.

Re-add the HQ SBC WAN Route

Before proceeding, replace the HQ SBC WAN route to the remote SBC.



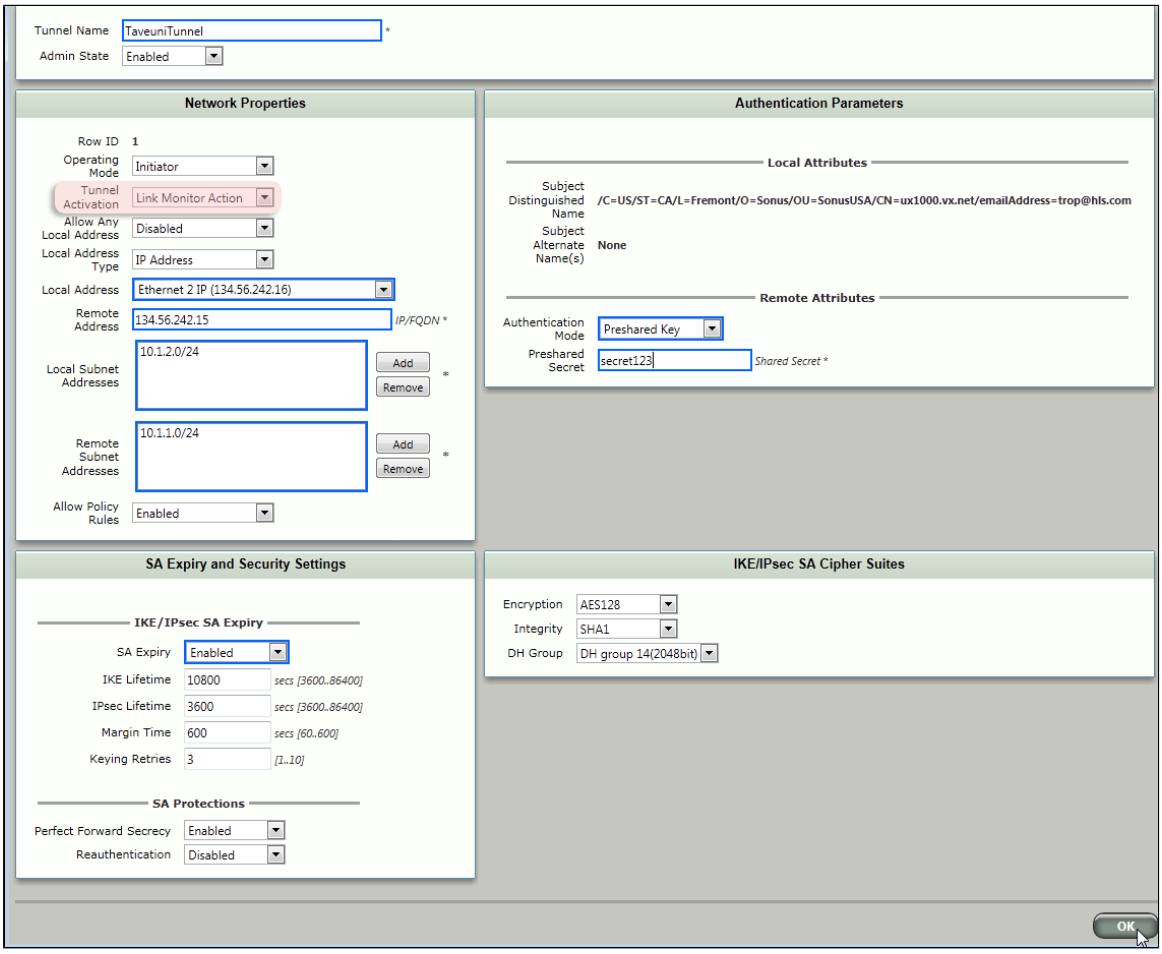
Configuring for Automated Switchover

With the successful testing of the static IPsec tunnel, it is time to make the tunnel dynamic so that the 3G4G link is

Copyright © 2015 Sonus Networks. All rights reserved.

only used activated when the WAN is down.

1. Modify the **Remote SBC** IPSec *Tunnel Activation* to *Link Monitor Action* and click *OK*.

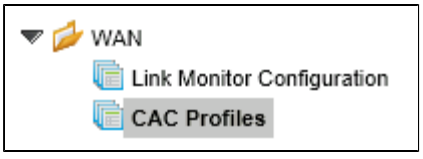


SBC 1000 CAC Profiles

The CAC profiles are transmitted to the Lync Server via the HQ SBC when the WAN transitions link states.

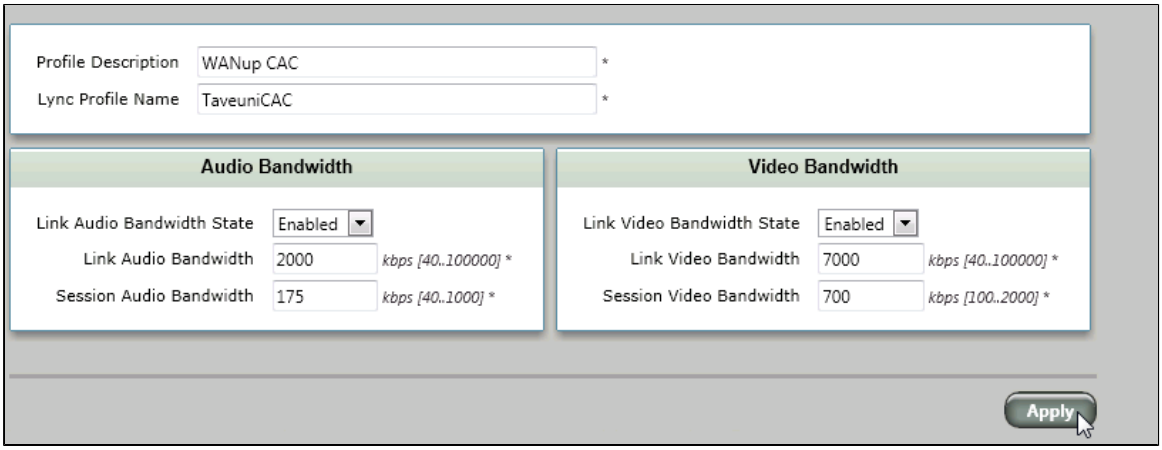
Create the CAC Profiles on the Remote SBC

1. Click *WAN* in the left-hand navigation and select *CAC Profiles*.

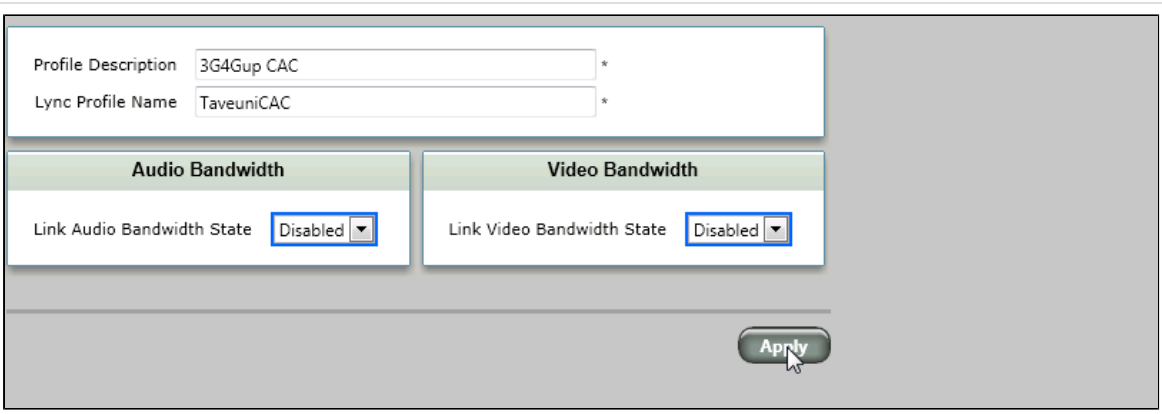


2. Create a profile for the WAN up situation. Set the bandwidths according to your desired WAN link configuration and capacity. Click *Apply*when finished.

Copyright © 2015 Sonus Networks. All rights reserved.



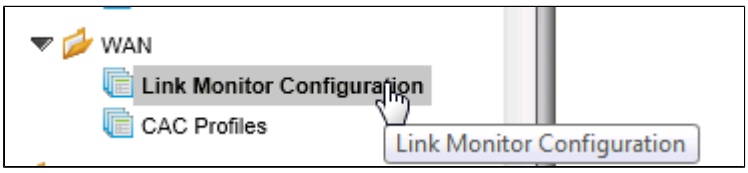
3. Now, create a CAC profile for WAN down. Setting the *Bandwidth State* to *Disabled*results in any HQ<>remote-network calls being routed over the PSTN.



SBC 1000 Link Monitor Configuration

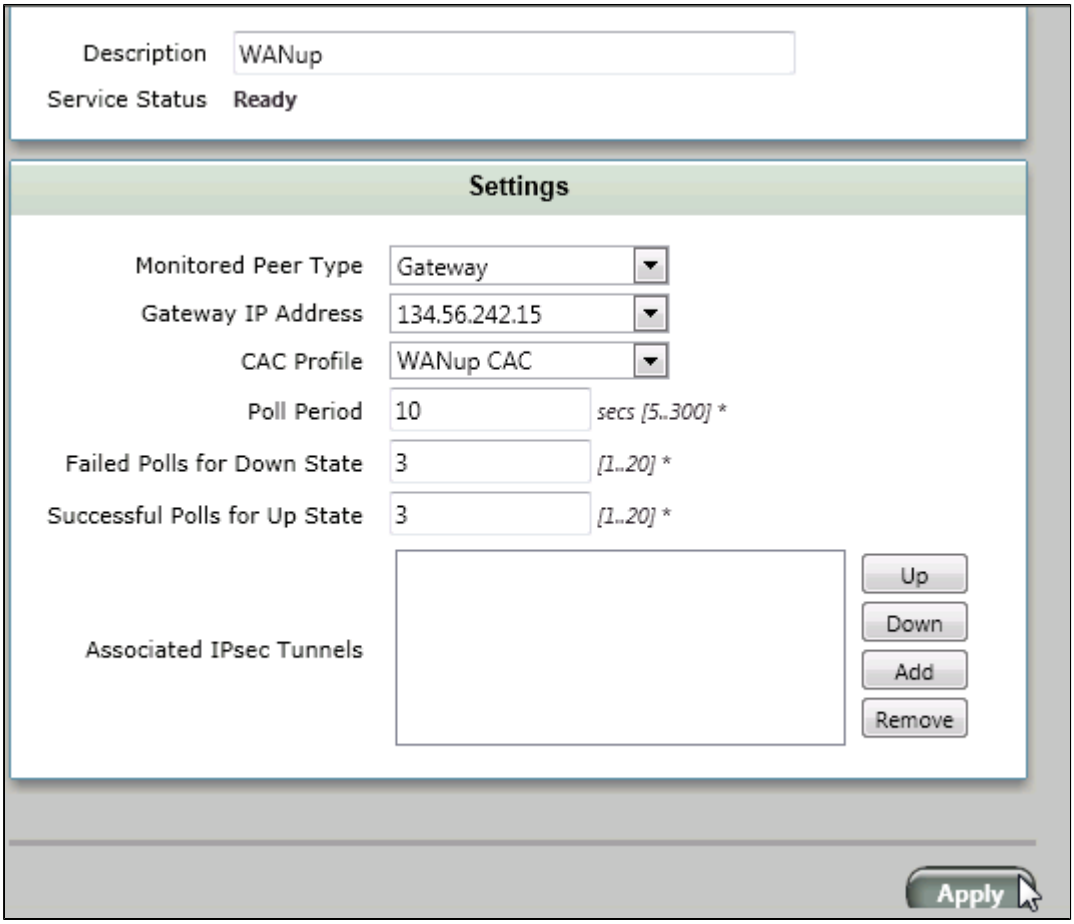
The Link Monitors provide the ability for the remote SBC to know whether the WAN is up and available.'

1. Click *Link Monitor Configuration*



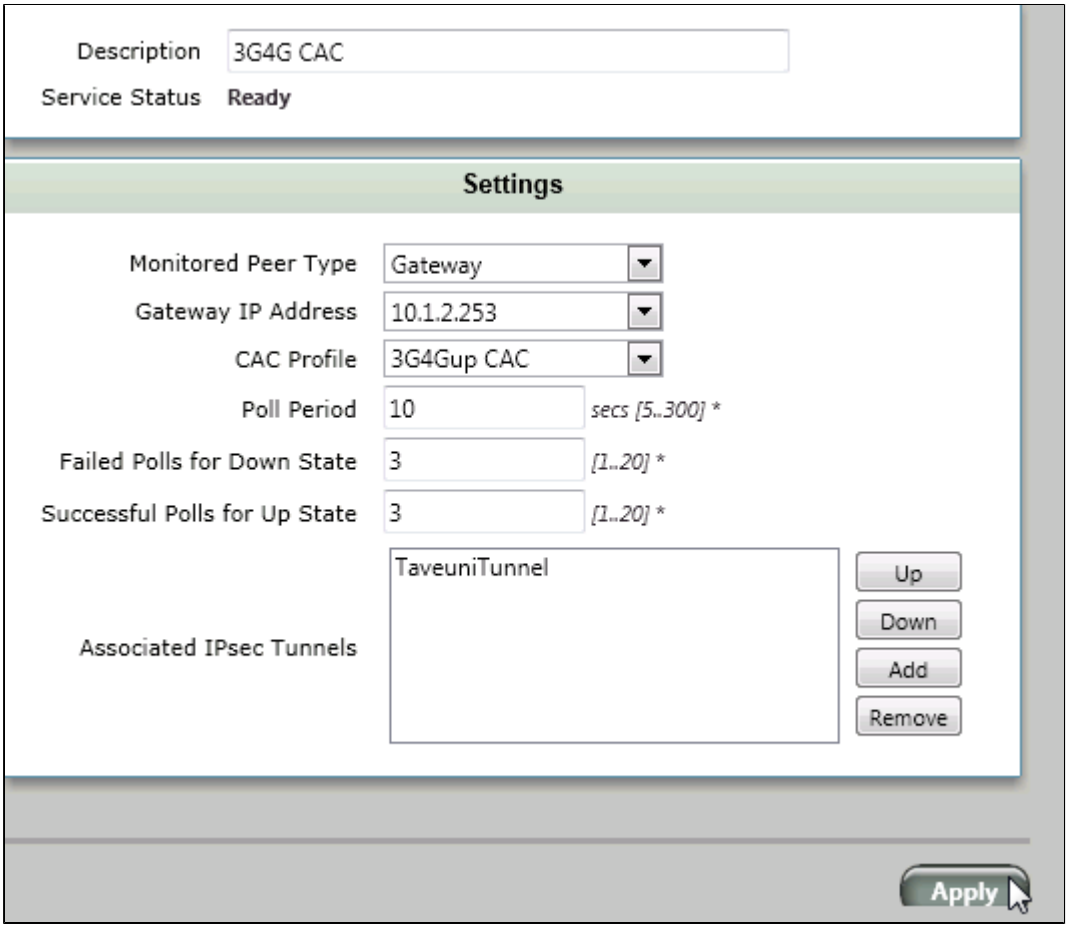
2. Add a monitor to monitor the public IP interface of the HQ SBC and click *Apply*.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Add a monitor to monitor the 3G4G router port. Associate this Link Monitor with the IPsec Tunnel you recently created. With this link activated (due to WAN down), the IPsec tunnel will be automatically started.

Copyright © 2015 Sonus Networks. All rights reserved.



Verification

Verify the following tables on the remote SBC

CAC Profile Table April 05, 2013 10:18:27

Total 2 CAC Profile Rows

Profile Description	Lync Profile Name	Link Audio Bandwidth (kbps)	Session Audio Bandwidth (kbps)	Link Video Bandwidth (kbps)	Session Video Bandwidth (kbps)	Primary Ke
WANup CAC	TaveuniCAC	2000	175	7000	700	1
3G4Gup CAC	TaveuniCAC	Disabled	N/A	Disabled	N/A	2

Link Monitor Configuration Table April 05, 2013 10:15:44

Total 2 Link Monitor Rows

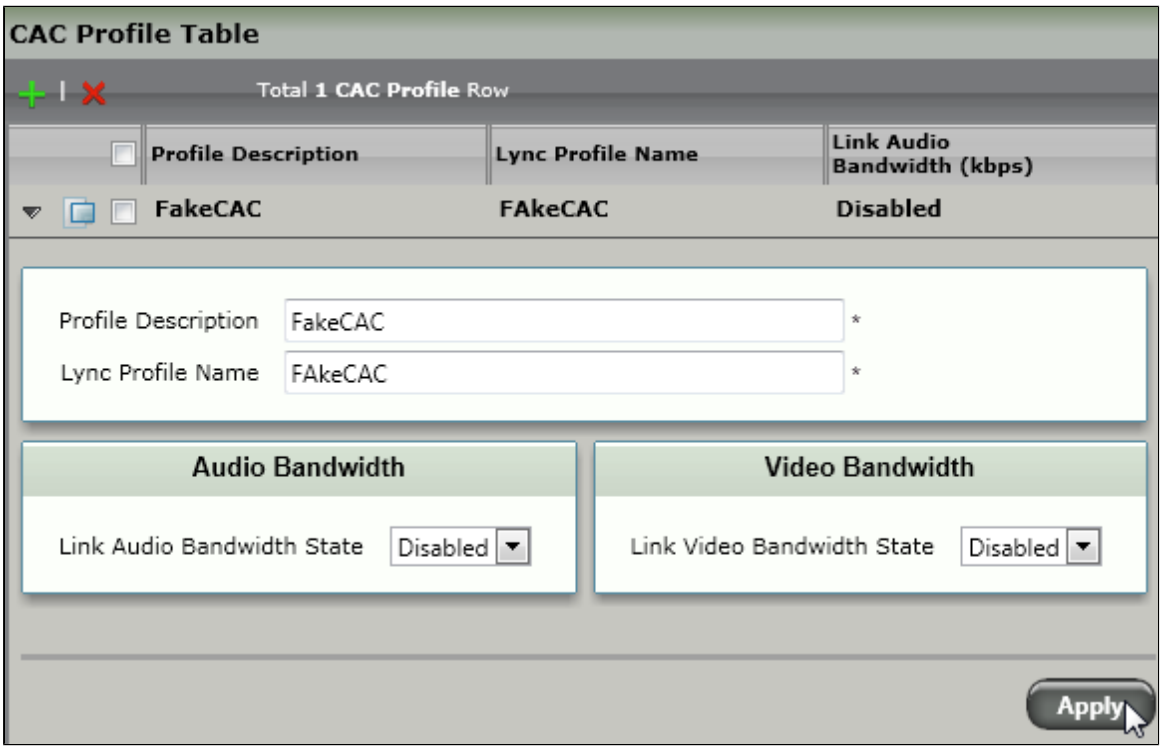
Description	IP Address/Host Name	CAC Profile	Service Status	Peer Type	Display	Primary Key
WANup	134.56.242.15	WANup CAC	Ready	Active Default Gatew...	Counters	1
3G4G CAC	10.1.2.253	3G4Gup CAC	Ready	Gateway	Counters	2

SBC 2000 Link Monitor Configuration

Configure a Link Monitor on the HQ SBC in order that it may dynamically adjust its internal routing table when the WAN link switches. The Link Monitor is configured to monitor the WAN side only.

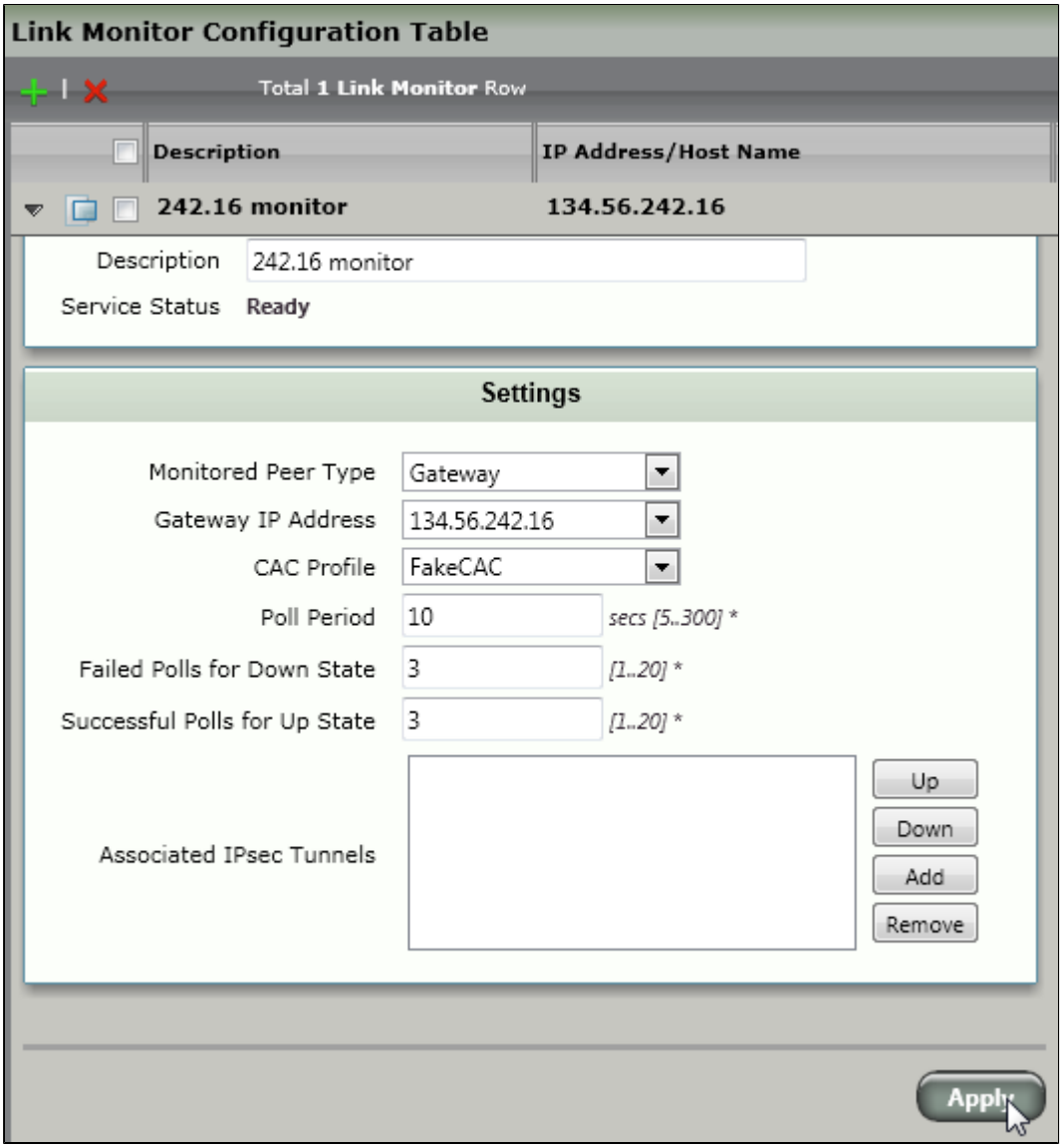
Copyright © 2015 Sonus Networks. All rights reserved.

1. Create a fake CAC entry. This entry will be ignored for purposes of bandwidth adjustment.



2. Create a Link Monitor that monitors the WAN interface of the remote SBC.

Copyright © 2015 Sonus Networks. All rights reserved.



Verification

Verify the condition of the routes and IPsec links.

WAN Link Up

HQ SBC

With the WAN link up, the HQ SBC routing table and Link Monitor should resemble the following.

Copyright © 2015 Sonus Networks. All rights reserved.

Routing Table

Total **7 IP Routing Table** Rows

Network Address	Gateway	Next Hop Interface	Type	Metric
0.0.0.0/0	134.56.242.1	Ethernet 3 IP	Static	1
10.1.1.0/24		Ethernet 1 IP	Connected	0
10.1.2.0/24	134.56.242.16	Ethernet 3 IP	Static	1

Link Monitor Configuration Table

Total **1 Link Monitor** Row

Description	IP Address/Host Name	CAC Profile	Service Status	Peer Type
242.16 monitor	134.56.242.16	FakeCAC	Ready	Gateway

Remote SBC

1. With the WAN link up, the remote SBC's routing table should point to the WAN interface on the HQ SBC.

Routing Table April 09, 2013 05:52:50

Total **4 IP Routing Table** Rows

Network Address	Gateway	Next Hop Interface	Type	Metric	Administrative Distance
0.0.0.0/0	134.56.242.15	Ethernet 2 IP	Static	1	1
10.1.2.0/24		Ethernet 1 IP	Connected	0	0

2. The Link Monitor Table should be *Ready*on the WAN link

Link Monitor Configuration Table April 09, 2013 05:54:59

Total **2 Link Monitor** Rows

Description	IP Address/Host Name	CAC Profile	Service Status	Peer Type	Display	Primary Key
WANup	134.56.242.15	WANup CAC	Ready	Active Default Gatew...	Counters	1
3G4G CAC	10.1.2.253	3G4Gup CAC	Ready	Gateway	Counters	2

3. The IPsec tunnel should be *Link Down*

IPsec Tunnel Table April 09, 2013 05:55:32

Total **2 IPsec Tunnel Table** Rows

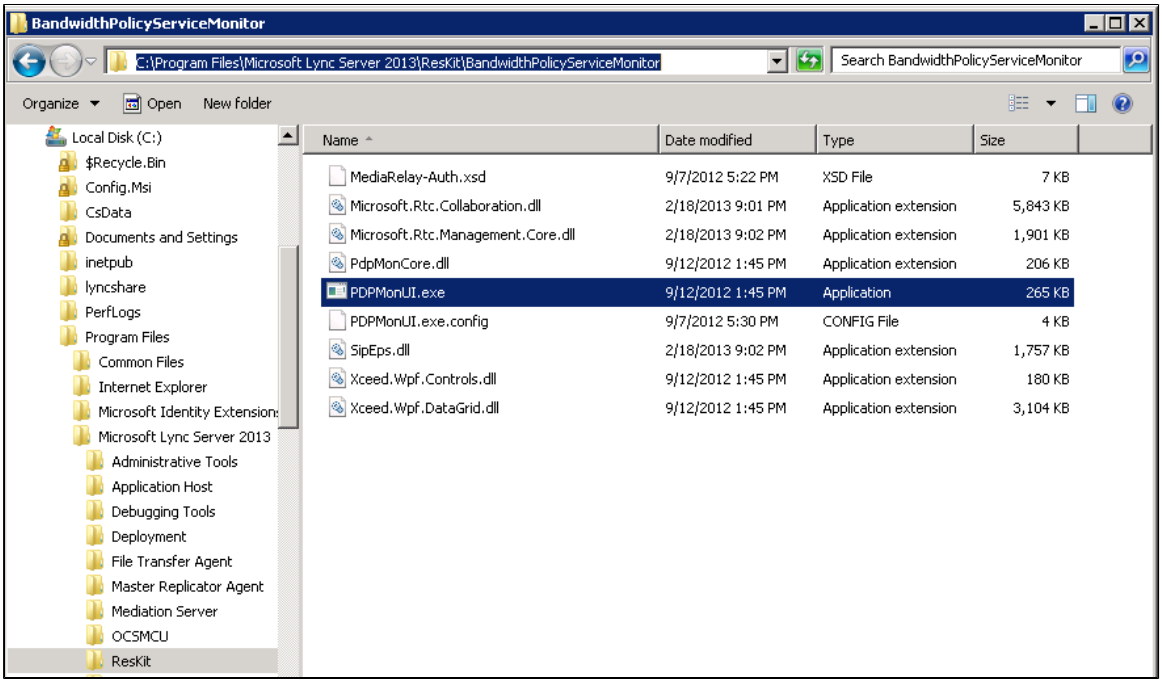
Tunnel Name	Local Address	Remote Address	Peer Authentication Mode	Admin State	Service Status	Primary Key
TaveuniTunnel	10.1.2.71	134.56.242.15	PreShared Key		Link Down	1

Lync Server

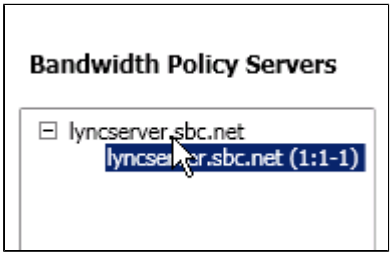
Verify the Lync Bandwidth Profile using the Bandwidth Policy Service Monitor, which is installed as a component of the optional Lync Server Resource Kit (available from the Microsoft Lync Server website).

1. Open Windows Explorer to C:\Program Files\Microsoft Lync Server 2013\ResKit\BandwidthPolicyServiceMonitor and select *PDPMonUI.exe*.

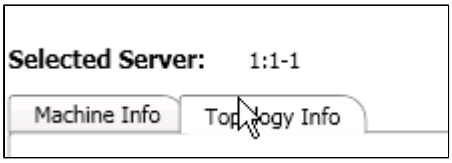
Copyright © 2015 Sonus Networks. All rights reserved.



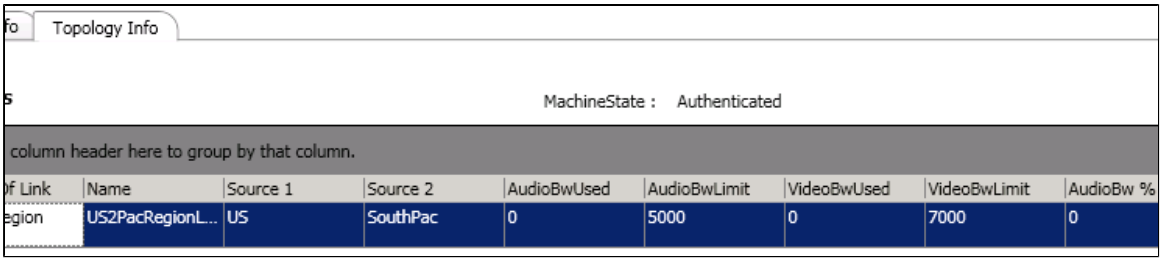
2. Expand the server name in the left-hand navigation and select the expanded server.



3. Click the *Topology Info*tab



4. Verify the bandwidth settings are for the WAN up values.



Lync Clients

Test a call between a HQ and Remote Lync client. Calls between HQ and Lync clients should connect directly over

Copyright © 2015 Sonus Networks. All rights reserved.

the WAN without need for a PSTN connection.

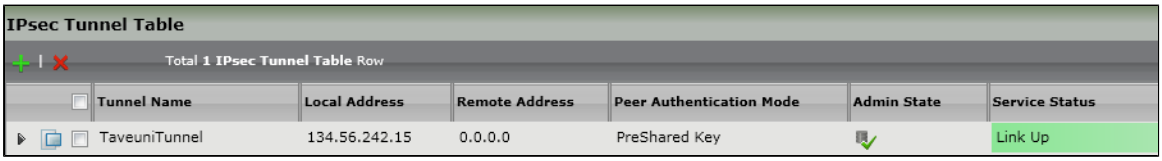
WAN Link Down

Downing the WAN Link should result in the following status. With the WAN link down, verify your implementation to the following:

HQ SBC Status

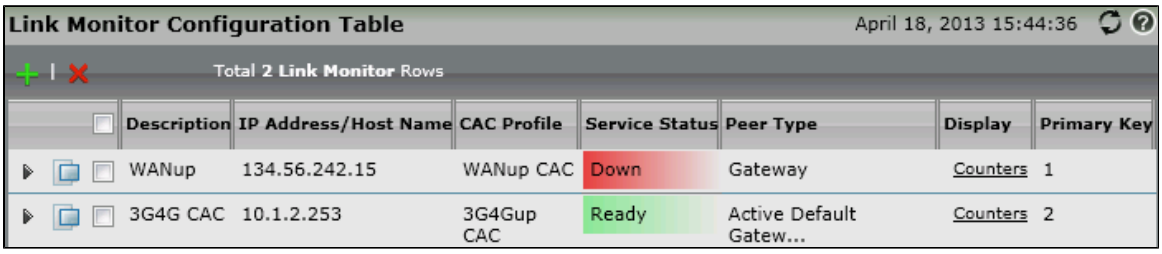
1. On the HQ SBC, the WAN Link Monitor should show down and the IPsec tunnel up.

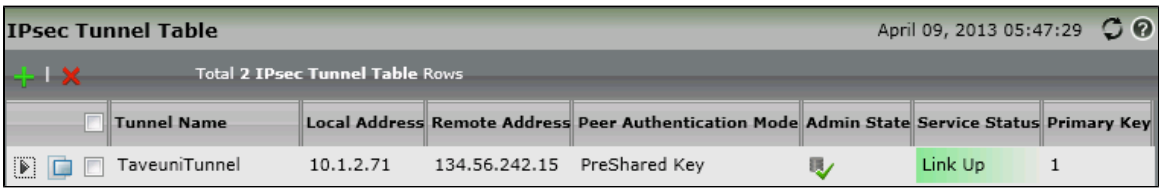




Remote SBC Status

On the Remote SBC, the Link Monitor should show the 3G4G link up, the WAN link down, and the IPsec tunnel up.

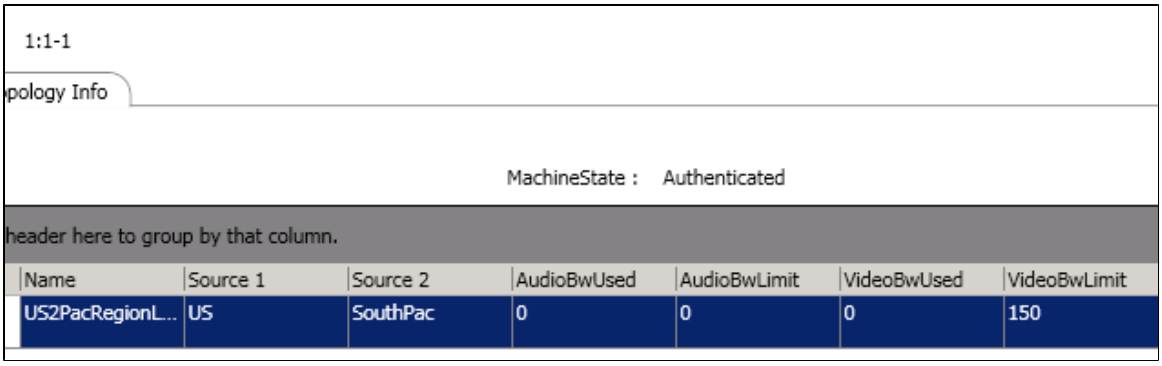




Lync Server

Within two or three minutes, the Bandwidth Policy should automatically update to the WAN down bandwidth values.

Copyright © 2015 Sonus Networks. All rights reserved.



Lync Clients

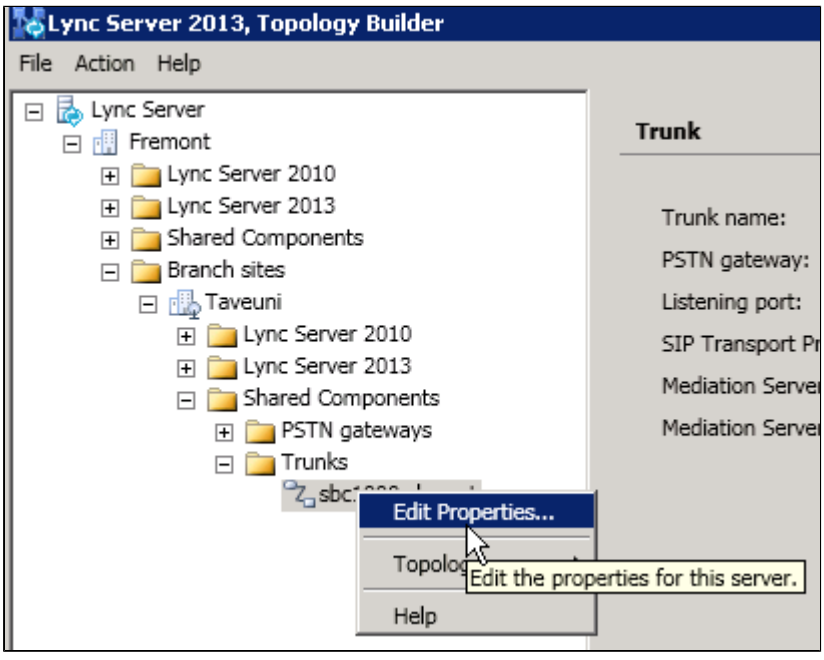
Test a call between a HQ and Remote Lync client. In the WAN down condition, you should be able to call between HQ and Remote Lync clients. The calls should utilize the PSTN connection between the SBCs.

> Remember, for Lync implementations, the SBC is a PSTN gateway for the Lync Server. When in the WAN down condition, the Lync server will send calls to the remote PSTN (SBC) gateway. You must configure the customary SBC routes and transformation tables that would be used for calls to/from Lync.

Setting the Remote SBC to TLS

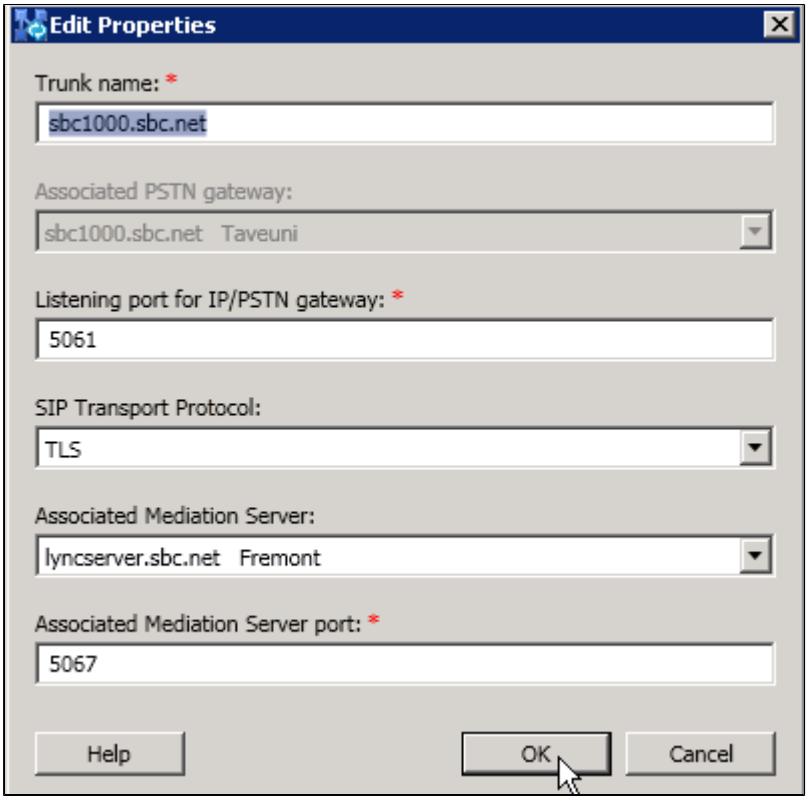
The remote SBC must beconfigured to TLS/SRTP in order for the remote Lync clients to send calls over the PSTN during a 3G4G failover. The following steps will assist you in configuring the Lync Server and remote SBC for TLS/SRTP.

1. On the Lync Server, start the Topology Builder and *Edit Properties*for the remote site Trunk.

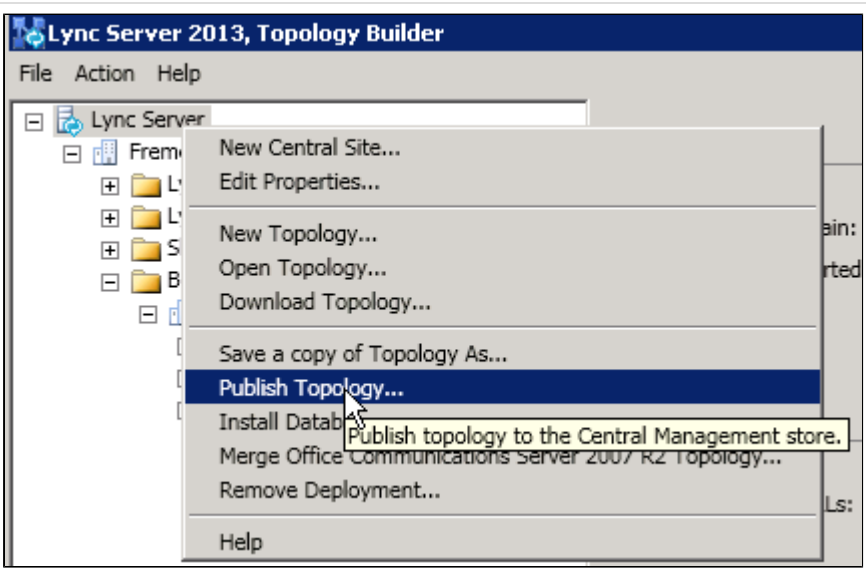


2. Change the port and configuration to support TLS as shown.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Publish the topology.

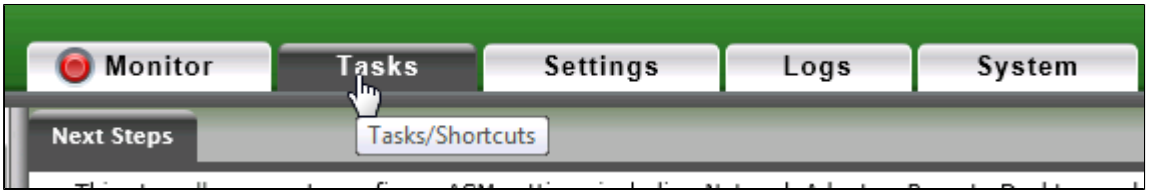


Certificate for the SBC

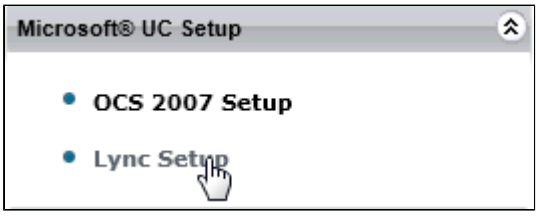
Certificates are required for TLS/SRTP functionality. The following steps will assist you in installing certificates on the remote SBC.

1. Click the *Tasks*tab.

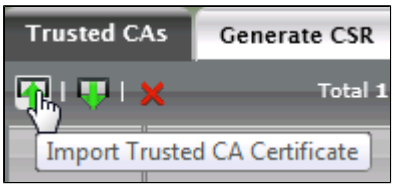
Copyright © 2015 Sonus Networks. All rights reserved.



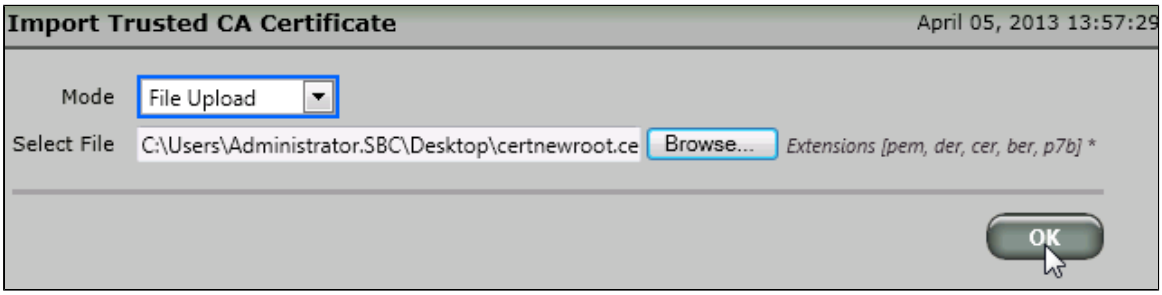
2. Click *Lync Setup*in the left-hand navigation



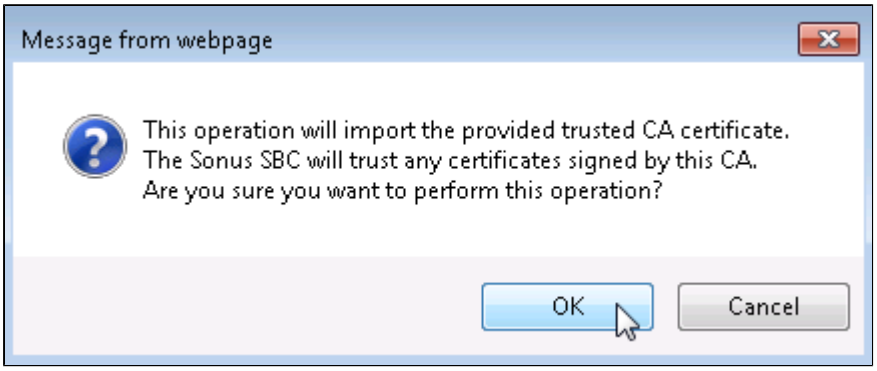
3. Obatin the root certificate from your network administrator and copy it to your PC. From the webui, click *Import Trusted CA Certificate*as shown.



4. Set the *Mode* to *File Upload* and *Browse*to find the file containing the root certificate.

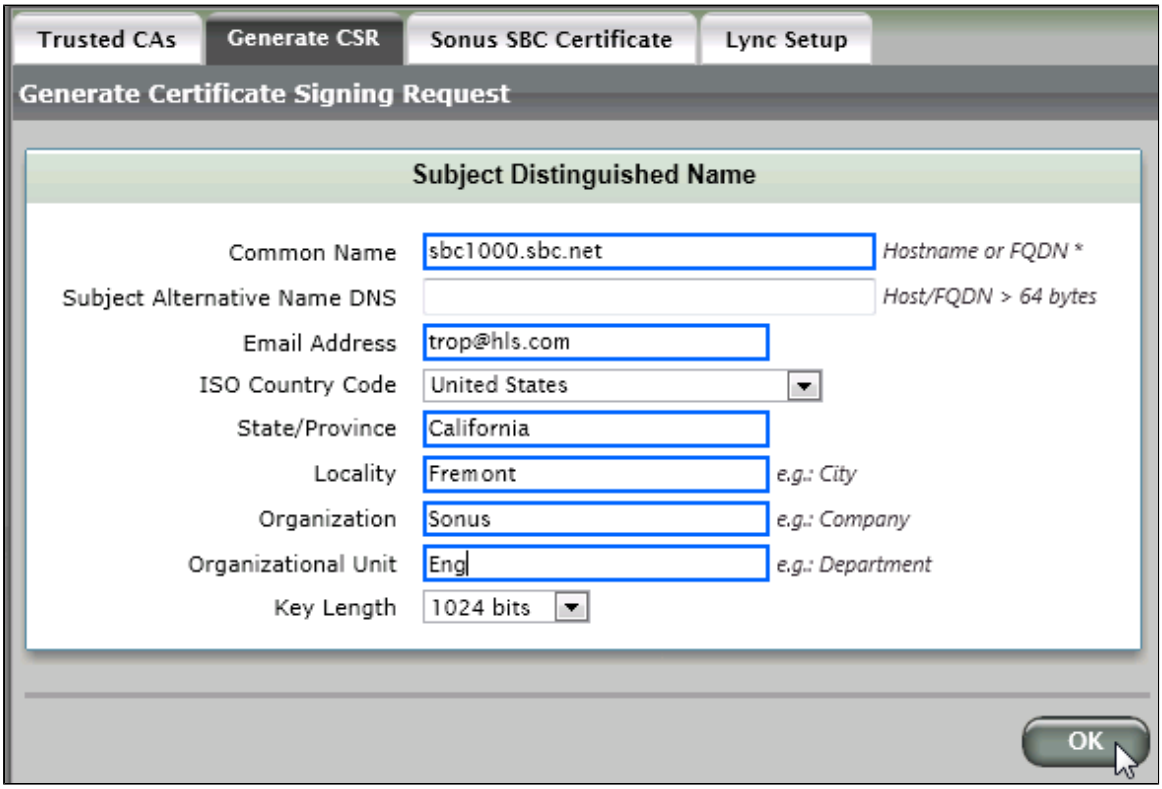


5. Click *OK*to import the root certificate.



6. Click the *Generate CSR*to generate a certificate request for the SBC. You will send this certificate request to be signed by the your certificae authority.

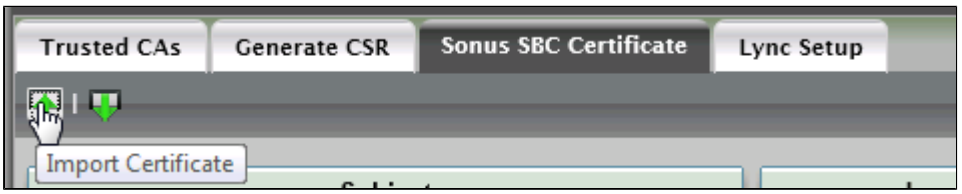
Copyright © 2015 Sonus Networks. All rights reserved.



7. Copy and paste the certificate request into a file and send it to your root certificate authority for signing.

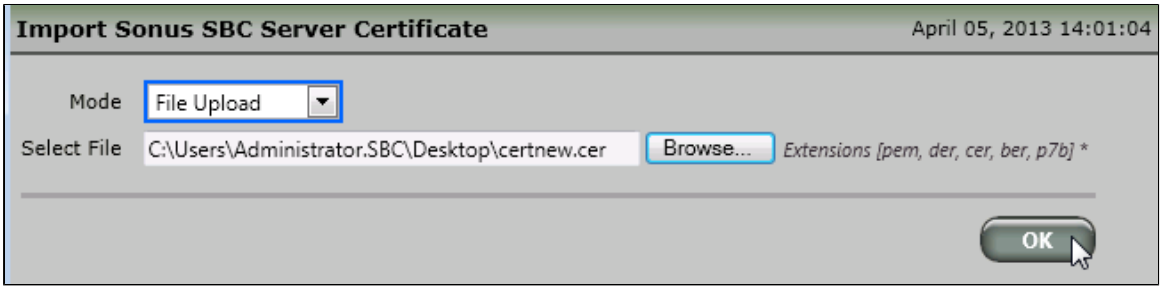


8. When the signed certificate is returned, click the *Sonus SBC Certificate*tab and import the certificate.

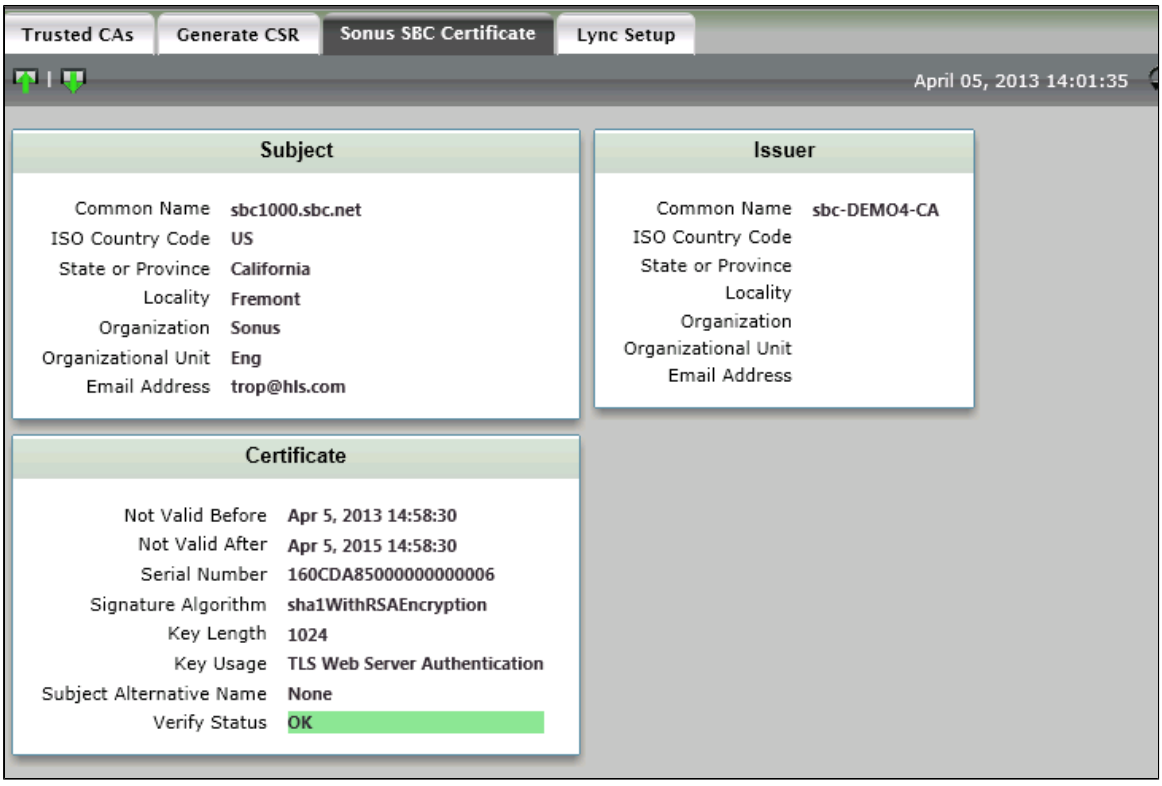


9. Set the *Mode* to *File Upload* and *Browse*to find the file containing the SBC certificate.

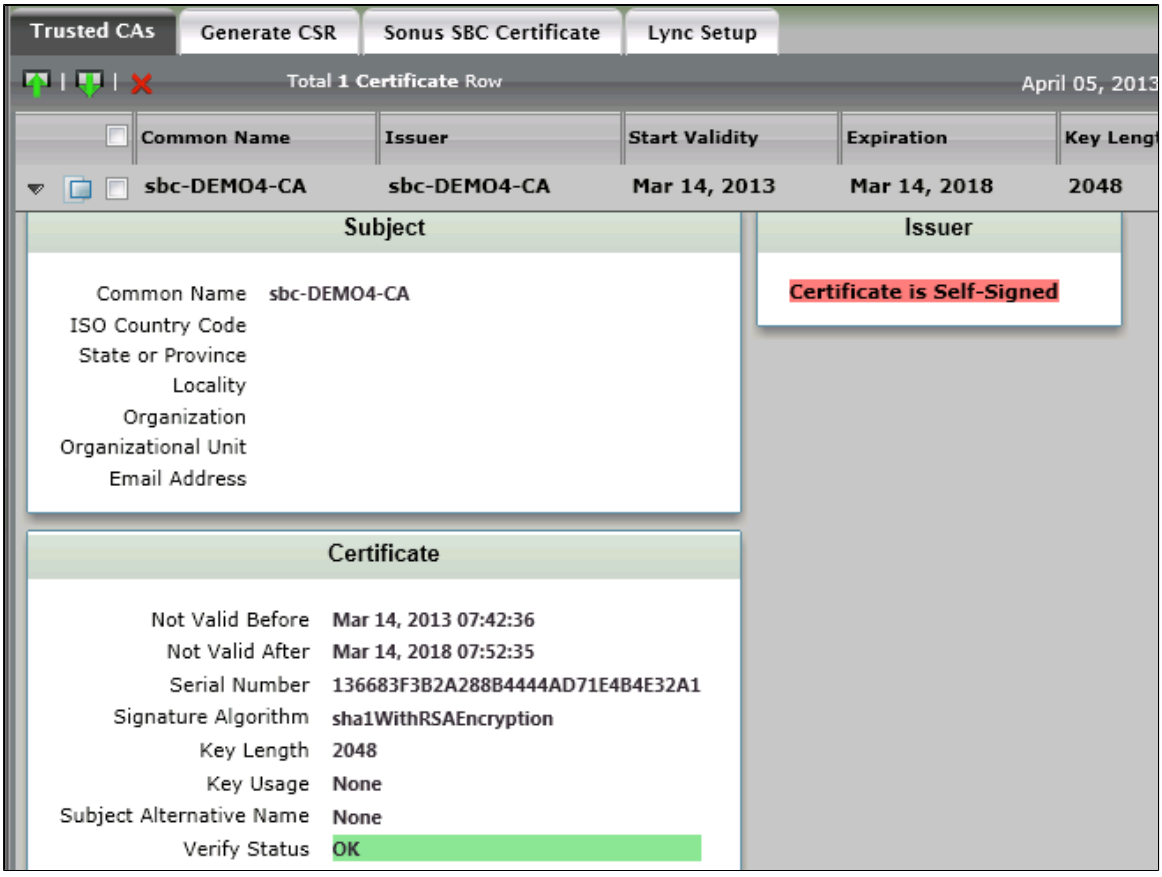
Copyright © 2015 Sonus Networks. All rights reserved.



10. Verify the SBC and root certificates

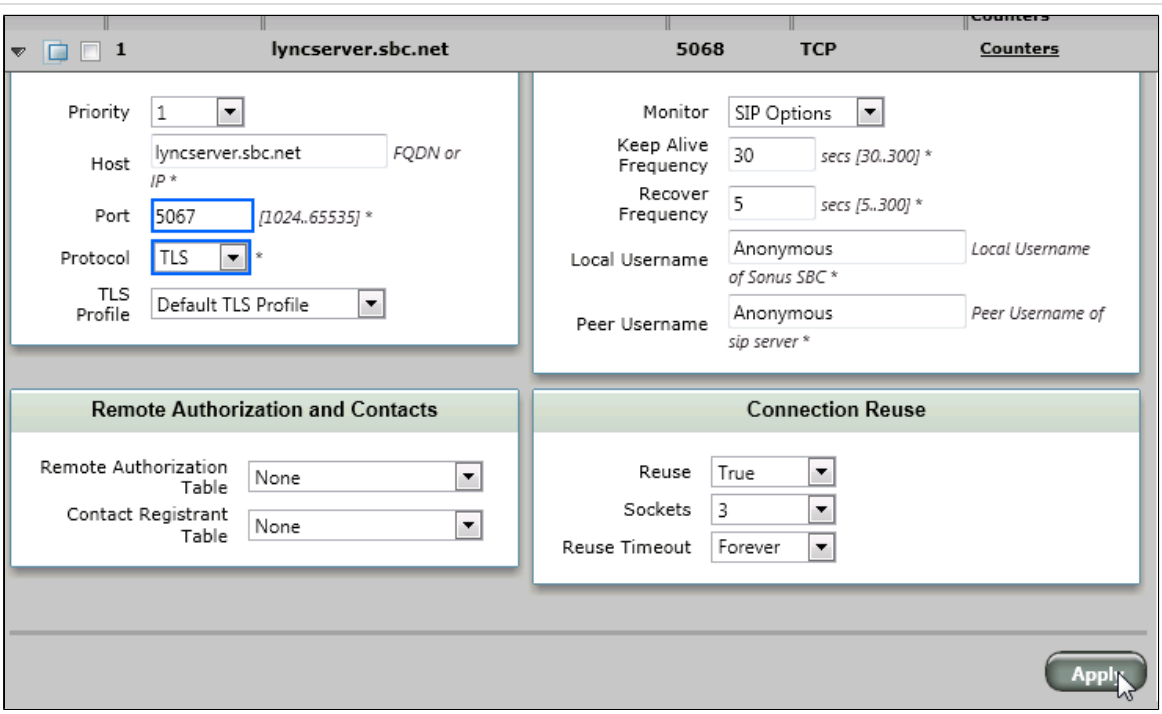


Copyright © 2015 Sonus Networks. All rights reserved.



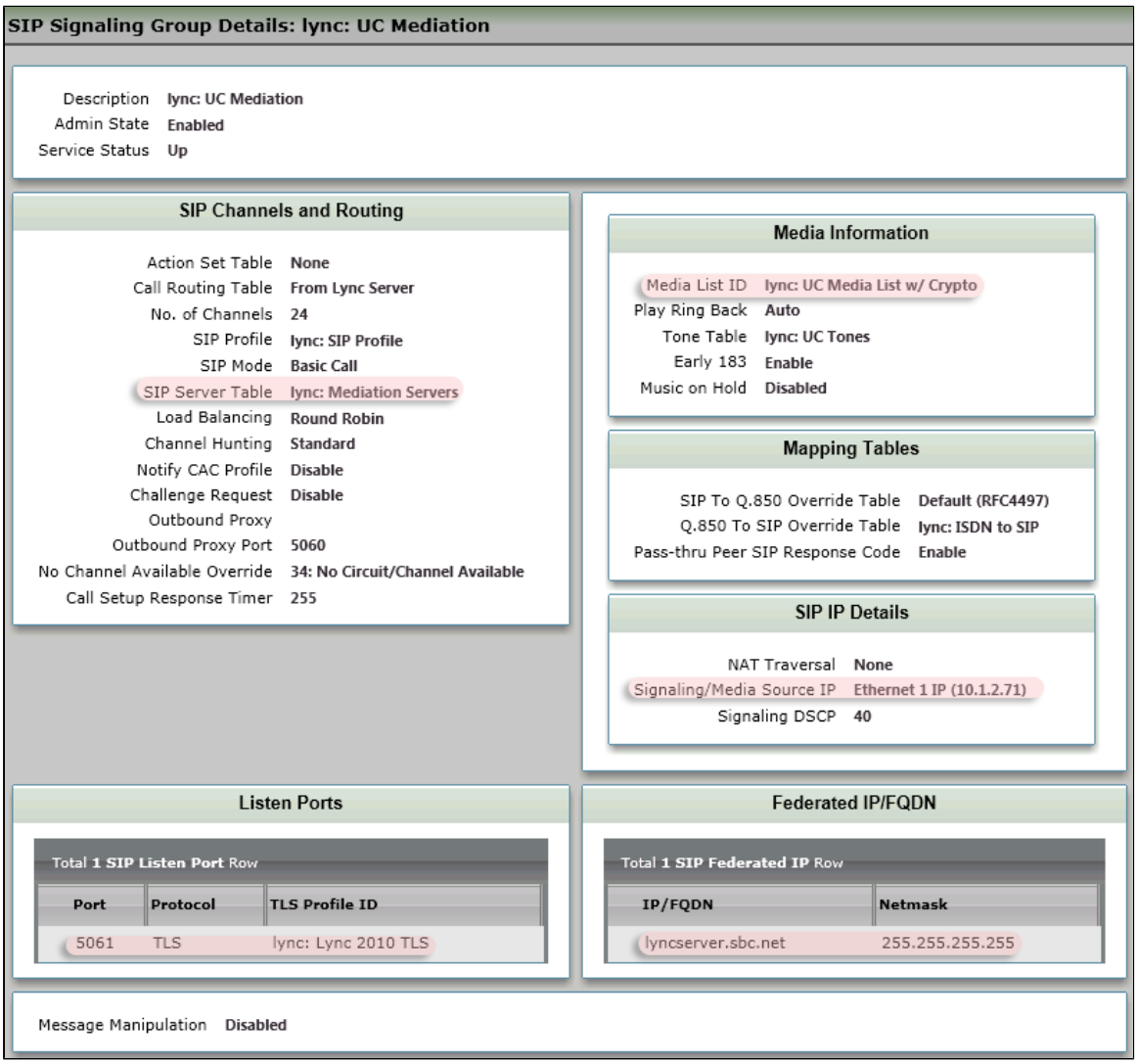
Setting the SIP Server and Signaling Group for TLS/SRTP

1. On the remote SBC, set/create the Lync Server SIP Server as shown.

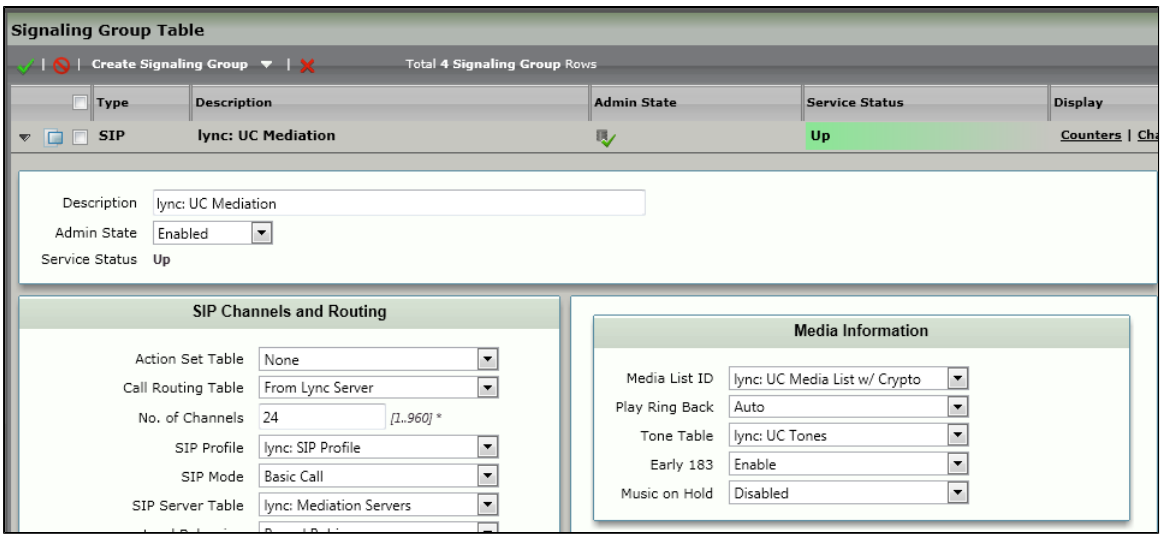


2. Set/create a Lync Server Signaling Group as shown.

Copyright © 2015 Sonus Networks. All rights reserved.



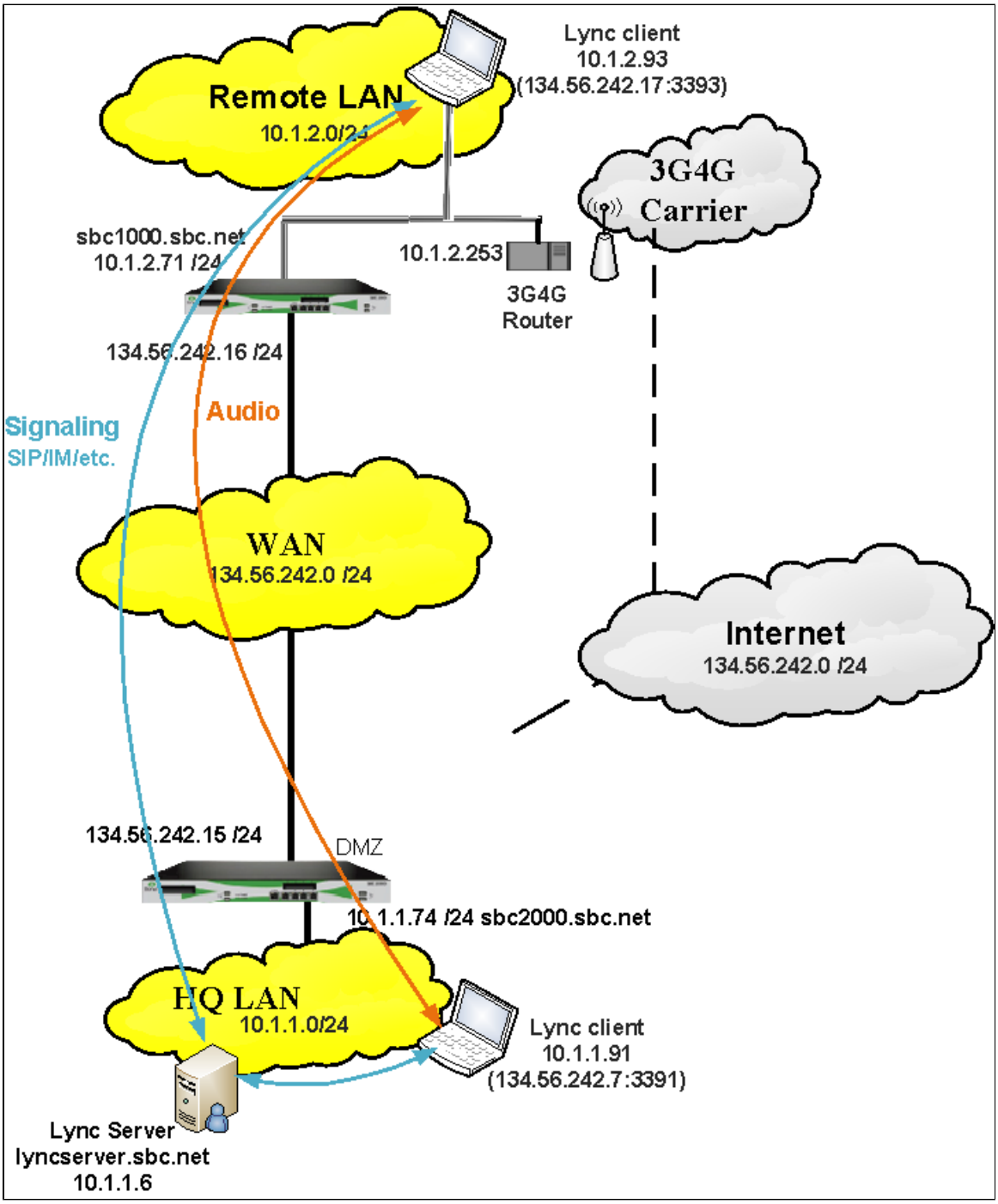
3. The Lync Server Signaling Group should come up



Copyright © 2015 Sonus Networks. All rights reserved.

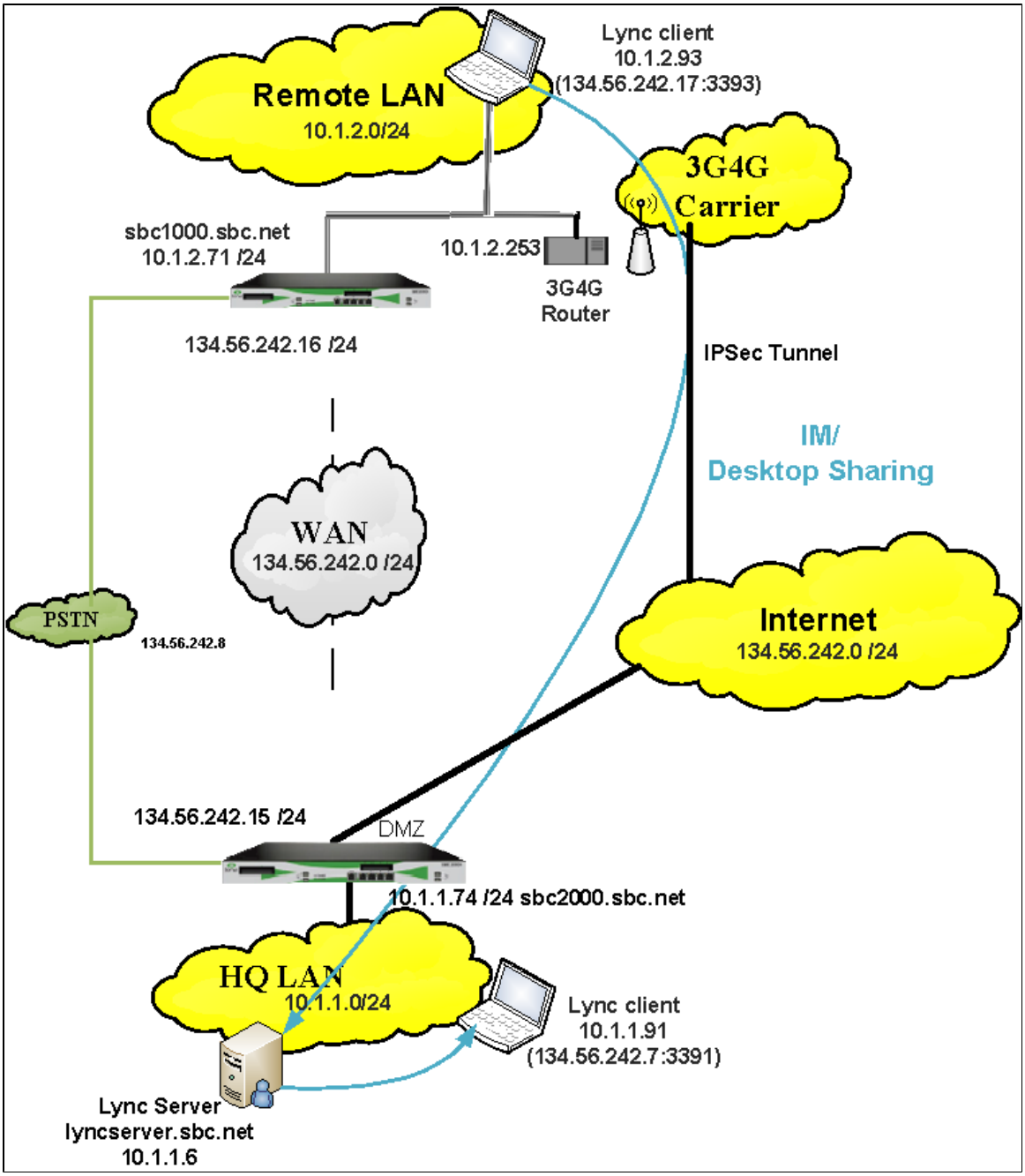
RBA Data Flows

WAN Up Flow



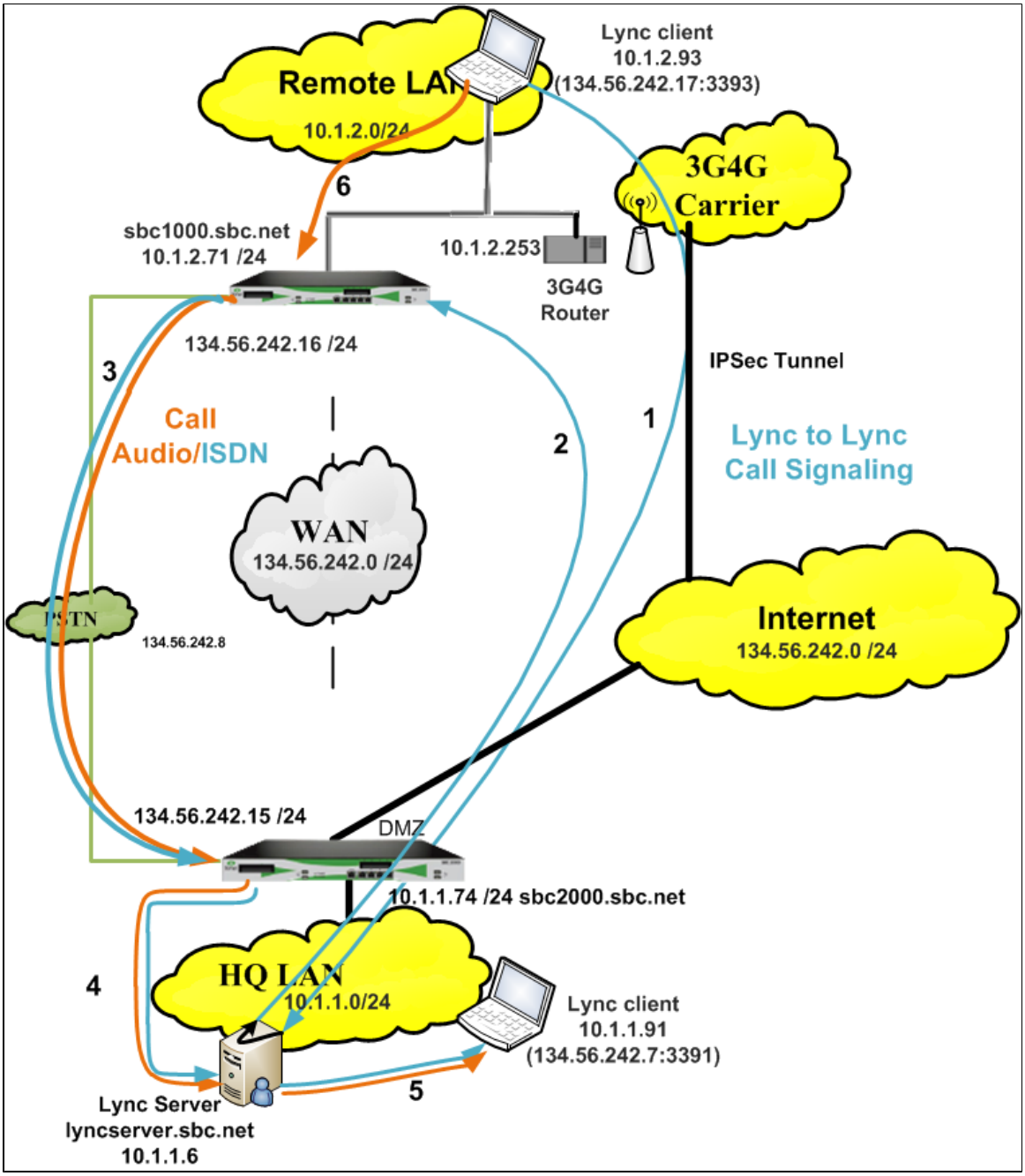
WAN Down Instant Message Flow

Copyright © 2015 Sonus Networks. All rights reserved.



WAN Down Lync-to-Lync Call Flow

Copyright © 2015 Sonus Networks. All rights reserved.



1. As an IP router, the SBC forwards the SIP request from the remote Lync to the Lync Server
2. Lync server sends a SIP request to the remote SBC (as a SIP --> PSTN gateway)
3. Remote SBC dials the HQ SBC via PSTN
4. HQ SBC (as a SIP Gateway) sends a SIP request to the Lync server
5. Lync Server sends SIP Request to the HQ Lync client
6. Remote Lync client audio bypasses directly to the remote SBC.

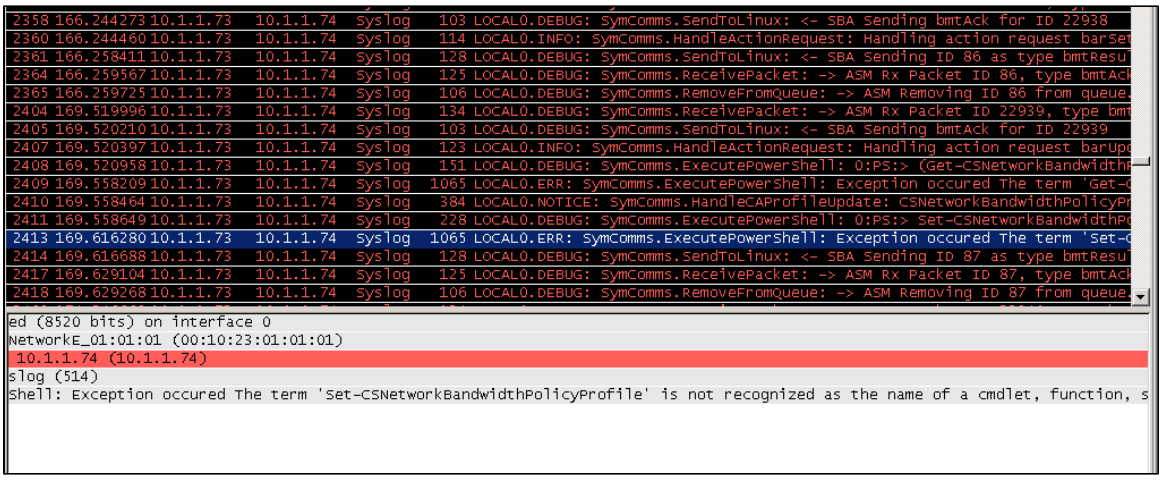
Troubleshooting

This section contains troubleshooting tips and suggests for various issues that may arise during RBA implementation.

Copyright © 2015 Sonus Networks. All rights reserved.

Prepare SBA not run

A wireshark trace which shows an exception due to an unrecognized cmdlet is likely due to the *Prep SBA* function not being executed. Review the *Configuring the RBA* section of this document.



RBA computer not a member of RTCUniversalServerAdmins group

Should the CAC bandwidths fail to change when the active link is switched between the WAN and the 3G4G link and this message appears in the RBA system Event Log, then the RBA computer (ASM) is not a member of the RTCUniversalServerAdmins group. See the *Domain Controller Configuration* section of this document.

```
Syslog message: LOCAL0.ERR: SymComms.ExecutePowerShell: Exception occured Cannot
open database "xds" requested by the login. The login failed.\r\nLogin failed for
user 'SBC\RBA1$'.. Could not connect to SQL server : [Exception=
```

A gpresult comamnd run from directly from the RBA computer (ASM) which shows that the computer is not a member of the RTCUniversalServerAdmins group.

C:\Users\Administrator>gpresult /R

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 4/5/2013 at 9:07:11 AM

RSOP data for SBC\Administrator on RBA1 : Logging Mode

OS Configuration: Member Server
OS Version: 6.1.7601
Site Name: Default-First-Site-Name
Roaming Profile: N/A
Local Profile: C:\Users\Administrator
Connected over a slow link?: No

COMPUTER SETTINGS

Copyright © 2015 Sonus Networks. All rights reserved.

CN=rba1,CN=Computers,DC=sbc,DC=net
Last time Group Policy was applied: 4/5/2013 at 8:06:36 AM
Group Policy was applied from: demo4.sbc.net
Group Policy slow link threshold: 500 kbps
Domain Name: SBC
Domain Type: Windows 2000

Applied Group Policy Objects

Default Domain Policy

The following GPOs were not applied because they were filtered out
---
Local Group Policy
Filtering: Not Applied (Empty)

The computer is a part of the following security groups

System Mandatory Level
Everyone
BUILTIN\Users
NT AUTHORITY\SERVICE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
BITS
CertPropSvc
EapHost
hkmsvc
IKEEXT
iphlpsvc
LanmanServer
MMCSS
MSiSCSI
RasAuto
RasMan
RemoteAccess
Schedule
SCPolicySvc
SENS
SessionEnv
SharedAccess
ShellHWDetection
wercplsupport
Winmgmt
wuauserv
LOCAL
BUILTIN\Administrators

Service Status Stays Yellow

Check the routing table on the remote SBC. The remote SBC **must** use default routes (0.0.0.0/0) rather than network routes.

Copyright © 2015 Sonus Networks. All rights reserved.

Link Monitor Configuration Table April 05, 2013 09:57:45

Total 2 **Link Monitor** Rows

	Description	IP Address/Host Name	CAC Profile	Service Status	Peer Type	Display	Primary Key
▶	WANup	134.56.242.15	WANup CAC	Ready	Gateway	Counters	1
▶	3G4G CAC	10.1.2.253	3G4Gup CAC	Ready	Gateway	Counters	2

Static IP Route Table April 05, 2013 09:58:13

Total 3 **IP Route** Rows

	Row ID	Destination IP	Mask	Gateway	Metric	Primary Key
	1	10.1.1.0	255.255.255.0	134.56.242.15	1	1
	2	134.56.105.0	255.255.255.0	134.56.242.1	1	2
	3	10.1.1.0	255.255.255.0	10.1.2.253	2	3

Route Table with No Default Routes

OPTIONS with Carrier's IP address

If the HQ SBC receives OPTIONS with the 3G4G carrier's source IP address, then the configured routing or hosts are incorrect. Make sure that the SBC are configured to use **only** the LAN interface addresses.

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-04-04 17:01:32,550] 4202 0031 com.sonus.sbc.sip DEBUG (TransportLayer.cpp:810)
- DataReadCB: Received message on [134.56.242.15]:5060 from [166.137.185.63]:34539
size=469, data: 0x2beb24, current chunk: 0
[2012-04-04 17:01:32,550] 4203 0030 com.sonus.sbc.sip TRACE (SipMessage.cpp:98) -
SipMessage: ctor msg 0x320918 35789
[2012-04-04 17:01:32,551] 4204 002f com.sonus.sbc.sip TRACE (MessageHeader.cpp:301)
- decodeLite: headerType=Via, commaDetection=1
[2012-04-04 17:01:32,551] 4205 002e com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type Allow
[2012-04-04 17:01:32,551] 4206 002d com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type Call-ID
[2012-04-04 17:01:32,551] 4207 002c com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type Content-Length
[2012-04-04 17:01:32,551] 4208 002b com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type CSeq
[2012-04-04 17:01:32,551] 4209 002a com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type From
[2012-04-04 17:01:32,551] 4210 0029 com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type Max-Forwards
[2012-04-04 17:01:32,551] 4211 0028 com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type Supported
[2012-04-04 17:01:32,551] 4212 0027 com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type To
[2012-04-04 17:01:32,551] 4213 0026 com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type User-Agent
[2012-04-04 17:01:32,551] 4214 0025 com.sonus.sbc.sip TRACE (SipMessage.cpp:634) -
decodeHeaders: SIP message Header type Via
[2012-04-04 17:01:32,551] 4215 0024 com.sonus.sbc.sip DEBUG (SipMessage.cpp:1202) -
decodedLength:469 decoded 0x320918:
[2012-04-04 17:01:32,551] 4216 0023

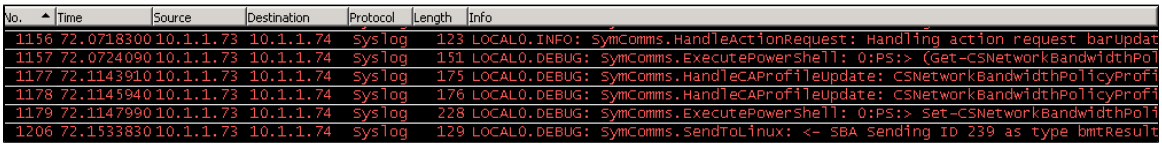
OPTIONS sip:sbc2000.sbc.net:5060 SIP/2.0
Allow: INVITE, ACK, CANCEL, BYE, UPDATE, NOTIFY, OPTIONS, REFER, REGISTER
Call-ID: call-71280200-0000-0010-0C13-0@10.1.2.71
Content-Length: 0
CSeq: 123 OPTIONS
From:  <sip:Anonymous@10.1.2.71:5060>;tag=8638f210-1
Max-Forwards: 70
Supported: replaces,update,100rel
To:  <sip:Anonymous@sbc2000.sbc.net:5060>
User-Agent: SONUS SBC1000/2000 3.0.0v222 UX
Via: SIP/2.0/UDP 10.1.2.71:5060;branch=z9hG4bK-UX-8638-f210-0180


[2012-04-04 17:01:32,552] 4217 0022 com.sonus.sbc.sip TRACE
(sipApplication.cpp:1264) - tlDataReceived: No errors found. Processing message.
[2012-04-04 17:01:32,552] 4218 0021 com.sonus.sbc.sip TRACE
(sipSignalingGroup.cpp:1522) - {SG(1) 0x30b808} CanAccept: Reject msg: call=1,
transport=0, filter=0 localPort=0
[2012-04-04 17:01:32,552] 4219 0020 com.sonus.sbc.sip DEBUG
(sipSignalingGroupConfig.cpp:713) - getBestSubnet: 166.137.185.63 - 0.0.0.0
[2012-04-04 17:01:32,552] 4220 001f com.sonus.sbc.sip DEBUG
(sipSignalingGroupConfig.cpp:713) - getBestSubnet: 166.137.185.63 - 166.137.185.63
[2012-04-04 17:01:32,552] 4221 001e com.sonus.sbc.sip DEBUG
(sipSignalingGroupConfig.cpp:713) - getBestSubnet: 166.137.185.63 - 0.0.0.0
```

RBA Command Working Properly

Copyright © 2015 Sonus Networks. All rights reserved.

This wireshark trace shows a properly working cmdlet to change the CAC bandwidth policies.



rev 0.2

Remote Update of ASM Recovery Partition

This article describes the steps necessary to update remotely the ASM Recovery Partition. While the recommended way is to use a flash drive locally plugged on the ASM in order to load a new ASM image into the system, we now support a method who do not require a physical access the SBC. The difficulty comes from getting the approx. 4GB file onto the ASM. You will need a way of transmitting this large ASM Image to the ASM over the network.

On this Page

- Update of ASM Recovery Partition Overview
- Before You Begin
  - Upload the ASM image into the ASM
- Update of ASM Recovery Partition

Related Articles

- Working with Microsoft Unified Communications
- Updating the ASM Recovery Partition

Update of ASM Recovery Partition Overview

The goal of this article is to help partner to update the recovery partition with a new ASM image (ie: Lync 2013 ASM image) in order to re-initialize with a new type of ASM image. This can be use in a process to remotely update the SBA from Lync 2010 to Lync 2013.

Before You Begin

Before proceeding, make sure that you have the appropriate ASM Image, downloadable from the Sonus SBC 1000-2000 Download Center. Multiple images are available, so be sure to select the image relevant to your system. It is a single file ASMimage.tar.

Upload the ASM image into the ASM

You will also need a way of getting this file onto the ASM - this can be done in any way you feel appropriate, such as:

- Putting the image file on a Windows or Samba server that the UX is able to reach.
- Using the file transfer facilities of Remote Desktop Connection. This can be done by allowing the ASM to access the local resources of your PC (enabled in Options, Local Resources, More, Drives), or by using the its clipboard Copy/Paste functionality (**Copy** the file in Windows Explorer of the local PC, and **Paste** it in the

Copyright © 2015 Sonus Networks. All rights reserved.

Remote Desktop session). Note that these methods transfers files quite slowly.
- Using the ASM itself to download the image directly from the Sonus SBC 1000-2000 Download Center . To do this, you will need to add ftp://ftp.net.com/ to Internet Explorer's Trusted Site list.

Update of ASM Recovery Partition

Once these have been satisfied, perform the following:

1. Enable Remote Desktop on the ASM (if it is not enabled already), as described in Enabling and Disabling Remote Desktop on the ASM .
2. Set an Administrator Password on the ASM, to facilitate this remote login - see Changing the ASM Admin Password.
3. Open Remote Desktop Connection and connect to the ASM (using the IP address configured earlier). Log in as Administrator, with the password entered in the previous step.
4. Once in the remote session, transfer the ASMimage.tar file onto the ASM using your chosen transfer method. Once it is on the system, move it to the root of the **C:** drive.
5. Now minimize the Remote Desktop session and return to the UX web UI, and select **Update ASM Recovery Partition**. from the **Tasks** tab. Ignore the USB references here - the operation will execute using the file we put on the **C:** drive.
6. Click **Apply**, and the process will begin. This will take about 5 minutes and report when it is complete.
7. Finally, return to the Remote Desktop session, and delete the ASMimage.tar file.

Lync Related Best Practices

The pages in this set of best practice articles relate to configuration and deployment of Microsoft Lync in conjunction with the Sonus SBC 1000/2000 series.

Using SBC to Process Lync to Lync Calls (Replicating an upstream forked call flow in a downstream installation)

Configuring the Sonus SBC 1000-2000 and Lync to Support Enhanced Emergency (911) Services

Configuring the Sonus SBC 1000-2000 for Lync E911 with PSAP Callback Number

LYNC side Gateway Failover Configuration

Lync 2013 Call Forwarding Integration to an ITSP

Using SBC to Process Lync to Lync Calls (Replicating an upstream forked call flow in a downstream installation)

Table of Contents

- Prerequisites
- Summary
- Configuration Prerequisites
  - Lync Server Configuration
  - Active Directory Configuration
- SBC Configuration
  - Active Directory Integration
  - Active Directory Verification
  - SBC AD-based Call Routing
- Making a Call
- Logs

Copyright © 2015 Sonus Networks. All rights reserved.

About this Page

- This document details how to configure the SBC to interoperate with Lync's ms-skip-rnl (RNL, Reverse Name Lookup) function.
- This document details how to configure the SBC for Active Directory (AD) Call Routing.
- This document outlines how to configure a downstream SBC to replicate the forked call flow possible in an upsteam SBC installation.

Related Articles

- SIP Message Manipulation
- Managing Signaling Groups

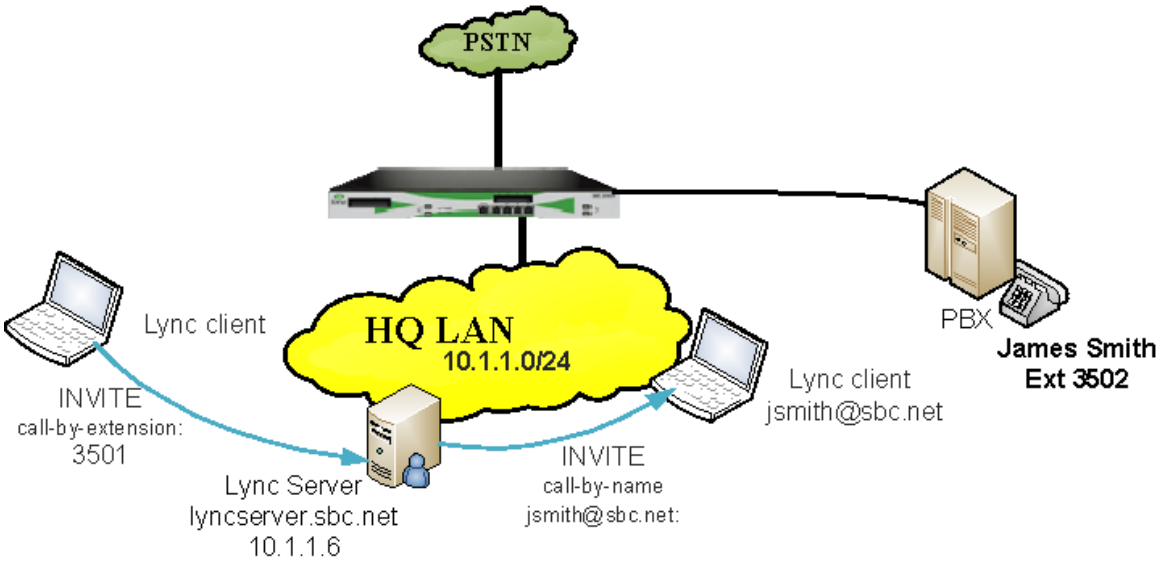
Prerequisites

Requires Sonus SBC1000/2000 Version 2.2 or later

Lync's RNL feature only functions when users dial by extension number. Even with RNL configured, the typical dial-by-name usage will continue to signal direct lync-to-lync calls.

Summary

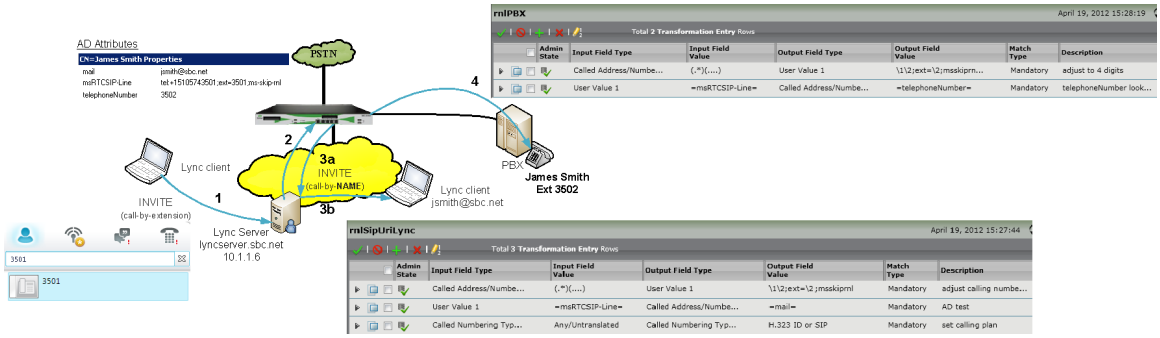
By default, when a Lync user dials another user via extension number, the Lync Server will attempt to match the extension number to an existing Lync user using RNL, Reverse Name Lookup. If a match is found, the call is effectively signaled directly between the two lync clients. If the RNL fails, the Lync Server routes the call to the associated PSTN gateway.



In cases wherein a network contains both Lync and PBX, but the SBC is installed downstream of the PBX, the RNL features offers a method of permitting the PSTN gateway (as opposed to the Lync Server) to perform the call routing function for all Lync-originated calls. In so doing, it is possible to use the forking feature on the PSTN gateway to simultaneously fork a Lync-originated call to a PBX extension and a Lync client. Although this capability is possible

Copyright © 2015 Sonus Networks. All rights reserved.

via the Lync client's *forward* function, that feature must be invoked individually by each user rather than programatically for all users via Lync's administator's tools.



Step	Action
1	Lync client dials by extension, forwards INVITE to Lync Server
2	Lync Server skips RNL, forwards INVITE to SBC
3a	SBC performs AD call routing, sends SIP-URI INVITE to Lync Server
3b	As INVITE is by name (i.e. URI, jsmith@sbc.net), Lync forwards INVITE to Lync client
4	Simultaneously to Step 3, SBC uses AD call routing to fork call to PBX extension

The ms-skip-rnl causes dial-by-extension calls to be routed by the SBC rather than the Lync Server (the Lync Server forwards all INVITEs directly to the SBC). Then, using the SBC's AD-integrated routing, it is possible to fork the dial-by-extension calls to the Lync Server and PBX, thus replicating the functionality of a SBC upstream installation.

The RNL function complicates installations that contain remote SBCs. Dial-by-extension calls made from remote sites will be processed by the SBC at the remote sites. From there, the remote SBC will need to send the Lync forked leg back to the Lync Server and the PBX fork leg to the PBX. The design of the network must either send the calls directly from the remote SBC to the Lync Server, or send them to the HQ SBC which can then route the call to the Lync Server.

Another complication arises as calls from Lync, which would normally only be destined for the PSTN/PBX, could be destined to the PSTN, PBX or Lync. Call route and translation tables will need to be constructed to account for calls from Lync that are subsequently returned to Lync.

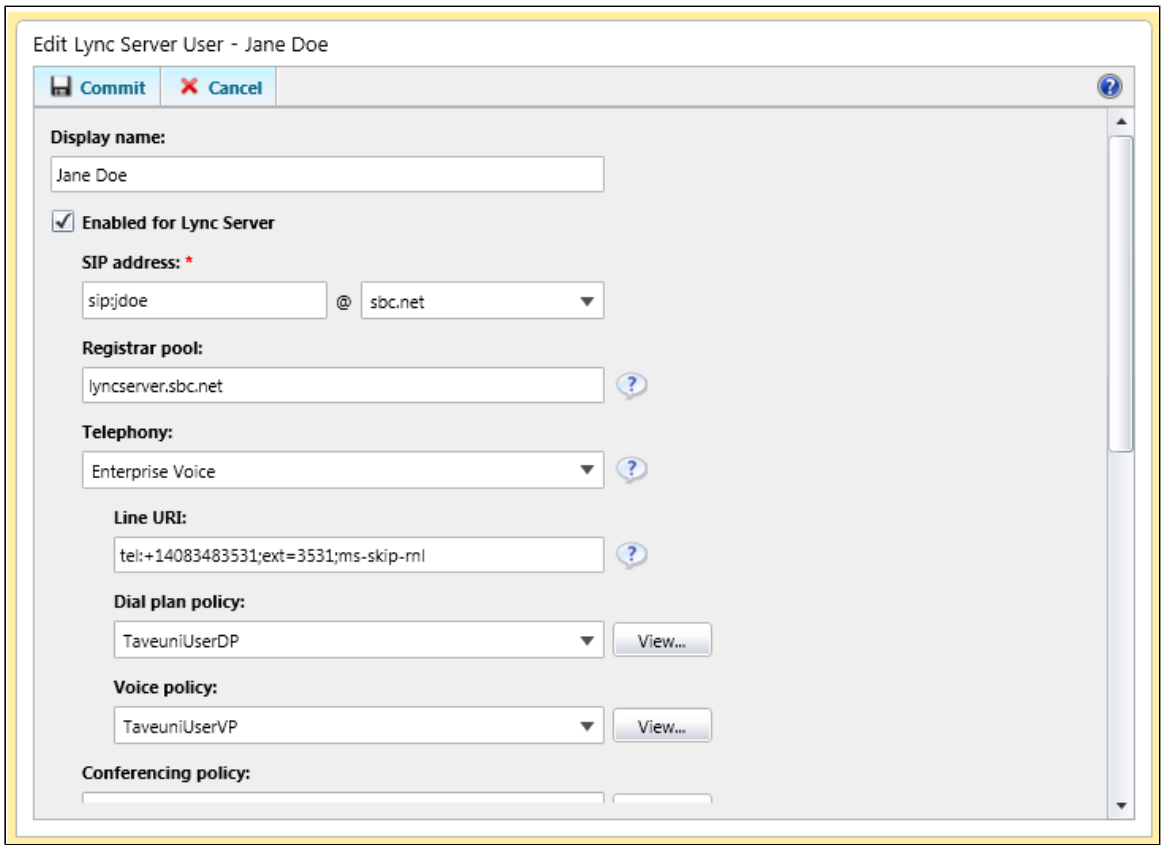
Configuration Prerequisites

Lync Server Configuration

To permit the RNL function, the Lync caller's Line URI must be configured with an *;ext* **and** the *ms-skip-rnl* tag.

Copyright © 2015 Sonus Networks. All rights reserved.

1. Add or modify the caller's Lync record



Active Directory Configuration

For purposes of this document, the *Work Phone* AD attribute will be used to store the target PBX number.

2. Add or modify the callee's AD record

Copyright © 2015 Sonus Networks. All rights reserved.



SBC Configuration

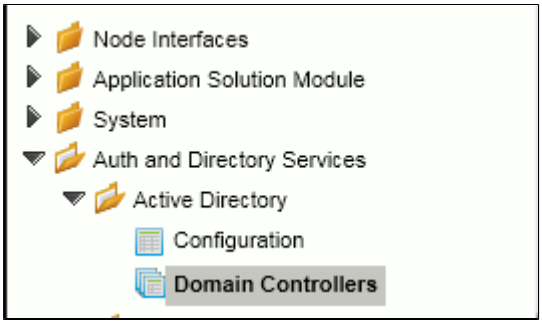
The SBC must be configured for:

- Active Directory Integration
- Forked Calling
- AD-based Call Routing

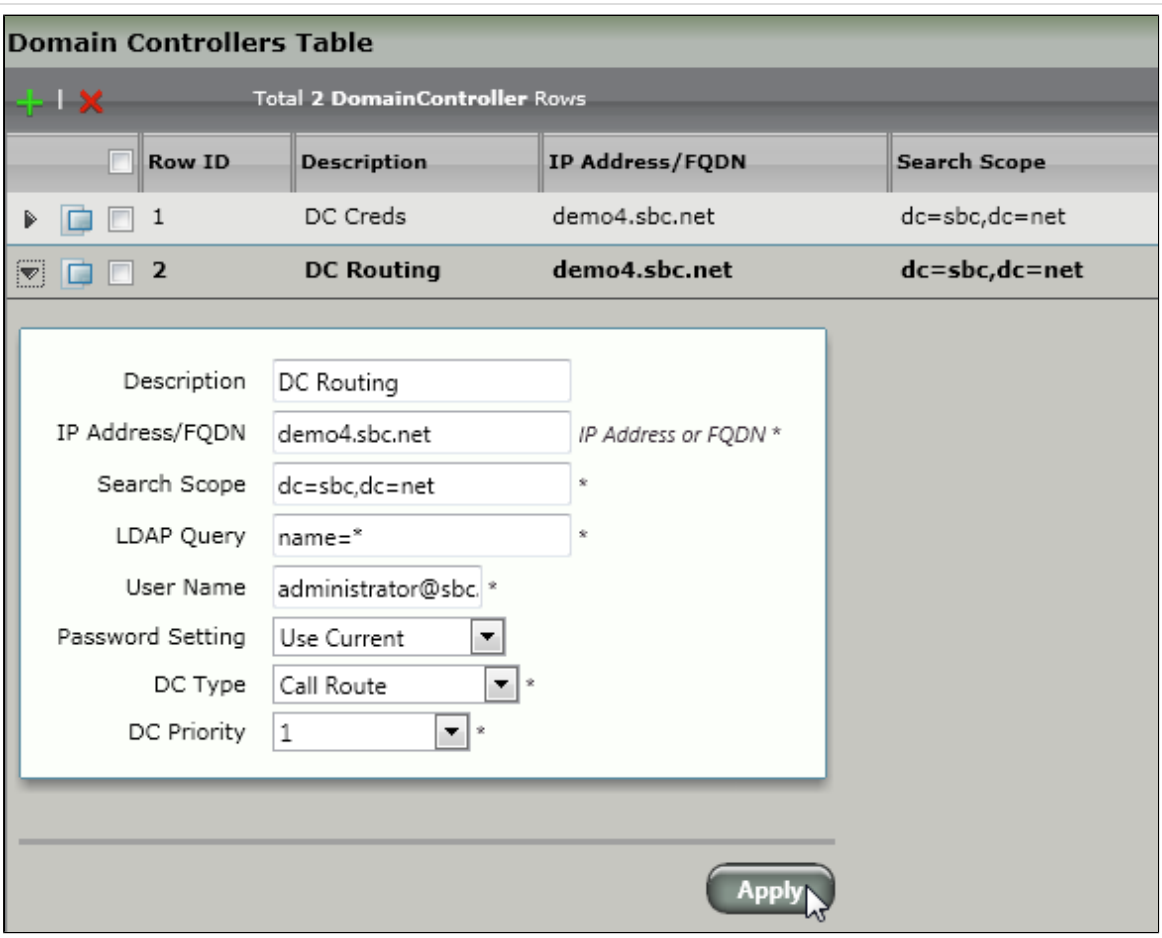
Active Directory Integration

1. Click the *Settings* tab in the top nagivation, then select *Domain Controllers* in the left-hand navigation

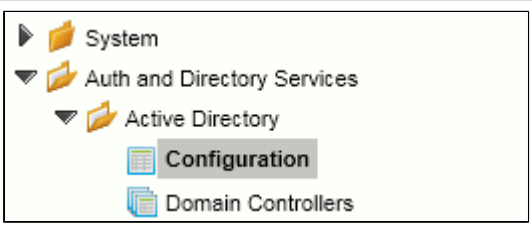
Copyright © 2015 Sonus Networks. All rights reserved.



2. Enter the AD information for your network



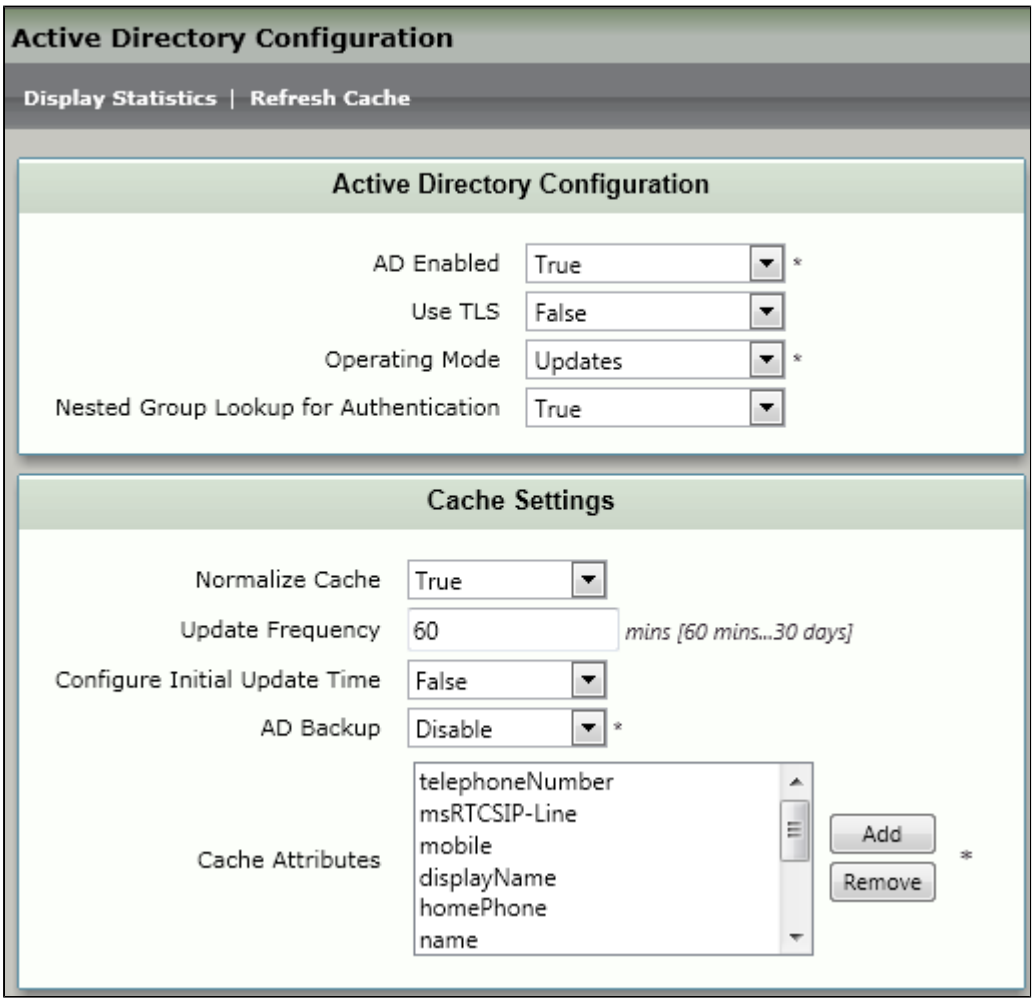
3. Click *Configuration* in the left-hand navigation.



4. Configure the *Active Directory Configuration* as shown. Add whatever *Cache Attributes* you plan to use.

Copyright © 2015 Sonus Networks. All rights reserved.

The minimum configuration for this example document should include the attributes: msRTCSIP-Line, name, displayName, mail, telephoneNumber



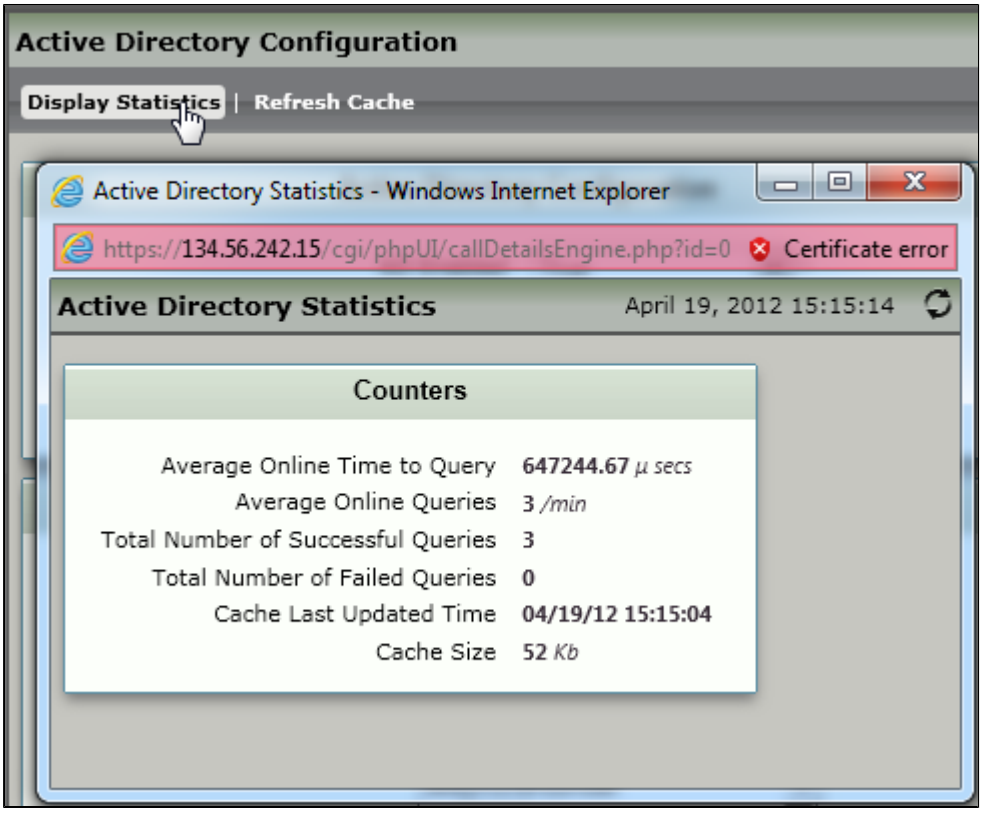
Active Directory Verification

1. With the AD configuration completed, click *Refresh Cache*.

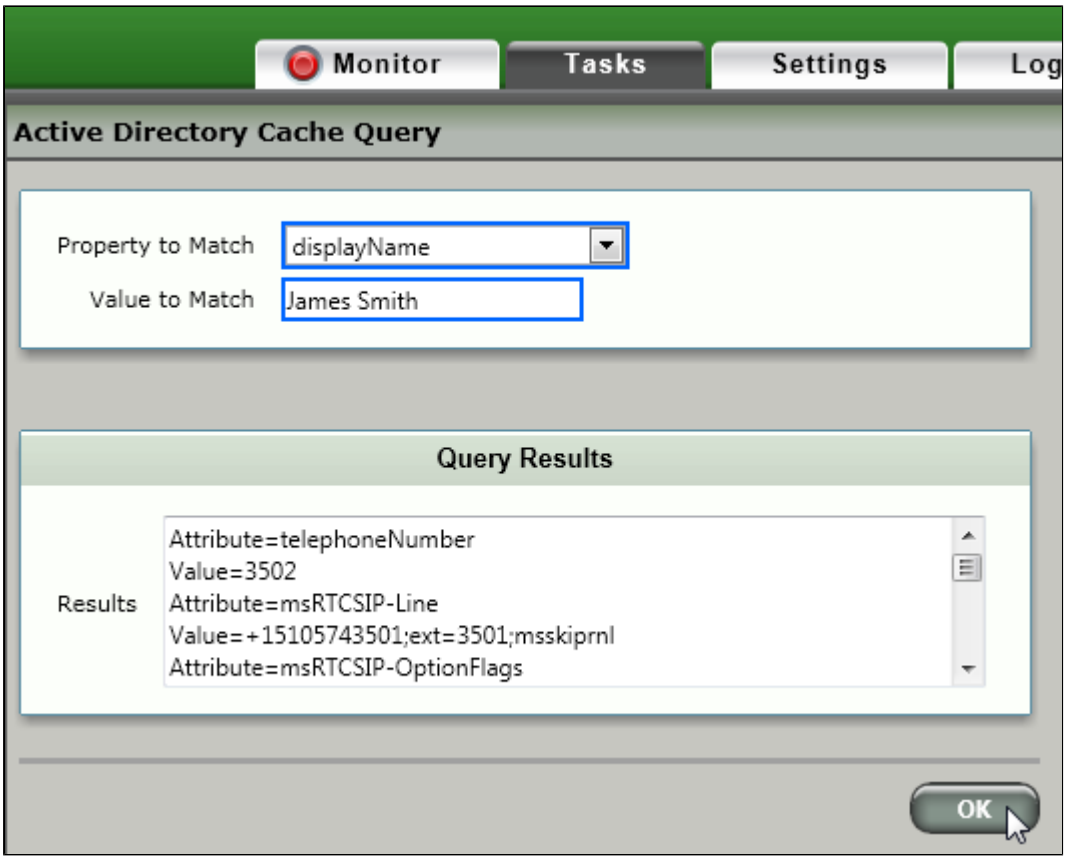


2. Click *Display Statistics* and verify that the AD queries are succeeding.

Copyright © 2015 Sonus Networks. All rights reserved.



3. Select the *Tasks* tab in the top navigation and click *Active Directory Cache Query*. In the form, pick an AD attribute from the pulldown and supply a corresponding value.

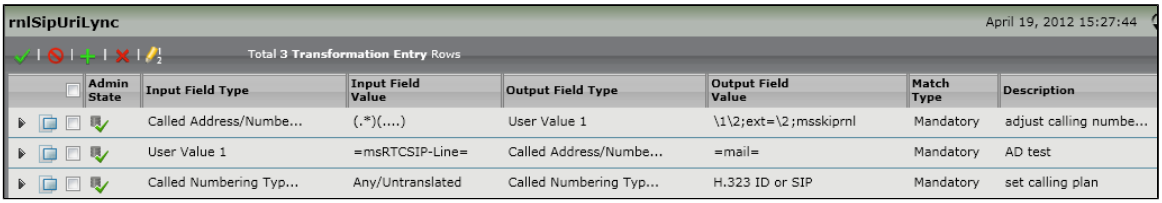


Copyright © 2015 Sonus Networks. All rights reserved.

Queries of the msRTCSIP-Line must match precisely what appears in the Lync *Line URI* for the desired user.

SBC AD-based Call Routing

1. Create a transformation table. The entries in this transformation table:



rnlSipUriLync — April 19, 2012 15:27:44

Total 3 Transformation Entry Rows

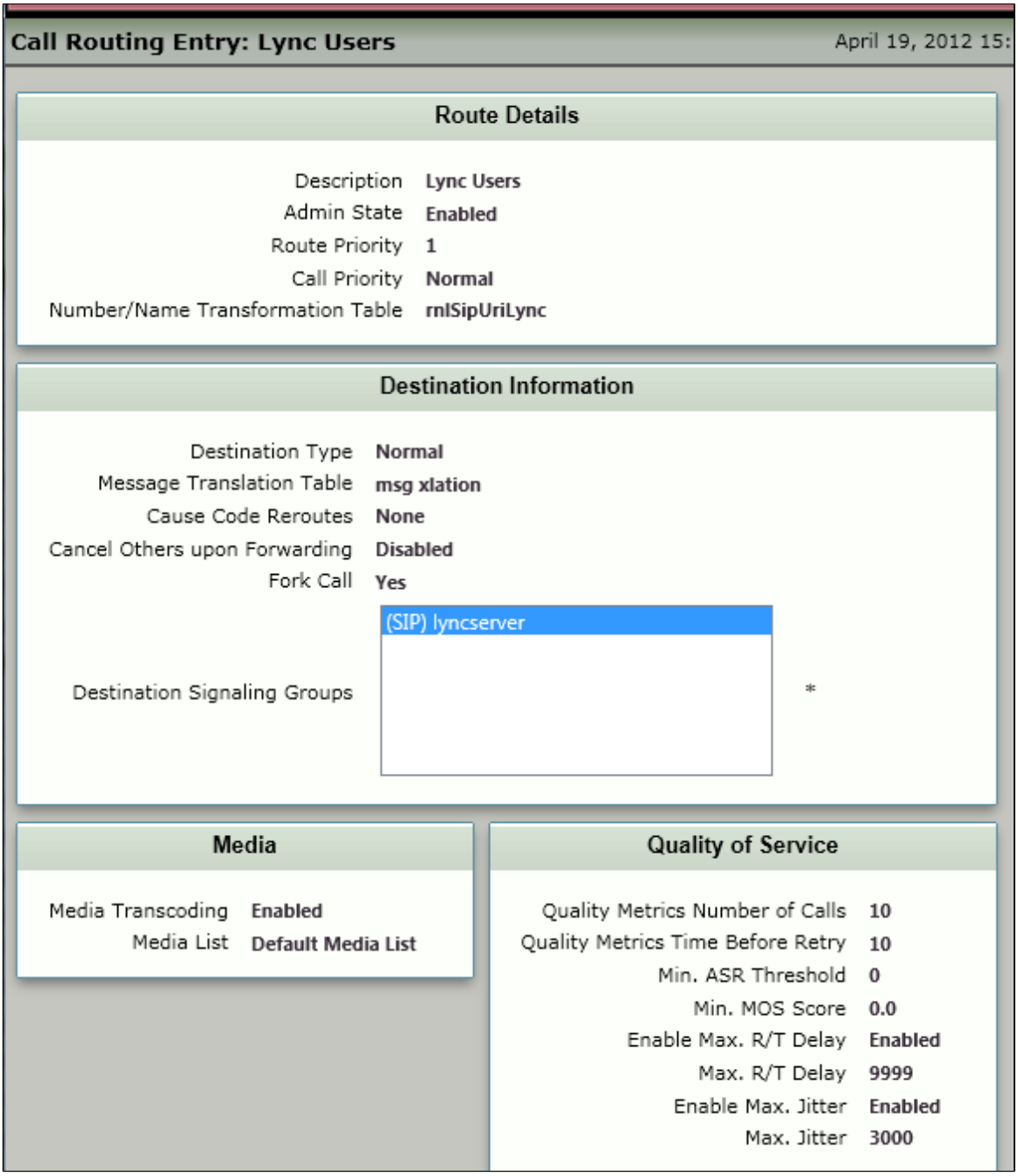
Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
	Called Address/Numbe...	(.*)(....)	User Value 1	\1\2;ext=\2;msskiprnl	Mandatory	adjust calling numbe...
	User Value 1	=msRTCSIP-Line=	Called Address/Numbe...	=mail=	Mandatory	AD test
	Called Numbering Typ...	Any/Untranslated	Called Numbering Typ...	H.323 ID or SIP	Mandatory	set calling plan

- Strip the calling number to 4 digits, then assembles the called number information into a form that matches the msRTCSIP-Line (Lync User URI) and places that information in the *User Value 1* IE.
  - \2 = the four digit extension
  - \1 = the digits preceeding the extension
- Searches msRTCSIP-Line for a match to the value contained in *User Value 1*. If there is a match, the value from the *mail* AD attribute is placed in the *Called Number* IE. The mail value is used as the call returning to Lync must be dialed as a SIP URI as opposed to the Tel URI typically used for SIP Gateway calls to Lync Server.
- Sets the *Called Numbering Type* to *H.323/SIP*.

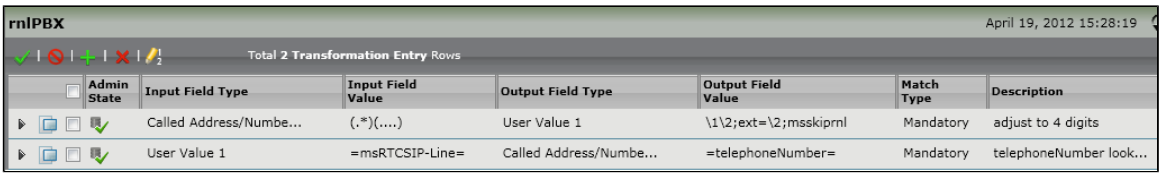
The AD *Normalize Cache* function automatically removes dashes (-) from AD attribute values, thus ms-skip-rnl becomes msskiprnl for purposes of matching in the transformation table.

2. Create a call route to send the call to Lync. Be sure to set *Fork Call* to *Yes* and set the corresponding transformation table.

Copyright © 2015 Sonus Networks. All rights reserved.



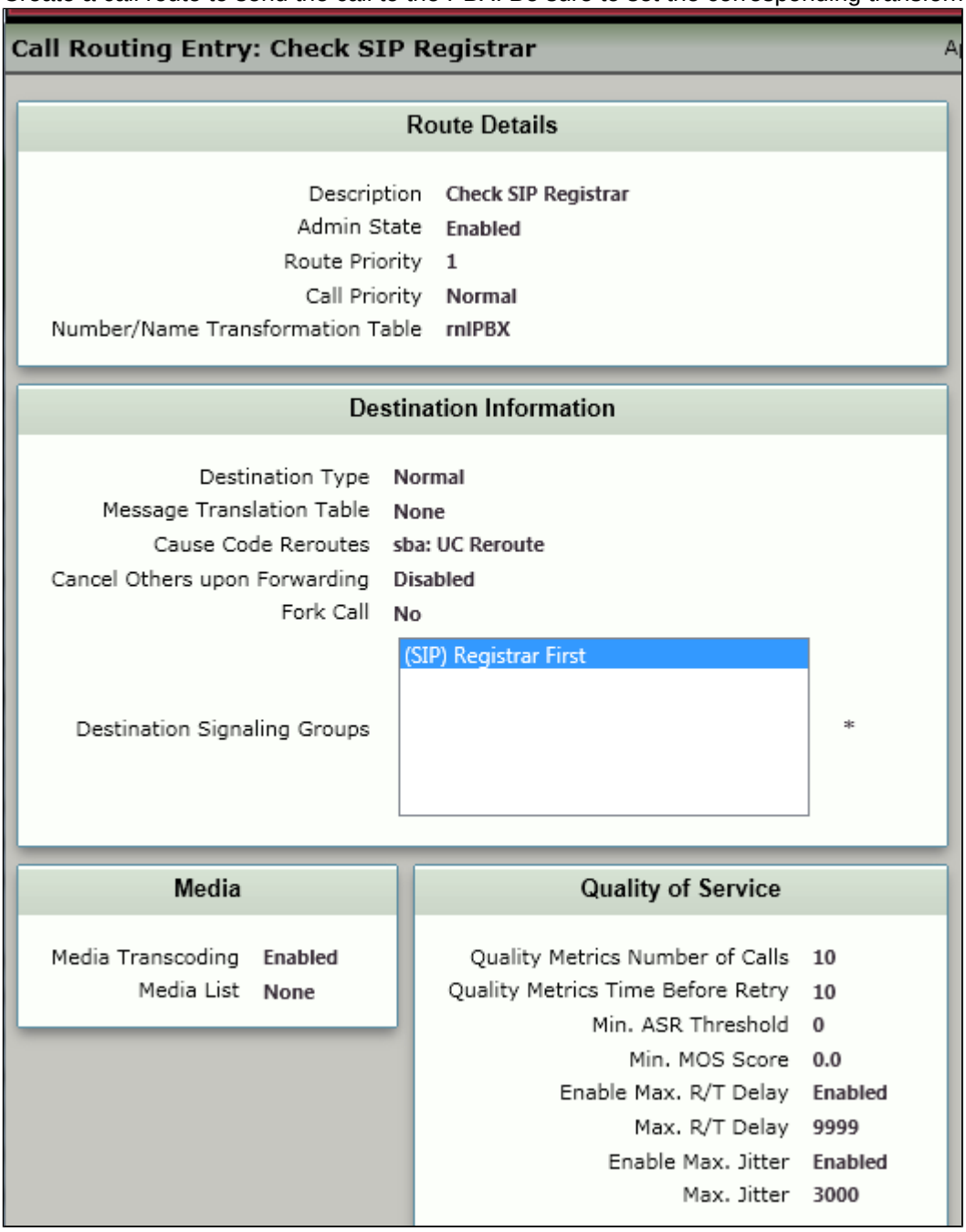
3. Create a transformation table.



- Strip the calling number to 4 digits, then assembles the called number information into a form that matches the msRTCSIP-Line (Lync User URI) and places that information in the *User Value 1* IE.
- Searches msRTCSIP-Line for a match to the value contained in *User Value 1*. If there is a match, the value from the *telephoneNumber* (Work Phone) AD attribute is placed in the *Called Number* IE.

Copyright © 2015 Sonus Networks. All rights reserved.

4. Create a call route to send the call to the PBX. Be sure to set the corresponding transformation table.

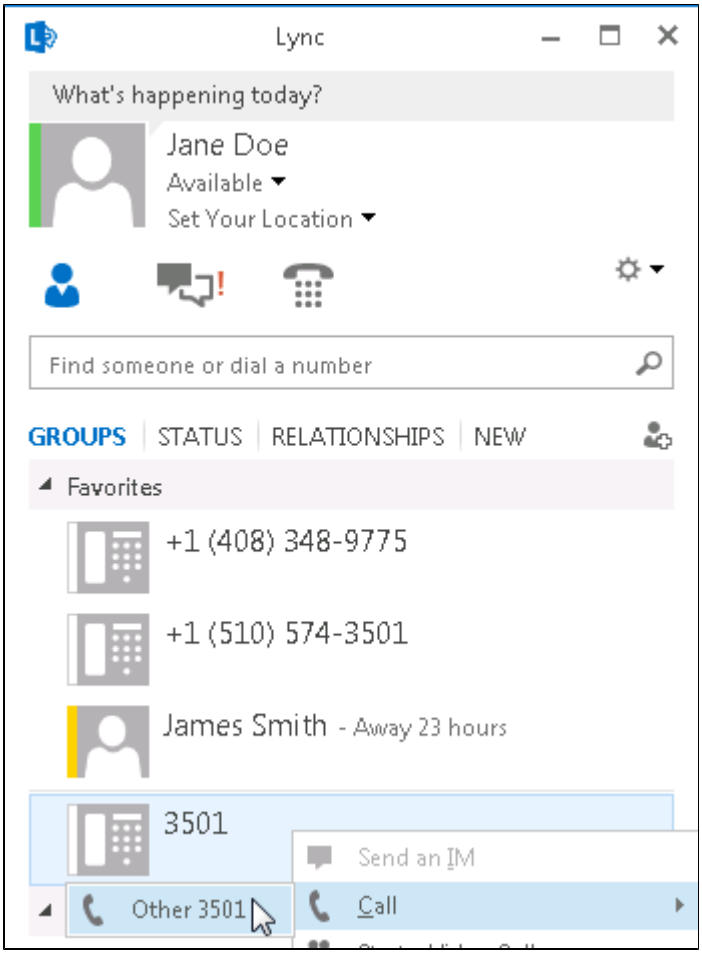


This document uses a SIP Phone registered to the SBC as opposed to a PBX. Adjust the call route and signaling group for your specific network implementation.

Making a Call

You must call by extension to employ the RNL feature and have the call processed by the SBC. Call by Lync will continue to be routed by the Lync Server.

Copyright © 2015 Sonus Networks. All rights reserved.



Logs

```
2012-04-21 11:36:27,041] 5908 0009 com.sonus.sbc.ccc INFO (fsmco.cpp:2095) -
[2749][CID:150] Requesting call route for route table 1, called# [+15105743501]
[2012-04-21 11:36:27,041] 5909 0008 com.sonus.sbc.ccc.libcommon TRACE
(AFSessionManagementLayer.cpp:1219) - [0x0c000838]
SMSession::SendSessionRequest(ObjHandle=0x690c84)
[2012-04-21 11:36:27,041] 5910 0007 com.sonus.sbc.ccc.libcommon TRACE
(AFSessionManagementLayer.cpp:1121) - Checking CBO(0x6d2f58) for
SMSession(UID=0x0c0021d2 | ObjHandle=0x7570d8)
[2012-04-21 11:36:27,041] 5911 0006 com.sonus.sbc.ccc.libcommon TRACE
(AFSessionManagementLayer.cpp:1467) - SMSession::Stored CBO-UID
(UID=0xc0008a2|ObjHandle=0x6d2f58) for Session (Uid=0x0c0021d2 | ObjHandle=0x7570d8)
[2012-04-21 11:36:27,041] 5912 0005 com.sonus.sbc.ccc.libcommon TRACE
(AFSessionManagementLayer.cpp:1472) - (+)SMSession: creating session
(UID=0x0c0021d2|ObjHandle=0x7570d8) level=1 session id=151, PID=0x0c00,
<parent>0xc000838|0x690c84.
[2012-04-21 11:36:27,041] 5913 0004 com.sonus.sbc.ccc.libcommon TRACE
(AFSessionManagementLayer.cpp:1486) - SMSession: new session
(UID=0x0c0021d2|ObjHandle=0x7570d8) id=32919 subsession id=32769 pCBO=0x6d2f58,
<parent>0xc000838|0x690c84.
[2012-04-21 11:36:27,041] 5914 0003 com.sonus.sbc.ccc.libcommon DEBUG
(AFSessionManagementLayer.cpp:1790) - Sending REQ: session id=15:32919/32769/0
message=MSG_CR_ROUTE msg len=166 end session=0
sessions={lvl=0}<parent>0x0|(nil)-[this]0xc000838|0x690c84-(sub)0xc0021d2|0x7570d8.
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
Process ID 5745
[2012-04-21 11:36:27,041] 5915 0002 com.sonus.sbc.ccc INFO (smmgr.h:77) - [2750]Sent
Session REQ MSG_CR_ROUTE/0x70e6a0 on Parent Session:0x690c84 Session:0x7570d8
[2012-04-21 11:36:27,042] 5916 0001 com.sonus.sbc.ccc DEBUG (fsmco.cpp:2595) -
[2751][FSMCo[CID:150]][cosW4_IB_ADD_LEG]=>[cosSETUP]
[2012-04-21 11:36:27,043] 5917 0009 com.sonus.sbc.route.libcommon DEBUG
(AFSessionManagementLayer.cpp:645) - SMConnection: Received REQ: id=12:32919/32769/0
session bit=1 moredata bit=0 message=MSG_CR_ROUTE
[2012-04-21 11:36:27,043] 5918 0008 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1472) - (+)SMSession: creating session
(UID=0x110008cf|ObjHandle=0x1f27d0) level=1 session id=32919, PID=0x1100,
<parent>0x11000014|0x1e8db4.
[2012-04-21 11:36:27,043] 5919 0007 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1486) - SMSession: new session
(UID=0x110008cf|ObjHandle=0x1f27d0) id=32919 subsession id=32769 pCBO=0x190a38,
<parent>0x11000014|0x1e8db4.
[2012-04-21 11:36:27,043] 5920 0006 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:736) - SMconnection (0x1e8da0):
session=0x1f27d0(0x1e8db4) pCBO=(nil), pCBOFunction=0x190a38.


[2012-04-21 11:36:27,043] 5921 0005 com.sonus.sbc.route INFO (callrouter.cpp:2193) -
Handling route request.
[2012-04-21 11:36:27,044] 5922 0004 com.sonus.sbc.route INFO (callrouter.cpp:2272) -
Using table Default Route Table (1) to route call.
[2012-04-21 11:36:27,044] 5923 0003 com.sonus.sbc.route DEBUG (translation.cpp:1293)
- Performing MANDATORY transformation using entry adjust calling number AD lookup
(13.1(1)).
[2012-04-21 11:36:27,044] 5924 0002 com.sonus.sbc.route DEBUG (translation.cpp:636)
- Successful regex match of "tfCalledNumber" field for "(.*)(....)" (updated
"(.*)(....)") with input of "+15105743501"
[2012-04-21 11:36:27,044] 5925 0001 com.sonus.sbc.route DEBUG (translation.cpp:681)
- Regex replacement output of "tfUserValue1" field is
"+15105743501;ext=3501;msskiprnl"
[2012-04-21 11:36:27,045] 5926 0001 com.sonus.sbc.route INFO (translation.cpp:1206)
- Doing AD lookup for field 'msRTCSIP-Line' with value
'+15105743501;ext=3501;msskiprnl'
{panel}
{panel}
[2012-04-21 11:36:27,045] 5927 0001 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1273) -
SMSession::SendTransactionRequest(UID=0x1100000c | ObjHandle=0x1802b4)
[2012-04-21 11:36:27,045] 5928 0001 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1472) - (+)SMSession: creating session
(UID=0x110008d0|ObjHandle=0x1f55f0) level=2 session id=1012, PID=0x1100,
<parent>0x1100000d|0x189488.
[2012-04-21 11:36:27,045] 5929 0001 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1491) - SMSession: new session
(UID=0x110008d0|ObjHandle=0x1f55f0) id=0 subsession id=33780 pCBO=0xef378,
<parent>0x1100000d|0x189488.
[2012-04-21 11:36:27,046] 5930 0001 com.sonus.sbc.route.libcommon DEBUG
(AFSessionManagementLayer.cpp:1790) - Sending REQ: transaction id=10:0/33780/0
message=MSG_ADS_AD_QUERY msg len=81 end session=0
sessions={lvl=1}<parent>0x1100000c|0x1802b4-[this]0x1100000d|0x189488-(sub)0x110008d0|0
Process ID 5670
[2012-04-21 11:36:27,046] 5931 0009 com.sonus.sbc.ads.libcommon DEBUG
(AFSessionManagementLayer.cpp:645) - SMConnection: Received REQ: id=10:0/33780/0
session bit=0 moredata bit=0 message=MSG_ADS_AD_QUERY
[2012-04-21 11:36:27,046] 5932 0008 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1121) - Checking CBO(0xd0790) for
SMSession(UID=0x1b000586 | ObjHandle=0x1d9888)
[2012-04-21 11:36:27,046] 5933 0007 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1467) - SMSession::Stored CBO-UID
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
(UID=0x1b000001|ObjHandle=0xd0790) for Session (Uid=0x1b000586 | ObjHandle=0x1d9888)
[2012-04-21 11:36:27,046] 5934 0006 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1472) - (+)SMSession: creating session
(UID=0x1b000586|ObjHandle=0x1d9888) level=2 session id=33780, PID=0x1b00,
<parent>0x1b000019|0xfb6c0.
[2012-04-21 11:36:27,046] 5935 0005 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1491) - SMSession: new session
(UID=0x1b000586|ObjHandle=0x1d9888) id=0 subsession id=33780 pCBO=0xd0790,
<parent>0x1b000019|0xfb6c0.
[2012-04-21 11:36:27,046] 5936 0004 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:736) - SMconnection (0xfe328):
transaction=0x1d9888(0xfb6c0) pCBO=0xd0790, pCBOFunction=(nil).

[2012-04-21 11:36:27,046] 5937 0003 com.sonus.sbc.ads DEBUG
(ActiveDirectoryManager.cpp:782) - Got a new Request...
[2012-04-21 11:36:27,046] 5938 0002 com.sonus.sbc.ads DEBUG
(ActiveDirectoryManager.cpp:786) - MSG_ADS_AD_QUERY


[2012-04-21 11:36:27,046] 5939 0001 com.sonus.sbc.ads DEBUG
(ActiveDirectoryWorker.cpp:381) - PrepareWorker for AD Query thread object:
(0x1147b0), m_eActionType: 3, atAction: 3
[2012-04-21 11:36:27,047] 5940 0009 com.sonus.sbc.ads TRACE
(ActiveDirectoryWorker.cpp:96) - Getting to work on thread object: (0x1147b0),
m_eActionType: 3
[2012-04-21 11:36:27,047] 5941 0008 com.sonus.sbc.ads DEBUG
(ActiveDirectoryWorker.cpp:99) - Start processing AD action thread object:
(0x1147b0)!
[2012-04-21 11:36:27,047] 5942 0007 com.sonus.sbc.ads DEBUG
(ActiveDirectoryCache.cpp:771) - Search Key: msRTCSIP-Line and Value:
+15105743501;ext=3501;msskiprnl.
[2012-04-21 11:36:27,047] 5943 0006 com.sonus.sbc.ads DEBUG
(ActiveDirectoryCache.cpp:822) - Found matching record with 8 entries.


[2012-04-21 11:36:27,047] 5944 0005 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1291) - SMSession::SendResponse(UID=0x1b000586 |
ObjHandle=0x1d9888)
[2012-04-21 11:36:27,048] 5945 0004 com.sonus.sbc.ads.libcommon DEBUG
(AFSessionManagementLayer.cpp:1913) - Sending RSP: state=1 transaction
id=10:0/33780/0 message=MSG_ADS_AD_QUERY msg len=543 end session=0
sessions={lvl=2}<parent>0x1b000019|0xfb6c0-[this]0x1b000586|0x1d9888. Process ID
5473
[2012-04-21 11:36:27,048] 5946 0003 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1499) - (-)SMSession: destructing session
(UID=0x1b000586|ObjHandle=0x1d9888) id=33780 state=4 level=2, <parent>0x0|(nil).
[2012-04-21 11:36:27,048] 5947 0002 com.sonus.sbc.ads TRACE
(ActiveDirectoryWorker.cpp:94) - Worker thread object: (0x1147b0) is ready to get to
work.
[2012-04-21 11:36:27,048] 5948 0001 com.sonus.sbc.ads DEBUG
(ActiveDirectoryManager.cpp:915) - Request serviced.
[2012-04-21 11:36:27,049] 5949 0001 com.sonus.sbc.msc TRACE
(MscIndicationsMainBL.c:343) - connID=0x00000000 is DevID  >>*** Indication
FC=0x04fd P1=0000 P2=0001 P3=03e3 free[99.500000] used [0.500000]
[2012-04-21 11:36:27,049] 5950 0001 com.sonus.sbc.msc TRACE (dspalloc.c:262) -
dspa_UpdateDSPUtilization(dsp=0, utilization=995)

[2012-04-21 11:36:27,049] 5951 0001 com.sonus.sbc.msc TRACE
(MscIndicationsMainBL.c:285) - connID=0x00000000 is DevID  >>*** Indication
FC=0x04fa P1=0000 P2=0001 P3=03e3 free[99.500000] used [0.500000]
[2012-04-21 11:36:27,050] 5952 0001 com.sonus.sbc.route.libcommon TRACE
(AFEventLoop.cpp:110) - AFEventLoop::Monitor: Adding event info fd=13 for
events=0x1, info=0x1f5008, pCBO=0x1f1fb0
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-04-21 11:36:27,050] 5953 0001 com.sonus.sbc.route.libcommon DEBUG
(AFSessionManagementLayer.cpp:792) - SMConnection (0x1802a0): Received RESP: session
id=10:0/33780/0 message=MSG_ADS_AD_QUERY len=543 end sesion=0, moredata=0
[2012-04-21 11:36:27,050] 5954 0001 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:867) - SMconnection (0x1802a0):
transaction=<parent>0x1100000d|0x189488-[sess]0x110008d0|0x1f55f0 pCBO=(nil),
pCBOFunction=0xef378.
[2012-04-21 11:36:27,050] 5955 0001 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1499) - (-)SMSession: destructing session
(UID=0x110008d0|ObjHandle=0x1f55f0) id=33780 state=4 level=2, <parent>0x0|(nil).

[2012-04-21 11:36:27,050] 5956 0001 com.sonus.sbc.route DEBUG (callrouter.cpp:3735)
- Got AD lookup response with 8 field/value pairs.
[2012-04-21 11:36:27,051] 5957 0001 com.sonus.sbc.route INFO (callrouter.cpp:2193) -
Handling route request.
[2012-04-21 11:36:27,051] 5958 0001 com.sonus.sbc.route DEBUG (callrouter.cpp:2196)
- Using AD lookup response in request.
[2012-04-21 11:36:27,051] 5959 0001 com.sonus.sbc.route INFO (callrouter.cpp:2272) -
Using table Default Route Table (1) to route call.
[2012-04-21 11:36:27,051] 5960 0001 com.sonus.sbc.route DEBUG (translation.cpp:1293)
- Performing MANDATORY transformation using entry AD test (13.2(2)).
[2012-04-21 11:36:27,051] 5961 0001 com.sonus.sbc.route DEBUG (translation.cpp:618)
- non wildcard AD, proceed as normal
[2012-04-21 11:36:27,052] 5962 0001 com.sonus.sbc.route DEBUG (translation.cpp:636)
- Successful regex match of "tfUserValue1" field for "=msRTCSIP-Line=" (updated
"\+15105743501;ext=3501;msskiprnl") with input of "+15105743501;ext=3501;msskiprnl"
[2012-04-21 11:36:27,052] 5963 0001 com.sonus.sbc.route DEBUG (translation.cpp:681)
- Regex replacement output of "tfCalledNumber" field is "jsmith@sbc.net"
[2012-04-21 11:36:27,052] 5964 0001 com.sonus.sbc.route DEBUG (translation.cpp:1293)
- Performing MANDATORY transformation using entry set calling plan (13.3(3)).

[2012-04-21 11:36:27,053] 5967 0001 com.sonus.sbc.route DEBUG (translation.cpp:1293)
- Performing MANDATORY transformation using entry adjust to 4 digits (14.1(1)).
[2012-04-21 11:36:27,053] 5968 0001 com.sonus.sbc.route DEBUG (translation.cpp:636)
- Successful regex match of "tfCalledNumber" field for "(.*)(....)" (updated
"(.*)(....)") with input of "+15105743501"
[2012-04-21 11:36:27,053] 5969 0001 com.sonus.sbc.route DEBUG (translation.cpp:681)
- Regex replacement output of "tfUserValue1" field is
"+15105743501;ext=3501;msskiprnl"
[2012-04-21 11:36:27,053] 5970 0001 com.sonus.sbc.route INFO (translation.cpp:1206)
- Doing AD lookup for field 'msRTCSIP-Line' with value
'+15105743501;ext=3501;msskiprnl'


[2012-04-21 11:36:27,054] 5971 0001 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1273) -
SMSession::SendTransactionRequest(UID=0x1100000c | ObjHandle=0x1802b4)
[2012-04-21 11:36:27,054] 5972 0001 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1472) - (+)SMSession: creating session
(UID=0x110008d1|ObjHandle=0x1f2c88) level=2 session id=1013, PID=0x1100,
<parent>0x1100000d|0x189488.
[2012-04-21 11:36:27,054] 5973 0001 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1491) - SMSession: new session
(UID=0x110008d1|ObjHandle=0x1f2c88) id=0 subsession id=33781 pCBO=0xef378,
<parent>0x1100000d|0x189488.
[2012-04-21 11:36:27,054] 5974 0013 com.sonus.sbc.route.libcommon DEBUG
(AFSessionManagementLayer.cpp:1790) - Sending REQ: transaction id=10:0/33781/0
message=MSG_ADS_AD_QUERY msg len=81 end session=0
sessions={lvl=1}<parent>0x1100000c|0x1802b4-[this]0x1100000d|0x189488-(sub)0x110008d1|0
Process ID 5670
[2012-04-21 11:36:27,055] 5975 0012 com.sonus.sbc.ads.libcommon DEBUG
(AFSessionManagementLayer.cpp:645) - SMConnection: Received REQ: id=10:0/33781/0
session bit=0 moredata bit=0 message=MSG_ADS_AD_QUERY
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
[2012-04-21 11:36:27,055] 5976 0011 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1121) - Checking CBO(0xd0790) for
SMSession(UID=0x1b000587 | ObjHandle=0x1d9888)
[2012-04-21 11:36:27,055] 5977 0010 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1467) - SMSession::Stored CBO-UID
(UID=0x1b000001|ObjHandle=0xd0790) for Session (Uid=0x1b000587 | ObjHandle=0x1d9888)
[2012-04-21 11:36:27,055] 5978 000f com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1472) - (+)SMSession: creating session
(UID=0x1b000587|ObjHandle=0x1d9888) level=2 session id=33781, PID=0x1b00,
<parent>0x1b000019|0xfb6c0.
[2012-04-21 11:36:27,055] 5979 000e com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1491) - SMSession: new session
(UID=0x1b000587|ObjHandle=0x1d9888) id=0 subsession id=33781 pCBO=0xd0790,
<parent>0x1b000019|0xfb6c0.
[2012-04-21 11:36:27,055] 5980 000d com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:736) - SMconnection (0xfe328):
transaction=0x1d9888(0xfb6c0) pCBO=0xd0790, pCBOFunction=(nil).


[2012-04-21 11:36:27,055] 5981 000c com.sonus.sbc.ads DEBUG
(ActiveDirectoryManager.cpp:782) - Got a new Request...
[2012-04-21 11:36:27,055] 5982 000b com.sonus.sbc.ads DEBUG
(ActiveDirectoryManager.cpp:786) - MSG_ADS_AD_QUERY


[2012-04-21 11:36:27,055] 5983 000a com.sonus.sbc.ads DEBUG
(ActiveDirectoryWorker.cpp:381) - PrepareWorker for AD Query thread object:
(0x1147b0), m_eActionType: 3, atAction: 3
[2012-04-21 11:36:27,055] 5984 0009 com.sonus.sbc.ads TRACE
(ActiveDirectoryWorker.cpp:96) - Getting to work on thread object: (0x1147b0),
m_eActionType: 3
[2012-04-21 11:36:27,055] 5985 0008 com.sonus.sbc.ads DEBUG
(ActiveDirectoryWorker.cpp:99) - Start processing AD action thread object:
(0x1147b0)!
[2012-04-21 11:36:27,056] 5986 0007 com.sonus.sbc.ads DEBUG
(ActiveDirectoryCache.cpp:771) - Search Key: msRTCSIP-Line and Value:
+15105743501;ext=3501;msskiprnl.
[2012-04-21 11:36:27,056] 5987 0006 com.sonus.sbc.ads DEBUG
(ActiveDirectoryCache.cpp:822) - Found matching record with 8 entries.


[2012-04-21 11:36:27,056] 5988 0005 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1291) - SMSession::SendResponse(UID=0x1b000587 |
ObjHandle=0x1d9888)
[2012-04-21 11:36:27,056] 5989 0004 com.sonus.sbc.ads.libcommon DEBUG
(AFSessionManagementLayer.cpp:1913) - Sending RSP: state=1 transaction
id=10:0/33781/0 message=MSG_ADS_AD_QUERY msg len=543 end session=0
sessions={lvl=2}<parent>0x1b000019|0xfb6c0-[this]0x1b000587|0x1d9888. Process ID
5473
[2012-04-21 11:36:27,056] 5990 0003 com.sonus.sbc.ads.libcommon TRACE
(AFSessionManagementLayer.cpp:1499) - (-)SMSession: destructing session
(UID=0x1b000587|ObjHandle=0x1d9888) id=33781 state=4 level=2, <parent>0x0|(nil).
[2012-04-21 11:36:27,056] 5991 0002 com.sonus.sbc.ads TRACE
(ActiveDirectoryWorker.cpp:94) - Worker thread object: (0x1147b0) is ready to get to
work.
[2012-04-21 11:36:27,056] 5992 0001 com.sonus.sbc.ads DEBUG
(ActiveDirectoryManager.cpp:915) - Request serviced.
[2012-04-21 11:36:27,057] 5993 004c com.sonus.sbc.route.libcommon TRACE
(AFEventLoop.cpp:110) - AFEventLoop::Monitor: Adding event info fd=14 for
events=0x1, info=0x18d8c8, pCBO=0x1f1688
[2012-04-21 11:36:27,058] 5994 004b com.sonus.sbc.route.libcommon TRACE
(AFEventLoop.cpp:143) - going to unmonitor FD: 0x0000000d
[2012-04-21 11:36:27,058] 5995 004a com.sonus.sbc.route.libcommon DEBUG
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
(AFSessionManagementLayer.cpp:792) - SMConnection (0x1802a0): Received RESP: session
id=10:0/33781/0 message=MSG_ADS_AD_QUERY len=543 end sesion=0, moredata=0
[2012-04-21 11:36:27,058] 5996 0049 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:867) - SMconnection (0x1802a0):
transaction=<parent>0x1100000d|0x189488-[sess]0x110008d1|0x1f2c88 pCBO=(nil),
pCBOFunction=0xef378.
[2012-04-21 11:36:27,058] 5997 0048 com.sonus.sbc.route.libcommon TRACE
(AFSessionManagementLayer.cpp:1499) - (-)SMSession: destructing session
(UID=0x110008d1|ObjHandle=0x1f2c88) id=33781 state=4 level=2, <parent>0x0|(nil).


[2012-04-21 11:36:27,058] 5998 0047 com.sonus.sbc.route DEBUG (callrouter.cpp:3735)
- Got AD lookup response with 8 field/value pairs.
[2012-04-21 11:36:27,058] 5999 0046 com.sonus.sbc.route INFO (callrouter.cpp:2193) -
Handling route request.
[2012-04-21 11:36:27,058] 6000 0045 com.sonus.sbc.route DEBUG (callrouter.cpp:2196)
- Using AD lookup response in request.
[2012-04-21 11:36:27,058] 6001 0044 com.sonus.sbc.route INFO (callrouter.cpp:2272) -
Using table Default Route Table (1) to route call.
[2012-04-21 11:36:27,058] 6002 0043 com.sonus.sbc.route DEBUG (translation.cpp:1293)
- Performing MANDATORY transformation using entry telephoneNumber lookup for
extension (14.2(2)).
[2012-04-21 11:36:27,059] 6003 0042 com.sonus.sbc.route DEBUG (translation.cpp:618)
- non wildcard AD, proceed as normal
[2012-04-21 11:36:27,059] 6004 0041 com.sonus.sbc.route DEBUG (translation.cpp:636)
- Successful regex match of "tfUserValue1" field for "=msRTCSIP-Line=" (updated
"\+15105743501;ext=3501;msskiprnl") with input of "+15105743501;ext=3501;msskiprnl"
[2012-04-21 11:36:27,059] 6005 0040 com.sonus.sbc.route DEBUG (translation.cpp:681)
- Regex replacement output of "tfCalledNumber" field is "3502"
[2012-04-21 11:36:27,059] 6006 003f com.sonus.sbc.route INFO (callrouter.cpp:2403) -
```

Copyright © 2015 Sonus Networks. All rights reserved.

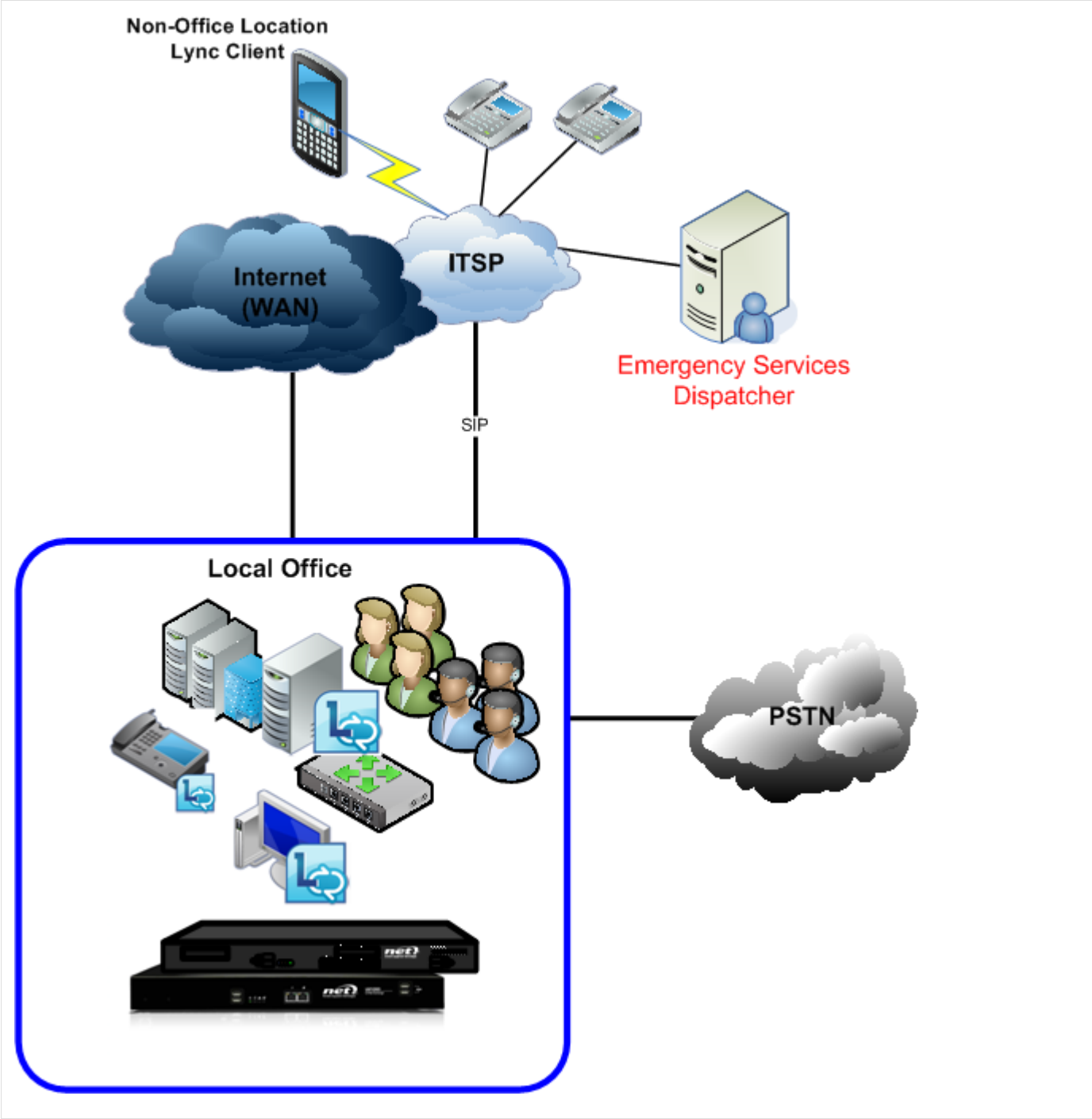
```
Successful completed forked route request with entry Check SIP Registrar (1.2(2))
m_eCallForked(0) count(1/8)
```

Configuring the Sonus SBC 1000-2000 and Lync to Support Enhanced Emergency (911) Services

In this article, we describe the necessary steps to configure Sonus SBC 1000/2000 and Lync for Enhanced Emergency Services (E911) support.

Topology

Copyright © 2015 Sonus Networks. All rights reserved.



On this Page:

- Overview
- Central Site Configuration
  - Location Policy Configuration
  - Dial Plan Configuration
  - Route Configuration
  - Trunk Configuration
  - Create a Location Information Server (LIS) Subnet
  - Location Policy Configuration
- Sonus SBC 1000/2000 Configuration
  - SIP Profiles

Copyright © 2015 Sonus Networks. All rights reserved.

        - Number Transformation
        - Call Routing
    - Call Flow

Overview

In the context of Internet Telephony, there are two types of 911 (emergency) calls, **Basic** and **Enhanced**:

- Basic 911 calls contain no location information
- Enhanced 911 calls do contain location information

When **Enhanced Emergency Services** are enabled in Lync, location information about a 911 caller is passed to the destination (emergency services dispatcher, police, fire, etc.). 911 calls from Lync clients signed-in at an office location include location information, calls from Lync clients not signed in at an office location (e.g., Starbucks, public library, etc.) are connected to the destination using a fallback 911 route which does not contain location information.

Related Articles

- Configure Enhanced 9-1-1
- Lync Setup

Central Site Configuration

The Lync side configuration steps are accomplished using the following tools:

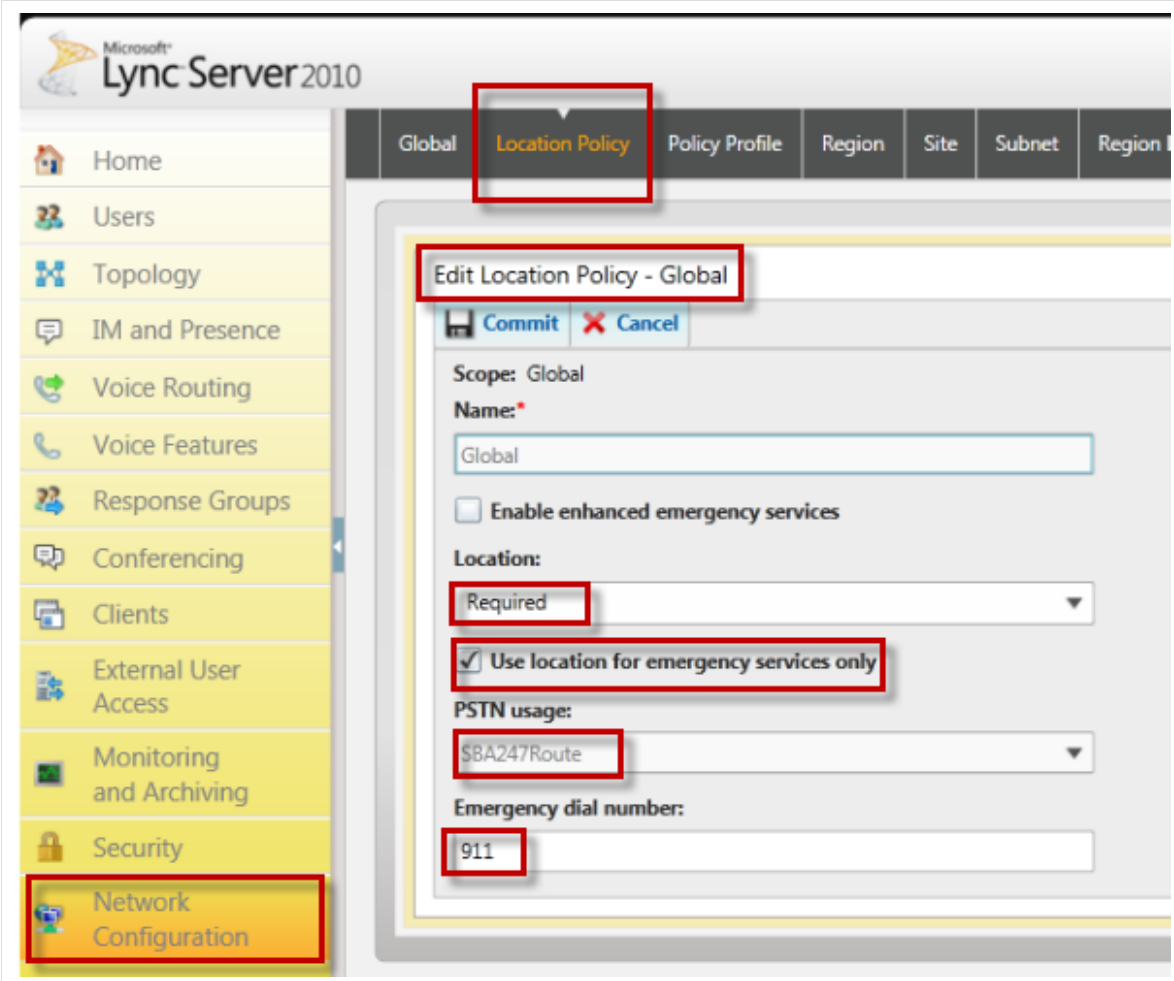
- Lync Server 2010 Configuration Manager
- Lync Server Management Shell

Location Policy Configuration

To configure the location policy:

1. Launch **Lync Server 2010 Configuration Manager**.
2. Click **Network Configuration** on left pane.
3. Click **Location Policy** on right pane.
4. Edit the **Global** Location Policy as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



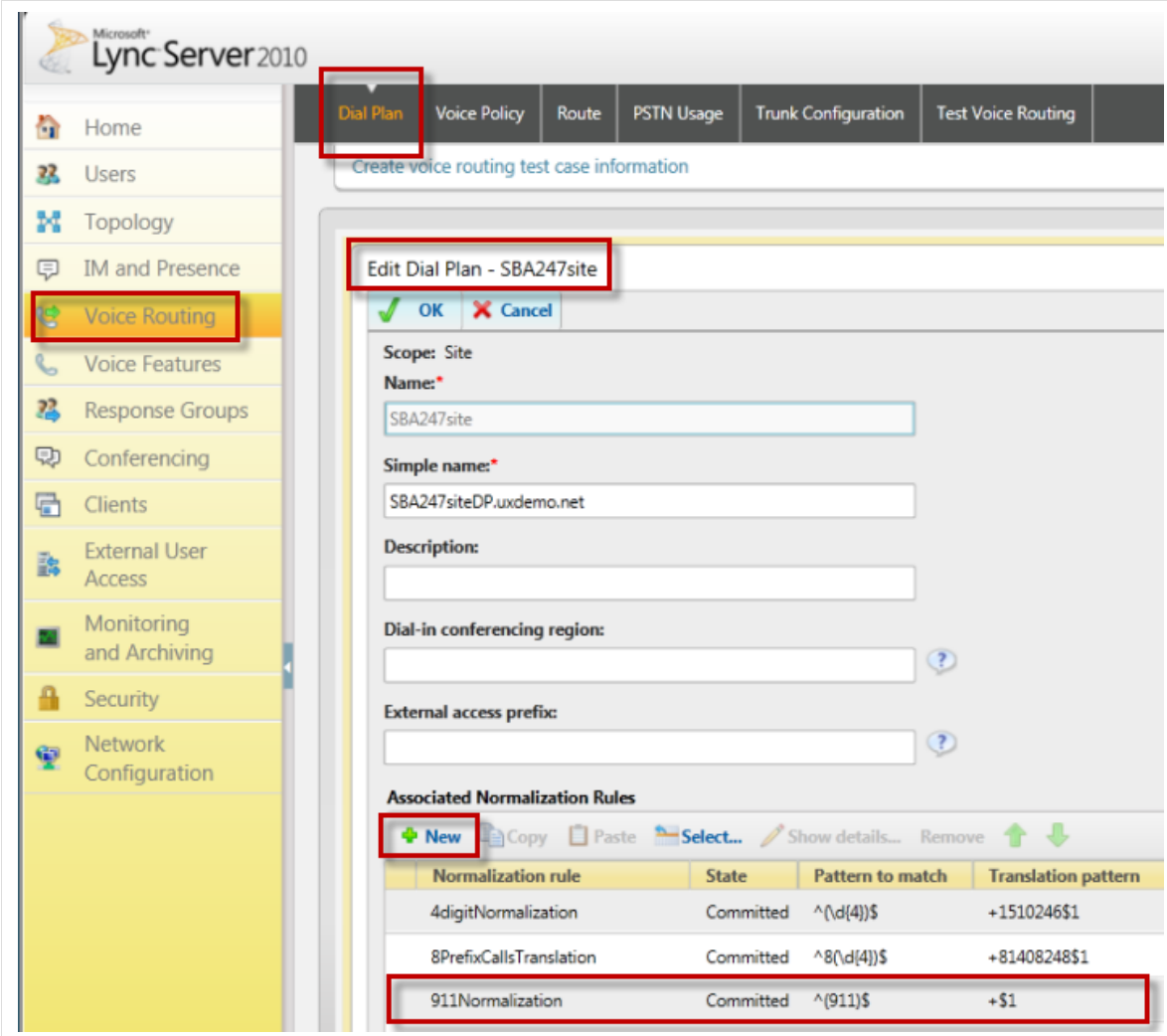
⚠ Make sure to **Commit** the changes after configuring the attributes shown above.

Dial Plan Configuration

To configure a dial plan:

1. Launch **Lync Server 2010 Configuration Manager**.
2. Click **Voice Routing** on left pane.
3. Click **Dial Plan** on right pane.
4. Edit the **Dial Plan** as required.
5. Add a new **Normalization Rule** for 911 call as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.

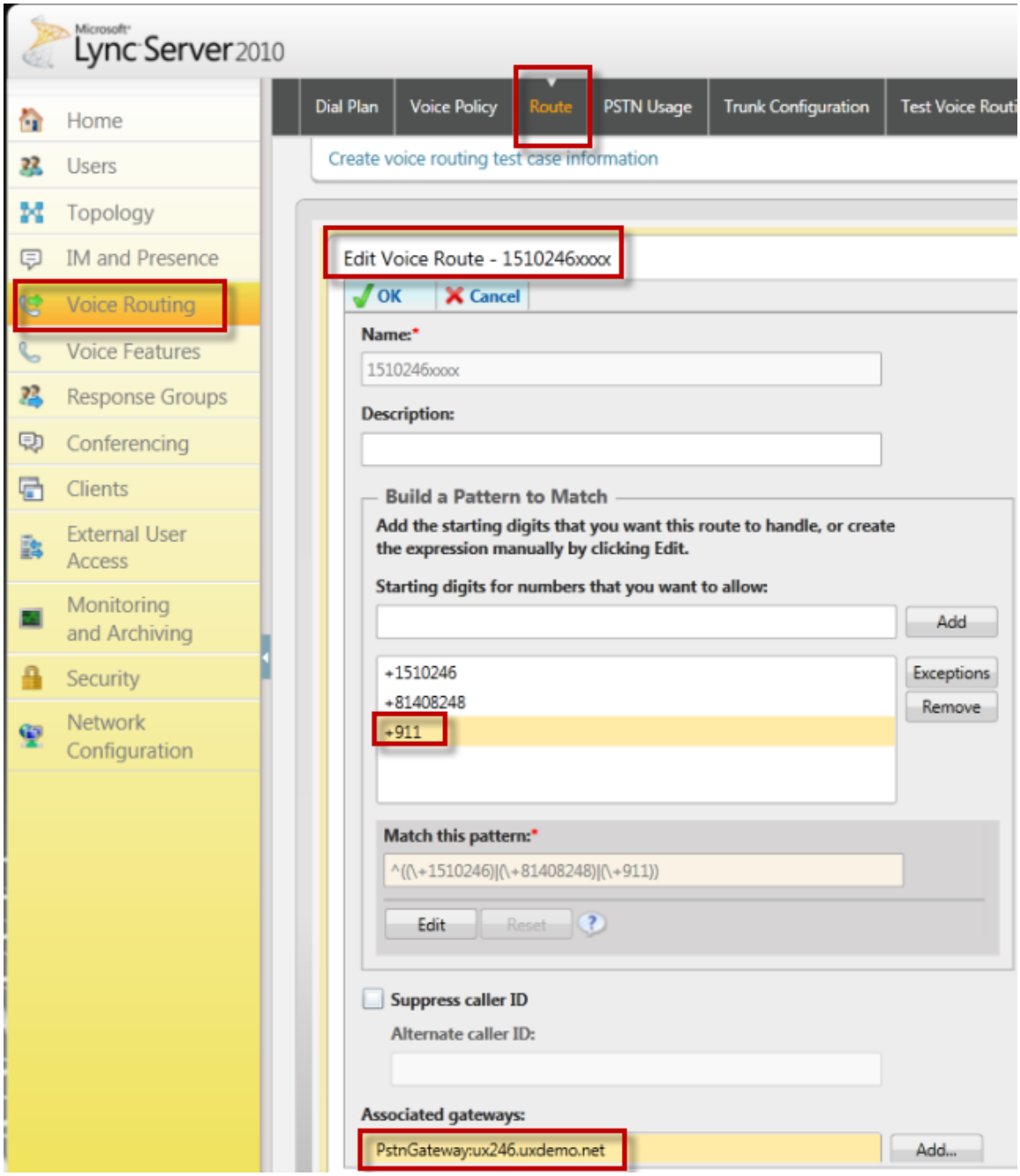


⚠ Make sure to **Commit** the changes after configuring the attributes shown above.

Route Configuration

1. Launch **Lync Server 2010 Configuration Manager**.
2. Click **Voice Routing** on left pane.
3. Click **Route** on right pane.
4. Edit the relevant **Voice Route** and add a new **Pattern** for 911 call.
5. Be sure to have the relevant Sonus SBC 1000/2000 gateway selected in **Associated Gateways** field as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.

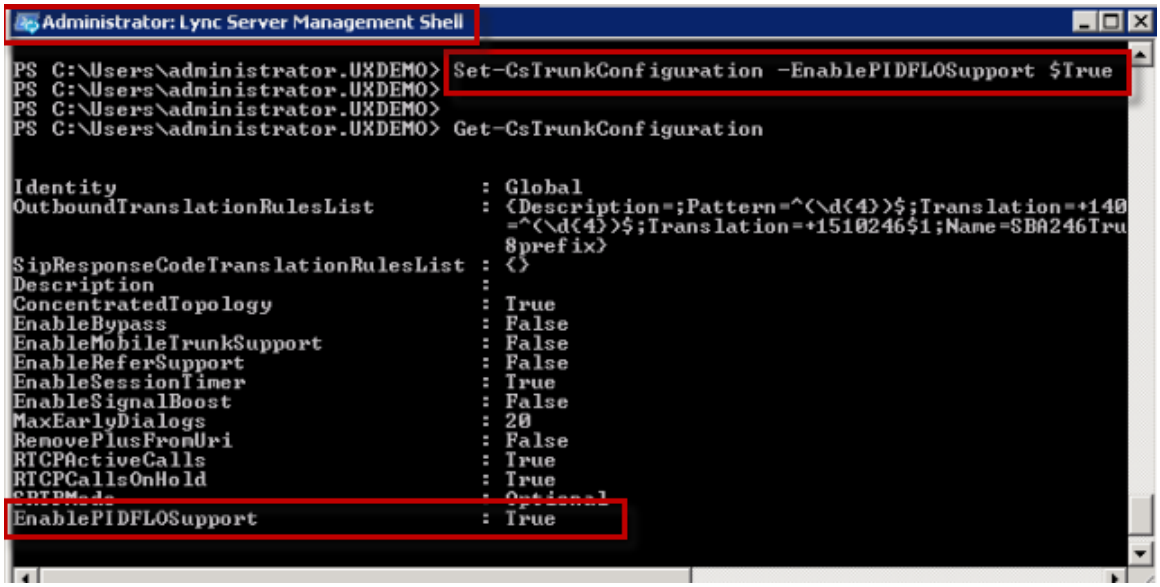


⚠ Make sure to **Commit** the changes after configuring the attributes shown above.

Trunk Configuration

1. Launch **Lync Server Management Shell**.
2. Check the Trunk Configuration using `Get-CSTrunkConfiguration` command.
3. Verify that `EnablePIDFLOSupport` attribute is **True**. If not:
    a. Run the `Set-CSTrunkConfiguration -EnablePIDFLOSupport $True` script.
    b. Press **Enter**.
    c. Verify that script `Get-CSTrunkConfiguration` returns a `EnablePIDFLOSupport` attribute as **True** , as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.

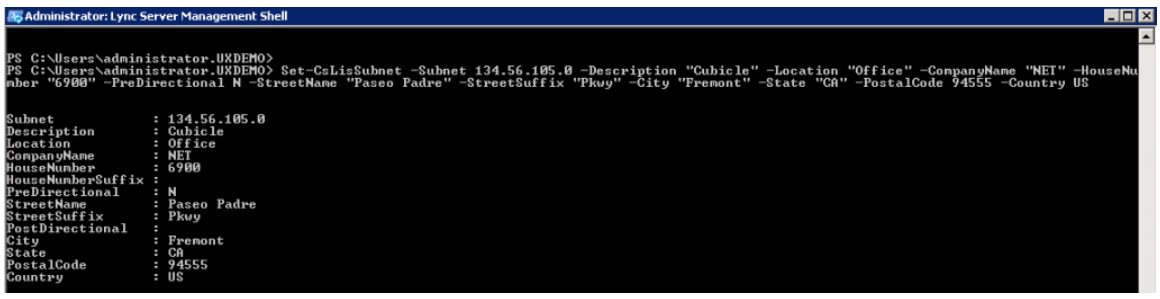


Create a Location Information Server (LIS) Subnet

This set of steps creates a Location Information Server (LIS) subnet. LIS Subnets are used to associate a location with a specific subnet. LIS Subnets are used in Enhanced 9-1-1 (E9-1-1) Enterprise Voice implementations to notify an emergency services operator of the caller's location.

To create a Location Information Server Subnet:

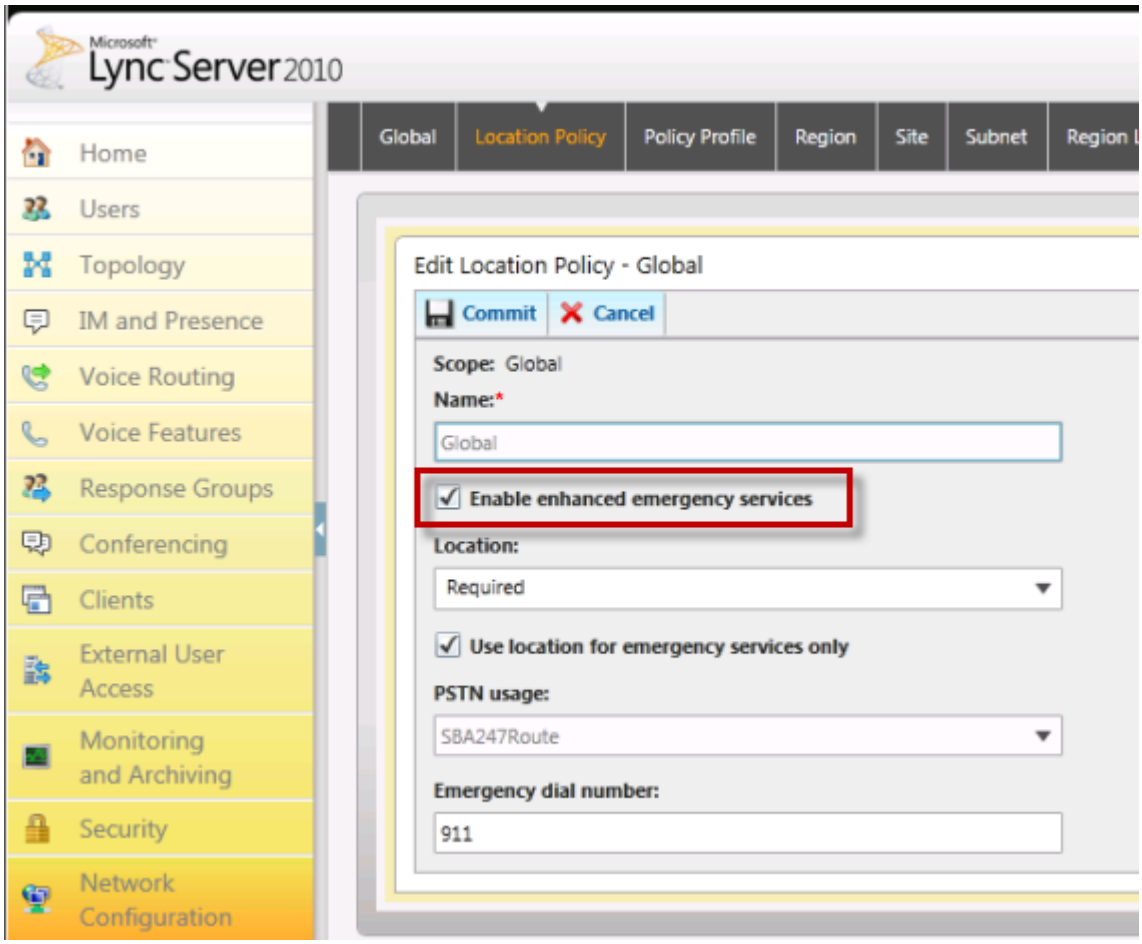
1. Launch **Lync Server Management Shell**.
2. Type `Set-CsLisSubnet -Subnet 134.56.105.0 -Description "Cubicle" -Location "Office" -CompanyName "Sonus" -HouseNumber "6900" -PreDirectional N -StreetName "Paseo Padre" -StreetSuffix "Pkwy" -City "Fremont" -State "CA" -PostalCode 94555 -Country US` as shown below.
3. Press **Enter**.



Location Policy Configuration

1. Launch **Lync Server 2010 Configuration Manager**.
2. Click **Network Configuration** on left pane.
3. Click **Location Policy** on right pane.
4. Edit the relevant **Voice Route**.
5. Select the **Enable enhanced emergency services** check box.

Copyright © 2015 Sonus Networks. All rights reserved.



⚠ Make sure to **Commit** the changes after configuring the attributes shown above.

Sonus SBC 1000/2000 Configuration

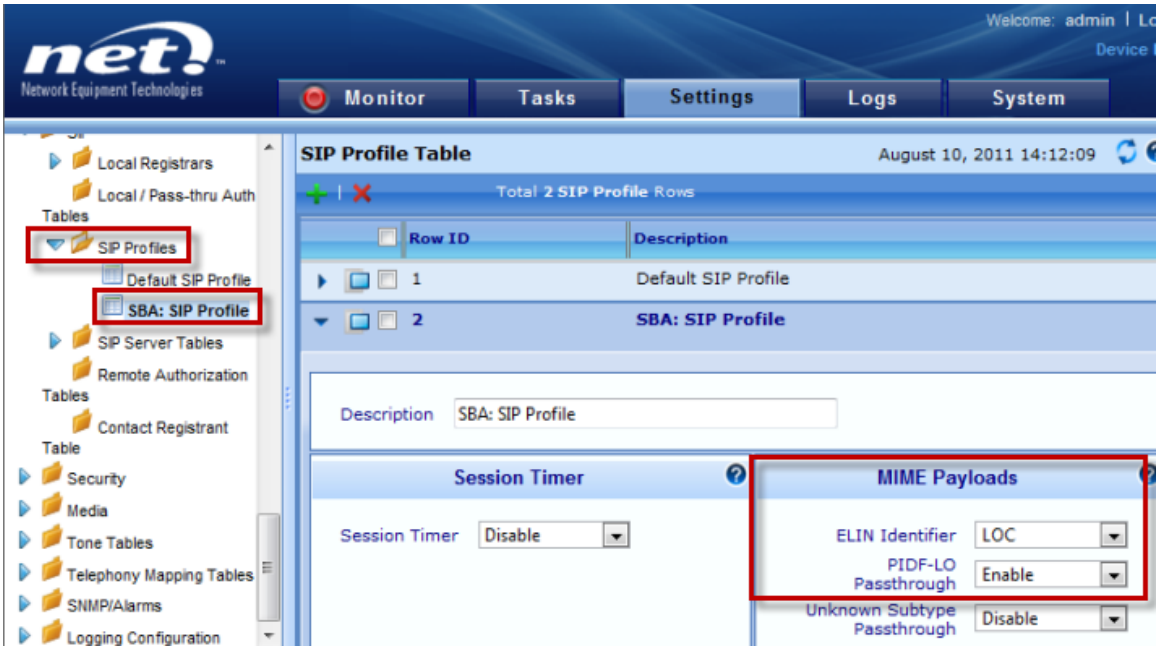
The configuration steps on the Sonus SBC 1000/2000 are achieved directly via the WebUI broken down in the following sections:

- #SIP Profile
- #Number Transformation
- #Call Routing Table

SIP Profiles

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP Profiles > *relevant SIP Profile***.
3. In the **MIME Payloads**panel:
    a. Configure the ELIN Identifier field as shown below:
    b. Configure the PDIF-LO Passthrough fieldas shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



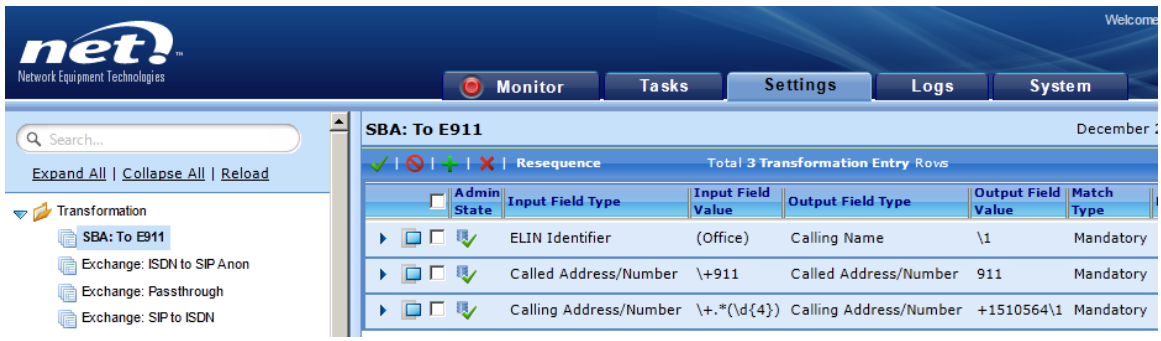
Number Transformation

In this exercise we create two Transformation Tables to route calls to a **911 Provider** over SIP trunking:

- Transformation for calls from Lync clients signed-in at **Office** Locations.
- Transformation for calls from Lync clients signed-in at **Remote** Locations such as Starbucks, etc..

Transformation Table for calls to E911

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Transformation**.
3. Create a new Transformation Table with **ELIN Identifier**, **Called Address/Number**, and **Calling Address/Number**field types as shown below.

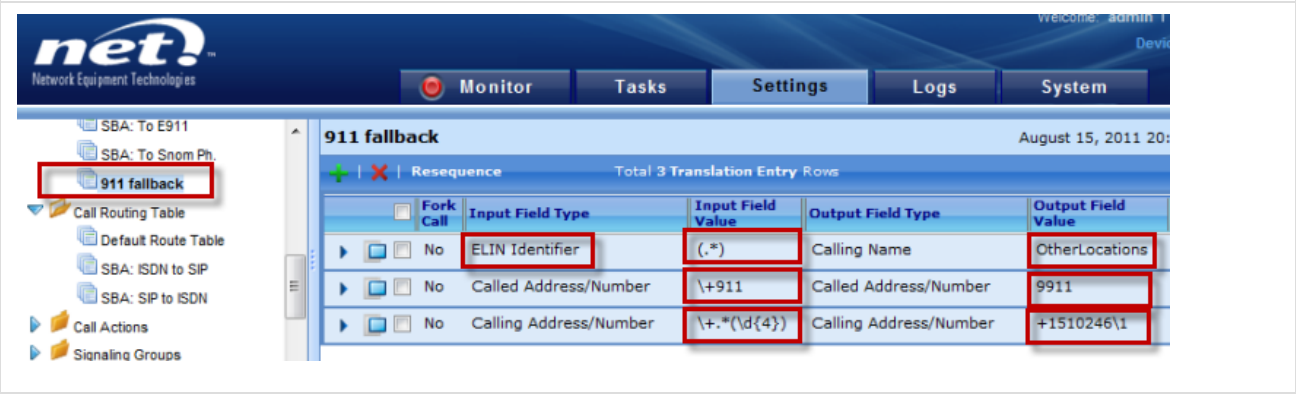


> The Input Match Field value "Office" is only an example. Instead of exact match, you could use a partial string match or a regular expression to catch all (`.*`).

Transformation Table for 911 Fallback calls

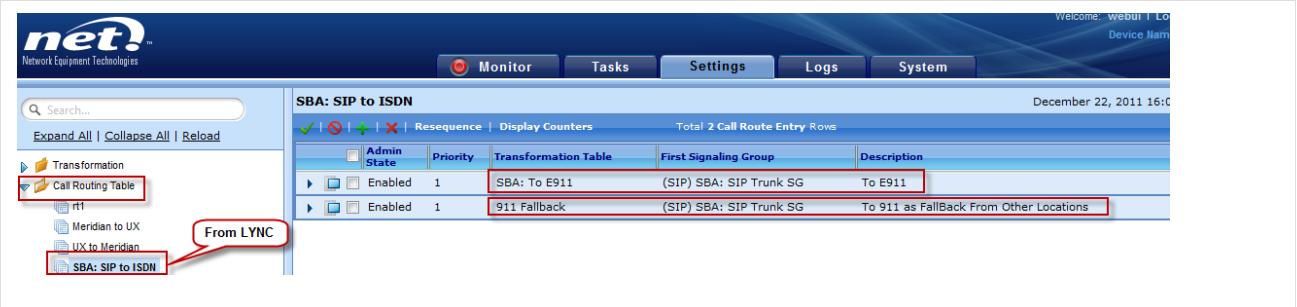
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Transformation**.
3. Create a new **Transformation Table** with **ELIN Identifier**, **Called Address/Number**, and **Calling Address/Number**field types as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



Call Routing

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table**.
3. Click the relevant **Call Route** table used for calls received from Lync.
4. Add two entries in the table: one for calls with configured **Office** Location Information, and another one that does not have the Location Information as **Office**. Note that both route entries are destined to **911 Provider** over a SIP Trunk.



Note that when integrating with E911 providers, the Call Priority may have to be set to Emergency.

Call Flow

With above configuration, when a 911 call from Lync client arrives on the Sonus SBC 1000/2000 with the Location Information as **Office**, Lync will then provide the relevant location profile in the Inbound INVITE message. Sonus SBC 1000/2000 then passes this information to the **911 Provider** in the outbound INVITE message.

This can be verified in the logs by tracing the relevant inbound INVITE message from Lync to Sonus SBC 1000/2000:

Copyright © 2015 Sonus Networks. All rights reserved.



Configuring the Sonus SBC 1000-2000 for Lync E911 with PSAP Callback Number

On this Page

Copyright © 2015 Sonus Networks. All rights reserved.

- Overview
- Best Practice Use Case
  - Topology
  - Scenario
- Configuration
  - Lync-side Configuration
  - Sonus SBC 1000/2000-side Configuration
    - Lync 2010 Setup
    - E911 Specific Settings on Sonus SBC 1000/2000
- Verification
  - Lync User Makes a 911 Call
  - 911 Operator Performs Callback on Previous Call
  - Emergency Calls in Alarm View

Related Articles

- Configuring the Sonus SBC 1000-2000 and Lync to Support Enhanced Emergency (911) Services

Overview

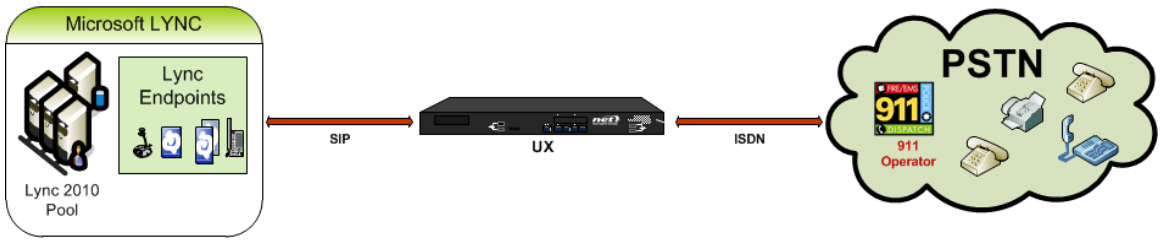
This article is to describe the necessary configuration steps for **Sonus SBC 1000/2000 Emergency Services for Lync E911 - PSAP Callback**

Public Safety Answering Point (PSAP) Callback is an important Sonus SBC 1000/2000 feature supporting 911/E911. In the LYNC E911 architecture, the Emergency Location Identification Number (ELIN) number is the PSAP call back number that the emergency service operator can call to reach the original 911 caller. This article explains how to configure the Sonus SBC 1000/2000 for E911 Calback functionality in a LYNC deployment.

Best Practice Use Case

Topology

In this best practice example, we will be configuring a Sonus SBC 1000/2000 node for the Lync E911 with a PSAP callback number in following topology:



Scenario

1. Be sure that the Sonus SBC 1000/2000 is defined and configured in the Microsoft Lync Server 2010 Topology and Control Panel.
2. Complete the 911 specific settings in Microsoft Lync Server 2010 Control Panel.
3. Configure the Sonus SBC 1000/2000 node as a gateway in Microsoft Lync Server 2010 - Sonus SBC 1000/2000 Gateway - PSTN topology:
   - With Lync E911 enabled

Copyright © 2015 Sonus Networks. All rights reserved.

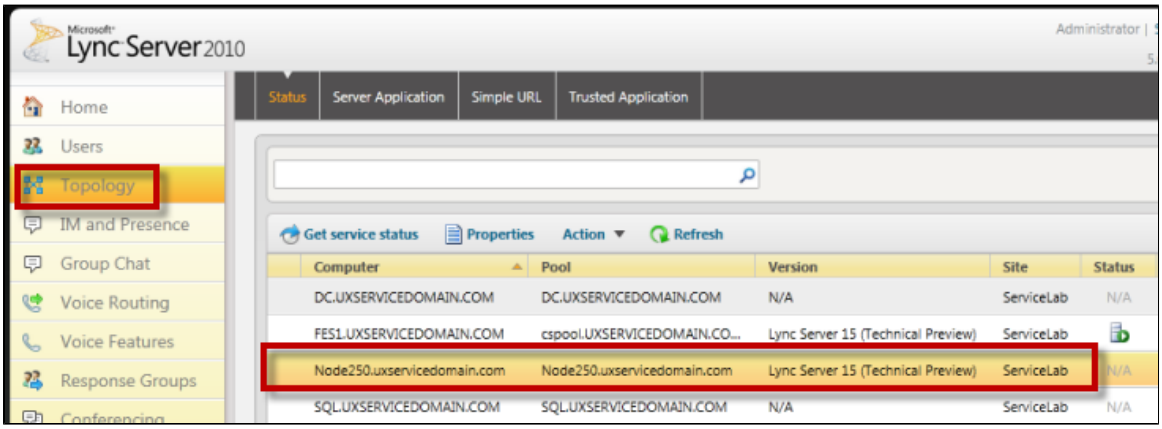
- With **Emergency Callback** Number as **2020**.
- With **PSAP** Number as **2020**.

4. Have Lync Client make a successful E911 call
   - Verify the call is successful
5. Have Lync Client make a E911 call, then disconnect before the 911 Operator answers the call.
   - Verify that 911 Operator can make a successful callback to the **PSAP Callback number**
   - Verify that Sonus SBC 1000/2000 redirects the PSAP callback call to the Lync client who initiated the E911 call.

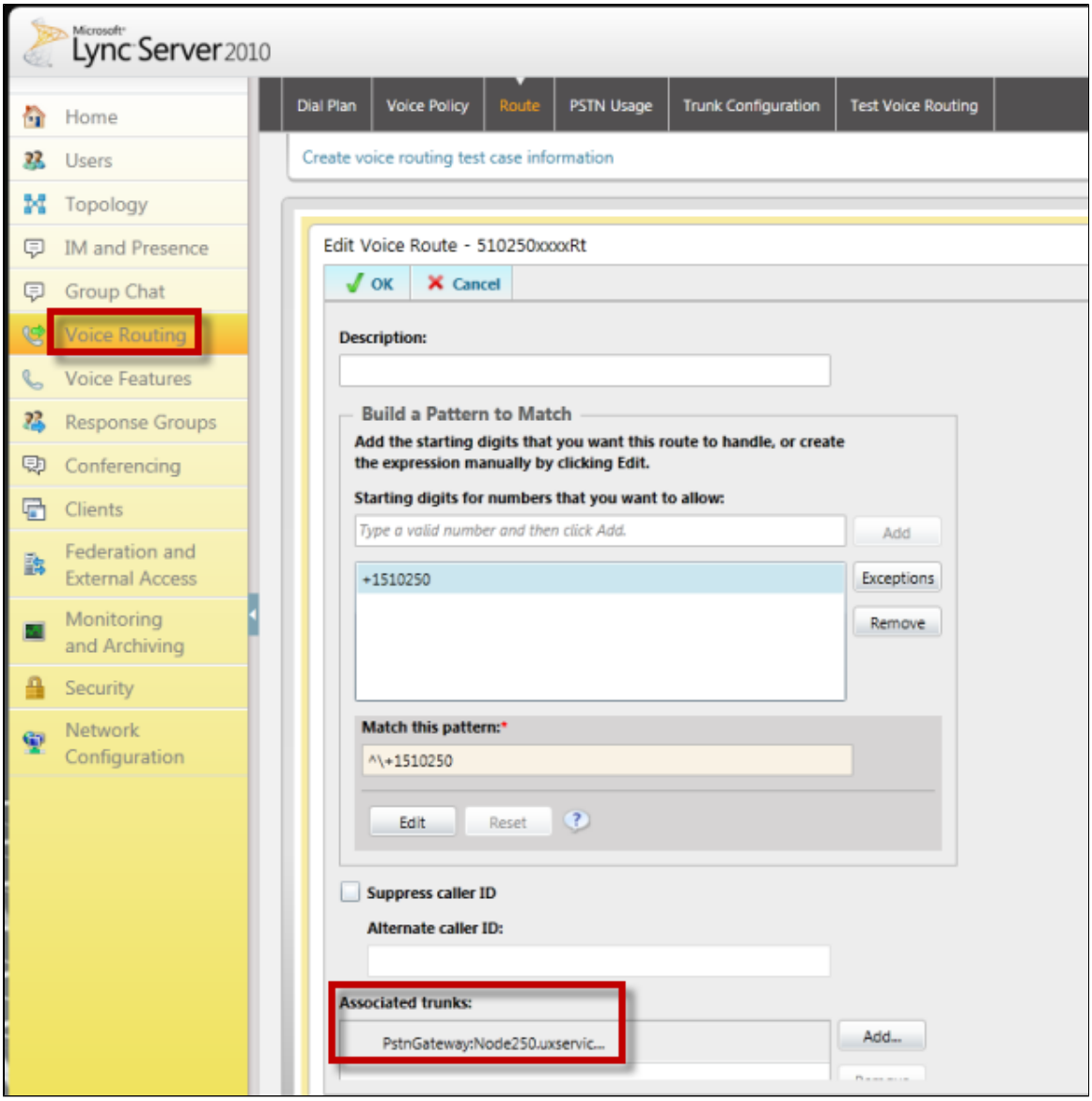
Configuration

Lync-side Configuration

Verify that Sonus SBC 1000/2000 is added to Microsoft Lync Server 2010 Topology and Control Panel as directed by Microsoft Lync Server 2010 Deployment Guides and it appears correctly in Microsoft Lync Server 2010 Control Panel as shown below:



Copyright © 2015 Sonus Networks. All rights reserved.



On the Microsoft Lync 2010 Front End Server, launch **Lync Server Management Shell** and run the following commands to enable "PDIFLOSupport" and to create a **Location Information Server (LIS) Subnet** as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.

```
PS C:\Users\administrator.UXSERVICEDOMAIN> Set-CsTrunkConfiguration -EnablePIDFLOSupport $True
PS C:\Users\administrator.UXSERVICEDOMAIN> Get-CsTrunkConfiguration

Identity                              : Global
OutboundTranslationRulesList          : {}
SipResponseCodeTranslationRulesList   : {}
OutboundCallingNumberTranslationRulesList :
{Description=;Pattern=^(\d{4})$;Translation=+1510250$1;Name=510250xxxxTrunk}
PstnUsages                            : {}
Description                           :
ConcentratedTopology                  : True
EnableBypass                          : True
EnableMobileTrunkSupport              : False
EnableReferSupport                    : True
EnableSessionTimer                    : False
EnableSignalBoost                     : False
MaxEarlyDialogs                       : 20
RemovePlusFromUri                     : False
RTCPActiveCalls                       : True
RTCPCallsOnHold                       : True
SRTPMode                              : Required
EnablePIDFLOSupport                   : True
EnableRTPLatching                     : False
EnableOnlineVoice                     : False
ForwardCallHistory                    : False
Enable3pccRefer                       : False

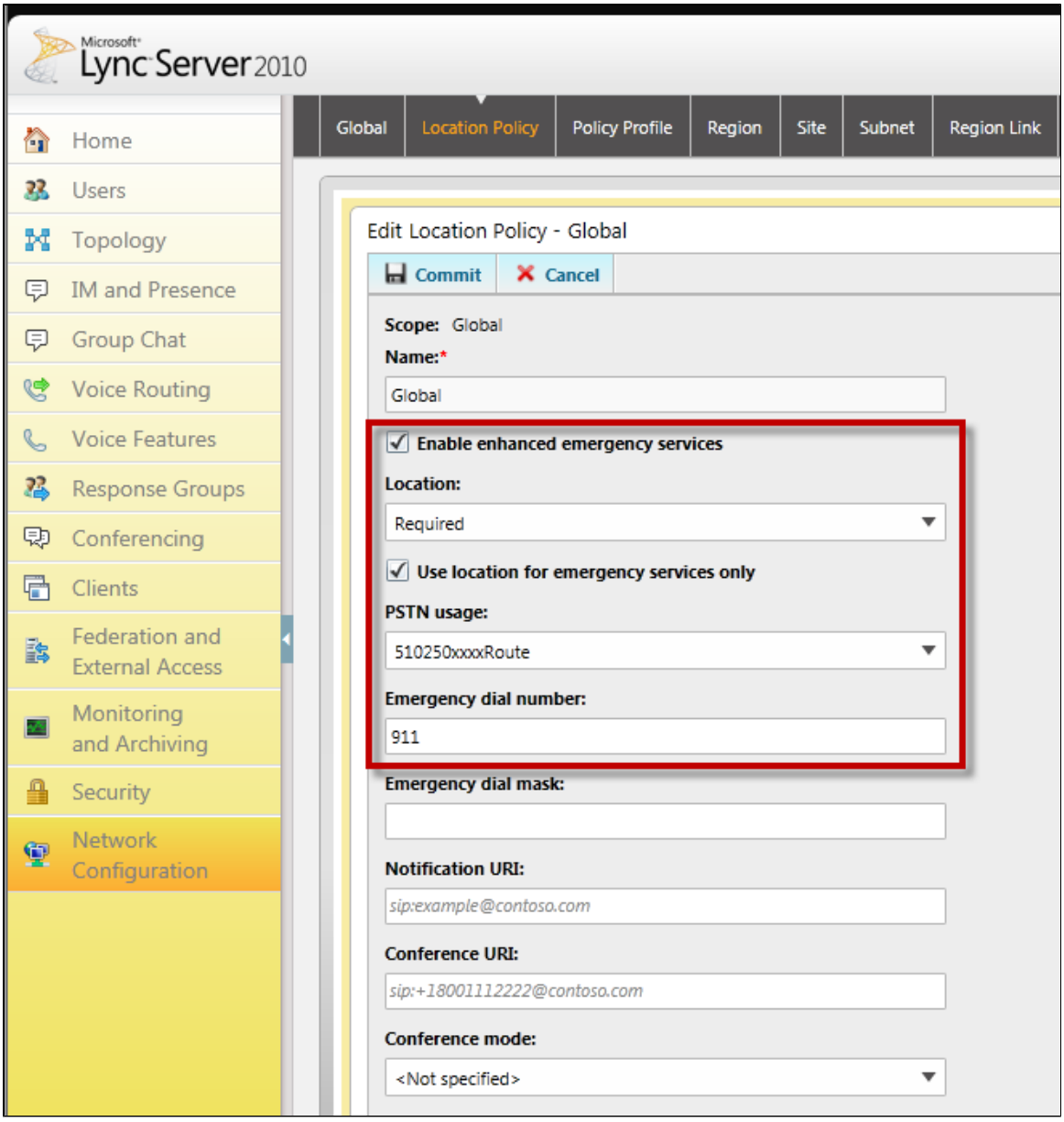
PS C:\Users\administrator.UXSERVICEDOMAIN> Set-CsLisSubnet -Subnet 134.56.105.0 -Description "Cubicle" -Location
"Office" -CompanyName "NET" -HouseNumber "6900" -PreDirectional N -StreetName "Paseo Padre" -StreetSuffix "Pkwy" -
City "Fremont" -State "CA" -PostalCode 94555 -Country US


Subnet             : 134.56.105.0
Description        : Cubicle
Location           : Office
CompanyName        : NET
HouseNumber        : 6900
HouseNumberSuffix  :
PreDirectional     : N
StreetName         : Paseo Padre
StreetSuffix       : Pkwy
PostDirectional    :
City               : Fremont
State              : CA
PostalCode         : 94555
Country            : US

PS C:\Users\administrator.UXSERVICEDOMAIN>
```

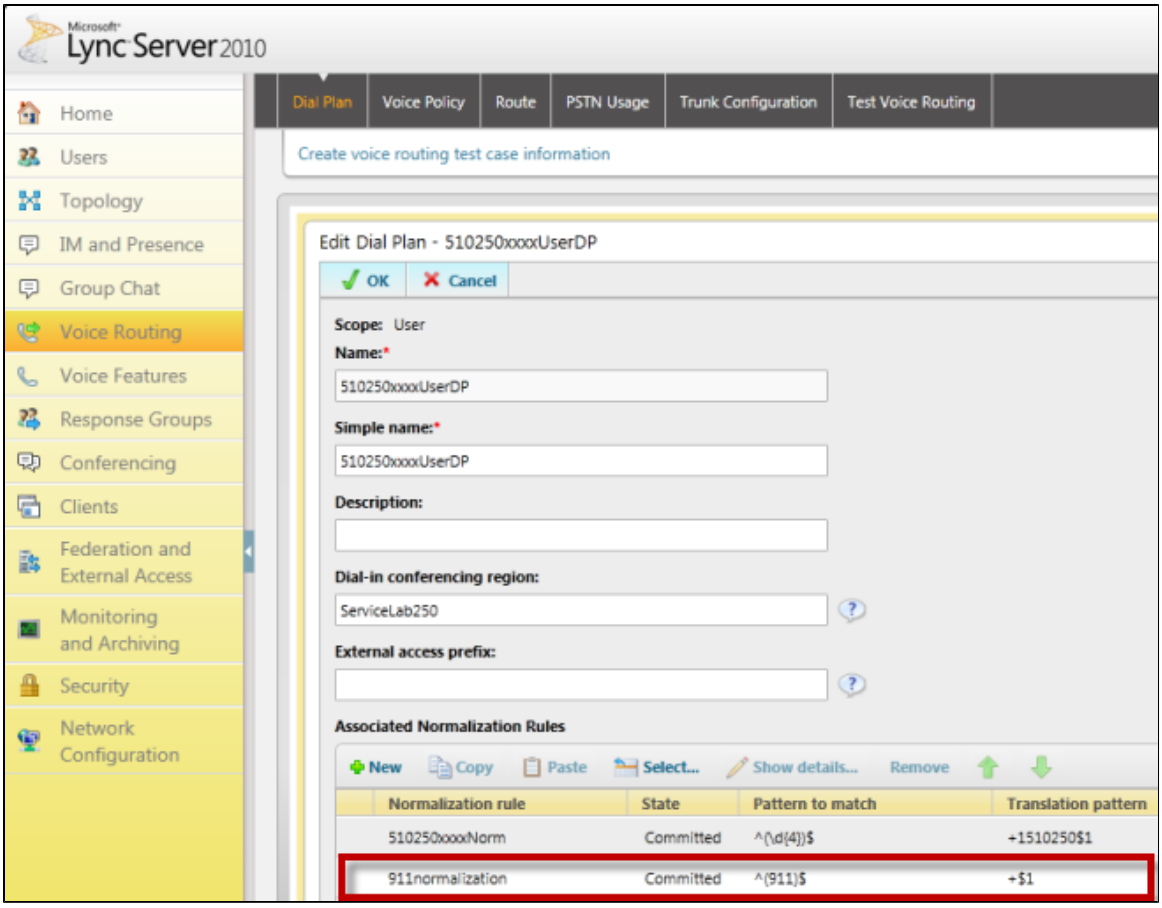
On the Microsoft Lync 2010 Front End Server, launch **Microsoft Lync Server Control Panel** and configure the Location Policy as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



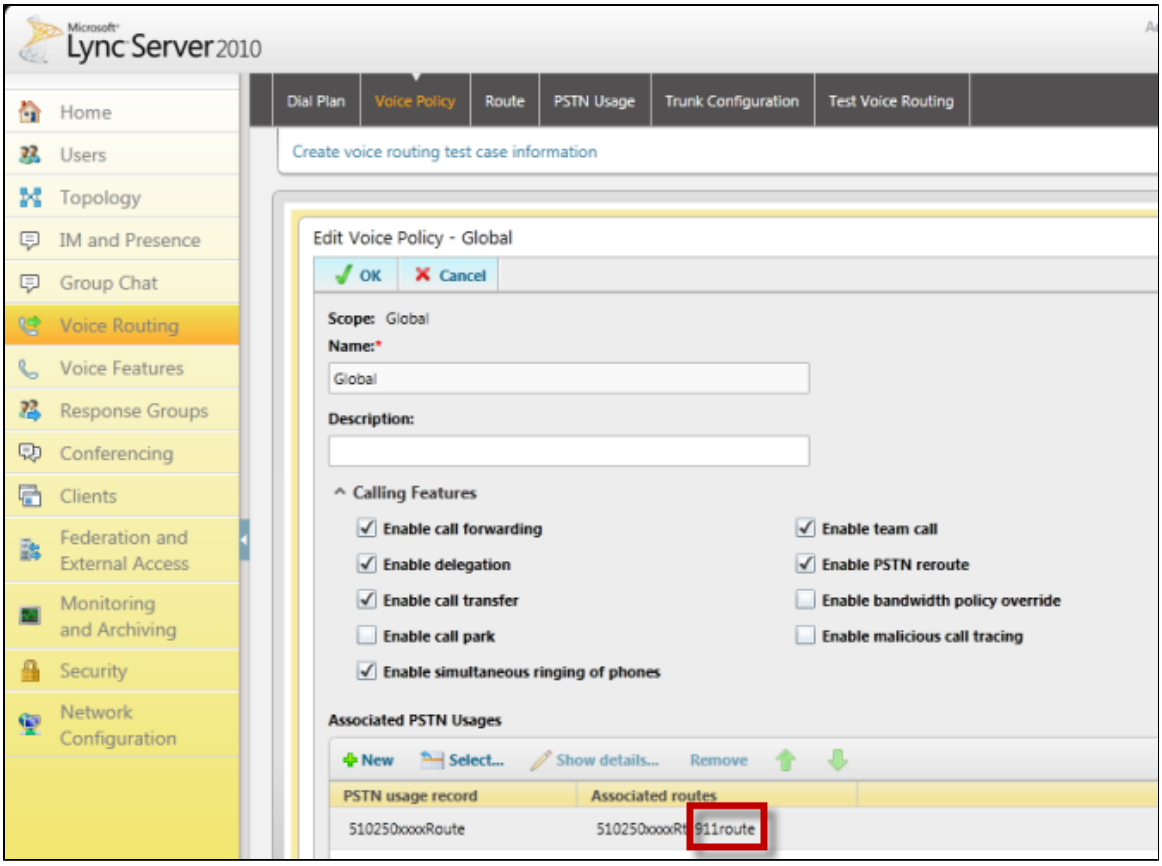
On the Microsoft Lync 2010 Front End Server, launch **Microsoft Lync Server Control Panel** and configure the Associated Normalization Rules with 911 dialing as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.

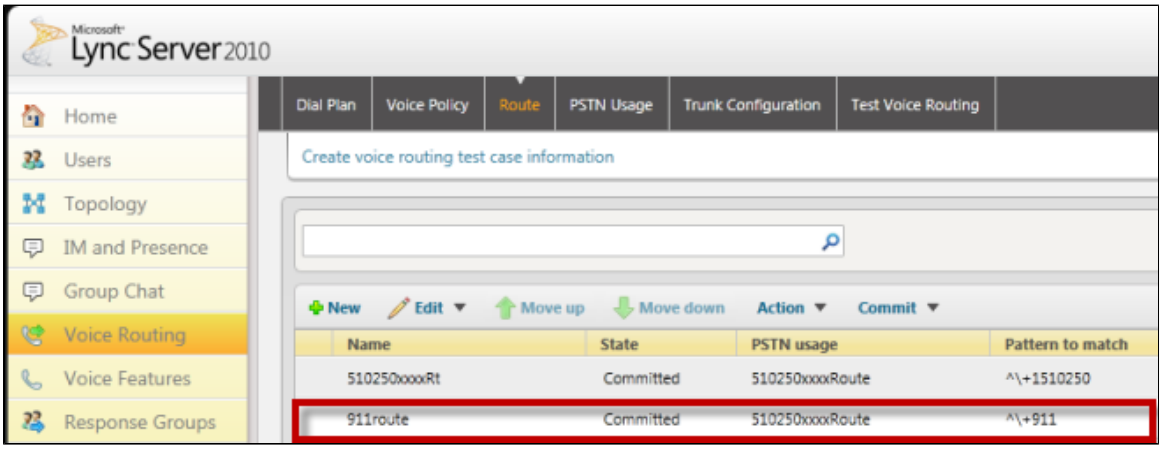


On the Microsoft Lync 2010 Front End Server, launch **Microsoft Lync Server Control Panel** and configure the Voice Policy with 911 route as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



On the Microsoft Lync 2010 Front End Server, launch **Microsoft Lync Server Control Panel** and verify that relevant Call Route contains the 911 pattern match as shown below:

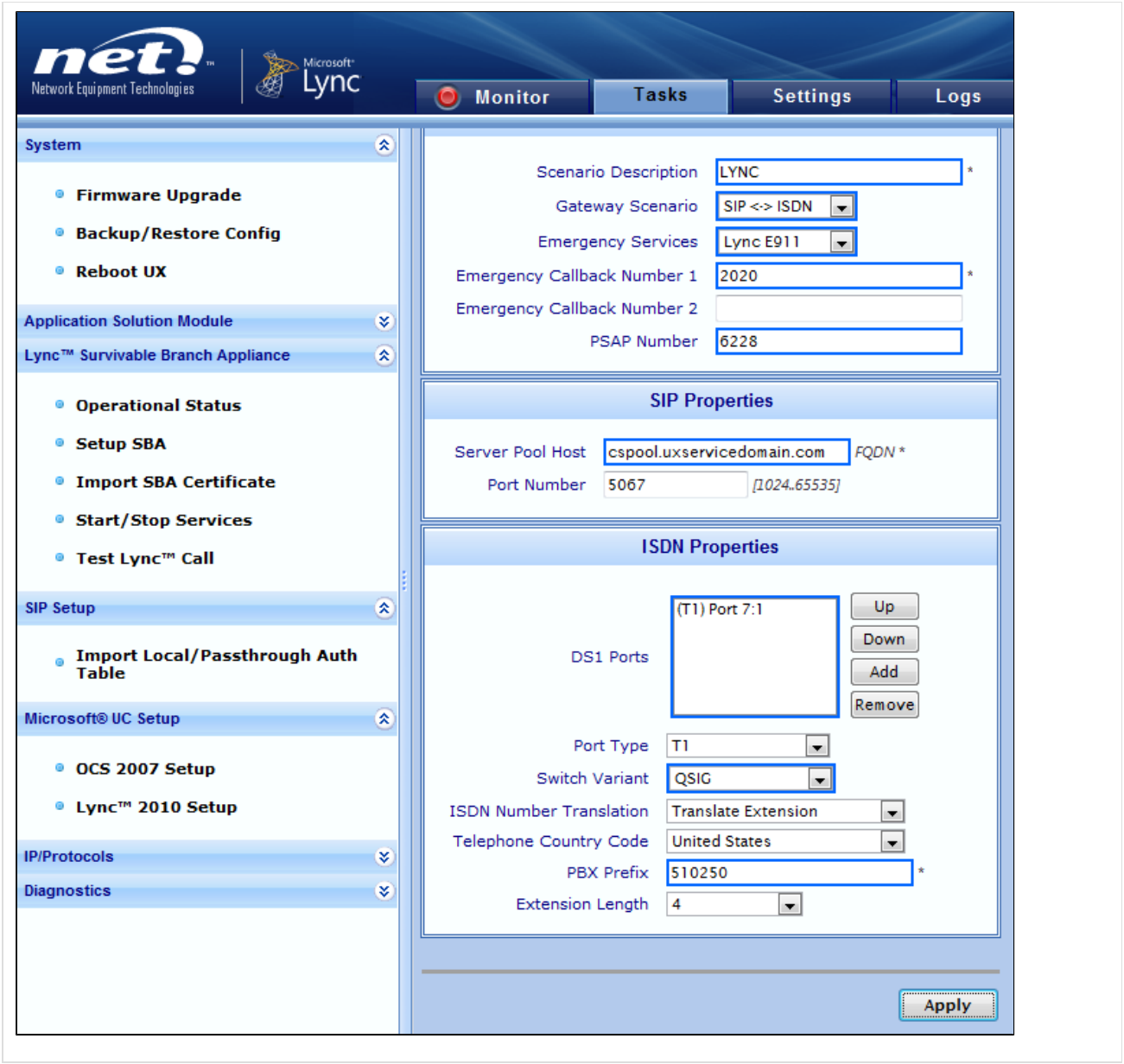


Sonus SBC 1000/2000-side Configuration

Lync 2010 Setup

1. Launch your preferred explorer and logon to Sonus SBC 1000/2000 WebUI.
2. Click the **Tasks** tab.
3. In the left navigation menu, click* Lync 2010 Setup* (in the Microsoft UC Setup section).
4. Fill-in the setup fields and click Apply as shown in below example:

Copyright © 2015 Sonus Networks. All rights reserved.



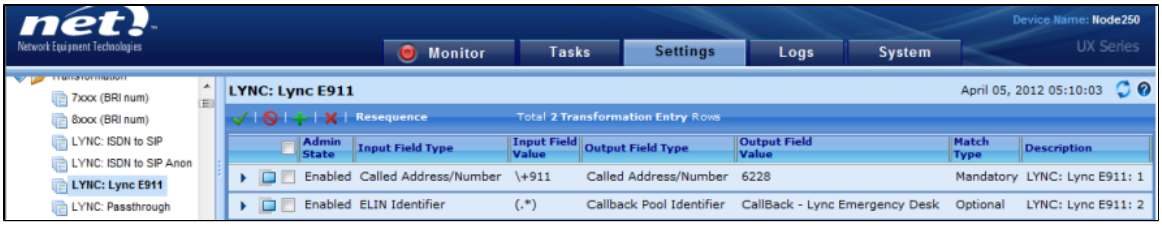
E911 Specific Settings on Sonus SBC 1000/2000

Upon a successful **Lync 2010 Setup** run, wizard will create your Sonus SBC 1000/2000 node for the minimum required settings for SIP to ISDN and ISDN to SIP calls. In addition, Emergency Service will be enabled and relevant configuration will be set. In this section, we will only verify the Emergency Service related configuration fields settings.

Transformation Table

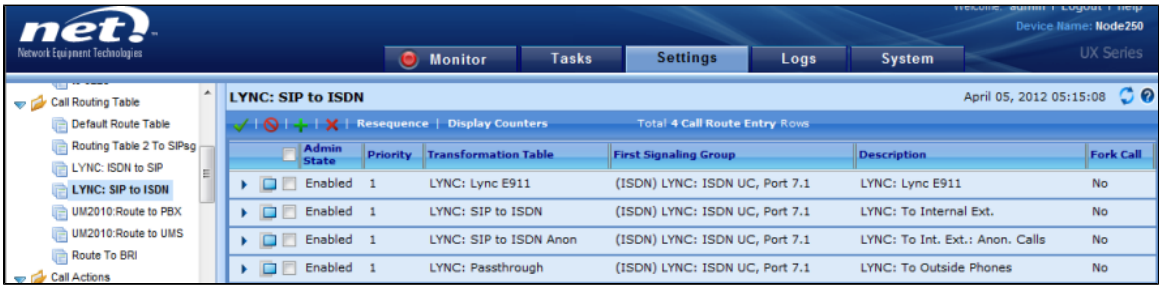
The wizard creates the following transformation table entry for 911 calls in the outbound direction which are directed to PSAP number as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



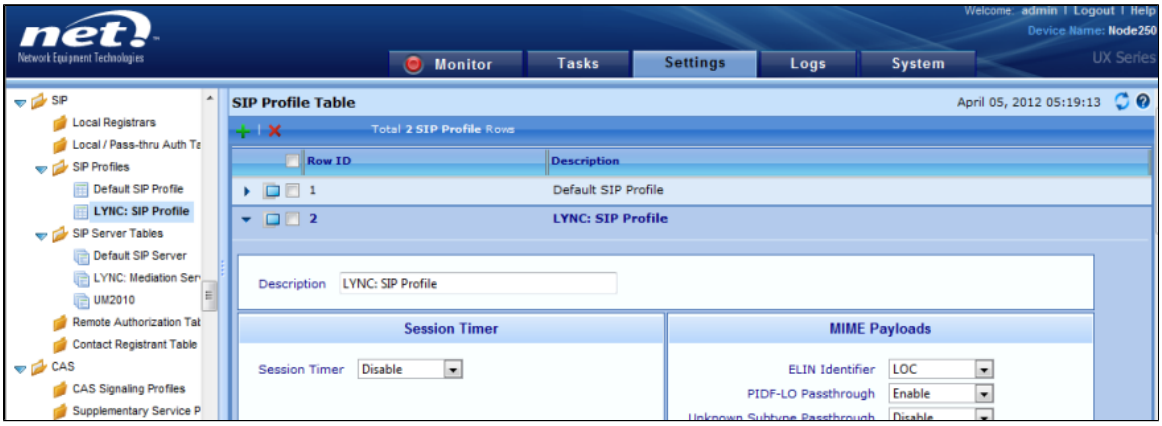
SIP to ISDN Call Route Entry

The wizard creates the following SIP to ISDN Call Route Entry for 911 calls in the outbound direction which are directed to relevant ISDN Signaling Group as shown below:



SIP Profile

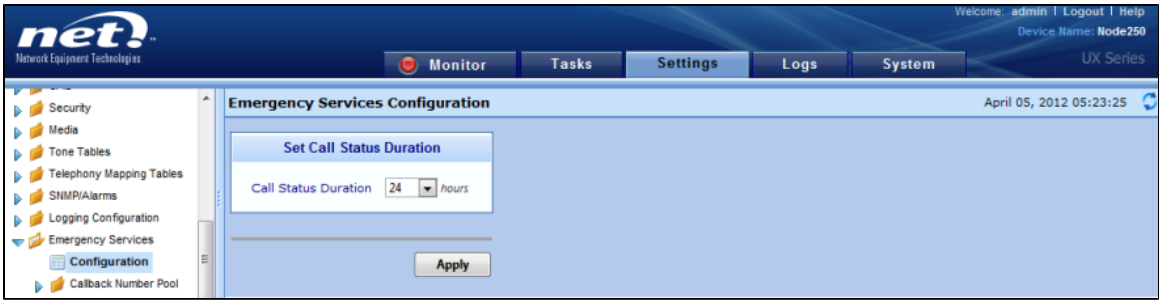
The wizard creates the following SIP Profile configured with the ELIN Identifier and PIDF-LO enabled as shown below:



Emergency Services Configuration

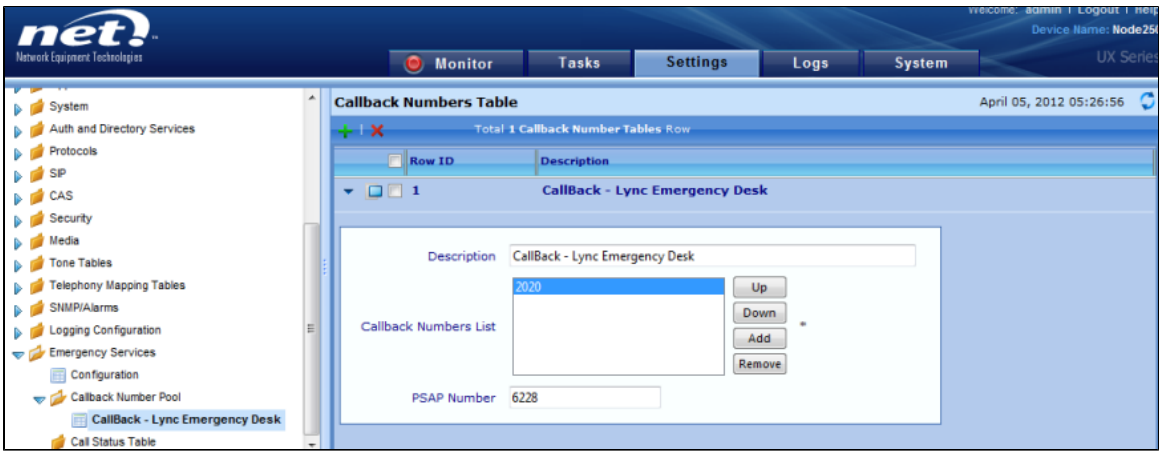
The wizard creates the Emergency Services configured with 24 hours Call Status Duration (default) as shown below (note that this is a 1 through 24 hour configurable item):

Copyright © 2015 Sonus Networks. All rights reserved.



Callback Number Pool

Make sure that the Callback Number Pool is created with the Callback number (**2020** in this example) and with the PSAP number (**6228** in this example) as shown below:



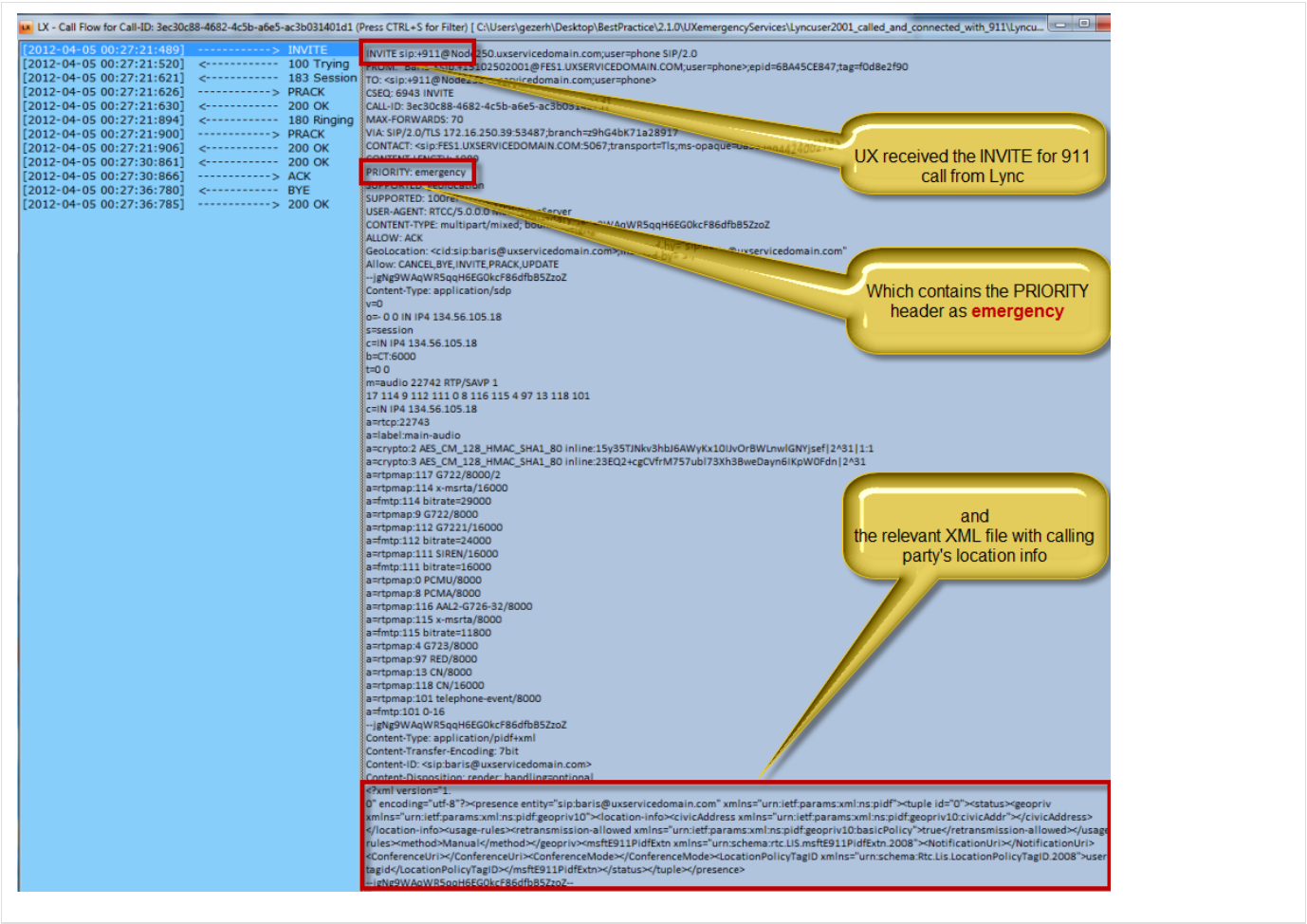
Verification

Lync User Makes a 911 Call

1. Lync User `+1(510)250-2001` dials `+911`.
2. Call is routed to the Sonus SBC 1000/2000.
3. The Sonus SBC 1000/2000 transforms the called party number `+911` to the PSAP number `6228` and sends it out to the PSTN.
4. When the 911 Operator `6228` answers the call, parties go on-hook and terminate the call.

The relevant *SIP INVITE* message for above call setup is as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.

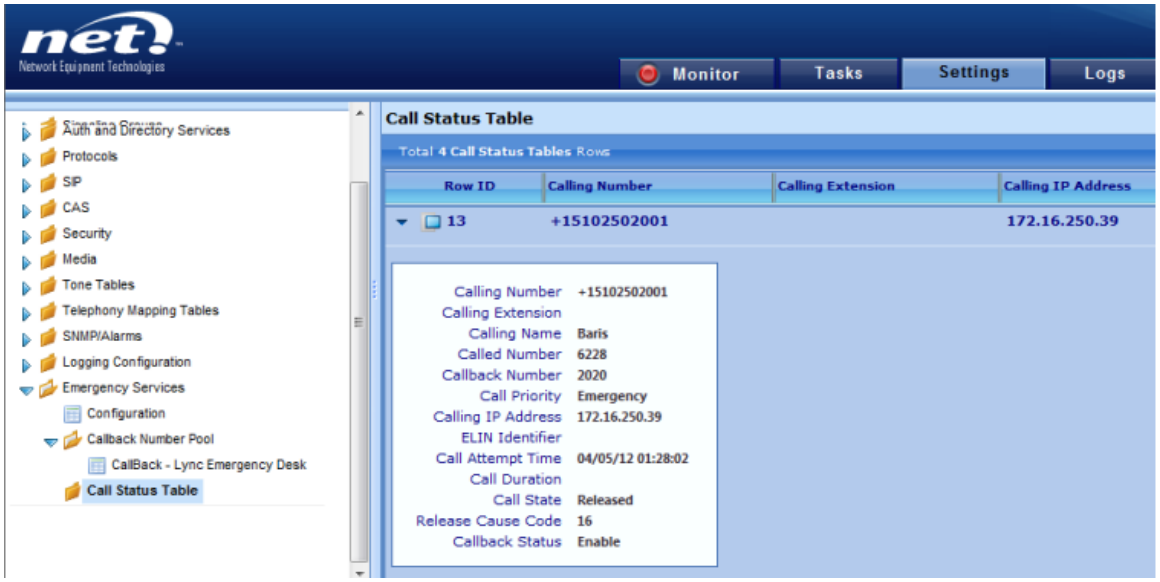


The Sonus SBC 1000/2000 sends out this INVITE message to PSTN as a *ISDN SETUP* message as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



Sonus SBC 1000/2000 WebUI > Settings - Call Status Table (in navigation pane) lists the relevant Emergency Call as shown below:

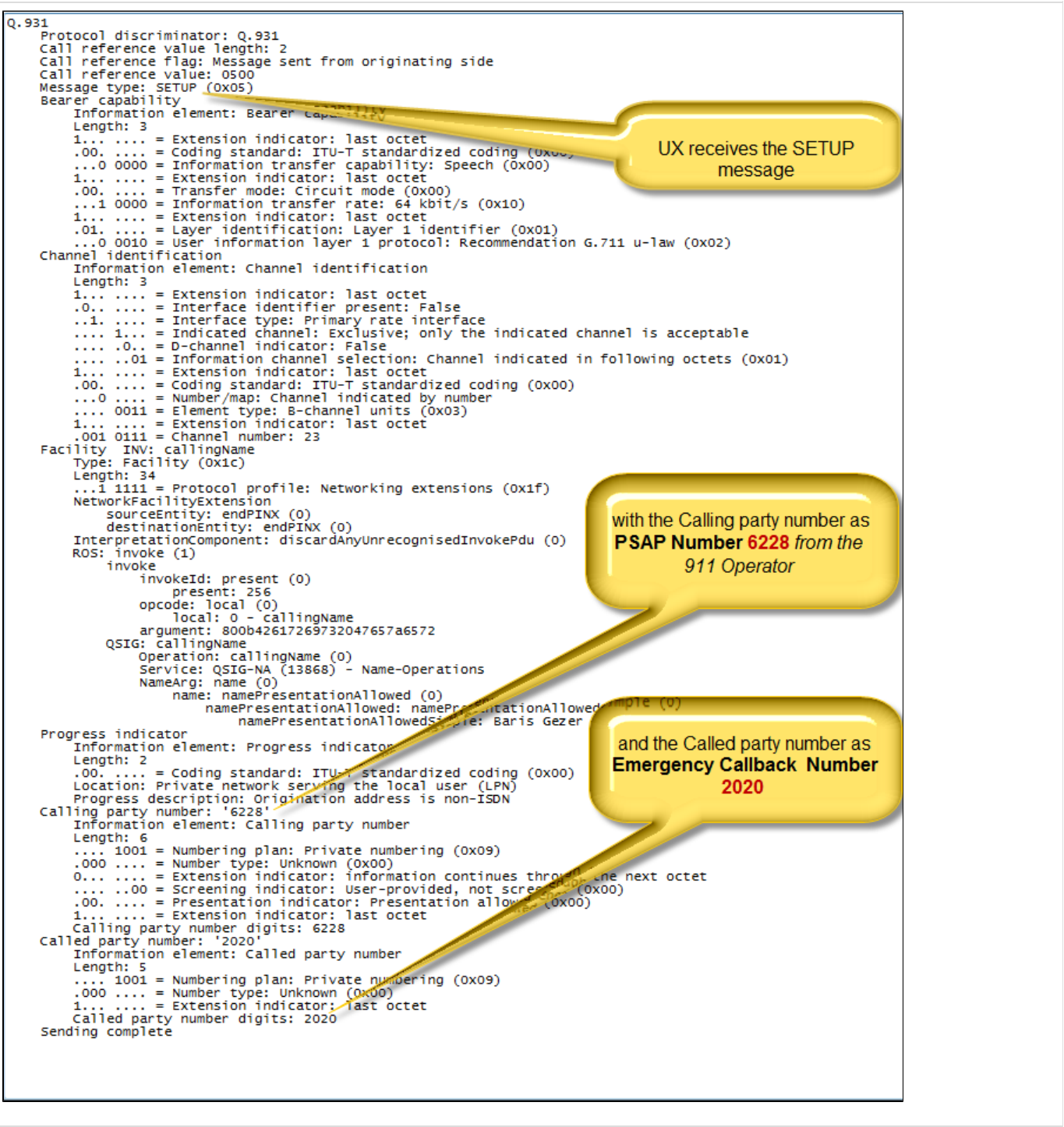


Copyright © 2015 Sonus Networks. All rights reserved.

911 Operator Performs Callback on Previous Call

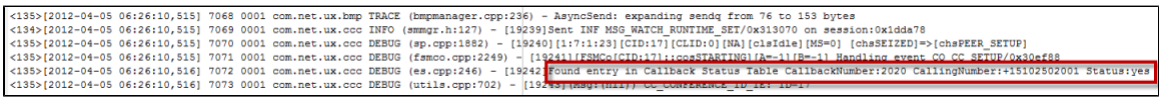
1. 911 Operator PSAP number `6228` performs a callback to Emergency Callback Number `2020`.
2. Sonus SBC 1000/2000 Receives the *ISDN SETUP* message
3. Sonus SBC 1000/2000 finds an entry in **Callback Status Table** for Callback Number `2020` with the relevant Calling Number `+1(510)250-2001`
4. Sonus SBC 1000/2000 routes the call to Lync, and Lync reaches out to the original calling party `+1(510)250-2001`

The relevant *ISDN SETUP* message for above call setup, as shown below:

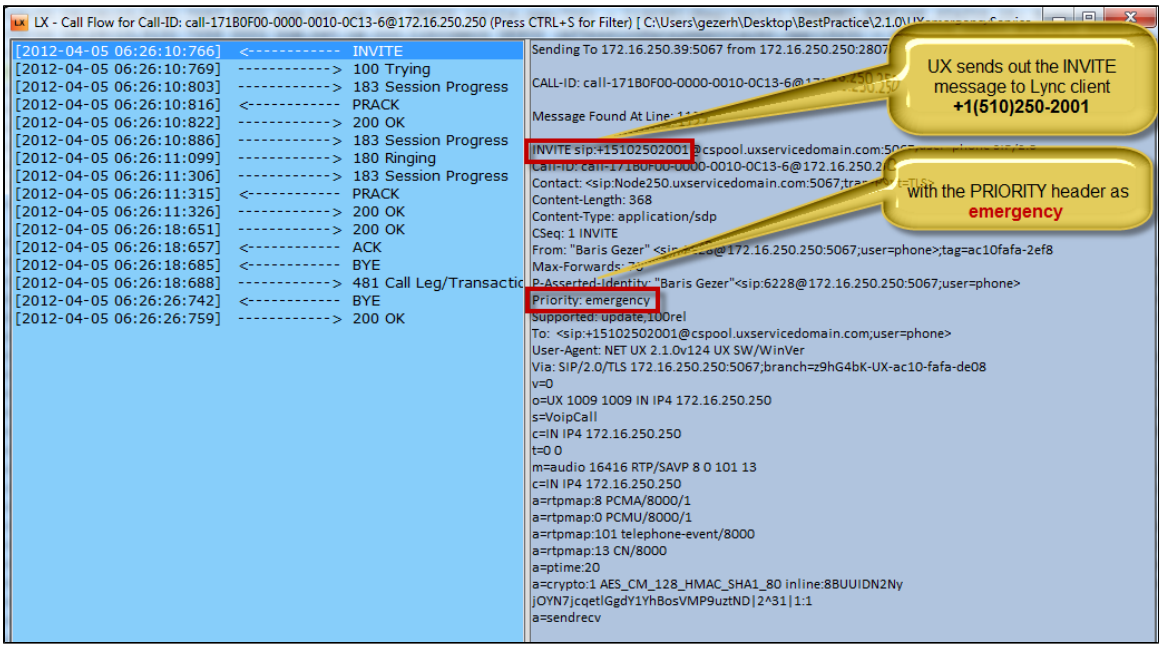


Sonus SBC 1000/2000 Lookup finds the relevant entry in Callback Status Table, as shown below:

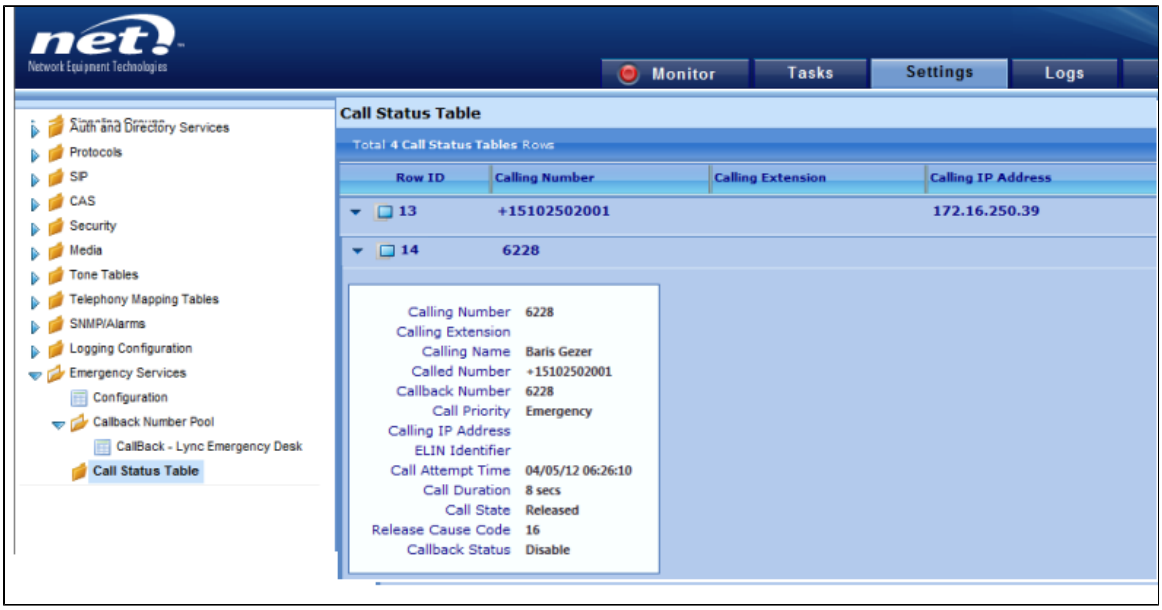
Copyright © 2015 Sonus Networks. All rights reserved.



Sonus SBC 1000/2000 routes the call and send a S_SIP INVITE_ message to the Lync Server, as shown below:



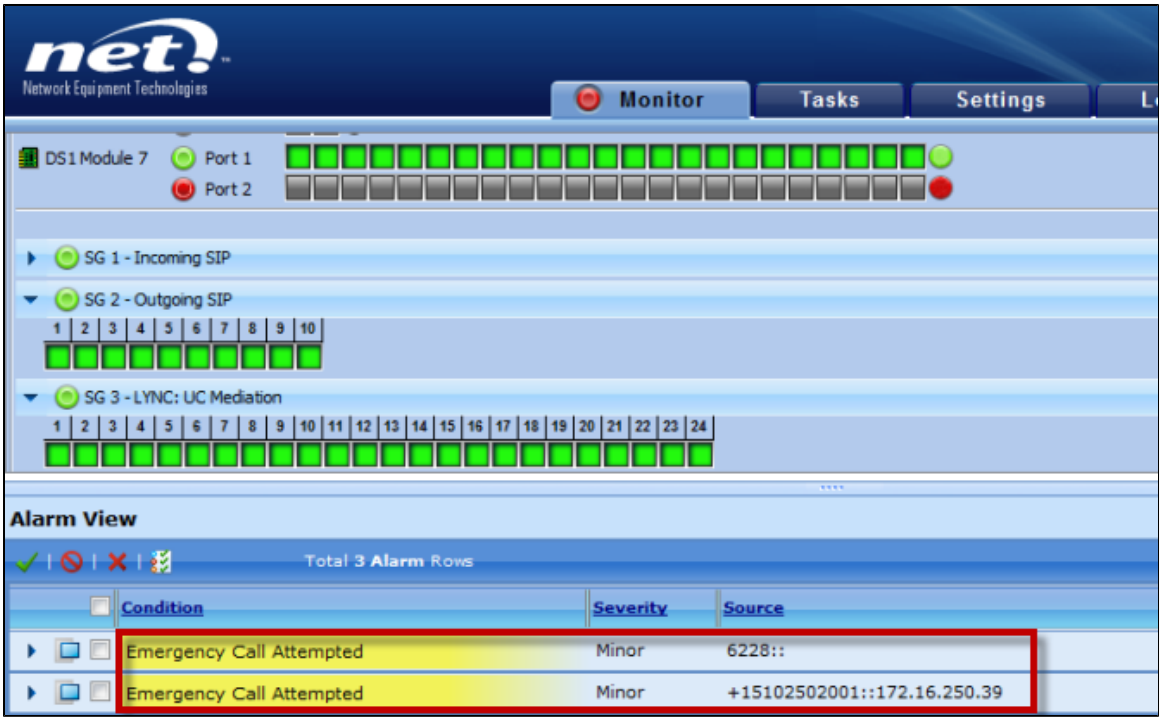
Sonus SBC 1000/2000 Call Status Table logs this call well, as shown below:



Emergency Calls in Alarm View

Every time an Emergency 911 call or PSAP callback call is received on the Sonus SBC 1000/2000, Sonus SBC 1000/2000 throws an alarm with its relevant information as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



LYNC side Gateway Failover Configuration

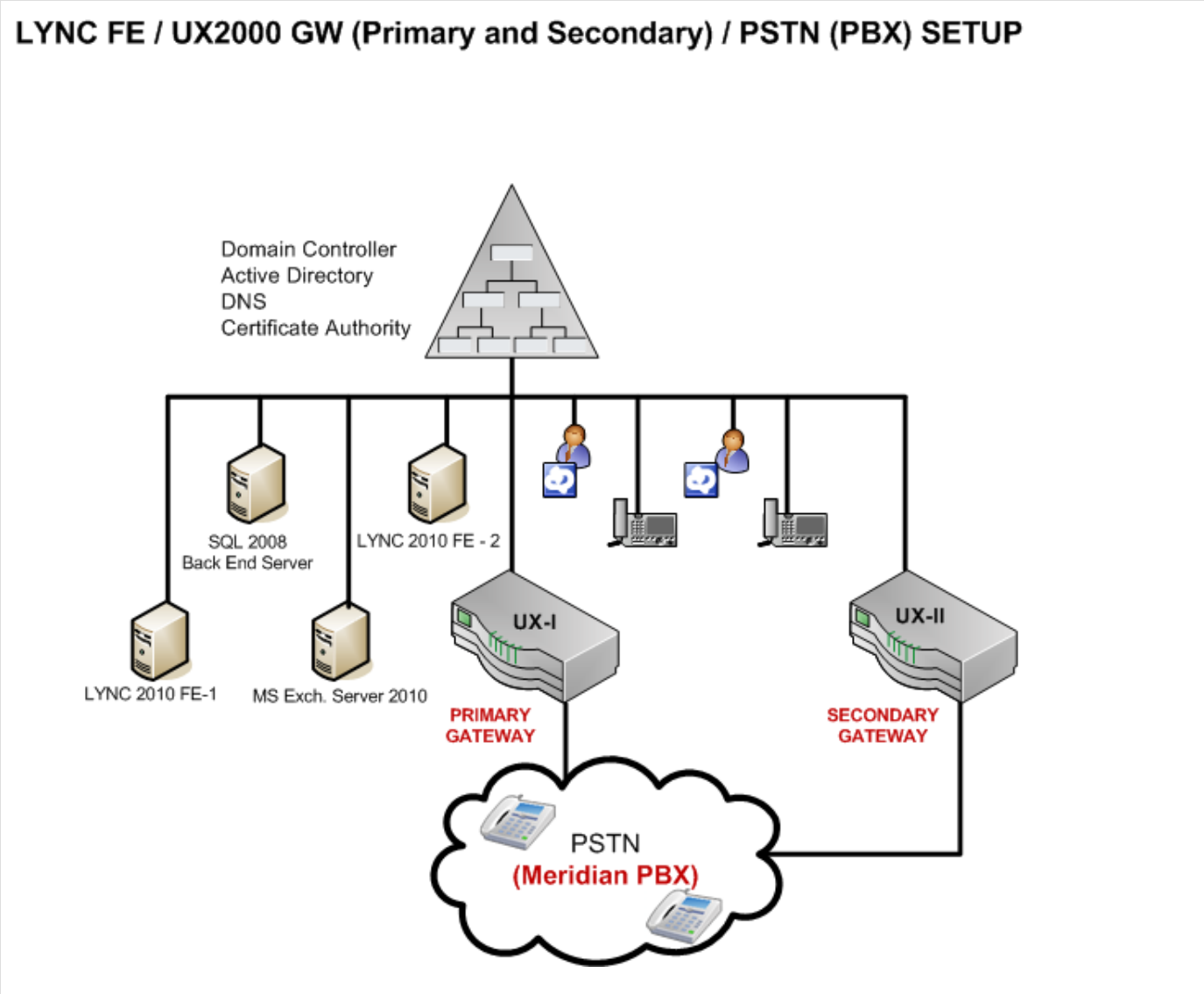
When the gateway in a **Lync - Sonus SBC 1000/2000 - PBX** topology fails, a Lync client will lose its connectivity with PSTN. The use of a back-up or fail-over gateway becomes highly desirable in order to maintain connectivity between Lync and PSTN.

This article describes the steps necessary to configure an additional Sonus SBC 1000/2000 as a fail-over gateway along with the necessary Lync topology configuration bits. For the purpose of this article, it is assumed that **PBX – Sonus SBC 1000/2000 (Primary) – Microsoft Lync 2010** configuration is already in place with MTLS/SRTP as the SIP Transport as shown in the diagram below.

✅ Configuring a **Lync - Sonus SBC 1000/2000 - PBX** topology with a single Sonus SBC 1000/2000 is described in Lync Setup.

Topology

Copyright © 2015 Sonus Networks. All rights reserved.



Overview

This is a two-part process; in the first part of the process, we use the Lync 2010 Setup Wizard on two different Sonus SBC 1000/2000s to point each of them at the same Lync Pool. In the second part, we do the complementary action on the Lync side by specifying both of the Sonus SBC 1000/2000s as PSTN Gateways using the Lync 2010 Topology Builder.

- Sonus SBC 1000/2000 Configuration
  - Primary Sonus SBC 1000/2000 Configuration
  - Secondary Sonus SBC 1000/2000 Configuration
- LYNC Topology Configuration
  - Defining the Gateway
  - Associating the Gateway with a Mediation Server
  - Configuring the LYNC Voice Routing

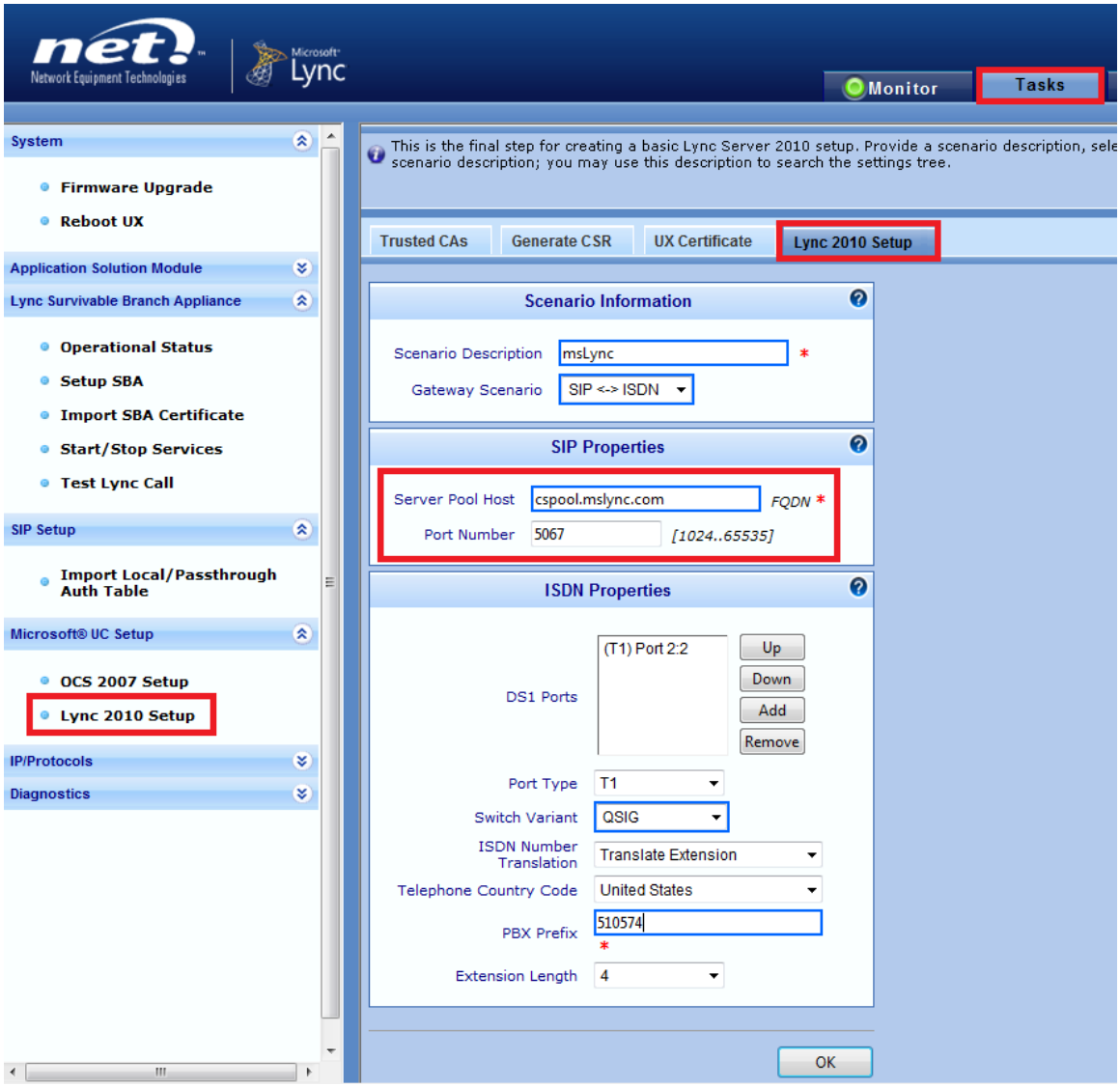
Sonus SBC 1000/2000 Configuration

Both Sonus SBC 1000/2000s are configured with the **Lync 2010 Setup Wizard** to interoperate with a Lync 2010 Pool as shown in the figure below.

Copyright © 2015 Sonus Networks. All rights reserved.

For this exercise, the following are the identities of the pool and Sonus SBC 1000/2000 devices:

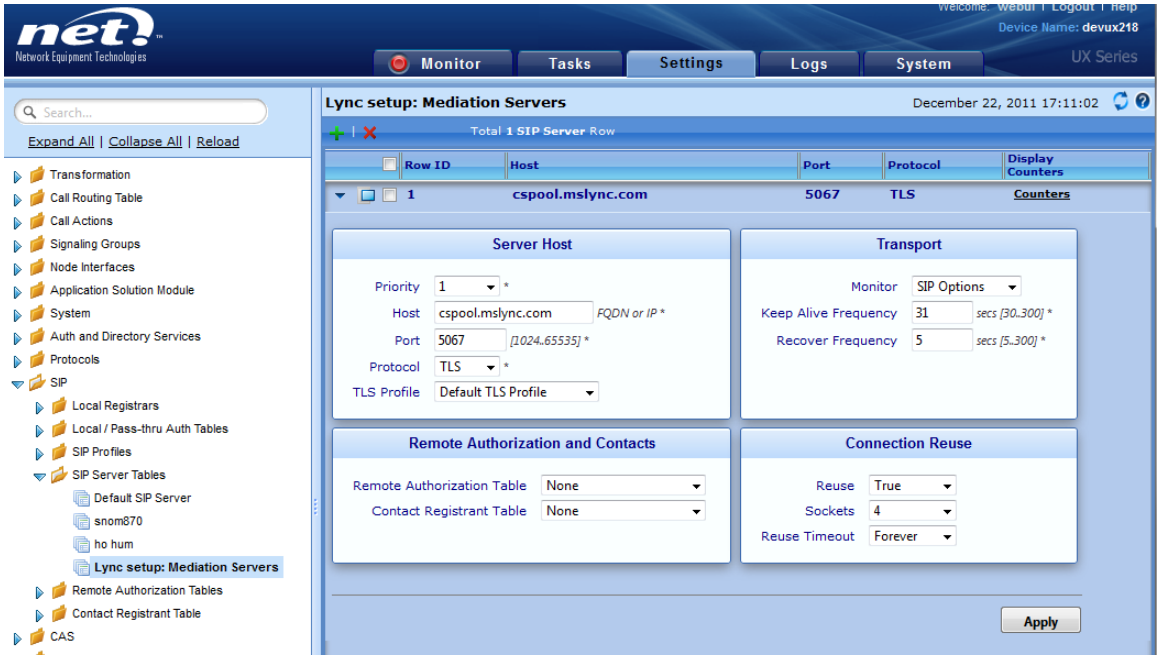
- Lync Pool Name: *cspool.mxlync.com*
- Primary Sonus SBC 1000/2000: *testux212.mslync.com*
- Secondary Sonus SBC 1000/2000: *testux226.mslync.com*



Primary Sonus SBC 1000/2000 Configuration

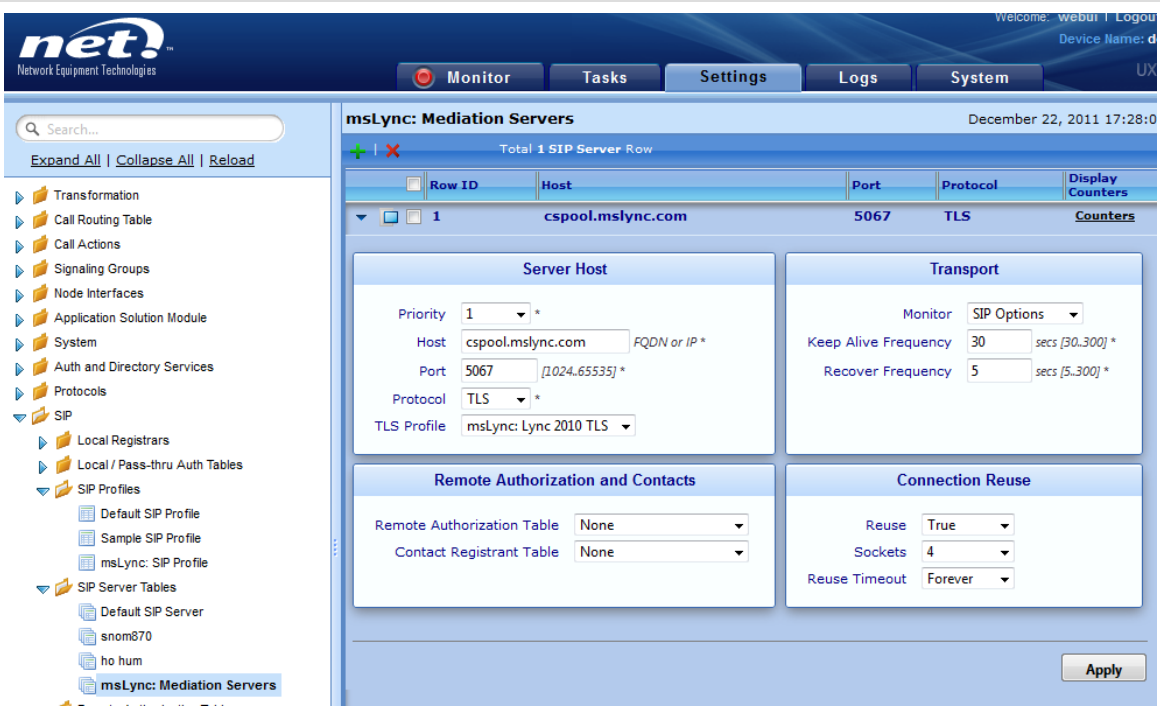
After successfully running the wizard, a primary Sonus SBC 1000/2000 is configured for Lync 2010 Interoperability as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



Secondary Sonus SBC 1000/2000 Configuration

After successfully running the wizard, a secondary Sonus SBC 1000/2000 is configured for Lync 2010 Interoperability as shown below.



LYNC Topology Configuration

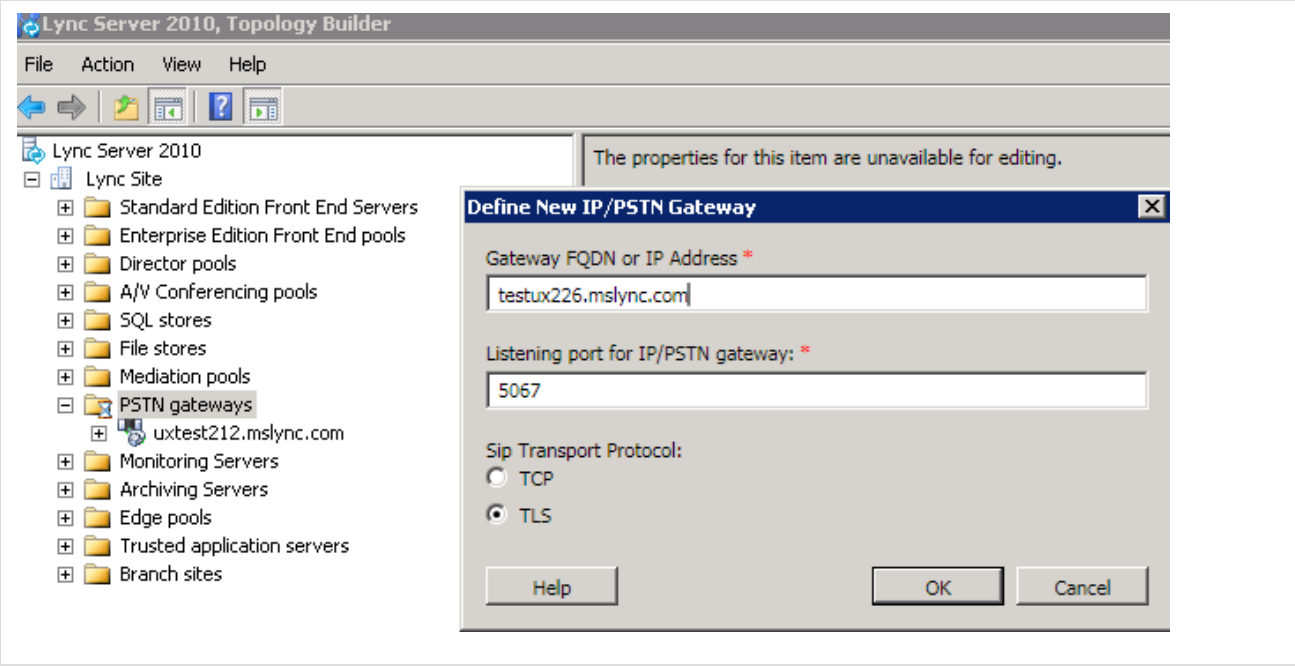
To add the secondary Sonus SBC 1000/2000 Node into the Lync Topology, please follow these steps:

Defining the Gateway

Copyright © 2015 Sonus Networks. All rights reserved.

To define the gateway:

1. Use Remote Desktop to connect to the Lync Front End Server.
2. Launch the Topology Builder.
3. In the left pane, right-click on **PSTN gateways**.
4. Select **Define New Gateway**to add the secondary Sonus SBC 1000/2000 gateway as shown below.

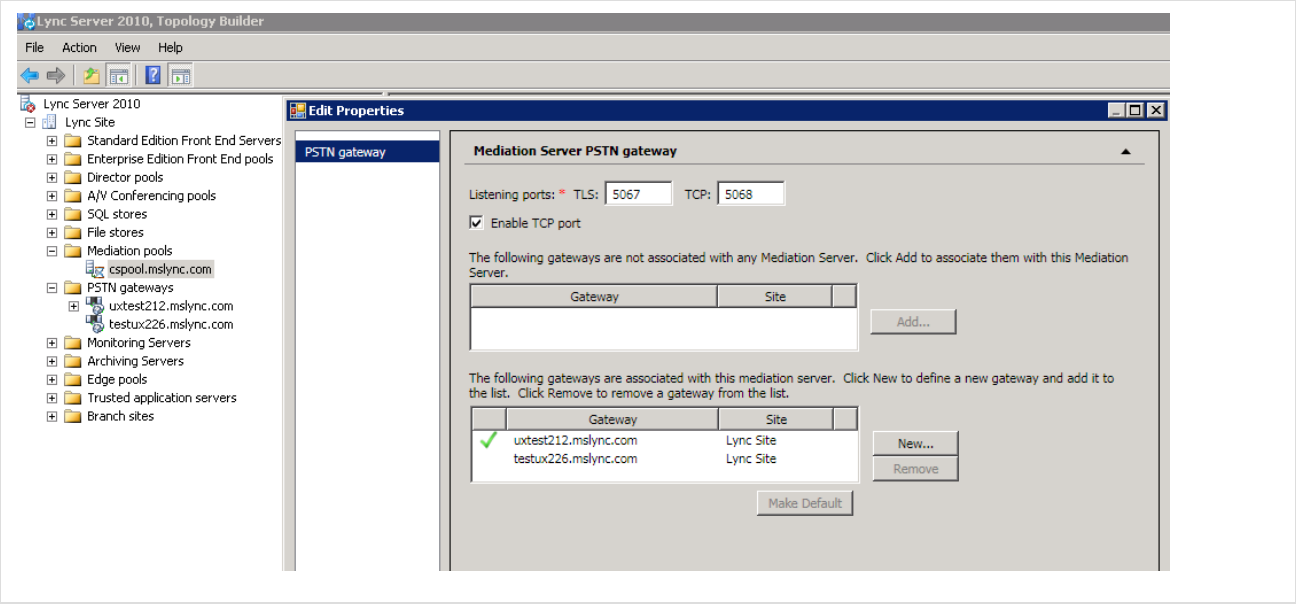


Associating the Gateway with a Mediation Server

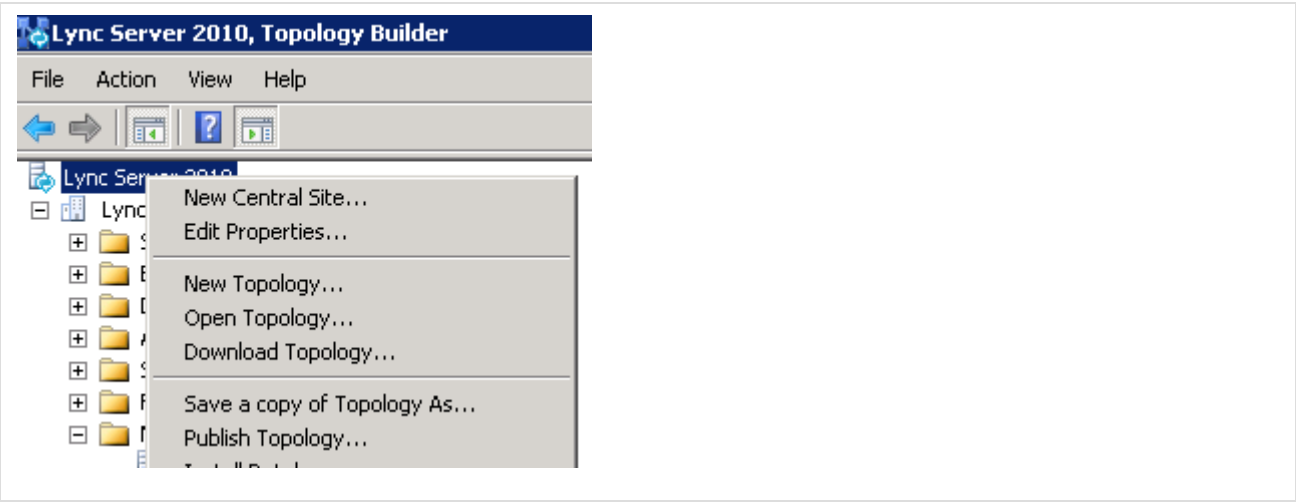
To associate the gateway:

1. Use Remote Desktop to connect to the Lync Front End Server.
2. Launch the Topology Builder.
3. In the left pane select **Mediation pools > *relevant pool***.
4. Right-click, then select **Edit** to open its properties.
5. Select the newly added Sonus SBC 1000/2000 gateway from the list.
6. Click **Add...**to associate it with the Mediation Server as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



7. Use Remote Desktop to connect to the Lync Front End Server.
8. Launch the Topology Builder.
9. Right-click on **Lync Server 2010** in left pane.
10. Select **Publish Topology...**as shown below.

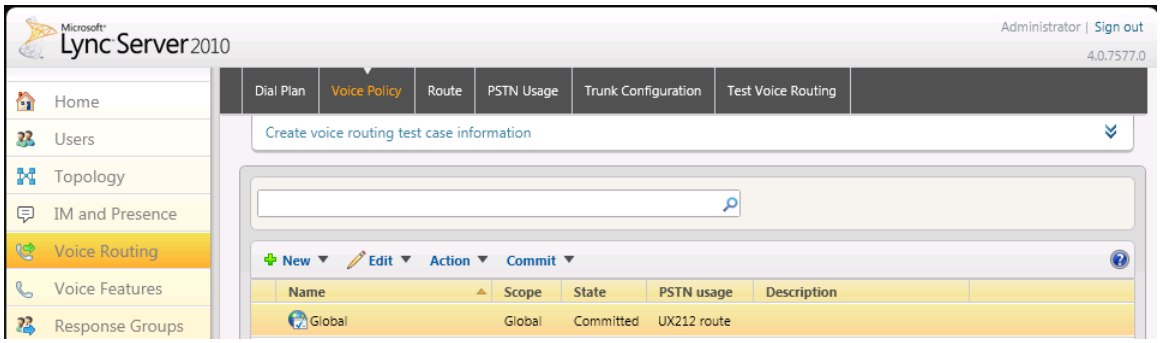


Configuring the LYNC Voice Routing

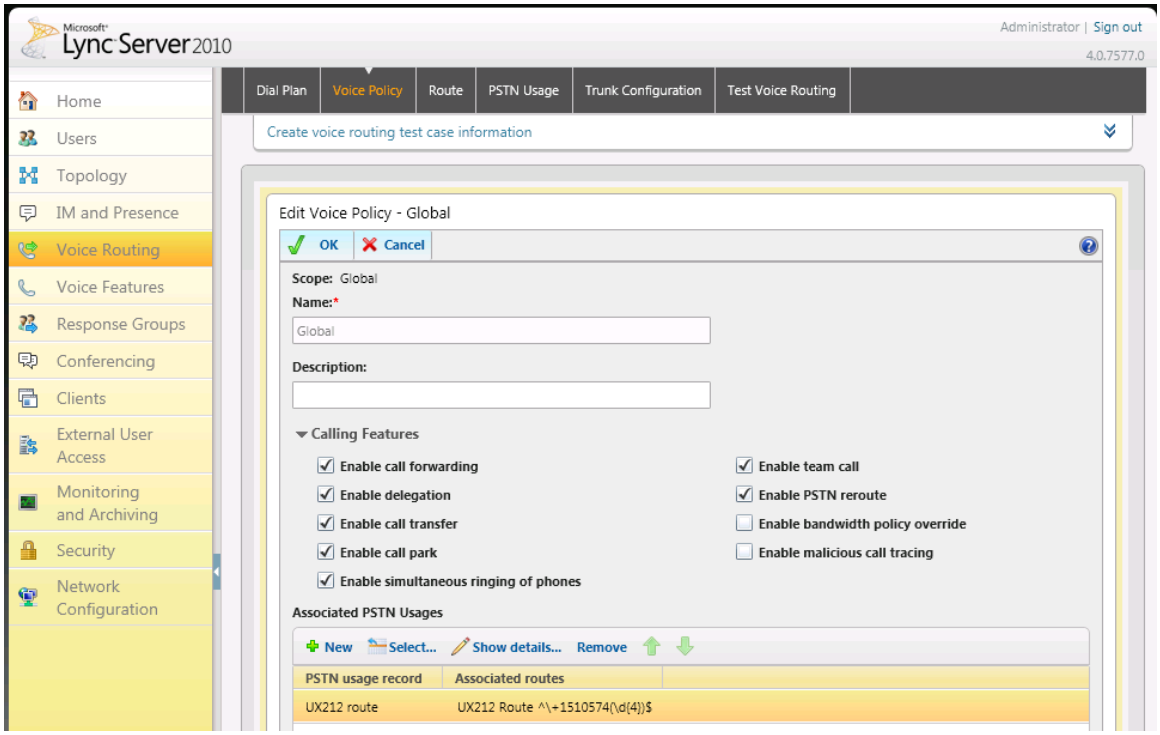
To configure voice routing:

1. Open the **LYNC Server 2010**configuration page:
    a. Enter the URL of the Front-End pool (**https://<fqdn of the front end pool>/cscp**).
2. Click **Voice Routing** in the left pane.
3. Click **Voice Policy** in the right pane.
4. Double-click the relevant policy_ in the list.

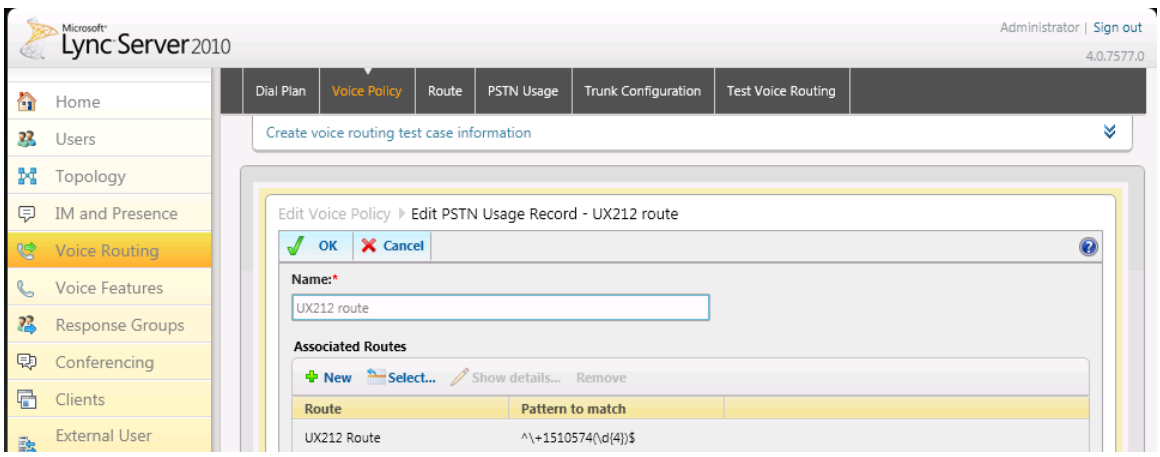
Copyright © 2015 Sonus Networks. All rights reserved.



5. Double click the relevant PSTN usage record.

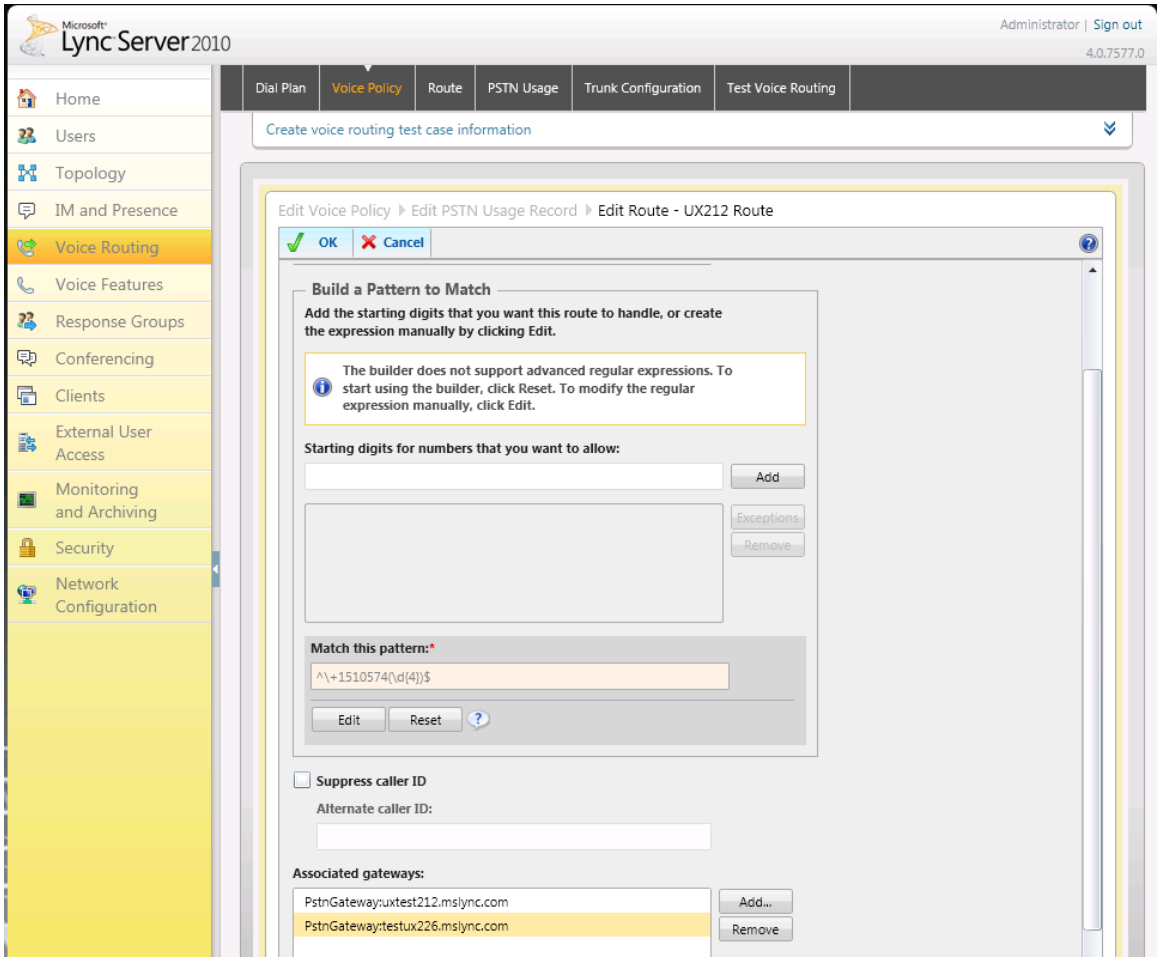


6. Double Click on the Route entry.



7. Add the secondary Sonus SBC 1000/2000 gateway into Associated Gateways list

Copyright © 2015 Sonus Networks. All rights reserved.



8. Click OK, OK, and OK to exit out of the Voice Policy configuration.

Lync 2013 Call Forwarding Integration to an ITSP

This document outlines the steps required to ensure that calls forwarded from Lync 2013 to the ITSP contain a phone number that the ITSP will accept.

On This Page

- The Original Problem
- Configuration Details
  - Configuration Overview
  - Lync 2013 Required Configuration
  - SBC 1000-2000 Configuration
    - Diversion header
    - From header
    - P-Asserted-Identity (PAI) header
- Additional Information

Copyright © 2015 Sonus Networks. All rights reserved.

Related Articles
• Creating and Modifying Entries to Transformation Tables • SIP Message Manipulation Overview • SIP Message Manipulation • SIP Message Manipulation Document Catalog • 6 Steps to Creating Effective SMM Rules • Managing Signaling Groups

Devices Affected	
Models	**Versions**
SBC 1000/2000	3.0.2v242 and higher

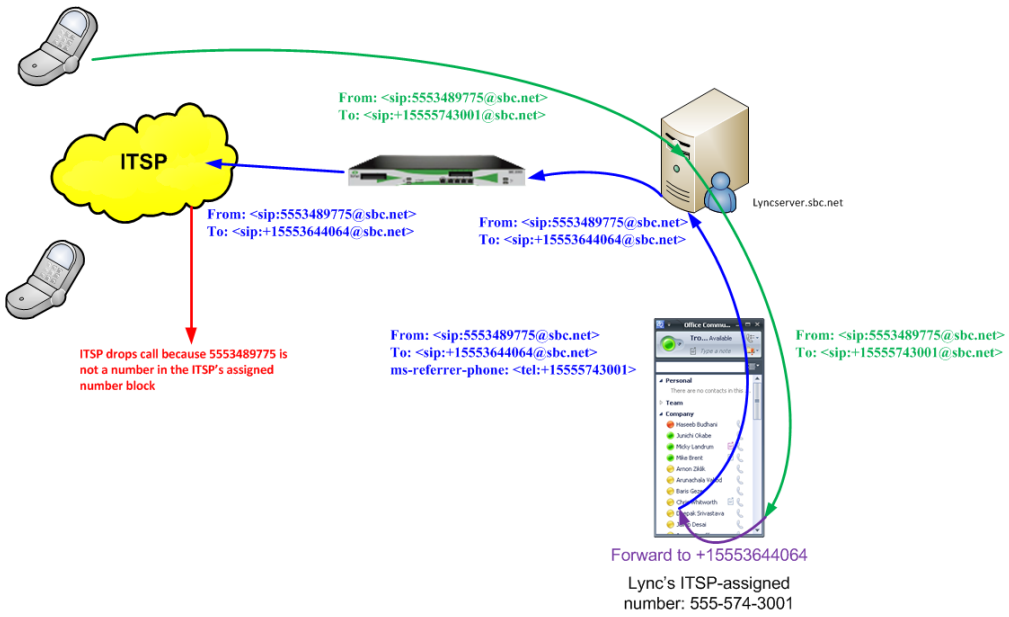
⚠ This article is only applicable to Lync 2013. It is not applicable to Lync 2010 installations.

The Original Problem

As some SIP Trunk providers require that calls originate from the number range the ITSP has assigned to the customer, it is necessary to ensure that all calls from SBC to the ITSP have a FROM, DIVERSION or P-Asserted-Identity (PAI) number which is from the ITSP-assigned range. For instance, if the carrier has assigned a customer 574-1000 to 574-9999, the calling number, diversion, or PAI for any SBC --> ITSP call must fall within that range.

However, calls that are forwarded by Lync 2013 back to the SIP Trunk contain the calling number (FROM header) of the original calling number rather than the Lync 2013 number. In this case, the ITSP refuses to route the call because the calling number is that of the original caller, not an ITSP-assigned number.

The following call flow diagram depicts the scenario where the call forwarded by Lync 2013 does not have History-Info



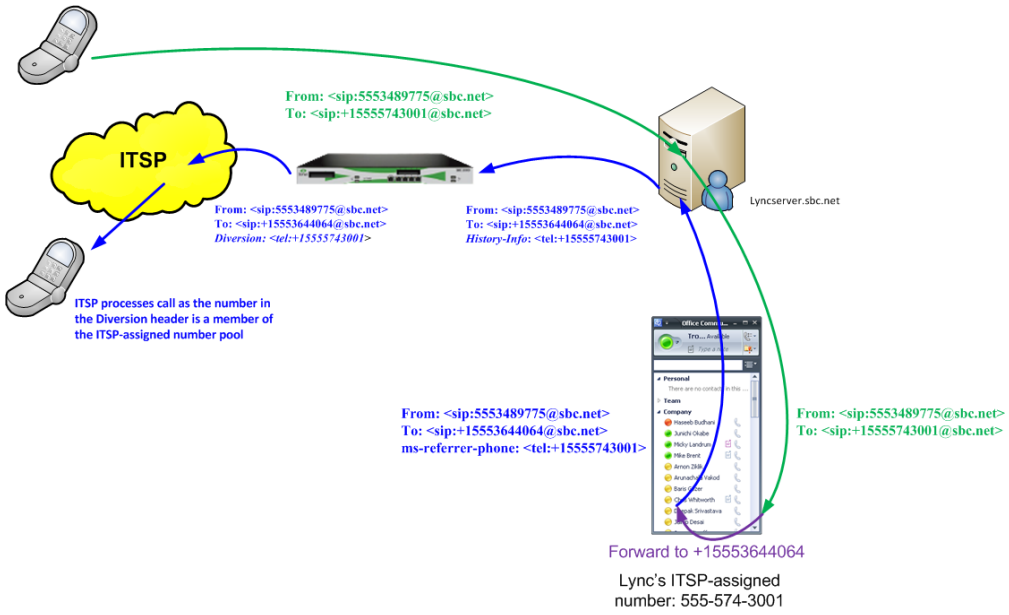
Copyright © 2015 Sonus Networks. All rights reserved.

Configuration Details

Configuration Overview

Configure Lync 2013 Server to supply History-Info on forwarded calls, then use the SBC to convert the number in the History-Info header to a SIP header the ITSP will accept for calling authorization.

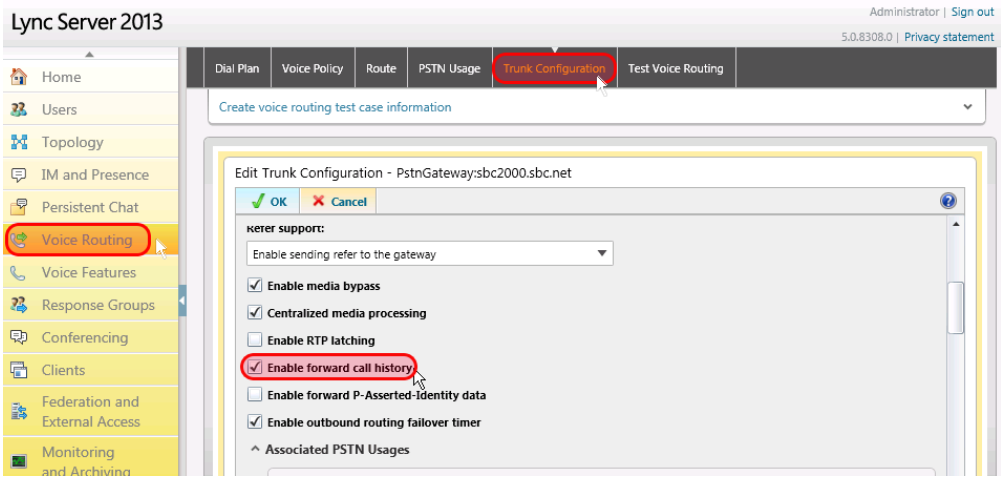
The following call flow diagram shows a Lync Server configured to supply History-Info on forwarded calls:



Lync 2013 Required Configuration

The Lync Server Trunk Configuration must be configured to supply History-Info on forwarded calls

To enable Lync Server to Send History-Info, navigate to "Voice Routing", "Trunk Configuration" and check the "Enable forward call history" option



SBC 1000-2000 Configuration

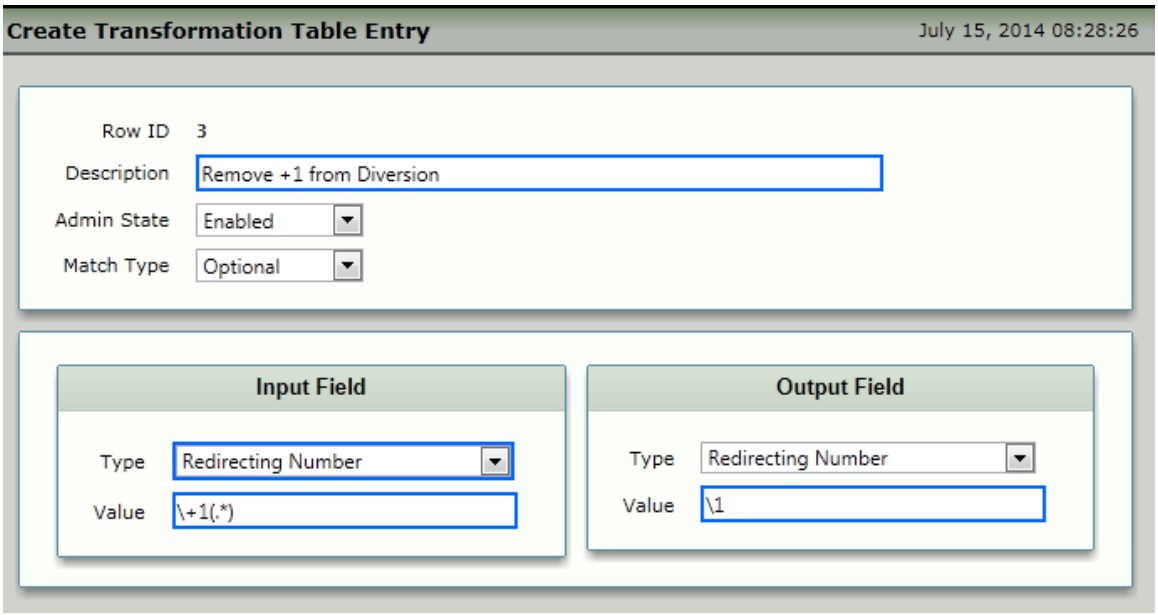
The SBC can be configured to supply Diversion, From, and/or PAI headers to the ITSP. Use the sections below to provide the desired header.

Copyright © 2015 Sonus Networks. All rights reserved.

Diversion header

The SBC will automatically map Lync's History-Info header into a Diversion header when sending the call to the ITSP. No other configuration is required in order to send a Diversion Header to the ITSP.

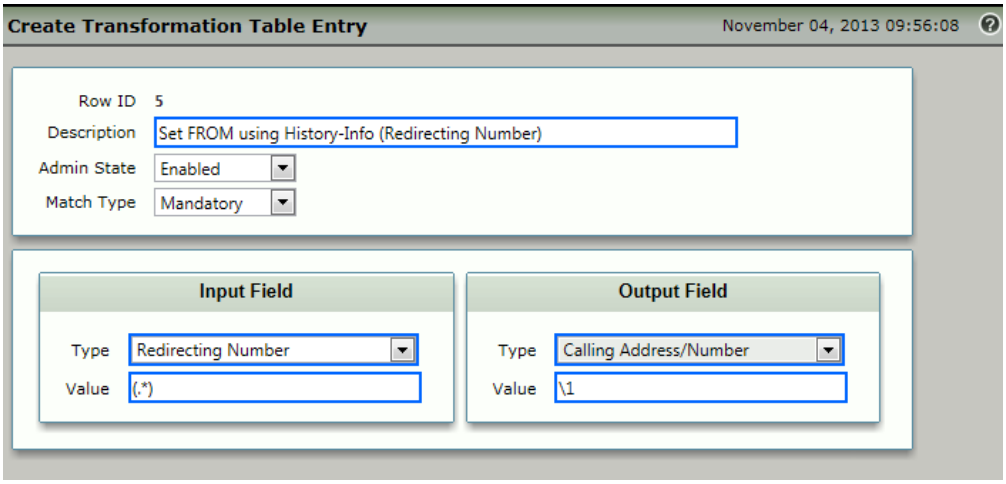
Modifying the outgoing Diversion Header number is achieved by simply making an entry in the Transformation Table. The Transformation Entry below removes the +1 from the Diversion Header.



From header

The incoming History-Info header is automatically mapped into the SBC's transformation table *Redirecting Number* IE. To send the History-Info number as the From (calling) number, add the entry below to the appropriate transformation table.

Set the *Calling Number* using History-Info:



P-Asserted-Identity (PAI) header

A SIP Message Manipulation (SMM) permits setting the PAI number using the History-Info number. Several steps are required:

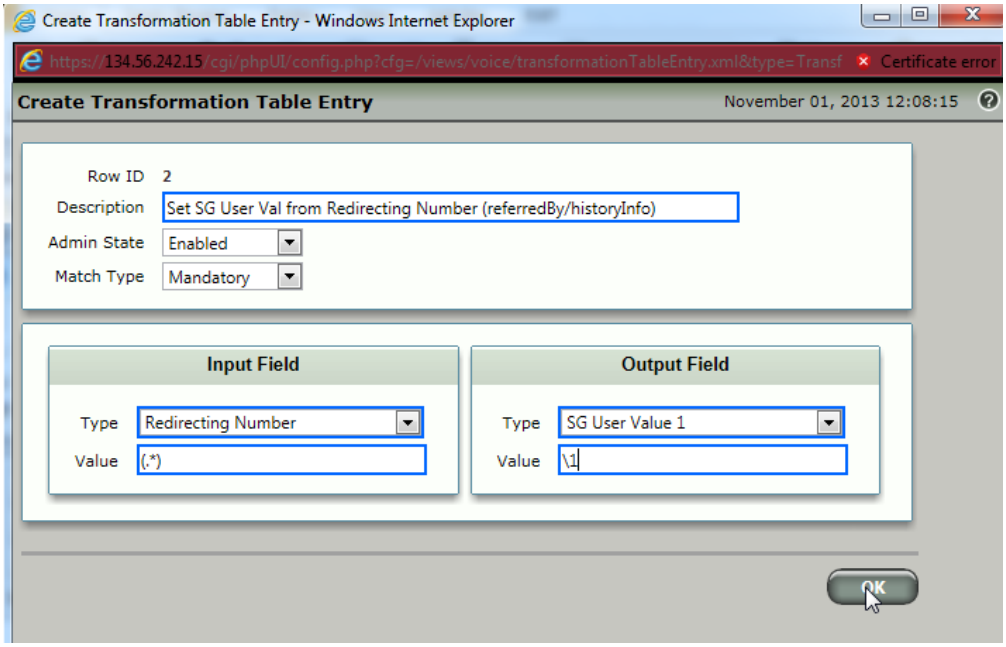
Copyright © 2015 Sonus Networks. All rights reserved.

1. In the transformation table, set *SG User Value 1* IE from the *Redirecting Number* IE.
2. Create a SMM Rule to insert *SG User Value 1* into the PAI header.
3. Add the SMM Rule to the ITSP Signaling Group.

> The SMM configuration below contains just the salient elements for creating the necessary SMM Rule. See SIP Message Manipulation - Setting the P-Asserted Identity for step-by-step instructions on creating a SMM Rule. Be sure to substitute the steps below as appropriate when building the SMM Rule.

Step 1: Transformation Table Configuration

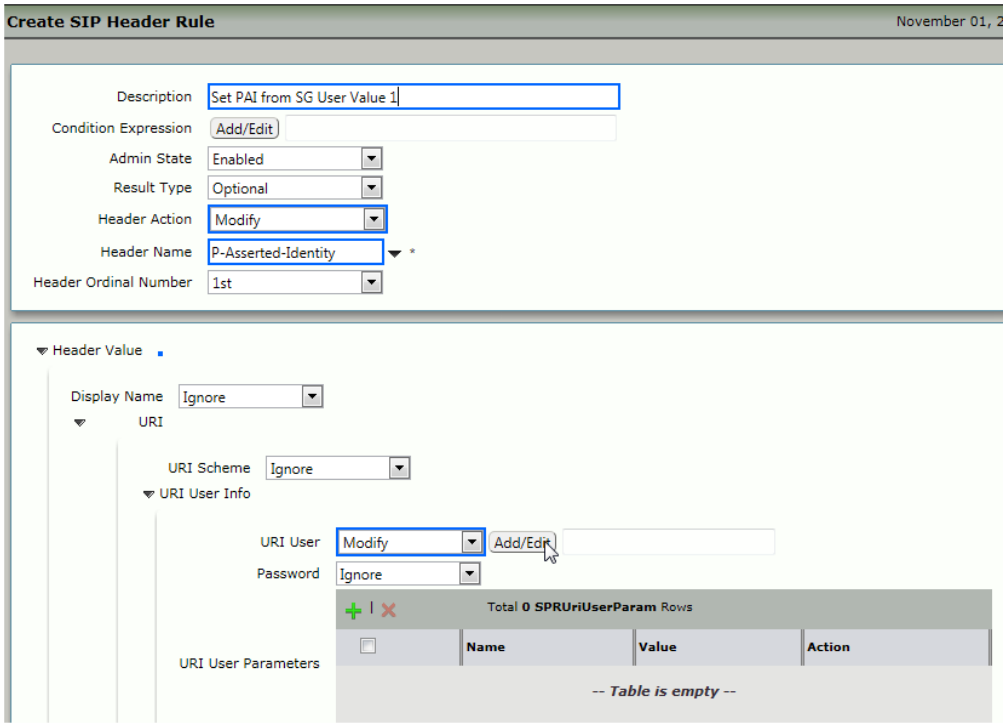
- In the transformation table, set *SG User Value 1* IE from the *Redirecting Number* IE



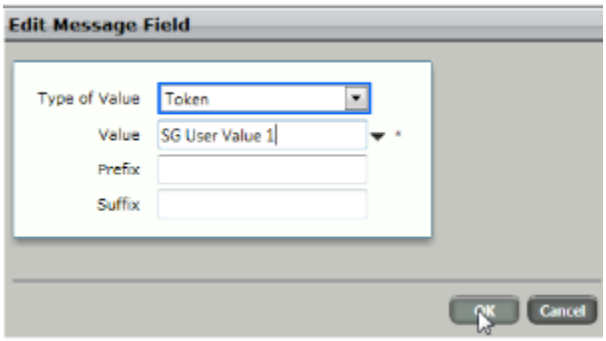
Step 2: SIP Message Manipulation Configuration

- Create a SMM Rule to set the URI User (the PAI number) in the P-Asserted-Id header.

Copyright © 2015 Sonus Networks. All rights reserved.

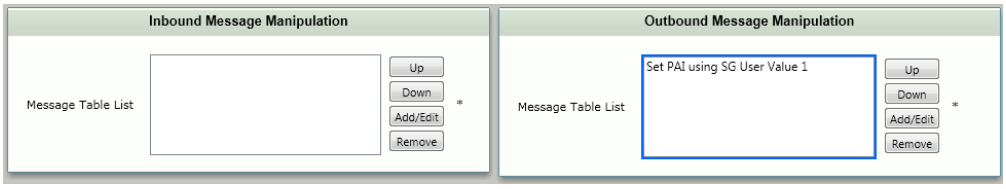


- Configure the Add/Edit to retrieve the number from SG User Value 1.



Step 3: Add the SMM Rule to the ITSP Signaling Group

- Add the newly created SMM Rule to the Outbound Message Manipulation section of the ITSP Signaling Group.



Additional Information

See Lync Referred-by and ITSP SIP Trunks for information regarding Lync 2010, Lync-forwarded calls, and ITSP integration. This SolutionBase article will not function for Lync 2010 installations.

Copyright © 2015 Sonus Networks. All rights reserved.

In testing, the Lync Server did not dynamically update its configuration when the *Enable Forward Call History* was changed. A combination of restarting the Lync Server Front-End and Mediation Server services was successful in enabling the Lync Server to include the History-Info header.

SBC 1k/2k Release 3.0.2v242 automatically maps the incoming number from Referred-By and History-Info in the transformation table's *Redirecting Number* IE. For outgoing call legs, the SBC will automatically create a Diversion header if a number is present in the *Redirecting Number* IE.

SIP Registration

This set of pages deals with SIP registration on the SBC 1000/2000

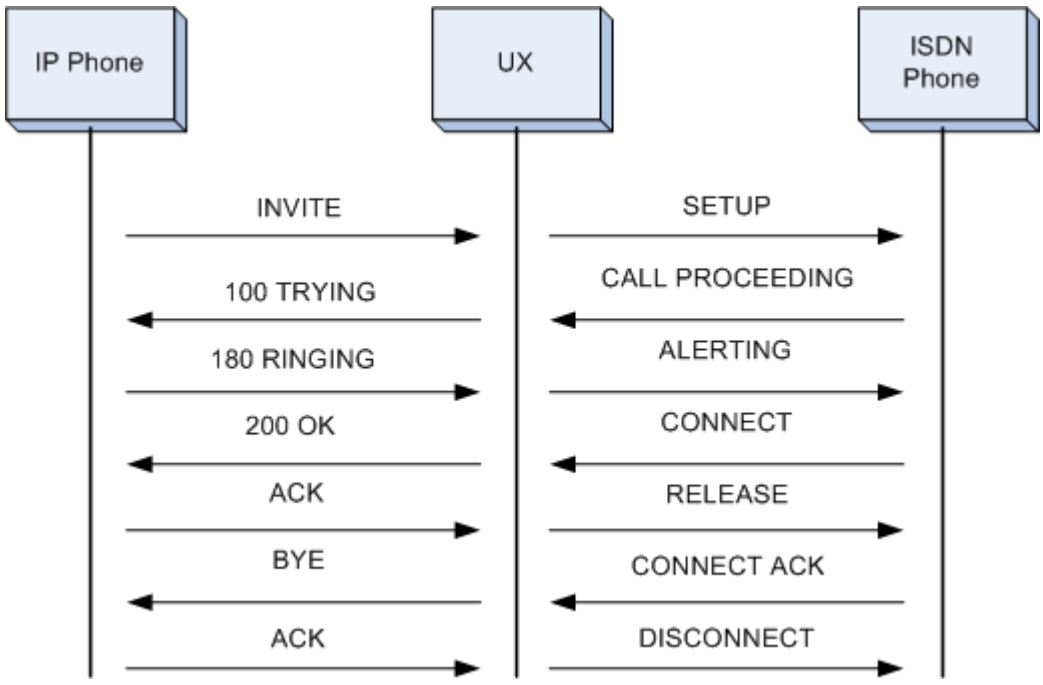
SIP Phone Registration and SIPph to Sonus SBC 1000-2000 to ISDN call

SIP Registration using Authorization Tables

SIP Phone Registration and SIPph to Sonus SBC 1000-2000 to ISDN call

This article describes the steps necessary to configure the Sonus SBC 1000/2000 so that a call may be placed from a SIP phone through the Sonus SBC 1000/2000 to an ISDN endpoint as depicted by the following call flow:

Topology



On this page:

Copyright © 2015 Sonus Networks. All rights reserved.

- Sonus SBC 1000/2000 Configuration
  - SIP Local Registrar Table Configuration
  - Transformation Table Configuration
  - Call Routing Table Configuration
  - SIP Signaling Group Configuration
  - ISDN Port Configuration
  - ISDN Signaling Group Configuration
- Verification
  - Endpoint Registration:

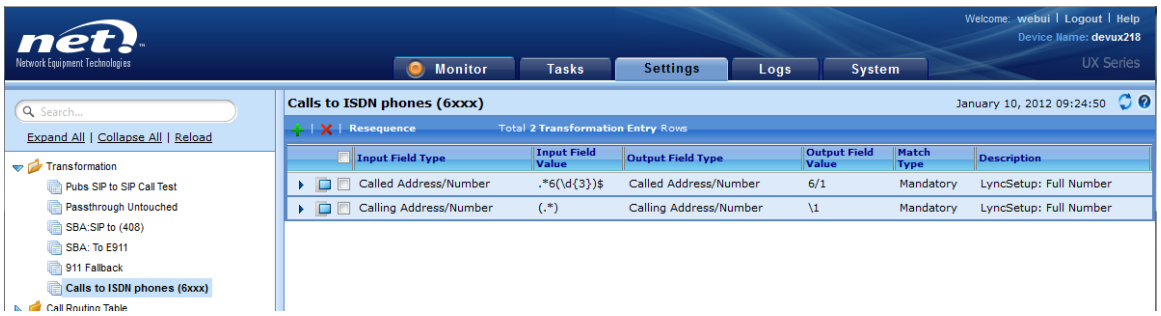
Sonus SBC 1000/2000 Configuration

SIP Local Registrar Table Configuration

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Local Registrars**
3. Add a new SIP Local Registrar.

Transformation Table Configuration

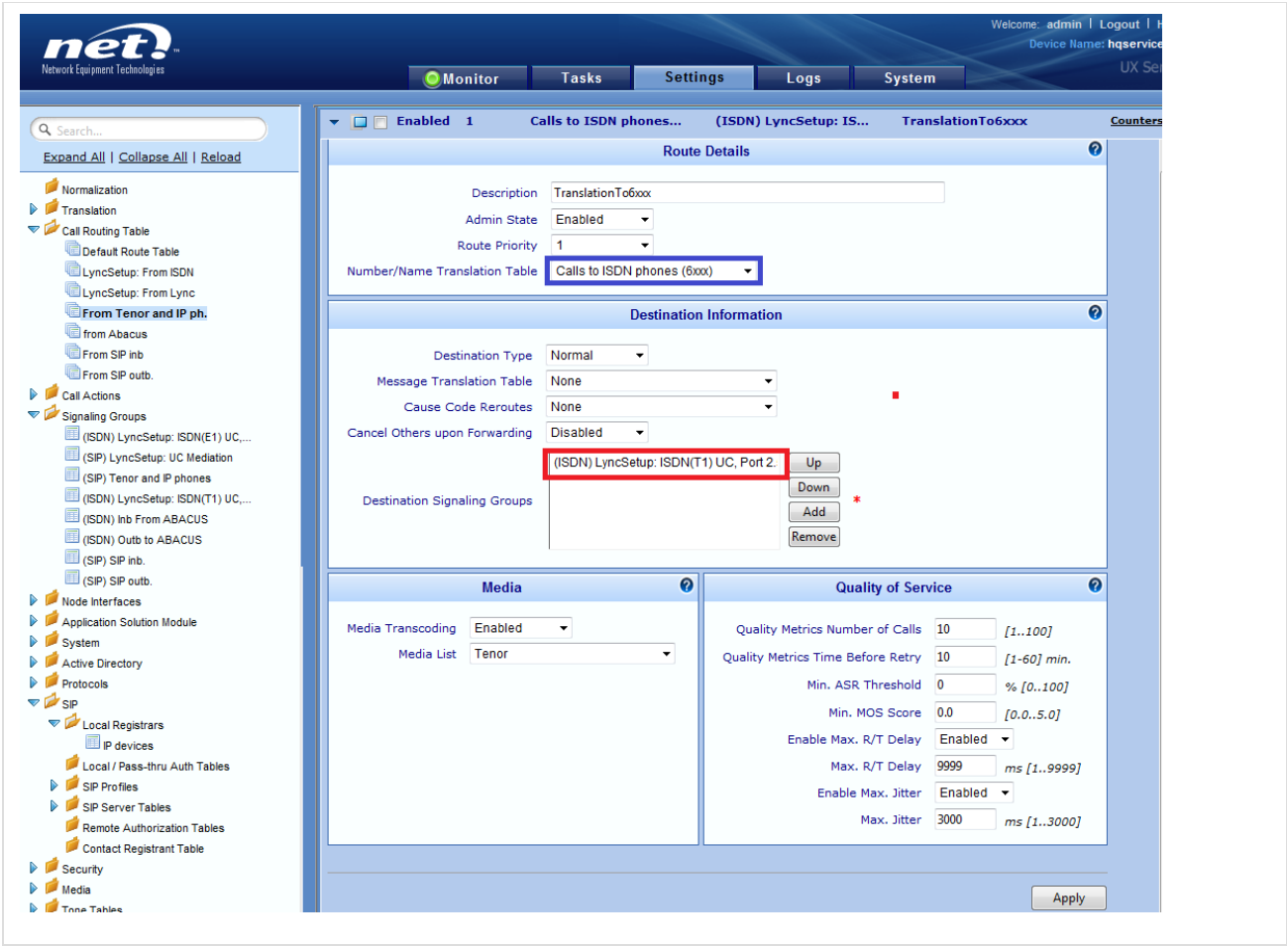
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Transformation**
3. Add a new Transformation Table.
4. Add two entriesto the new Transformation Table as show below.



Call Routing Table Configuration

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table**
3. Add a new Call Routing Table.
4. Add an entryto the new Call Routing Table and configure it as shown below.

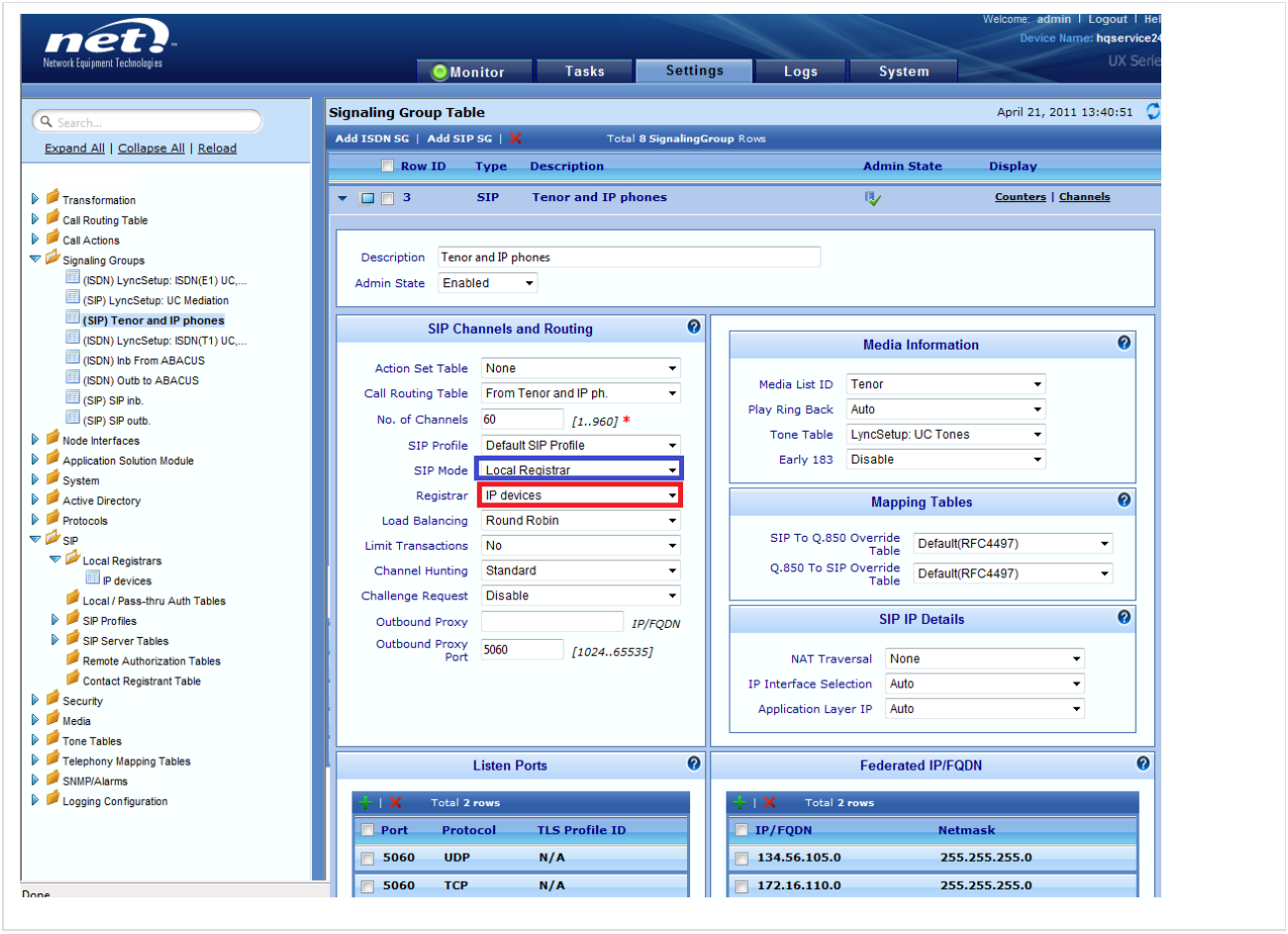
Copyright © 2015 Sonus Networks. All rights reserved.



SIP Signaling Group Configuration

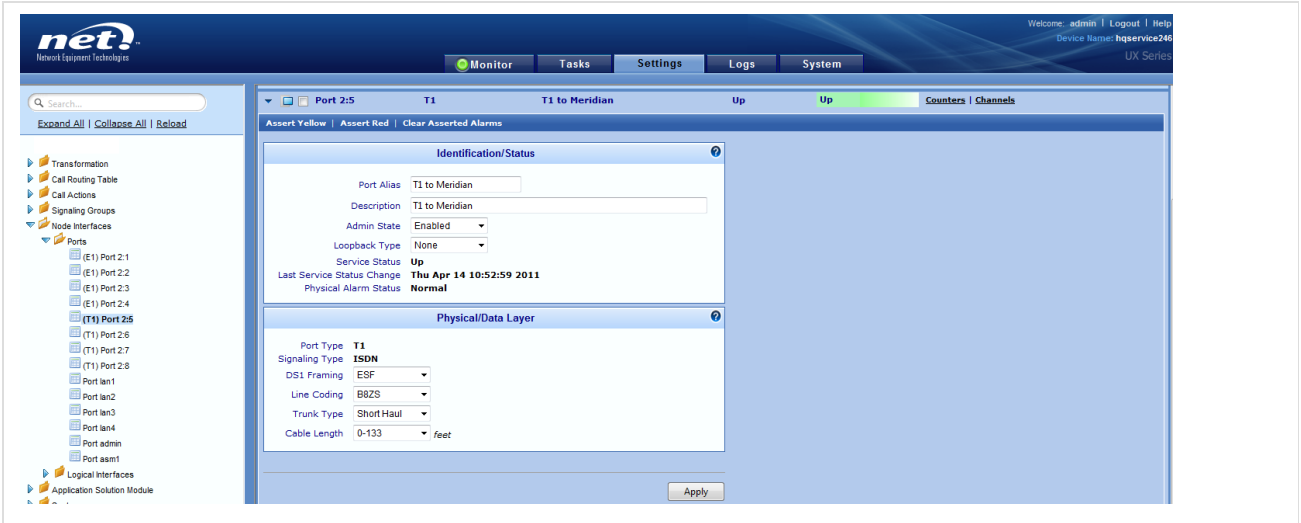
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Add a new SIP Signaling Groupand configure it as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



ISDN Port Configuration

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**.
3. Click the port you wish to configure.
4. Configure the portas shown below.

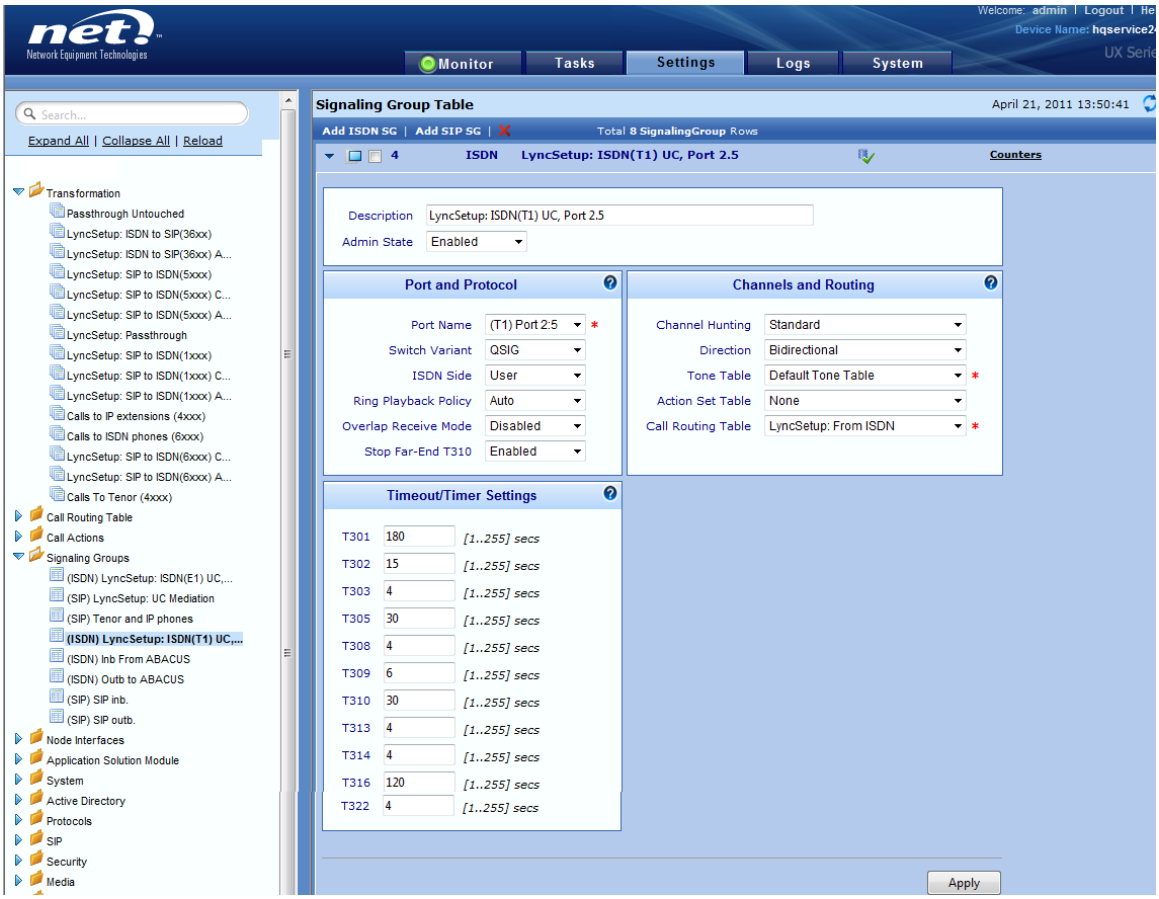


ISDN Signaling Group Configuration

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.

Copyright © 2015 Sonus Networks. All rights reserved.

3. Add a new ISDN Signaling Group.
4. Configure the new ISDN Signaling Group as shown below.



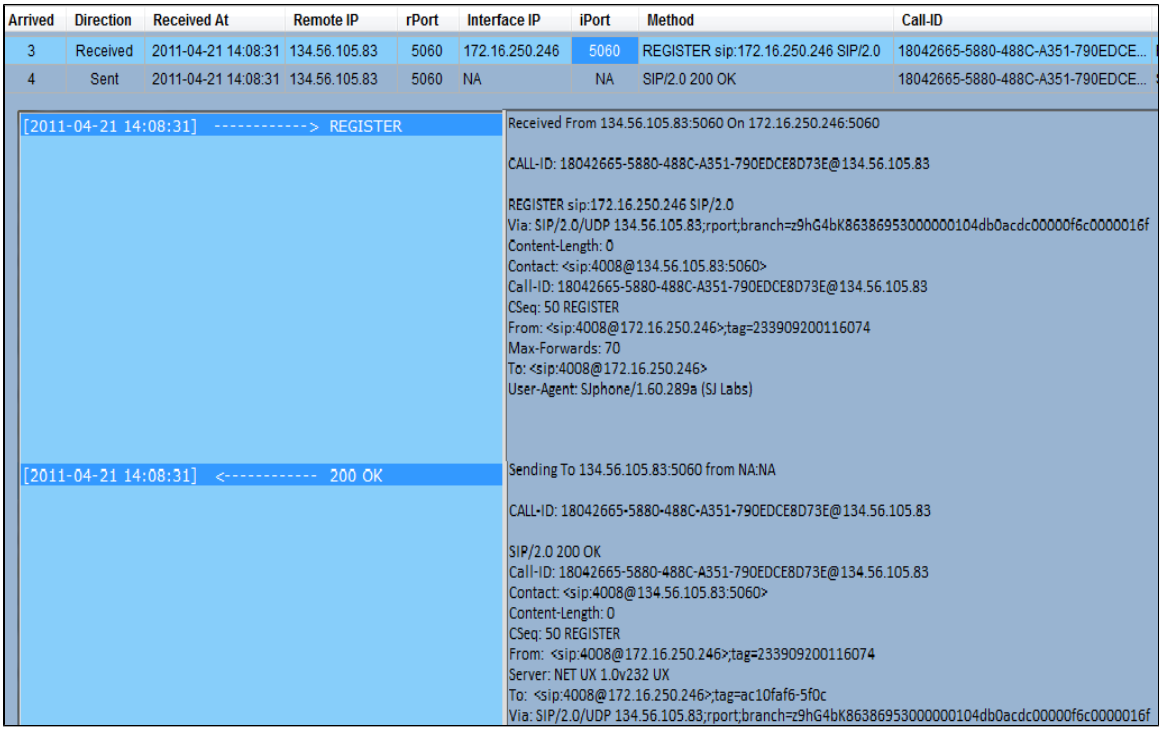
Verification

Endpoint Registration:

When the endpoint registers, the registration request arrives to the Sonus SBC 1000/2000 through the SIP signaling group, the Sonus SBC 1000/2000 responds to the REGISTRATION request with a 200 OK – a successful SIP endpoint registration occurs.

Using the **Log Exchange** utility, you can quickly verify the relevant SIP messaging:

Copyright © 2015 Sonus Networks. All rights reserved.



SIP Registration using Authorization Tables

This article describes the steps necessary to configure the features required for a SIP endpoint to register with the Sonus SBC 1000/2000 using Local/Pass-through Authorization Tables:

- Sonus SBC 1000/2000 Configuration
  - Add an Entry to the Local Registrar Table
  - Add a Local/Pass-through Authorization Table
  - Add an Entry to the Local/Pass-through Authorization Table
  - Add a Call Routing Table
  - Add and Configure a SIP Signaling Group
- Endpoint Registration
  - Endpoint Configuration
  - Registration Verification

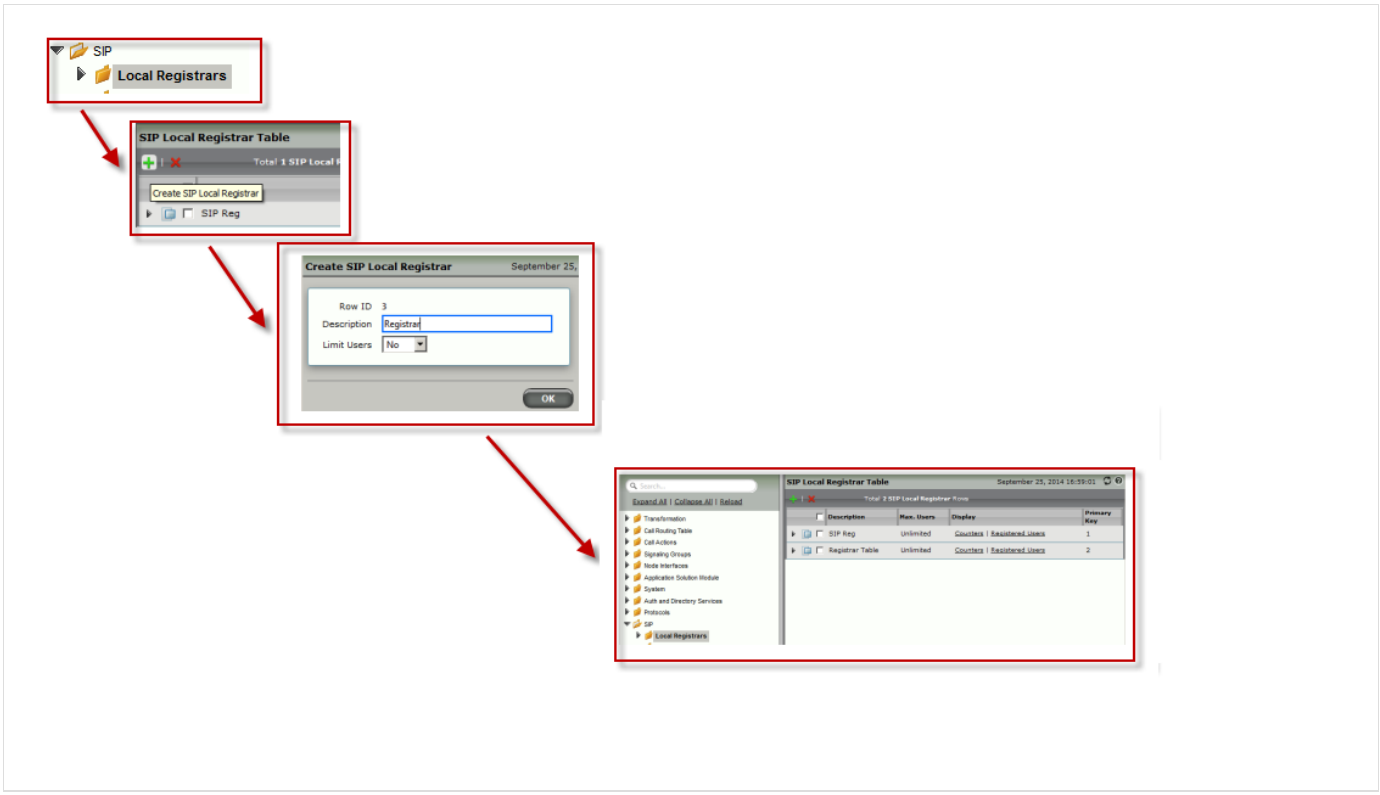
Sonus SBC 1000/2000 Configuration

Add an Entry to the Local Registrar Table

To add a Local Registrar Table entry:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Local Registrars**
3. Click the **Create SIP Local Registrar** (+) icon.
4. Enter a name for the table entry.
5. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.

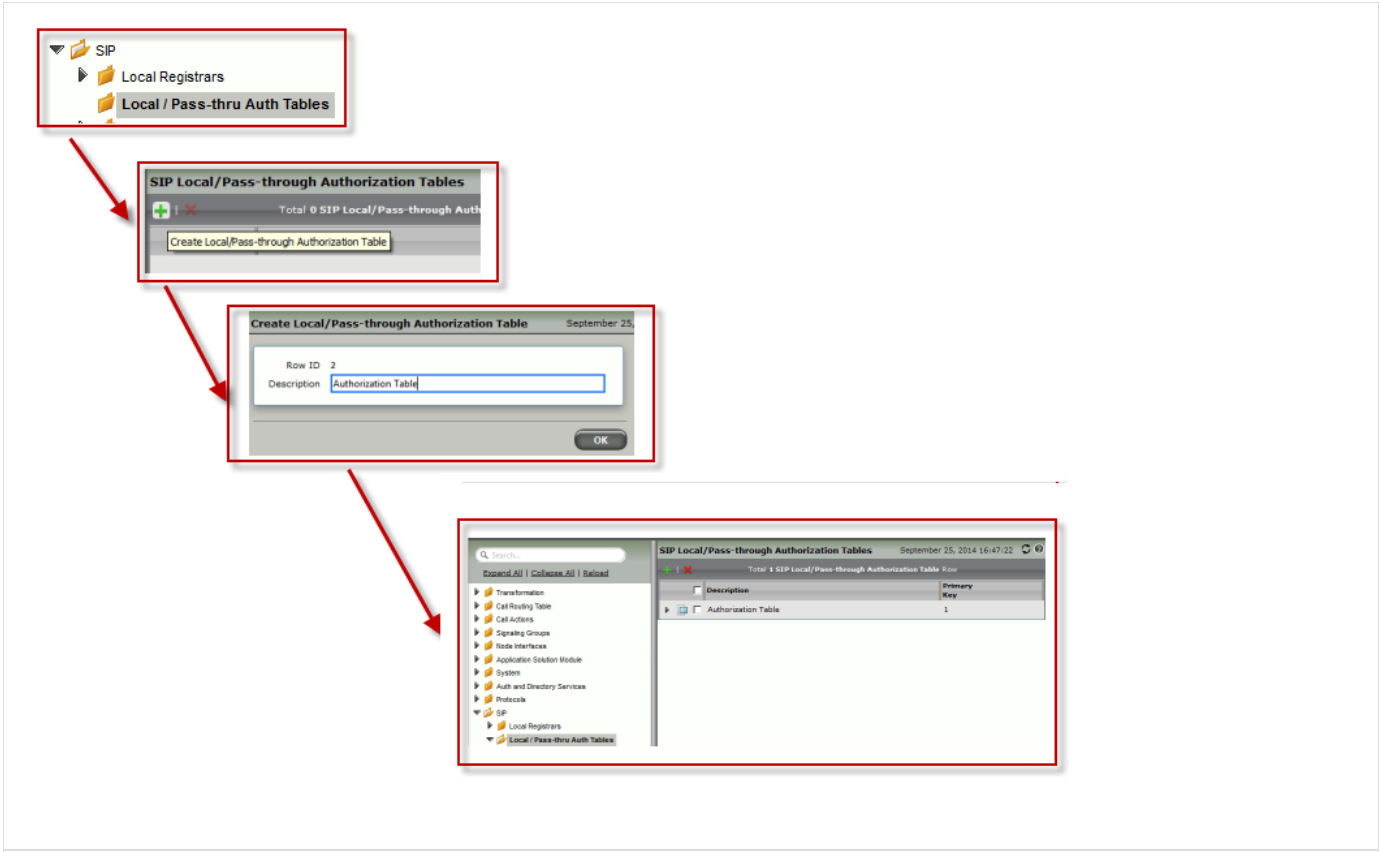


Add a Local/Pass-through Authorization Table

To add a Local/Pass-through Auth Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Local/Passthru Auth Tables.**
3. Click the **Create Local/Pass-through Authorization Table** ( ) icon.
4. Enter a name for the table entry (i.e: Authorization Table).
5. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.

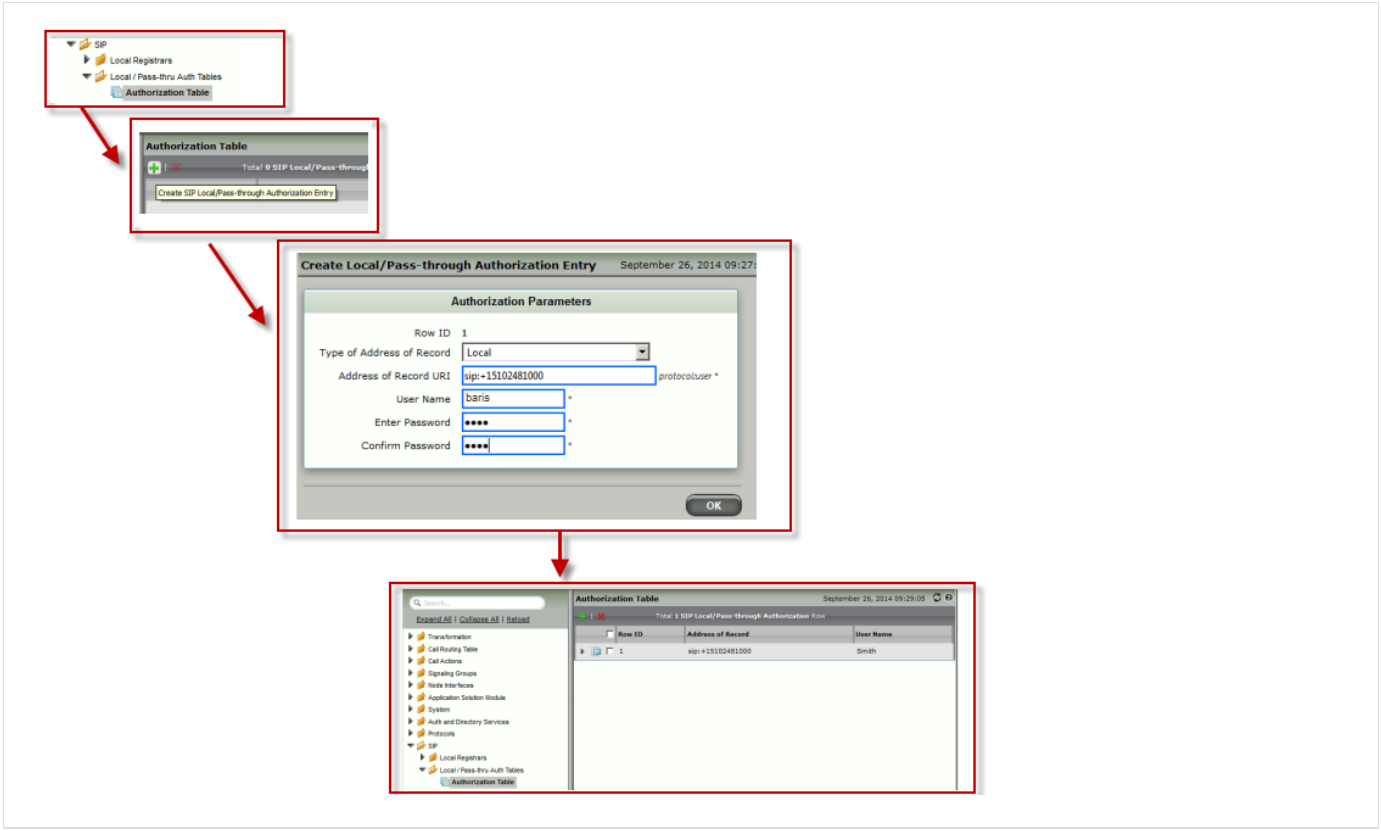


Add an Entry to the Local/Pass-through Authorization Table

To add an entry to the table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > Local/Pass-thru Auth Tables**.
3. Click the **Authorization Table** entry.
4. Click the **Create Local/Pass-through Authorization Entry** (+) icon.
5. Complete the Authorization Parameters fields as shown below.
6. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.

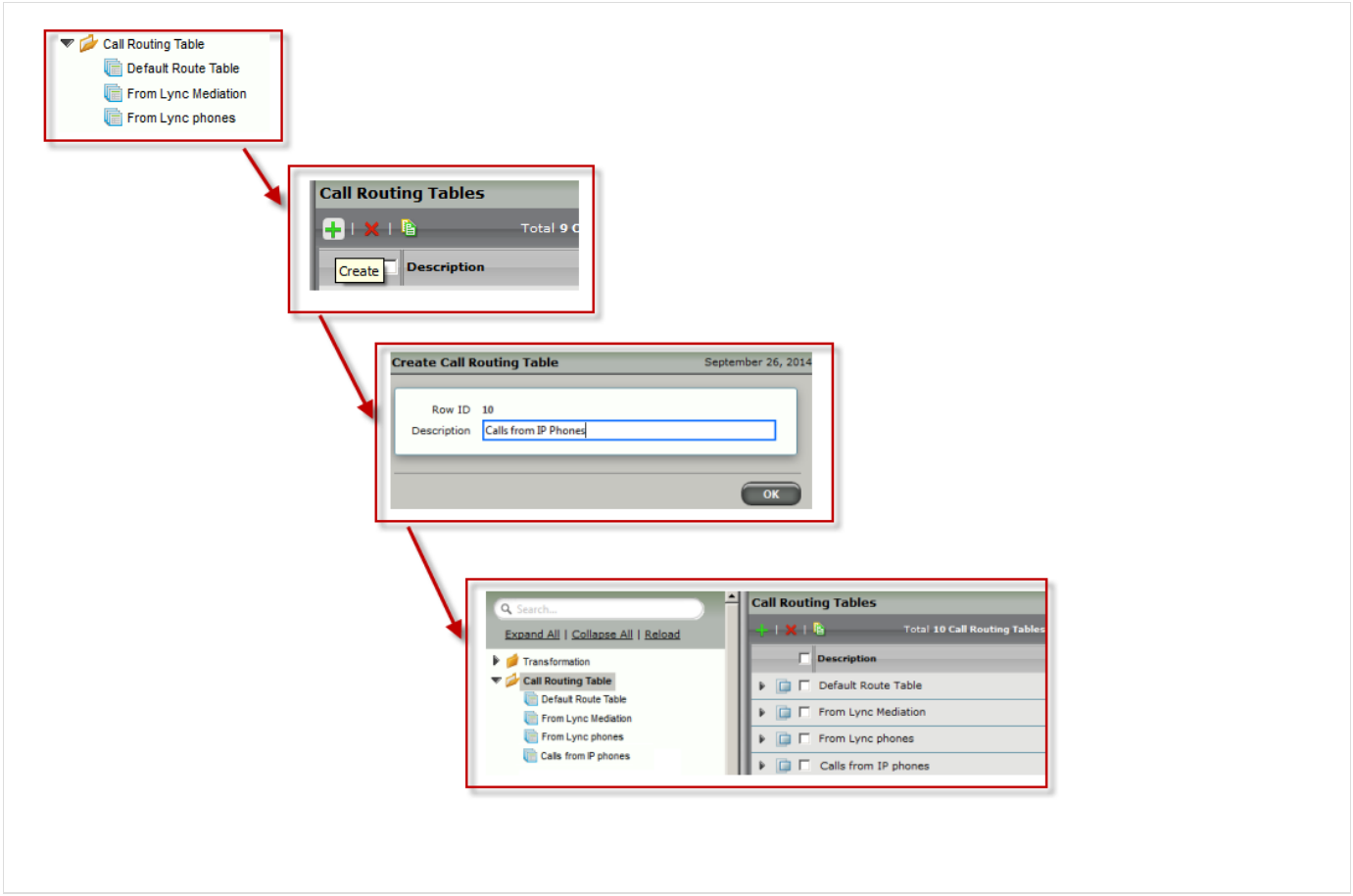


Add a Call Routing Table

To add a Call Routing Table:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table**.
3. Click the **Create** (+) icon.
4. Enter a desired name in the **Description** field.
5. Click **OK**.

Copyright © 2015 Sonus Networks. All rights reserved.

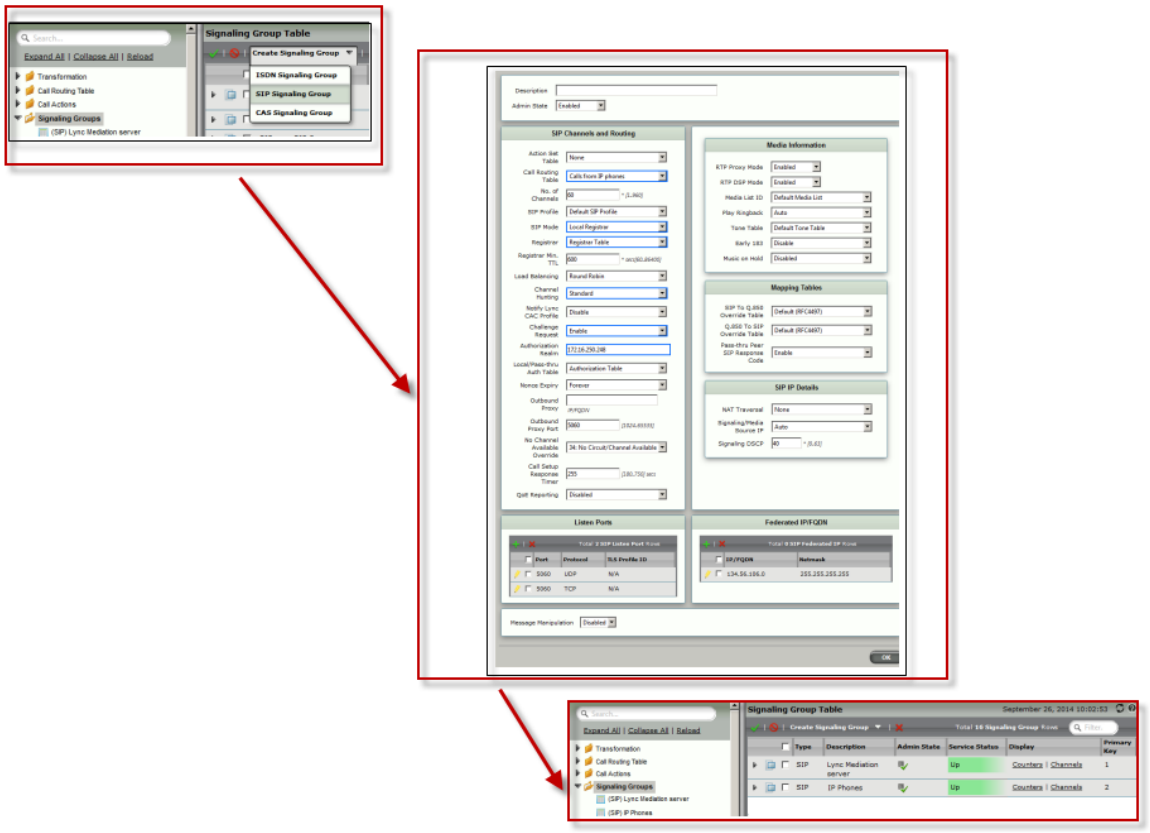


Add and Configure a SIP Signaling Group

To add and configure a Signaling Group:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click **Create Signaling Group** and select **SIP Signaling Group**.
4. Configure the Signaling Group as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



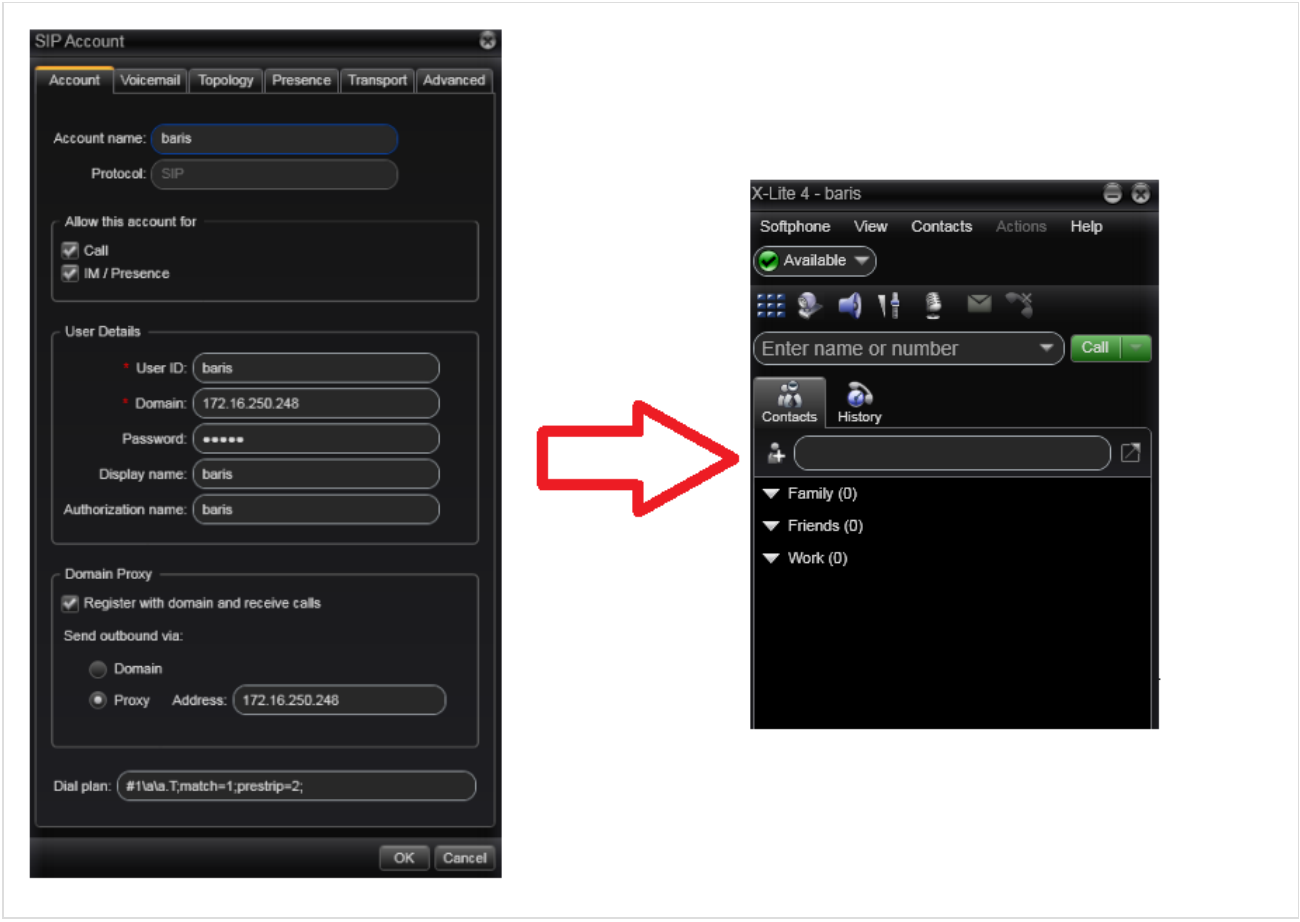
Endpoint Registration

Endpoint Configuration

To configure the endpoint:

1. Configure the endpoint with the user's credentials and Sonus SBC 1000/2000's IP address.
2. Click **OK**to register it with Sonus SBC 1000/2000 as shown below.

Copyright © 2015 Sonus Networks. All rights reserved.



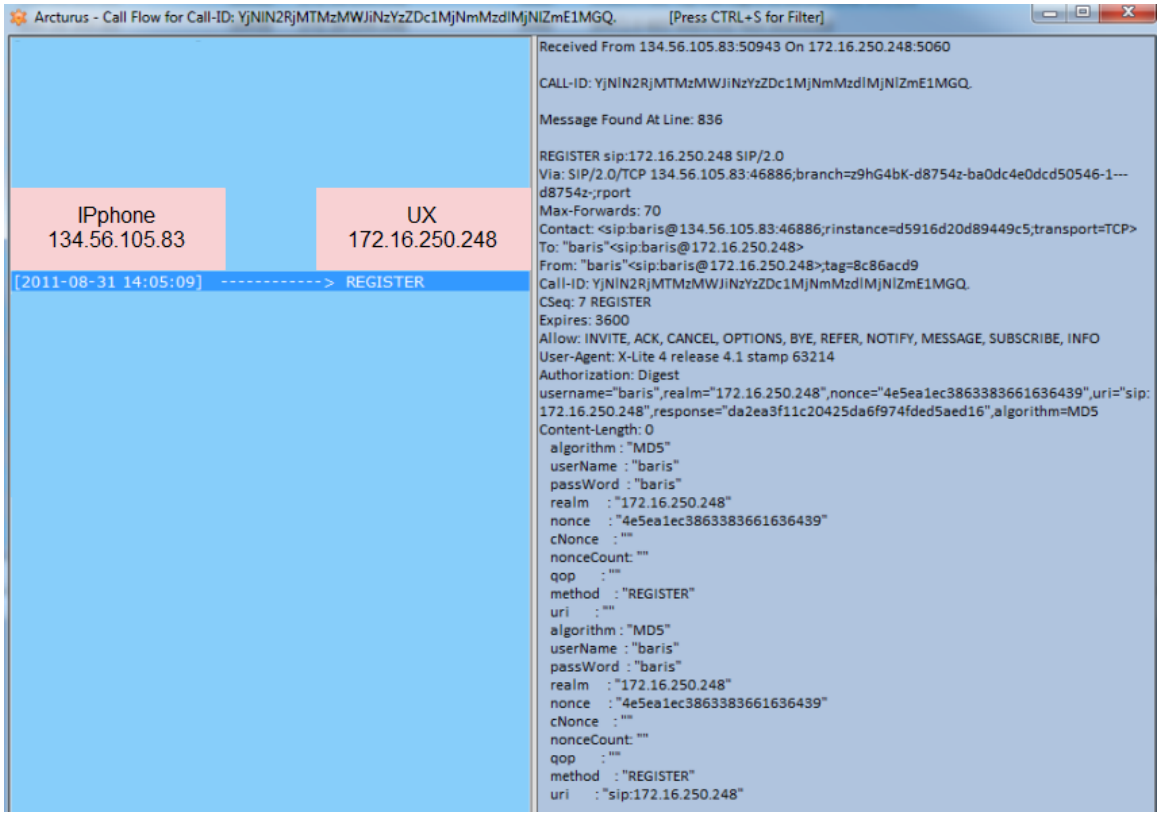
Registration Verification

When the endpoint registers, the registration request comes to the node through the SIP Signaling Group and Sonus SBC 1000/2000 responds to the REGISTRATION request with a 200 OK message.

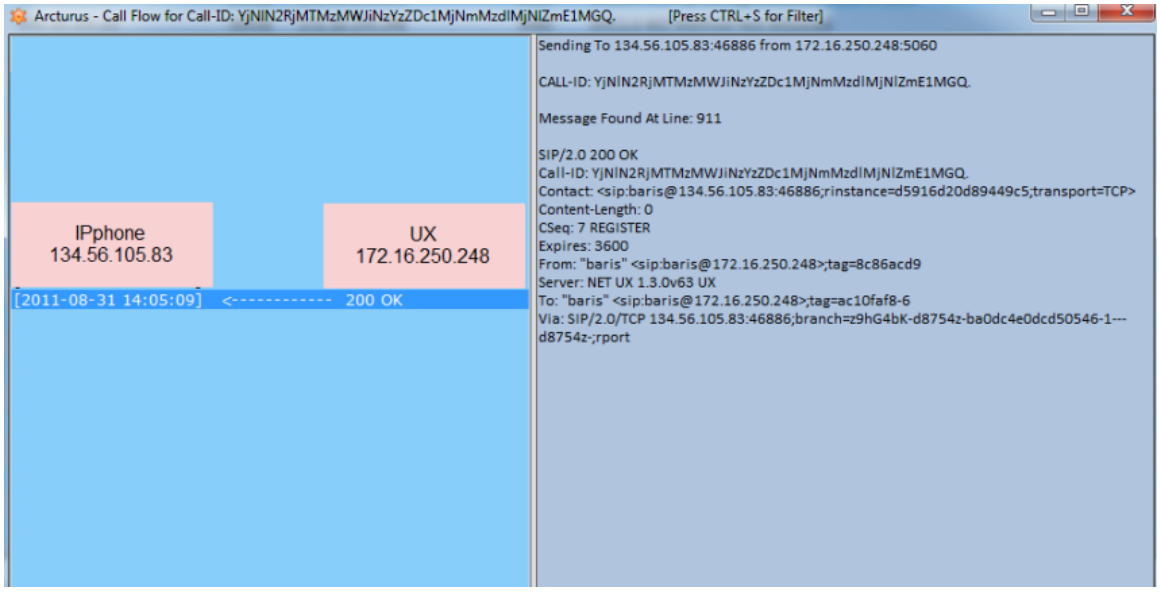
Using the **Log Exchange** utility, you can easily verify the relevant SIP messaging for a successful SIP endpoint registration:

Register Message

Copyright © 2015 Sonus Networks. All rights reserved.

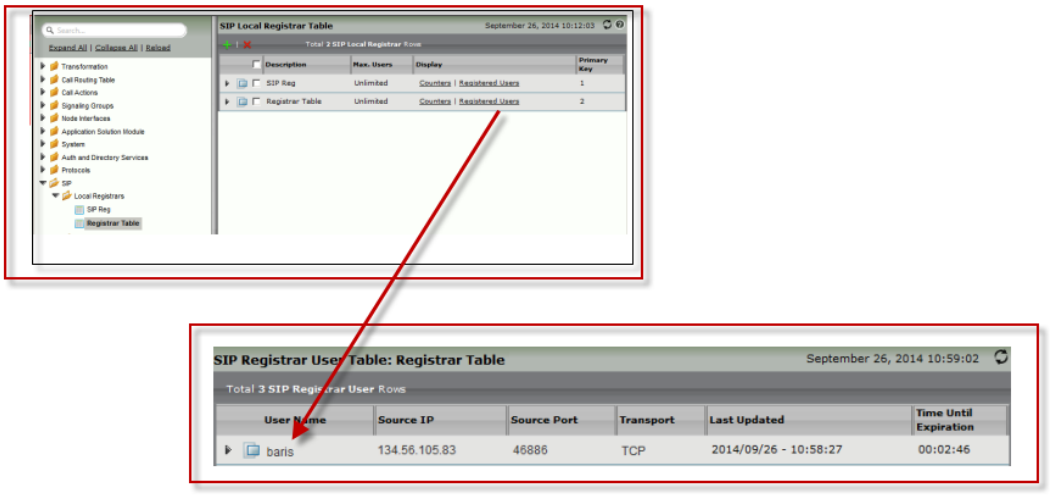


200 OK Message



Upon successful registration, the Sonus SBC 1000/2000 **Registrar Table** also displays the endpoint as a **Registered User** as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



Deploying the Sonus SBC 1000-2000

This set of best practice articles describe how to deploy the SBC 1000/2000 in various network topologies.

Upstream Deployment of a Sonus SBC 1000-2000 in a PSTN - SBC - eUM Toplogy

Using Tenor as an Analog Device in a Lync SBC SBA Deployment

- Configuring Valcom For Use With Tenor

Deploying the Sonus SBC 1000-2000 with OCS2007 R2 using the ASM as a Mediation Server

Upstream Deployment of a Sonus SBC 1000-2000 in a PSTN - SBC - eUM Toplogy

This article describes the process of configuring a Sonus SBC 1000/2000 to be deployed Upstream in a PSTN - Sonus SBC 1000/2000 - Microsoft Exchange 2007/2010 Unified Messaging Server environment. In this example the Sonus SBC 1000/2000 serves as a gateway between the PBX, Exchange Unified Messaging Server, and the PSTN; none of which are directly connected to the other:

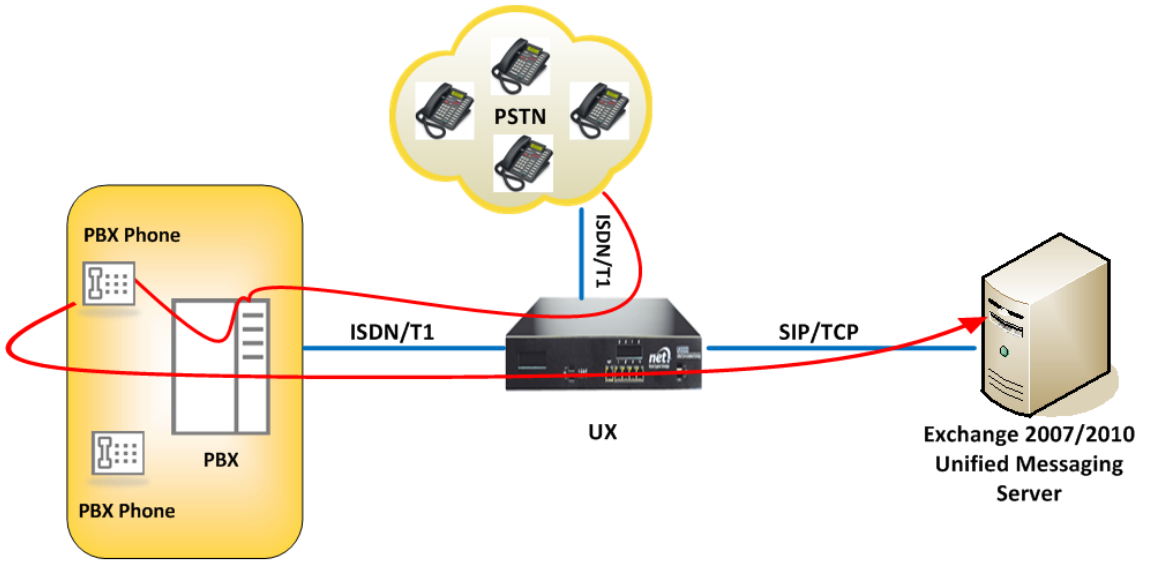
- Before You Begin
- Configuration Overview
- Configuring the Sonus SBC 1000/2000
  - SIP Server Table
  - Transformation Table
  - Call Routing Table
  - Port Configuration
  - Signaling Groups

Copyright © 2015 Sonus Networks. All rights reserved.

- System Timing Configuration
- Sonus SBC 1000/2000 Signaling Group Status Verification

The diagram below illustrates the topology and a typical call scenario:

Topology



Endpoints Depicted in this configuration are:

PBX phones: 622x numbers.
PSTN phones: 5xxx numbers.
eUMS Subscriber Access number: 6255
eUMS Auto Attendant number: 6256

The RED arrow in above diagram indicates the following scenario:

1) PBX Phone-I- receives a call from a PSTN phone.
2) PBX Phone-I- does not answer the call.
3) Call gets diverted to the Subscriber Access number with PBX Phone-I-'s number in the DIVERSION header in SIP INVITE message.
4) eUMS places the call in PBX Phone-I-'s Voice Mail box.
5) Calling Party leaves a voice mail for PBX Phone-I-.

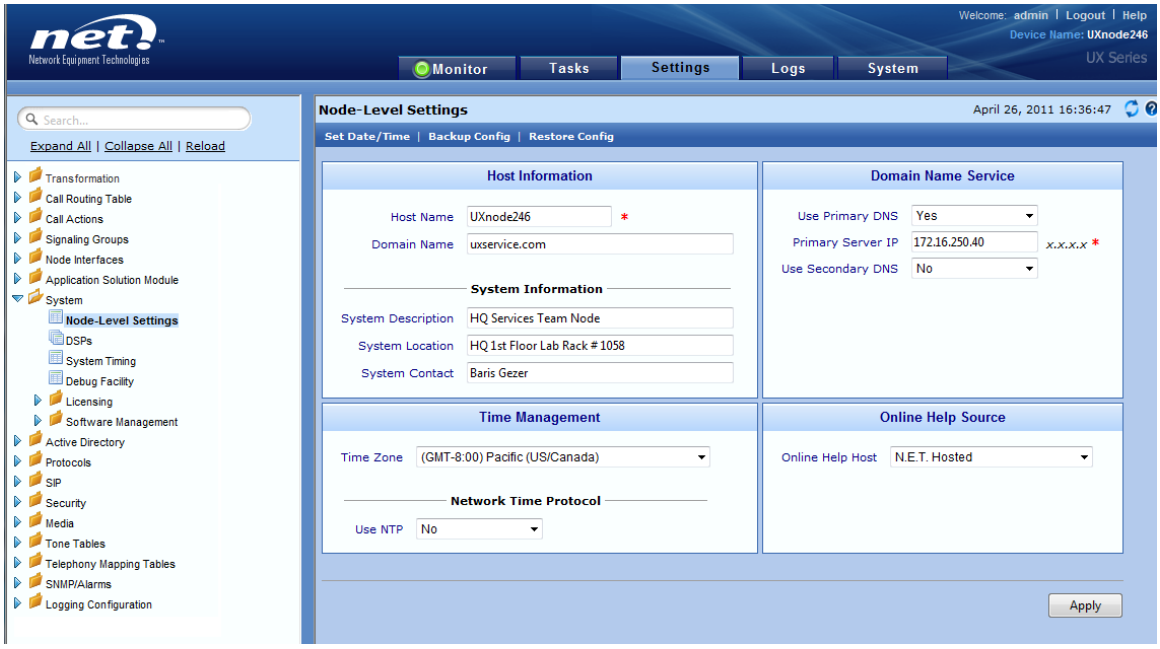
Furthermore, calls to/from SA/AA numbers, Fax calls, MWI are the additional supported call scenarios in this deployment.

Before You Begin

Launch the WebUI and verify the node level settings:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > Node Level Settings**
3. Verify that all the fields have been populated as indicated in the image below.
   ⚠️ Use the IP address from **YOUR** Primary Domain Server, not the sample IP address in the image.

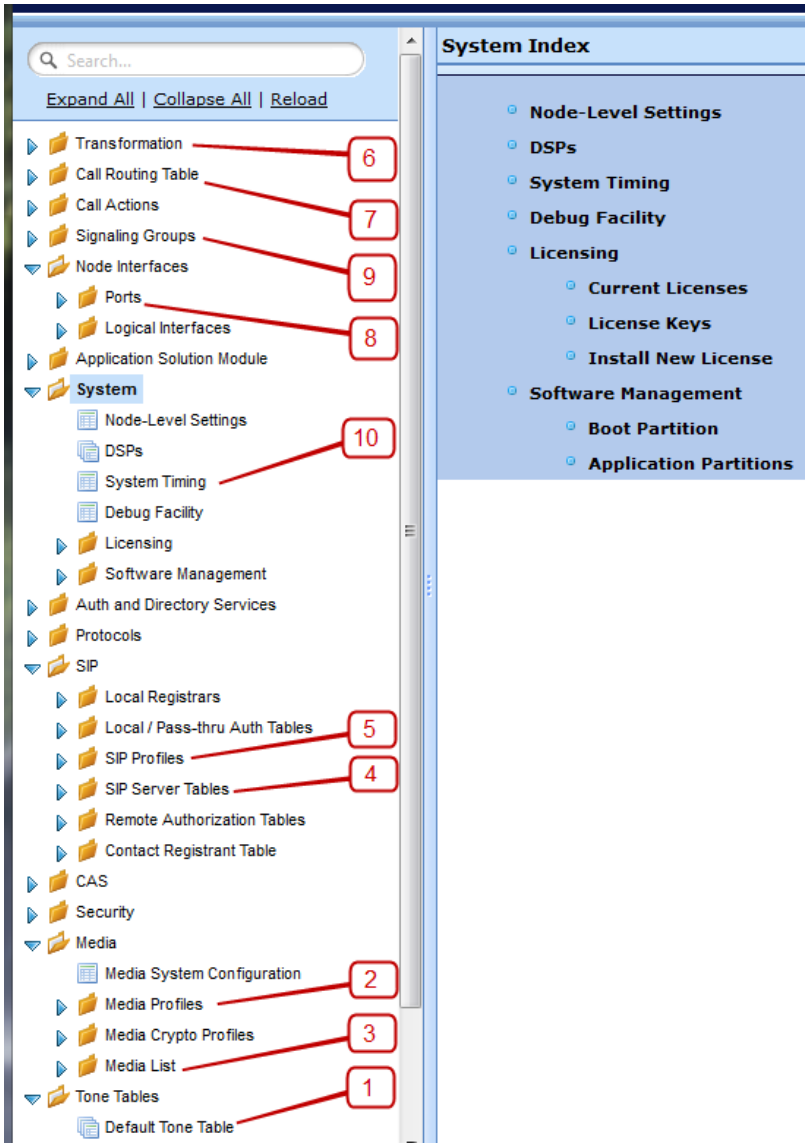
Copyright © 2015 Sonus Networks. All rights reserved.



Configuration Overview

The Sonus SBC 1000/2000 integration with the MS Exchange 2007/2010 Unified Messaging Server requires specific configuration steps to be completed using the WebUI to allow it to function properly in the topology described above.

Copyright © 2015 Sonus Networks. All rights reserved.



1. **Default Tone Table**: A factory default Sonus SBC 1000/2000 configuration contains the "Default Tone Tabl entry. This article's configuration requires it, ensure its presence in your configuration.
2. **Default Media Profile(s)**: the default G.711A/Mu-Law profile is used in this example.
3. **Default Media List**: the Default Media List is used in this example.
4. **Create a SIP Server Table**: In this example we add a SIP Server table entry for the Exchange 2007/2010 Server.
5. **Create a SIP Profile**: you can create a custom SIP Profile or use the default. The default is used in this example.
6. **Create a Transformation Table**: this table is used in the relate Call Routing tables and for Called/Calling Number transformations.
7. **Create a Call Routing Table**: in this example we create two table entries, one for ISDN and another for SIF They are required in the relevant Signaling Groups.
8. **Configure a DS1 Port**: this port is associated with the Physical PRI (T1/E1) connection.
9. **Create two Signaling Groups**: One Signaling Group will be designated for for SIP and the other is for ISDN
10. **Set the System Timing**: you can configure the Clock Source to use the Sonus SBC 1000/2000 system cloc or a network source, depending on your PBX.

Configuring the Sonus SBC 1000/2000

Copyright © 2015 Sonus Networks. All rights reserved.

SIP Server Table

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Server Tables**.
3. Create a new *IP Server Table.
   The SIP Server Tables page is a table of SIP Server Tables.
4. Configure the new SIP Server Tableas shown in the illustration below.



Transformation Table

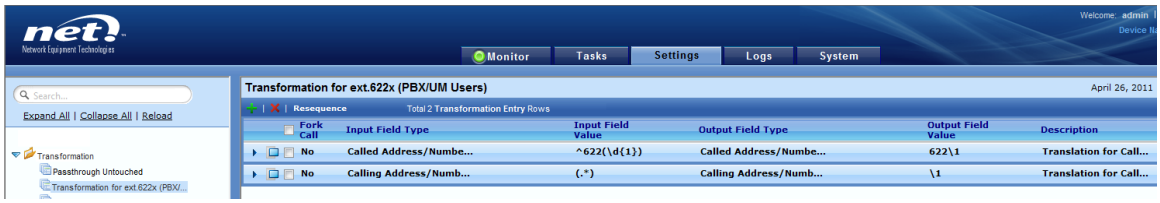
1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Transformation**
3. Add a new Transformation Table.
   The Transformation Table page is a table of Transformation Tables.
4. In the left navigation pane, click the Transformation table created in the previous step.



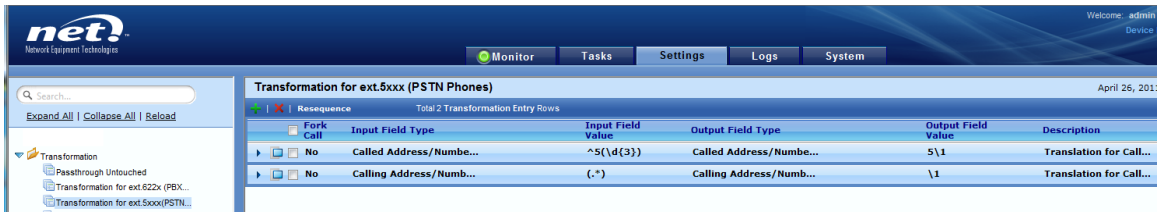
5. Add Calling / Called Party Number transformations to each one of these transformation rules as shown below.

Transformation Rule to reach PBX Endpoints

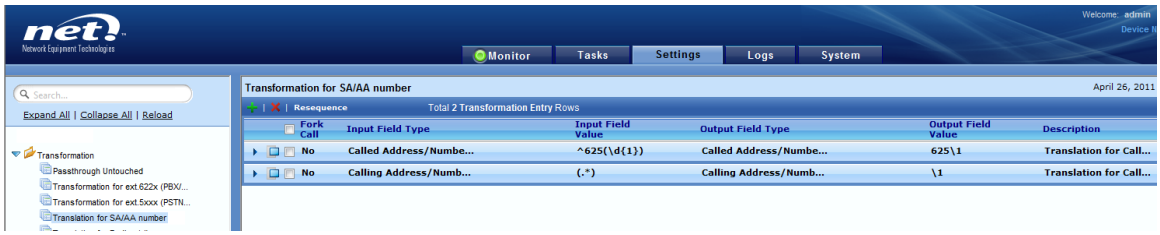
Copyright © 2015 Sonus Networks. All rights reserved.



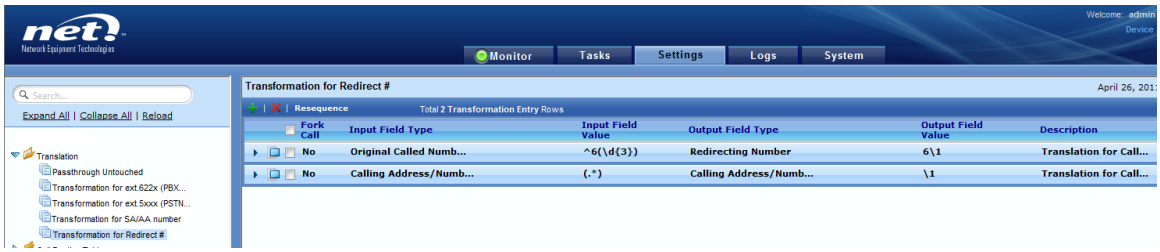
Transformation Rule to reach PSTN Phones



Transformation Rule to reach SA/AA numbers



Transformation Rule to reach called party's voicemail (VM) box



Call Routing Table

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing Table**.
3. Add an entry to the Call Routing Table. Name it ***Calls from ISDN (PBX)***.
4. Create two more entries. Name them ***Calls from Exch*** and ***Calls From PSTN***.
   In this deployment, three call route table entries are required for the relevant Signaling Groups.

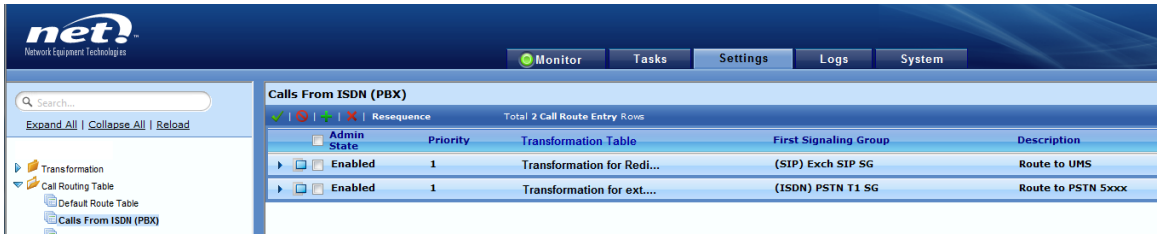
Copyright © 2015 Sonus Networks. All rights reserved.



Route Table for Calls from PBX phones

This table requires two entries:

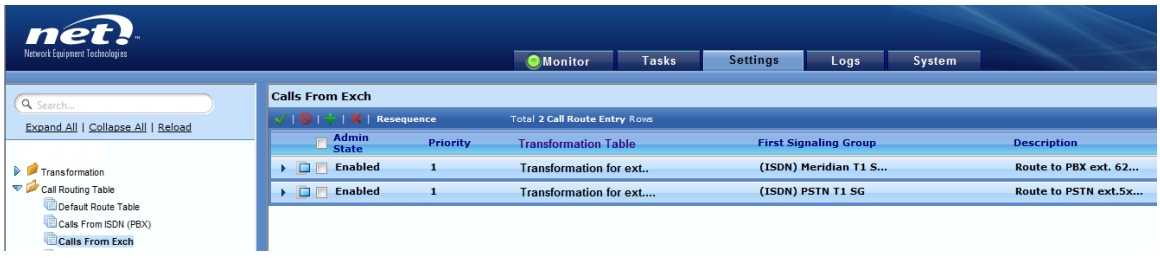
- One for routing calls to Redirected party's VM boxes in Exchange 20xx Unified Messaging Server (eUMS).
- Another one for routing the calls to 5xxx PSTN phones.



Route Table for Calls from Exchange Server

This table requires two entries:

- One for routing calls to 622x PBX phones via eUMS Auto Attendant or Subscriber Access prompts.
- Another one for routing calls to 5xxx PSTN phones via eUMS Auto Attendant or Subscriber Access prompts.



Route Table for Calls from PSTN phones

This table requires two entries:

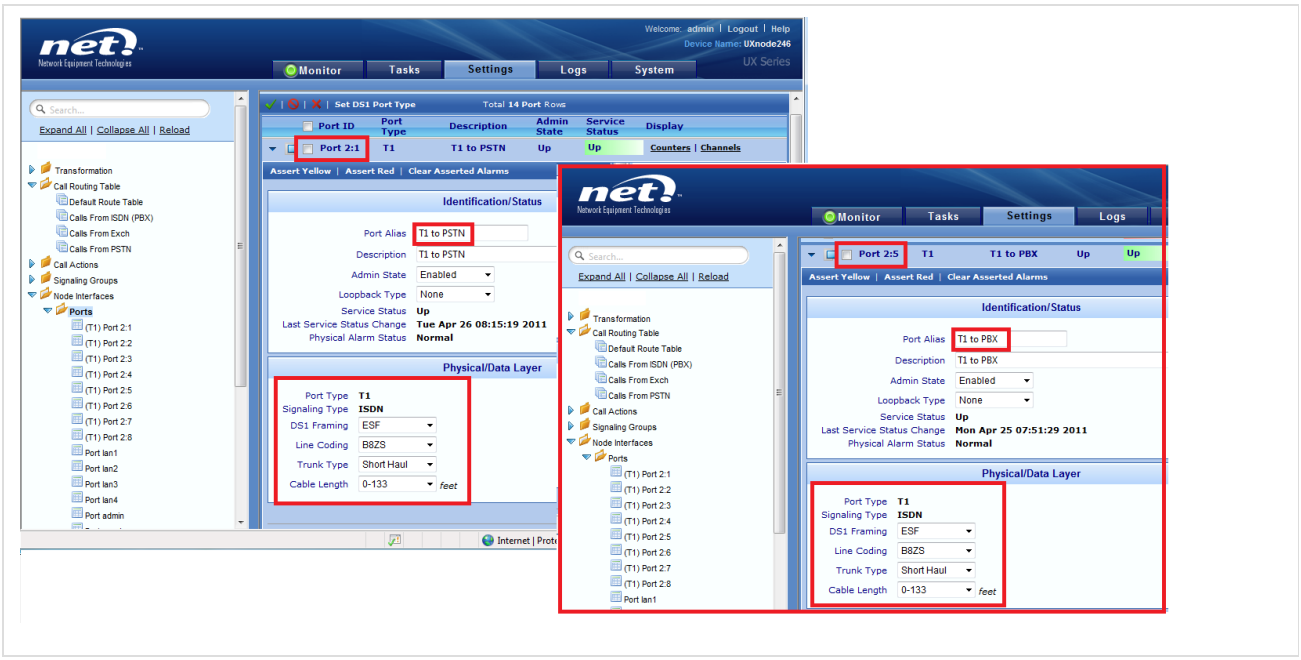
- One for routing calls to 622x PBX phones.
- Another one for routing calls to 625x eUMS Auto Attendant or Subscriber Access numbers.

Copyright © 2015 Sonus Networks. All rights reserved.



Port Configuration

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Node Interfaces > Ports**
3. Click the **expand** (▶) icon in the table next to the port used to connect the physical PRI line.
4. Complete the fields as shown below.
   ⚠Note that you will have to configure two Ports here, one for T1 connection to PBX, and another for T1 connection to PSTN, which will eventually be used in the relevant ISDN Signaling Groups

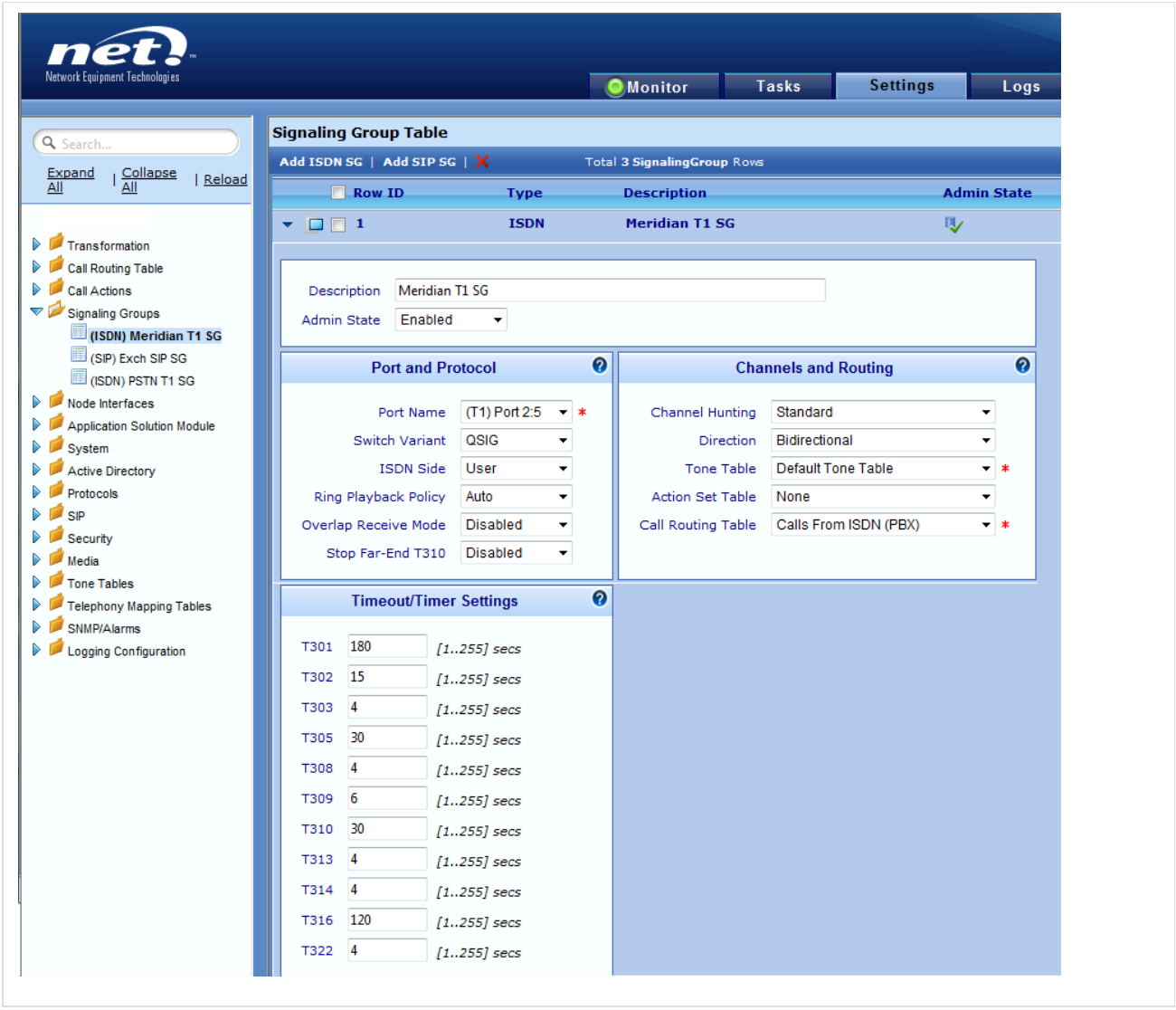


Signaling Groups

ISDN Signaling Group for PBX Connection

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click the **Add ISDN SG** text at the top of the Signaling Group Table.
4. Populate the fields as shown below.
5. Click **OK**.

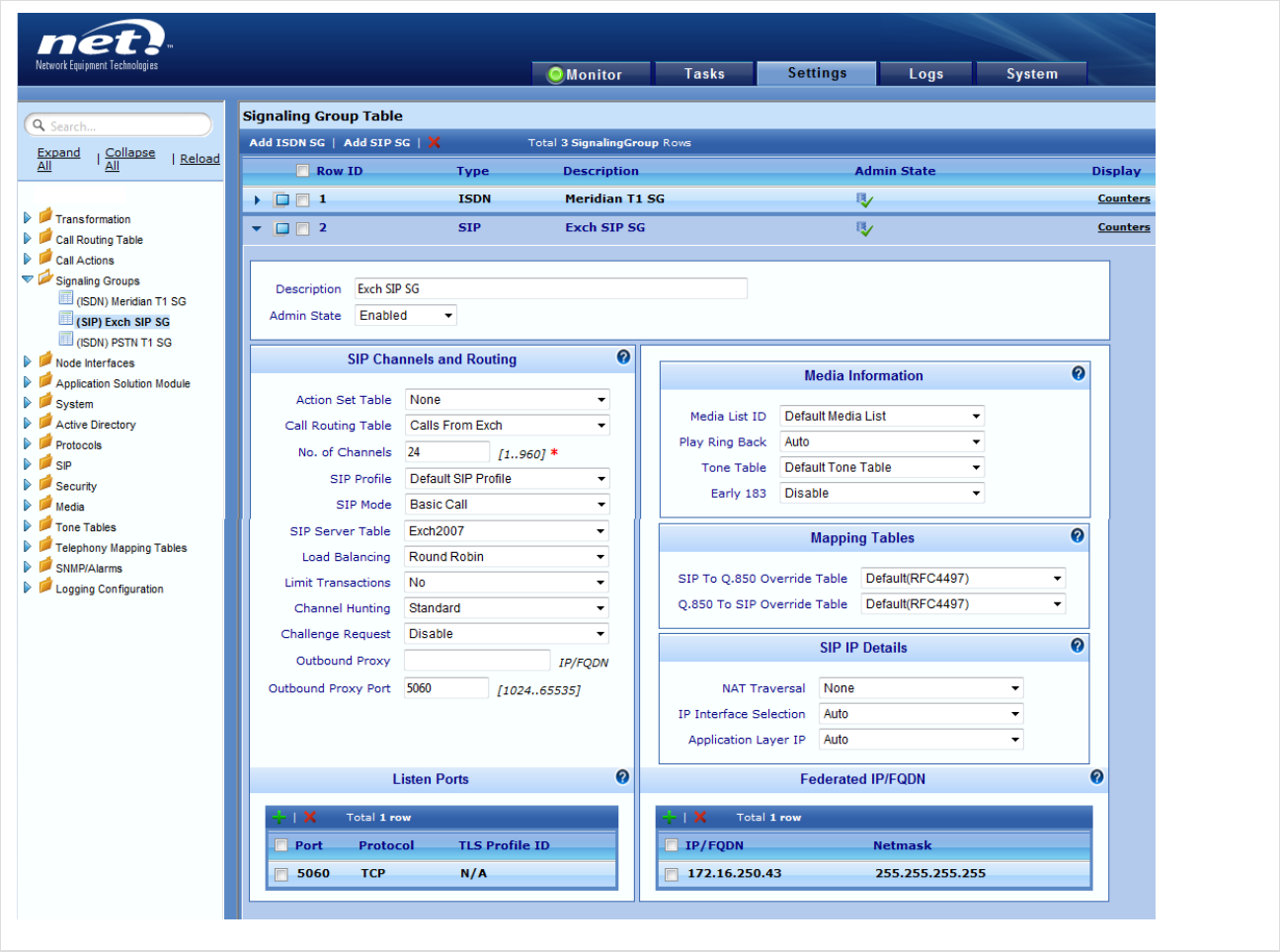
Copyright © 2015 Sonus Networks. All rights reserved.



SIP Signaling Group for Exchange 20xx Unified Messaging Server Connection

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click the **Add SIP SG** text at the top of the Signaling Group Table.
4. Populate the fields as shown below.
5. Click **OK**.

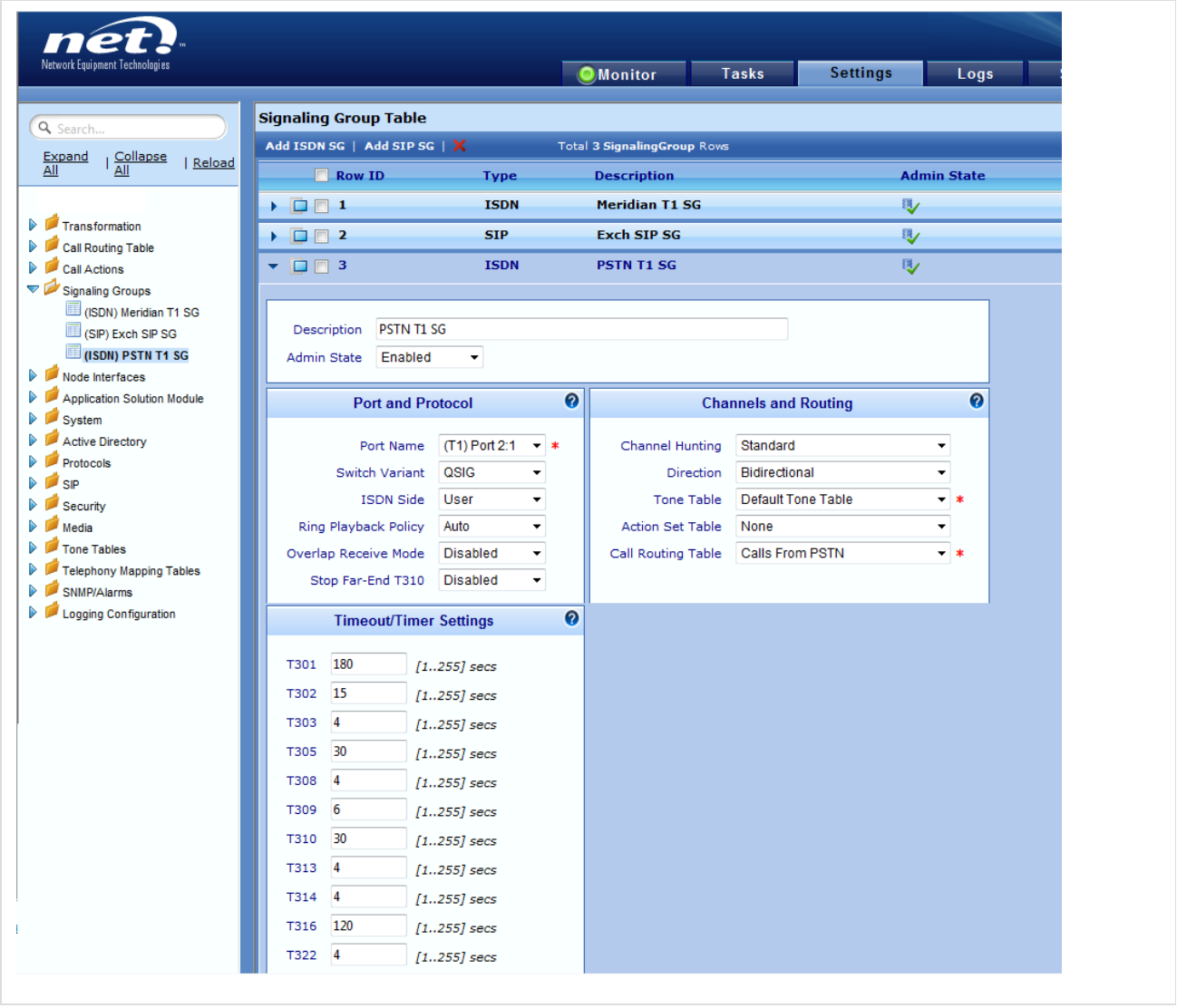
Copyright © 2015 Sonus Networks. All rights reserved.



ISDN Signaling Group for PSTN Connection

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click the **Add ISDN SG** text at the top of the Signaling Group Table.
4. Populate the fields as shown below.
5. Click **OK**

Copyright © 2015 Sonus Networks. All rights reserved.



6. At this point, the Signaling Groups should appear like so:

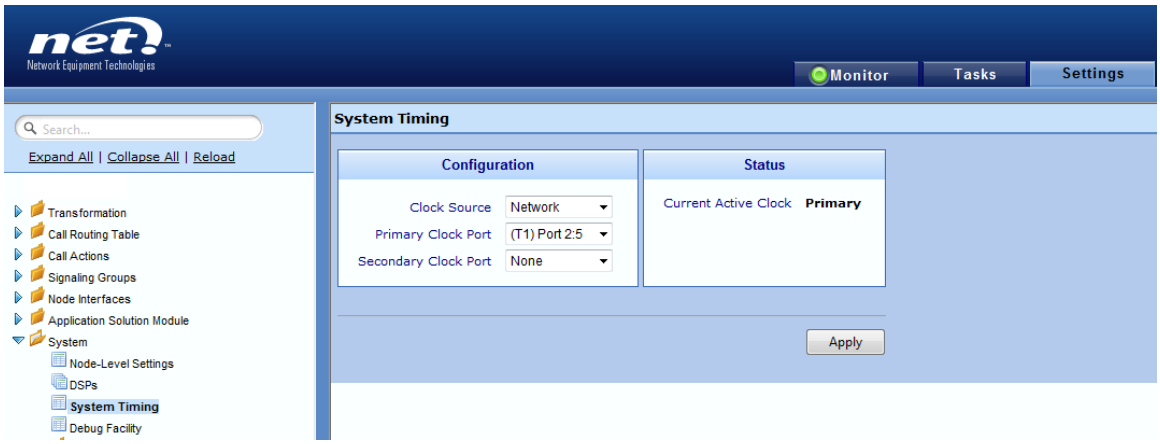


System Timing Configuration

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **System > System Timing**.
3. Configure the Clock Source either as System or the Network, depending on your PBX timing settings.
   In this exercise, the Sonus SBC 1000/2000 node is reading the system time from the network therefore

Copyright © 2015 Sonus Networks. All rights reserved.

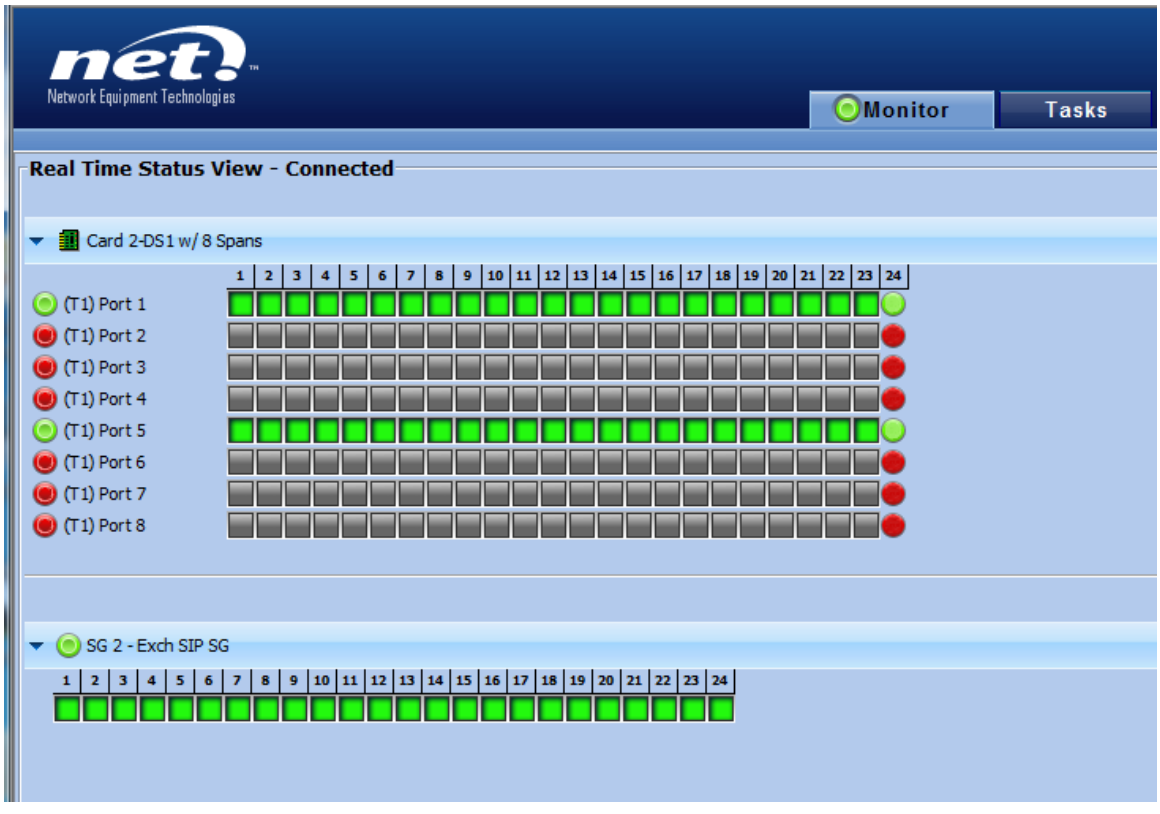
the configuration is done as shown below:
For more information about system timing see, Configuring the System Clock Source



Sonus SBC 1000/2000 Signaling Group Status Verification

After having completed the configuration steps above, and the relevant configuration on Exchange 20xx Unified Messaging Server, verify the signaling group status:

1. In the WebUI, click the **Monitor** tab.
2. Verify that all three Ports come up as shown below:



Using Tenor as an Analog Device in a Lync SBC SBA Deployment

Copyright © 2015 Sonus Networks. All rights reserved.

The Tenor can be used to provide FXS analog capability to the Sonus SBC 2000, allowing for FAX connectivity. In this article, we describe the steps necessary to deploy a Tenor as an analog device in a **Sonus SBC 1000/2000 - Lync SBA** topology. The overall configuration comprises three components: the Lync Server, the Tenor, and the Sonus SBC 1000/2000:

- Before You Begin
- Lync Configuration
  - Creating analog End Point using the New-CsAnalogDevice Command
  - Explanation of New-CsAnalogDevice
- Tenor configuration
  - Requirements for Tenor
  - Run the Tenor Wizard
  - Additional Post-wizard Settings and Configuration Verrification
  - Sample Tenor AF Configuration File
- Sonus SBC 1000/2000 configuration
  - Requirements and Prerequisites
  - SIP Registrar Table
  - Media List Configuration
  - Translation Table
  - Signaling Group (uses UDP only)
  - Call Routing Table
- Troubleshooting Techniques
  - Troubleshooting FAX Calls Between the Tenor and PSTN

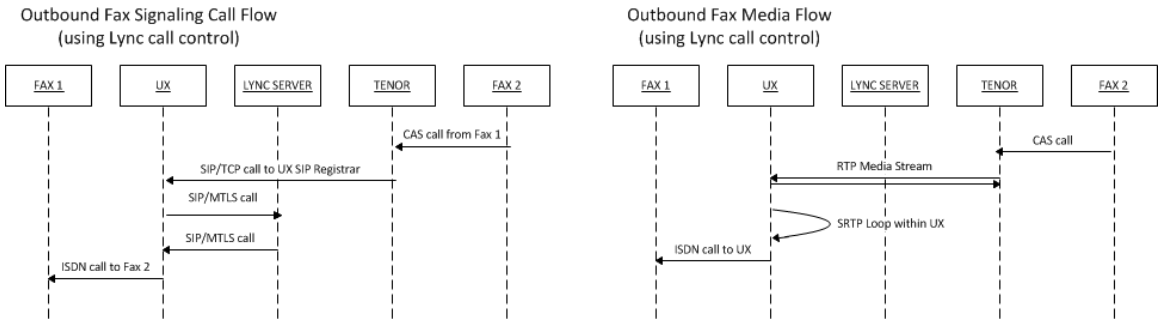
Notes:

In this article, G.711 voice codec is used and CNG Tone Detection is disabled:

When CNG detection is disabled, the Sonus SBC 1000/2000 lets the Calling fax machine on either side, ISDN or SIP, to send CNG. However, the Sonus SBC 1000/2000 is *actively listening* for and detecting the Fax **Answer message** that the Answerin fax machine sends because Fax pass-thru is enabled.

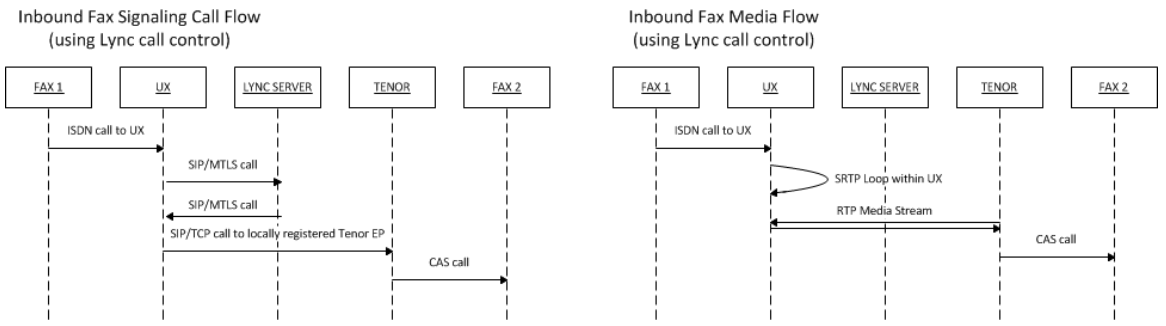
The following diagrams depict the signaling and media flow of the Analog End Point of LYNC in this deployment.

Outbound Fax call flow using Lync call control (signaling and media)



Inbound Fax call flow using Lync call control (signaling and media)

Copyright © 2015 Sonus Networks. All rights reserved.



Related Information

In this deployment, following LYNC topology entities, PBX, and numbering plans are used:

FQDN	IP Address	Description
uxdemo.net	134.56.105.30	LYNC SBA Domain
rdc.uxdemo.net	134.56.105.30	DNS/AD/Ent. Root CA
sba247.uxdemo.net	134.56.105.247	FQDN of Lync SBA Pool
ux246.uxdemo.net	134.56.105.246	FQDN of the Sonus SBC 2000 GW
Tenor AF	134.56.105.41	Analog Device
Nortel Meridian	N/A	ISDN PBX

LYNC SBA Users	Line URI
sip:SBAuser1@uxdemo.net	tel:+15102461001
sip:SBAuser2@uxdemo.net	tel:+15102461002

LYNC SBA ANALOG Users	Line URI

Copyright © 2015 Sonus Networks. All rights reserved.

sip:ae11467d-d09d-4e78-ad2a-e4615b79ac57@Sonus SBC 1000/2000DEMO.Sonus (ANALOGph1)	tel:+15102462001
sip:80274280-9a22-43d9-b194-2640904c3e54@Sonus SBC 1000/2000DEMO.Sonus (ANALOGph2)	tel:+15102462002
sip:3f1e38d7-c8a3-425a-818c-bae3f2c28d62@Sonus SBC 1000/2000DEMO.Sonus (Fax1)	tel:+15102462003

Meridian Endpoints	Extensions
PBX Ph1	ext: 6228
PBX Ph2	ext: 6222

Before You Begin

The Sonus SBC 1000/2000 SBA must already be configured. If not, configure and deploy the Lync SBA following the instructions in Deploying the Survivable Branch Appliance.

Lync Configuration

Creating analog End Point using the New-CsAnalogDevice Command

Analog Endpoints must be created from the Lync Management Shell using the New-CsAnalogDevice cmdlet.

1. On the Lync Server, go to **Start > Microsoft Lync Server 2010 > Lync Server Management Shell**. Enter the command as shown below.

For Aanalog Phone Endpoints:

```
New-CsAnalogDevice \-LineUri tel:+15102462001 \-DisplayName "Analogph1"
\-RegistrarPool cspool.uxdemo.net \-AnalogFax $false \-Gateway ux246.uxdemo.net \-OU
"ou=Analog,dc=uxdemo,dc=net"
```

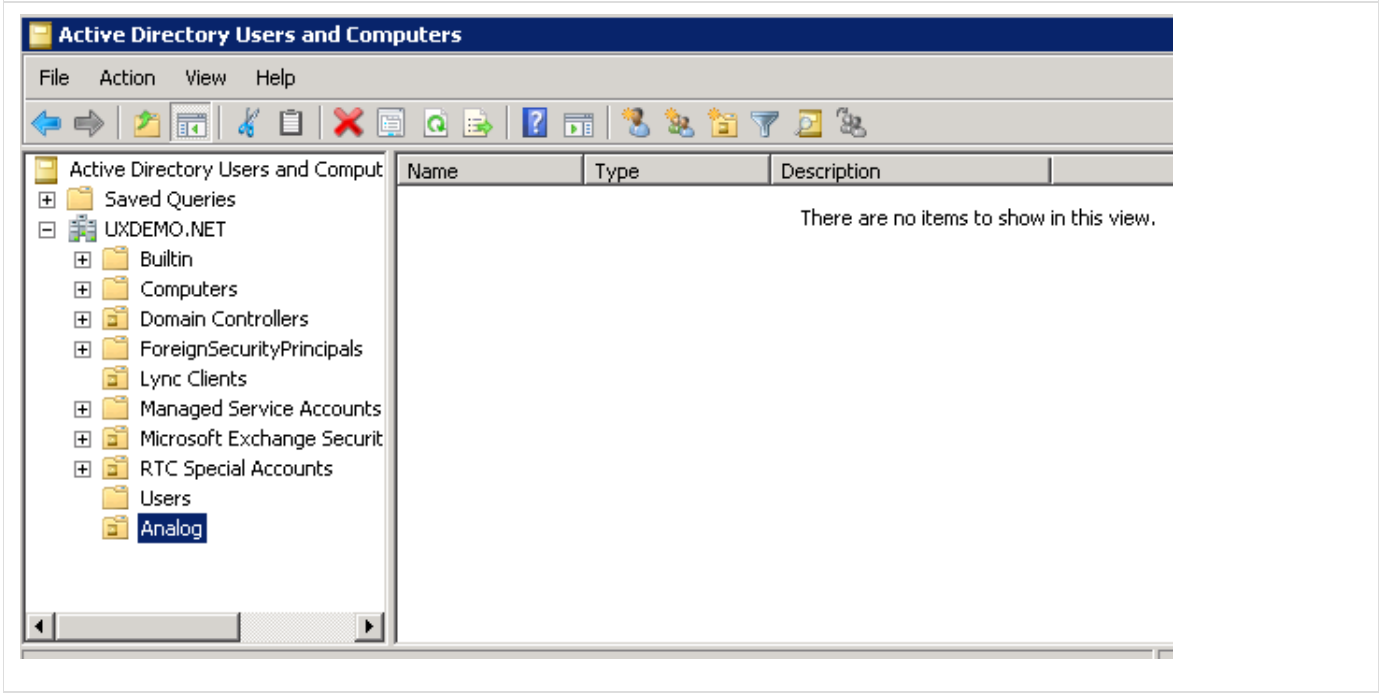
For Analog FAX Endpoints:

```
New-CsAnalogDevice \-LineUri tel:+15102462003 \-DisplayName "Fax1" \-RegistrarPool
cspool.uxdemo.net \-AnalogFax $true \-Gateway ux246.uxdemo.net \-OU
"ou=Analog,dc=uxdemo,dc=net"
```

⚠ Before running the commands above, make sure that the relevant Organizational Unit(OU) (in this example it is named **Analog**) exists in Active Directory. On a machine that can access the Active Directory Users and Computers snap-in, launch the Active Directory Users and Computers snap-in and verify that OU is present as shown in below

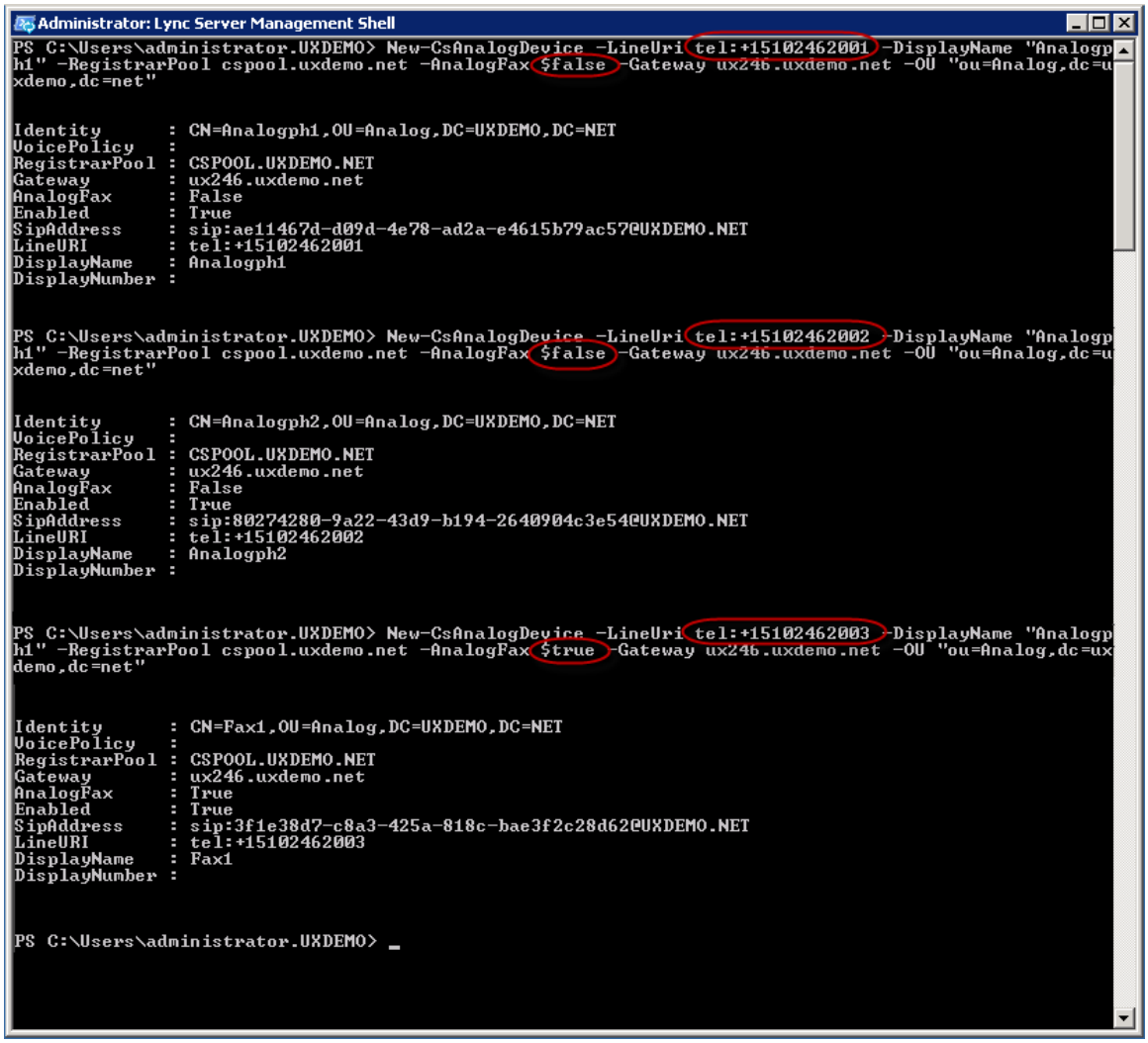
Copyright © 2015 Sonus Networks. All rights reserved.

screenshot:



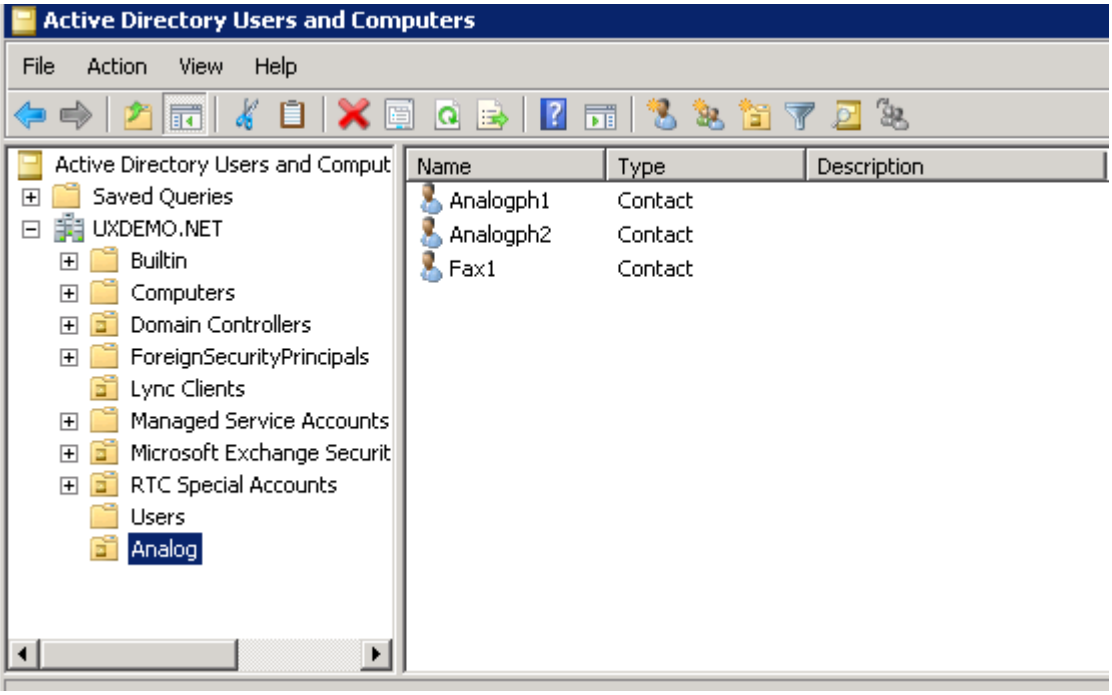
- Launch the **Lync Management Shell** and run the relevant commands to create both Analog Phone and Analog Fax Endpoints as shown in below screenshot:

Copyright © 2015 Sonus Networks. All rights reserved.



- Verify in Active Directory Users and Computers snap-in that relevant users are created successfully in **Analog** Organizational Unit as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



Explanation of New-CsAnalogDevice

The New-CsAnalogDevice cmdlet instructs Lync to route calls from the analog device to the gateway specified in the -Gateway switch of the cmdlet; thus, ensuring that Fax calls will safely be transmitted over PSTN.

Tenor configuration

Requirements for Tenor

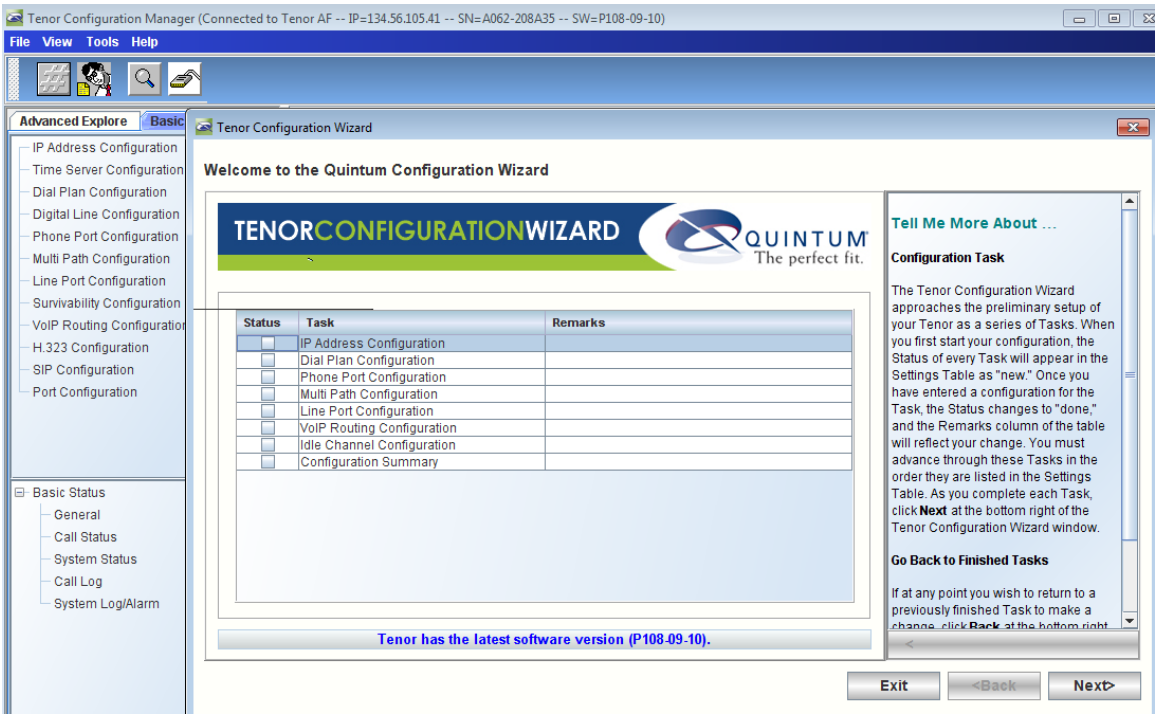
These instructions assume that:

- The Tenor gateway is running **P108-09-10** or newer software release.
- The Tenor Configuration Manager is **CM108-19-00** or newer.

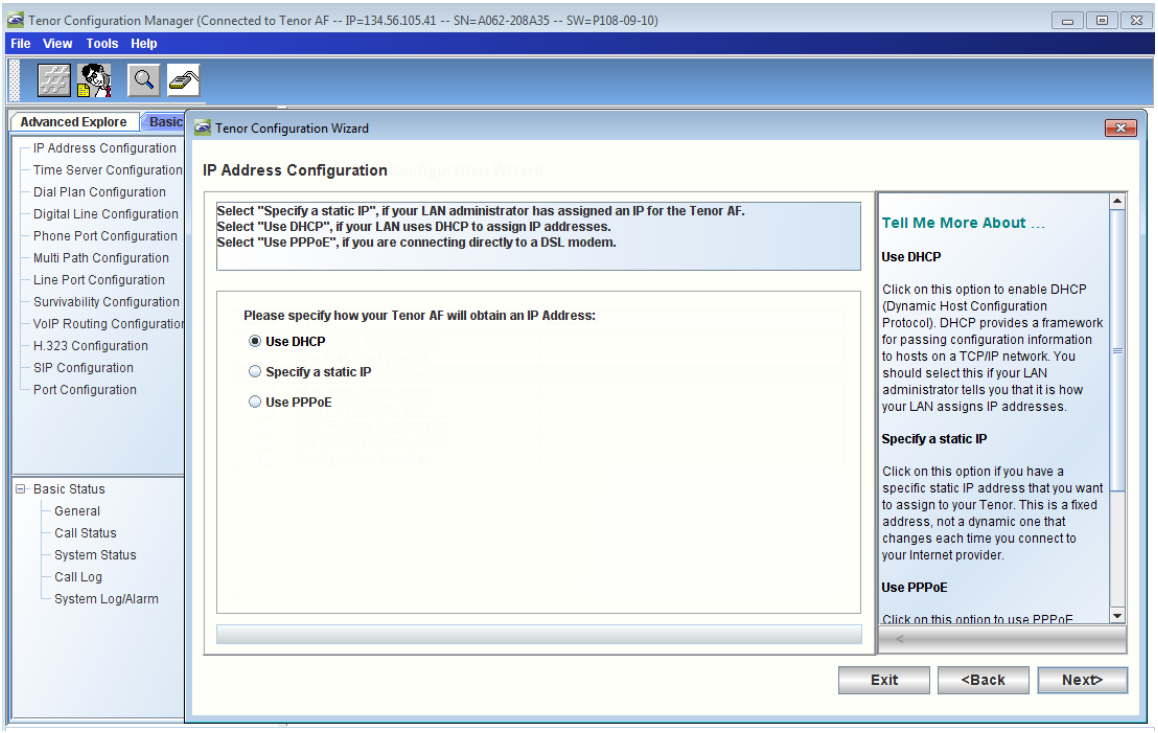
Run the Tenor Wizard

- Launch the Quintum Configuration Manager and connect to your Tenor Device
- Upon connecting to the device, Configuration Wizard will run automatically
- Follow the Wizard Steps and enter the relevant IP addresses, Analog Endpoint numbers..etc. as shown below

Copyright © 2015 Sonus Networks. All rights reserved.

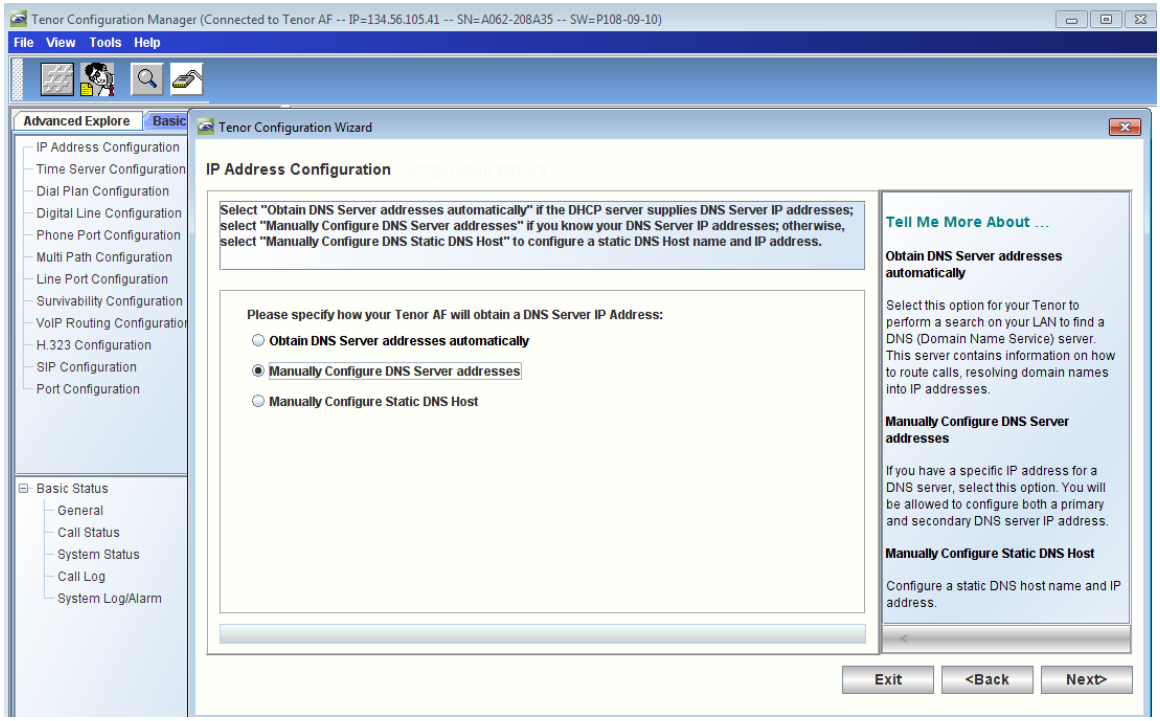


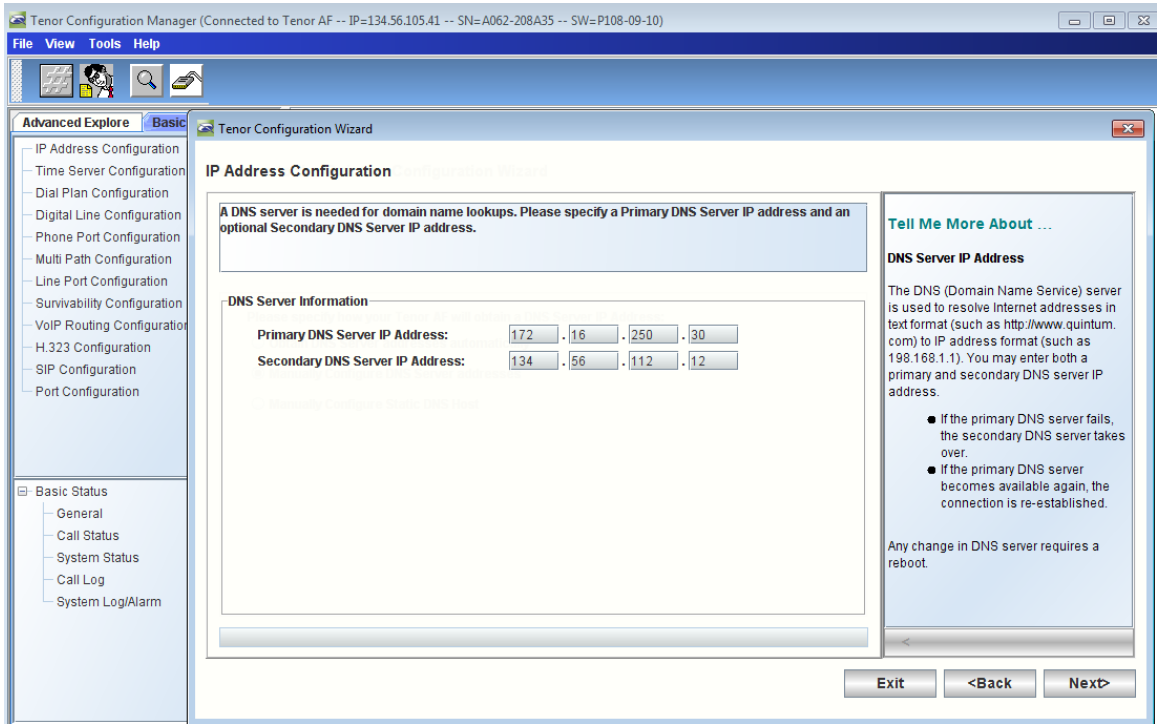
- For this exercise we are using DHCP for the Tenor IP address configuration



- Enter the DNS IP address which is used in LYNC SBA Deployment Topology

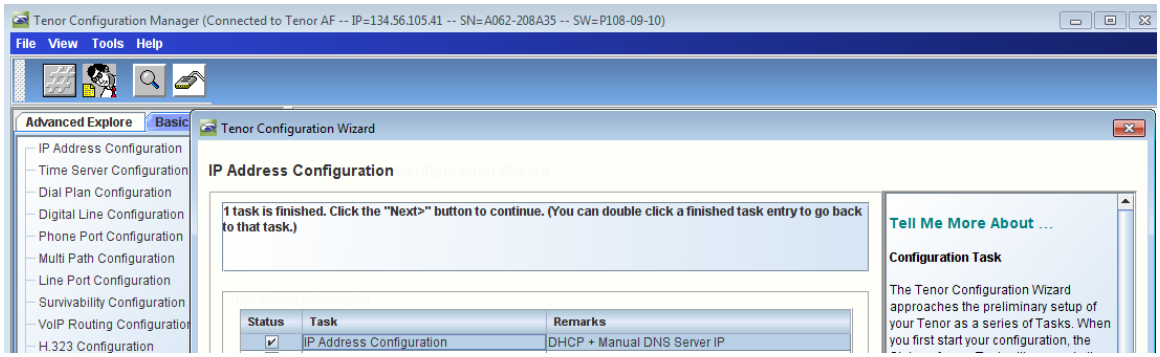
Copyright © 2015 Sonus Networks. All rights reserved.



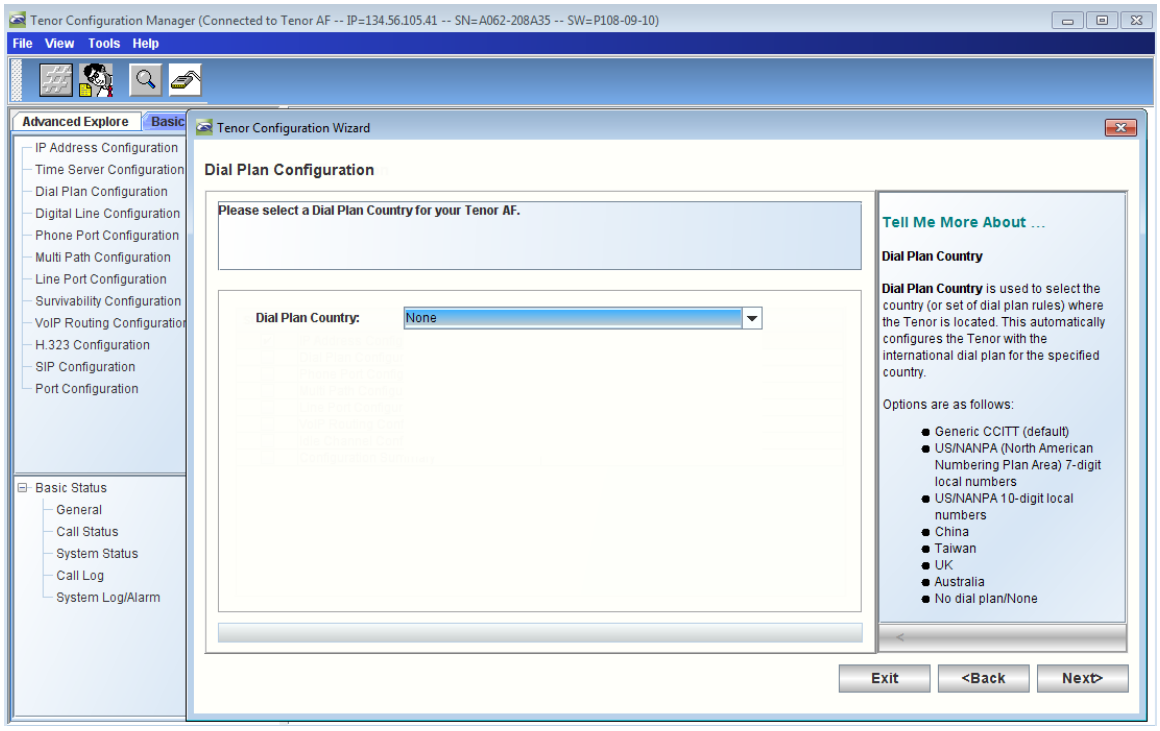


- Verify that IP Address Configuration is completed as shown below

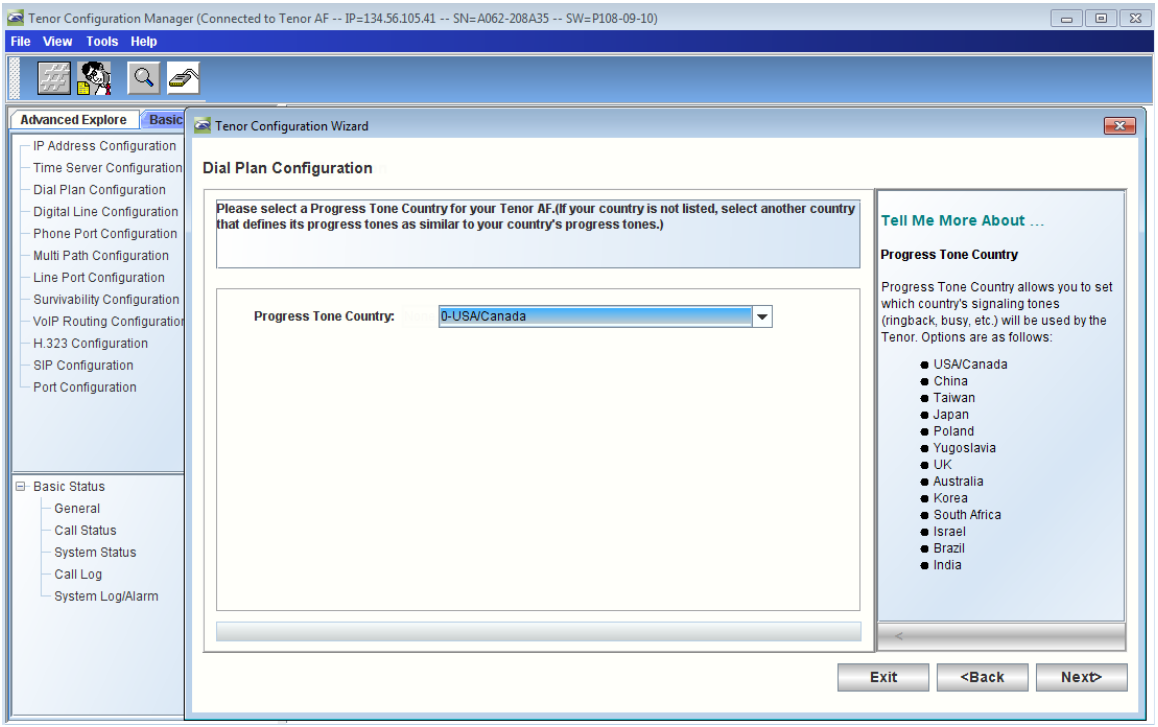
Copyright © 2015 Sonus Networks. All rights reserved.



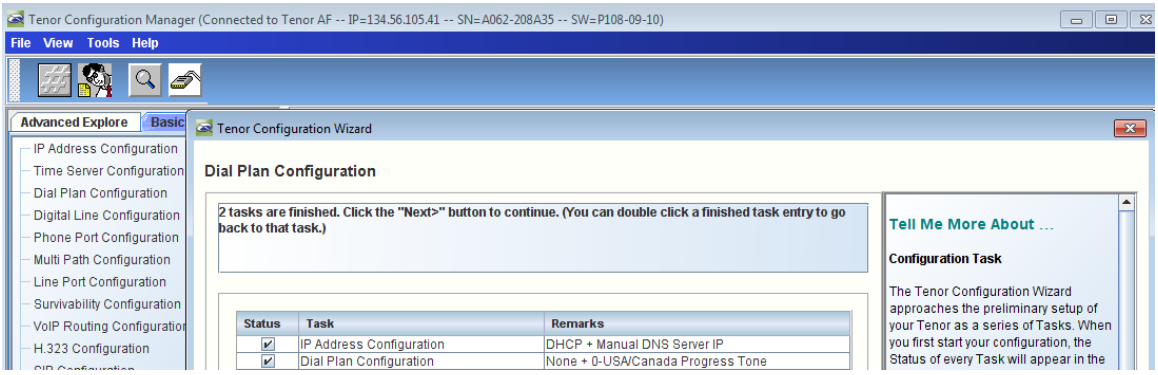
- Continue the wizard steps for Dial Plan Configuration



Copyright © 2015 Sonus Networks. All rights reserved.

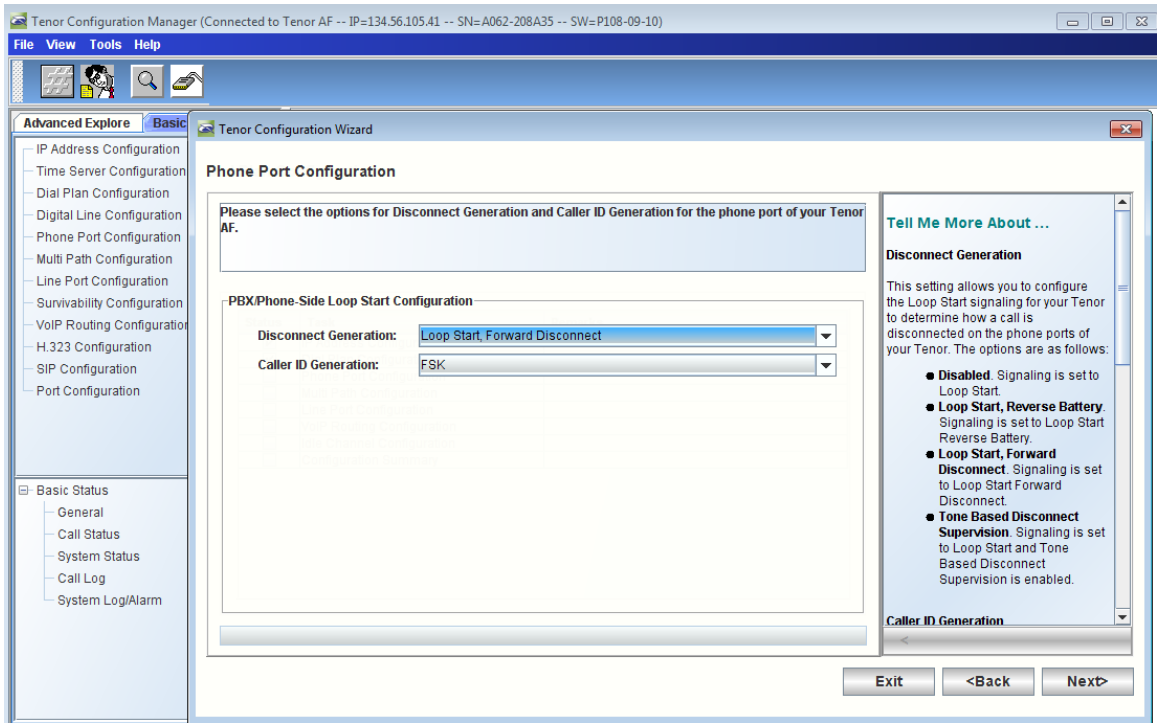


- Verify that Dial Plan Configuration is completed as shown below

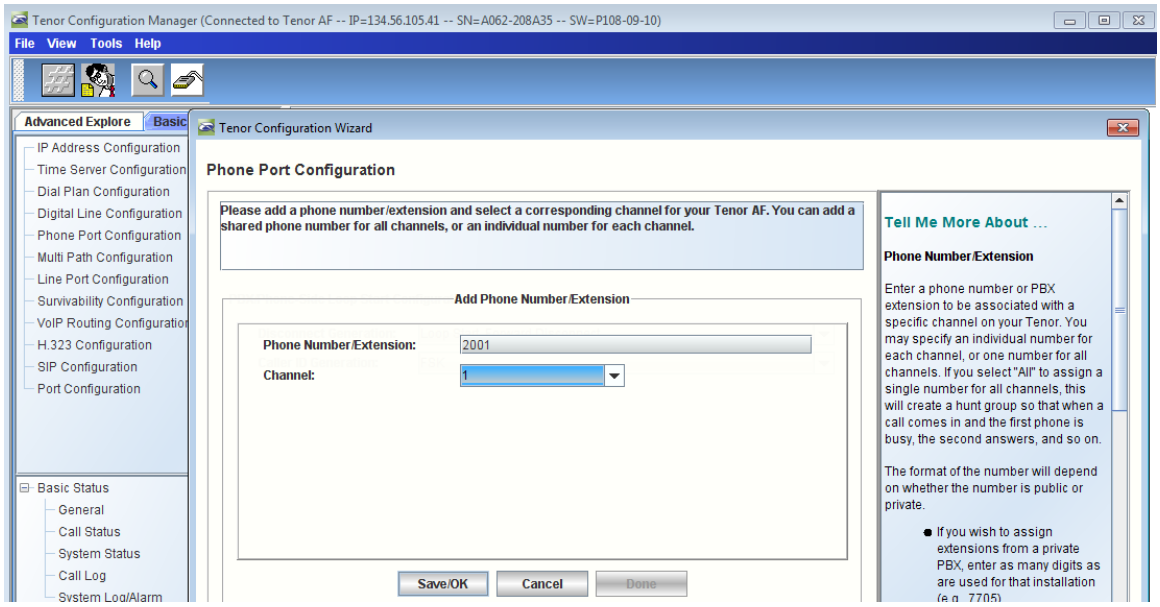


- Continue the wizard steps for Phone Port Configuration

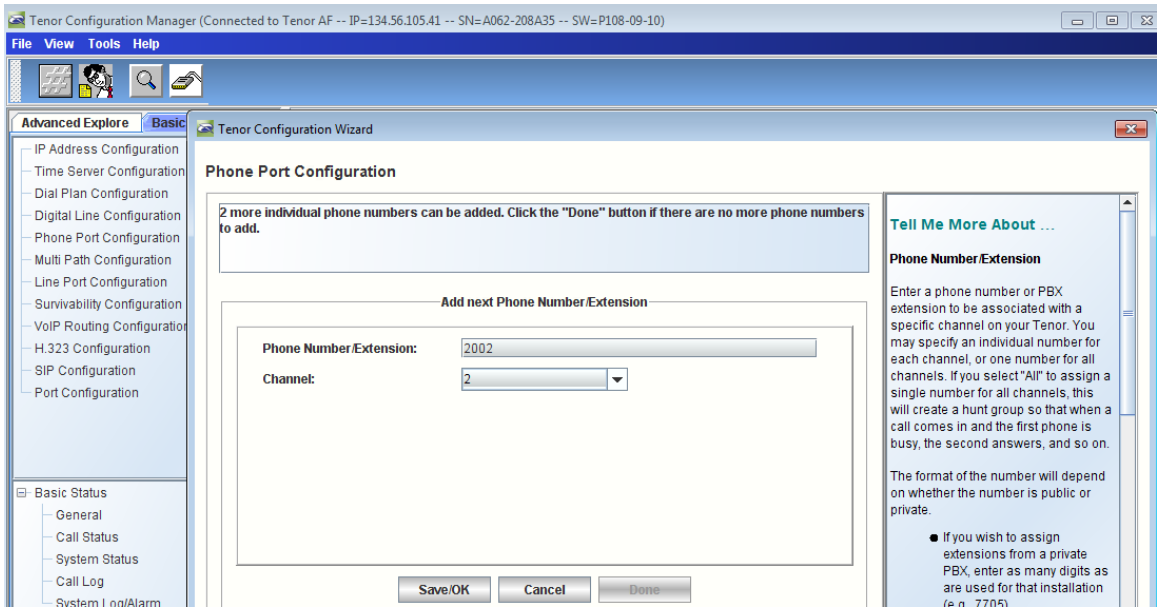
Copyright © 2015 Sonus Networks. All rights reserved.



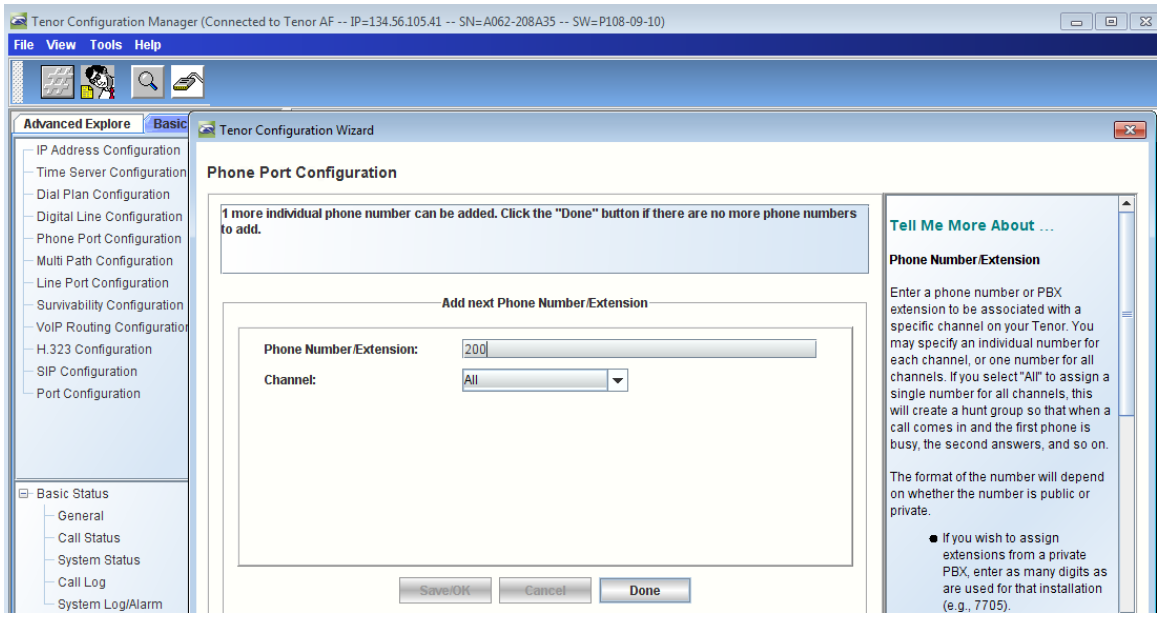
- Enter the relevant Phone Number/Extension (in this example we are using 2001 and 2002 users for the Analog phone endpoints)



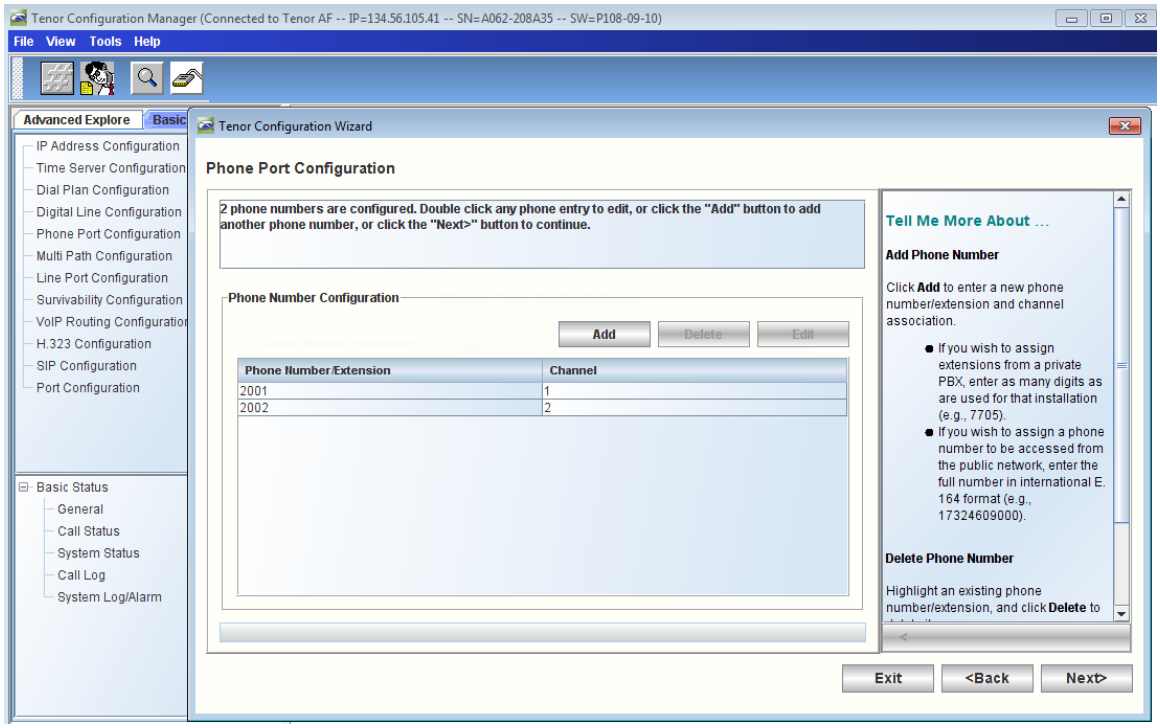
Copyright © 2015 Sonus Networks. All rights reserved.



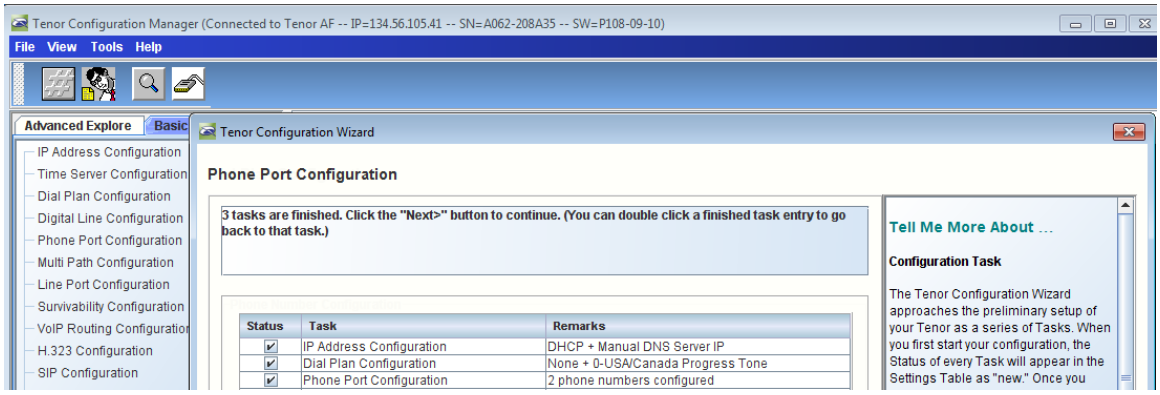
- Hit on "Save/OK" and then the "Done" buttons



Copyright © 2015 Sonus Networks. All rights reserved.

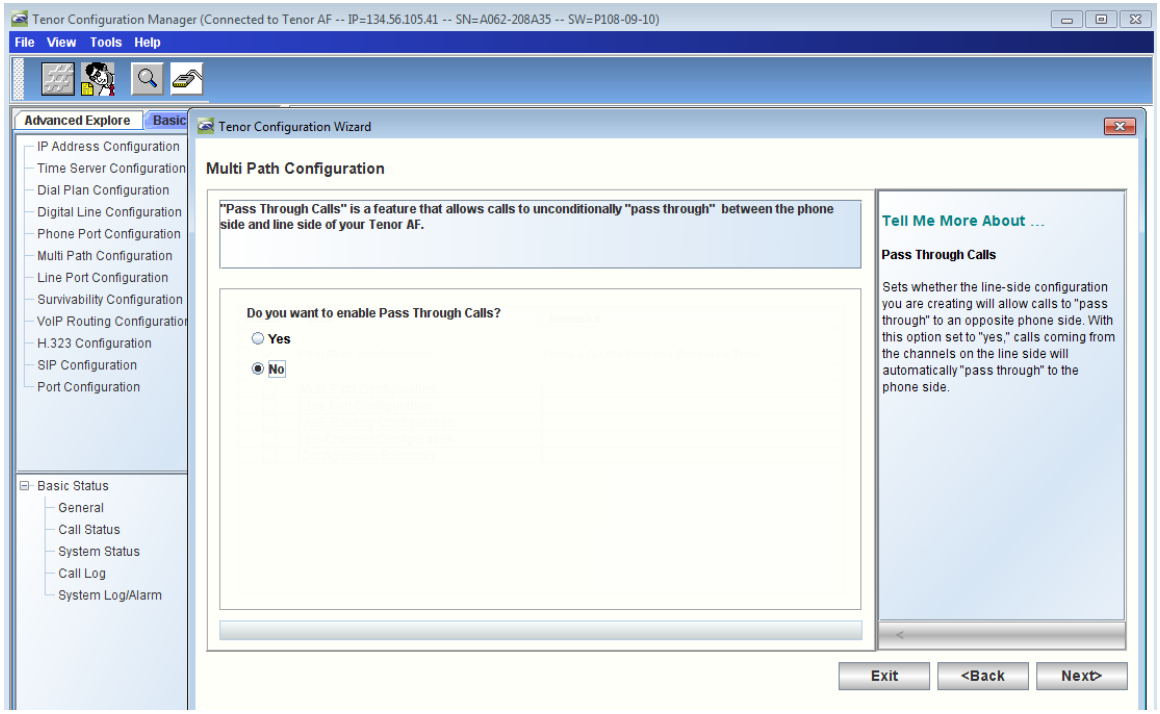


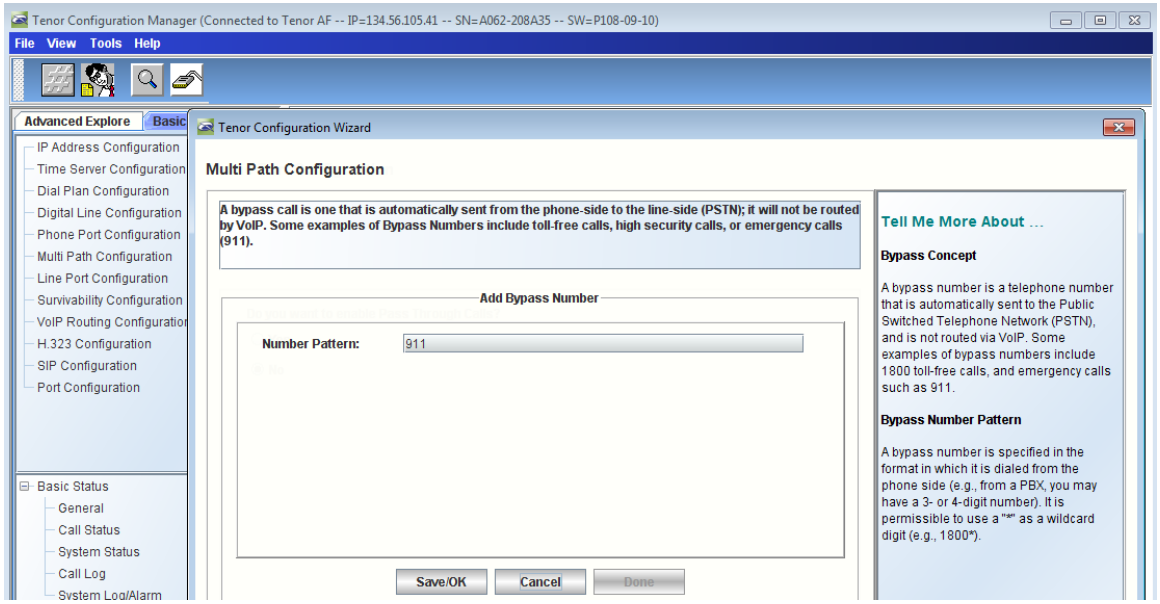
- Verify that Phone Port Configuration is completed as shown below



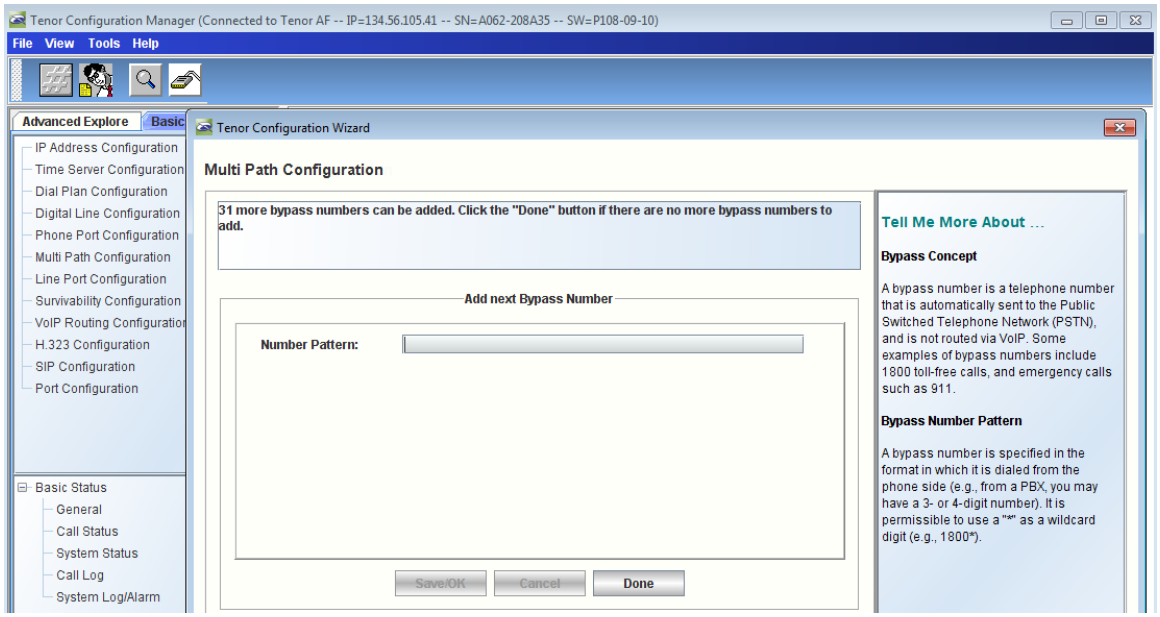
- Continue the wizard steps for Multi Path Configuration

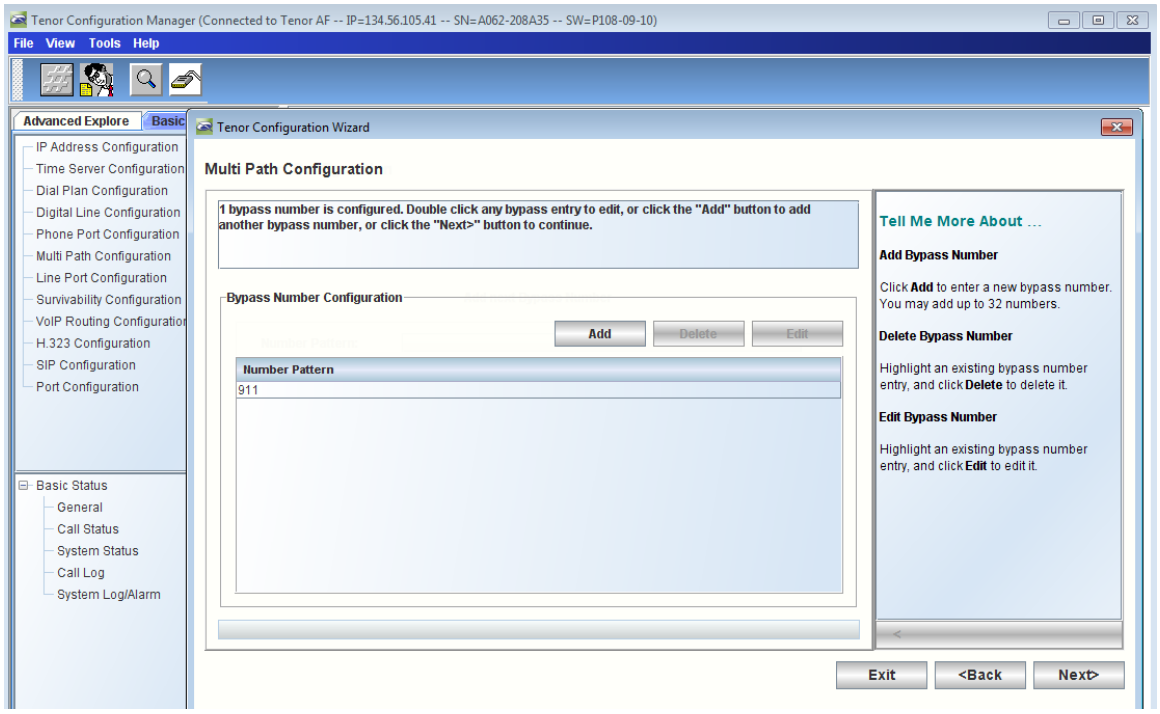
Copyright © 2015 Sonus Networks. All rights reserved.





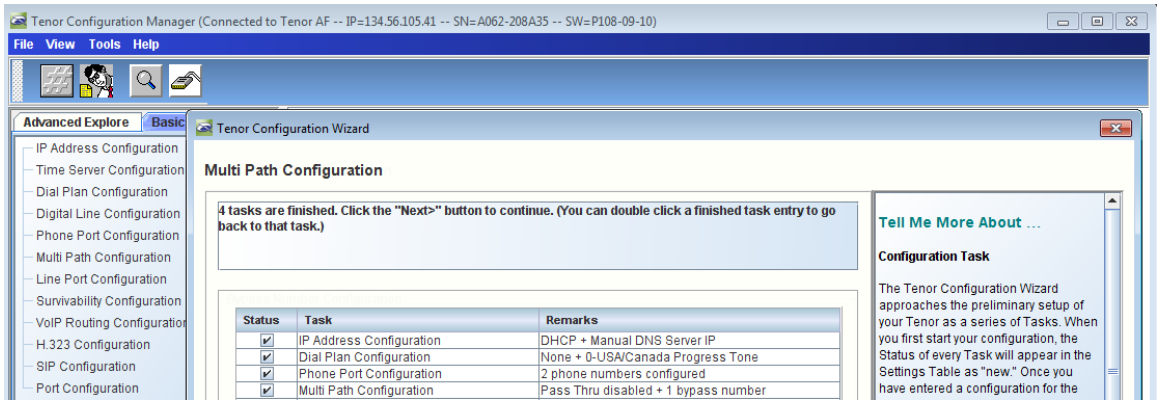
Copyright © 2015 Sonus Networks. All rights reserved.



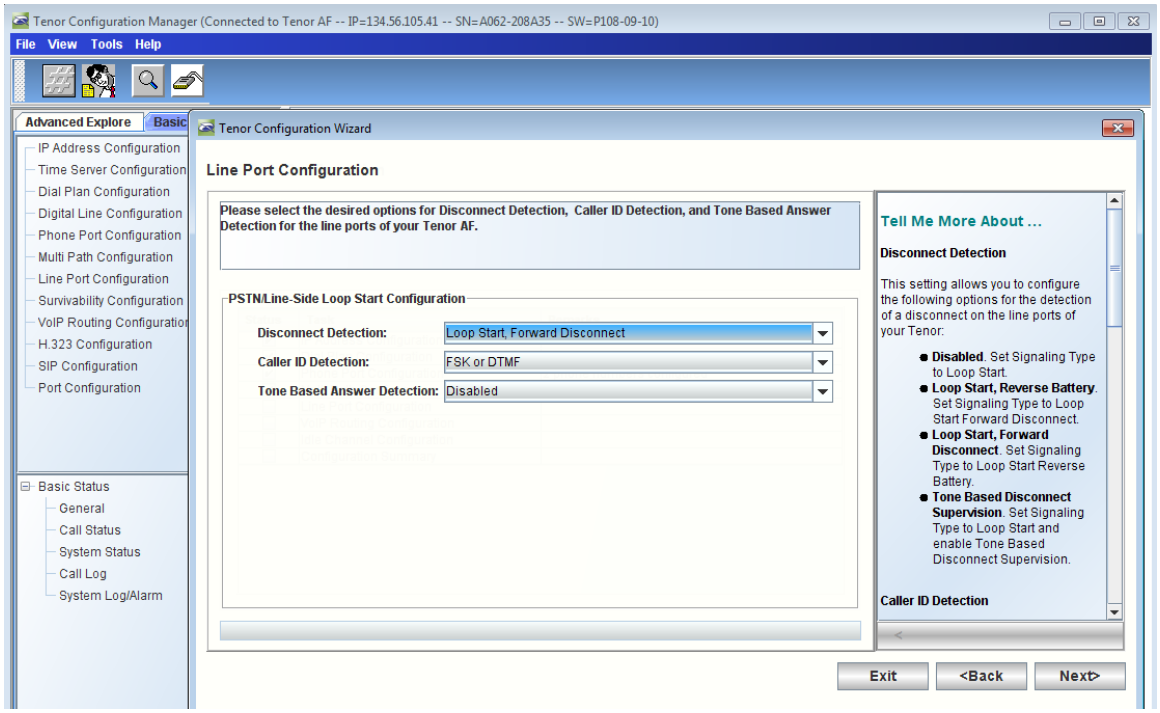


- Verify that Multi Path Configuration is completed as shown below

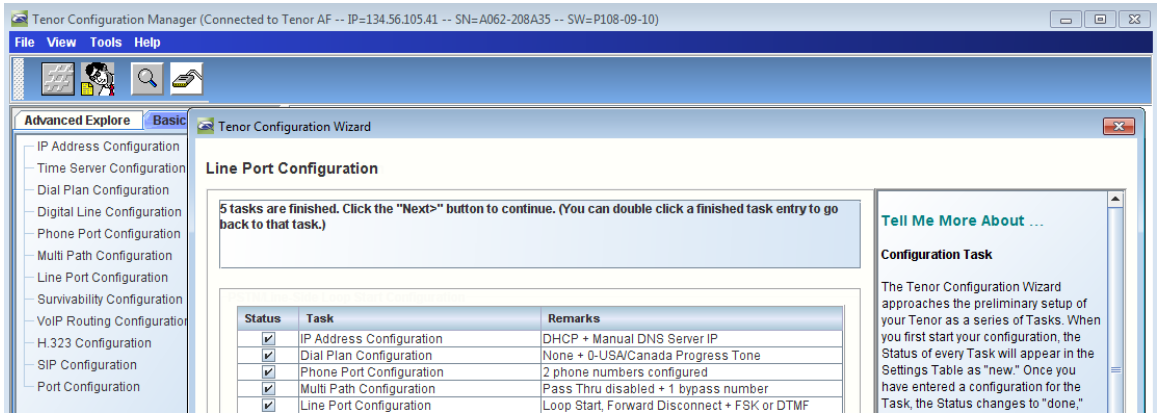
Copyright © 2015 Sonus Networks. All rights reserved.



- Continue the wizard steps for Line Port Configuration

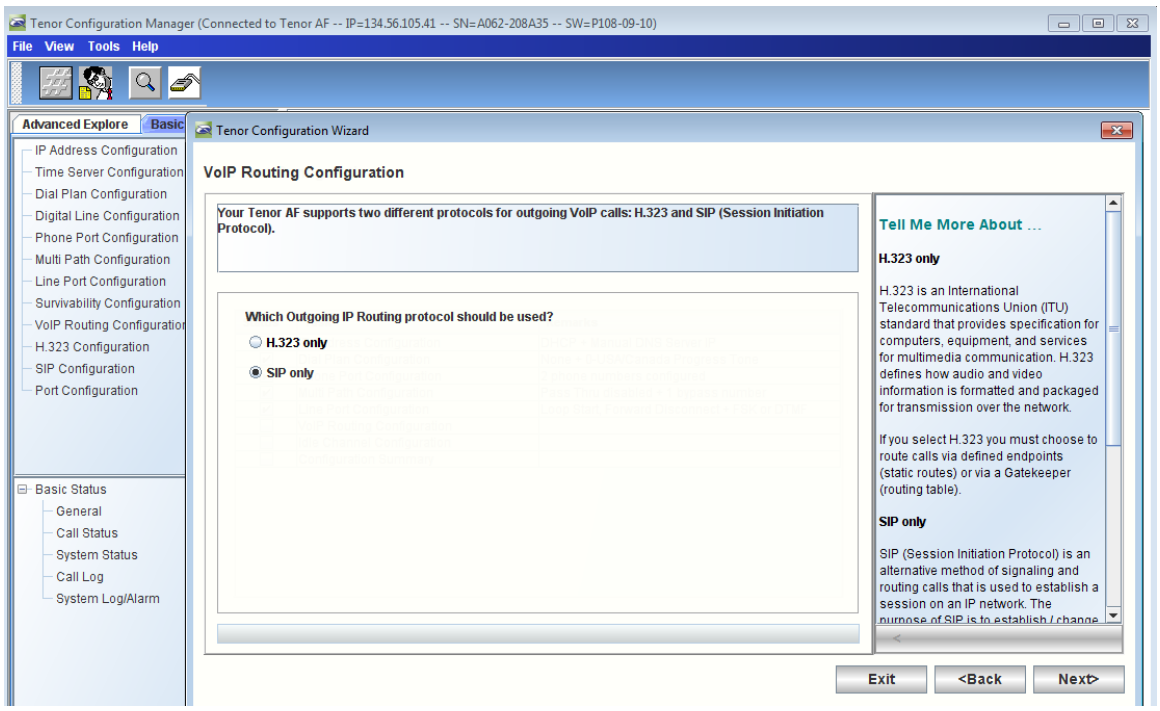


- Verify that Line Port Configuration is completed as shown below

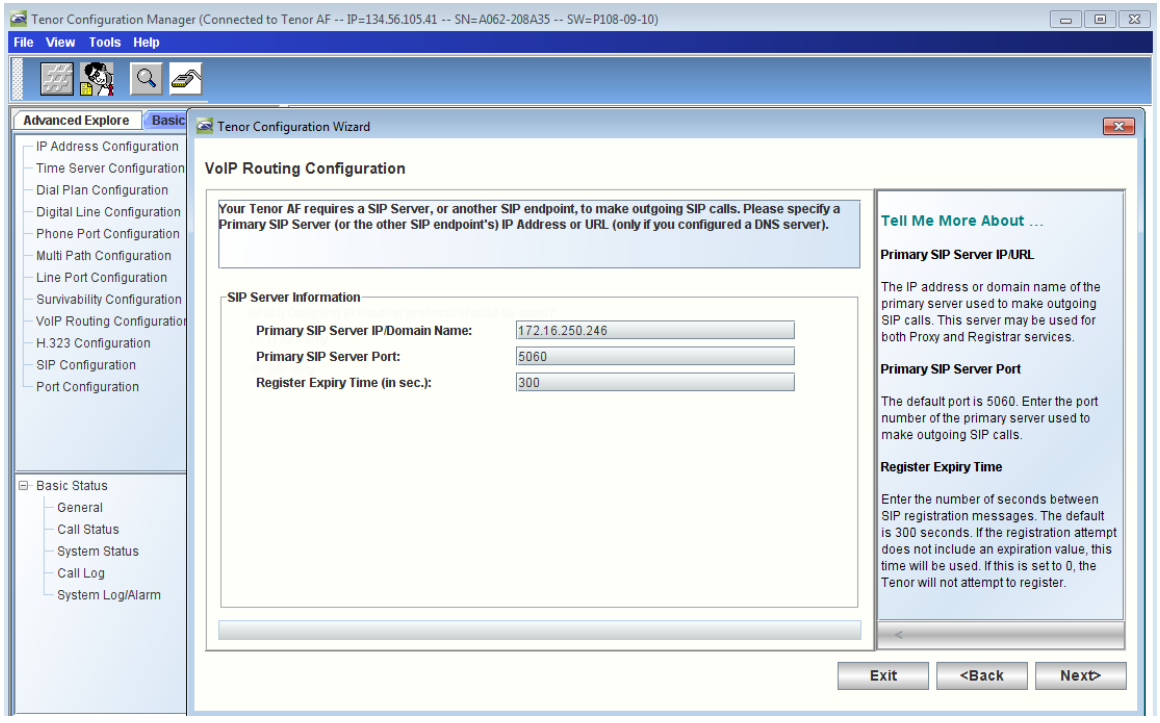


- Continue the wizard steps for VoIP Routing Configuration

Copyright © 2015 Sonus Networks. All rights reserved.

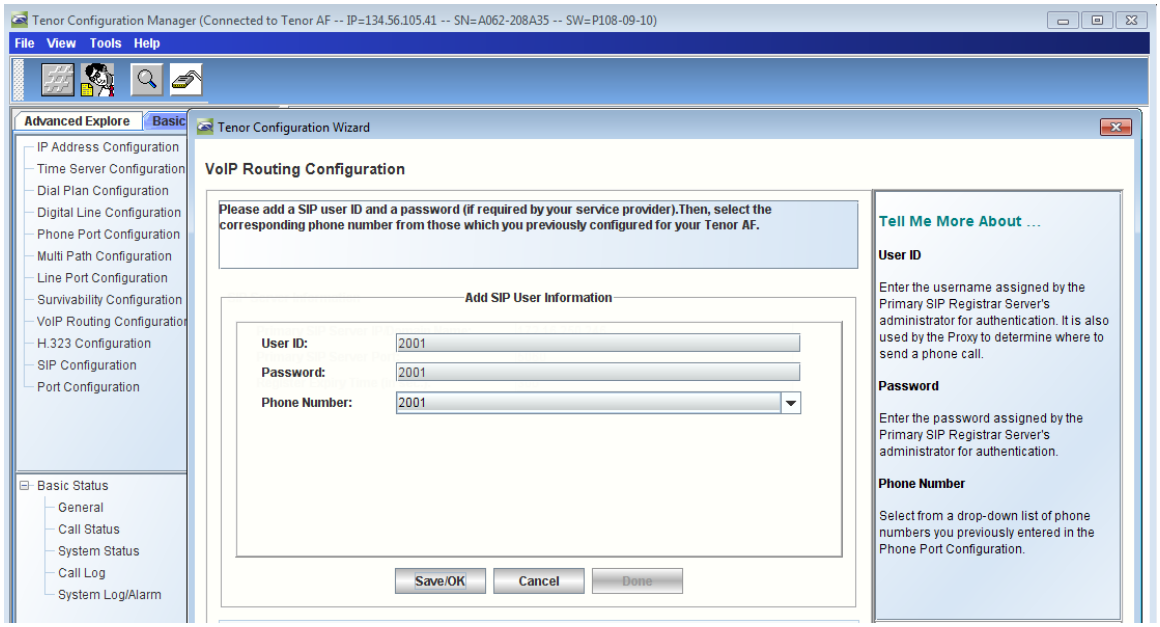


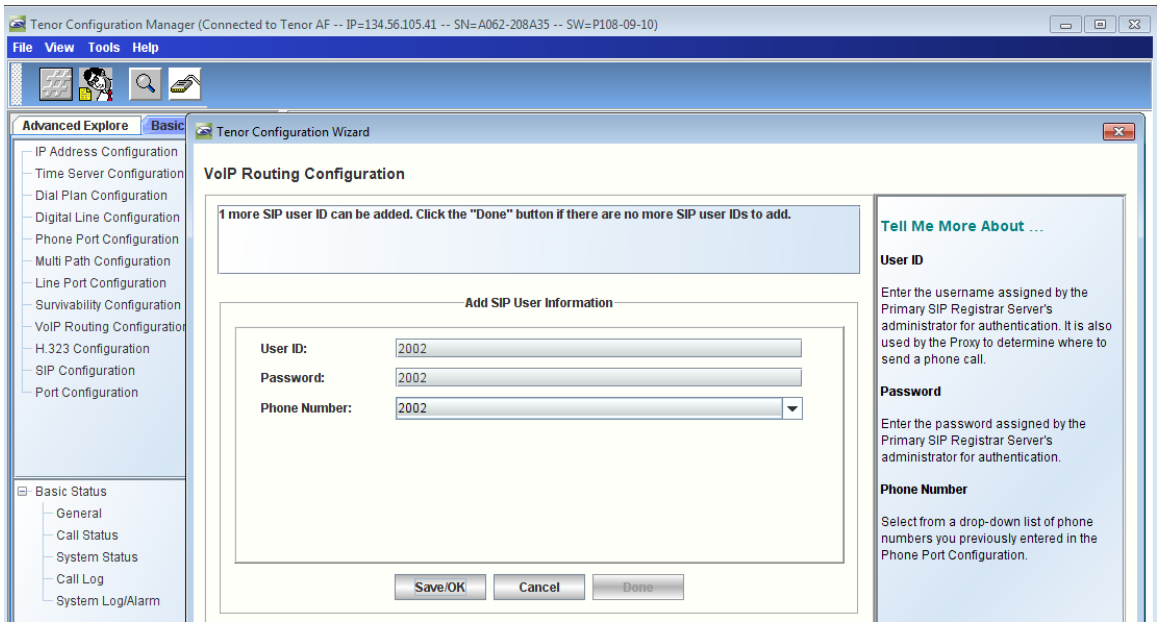
- Enter the Sonus SBC 1000/2000 2000 Gateway IP address in the Primary SIP Server IP/Domain Name field and the relevant Port (5060 in this case)



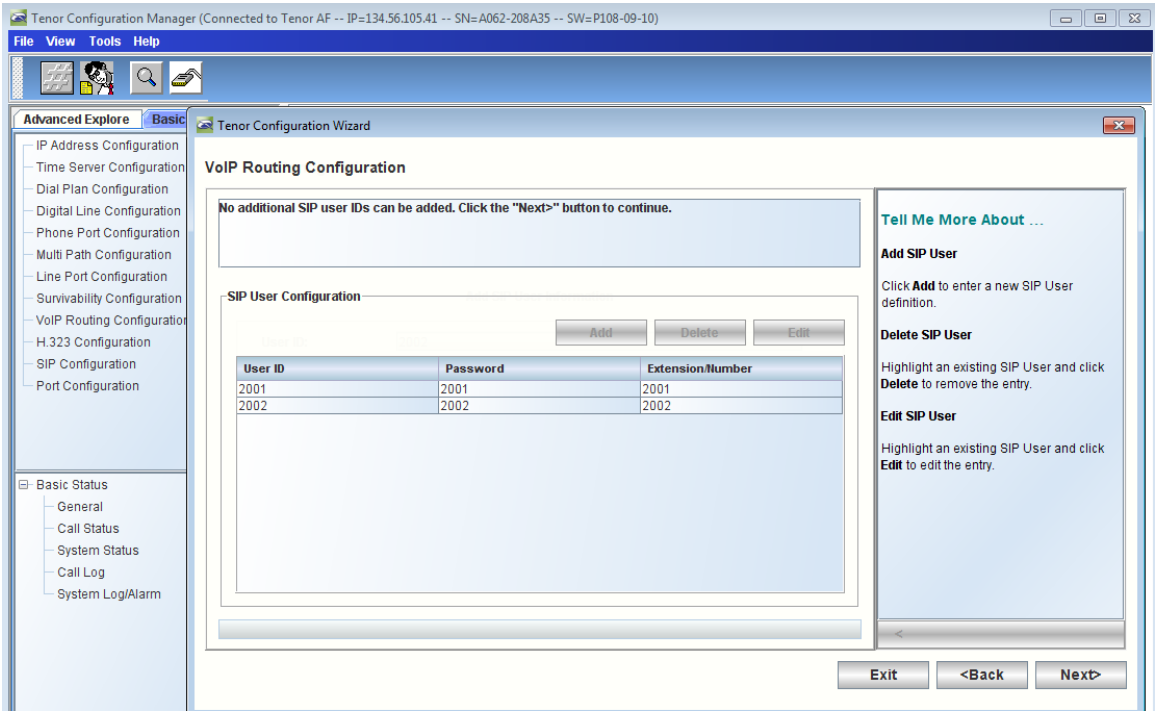
- Enter the SIP user information for the related 2001 and 2002 users

Copyright © 2015 Sonus Networks. All rights reserved.

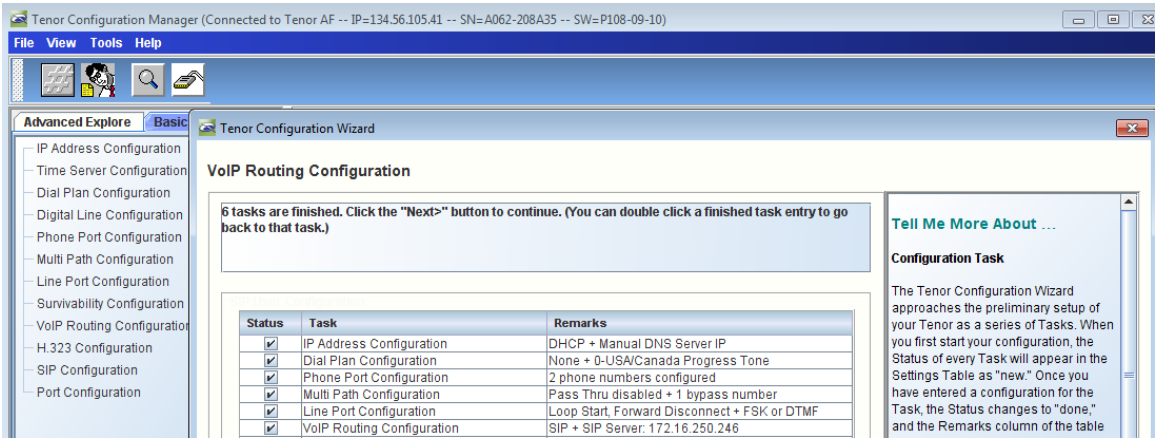




Copyright © 2015 Sonus Networks. All rights reserved.

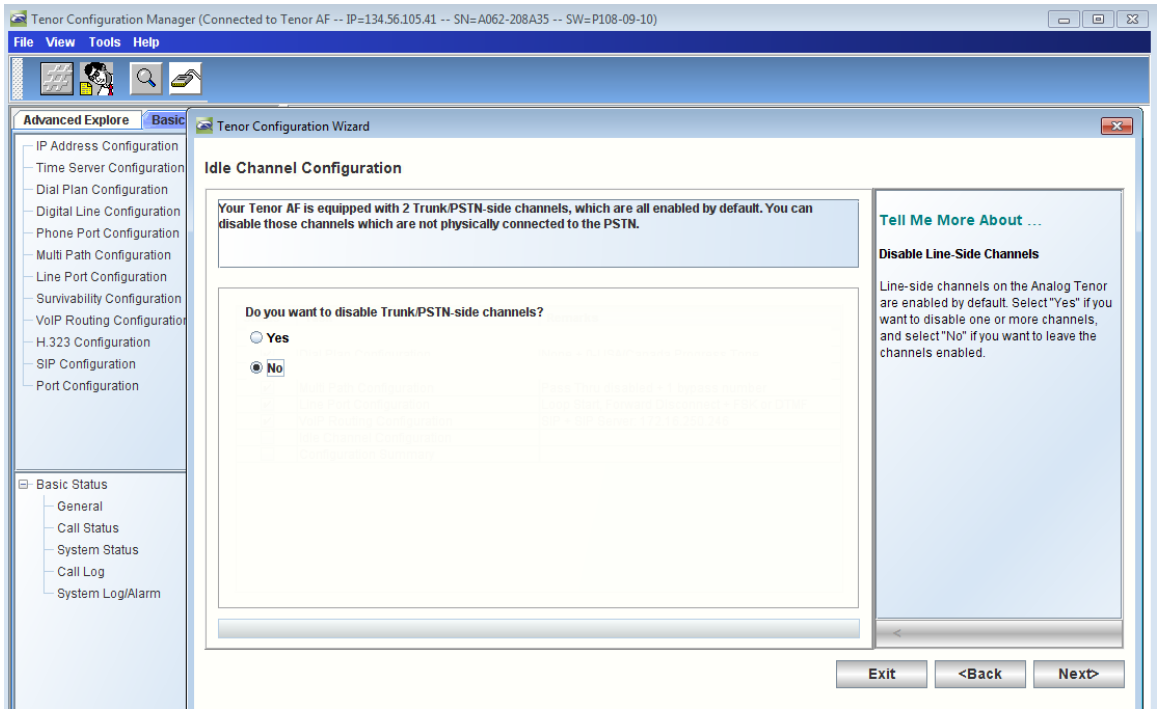


- Verify that VoIP Routing Configuration is completed as shown below

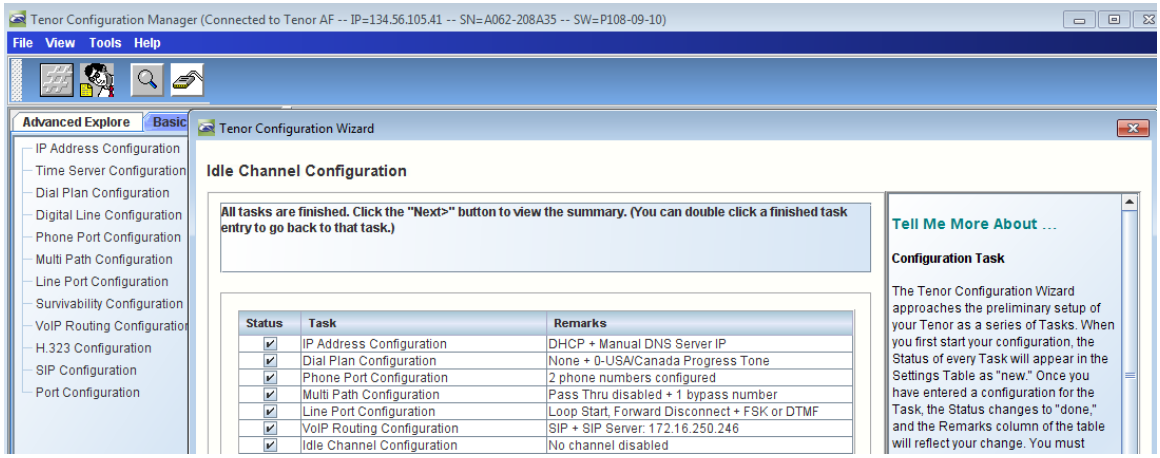


- Continue the wizard steps for Idle Channel Configuration

Copyright © 2015 Sonus Networks. All rights reserved.

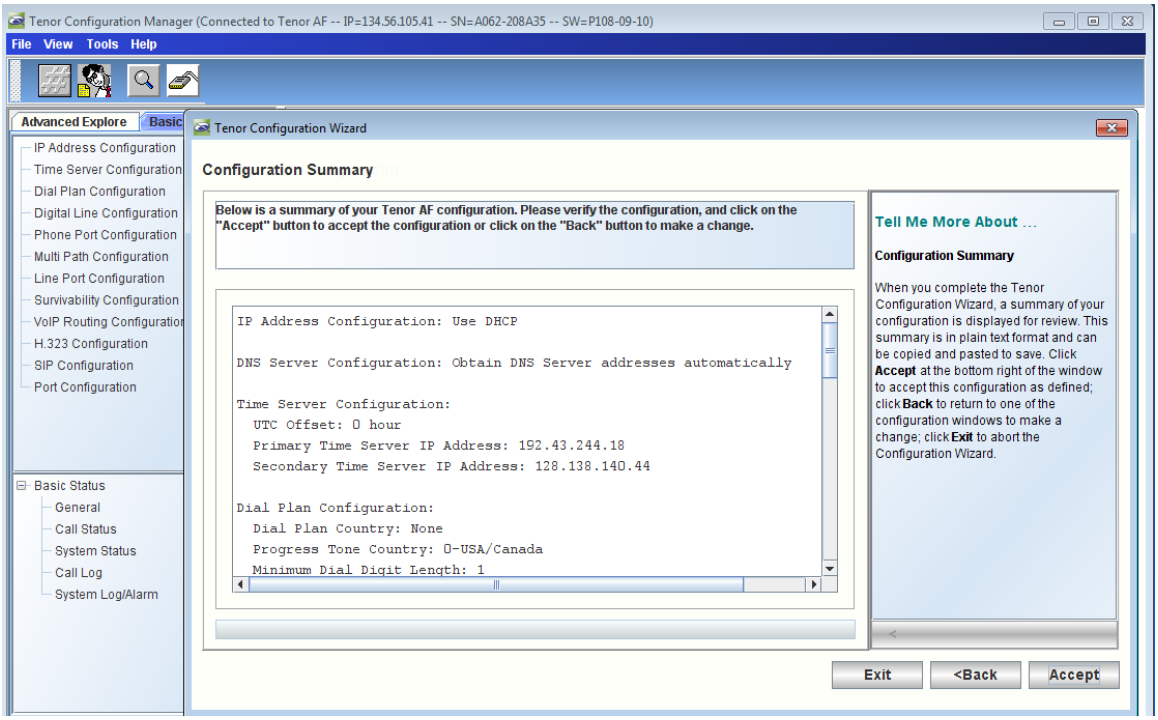


- Verify that Idle Channel Configuration is completed as shown below

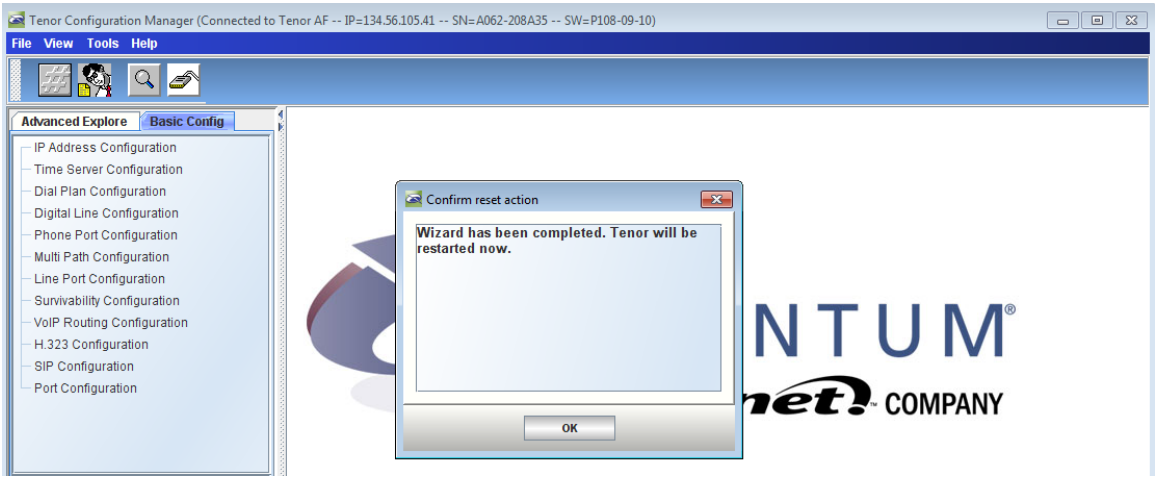


- Hit on Accept button on Configuration Summary to complete the wizard run

Copyright © 2015 Sonus Networks. All rights reserved.



- Hit OK to restart the Tenor device as shown below

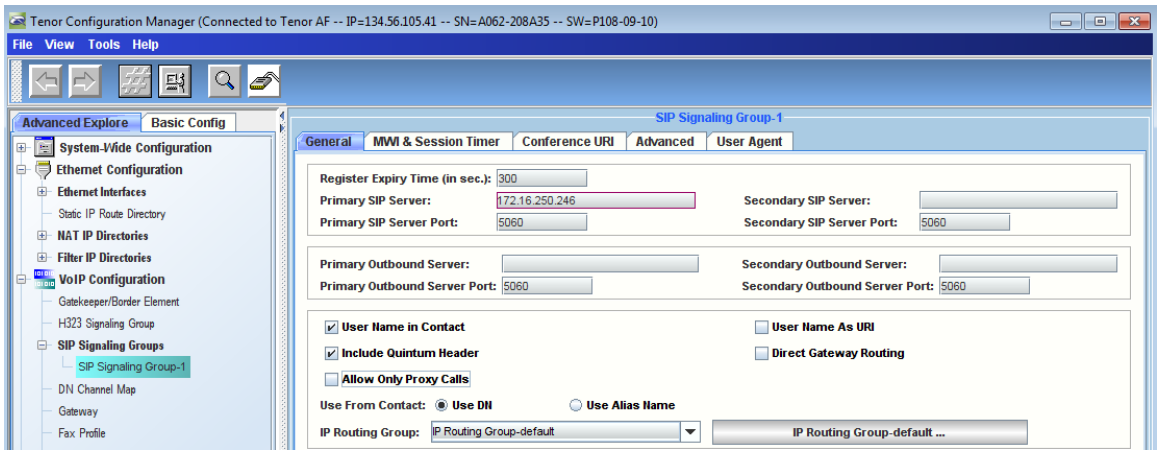


Additional Post-wizard Settings and Configuration Verrification

Verifying the SIP Signaling Group Options

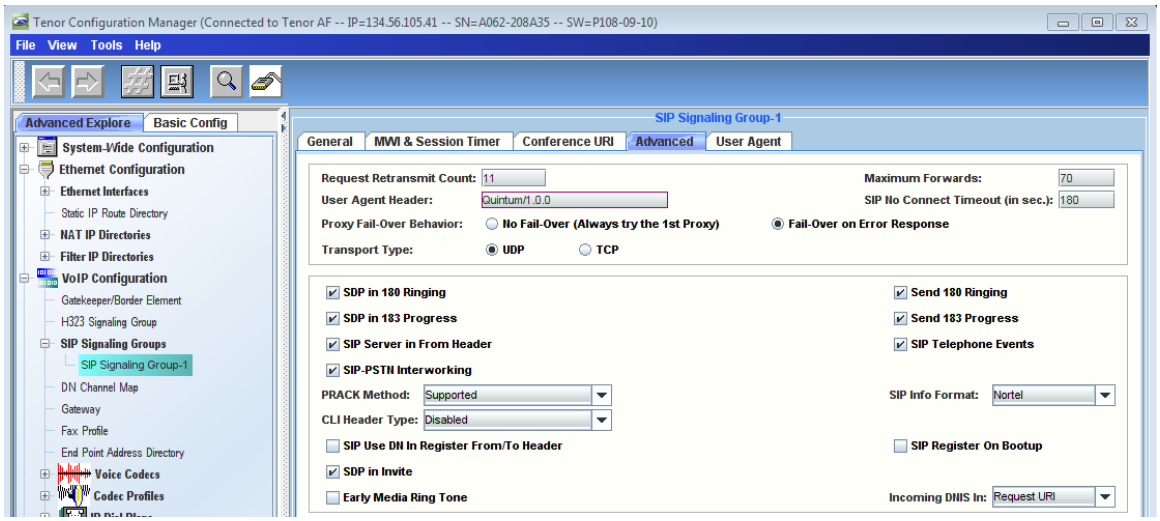
- Reconnect to Tenor Device using the Configuration Manager and Verify that SIP Signaling Group is configured In General Tab as shown below

Copyright © 2015 Sonus Networks. All rights reserved.



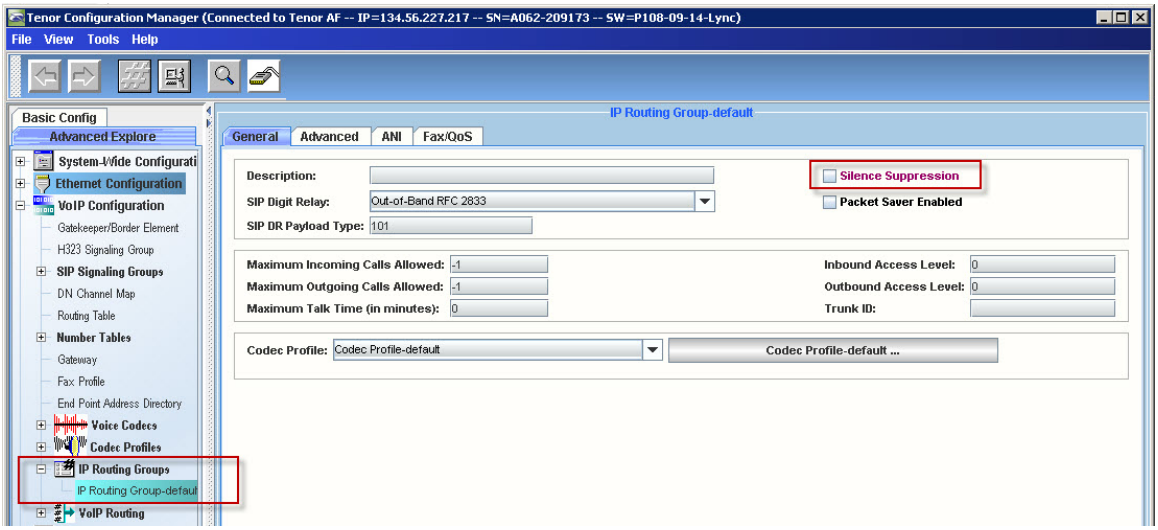
- Verify that SIP Signaling Group is configured in Advanced Tab as shown below

> The Transport Type **must be set to UDP**.



Verify that the Silence Suppression parameter in the IP Routing Group is disabled

Copyright © 2015 Sonus Networks. All rights reserved.

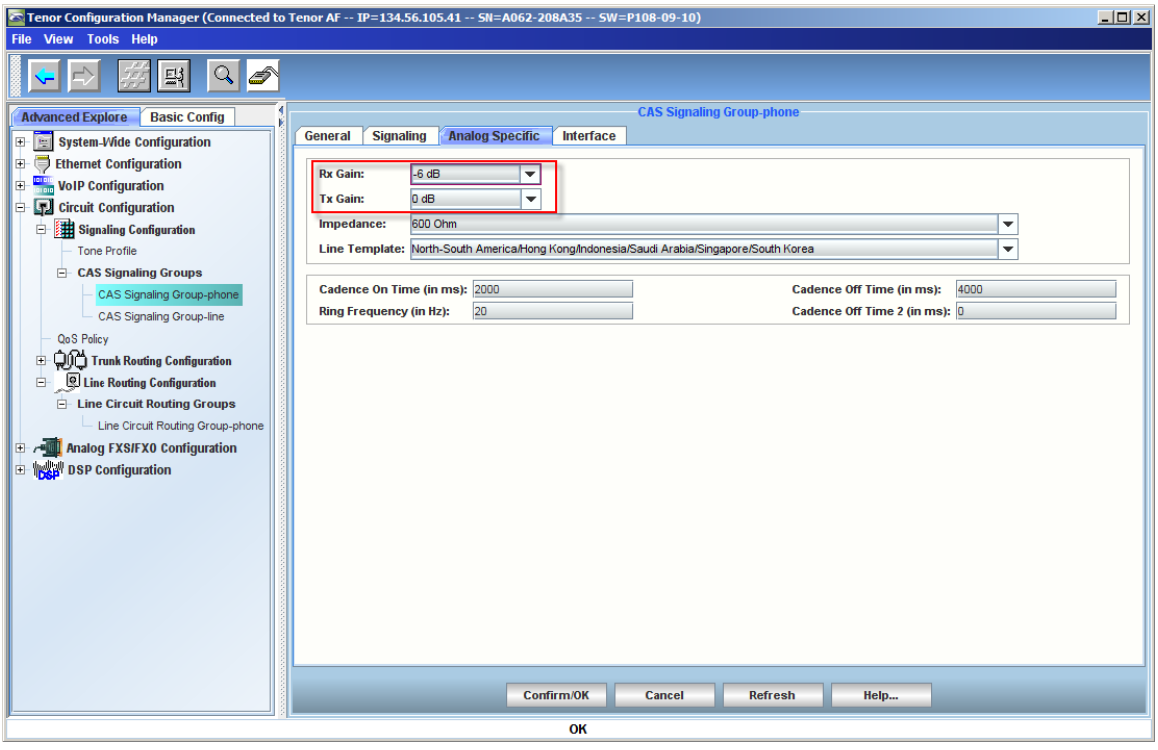


Verify the Tx/Rx Gain Values in the CAS Signaling Groups

Verify the following settings in Tenor:

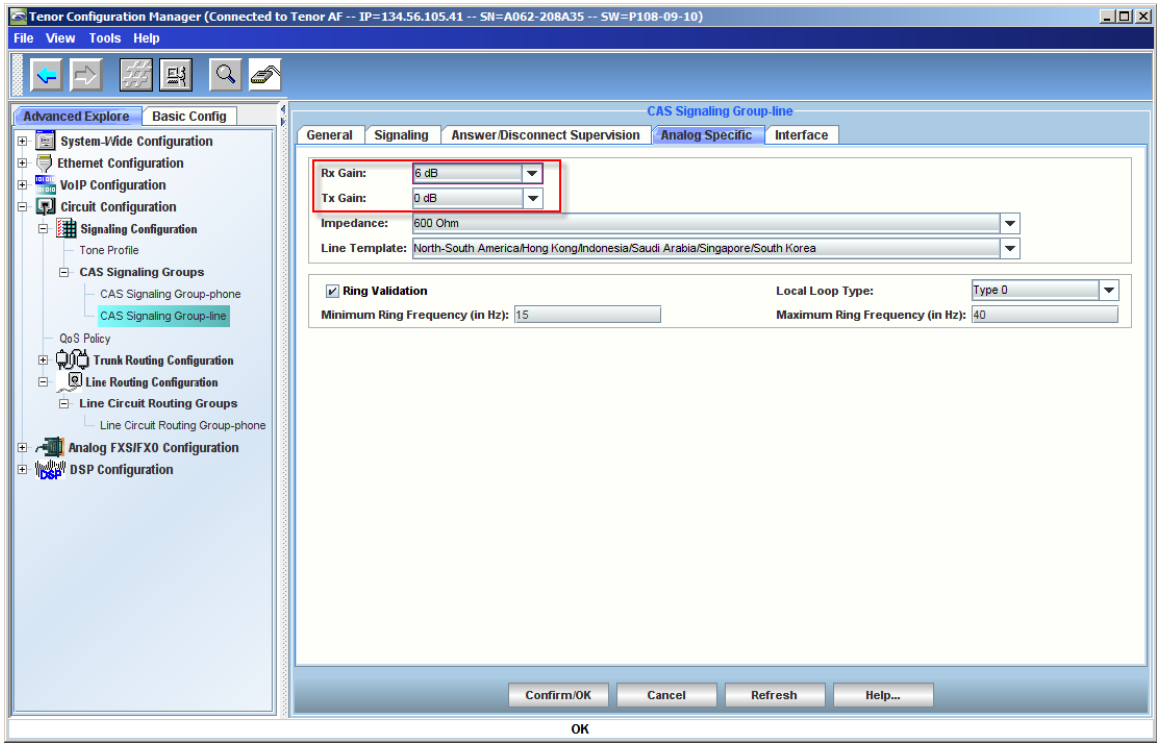
CAS Signaling Group	Rx Gain	Tx Gain
CAS Signaling Group - Phone:	-6	0
CAS Signaling Group - Line:	6	0

- Verify Tx/Rx gain values in the CAS signaling groups - Phone



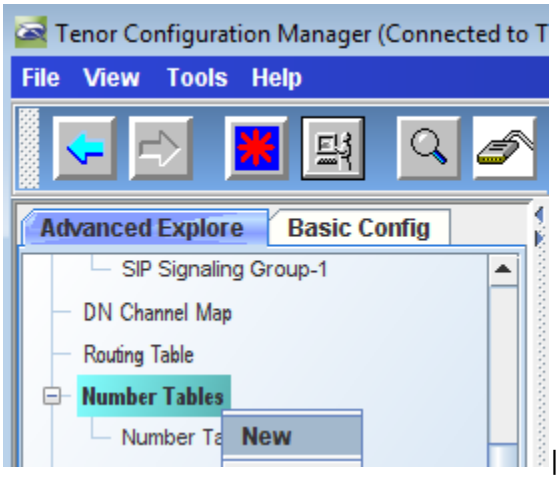
- Verify Tx/Rx gain values in the CAS signaling groups - Line

Copyright © 2015 Sonus Networks. All rights reserved.



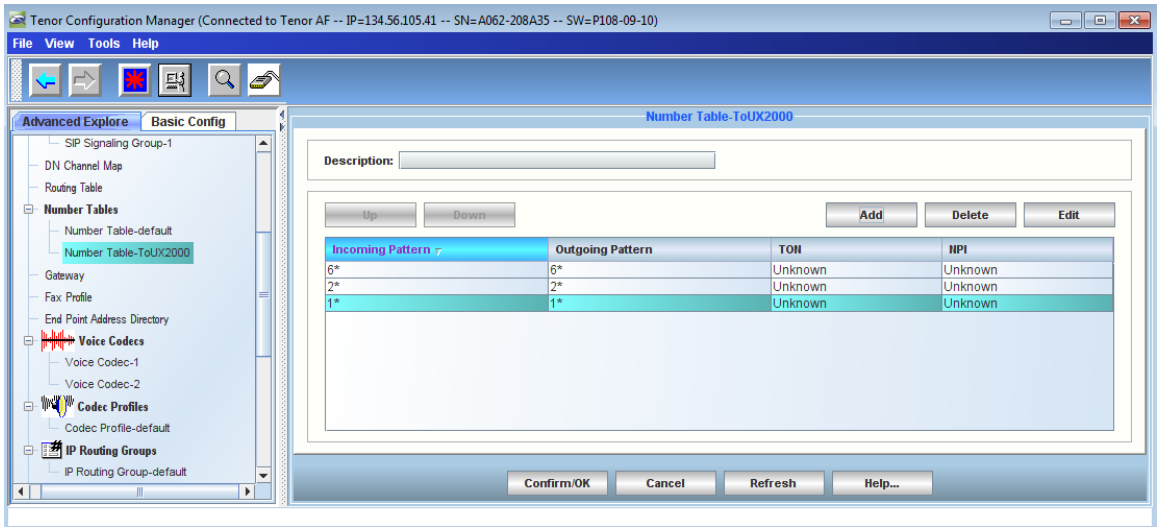
Creating a Route For Calls From Tenor to Lync

- In Configuration Manager, right click on Number Tables in left pane and select New as shown below

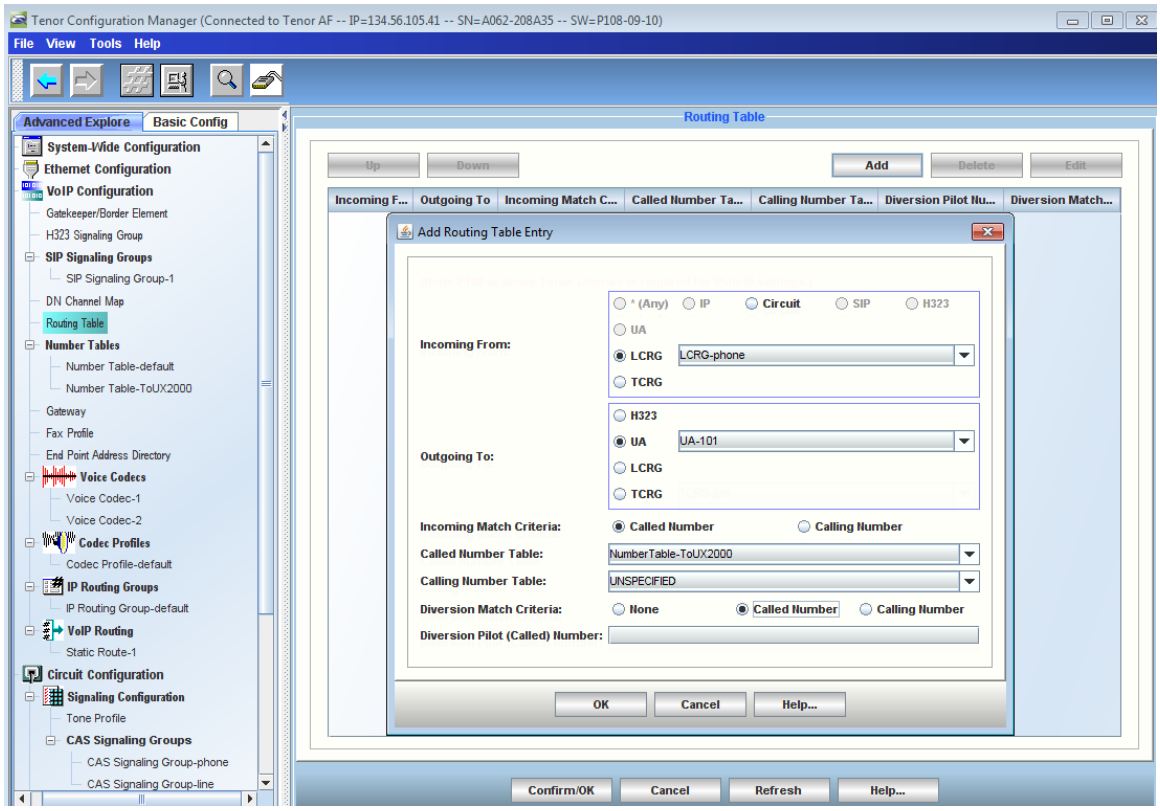


- Create a new Number Tables to allow Analog Endpoints to be able to make calls to LYNC endpoints as wells as to PBX endpoints as shown below

Copyright © 2015 Sonus Networks. All rights reserved.

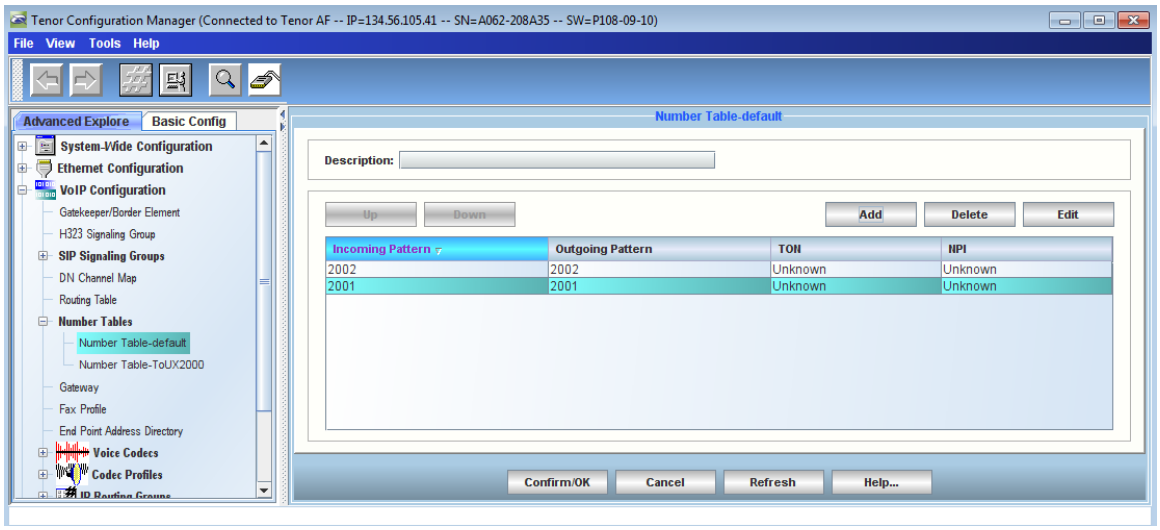


- Create an entry in the Routing Table as shown below

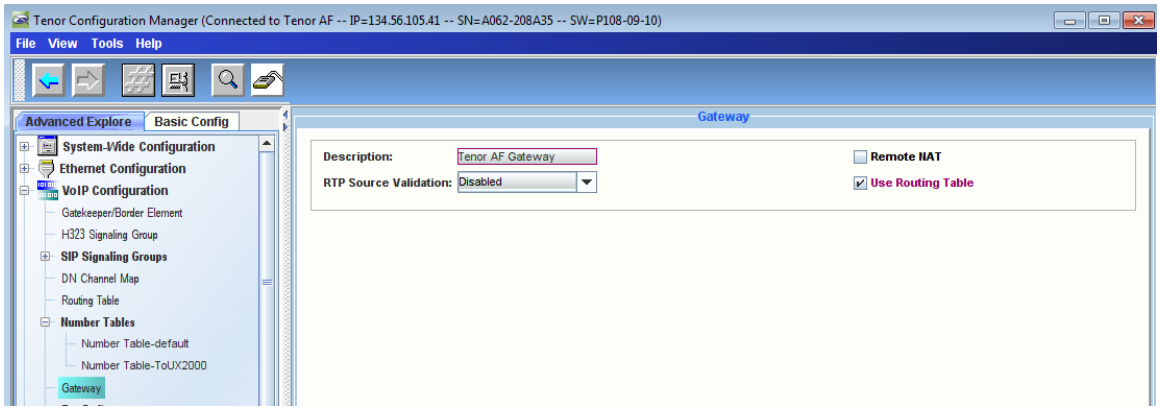


- Modify the default Number Table to allow incoming calls to Tenor Device as shown below

Copyright © 2015 Sonus Networks. All rights reserved.



- Verify that "Use Routing Table" option is selected in Gateway configuration field as shown below

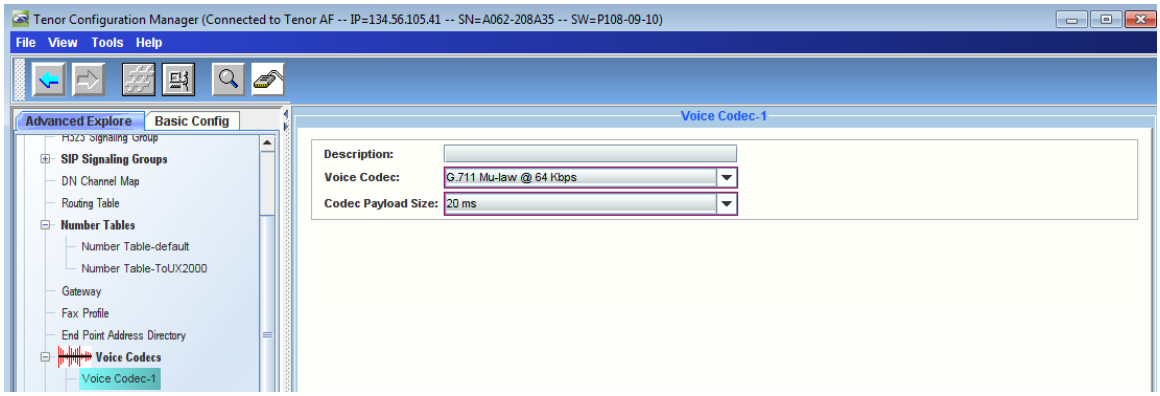


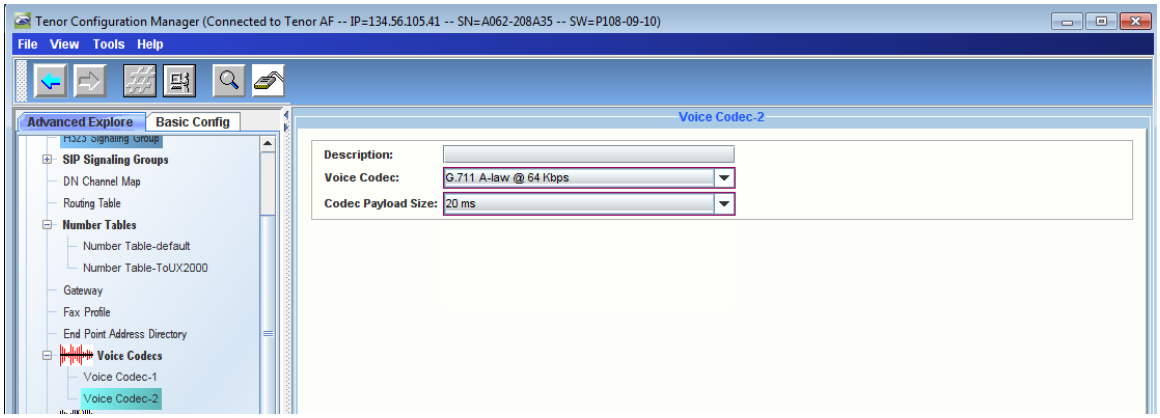
Verifying Codec Selection

> Ensure that the codec settings are identical with the matching codec in Sonus SBC 1000/2000.
> Use **only** G.711U and/or G.711A.

- Verify that Voice Codec settings are configured correctly as shown below

Copyright © 2015 Sonus Networks. All rights reserved.

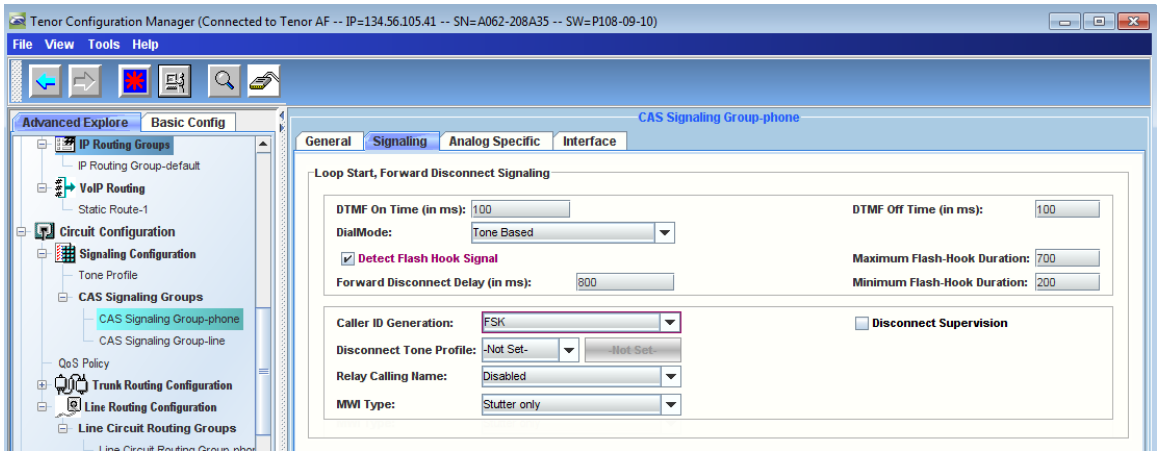




Verify Supplementary Services Enabled

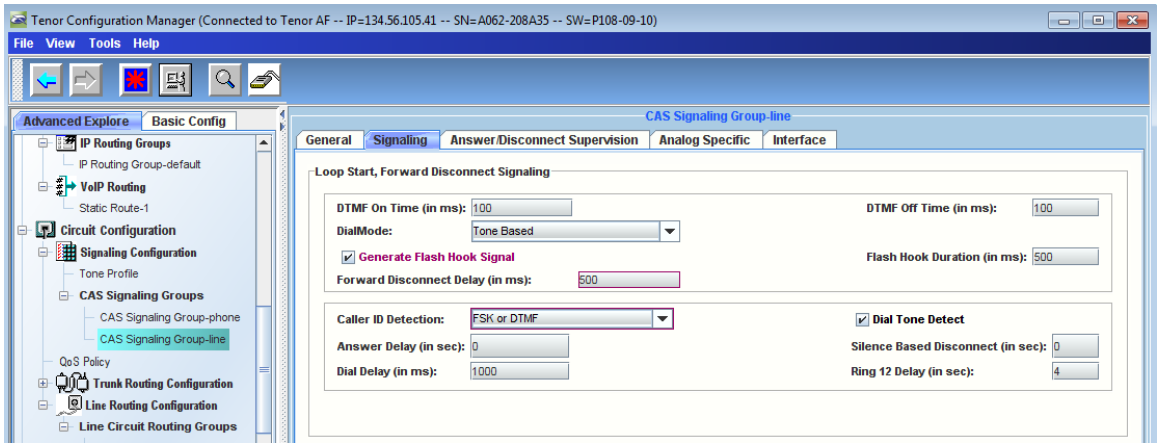
Tenor supports the following supplementary services - Hold/Unhold, Unattended (Blind) Transfer, and Attended (Consultative) Transfer. These features can be enabled and configured using either a Line Circuit Routing Group (LCRG) or Trunk Circuit Routing Group (TCRG). Follow the configuration steps below:

- Verify that "Detect Flash Hook Signal" option is selected in CAS Signaling Group-phone > Signaling Tab

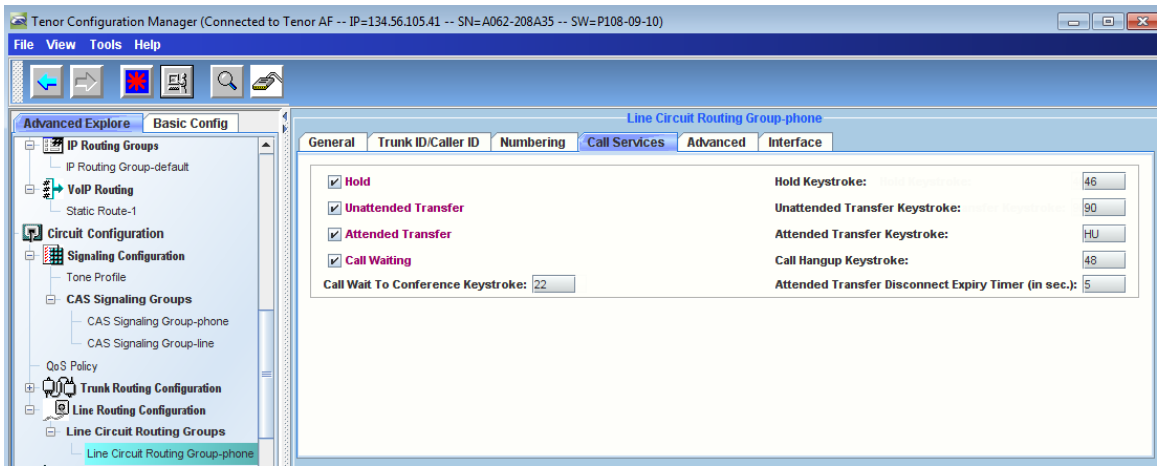


- Verify that "Generate Flash Hook Signal" option is selected in CAS Signaling Group-line > Signaling Tab

Copyright © 2015 Sonus Networks. All rights reserved.



- Verify that Call Services are selected in Line Circuit Routing Group-phone > Call Services Tab



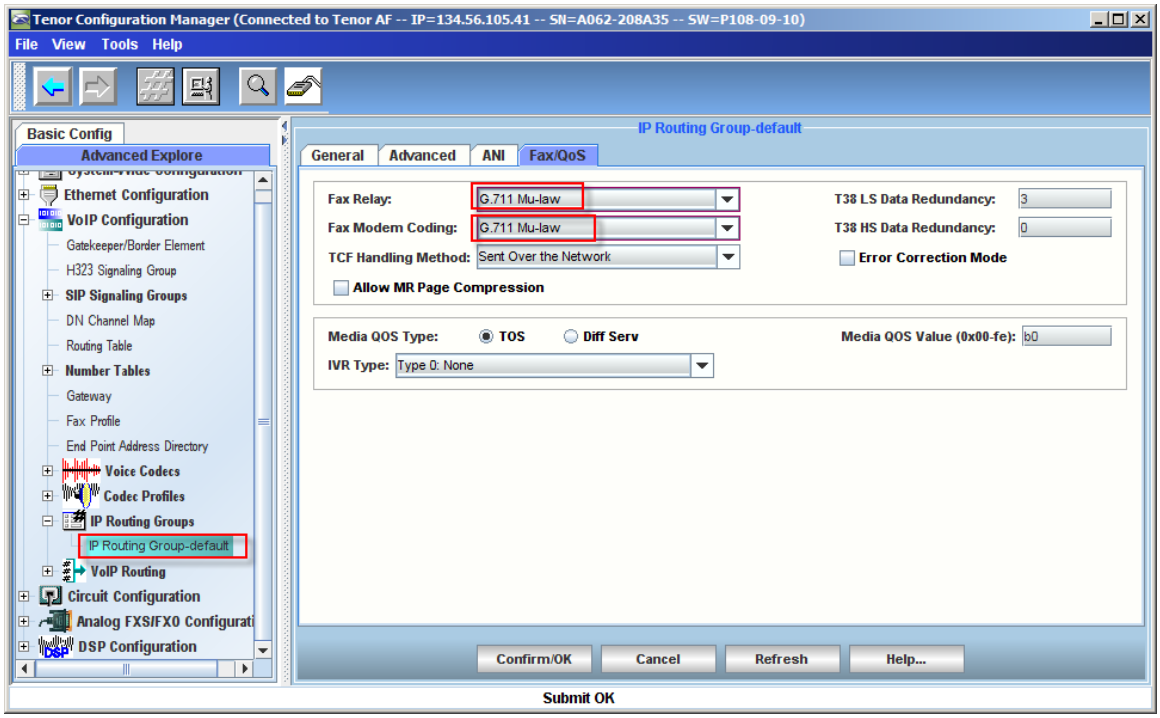
Change Fax Relay from T.38 without Fallback to G.711

- Make sure that Fax Relay is set to G.711.

> The codec should be either G.711U or G.711A depending on your particular environment.

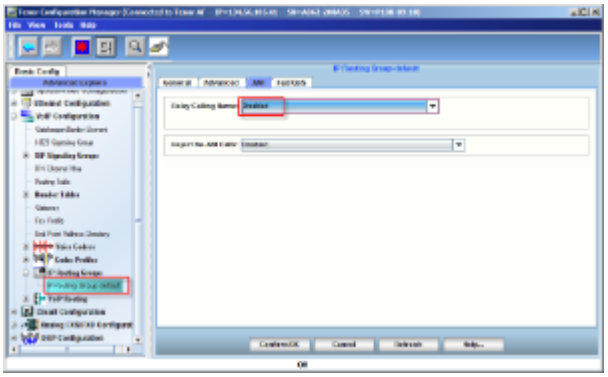
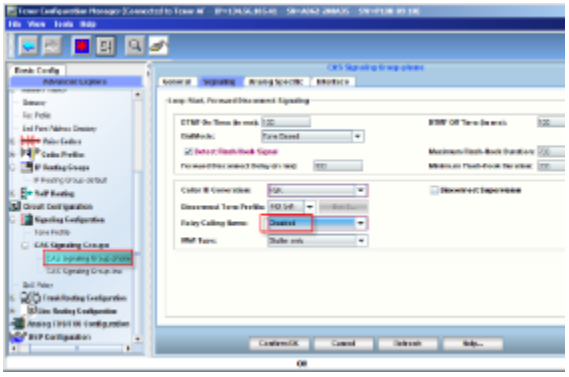
- Enable both, **Fax Relay** and **Fax Modem Coding**:
  - **Fax Relay:** This command configures how the Tenor signals the other end to tell the peer how to switch over to the correct protocol for a fax call. When **FaxRelay** is set to anything other than 0, there will be a short delay in training as the Tenor determines whether the device at the other end is a fax machine or a modem
  - **Fax Modem Coding:** Enable the **Fax Modem Coding** configuration option if the Tenor will be used to make modem calls (remote door/elevator control).
    When the Tenor is configured for modem over IP calls, **FaxModemCoding** allows you to select which codec will be used.
    When **FaxRelay** is set to 0 (Disabled), Modem over IP (MoIP) takes over, and all fax calls will be sent as MoIP passthrough with the codec specified by the FaxModemCoding setting.
    When **FaxRelay** is set to anything other than 0, there will be a short delay in training as the Tenor determines whether the device at the other end is a fax machine or a modem.

Copyright © 2015 Sonus Networks. All rights reserved.

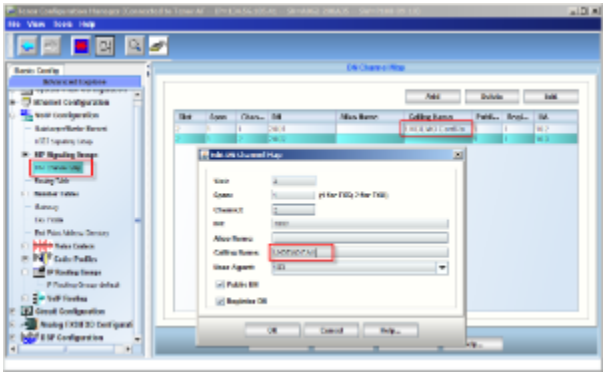
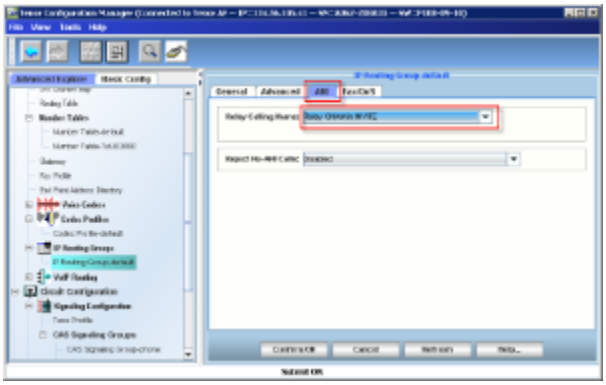
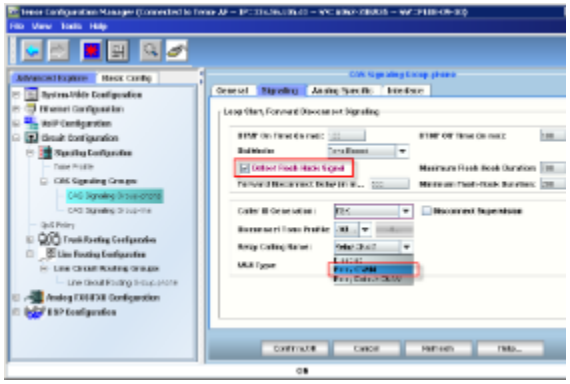
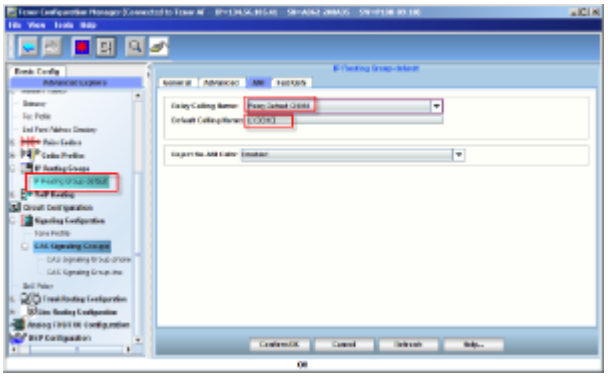
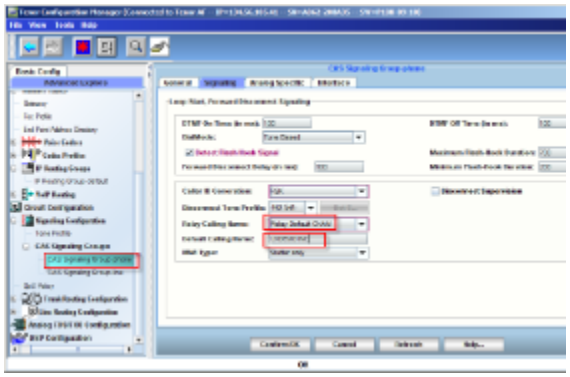


Configuring the Relay of Calling Name (CNAM)

The configuration of the Calling Name (CNAM) is optional. Tenor can relay CNAM in both directions Analog to SIP and SIP to Analog.

	Analog to SIP	**SIP to Analog**
Not send CNAM	`VoIP Configuration > IP Routing Groups > IP Routing Group-default > ANI > Relay Calling Name -` **`Disabled`** 	`Circuit Configuration > Signaling Confi > CAS Signaling Groups > CAS Signaling Group-phone > Relay Calling name -` **`Disab d`** 

Copyright © 2015 Sonus Networks. All rights reserved.

Send the CNAM	Send the CNAM of each analog line as configured in the DN Channel Map: 1. First add the Calling Name in the channel mapping for each channel. `VoIP Configuration > DN Channel Map > Calling Name -` **`Free text`**  2. Secondly select the global default behavior. `VoIP Configuration > IP Routing Group > IP Routing Group-default > ANI > Relay Calling name -` **`Relay CNAM in INVITE`** 	Send the CNAM from the SIP call leg. `Circuit Configuration > Signaling Confi > CAS Signaling Groups > CAS Signaling Group-phone > Signaling > Relay Calling Name -` **`Relay CNAM`** 
Send default CNAM	Send a default CNAM for all calls regardless of the Calling Name of the originating channel. `VoIP Configuration > IP Routing Group > IP Routing Group-default > ANI > Relay Calling name >` **`Relay Default CNAM`** `> Default Calling Name -` **`Free text`** 	Send a default CNAM for all calls regardless of the Calling Name of the originating channel. `Circuit Configuration > Signaling Confi > CAS Signaling Groups > CAS Signaling Group-phone > Signaling > Relay Calling Name >` **`Relay Default CNAM`** `> Default Call Name -` **`Free text`** 

Copyright © 2015 Sonus Networks. All rights reserved.

Sample Tenor AF Configuration File

Click here to see the Tenor AF DB file Software Version P108-09-10

```
# /*<-- System Info. Do not overwrite!
# Product: Tenor AF
# IP: 134.56.105.41
# Subnet: 255.255.255.0
# Gateway: 134.56.105.1
# Software: P108-09-10
# Serial Number: A062-208A35
# DB: DB_CMS_M15_A019_V13.0.0_080109
# Updated: WED JUN 22 22:56:23 2011
# -->*/
config
table off
VOIPNetwork 1
SIte 1
TimeServer 1
set UTCOffset 0:00
set PrimaryServerIPAddr 134.56.113.11
set SecondaryServerIPAddr 128.138.140.44
DialPlan 1
set MAXDNlength 30
set MINDNlength 1
set LongDistancePrefix ""
set CarrierPrefixPattern ""
set INTernationaLPrefix[1] ""
set DialPlanCountry 255
UserProgramDialPlan 1
PRIVateNumberingPlan 1
MasterChassis 1
set Type 6
set DBVersion "DB_CMS_M15_A019_V13.0.0_080109"
set SNMPTrapCommunity "trap community"
IVRFileServer 1
SYSLogServer 1
set id "1"
CDRServer 1
set id "1"
CDRServer 2
set id "2"
set CDRServerPort 9003
new ChannelGroup phone
ChannelGroup phone
new ChannelGroup line
ChannelGroup line
NMSServer 1
DNSHosts 1
DNSServer 1
set UseConfiguredDNSServers 1
set PrimaryServerIPAddr 172.16.250.30
set SecondaryServerIPAddr 134.56.112.12
RadiusInfo UserServer
set name "User Authentication Server"
RadiusInfo EndpointServer
set name "Endpoint Authorization Server"
RadiusInfo RoutingServer
set name "External Routing Server"
DOMain 1
set Company "Quintum"
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
ZOne 1
GateWay 1
set Description "Tenor AF Gateway"
set OutgoingIPRouting 1
set UseRoutingTable 1
VoiceCodec 1
set name ""
set CodecVoiceCoding 9
set CodecPayloadSize 20
set ucVar2 0
VoiceCodec 2
set name ""
set CodecVoiceCoding 8
set CodecPayloadSize 20
set ucVar2 0
CodecProfile default
CASSignalingGroup phone
set id "phone"
set SignalingType 3
set FlashhookSignal 1
set ForwardDisconnectDelay 800
set CallerIDGeneration 1
set RXGain -6
set TXGain 0
CASSignalingGroup line
set id "line"
set ORientation 0
set SignalingType 3
set FlashhookSignal 1
set ForwardDisconnectDelay 500
set CallerIDDetection 1
set RXGain 6
set TXGain 0
SIPSignalingGroup 1
set PrimarySIPServer "172.16.250.246"
set AllowOnlyProxyCalls 0
set SipPstnInterworking 1
set UserAgentHeader "Quintum/1.0.0"
change 1 lp 5060
add 5061 ua 102 pu 2001 ppw 2001 c[1] 2001
add 5062 ua 103 pu 2002 ppw 2002 c[1] 2002
H323SignalingGroup 1
TrunkCircuitRoutingGroup line
set id "line"
set EndOfDialDigit #
LineCircuitRoutingGroup phone
set id "phone"
set EndOfDialDigit #
set CallWaiting 1
set HolD 1
set UnattendedTRansfer 1
set AttendedTRansfer 1
FaxProfile 1
set FaxNominalDelay 200
IPRoutingGroup default
set EndOfDialDigit #
set MediaQOSValue b0
set SignalingQOSValue b0
ToneProfile 1
set id "1"
DNChannelMap 1
add 2001 ua 102
add 2002 ch 2 ua 103
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
NumberTable default
set id "default"
add 2001 op 2001
add 2002 op 2002
new NumberTable ToSonus SBC 2000
NumberTable ToSonus SBC 2000
set id "ToSonus SBC 2000"
add 1* op 1*
add 2* op 2*
add 6* op 6*
RoutingTable 1
add LCRG-phone ot UA-101 cdnt NT-ToSonus SBC 2000 dmc cd
GateKeeperParam 1
EndPointAddressDirectory 1
QOSPolicy 1
RouteDirectory 1
StaticRoute 1
set id "1"
table on

ChannelGroup phone
set SignalingGroupAttached CASSignalingGroup-phone
set RoutingGroupAttached LineCircuitRoutingGroup-phone
ChannelGroup line
set SignalingGroupAttached CASSignalingGroup-line
set RoutingGroupAttached TrunkCircuitRoutingGroup-line
CodecProfile default
set VoiceCodecAttached[1] VoiceCodec-1
set VoiceCodecAttached[2] VoiceCodec-2
TrunkCircuitRoutingGroup line
LineCircuitRoutingGroup phone
IPRoutingGroup default
set CodecProfileAttached CodecProfile-default
StaticRoute 1
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
set IPRoutingGroupAttached IPRoutingGroup-default
# DO NOT TOUCH: Integrity Checked!
```

Click here to see the Tenor AF DB file Software Version P107-09-10

```
# /*<-- System Info. Do not overwrite!
# Product: Tenor AF
# IP: 10.0.0.164
# Subnet: 255.255.255.0
# Gateway: 10.0.0.1
# Software: P107-09-10
# Serial Number: A062-999999
# DB: DB_CMS_M14_A018_V12.0.0_121107
# Updated: SAT JUN 25 20:32:46 2011
# -->*/
config
table off
VOIPNetwork 1
SIte 1
TimeServer 1
set UTCOffset 0:00
set PrimaryServerIPAddr 10.0.0.10
set SecondaryServerIPAddr 10.0.2.10
DialPlan 1
set MAXDNlength 30
set MINDNlength 1
set LongDistancePrefix ""
set CarrierPrefixPattern ""
set INTernationaLPrefix[1] ""
set DialPlanCountry 255
set ProgressToneCountry 6
UserProgramDialPlan 1
IPDialPlan default
PRIVateNumberingPlan 1
MasterChassis 1
set Type 6
set DBVersion "DB_CMS_M14_A018_V12.0.0_121107"
set SNMPTrapCommunity "trap community"
IVRFileServer 1
SYSLogServer 1
set id "1"
CDRServer 1
set id "1"
CDRServer 2
set id "2"
set CDRServerPort 9003
new ChannelGroup phone
ChannelGroup phone
NMSServer 1
DNSHosts 1
DNSServer 1
set PrimaryServerIPAddr 10.0.0.10
set SecondaryServerIPAddr 10.0.2.10
RadiusInfo UserServer
set name "User Authentication Server"
RadiusInfo EndpointServer
set name "Endpoint Authorization Server"
RadiusInfo RoutingServer
set name "External Routing Server"
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
DOMain 1
set Company "Quintum"
ZOne 1
GateWay 1
set Description "Tenor AF Gateway"
set OutgoingIPRouting 1
NumberDirectories 1
BypassNumberDirectory 1
set id "1"
HuntLDNDirectory pub1
set id "pub1"
HuntLDNDirectory prv1
set id "prv1"
set LDNType 1
CallerIDXlationDirectory 1
set id "1"
InboundDNISXlationDirectory 1
set id "1"
HopoffNumberDirectory 1
set id "1"
VoiceCodec 1
set name "G711A"
set CodecVoiceCoding 8
set CodecPayloadSize 20
set ucVar2 0
VoiceCodec 2
set name "G711U"
set CodecVoiceCoding 9
set CodecPayloadSize 20
set ucVar2 0
CodecProfile default
CASSignalingGroup phone
set id "phone"
set SignalingType 3
set ForwardDisconnectDelay 800
set CallerIDGeneration 1
set RXGain -6
set TXGain 0
CASSignalingGroup line
set id "line"
set ORientation 0
set ForwardDisconnectDelay 500
set RXGain 6
set TXGain 0
SIPSignalingGroup 1
set PrimarySIPServer "172.23.197.30"
set AllowOnlyProxyCalls 0
set UserAgentHeader "Quintum/1.0.0"
change 1 lp 5060 pu 200829 ppw 200829 c[1] 200829
add 5061 ua 102 pu 200827 ppw 200827 c[1] 200827
H323SignalingGroup 1
TrunkCircuitRoutingGroup line
set id "line"
set EndOfDialDigit #
LineCircuitRoutingGroup phone
set id "phone"
set EndOfDialDigit #
set ModemBypass 1
FaxProfile 1
set FaxNominalDelay 200
IPRoutingGroup default
set EndOfDialDigit #
set MediaQOSValue b0
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
set FaxRelay 3
set SignalingQOSValue b0
ToneProfile 1
set id "1"
DNChannelMap 1
add 200829 ua 101
add 200827 ch 2 ua 102
GateKeeperParam 1
EndPointAddressDirectory 1
QOSPolicy 1
RouteDirectory 1
StaticRoute 1
set id "1"
table on

ChannelGroup phone
set SignalingGroupAttached CASSignalingGroup-phone
set RoutingGroupAttached LineCircuitRoutingGroup-phone
CodecProfile default
set VoiceCodecAttached[1] VoiceCodec-1
set VoiceCodecAttached[2] VoiceCodec-2
TrunkCircuitRoutingGroup line
set HopoffNumberDirAttached[1] HopoffNumberDirectory-1
LineCircuitRoutingGroup phone
set BypassNumberDirAttached[1] BypassNumberDirectory-1
set PUBHuntLdnDirAttached[1] HuntLDNDirectory-pub1
set PRIVHuntLdnDirAttached[1] HuntLDNDirectory-prv1
IPRoutingGroup default
set CodecProfileAttached CodecProfile-default
set IPDialPlanAttached IPDialPlan-default
StaticRoute 1
```

Copyright © 2015 Sonus Networks. All rights reserved.

```
set IPRoutingGroupAttached IPRoutingGroup-default
# DO NOT TOUCH: Integrity Checked!
```

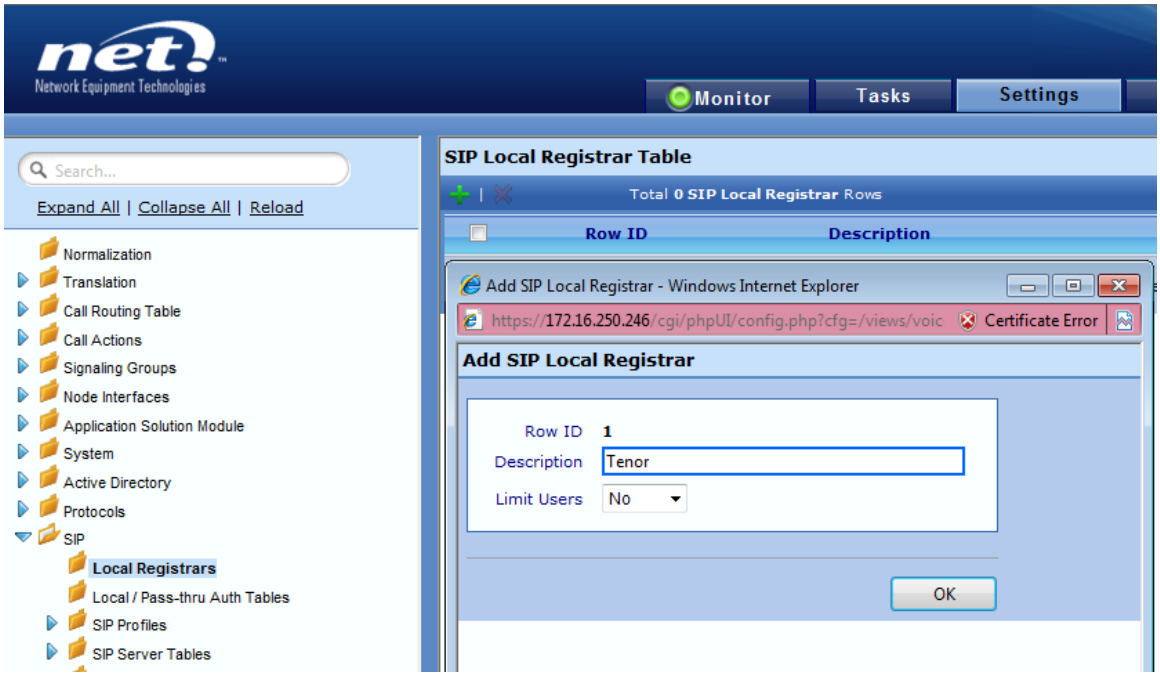
Sonus SBC 1000/2000 configuration

Requirements and Prerequisites

- This document assumes that Sonus SBC 1000/2000 Lync 2010 wizard was ran prior to the configuration
- Running the Lync 2010 wizard will ensure SRTP towards Lync is set to Required
- Media bypass must be enabled in Lync

SIP Registrar Table

- Browse to Sonus SBC 1000/2000 2000 WebUI > Settings Tab > SIP / Local Registrars (in left pane)
- Click on Add button and add a SIP Local Registrar Entry as shown below



Media List Configuration

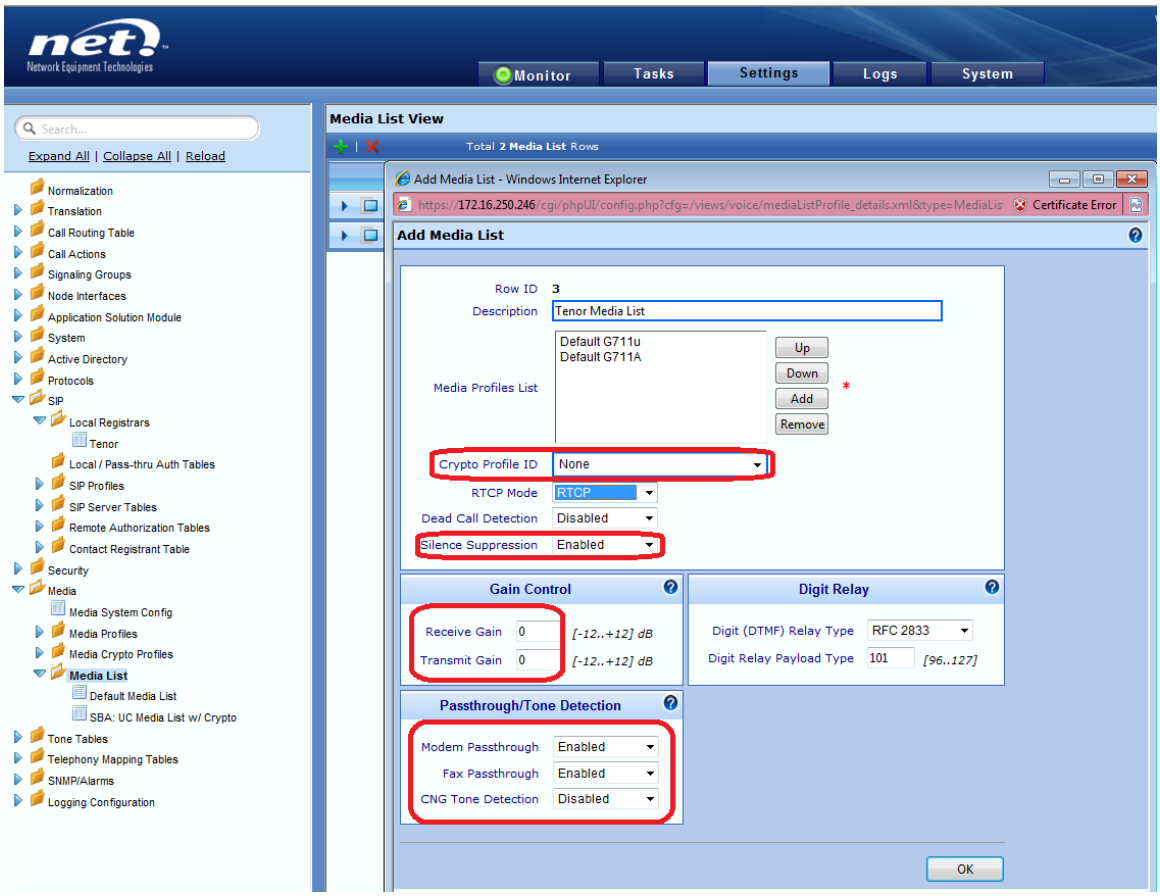
- Browse to Sonus SBC 1000/2000 2000 WebUI > Settings Tab > Media List (in left pane)
- Click on Add button and add a Media List Entry as shown below

Make sure to have following settings are configured in Tenor Media List:

CNG	Disabled
Fax passthru	Enabled
Modem Passthru	Enabled

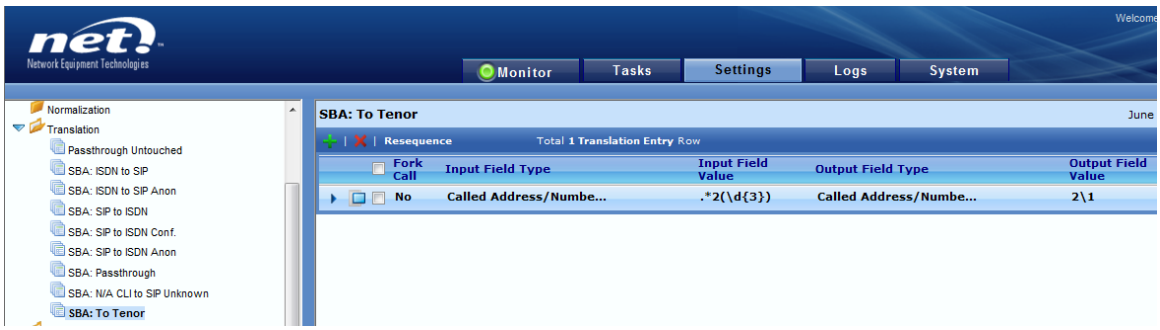
Copyright © 2015 Sonus Networks. All rights reserved.

Silence Suppression	Enabled
Rx/Tx Gain	0



Translation Table

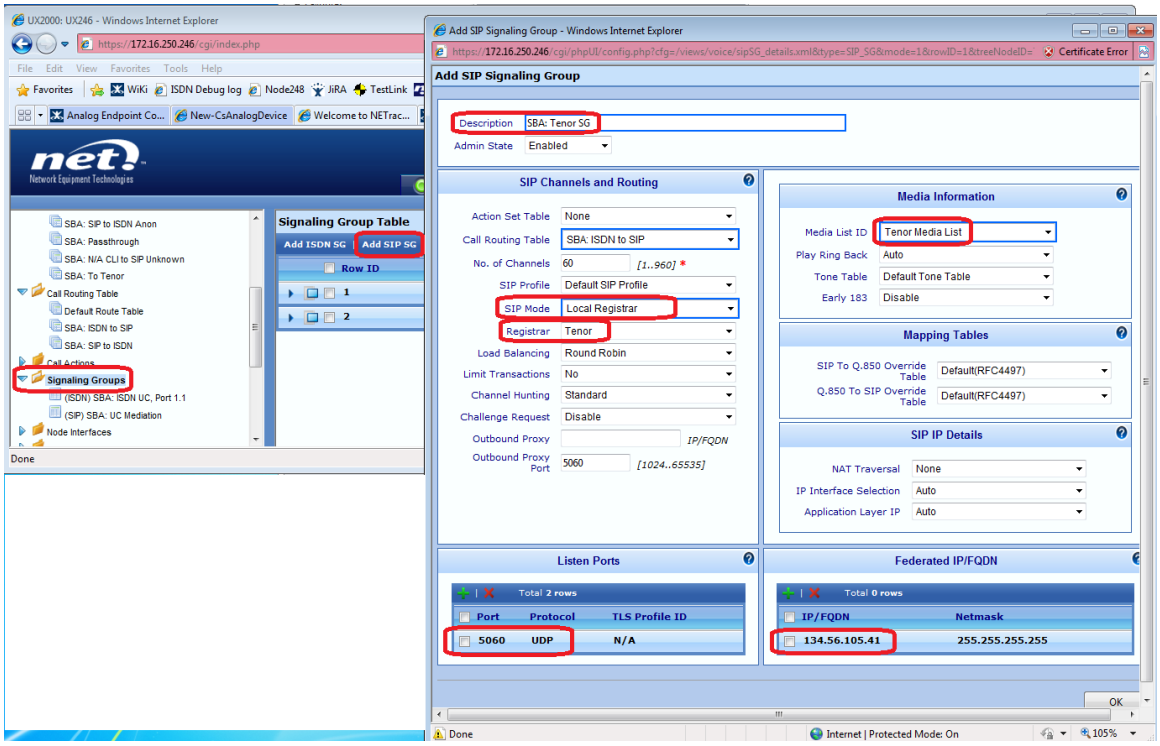
- Browse to Sonus SBC 1000/2000 2000 WebUI > Settings Tab > Translation (in left pane)
- Click on Add button and add a Translation Table with following entry as shown below



Signaling Group (uses UDP only)

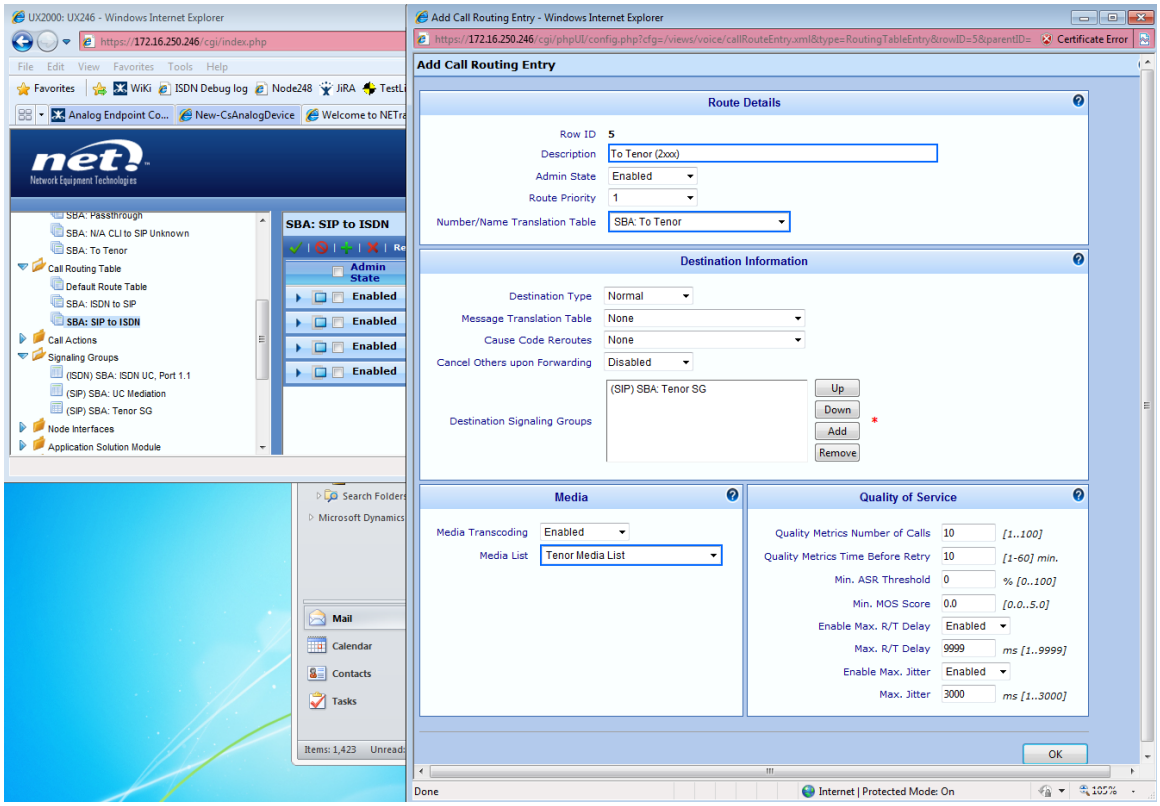
- Browse to Sonus SBC 1000/2000 2000 WebUI > Settings Tab > Signaling Groups (in left pane)
- Click on Add SIP SG button and add a SIP Signaling Group for Tenor Device connectivity as shown below

Copyright © 2015 Sonus Networks. All rights reserved.



Call Routing Table

- Browse to Sonus SBC 1000/2000 2000 WebUI > Settings Tab > Call Routing Table (in left pane)
- Click on **SIP to ISDN** Call Route Table and hit Add ⊕ button to add an entry to route calls to Tenor (for those with 2xxx extension in this example)



Copyright © 2015 Sonus Networks. All rights reserved.

- Re-sequence the Call Route entries in this table to make sure that calls to 2xxx extensions (Analog Endpoints) will use the entry that you just created in previous step



Troubleshooting Techniques

Troubleshooting FAX Calls Between the Tenor and PSTN

- If you are getting comm errors on the Fax machine, check the following resources for solutions:
  - comm error 350 - disable ECM
  - error codes 242,346,321,344,388,283 - The first 2 settings you want to change are the error correction (ECM) and v.34 these are on by default you would want these off.
- If faxes are failing, check the E1 port counters for slips and frame errors.
  - Click here to see a screenshot of a *bad* E1 line

Copyright © 2015 Sonus Networks. All rights reserved.



- The frame errors and the slips counters must **not**be increasing. You can check if they are increasing by resetting the counters. If the errors are increasing, the issue could be caused by one of the following:
  - System timing / clocking. Check the clock source (System -> System Timing) - it should be set to Network/T1/E1 port and not System/Free run. If the clock source is set to Network, but the Current Active Clock shows as Free run, click Apply and ensure that Current Active Clock is now set to Primary. This should resolve the clocking issue as long as the error counters do not increase.
  - If the Tenor is not configured to register with the Sonus SBC 1000/2000 local SIP registrar and the SIP Signaling group in Sonus SBC 1000/2000 constantly goes down, check the contents of the **var_config.cfg** file (from Tenor Config Manager -> Tools -> Var_config -> Edit) and delete the line specifying the transport protocol as in P108 it is obsolete.
  - Bad E1 cable. Replace the cable.

Copyright © 2015 Sonus Networks. All rights reserved.

- Faulty RJ45 jacks. Replace the cable or fix the Rj45 jacks.
- Faulty RJ45 socket. Try configuring a different T1/E1 port. Visually check the pins in the E1/T1 ports for any differences.

Configuring Valcom For Use With Tenor

This article describes the configuration of Valcom.

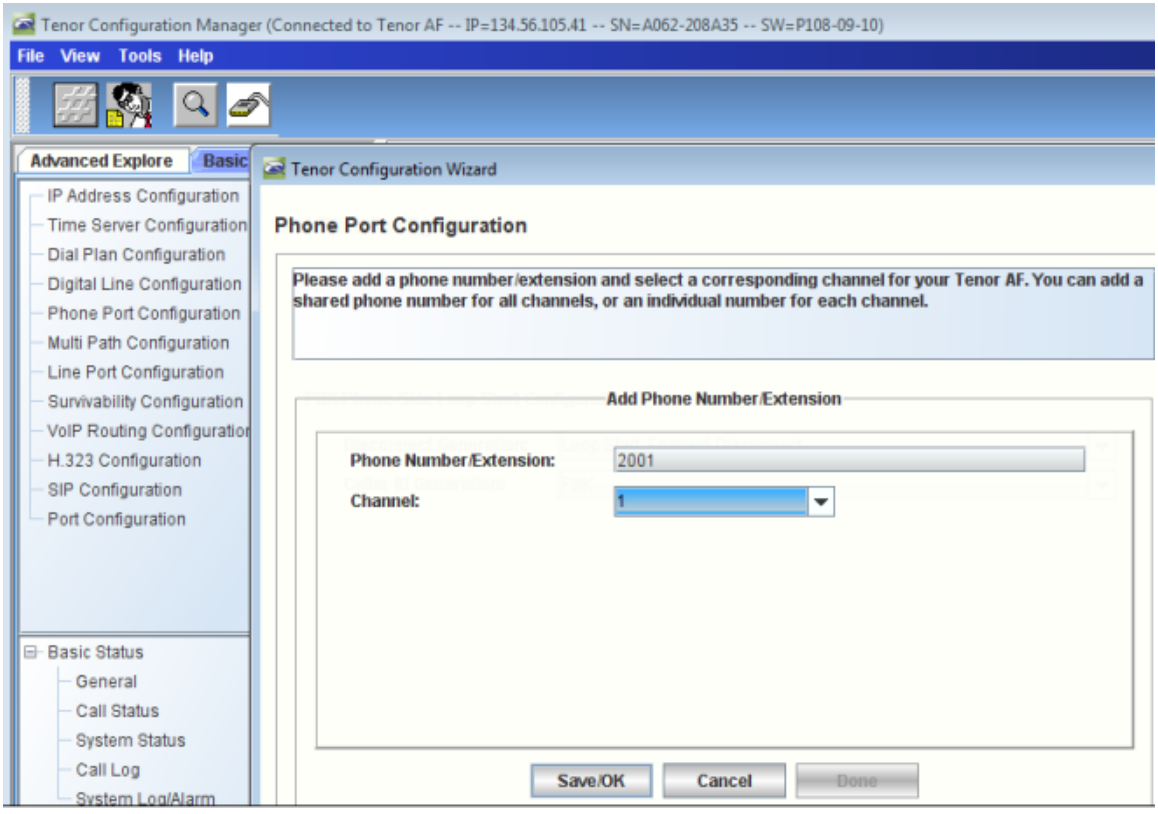
On Using a Tenor as an Analog Device in a Lync UX SBA Deployment page we described the analog endpoints configuration for Lync - SBC1(or 2) K - Tenor setup. If Valcom paging devices are desired to be used as the analog endpoints, further configuration is needed on Valcom side.

Let's remember the analog endpoint creation on Lync and Tenor first!

For the Lync analog endpoint configuration, an analog endpoint had to be created using the Lync Management Shell as:

```
New-CsAnalogDevice -LineUri tel:+15102462001 -DisplayName "Analogph1" -RegistrarPool
cspool.uxdemo.net -AnalogFax $false -Gateway
ux246.uxdemo.net -OU "ou=Analog,dc=uxdemo,dc=net"
```

and on Tenor point of view, we had to configure the relevant endpoint as shown below (for further steps on Tenor side configuration please refer to Using a Tenor as an Analog Device in a Lync UX SBA Deployment) :



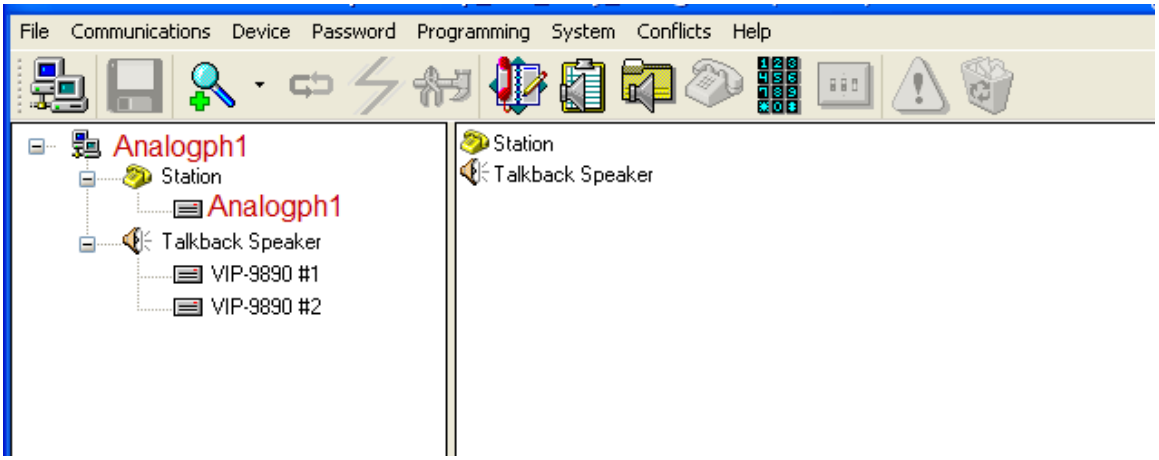
If we need the actual analog endpoints as Valcom paging devices, following steps has to be completed on Valcom side.

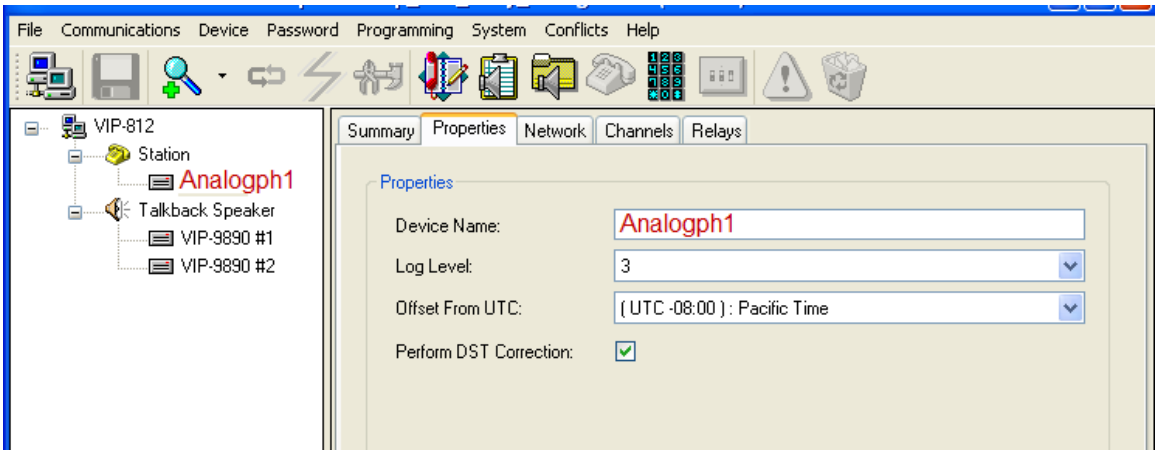
Launch the Valcom IP Solution Setup Tool and connect to the paging device as shown below (for further details of

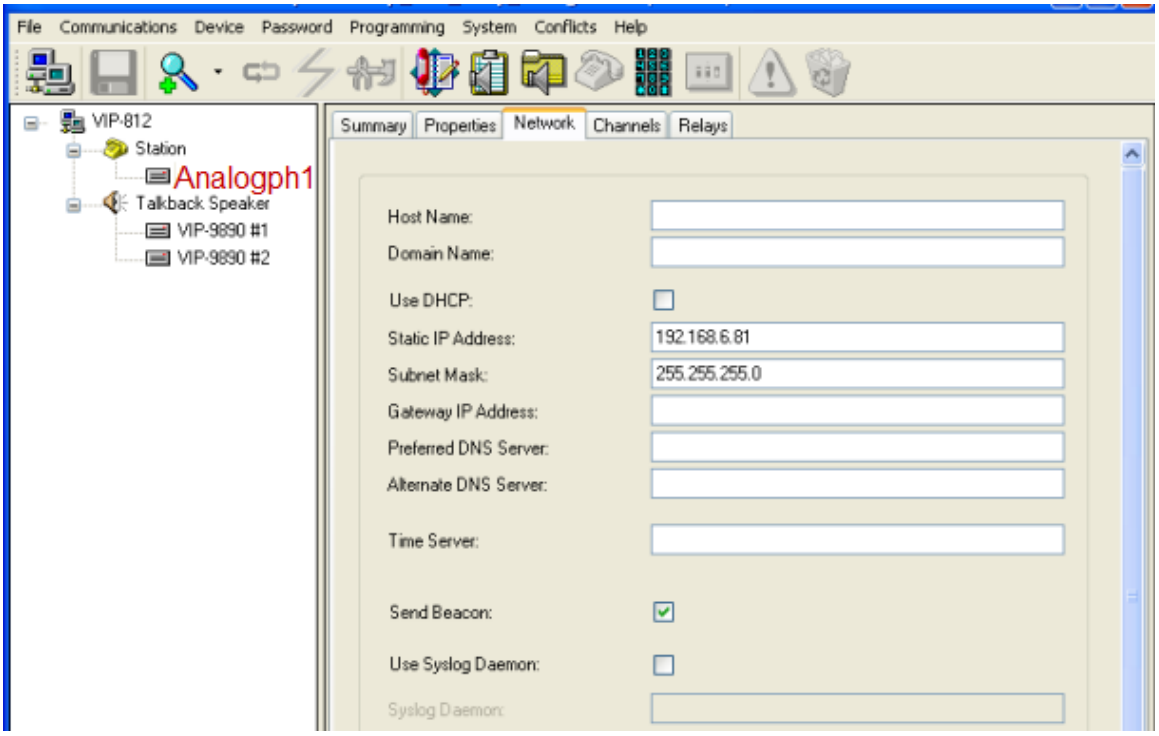
Copyright © 2015 Sonus Networks. All rights reserved.

Valcom IP Solution Setup Tool manual):

Configure desired name and IP address for your device as shown below:

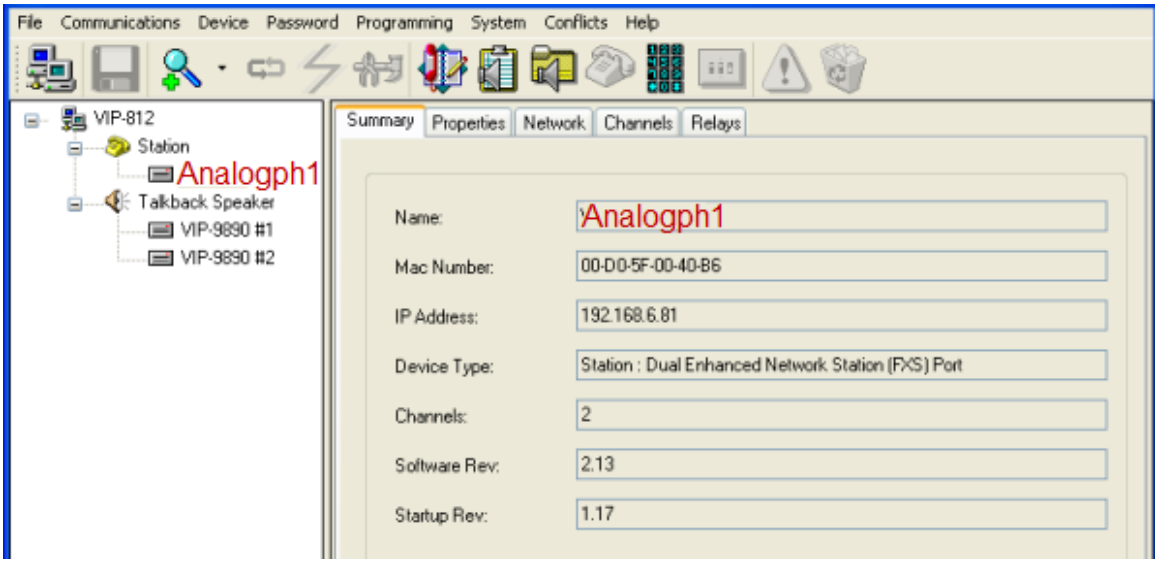




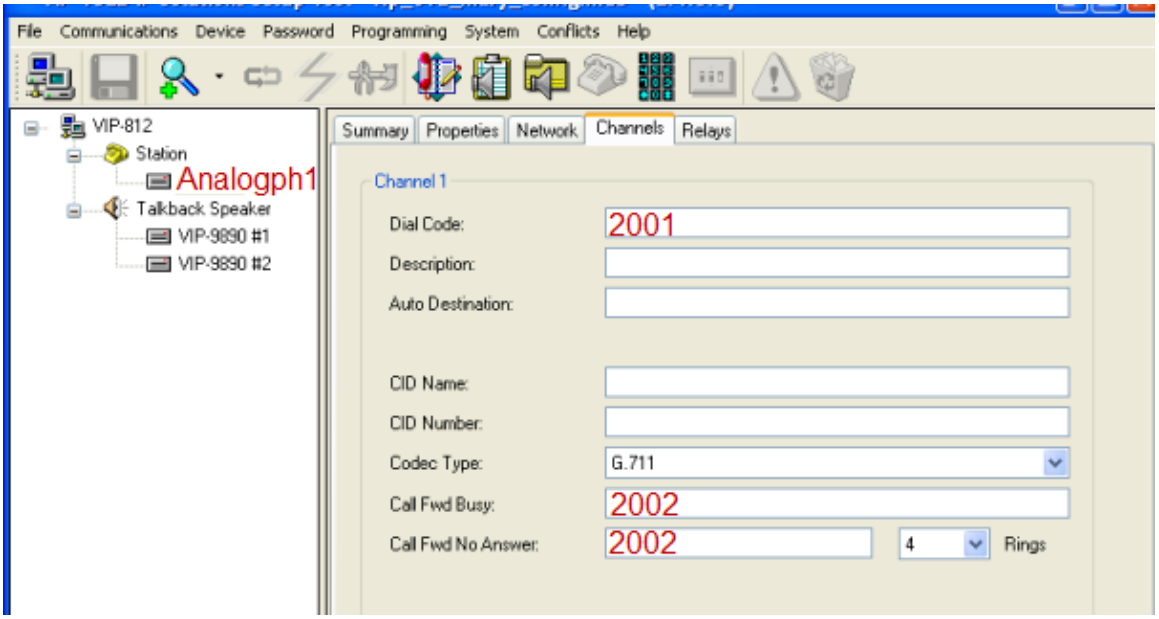


Copyright © 2015 Sonus Networks. All rights reserved.

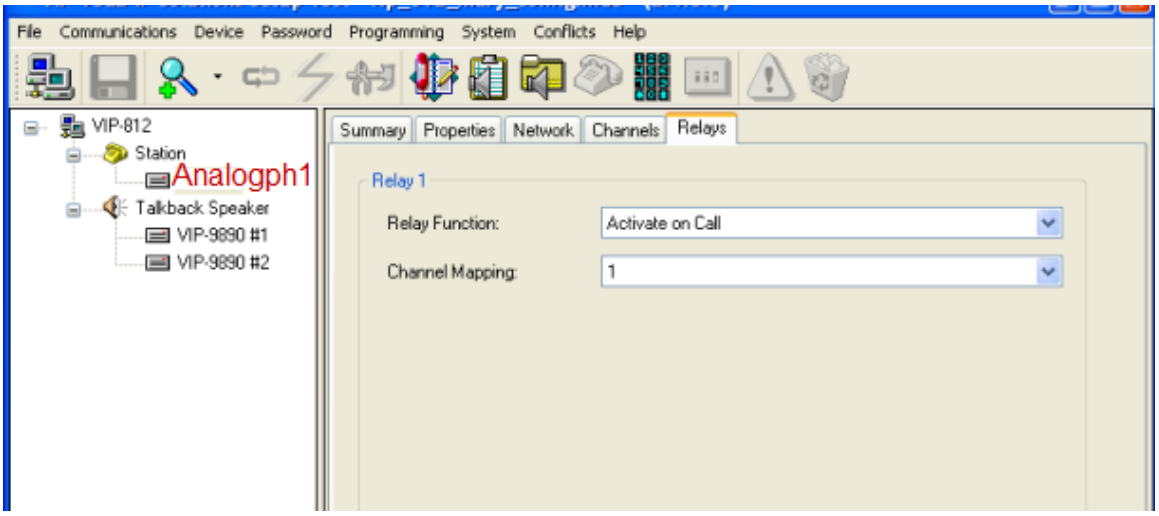
Following depicts the Properties of the device:



Now configure the dial code (extension number) for your endpoint as shown below:



Copyright © 2015 Sonus Networks. All rights reserved.



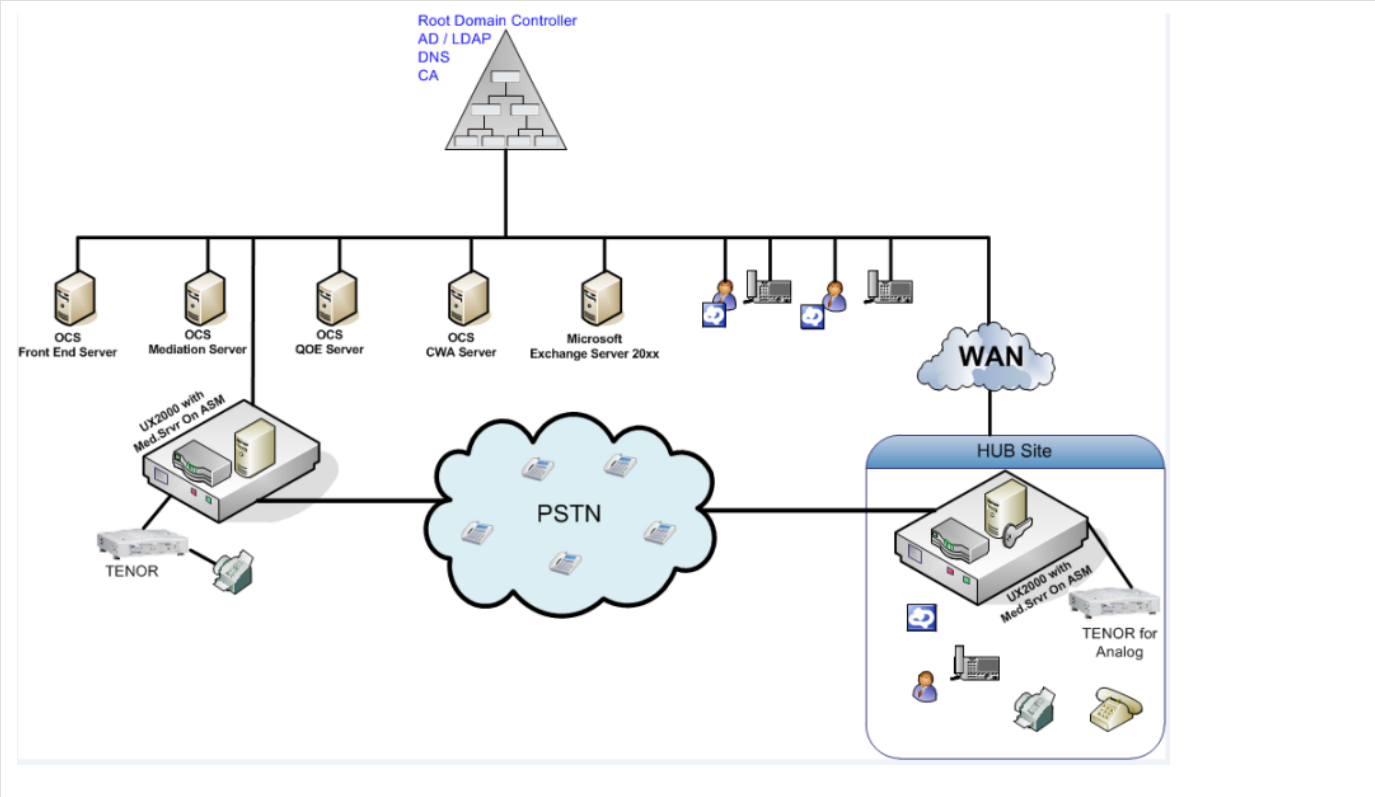
Deploying the Sonus SBC 1000-2000 with OCS2007 R2 using the ASM as a Mediation Server

This article describes how to configure an Application Solution Module (ASM) on a Sonus SBC 1000/2000 as an OCS2007 R2 Mediation Server deployable in a **PSTN - Sonus SBC 1000/2000 - Microsoft Office Communication Server 2007 R2** topology. This solution provides you with an integrated gateway and mediation server that resides between the PSTN and the OCS servers on the enterprise network:

- High-Level Configuration Overview
- Configuration
  - ASM Tasks
  - OCS Tasks
  - Sonus SBC 1000/2000 Gateway Tasks

Topology

Copyright © 2015 Sonus Networks. All rights reserved.



High-Level Configuration Overview

For this particular deployment, we'll need to configure three devices:

1. Application Solution Module (ASM)
2. The OCS Server
3. The Sonus SBC 1000/2000 Gateway

Below is an outline of each device's high-level configuration steps:

#ASM Tasks

1. Load a New ASM image without the Lync SBA.
   ✅ For Lync SBA Deployments, please see Deploying the Survivable Branch Appliance
2. Re-initialize the ASM.
3. Configure the ASM and DNS IP Addresses
4. Enable Remote Desktop connectivity.

#OCS Tasks

1. Connect to the ASM using Remote Desktop.
2. Set the host name and join the OCS domain.
3. Add the Active Directory Domain Services (ADDS) role to enable AD Domain Controller tools along with:
   - .Net Framework 3.5 SP1
   - Desktop Experience
   - Telnet Cli
4. Update Windows.
5. Install Visual C++ Redistributable.
6. Install the Mediation Server application.

#Sonus SBC 1000/2000 Gateway Tasks

Copyright © 2015 Sonus Networks. All rights reserved.

Asusming that Sonus SBC 1000/2000 gateway's IP address, host name information is already configured on the unit, the following steps should be performed to integrate the Sonus SBC 1000/2000 gateway with Microsoft OCS 2007 R2 Mediation Server:

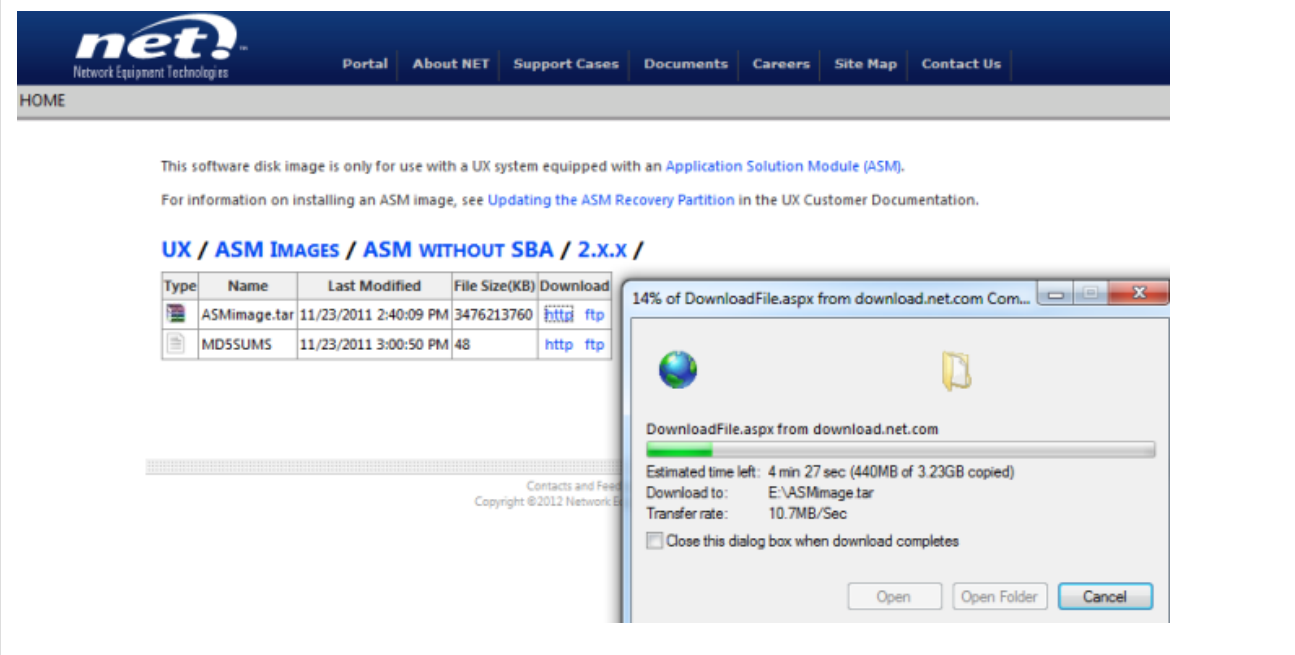
1. Ensure to have the necessary license on the Sonus SBC 1000/2000
2. Run the OCS 2007 Setup task
3. Connect the PRI cable to the relevant ISDN port to allow PSTN - Sonus SBC 1000/2000 connection

Configuration

ASM Tasks

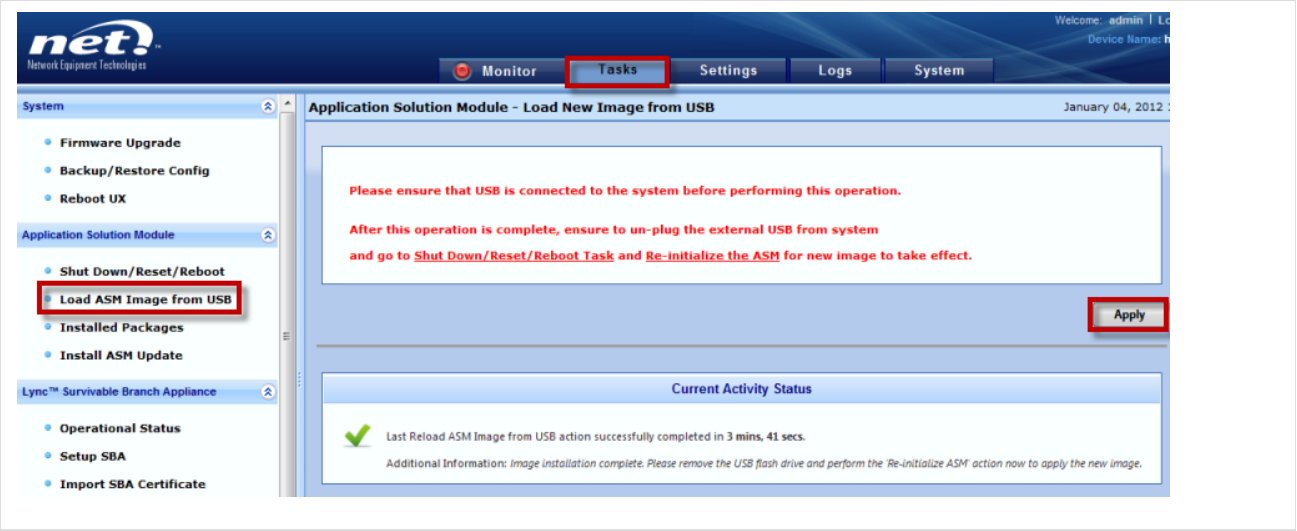
Load ASM Image from USB

1. Download the latest ASM image (without SBA) from the Sonus SBC 1000-2000 Download Center into a USB flash drive as shown below:
   For the details please refer to Updating the ASM Recovery Partition.



2. Insert the prepared flash drive into one of the ASM USB ports of the Sonus SBC 1000/2000 system
3. Launch WebUI and browse to > Task (tab) > Application Solution Module (in left pane) > Load ASM Image from USB and hit Apply (in right pane)

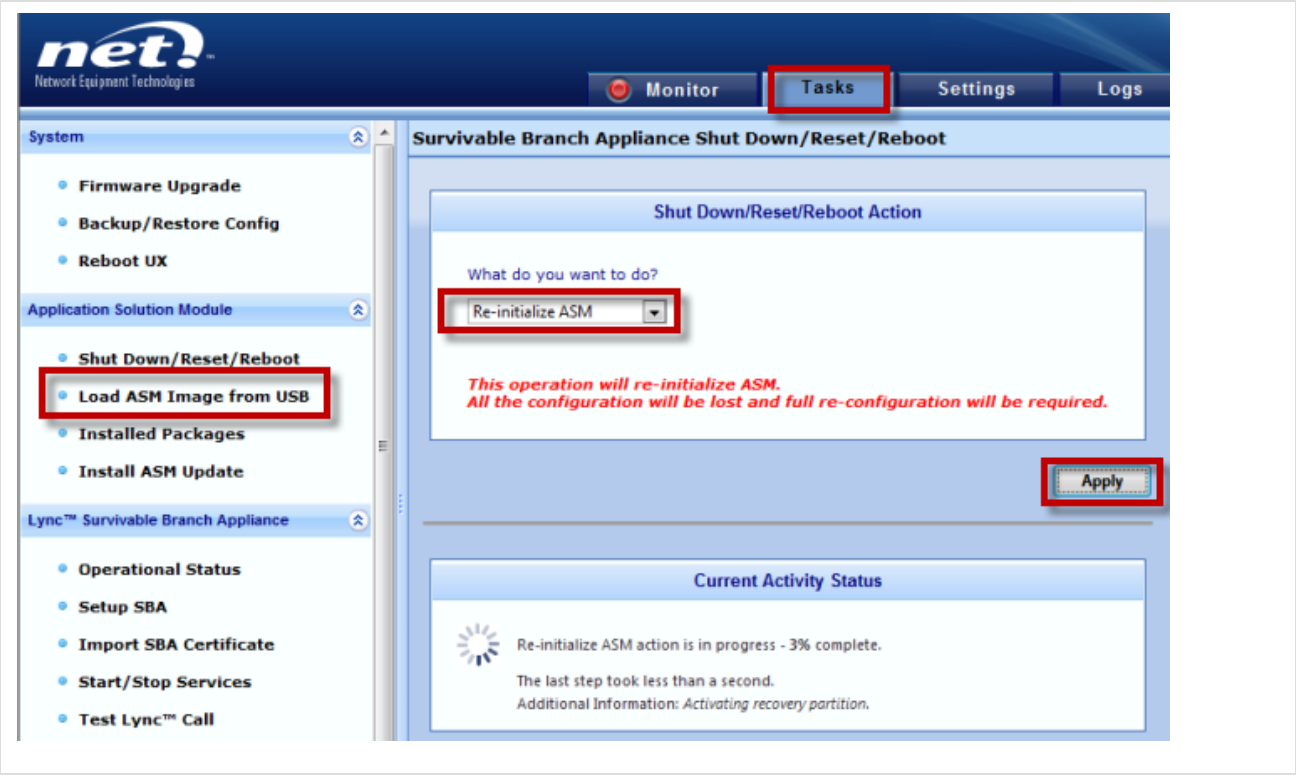
Copyright © 2015 Sonus Networks. All rights reserved.



4. Upon task completion, follow the instructions on the display and:
    - Unplug the external USB from system
    - Follow the next step to re-initialize the ASM for new image to take effect

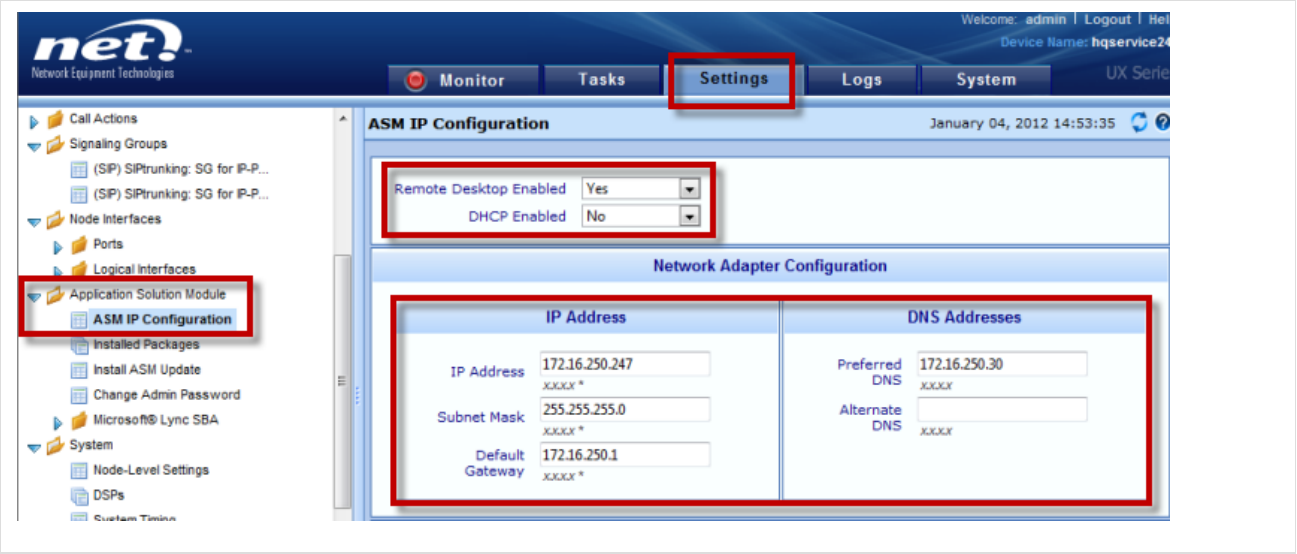
Re-initializing ASM

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, under the **Application Solution Module**, click **Shut Down/Reset/Reboot**.
3. Select **Re-initialize ASM**from the dropdown menu and hit Apply:

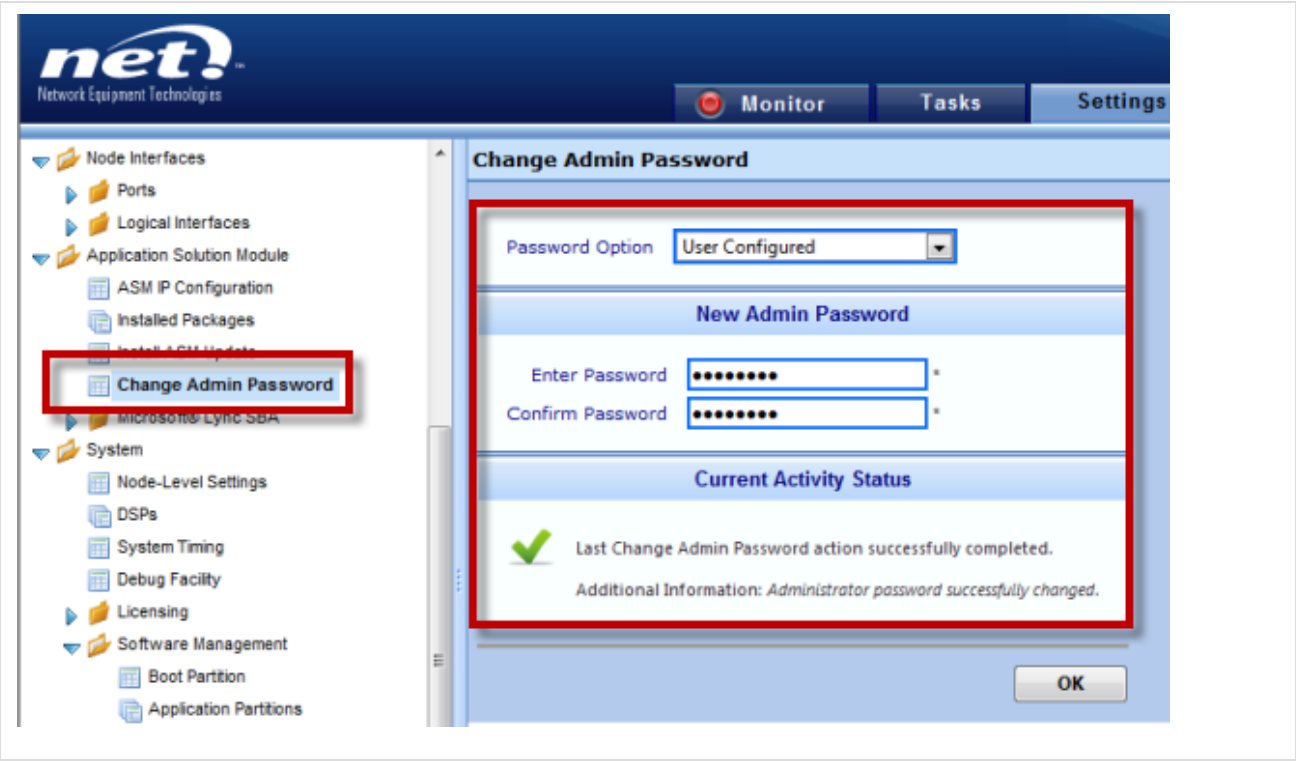


4. Upon completion, verify that the ASM IP address is configured and Remote Desktop is enabled as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



5. Ensure to change the ASM admin password to something you'll remember because the next steps will require you to login remotely to ASM for the Mediation Server installation:



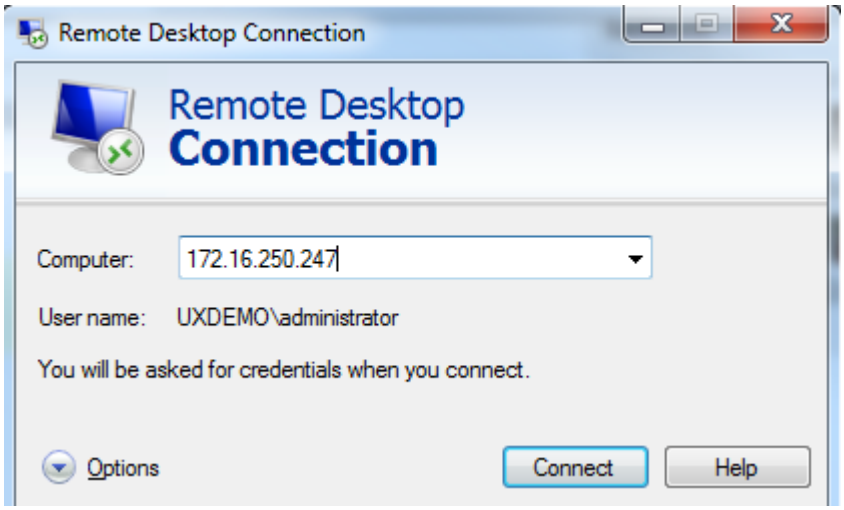
OCS Tasks

Domain Join

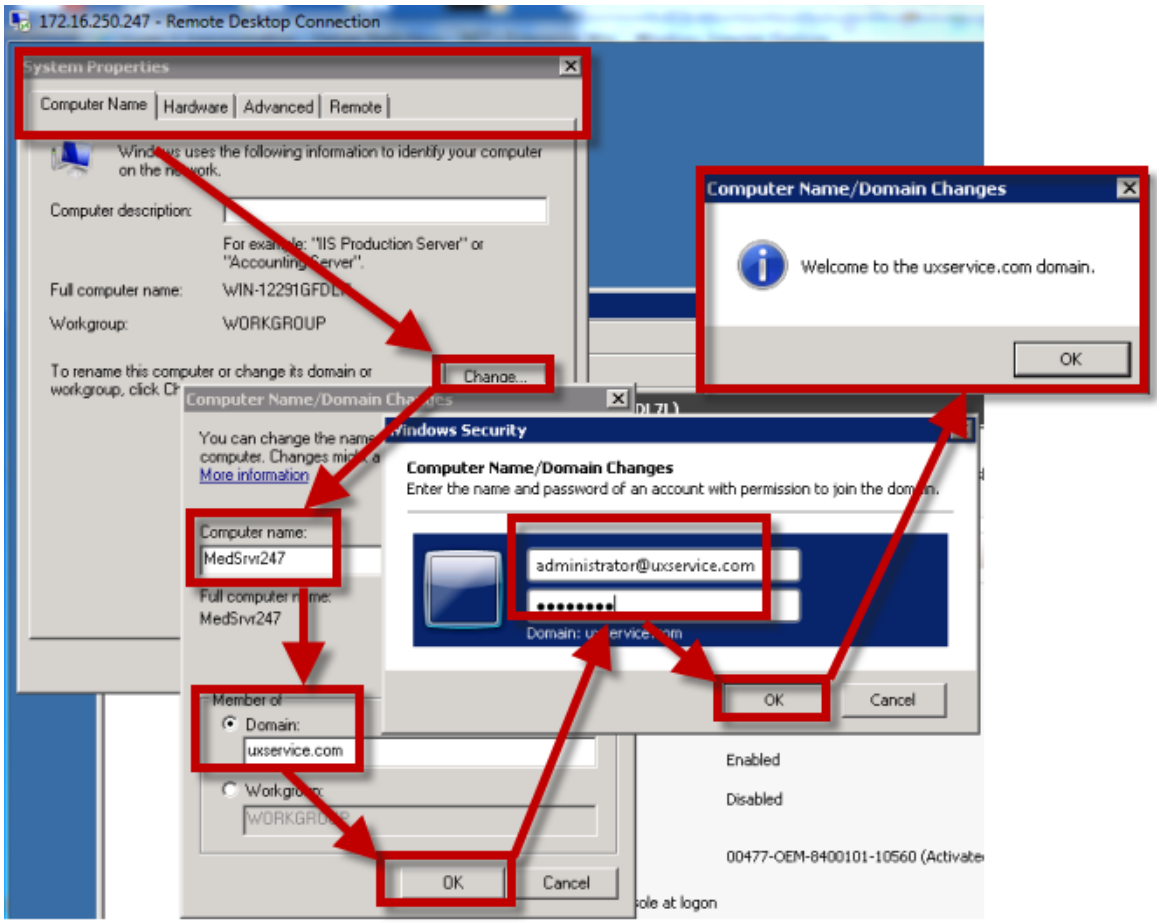
As part of the Microsoft OCS 2007 R2 deployment requirements, every OCS Server must be domain joined. For further details about the OCS 2007 R2 deployment, please refer to Microsoft Documents.

1. To join to domain, Remote Desktop to the ASM:

Copyright © 2015 Sonus Networks. All rights reserved.

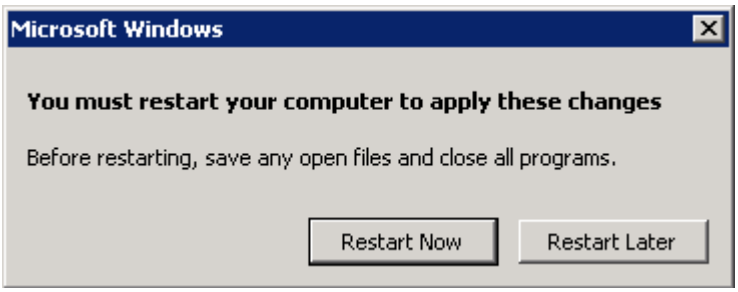


2. Change the host name and join to OCS domain:



3. Restart the ASM as prompted after successful join to domain as shown below:

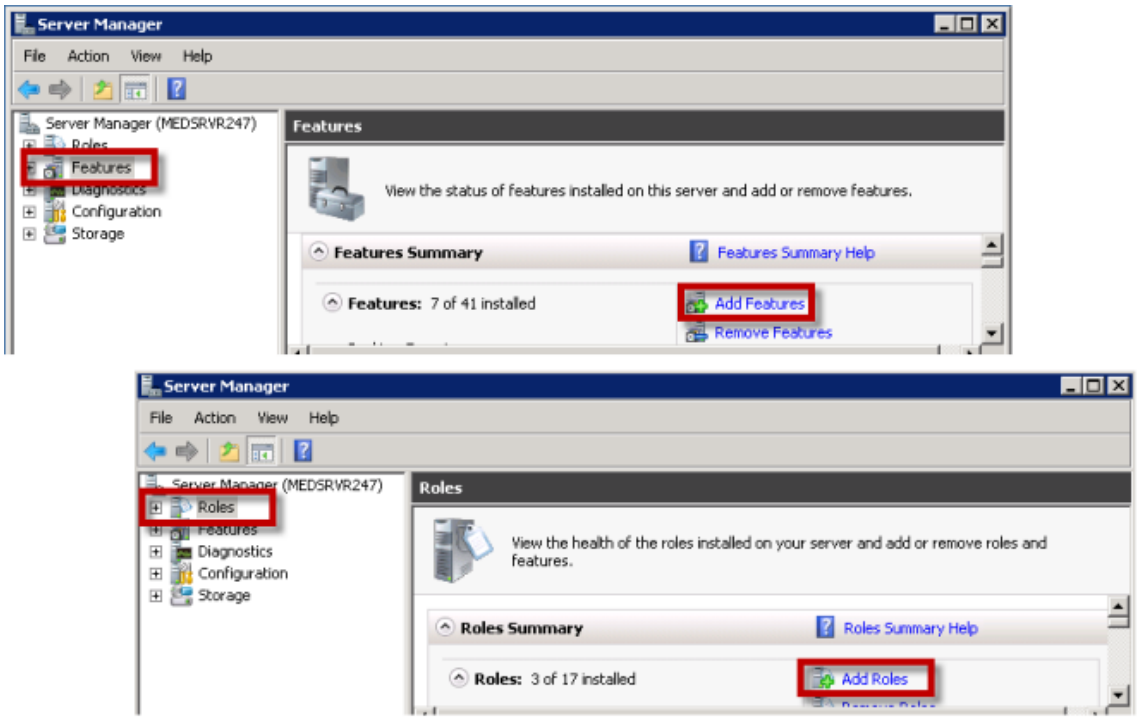
Copyright © 2015 Sonus Networks. All rights reserved.



Mediation Server Prerequisites

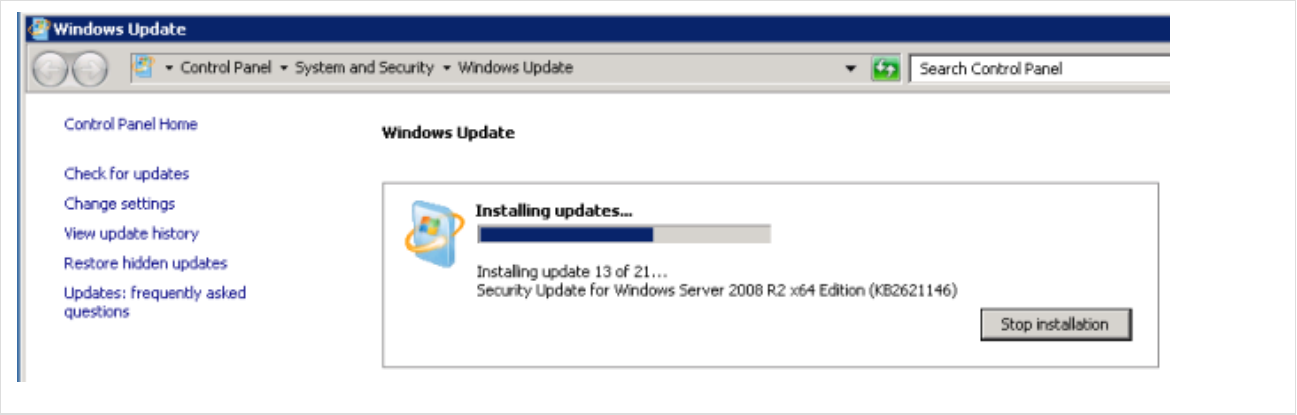
Microsoft OCS 2007 R2 Mediation Server installation requires Several Roles and Features installation on the server PC. For further details, please refer to Microsoft Documents.

1. Remote Desktop to the ASM using the OCS installer privileges.
   Note: In this example we are using domain administrator account.
2. Install the Active Directory Domain Services (ADDS) **role**using the Server Manager as shown below:



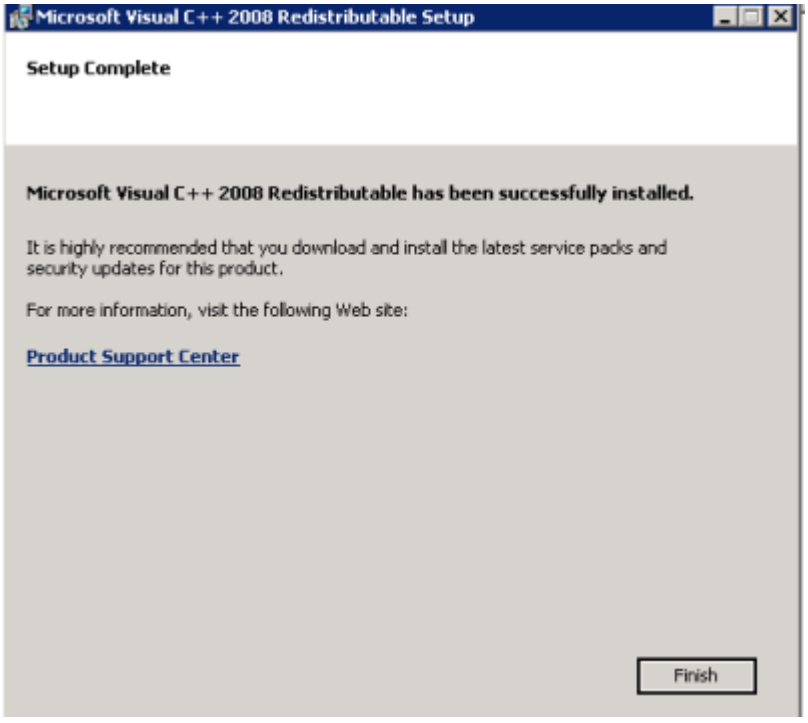
3. Upon completion, restart the ASM as prompted and relogin using the OCS installer privileges once again.
4. Run Windows Update until everything is updated.

Copyright © 2015 Sonus Networks. All rights reserved.



5. Up on completion, restart the ASM as prompted and relogin using the OCS installer privileges.
6. Download Visual C++ Redistributable 2008 (x64) from MS downloadsand install it.

> OCS 2007 R2 Mediation Server installation requires Visual C++ Redistributable 2008 already installed before the Mediation Server deployment. As a matter of fact, Microsoft OCS 2007 R2 installation CD contains the 32 bit executable in its support folder, and this version is a sufficient prerequisite on Windows 2003 R2 and Windows 2008 R2 Operating Systems. However, **Sonus SBC 1000/2000 ASM System Release 2.0** base image is Windows 2008 R2 with **Service Pack 1**; and if the 32 bit version of the VC++ Redistributable 2008 is installed on Windows 2008 R2 with Service Pack 1, the Mediation Server bits installation attempt **fails** since the SP 1 does further check on the prerequisites and expects the **64 bit VC++ 2008 Redistributable** package installed.

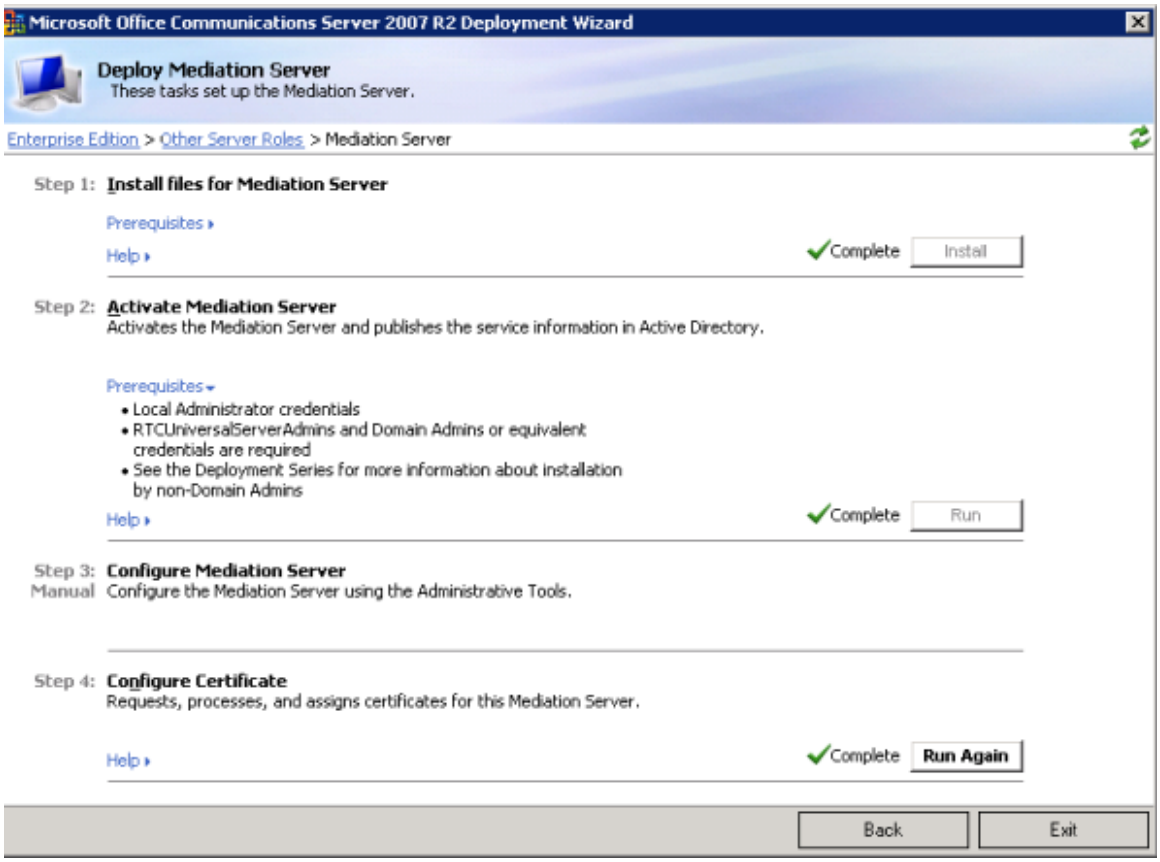


Mediation Server Installation

1. Run Microsoft Office Communications Server 2007 R2 Deployment Wizard
2. Install and Run the the following steps in Enterprise Edition > Other Server Roles > Mediation Server in the wizard:
   - Step 1: Install files for Mediation Server
   - Step 2: Activate Mediation Server

Copyright © 2015 Sonus Networks. All rights reserved.

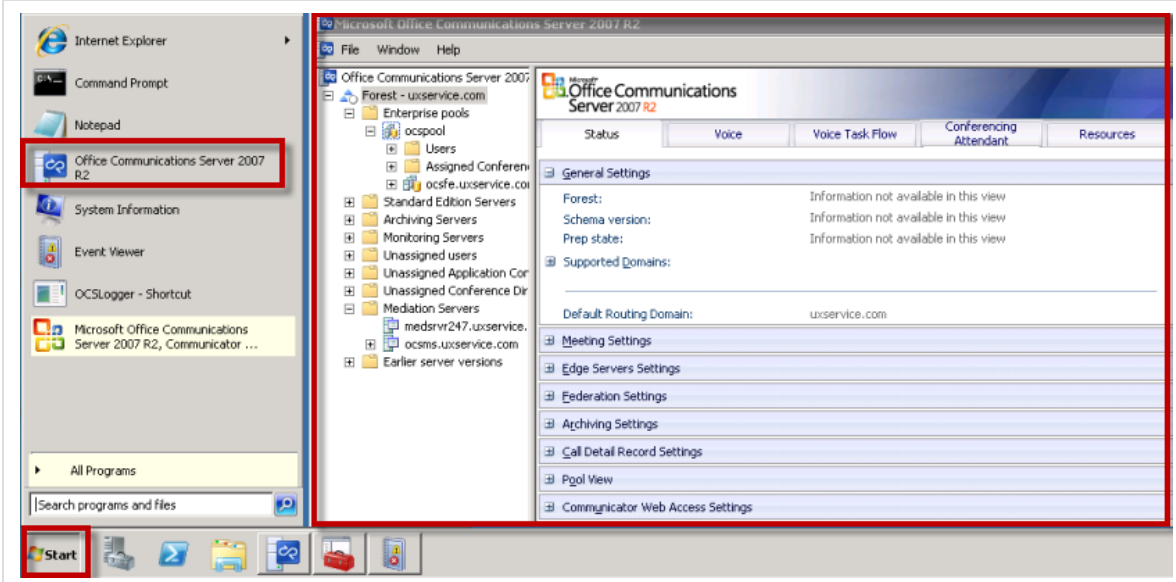
- Step 4: Configure Certificates



OCS Voice Properties Configuration

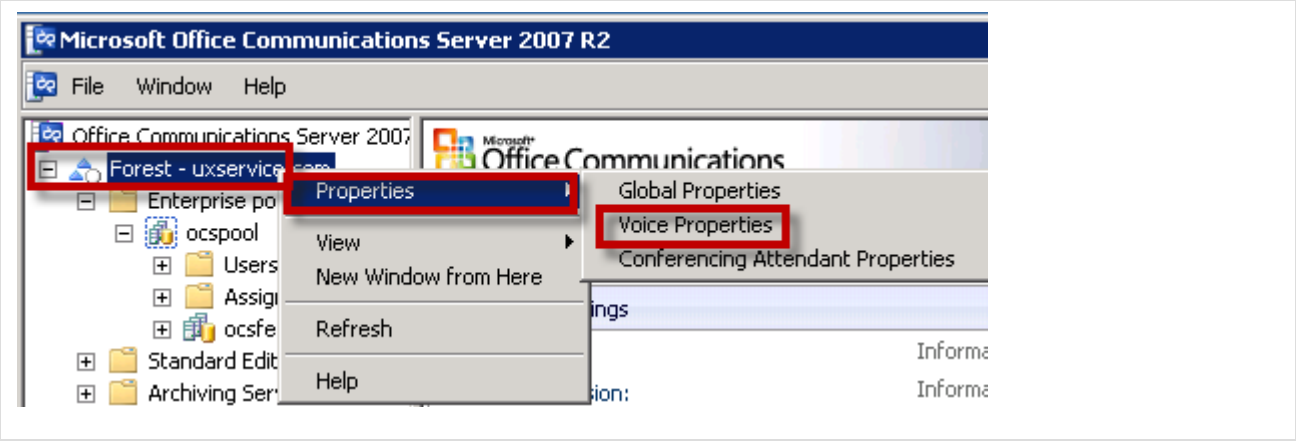
On the OCS Front End Server:

1. Login with OCS administrator privileges
2. Launch **Microsoft Office Communications Server 2007 R2 configuration snap-in**:

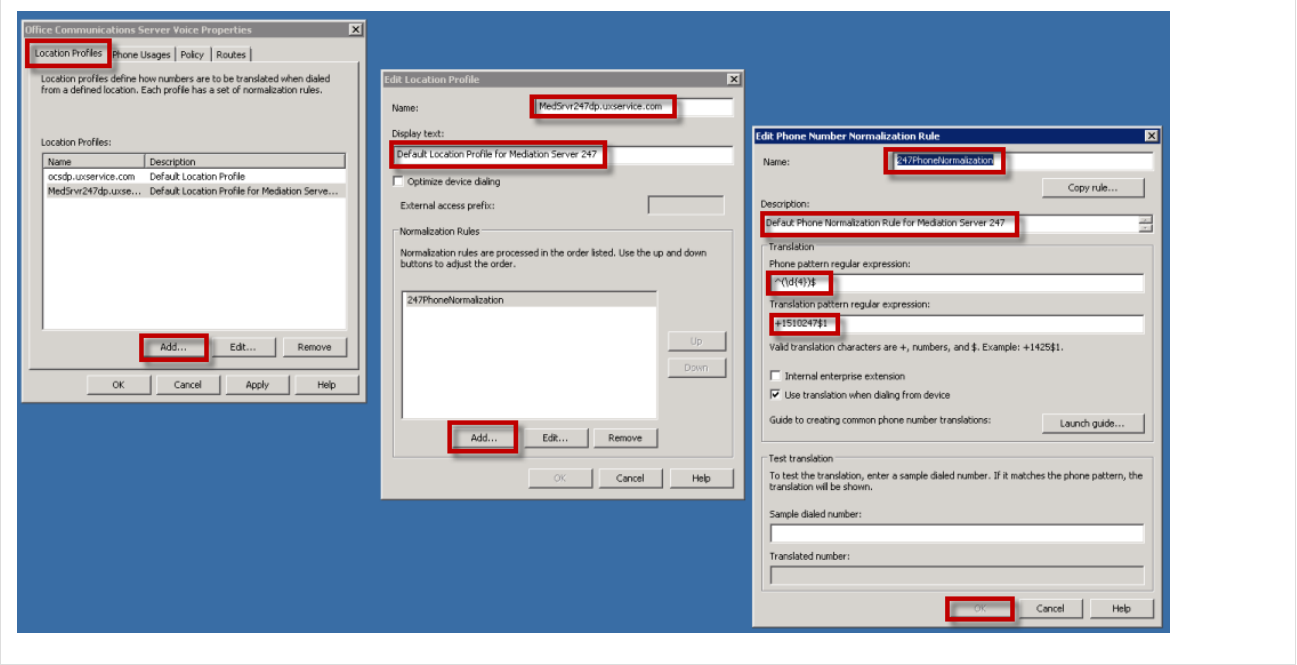


Copyright © 2015 Sonus Networks. All rights reserved.

3. Launch Voice Properties as shown below:

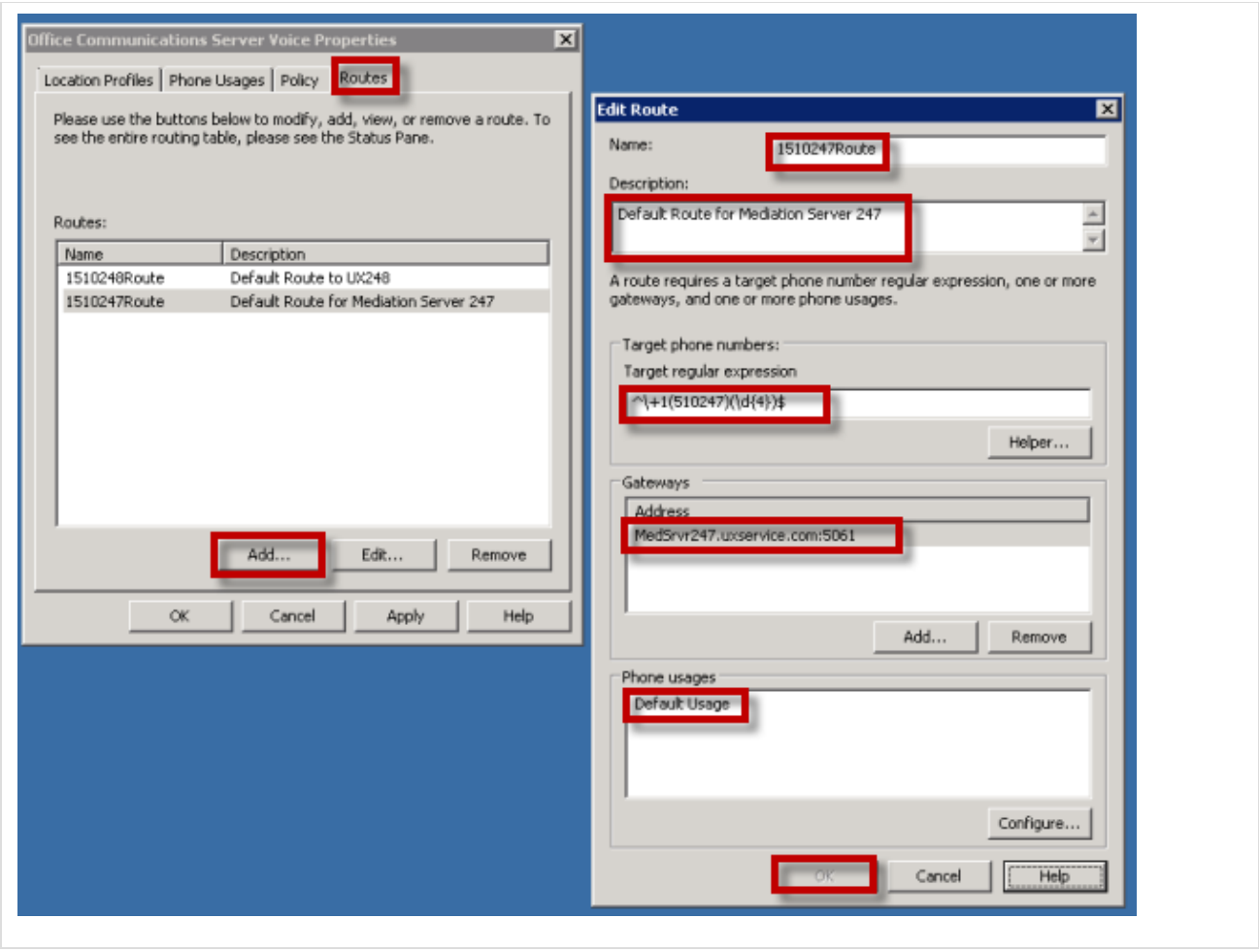


4. Add a new **Location Profile**as shown below with desired number normalization:

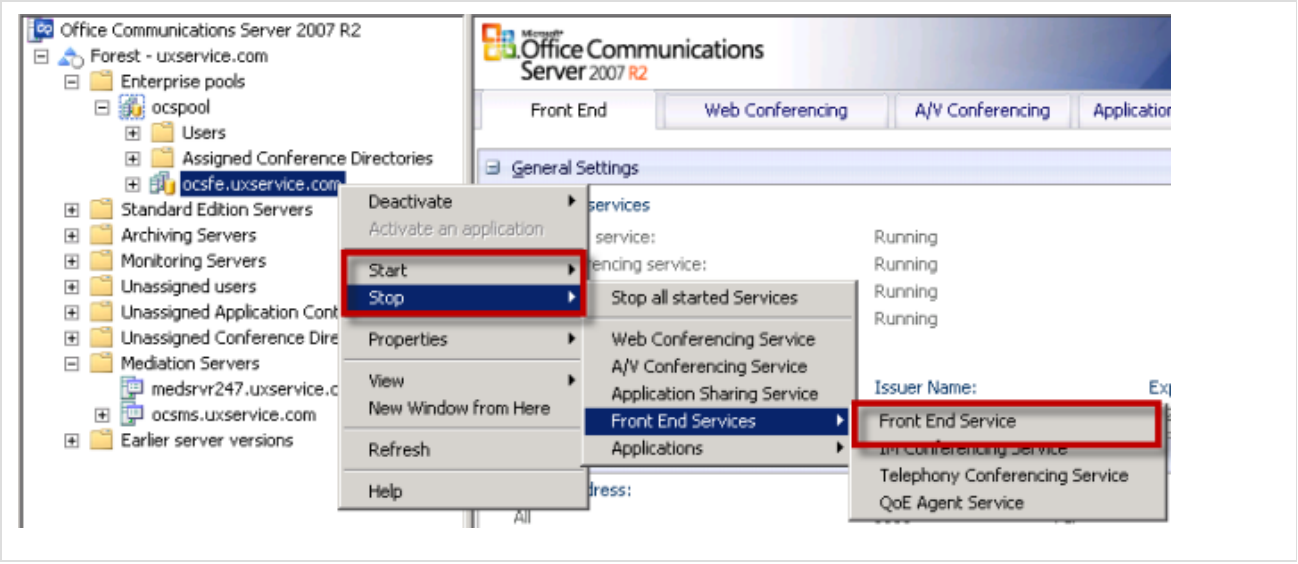


5. Add a new **Route**and ensure to have the correct Mediation Server selected in the Gateways field, along with the other marked fields as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



6. Close the Voice Properties and stop & start the Front End Server



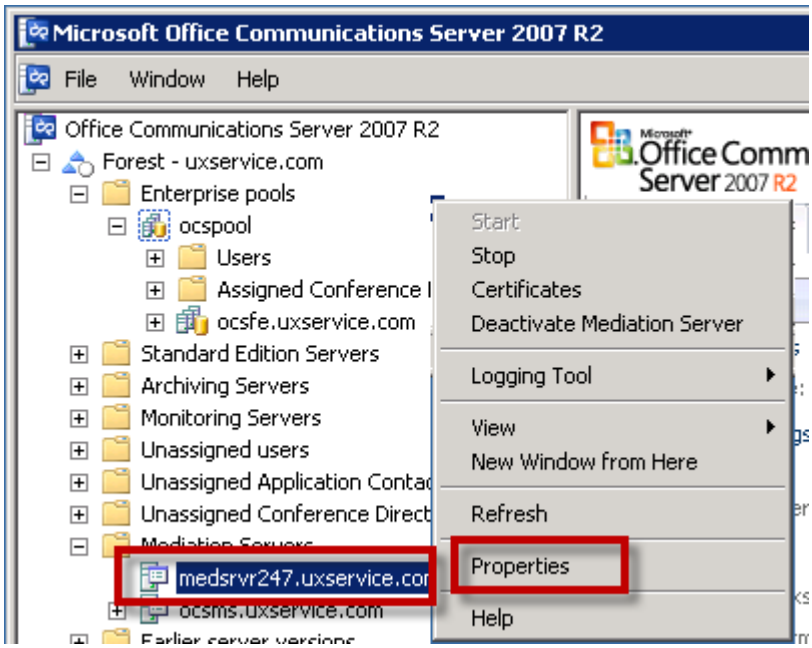
Mediation Server Configuration

On the OCS Front End Server:

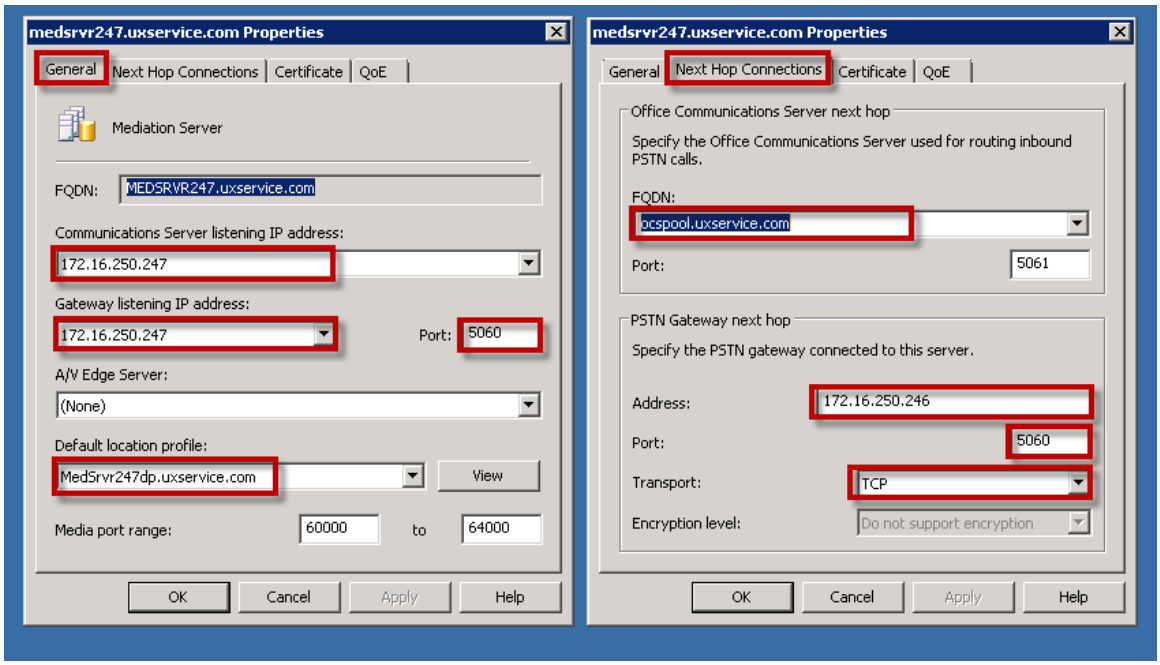
1. Login with OCS administrator privileges
2. Launch **Microsoft Office Communications Server 2007 R2 configuration snap-in**

Copyright © 2015 Sonus Networks. All rights reserved.

3. Open the relevant Mediation Server Properties as shown below:



4. Configure the General and Next Hop tabs as shown below — this is required to associate the Mediation Server with the Sonus SBC 1000/2000 gateway to allow inbound and outbound calls:



5. Start the Mediation Server as shown below:

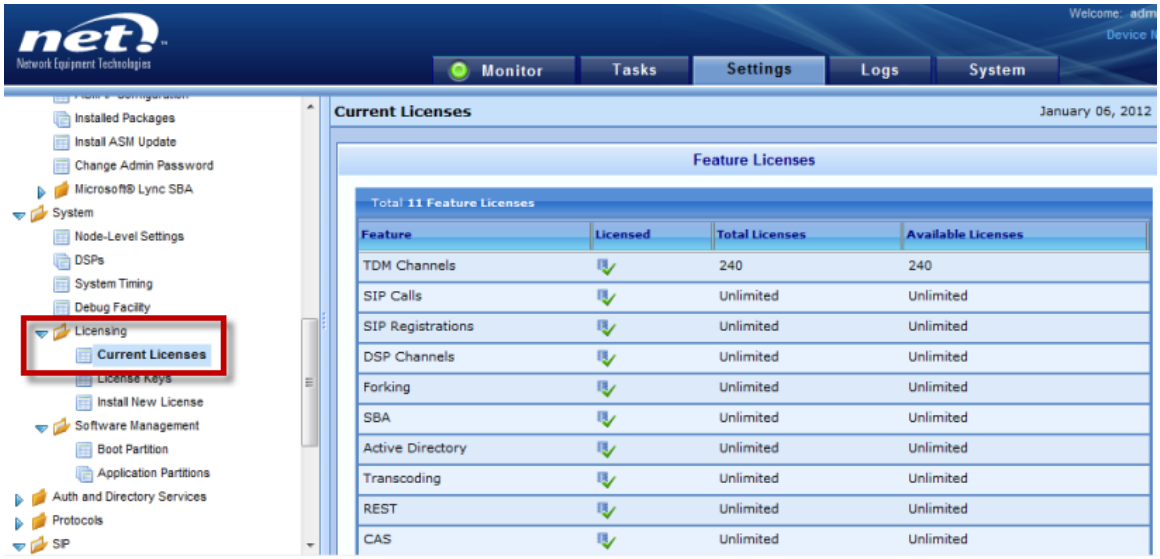
Copyright © 2015 Sonus Networks. All rights reserved.



Sonus SBC 1000/2000 Gateway Tasks

License Verification

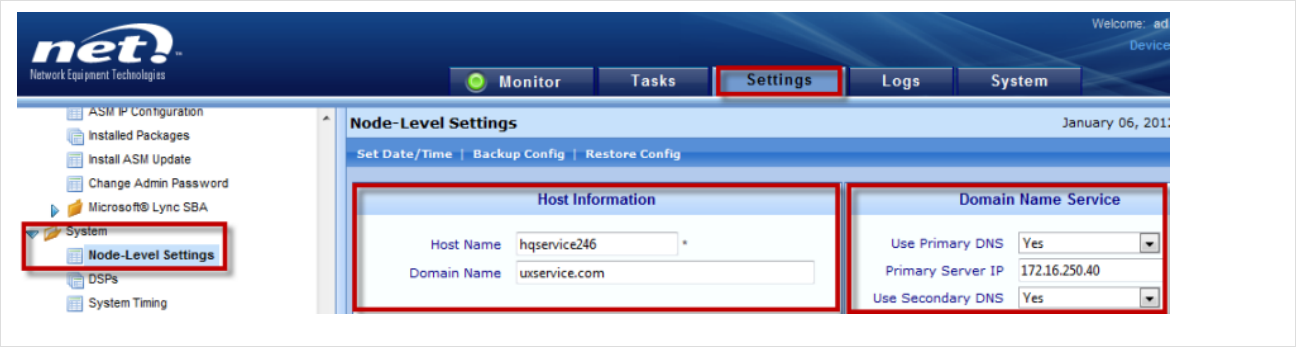
1. Login to the Sonus SBC 1000/2000 WebUI
2. Verify that you have a valid license as shown below:



Node-Level Settings Verification

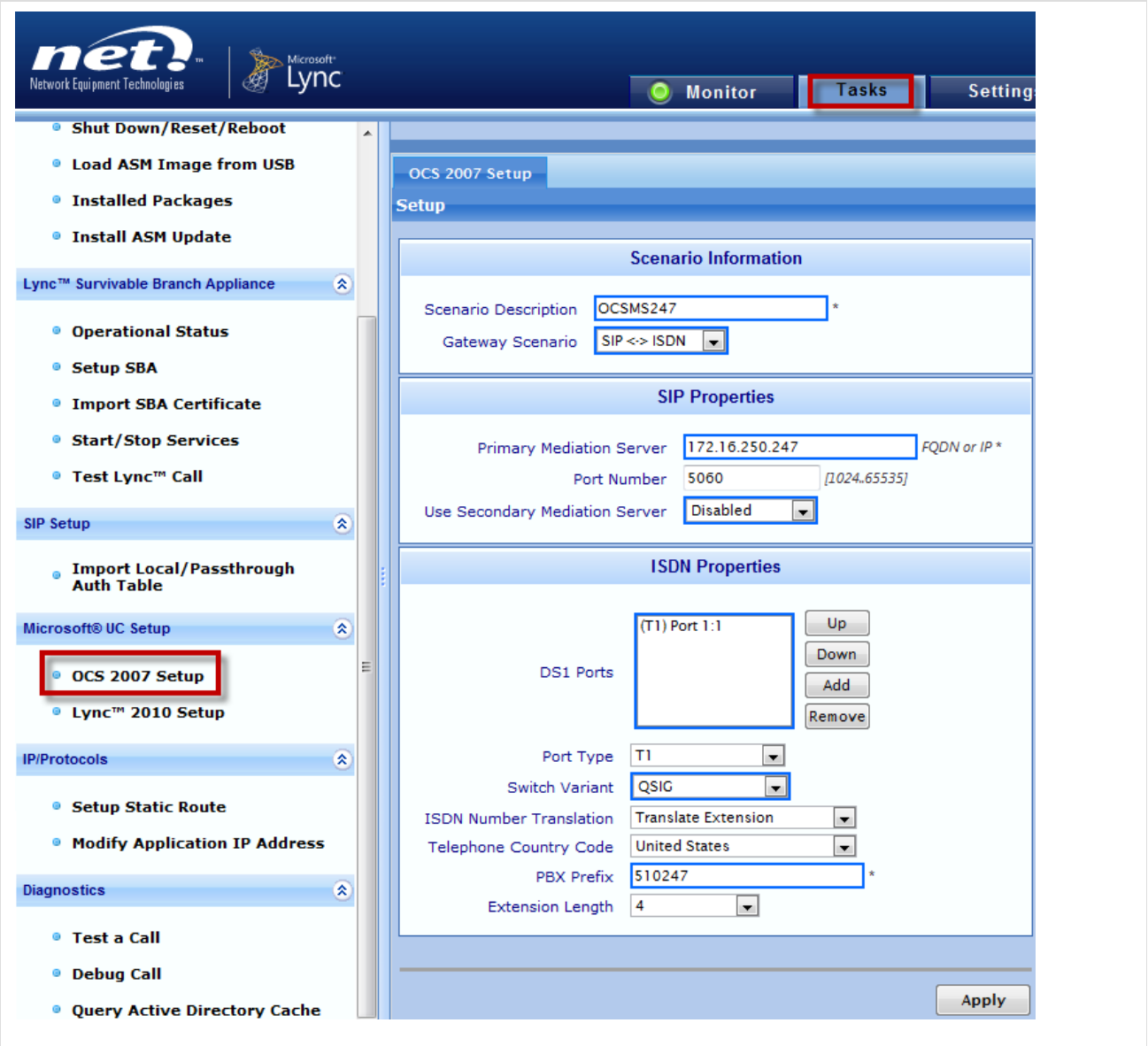
1. Login to the Sonus SBC 1000/2000 WebUI
2. Verify that the host name, domain name, and DNS information are correctly entered as shown below:

Copyright © 2015 Sonus Networks. All rights reserved.



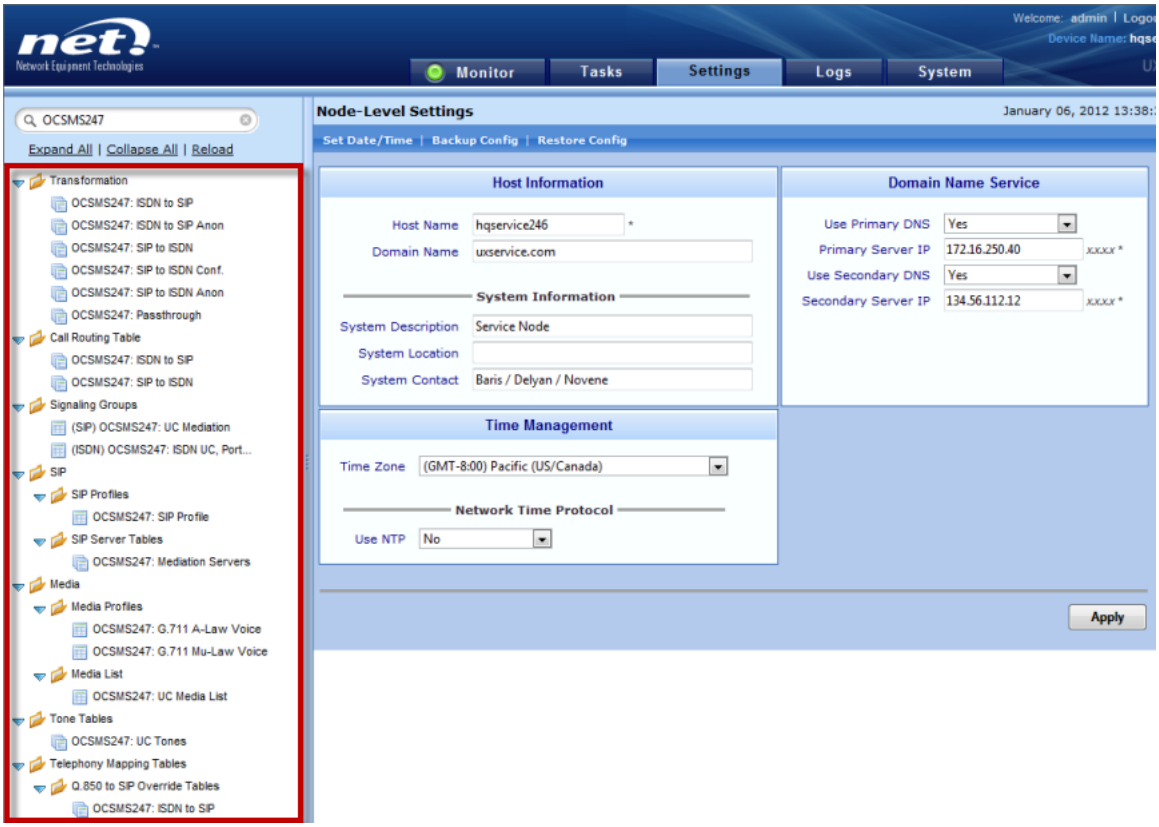
Running the Sonus SBC 1000/2000 OCS 2007 Configuration Wizard

1. Login to the Sonus SBC 1000/2000 WebUI
2. Under the Tasks tab, run [OCS 2007 Setup](#)wizard as shown below:

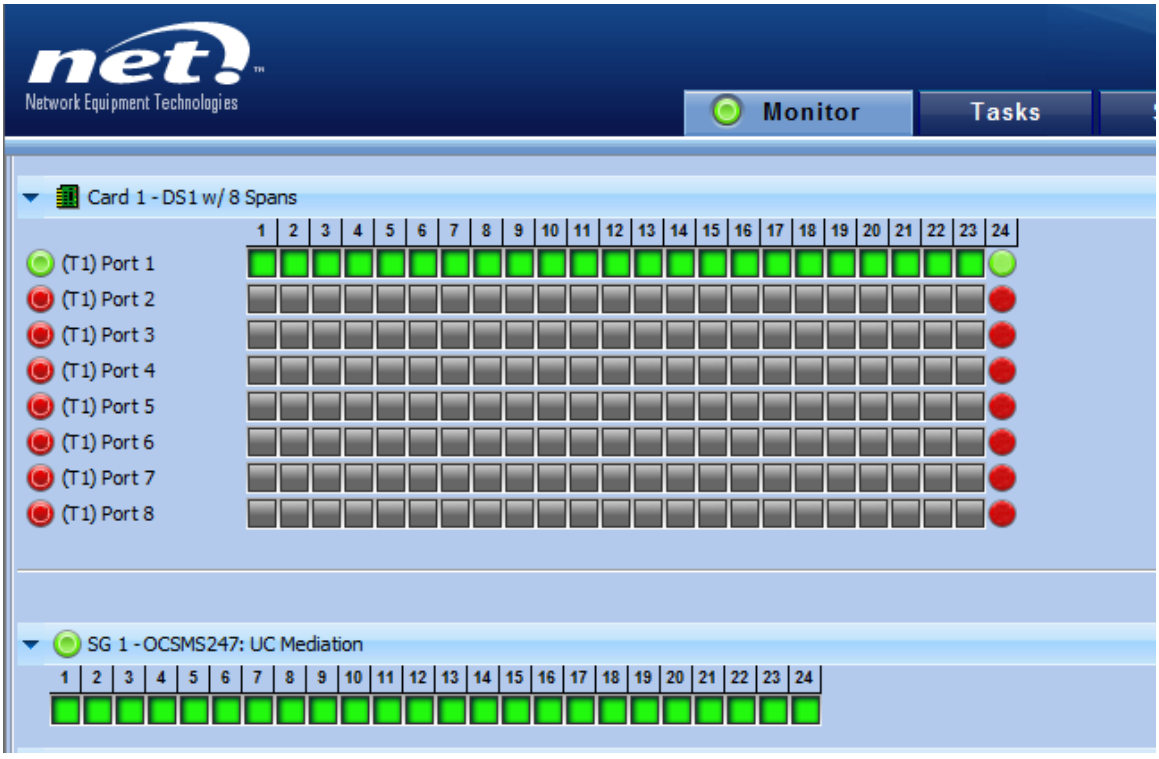


3. The outcome of this task will create all the necessary Sonus SBC 1000/2000 configuration data elements/resources:

Copyright © 2015 Sonus Networks. All rights reserved.



4. Upon task completion, connect the PRI cable to the relevant port (it is 1:1 in this example) to allow PSTN - Sonus SBC 1000/2000 connectivity.
5. At this point, the real-time monitor viewwill display the following:



Copyright © 2015 Sonus Networks. All rights reserved.

At this stage, calls between PSTN and OCS 2007 R2 in following setup can be placed and answered successfully:

PSTN isdn Sonus SBC 1000/2000 (172.16.250.246) sip/tcp Mediation Server (resides on ASM - 172.16.250.247 Front End Server Pool / MOC

How to Enable, Collect, and Provide Log Files From The SBC 1000-2000 SBA

Do not publish this page. This page is in the process of being edited for branding, content, etc...
9-13-3013

Table of Contents

- Overview
- Use Case
  - Setup
  - Scenario
- Files to be provided
  - SBC Configuration Backup File
  - Logs
    - Enabling Logging
      - SBC Logs
      - Lync (SBA) Logs
    - Executing the Scenario in Question
    - Collecting the Logs
      - UX Logs
      - Lync (SBA) Logs
      - UXSBA/ASM Logs
  - Provide the Logs

About this Page

This is a best practice on how to enable, collect, and provide traces and logs from a UX gateway and from ASM.

Overview

Copyright © 2015 Sonus Networks. All rights reserved.

In the process of troubleshooting issues in your voice network, you may need to collect logs from UX or from Application Solution Module (ASM) yourself, or you may be asked by NET TAC to do it. In most cases, when a CRM case is opened, NET TAC will request the relevant logs and configuration backup. In most cases, NET TAC engineers will need the following files as the minimum requirement to start their analysis:

1. UX configuration backup file
2. WebUI log with following subsystems enabled:
    - Call Routing Service
    - Common Call Control
    - Media Stream Control Service
    - SIP Stack Service
    - ISDN Protocol
3. Brief description of the scenario in question with the calling and called party numbers
4. Peer IP addresses
5. The Lync Server 2010 Log
6. UXSBA, ASM (SBA) logs from ASM machine

Use Case

Setup

SBC gateway is configured in following setup:

```
PSTN -- [SBC gateway] -- [SBC SBA] -- [Lync SBA client]
```

Scenario

1. The Lync SBA client calls a PSTN number
2. The call in question is placed, and an SBA event log states that the gateway is marked as down

Once the issue is addressed with a CRM case, be sure to include the following files for a quicker resolution:

Files to be provided

SBC Configuration Backup File

1. Procedure to backup SBC configuration file is explained in Backing Up Data

Logs

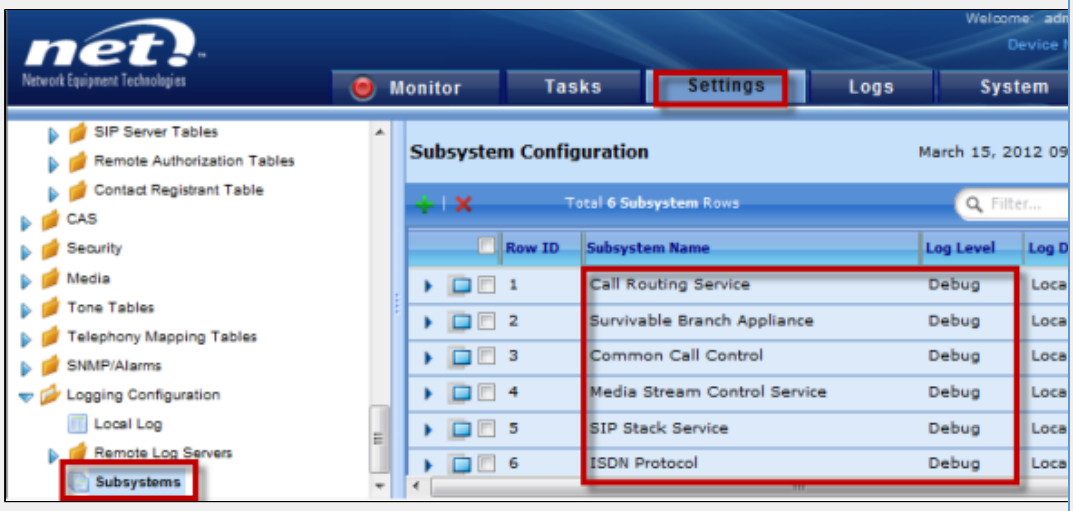
Enabling Logging

SBC Logs

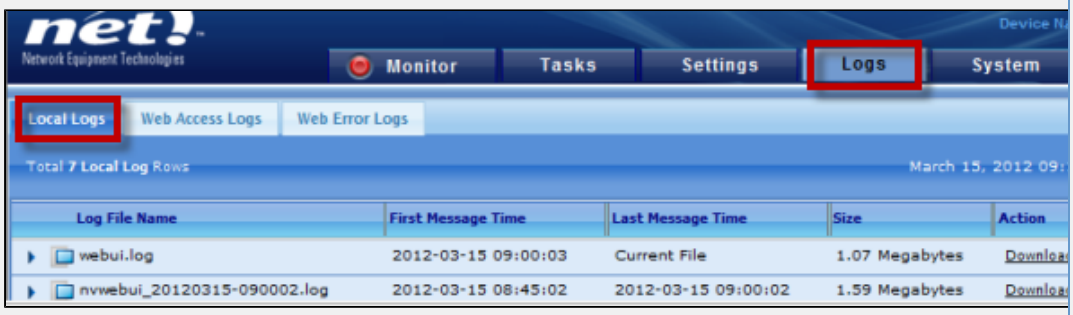
Copyright © 2015 Sonus Networks. All rights reserved.

SBC 2000

1. Launch your preferred browser and log into SBC WebUI
2. In the WebUI, click **Settings**.
3. In the left navigation pane, go to **Logging Configuration / Subsystems**.
4. Add the following subsystems with the log level of **Debug** as shown on following screenshot



5. Rotate the log as shown on the following screenshot:



SBC 1000

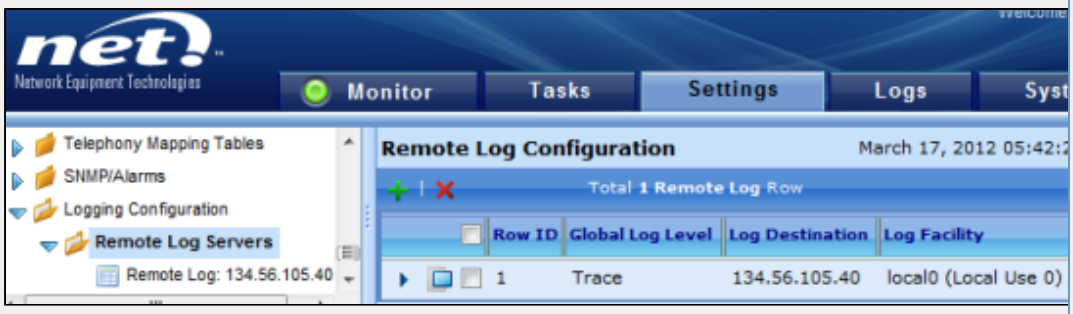
1. Make sure to have a syslog server installed in your network; preferably Log Exchange (LX), which you can download from NET Downloads.

   Need to find a good link for this download

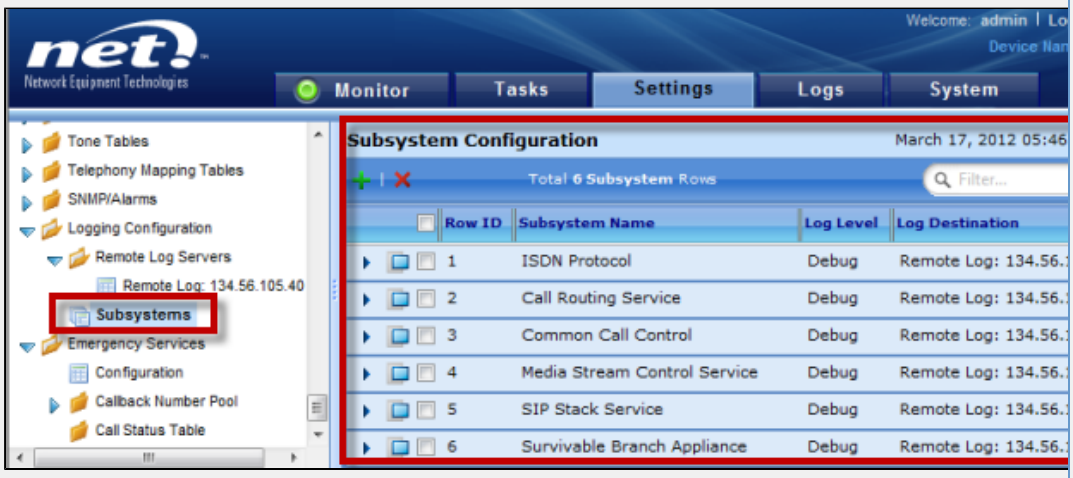
2. In the WebUI, click the Settings tab.
3. In the left navigation pane, go to **Logging Configuration > Remote Log Servers**.

Copyright © 2015 Sonus Networks. All rights reserved.

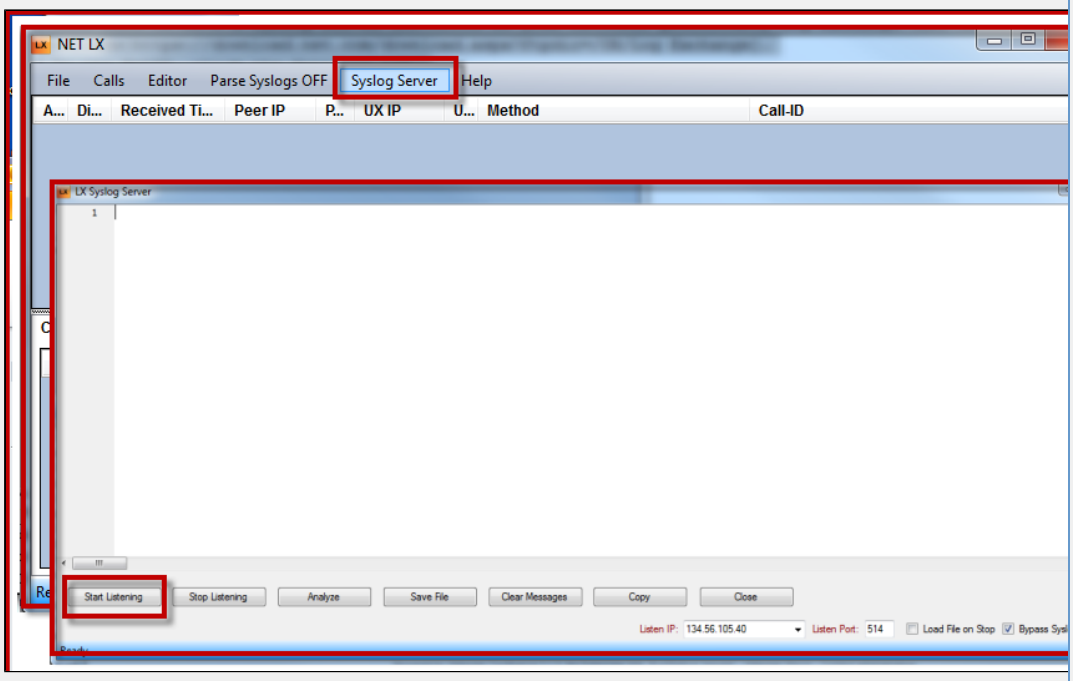
4. Add Remote Log Server as show on the following screenshot (Log Destination is where the NET Log Exchange (LX) is installed)



5. In the WebUI, click the Settings tab.
6. In the left navigation pane, go to **Logging Configuration > Subsystems** and add the following subsystems as show on the following screenshot.



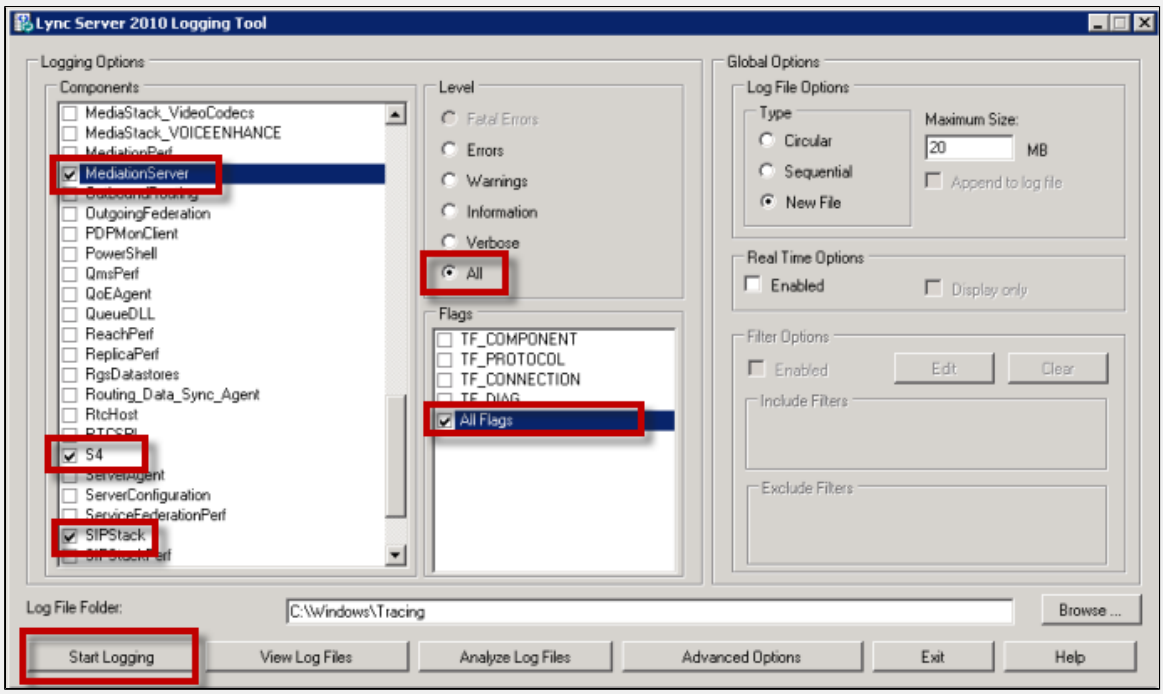
7. Launch the Log Exchange (LX) on the Syslog Server Machine
8. Click **Syslog Server**
9. Click **Start Listening** as shown on the following screenshot.



Copyright © 2015 Sonus Networks. All rights reserved.

Lync (SBA) Logs

1. Remote Desktop into SBA machine (ASM)
2. Launch the Lync Server 2010 Logging Tool
3. Enable **Mediation Server**, **S4**, and **SIPStack** components with Level **All**, and Flags **All** for each component
4. Click **Start Logging** as shown on the following screenshot:



Executing the Scenario in Question

Execute the scenario (i.e: Lync client calls to PSTN number, call is reproduced.)

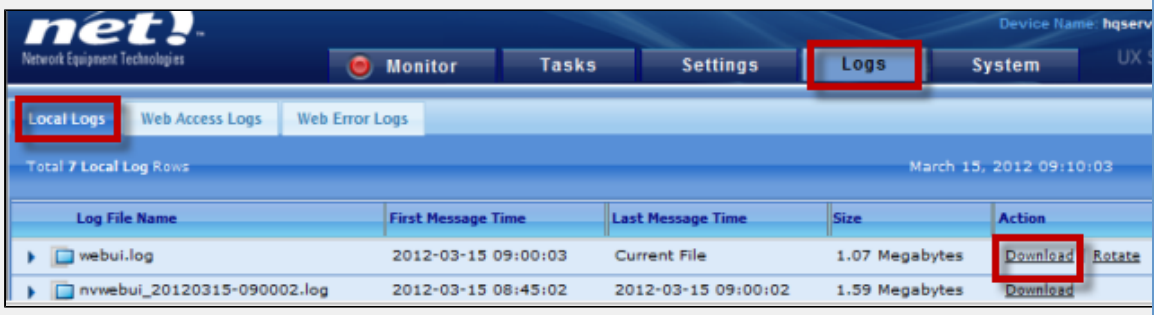
Collecting the Logs

UX Logs

SBC2000

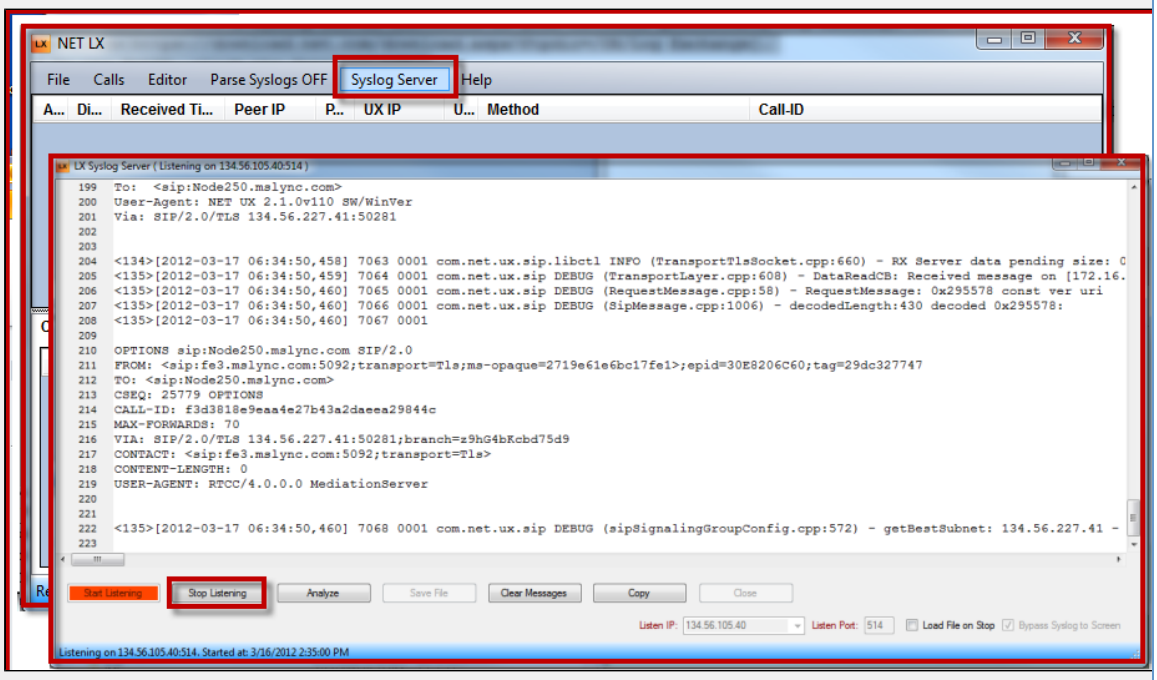
Copyright © 2015 Sonus Networks. All rights reserved.

1. Launch a supported browser and log into UX WebUI
2. In the WebUI, click the **Settings** tab.
3. In the left navigation pane, go to **Logging Configuration / Subsystems**.
4. Download the log as shown on the following screenshot:



SBC1000

1. On Syslog Server machine, click **Stop Listening** on LX Syslog Server as shown on the following screenshot:



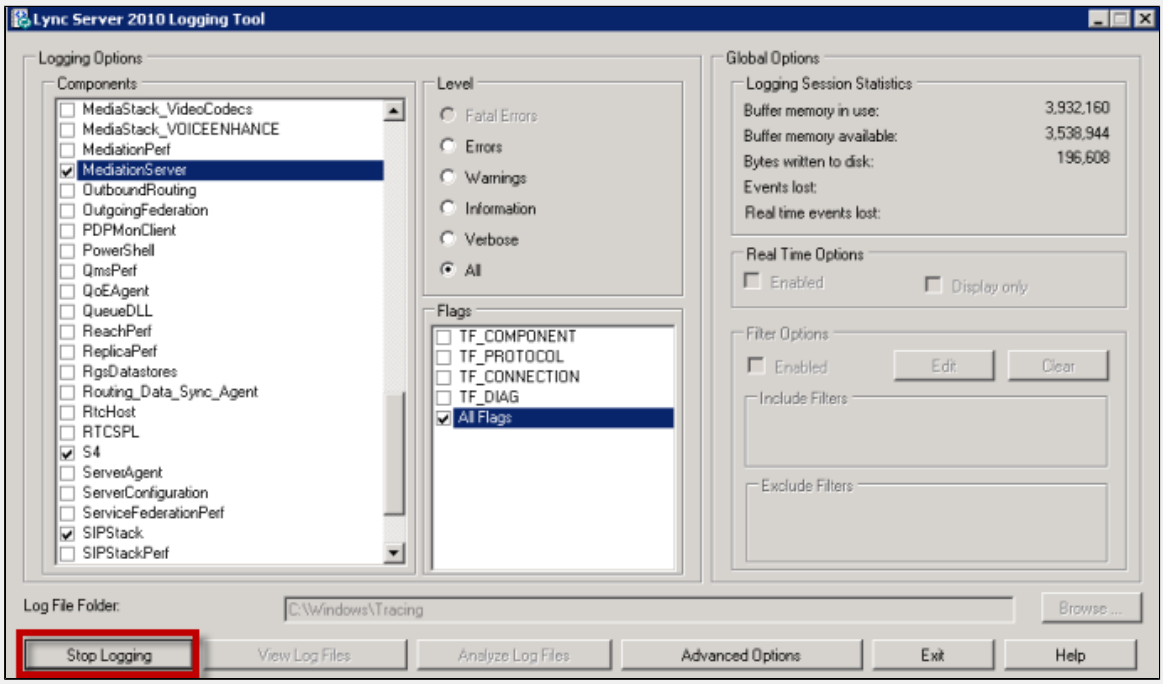
2. Click **Save File** button and save it as **.log** or **.txt** file.

Lync (SBA) Logs

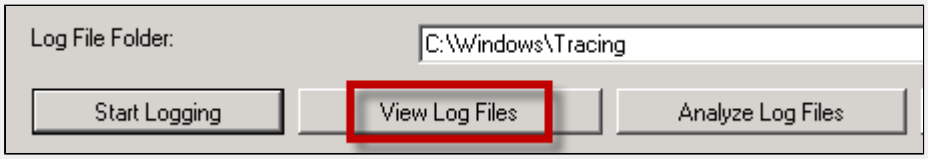
1. Remote Desktop into SBA machine (ASM)
2. In the Lync Server 2010 Logging Tool

Copyright © 2015 Sonus Networks. All rights reserved.

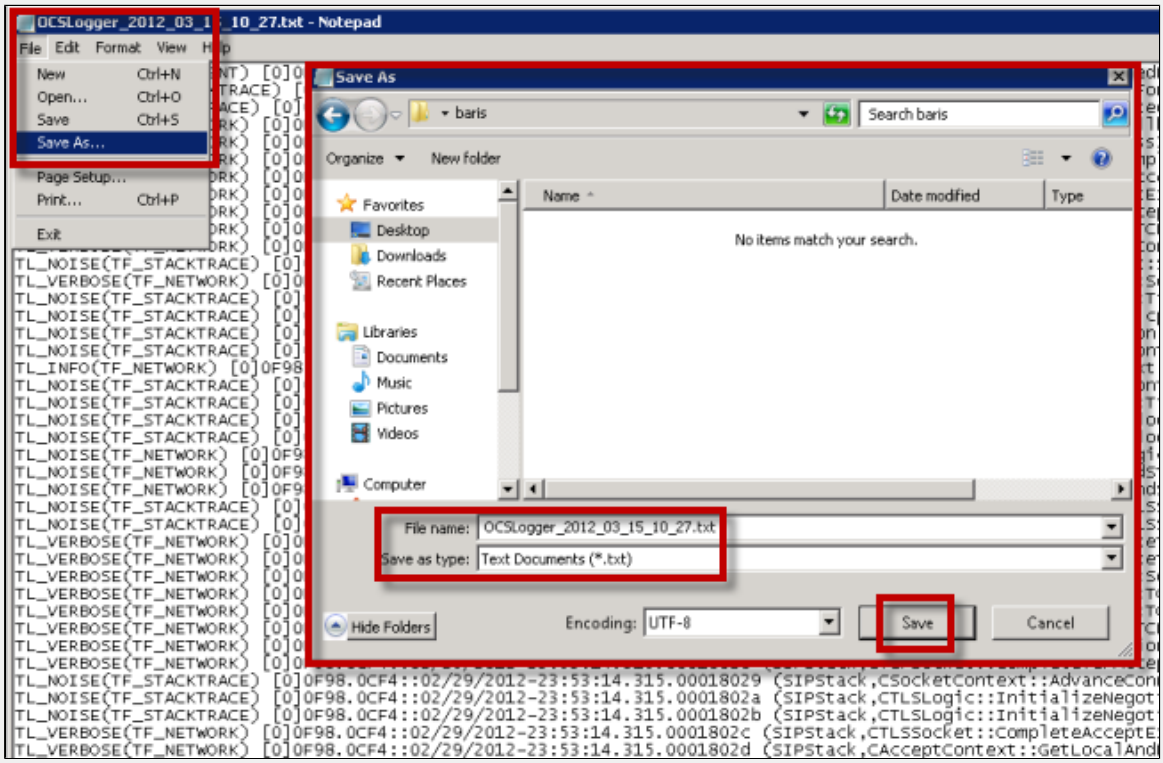
3. Hit **Stop Logging** as shown on the following screenshot:



4. Hit **View Log Files** on Lync Server 2010 Logging Tool as shown on the following screenshot



5. Save the log as txt file as shown on the following screenshot

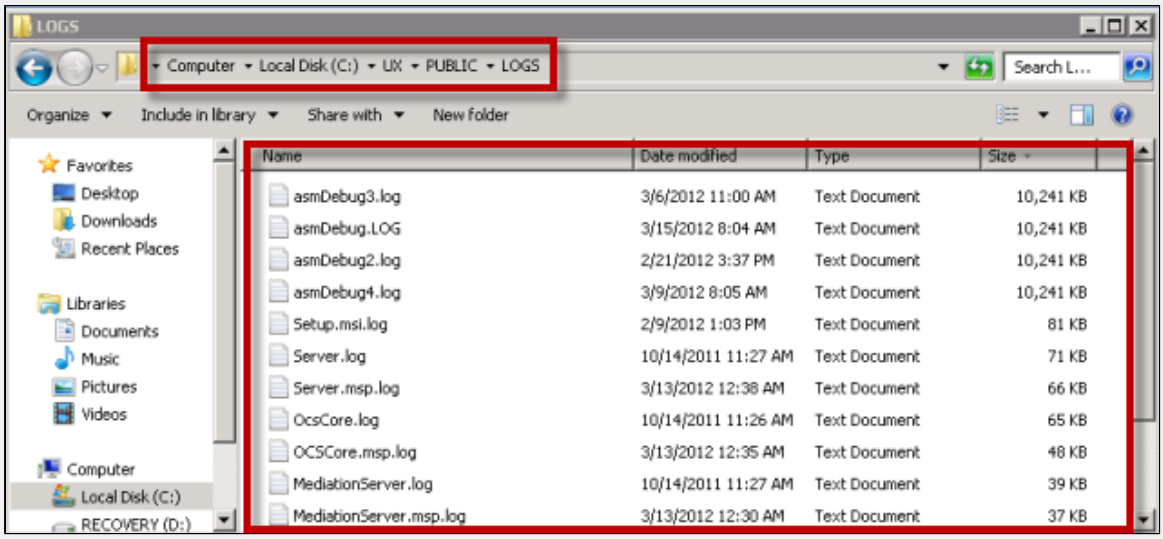


Copyright © 2015 Sonus Networks. All rights reserved.

UXSBA/ASM Logs

1. Remote Desktop into SBA machine (ASM)
2. Use Windows Explorer to navigate to the **C:\UX\PUBLIC\LOGS**directory as shown below and collect/copy all files in this directory as shown on the following screenshot

> Verify the directory path above.



Provide the Logs

Once you have the necessary logs compress all files into ZIP or RAR format and provide them to Sonus Service Representative. Depending on the size of the files, you may either email them or upload them onto our FTP site: ftp://brinks.net.com/pub/. Instructions about uploading the files will be provided with your case.

> Update the upload site link. Do we have such a link (Sonus)?

Configuring The SBC 1000-2000 with ISDN IDA-P Switch Variant

This article describes the steps necessary to configure the Sonus SBC 1000/2000 for the IDA-P ISDN protocol variant.

On This Page

- Sonus SBC 1000/2000 Configuration for ISDN variant IDA-P

Related Articles
Creating and Modifying ISDN Signaling Groups

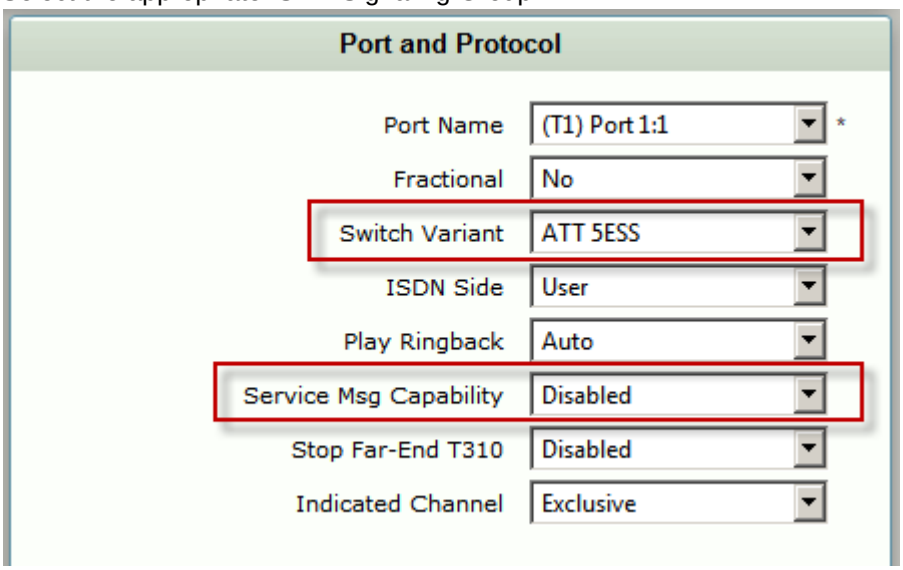
Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000/2000 Configuration for ISDN variant IDA-P

Integrated Digital Access - Primary (IDA-P) is a service commonly provided by PCCW in Hong Kong.

To configure the SBC 1000-2000 for the IDA-P switch variant:

1. Login to the WebUI.
2. Click the **Settings** tab.
3. In the left navigation pane, go to **Signaling Groups**.
    a. Select the appropriate ISDN Signaling Group.



4. In the **Port and Protocol**panel:
    a. Select **ATT 5ESS** in the **Switch Variant** list box.
    b. Select **Disabled** in the **Service Msg Capability** list box.
5. Click **Apply**.

Upgrading the ASM Image From Windows-Only to Lync SBA

This document contains specific upgrade notes for customers planning to upgrade the Windows-only ASM image to Lync Survivable Branch Appliance (SBA) ASM image.

- Overview
- Process to Upgrade the ASM Image From Windows-only to Lync SBA
    - Upgrading the UX Communication service
    - Upgrading the SBC to Release 3.0
    - Upgrading the ASM Recovery Partition
    - Re-Initializing the ASM

> **Before You Upgrade**
>
> If the SBC is running a Release prior to Release 3.0, it is required that the SBC is upgraded to the latest Release 3.0. To upgrade the SBC firmware, follow the instructions from [Upgrading Sonus SBC 1000-2000]
> .

Overview

1. This process consists of four steps.
2. Upgrade the UX Communication service (covered in the upgrade notes for Release 3.0).Upgrade the SBC to

Copyright © 2015 Sonus Networks. All rights reserved.

Release 3.0 (covered in the upgrade notes for Release 3.0).
3. Upgrade the ASM Recovery Partition.
4. Re-initialize the ASM.

Process to Upgrade the ASM Image From Windows-only to Lync SBA

Upgrading the UX Communication service

Upgrade the SBC Communication service by following the instructions in Upgrading the SBC Communication Service.

Upgrading the SBC to Release 3.0

Upgrade the SBC to Release 3.0 by following the instructions in the SBC 1000-2000 3.0 Upgrade Notes.

Upgrading the ASM Recovery Partition

Important

- Complete the upgrade of the SBC to the latest Release 3.0 as noted above before proceeding with this section.
- The ASM must be re-initialized after upgrading the ASM Recovery Partition.

This step is required to ensure that the ASM Recovery Partition is correctly provisioned with the 3.0 Lync SBA image, should it be necessary at a future date to restore the system from this partition. See Managing the ASM for details on the recovery partition.

1. Download the Lync SBA Recovery Partition image file from the Salesforce Portal.
2. Follow the instructions outlined in Updating the ASM Recovery Partition.

Note that the existing Windows-only image will not be deleted and will be preserved as an option in the *Application Solution Module Reinitialize* dialog along with the Lync 2010 or 2013 SBA image.

Re-Initializing the ASM

Proceed with the ASM Re-initialization only after the ASM Recovery Partition has been upgraded to the latest ASM image.

Configuring SBC 1000-2000 for Broadsoft Compatibility

This set of best practice articles describe how to configure the SBC 1000/2000 for compatibility with Broadsoft.

Articles In This Set
Configuring the SBC 1000-2000 for BroadSoft SUBSCRIBE/NOTIFY

Copyright © 2015 Sonus Networks. All rights reserved.

Related Documents
• BroadSoft Partner Configuration Guide: IPPBX-PBX Trunking • BroadSoft Partner Configuration Guide: Sonus SBC 1000/2000 • BroadSoft Partner Configuration Guide: SIP Access Device Configuration

Configuring the SBC 1000-2000 for BroadSoft SUBSCRIBE/NOTIFY

Overview

The Sonus SBC 1000/2000 now supports SUBSCRIBE/NOTIFY requests for BroadSoft compatibility (SIP endpoints use the SUBSCRIBE/NOTIFY mechanism to get notifications about a specific resource from other endpoints). The Interop Mode option in the SBC Signaling Group configuration enables the SBC to passthrough SIP messages such as NOTIFY, SUBSCRIBE, and REGISTER. These messages are also forwarded to the BroadSoft server.

Through configuration (detailed below), the SBC uses the SUBSCRIBE/NOTIFY mechanism to support the following Advanced Phone Services and Access Device Services (Call Control) features:

Advanced Phone Services

- Busy Lamp Field
- Feature Key Synchronization
- Shared Call Appearance

Access Device Services (Call Control)

- Call Waiting
- Call Hold
- Blind Transfer
- Attendant Transfer
- Local Conference
- Network Conference
- Call Forwarding

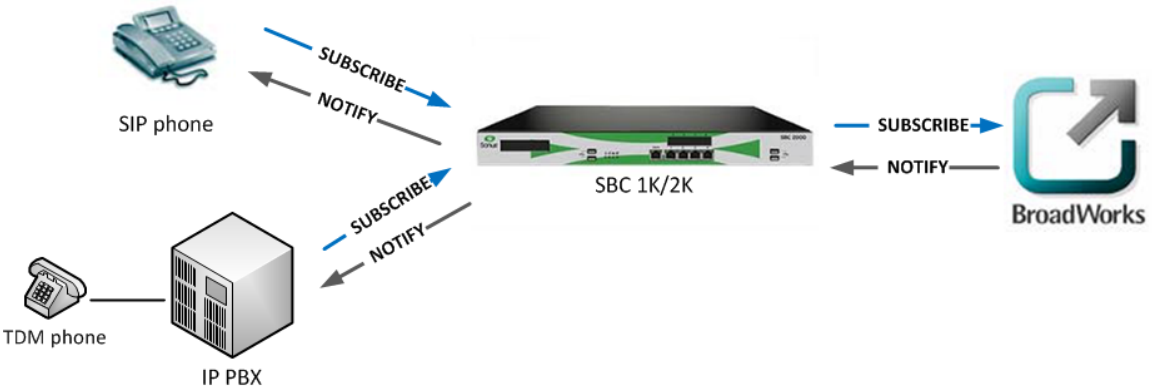
> For specific configuration of the Access Device Services (Call Control) features, please refer to BroadSoft and/or the endpoint configuration documentation.

Network View

A BroadSoft (BroadWorks) server maintains voice mail information for all of its registered users. When a user receives a voice message, the BroadSoft server communicates this information in a NOTIFY request to users. These messages then pass through the Sonus SBC as shown below in the network layout.

On the local side, the network layout displays the Sonus SBC receiving requests from SIP endpoints that are configured in the BroadSoft server. From the BroadSoft side, it shows the Sonus SBC forwarding the requests to the Broadsoft server. This diagram also displays the reverse path for the responses.

Copyright © 2015 Sonus Networks. All rights reserved.



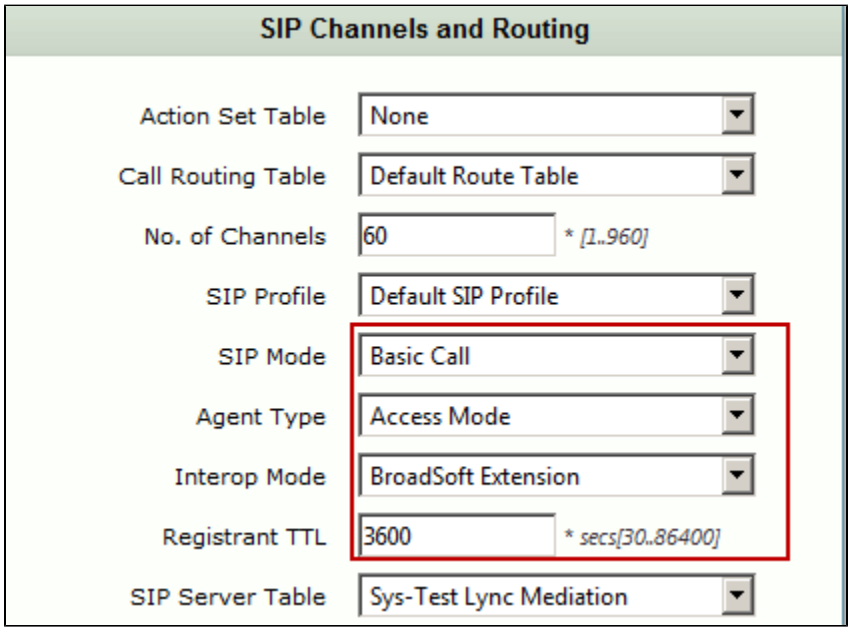
How to configure the SBC to interoperate with BroadSoft messaging

In order for the SBC to pass through BroadSoft NOTIFY/SUBSCRIBE messages, you must create two Signaling Groups (Phone-side and BroadSoft-side) within the SBC. These Signaling Groups receive, respond, and forward requests from SIP endpoints that are configured in the BroadSoft server. The information below details how to configure these Signaling Groups.

Step 1. Create Broadsoft Signaling Group to receive Message status

The BroadSoft Signaling Group in the SBC is configured to receive message notifications from the BroadSoft server. Create this Signaling Group as follows:

1. Create a new **BroadSoft** Signaling Group (for details on how to create a Signaling group, see Creating and Modifying SIP Signaling Groups).
2. From the **SIP Mode** drop down box, select **Basic Call.**
3. From the **Agent Type** drop down box, select **Access Mode.**
4. From the **Interop Mode** drop down box, select **BroadSoft Extension.**
5. In the **Registrant TTL** box**,** enter **3600** (default entry).
6. For all other configuration elements, see Creating and Modifying SIP Signaling Groups.
7. Save the configuration.

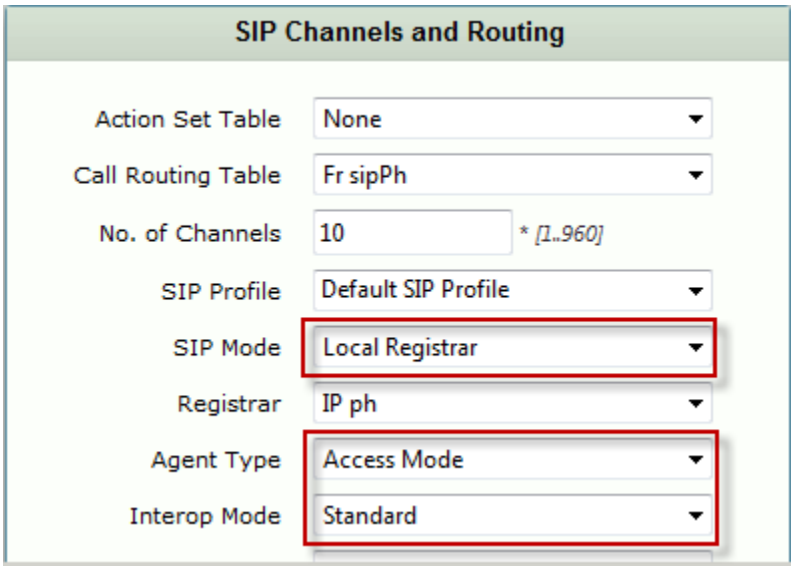


Step 2. Create Local Registrar Signaling Group

Copyright © 2015 Sonus Networks. All rights reserved.

The Local Registrar Signaling group in the SBC is configured to accept NOTIFY/SUBSCRIBE messages from SIP endpoints. Create this Signaling Group as follows:

1. Create a new **Local Registrar** Signaling Group. This is the destination Registrar Signaling Group (the Registrar database is queried to find contact details of the user, since BroadSoft users are registering endpoints). For details on how to create a Signaling Group, see Creating and Modifying SIP Signaling Groups .
2. From the **SIP Mode** drop down box, select **Local Registrar**.
3. From the **Agent Type** drop down box, select **Access Mode**.
4. From the **Interop Mode** drop down box, select **Standard**.
5. For all other configuration elements, see Creating and Modifying SIP Signaling Groups.



Configuring SBC 1000-2000 for Multiple Media Streams (Video Call Passthrough)

- How Multiple Media Streams work
- Configuration
  - Step 1: Configure Media Stream Type
  - Step 2: Configure Priority for Media Stream Type
- Usage Examples
  - Audio Stream Only - Video Passthrough Disabled (Default configuration)
  - Proxy Mode - Video Passthrough Enabled
  - Mixed Media (Hybrid) Mode - Video Passthrough Enabled
- Limitations/Guidelines

How Multiple Media Streams work

The SBC enables multiple media streams, which includes Video Call Passthrough support. Video codecs are transparently passed through the SBC and are negotiated end to end.

Specific configuration allows multiple media streams to be bundled in the Proxy Media mode (through Audio/Fax Stream Proxy Mode enabled). As a result, all media streams (Audio/Video/Application) are passed through the SBC. The media streams can have mixed (hybrid) modes, which enables audio to be transcoded and video to be in Proxy

Copyright © 2015 Sonus Networks. All rights reserved.

mode.

- Proxy Mode enables multiple media streams to be bundled in Proxy media mode; all media streams (Audio/Video/Application) are passed through the SBC.
- Mixed Media (Hybrid) mode allows the SBC to handle multiple streams with different media modes (DSP & Proxy) in the same call; audio is transcoded and video/application is in Proxy media mode.

> We recommend using Mixed Media (Hybrid) mode over Proxy mode. Mixed Media (Hybrid) mode allows the SBC to handle multiple streams with different media modes (DSP & Proxy) in the same call; audio is transcoded and video/application is in Proxy media mode.

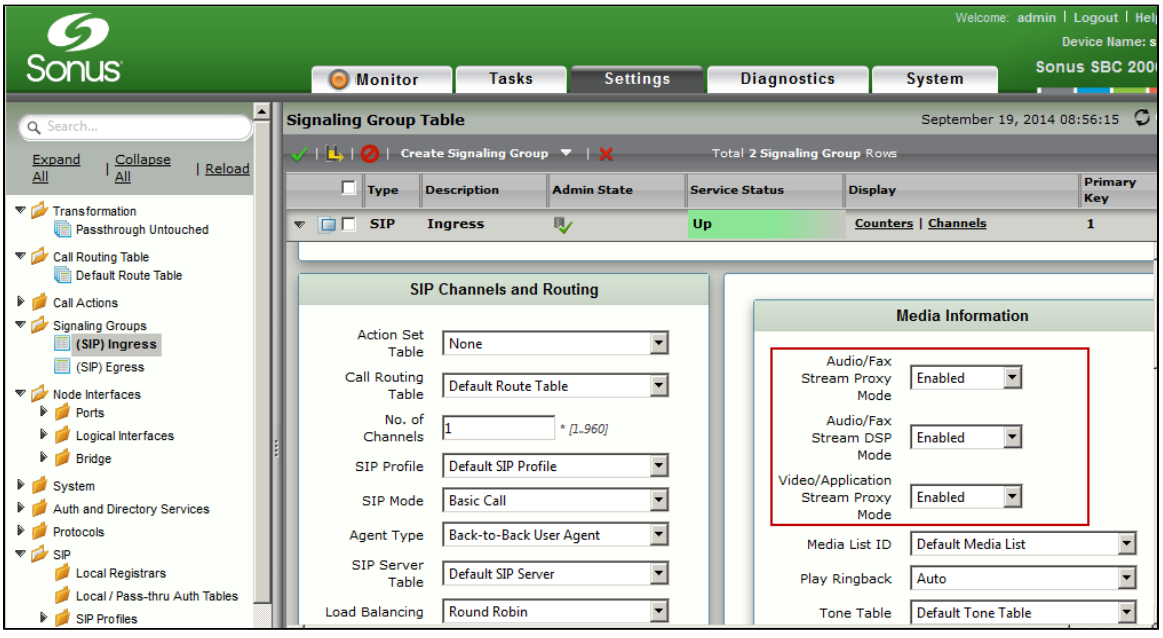
Configuration

The below steps outline the basic configuration for using Video Call Passthrough. See Usage Examples below for specific configuration. For detailed field configuration, see Creating and Modifying SIP Signaling Groups and Creating and Modifying Entries to Call Routing Tables.

Step 1: Configure Media Stream Type

Through the SIP Signaling group's Media Information, a mode enabled state can be selected for each media stream type.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click on the desired Signaling Group.
4. From the Media Information, enable/disable the Media Stream Mode:
    - **Audio/Fax Stream Proxy Mode**. Media stream is proxied and switched between endpoints in order to negotiate common media capabilities and handle unsupported/unknown audio codecs. Does not require DSP resources.
    - **Audio/Fax Stream DSP Mode**.DSP resources are used for media handling, but capabilities/features are not facilitated between endpoints that are not supported within the SBC (codec/capability mismatch).
    - **Video/Application Stream Proxy Mode.** Media stream is proxied and switched between endpoints in order to negotiate common media capabilities. Does not require DSP resources.

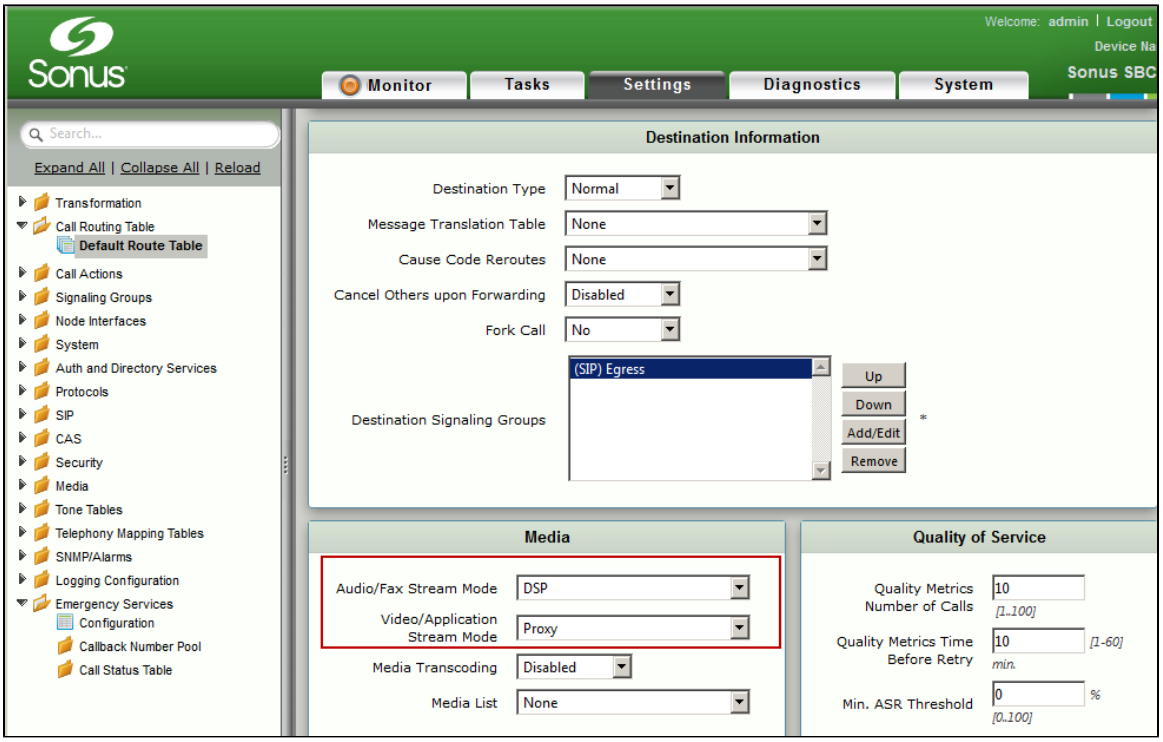


Copyright © 2015 Sonus Networks. All rights reserved.

Step 2: Configure Priority for Media Stream Type

Through the Call Route Table, a **media priority** can be selected for each of these media stream types (Audio/Fax Stream, Video/Application Stream).

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Call Routing**
3. Click on the desired Call Routing Table
4. From Media Information, select the following:
    - **Audio Fax Stream Mode.** Select an option. See Creating and Modifying Entries to Call Routing Tables
    - **Video/Application Stream Mode**. Enable or Disable. When disabled, the SBC will **not** proxy or switch media stream between endpoints.



Usage Examples

Audio Stream Only - Video Passthrough Disabled (Default configuration)

Component	How to Configure
Inbound Signaling Group Entry	• **Audio**: Audio/Fax Stream Proxy Mode - **Enabled** Audio/Fax Stream DSP Mode- **Enabled** • **Video**: Video/Application Stream Proxy Mode - **Enabled**

Copyright © 2015 Sonus Networks. All rights reserved.

Outbound Signaling Group Entry	• **Audio**: Audio/Fax Stream DSP Mode - **Enabled** Audio/Fax Stream DSP Proxy - **Enabled** • **Video**: Video/Application Stream Proxy Mode - **Enabled**
Call Route Entry	• **Audio**: Audio/Fax Stream Mode - **DSP Preferred over Proxy** • **Video**: Video/Application Stream Mode - **Disabled**

Proxy Mode - Video Passthrough Enabled

Proxy Mode enables multiple media streams to be bundled in Proxy media mode; all media streams (Audio/Video/Application) are passed through the SBC.

For this configuration there are two outcomes:

- For Audio Stream only: Audio stream on Proxy Mode.
- For Multiple Streams: All streams on Proxy Mode.

Component	How to Configure
Inbound Signaling Group Entry	• **Audio**: Audio/Fax Stream Proxy Mode - **Enabled** Audio/Fax Stream DSP Mode - **Enabled** • **Video**: Video/Application Stream Proxy Mode - **Enabled**
Outbound Signaling Group Entry	• **Audio**: Audio/Fax Stream Proxy Mode - **Enabled** Audio/Fax Stream DSP Mode - **Enabled** • **Video**: Video/Application Stream Proxy Mode - **Enabled**
Call Route Entry	• **Audio**: Proxy Preferred over DSP - **Enabled** • **Video**: Video/Application Stream Mode - **Proxy**

Mixed Media (Hybrid) Mode - Video Passthrough Enabled

Mixed Media (Hybrid) mode allows the SBC to handle multiple streams with different media modes (DSP & Proxy) in the same call; audio is transcoded and video/application is in Proxy media mode.

For this configuration there are two outcomes:

- For Audio Stream only: Audio stream on DSP Mode.
- For Multiple Streams: Hybrid with DSP/Proxy

Component	How to Configure

Copyright © 2015 Sonus Networks. All rights reserved.

Inbound Signaling Group Entry	• **Audio**: Audio/Fax Stream Proxy Mode - **Enabled** Audio/Fax Stream DSP Mode- **Enabled** • **Video**: Video/Application Stream Proxy Mode - **Enabled**
Outbound Signaling Group Entry	• **Audio**: Audio/Fax Stream Proxy Mode - **Enabled** Audio/Fax Stream DSP Mode- **Enabled** • **Video**: Video/Application Stream Proxy Mode - **Enabled**
Call Route Entry	• **Audio**: Audio/Fax Stream Mode - **DSP preferred over Proxy** • **Video**: Video/Application Stream Mode - **Proxy**

Limitations/Guidelines

- The SBC does not support Video Call Transfers in Release 4.0.
- Call forwarding from Mixed Media (Hybrid) to Proxy mode is not currently supported.
- Video call transfer in Non-Broadsoft environment is not support (REFER pass-through is not supported).
- Forked calls is applicable only to matching media mode call route entries.
- 911 call routing entries should not use proxy modes in order to avoid possible call failures (due to absence of transcoding and media mismatch between the end points).

How Incoming Calls are Handled when Server is Unreachable

IN PROGRESS

- Basic Call Mode with Agent Type as "Back-to-Back User Agent" Configuration - How Incoming Calls are handled
  - Scenario 1: Registration to server fails; Monitor using SIP Options for the corresponding SIP Server is incorrectly configured.
  - Scenario 2: Monitor using SIP Options for SIP Server fail; Registration to server is not configured
  - Scenario 3: Registration to server succeeds; Monitor using SIP options for SIP Server fail
  - Scenario 4: Registration to server fails; Monitor using SIP Options for SIP Server are successful
  - Scenario 5: Both Registration and Monitor using SIP Options for SIP Server fail
  - Scenario 6: Receiving a 3xx/4xx/5xx/6xx response to Register with a Retry after header
  - Scenario 7: Receiving final 5xx/6xx (without Retry after header) failure responses to Register
  - Scenario 8: Receiving 3xx/4xx (without Retry after header) response to Register
- Forward Register after Local Processing Mode - How Incoming Calls are handled in the Sonus SBC 1000/2000
  - Scenario 1: Registration fails; Fwd Register Option not configured
  - Scenario 2: Fwd Register Option fails; Registration not configured
  - Scenario 3: Registration fails; Fwd Register Option succeeds
  - Scenario 4: Registration succeeds; Fwd Register Option fails
- Troubleshoot Configuration for connection to a Server
  - Verify Signaling Group
  - Verify Registration/Monitor for SIP Options (for SIP Server)
  - Verify Configuration for Contact Registrant
  - Verify Forward Register Option

Copyright © 2015 Sonus Networks. All rights reserved.

This Best Practice describes how the Sonus SBC 1000/2000 handles incoming calls when the Server is down or unreachable. The Sonus SBC routes the calls according to general configuration guidelines. The information below includes expected behavior for call routing when there is a problem reaching the server (i.e, registration fails, wrong configuration, etc.).

> This Best Practice assumes the following:
>
> - Incoming call is based on Federated IP/Signaling Group listen port/transport protocol.
> - Incoming call is one of the following: ISDN, SIP, or CAS.

Basic Call Mode with Agent Type as "Back-to-Back User Agent" Configuration - How Incoming Calls are handled

Below are the components of a basic configuration

- Endpoint is registered with the SBC 1000/2000 (see Creating and Modifying Entries in Contact Registrant Tables).
- SBC's Signaling Group is configured to send requests to a server (see Creating and Modifying Entries in SIP Server Tables).

Scenario 1: Registration to server fails; Monitor using SIP Options for the corresponding SIP Server is incorrectly configured.

The Sonus SBC handles the calls as follows:

- Incoming call is allowed. Since the server is down, the Signaling Group's Server Status is set as **Down**. Instead of attempting to send calls to the server, the call proceeds to the next Signaling Group (if configured based on the routing policy).
- Based on routing configuration, incoming calls are made without any post dial delay to the configured SIP or ISDN trunk.

Scenario 2: Monitor using SIP Options for SIP Server fail; Registration to server is not configured

The Sonus SBC handles the calls as follows:

- The incoming call is allowed. Instead of attempting to send calls to the Server (since the Server is down). the call will proceed to the next Signaling Group (if configured based on the routing policy).
- Based on routing configuration, incoming calls are made without any post dial delay to the configured SIP or ISDN trunk.

Scenario 3: Registration to server succeeds; Monitor using SIP options for SIP Server fail

When a very high registration expires (**Global Time to Live TTL**) interval is configured (configuration available through the Contact Registrant Table), ensure it is sent more frequently. For example, set the registration interval less than the time set for the Registration to expire.

The Sonus SBC handles the calls as follows:

- The incoming call is allowed. If Registration is still valid, the Server and corresponding Signaling Group's Server status is **not** marked as **Down**. Calls are attempted to the Server. If no response, the call proceeds to the next Signaling Group if configured based on routing policy.
    - **Case 1.** The Far end supports Monitor using SIP options and the Registration interval is configured to

Copyright © 2015 Sonus Networks. All rights reserved.

be higher than the option interval. The Options response fails, which indicates the Server is down (there may be a post dial delay as the Signaling Group's Server status is not set to **Down**).

- **Case 2**. The far end does not support Monitor using SIP options and the Registration Interval (Global Time to Live or Failed Registration Retry Timer) is configured to be higher than the registration interval. In this case, the Monitor using SIP options response failure is not an indication that the Server is down. Since the Signaling Group's Server Status is not set to Down, the call proceeds normally.

Scenario 4: Registration to server fails; Monitor using SIP Options for SIP Server are successful

The Sonus SBC handles the calls as follows:

- Incoming calls are allowed. If Registration (through Contact Registrant Table) fails, but Option responses (through the SIP Server Table) are successful, the Signaling Group's Server status is not set to **Down**. Possibilites for the registration failure could be that the Registration was misconfigured and the Server may still be up (as evident from successful Options responses).

Scenario 5: Both Registration and Monitor using SIP Options for SIP Server fail

The Sonus SBC handles the calls as follows:

- Incoming calls are allowed. Since the Server is down, the Signaling Group's Server status is set to **Down**.
- Calls proceed to the next Signaling Group if configured based on routing policy.
- Based on routing configuration, incoming calls are made without any post dial delay to the configured SIP or ISDN trunk.

Scenario 6: Receiving a 3xx/4xx/5xx/6xx response to Register with a Retry after header

The Sonus SBC handles the calls as follows:

- The corresponding session fails.
- The retry-handling is relevant only for Registrations; it will still allow registrations to be retried to the corresponding server but the Invite requests will not route if all the corresponding sessions fail and the Signaling Group's Server status is set to **Down**.

Scenario 7: Receiving final 5xx/6xx (without Retry after header) failure responses to Register

The Sonus SBC handles the calls as follows:

- The corresponding session fails.
- The retry-handling is relevant only for Registrations; it will still allow registrations to be retried to the corresponding server but the Invite requests will not route if all the corresponding sessions fail and the Signaling Group's Server status is set to **Down**.

Scenario 8: Receiving 3xx/4xx (without Retry after header) response to Register

The Sonus SBC handles the calls as follows:

- The corresponding session is up.
- Invite requests are routed to the corresponding Signaling Group (the status is set to **Up**).

Forward Register after Local Processing Mode - How Incoming Calls are

Copyright © 2015 Sonus Networks. All rights reserved.

handled in the Sonus SBC 1000/2000

Below are the components of a configuration that includes Forward Register after Local Processing Mode (configured through the SIP Signaling Group).

- Endpoint is registerd with the Sonus SBC.
- SBC has a Signaling Group configured to send requests to a Server.
- Signaling Group is configured with **Fwd Register After Local Processing** as the SIP Mode.
- A signaling group is assocated with both call origination and termination device.

Scenario 1: Registration fails; Fwd Register Option not configured

The Sonus SBC handles the calls as follows:

- Even through the Server is down (and single Signaling group is used), the Signaling Group's Server status is **not** set to **Down**.
- The incoming call will not attempt to reach the Server and will follow the routing policy to try the next SIP/ISDN/CAS trunk using the associated Signaling Group.

Scenario 2: Fwd Register Option fails; Registration not configured

The Sonus SBC handles the calls as follows:

- Even through the Server is down (and single Signaling group is used), the Signaling Group's Server status is **not** set to **Down**.
- The incoming call will not attempt to reach the Server and will follow the routing policy to try the next SIP/ISDN/CAS trunk using the associated Signaling Group.

Scenario 3: Registration fails; Fwd Register Option succeeds

The Sonus SBC handles the calls as follows:

- Normal call flow for incoming call. In case the Server is down, there may be post dial delay in attempting to call the Server.

Scenario 4: Registration succeeds; Fwd Register Option fails

The Sonus SBC handles the calls as follows:

- Normal call flow for incoming call. In case the Server is down, there may be post dial delay in attempting to call the Server.

Troubleshoot Configuration for connection to a Server

To troubleshoot a server failure due to configuration, verify the current Registration and SIP Server Options configured on the Sonus SBC 1000/2000.

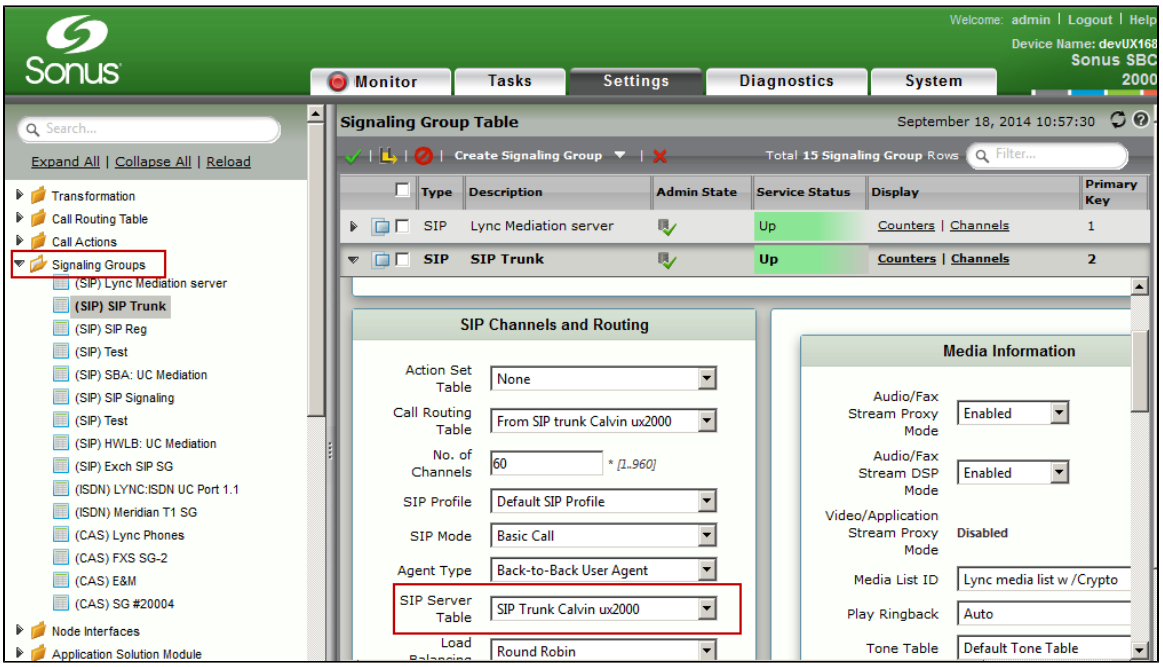
Verify Signaling Group

In the Signaling Group screen, the selections available in the **SIP Server Table** drop down list are derived from the entries configured in the SIP Server Table. This signaling group is used in the SIP Server Table and corresponds to the Server being contacted.

Verify the Signaling Group Server Table selected for this specific signaling group as follows:

Copyright © 2015 Sonus Networks. All rights reserved.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click on the desired SIP Signaling Group.
4. In the **SIP Channels and Routing** portion**,** verify the **SIP Server Table** selected.
5. Change or update as necessary. See Creating and Modifying SIP Signaling Groups.



Verify Registration/Monitor for SIP Options (for SIP Server)

Through the SIP Server Table, you choose the Contact Registrant table that will be used by a Signaling Group to register one or more contacts to a registrar. Contact Registrant Tables are used to manage contacts that are registered to a SIP server. When Monitor using SIP options is selected, an Options message is sent to the server with more detailed information, such as how often the Sonus SBC 1000/2000 queries the server with an Options message to determine the server's availability.

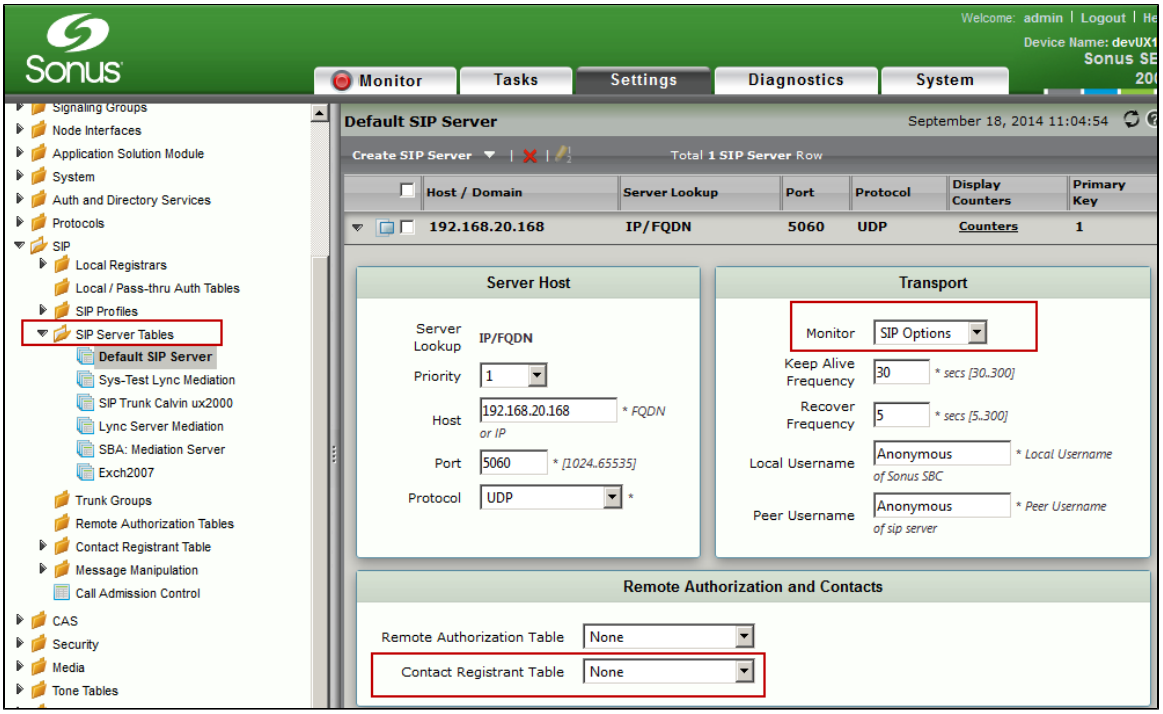
When a Server is unreachable and the problem is registration failing or SIP options not being successful, you can verify the configuration as follows:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP > SIP Server Table.**
3. Select the desired **SIP Server table** that corresponds to the Server being contacted.
4. Click the **Contact Registrant Table** drop down box. All available registration tables listed in the Contact Registrant Tables are displayed.

> When a challenge (401/407) is issued by the server, the table selected from the **Remote Authorization** drop down list is used by a SIP Server Table.

5. From the **Monitor** drop down list, select **SIP options**.
6. Verify the configuration and adjust, if necessary. See Creating and Modifying Entries in SIP Server Tables.

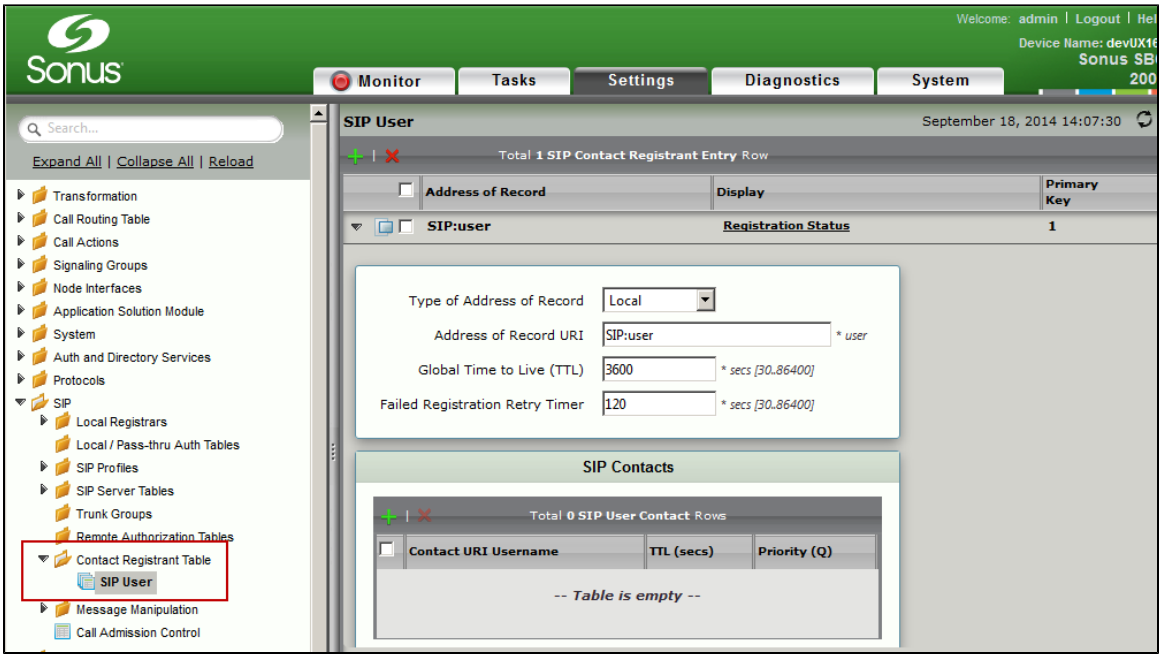
Copyright © 2015 Sonus Networks. All rights reserved.



Verify Configuration for Contact Registrant

The configuration configured in the Contact Registrant Tables is used to manage contacts that are registered to a SIP server. If registration to a Server is successful, but the Monitor using SIP Options fail, verify the following configuration.

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **SIP** > **Contact Registrant Table.**
3. Click the table that corresponds to the Server.
4. Verify the configuration (i.e. **Global Time to Live**) and adjust, if necessary. See Creating and Modifying Entries in Contact Registrant Tables.

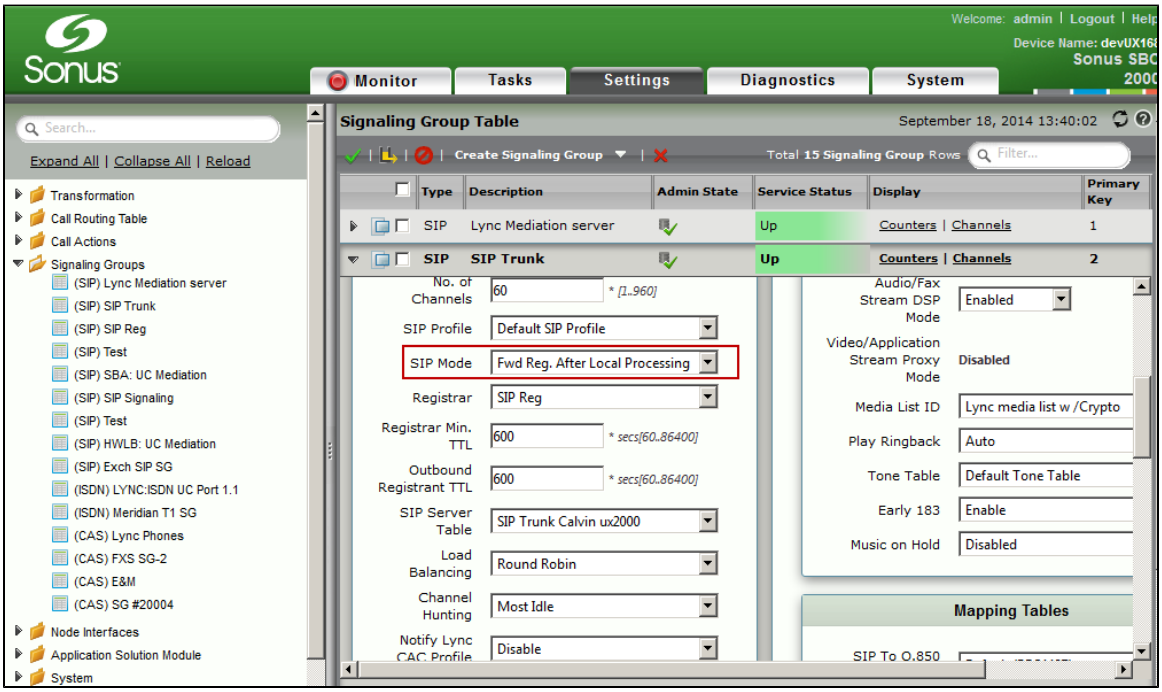


Copyright © 2015 Sonus Networks. All rights reserved.

Verify Forward Register Option

If registration to a Server is successful, but the Forward Register option fails, verify the following configuration:

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Signaling Groups**.
3. Click on the desired Signaling group that corresponds to the Server.
4. From the **SIP Mode** drop down list, select **Fwd Reg. after Local Processing**.



Copyright © 2015 Sonus Networks. All rights reserved.

SBC 1000-2000 Releases

Latest Release: Unified Exchange (Sonus SBC 1000/2000) 4.0.0

> **Read the full release notes.**

Please view the release notes to get up-to-date information about the improvements made in each release. If upgrading from a previous version of Sonus SBC 1000/2000 please pay attention to the Upgrade Notices of the latest version and any version of Sonus SBC 1000/2000 that your are 'skipping' during the upgrade.

Previous Production Releases

See the complete list of Release Notes for information about older releases.

Production Releases

Latest Release: Unified Exchange (Sonus SBC 1000/2000) 4.0.0

> **Read the full release notes.**

All Release Notes

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000/2000 4.0

- SBC 1000-2000 4.0.1 Release Notes
- SBC 1000-2000 4.0 Release Notes

Sonus SBC 1000/2000 3.2

- SBC 1000-2000 3.2.2 Release Notes
- SBC 1000-2000 3.2.1 Release Notes
- SBC 1000-2000 3.2 Release Notes

Sonus SBC 1000/2000 3.1

- SBC 1000/2000 3.1.3 Release Notes
- SBC 1000-2000 3.1.2 Release Notes
- SBC 1000-2000 3.1.1 Release Notes
- SBC 1000-2000 3.1 Release Notes

Unified Exchange (Sonus SBC 1000/2000) 3.0

- SBC 1000/2000 3.0.4 Release Notes
- SBC 1000/2000 3.0.3 Release Notes
- SBC 1000/2000 3.0.2 Release Notes
- SBC 1000/2000 3.0.1 Release Notes
- SBC 1000/2000 3.0 Release Notes

Unified Exchange (Sonus SBC 1000/2000) 2.2

- UX 2.2.1 Release Notes
- UX 2.2 Release Notes

Unified Exchange (Sonus SBC 1000/2000) 2.1

- UX 2.1.3 Release Notes
- UX 2.1.2 Release Notes
- UX 2.1.1 Release Notes
- UX 2.1 Release Notes

Unified Exchange (Sonus SBC 1000/2000) 2.0

- UX 2.0.2 Release Notes
- UX 2.0.1 Release Notes
- UX 2.0 Release Notes

SBC 1000-2000 4.1 Release Notes

January 6, 2015

The Sonus team is proud to deliver a brand new version of the industry's best Unified Communications, Enterprise Session Border Controller and Multi-Service Business Gateway.

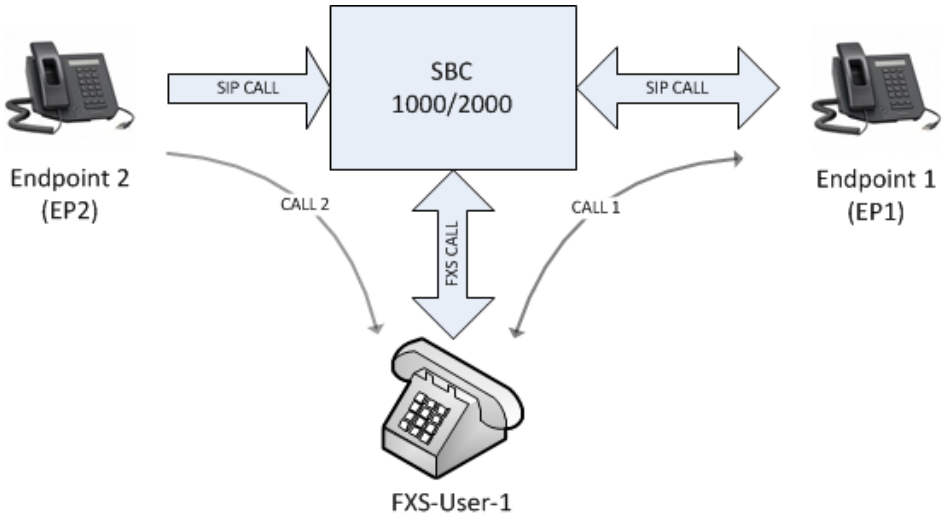
Sonus SBC 1000/2000 System Release 4.1.0 build 369 is a feature release and provides new features and enhancements to the Sonus SBC 1000/2000 product line.

Copyright © 2015 Sonus Networks. All rights reserved.

New Features

FXS Call Waiting Support

Beginning with Release 4.1.0, the SBC 1000/2000 now supports call waiting for devices terminated on an SBC 1000/2000 FXS port.



E911: Enable Use of ELIN Numbers In CompanyName Field

SBC 1000/2000 Version 4.1.0 now includes the Emergency Location Identification Number (ELIN) in the CompanyName field for each location as specified in the Microsoft Lync documentation.

This enhances the scalability of the SBC 1000/2000 deployment in a Lync environment. For more information see the Managing Transformation Tables section in the user documentation.

Partial Export-Import in User Interface

SBC 1000/2000 Version 4.1.0 introduces the ability to import and export partial configurations to and from other SBC 1000/2000 units.

Dynamic Host Resolution

SBC1000/2000 Version 4.1.0 introduces internal Dynamic Host Resolution. This feature allows the SBC to utilize an internal DNS server as a Branch Office DNS, allowing the Lync client to resolve the SBA FQDN and mutual FQDN resolution between the SBC and the SBA. For more information see: Managing the Hosts Table.

SIP INVITE Support with Replace

SBC1000/2000 Version 4.1.0 introduces the support for the SIP INVITE method with Replace, also known as a Call Pick-up feature. This feature enables an external device to pick-up an existing call, in either an alerting or collecting state, on the SBC.

Copyright © 2015 Sonus Networks. All rights reserved.

Software Upload Progress Bar

SBC1000/2000 Version 4.1.0 introduces the presence of a software upload progress bar. This user experience enhancement helps the user monitor the progress of the software upload process. Progress is displayed for the following stages of the upgrade process:

- File upload
- Partition preparation
- Writing the firmware image

TLS v1.2 Support

SBC1000/2000 Version 4.1.0 introduces support for the TLS v1.2 specifications. For more information about this feature see: Managing TLS Profiles.

Release Notices

Be aware that this upgrade has **strict dependencies** . To ensure a successful upgrade, you **must follow the** SBC 1000-2000 4.1.0 Upgrade Notes.

- For a listing of known issues and limitations, please review the Notes and Limitations page.
- For system performance information, see the Sonus SBC 1000/2000 System Performance and Capacity page.

Updates and Fixes in this Release

Bug ID	Headline
SYM-18353	Not responding to SIP UNREGISTER challenge when contact modified
SYM-17243	Alert user when SDP contains SRTP, but SIP signalling has TCP/UDP
SYM-18165	Expand upper limit for call progress tones to 3400 Hz
SYM-18279	Allow video call rerouting upon call failure in Survivable Mode
SYM-18380	Remove SHA384 hardware acceleration
SYM-17765	MediaStreamController memory leak with certain downstream forking
SYM-17534	SBC 1000 main board DSP Ethernet packet switching reliability
SYM-17372	Enhance SIP Server Entry WebUI Dialog

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-18303	SIP INVITE without SDP results in no audio
SYM-18304	CAS SG call forward options apply to analog FXS only
SYM-17448	SIP WARNING header not passed through
SYM-17950	G.722.2 to G.729 transcode call audio quality
SYM-17417	Contact Registrant table modification take effect only by removing/adding the table to server
SYM-17616	SIP with DNS-SRV stability improvements
SYM-17878	SBC2k SIP Stopped Processing shortly after upgrade **
SYM-17365	Alarm grammar enhancements
SYM-17375	MSC Transcoding and Video Passthrough log enhancements
SYM-17299	Include "transport=" parameter in REGISTER from UX Contact Registrant Table
SYM-18113	Microsoft® Lync Setup Emergency Callback Number format does not allow '+'
SYM-18169	Prevent switch to modem pass-through after T38 is negotiated
SYM-18218	SMM rule for custom header fails parsing if not configured in lower case
SYM-18239	Call Routing table name spelling error generated by Microsoft® Lync wizard
SYM-18114	Decrease delay between Register Requests from 1Sec to 200mSec when not staggering
SYM-18168	Validate Server FQDN not set to a default value
SYM-17621	SBC 2000 management bus access enhancements
SYM-18271	SBA should use static IP during initial setup
SYM-18003	Persistent socket re-use for outgoing call transfer and redirect transaction flows
SYM-17308	Microsoft® Active Directory Server may take longer than 15 seconds to respond
SYM-17386	Suppress erroneous SIP error log message for Music on Hold call flow
SYM-17049	Support CED/CNG relay in T.38
SYM-17353	REST SIP Server configuration access
SYM-17902	Reject non repudiation certificates at run-time
SYM-17952	Enforce 500ms lower bound for CAS R2 inter-digit timer
SYM-17227	Incorrect transport used to phones registered with TLS
SYM-17385	Ensure refreshed ARP cache for active video call endpoints
SYM-17461	Remove non-alpha numeric characters from AlarmConfiguration.csv
SYM-17357	Save and Restore SSRC for TX audio stream during call transfer
SYM-17345	SIP SG Protocol and Listen Port configuration REST validation
SYM-15731	Eliminate duplicate state change messages for SG and channel state changes
SYM-16673	Handle optiontags in multiple require header lines sent in SIP Messages

SBC 1000-2000 4.1 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 4.1.0.

- Notes for All SBC 1000-2000 Systems

Copyright © 2015 Sonus Networks. All rights reserved.

- UX2000 eUSB Upgrade Note
- Upgrading from a 2.x Release?
  - Mandatory Configuration Backup
  - New Base License for Release 3.1 and Higher
- Further Notes for SBC Systems with Built-in ASM's
  - Upgrading the SBC Communication Service
  - Installing the SBA Lync Server Cumulative Updates
  - Installing Windows Service Packs and Windows Updates Using ASM Roll-up Update

Before You Upgrade
The user account internal database format has changed between Release 3.1 and prior releases. As such, SBC nodes **will not operate correctly** if they are downgraded back to 3.0.x (or earlier) and the 3.1 configuration is left on the system. A configuration backup **must be performed** before the upgrade can proceed, so that it can be restored should a downgrade be necessary.

Notes for All SBC 1000-2000 Systems

Please observe and perform the following extra operations - they are specific to this 3.1 release.

Recommended Boot Image Upgrade

A new Boot Image upgrade (U-Boot 3.1.6o) is available with the release of the Sonus SBC 1000/2000 R3.1.0 b283 software.

Although upgrading the Boot Image is not mandatory, it is highly recommended. This release of the Boot Image remedies a known issue with resetting the SBC 1000/2000 to factory defaults.

UX2000 eUSB Upgrade Note

The eUSB based flash drive may require a firmware update. This is an automatic process and is executed as a part of the internal upgrade process. If the eUSB firmware is upgrded, the SBC2000 reboot process will run approximately one minute longer than usual.

This is applicable to the SBC2000 only.

NOTE: Loss of Logs and Core Dumps

If the eUSB upgrade is executed, all logs and core dumps will be lost. However the SBC Configuration will not be affected.

Upgrading from a 2.x Release?

If you are upgrading from a release prior to 3.0, please follow the instructions in the SBC 1000-2000 3.0 Upgrade Notes, **in addition** to these.

Mandatory Configuration Backup

A configuration backup must be performed before proceeding with the SBC upgrade. Instructions on how to do this, along with the upgrade procedure itself, are included in the general SBC upgrade guide.

New Base License for Release 3.1 and Higher

Copyright © 2015 Sonus Networks. All rights reserved.

After the upgrade to 3.1, a new Base License will have to be installed. You can obtain the 3.1 Base License from your Salesforce Portal.

Further Notes for SBC Systems with Built-in ASM's

Upgrading the SBC Communication Service

Upgrading the SBC Communications Service is covered in the general SBC upgrade guide. Make sure that it is upgraded, then follow the remaining instructions here - extra steps are required to update the ASM Recovery Partition.

Installing the SBA Lync Server Cumulative Updates

> You may skip this section if your SBC 1000-2000 hardware is not configured with a built-in ASM deployed as a Lync SBA.

Microsoft has released the following Cumulative Updates for these respective Lync Server releases:

Release	CU number	Release Date	More Information
Lync Server 2010	Cumulative Update 11	January 2014	KB2493736
Lync Server 2013	Cumulative Update 7	October 2014	KB2809243

Perform the following to apply this update to the Lync deployed ASM:

1. Download the CU package from the Salesforce Portal.
2. Follow the instructions outlined in Installing Cumulative Updates for Lync SBA.

Installing Windows Service Packs and Windows Updates Using ASM Roll-up Update

Release 2.2 introduced new functionality to install Windows Service Packs and Windows Updates - ASM Roll-up Update. Sonus publishes **Update Packs** on a regular basis through the Salesforce Portal. The Update Packs work with Windows Update and other Non-Windows updates in order to keep the ASM up-to-date. The Update Packs contain tested and authorized Windows updates. Note that the Update Packs do not contain the actual Windows Service Packs and Updates. Once the Update Pack has been installed, the Windows Update State link in the Operational Status section will change to **Updates Available - Install**. The actual updates are installed using this link.

SBC 1000-2000 4.0 Release Notes

October 14, 2014

The Sonus team is proud to deliver a brand new version of the industry's best Unified Communications, Enterprise Session Border Controller and Multi-Service Business Gateway.

Sonus SBC 1000/2000 System Release 4.0.0 build 353 is a feature release and provides new features and enhancements to the Sonus SBC 1000/2000 product line.

New Features

Copyright © 2015 Sonus Networks. All rights reserved.



Broadsoft Interoperability

Release 4.0.0 includes Broadsoft® validation that the SBC 1000/2000 is interoperable with the Broadsoft® Broadworks Server as an Enterprise SBC.

Features include;

- Video media Pass-through
- Broadsoft Remote Survivability
- Broadsoft Enterprise Trunking Support
- Registration Pass-through
- Subscribe/Notify Pass-through
- SIP INFO DTMF Support
- Advanced Phone Services (Busy Lamp, Feature Key, Shared Call)



Alternate RADIUS Connectivity Check

Release 4.0.0 of the SBC 1000/2000 introduces a mechanism to ensure connectivity to RADIUS Accounting and Authorization Servers which which do not support RFC 5997. The RADIUS server configuration now provides two options for the connectivity packet type; (1) Status-Server (RFC 5997), or (2) Request (Access-Request or Accounting-Request).

For more details about this feature, see Creating and Modifying RADIUS Servers.



Syslog Server Setup Enhancement

Release 4.0.0 of the SBC 1000/2000 introduces the ability to setup Syslog servers during the initial setup wizard of the SBC 1000/2000.

For more information, see Running Initial Setup.



Restart Reports

Release 4.0.0 of the SBC 1000/2000 introduces the availability of restart reports. Restart Reports simplifies troubleshooting the SBC 1000/2000 by providing the following information under Diagnostics Tab of the Web-based user interface.

- A list of the past SBC restarts along with reasons for each
- Display of log messages from Hardware Power-On-Self-Test
- A list of all core files and the user-friendly Web-based user interface for deleting or transferring core files from SBC 1000/2000 to a management PC

For more information, see Restart Reports.



Real-time Monitor

Release 4.0.0 of the SBC 1000/2000 introduces a new and improved Real-time monitor. The new Real-time monitor employs HTML 5 WebSockets and CSS, eliminating the need to open non-standard management ports (TCP port 2004) as well as eliminating the need for a Java® plug-in.

For more information, see the following pages in the Sonus SBC 1000/2000 documentation:

- Monitoring Real Time Status
- Supported Platforms

Copyright © 2015 Sonus Networks. All rights reserved.



SG3 to G3 FAX Fallback Support

Release 4.0.0 of the SBC 1000/2000 introduces support for connections made between two Super G3 (SG3) fax machines.

If enabled, the SG3 to G3 Fax Fallback feature, modifies the negotiation process of end-to-end SG3 to SG3 fax devices to negotiate T.38 G3 fax data rates.

For more information, see the following pages in the Sonus SBC 1000/2000 documentation:

- Managing Media Profiles
- Creating and Modifying Fax Profiles



G.722 and G.722.2 (AMR-WB) Wide Band Codec Support

Release 4.0.0 of the SBC 1000/2000 introduces support for G.722 and G.722.2 Wide Band codecs, including transcoding between Wide Band codecs as well as between Wide Band and supported Narrow Band codecs. This enhancement is supported through the Media Profiles.

For more information about this feature, see Managing Media Profiles.



Adjusted RTP Port Range

Release 4.0.0 of the SBC 1000/2000 includes a modification to the valid range of the RTP Port Range Start Port parameter. The range is now ports 1024 through 32767 inclusive to avoid potential conflicts with Linux kernel ephemeral port range. The previous range was ports 1024 through 65534.

Release Notices

Be aware that this upgrade has **strict dependencies**. To ensure a successful upgrade, you **must follow the** SBC 1000-2000 4.0 Upgrade Notes.

Sonus is aware of and working to address the Bash CVE-2014-6271 and CVE-2014-7169 vulnerability issue.

For more information see Bash Vulnerability CVE-2014-6271 and CVE-2014-7169 aka Shellshock

- For a listing of known issues and limitations, please review the Notes and Limitations page.
- For system performance information, see the Sonus SBC 1000/2000 System Performance and Capacity page.

Updates and Fixes in this Release

Bug ID	Headline
SYM-17330	SIP log message removal

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-17303	Allow filtering of Authorization header qop parameter via SMM regex rule
SYM-17337	Security: Add 'exit' after all header("Location:") calls
SYM-17331	Security: Disable telnet before initial setup
SYM-17339	Security: Hide all file path information from Error dialogs
SYM-17338	Security: Do not accept arbitrary file paths
SYM-17332	Security: Restrict served web page data when not authenticated
SYM-17223	Fix issue installing ASM/SBA updates from the Settings page
SYM-16464	IPC session management enhancement
SYM-17232	Contact-URI parameter decode failure
SYM-17217	Enhance SIP ERROR log message
SYM-16576	ISDN log message removal
SYM-17211	Increase the TLS Handshake timeout to 30 secs for the Microsoft® Lync setup wizard
SYM-17167	Add online help for Diagnostics "Port Mirror"
SYM-16881	Fix erroneous alarms generated after first system start-up after upgrade from R3.1.x or earlier code
SYM-16886	CAS process stability improvement when using drain mode
SYM-16877	MSC process stability improvement
SYM-16635	Flush TLS profile context when CA is flushed
SYM-16940	MSC process stability improvement
SYM-16951	Add status update for system vitals
SYM-16276	Fix incorrect counters in the "SIP Server Counters" Web User Interface view
SYM-16217	Improve Local Passthru Auth table data validation when importing .csv file
SYM-14854	Column sorting on ASM Windows Firewall Rule Web User Interface
SYM-16218	Log message removal
SYM-16438	Accept register requests only for enabled SG's
SYM-16930	SIP transport layer socket error handling enhancement
SYM-16794	Backup configuration contains incorrect Platform Type
SYM-14967	Reordered Domain Controller attributes in table and detail Web User Interface
SYM-16780	SIP memory leak with invalid certificate installed
SYM-16738	REST partial factory default action failed
SYM-16681	If RADIUS user matches a local user, but logs in using RADIUS passwd, they are forced to change passwd
SYM-16740	System-restore failed in REST and WebUI with error code 20027
SYM-16683	Disable saved login password field in Firefox and Chrome
SYM-15974	TLS Alarm generated for invalid Web User Interface session id
SYM-16592	Uxlogd process made restartable and monitored
SYM-16638	Retrieve exception when install file is missing at SBCComms boot-time
SYM-16627	Modify signature authentication of ASM installer files

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-16457	Correct help web links
SYM-16523	MOH deriving audio from FXS live audio stream does not function across reboot
SYM-16281	Allow import of multiple Trusted CA certificate with same commonName
SYM-16379	Additional configuration validation for platform type mismatch
SYM-16229	Support multiple Microsoft® ActiveDirectory™ group membership lists
SYM-16373	SIP process stability improvements
SYM-16329	Passphrase explanation text Web UI enhancements
SYM-16377	Update platform type values
SYM-16663	Offer configured media list when RE-INVITE is received without SDP
SYM-12968	Determine the status of a SG and SIP Server table based on the status of outbound SIP registration in Registrant Table
SYM-16617	Parsing embedded Reason header in History-Info
SYM-16679	Text field width adjustment in Web User Interface combo boxes
SYM-16397	Alarm for USB flash storage mounting failure
SYM-11809	Hold Invite (Inactive SDP) not sent when Analog FXS port does a Hook-flash
SYM-16567	Unpopulated SBC 2000 PSU displayed as "N/A" in the Card/Module Status view
SYM-16398	Restructured Microsoft® Domain Controller request/response handler
SYM-16328	SBC 2000 FXS ports may not display in the port view
SYM-16223	FXS call does not clear if associated CAS SG is disabled during call
SYM-16280	Missing ID in Certificate non-volatile data store
SYM-16360	Early Media detection stopped on all forked legs if one of them sends 180 Ringing w/o SDP
SYM-16358	Restore configuration platform validation enhancement
SYM-16364	Enable file browser field after backup in Upgrade page
SYM-16272	T1 or E1 port without SG can cause the erroneous real time monitor channels status
SYM-16265	SIP Profile: UA Header/Trusted Interface Interaction
SYM-15986	SNMP retry modification for failed FQDN look-ups
SYM-16275	Add ability to clear DHCP leases, and clear the leases automatically after initial configuration
SYM-8984	SIP INVITE MaxForwards not decremented
SYM-13477	Calling Party number support in CAS E&M
SYM-15400	Incorrect destination when sending SIP 481 response to cancel request using UDP transport
SYM-16278	Web User Interface Backup passphrase text modification
SYM-16279	Web User Interface Restore Configuration to Sonus SBC dialog text modification
SYM-14488	Populating FXO channel number doesn't route calls unless all channels in SG are configured with a channel number
SYM-14048	Node/Module Inventory Table sorting consistent across platform models

SBC 1000-2000 4.0 Upgrade Notes

Copyright © 2015 Sonus Networks. All rights reserved.

This document contain specific upgrade notes for customers planning to upgrade to SBC 4.0.0.

- Notes for All SBC 1000-2000 Systems
- UX2000 eUSB Upgrade Note
- Upgrading from a 2.x Release?
  - Mandatory Configuration Backup
  - New Base License for Release 3.1 and Higher
- Further Notes for SBC Systems with Built-in ASM's
  - Upgrading the SBC Communication Service
  - Installing the SBA Lync Server Cumulative Updates
  - Installing Windows Service Packs and Windows Updates Using ASM Roll-up Update

Before You Upgrade
The user account internal database format has changed between Release 3.1 and prior releases. As such, SBC nodes **will not operate correctly** if they are downgraded back to 3.0.x (or earlier) and the 3.1 configuration is left on the system. A configuration backup **must be performed** before the upgrade can proceed, so that it can be restored should a downgrade be necessary.

Notes for All SBC 1000-2000 Systems

Please observe and perform the following extra operations - they are specific to this 3.1 release.

Recommended Boot Image Upgrade

A new Boot Image upgrade (U-Boot 3.1.6o) is available with the release of the Sonus SBC 1000/2000 R3.1.0 b283 software.

Although upgrading the Boot Image is not mandatory, it is highly recommended. This release of the Boot Image remedies a known issue with resetting the SBC 1000/2000 to factory defaults.

UX2000 eUSB Upgrade Note

The eUSB based flash drive may require a firmware update. This is an automatic process and is executed as a part of the internal upgrade process. If the eUSB firmware is upgrded, the SBC2000 reboot process will run approximately one minute longer than usual.

This is applicable to the SBC2000 only.

NOTE: Loss of Logs and Core Dumps

If the eUSB upgrade is executed, all logs and core dumps will be lost. However the SBC Configuration will not be affected.

Upgrading from a 2.x Release?

If you are upgrading from a release prior to 3.0, please follow the instructions in the SBC 1000-2000 3.0 Upgrade Notes, **in addition** to these.

Mandatory Configuration Backup

Copyright © 2015 Sonus Networks. All rights reserved.

A configuration backup must be performed before proceeding with the SBC upgrade. Instructions on how to do this, along with the upgrade procedure itself, are included in the general SBC upgrade guide.

New Base License for Release 3.1 and Higher

After the upgrade to 3.1, a new Base License will have to be installed. You can obtain the 3.1 Base License from your Salesforce Portal.

Further Notes for SBC Systems with Built-in ASM's

Upgrading the SBC Communication Service

Upgrading the SBC Communications Service is covered in the general SBC upgrade guide. Make sure that it is upgraded, then follow the remaining instructions here - extra steps are required to update the ASM Recovery Partition.

Installing the SBA Lync Server Cumulative Updates

> You may skip this section if your SBC 1000-2000 hardware is not configured with a built-in ASM deployed as a Lync SBA.

Microsoft has released the following Cumulative Updates for these respective Lync Server releases:

Release	CU number	Release Date	More Information
Lync Server 2010	Cumulative Update 11	January 2014	KB2493736
Lync Server 2013	Cumulative Update 7	October 2014	KB2809243

Perform the following to apply this update to the Lync deployed ASM:

1. Download the CU package from the Salesforce Portal.
2. Follow the instructions outlined in Installing Cumulative Updates for Lync SBA.

Installing Windows Service Packs and Windows Updates Using ASM Roll-up Update

Release 2.2 introduced new functionality to install Windows Service Packs and Windows Updates - ASM Roll-up Update. Sonus publishes **Update Packs** on a regular basis through the Salesforce Portal. The Update Packs work with Windows Update and other Non-Windows updates in order to keep the ASM up-to-date. The Update Packs contain tested and authorized Windows updates. Note that the Update Packs do not contain the actual Windows Service Packs and Updates. Once the Update Pack has been installed, the Windows Update State link in the Operational Status section will change to **Updates Available - Install**. The actual updates are installed using this link.

SBC 1000-2000 4.0.1 Release Notes

Sonus SBC 2000 System Release 4.0.1 build 354 is a maintenance release, providing the hot fix listed below.

Release 4.0.1 applies to the SBC 2000 only, and does not apply to the SBC 1000.

Don't have SBC 4.0 yet?

Take a look at the new features and other highlights in the SBC 1000-2000 4.0 Release Notes.

Copyright © 2015 Sonus Networks. All rights reserved.

Ready to upgrade to 4.0.1?

Review the SBC 1000-2000 4.0.1 Upgrade Notes
Download Latest Version

Upgrades and Fixes in this Release

Bug ID	Headline
SYM-17981	SBC 2000 System Management Bus stability enhancement

SBC 1000-2000 4.0.1 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 4.0.1.

- Mandatory configuration backup
- Upgrading from SBC 1000-2000 version 4.0.0
- Upgrading from prior releases
  - Upgrade for 3.0 and later
  - Upgrades prior to 3.0

Mandatory configuration backup

A configuration backup must be performed before proceeding with the SBC upgrade. Instructions on how to do this, along with the upgrade procedure itself, are included in the general SBC upgrade guide.

Upgrading from SBC 1000-2000 version 4.0.0

There are no special considerations for upgrading from an earlier 4.0.x release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

NOTE: You must be running 3.0.x or higher prior to upgrading to 4.0.x

Upgrade for 3.0 and later

The upgrade instructions for 4.0.1 are the same as those for 4.0.0. Please follow the instructions outlined in the SBC 1000-2000 4.0 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

Upgrades prior to 3.0

If upgrading from a release prior to 3.0, take note of the following steps:

1. Perform a mandatory configuration upgrade while still on **2.2.1 build 207.**
2. Follow the instructions in SBC 1000-2000 3.0 Upgrade Notes, in addition to the SBC 1000-2000 4.0 Upgrade Notes. Specifically, upgrade as follows:
   a. Upgrade from **2.2.1 build 207** to **3.0** GA build for download.
   b. Proceed with upgrade from **3.0** to **4.0.x**.

Copyright © 2015 Sonus Networks. All rights reserved.

As part of Release 3.0, all SIP-SIP call sessions now require a SIP license. This new license key must be applied **before** upgrading to 3.0. For details, see the Release Notes,

SBC 1000-2000 3.2 Release Notes

July 22, 2014

The Sonus team is proud to deliver a brand new version of the industry's best unified communications, enterprise session border controller and multi-service business gateway. **Sonus SBC 1000/2000 System release 3.2.0 build 315** is a feature release and provides new features and enhancements to the Sonus SBC 1000/2000 products

New Features



Password Recovery

This feature allows for the recovery of passwords when they have been lost or forgotten. This feature may be turned on during initial configuration or anytime thereafter through the UI. Simply pressing the reset button for three seconds creates a temporary administrator user and password that can be used to reset the passwords of existing users.



TDM Port Licensing

Beginning with release 3.2.0, the SBC 1000/2000 series requires a license for each TDM port.



Custom Passphrases

This new feature allows the use of a custom passphrase to re-encrypt passwords in an exported configuration file so that the passwords can be decrypted by the importing node.



SHA-2 256 Support

Beginning with release 3.2.0, the SBC 1000/2000 series supports SHA-2 256 certificates.



Redundant Ethernet for SBC 1000

Version 3.2 introduces support for Redundant Ethernet functionality on the SBC1000. The SBC1000 Redundant Ethernet functionality is the same as the SBC2000, including limitations.

For more information about this feature, see Working with Multiple Spanning Trees

Copyright © 2015 Sonus Networks. All rights reserved.



ASM Operating Mode Detection

Version 3.2 introduces the ASM Operating Mode Detection (ASM Support Mode) functionality. The support mode for the ASM module is now dependent upon whether or not the customer has installed third-party software on the ASM.

There are three modes:

- **Appliance Certified Mode:** The ASM image contains v3.2 SbcComms or later and no third-party software has been installed.
- **Appliance Controlled Mode:** The original ASM image was a version previous to 3.2 and has been upgraded.
- **Server:** A third-party software installation has been detected by the ASM.



ASM Image Version Deployment Warning

The ASM is shipped with two versions of Microsoft Lync, 2010 and 2013. Microsoft Lync 2010 is the default installation. If SBA is being deployed in a Lync 2013 environment, the SBA must be running Lync 2013, otherwise the deployment will fail in the certificate phase. A warning now appears in the Deploy SBA tab,



TLS Session Resumption

The TLS Session Resumption feature improves latency and computational cost (when persistent TCP/IP socket connection is disabled) by providing the ability to resume or share the same negotiated secret key data between multiple connections. The TLS server session resumption period is set to 300 seconds for which a maximum of 1500 cached sessions are retained. This feature is supported on both the TLS server and client side.

Copyright © 2015 Sonus Networks. All rights reserved.

> ⚠ Be aware that this upgrade has **strict dependencies** . To ensure a successful upgrade, you **must follow the** **SBC 1000-2000 3.2 Upgrade Notes** .

- For a listing of known issues and limitations, please review the Notes and Limitations page.
- For system performance information, see the Sonus SBC 1000/2000 System Performance and Capacity page.

Monitor Fails When Port Description Contains a Semi-colon

If the port description field contains a semi-colon followed by a space and additional text, the Monitor will not initialize fully. This issue is addressed in the next release of software (v4.0).

Work Around

Modify the DS1 Port Description(s) such that there are no semi-colons.

CA Certificate Effectivity

When a CA certificate is deleted or replaced, the old CA certificate remains in effect until the SBC is rebooted. This issue will be addressed in a future release.

Shipping Policy Update

With the introduction of Release 3.2 of the SBC 1000/2000, Sonus now ships the following field installable/field replaceable hardware options in cartons separate from the SBC 2000 systems they are ordered with:

- **SBC-2K-CRD-T1E1:** SBC2000 T1/E1 Module w/1 T1/E1, Licensable growth to 8 T1/E1
- **SBC-2K-CRD-24FXS:** Telco Module, 24 FXS Ports
- **SBC-2K-PSU-AC:** SBC2000 AC Power Supply

Installing any or all of these components can be completed in a matter of minutes using the SBC2000 installation instructions on the Sonus support site. These components slide and lock into place in clearly marked locations and no special training or tools are required. The system software automatically recognizes the card and provided tools to configure it.

> ⚠ The T1/E1 and FXS cards are **not** hot-swappable. Therefore, the system **must powered down** befo re installing theses options.

See the SBC 1000/2000 Installation and Upgrade Guide for more information about rack mounting and installation requirements. Please contact your Sonus Channel Account Manager or Sonus Support for any further quesitons.

Updates and Fixes in this Release

Bug ID	Headline

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-16213	DoS security vulnerability in rsync (CVE-2014-2855)
SYM-16169	Security vulnerability in strongSwan (CVE-2014-2338)
SYM-16103	Configuration Manager may raise 'new configuration' alarm in error in certain circumstances
SYM-16092	Diversion with two ordinals is truncated to the first ordinal
SYM-16202	Microsoft Active Directory (AD) login may fail when user is a member of a large number of groups
SYM-16160	Fixed hotline support for T1/CAS/FXS
SYM-16120	UC-CallStats.my MIB modification
SYM-16119	Mask Remote Authorization Table Entry on REST importconfig
SYM-16051	ISDN channels may not be released after the call is cleared by a disconnected with PI in-band info
SYM-16059	Show only valid ISDN signaling switch variants based upon T1/E1 selection in Create/Modify SG
SYM-16228	Selection of alternate TLS profile ID in the SIP SG does not take affect
SYM-16224	REST bulk GET for Microsoft Active Directory (AD) controller status return extra id 65535
SYM-15368	Synchronize reporting of card/module status in WebUI
SYM-16100	Remove challenge call SIP user password from syslog
SYM-15993	Missing Radius Config, Runtime and Statistics REST APIs
SYM-15994	Missing REST API for Domain controllers status
SYM-15963	SBA service may restart
SYM-15088	Enhance debug facility for Registrar
SYM-15946	TDM port operational status as shown in the details view incorrect
SYM-15947	No audio may occur in certain outbound call flows
SYM-15972	Transport layer epoll_ctl error recovery
SYM-15992	Modify Monitor applet permissions to support Java™ Runtime Environment (JRE) 8
SYM-15777	Initiating SDP Offer with transcoding may contain incorrect codec order
SYM-15584	Microsoft Lync 2013 user can't hear Ringback tone when calling to PBX
SYM-15593	Handle escaped fields in From tag
SYM-15556	Session timer operation upon receipt of SIP 422 response
SYM-15820	Provisional handling improvement while in a connected state
SYM-15818	SMM issue encoding SG user value token
SYM-15999	Media Stream Controller stability improvement
SYM-15497	SBC 2000 eUSB in read-only state
SYM-15975	Allow empty IP domain in the initial setup wizard
SYM-16040	Fix case sensitivity issue between ActiveDirectory field in routing table and cache
SYM-16021	Fix CAS apply to channel 'Add' button visibility
SYM-15553	Improve configuration validation to prevent RTP/RTCP media port conflicts
SYM-15545	Fix messaging framework timeout errors seen with high OPTIONS exchange traffic
SYM-15736	SIP response may be sent to incorrect destination

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-15750	Support delayed release when receiving multiple Progress Indicator IEs
SYM-15592	ITSP SIP trunk capacity issue observed
SYM-15744	Respond with SIP 488 response code when offered no matching codecs
SYM-15594	Inconsistency between active alarms and Alarm LED state
SYM-15674	Allow RC2 for PKCS12 certificate import
SYM-15702	Initial ISDN Status Enquiry sent with wrong CRV length on BRI
SYM-15867	Throttle the ICMP response trace logs for Syslog server requests from SBC
SYM-14878	Enhance IPSec subnet scaling
SYM-15369	Report number of current calls in progress in CAS SG
SYM-14933	No audio after call transferred on ISDN BRI trunk
SYM-15772	Online help page for CAC
SYM-15453	CommonCallControl messaging session cleanup upon call failure
SYM-15778	UPDATE transaction handling improvement
SYM-15815	Improve ISDN SG tone table configuration validation
SYM-12311	Remove requirement to enter Primary Address and Net Mask when interface Admin State is Disabled
SYM-10860	Limit UX maximum hosts entry to 50 from REST API
SYM-15570	Allow the import of certificate containing multiple CN-ID's
SYM-15543	Common Call Control stability improvement
SYM-15523	Create SIP Server table with re-use timeout set to forever from Microsoft Lync Wizard
SYM-15457	Link monitor configuration sub net validation improvement
SYM-15569	SIP call hold/resume disconnect when transcoding from G729 to G711
SYM-15403	SIP memory usage improvement for TLS transport without socket re-use
SYM-15575	Event log message reduction
SYM-15598	SMM failed to add a PPI header with TEL-URI
SYM-15058	Add peak usage of counters in WebUI
SYM-15194	Fix DNS SIP server counters port when configured for TLS port other than 5060
SYM-15304	Extra packet with XML document containing success code returned immediately after backup response
SYM-15377	Enable ASM Microsoft Windows Update Action via REST
SYM-15367	Enable ASM Microsoft Lync Cumulative Update via REST
SYM-15188	Remove the backup config file on the SBC 1000 after it is saved
SYM-15041	Fix resource leak when modifying default VLAN via REST API
SYM-15136	Support PRACK with SDP
SYM-15083	Fixed SBC 1000 ASM service status inconsistency
SYM-15170	Fixed RFC2833 payload type DSP configuration
SYM-15401	Support ISDN Facility message reception prior to Call Proceeding
SYM-15193	DNS SRV servers may not be properly cached depending upon upon priority value

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-15398	Modify MAC address validation for SBC 1000
SYM-15490	BMP stability improvement
SYM-15462	Modify ASM/QOE alarm grammar
SYM-15492	Creation of Active Directory domain controller entry for authentication incorrectly requires LDAP query
SYM-15521	Include SBC FDQN in Microsoft QoE database look-up to support large networks
SYM-15557	Disable mode 6 and 7 NTP query responses
SYM-15460	Disconnect call after 20 downstream dialogs reached
SYM-15431	Add "SIP-TLS handshake failed to start negotiation" Alarm
SYM-15405	Fixed SIP signaling source set to a VLAN
SYM-15456	Add ASM Inventory information to sbconconfig REST API resource
SYM-15404	Enhance SIP application socket error handling
SYM-13010	Generate an alarm in the event of a CAC update failure
SYM-14846	SIP application UDP transport memory optimization
SYM-14842	CAS R2 may send wrong DNIS and ANI to the signaling peer
SYM-15040	Allow modification of default VLAN if secondary IP address configured
SYM-15057	Disallow configuration restore if platform type mismatch
SYM-15022	Modify Feature Licenses page to reflect DSP resources
SYM-15056	Retransmitted INVITE to incorrect SIP server
SYM-14939	Allow unregistrations in CAC overload condition
SYM-14938	Ensure any pending SIP Overload alarm is cleared when CAC is disabled
SYM-15067	BMP stability improvement
SYM-14941	SIP registration stability improvement
SYM-14971	Improve session cleanup in the case of forked inbound registrations
SYM-14984	Symsock application stability improvement when modifying default VLAN via REST API
SYM-14978	Fix GET /rest/asmfactoryimage/x REST API command
SYM-14973	Static ARP REST documentation change
SYM-14972	RIP and OSPF REST documentation change
SYM-15020	Avoid refresh Registers when Unregister configuration changed
SYM-15097	Raise alarm if system configuration is generated from a newer software release
SYM-15149	Improve validation for Debug Facility IgnoreICMP command via REST
SYM-15166	Add support for encode/decode Allow-Event header
SYM-13430	MediaStreamController stability improvement
SYM-15109	ActiveDirectory logins may stop functioning
SYM-15181	Add timestamp to Java Monitor Applet
SYM-2439	Reflect Blue Alarm condition on SBC 2000 front panel LED
SYM-15191	Added SIP content-Length and content-Type validation

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-15187	REST API documentation improvement
SYM-15106	Fixed RTP port allocation mechanism in certain SIP transfer call flows
SYM-15148	SIP application Call Session stability improvement
SYM-15075	Alarm generation for SRV record resolution errors
SYM-15074	Fixed QOE alarm clearing and severity
SYM-15072	SIP registration stability improvement
SYM-15077	SIP FQDN error handling stability improvement
SYM-15076	Correct clearing event for TLS handshake failure
SYM-15086	Pre-shared secret in IPsec Tunnel is shown in plain text in WebUI
SYM-14488	Support non-sequential numbering for FXO Channel Phone Numbers
SYM-14048	Fix sorting of Node/Module Inventory table to be consistent across SBC models
SYM-14944	Improve SIP application DNS error handling
SYM-14943	Improve osys syslog memory utilization reporting
SYM-14946	Fix formatting of Debug Facility "sg register" command output
SYM-14884	Fix decoding SIP message History-Info header
SYM-14896	SIP should honor Session-Expires value contained in 200 OK response received
SYM-14785	Excessive SIP memory utilization
SYM-14885	Fixed RTP port allocation mechanism in certain SIP early update call flows
SYM-14931	SIP application TLS connection re-use timeout stability improvement
SYM-14909	Re-level SIP, CommonCallControl, ISDN, and MediaStreamController syslog Error messages
SYM-14789	Check contact-URI not only user portion of contact header
SYM-15062	Forward registration after local processing when using FQDN
SYM-15046	Allow restoration of system configuration > 2MB via REST API
SYM-15027	Fix debug log output from SBC Monitor Java applet
SYM-15021	Remove obsolete table uxChannelTable from SNMP
SYM-15017	Fix SNMP SG call counters operation after graceful call termination
SYM-15050	Mark non-INVITE server transactions as complete after sending response
SYM-15059	Block support for SSLv2 in a fallback mode where higher protocol version capability was not advertised
SYM-15079	Fixed specific interface diagnostics ping function from WebUI
SYM-15066	SIP application stability improvement
SYM-14982	Debug facility may incorrectly indicated that "USB is not mounted"
SYM-14957	Change FQDN routing look-up to be case insensitive
SYM-14958	Alter parsing of SIP messages containing multipart/alternative SDP
SYM-14954	Fix usage of SRV Record Weight in DNS Server configuration
SYM-14949	Reduce syslogd log severity level as appropriate
SYM-14948	Hide LDAP Query for Authentication Domain Controllers

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-14961	Messaging Framework stability improvement
SYM-14962	Force DNS refresh upon host change configuration
SYM-14976	SIP Application stability improvement
SYM-14947	CAS R2 logging at Trace level may include incorrect ANI characters on termination leg
SYM-14963	Improve CAS R2 stop tone message filtering
SYM-14899	Adjusted SIP log message verbosity levels

SBC 1000-2000 3.2 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 3.2.0.

- Notes for All SBC 1000-2000 Systems
- UX2000 eUSB Upgrade Note
- Upgrading from a 2.x Release
  - Mandatory Configuration Backup
  - New Base License for Release 3.1 and Higher
- Further Notes for SBC Systems with Built-in ASM's
  - Upgrading the SBC Communication Service
  - Installing the SBA Lync Server Cumulative Updates
  - Installing Windows Service Packs and Windows Updates Using ASM Roll-up Update

Before You Upgrade
The user account internal database format has changed between Release 3.1 and prior releases. As such, SBC nodes **will not operate correctly** if they are downgraded back to 3.0.x (or earlier) and the 3.1 configuration is left on the system. A configuration backup **must be performed** before the upgrade can proceed, so that it can be restored should a downgrade be necessary.

Notes for All SBC 1000-2000 Systems

Please observe and perform the following extra operations - they are specific to this 3.1 release.

Recommended Boot Image Upgrade

A new Boot Image upgrade (U-Boot 3.1.6o) is available with the release of the Sonus SBC 1000/2000 R3.1.0 b283 software.

Although upgrading the Boot Image is not mandatory, it is highly recommended. This release of the Boot Image remedies a known issue with resetting the SBC 1000/2000 to factory defaults.

UX2000 eUSB Upgrade Note

The eUSB based flash drive may require a firmware update. This is an automatic process and is executed as a part of the internal upgrade process. If the eUSB firmware is upgrded, the SBC2000 reboot process will run approximately one minute longer than usual.

This is applicable to the SBC2000 only.

Copyright © 2015 Sonus Networks. All rights reserved.

NOTE: Loss of Logs and Core Dumps

If the eUSB upgrade is executed, all logs and core dumps will be lost. However the SBC Configuration will not be affected.

Upgrading from a 2.x Release

If you are upgrading from a release prior to 3.0, please follow the instructions in the SBC 1000-2000 3.0 Upgrade Notes, **in addition** to these.

1. Perform a mandatory configuration upgrade while still on **2.2.1 build 207.**
2. Follow the instructions in SBC 1000-2000 3.0 Upgrade Notes, in addition to the SBC 1000-2000 3.2 Upgrade Notes. Specifically, upgrade as follows:
    a. Upgrade from **2.2.1 build 207** to **3.0** GA build for download.
    b. Proceed with upgrade from **3.0** to **3.x**

As part of Release 3.0 release, all SIP-SIP call sessions now require a SIP license. This new license key must be applied **before** upgrading to 3.0. For details, see Release Notes,

Mandatory Configuration Backup

A configuration backup must be performed before proceeding with the SBC upgrade. Instructions on how to do this, along with the upgrade procedure itself, are included in the general SBC upgrade guide.

New Base License for Release 3.1 and Higher

After the upgrade to 3.1, a new Base License will have to be installed. You can obtain the 3.1 Base License from your Salesforce Portal.

Further Notes for SBC Systems with Built-in ASM's

Upgrading the SBC Communication Service

Upgrading the SBC Communications Service is covered in the general SBC upgrade guide. Make sure that it is upgraded, then follow the remaining instructions here - extra steps are required to update the ASM Recovery Partition.

Installing the SBA Lync Server Cumulative Updates

You may skip this section if your SBC 1000-2000 hardware is not configured with a built-in ASM deployed as a Lync SBA.

Microsoft has released the following Cumulative Updates for these respective Lync Server releases:

Release	CU number	Release Date	More Information
Lync Server 2010	Cumulative Update 11	January 2014	KB2493736
Lync Server 2013	Cumulative Update 7	October 2014	KB2809243

Perform the following to apply this update to the Lync deployed ASM:

Copyright © 2015 Sonus Networks. All rights reserved.

1. Download the CU package from the Salesforce Portal.
2. Follow the instructions outlined in Installing Cumulative Updates for Lync SBA.

Installing Windows Service Packs and Windows Updates Using ASM Roll-up Update

Release 2.2 introduced new functionality to install Windows Service Packs and Windows Updates - ASM Roll-up Update. Sonus publishes **Update Packs** on a regular basis through the Salesforce Portal. The Update Packs work with Windows Update and other Non-Windows updates in order to keep the ASM up-to-date. The Update Packs contain tested and authorized Windows updates. Note that the Update Packs do not contain the actual Windows Service Packs and Updates. Once the Update Pack has been installed, the Windows Update State link in the Operational Status section will change to **Updates Available - Install**. The actual updates are installed using this link.

SBC 1000-2000 3.2.1 Release Notes

Sonus SBC 1000/2000 System Release 3.2.1 build 322 is a maintenance release, providing the hot fixes listed below.Don't have SBC 3.2 yet?

Take a look at the new features and other highlights in the SBC 1000-2000 3.2 Release Notes.

Ready to upgrade to 3.2.1?

Review the SBC 1000-2000 3.2.1 Upgrade Notes
Download Latest Version

Upgrades and Fixes in this Release

Bug ID	Headline
SYM-17330	SIP log message removal
SYM-17303	Allow filtering of Authorization header qop parameter via SMM regex rule
SYM-17223	Fix issue installing ASM/SBA updates from the Settings page
SYM-17331	Security: Disable telnet before initial setup
SYM-17337	Security: Add 'exit' after all header("Location:") calls
SYM-17339	Security: Hide all file path information from Error dialogs
SYM-17338	Security: Do not accept arbitrary file paths in syslogDetails.php
SYM-16999	Supplement alarm/event state changes with logging entry
SYM-16749	Remove domain name from SAN of the ASM/SBA certificate request
SYM-17053	Fix source id for alarm/events
SYM-16843	Options method Dead Call Detection
SYM-17107	Review alarm/event descriptions
SYM-16931	Periodically log SIP application level resource usage

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-16634	SIP Memory leak upon receipt of certain ICMP response
SYM-16464	IPC session management enhancement
SYM-17151	Domain Controller Alarms not shown properly if same DC as Auth & Call Route
SYM-17211	Increase the TLS Handshake timeout to 30 secs for the Microsoft® Lync setup wizard
SYM-17178	Chrome browser compatibility enhancement
SYM-17232	Contact-URI parameter decode failure
SYM-17155	Retransmission of ACK to 200 OK after transition to connected state
SYM-16734	Create 'Pending' status for Microsoft® QoE server to be used for intermediate states
SYM-16877	MSC process stability improvement
SYM-16635	Flush TLS profile context when CA is flushed
SYM-16881	Fix erroneous alarms generated after first system start-up after upgrade to R3.2.x
SYM-16592	Uxlogd process made restartable and monitored
SYM-17008	SIP process stability improvement
SYM-16951	Add status update for system vitals
SYM-16992	SIP process stability improvement
SYM-6797	Fix DS1 Port / SG statistics (call counters for blocked and active calls)
SYM-16940	MSC process stability improvement
SYM-16886	CAS process stability improvement when using drain mode
SYM-16582	Disable selecting T.38 as the only, or as first codec in media list
SYM-16780	SIP memory leak with invalid certificate installed
SYM-16799	SIP REGISTER request is not forwarded if domain name is not configured
SYM-16800	Web UI / JASON serialization of single quotes
SYM-16779	Inbound calls fail to find SG reboot required to work around
SYM-16794	Config Backup with passphrase wipes out value in PlatformType tag in backup XML file
SYM-16760	SIP responds to a=inactive with a=sendrec
SYM-16738	REST partial factory default action failed
SYM-16665	SBC 1000 is not sending ACK for the 200 OK - MOH resume
SYM-16681	If RADIUS user matches a local user, but logs in using RADIUS passwd, they are forced to change passwd
SYM-16740	System-restore failed in REST and WebUI with error code 20027
SYM-16755	Enable audio path regardless of ISDN Progress Indicator type or presence
SYM-16607	Match phone context in received INVITE request
SYM-16409	Enhance R2 protocol sniff to function on a single E1 span
SYM-16427	Intermittent clearing of IPSec flow statistics counters
SYM-16229	Support multiple Microsoft® ActiveDirectory™ group membership lists
SYM-16446	Corrected SNMP trap OID ordering issue
SYM-16445	CCC process stability improvement

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-16430	Allow real-time monitor FXO channel call information display
SYM-16400	Incorrect real-time monitor call direction displayed for mediation bypass calls
SYM-16425	Enable TDM media path upon CONNECT without Progress Indicator and Alerting
SYM-16379	Additional configuration validation for platform type mismatch
SYM-16260	SBC 1000 debug Facility ad_cache command returns no results with USB drive installed
SYM-16452	Do not populate ingress SDP offer to egress leg, if egress is not in RTP Proxy mode
SYM-15363	NTT Caller ID
SYM-16232	DS1 Sync Alarm
SYM-16281	Allow import of multiple Trusted CA certificate with same commonName
SYM-16329	Passphrase explanation text Web UI enhancements
SYM-16389	SIP routing fail-over
SYM-16384	ACK should not include require: header
SYM-16377	Update platform type values
SYM-16390	Terminate Register Session when Register Server Session ends in RTP Proxy mode
SYM-16638	Retrieve exception when install file is missing at SBCComms boot-time
SYM-16632	Close sessions when session termination is challenged
SYM-16663	Offer configured media list when RE-INVITE is received without SDP
SYM-16660	Block the creation of more than 32 rows for Message Rules withing a single Message Rule Table entry
SYM-16662	Wrong reboot reason indicated in system_restart_log for configuration restoration
SYM-16717	"Last Reboot Reason" periodic log message descriptive text modification
SYM-14863	NTT Caller ID
SYM-16627	Modify signature authentication of ASM installer files
SYM-16523	MOH deriving audio from FXS live audio stream does not function across reboot
SYM-16512	Directory Services process stability improvement
SYM-16467	Maximum number of multiple spanning tree instances is 32
SYM-16457	Correct help web links
SYM-16602	Sending wrong SIP Server in "TO" header causing 403 Forbidden from Office 365
SYM-16536	Incorrect audio stream reported to the Microsoft® QoE Server for packet loss and jitter
SYM-16593	Expanded value range for 'max message play time'
SYM-16578	Allow early update for SIP to TDM since transcoding is done regardless of license

SBC 1000-2000 3.2.1 Upgrade Notes

Copyright © 2015 Sonus Networks. All rights reserved.

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.2.1.

- Mandatory configuration backup
- Upgrading from SBC 1000-2000 version 3.2.0
- Upgrading from prior releases
  - Upgrade for 3.0 and later
  - Upgrades prior to 3.0

Mandatory configuration backup

A configuration backup must be performed before proceeding with the SBC upgrade. Instructions on how to do this, along with the upgrade procedure itself, are included in the general SBC upgrade guide.

Upgrading from SBC 1000-2000 version 3.2.0

There are no special considerations for upgrading from an earlier 3.2.x release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

NOTE: You must be running 3.0.x or higher prior to upgrading to 3.2.x

Upgrade for 3.0 and later

The upgrade instructions for 3.2.1 are the same as those for 3.2.0. Please follow the instructions outlined in the SBC 1000-2000 3.2 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

Upgrades prior to 3.0

If upgrading from a release prior to 3.0, take note of the following steps:

1. Perform a mandatory configuration upgrade while still on **2.2.1 build 207.**
2. Follow the instructions in SBC 1000-2000 3.0 Upgrade Notes, in addition to the SBC 1000-2000 3.2 Upgrade Notes. Specifically, upgrade as follows:
   a. Upgrade from **2.2.1 build 207** to **3.0** GA build for download.
   b. Proceed with upgrade from **3.0** to **3.x**

As part of Release 3.0 release, all SIP-SIP call sessions now require a SIP license. This new license key must be applied **before** upgrading to 3.0. For details, see Release Notes,

SBC 1000-2000 3.2.2 Release Notes

Sonus SBC 1000/2000 System Release 3.2.2 build 327 is a maintenance release, providing the hot fixes listed below.Don't have SBC 3.2 yet?

Copyright © 2015 Sonus Networks. All rights reserved.

Take a look at the new features and other highlights in the SBC 1000-2000 3.2 Release Notes.

Ready to upgrade to 3.2.2?

Review the SBC 1000-2000 3.2.2 Upgrade Notes
Download Latest Version

Upgrades and Fixes in this Release

Bug ID	Headline
SYM-17981	SBC 2000 System Management bus stability enhancement
SYM-17955	SBC sends SIP REGISTER after receiving 401 w/stale=false
SYM-17879	Login to SBC from another browser during software upload fails
SYM-17963	Unable to download Microsoft® Active Directory cache file from Web UI on SBC 2000
SYM-17342	First call after reboot on an FXS port may fail in certain configurations
SYM-17557	SBC may not send SIP REGISTER when TTL expired
SYM-17490	Erroneous alarm generated upon E911 call
SYM-17676	SBC may assign inbound call bearer channel on E1 span "D" Channel
SYM-17370	Enhance parser to support SIP URI with % character in Refer-To header
SYM-17769	Excessive Microsoft® Active Directory interface worker threads
SYM-17347	Disable DES-CBC-SHA cipher for Web UI Monitor port
SYM-17273	Nonce counter not incremented for refresh Registrations
SYM-17209	Unable to install software patch release via Web UI
SYM-16765	SBC may store duplicate records in Microsoft® Active Directory cache

SBC 1000-2000 3.2.2 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.2.2.

- Mandatory configuration backup
- Upgrading from SBC 1000-2000 version 3.2.x
- Upgrading from prior releases
  - Upgrade for 3.0 and later
  - Upgrades prior to 3.0

Mandatory configuration backup

A configuration backup must be performed before proceeding with the SBC upgrade. Instructions on how to do this, along with the upgrade procedure itself, are included in the general SBC upgrade guide.

Upgrading from SBC 1000-2000 version 3.2.x

There are no special considerations for upgrading from an earlier 3.2.x release, beyond those mentioned in the

Copyright © 2015 Sonus Networks. All rights reserved.

general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

> **NOTE:** You must be running 3.0.x or higher prior to upgrading to 3.2.x.

Upgrade for 3.0 and later

The upgrade instructions for 3.2.2 are the same as those for earlier 3.2.x releases. Please follow the instructions outlined in the SBC 1000-2000 3.2 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

Upgrades prior to 3.0

If upgrading from a release prior to 3.0, take note of the following steps:

1. Perform a mandatory configuration upgrade while still on **2.2.1 build 207.**
2. Follow the instructions in SBC 1000-2000 3.0 Upgrade Notes, in addition to the SBC 1000-2000 3.2 Upgrade Notes. Specifically, upgrade as follows:
    a. Upgrade from **2.2.1 build 207** to **3.0** GA build for download.
    b. Proceed with upgrade from **3.0** to **3.x**

As part of Release 3.0, all SIP-SIP call sessions now require a SIP license. This new license key must be applied **before** upgrading to 3.0. For details, please see the 3.0 Release Notes.

SBC 1000-2000 3.1 Release Notes

January 6, 2014

The Sonus team is proud to deliver a brand new version of the industry's best unified communications, enterprise session border controller and multi-service business gateway. **Sonus SBC 1000/2000 System release 3.1.0** is a feature release and provides new features and enhancements to the Sonus SBC 1000/2000 products

New Features



Microsoft Lync Quality of Experience (QoE) Reporting

Release 3.1 introduces the Microsoft Lync QoE feature. The Quality of Experience (QoE) feature enables statistics reporting of all call legs to a QoE Server in order to provide quality monitoring. The information collected helps administrators better understand the media quality that users experience. With QoE monitoring, the administrators can:

- Record statistics for the SIP trunk leg of the call
- Gather statistics on media quality at individual locations or based on a grouping of subnets.
- Proactively monitor and troubleshoot media quality of experience issues.
- Perform diagnostics in response to VoIP user complaints.
- View trends that can help them with post-deployment growth and measure results against the service level agreement.

For more information about this feature, see: Configuring Quality of Experience (QoE) Settings.

Copyright © 2015 Sonus Networks. All rights reserved.



RTP Proxy

Release 3.1 introduces the RTP Proxy feature. This provides efficient use of audio DSP resources by avoiding their use when both endpoints are SIP devices and have the ability to negotiate common media capabilities without the need for transcoding. It allows the establishment of audio calls when both endpoints are able to negotiate common codecs and media characteristics (i.e., ptime, etc). This feature also enables the support of unknown codecs. For more information about this feature, see: Creating and Modifying SIP Signaling Groups



SLA Thresholds and Historical Statistics Reporting

Release 3.1 introduces the ability for users to configure Threshold Crossing Alerts thresholds and collect historical statistics about system usage. Previously, statistics were only available via SNMP, beginning with Release 3.1 historical statistics will be available via the REST interface. For more information on this feature see: Working with Historical Data and TCA Thresholds



Programmatic Device Interface

The REST interface has been significantly enhanced to include almost all of the configuration and management functionality, including initial SBA setup.



Redundant Ethernet

Release 3.1 introduces the redundant Ethernet (multiple spanning tree) feature. This feature provides the SBC 2000 with the ability to connect two Ethernet ports of SBC's to two different switches which in turn provide access to the same network. This is useful because when one switch fails the other switch will provide access to the network.

It should be noted that this feature handles the failures of a switch in the network or the Ethernet ports on the UX by finding a different path around the failure. For more information about this feature see: Working with Multiple Spanning Trees



SBC 1000/2000 Management Security

Release 3.1 introduces significant security improvements and protection against brute force password breaking. Minimum password complexity rules, limits on failed login attempts, and password lifetime options have also been added. For more information about this feature see: Managing Global Security Options



DNS Service Record Queries

Release 3.1 introduces DNS SRV record queries. This feature enables the SBC's SIP module to create SIP server tables based on SRV record queries. For more information about this feature see: Managing SIP Server Tables and Creating and Modifying Entries in SIP Server Tables.



Exportable SBC and SBA Certificates

In Release 3.0 and earlier the WebUI provided facilities to expert the Sonus SBC and SBA 1000/2000 Certificates, how ever there was no facility to export a private key for those certificates. Beginning with Revision 3.1 the private keys are provided by means of a secure (user supplied) password protected PKCS12 file. The PKCS12 file can be imported on another node if the proper user supplied password.

Copyright © 2015 Sonus Networks. All rights reserved.



ISDN Facility Message Analysis Support

In Release 3.0 the SBC 1000/2000 gateway supported sending and retrieving the redirecting number carried in the facility element when connecting to PBX using QSIG switch variant. Beginning with Release 3.1, the SBC 1000/2000 gateway applies these functions to the EuroISDN variant based on ETS 300 207-1 and ETS 300 196-1 standards. This feature capability allows making routing decisions based on the redirecting number provided by PSTN through a Facility element.



Power On System Test (POST) Diagnostic Logs

This feature allows the users to display and download Power On System Test results using the Debug Facility option in the SBC 1000/2000 WebUI.



Node Info Logging

The node information logging in Release 3.1 has been enhanced to include additional details, including: hostname, presence of an SBA, last reboot reason, and system uptime.

Release Notices

> Be aware that this upgrade has **strict dependencies** . To ensure a successful upgrade, you **must follow the** **SBC 1000-2000 3.1 Upgrade Notes** .

- For a listing of known issues and limitations, please review the Notes and Limitations page.
- For system performance information, see the Sonus SBC 1000/2000 System Performance and Capacity page.

Updates and Fixes in this Release

Bug ID	Headline
SYM-14787	Disallow NULL (empty) passwords for AD Binds
SYM-14868	AD user mapped to Audit User on SBC 1K/2K does not get authorized
SYM-14790	Intermittent SIP Application restart with registered SIP endpoints
SYM-14883	Fix empty password string validation for Partial Config Import
SYM-14869	SIP call leg is dropped in dial-in conference
SYM-14880	Radius should not echo password (shared secret) in clear text
SYM-14771	SBC returns 488 "Not Acceptable Here" to re-INVITE w/o SDP that causes one way audio
SYM-14610	Call disconnects after attempting to resume call that was placed on hold
SYM-14653	DSP in incorrect state after in-use for a period of time resulting in call failures

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-14864	When using Tagged VLANs, SBC uses IP address of Logical Interface Instead of IP address of VLAN in SIP registrations
SYM-10528	Alarm view auto-refresh interval update doesn't take effect until current timer has expired
SYM-11432	Condition Rule Description shows as a number rather than string
SYM-4562	Call Id permanently locked by Call Independent SETUP
SYM-14552	SIP leaking call sessions in certain environments leading to instability
SYM-11496	UX log does not show SIP messages modified by SMM
SYM-14862	ASM/SBA: Does not update Current Status on IP config change if the previous action failed
SYM-14212	Service Status is N/A for all hardware modules except SBC 2000 Line Cards in System Overview Cards/Modules Table
SYM-13040	Configured Session Refresh Method not used depending on 200 OK response/header
SYM-14027	REST Docs updated to identify ifName to Port Name mapping for Ethernet ports and Logical Interfaces
SYM-10840	Monitor applet displays call connected without 200 OK response for INVITE
SYM-13227	SBA & PMAPI INFO log still generated when Syslog log level set to lower verbosity
SYM-14001	Current Status does not display correctly if ASM default gateway is modified
SYM-13384	Monitor Java applet is digitally signed by Sonus
SYM-14535	Unable to change Domain Controller password in WebUI
SYM-14582	Improve performance of certain older Point-of-Sale modems
SYM-14150	Internal process Connection Failure error path memory leak
SYM-14702	SIP registration licenses aren't being released with certain devices
SYM-14236	E911 PID-LO data sent to 911Enable service is incorrect
SYM-14740	Hostname configuration in node-level settings results in error message in log file
SYM-14774	FXO port state shown as unknown. Unable to add FXO port to CAS SG
SYM-14471	SIP Registration with Authentication incorrectly reflected in counter statistics
SYM-14783	Allow enabling the global log level to capture process start-up sequences after doing factory default
SYM-14650	Enhance ASM Windows Update error messages
SYM-8436	Removing Yellow alarm to remote peer when using CAS R2 leaves channel in release state
SYM-14673	"Help" broken on Monitor applet: goes to about:blank
SYM-8291	Updated OK button during On-Step Upgrade
SYM-14039	Any value can be entered for protocol in Address of Record URI field for CRT entry
SYM-14606	Enhanced validation to support IP address in addition to FQDN for TLS
SYM-14735	BMP application restart in certain scenarios
SYM-14700	CAA conference drops Tenor analog call after connecting
SYM-14499	Add pop-up to CSR generation window after 'OK' button is clicked
SYM-14468	Cseq value in a request is always incremented previous received one
SYM-14516	AD authentication rights given by the latest group membership
SYM-14491	Hold/Unhold failure when initiated by Lync between FXS and Lync

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-14527	RURI with tel: drops telephone number
SYM-13454	Lync SBA is restarting if SBC 1000 is restarted
SYM-14487	SIP abnormal termination
SYM-14521	Music-on-Hold failure if the a= attribute value is set to sendonly (a=sendonly) by the endpoint that is placing the call on hold
SYM-14448	Retain order of Record-Route header fields in SBC Route response.
SYM-14339	Put Min-SE in session refresh as documented in RFC 4028
SYM-14515	Add configuration item to control c= line in media section of SDP
SYM-10098	Pop-up windows used to specify date for the Export Date Range stays visible
SYM-14275	G.711 to T.38 Fax Transcoding failure
SYM-14310	Incorrect Current Activity Status after SBA joined domain
SYM-14496	"SG_MEDIA_ENDPOINT_IE(0x480) not found" error generated when SBC under load
SYM-14563	Add route name to transformation processing in log
SYM-14439	SBC sends RTP event in wrong Payload Type
SYM-7924	Range validation improvement for RTP/RTCP ports
SYM-14604	Local/Pass-through Authorization Table does not accept an entry with Type of AoR as Remote
SYM-14497	Unable to apply SMM rule to SRTP crypto line
SYM-13177	TLS Handshake Alert Failure alarm not cleared
SYM-14418	Update Options Tag configured to 'Not Present', but Allow header still contains Update
SYM-14565	Intermittent DS1 port initialization failure with fast link activation
SYM-10464	Remove SIP Profile Timer C from configuration
SYM-12851	Handle extra headers in Refer-To
SYM-13245	NTT CID detection issue
SYM-10920	Send BYE and drop call on Park with Lync
SYM-12877	Send NOTIFY for REFER after 603 Decline
SYM-14202	Power on SBA action starts even when the ASM is not in shutdown state
SYM-9085	SBC processes INVITE, upon receipt of an INVITE request with Expires header set to 0
SYM-11351	Header case not preserved
SYM-14066	Forwarded call from Lync 1 to Lync 2 failed due to missing server's FQDN in the "From" header
SYM-14061	183 changes the codecs order
SYM-14205	Intermittent abnormal SIP and CCC termination in certain environments
SYM-14042	One way audio on Lync calls 15-30 minutes after call retrieved from Hold
SYM-14256	"From" header not correct when CRT Type of AoR set to Local or Remote
SYM-14257	Retry Non-Stale Nonce=FALSE attempts to send REGISTER
SYM-14049	SBC 2000 power supply status indication
SYM-14251	UPDATE/re-INVITE for session refresh that always have the Min-SE even it has not received on that dialog

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-14241	SIP abnormal termination when TCP ping is used
SYM-14127	Interpretation APDU incorrectly abbreviated
SYM-14147	SBC not sending OPTIONS if unresolved FQDN of peer
SYM-14154	200 OK for re-INVITE has no Allow header
SYM-14163	Call fails when SBC receives a re-INVITE without SDP
SYM-14169	SBC not sending registration to SIP trunk provider after a connection drop
SYM-14168	Generate a new From-tag in REGISTER for refresh
SYM-14279	To-tag in 200 OK to CANCEL is missing
SYM-14120	Add Registration debug facility
SYM-14188	Add additional SIP debug commands to REST interface
SYM-14190	Lync Transfer Fails with Refer and Media Bypass enabled
SYM-14182	SIP memory leak and abnormal termination when running load with Fwd Reg. After Local Processing
SYM-14106	Call Transfer Fails. SBC does not appear to create Invite based on Refer
SYM-14107	Support for Firefox 24
SYM-14194	CAS R2 stop tone failure
SYM-14360	Early Updates messages responded to with 200 OK, but no SDP information
SYM-10652	Missing "extension" in msRTC-SIP attribute in AD Cache
SYM-14173	Unnecessary header in error response
SYM-13434	Rare SIP start-up initialization failure
SYM-14325	When Contact URI Randomizer is enabled and incoming INVITE does not have randomized request-URI, the called number is NULL
SYM-14299	Register session not cleaned up, if the contact registrant is removed from sip server configuration
SYM-9724	SBC needs to support contact:* for removing all bindings from a user (FROM header)
SYM-14297	Removing URI host should remove '@'
SYM-14056	SBC does not send SIP 481 to an unknown session
SYM-14178	Call terminated due to session timer mismatch
SYM-12831	Fwd REGISTER request does not transfer multiple CONTACTS separated by delimiter
SYM-13214	Support configuration of up to 8 VSI/VIVO DHCP option attributes
SYM-14140	SBC Does Not Route SIP Notify and Sends 503
SYM-5283	After SRTP key change, first hold from Lync fails
SYM-9123	SBC does not reject a Cancel request with a Via header set with a different branch parameter
SYM-13383	ASM failure intermittently indicated
SYM-14030	Operational status on the ASM did not update properly
SYM-14078	QSIG DiversionCounter not set correctly when performing SIP to ISDN redirect
SYM-13951	Blind transfer from Lync to PSTN one way audio
SYM-13653	SBC will not send REGISTER if unresolved host FQDN

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-13646	QSIG configuration change is volatile
SYM-13971	Incorrect CSeq handling for an SIP UnRegister
SYM-14006	Warn user if transformation table entries are disabled for a route
SYM-14007	Local Registrar user table WebUI presentation
SYM-14005	Increase size of Create Remote Authorization entry window
SYM-14003	MSC abnormal termination
SYM-14002	SIP abnormal termination
SYM-13532	Call Details for unallocated DS1 channel error
SYM-13368	Fixed TEI filtering resulting in Ingress BRI call failure
SYM-14104	SIP Transfer license enhancement
SYM-13347	Disallow IPsec tunnel with local 0.0.0.0/0 subnet
SYM-13301	IPsec tunnel does not not started if activation configuration is changed to Always
SYM-13316	Host name and DHCP Server settings should remain after a partial Factory Default
SYM-13389	IPsec link up despite subnet negotiation failure
SYM-13396	SNMP abnormal termination
SYM-5648	Framework ABORT Log message text clarification
SYM-13501	Disallow deletion of non-present static routes
SYM-13466	DSP abnormal termination under load
SYM-13465	CCC application restart, causing call failures
SYM-14010	Modified upload software error messages
SYM-13498	Unable to open SG Call Counters if special characters are present in the SG name
SYM-14083	Corrected TSI connection timing for TDM-SIP calls
SYM-14073	Alarm generated for a non-present hardware module
SYM-14060	Add configuration item in SIP profile for refresher failure handling
SYM-14057	REGISTER is incorrectly sent for first CRT entry if second entry is deleted after reboot
SYM-14053	One-way audio for a BRI call using overlap dialing
SYM-14054	SIP Transfer license enhancement
SYM-14098	REST linkmonitor resource DELETE fails
SYM-14094	SMM Regex "+" character will be removed when description is changed
SYM-14082	ACK message should not have P-headers
SYM-14091	Modify SG User value trace message
SYM-14080	Radius application restart
SYM-14077	Clicking 'Add/Edit' button or modifying description will change SMM literal value
SYM-14016	Creation of an ACL Rule table from REST unsuccessful
SYM-14052	Corrected AD attribute enforcement
SYM-14026	Allow multiple provisional messages to pass-through in Alerting state

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-14036	CTRL+Left Arrow doesn't move a word in a WebUI text field
SYM-14025	SBC incorrectly sends REGISTER w/Auth
SYM-14023	Intermittent DS1 port initialization failure with fast link activation
SYM-14018	"No Server cluster found" error messages generated when using Local Registrar
SYM-14022	Register is incorrectly sent when CRT assigned and SIP SG is in disabled state
SYM-14037	User part of Contact URI in Response is not randomized if called number is not the pilot number
SYM-14035	"Play Ringback" label is not consistent across Signaling Groups.
SYM-14051	Calling SBC sends UPDATE for session refresh and not send BYE
SYM-14044	SMM configuration Import/Export failure
SYM-14047	Exported certificate .der file is not Importable into the same node
SYM-13365	Reword WebUI text to allow loading an ASM Image without a flash drive
SYM-13105	Handle missing CRLF in SDP of ingress SIP message
SYM-13487	Incorrect SNMP System Description, Location, and Contact Validation values
SYM-7835	Enhanced validation of static route entries to disallow duplicates
SYM-13553	Port pop out table window is editable
SYM-9330	SBC does not responds to Register Request without Contact Header
SYM-13964	SIP abnormal termination
SYM-13275	Duplicate entries for call routing domain controllers allowed in Active Directory DC configuration
SYM-13277	IPsec responder uses pre-shared Remote Identified configuration
SYM-13262	SNMP application restart
SYM-13274	Fixed gradual SIP and CCC memory leak
SYM-13273	Enhanced IPSec tunnel configuration validation
SYM-13297	Windows firewall is able to create a deny rule for a specific required port
SYM-13298	Ringback not sent continuously when FXS ports calls another FXS port with CallerID enabled
SYM-13299	No Music on Hold audio when both endpoint on a call go on Hold/Unhold with "Live" audio source configured
SYM-13295	IPsec Statistics do not show negotiated addresses and subnets
SYM-13285	SIP abnormal termination
SYM-12985	FXS analog caller ID detects extra digit
SYM-12919	MSC abnormal termination
SYM-12984	MDMF Caller Id Generation Does Not Work For Odd Number Of Characters.
SYM-13074	Loss of connectivity to IPSec monitored host may result deterministic default route
SYM-12893	CMM secure connections table not updated upon IPSec SA deletion
SYM-12741	V.34 Fax pass-through handshaking failures
SYM-13304	SIP SG not responding to OPTIONS request
SYM-12394	Changed TIP/Ring polarity when generating Caller ID on FXS
SYM-13081	WebUI Large file upload support

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-13127	Add IPsec tunnel setup failure alarm
SYM-13224	Intermittent kernel panic during IPSec load
SYM-13241	Update Link Monitor Alarm condition
SYM-13210	SBC originated CANCEL on forked call does not eliminated missed call notification with Lync
SYM-13203	SMM is not used on Re-INVITE
SYM-13138	CAS abnormal termination when using Tone Disconnect Supervision
SYM-13168	CAS abnormal termination
SYM-13193	SBC unable to process certain History-info headers
SYM-13242	Link Monitor service status changes after poll configuration update
SYM-13387	SBC stops progress tone on SIP Registrar after initiating REFER on Lync
SYM-13388	SBC attempts to start an IPsec tunnel associated with inactive Link Monitor
SYM-13391	Increase range of supported XFRM policy ID's
SYM-13392	Restart required after certificate change
SYM-13372	Fixed WebUI Network Monitoring index/folder page
SYM-13370	SIP abnormal termination
SYM-13308	Send empty calling name in ISDN NI-2 as nameNotAvailable
SYM-13364	SIP abnormal termination
SYM-13369	NSM abnormal termination when IPSec under load
SYM-13397	Add/Remove buttons present on IPsec tunnel pop-up
SYM-13467	Enhance CAS SG configuration validation
SYM-13472	SBC intermittently brings SG down when performing ISDN E1 loop back upon reboot
SYM-13479	Attended transfer not functional when all endpoints are FXS devices
SYM-13457	Operational Status should indicate both Microsoft Windows up-time and SBC Comms up-time
SYM-13324	Allow SIP Options to piggyback on re-used connections
SYM-13320	No ring back on forwarded call after original termination disconnected
SYM-13315	Further distinguish "Called" from "Calling" on WebUI Transformation entry
SYM-13313	Blind Transfer w/"Live" Music on Hold source not functional when using FXS device
SYM-13319	Fixed ISDN bad number support
SYM-13311	Use correct timezone setting upon system reboot
SYM-13332	Change the User-Agent header to be specific for the type of SBC
SYM-13341	Selecting time zone UTC+12 displays incorrect time
SYM-13344	Added SMM Regex empty expression support
SYM-13310	Discard lost DNS queries statistic once same FQDN federated IP added
SYM-13314	Fix REST FXS Port Query
SYM-13179	Alert user if a USB Flash drive is present when performing an ASM reboot
SYM-13355	Delay AD cache refresh after reboot until network ready

Copyright © 2015 Sonus Networks. All rights reserved.

SBC 1000-2000 3.1 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 3.1.

- Notes for all SBC 1000-2000 systems
- Upgrading from a 2.x release?
  - Mandatory configuration backup
  - New Base License for Release 3.1
- Further notes for SBC systems with built-in ASM's
  - Upgrading the SBC Communication Service
  - Installing the SBA Lync Server Cumulative Updates
  - Installing Windows Service Packs and Windows Updates using ASM Roll-up Update

Before You Upgrade
The user account internal database format has changed between Release 3.1 and prior releases. As such, SBC nodes **will not operate correctly** if they are downgraded back to 3.0.x (or earlier) and the 3.1 configuration is left on the system. A configuration backup **must be performed** before the upgrade can proceed, so that it can be restored should a downgrade be necessary.

Notes for all SBC 1000-2000 systems

Please observe and perform the following extra operations - they are specific to this 3.1 release.

Recommended Boot Image Upgrade

A new Boot Image upgrade (U-Boot 3.1.6o) is available with the release of the Sonus SBC 1000/2000 R3.1.0 b283 software.

Although upgrading the Boot Image is not mandatory, it is highly recommended. This release of the Boot Image remedies a known issue with resetting the SBC 1000/2000 to factory defaults.

Upgrading from a 2.x release?

If you are upgrading from a release prior to 3.0, please follow the instructions in the SBC 1000-2000 3.0 Upgrade Notes, **in addition** to these.

Mandatory configuration backup

A configuration backup must be performed before proceeding with the SBC upgrade. Instructions on how to do this, along with the upgrade procedure itself, are included in the general SBC upgrade guide.

New Base License for Release 3.1

After the upgrade to 3.1, a new Base License will have to be installed. You can obtain the 3.1 Base License from your Salesforce Portal.

Further notes for SBC systems with built-in ASM's

Upgrading the SBC Communication Service

Upgrading the SBC Communications Service is covered in the general SBC upgrade guide. Make sure that it is

Copyright © 2015 Sonus Networks. All rights reserved.

upgraded, then follow the remaining instructions here - extra steps are required to update the ASM Recovery Partition.

Installing the SBA Lync Server Cumulative Updates

> You may skip this section if your SBC 1000-2000 hardware is not configured with a built-in ASM deployed as a Lync SBA.

Microsoft has released the following Cumulative Updates for these respective Lync Server releases:

Release	CU number	Release Date	More Information
Lync Server 2010	Cumulative Update 12	April 2014	KB2493736
Lync Server 2013	Cumulative Update 7	October 2014	KB2809243

Perform the following to apply this update to the Lync deployed ASM:

1. Download the CU package from the Salesforce Portal.
2. Follow the instructions outlined in Installing Cumulative Updates for Lync SBA.

Installing Windows Service Packs and Windows Updates using ASM Roll-up Update

Release 2.2 introduced new functionality to install Windows Service Packs and Windows Updates - ASM Roll-up Update. Sonus publishes **Update Packs** on a regular basis through the Salesforce Portal. The Update Packs work with Windows Update and other Non-Windows updates in order to keep the ASM up-to-date. The Update Packs contain tested and authorized Windows updates. Note that the Update Packs do not contain the actual Windows Service Packs and Updates. Once the Update Pack has been installed, the Windows Update State link in the Operational Status section will change to **Updates Available - Install**. The actual updates are installed using this link.

SBC 1000-2000 3.1.1 Release Notes

Sonus SBC 1000/2000 System Release 3.1.1 is a maintenance release, providing the hot fixes listed below.

Don't have SBC 3.1 yet?

Take a look at the new features and other highlights in the SBC 1000-2000 3.1 Release Notes.

Ready to upgrade to 3.1.1?

Review the SBC 1000-2000 3.1.1 Upgrade Notes
Download Latest Version

Upgrades and Fixes in this Release

Bug ID	Headline
SYM-15136	No response generated for PRACK with SDP
SYM-15404	Improved transport layer error handling
SYM-15431	Added alarm for TLS negotiation failure due to invalid certificate
SYM-15454	SG OPTION transaction cleanup upon event failure
SYM-15398	SBC 1000 MAC address validation enhancement

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-15367	Increase allowable size of SBA Update via REST API
SYM-15170	Support for alternate RFC2833 payload types
SYM-15083	SBC 1000 ASM service status indication
SYM-15194	DNS SIP Server Counters window correctly displays non-standard port
SYM-15457	IP subnet validation should not be performed when deleting link monitor entries
SYM-15401	Correctly handle receipt of ISDN Facility prior to Call Proceeding message
SYM-15557	NTP reflection attack security enhancement
SYM-15490	Enhance system recovery behavior upon BMP process restart
SYM-15492	Remove LDAP Query field from Create AD Domain Controller WebUI window
SYM-15460	Disconnect excessive early dialogs
SYM-15041	Fix issue modifying default VLAN via REST API
SYM-15304	Remove XML status block from all downloads via REST API
SYM-15058	Add SG and License historical usage counters to the Web UI
SYM-15521	Modify retrieval of QoE monitoring database location to support large networks
SYM-15456	Extend REST API sbaconfig resource to include inventory data
SYM-15193	Correctly populate priority 0 DNS SRV records in the DNS SRV Server table
SYM-15377	Add support to perform ASM Windows Updates via REST API
SYM-15462	Fix QoE alarm description
SYM-15188	Remove SBC 1000 backup config file after downloading
SYM-14935	Remove unnecessary event logs
SYM-14978	REST API command GET /rest/asmfactoryimage/x always return data for the first image
SYM-15086	Change IPSec tunnel pre-shared secret field type
SYM-15106	No audio on consultative transfers involving forked calls
SYM-14972	REST API documentation change for RIP and OSPF
SYM-14973	REST API documentation change for static ARP
SYM-15022	Change DSP channels to DSP resources in License Web UI page
SYM-15056	Fixed Ethernet address for retransmitted INVITE with VIA header to secondary SIP server
SYM-15020	Stop refresh timers when the Contact Registrant table is removed
SYM-15040	Modifying default VLAN not allowed if secondary IP address configured
SYM-15109	Turning Active Directory Server off and then on prevents AD logins
SYM-15148	Fixed SIP session handling if the called party sends BYE before answering the call
SYM-15191	Support Microsoft Exchange 2010 response to SIP OPTIONS
SYM-13430	MSC call forking stability enhancement
SYM-14736	Improved SIP listening port error handling
SYM-2439	Reflect DS1 Blue Alarm condition on SBC front panel LED
SYM-15187	REST API documentation update

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-15181	Add Monitor applet JAR file signature timestamp
SYM-15149	Add REST API validation for debug facility IgnoreICMP command
SYM-15097	Raise Alarm if SBC configuration is from a newer software release
SYM-15057	Allow configuration restoration only from the same product type
SYM-15077	SIP FQDN error handling enhancement
SYM-14842	Disable echo canceller for signaling-only DSP resources
SYM-14984	VLAN configuration validation enhancement
SYM-14846	SIP stability enhancement when using UDP transport
SYM-14941	SIP Server fails to start Registrations intermittently
SYM-15074	Alarm for errors storing QoE information should auto-clear
SYM-15075	Alarm for errors in resolving SRV record should auto-clear
SYM-15076	Alarm for errors in TLS handshake should auto-clear
SYM-15072	SIP stability enhancement
SYM-14971	SIP session cleanup of forked ingress Registers
SYM-14939	Allow unregister when in CAC overload condition
SYM-14938	SIP overload detected alarm does not clear after CAC disabled
SYM-14785	SIP stability enhancement with registrar SG
SYM-14957	Make SIP destination call routing comparison case insensitive
SYM-14962	Reload DNS cache upon relevant configuration change
SYM-14958	Correctly parse INVITE with Content-Type header configured as "multipart/alternative"
SYM-14789	Expand SIP contact-URI header parsing
SYM-14961	Inter-Process communication framework enhancement
SYM-14946	Debug facility 'sg register' output message formatting
SYM-14885	Fix intermittent one-way audio caused by handling of early update
SYM-14896	Use session timer value contained in Session–Expires header of 200 OK for initial INVITE
SYM-14906	Remove 'Refresh Method' from SIP configuration
SYM-14943	Fix free memory report in osys log message
SYM-14947	Ensure null termination of CAS R2 ANI
SYM-14884	Fix parsing of SIP History-Info header
SYM-14949	Reduced priority for syslog log entries related to periodic ID and node status
SYM-14977	Handle Re-INVITE without SDP in third party call control call flows
SYM-15062	SBC does not forward Re-Register when FQDN is used
SYM-15059	Disallow certain SSLv2 sessions in fallback mode
SYM-15050	SBC does not forward or respond to Re-INVITE in transfer call flow
SYM-15064	Allow adding remote entries into the SIP Local/Pass-though authorization table
SYM-15066	SIP stability enhancement

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-15079	Fix ping by interface via Web UI
SYM-15046	Fix configuration restore for files >2 MB via REST API
SYM-14976	SIP stability enhancement
SYM-15021	Remove uxChannelTable from SNMP MIB
SYM-15017	Fix SNMP MIB call counters to reflect errored and rejected call flows
SYM-15027	Fix debug logging from the Monitor applet

SBC 1000-2000 3.1.1 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.0.2.

- Upgrading from SBC 1000-2000 version 3.1.0
- Upgrading from prior releases

Upgrading from SBC 1000-2000 version 3.1.0

There are no special considerations for upgrading from an earlier 3.1.x release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

The upgrade instructions for 3.1.1 are the same as those for 3.1.0. Please follow the instructions outlined in the SBC 1000-2000 3.1 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

SBC 1000-2000 3.1.2 Release Notes

Sonus SBC 1000/2000 System Release 3.1.2 is a maintenance release, providing the hot fixes listed below.

Don't have SBC 3.1 yet?

Take a look at the new features and other highlights in the SBC 1000-2000 3.1 Release Notes.

Ready to upgrade to 3.1.2?

Review the SBC 1000-2000 3.1.2 Upgrade Notes
Download Latest Version

Upgrades and Fixes in this Release

Bug ID	Headline
SYM-16169	Security vulnerability in strongSwan (CVE-2014-2338)

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-16160	Fixed hotline support for T1/CAS/FXS
SYM-16119	Mask Remote Authorization Table Entry on REST importconfig
SYM-16202	Microsoft Active Directory (AD) login may fail when user is a member of a large number of groups
SYM-16224	REST bulk GET for Microsoft Active Directory (AD) controller status return extra id 65535
SYM-16228	Selection of alternate TLS profile ID in the SIP SG does not take affect
SYM-16260	Debug facility ad_cache command returns no results with USB drive installed on SBC 1000
SYM-16051	ISDN channels may not be released after the call is cleared by a disconnected with PI in-band info
SYM-16103	Configuration Manager may raise 'new configuration' alarm in error in certain circumstances
SYM-16092	Diversion with two ordinals is truncated to the first ordinal
SYM-16100	Remove challenge call SIP user password from syslog
SYM-15963	SBA service may restart
SYM-15994	Missing REST API for Domain controllers status
SYM-16120	UC-CallStats.my MIB modification
SYM-16389	Correct Remote Authorization Table match logic
SYM-15993	Missing Radius Config, Runtime and Statistics REST APIs
SYM-15992	Modify Monitor applet permissions to support Java™ Runtime Environment (JRE) 8
SYM-15947	No audio may occur in certain outbound call flows
SYM-15972	Transport layer epoll_ctl error recovery
SYM-15820	Provisional handling improvement while in a connected state
SYM-15584	Lync 2013 user can't hear Ringback tone when calling to PBX
SYM-15556	Session timer operation upon receipt of SIP 422 response
SYM-15593	Handle escaped fields in From tag
SYM-15777	Initiating SDP Offer with transcoding may contain incorrect codec order
SYM-15940	Fix the factory default CCPE configuration token
SYM-15999	Media Stream Controller stability improvement
SYM-15946	TDM port operational status as shown in the details view incorrect
SYM-15975	Allow empty IP domain in the initial setup wizard
SYM-16043	Correct media Sample rate and Payload type in QoE reports
SYM-16021	Fix CAS apply to channel 'Add' button visibility
SYM-15744	Respond with SIP 488 response code when offered no matching codecs
SYM-15772	Online help page for CAC
SYM-15778	UPDATE transaction handling improvement
SYM-15736	SIP response may be sent to incorrect destination
SYM-15594	Inconsistency between active alarms and Alarm LED state
SYM-14878	Enhance IPSec subnet scaling
SYM-14933	No audio after call transferred on ISDN BRI trunk

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-15592	ITSP SIP trunk capacity issue observed
SYM-15815	Improve ISDN SG tone table configuration validation
SYM-15702	Initial ISDN Status Enquiry sent with wrong CRV length on BRI
SYM-15750	Support delayed release when receiving multiple Progress Indicator IEs
SYM-15818	SMM issue encoding SG user value token
SYM-15867	Throttle the ICMP response trace logs for Syslog server requests from SBC
SYM-15543	Common Call Control stability improvement
SYM-15598	SMM failed to add a PPI header with TEL-URI
SYM-15575	Event log message reduction
SYM-15570	Allow the import of certificate containing multiple CN-ID's
SYM-15674	Allow RC2 for PKCS12 certificate import
SYM-15569	SIP call hold/resume disconnect when transcoding from G729 to G711
SYM-15403	SIP memory usage improvement for TLS transport without socket re-use
SYM-15457	Link monitor configuration sub netvalidation improvement

SBC 1000-2000 3.1.2 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.1.2.

- Upgrading from SBC 1000-2000 versions 3.1.0 and 3.1.1
- Upgrading from prior releases

Upgrading from SBC 1000-2000 versions 3.1.0 and 3.1.1

There are no special considerations for upgrading from an earlier 3.1.x release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

The upgrade instructions for 3.1.2 are the same as those for 3.1.0. Please follow the instructions outlined in the SBC 1000-2000 3.1 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

SBC 1000-2000 3.1.3 Release Notes

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000/2000 System Release 3.1.3 build 304 is a maintenance release, providing the hot fixes listed below.Don't have SBC 3.1 yet?

Take a look at the new features and other highlights in the SBC 1000-2000 3.1 Release Notes.

Ready to upgrade to 3.1.3?

Review the SBC 1000-2000 3.1.3 Upgrade Notes
Download Latest Version

Upgrades and Fixes in this Release

Bug ID	Headline
SYM-17105	Add help link to Microsoft® Internet Explorer compatibility view warning
SYM-17159	Updated Microsoft® Internet Explorer unsupported version banner warning
SYM-16634	SIP Memory leak upon receipt of certain ICMP response
SYM-16631	Use configured host FQDN instead of DNS CNAME or alias
SYM-17222	Continue processing QoE updates in the event of an update failure
SYM-17194	Online help page for Microsoft® Lync setup Web User Interface tab
SYM-17336	Enhance Web User Interface ping and traceroute input validation
SYM-17257	Alarm decode key parse error
SYM-16999	Supplement alarm/event state changes with logging entry
SYM-16843	Options method Dead Call Detection
SYM-16943	On screen warning for Microsoft® Internet Explorer compatibility mode
SYM-16931	Periodically log SIP application level resource usage
SYM-16715	Enhance SIP transaction level error handling
SYM-17053	Fix source id for alarm/events
SYM-17151	Domain Controller Alarms not shown properly if same Domain Controller used for Auth & Call Route
SYM-17156	Send ACK's to retransmitted 200 OK's after transitioned to connected state
SYM-17107	Events 15.03 and 15.04 need to have description changed
SYM-6797	DS1 port call counters return zero for blocked, in/out blocked and in/out active calls.
SYM-17009	SIP process stability improvement
SYM-16734	Create 'Pending' status for Microsoft® QoE server to be used for intermediate states
SYM-16755	Enable audio path regardless of ISDN Progress Indicator type or presence
SYM-16717	"Last Reboot Reason" periodic log message descriptive text modification
SYM-16749	Remove domain name from SAN of the ASM/SBA certificate request
SYM-16665	SBC 1000 is not sending ACK for the 200 OK - MOH resume
SYM-16607	Match phone context in received INVITE request
SYM-16760	SIP responds to a=inactive with a=sendrec

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-16582	Disable selecting T.38 as the only, or as first codec in media list
SYM-16800	Web User Interface / JASON serialization of single quotes
SYM-16779	Inbound calls fail to find Signaling Group; reboot required to work around
SYM-16799	SIP REGISTER request is not forwarded if domain name is not configured
SYM-15363	Japan (NTT) Caller ID enhancement
SYM-16660	Block the creation of more than 32 rows for Message Rules withing a single Message Rule Table entry
SYM-16232	DS1 Sync Alarm
SYM-16662	Wrong reboot reason indicated in system_restart_log for configuration restoration
SYM-14863	Japan (NTT) Caller ID enhancement
SYM-16284	Support CDR attribute for SIP PPI header value in INVITE message
SYM-16557	Set early media negotiated for TDM endpoint upon receipt of Progress Indicator
SYM-16566	Call Control process made non-restartable
SYM-16578	Allow early update for SIP to TDM since transcoding is done regardless of license
SYM-16602	Sending wrong SIP Server in "TO" header causing 403 Forbidden from Office 365
SYM-16632	Close sessions when session termination is challenged
SYM-16512	Directory Services process stability improvement
SYM-16373	SIP process stability improvement
SYM-16467	Maximum number of multiple spanning tree instances is 32
SYM-16072	FXS port call counter Web User Interface view XML parse error
SYM-16430	Allow real-time monitor FXO channel call information display
SYM-16446	Corrected SNMP trap OID ordering issue
SYM-16593	Increased allowable range for 'max message play time'
SYM-16536	Incorrect audio stream reported to the Microsoft® QoE Server for packet loss and jitter

SBC 1000-2000 3.1.3 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.1.3.

- Upgrading from SBC 1000-2000 versions 3.1.0 through 3.1.2
- Upgrading from prior releases

Upgrading from SBC 1000-2000 versions 3.1.0 through 3.1.2

There are no special considerations for upgrading from an earlier 3.1.x release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

Copyright © 2015 Sonus Networks. All rights reserved.

The upgrade instructions for 3.1.3 are the same as those for 3.1.0. Please follow the instructions outlined in the SBC 1000-2000 3.1 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

SBC 1000-2000 3.1.4 Release Notes

Sonus SBC 1000/2000 System Release 3.1.4 build 307 is a maintenance release, providing the hot fixes listed below.Don't have SBC 3.1 yet?

Take a look at the new features and other highlights in the SBC 1000-2000 3.1 Release Notes.

Ready to upgrade to 3.1.4?

Review the SBC 1000-2000 3.1.4 Upgrade Notes
Download Latest Version

Upgrades and Fixes in this Release

Bug ID	Headline
SYM-17981	SBC 2000 System Management bus stability enhancement
SYM-17963	Unable to download Microsoft® Active Directory cache file from Web UI on SBC 2000
SYM-17955	SBC sends SIP REGISTER after receiving 401 w/stale=false
SYM-17879	Login to SBC from another browser during software upload fails
SYM-17557	SBC may not send SIP REGISTER when TTL expired
SYM-17473	SIP Error log cleanup
SYM-17676	SBC may assign inbound call bearer channel on E1 span "D" Channel
SYM-17370	Enhance parser to support SIP URI with % character in Refer-To header
SYM-17490	Erroneous alarm generated upon E911 call

SBC 1000-2000 3.1.4 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.1.4.

- Upgrading from SBC 1000-2000 versions 3.1.0 through 3.1.3
- Upgrading from prior releases

Upgrading from SBC 1000-2000 versions 3.1.0 through 3.1.3

There are no special considerations for upgrading from an earlier 3.1.x release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

The upgrade instructions for 3.1.4 are the same as those for 3.1.0. Please follow the instructions outlined in the SBC 1000-2000 3.1 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has

Copyright © 2015 Sonus Networks. All rights reserved.

a **built-in ASM**.

SBC 1000-2000 3.0 Release Notes

Release Part Number: 481-40174-006

May 8, 2013

The Sonus team is proud to deliver a brand new version of the industry's best unified communications, enterprise session border controller and multi-service business gateway. Sonus SBC 1000/2000 System release 3.0.0 is a feature release and provides new features and enhancements to the Sonus SBC 1000/2000 products

Highlights of this Release:

- New Features
  - Branch Survivability Using 3G/4G
  - ASM Firewall Filtering
  - Asynchronous DNS Support
  - STUN Packet Control
  - DHCP Client
  - NAT Support
  - IP-IP T.38 passthrough and T.38 transcoding Support
  - NET to Sonus Rebranding
- Feature Enhancements
  - Call Forwarding on FXS Ports
  - Forked Calls Support for Call Completed Elsewhere Reason Header to Prevent missed Call Notifications in Lync or OCS
  - SIP Registration Enhancements
- Release Notices
  - SIP-SIP Licensing Support Changes
- Updates and Fixes in this Release

Download the latest version:

- First read the Release Notices for important information about this release.
- See the full list of Updates and Fixes in this Release.

Download Now

New Features



Branch Survivability Using 3G/4G

Copyright © 2015 Sonus Networks. All rights reserved.

This feature provides an alternative for maintaining Branch Office connectivity to the Headquarters facility in event of a failure of the primary WAN link, by redirecting traffic via IPsec tunnels across a backup network connection. Backup network connections are typically: 3G/4G Wireless or DSL cable modem/routers.

Many enterprises employ multiple branch sites connected to the headquarters (HQ) facility through a WAN link provided by a telecom vendor. Microsoft Lync ® clients at the branch office maintain connectivity with the corporate Lync server located at the headquarters. In the event of a telecommunication failure the WAN link may fail, thereby breaking connectivity between the branch and the HQ.

Sonus SBC devices are capable of interoperating with Microsoft's Lync solution for branch survivability in the event of such network failures. An SBC 1000 or SBC 2000 deployed at the branch-site can monitor the network links, identify such failures an switchover to a backup network connection, restoring IP layer connectivity between the branch and HQ. Thereafter by using the configuration data, voice and data connectivity may be restored between the branch and HQ, taking into account the security of data over the public Internet and the fact that the 3G/4G backup network connection usually has less bandwidth than the WAN link.

Sonus is the first and only vendor of Microsoft Lync Resilient Branch Appliance (RBA) solution providing branch survivability for Lync enterprises that is compliant with SBAv2 specifications.

For more information about this feature, see: Working with Branch Survivability and Configuring 3G4G Failover.



ASM Firewall Filtering

Beginning with release 3.0 the Sonus SBC 1000/2000 includes the ability to configure ACLs on the ASM Windows Firewall. This allows enterprise administrators to easily manage Microsoft Lync SBA as a true appliance through the single integrated Web User Interface of the SBC in the branch office. This feature is separate from the SBC 1000/2000 IP Protocol ACLs which may b applied to the ASM Port for inbound and forwarding traffic on the SBC 2000.

For more information about this feature, see: Managing the Windows Firewall on the ASM



Asynchronous DNS Support

Beginning with release 3.0 the Sonus SBC 1000/2000 supports Asynchronous DNS for SIP. Other applications and protocols, such as: RADIUS and AD continue to rely on synchronous DNS.



STUN Packet Control

Beginning with release 3.0 the Sonus SBC 1000/2000 includes the ability to control whether or not the SBC sends STUN packe on RTP/RTCP during call setup on outbound IP call legs.

For more information about this feature, see: Configuring the Media System.

Copyright © 2015 Sonus Networks. All rights reserved.



DHCP Client

Release 3.0 of the Sonus SBC 1000/2000 includes DHCP client functionality. Initial configuration of the SBC is now simplified with the availability of the DHCP client. SBC 1000 and SBC 2000 now have the same bring up procedure with release 3.0 and t use of Admin port with SBC 2000 is no longer recommended.

For more information about this feature, see: Managing the DHCP Client and Running Initial Setup.



NAT Support

Beginning with release 3.0, the Sonus SBC 1000/2000 supports Network Address Translation (NAT) allowing the SBC to functi as a true edge device, providing internet connectivity between hosts on local and private networks, and the public domain.

For more information about this feature, see: Working with NAT and Port Forwarding.



IP-IP T.38 passthrough and T.38 transcoding Support

Beginning with release 3.0 the Sonus SBC 1000/2000 now support T.38 passthrough for IP-IP enabling interworking with IP-FA servers in enterprise networks and other IP devices/SIP Trunks. Release 3.0 also supports G.711 to T.38 transcoding enabling FAX interworking for enterprises deploying SIP trunks.



NET to Sonus Rebranding

Beginning with release 3.0 the SBC 1000/2000 Web User Interface and documentation has been rebranded to match the Sonu brand guidelines. The Sonus SBC 1000 and Sonus SBC 2000 were formerly known as the NET UX1000 and UX2000.

Feature Enhancements



Call Forwarding on FXS Ports

Beginning with release 3.0 the Sonus SBC 1000/2000 now supports call forwarding on FXS ports.

Copyright © 2015 Sonus Networks. All rights reserved.



Forked Calls Support for Call Completed Elsewhere Reason Header to Prevent missed Call Notifications in Lync or OCS

In the event an incoming call is forked by the Sonus SBC 1000/2000 to multiple devices including SIP endpoints such as Lync and the call is answered by one of the non-Lync forked endpoints, the Sonus SBC 1000/2000 will include a Reason header in th CANCEL message with a *Call completed elsewhere* attribute to prevent the Lync or OCS server from posting a missed call notification.



SIP Registration Enhancements

The Sonus SBC 1000/2000 SIP server table now includes the capability to resequence the servers in the table. Additionally the Contact Registration table now includes a link to the Address of Record (AOR) for each registered user.

Release Notices

> ⚠ Be aware that this upgrade has **strict dependencies**. To ensure a successful upgrade, you **must follow the SBC 1000-2000 3.0 Upgrade Notes**.

- For a listing of known issues and limitations, please review the Notes and Limitations page.
- For system performance information, see the Sonus SBC 1000/2000 System Performance and Capacity page.

SIP-SIP Licensing Support Changes

Beginning with release 3.0 of the Sonus SBC 1000/2000 software, all SIP-SIP calls require a SIP license. Existing Sonus SBC 1000/2000 customers who purchased their systems and recieved SIP Licenses prior to January 1, 2013 are not affected by this change and should contact their Sonus sales representative for a *grandfathered* SIP License. No SIP license is required for SIP calls between Sonus (Formerly NET) devices.

NOTE: A single SIP *session* is defined as having two IP call legs - one inbound and one outbound. One license is required per *session*, not per leg.

Only one call case requires a SIP call license. This is the case where both inbound and outbound channels are SIP. The exception for SIP calls to another SBC 1000, SBC 2000, the Sonus Tenor Series or the Sonus VX Series, however, still exists. If one or both of the call legs are to one of these devices then a SIP call license will not be used.

Updates and Fixes in this Release

Bug ID	Headline
SYM-13315	Transformation Entry: Called versus Calling doesn't stand out enough

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-12741	Problems with Faxing
SYM-12394	Sanyo phone does not detect NTT caller ID
SYM-13237	Include a text file with the hardware inventory into the backup config file
SYM-13250	Increase max display length for columns in Transformation, Call Route, Action Config, and Action Set tables
SYM-13231	Print SN, HW ID, and software release in the debug logs periodically every 30 seconds
SYM-13197	Uploading firmware from Application Partition checks config backup status
SYM-13165	SCOM 2012 not discovering the modules
SYM-13139	Enable SIP Session Timers by default
SYM-11190	When UX tears down an FXS call (due to service affecting config change) UX should provide dial tone if the phone still off hook
SYM-9726	No alarm when server is unreacheable
SYM-10622	Japan CID detection fails
SYM-13061	Create Call Routing Entry window has Row ID as 1
SYM-12963	Unable to make modifications to SIP Server Table - error when trying to Apply
SYM-12918	Window size for detailed call Information is not big enough
SYM-12910	Translate the enumerated AD/LDAP value of the Result Code to human readable form
SYM-4779	Fallback to Passthrough from T.38 failed
SYM-12424	CAS trying to send Release Complete twice
SYM-11372	SBCPR: UX does not modify the content length
SYM-8413	Forked calls cannot support T.38 and use more DSP capacity
SYM-9619	Make the SIP trace to be efficient with appendDump
SYM-12264	ACK generated by SBC2000 is responded with 400 Bad Request by CUCM
SYM-10676	T1 CAS Loop Start FXS has no CID
SYM-12159	SHM header not transfered in UserValue from ingress to egress SG
SYM-12483	Changing Priority in SIP Contacts of Contact Registrant Table has no effect
SYM-12142	Support for backup and restore for large configurations

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-4947	Disable direct remote root login
SYM-12663	Remove "Media Transcoding Unlicensed" alarm
SYM-4270	UX Echo canceller needs a "Standard(Sparse Filter EC)" and "Enhanced(Dual Filter EC)" mode
SYM-11389	SBCPR : UX does not add modify the display name in contact
SYM-7672	UX needs to send 488 when unable to find listener
SYM-10544	UX1000: MSC and CCC cored after 7 days load test
SYM-12208	Modify SMM Header to be less confusing
SYM-9515	UX DCD behavior needs to be updated
SYM-12624	U-boot: Update memory timing
SYM-10941	UX respond 503 to a INVITE with g711 alaw over TCP
SYM-12265	SBC2000 is not generating INVITE to CONF-ID coming in REFER-TO Header
SYM-9907	RTCP: Invalid NTP timestamp in RTCP sender reports
SYM-11794	Display issue in nav tree when SPR condition rule has lengthy name
SYM-10976	UPDATE sent from UAC prior to receiving 18x is incorrectly processed by UX
SYM-12460	Cannot set date in Settings Tab with IE 9
SYM-12423	Rename error counter "Due to No Trunk" to "Due to No Signaling Group"
SYM-10092	ADNS implementation and test
SYM-1976	Voice Codec, G.726: Only 32K should be allowed from UI
SYM-12136	UX2000 Linecard init (PS_ENABLE) cleanup
SYM-10559	UI Performance improvement for very long certificate expirations
SYM-10550	UX does not throw an response '414 Request URI too long' for a request with URI of length 275 characters
SYM-12367	Debug facility not passing + along to server
SYM-10642	Misuse of IE API (ChangeIEData) could cause data corruption
SYM-12260	SNMP File fails to parse due to multiple quotes in description
SYM-8472	Import Local/Passthrough Auth Table Entries: Parser doesn't throw exception when protocol is missing from URI

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-12140	Memory tracking in libcommon: When writing tracking report, code does not check for error condition
SYM-4572	Long divertingLegInformation2 APDUs not decoded correctly
SYM-11368	O/A: Early UPDATE post 183 sent from UAS fails
SYM-11493	When SIP header rules popup is clicked it throws an exception
SYM-11929	QSIG diversionCounter value not passed through
SYM-11933	QSIG Original Called Number incorrectly mapped to SIP Diversion header
SYM-6734	Debug dump action broken for Watch service from Web UI
SYM-6946	Inband Indicator is not shown on the monitor applet
SYM-11433	Tooltips provided only for truncated table values
SYM-13203	SMM is not used on Re-INVITE

SBC 1000-2000 3.0 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 3.0:

- Notes for all SBC 1000-2000 systems
  - Changes to SIP Licensing Support
  - New Boot Image for Release 3.0
  - Mandatory configuration backup
  - New Base License for Release 3.0
- Further notes for SBC systems with built-in ASM's
  - Upgrading the SBC Communication Service
  - Upgrading the ASM Recovery Partition
  - Installing the SBA Lync Server Cumulative Updates
  - Installing Windows Service Packs and Windows Updates using ASM Roll-up Update

Before You Upgrade

The configuration format has changed significantly between Release 2.2.x and Release 3.0. As such, SBC nodes **will not operate correctly** if they are downgraded back to 2.2.x and the 3.0 configuration is left on the system. A configuration backup **must be performed** before the upgrade can proceed, so that it can be restored should a downgrade be necessary. Furthermore, should it be necessary to downgrade, it is required that you load the latest 2.2.x release in order to reliably be able to restore your configuration backup. Once the restore has been performed, you can move to a different release.

If your SBC 1000-2000 has **a built-in ASM**:

Please note that the ASM base image has changed with SBC 3.0. You will need to **upgrade the ASM Recovery Partition** image as outlined in these upgrade notes – refer to the #Upgrading the ASM Recovery Partition section.

Copyright © 2015 Sonus Networks. All rights reserved.

Notes for all SBC 1000-2000 systems

Please observe and perform the following extra operations - they are specific to this 3.0 release.

Changes to SIP Licensing Support

As outlined in the Release Notes, all SIP-SIP call sessions now require a SIP license. Systems purchased before March 31, 2013 and provided with free SIP Licenses are grandfathered and no purchase is necessary. Contact your Sonus sales representative to acquire a new (free) SIP license key.

> **Before you upgrade**
>
> The new SIP license key **must** be applied before upgrading the system software to version 3.0.

Only one call case requires a SIP call license. This is the case where both inbound and outbound channels are SIP. The exception for SIP calls to another SBC 1000, SBC 2000, the Sonus Tenor Series or the Sonus VX Series, however, still exists. If one or both of the call legs are to one of these devices then a SIP call license will not be used.

New Boot Image for Release 3.0

> **Prerequisites**
>
> Before proceeding, check the current firmware version of the SBC.
>
> - The firmware version must be R2.2.1 build 207 or higher. Otherwise, the Boot Image installation will fail.
> - For more information, see SYM-13124

Release 3.0 requires an update to the system's Boot Image. The Boot Image must be updated at the beginning of the upgrade process. Obtain the new Boot Image from your Salesforce Portal, then install it by following the Upgrading the Boot Image page.

Mandatory configuration backup

A configuration backup must be performed before proceeding with the SBC upgrade. Instructions on how to do this, along with the upgrade procedure itself, are included in the general SBC upgrade guide.

New Base License for Release 3.0

After the upgrade to 3.0, a new Base License will have to be installed. You can obtain the 3.0 Base License from your Salesforce Portal.

Further notes for SBC systems with built-in ASM's

Upgrading the SBC Communication Service

Upgrading the SBC Communications Service is covered in the general SBC upgrade guide. Make sure that it is upgraded, then follow the remaining instructions here - extra steps are required to update the ASM Recovery Partition.

Upgrading the ASM Recovery Partition

Copyright © 2015 Sonus Networks. All rights reserved.

Important

1. You can only proceed with this section once you have completed the #General Upgrade Instructions outlined above.
2. You do not need to re-initialize the ASM after upgrading the ASM Recovery Partition.

This step is required to ensure that the ASM Recovery Partition is correctly provisioned with the 3.0 image files, should it be necessary at a future date to restore the system from this partition. See Managing the ASM for details on the recovery partition.

1. Download the image from the Salesforce Portal.
2. Follow the instructions outlined in Updating the ASM Recovery Partition.

Installing the SBA Lync Server Cumulative Updates

You may skip this section if your SBC 1000-2000 hardware is not configured with a built-in ASM deployed as a Lync SBA.

Microsoft has released the following Cumulative Updates for these respective Lync Server releases:

Release	CU number	Release Date	More Information
Lync Server 2010	Cumulative Update 8	March 2013	KB2493736
Lync Server 2013	Cumulative Update 7	October 2014	KB2809243

Perform the following to apply this update to the Lync deployed ASM:

1. Download the CU package from the Salesforce Portal.
2. Follow the instructions outlined in Installing Cumulative Updates for Lync SBA.

Installing Windows Service Packs and Windows Updates using ASM Roll-up Update

Release 2.2 introduced new functionality to install Windows Service Packs and Windows Updates - ASM Roll-up Update. Sonus publishes **Update Packs** on a regular basis through the Salesforce Portal. The Update Packs work with Windows Update and other Non-Windows updates in order to keep the ASM up-to-date. The Update Packs contain tested and authorized Windows updates. Note that the Update Packs do not contain the actual Windows Service Packs and Updates. Once the Update Pack has been installed, the Windows Update State link in the Operational Status section will change to **Updates Available - Install**. The actual updates are installed using this link.

SBC 1000-2000 3.0.1 Release Notes

Sonus SBC 1000/2000 System release 3.0.1 is a maintenance release. In addition to hot fixes, this build includes added/updated configuration options for the SBC 1000/2000.

- Updated and added Remote Authorization options **From URI User Match** and **Regex** (for URI User match criteria).---**SYM-12213**
- Added ability to resequence entries in Remote Authorization table. **---SYM-12213**
- Added **Stagger Registration** (registration requests able to be staggered) to SIP Server Table. **---SYM 12335**
- Added **Clear Remote Registration on Startup** (for registration on startup) to SIP Server Table. **---SYM 12334**

Copyright © 2015 Sonus Networks. All rights reserved.

- Added **Contact URI Randomizer** (random user values for outgoing Register messages) to SIP Server Table. **---SYM 12360**
- Added **Failed Registration Retry Timer** (sets the wait time after a failed registration) to Contact Registrant Table. **---SYM 12336**
- Updated definitions for **Type of Address Record** in Contact Registrant table. **---SYM 12189**
- Added Restart Service and ability to enable/disable multiple IPsec tunnel entries. **---SYM 13392**

Don't have UX 3.0 yet?

Take a look at the new features and other highlights in the SBC 1000-2000 3.0 Release Notes.

Ready to upgrade to 3.0.1?

Review the SBC 1000-2000 3.0.1 Upgrade Notes
Download Latest Version

Updates and Fixes in this Release

Bug ID	Headline
SYM-13383	ASM Restart failure intermittantly popping up
SYM-13368	inbound BRI calls failing
SYM-13396	Application restart sym-snmp
SYM-14110	UX does not update config tree with self signed cert for an expired certificate
SYM-14113	Intermediate root chained cert displays incorrect status for an expired cert
SYM-14083	Popping noise heard when phone is answered
SYM-14080	radius core generated after brought up radius servers when the servers down for a long time
SYM-14078	SIP is not setting QSIG diversionCounter IE based on Referred-By in SIP-ISDN redirect
SYM-14025	SBC sends REGISTER w/Auth even received 401 w/stale=FALSE to REGISTER w/Auth
SYM-14026	Need to allow multiple provisional mesages to pass-through from outbound to inbound in alerting state
SYM-14104	Transfer to SIP destination fails due to SIP call license unavailability
SYM-14098	REST linkmonitor resource DELETE fails
SYM-14094	"+" in RegEx in SMM will be removed when Description is changed
SYM-14073	Alarm generated by an unexisting (not installed) ASM/SBA on UX and on SCOM

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-14054	Transfering a TDM/SIP call to another SIP destination asks for a SIP license
SYM-14077	Configured Literal Value in SMM as 'id' will be showed/changed as "1:3" when click 'Add/Edit' button again or modify the description
SYM-14036	CTRL+Left Arrow doesn't move a word in any text field in WebUI
SYM-14051	Calling SBC sends UPDATE for session refresh and not send BYE even refresher is uas
SYM-14057	REGISTER is incorrectly sent for first CRT entry if second entry is deleted after reboot
SYM-14082	ACK message should not have P-headers
SYM-14060	Add configuration item in SIP profile for refresher failure handling
SYM-14044	Importing exported SMM configuration failed
SYM-14053	One way voice on with BRI ISDN Overlap
SYM-14052	AD authentication only first configuration asks for attributes list
SYM-14030	ASM : Operational status on the ASM did not update properly
SYM-14035	"Play Ringback" label is not consistent across Signaling Groups.
SYM-14007	Display problems with Local Registrar User Table
SYM-14005	Create Remote Authorization entry window size should be larger for new fields
SYM-14022	Register is incorrectly sent when CRT assinged and SIP SG is in disabled state
SYM-14047	Exported certificate .der file is unreadable and cannot be Imported into the same SBC node
SYM-14037	User part of Contact URI in Response is NOT randomized if called number is NOT pilot number
SYM-14010	Error message need be updated for upload image
SYM-14016	Creation of a ACL Rule table from REST fails.
SYM-14018	No Server cluster found ERROR messages generated when using Local Registrar
SYM-14023	ISDN incompatibility with dialogic card CG-6060.
SYM-13646	QSIG Switch Specific change is lost after reboot
SYM-13971	Lower CSeq in REGISTER after UnRegister than previous one causes SBC gets 400 bad request
SYM-14002	SIP crashed while running Transport Switch Timer testing
SYM-14003	MSC crashed during SIP/TLS perfomance testing

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-13041	Memory Leak in SYM-SIP Process
SYM-13045	SBC does not send REGISTER w/Authorization
SYM-13046	Failed Registration Retry Timer option does function predictably
SYM-13251	Change Global TTL in CRT results in sending new REGISTER before UnREGISTER w/ Auth
SYM-13335	Validation required for "Address of Record URI" when Type of AoR is "Static"
SYM-13340	1st UPDATE has configured Min-SE value even received Min-SE in INVITE had larger value
SYM-13202	SBC sends CANCEL instead of BYE when received CANCEL from Caller before receiving 200OK from Callee
SYM-13282	Route header is not needed in CANCEL request
SYM-13350	No Registration sent after reboot
SYM-13229	Calling/Called Subaddress in transformation table are blank
SYM-13307	No Require header in 200OK to UPDATE even SBC set refresher=uac
SYM-13323	Origin Field Username field should NOT allow whitespaces
SYM-13322	Default value for Send Number of Audio Channels is "False" for new SIP Profile, should be "True"
SYM-13136	No contact header in 200OK for UPDATE
SYM-13119	Remove headers from 100 trying that is not allowed
SYM-13131	Re-INVITE is not sent when using Session Timer w/ Outbound Proxy in SIP SG
SYM-13531	No Route header in ACK to 200OK for 2nd Re-INVITE
SYM-5913	Change the SIP Contact Registrant Address of Record URI label of protocol:user@host to user@host. protocol: is not needed
SYM-13528	200OK for UPDATE has no Allow header
SYM-13317	SBC does not send CANCEL to SP even received CANCEL from LAN while retransmission Ini-INVITE
SYM-13951	Blind transfer from Lync to pstn one way audio
SYM-13301	IPsec tunnel not started if activation changed to Always
SYM-13324	SIP Options TCP is not always predictable
SYM-13127	Need an alarm to indicate IPsec tunnel setup failure
SYM-13319	SBC adds incoming called number to BADNUMBER when gets error code even ISDN port is configured as USER/TE

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-13347	IPsec tunnel with 0.0.0.0/0 subnet locks up the system
SYM-13295	IPsec Statistics do not show negotiated addresses, subnets
SYM-13479	Attended transfer does not work in all cases
SYM-13498	Unable to open SG Call Counters if special characters are present in the SG name
SYM-13271	TDM to SIP call has Clipped Audio when input volume is loud
SYM-13459	TDM to UX to SIP/TCP to Lync, no SIP disconnect/cancel
SYM-13504	ISDN Glare causes CCC to crash
SYM-13501	Deletion of static routes even if none present
SYM-13653	UX will not send REGISTER if it can't resolve the host FQDN
SYM-13389	IPsec Link Up after subnet negotiation failure
SYM-13532	Error Channel Not Found returned when trying to get Call Details for a DS1 channel that is unallocated
SYM-13552	Initial Setup Screen uses net.com as domain name example, change to sonus.net
SYM-13467	Configuration Error message sent at incorrect time
SYM-13472	UX intermittently brings the SG down on ISDN E1 loopback on reboot
SYM-13457	Operational Status should show windows uptime and SBA / UX comms uptime
SYM-13391	IP packets received via IPsec tunnel not forwarded
SYM-13074	Loss of connectivity to Monitored Host may cause unpredictable system behavior
SYM-13452	Can't join the domain with the ASM using the Standalone image.
SYM-13193	UX can't read some History-info header

$body

SBC 1000-2000 3.0.1 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.0.1

- Upgrading from UX 3.0.0
- Upgrading from prior releases

Upgrading from UX 3.0.0

Copyright © 2015 Sonus Networks. All rights reserved.

There are no special considerations for upgrading from a 3.0.0 release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

The upgrade instructions for 3.0.1 are the same as those for 3.0.0. Please follow the instructions outlined in the SBC 1000-2000 3.0 Upgrade Notes. - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

SBC 1000-2000 3.0.2 Release Notes

Sonus SBC 1000/2000 System release 3.0.2 is a maintenance release, providing the hot fixes listed below.

Don't have SBC 3.0 yet?

Take a look at the new features and other highlights in the SBC 1000-2000 3.0 Release Notes.

Ready to upgrade to 3.0.2?

Review the SBC 1000-2000 3.0.2 Upgrade Notes
Download Latest Version

Updates and Fixes in this Release

Bug ID	Headline	Build
SYM-15556	TLS transport layer error handling enhancement	283
SYM-15557	NTP reflection attack security enhancement	283
SYM-15170	Support for alternate RFC2833 payload types	283
SYM-15454	SG OPTION transaction cleanup upon event failure	283
SYM-15460	Disconnect excessive early dialogs	283
SYM-15304	Remove XML status block from all downloads via REST API	283
SYM-15401	Correctly handle receipt of ISDN Facility prior to Call Proceeding message	283
SYM-15398	SBC 1000 MAC address validation enhancement	283
SYM-15404	Improved transport layer error handling	283
SYM-14736	Improved SIP listening port error handling	283
SYM-15086	Change IPSec tunnel pre-shared secret WebUI field type	283
SYM-15181	Add Monitor applet JAR file signature timestamp	283
SYM-15056	Fixed Ethernet address for retransmitted INVITE with VIA header to secondary SIP server	283
SYM-15106	No audio on consultative transfers involving forked calls	283
SYM-13430	MSC call forking stability enhancement	283
SYM-15062	SBC does not forward Re-Register when FQDN is used	283
SYM-15064	Allow adding remote entries into the SIP Local/Pass-though authorization table	283
SYM-14885	Fix intermittent one-way audio caused by handling of early update	283

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-15050	SBC does not forward or respond to Re-INVITE in transfer call flow	283
SYM-15066	SIP stability enhancement	283
SYM-14976	SIP stability enhancement	283
SYM-14785	SIP stability enhancement with registrar SG	283
SYM-14958	Correctly parse INVITE with Content-Type header configured as "multipart/alternative"	283
SYM-14957	Make SIP destination call routing comparison case insensitive	283
SYM-14961	Inter-Process communication framework enhancement	283
SYM-14977	Handle Re-INVITE without SDP in third party call control call flows	283
SYM-15059	Disallow certain SSLv2 sessions in fallback mode	283
SYM-14946	Debug facility 'sg register' output message formatting	283
SYM-15017	Fix SNMP MIB call counters to reflect errored and rejected call flows	283
SYM-14789	Expand SIP contact-URI header parsing	283
SYM-14896	Use session timer value contained in Session–Expires header of 200 OK for initial INVITE	283
SYM-14884	Fix parsing of SIP History-Info header	283
SYM-14943	Fix free memory report in osys log message	283
SYM-14883	Partial configuration import password field validation	283
SYM-14868	Authorization of Microsoft Active Directory audit user	283
SYM-14610	SIP INVITE modification on 401 resulting in call disconnect on call resume	283
SYM-14771	Fix acknowledgment of Re-INVITE without SDP resulting in one-way audio	283
SYM-14653	MSC attended transfer call flow stability enhancement	283
SYM-13384	Sign Java Monitor applet to prevent browser security warnings	270
SYM-14787	Disallow NULL (empty) passwords for Active Directory binds	270
SYM-14790	SIP abnormal termination	270
SYM-14668	Recover user passwords if newer configuration is restored to an SBC1000/2000 running earlier software versions	270
SYM-14774	FXO port state shown as unknown. Unable to add FXO port to CAS SG	270
SYM-14783	Add support to enable start-up global log levels	270
SYM-14535	Unable to change Domain Controller password in WebUI	270
SYM-14684	A=crypto line being passed to ITSP on Re-Invite adversely affecting call with 400 Bad SDP	270
SYM-14650	Enhance ASM Windows Update error messages	270
SYM-14236	Address incorrect E911 PIDF-LO data sent to PSAP	270
SYM-14740	Hostname configuration in node-level settings results in error message in log file	270
SYM-14471	SIP Registration with Authentication incorrectly reflected in counter statistics	270
SYM-14702	SIP Registration incorrectly released	270
SYM-14504	NETBIOS hostname truncated when Lync 2013 SBA joins domain	270
SYM-14677	ISDN to SIP performance test call failures	270

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-14673	"Help" broken in Java Monitor applet: goes to about:blank	270
SYM-10098	Pop-up window used to specify date for the Export Date Range stays visible	270
SYM-14516	Active Directory authentication rights given by the latest group membership	270
SYM-14511	TLS negotiation issues after R1.3.2 to R2.2.1 software upgrade	270
SYM-14491	Hold/Unhold failure when initiated by Lync between FXS and Lync	270
SYM-14521	Music-on-Hold failure if the a= attribute value is set to sendonly (a=sendonly) by the endpoint that is placing the call on hold	270
SYM-14522	SBC2000 T1 ISDN port remains in an unknown state when connected to a VX1800	270
SYM-14563	Add route name to transformation processing in log	270
SYM-14582	Improve performance of certain older Point-of-Sale modems	270
SYM-14548	Incorrect borders around table cells on-hover in WebUI	270
SYM-14499	Add pop-up window to CSR generation after OK is clicked	270
SYM-14527	RURI with tel: drops telephone number	270
SYM-13454	Lync SBA is restarting if SBC 1000 is restarted	270
SYM-14496	"SG_MEDIA_ENDPOINT_IE(0x480) not found" error generated when SBC under load	270
SYM-14439	SBC sends RTP event in wrong Payload Type	270
SYM-14275	G.711 to T.38 Fax Transcoding failure	270
SYM-14515	Add configuration item to control c= line in media section of SDP	270
SYM-14487	SIP stability improvement	270
SYM-14407	Redirect number not passed to Diversion header on the SIP Invite	270
SYM-14339	Put Min-SE in session refresh as documented in RFC 4028	270
SYM-14360	Early Update messages responded to with 200 OK with no SDP information	270
SYM-14049	Resource Manager returns incorrect data when power supply not present	270
SYM-14468	CSeq value in a request is always incremented previous received one	270
SYM-14188	Add additional SIP debug commands to REST interface	270
SYM-14310	Incorrect Current Activity Status after SBA joined domain	270
SYM-14297	Removing URI host should remove '@'	270
SYM-14448	Retain order of Record-Route header fields in SBC Route response	270
SYM-14753	MSC stability improvement	261
SYM-14042	One-way audio on Lync calls 15-30 minutes after call retrieved from Hold	261
SYM-14325	When Contact URI Randomizer is enabled and incoming INVITE does not have randomized request-URI, the called number is NULL	261
SYM-14173	Unnecessary header in error response	261
SYM-14251	UPDATE/Re-INVITE for session refresh that always have the Min-SE even it has not received on that dialog	261
SYM-14279	To-tag in 200 OK to CANCEL is missing	261
SYM-14299	Register session not cleaned up, if the contact registrant is removed from sip server configuration	261

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-14190	Call Transfer Fails with Refer and Media Bypass enabled	261
SYM-14168	Generate a new From-tag in REGISTER for refresh	261
SYM-14256	From header not correct when CRT Type of AoR set to Local or Remote	261
SYM-14257	Retry Non-Stale Nonce = FALSE not working, reattempts to send REGISTER	261
SYM-14169	SBC not sending registration to SIP trunk provider after a connection drop	261
SYM-14066	Forwarded call from Lync 1 to Lync 2 failed due to missing server's FQDN in the "From" header	261
SYM-14163	Call fails when ITSP sends a (Re-)INVITE without SDP	261
SYM-14182	SIP memory leak and core dump when running load with Fwd Reg. After Local Processing	261
SYM-14241	SIP Service stability improvement	261
SYM-14194	CAS R2 deployment issues in Mexico	261
SYM-9724	SBC needs to support contact:* for removing all bindings from a user (FROM header)	261
SYM-10652	AD Caching Issue - missing "extension" in msRTC-SIP attribute	261
SYM-14154	200 OK for Re-INVITE has no Allow header	261
SYM-14061	183 Session Progress changes the codecs order	261
SYM-14107	Support for Firefox 24	261
SYM-14106	Call Transfer Fails	261
SYM-14147	SBC not sending OPTIONS if it could not resolve FQDN of remote peer	261

SBC 1000-2000 3.0.2 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.0.2.

- Upgrading from SBC 1000-2000 versions 3.0.0 or 3.0.1
- Upgrading from prior releases

Upgrading from SBC 1000-2000 versions 3.0.0 or 3.0.1

There are no special considerations for upgrading from an earlier 3.0.x release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

The upgrade instructions for 3.0.2 are the same as those for 3.0.0. Please follow the instructions outlined in the SBC 1000-2000 3.0 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

SBC 1000-2000 3.0.3 Release Notes

Sonus SBC 1000/2000 System release 3.0.3 is a maintenance release, providing the hot fixes listed below.

Don't have SBC 3.0 yet?

Copyright © 2015 Sonus Networks. All rights reserved.

Take a look at the new features and other highlights in the SBC 1000-2000 3.0 Release Notes.

Ready to upgrade to 3.0.3?

Review the SBC 1000-2000 3.0.3 Upgrade Notes
Download Latest Version

Updates and Fixes in this Release

Bug ID	Headline
SYM-16169	Security vulnerability in strongSwan (CVE-2014-2338)
SYM-16119	Mask Remote Authorization Table Entry on REST importconfig
SYM-16224	REST bulk GET for AD controller status return extra id 65535
SYM-16100	Remove challenge call SIP user password from syslog
SYM-16362	DoS Security vulnerability in strongSwan (CVE-2014-2891)
SYM-16228	Selection of alternate TLS profile ID in the SIP SG does not take affect
SYM-16280	Unable to Restore Previous Sonus Certificate
SYM-15993	Missing Radius Config, Runtime and Statistics REST APIs
SYM-15992	Modify Monitor applet permissions to support Java™ Runtime Environment (JRE) 8
SYM-15972	Transport layer epoll_ctl error recovery
SYM-15963	SBA service restarts periodically
SYM-15994	Missing REST API for Domain controllers status
SYM-15593	Handle escaped fields in From tag
SYM-16000	Insufficient disk space for upload firmware when upgrading SBC 1000
SYM-15556	Session timer operation upon receipt of SIP 422 response
SYM-15820	Provisional handling improvement while in a connected state
SYM-15777	Initiating SDP Offer with transcoding may contain incorrect codec order
SYM-15584	Lync 2013 user can't hear Ringback tone when calling to PBX
SYM-15815	Improve ISDN SG tone table configuration validation
SYM-15592	ITSP SIP trunk capacity issue observed
SYM-15575	Event log message reduction
SYM-15569	SIP call hold/resume disconnect when transcoding from G729 to G711
SYM-15778	UPDATE transaction handling improvement
SYM-14933	No audio after call transferred on ISDN BRI trunk
SYM-15403	SIP memory usage improvement for TLS transport without socket re-use
SYM-15598	SMM failed to add a PPI header with TEL-URI
SYM-15736	SIP response may be sent to incorrect destination

Copyright © 2015 Sonus Networks. All rights reserved.

SBC 1000-2000 3.0.3 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.0.3.

- Upgrading from SBC 1000-2000 versions 3.0.0 through 3.0.2
- Upgrading from prior releases

Upgrading from SBC 1000-2000 versions 3.0.0 through 3.0.2

There are no special considerations for upgrading from an earlier 3.0.x release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

The upgrade instructions for 3.0.3 are the same as those for 3.0.0. Please follow the instructions outlined in the SBC 1000-2000 3.0 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

SBC 1000-2000 3.0.4 Release Notes

Sonus SBC 1000/2000 System Release 3.0.4 build 291 is a maintenance release, providing the hot fixes listed below.

Don't have SBC 3.0 yet?

Take a look at the new features and other highlights in the SBC 1000-2000 3.0 Release Notes.

Ready to upgrade to 3.0.4?

Review the SBC 1000-2000 3.0.4 Upgrade Notes
Download Latest Version

Updates and Fixes in this Release

Bug ID	Headline
SYM-16943	On screen warning for Microsoft® Internet Explorer compatibility mode
SYM-16944	Update web user interface help links to sonusnet.com domain
SYM-16751	SIP memory leak
SYM-17159	Updated Microsoft® Internet Explorer unsupported version banner warning

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-16284	Support CDR attribute for SIP PPI header value in INVITE message
SYM-16557	Set early media negotiated for TDM endpoint upon receipt of Progress Indicator
SYM-15181	Add Monitor applet Java™ Archive (JAR) file signature time stamp
SYM-16566	Call Control process made non-restartable
SYM-16373	SIP process stability improvement

SBC 1000-2000 3.0.4 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to SBC 1000-2000 3.0.4.

- Upgrading from SBC 1000-2000 versions 3.0.0 through 3.0.3
- Upgrading from prior releases

Upgrading from SBC 1000-2000 versions 3.0.0 through 3.0.3

There are no special considerations for upgrading from an earlier 3.0.x release, beyond those mentioned in the general SBC 1000-2000 upgrade guide.

Upgrading from prior releases

The upgrade instructions for 3.0.4 are the same as those for 3.0.0. Please follow the instructions outlined in the SBC 1000-2000 3.0 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

UX 2.2 Release Notes

Release Part Number: 481-40174-006

October 11, 2012

The NET/Sonus team is proud to deliver a brand new version of the industry's best unified communications, enterprise session border controller and multi-service business gateway. UX System release 2.2.0 is a feature release and provides new features to the UX products

Copyright © 2015 Sonus Networks. All rights reserved.

Highlights of this Release:

- New Features
  - VLAN Support
  - SIP Message Manipulation
  - UX ASM Update Installer
  - DHCP Server Functionality
  - ISDN Overlapped Sending
  - ASM/SBA Windows Event Logs
  - Dynamic Routing
  - Access Control Lists
  - Multiple Logical Interface Support
  - Multiple Forest Domain Controller Support
  - UX1000 - UI Factory Default Support
  - Ping and Traceroute Support
  - DIFFServ DSCP Support
  - Port Mirroring
  - SBA Windows Event Logs
- Feature Enhancements
  - Nested Group Support for Active Directory
  - Alarms and Events
  - Adjustment in Transformation Table Rules using Regular Expressions
- Release Notices
- Updates and Fixes in this Release

Download the latest version:

- First read the #Release Notices for important information about this release.
- See the full list of #Updates and Fixes in this Release.



New Features



VLAN Support

Beginning with Release 2.2.0 the UX supports Ethernet VLANs. Users may add VLANs in the rage of 2-3999. User configured VLANs differ from the system VLANs (4000-4095) in that system VLANs are used internally and are not exposed to the user wit the exception of VLAN 4031 (Application VLAN). When a user adds a VLAN the system automatically add a VLAN logical interface, configurable as a normal logical interface. This feature also includes VLAN Counters.

With the addition of 802.1Q (VLAN) support, the routed mode is deprecated and all items in the routed mode will be upgraded t switched mode.

For more information, see the following section(s) in the UX User's Guide:

- Managing VLANs
- Adding and Modifying VLANs

Copyright © 2015 Sonus Networks. All rights reserved.



SIP Message Manipulation

Beginning with Release 2.2.0 the UX supports SIP Message Manipulation. The SIP Message Manipulation feature is used at SI Signaling Group Ingress and Egress to manipulate the incoming or outgoing message. This feature can be used for interoperability with different vendor equipment and for correcting any fixable protocol errors in SIP messages on fly without any changes in node release firmware/software.

For more information, see the following section(s) in the UX User's Guide:

- SIP Message Manipulation
- Managing Condition Rule Tables
- Managing Message Rule Tables
- Using the Condition Expression Builder



UX ASM Update Installer

Beginning with Release 2.2.0 the UX has the ability to update the ASM with the latest Windows and NET updates in a single package and in a controlled manner. You can obtain update packs from the NET Support site.

For more information, see the following section(s) in the UX Installation and Upgrade Guide:

- ASM Roll-up Update



DHCP Server Functionality

Beginning with Release 2.2.0 the UX includes DHCP server functionality, providing IP addresses to hosts on the branch office LAN. This feature along with other SBC features allows the UX to function as the only edge device between the branch office LAN and the ISP WAN.

For more information, see the following section(s) in the UX User's Guide:

- Managing the DHCP Server



ISDN Overlapped Sending

Beginning in Release 2.2.0 the UX supports ISDN Overlapped sending. This allows the calls to route before all the digits have been collected. The overlapped sending functionality is enabled and configured in the ISDN Signaling Group.

For more information, see the following section(s) in the UX User's Guide:

Copyright © 2015 Sonus Networks. All rights reserved.

- Adding and Modifying ISDN Signaling Groups



ASM/SBA Windows Event Logs

Beginning in Release 2.2.0 the UX supports Windlws system event logs and Lync server event logs, including export functionality.

For more information, see the following section(s) in the UX User's Guide:

- Viewing and Exporting Windows Event Logs on the ASM



Dynamic Routing

Beginning in Release 2.2.0 the UX supports dynamic routing. Supported dynamic routing protocols are RIPv2 and OSPF.

For more information, see the following section(s) in the UX User's Guide:

- Working with Dynamic Routing
- Managing Router Instances



Access Control Lists

Beginning in Release 2.2.0 the UX supports Access Control Lists (ACLs) for filtering packets, providing improved device securit and reduced malicious network traffic. ACLs impose security by allowing only specified types of packets to flow on specified ports.

The ACL's can be used to seperate the management and voice traffic onto different interfaces.

For more information, see the following section(s) in the UX User's Guide:

- Managing Access Control Lists



Multiple Logical Interface Support

Beginning in Release 2.2.0 the UX supports multiple logical interfaces.

For more information, see the following section(s) in the UX User's Guide:

- Managing Logical Interfaces

Copyright © 2015 Sonus Networks. All rights reserved.



Multiple Forest Domain Controller Support

Beginning in Release 2.2.0 the UX provides support for domain controllers belonging to multiple forests with different logon credentials and different roles.

For more information, see the following section(s) in the UX User's Guide:

- Configuring UX for Active Directory
- Managing Domain Controllers
- Adding and Modifying Domain Controllers



UX1000 - UI Factory Default Support

Beginning in Release 2.2.0 the UX can now be set back to factory defaults through the WebUI, as well as the previous methods

For more information, see the following section(s) in the UX User's Guide:

- Resetting UX to Factory Defaults



Ping and Traceroute Support

Beginning in Release 2.2.0 the UX provides Ping and Traceroute diagnostic functionality through the WebUI.

For more information, see the following sections in the UX User's Guide:

- Testing Network Connections



DIFFServ DSCP Support

Beginning in Release 2.2.0 the UX provides configurable DSCP supoort.

UX product family is used for processing and transporting voice and video media in the enterprise networks in real-time. Very high Quality of Service (QoS) is critical in order for media to be reconstructed in real-time. Media processing and transport operations for non-real-time use-cases (such as downloads) does not require the same high QoS and is tolerant of very high jitt and high delay. *Soft-real-time* cases such as playback high jitter and delay are rarely an issue.

For more information, see the following sections in the UX User's Guide:

- Adding and Modifying SIP Signaling Groups
- Adding and Modifying Media Lists

Copyright © 2015 Sonus Networks. All rights reserved.



Port Mirroring

Beginning in Release 2.2.0 the UX provides support for port mirroring.

For more information, see the following sections in the UX User's Guide:

- Working with Port Mirroring



SBA Windows Event Logs

Beginning in Release 2.2.0 the UX provides the ability to view SBA Windows Events in the user interface.

For more information, see the following sections in the UX User's Guide:

- Viewing and Exporting Windows Event Logs on the ASM

Feature Enhancements



Nested Group Support for Active Directory

Additional Active Directory support functionality has been added in Release 2.2.0. This enhancement allows the UX to see the group memberships of an individual. Group membership is discoverable throughout the entire hierarchy of an individuals groups For example; John Doe is a member of the Developers group, and the Developers group is a member of Administrators, and Administrators are members of XYZ group. The entire group membership structure for John Doe is now discoverable by the UX and can be used for authentication.



Alarms and Events

Alarm for Non-DTMF digits. With the exception of a **+** as the first character in conjunction with E911, a low level alarm is generated if the Transformation Table sends a non-DTMF digit in the Called Party Number or Calling Party Number field. Valid DTMF characters include **0-9**, **A-D**, *, and #.



Adjustment in Transformation Table Rules using Regular Expressions

Copyright © 2015 Sonus Networks. All rights reserved.

UX Transformation tables rules always require regular expression grouping. The grouping allows portions of the match to be passed to the output. If the regular expression is not surrounded in braces, the output replacement will not function correctly. Th behavior is different from past releases, so please read UX Service Advisory 2012-10-12 for details.

Release Notices

> ⚠ Be aware that this upgrade has **strict dependencies**. To ensure a successful upgrade, you **must follow the UX 2.2 Upgrade Notes**.

- For a listing of known issues and limitations in this release, please review the Notes and Limitations page.
- For system performance information, see the UX System Performance and Capacity page.

Updates and Fixes in this Release

Bug ID	Headline
SYM-11630	Msc Core, while handling the session terminate messages.
SYM-11702	Incoming history-info header with Tel uri format, outgoing diversion has wrong header uri
SYM-7972	CAS Network Side does not continue with outbound call if inbound call released due to glare condition
SYM-8167	Ability to use existing call block for another call
SYM-11532	UX sends re-INVITE with incorrect From-URI when it received REFER with Refer-To header without replace parameter
SYM-11332	3.1k Audio is swapped with Restricted Data in Config drop down.
SYM-11107	FXS ch stuck in connected state after a FXS to FXS transfer to Lync call
SYM-11425	Segmented ALERT and CONNECT messages not properly processed after reassembling
SYM-11537	ISDN Restart with multiple channels is responded to with multiple Restart Ack messages and not one single message
SYM-11077	Intermittent msc.vapi error DSP timelsot
SYM-11349	E911 Call back to multiple Lync End ports simultaneously failed on audio verification due to call disconnected because the hold failed
SYM-11397	MWI intermittently not working
SYM-8387	Change IP address with SIP SG configured, the invite sends out with old address in SDP
SYM-5326	SNMP service restarted during high load testing
SYM-8053	Egress channel left in Connected state after ISDN Outbound Glare call.
SYM-7136	Config Errors don't provide enough information to resolve validation issues

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-8477	R2 CAS Signaling Channel Out Of Service after physical line unplugged then restored.
SYM-8037	UX1000: CAS R2 mismatched CD bits between systems does not result in the CAS channels going OOS
SYM-7111	CCC doesn't handle channel ISDN channel glare negotiation if channel arrives in ALERT message
SYM-7175	SIP OP: Changing proxy FQDN causes resolution failure resulting in UX sending options to 0.0.0.0
SYM-10452	Add support for Netherlands caller id blocking
SYM-9855	Incoming Calls Blocked counter not working.
SYM-10001	Screening Indicator on Outbound Channel Properties page inaccurate
SYM-10926	UX does not open audio in case of double hold
SYM-11207	Calls drop out mid conversation
SYM-10934	UX drops audio on blind transfer
SYM-11078	Noise and static when playing MOH with presence of BRI but no DS1 card.
SYM-11051	FAX from TDM to Lync pass through stop working
SYM-11056	Alpha sort the Tranformation Table pulldown in the Action Set
SYM-11126	Contact Header does not contain Calling Number
SYM-9138	Unable to Defragment and parse SIP messages
SYM-11032	sym-snmp core on UX2000
SYM-11047	Noise/Static on FXS to BRI or ISDN calls
SYM-10782	Controlled Transmit/Receive Slips on DS1 Port Counters incorrectly displayed
SYM-11067	SIP FQDN config verify delay
SYM-8213	Calling Party digits passed to CAS R2 if ingress SIP message includes Privacy: id header
SYM-11010	Allow AD lookup to be done more than once per transformation table
SYM-10979	UX1000 is populating the Diversion Header with the wrong Host Name/IP Address
SYM-11017	Fragmented packets not handled by UX
SYM-5312	Put Elapsed Time in the SBA Status for reimaging
SYM-11070	Regex replacement gives inconsistent results when using complex input matching
SYM-10693	Modem over SIP does not Establish

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-3729	Modem Pass-through not working consistently
SYM-10937	When changing from T1* 2-port card to T1* 8-port UX2000 did not initialize T1* 8-port card correctly, missing ports 4-8.
SYM-10895	Dead Call Detect often does not work
SYM-10936	O/A - Early UPDATE after 183 fails, with media transcoding enabled
SYM-10879	Blind transfer has no ringback after first call reject
SYM-10894	Call Route Priority does not work
SYM-9939	RTP SSRC is always 0x12345678 for Conf DSP types, SSRC should be random so the stream cannot be spoofed.
SYM-10538	Contact Registration: UX does not send REGISTER on receipt for 423
SYM-10064	Support flash based backup and restore for multiple private keys on CSR generation and signed certificate import
SYM-10628	Removing the UX1000 flash at run time can potentially overrun the filesystem with coredumps
SYM-11008	UX2000 power supply module hot-insert - detection not working
SYM-7480	UX does not automatically add the Trusted CA certs when you import a .p7b into the server cert
SYM-10744	UX drops syslog TCP connection on configuration change
SYM-7998	Order of Codecs in INVITE SDP does not match Media Profile List
SYM-8068	No audio on multiple blind transfer
SYM-10897	UX flooding the SIP channel when using toll bypass
SYM-10739	UX needs to handle annexb parameter for G.729
SYM-10763	Dial tone sometimes is not provided when flash hook during dialing digits
SYM-10675	After UX Reboot FXS SG Service Status shows UP while Admin State is Disabled
SYM-10651	Issue populating Calling Name with Active Directory display names that contain a comma
SYM-10552	AD Cache Normalization Problem
SYM-10662	UX advertise wrong IP (old UX IP) in SDP if SIP IP Details configured to Bind to specific lan port.
SYM-10646	AD Cache truncated at startup search may fail and no online AD search is done
SYM-10619	Network Specific Facilities IE needed for ATT 5ESS as a configuration option

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-9179	If FXS port is in offhook state when UX is rebooted, the driver should connect the voice path.
SYM-5828	UX should support AD login using explicit UPN
SYM-10631	UX sends ACK to different port from contact-uri of 200OK even no outbound proxy setting
SYM-10458	During SBA deployment, We are not able to rerun properly the Start Replication if the first time fail
SYM-10533	RADIUS server counters link doesn't work if both auth and accounting are disabled
SYM-10735	Mandatory match should clear optional match requirements if no optional rule matches
SYM-10745	False detection of glare handling on outbound ISDN calls
SYM-10783	Fix bugs in REST documentation for some resources
SYM-10761	When set FXS SG to Outbound, Tone table for the SG is not configurable anymore
SYM-10747	Need A-Law/M-Law Conversion For E1-FXS Calls
SYM-10715	REFER from Mediation does not have Ms-opaque tag in REFER-TO header, but in the Contact. UX constructs INVITE without username portion in the To:
SYM-10695	After timeout on off-hook without dialing any digits analog phone gets fast busy tone but RT Status view is still showing C
SYM-10686	Application Service restart on UX2000 for CCC
SYM-10696	UX2000 - after replacing DS1 card with FXS card, unable to delete DS1 ports
SYM-10712	Need CAS to log FXS Inter-digit timer start info
SYM-8154	No audio on blind transfer involving hold
SYM-10767	Add ID for label elements so automation can find them
SYM-10547	UX sends 501 response for a codec mismatch
SYM-10625	Add restart of registers when sg is down and then sg changed to up if registers are configured on sip server
SYM-10684	Webui gives a wrong error message when configure Maximum Flashhook Duration less than Minimum Flashhook Duration
SYM-9698	When FXO CID type is Japan, NTT and UX1000 receives a call from Tenor FXS, MSC does not detect CID and the call fails.
SYM-9917	UX does not respond to 487 with ack message
SYM-10518	Diversion header in outb.INVITE uses incorrect Diversion header althoug the "Redirecting number" is previously transformed correctly

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10537	AD Caching in "updates" mode causes performance issues during load testing
SYM-10627	Debug Facility: Web Interface / 'list corefiles' does not recognize mounted USB flash drives on UX1000.
SYM-10549	"Replaces" option should be supported by UX under SIP Profile
SYM-10601	BRI CALL PROCEEDING sent with incorrect Channel ID
SYM-10640	Cannot modify any of the linecard port parameters
SYM-10600	UX wizard screen errors out when the valid domain name of "e.uh.edu" is used as the internet domain name
SYM-10563	UX does not allow user to change ethernet 2 IP address even all SIP SG are disabled
SYM-10557	In the SIP Contact Registrant, Add SIP Contact, specify that Contact must be username only, not URI
SYM-10553	Overlap Recieve problem with UX 2.1.0
SYM-10545	TSI TDM Stream input bit delay incorrect for UX2000 FXS Line Card
SYM-10526	Transcoding G729/G711-A law to G711-u codec fails
SYM-8468	CAS R2 call dropped if B-7 Subscriber line free, no charge is received
SYM-10282	UX does an audio cut through on hold from FXS when lync resumes the call
SYM-10110	MSC "Conference not found" errors printed with CAS to ISDN calls
SYM-10111	Early media from a different IP specified in the 183 does not flow to the DSP, dropped by network policy
SYM-10288	FAX Passthrough not working
SYM-10028	UX should not allow T1 to be set below 100ms
SYM-10040	Calls fail on one Channel
SYM-10049	ux2000: MSC crashed after 57 hours ISDN to SIP loopback test
SYM-10472	Lync client cannot hear BT from ISDN if 'Play Inband Message post-disconnect' is Yes
SYM-10506	UX does not respond to an inbound request while trying to setup call (referred call) on the outbound
SYM-10514	options web ui needs to have additonal username fields for iteroperability
SYM-10505	Setting Play Ringback=Always does not work
SYM-10496	Exceeding maximum call forking causes endpoints to stop ringing; caller hears ringback
SYM-10503	UX1000 FXS port calibration does not complete correctly.
SYM-10495	Transformation list in drop down for "Add Call Route Entry" should be in alphabetical order.

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10450	UX Not Negotiating TLS With Office 365 Server
SYM-4979	Need a new debug-facility to display detailed call related info for a given call
SYM-10501	Extend config reference to strings
SYM-10086	Outbound Channel Properties screen shows incorrect Number Type
SYM-9847	UX used as SBC for ITSP SIP to LYNC SIP when LYNC hangs up and UX sends BYE to ITSP UX changes the source TCP port
SYM-9895	UX should send CANCEL even Play Inband Message post-disconnect is enabled if call is not connected yet
SYM-9926	Transformation name ordering is case sensitive.
SYM-9914	UX does not set Calling Name properly in the from if the trusted interface is disabled
SYM-9975	Sym-isdn crashes if call received on remotely blocked circuit.
SYM-9977	FXS port gets hung when transferring call from Lync to another FXS port.
SYM-9995	DISC with incorrectly encoded Cause IE sent after T313 expiry.
SYM-9967	UX still sends multiple 183 Progress after accepting a CANCEL
SYM-9965	PR: UX continues to process inbound REGISTERs when SG is down
SYM-9961	PR: Malformed Contact header in outbound REGISTER
SYM-9936	Errored Calls counter not working.
SYM-4698	Generate SBA CSR under Settings grey's itself out if you have completed the SBA wizard
SYM-9717	Need handling switch between MOH source from Live and File on the fly
SYM-9850	BRI calls rejected with "rearranged channel NOT available" error
SYM-9874	Rethink CCC Sanity Timer (was UX is still taking the default T301 = 180 sec when change it into 240 sec)
SYM-9824	Lync generates Errors with event ID 25020. UX does not have a user portion of the to: header sent on the INVITE after the REFER
SYM-9819	PR: On transport failure UX does not attempt to setup transport with the second server
SYM-9999	Transformation table allow user to configure output ELIN Identifier but UX does nothing to it
SYM-9800	UX closes Signaling Group Initial Configuration dialog if User Does Not Enter Required Information
SYM-9893	calling number shows as callback number during 911 call using CAS R2
SYM-10012	Filter Called or Calling Party numbers for R2 to 0-9 only instead of standard DTMF (0-9, A-F, * and #)

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10074	IP leg functionality in CCC simulator part of MSC does not work due to MSC restructuring done in R2.1
SYM-10075	Called Number in outgoing ISDN MWI not updated after transformation
SYM-10070	UX Not Handling Referred-By Header in SIP INVITE And Does Not Send Diverion In Follow-on INVITE
SYM-10069	UX sends RELEASE COMPLETE with cause code 96 on all inbound calls from Alcatel PBX
SYM-10057	Add a command to the sym-analog-mfg routine to control the bypass relays on the FXS card
SYM-10068	Channel lockup after T313 expiry.
SYM-10100	Bad CAS line may permanently lock up all TDM licenses
SYM-10102	SIP Channels on Lync SG are stuck in Releasing state
SYM-10279	DTMF twist implementation is incorrect--high frequency group is being sent at lower strength
SYM-10280	Need configurable option to add Progress Indicator IE to outbound ISDN SETUP
SYM-10317	Unsolicited UA frame in BRI doesn't cause TEI Verify/Check Request response
SYM-10251	Audio law on FXS is incorrect if PRI ports are configured to E1 and disabled.
SYM-10104	Do not use DSP's if the call transitions to TDM-TDM
SYM-10108	Registrar Minimum TTL on signaling group is incorrectly named
SYM-10023	PR: REGISTER refresh not going to peer server
SYM-10024	FXO : No progress tone (fast busy) for a busy end point over FXO
SYM-10025	Switch Timer: With Reuse ON, switch timer value does not take effect
SYM-10016	Incorrect retransmission interval of Identity Request message
SYM-10283	Analog Relay Configuration missing when DS1 card not present
SYM-10004	UX Reject the inbound BRI call when B channel 1 is blocked
SYM-10010	UX needs to provide configuration for passing through ISDN Facility messages, some PBX's do not accept them
SYM-10029	Some attribute haven't documentation in the last REST API
SYM-10032	New SIP signaling groups should have Music on hold disabled
SYM-10045	MOH is stops when both endpoints are put on-hold / MOH Source = Live
SYM-10046	UX doesn't send original NumPlan and NumType as received in inbound Overlap dialing SETUP message

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10050	AD Lookup fails against userPrincipalName attribute
SYM-10043	MOH audio doesn't stop after the call is transfered. / MOH Source = Live
SYM-10041	"TDM" channels licenses are not increased for FXO cards in upper slots
SYM-10039	Performance improvement in Registrar database area for contact search during call scenarios.

UX 2.2 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to UX 2.2:

- Notes for UX nodes without built-in ASM's
- Notes for UX nodes with built-in ASM's
  - Upgrading UX and the UX Communication Service
  - Upgrading the ASM Recovery Partition
  - Installing the SBA Lync Server 2010 Cumulative Update 7 (CU7) October 2012
  - Installing Windows Service Packs and Windows Updates using ASM Roll-up Update

Before You Upgrade

The configuration format has changed significantly between Release 2.1.x and Release 2.2. As such, UX nodes **will not operate correctly** if they are downgraded back to 2.1.x and the 2.2 configuration is left on the system. A configuration backup **must be performed** before the upgrade can proceed, so that it can be restored should a downgrade be necessary.

If your UX has **a built-in ASM**:

Please note that the ASM base image has changed with UX 2.2. You will need to **upgrade the ASM Recovery Partition** image as outlined in these upgrade notes – refer to the #Upgrading the ASM Recovery Partition section.

Notes for UX nodes without built-in ASM's

A configuration backup must be performed before proceeding with the UX upgrade. Instructions on how to do this, along with the upgrade procedure itself, are included in the general UX upgrade guide.

Notes for UX nodes with built-in ASM's

Upgrading UX and the UX Communication Service

A configuration backup must be performed before proceeding. Follow the instructions in the general UX upgrade guide first, including the backup steps. Once completed, return to this page and follow the remaining instructions here - extra steps are required to update the ASM Recovery Partition.

The general upgrade guide will first ask to upgrade the UX Communication Service, and then upgrade the UX software as the next step. **Please note that if you are upgrading from 1.3.x,** once you upgrade the UX Communication Service to 2.2, it may not be able to communicate properly with the UX system until the UX software is also upgraded to 2.2. Do not be alarmed - this is because UX Communication Service version 2.x are not backwards compatible with UX software versions 1.3.x or earlier. Verify the UX Communication Service version number once both have been upgraded.

Upgrading the ASM Recovery Partition

Copyright © 2015 Sonus Networks. All rights reserved.

If your UX hardware is not configured with a built-in ASM, skip this section.

Important

1. You can only proceed with this section once you have completed the #General Upgrade Instructions outlined above.
2. You do not need to re-initialize the ASM after upgrading the ASM Recovery Partition.

This step is required to ensure that the ASM Recovery Partition is correctly provisioned with the 2.2 image files, should it be necessary at a future date to restore the system from this partition. See Managing the ASM for details on the recovery partition.

1. Download the image from the UX Download Center.
   - The ASM Image is located under: UX ASM Images ... `2.2.x and later`.
2. Follow the instructions outlined in Updating the ASM Recovery Partition.

Installing the SBA Lync Server 2010 Cumulative Update 7 (CU7) October 2012

You may skip this section if your UX hardware is not configured with a built-in ASM deployed as a Lync SBA.

Microsoft has released Cumulative Update 7 (CU7) that is dated October 2012 for Lync Server 2010 (KB2493736). Apply this update to the ASM deployed as a Lync SBA:

1. Download the CU7 package from the UX Download Center.
   - The SBA Lync CU is located under: UX Lync Updates 2.2.x and later `ASM_Lync_2010_CU7.pkg`.
2. Follow the instructions outlined in Installing Cumulative Updates for Lync SBA.

Installing Windows Service Packs and Windows Updates using ASM Roll-up Update

UX R2.2 introduces a new functionality to install Windows Service Packs and Windows Updates - ASM Roll-up Update. NET publishes **Update Packs** on a regular basis through the NET Download Center . The Update Packs work with Windows Update and other Non-Windows updates in order to keep the ASM up-to-date. The Update Packs contain tested and authorized Windows updates. Note that the Update Packs do not contain the actual Windows Service Packs and Updates. Once the Update Pack has been installed, the Windows Update State link in the Operational Status section will change to **Updates Available - Install**. The actual updates are installed using this link.

UX 2.2.1 Release Notes

Unified Exchange (UX) 2.2.1 build 221 is a maintenance release, providing the hot fixes listed below.

Don't have UX 2.2 yet?

Take a look at the new features and other highlights in the UX 2.2 Release Notes.

Ready to upgrade to 2.2.1?

Review the UX 2.2.1 Upgrade Notes

Copyright © 2015 Sonus Networks. All rights reserved.

Download Latest Version

Updates and Fixes in this Release

Bug ID	Headline	Build
SYM-15992	Modify Monitor applet permissions to support Java™ Runtime Environment (JRE) 8	221
SYM-15181	Timestamp signed Java™ Applet JAR	221
SYM-13384	Sign Java™ Monitor Applet to prevent browser security warnings	219
SYM-14668	Recover user passwords if newer configuration is restored to an SBC1000/2000 running earlier software versions	219
SYM-14412	MSC abnormal termination on certain Lync to Analog calls	219
SYM-10098	Pop-up window used to specify date for the Export Date Range stays visible	219
SYM-14511	TLS negotiation issues after after software upgrade to R2.2.1	219
SYM-14258	CAS R2 Calls fail after upgrading to release 2.2.1	219
SYM-14006	Warn user if transformation table entries under a route are disabled	219
SYM-14061	183 Session Progress changes the codec order	219
SYM-13368	Multipoint BRI TE mode interworking	219
SYM-13383	Intermittent ASM failure alarm	219
SYM-13396	Intermittent SNMP deamon process restart	219
SYM-13465	Intermittent Call Control process restart	219
SYM-13319	Corrected Japanese ISDN cause code 84 (bad number) logic	219
SYM-13459	No SIP disconnect/cancel when originator disconnects the call in TDM->SBC->Lync call flow	219
SYM-13324	Fix TCP SIP Options issue	219
SYM-13345	Fix the tel-uri for SIP headers that are of generic URI type.	219
SYM-13394	Support for uploading of large files via the WebUI	219
SYM-13238	Add Serial Number to the Overview report above Hardware ID	219
SYM-12974	Intermittent Web session termination during node upgrade	219
SYM-13254	Active Directory does not allow deleting the last Auth Domain Controller	219
SYM-13195	MSC/CCC abnormal termination	219
SYM-13308	Added 'Name Is Not Available' support in NI-2 ISDN	219
SYM-13330	Add configuration backup step to the Upgrade Task	219
SYM-13314	FXS Port query not working via REST	219
SYM-13092	Resolved ISDN Overlap memory leak	207
SYM-13187	SBC1000 Node failed to backup configuration file through both WebUI and REST	207
SYM-13215	FXS calls no media after upgrade to 2.2.1b205	207
SYM-13124	SBC1000 boot upgrade is not accepting .gz file	207

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-13048	Unable to view "Operational Status" in Tasks. Operation times out.	207
SYM-12953	Automate the configuration backup export when upgrade is initiated	207
SYM-12920	CAS Does Not Pass Caller Name	207
SYM-12985	FSK Analog Caller Id Detects Extra Digit	207
SYM-13049	PSTN in Colombia Rejects R2 Emergency Calls With Congestion Reason	207
SYM-12984	MDMF Caller Id Generation Does Not Work For Odd Number Of Characters.	207
SYM-13014	PHP Exception Error missing a space between "errors" and "occurred"	205
SYM-13012	Import failure of backup SMM configuration	205
SYM-12811	Manual local log rotate results in out of sequence logs	205
SYM-13018	SIP stability improvements	205
SYM-12474	SBC reboot identified in some environments	205
SYM-13019	Fixed SIP TCP transport message handling	205
SYM-13039	REST support for FXS Port Service Status	205
SYM-12823	Intermittent media path issue when Dual Forking is enabled	205
SYM-11630	MSC stability improvements	205
SYM-12157	Cause code re-routing does not work with on board call Forking	205
SYM-12919	MSC stability improvements	205
SYM-12937	CAS-R2 license leak	205
SYM-12891	SBA service RDP stability improvements	205
SYM-12873	Improved SBA service exception handling	205
SYM-12742	IE 7 code upload workaround browser detection improvement	205
SYM-12913	Call in POTS line is detected with wrong digits	205
SYM-12743	UX does not correctly switch to T.38	205
SYM-12777	Outbound SMM Manipulation of FROM field over-riden by SIP Profile	205
SYM-12441	UX1000 stops processing incoming calls from FX0	205
SYM-12463	UX1000 Phantom FXO calls reported by CAS Debug Facility	205
SYM-11713	Popping noise occuring during calls	205
SYM-12469	Improved handling of Group-C tones on CAS R2	205
SYM-12771	SYM-CAS crashes with coredump causing the UX to reboot after adding 25th port in the same CAS SG	205
SYM-12650	Add AD cache size units in KB to the AD Statistics page	205
SYM-12746	Application Service Restarted sym-sip during Lync Interop Testing for Certification	205
SYM-12683	UX interop problem with PBX in China on PSTN to PBX calls forwaded back to PSTN	205
SYM-12726	UX cause code reroute not working	205
SYM-12389	UX2000: Sessions leak observed with IP to IP calls	205
SYM-12634	DSP Crash	205
SYM-12646	Unable to set the Media list in call route	205

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-12645	UX failing to parse SIP messages particularly on SIP phone registratiions/issues parsing LYNC team group simring with media bypass	205
SYM-12534	E911 call back fails, UX1000 drops Ext. Info	205
SYM-12233	WebUI become slow and ASM page return Timeout popup only on Ux2k	205
SYM-12454	Changing port in ISDN SG shows wrong SG status	205
SYM-12525	WebUI access very slow when ASM added to system	205
SYM-12464	MSC crash	205
SYM-12426	CallRouter crash	205
SYM-12512	Lync 2010 label left in Lync 2013 SBA binaries	205
SYM-12278	UX reboot with msc.vapi ERROR but no corefile	205
SYM-12269	SBC2000 is Not Relaying DTMF EVENTS	205
SYM-12494	UX uses wrong diversion header when presented with 2	205
SYM-12356	Investigate/Fix software upgrade issue in IE with Compatibility mode	205
SYM-12359	DMS100: intermittent call disconnect after alert.	205
SYM-12493	need to ensure user agent changes for SBC are handled in 2.x prior releases	205
SYM-12377	911 calls to e911 provider failed by the e911 provider due to wrong XML encapsulation	195
SYM-12351	UX does not appear to be responding to 2nd 407 authorization request correctly	195
SYM-12399	FXO Port Last Optimized shows date and time even not calibrated after reboot	195
SYM-12416	Incorrect output field in default "Passthrough Untouched" transformation table	195
SYM-12344	Avaya to Lync calls experience no audio after upgrade	195
SYM-12370	Media Stream Crash in high load condition	195
SYM-11531	No early media audio heard on forked call when UX gets 4xx response	195
SYM-12357	sym-trapd package makefile references old version of net-snmp library	195
SYM-12348	UX sends Re-INVITE to second call leg when media transcoding is enabled	195
SYM-10076	ux1000: MSC conferences leak	195
SYM-12349	No early media heard on Lync	195
SYM-12186	MSC cored in MTLS high loads	195
SYM-11927	If loading ASM image from USB, it seems to unmount the drive share afterwards, this should not happen.	195
SYM-12358	Increase the delay between enabling power to the line card and checking the board health status.	195
SYM-11577	Call Router leaks memory when timeout from AD Lookup occurs	195
SYM-12361	UX trying to refresh AD cache update mode at sporadic times does not match the update timer	195
SYM-12326	Call Transfer - 10 Second Audio Delay	195
SYM-12325	UDP Port scan against UX causes UDP S/G to go down and not recover	195
SYM-12176	UX stops playing progress tone on inbound SIP Registrar on call reject on ISDN	195
SYM-12215	SNMP does not properly report number of current calls	195
SYM-12314	Alarm Configuration Severity Changes Not Persisting Across Reboot	195

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-12195	Turn OFF Blue Hotswap LED on SBC2000 Linecards	195
SYM-12310	When Transcoding is unlicensed UI should hardcode "0" (disabled) for Media Transcoding setting	195
SYM-12227	UX not using Second DNS Server	195
SYM-12307	ISDN CONNECT IEs are being dropped and not passed through UX	195
SYM-11926	Add throttling to AD during cache refresh	195
SYM-12187	TDM licenses don't match number of installed TDM ports	195
SYM-12205	Change AD from Updates to Online, cache does not get deleted and memory not released	195
SYM-12157	Cause code re-routing does not work with On-board call Forking	195
SYM-12232	SIP crash then next day inbound calls failing	195
SYM-12319	Enhance WebUI to work with Internet Explorer 10	195
SYM-12212	Unable to edit Message Translation table entries	189
SYM-12155	REGISTER request has contact header without contact-URI	189
SYM-12153	Unable to login into WebUI when flash is full	189
SYM-11669	UX stopped processing calls went unresponsive had to power cycle to recover	189
SYM-9122	UX does not set "Presentation", "Screening" and Redirecting Number	189
SYM-12158	No Documentation for REST support in FactoryDefault R2.2.1	189
SYM-12152	Forward After Processing REGISTER fails when the SIP Server is configured to FQDN rather than actual IP address.	189
SYM-12160	No tag value in FROM header	189
SYM-12163	Occasionally sym-trapd.conf is not created at start up, resulting in no traps being sent	189
SYM-11923	avoid unescaped script tags in calldetailsengine and calltableengines	189
SYM-11800	No voice after unattended Lync transfer.	189
SYM-11779	Value of Edit Message Field that shows 'conma and blank' as %2C%20	189
SYM-11802	Help buttons not linked to documentation pages	189
SYM-11630	Msc Core, while handling the session terminate messages.	189
SYM-11814	Interop issue with Carrier for ISDN Busy ringback tone	189
SYM-11709	Delete RIP and add RIP back with more than one interface, the WebUI pops error; and RIP will only have one interface	189
SYM-11617	UX did not create INVITE with DTMF option after SIP REFER	189
SYM-11638	UX to LYNC teamgroup SIM ring calls failing	189
SYM-11818	WEBUI freezing will not allow changes in signaling group or media list	189
SYM-11642	SIP headers with ordinal number not modified by Outbound policy.	189
SYM-11649	UX stopped processing calls for about 30 minutes	189
SYM-11658	UX1000 BRI Lync Wizard problems	189
SYM-11424	UX keeps sending REGISTER request even contact registrant entry has been deleted	189
SYM-11635	UX sets UA header in message even UA header field in SIP profile is blank	189
SYM-11168	UX1000 - Support system level configurable for companding law type	189

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-11928	Issue with Record-Route when used for sending BYE	189
SYM-11936	SMM Raw Message Rule Replaces Plus Sign With Space	189
SYM-11937	UX does not add an Allow header in re-INVITE	189
SYM-10841	TLS INVITE selects non existing TLS profile	189
SYM-11890	Delayed media broken when PRACK is not supported on the caller	189
SYM-11820	UX Not Reading SIP History Info Header From Lync 2013 on Call Forward	189
SYM-10519	BRI channel stuck in Releasing state	189
SYM-11805	UX SCOM 2007 MP fails to install on some SCOM Management systems	189
SYM-11823	Host portion of Contact-URI is incorrect	189
SYM-11813	Unable to modify PAI using SIP Message Manipulation	189
SYM-11819	UX1000 FXS Port loop current limit should be 23mA per the Functional Spec	189
SYM-11640	User is added to Active Sessions when authenticated but not authorized	189
SYM-11720	UX does not open audio on call park	189
SYM-11722	AD lookup fails to cache attributes if they have a leading space character	189
SYM-11724	UX fails to send out an INVITE containing Replaces and Referred-by header when it receives a REFER	189
SYM-11438	Header Rules Limit not enforced per-table	189
SYM-11754	Decode escaped header format for history-info	189
SYM-10893	UX always sends re-INVITE to ITSP when received REFER from Lync	189
SYM-11816	Fix resources that were missing from 2.2 REST API docs	189
SYM-9818	Egress Calls Completed counter incremented with CONNECT message.	189
SYM-6807	Incorrect number of System user count when no webui user login	189
SYM-5193	Multiple Redirecting Number IEs not passed to ISDN	189

UX 2.2.1 Upgrade Notes

This document contains specific upgrade notes for customers planning to upgrade to UX 2.2.1:

- Upgrading from UX 2.2.0
- Upgrading from prior releases

Upgrading from UX 2.2.0

There are no special considerations for upgrading from earlier 2.2.x releases, beyond those mentioned in the general UX upgrade guide.

Upgrading from prior releases

The upgrade instructions for 2.2.1 are the same as those for 2.2.0. Please follow the instructions outlined in the UX 2.2 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

Copyright © 2015 Sonus Networks. All rights reserved.

UX 2.1 Release Notes

Release Part Number: 481-40174-006

April 23, 2012

The NET Unified Exchange (UX) team is proud to deliver a brand new version of the industry's best unified communications, enterprise border controller and multi-service business gateway applications. **Unified Exchange (UX) 2.1.0** is a feature release delivering: UX1000 BRI Support, UX1000 FXO Support, Music on Hold, Lync E911 PSAP Callback Support, and SIP Phone Survivability.

Highlights of this Release:

- New Features
  - UX1000 ISDN BRI Support
  - UX1000 FXO Support
  - Music On Hold
  - Lync E911 - PSAP Callback Support
  - SIP Phone Survivability
- Enhancements
  - SIP Diversion Implementation
  - Configurable Transport Timeout Timer
  - DiffServe QoS Implementation
  - Enable and Disable Transformation Table Entries
- Release Notices
- Updates and Fixes in this Release

Download the latest version:

- First read the #Release Notices for important information about this release.
- See the full list of #Updates and Fixes in this Release.





New Features



UX1000 ISDN BRI Support

Beginning with Release 2.1 the UX1000 now supports ISDN BRI. The UX1000 supports up to three 4-port BRI cards for a total twelve BRI ports.
For more information see the following sections in the UX User's Guide:

- UX1000 BRI Card
- Adding and Modifying ISDN Signaling Groups
- Configuring BRI Ports

Copyright © 2015 Sonus Networks. All rights reserved.



UX1000 FXO Support

Beginning with Release 2.1 the UX1000 now supports FXO interfaces. The UX1000 supports up to six 4-port FXO cards for a total of 24 FXO ports.
For more information see the following sections in the UX User's Guide:

- UX1000 FXO Cards
- Adding and Modifying CAS Signaling Groups
- Adding and Modifying FXO CAS Profiles
- Configuring FXO Ports



Music On Hold

Beginning with Release 2.1 NET introduces Music On Hold (MOH). The Music On Hold feature allows you to play music or othe audio while a call is on hold and is available to all call types (SIP, ISDN, CAS). MOH is supported on both the UX1000 and UX2000 platforms.
For more information about Music On Hold see the following sections in the UX User's Guide:

- Configuring the UX for Music On Hold
- Uploading Music on Hold Files
- Configuring the Media System
- Adding and Modifying SIP Signaling Groups



Lync E911 - PSAP Callback Support

Beginning with Release 2.1 UX supports LYNC E911 PSAP Callback user extension bindings. The duration for which the bindings are maintained are configurable. The UX supports pools of ELIN (callback) numbers for Lync users. UX also supports load balancing and failover on multiple UXs.
For more information about Lync E911 PSAP Callback Support, see the following sections in the UX Customer Documentation:

- Working with Enhanced 911 Devices
- Best Practices - Configuring UX for Lync E911 with PSAP Callback Number



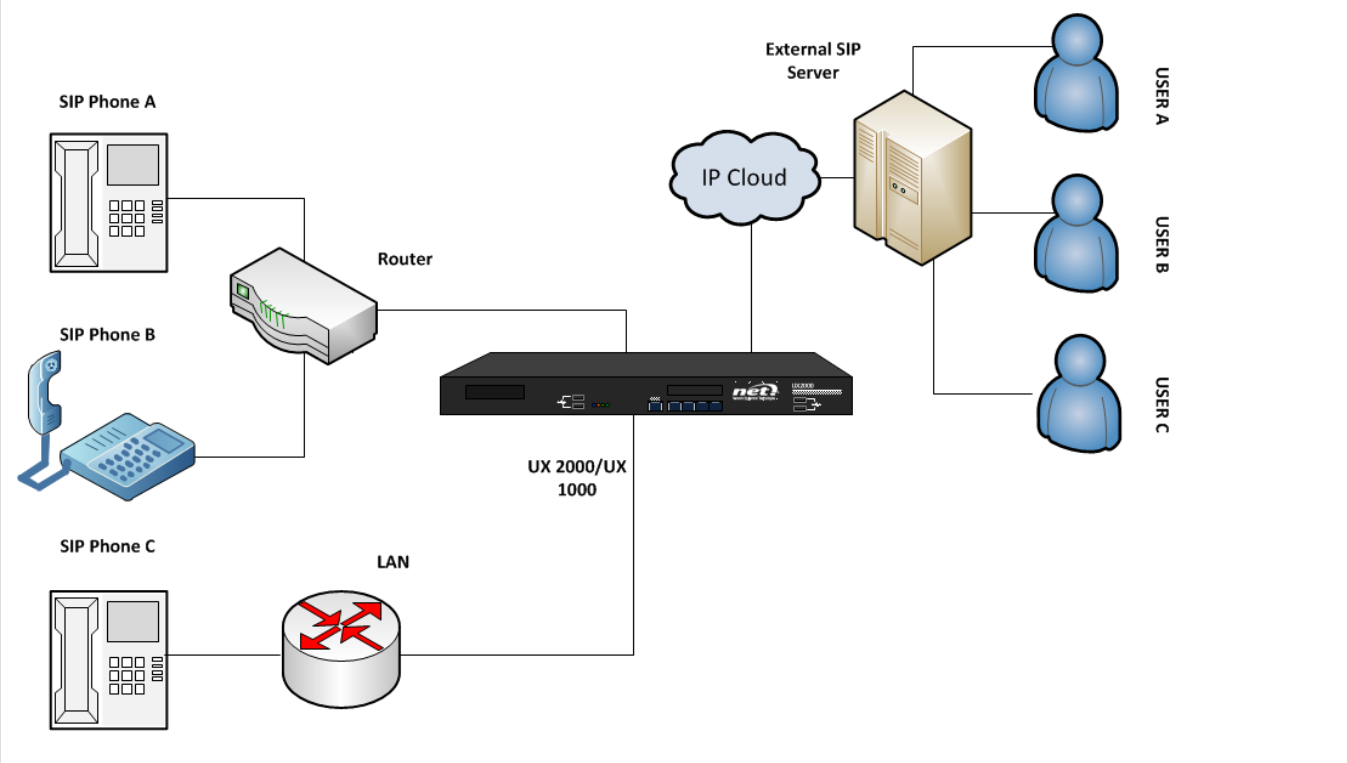
SIP Phone Survivability

The UX SIP Phone Survivability feature provides site survivability for branch offices in the event of a loss of connectivity with a Remote SIP Server.

Copyright © 2015 Sonus Networks. All rights reserved.

When the UX is configured for Forward Registration after Local Processing in the SIP Signaling Group, each phone's SIP AOR captured by the UX before it is passed on to the External SIP Server. In the event of a loss of connectivity, i.e., WAN outage, local SIP phone connectivity within the branch is preserved by the UX acting as the local SIP Registrar.

The SIP Phone Survivability configuration and behavior is documented in the UX User's Guide.



Enhancements

6

SIP Diversion Implementation

UX provides a mapping of incoming Request History-Info and Referred-by headers to outgoing Diversion headers to SIP server UAs and proxies in the forward path. The scope of this feature is mainly interworking between the SIP history-info ingress side and the redirecting number egress side, and does not include the functionality of history-info feature (RFC4244) itself.

7

Configurable Transport Timeout Timer

Beginning with Revision 2.1 the UX supports a configurable Transport Timeout Timer. When Outbound connections are attempted and the far end blocks the attempt, this timer is used to timeout the connection. This feature allows the user to configure the value for this timer through WebUI.

For more information about this feature, see the following section in the UX Customer Documentation:

- Adding and Modifying SIP Profiles

Copyright © 2015 Sonus Networks. All rights reserved.



DiffServe QoS Implementation

UX marks all outgoing media packets ((S)RTP and (S)RTCP) with the configured DSCP value. The DSCP value is applied only media packets and not to signaling or protocol packets. This may be used by the network operators to classify these packets ar provide higher priority queues in the core routers/switches in the network.

This feature is configured in the Media System Configuration page of the User Interface.



Enable and Disable Transformation Table Entries

Beginning with Revision 2.1 the UX supports the ability to enable and disable individual entries in Transformation Tables.

For more information about this feature, see Adding and Modifying Entries to Transformation Tables in the UX User's Guide.

Release Notices

> If you are upgrading from a version **prior to 2.0**, be aware that this upgrade has **strict dependencies**. To ensure a successful upgrade, you **must follow the UX 2.1 Upgrade Notes**.

- For a listing of known issues and limitations in this release, please review the Notes and Limitations page.
- For system performance information, see the UX System Performance and Capacity page.

Updates and Fixes in this Release

Bug ID	Headline
SYM-9800	UX closes Signaling Group Initial Configuration dialog if User Does Not Enter Required Information
SYM-9336	If after a UX reboot DSPs cannot be downloaded, don't bring up T1/E1 lines
SYM-7711	Tone Tables missing Disconnect Tone Type
SYM-9891	E911: UX not passing through Supported: geolocation and Geolocation Headers
SYM-9760	UX MIB for AD UP and other events does not include a 'none' for alarm severity
SYM-9877	ISDN call state not updated correctly on T313 expiry
SYM-9757	DTMF payload type should not need to be the same to pass DTMF
SYM-9781	FXS Channel phone number starting with 0 has first digit truncated

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-4455	UX does not accept alternate channel selection
SYM-5635	UX - 500 Internal Server Error calling Cisco SPA-502 SIP Phone
SYM-9101	Logs will not rotate Webui Log stuck at 200Meg
SYM-9042	UI: system uptime incorrectly displayed after reach to month
SYM-8155	Update Dump method to not print user passwords
SYM-8932	UX shows non-installed DSP
SYM-8362	under race condition, some calls hang on connected state after stopped the sip to sip with forking long duration tests
SYM-9095	Service version display on Task tab for Lync SBA does not display correct version installed
SYM-8829	DNS problems failover to secondary DNS server
SYM-9790	UX does not do Round Robin Load Balancing between servers in SIP Server table.
SYM-8403	Move the secondary to primary address after apply disabled the secondary address
SYM-8901	UX1000 : Debug facility for webui does not work for UX1000.
SYM-9535	TLS handshake with IP uses as common name in certificate failing with SSL error code 27 (certificate not trusted)
SYM-9582	UX does not release ISDN channel after received DISC w/PI=8 with configuration even Lync sends CANCEL
SYM-9583	Message Translation to convert Alert with no IE to either Progress or Alert with IE not working in SIP to SIP
SYM-9168	487 request terminated not being sent to originating SIP call leg
SYM-9159	After adding 102nd Transformation table entry all previous entries disappear from table. Deleting last last entry added restores all previous entries.
SYM-9138	Unable to Defragment and parse SIP messages
SYM-9130	Host FQDN in SIP Server table cannot have a digit in last domain part
SYM-6811	UX is not playing Inband messages when a PROGRESS indicator is provided on the ISDN DISCONNECT message
SYM-9503	When SG has Static NAT and Bind IP Interface is set, UX uses application IP and port 0 in From header, not NAT IP
SYM-9118	Issue passing through ISDN codeset 6 shift
SYM-6913	Calling name not being passed from PSTN to LYNC via facility message

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-8904	Session progress SDP and 200 ok SDP o= session number and version do not match
SYM-8899	UX does not apply new SIP profile value immediately to SIP-OPTIONS
SYM-8886	AD Backup Failed messages seen on UX1000 without External USB drive
SYM-9103	Downgrade Software Partition Issue - UX Becomes Unresponsive
SYM-8804	MWI. UX sends wrong IP address in NOTIFY message SIP URI.
SYM-8020	Reload button for webui.log disappears
SYM-9016	200 OK for answered sent to the wrong IP
SYM-9144	'FQDN in From Header' setting should be applied to REGISTER request as well
SYM-8882	UX keeps sending REGISTER to ITSP even SG is disabled
SYM-9525	When Outbound Proxy is configured and NOT reachable, UX should NOT route calls to server entries
SYM-8973	UX1000 Modify IP Task: Ethernet 2 should be optional
SYM-7662	FXS transmits incorrect bit pattern in Reverse Battery state.
SYM-8233	Early-Media continues on invalid channel
SYM-7640	Reset of Call Counters for ISDN not actually resetting the values
SYM-2262	Service Status should be made available, and shown, for Signaling Groups
SYM-7655	Caller ID Japanese NTT Caller ID failed UX1000
SYM-8086	In case of CAS R2->SIP failed call, provide Congestion for 30 seconds, then Answer/Hangup
SYM-9083	Order of the transformation rules is not the same between the original and its copy of an entry of the transformation table.
SYM-6961	Multiple contacts are not getting registered in single REGISTER method in UX
SYM-4522	RT Monitor View refresh degrades the performance under high load
SYM-7506	WEBUI - Shows "Last Test Call action failed" but actually it success.
SYM-8920	UX does not support Wild Card Certificates FQDN match for TLS Operation
SYM-7685	The B-channels should be unblocked after delete then add back the ISDN SG
SYM-9265	Calling name on "Call information" from real time view / channel table is always blank
SYM-8342	CAS Channel incorrectly indicated as ISDN in Outbound Channel Properties table

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-9141	SIP Server Entry default value for Priority (None) doesn't make sense
SYM-6923	SDP Origin field not decoded due to spaces
SYM-8352	Q.850 Cause 63 sent with incorrect Location
SYM-7971	CAS User Side Glare Outbound calls released with incorrect Cause.
SYM-9463	Can't open/close/open rows in tables within Tasks tab which don't have inner tab defined (e.g.: ASM Installed Packages)
SYM-8205	Global UX runtime counters do not stick - getting flushed automatically in about an hour
SYM-7967	No dial tone detected Alarm not generated
SYM-8213	Calling Party digits passed to CAS R2 if ingress SIP message includes Privacy: id header
SYM-9107	FXS port gain setting should stay even If profile country is changed
SYM-8400	Attended transfered from Lync analog Endpoint fails when BYE is sent before NOTIFY
SYM-8800	Issues when ip address for UX gateway is changed in DNS
SYM-7061	SIP ST: UPDATE not being sent before call disconnect when refresh not received from peer
SYM-9071	UX1000: Error when trying to download .bin corefile from debug facility.
SYM-8506	Introduce the drop down selection for lifetime value for media crypto profiles.
SYM-8096	Call Transfer works even if disabled in Supplementary Services Profile
SYM-7663	CDR Configuration in WEBUI allows Accounting Port Setup to a restricted Authentication Port 1812
SYM-8298	Update Settings "Application Partitions" UI to remove confusion
SYM-8760	"Twist" needs to be provided in DTMF digits generated by the UX DSP
SYM-7666	Counters of RADIUS Accounting Servers do NOT clear Statistics after Acct Mode change in WEBUI
SYM-7595	"SG taken out of service" alarm doesn't show when only one SG using the same SIP server
SYM-7638	Federated IP Validation in configvalidators.cpp shouldn't use libctl headers
SYM-8629	Placement of Controlled Slips on DS1 Port Counters screen
SYM-8598	When try to copy Call routing table with disabled destination SG, webui shows error dialog. But copying is completed.
SYM-7789	UX1000: There is no error message if using wrong IP address to configure the ASM IP

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-7878	Need to disable action buttons immediately after being selected until process finishes and provide feedback when appropriate
SYM-4205	SIP diversion-screen, diversion-privacy parameters not used to populate ISDN Redirecting Number IE.
SYM-4050	Outgoing SIP Diversion header missing diversion-privacy, diversion-screen parameters
SYM-7036	Reset the root password to the hardware ID based password after a config restore
SYM-5850	SIP should provide the in/out current(active) call counters to SNMP
SYM-8006	Unavailable Seconds not declared
SYM-8244	No instant visual feedback when Setting Active Partition due to response lag for up to 13 seconds
SYM-7920	Fractional T1/E1: Display error if user blocks/unblock/resets un-configured B-channels
SYM-8003	Bursty Errored Seconds counter not working.
SYM-8026	After layer 1 admin disabled then enabled, the B-channels and D-channel should not up when the ISDN SG admin is disabled
SYM-8182	BMP-TLS Handshake Alert Failure Alarm sent on startup occasionally
SYM-7379	Unacknowledged provisional response should be rejected with 5xx

UX 2.1 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to UX 2.1:

- Upgrading from UX 2.0.x to 2.1
- Upgrading from UX 1.3.x to 2.1
  - General Upgrade Instructions
  - Upgrading the ASM Recovery Partition
  - Installing the SBA Lync Server 2010 Cumulative Update 7 (CU7) October 2012

> **Before You Upgrade**
>
> If you are:
>
> - Upgrading from **1.3.x**, and
> - Your UX has **a built-in ASM**:
>
> Please note that the ASM base image has changed with UX 2.x. You will need to **upgrade the ASM Recovery Partition** image as outlined in these upgrade notes – refer to the #Upgrading from UX 1.3.x to 2.1 section.

Upgrading from UX 2.0.x to 2.1

There are no special considerations for upgrading from 2.0.x releases, beyond those mentioned in the general UX upgrade guide.

Copyright © 2015 Sonus Networks. All rights reserved.

Upgrading from UX 1.3.x to 2.1

General Upgrade Instructions

In this section, you will be tasked to follow the instructions in the general UX upgrade guide (non-version specific) first. Once completed, you will need to follow the remaining instructions outlined on this page - these are the UX 2.x version-specific instructions.

> If your UX is configured as a Lync SBA with **a built-in ASM**, the general upgrade guide will first ask to upgrade the UX Communication Service, and then upgrade the UX software as the next step. **Please note that once you upgrade the UX Communication Service to 2.1, it will no longer be able to communicate with the UX system until the UX software is also upgraded to 2.1**. Do not be alarmed - this is because UX Communication Service version 2.x are not backwards compatible with UX software versions 1.3.x or earlier. Verify the UX Communication Service version number once both have been upgraded.

Once you have finished with the general upgrade guide, please follow the version-specific instructions below

Upgrading the ASM Recovery Partition

You may skip this section if your UX hardware is not configured with a built-in ASM.
You can only proceed with this section once you have completed the #General Upgrade Instructions outlined above.

This step is required to ensure that the ASM Recovery Partition is correctly provisioned with the 2.x image files, should it be necessary at a future date to restore the system from this partition. See Managing the ASM for details on the recovery partition.

1. Download the image from the UX Download Center.
   - The ASM Image is located under: UX ASM Recovery Images ... 2.x.x
2. Follow the instructions outlined in Updating the ASM Recovery Partition.
   Note: You do not need to Re-initialize the ASM.

Installing the SBA Lync Server 2010 Cumulative Update 7 (CU7) October 2012

You may skip this section if your UX hardware is not configured with a built-in ASM deployed as a Lync SBA.

Microsoft has released Cumulative Update 7 (CU7) that is dated October 2012 for Lync Server 2010 (KB2493736). Apply this update to the ASM deployed as a Lync SBA:

1. Download the CU7 package from the UX Download Center
   - The SBA Lync CU is located under: UX Lync Updates `sba-lync-cu7.zip`
2. Follow the instructions outlined in Installing Cumulative Updates for Lync SBA

UX 2.1.1 Release Notes

May 21 2012

Unified Exchange (UX) 2.1.1 is a maintenance release. In addition to hot fixes, UX Version 2.1.1 includes two major improvements:

- Availability improvement: The system now correctly recovers from DSP crashes without rebooting — **SYM-9432** and **SYM-9946**.

Copyright © 2015 Sonus Networks. All rights reserved.

- Major bug fix: Resolved crashes that were occurring under high load — **SYM-9964** and **SYM-10049**.

Don't have UX 2.1 yet?

Take a look at the new features and other highlights in the UX 2.1 Release Notes.

Ready to upgrade to 2.1.1?

Review the UX 2.1.1 Upgrade Notes
Download Latest Version

Updates and Fixes in this Release

Bug ID	Headline
SYM-10449	ISDN TE does not transition from state F3 to F4 upon PH-ACTIVATE REQUEST
SYM-10450	UX Not Negotiating TLS With Office 365 UM Server
SYM-8973	UX1000 Modify IP Task: Ethernet 2 should be optional
SYM-10049	MSC crashed after 57 hours ISDN to SIP loopback test
SYM-10075	Called Number in outgoing ISDN MWI not updated after transformation
SYM-10045	MOH is stops when both endpoints are put on-hold / MOH Source = Live
SYM-9953	REL sent at T310 expiry has incorrect Cause
SYM-9936	Errored Calls counter not working
SYM-10102	SIP Channels on Lync SG are stuck in Releasing state
SYM-9975	Sym-isdn crashes if call received on remotely blocked circuit.
SYM-10004	UX Reject the inbound BRI call when B channel 1 is blocked
SYM-9995	DISC with incorrectly encoded Cause IE sent after T313 expiry.
SYM-10282	UX does an audio cut throgh on hold from FXS when lync resumes the call
SYM-10280	Need configurable option to add Progress Indicator IE to outbound ISDN SETUP
SYM-10038	When sym-sip restarts License manager should release the SIP license
SYM-10283	Analog Relay Configuration missing when DS1 card not present

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10251	Audio law on FXS is incorrect if PRI ports are configured to E1 and disabled
SYM-10317	Unsolicited ISDN UA frame in BRI doesn't cause TEI Verify/Check Request response
SYM-10025	SIP Transport Switch Timer: With Reuse ON, switch timer value does not take effect
SYM-10010	UX needs to provide configuration for passing through ISDN Facility messages, some PBX's do not accept them
SYM-9466	Change DSCP value some times cause the Web UI hangs on "Apply changes--Please wait" for long time
SYM-10108	Registrar Minimum TTL on signaling group is incorrectly named
SYM-9914	UX does not set Calling Name properly in the from if the presentation is restricted
SYM-10104	Do not use DSP's if the forked call transitions to TDM-TDM
SYM-9961	Malformed Contact header in outbound REGISTER
SYM-10100	Bad CAS line may permanently lock up all TDM licenses
SYM-10070	UX Not Handling Referred-By Header in SIP INVITE And Does Not Send Diverion In Follow-on INVITE
SYM-10039	Performance improvement in Registrar database area for contact search during call scenarios.
SYM-9850	BRI calls rejected with "rearranged channel NOT available" error
SYM-10068	ISDN Channel lockup after T313 expiry.
SYM-9999	Transformation table allow user to configure output ELIN Identifier but UX does nothing to it
SYM-10024	No progress tone (fast busy) for a busy end point over FXO
SYM-10016	Incorrect retransmission interval of Identity Request message
SYM-10050	AD Lookup fails against userPrincipalName attribute
SYM-9819	On transport failure UX does not attempt to setup transport with the second server
SYM-9824	Lync generates Errors with event ID 25020. UX does not have a user portion of the to: header sent on the INVITE after the REFER
SYM-9967	UX still sends multiple 183 Progress after accepting a CANCEL
SYM-9926	Transformation name ordering is case sensitive.
SYM-9895	UX should send CANCEL even Play Inband Message post-disconnect is enabled if call is not connected yet
SYM-9893	Calling number shows as callback number during 911 call using CAS R2
SYM-10002	SYM-SIP crashed during heavy register load tests

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10012	Filter Called or Calling Party numbers for R2 to 0-9 only instead of standard DTMF (0-9, A-F, * and #)
SYM-10046	UX doesn't send original NumPlan and NumType as received in inbound Overlap dialing SETUP message
SYM-10043	MOH audio doesn't stop after the call is transfered. / MOH Source = Live
SYM-10032	New SIP signaling groups should have Music on hold disabled
SYM-10054	ISDN TEI management messages sent with incorrect TEI

UX 2.1.1 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to UX 2.1.1:

- Upgrading from UX 2.0.x to 2.1.1
- Upgrading from UX 1.3.x to 2.1.1

Upgrading from UX 2.0.x to 2.1.1

There are no special considerations for upgrading from 2.0.x releases, beyond those mentioned in the general UX upgrade guide.

Upgrading from UX 1.3.x to 2.1.1

The upgrade instructions for 2.1.1 are the same as those for 2.1. Please follow the instructions outlined in the UX 2.1 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

UX 2.1.2 Release Notes

Unified Exchange (UX) 2.1.2 is a maintenance release. It adds support for the UX2000 24 port FXS card. Please contact your NET account representative for ordering information.

Starting with UX 2.1.2b158 the codec order for SIP to SIP calls when transcoding is enabled has changed.
Unlike previous releases, UX does not minimize transcoding by placing the inbound codec on the top of the list.
It follows the codec list as it is specified in the media list.

When transcoding is disabled, UX follows the previous behavior.

In addition to hot fixes, UX Version 2.1.2 includes several compatibility improvements:

- Added support for the new UX2000 24-port FXS card.
- Fixed one way audio on loaded UX1000 after running for a week — **SYM-10488**.
- AD cache is no longer case sensitive — **SYM-10552**.
- Wider range of FXO Calibration and Dial Tone Detection re-enabled (not functioning since build 146) — **SYM-10664**.
- Additional support of LX for tracking ISDN calls — **SYM-10220**.
- SDP advertises correct IP address when binding to LAN port — **SYM-10662**.
- ISDN PRI Overlap Receiving works with additional carriers — **SYM-10553**.

Copyright © 2015 Sonus Networks. All rights reserved.

- UX correctly connects Exchange UM *Play on Phone* sessions — **SYM-10549**.
- Fax pass-through and FAX SIP calls are passed more reliably — **SYM-10288**, **SYM-10677**.
- When Music On Hold is disabled, Hold is no longer passed to the remote leg — **SYM-10494**.

Don't have UX 2.1 yet?

Take a look at the new features and other highlights in the UX 2.1 Release Notes.

Ready to upgrade to 2.1.2?

Review the UX 2.1.2 Upgrade Notes
Download Latest Version

Updates and Fixes in this Release

Bug ID	Headline
SYM-11056	Alphabetical sort the Tranformation Table pulldown in the Action Set
SYM-11047	Noise/Static on FXS to BRI or ISDN calls in certain hardware configurations
SYM-11145	UXcomm does not return a failure for unknown actions which can result in forward compatibility timeouts
SYM-11078	Noise and static when playing MOH with presence of BRI but no DS1 card
SYM-11162	UX2000 MSC core while changing Caller-ID mode from DTMF Reverse Battery to FSK, no ring
SYM-10979	UX1000 is populating the Diversion Header with the wrong interface Host Name/IP Address
SYM-10693	Modem over SIP does not Establish
SYM-10895	Dead Call Detect often does not work for SIP to SIP calls
SYM-11017	Fragmented UDP packets not handled by UX
SYM-10879	Blind transfer has no ringback after first call reject
SYM-10934	UX drops audio on blind transfer
SYM-11032	Application restart error: sym-snmp crashed with high SNMP traffic
SYM-11051	FAX from TDM to Lync pass through stoped working
SYM-11066	Error in Display name encoding in Q931 layer
SYM-10945	Increase certificate store to support for downgrading from R2.2

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10811	T1 loop start FXO channel does not populate Own Number on call from T1 loop start FXS
SYM-3729	Modem Pass-through not working consistently
SYM-10978	Single lookup on DSP resource fails for certain call ids
SYM-10937	When changing from T1* 2-port card to T1* 8-port UX2000 did not initialize T1* 8-port card correctly, missing ports 4-8.
SYM-10897	UX flooding the SIP channel when the DNS resolution fails
SYM-10756	Support for SCOM 2012
SYM-8068	No audio on multiple blind transfers
SYM-10894	Call Route Priority does not work consistently
SYM-10744	UX drops syslog TCP connection on configuration change
SYM-10843	ASM Failure Recovered" 2992 times in the past two days
SYM-10739	UX needs to handle annexb parameter for G.729
SYM-10763	Dial tone sometimes is not provided when flash hook during dialing digits
SYM-10780	When ISDN calls to FXS noticeable static sound is always heard at the beginning of ringback if set Caller ID Type to FSK
SYM-10675	After UX Reboot FXS SG Service Status shows UP while Admin State is Disabled
SYM-10458	During SBA deployment, We are not able to rerun properly the Start Replication if the first time fail
SYM-10781	When FXS blind transfers ISDN1 to ISDN2, inband ringback tone should be played on ISDN1 instead of local tone
SYM-10798	Add additional test option to sym-analog-mfg to allow test of the UX2000 FXS LED
SYM-10696	UX2000 - after replacing DS1 card with FXS card, unable to delete DS1 ports
SYM-10715	REFER from Mediation does not have Ms-opaque tag in REFER-TO header, but in the Contact. UX constructs INVITE without username portion in the To:
SYM-10651	Issue populating Calling Name with Active Directory display names that contain a comma
SYM-10653	RADIUS not working running PhonEXONE RADIUS server software on the ASM
SYM-10730	Need to block sending MOH play/stop commands to DSP if there is NO file uploaded
SYM-10488	Two UX1000 with same issue "one way audio after running for a week"
SYM-10747	Need A-Law/M-Law Conversion For E1-FXS Calls

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10761	When set FXS SG to Outbound, Tone table for the SG is not configurable anymore
SYM-10623	SNMP dies and kill snmp command is needed to restart the process
SYM-10533	RADIUS server counters link doesn't work if both auth and accounting are disabled
SYM-10679	WEBUI displays a wrong CAS Supplementary Service profile name when the name has lengths 64
SYM-10664	FXO Calibration fails
SYM-10695	After timeout on off-hook without dialing any digits analog phone gets fast busy tone but RT Status view is still showing C
SYM-10686	Application Service restart on UX2000 for CCC
SYM-10735	Mandatory match should clear optional match requirements if no optional rule matches
SYM-10677	Sending a FAX over SIP makes UX2000 crash
SYM-10220	Log Conference ID (CID) in SIP and ISDN debug log
SYM-10678	Hold/Resume not working when connecting with SIP to Cisco Call manger
SYM-10669	Change Install New License screen wording
SYM-10671	Wrong payload size used when UX transcodes call.
SYM-10662	UX advertise wrong IP (old UX IP) in SDP if SIP IP Details configured to Bind to specific lan port.
SYM-10619	Network Specific Facilities IE needed for ATT 5ESS as a configuration option, same as VX support
SYM-10631	UX sends ACK to different port from contact-uri of 200OK even no outbound proxy setting
SYM-10655	High temp alarm issue randomly seen
SYM-10659	UX2000 - new directory for 24FXS CPLD file
SYM-10657	UX stops processing calls
SYM-10548	TCP: UX closes connection when sending a RE-INVITE for challenged calls.
SYM-10552	AD Cache Normalization Problem
SYM-10646	AD Cache truncated at startup search may fail and no online AD search is done
SYM-9179	If FXS port is in offhook state when UX is rebooted, the driver should connect the voice path.
SYM-10566	DSP license leaking
SYM-10557	In the SIP Contact Registrant, Add SIP Contact, specify that Contact must be username only, not URI

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10563	UX does not allow user to change ethernet 2 IP address even all SIP SG are disabled
SYM-10537	AD Caching in "updates" mode causes performance issues during load testing
SYM-10600	UX wizard screen errors out when the valid domain name of "e.uh.edu" is used as the internet domain name
SYM-10602	When javascript validation fails on custom 'onSubmit' validator, "Apply" button never comes back w/o refresh
SYM-10640	Cannot modify any of the linecard port parameters
SYM-9917	UX does not respond to 487 with ack message
SYM-10636	UX2000 FXS DC Profile and BAT Changes
SYM-10627	Debug Facility: Web Interface / 'list corefiles' does not recognize mounted USB flash drives on UX1000.
SYM-10624	UX2000 FXS: New AC Profiles needed, to match UX1000 Loss Plan
SYM-10601	BRI CALL PROCEEDING sent with incorrect Channel ID
SYM-10549	"Replaces" option should be supported by UX under SIP Profile
SYM-10541	UX crashed
SYM-10518	Diversion header in outb.INVITE uses incorrect Diversion header althoug the "Redirecting number" is previously transformed correctly
SYM-10553	Overlap Recieve problem with UX 2.1.0
SYM-10558	UX2000/MOH: Unable to load new MOH Audio file - "Error Code 4"
SYM-10500	sym-sip constantly restarting
SYM-10513	Clean up display of alarm 12.1
SYM-10556	Modify libiptapi to interact with conntrack directly.
SYM-10430	DSP crashed while reproducing bug sym-9822
SYM-9509	ASM Failure Recovered alarm. 10 - 12 times a day
SYM-10507	FQDN in From Header parameter in SIP Profile did not change the TO URI in 2.0.2v139 & 2.1v142
SYM-10522	MSC cored; invalid errors are being logged.
SYM-10497	CAS channel doesn't receive signalling response
SYM-10545	TSI TDM Stream input bit delay incorrect for UX2000 FXS Line Card
SYM-10526	Transcoding G729/G711-A law to G711-u codec fails

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-10539	UX1000 - Calls are failing on the third DSP daughtercard
SYM-10517	Switching DC in AD config throws error: The following errors occured: Validation Error - Out of range value for resource ADConfig ID.
SYM-10514	options web ui needs to have additonal username fields for iteroperability
SYM-10288	FAX Passthrough not working
SYM-10028	UX should not allow T1 to be set below 100ms
SYM-10040	Calls fail on one Channel
SYM-10530	ISDN log shows wrong port identifier in log for BRI for card slots other than 1
SYM-10454	UX leaking FDs with socket error 24
SYM-10503	UX1000 FXS port calibration does not complete correctly.
SYM-10527	UX1000 WebUI is showing IP address as configurable for the ASM Ethernet port when it shouldn't be
SYM-10506	UX does not respond to an inbound request while trying to setup call (referred call) on the outbound
SYM-10505	Setting Play Ringback=Always does not work
SYM-10111	Early media from a different IP specified in the 183 does not flow to the DSP, dropped by network policy
SYM-10472	Lync client cannot hear BT from ISDN if 'Play Inband Message post-disconnect' is Yes
SYM-10110	MSC "Conference not found" errors printed with CAS to ISDN calls
SYM-10496	Exceeding maximum call forking causes endpoints to stop ringing; caller hears ringback
SYM-10494	Hold not propagated to the other leg

UX 2.1.2 Upgrade Notes

This document contains specific upgrade notes for customers planning to upgrade to UX 2.1.2:

- Upgrading from UX 1.3.x to 2.1.2
- Upgrading from UX 2.0.0 and later

Upgrading from UX 1.3.x to 2.1.2

The upgrade instructions for 2.1.2 are the same as those for 2.1. Please follow the instructions outlined in the UX 2.1 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

Upgrading from UX 2.0.0 and later

There are no special considerations for upgrading from these releases, beyond those mentioned in the general UX

Copyright © 2015 Sonus Networks. All rights reserved.

upgrade guide.

UX 2.1.3 Release Notes

Unified Exchange (UX) 2.1.3 build 185 is a maintenance release. In addition to hot fixes, this build includes the following major improvements:

- Support for large fragmented SIP messages — **SYM-9138**.
- Resolved issue where nodes connected to many SIP servers (with TLS) become unresponsive — **SYM-11669**.
- Further improved support for Lync team calling — **SYM-11795**.
- Media system stability improvements. — **SYM-12464**.
- Resolved issue where Dual Forking calls lose audio — **SYM-12823**.
- CAS R2 Emergency calls are no longer rejected by Columbia's PSDN — **SYM-13049**.
- Improved handling of Group-C tones on CAS R2 — **SYM-12469**.

Don't have UX 2.1 yet?

Take a look at the new features and other highlights in the UX 2.1 Release Notes.

Ready to upgrade to 2.1.3?

Review the UX 2.1.3 Upgrade Notes
Download Latest Version

Updates and Fixes in this Release

Bug ID	Headline	Build
SYM-13048	Intermittent timeout viewing SBA "Operational Status" in Tasks	185
SYM-13049	Colombia PSTN Rejects CAS-R2 Emergency Calls with Congestion Reason	185
SYM-12823	Intermittent media path issue when Dual Forking is enabled	185
SYM-12811	Manual local log rotate results in out of sequence logs	185
SYM-12469	Improved handling of Group-C tones on CAS R2	185
SYM-12534	E911 call back does not include caller extension	185
SYM-12646	Unable to set the Media list in call route	185
SYM-12464	MSC stability improvements	181
SYM-12359	Intermittent call disconnect after alert when using ISDN DMS100	181

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-11927	USB drive unmount operation performed after loading ASM image	181
SYM-12163	Intermittent SNMP trap disable occurs at boot time	181
SYM-5326	SNMP service stability improvements	181
SYM-12358	Improved Line Card PSU health check algorithm	181
SYM-12195	Turn OFF blue hot-swap LED on UX2000 Line Cards	181
SYM-12310	Validation to disallow enabling Media Transcoding setting if feature is unlicensed	181
SYM-12307	ISDN CONNECT IEs are being dropped and not passed through UX	181
SYM-11328	No ringback tone when ISDN BRI calls to ISDN BRI forking to ISDN BRI	176
SYM-12176	UX stops playing progress tone on inbound SIP Registrar on call reject on ISDN	176
SYM-9122	UX does not set "Presentation", "Screening" and Redirecting Number	176
SYM-12157	Cause code re-routing does not work with on board call Forking	176
SYM-11669	UX stopped processing calls if a large number of TLS based SIP servers are configured	176
SYM-11818	WEBUI will not allow changes in signaling group or media list	176
SYM-12161	SNMP Traps are not being sent	176
SYM-12153	Unable to login into WebUI due to full flash storage	176
SYM-11890	Delayed media broken when PRACK is not supported on the caller	176
SYM-11649	RTP port leak in certain call forking scenarios	176
SYM-11658	UX1000 BRI Lync Wizard problems	176
SYM-11638	UX to LYNC teamgroup SIM ring calls failing	176
SYM-11630	MSC stability improvements	176
SYM-11537	ISDN Restart with multiple channels is responded to with multiple Restart Ack messages and not one single message	176
SYM-11107	FXS channel remains in connected state after a FXS to FXS transfer to Lync call	176
SYM-11332	3.1k audio is swapped with Restricted Data in WEBUI config drop down	176
SYM-11425	Segmented ALERT and CONNECT messages not properly processed after reassembling	176
SYM-11397	Intermittent MWI functionality	176

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-11349	E911 Call back to multiple Lync End ports simultaneously failed on audio verification due to call disconnected because the hold failed	165
SYM-11245	Change the Settings Tab, Security, Certificates, Server Certificates to UX Certificate as it is in the Tasks Tab, Lync Setup	165
SYM-11309	MSC stability improvements	165
SYM-9138	Unable to de-fragment and parse SIP messages	165
SYM-11207	Calls drop out mid conversation	165
SYM-10926	UX does media stream issue in case of a double hold	165
SYM-11256	UX unable to resolve outbound proxy FQDN	165
SYM-11126	Contact Header does not contain Calling Number	165

UX 2.1.3 Upgrade Notes

This document contains specific upgrade notes for customers planning to upgrade to UX 2.1.3:

- Upgrading from UX 1.3.x to 2.1.3
- Upgrading from UX 2.0.0 and later

Upgrading from UX 1.3.x to 2.1.3

The upgrade instructions for 2.1.3 are the same as those for 2.1. Please follow the instructions outlined in the UX 2.1 Upgrade Notes - be sure to follow the special instructions listed there, particularly if your system has a **built-in ASM**.

Upgrading from UX 2.0.0 and later

There are no special considerations for upgrading from these releases, beyond those mentioned in the general UX upgrade guide.

UX 2.0 Release Notes

Release Part Number: 481-40174-006

30 November 2011

The NET Unified Exchange (UX) team is proud to deliver a brand new version of the industry's best unified communications, enterprise border controller and multi-service business gateway applications. Unified Exchange (UX) 2.0.0 is a feature release delivering: the UX1000 Unified Communications Gateway and Session Border Controller for small to mid-sized deployments, Call Detail Records (CDR), Fractional T1/E1 Support, CAS Signalling Support, and Microsoft SCOM Support.

Copyright © 2015 Sonus Networks. All rights reserved.

Highlights of this Release:

- New Hardware
  - Introducing the UX1000
- New Software
  - Call Detail Records (CDR) Support
  - Fractional T1/E1 Support
  - CAS Support
  - Microsoft System Center Operations Manger (SCOM) Support
- Enhancements
  - WebUI Speed Improvement
  - Active Directory (AD) Cache Refresh
  - SIP URI Extensions
  - Call Name and Number from the SIP From Header (CCNF)/Privacy Support
  - Additional UX API Methods
- Release Notices
- Updates and Fixes in this Release

Download the latest version:

- First read the #Release Notices for important information about this release.
- See the full list of #Updates and Fixes in this Release.





New Hardware



Introducing the UX1000



NET is pleased to announce the release of the **UX1000 Unified Communications Gateway and Session Border Controller** f small to mid-sized deployments.

The UX1000 offers true any-to-any signaling translation and media interworking between Lync and legacy analog, TDM clients and PSTN endpoints. The UX1000 can simultaneously connect to legacy TDM PBXs and the PSTN through two T1/E1 PRI por In addition to the PRI ports, up to 24 FXS ports are available for analog phones, faxes, and the PSTN.

In parallel, the UX1000 also interconnects IP-based endpoints (i.e. IP PBXs, non-Lync SIP clients) and public VoIP networks (e ITSPs) to the Lync clients.

With NET's optional SmartSIP application, there's no need to replace your legacy non-Lync SIP clients. The UX1000 can report

Copyright © 2015 Sonus Networks. All rights reserved.

non-Lync SIP client user states (e.g. presence, user busy, etc.) to Lync clients.

The UX1000 offers a wide range of I/O and call capacities (4 to 84 concurrent PSTN/analog VoIP connections) to optimize branch office enhanced gateway/Survivable Branch Appliance (SBA) costs. Simultaneously, the UX1000 can support up to 45 I to IP calls. SRTP (secured VoIP media) and TLS (secured VoIP signaling) are fully supported with no impact on call capacity. Voice media quality is enhanced, given the latest generation embedded IP switching fabric at the core of the UX1000 system.

Supported hardware in this release for the UX1000:

- FXS and DS1 (T1/E1)
- Medium Capacity DSP
- ECC and Non-ECC Application Solution Module (ASM)

The UX1000 base system includes:

- Two 10/100/1000base-T software configurable WAN/LAN interfaces, routable up to 100 Mbps in a full duple mode.
- One medium capacity DSP
- Six legacy I/O voice port slots (3 in a top row on the back of the chassis, 3 in a bottom row) that support the following:
    - One to six quad port FXS (Foreign eXchange Station) analog cards to connect to legacy phones, faxes, etc.

For more information, see UX1000 Hardware Specifications.

New Software



Call Detail Records (CDR) Support

Beginning in version 2.0, UX supports the logging of accounting and call metrics related data on RADIUS based accounting servers. The UX functions as a RADIUS client; gathering, queuing and transmitting Call Detail Records to the RADIUS accounting server.

The CDR feature of the UX enables administrators and users to gather a wealth of information specific to calls placed and/or received through the UX. Call Detail Records are stored on a RADIUS server using both a standard Radius Dictionary and a NE specific RADIUS Dictionary that can be retrieved from the server at anytime.

For more information about this feature, see Working with Call Detail Records.



Fractional T1/E1 Support

Beginning in version 2.0 UX supports Fractional T1/E1 ports. Typically, branch offices do not lease full T1/E1 resources and therefore are limited to the number of channels through which they can connect to their carrier. Partial T1/E1 support on the UX allows the user to configure the number of B-channels on a port to match the number of leased channels. The D-channels for T and E1 remain numbers 24 and 16 respectively.

For more information about this feature, see Managing Telephony Ports.

Copyright © 2015 Sonus Networks. All rights reserved.



CAS Support

Beginning with version 2.0 the UX2000 and UX1000 support **Channel Associated Signaling (CAS)** signaling. The CAS signalling provides the UX series with additional PSTN and PBX interoperability. CAS support is available in the following variants:

Digital	Analog

• E&M
  ○ Wink Start
  ○ Immediate Start
• Loopstart
  ○ Exchange (FXO)
  ○ Subscriber (FXS)
	• FXS
	• Supplementary Services
	  ○ Hold/Resume
	  ○ Transfer

Dial plans are not supported in this release, however inter-digit timeouts can be used to indicate the completion of dialing.

Caller ID Generation is supported for analog FXS with a Caller ID length limitation of 32 characters. For more information about this feature, see Working with CAS.



Microsoft System Center Operations Manger (SCOM) Support

Microsoft System Center Operations Manager 2007 (SCOM) is a Windows application management system which allows IT departments to monitor the health of windows machines and server applications from a central location. The UX SCOM Management Pack allows customers in a Microsoft Server Environment to monitor the health of their UX systems using SCOM.

Delivery
SCOM Packs are delivered as a management pack file. For more information about this feature, see Working with SCOM.

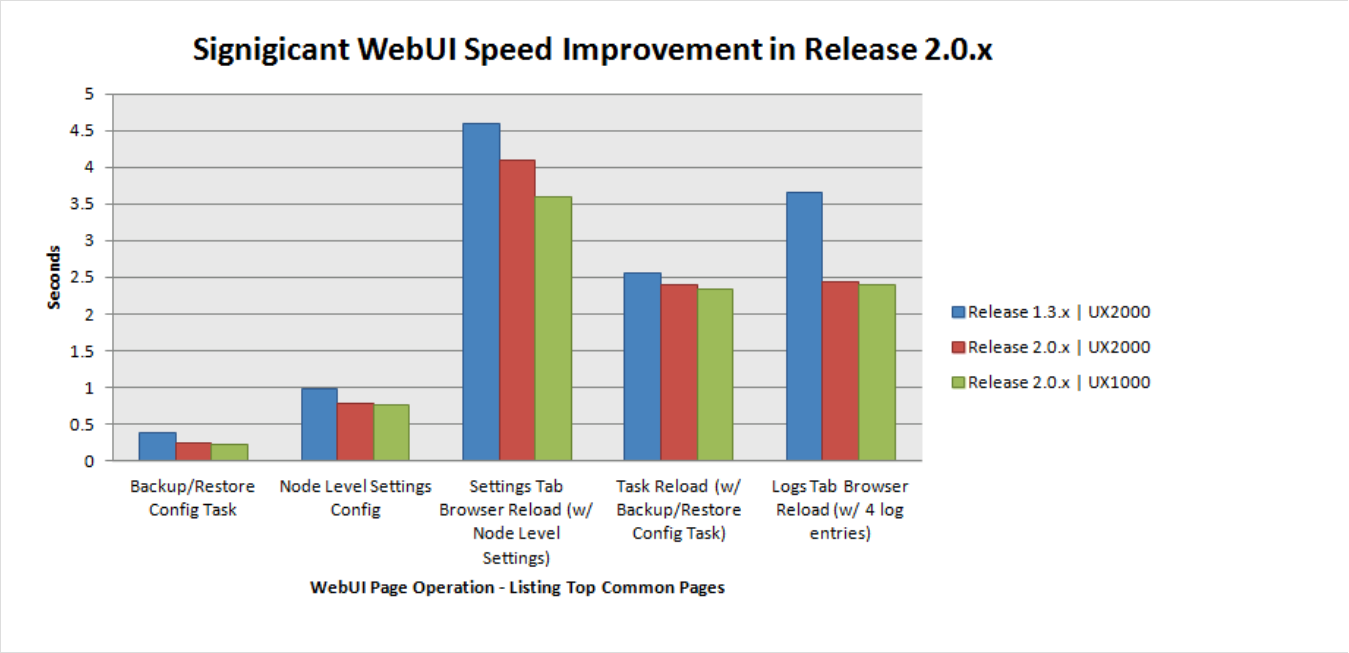
Enhancements



WebUI Speed Improvement

Users upgrading to version 2.0 will notice a significant speed improvement when operating the UX Web Interface. The chart below outlines the acceleration introduced in this release compared to the last release and broken down by UX model. The lowe the bar, the faster the UI response speed.

Copyright © 2015 Sonus Networks. All rights reserved.



The UX1000 has the fastest response time as a result of its newer CPU.

7

Active Directory (AD) Cache Refresh

UX employs a Local AD Cache in an effort to enhance system performance and survivability. Beginning in version 2.0, the UX now supports a manual Local AD Cache refresh feature enhancement.

In addition to scheduled periodic AD Cache updates, the UX allows you to refresh (update) the AD Cache manually. Typically th feature is used to make user information available immediately after they are added to Active Directory, rather than wait for the automatic update, which might take as long as 30 days.

Additionally, the minimum automatic cache update period on the Active Directory Configuration page has been changed from 5 60 minutes. For more information about this feature enhancement, see the Managing Active Directory Caching and Statistics.

8

SIP URI Extensions

Additional support has been added in the Transformation Table, Input and Output types. The following matching attributes have been added in version 2.0:

- Calling Phone Context
- Called Phone Context
- Calling Extension
- Called Extension

For more information about this feature enhancement, see the SIP URI Manipulation.

Copyright © 2015 Sonus Networks. All rights reserved.



Call Name and Number from the SIP From Header (CCNF)/Privacy Support

Beginning with version 2.0, UX supports the ability to always use the identity asserted in the SIP From header. This feature is implemented in a SIP Profile by Enabling the Use Calling Number Name of FROM Header attribute in the Header Customizatio panel. See Adding and Modifying SIP Profiles for more information.



Additional UX API Methods

UX API developers and system administrators upgrading to version 2.0 will have access to even more UX API methods. The following is a summary of the resources added in this release:

- Alarms, events and call stats dispatched by the UX system.
- Resources related to CAS signalling.
- Resources related to the UX application partitions — useful to manage software upgrades programmatically
- Resources related to the local logging functionality — useful to download logs in stored internally

For more information, see the API Reference listed in the UX API User's Guide.

Release Notices

> ⚠ Upgrading from a previous version of UX to version 2.0 has **strict dependencies**. To ensure a successful upgrade, you **must follow the UX 2.0 Upgrade Notes**

- For a listing of known issues and limitations in this release, please review the Notes and Limitations page.
- For system performance information, see the UX System Performance and Capacity page.

Updates and Fixes in this Release

Bug ID	Headline
SYM-3144	UX showing Linux kernel version in SNMP host information
SYM-8249	Change the error msg in file upload "Invalid Image Type" to be more meaningful of the error condition
SYM-7473	Auto Build Sanity: Seemingly benign spammy MSC VAPI error messages being thrown twice a second during ISDN to SIP call churn
SYM-7411	Forking not happenning after re-route and there is one way audio between PSTN and SIP Phone 1
SYM-7312	SIP ST: UX does not send BYE to cleanup call for an expired transaction
SYM-5272	Servicability: add a periodic UX system state monitor w/ logged output

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-6932	Multi-IP setup, the SIP Signaling group is down when SG SIP IP Details is set to Auto/Auto
SYM-5929	CONTACT in SIP Register has Application IP instead of IP from MultiIP interface
SYM-7292	UX Configured with Public and Private Ethernet Interfaces is Using Private IP Address in VIA Header for SIP Registration Requests to Public SIP Server
SYM-5662	Outbound ISDN Glare condition not handled
SYM-7311	PHP restart when request and log rotate occur at same time
SYM-7774	UX rebooted.
SYM-4596	Netconsole - "activepartition" command shows wrong active partition
SYM-4564	Switching to the other partition left UX in a strange state
SYM-7215	Wording on SRTP Key Derivation Rate make SRTP configuration confusing
SYM-7170	Unresolvable FQDN in SG's Federated IP list causes SG to be taken down
SYM-7944	Turn off extra clock signal in UX1000 hardware.
SYM-7029	ntpd Core File upon Rebooting UX Node
SYM-7511	UX Not Using Record Route Address
SYM-6471	Unblocking channels through WebUI still shows Channel out of service alarm. THe alarm is not auto cleared.
SYM-7912	UX1000: After took build 81 and switched partition, the node keeps rebooting; no corefiles but the sym-tip missing before rebooted itself
SYM-7703	Missing supported/require headers in Re-invites and final responses
SYM-7043	INVITE from 302 not sent to CONTACT, put back through routing engine instead
SYM-7126	The "Remove" button in several WebUI displays have the last "e" partially cut off (IE9 and IE8 w/ XP only)
SYM-6729	WEBUI should show the configured active alarm refresh interval in the "Change the alarm view properties" window.
SYM-7040	SIP ST: UX not acting as default refresher
SYM-7819	Conductor (u-boot) target in flute is broken.
SYM-7345	Transformation Pane on first display in WebUI is empty after Setup Wizard creates configuration. Reload corrects display.
SYM-5317	Standard syslog() calls don't work
SYM-7202	UI shouldn't allow call forking if its not licensed

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-5273	Run a periodic cleanup task that removes old core files
SYM-7219	HTTP code error different for different resource, when trying to delete a table which is being used in other resources.
SYM-7564	SIP call failures for missing headers have the wrong debug level (too low)
SYM-7309	An UI error is popped up when the ISDN SG (created without any value in the description field) counters are refreshed
SYM-4723	rotating log file saves(& renames) the old webui.log with "log_20101130-123456" which is not a correct file extension.
SYM-6832	External IP Routing issues with Class B Subnet
SYM-5018	DS1 Counters Returning 0 (DM, SES, and CSS)
SYM-5466	Insert a six-digit counter for all syslog bound messages
SYM-5609	Conditional compilation of ZebOS and Marvell code
SYM-7351	build system sometimes fails on trapgen and cpld due to make remaking
SYM-7158	memory leak detection system not working
SYM-7350	MSC crashes with IP to IP calls
SYM-7344	Progress message received after Alert causes call to disconnect

UX 2.0 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to UX 2.0:

- Upgrading from UX 1.2.x or 1.3.x to 2.0
  - General Upgrade Instructions
  - Upgrading the ASM Recovery Partition
  - Installing the SBA Lync Server 2010 Cumulative Update 4 (CU4) November 2011
  - Licensing Changes
  - Recommended Browsers
- Upgrading from UX 1.0.3

> **Before You Upgrade**
>
> Please note the following points before starting your upgrade:
>
> - If your UX is configured as a Lync SBA with **a built-in ASM** — please note that the ASM base image has changed with UX 2.0. You will be tasked to upgrade the ASM Recovery Partition image as outlined in this upgrade notes.
> - If you are upgrading from **UX 1.0.3 or earlier**, please read the '#Upgrading from UX 1.0.3' section below **before** starting your upgrade.

Upgrading from UX 1.2.x or 1.3.x to 2.0

Copyright © 2015 Sonus Networks. All rights reserved.

General Upgrade Instructions

In this section, you will be tasked to follow the instructions in the general UX upgrade guide (non-version specific) first. Once completed, you will need to follow the remaining instructions outlined on this page - these are the UX 2.0 version-specific instructions.

> If your UX is configured as a Lync SBA with **a built-in ASM**, the general upgrade guide will first ask to upgrade the UX Communication Service, and then upgrade the UX software as the next step. **Please note that once you upgrade the UX Comm. Service to 2.0, it will no longer be able to communicate with the UX system until the software is upgraded to 2.0**. Do not be alarmed by this as the UX Comm. Service version 2.0 are not backwards compatible with UX software versions 1.3.x or earlier. You may postpone the UX Comm. Service version verification after having upgrade the UX software.

Once you have finished with the general upgrade guide, please follow the version-specific instructions below

Upgrading the ASM Recovery Partition

You may skip this section if your UX hardware is not configured with a built-in ASM.
You can only proceed with this section once you have completed the #General Upgrade Instructions outlined above.

This step is required to ensure that the ASM Recovery Partition is correctly provisioned with the R2.0 image files, should it be necessary at a future date to restore the system from this partition. See Managing the ASM for details on the recovery partition:

1. Download the image from the UX Download Center
   - The ASM Image is located under: UX ASM Images ... 2.x.x
2. Follow the instructions outlined in Updating the ASM Recovery Partition
   Note: You do not need to re-initialize the ASM.

Installing the SBA Lync Server 2010 Cumulative Update 4 (CU4) November 2011

You may skip this section if your UX hardware is not configured with a built-in ASM deployed as a Lync SBA.

Microsoft has released a cumulative update 4 (CU4) that is dated November 2011 for Lync Server 2010 (KB2514982). Apply this update to the ASM deployed as a Lync SBA:

1. Download the latest CU4 from the UX Download Center
   - The SBA Lync CU is located under: UX Lync Updates `sba-lync-cu4.zip`
2. Follow the instructions outlined in Installing Cumulative Updates for Lync SBA

Licensing Changes

UX 2.0 introduces CAS and Call Detail Recording (CDR). After having upgraded to 2.0, you must apply the **Base License** to enable and use those features. The UX Base Licenses are available for download on the NET Download website:

1. Download the UX 2.0 Base License from the UX Download Center
2. Open the Base License file using a text editor
3. Copy the contents of the file and Install the license

Verify that both CDR and CAS features are now licensed (will appear as 'Unlimited') by viewing the current licenses.

Copyright © 2015 Sonus Networks. All rights reserved.

Recommended Browsers

The following browsers are recommended for use with UX 2.0:

1. Internet Explorer 8 and 9
2. Firefox 7.x

For more details, refer to Supported Platforms

Upgrading from UX 1.0.3

If you are upgrading from UX 1.0.3 to UX 2.0, you **must upgrade to the latest 1.3.x release first** (1.3.2 recommended). To do this:

1. Follow the instructions in the UX 1.3 Upgrade Notes.
2. Once on 1.3.x, follow the UX 2.0 Upgrade Notes (outlined in the section above) to upgrade UX to 2.0.

UX 2.0.1 Release Notes

Note: This release has been superseded by release software version 2.0.2 - please see UX 2.0.2 Release Notes .

23 Dec 2011

Unified Exchange (UX) 2.0.1 is a maintenance release. In addition to bug fixes, UX release version 2.0.1 fully supports CAS R2 Signaling and also widens the list of countries supported by the Tone Table .

Don't have UX 2.0 yet?

Take a look at the new features and other highlights in the UX 2.0 Release Notes.

Ready to upgrade to 2.0.1?

Review the UX 2.0.1 Upgrade Notes

Updates and Fixes in this Release

Bug ID	Headline
SYM-8743	UX1000 with single DS1 interface having one way audio issue.
SYM-8685	Configuration for the Reuse Timout parameter under Connection Reuse in SIP server table does not accept a configured value
SYM-8508	Node crashed under heavy load
SYM-8670	SIP Server attempts to connect to TCP port 0 on startup
SYM-8589	Post-Login message does not work in 1.3.2 and 2.0.1

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-8398	No audio between end points on second attended transfer
SYM-8627	SIP Server Counters cannot be cleared
SYM-8390	Seemingly benign spammy SIP error messages being thrown 4 times a second during ISDN to SIP call churn @ 1CPS
SYM-7468	ISDN to ISDN call does not route (SIP to ISDN using same route works fine)
SYM-5802	UX declares the SG down if one of the IP's resolved in an FQDN is down
SYM-8240	Remotely blocked R2 channels initialize to Idle state on startup.
SYM-8486	FXS interrupt latency improvement
SYM-8513	DS1 Alarm not reported if OOF signal received
SYM-8520	sym-sip process crashed under very low call load
SYM-8305	ISDN Calling Number with Allowed Presentation mapped to Anonymous SIP INVITE
SYM-8480	CAS R2 sends CPC request after Calling Party Number received.
SYM-7171	Need to raise an alarm on configuration validation at startup if it fails.
SYM-8496	The ASM IP address is changed when we use the REST partial import with default mask
SYM-8304	UX sends reINVITE with T.38 even when CNG tone detection is disabled
SYM-8510	Large count of audio hits and clipping observed during performance load
SYM-8501	Remove CAS R2 Group I Calling Party's Category "None" option
SYM-8297	HDLC counters displayed for DS1 CAS ports
SYM-8327	No way to remove primary IP address from NIC
SYM-8437	Calls from PSTN to Lync have one way audio (no audio from Lync / UM to PSTN) if the user is on the edge server or exchange answers
SYM-8379	UX1000: MSC Leak with 20 IP to IP calls
SYM-8484	Conference calls from Lync is not working
SYM-8386	P-Asserted Name with Privacy ID header passed to ISDN with Allowed Presentation
SYM-8364	SIP generating excessive alarm/trap traffic on DNS resolution failure
SYM-8355	Mondify Ethernet IP address from Tasks tab set configure default route to No will not return task completed page
SYM-7976	UX does not allow many countries cadence tones to be configured, the minimum freqency cannot be configured

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-8392	msc cored twice during 12 hours performance test
SYM-8306	P-Asserted identity, Privacy headers not sent to trusted SIP SG
SYM-8210	Incorrect outgoing Screening Indicator if Calling PN derived from SIP P-Asserted-Identity
SYM-8450	Ingress SG plays no Ringback if egress SG configured for R2 DTMF.
SYM-8469	Lync to PSTN calls not working
SYM-8378	Some Help links are pointing to the wrong doc pages even when the Help ID link is correct
SYM-8127	Q921 port stats RxREJ frame count show 0 even when is supposed to be > 0 when a user clicks on counters in webui
SYM-8183	The same channel can be assigned to multiple CAS SGs
SYM-8365	Alarm Manager memory leak
SYM-8246	No ringback tone heard when make call from FXS to PSTN over CAS E&M
SYM-8139	REST Error code 7 is reported when import an XML file from another node.
SYM-8361	CAS Channel state not updated after physical connection lost
SYM-8363	snmpd died over weekend test, need be restarted
SYM-8307	Add new entry in the SIP server with TCP / TLS should have connection re-use enabled
SYM-8170	UX fails to disconnect R2 call if metering with Pulsed Clear Back enabled
SYM-8394	CAS ERROR failureTone: no mscCall FXS calls
SYM-8382	No response to incoming SIP NOTIFY if request routed to CAS SG
SYM-8384	ISDN channel stuch in releasing state after the call is terminated
SYM-7036	Reset the root password to the hardware ID based password after a config restore
SYM-8308	ISDN SETUP with Restricted Presentation triggers SIP INVITE with incorrect P-Asserted-Identity header
SYM-8111	CDR: CDRs Logged WITH Mismatched Shared Secret between RADIUS Accounting Server and Client / UX
SYM-8185	Both calling and called parties kept hearing ringing tone after the call was answered when Lync to Lync call over CAS R2
SYM-8191	No ringback tone heard when simulring Lync and PSTN
SYM-7905	Egress calls made to R2 SG fail after SG disabled then enabled.
SYM-7926	ISDN to R2 calls fail occasionally, no ALERTING sent.

Copyright © 2015 Sonus Networks. All rights reserved.

UX 2.0.1 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to UX 2.0.1:

- Upgrading from UX 1.2.x or 1.3.x to 2.0.1
- Upgrading from UX 1.0.3

Upgrading from UX 1.2.x or 1.3.x to 2.0.1

The upgrade instructions for 2.0.1 are the same as those for 2.0. Please follow the instructions outlined in the UX 2.0 Upgrade Notes.

Upgrading from UX 1.0.3

If you are upgrading from UX 1.0.3 to UX 2.0.1, you **must upgrade to the latest 1.3.x release first** (1.3.2 recommended). To do this:

1. Follow the instructions in the UX 1.3 Upgrade Notes.
2. Once on 1.3.x, follow the UX 2.0.1 Upgrade Notes (outlined in the section above) to upgrade UX to 2.0.1.

UX 2.0.2 Release Notes

Apr 18 2012

Unified Exchange (UX) 2.0.2 is a maintenance release. In addition to hot fixes, UX release version 2.0.2 includes a major fix and two significant improvements:

- Significant performance improvement: Enhanced the UX1000 DSP modules, effectively **doubling the SIP to SIP / SBC calls** — **SYM-8908**.
- Major bug fix: Resolved a UX2000 Digital Signal Processing (DSP) crash when fax calls switch back to voice — **SYM-8423**.
- Capacity improvement: The 100 entry limit for Transformation Tables has been resolved — **SYM-9159**.
- Availability improvement: Frequent SNMP polling no longer impacts call processing — **SYM-9915**.

For more information about the UX1000 performance and call capacity, please see UX1000 DSP Capacities (details are only accessible to **logged in** UX partners and customers).

Don't have UX 2.0 yet?

Take a look at the new features and other highlights in the UX 2.0 Release Notes.

Ready to upgrade to 2.0.2?

Review the UX 2.0.2 Upgrade Notes
Download Latest Version

Updates and Fixes in this Release

Copyright © 2015 Sonus Networks. All rights reserved.

Bug ID	Headline
SYM-9915	UX stopped processing calls and was not accessible power restart required
SYM-10022	Port MSC change for ISDN channel move case from R2.1.0 to R2.0.2
SYM-9760	UX MIB for AD UP and other events does not include a 'none' for alarm severity
SYM-4455	UX does not accept alternate channel selection
SYM-9900	FXS to FXS call failed
SYM-9781	FXS Channel phone number starting with 0 has first digit truncated
SYM-9764	Lync config task: Change default Q.850->SIP mapping to translate ISUP cause codes that map to 503 Service Unavailable to 480 Temporarily Unavailable
SYM-9860	Backport fix for incorrectly configuring UX1000 with 4-port DS1 and missing ports on downgrades.
SYM-9877	ISDN call state not updated correctly on T313 expiry
SYM-9103	Downgrade Software Partition Issue - UX Becomes Unresponsive
SYM-6811	UX is not playing Inband messages when a PROGRESS indicator is provided on the ISDN DISCONNECT message
SYM-9582	UX does not release ISDN channel after received DISC w/PI=8 with configuration even Lync sends CANCEL
SYM-9138	Unable to Defragment and parse SIP messages
SYM-9757	DTMF payload type should not need to be the same to pass DTMF
SYM-9784	UX does not respond to SIP Options with UDP transport.
SYM-8904	Session progress SDP and 200 ok SDP o= session number and version do not match
SYM-6913	Calling name not being passed from PSTN to LYNC via facility message
SYM-9702	ISDN to FXS call sends channel IE in ISDN connect message with wrong value
SYM-9583	Message Translation to convert Alert with no IE to either Progress or Alert with IE not working in SIP to SIP
SYM-9495	Radius cored when running CDR automation
SYM-9535	TLS handshake with Level 3 failing with SSL error code 27 (certificate not trusted)
SYM-9503	When SG has Static NAT and Bind IP Interface is set, UX uses application IP and port 0 in From header, not NAT IP
SYM-9514	Backport data migration fix for RAD_RADIUS_CONFIG Authentication setting being wrong in the default configuration

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-9159	After adding 102nd Transformation table entry all previous entries disappear from table. Deleting last last entry added restores all previous entries.
SYM-8886	AD Backup Failed messages seen on UX1000 without External USB drive
SYM-9168	487 request terminated not being sent to originating SIP call leg
SYM-9118	Issue passing through codeset 6 shift
SYM-9337	fix legacyIE serialize
SYM-9444	SNMP dies and config change is required to make it restart
SYM-9177	SYM-ISDN/UX crash
SYM-8804	MWI. UX sends wrong IP address in NOTIFY message SIP URI.
SYM-9130	Host FQDN in SIP Server table cannot have a digit in last domain part
SYM-8899	UX does not apply new SIP profile value immediately to SIP-OPTIONS
SYM-9081	W15:Call transfer from a Lync Client to a PSTN phone fails
SYM-9016	200 OK for answered sent to the wrong IP
SYM-8981	Muliple entries in Remote authorization table bound by SIP server table 1st entry always used for Proxy authorization username
SYM-8939	UX1K drops fax call due to misformated T.38 re-invite
SYM-8956	Calls from Lync analog (Tenor) to UX -> Lync -> UX -> PSTN fails after upgrade from R1.3 to R2.0 if E164 numbering (+1 etc) is not used in the Lync deployment
SYM-8960	UX drops audio packets when media source IP and signaling IP do not match
SYM-9044	Tel: URI not working in From line for proper call routing
SYM-9056	ISDN Core dump after swinging ISDN PBX PRI on to the UX
SYM-9076	Issues with Importing Root CA from http://www.valicert.com/
SYM-9017	For a PSTN-PSTN call, UX is sending CANCEL to the wrong Lync server.
SYM-8887	Ringback not played when ROLM calls a analog (Tenor) registered end point on Lync
SYM-8927	PSTN leg dropped from Lync dial-in conference when UX-Lync mediation SRTP set "Not supported"
SYM-8902	INVITE with Auth has resolved IP address in host portion of Request-URI
SYM-8942	Enhanced SIP matching not able to remove ;ext label

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-8978	need to add online help for DS1 relay configuration
SYM-8970	UX is sending CANCEL to the wrong server in the Lync pool.
SYM-8969	Ux certificate must add the Common Name before the Alternative name in the SAN field.
SYM-8908	Double the number of IP to IP calls on the C3XX DSP's
SYM-8916	AD in "Updates" (cached) mode needs to support simple matching
SYM-8934	Installing certificates generates errors
SYM-8924	UX does not answer OPTION send from Mediation server
SYM-8936	T310 timer adjustments do not stick in the ISDN SG
SYM-8914	Erratic call failures in an ISDN Meridian deployment
SYM-8903	Online help page not found for the Contact Registrant table
SYM-8913	Early media from UAS is causing a CCC crash on UX.
SYM-8350	Calls to internal IP PABX calls faling UX does not respond to SIP UPDATE
SYM-8833	dsp command is missing.
SYM-8762	Call from PSTN SIP trunk to Lync has no audio in either direction.
SYM-8832	MWI Notify under NI-2 is sent with wrong call reference length
SYM-8883	Single SIP Channel Appears Stuck in Releasing - Reported in Channel Table
SYM-8889	UX gets decode error when incoming INVITE has Referred-by header with tel uri
SYM-8481	Upgrading from 1.3.2 to 2.0 and DNS stops working.
SYM-8749	no way and one way audio issues with phone > CS2k > UX > Exchange
SYM-7985	UX implementation with co-existing Exchange UM 2010 and 2007 servers
SYM-8744	SIP Cluster went down Major alarm left after all SG's have come up
SYM-8793	After upgrade to R2.0.1 build 118, UX fails inbound ISDN calls with cause code 47 and CAS errors
SYM-8678	There is no ringback tone heard when make call from ISDN to ISDN then re-route to SIP
SYM-8509	B channel problems
SYM-8754	CRC corruption and FXS failure on testing new UX1000 main boards.
SYM-8700	UX does not unhold call during SIP-ISDN interop transfer

Copyright © 2015 Sonus Networks. All rights reserved.

SYM-8761	Remove AGC from Media List
SYM-8758	UX not sending SIP URI in SIP cancel
SYM-8748	Javascript error when post login message is available
SYM-8688	ISDN Channel stuck in Releasing state after DISConnect glare
SYM-8431	sym-cas crashed while making R2 calls
SYM-8701	Analog Manufacturing Test does not report off-hook failure If run just for one cycle.

UX 2.0.2 Upgrade Notes

This document contain specific upgrade notes for customers planning to upgrade to UX 2.0.2:

- Upgrading from UX 1.2.x or 1.3.x to 2.0.2
- Upgrading from UX 1.0.3

Upgrading from UX 1.2.x or 1.3.x to 2.0.2

The upgrade instructions for 2.0.2 are the same as those for 2.0. Please follow the instructions outlined in the UX 2.0 Upgrade Notes.

Upgrading from UX 1.0.3

If you are upgrading from UX 1.0.3 to UX 2.0.2, you **must upgrade to the latest 1.3.x release first** (1.3.2 recommended). To do this:

1. Follow the instructions in the UX 1.3 Upgrade Notes.
2. Once on 1.3.x, follow the UX 2.0.2 Upgrade Notes (outlined in the section above) to upgrade UX to 2.0.2.

Upgrade Notes Overview

Each major Sonus SBC 1000/2000 release comes with specific recommendations for upgrading from the previous major version. We **strongly recommend** reading the upgrade notes for all major versions between your current version and the version to which you are upgrading.

Below is a list of upgrade notes for all previous major and minor releases of Sonus SBC 1000/2000, each of which has important information you should be aware of for your Sonus SBC 1000/2000 upgrade:

- SBC 1000-2000 4.0.1 Upgrade Notes
- SBC 1000-2000 4.0 Upgrade Notes
- SBC 1000-2000 3.2.2 Upgrade Notes
- SBC 1000-2000 3.2.1 Upgrade Notes
- SBC 1000-2000 3.2 Upgrade Notes
- SBC 1000-2000 3.1.3 Upgrade Notes
- SBC 1000-2000 3.1.2 Upgrade Notes
- SBC 1000-2000 3.1.1 Upgrade Notes
- SBC 1000-2000 3.1 Upgrade Notes

Copyright © 2015 Sonus Networks. All rights reserved.

- SBC 1000-2000 3.0.4 Upgrade Notes
- SBC 1000-2000 3.0.3 Upgrade Notes
- SBC 1000-2000 3.0.2 Upgrade Notes
- SBC 1000-2000 3.0.1 Upgrade Notes
- SBC 1000-2000 3.0 Upgrade Notes
- UX 2.2.1 Upgrade Notes
- UX 2.2 Upgrade Notes
- UX 2.1.3 Upgrade Notes
- UX 2.1.2 Upgrade Notes
- UX 2.1.1 Upgrade Notes
- UX 2.1 Upgrade Notes
- UX 2.0.2 Upgrade Notes
- UX 2.0.1 Upgrade Notes
- UX 2.0 Upgrade Notes

You will find the upgrade notes attached to the release notes for the relevant version.

Service Advisories

This page lists published service advisories for Sonus customers, partners, and Sonus SBC 1000/2000 system administrators:

- SBC 1000-2000 Service Advisory 2014-06-26
- SBC 1000-2000 Service Advisory 2013-12-18
- SBC 1000-2000 Service Advisory 2013-06-05
- UX Service Advisory 2012-10-12
- UX Service Advisory 2012-05-25
- UX Service Advisory 2012-04-26
- UX Service Advisory 2012-04-18
- UX Service Advisory 2012-02-08
- UX Service Advisory 2012-01-26
- UX Service Advisory 2012-01-04
- UX Service Advisory 2011-12-16
- UX Service Advisory 2011-09-12
- UX Service Advisory 2011-06-28
- UX Service Advisory 2011-06-23
- UX Service Advisory 2011-06-08
- UX Service Advisory 2011-05-26
- UX Service Advisory 2011-04-14

SBC 1000-2000 Service Advisory 2014-06-26

Announcing availability of SBC 1000/2000 system release 3.1.2 build 297

Purpose of the Service Advisory

1. An enhancement to the Remote Authorization Table has been introduced in software release 3.1.2 build 297.
2. An enhancement to the Monitor application that ensures interoperability with recent JRE 7 and JRE 8 security changes.

Applies to

This Service Advisory applies to all SBC 1000/2000 with or without built-in ASM modules that are running software release prior to 3.1.2 build 297.

Copyright © 2015 Sonus Networks. All rights reserved.

Details

1. After installing 3.1.2 build 296 or higher, some or all calls to a SIP Trunk no longer function due to authentication failure. The enhancement further restricts unknown and unauthorized users to place calls.
2. The Monitor application gives error `"Application Blocked by Security Settings"` or error `"Failed to validate certificate. The application will not be executed."` and the Monitor application fails to start.

Details

For more information, visit the following Solution Base articles:

1. Calls Fail to SIP Trunk After Installing SBC 1000-2000 version 3.1.2 build 296 or Higher
2. Monitor Application Fails to Load With Java Error

Upgrade verification

Once upgraded, verify the software version and build number match the following:

Software Version	3.1.2
Build Number	297

SBC 1000-2000 Service Advisory 2013-12-18

Session Manager enhancement introduced in version 3.x

Purpose of the Service Advisory

An enhancement to the Session Manager subsystem has been introduced in software release 3.x. The enhancement corrects a rare race condition within the SBC's internal communication that may cause the SBC to reboot.

Applies to

This Service Advisory applies to all SBC 1000/2000 with or without built-in ASM modules that are running software release prior to 3.x.

Details

A race condition was discovered in the internal communications within the SBC 1000/2000 in R2.2.1 or prior code. The race condition may cause the SBC to reboot as the SBC attempts to recover from the failure condition. The failure condition is exacerbated by heavy SBC processing load--a higher load increases the probability of experiencing the race condition.

While this condition is intermittent and does not affect the majority of installations, Sonus strongly recommends upgrading to R3.0.2.

To upgrade to system release 3.x

Copyright © 2015 Sonus Networks. All rights reserved.

Prerequisites

Prior to performing the upgrade to Software Release 3.0, you must complete the prerequisites listed in the Service Advisory from 2013-06-05 and in the SBC 1000-2000 3.0 Upgrade Notes.

Upgrade procedure

Upon completion of the prerequisites, proceed with the upgrade following the instructions in the SBC 1000-2000 3.0 Upgrade Notes.

After upgrading the SBC to version 3.0.0 build 241, proceed with upgrading to the latest maintenance 3.x release following the specific upgrade notes for that release.

SBC 1000-2000 3.0 Release Notes

SBC 1000-2000 3.0 Upgrade Notes

Upgrade verification

Once upgraded, verify the software version and build number match the following:

Software Version	3.0.0
Build Number	241

SBC 1000-2000 Service Advisory 2013-06-05

Announcing availability of SBC 1000/2000 system release 3.0.0 build 241

Purpose of the release

Applies to

- This Service Advisory applies to all SBC 1000/2000 with or without built-in ASM modules that are already running software release 2.2.x.

Details

Prior to performing the upgrade to Software Release 3.0, you must complete the prerequisites listed below and in the SBC 1000-2000 3.0 Upgrade Notes.

The following steps must be performed in the exact order listed below:

Copyright © 2015 Sonus Networks. All rights reserved.

Prerequisites

Before proceeding, check the current firmware version of the SBC.

- The firmware version must be R2.2.1 build 207 or higher. Otherwise, the Boot Image installation will fail.
- For more information, see SYM-13124

1. Install new Boot Image.
2. Install a new SIP license. For more details, see the SBC 1000-2000 3.0 Upgrade Notes.
3. If you are running a release prior to 2.2.x, upgrade to the latest release 2.2.x.
4. Export a configuration backup.
5. Install a new Base License.
6. Software Release 3.0.0 build 241 can now be installed.

SBC 1000-2000 3.0 Release Notes

SBC 1000-2000 3.0 Upgrade Notes

Upgrade verification

Once upgraded, verify the software version and build number match the following:

Software Version	3.0.0
Build Number	241

UX Service Advisory 2012-10-12

Announcing Availability of UX Software Release 2.2.0 Build 181

Purpose of the Service Advisory

UX Software Release **2.2.0 build 181** provides new features and enhancement. For a complete feature list, refer to the UX 2.2 Release Notes.

The purpose of this Service Advisory is to raise awareness of the need to update the ASM recovery partition and to review the Transformation table rules, if you are upgrading to UX Software Release 2.2.

Applicability

This Service Advisory applies to UX gateways with or without ASM modules.

For UX gateways with ASM modules deployed as a Lync SBA, upgrade of the ASM recovery partition is recommended.

If you have an SBA:

- It is important to update the ASM image in case the SBA should be re-initialized at any time in the future.
- If your UX was shipped with UX R2.1 or earlier, update the ASM image to the the R2.2.0 ASM image by following the UX 2.2 Upgrade Notes.
- The latest R2.2.0 ASM image available at the Sonus SBC 1000-2000 Download Center contains the Windows updates at the time of the R2.2.0 release date.

Copyright © 2015 Sonus Networks. All rights reserved.

- If your ASM has already been updated with the latest Windows updates, update the ASM image only.
- If your ASM has never been updated, go to ASM Roll-up Update and update the ASM. Then update the ASM image.

Recommended attention to a functional change in Transformation table:

⚠ Before upgrading to R2.2, you need to make sure that the Transformation table rules that perform number replacement adhere to the rules. Even though these rules may have worked in the past, they may fail now.

- Starting with UX R2.2 build 181, UX Transformation tables require regular expression grouping, or the output replacement will not function correctly. You need to have a regular expression grouping if you want to have a replacement. Consider the following examples:
  - **Up until UX R2.1**, in Transformation table rules that use regular expression (regex) to match input, regular expression grouping is required only if replacement is required. If you have a "default" Transformation table regex rule to match all numbers in the form of `.*` with output of `\1`, this would fail and the call router would ignore the input match and will preserve the original number. In reality, this accomplishes the desired effect. However, if the output is intended to replace the input number, for example to append a prefix of `5555#` (`5555#\1`), the rule would fail and the original number will be preserved.
  - **In UX R2.2**, grouping is always required. If you have any Transformation table rules that contains an input regex match that does not contain parenthesis and performs number replacement, you need to edit the rule and add the parenthesis around the string that is to be manipulated; for example, `(.*)`.

Details

1. Review the UX 2.2 Release Notes

2. Follow the UX 2.2 Upgrade Notes

3. Once upgraded, verify the software version and build number and ensure they match the following:
   - Software Version: **2.2.0**
   - Build Number: **181**

UX Service Advisory 2012-05-25

Announcing Availability of Sonus SBC 1000/2000 Software Release 2.1.1 Build 144

Purpose of the Release

UX software release 2.1.1 build 144 provides **features and enhancement**, as follows:

Unified Exchange (UX) 2.1.1 is a maintenance release. In addition to hot fixes, UX Version 2.1.1 includes two major improvements:
• Availability improvement: The system now correctly recovers from DSP crashes without rebooting — **SYM-9432** and **SYM-9946**.
• Major bug fix: Resolved crashes that were occurring under high load — **SYM-9964** and **SYM-10049**.

Applicability

This Service Advisory applies to UX gateways with or without ASM modules.

Copyright © 2015 Sonus Networks. All rights reserved.

Lync SBA update

For UX gateways with ASM modules deployed as a Lync SBA, upgrade of the UXSBA service is necessary. The current version is **2.1.1 build 144**.

Details

1. Review the UX 2.1.1 Release Notes

2. Follow the UX 2.1.1 Upgrade Notes

3. Once upgraded, verify the software version and build number and ensure they match the following:
   - Software Version: **2.1.1**
   - Build Number: **144**

UX Service Advisory 2012-04-26

Announcing Availability of UX Software Release 2.1.0 Build 137 and LX Software Release 1.0 build 33

Purpose of the Release

UX software release 2.1.0 build 137 provides features and enhancement, as follows:

- UX 1000 ISDN BRI Support
- UX 1000 FXO Support
- Music On Hold
- Lync E911 - PSAP Callback Support
- SIP Phone Survivability
- SIP Diversion Implementation
- Configurable Transport Timeout Timer
- DiffServe QoS Implementation
- Enable and Disable Transformation Table Entries.

LX software release 1.0.0 build 39 provides bug fixes, new enhancements and features.

New features include the capability to decode ISDN messages. You can download LX from UX Download site. To access the LX documentation, click here.

Applicability

This Service Advisory applies to UX gateways with or without ASM modules.

Lync SBA update

For UX gateways with ASM modules deployed as a Lync SBA, upgrade of the UXSBA service is necessary. The current version is **2.1.0 build 137**.

Did you know?

UX is the first platform to receive Microsoft Lync SBAv2 qualification. For more information, see: UX blog.

Details

Copyright © 2015 Sonus Networks. All rights reserved.

1. Review the UX 2.1 Release Notes

2. Follow the UX 2.1 Upgrade Notes

3. Once upgraded, verify the software version and build number and ensure they match the following:
    - Software Version: **2.1.0**
    - Build Number: **137**

UX Service Advisory 2012-04-18

Announcing availability of UX software release 2.0.2 build 139 and LX software release 1.0.0 build 27

Purpose of the release

UX software release **2.0.2 build 139** provides major fixes and improvements, significant performance and capacity improvements, resolved DSP crash, availability improvement based on SNMP memory leak fixes.

LX software release **1.0.0 build 27** provides bug fixes, new enhancements and features. You can download LX from UX Download site

Applies to

This Service Advisory applies to UX gateways with or without ASM modules.

> **Lync SBA update**
>
> For SUX gateways with ASM modules deployed as Lync SBA, upgrade of the UXSBA service is necessary. The current version is **2.0.2 build 139**.

Details

1. Review the UX 2.0.2 Release Notes

2. Follow the UX 2.0.2 Upgrade Notes

3. Once upgraded, verify the software version and build number and ensure they match the following:
    - Software Version: **2.0.2**
    - Build Number: **139**

UX Service Advisory 2012-02-08

> **Still Running UX Release 1.3.2?**
>
> Mandatory Upgrade of UX gateways to UX release software version 1.3.2 build 94 - **please read the UX Service Advisory 2012-01-26**.

Announcing availability of UX release software version 2.0.2 build 128

Purpose of the release

Copyright © 2015 Sonus Networks. All rights reserved.

NET recommends upgrading all UX gateways to software version 2.0.2.

Applies to

- This Service Advisory applies to UX gateways with or without built-in ASM modules that are already running software version 2.0.x.
- For gateways running software version 1.3.x, please read the UX Service Advisory 2012-01-26.

Details

1. Review the UX 2.0.2 Release Notes
2. Follow the UX 2.0.2 Upgrade Notes
3. Once upgraded, verify the software version and build numbermatch the following:

Software Version	2.0.2
Build Number	128

UX Service Advisory 2012-01-26

Announcing availability of UX Release version 1.3.2 build 94

Purpose of the release

UX release **version 1.3.2 build 94** contains some important stability fixes to the UX's digital signal processing, and provides end-users greater flexibility to configure the Line Echo Canceler to suit deployment needs. It is recommended that all UX gateways are upgraded to Sonus SBC 1000/2000 R1.3.2 build 94.

Applies to

This Service Advisory applies to UX gateways with or without built-in ASM modules.

Details

1. Review the UX 1.3.2 Release Notes
2. Follow the general UX upgrade guide
3. Once upgraded, verify the software version and build number match the following:

Software Version	1.3.2
Build Number	94

UX Service Advisory 2012-01-04

Copyright © 2015 Sonus Networks. All rights reserved.

Still Running UX Release 1.3.2?

Mandatory Upgrade of UX gateways to Sonus SBC 1000/2000 Release version R1.3.2 build 89 - **please read the UX Service Advisory 2011-12-16**.

Announcing availability of UX Release version R2.0.1 build 118

Purpose of the release

Unified Exchange (UX) 2.0.1 is a maintenance release. In addition to bug fixes, UX release version 2.0.1 fully supports CAS R2 Signaling and also widens the list of countries supported by the Tone Table

Applies to

This Service Advisory applies to UX gateways with or without built-in ASM modules.

Details

1. Review the UX 2.0.1 Release Notes
2. Follow the UX 2.0.1 Upgrade Notes
3. Once upgraded, verify the software version and build number match the following:

Software Version	2.0.1
Build Number	118

UX Service Advisory 2011-12-16

Announcing availability of UX Release version 1.3.2 build 89

Purpose of the release

UX **version 1.3.2 build 89** enhances the SIP audio quality under load. It is recommended that all UX gateways are upgraded to UX R1.3.2 build 89.

Applies to

This Service Advisory applies to UX gateways with or without built-in ASM modules.

Details

1. Review the UX 1.3.2 Release Notes
2. Follow the general UX upgrade guide
3. Once upgraded, verify the software version and build number match the following:

Software Version	1.3.2

Copyright © 2015 Sonus Networks. All rights reserved.

Build Number	89

UX Service Advisory 2011-09-12

Announcing availability of Sonus SBC 1000/2000 R1.3.0 build 69

Purpose of the release

UX release **1.3.0 build 69** provides major fixes and improvements, such as Lync E911 pass-through support, REST API (Web Services), No SIP License used when Calling NET Devices, Trusted Root Chain Display, SIP Outbound Proxy Support, Call Routing Features, Call Routing Transformation Table, Monitor Enhancement, SNMP Enhancements, SIP Session Timer, Server Certificate Upload Enhancement, ISDN Signaling Group ID Numbering Enhancement, SIP Signaling Group Federated IP Expansion Enhancement.

Applies to

This Service Advisory applies to UX gateways with or without ASM modules.

> **Lync SBA update**
>
> For UX gateways with ASM modules deployed as Lync SBA, upgrade of the UXSBA service is necessary. The current version is **1.3.0v69**.

Details

1. Review the UX 1.3 Release Notes
2. Follow the general UX upgrade guide
3. Once upgraded, verify the software version and build number and ensure they match the following:
   - Software Version: **1.3.0**
   - Build Number: **69**

UX Service Advisory 2011-06-28

Configuration Prerequisites prior to upgrading to UX R1.2.0

Reason

To ensure configuration prerequisites are met prior to upgrading to UX R1.2.0.

Applies to

This Service Advisory applies to all UX gateways that use Active Directory and/or have a E1/T1 interface card.

Details

Prior to upgrading to UX R1.2.0, ensure the following prerequisites are met:

- For UX gateways deployed with AD 2003, disable TLS in AD Configuration
- Ensure the Active Directory server has an A record as well as a record in the Reverse Lookup zone (PTR) in DNS
- Ensure DS1 Port 2 and Port 6 (8 port card only) are configured "Enabled" at all times (even if these ports are

Copyright © 2015 Sonus Networks. All rights reserved.

unused)

- Ensure the Active Directory logon name follows a pre-Windows 2000 AD login format

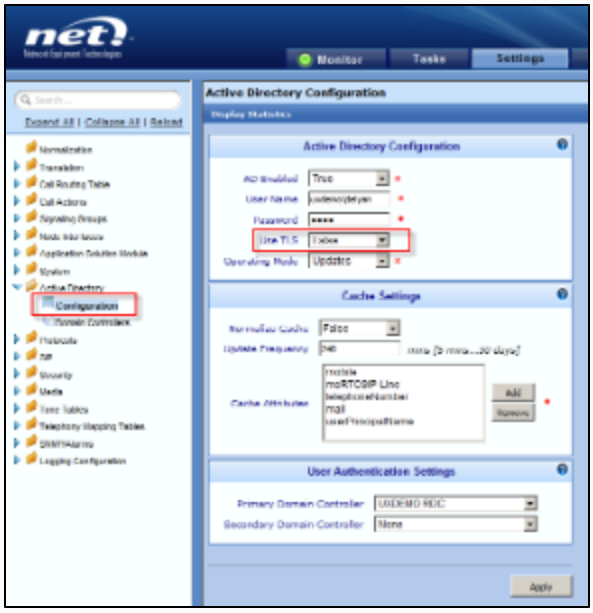
For UX gateways deployed with AD 2003, disable TLS in AD Configuration

Update on 07-22-2011

This issue as been resolved in UX 1.2.1 build 46. TLS can now be enabled with Active Directory 2003.

When UX is configured to work with Active Directory 2003, "Use TLS" in the Active Directory Configuration must be set to **False**.

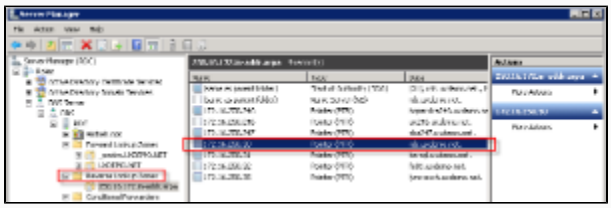
Windows Server 2008 R2 Active Directory Domain controllers fully support TLS with UX.



Ensure the Active Directory server has an A record as well as a record in the Reverse Lookup zone (PTR) in DNS

Copyright © 2015 Sonus Networks. All rights reserved.

In UX R1.2.0, UX no longer communicates with AD using clear text. Instead, SASL/Digest MD5 is used. SASL derives the servername portion of the SPN (server principal name) from DNS query for the PTR record of the IP address of the Active Directory server. If a PTR record is not available in DNS for the Active Directory server, then the AD bind using SASL will fail.



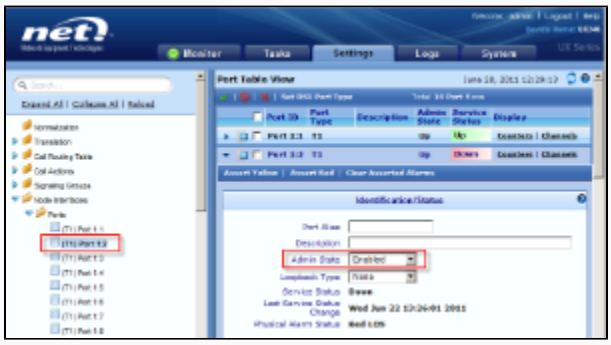
Ensure that the DNS server that contains the Active Directory A and PTR records is set under System -> Node-Level Settings -> Domain Name Service.

Warning:

If the AD user profile information has been changed at any time prior to the UX upgrade, the bind response from the Active Directory server will result in an error due to the MD5 hash string being stale for the user.
To resolve this issue, update the user password in the Active Directory server. This will force Active Directory to generate a new MD5 hash string used in SASL.

Ensure DS1 Port 2 and Port 6 (8 port card only) are configured "Enabled" at all times (even if these ports are unused)

Administratively disabling port 2 and port 6 may cause clocking errors on other ports. Even if unused, DS1 Ports 2 and 6 (8 port card only) on each interface card must be enabled as shown in the configuration screenshot below:

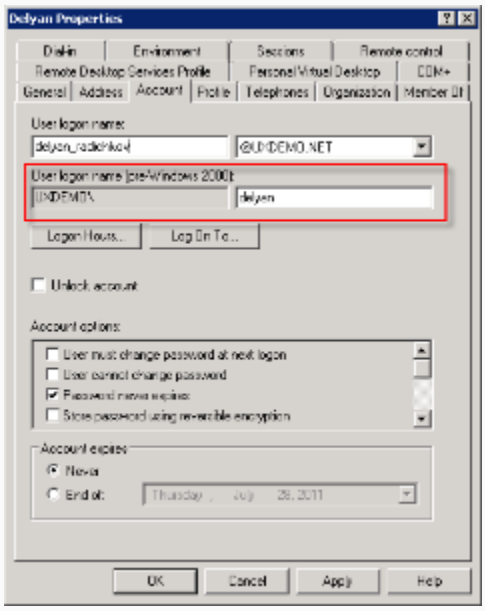


Ensure the Active Directory logon name follows a pre-Windows 2000 AD login format

Copyright © 2015 Sonus Networks. All rights reserved.

The pre-Windows 2000 logon name must be used in the AD config because Digest MD5 mechanism of SASL has a limitation where it can only use the pre-Windows 2000 (or the implicit User Principal Name) as logon names.

For example, following is a screenshot of a Windows 2008 R2 AD record showing the current as well as the pre-Windows 2000 user logon name:



In the context of the example screenshot above, the use of the following user logon names will produce the respective authentication results:

User Logon Name Format	Authentication Result
delyan_radichkov@uxdemo.net	Error
delyan@uxdemo.net	Success
uxdemo\delyan	Success

Warning:

If the AD user profile information has been changed at any time prior to the UX upgrade, the bind response from the Active Directory server will result in an error due to the MD5 hash string being stale for the user.
To resolve this issue, update the user password in the Active Directory server. This will force Active Directory to generate a new MD5 hash string used in SASL.

UX Service Advisory 2011-06-23

Announcing Availability of UX R1.2.0 build 39

Copyright © 2015 Sonus Networks. All rights reserved.

Purpose of the release

UX 1.2 is no longer supported in active documentation.

Applies to

This Service Advisory applies to UX gateways with or without ASM modules.

> **UX gateways with ASM modules deployed as Lync SBA**: an upgrade of the UXSBA service is strongly recommended. The current version of the UXSBA is **version 1.2.0 build 39**.
> Starting with UX version 1.2.0 build 39 onwards, each new UX build will have a corresponding UXSBA build labeled with the same build number.

Although an upgrade of the UXSBA service is not required, it is strongly recommended to always upgrade the UXSBA service (first) using the same version as the UX.

Details

1. Review the UX 1.2 Release Notes
2. Follow the general UX upgrade guide
3. Once upgraded, verify the software version and build numberand ensure they match the following:
    a. Base Software Version: **1.2.0**
    b. Software Build Number: **39**

UX Service Advisory 2011-06-08

Announcing availability of UX R1.0.3v241

Purpose of the release

UX release **1.0.3v241** provides major fixes and improvements, such as call forking stability, multiple DSP handling and memory / resource leaks. It is recommended that all UX's are upgraded.

Applies to

This Service Advisory applies to UX gateways with or without ASM modules.

> **Lync SBA update**
>
> For UX gateways with ASM modules deployed as Lync SBA, no upgrade of the UXSBA service is necessary. The current UXSBA version is **1.0.2v222**.

Details

1. Review the UX 1.0.3 Release Notes

2. Follow the general UX upgrade guide

3. Once upgraded, verify the software version and build number and ensure they match the following:
    - Software Version: **1.0.3**
    - Build Number: **241**

Copyright © 2015 Sonus Networks. All rights reserved.

UX Service Advisory 2011-05-26

Announcing availability of Lync 2010 Cumulative Update 2 (CU2) for the UX SBA

Reason

To allow customers and partners to update their SBA-equipped UX nodes as part of their upgrade to Lync 2010 Cumulative Update 2 (KB2493736).

Applies to

This Service Advisory applies only to UX gateways with ASM modules, loaded with the shipping Lync SBA components (4.0.7577).

Helpful Tip

You can see which, if any, Cumulative Updates you are running by Viewing the Installed Packages on the ASM - look at the following 4 packages.

- 3 "**Microsoft Lync Server 2010**" packages: **Mediation Server**, **Core Components**, **Front End Server**.
- 1 other package: **Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit**.

A version of 4.0.7577.0 indicates that no updates are installed. 4.0.7577.139 means that CU2 is already installed.

Prerequisite

Only SBA's that have been fully deployed can be updated to CU2. **Ensure that the SBA is configured and that all services are started before attempting to upgrade**.

Details

1. Download the `sba-lync-cu2.zip` file from here
2. Unzip the file to a temporary folder on your local computer - this will produce 4 update files:
   a. Mediation Server Update `MediationServer.msp`
   b. OCS Core Update `OCSCore.msp`
   c. Front End Server Update `Server.msp`
   d. UCMA Runtime Update `UcmaRuntime.msp`
3. Follow the instructions outlined in Installing Cumulative Updates for Lync SBA

The Service Versions (Mediation Service and Front-End Service) visible from the Operational Status will continue to report a version of 4.0.7577.0 after updating. This is normal.

UX Service Advisory 2011-04-14

Mandatory Upgrade of UX with Lync SBA

Reason

To provide NET customers and partners with an upgrade path to supported Lync SBA software

Applies to

Copyright © 2015 Sonus Networks. All rights reserved.

This Service Advisory applies only to UX gateways running ASM with Lync version prior to 4.0.7577.

> **Important Note**
>
> If the ASM is already running Lync version 4.0.7577, you do not need to update the ASM and you must skip step #5 below. The Lync version can be found listed under Installed ASM Packages.

> Note that after loading the ASM, the Branch side of the SBA configuration will be lost. You will have to complete the Lync SBA Branch Site Tasks again. We strongly recommend to unjoin the SBA from the Windows domain prior to loading the new ASM image.

Details

All UX units with SBA must be upgraded to the Generally Available Lync code and UX code.

> **Important Note**
>
> This upgrade procedure **must be performed in the following sequence** to ensure minimum downtime

1. Download the following from the UX Download Center:
   a. UX R1.0.2 `sw-release-1.0.2.tar.gz` from **1.0.2 > GA-v232**
   b. UX ASM Service `UX-ASM-UpdateService-1.0.2_v222.zip` from **ASM > UX-1.0.2-v222**
   c. UX RTM Lync SBA image `ASMimage.tar` from **ASM > UX-1.0.2-v222 > SBA**

2. Follow the general UX upgrade guide

3. Follow the instructions outlined in Updating the ASM Recovery Partition using `ASMimage.tar`

4. Follow the instructions outlined in Re-initializing the ASM – pay specific attention to the **Required Post Actions** listed on that page

Completing the upgrade steps in this order will ensure proper interoperability with Lync.

Copyright © 2015 Sonus Networks. All rights reserved.

Sonus SBC 1000-2000 Resources

The Product Information portion of the Unified Exchange documentation suite contains general information about the Sonus SBC 1000/2000 Series, including; Production Releases, Service Advisories, Terms and Conditions, Contact Information, Copyright and Trademark notices.

Sonus SBC 1000-2000 Download Center

SBC 1000-2000 Solution Base

Terms and Conditions

Copyright and Trademarks

Contacting Sonus

Sonus SBC 1000-2000 Interface Card Shipping Policy

Sonus SBC 1000-2000 Download Center

Registered Sonus customers and partners have the ability to download Sonus SBC 1000/2000 software updates directly from the Sonus download website for Upgrading Sonus SBC 1000-2000, Upgrading the SBC Communication Service Version, etc... In this page, we describe how registered members get access to those software downloads and provide a brief overview of the content available:

- Sonus SBC 1000/2000 Software Downloads Overview
  - ASM Images
  - ASM Roll-up Updates
  - Base Licenses
  - Log Exchange
  - Lync Updates
  - Sonus SBC 1000/2000 Software Updates
- How to Access the Sonus Global Support Portal

Sonus SBC 1000/2000 Software Downloads Overview

The Sonus SBC 1000/2000 download center provides registered customers and partners with the following downloadable software updates:

ASM Images

This section of the download center contains software images specifically for Sonus SBC 1000/2000 systems configured with a built-in Application Solution Module. These recovery images are typically used for re-initializing the ASM. For more details, see Updating the ASM Recovery Partition.

ASM Roll-up Updates

This section of the download center contains Update Packs for the ASM Roll-up system. For more information, see ASM Roll-up Update.

Base Licenses

Copyright © 2015 Sonus Networks. All rights reserved.

This section of the download center includes Base Licenses for the Sonus SBC 1000/2000. Base licenses activate features introduced in new major (and sometimes minor) versions of the Sonus SBC 1000/2000 software. To activate those features, you'll need to apply the base-license for the Sonus SBC 1000/2000 version you are upgrading to. For more details, see Working with Licenses.

Log Exchange

Software Download bundle LX1.0 contains the installers for Log Exchange (LX) - the SIP log analysis and Syslog Server utility for the Sonus SBC 1000/2000 and VX gateways. For more information see Log Exchange. For Release Notes and File Downloads, please visit the Global Services Toolbox.

Lync Updates

This section of the download center is specifically intended for Sonus SBC 1000/2000 systems with a built-in ASM module deployed as Lync SBA. It includes cumulative Lync server package updates that can be installed directly into the ASM via the Sonus SBC 1000/2000 web interface.

Sonus SBC 1000/2000 Software Updates

This section of the download center is broken down by Sonus SBC 1000/2000 release and includes the following content:

- **Sonus SBC 1000/2000 application firmware/software** update files (one for each Sonus SBC 1000/2000 Model) for Upgrading Sonus SBC 1000-2000.
- **Sonus SBC 1000/2000 Communication Service** update files for Upgrading the SBC Communication Service Version.
- **Schema** folder containing XSD files that can be used when building RESTful clients to communicate/control the Sonus SBC 1000/2000. For more details, see Sonus SBC 1000-2000 API User's Guide.
- **RADIUS** folder containing a Dictionary file to be used when Integrating with RADIUS. For more details, refer to the Vendor Specific Attributes Reference
- **MIBs** folder containing SNMP mib files to be used when Configuring Sonus SBC 1000-2000 for SNMP Management. For more details, refer to the SNMP MIBs Reference.
- **SCOM** folder containing the Microsoft System Center Operations Manger (SCOM) packs delivered as a management pack file. For more details, refer to Working with SCOM.

How to Access the Sonus Global Support Portal

> **Before you begin:**
> You will need a valid Salesforce Username and Password.

- Click here to access the Sonus Global Support Portal.

SBC 1000-2000 Solution Base

In addition to the documentation, registered customers and partners are granted access to the Sonus SBC 1000/2000 Solution Base. The solution base for Sonus SBC 1000/2000 includes problem/solution articles to various issues that may arise when deploying or operating Sonus SBC 1000/2000 gateways and Microsoft Lync 2010 Sonus SBC 1000/2000 SBA's.

How to Access the Sonus SBC 1000/2000 Solution Base

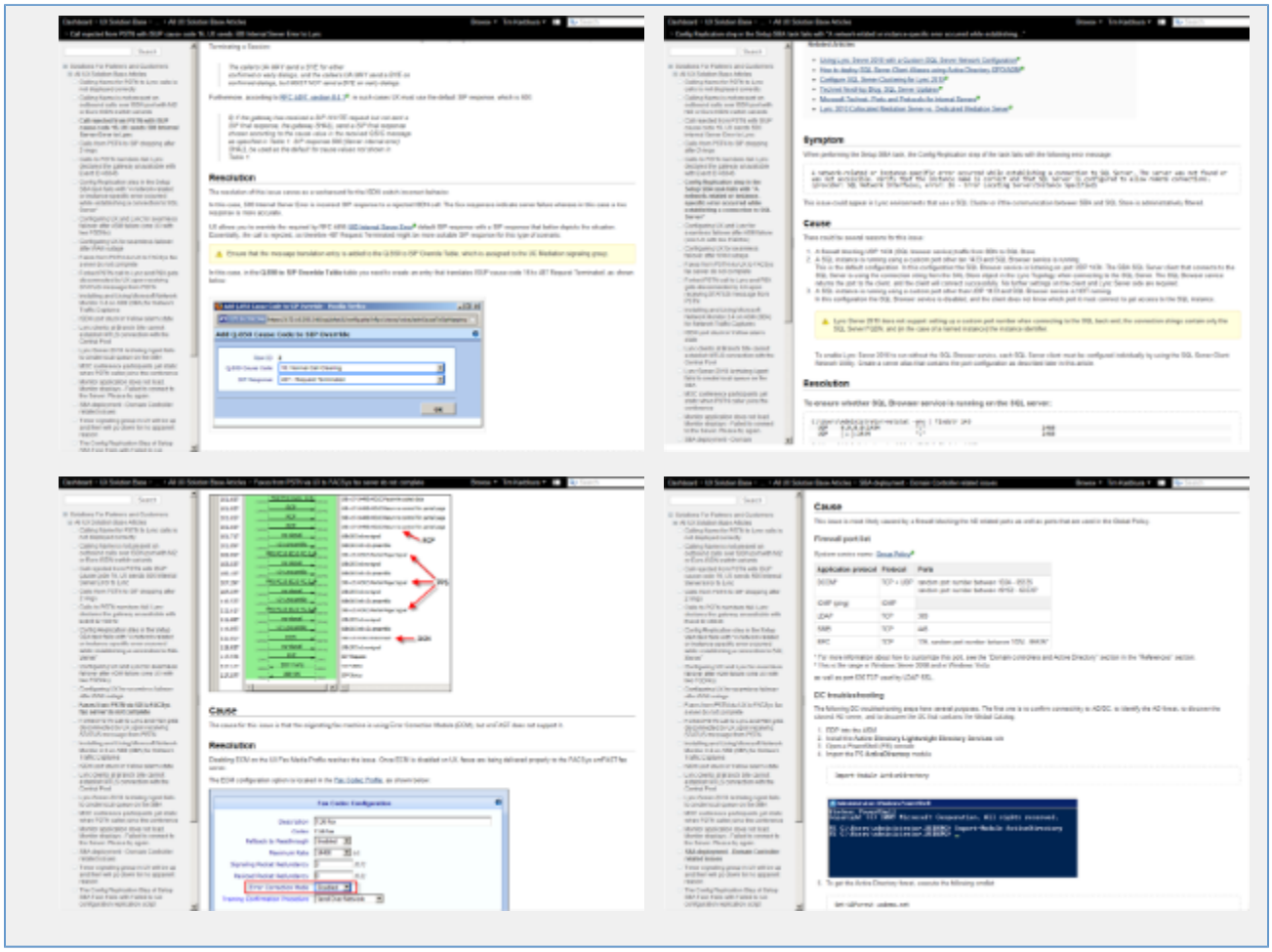
To access the Sonus SBC 1000/2000 Solution Base, you will need the following:

Copyright © 2015 Sonus Networks. All rights reserved.

- **A valid entitlement or software maintenance for Sonus SBC 1000/2000**.
- **A valid Sonus membership**. If you have not already registered, please do so by signing up.

Sonus SBC 1000/2000 Solution Base Samples

For a sneak peak of the Sonus SBC 1000/2000 Solution Base and what it has to offer, click the screenshots below:



Terms and Conditions

Use of this product is governed by the Sonus Networks, Inc. ("Sonus") Standard Terms and Conditions of Sale.

> Unless this product has been purchased pursuant to a separate agreement entered into by and between you and **Sonus** or an authorized **Sonus** reseller or distributor that includes authorized terms of use, by breaking the seal or opening the product packaging you hereby confirm that you have read, understand and agree to all terms relating to the use of this product located at: http://www.net.com/terms-of-sale

This product is covered by the NET Limited Warranty.

Copyright and Trademarks

This product contains components that are available under open source licenses or in the public domain. Sonus acknowledges the developers of the software programs listed below that Sonus has licensed pursuant to the referenced license agreement:

Copyright © 2015 Sonus Networks. All rights reserved.

- LibPCRE 7.8, license Copyright © 1997-2010 University of Cambridge, All rights reserved. Portions Copyright © 2007-2010, Google Inc., All rights reserved.
- LibXML2 2.7.3, license Copyright © 1998-2003 Daniel Veillard. All Rights Reserved.
- LightTPD 1.4.22, license Copyright © 2004, Jan Kneschke, incremental. All rights reserved.
- PHP 5.3.2, license Copyright © 1999 - 2010 The PHP Group. All rights reserved. This product includes PHP software, freely available from http://www.php.net/software
- OpenSSL 0.9.8g, 0.9.8k, license Copyright © 1998-2008 The OpenSSL Project. All rights reserved. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)
- Linux-PAM 0.99.6.3, license Copyright © 2006 Andrew G. Morgan <morgan@kernel.org>.
- PAM-LDAP 184, license Copyright © 2009 Luke Howard, PADL Software Pty. Ltd.
- OpenLDAP 2.4.21, license Copyright © 1999-2003 The OpenLDAP Foundation
- Net-SNMP 5.4.2.1, license Copyright various contributors, see license for details.
- U-Boot 1.1.6, license Copyright © 2000 - 2009 Wolfgang Denk, DENX Software Engineering, wd@denx.de.
- TIPC 1.7.6, license Copyright © 2003-2006, Ericsson AB. Copyright © 2005-2007, Wind River Systems. All rights reserved.
- BusyBox 1.4.2, license Copyright © 1999-2004 by Erik Andersen. All rights reserved.
- OpenWRT 8.09, license Copyright various contributors, see license for details.
- NTP, license Copyright © University of Delaware 1992-2010.
- tcpdump 3.9.4, license Copyright © 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 2000 The Regents of the University of California. All rights reserved.
- libpcap 0.9.4, license Copyright © 1993, 1994, 1995, 1996, 1997, 1998 The Regents of the University of California. All rights reserved.
- PCI Utilities 3.1.4, license Copyright © 1997--2009 Martin Mares <mj@ucw.cz>
- Dropbear 0.49, license Copyright various contributors, see license for details.
- DHTML Suite 1.9, license Copyright © 2006 Alf Magne Kalleland (post@dhtmlgoodies.com).
- SACK 1.6, license Copyright © 2005 Gregory Wild-Smith.
- XCache 1.3, license Copyright © 2005-2009, mOo, phpxcache@gmail.com, XCache. All rights reserved.
- TableLayout 2.0, license Copyright © 2001 Daniel Barbalace. All rights reserved.
- cassia 2.0.0.60, license Copyright © 2008 - 2009 Cassia Developers.
- php-csv-parser 1.0.1, license Copyright © 2008 Kazuyoshi Tlacaelel.
- cyrus-sasl 2.1.22, license Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved.
- freeradius-client-snapshot-20071022 srp-1, license Copyright © 2000 - 2009 Wolfgang Denk, DENX Software Engineering, wd@denx.de.
- pam-radius, license Copyright © 2000 - 2009 Wolfgang Denk, DENX Software Engineering, wd@denx.de.
- jQuery, license Copyright © 2010 The jQuery Project.
- jQuery UI, license Copyright © 2010 The jQuery Project.
- Norio Kobota, license Copyright (c) 2010, Norio Kobota All rights reserved.

The licensing terms of some of the open source products listed above require that Sonus make the binaries and/or source code of the specific version of the open source product used in the Sonus product available to the public. These libraries are available from their developers at the web sites listed above, however Sonuswill also provide them on request. To request a copy of the binaries and source code of any one of the open source products listed above, please contact Sonus Support.

The use of open source products may change between release versions. The list above applies to the current, released version of **Sonus SBC 1000/2000 4.1.x** series.

Disclaimer

This document presents information for users of the products of Sonus Networks, Inc. (“Sonus”), its affiliates and its subsidiaries (collectively, the “Sonus Group”). Network Equipment Technologies, Inc. is part of the Sonus Group.

Copyright © 2015 Sonus Networks. All rights reserved.

The Sonus Group does not assume any liability arising out of the application or use of any product or circuit described herein. No part of this document may be copied or reproduced in any form or by any means without the prior written permission of Sonus. For the most current user documentation, please contact your Sonus customer support representative.

Copyright

Copyright © 1999 - 2015 Sonus Networks, Inc. All rights reserved. Printed in the U.S.A. This item and the information contained herein are the property of the Sonus Group. This publication may be used, copied, or distributed only in accordance with the terms of the license agreement. Any other use, reproduction, or distribution may occur only upon Sonus' prior written consent.

Third-Party Copyrights

Open BSD Copyright (c) 1982, 1986, 1990, 1991, 1993. The Regents of the University of California. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE

FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT

LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the above disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Disclaimer and Restrictions

The material in this publication is for information only and is subject to change without notice. This material does not constitute a commitment

on the part of the Sonus Group. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, the Sonus Group assumes no liability resulting from technical or editorial errors or omissions, or for any damages whatsoever resulting from the furnishing, performance, or use of the information contained herein. The Sonus Group reserves the right to revise this publication, and to make changes on the content hereof without notice.

The information in this document may be used by customers solely for the use and understanding of the Sonus Group's products and solutions. This document is not meant to define an interface between products of the Sonus Group and any third party hardware or software. The Sonus Group reserves the right to change the design and implementation used for any of the tables, screens, field names, etc. to enhance its products as it sees fit.

Warranties

The material in this publication is for information only and is subject to change without notice. This material does not constitute a commitment

THIS INFORMATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING,BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. REFERENCES TO CORPORATIONS, THEIR SERVICES AND PRODUCTS, ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL THE SONUS GROUP BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS INFORMATION.

Descriptions of, or references to, products, services or publications within the Sonus Group's documentation do not imply endorsement of that product, service or publication. Sonus Networks makes no warranty of any kind with respect to the subject matter included herein, the products listed herein, or the completeness or accuracy of the information. Sonus Networks specifically disclaims all warranties, express, implied or otherwise, including without limitation, all warranties of merchantability and fitness for a particular purpose.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES MAY BE PERIODICALLY MADE TO THE INFORMATION HEREIN.

Trademarks

Sonus Networks, the Sonus Networks logo, Open Services Architecture, Insignus, SMARRT, Sonus Networks Insight, IMX, GSX9000, GSX4000, GSX4010, SBC 5100TM, SBC 5200TM, IMX, SBC9000, the Atreus logo, the Performance Technology, Inc. logo, Insight xAuthority, Monterey 8000, NexusWare, SEGway and SIP Xpress are either registered trademarks or trademarks of Sonus Networks, Inc. Open Services Partner Alliance and Sonus Networks CARE are service marks of Sonus Networks, Inc. The Sonus Group trademarks may not be used in connection with any product or service that is not the Sonus Group's in any manner that is likely to cause confusion among customers or in any manner that disparages or discredits the Sonus Group. All other product names mentioned herein are trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

Third-Party Trademarks

Apache is the http server, and Tomcat is the Servlet/JSP container developed by the Apache Software Foundation. — Rapid Service Introduction (RSI) System is a trademark of BayPackets, Inc. — Borland is a registered trademark, and AppServer is a trademark of Borland Software Corporation. — Dot Hill and SANnet are trademarks of Dot Hill Systems Corp. — Eclipse is a trademark of Eclipse Foundation, Inc. GoAhead and SelfReliant are registered trademarks of GoAhead Software, Inc. — IBM, Netcool, Rational, ClearCase, and WebSphere are registered trademarks of International Business Machines Corporation in the United States, other countries, or both. — Intel, Xeon, and Pentium are registered trademarks of Intel Corporation in the United States and/or other countries. — Iomega is a registered trademark of the Iomega Corporation, a wholly owned subsidiary of the EMC Corporation. — Macromedia is a registered trademark, and JRun is a trademark of Macromedia, Inc. in the U.S. and/or other countries. — DataDirect is a registered trademark of Progress Software Corporation. — Linux is a registered trademark of Linus Torvalds in the United States and/or other countries. — Microsoft, Microsoft Internet Explorer logo, Windows, Windows NT, Windows XP, and/or other Microsoft products referenced herein are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. — MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. — Netscape is a registered

Copyright © 2015 Sonus Networks. All rights reserved.

trademark of Netscape Communications Corporation in the U.S. and other countries. — Nokia is a registered trademark of Nokia Corporation. — Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. — Palm OS and Palm Powered are registered trademarks, and Palm is a trademark owned by or licensed to Palm, Inc. — Red Hat, RPM, JBoss, and all Red Hat-based trademarks are trademarks or registered trademarks of Red Hat, Inc. in the United States and/or other countries. — Sage Instruments is a copyright of Sage Instruments, Inc. — Service Availability and the Service Availability logo are trademarks used with the permission of their owner. — SnowShore, SnowShore Networks, and N20 are trademarks of Cantata Technology Inc. — SSH is an IETF protocol and OpenSSH is a derivative of the original and free ssh 1.2.12 release by Tatu Ylonen. SSH Secure Shell is a trademark of SSH Communications Security Corp. — Sun, Sun Microsystems, Java, JumpStart, Netra, Solaris, Solstice DiskSuite, and all trademarks that contain Sun, Solaris, or Java are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the United States and other countries. — iPlanet is a division of Sun Microsystems, Inc. — All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. — Telcordia is a registered trademark and LERG is a trademark of Telcordia Technologies, Inc. in the United States, other countries, or both. — Signalware is a registered trademark of Ulticom, Inc. — UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd. — VeriSign is a registered trademark, and Thawte Consulting is a wholly owned subsidiary of VeriSign, Inc. — Veritas is a trademark of Symantec Corporation or its affiliates in the U.S. and other countries. — WebLogic is a registered trademark of BEA Systems, Inc.

All other product names mentioned herein are trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the user’s own expense.

Compliance with Applicable Laws and Export Control Laws

Use of the information in this publication is governed by all applicable federal, state, and local laws. All information available in this publication is subject to U.S. export control laws and may also be subject to the laws of the country where you reside. Sonus Networks makes no representation that the content on this site is appropriate or available for use in other locations, and access to it from territories where the content is illegal and prohibited.

All Sonus Networks, Inc. products and publications are commercial in nature. Use, duplication, or disclosure by the United States Government is subject to the restrictions set forth in DFARS 252.227-7013 and FAR 52.227-19.

Embedded Software

Oracle Enterprise Edition is an embedded part of the Sonus Group product line. The programs included herein are subject to a restricted use license and can only be used in conjunction with this application. You are not allowed to navigate or modify the underlying database schema unless explicitly authorized in writing by Sonus.

Export Laws

Sonus Group product documentation includes technical information developed in the United States that may be subject to limitations on export imposed by the U.S. Department of State and the U.S. Department of Commerce.

Copyright © 2015 Sonus Networks. All rights reserved.

All use, distribution, and transfer of any technical information shall be in compliance with U.S. export laws and regulations.

Contacting Sonus

For information about sales and service contact Sonus Networks, Inc.

Sonus SBC 1000-2000 Interface Card Shipping Policy

With the introduction of Release 3.2 of the SBC 1000/2000, Sonus now ships the following field installable/field replaceable hardware options in cartons separate from the SBC 2000 systems they are ordered with:

- **SBC-2K-CRD-T1E1:** SBC2000 T1/E1 Module w/1 T1/E1, Licensable growth to 8 T1/E1
- **SBC-2K-CRD-24FXS:** Telco Module, 24 FXS Ports
- **SBC-2K-PSU-AC:** SBC2000 AC Power Supply

Installing any or all of these components can be completed in a matter of minutes using the SBC2000 installation instructions on the Sonus support site. These components slide and lock into place in clearly marked locations and no special training or tools are required. The system software automatically recognizes the card and provided tools to configure it.

> The T1/E1 and FXS cards are **not** hot-swappable. Therefore, the system **must powered down** before installing theses options.

Copyright © 2015 Sonus Networks. All rights reserved.