Installation and Maintenance Manual

AudioCodes One Voice™ for Microsoft Skype for Business

Mediant™ 1000B
Survivable Branch Appliance (SBA)
For Skype for Business

Version 7.2

Skype for Business

Microsoft Partner
Gold Communications

audiocodes

Contents

1 Introduction 9

1.1 Overview 9
1.2 Main Benefits 10
1.3 Specifications 10
1.4 Available Mediant 1000B SBA Models 11

Hardware Description 13

2 Verifying Package Contents 15

3 Physical Description 17

3.1 Front-Panel Description 17
3.2 Rear-Panel Description 18

Preparing SBA at Datacenter 19

4 Introduction 21

5 Adding SBA to Active Directory 23

6 Defining Branch Site Topology 27

Preparing SBA at Branch Site 37

7 Introduction 39

8 Modifying Default IP Address 41

8.1 Modifying IP Address of SBA Server 42
8.2 Modifying IP Address of SBC/Gateway 47
8.3 Re-Cabling SBA and SBC/Gateway to Network 48

9 Resumption of SBA Wizard after Initial Network Configuration 49

9.1 Step 1: Access the SBA Setup Wizard 49
9.2 Step 2: Configure SBC and Gateway LAN and WAN 50
9.2.1 Step 2-1: Configure E-SBC and Gateway LAN Connection 50
9.2.2 Step 2-2: Configure E-SBC and Gateway WAN Connection 52
9.3 Step 3: Change Local Administrator Password 53
9.4 Step 4: Set Date and Time Zone 54
9.5 Step 5: Join to the Domain 54
9.6 Step 6: Login to Domain 56
9.7 Step 7: Configure SBA Certificates 58
9.7.1 Generating a Certificate Signing Request (CSR) 58
9.7.1.1 Pending Requests 63
9.7.2 Importing an Existing Certificate 64
9.7.3 Assigning a Certificate 66
9.8 Step 8: Configure SBC/Gateway SBA Leg 69
9.9 Step 9: Configure SIP Trunk/IP-PBX Leg 71
9.10 Step 10: Configure Number Manipulation 73

9.11 Step 11: Run Cumulative Updates 74
9.12 Step 12: Start Services 75
9.13 Step 13: Complete Wizard 76
9.14 Step 14: Apply INI File to Device 78
9.15 Step 15: Post Wizard Actions 79

10 Using the SBA Management Interface 81

10.1 Viewing General SBA Details 82
10.2 SBA Configuration 84
10.2.1 Viewing and Configuring Network Interfaces 84
10.2.2 Viewing Installed SBA Components 86
10.2.3 Changing the Login Password 87
10.2.4 Configuring Date and Time 88
10.2.5 Configuring SNMP 89
10.2.6 Configuring Certificates 91
10.2.7 SBC/Gateway Certificate 91
10.2.8 Access List 94
10.3 Gateway-Related Operations 96
10.3.1 Viewing Gateway Information 96
10.3.1.1 Viewing Gateway Details 96
10.3.1.2 Viewing Gateway Alarms 97
10.3.2 Accessing Gateway's Web Interface 97
10.4 Performance Monitoring 98
10.4.1 Viewing Call Statistics 98
10.4.2 Viewing Registered Users Statistics 99
10.4.3 Viewing General SBA Server Statistics 100
10.5 Maintenance 102
10.5.1 Upgrading SBA Software and Cumulative Updates 102
10.5.2 Stopping and Starting SBA Services 103
10.5.3 Restarting SBA Server 103
10.5.4 Configuring Syslog 104
10.5.5 Viewing Logged SBA Management Interface Activities 105
10.5.6 Viewing Logged SBA Configuration Activities 106
10.6 Logging out of SBA Management Interface 107
10.7 Troubleshooting 108
10.7.1 Login Failure due to Connection Failure with SBA Service 108
10.7.2 SBA Topology not Created 108

Configuring Gateway/SBC Manually and Post-Wizard Tuning 109

11 Introduction 111

12 Configuring the Connection with the Mediation Server 113

12.1 Step 1: Configure Gateway Name 113
12.2 Step 2: Configure Routing Mode 113
12.3 Step 3: Proxy Sets 114
12.4 Step 4: Reasons for Alternative Routing 115
12.5 Step 5: Media Realms 117
12.6 Step 6: SIP Interfaces (SBC Only) 119
12.7 Step 7: IP Groups 121
12.7.1 SBC 121
12.8 Step 8: Routing 122

12.8.1 IP-to-Tel Routing....122
12.8.2 IP-to-IP Routing....124
12.9 Step 9: SIP TLS Connection....127
12.9.1 Step 9-1: Enable SIP TLS Listening Port....127
12.9.2 Step 9-2: Configure the NTP Server Address....127
12.9.3 Step 9-3: Configure the DNS Server....128
12.9.4 Step 9-4: Configure Gateway or E-SBC Certificate....130
13 Configure IP Profile....133
13.1 Configuring Early Media (Global Settings)....135
13.1.1 PSTN Gateway....135
13.1.2 Forking Handling-SBC....138
14 Configuring Voice Coders (with Silence Suppression)....139
15 Configuring Comfort Noise and Gain Control....141
16 Configuring FXS Ports and PSTN Trunks (Gateway Only)....143
16.1 Step 1: Enabling FXS Ports and PSTN Trunks....143
16.2 Step 2: Configuring the Channel Select Method....144
16.3 Step 3: Configuring the Trunk....146
16.4 Step 4: Configuring the TDM Bus....148
16.5 Step 5: Configuring FXS Port Transfer Behavior....149
17 Configuring Number Manipulation Rules....151
17.1 Configuring Gateway Number Manipulation....151
17.2 Configuring SBC Manipulation....152

Maintenance....155

18 Upgrading SBA to Skype for Business....157
18.1 SBA Upgrade Kits....157
18.2 Upgrading HDMX Module from HDD to SSD....158
18.3 Installing the SBA Skype for Business Image....160
18.4 Configuring the SBA....166
19 Installing Microsoft Cumulative Updates....167
20 Upgrading the OSN Module....169
21 SBA Skype for Business Recovery....171
22 Connection Methods to SBA Server....173
22.1 Direct Connection through HDMI....173
22.2 Serial Connection....176
22.3 Connecting through HTTP/S....178
22.4 Connecting to SBA through Remote Desktop....180
23 Resetting the SBA Server....181
23.1 Resetting SBA using OSN Module Handle....181
23.2 Resetting SBA through Windows....181
23.3 Resetting SBA through SBA Management Interface....182
23.4 Resetting SBA through CLI....182

24 Upgrading the BIOS on SBA Server 183
24.1 Verifying the Current BIOS Version 183
24.1.1 Viewing BIOS Version through Serial Connection 183
24.1.2 Viewing BIOS Version through Desktop Connection 183
24.2 Upgrading BIOS 184
24.2.1 Obtain the BIOS Image File 184
24.2.2 Create a Bootable BIOS File from a USB Dongle 184
24.2.3 Upgrade the BIOS on the OSN 186
25 Monitoring through SNMP 187
25.1 SNMP Trap Alarms 187
25.1.1 SBA Services Status Alarm 187
25.1.2 SBA Disk Space Alarm 188
25.1.3 SBA CPU Status Alarm 188
25.1.4 SBA Memory Status Alarm 189
25.1.5 SBA Certificate Expired Alarm 190
25.1.6 SBA Performance Counter Alarm 190
25.2 SNMP Performance Monitoring MIBs 191

Appendix 193

26 Running Anti-Virus Software 195
27 Configuring RAID 197
27.1 Prerequisites 197
27.2 Configuring RAID 1 198
28 Configuring NIC Teaming 203
28.1 Prerequisites 203
28.2 Creating a Team for the Network Adapters 203
28.3 Post Installation 207

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: April-03-2019

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Throughout this manual and unless otherwise specified, the term *device* refers to the Mediant 1000B SBA.

Notes and Warnings

Warning: The device is an INDOOR unit and thus, must be installed ONLY indoors. In addition, Ethernet port interface cabling must be routed only indoors and must not exit the building.

Avertissement: L'appareil est une unité d'INTERIEUR et doit donc obligatoirement être installé en intérieur. En outre, le câblage de l'interface du port Ethernet doit être acheminé uniquement en intérieur et ne doit pas sortir du bâtiment.

Warning: Installation of this device must be in a weather protected location of maximum ambient temperature of 40°C.

Avertissement: L'installation de cet appareil doit avoir lieu dans un local protégé des intempéries de température ambiante maximale de 40°C.

Warning: This device must be installed only in a restricted access location.

Avertissement: L'entretien de maintenance de cet appareil doit être effectué uniquement par un personnel de service qualifié dans des locaux à accès limité et l'appareil étant branché à une prise mise à la masse.

Warning: Service of the device must be made only by qualified service personnel.

Warning: The device must be connected only to a grounded AC mains power socket.

Document Revision Record

LTRT	Description
40112	RAID procedure updated; BIOS upgrade procedure updated; SBA upgrade procedure updated; Using the SBA Management interface updated; Adding SBA to AD updated; Defining Branch Site Topology updated; Connecting to SBA Management interface updated.
40113	Physical description added; SBA Wizard pages updated; supported browsers updated; URL to BIOS image download updated; section 'Upgrade the BIOS on the OSN' updated; compatible BIOS version specified; section 'Installing the SBA Skype for Business Image' updated.
40114	Updated for Ver. 7.2.24.
40115	Initial cabling and procedure for changing default IP address was updated.
40116	Note updated re BIOS ver. and note for CU update.
40117	Note for 3rd-party software; activation of Windows license on OSN3 module when Installing the SBA Skype for Business Image; new section - Configuring NIC Teaming OSN Server
40118	Microsoft CU URL link; section Upgrade the BIOS on the OSN was updated; typos.
40160	New corporate logos, URLs and screenshots updated; NIC Teaming added; New sections (SBC/Gateway Certificate; Access List); configuring HTTPS for SBA Web interface added
40161	OSN module updates; screenshots and text for changing default IP.
40162	Supplied HDMI cable type for monitor update; SNMP alarms added (acSBACpuStatusAlarm, acSbaPerfCounterAlarm, acSbaCertificateExpiredAlarm, and acSBAMemorytatusAlarm)

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

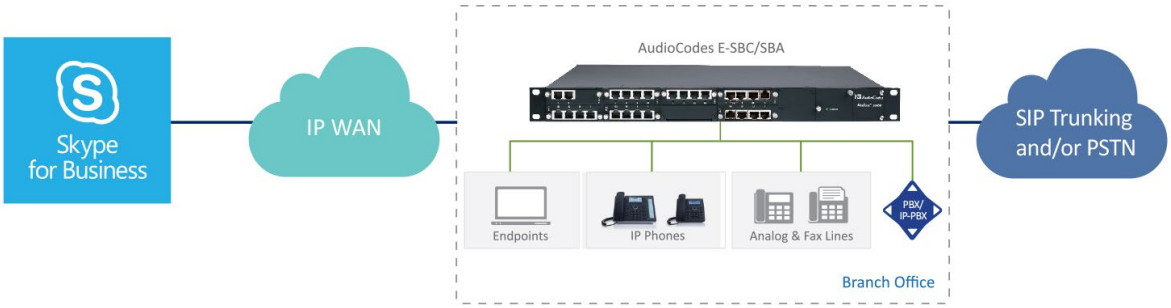
1 Introduction

This document provides step-by-step instructions on installing and configuring the Survivable Branch Appliance (SBA) application running on AudioCodes Mediant 1000B SBA.

1.1 Overview

Mediant 1000B SBA (referred to as the *device* in this document) is an essential element for multi-site deployments of Skype for Business and is fully **certified by Microsoft**. The device provides branch office voice resiliency, by ensuring continued access to Skype for Business services including voice and data communications, during Wide Area Network (WAN) failure scenarios where loss of connectivity occurs with the datacenter (typically at the Enterprise's headquarters). During survivability, the device maintains local call connectivity among Microsoft users located at the branch site (Skype for Business clients and devices such as IP phones). It can also provide call connectivity between the branch-site users and the PSTN (E1/T1 Trunk) during a WAN failure, if PSTN interfaces are ordered with the device.

Figure 1-1: Mediant 1000B SBA at Branch Office in Skype for Business Environment



The device has a 1U-modular chassis, providing Microsoft Skype for Business Server capabilities as well as optional, PSTN Gateway and Session Border Controller (SBC) capabilities. It also provides optional, direct connectivity to Analog Devices through customer-ordered Foreign eXchange Station (FXS) port interfaces.

The device provides an embedded, Web-based management tool called *SBA Management Interface*, for installing and configuring the SBA functionality. The tool also provides a setup wizard, which allows quick-and-easy initial SBA installation.

The SBA application is installed on a generic cPCI single-board computer module housed in the device chassis. The module name is Open Solution Network (OSN) and enables hosting of multiple third-party applications. The SBA application runs on Windows Server 2012 R2 operating system.

Important: Installation of any third-party software, except that which is included in the Mediant 1000B SBA package purchased from AudioCodes, on the device's OSN server must first be approved by AudioCodes.

The OSN module provides three network interface cards (NIC):

- Two "external" NICs (RJ-45 connectors) on the OSN module's front panel. Ethernet port #1 is enabled by default (192.168.0.20) and Ethernet port #2 is disabled. The external NIC is used to connect to the SBA application from your network. This connection also allows you to connect to the SBC/Gateway application's Web interface (through the internal NIC, as explained in the next bullet) for SBC/Gateway configuration.

- One "internal" NIC that connects to the internal chassis switch. This NIC is enabled and DHCP-client enabled. It allows communication between the SBA application and the SBC/Gateway application:
  - The Web interface of the SBC/Gateway can be accessed from the SBA Management Interface.
  - The SBA Management Interface can obtain and display status information from the SBC/Gateway.

Note: The SBA Skype for Business image also includes AudioCodes Auto-Attendant Interactive Voice Response (IVR) and Fax Server applications, offering a 90-day trial license period for each application. For more information go to https://www.audiocodes.com/solutions-products/products/products-for-microsoft-365/voice-applications.

1.2 Main Benefits

The device offers the following main benefits:

- Secured SIP trunk connectivity with an embedded qualified E-SBC
- Hosting communications-enabled business processes (CEBP) applications such as call recording, Auto-Attendant, Fax Server, third- party SIP phone Skype for Business integration
- PSTN connectivity in parallel and as fallback to SIP Trunk connectivity
- Full modularity and interface flexibility, including digital spans, analog ports and BRI interfaces
- Skype for Business migration support for branch offices with advanced call routing capabilities such as call forking and Active Directory look-up
- Support for emergency calling standards, including E911 and Emergency Location Identification Number (ELIN)

1.3 Specifications

Table 1-1: Mediant 1000B SBA Specifications

Item	Description
Maximum Skype for Business Users (SBA)	1000
Maximum PSTN Capacity (Channels)	192
Maximum Number of SBC Sessions	150
Ability to Host Additional Business Applications (SBA v2)	Yes
Modularity	Modular
Digital Interfaces	▪ 1, 2, 4, 6, 8 T1/J1 spans ▪ 1, 2, 4, 6 E1 spans ▪ Optional 1+1 or 2+2 fallback spans
Analog FXO and FXS Interfaces	▪ 4, 8, 12, 16, 20, 24 FXS/FXO ports ▪ 4 ports per module ▪ One lifeline port per FXS module
BRI Interfaces	▪ 4, 8, 12, 16, 20 BRI lines ▪ 4 BRI lines (8 calls) per module S/T interfaces

Item	Description
LAN	Up to 6 x 10/100 Base-TX Ethernet LAN ports configured in 1+1 redundancy or as individual ports
IPv6 Support	Yes
Physical Dimensions	1RU
Power Supply	Single/Dual AC power supply
Storage options	SSD RAID 1
Special Features for Microsoft Skype for Business	Call Forking, Active Directory look-up, Emergency Location Identification Number (ELIN)

1.4 Available Mediant 1000B SBA Models

The following table lists the orderable Mediant 1000B SBA models for Skype for Business.

Table 1-2: Mediant 1000B SBA Models

Model	Description
Mediant 1000B SBA-ES	Mediant 1000B SBA chassis installed with the following modules: ▪ **OSN3C Module:** ✓ 8-GB RAM ✓ USB 2.0 port for connecting peripheral devices such as SBA Dongle, USB hub (to which keyboard and mouse can be connected) ✓ Gigabit Ethernet interface (RJ-45) for connection to the network ✓ Console (serial) port (micro-USB) for serial communication ✓ HDMI interface (19-pin Type D, micro-HDMI port) for connection to graphic display monitor ▪ **HDMX Module:** Solid-state drive (SSD) **Note:** The OSN3C module has replaced the OSN3B module, which reached End-of-Sale status and is no longer being sold by AudioCodes. The main difference between these modules is that the OSN3B module provided 4-GB RAM.
Mediant 1000B SBA-EO	Mediant 1000B SBA chassis installed with the following modules: ▪ **OSN4B Module:** ✓ 16-GB RAM ✓ USB 2.0 port for connecting peripheral devices such as SBA Dongle, USB hub (to which keyboard and mouse can be connected) ✓ Gigabit Ethernet interface (RJ-45) for connection to the network ✓ Console (serial) port (micro-USB) for serial communication ✓ HDMI interface (19-pin Type D, micro-HDMI port) for connection to graphic display monitor ▪ **HDMX Module:** Solid-state drive (SSD) **Note:** The OSN4B module has replaced the OSN4 module, which reached End-of-Sale status and is no longer being sold by AudioCodes. The main difference between these modules is that the OSN4 module provided 8-GB RAM.

Model	Description
Mediant 1000B SBA	Mediant 1000B SBA chassis installed with the following modules: ▪ **OSN3 Module:** ✓ 2- or 4-GB RAM ✓ USB 2.0 port for connecting peripheral devices such as SBA Dongle, USB hub (to which keyboard and mouse can be connected) ✓ Gigabit Ethernet port interface (RJ-45) for connection to the network ✓ Serial interface port (RJ-45) for serial communication ▪ **HDMX Module:** Solid-state drive (SSD) **Note:** This module has reached **End-of-Sale** status and is no longer being sold by AudioCodes.

Note: If you have a Mediant 1000B SBA model with Lync Server, see Section 18 for upgrading to Skype for Business.

Part I

Hardware Description

2 Verifying Package Contents

Ensure that your Mediant 1000B SBA package is shipped with the following items:

- 4 x Anti-slide bumpers for desktop installation
- 19-inch rack mounting kit (two flanges and six screws)
- 1 x micro-HDMI (Type D) to standard-HDMI (Type A) 1.5m cable adaptor for monitor connections
- 1 x micro USB to USB cable adaptor 1.5m for serial connections
- 1 or 2 AC power cables (depending on customer order)
- 1 x USB dongle for SBA software upgrade and recovery procedure (Skype for Business Server)
- Microsoft Windows 2012 R2 license (in envelope and label affixed to module)
- Skype for Business Server license (in envelope and label affixed to module)

Check, retain and process any documents. If any items are missing or damaged, please contact your AudioCodes sales representative.

This page is intentionally left blank.

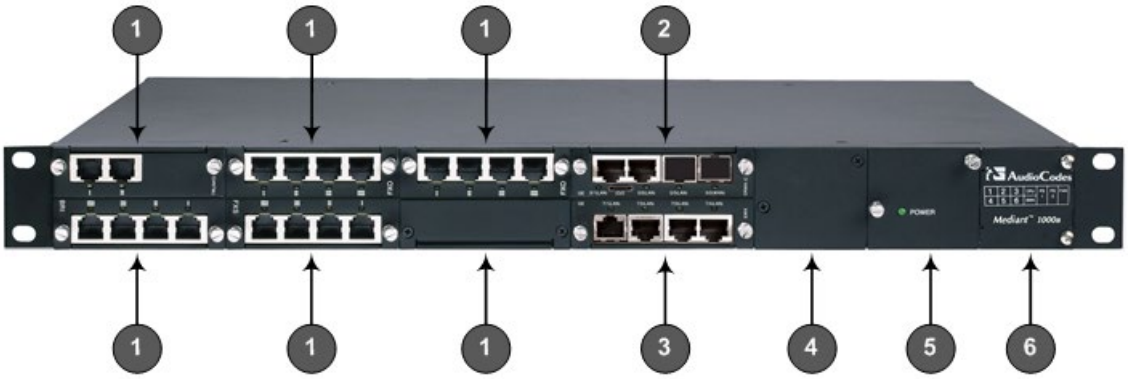
3 Physical Description

This section provides a brief description of the device's front and rear panels. For a detailed description, refer to the document *Mediant 1000B Gateway and E-SBC Hardware Installation Manual*.

3.1 Front-Panel Description

The front panel of the device provides various port interfaces for the **optional** SBC-Gateway functionality.

Figure 3-1: Front Panel



Note:

- The telephony interfaces are customer-ordered items and not shipped by default.
- The figure above is used only as an example. The number and type of interface modules depend on the ordered configuration.

Table 3-1: Front-Panel Description

Item #	Label / Module	Component Description
1	**FXS**, **FXO**, **BRI**, **TRUNKS**, **MPM**	(Optional) Telephony and DSP resource modules: ▪ FXS module ▪ FXO (or FXO G) module ▪ BRI module ▪ TRUNKS (E1/TE/J1) module ▪ MPM module (provides additional DSP resources) **Note:** The modules are customer-ordered items.
2	**CRMX**	CRMX module, providing the following: ▪ Gigabit Ethernet ports ▪ RS-232 serial port ▪ Reset pinhole button
3	**SWX**	(Optional) LAN Extension (SWX) module, providing four Gigabit Ethernet ports. **Note:** The module is a customer-ordered item.
4	**Power 1**	(Optional) Spare Power Supply module slot.

Item #	Label / Module	Component Description
		Note: The module is a customer-ordered item.
5	**Power 2**	Main Power Supply module.
6	**-**	Extractable Fan Tray module with a schematic displayed on its front panel showing the chassis' slot numbers.

3.2 Rear-Panel Description

The rear panel of the device provides the modules for the OSN server on which the SBA runs.

Figure 3-2: Rear Panel

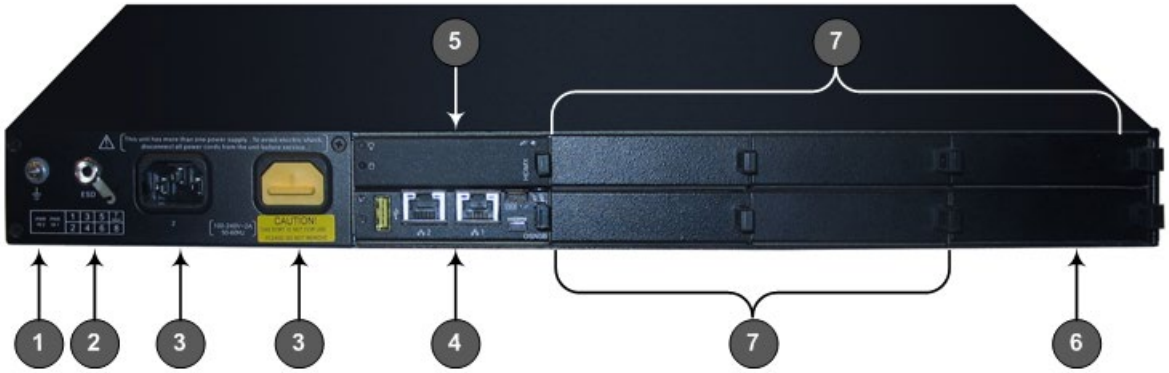


Table 3-2: Rear-Panel Description

Item #	Label	Description
1	⏚	Protective earthing screw.
2	ESD	Electrostatic Discharge (ESD) socket.
3	100-240V~1A	Dual AC Power Supply Entries.
4	OSN	OSN module. For available OSN modules, see Section 1.4 on page 11.
5	HDMX	Main hard-disk drive (HDD) or Solid-State Drive (SSD) AMC module for OSN server platform.
6	HDMX	Slot for second (optional) HDD or SSD for OSN server platform.
7	-	Unused and covered AMC module slots.

Part II

Preparing SBA at Datacenter

4 Introduction

Before you can install and configure the device at your branch office (*site*), you need to do the following at your datacenter (typically, at headquarters):

- Add the SBA to your Active Directory (see Section 5)
- Define and publish a new topology for the branch site at which your device is located (see Section 6)

This page is intentionally left blank

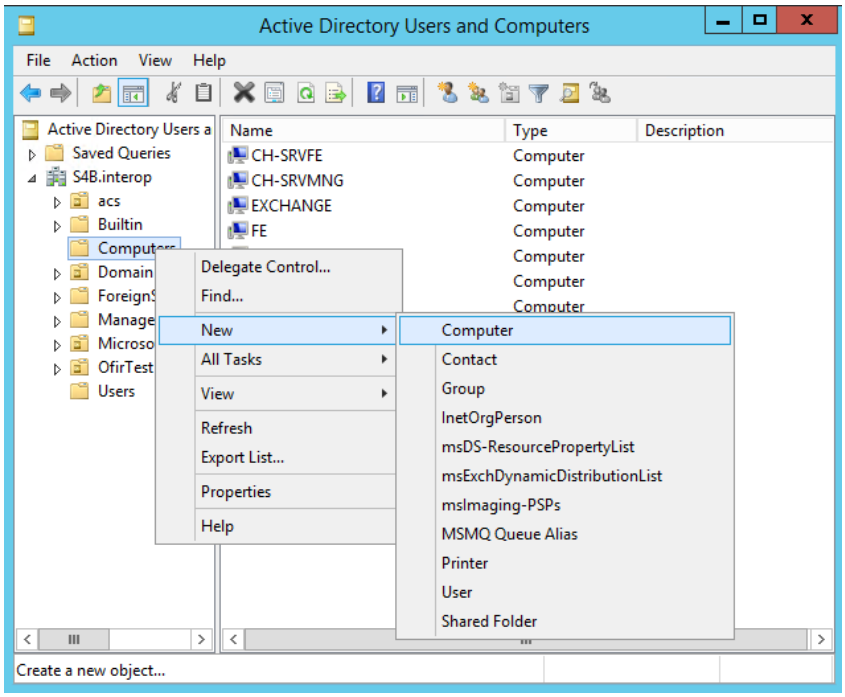
5 Adding SBA to Active Directory

At your datacenter, you need to add the SBA to Microsoft Active Directory (AD) Domain Services.

➢ **To add SBA to AD:**

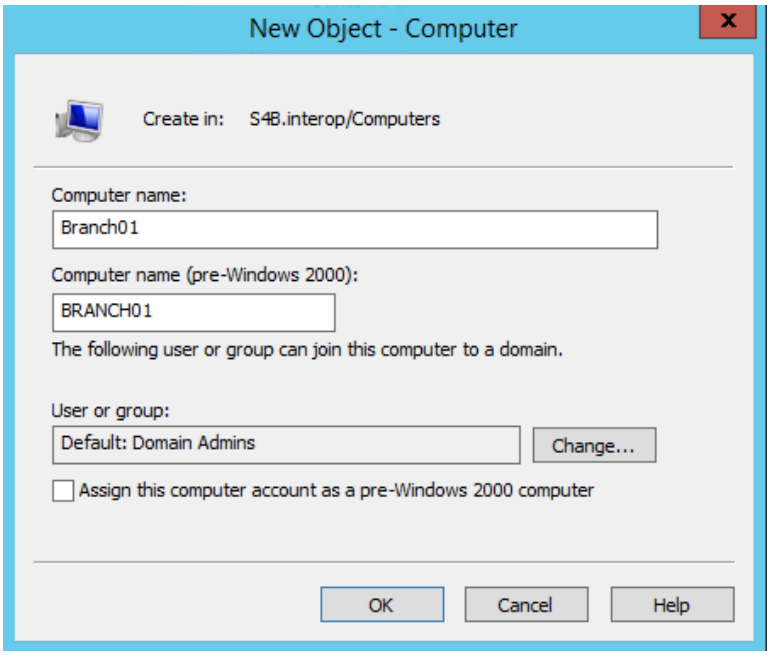
1. Start the Active Directory Users and Computers program (**Start** > **Active Directory Users and Computers**).
2. Right-click **Computers**, point to **New**, and then choose **Computer**, as shown below:

Figure 8-1: Active Directory Users and Computers – New Computer



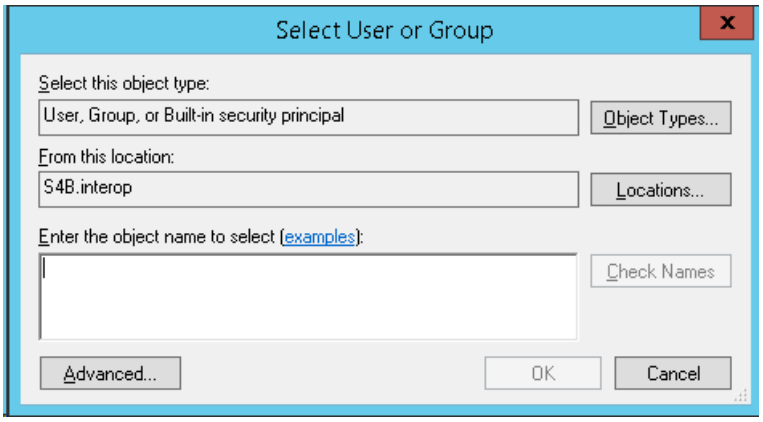
The following appears:

Figure 8-2: New Object - Computer Dialog Box



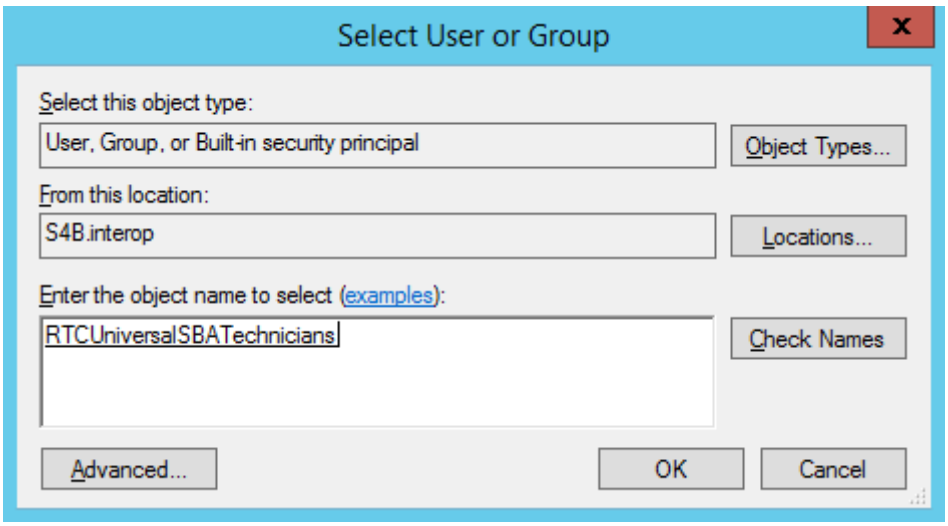
3. In the 'Computer name' field, enter the name of the SBA (e.g., Branch01), and then click **Change** to add a user or group that can join the SBA to the domain; the following appears:

Figure 8-3: Select User or Group Dialog Box

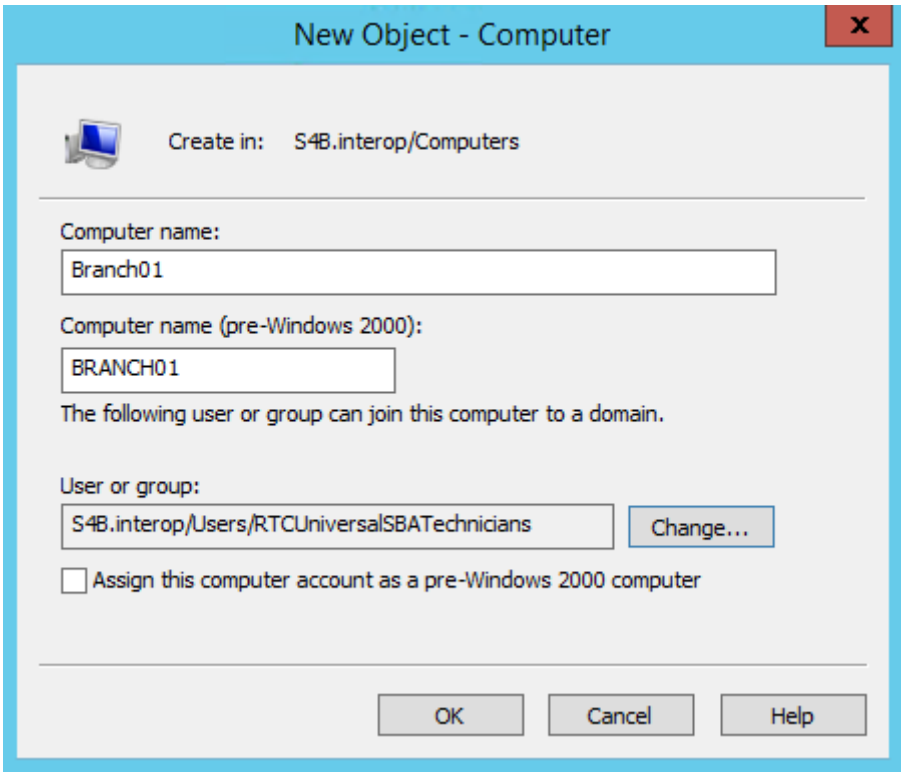


4. In the 'Enter the object name' text box, enter the "RTCUniversalSBATechnicians" group, and then click **Check Names** to make sure that you have entered the name correctly:

Figure 8-4: Group Added

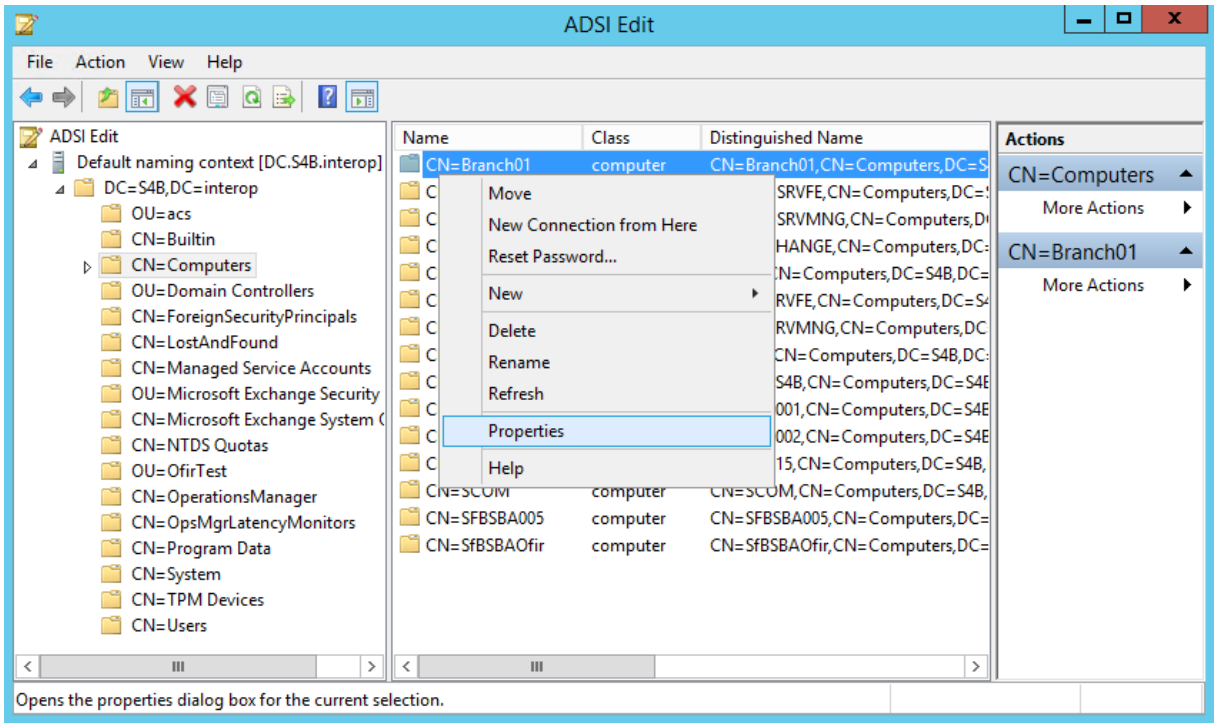


5. Click **OK**; the following appears:



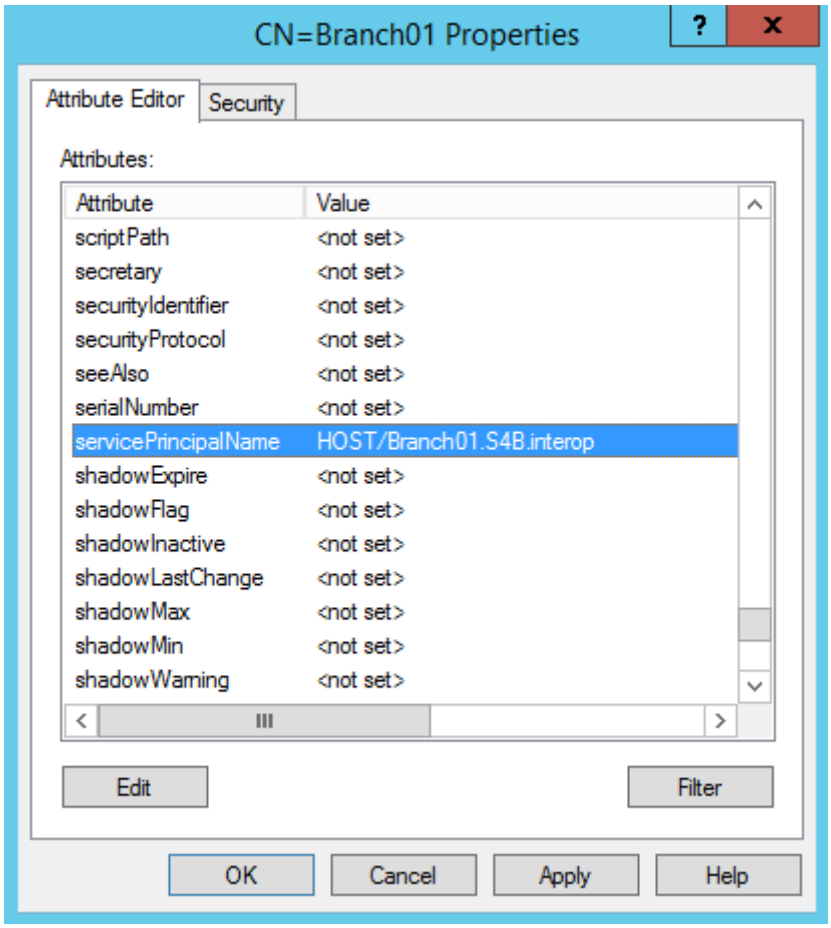
6. Click **OK** to save the SBA computer object.
7. Open the ADSI Edit program (**Start** > **ADSI Edit**).
8. Right-click the computer object (e.g., Branch01) that you created in the previous steps, and then from the shortcut menu, choose **Properties**, as shown below:

Figure 8-5: ADSI Edit – Opening Properties Dialog Box



9. In the Attributes list, select **servicePrincipalName**, and then click **Edit**.
10. In the 'Value to add' field, enter the value "HOST/<SBA's FQDN>" (e.g., HOST/Branch01.SFB.interop), click **Add**, and then click **OK** to save the attribute setting:

Figure 8-6: Attribute Editor



11. Click **OK** to save the computer object properties.

6 Defining Branch Site Topology

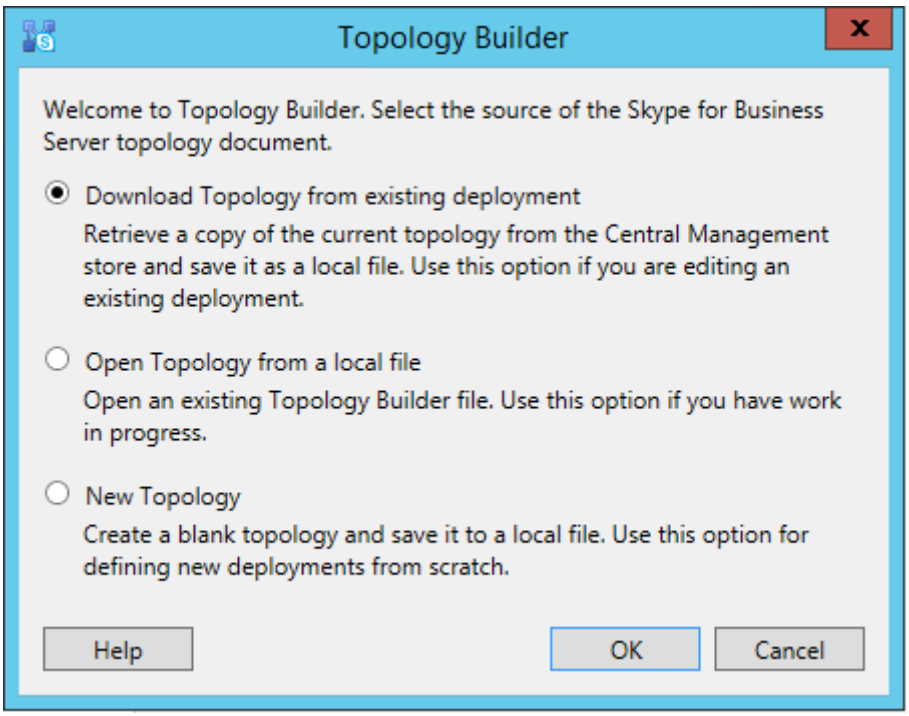
At the datacenter, you need to define and publish a new topology for the branch site at which your device is located. This is done using Microsoft's Skype for Business Server Topology Builder.

Note: Where Skype for Business Topology Builder refers to *PSTN Gateway*, it relates to the media gateway and/or session border controller (SBC) applications that are also supported on the device chassis. Through these applications, different SIP entities can be supported (e.g., a SIP trunk or PSTN trunk), which Topology Builder terms "trunks".

➢ **To define a new branch office topology for Mediant 1000B SBA:**

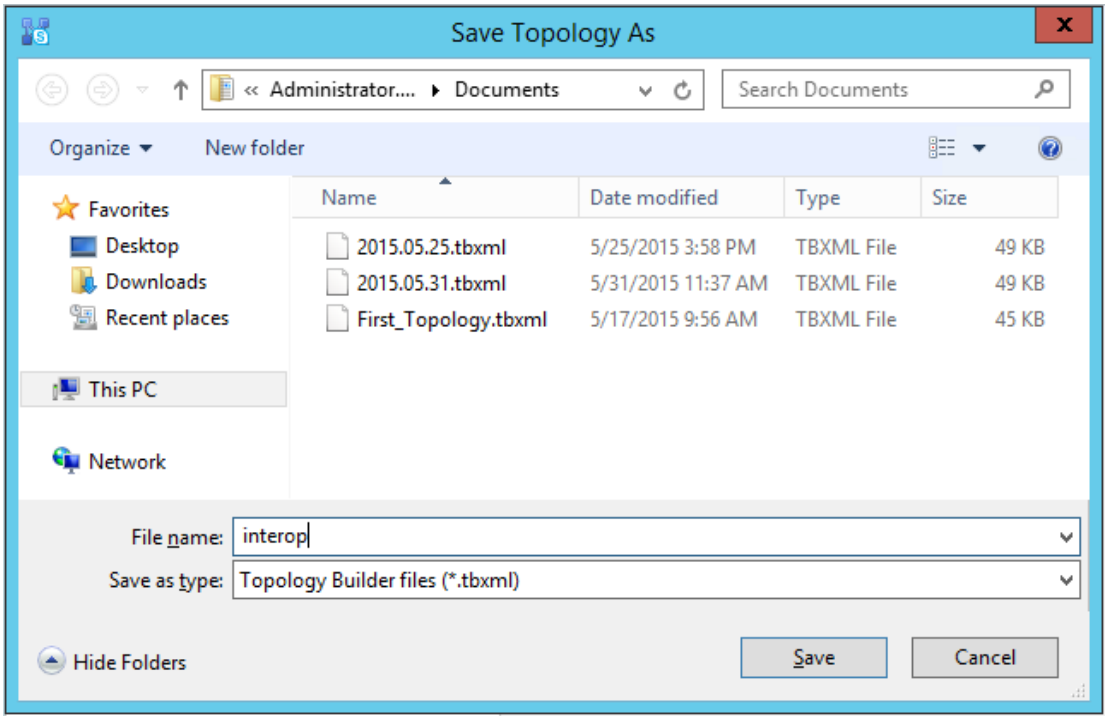
1. On the server where Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > **Skype for Business Server Topology Builder**); the following appears:

Figure 6-1: Topology Builder Dialog Box



2. Select **Download Topology from existing deployment**, and then click **OK**; you are prompted to save the downloaded topology:

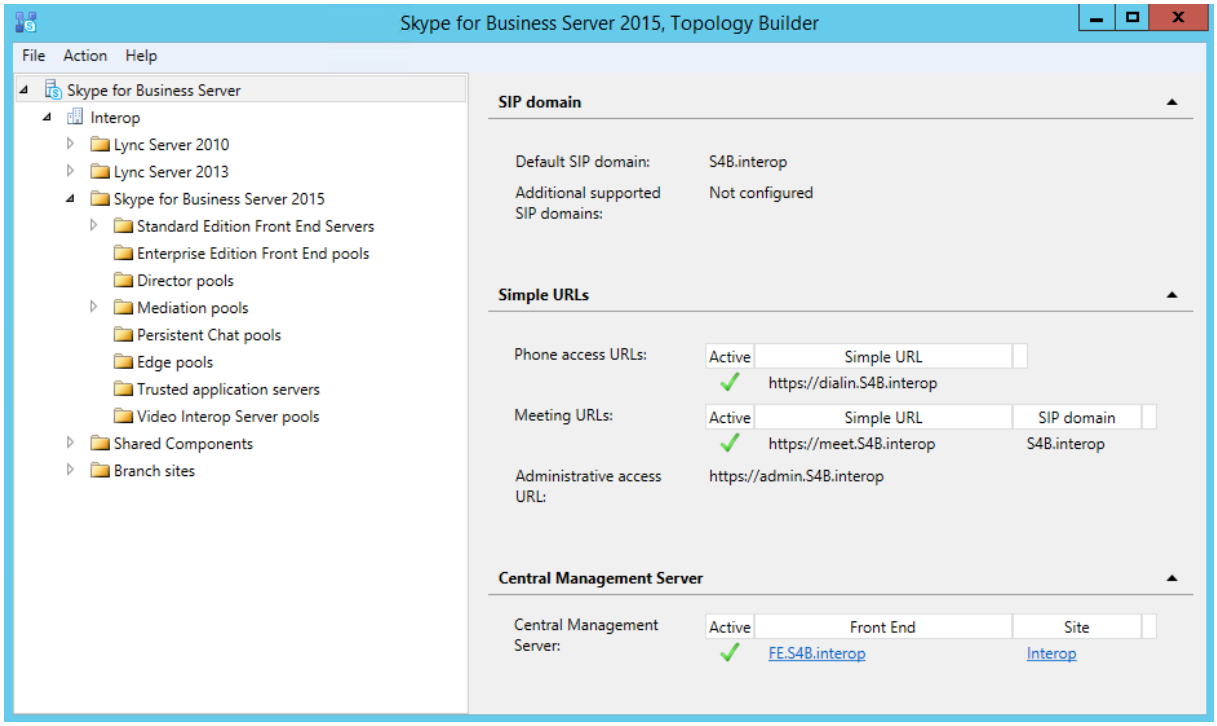
Figure 6-2: Save Topology



3. Enter a name for the topology file, and then click **Save**. This step enables you to roll back from any changes you make during installation.

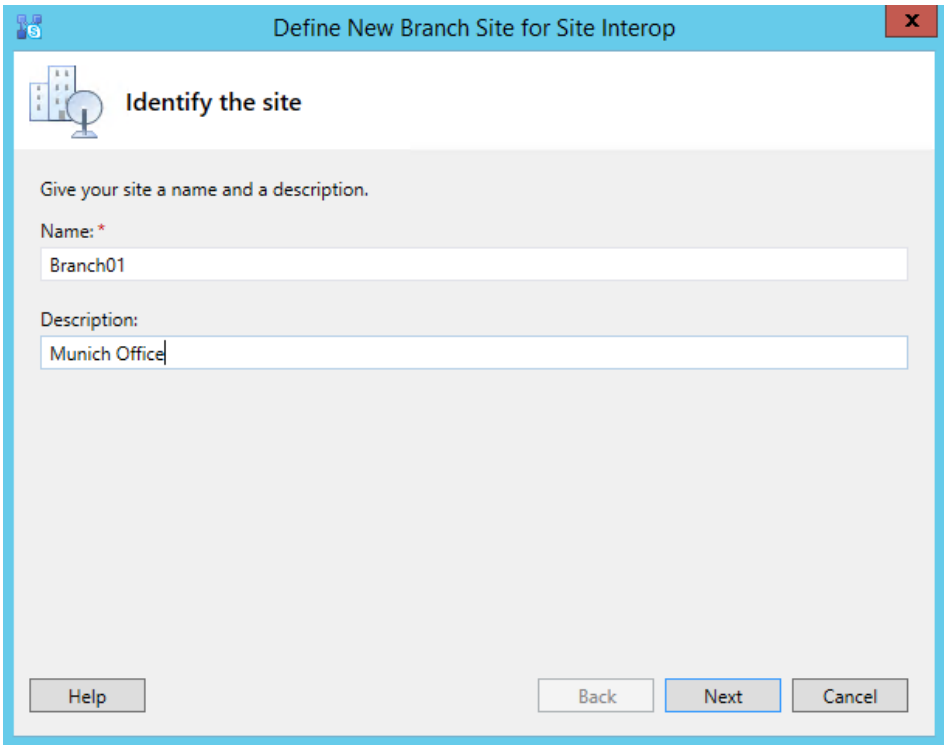
   The Topology Builder screen with the downloaded topology appears:

Figure 6-3: Downloaded Topology



4. In the Topology Builder tree, right-click the **Branch sites** node, and then from the shortcut menu, choose **New Branch Site**; the following appears:

Figure 6-4: Define New Branch Site – Name

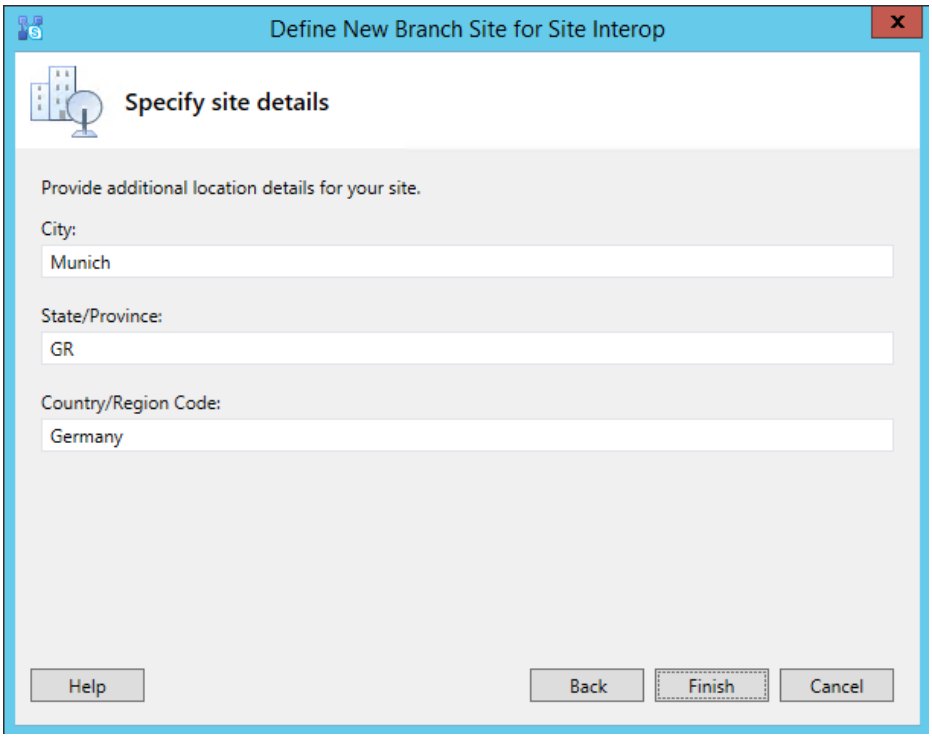


5. In the 'Name' field, enter the name of the branch site. You can also enter a description of the branch site in the 'Description' field (optional).

Note: The branch site name must be identical to the name of the computer on which the SBA is installed, as configured in Section 9.5.

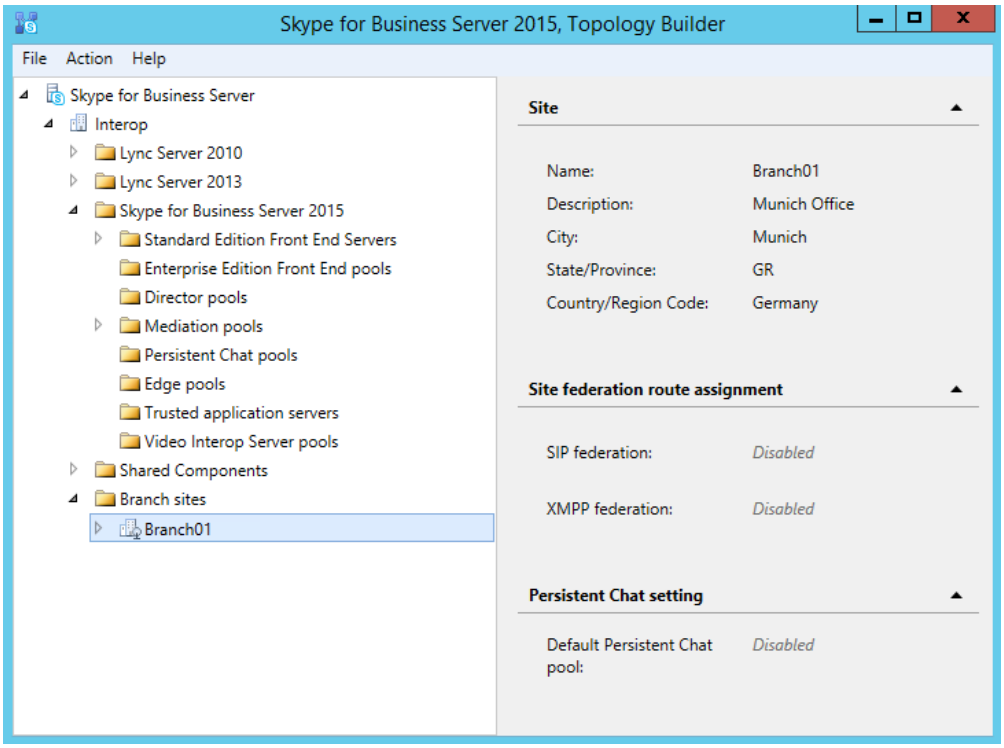
6. Click **Next**; the following appears:

Figure 6-5: Define New Branch Site - Details



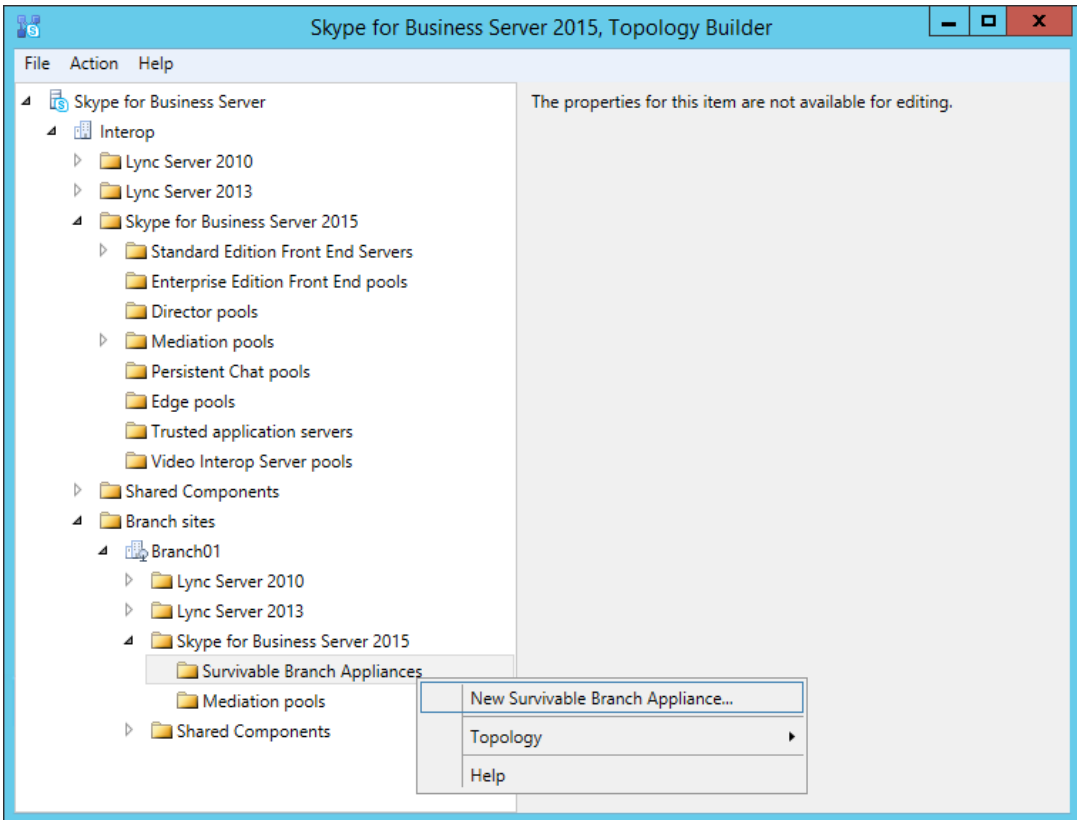
7. Provide details of the branch site:
   a. In the 'City' field, enter the name of the city in which the branch site is located.
   b. In the 'State/Province' field, enter the name of the state or region in which the branch site is located.
   c. In the 'Country/Region Code' field, enter the two-digit calling code for the country in which the branch site is located.
   d. Click **Finish**; the following appears:

Figure 6-6: New Branch Site Successfully Defined



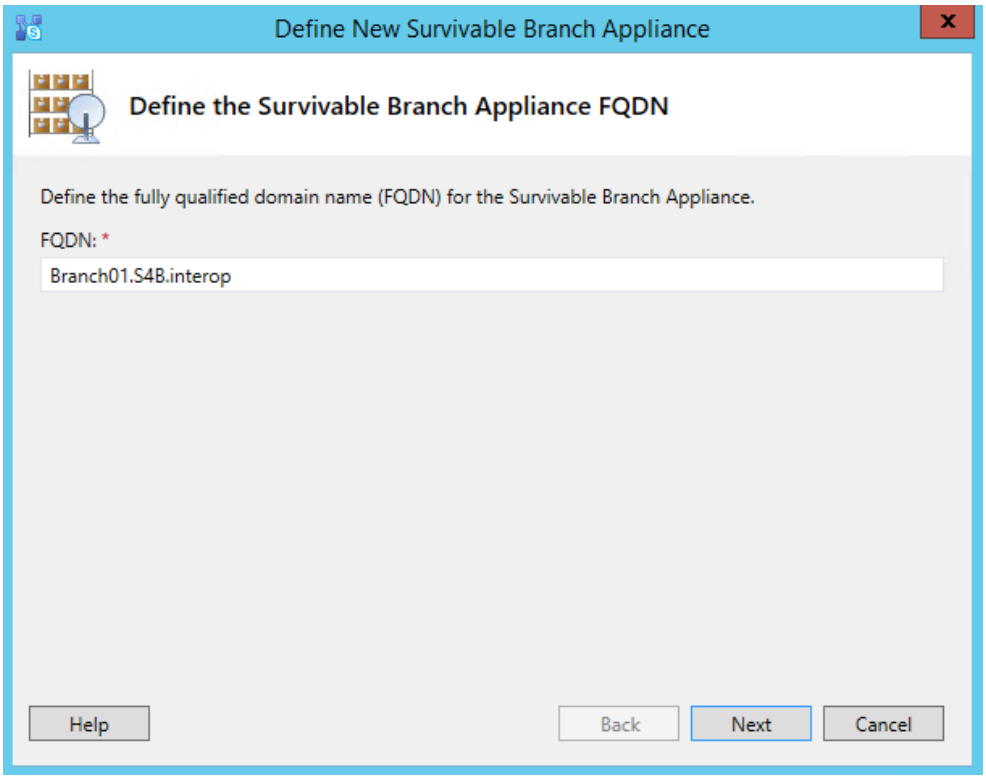
8. In the Topology Builder tree, expand the new branch site node that you created, right-click the required Microsoft platform to which you want to add the SBA (e.g. **Skype for Business Server 2015**), and then choose **New Survivable Branch Appliance**:

Figure 6-7: Select Skype for Business Folder to Add SBA



The following appears:

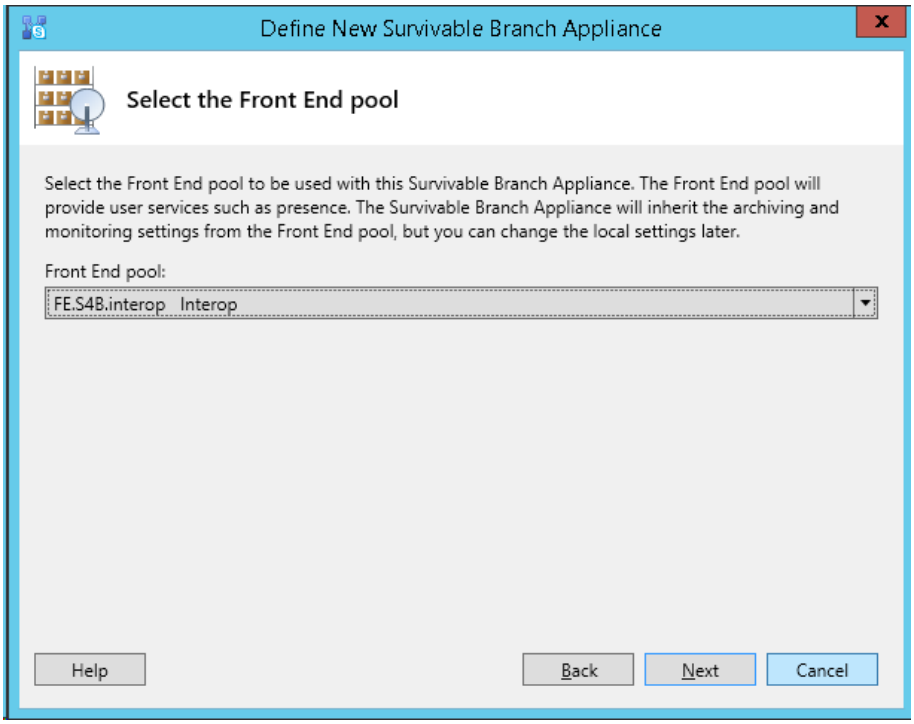
Figure 6-8: Define New Survivable Branch Appliance - FQDN



9. In the 'FQDN' field, enter the FQDN of the SBA, and then click **Next**; the following appears:

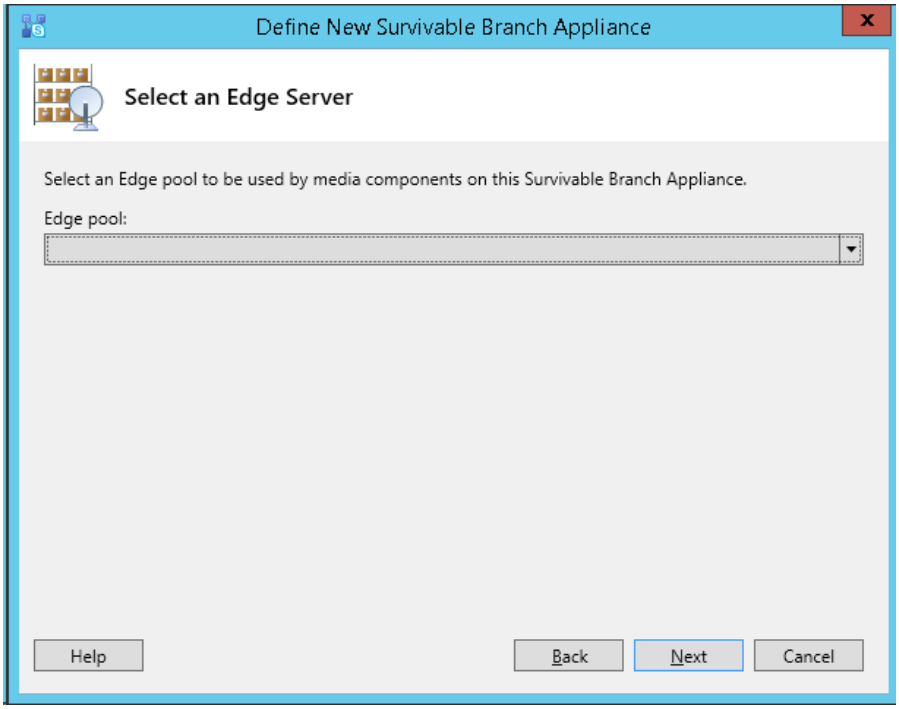
Note: The same FQDN must be configured for the SBC/gateway leg of the SBA in the SBA Wizard (see Section 9.8).

Figure 6-9: Define New Survivable Branch Appliance - Front End Pool



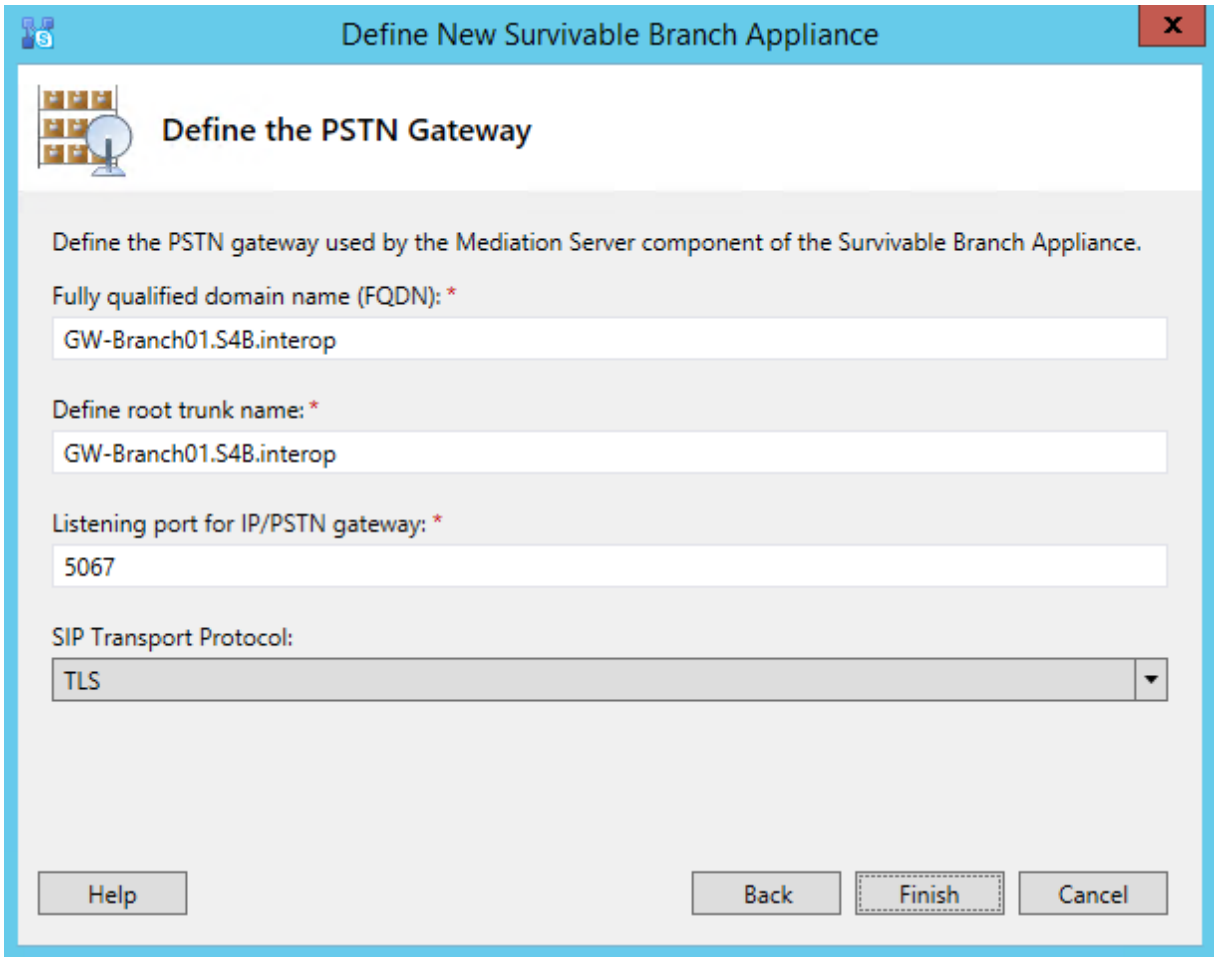
10. From the 'Front End pool' drop-down list, select the Front End pool to be used with the SBA, and then click **Next**; the following appears:

Figure 6-10: Define New Survivable Branch Appliance - Edge Pool



11. (Optional) From the 'Edge pool' drop-down list, select the Edge pool to be used with the SBA, and then click **Next**; the following appears:

Figure 6-11: Define New Survivable Branch Appliance - PSTN Gateway



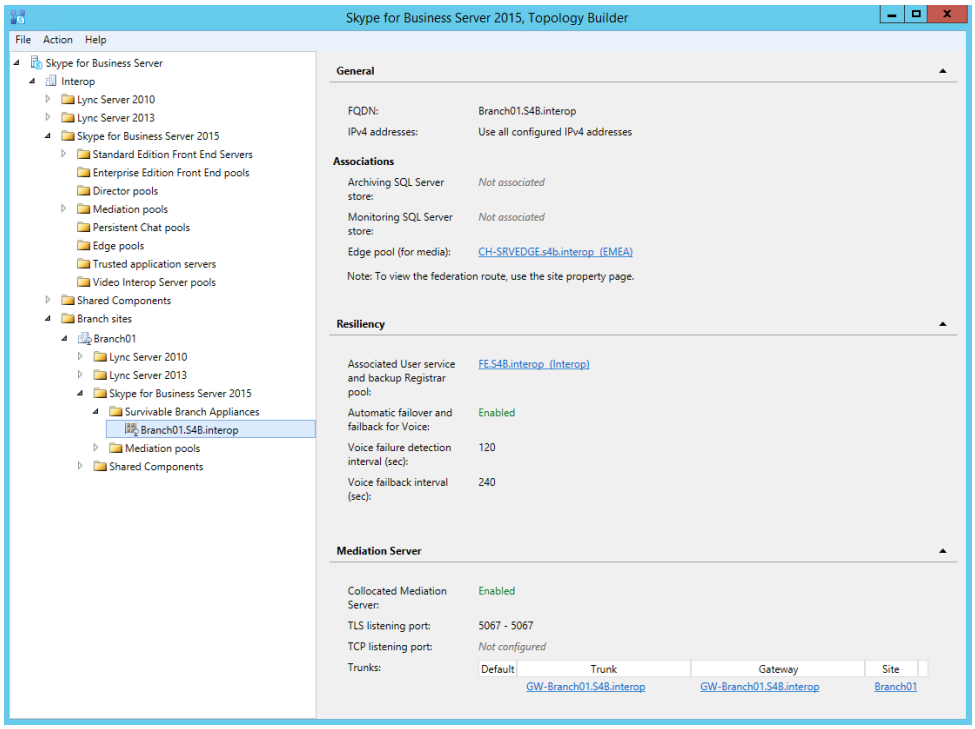
12. Define the PSTN Gateway:
    a. In the 'Fully qualified domain name' field, enter the FQDN (e.g., "GW-Branch01.S4B.interop") of the PSTN Gateway.
    b. In the 'Listening Port for IP/PSTN Gateway' field, enter the SIP listening port (e.g., "5067") of the PSTN Gateway ("trunk"). This is the port to which the Mediation Server sends SIP messages to the PSTN Gateway.
    c. In the 'SIP Transport Protocol' field, select the transport type (e.g., TLS) used by the PSTN Gateway ("trunk") for SIP messages.

Note:

- Configure the same FQDN for the 'SIP Domain' parameter in the SBA Setup Wizard (see sections 11.10 and 11.11) and for the 'Subject Name (CN)' of the TLS Context in the Web interface of the PSTN Gateway (see Section 13.8.4).
- Configure the same listening port and transport type for the PSTN Gateway in the SBA Setup Wizard (see sections 11.10 and 11.11).

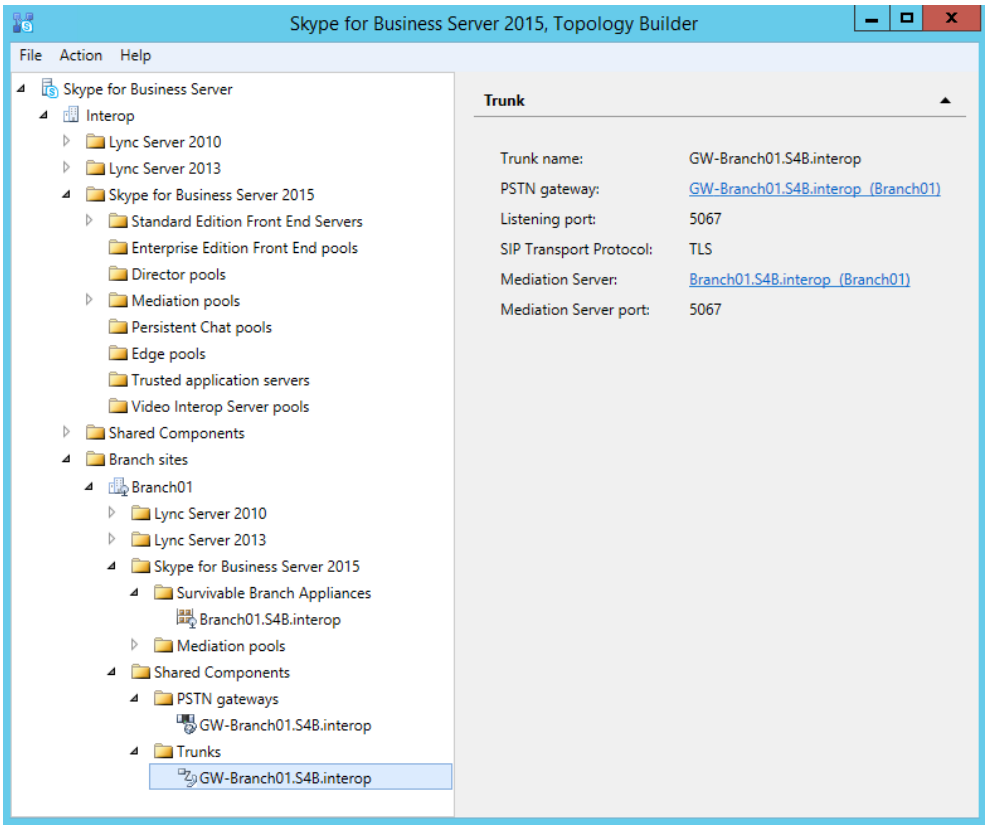
d. Click **Finish**; the new SBA is added under the **Survivable Branch Appliances** folder, as shown below:

Figure 6-12: SBA Branch Successfully Created



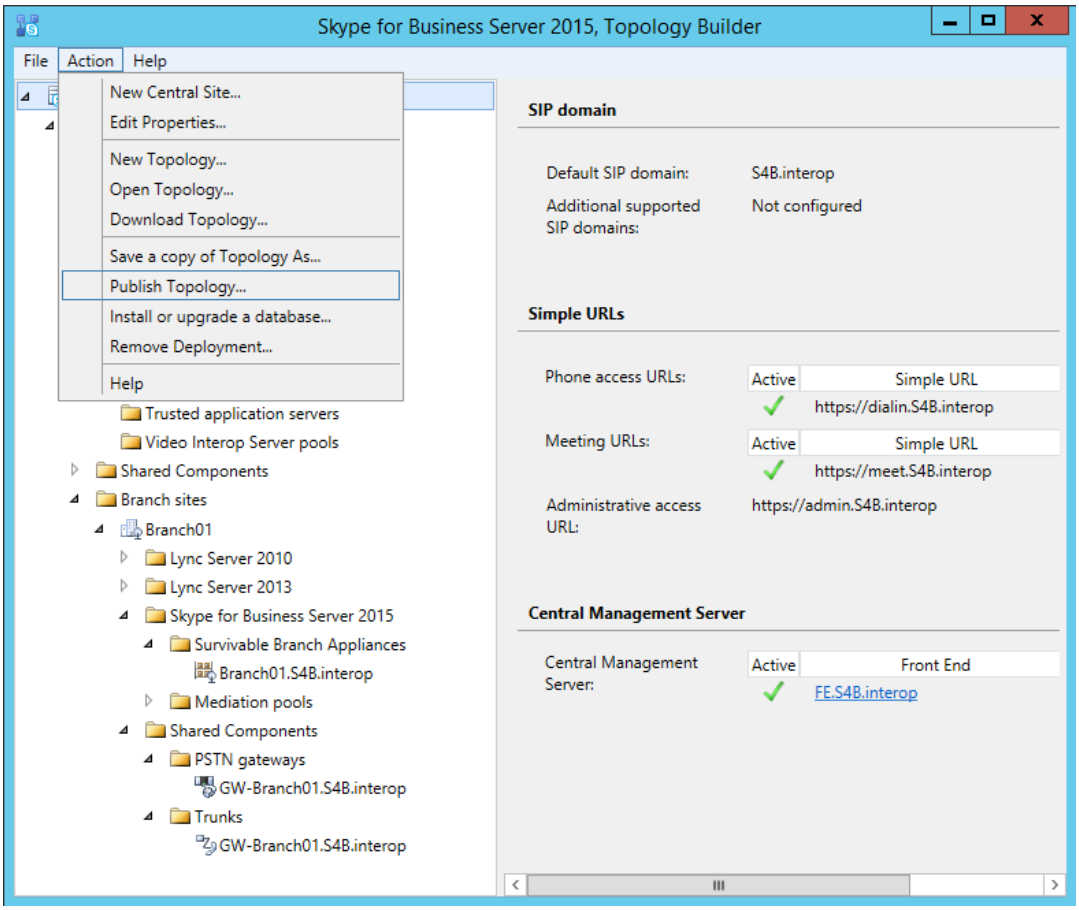
13. Open the **Shared Components** folder that is located under the SBA branch. You will notice that the PSTN Gateway and its trunk have been added to the respective folders, as shown in the example below:

Figure 6-13: Shared Components of SBA Branch



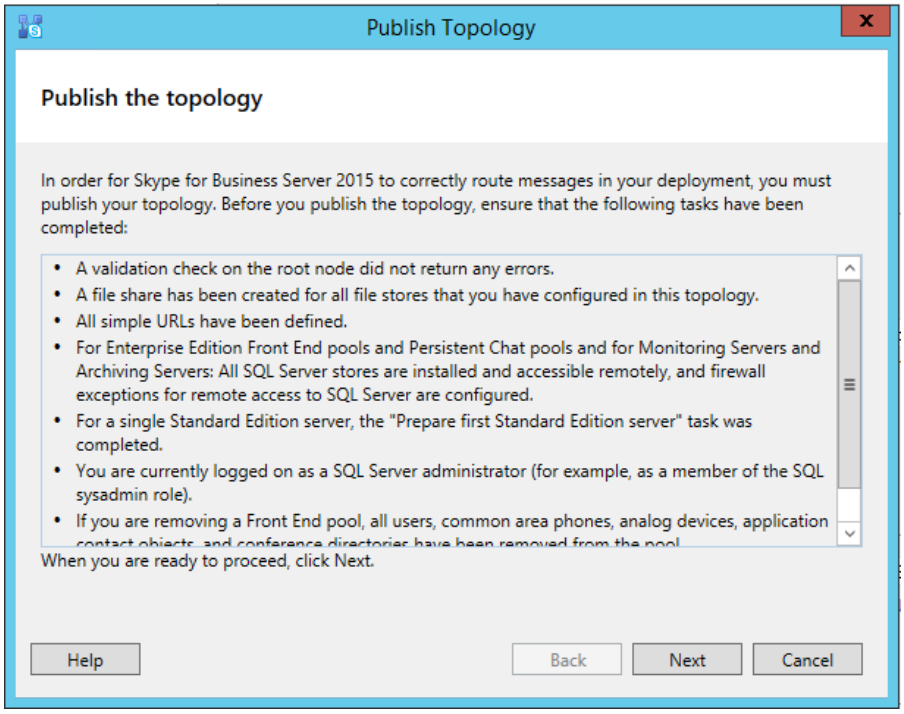
14. In the Topology Builder tree, select the root node, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 6-14: Publishing Topology



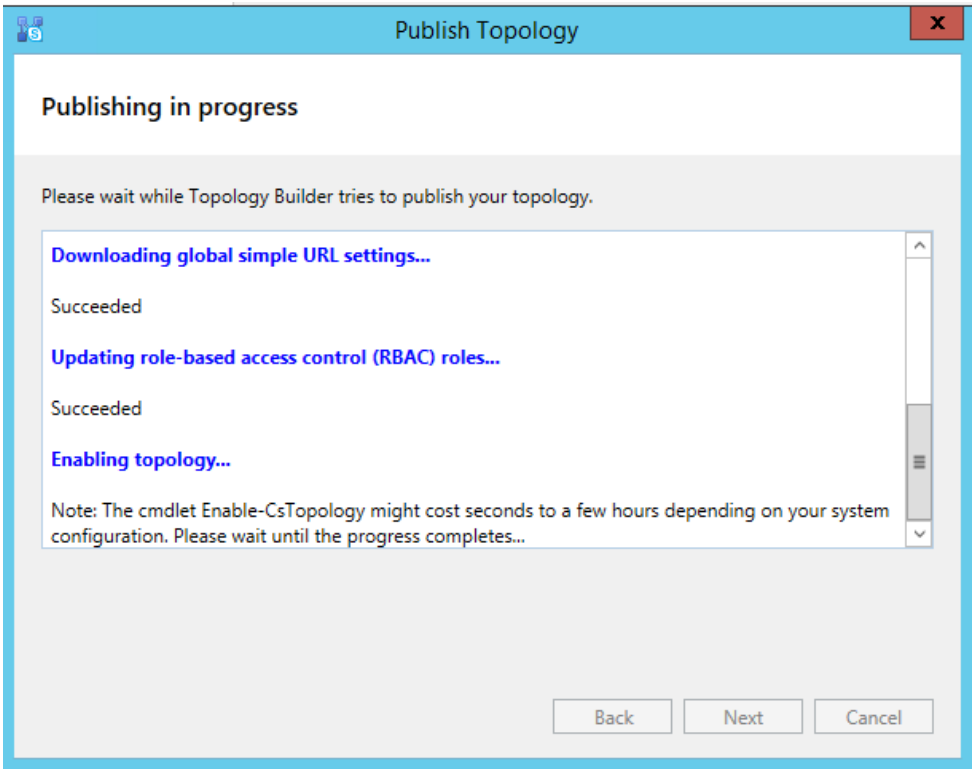
The following appears:

Figure 6-15: Publish Topology Confirmation



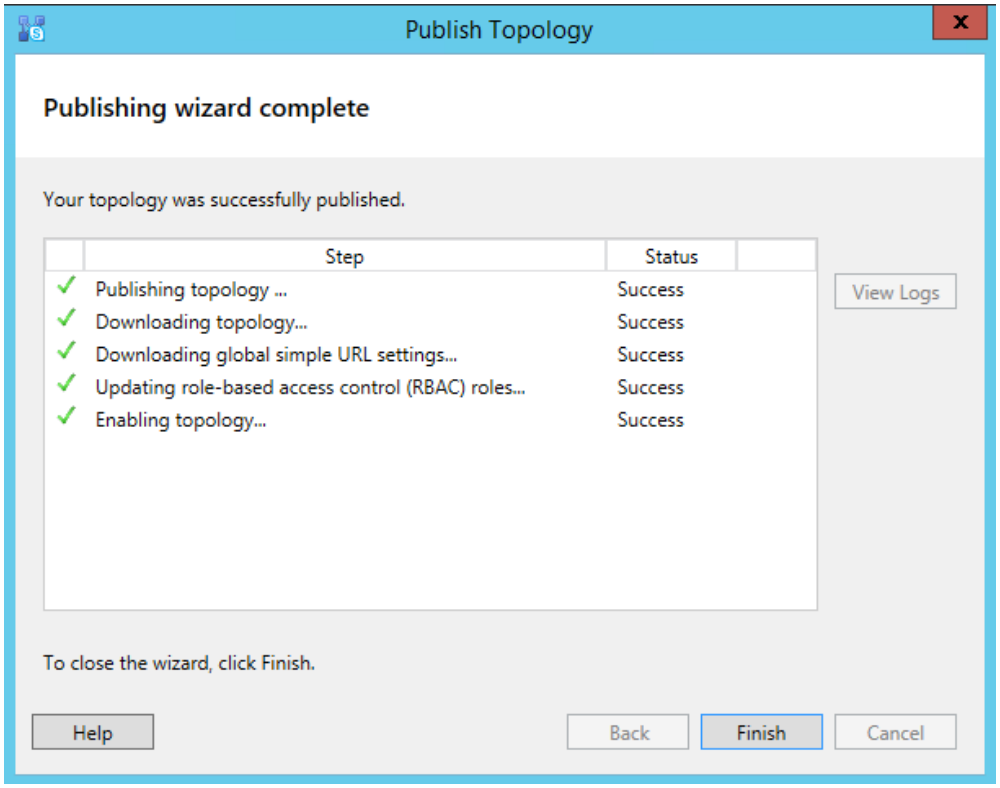
15. Click **Next**; the Topology Builder starts publishing your topology, as shown below:

Figure 6-16: Publishing in Progress



16. Wait until the publishing topology process completes successfully, as shown below:

Figure 6-17: Publishing Wizard Complete



17. Click **Finish**.

Part III

Preparing SBA at Branch Site

7 Introduction

This part describes the preparation of the device at the branch site, which includes the following main sections:

1. Modifying Default IP Address
2. Resumption of SBA Wizard after Initial Network Configuration
3. Using the SBA Management Interface

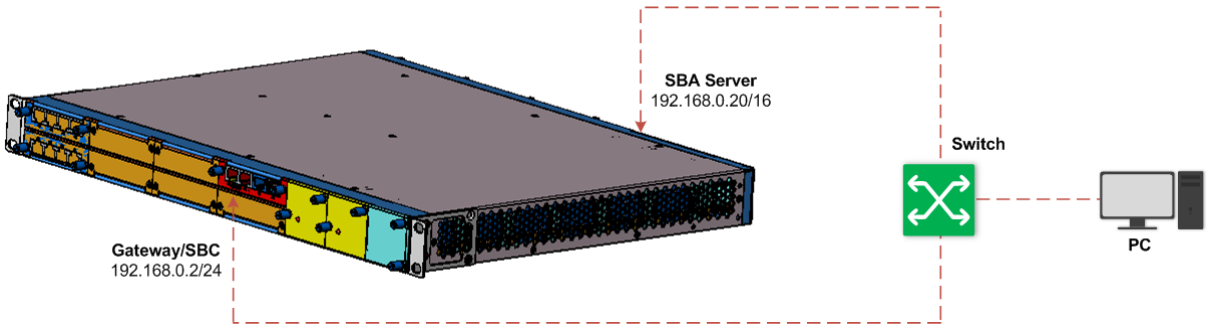
This page is intentionally left blank.

8 Modifying Default IP Address

This section describes how to assign a new IP address to the device's SBA and SBC/Gateway functionalities. These IP address are also used to access their management interfaces.

As the device provides not only SBA functionality but also optional SBC/Gateway functionality, for initial connection you need to cable both these functionalities to the network, as shown in the following illustration:

Figure 8-1: Initial Cabling – SBA and SBC/Gateway



Once cabled, you can change the default IP addresses of the SBA and SBC/Gateway to suit your networking scheme. The default IP addresses (and login usernames and passwords) are shown in the following table:

Table 8-1: Default IP Address of SBA and SBC/Gateway

Parameter	Value
SBA Server	
Management Network Interface	IP Address: 192.168.0.20/16
Management Login Credentials	▪ Username: Administrator (case-sensitive) ▪ Password: Pass123 (case-sensitive)
SBC/Gateway	
Management Network Interface	▪ IP Address: 192.168.0.2/24 ▪ Default Gateway: 192.168.0.1
Management Login Credentials	▪ Username: Admin (case-sensitive) ▪ Password: Admin (case-sensitive)

Modifying the IP addresses are done in the following stages:

1. Modifying IP Address of SBA Server
2. Modifying IP Address of SBC/Gateway
3. Re-Cabling SBA and SBC/Gateway to Network

Note: After modifying the IP addresses of the SBA and SBC/Gateway, your connection to their management interfaces will no longer be available at the default IP addresses.

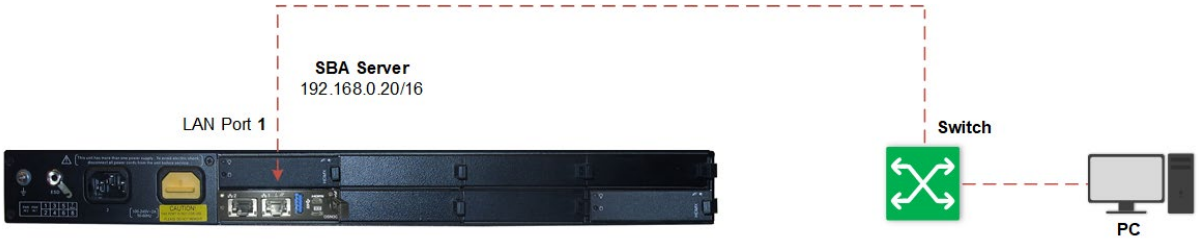
8.1 Modifying IP Address of SBA Server

The following procedure describes how to initially cable to the SBA Server to access its SBA Management interface to change its default IP address. When you initially access the SBA Management Interface, the SBA Setup Wizard starts.

➢ **To cable Mediant 1000B SBA for connecting to SBA Management interface:**

1. Keep your computer connected to your switch, as you did for the SBC/Gateway cabling in the previous section.
2. Using an RJ-45 Ethernet cable, connect the Ethernet port on the OSN module, located on the rear panel of the device, directly to the switch. The connection on the OSN module depends on the OSN module type:
   - **OSN3C and OSN4B Modules:**

Figure 8-2: Connecting OSN3C and OSN4B Module to Network



   - **OSN3B and OSN4 Modules:**

Figure 8-3: Connecting OSN3B and OSN4 Module to Network

   - **OSN3 Module:**

Figure 8-4: Connecting OSN3 Module to Network

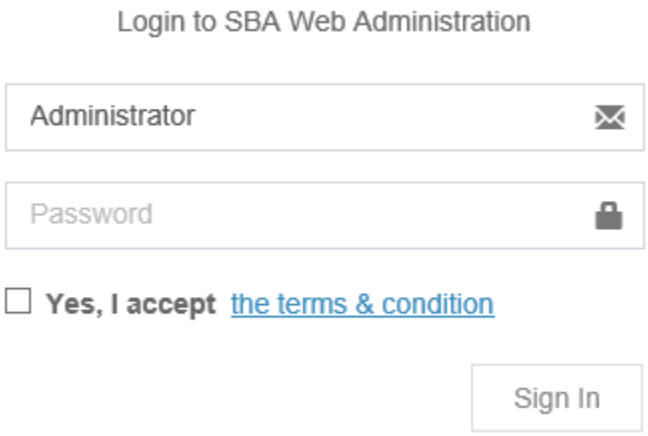
Note: From SBA Version 7.2.113, NIC Teaming is supported, whereby the GE1 and GE2 ports are a teaming interface (with a MAC and IP address).

3. Power on the device, by connecting the left (active) 100-240V~50-60 Hz AC power socket to a standard electrical outlet, using the supplied AC power cord:

Figure 8-5: Powering on Device

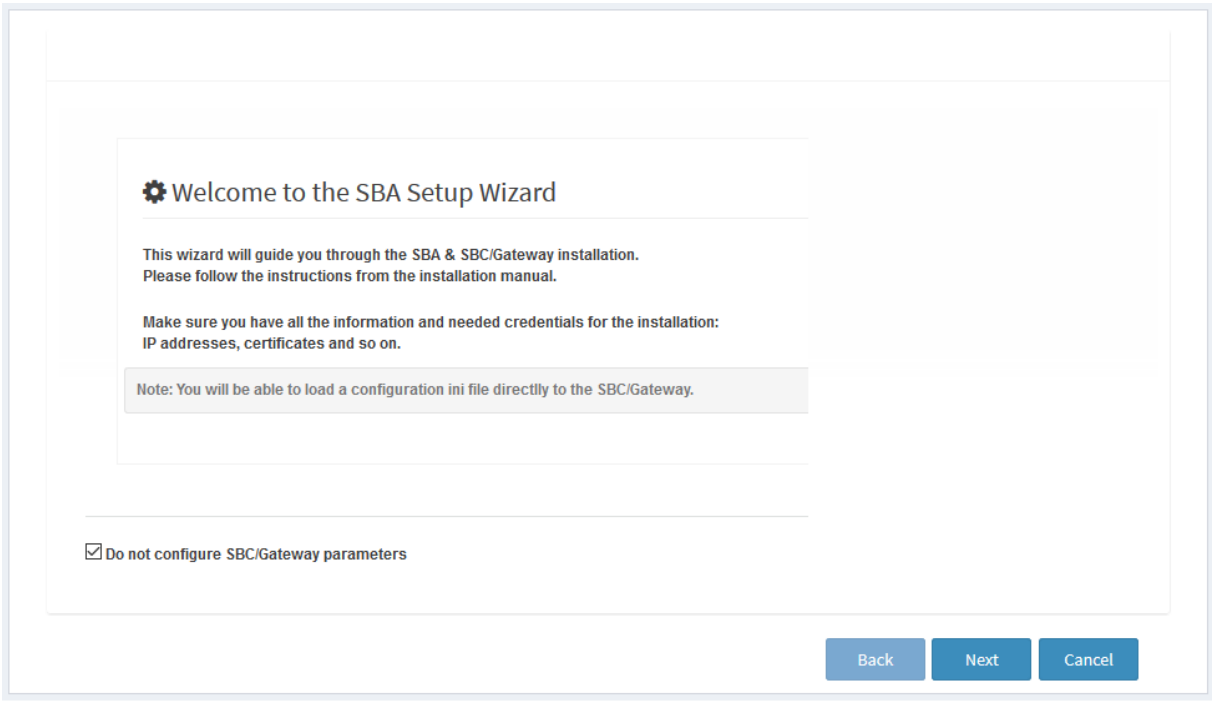
4. Open a standard Web browser (for supported browsers, see Section 10), and then in the URL address field, enter the SBA Server's default IP address; the Login screen of the SBA Management Interface appears:

Figure 8-6: SBA Management Interface - Login Screen



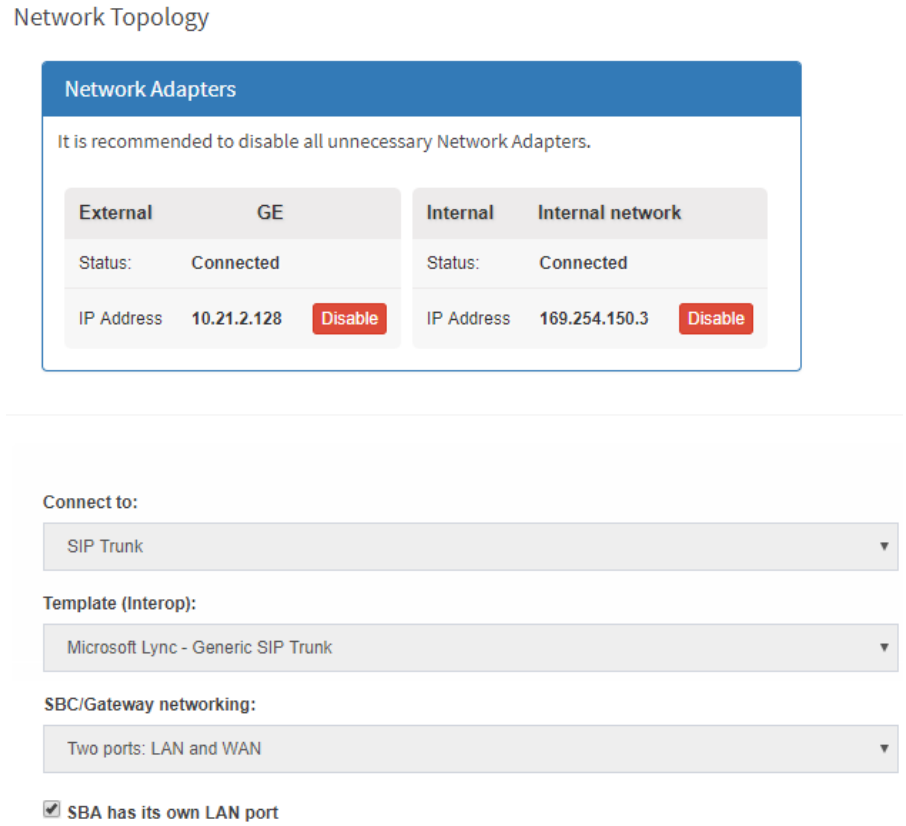
5. Enter the default username and password, select the **Yes, I accept the term and condition** check box, and then click **Sign In**; the Welcome page of the SBA Setup Wizard appears.
6. Select the **Do not configure E-SBC/gateway parameters** check box (default) to configure only SBA.

Figure 8-7: SBA Setup Wizard - Welcome



7. Click **Next**; the Network Topology page appears:

Figure 8-8: SBA Setup Wizard - Network Topology

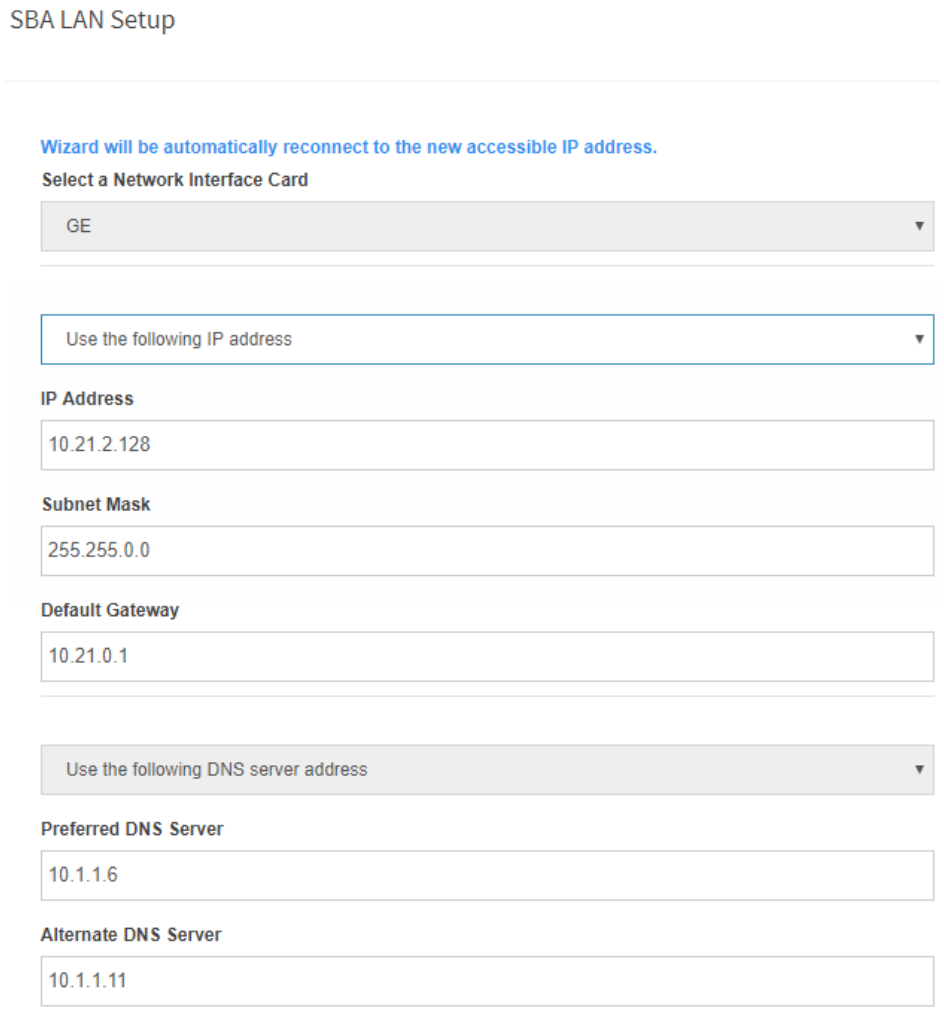


1. Configure the network topology: The SBA has an external network interface and an internal network interface (which is connected via the SBC/Gateway network). It is recommended to have only one interface connected (enabled).

Note: For SBA versions earlier than Version 7.2.113, the NIC Teaming feature is not supported and therefore, two external NICs (depending on hardware) -- GE1 (External 1) and GE2 (External 2) may be displayed. In this case, it's recommended to disable the external interface that is not used.

2. Click **Next**; the SBA LAN Setup page appears:

Figure 8-9: SBA Setup Wizard - SBA LAN Setup



3. Configure the IP addressing scheme for the SBA server:
   a. From the 'Select a Network Interface Card' drop-down list, select the required network card if there are several options. This should be the network card associated with the port that you enabled in the previous step.
   b. Select the **Use the following IP address**.
   c. In the 'IP Address', 'Subnet Mask' and 'Default Gateway' fields, enter a new IP address, subnet and default gateway for the SBA server.
   d. In the 'Preferred DNS Address' and 'Alternative DNS Address' fields, enter the primary and secondary DNS addresses, respectively. The primary DNS server address is necessary for later connecting the SBA server to the network domain in Section 11.7
4. Click **Next**; your connection with the SBA server **becomes unavailable at the default IP address** (due to the new IP address).

8.2 Modifying IP Address of SBC/Gateway

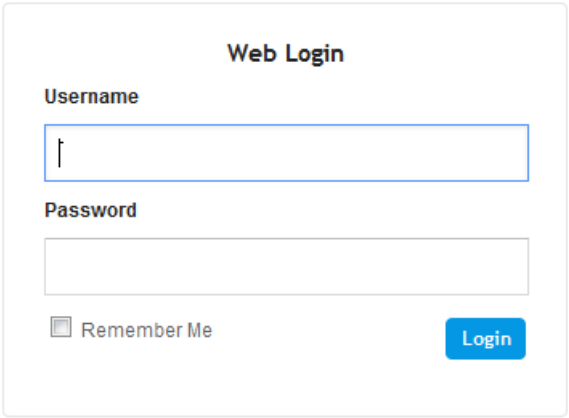
The following procedure describes how to initially cable to the SBC/Gateway in order to change its default IP address.

➢ **To change the default IP address of SBC/Gateway:**

1. Connect your computer to your switch.
2. Change the IP address and subnet mask of your computer to correspond with the default IP address of the SBC/Gateway.
3. Using an RJ-45 Ethernet cable, connect Ethernet port **0/1** or **0/2** on the CRMX module, located on the front panel of the device, directly to the switch:

4. On your computer, start a standard Web browser and in the URL address field, enter the default IP address to access the Web-based management interface of the SBC/Gateway; the Web interface's Web Login screen appears:

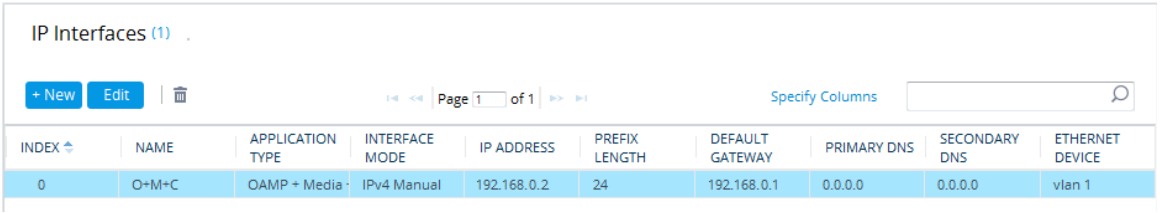
Figure 8-10: Web Login Screen



5. In the 'Username' and 'Password' fields, enter the default login username and password, and then click **Login**.

6. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**):

Figure 8-11: IP Interfaces Table



7. Select the OAMP interface ("O+M+C"), click **Edit**, and then modify the IP address and any other networking parameters, as desired.
8. Click **Apply**; your connection with the SBC/Gateway Web interface **becomes unavailable at the default IP address** (due to the new IP address).

Note: Keep the device connected to the power supply.

9. Change your computer's IP address so that it's in the same subnet as the new IP address which you configured for the SBC/Gateway.
10. Log in again to the Web interface of the SBC/Gateway, using its new IP address.
11. Click the **Save** button, located on the toolbar, to save your new IP address to flash memory.

8.3 Re-Cabling SBA and SBC/Gateway to Network

Once you have changed the IP addresses of the SBA and SBC/Gateway from their default settings, you need to connect the SBA and SBC/Gateway to the network in which you want to deploy your device.

➢ **To connect the SBA and SBC/Gateway to the network:**

1. Disconnect your device's local cable connection with the switch and computer.
2. Re-cable the SBA and SBC/Gateway to the network.
3. Continue configuring the SBA through the SBA Setup Wizard, as described in Section 9.

9 Resumption of SBA Wizard after Initial Network Configuration

Once you have assigned new IP addresses to the SBA and SBC/Gateway (as described in Section 8), you need to resume the SBA Setup Wizard to continue SBA configuration.

Note: The SBA Setup Wizard uses the term "*SBC*" and "*Gateway*" to refer to the session border controller (SBC) and media gateway applications respectively, which are also supported by the device. The Skype for Business Topology Builder refers to these applications as the "*PSTN Gateway*" and "*trunks*".

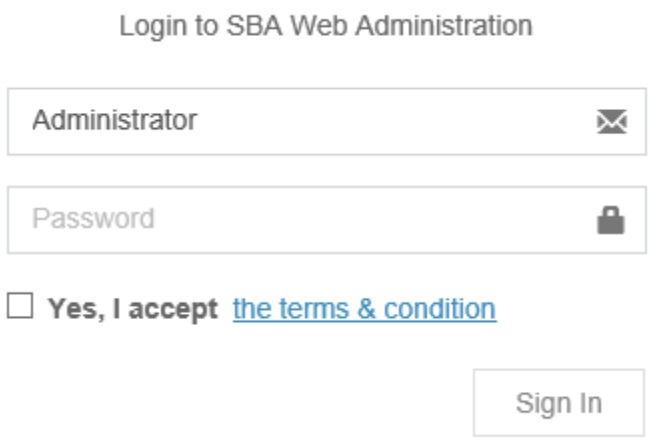
9.1 Step 1: Access the SBA Setup Wizard

The following procedure describes how to access the SBA at its new IP address.

➢ **To access the SBA and resume SBA Setup Wizard:**

1. From a computer connected to the network, open a Web browser, and then enter the new IP address that you assigned to the SBA server in Section 8.1; the following appears:

Figure 9-1: SBA Management Interface - Login Screen



2. Enter the default username and password, select the **Yes, I accept the term and condition** check box, and then click **Sign In**; the SBA Setup Wizard resumes at the next wizard page.

Note: The default username is **Administrator** (case-sensitive) and the default password is **Pass123** (case-sensitive).

9.2 Step 2: Configure SBC and Gateway LAN and WAN

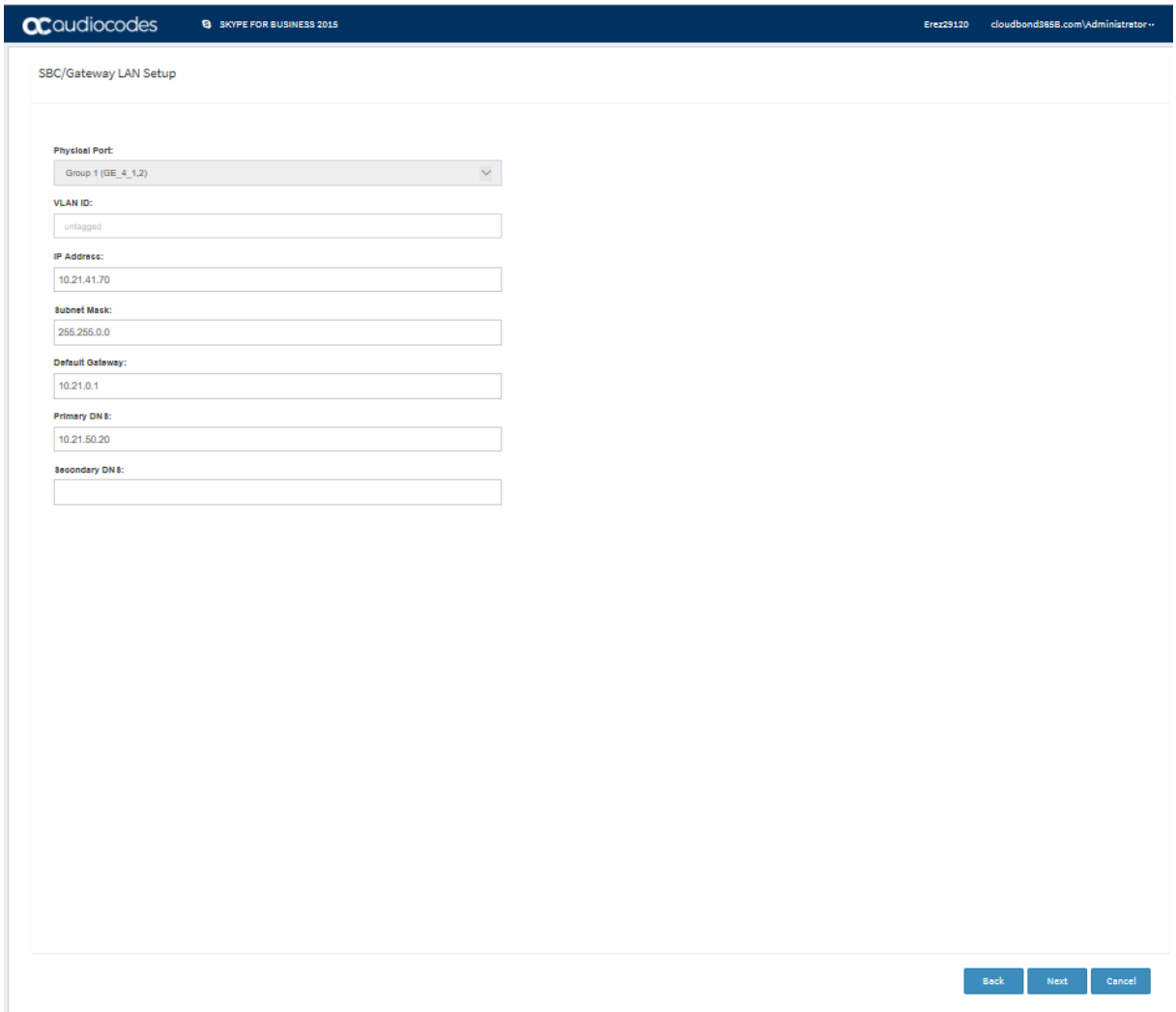
This step describes how to setup the connection of the gateway/SBC application to the Enterprise LAN or Enterprise WAN (depending on your Network Topology configuration (see Section 11.2).

Note: This step is only relevant if you are configuring the E-SBC/gateway parameters.

9.2.1 Step 2-1: Configure E-SBC and Gateway LAN Connection

This step describes how to setup the connection of the gateway/SBC application to the Enterprise LAN.

Figure 9-2: SBA Wizard LAN Leg



➢ **This step defines the following parameters:**

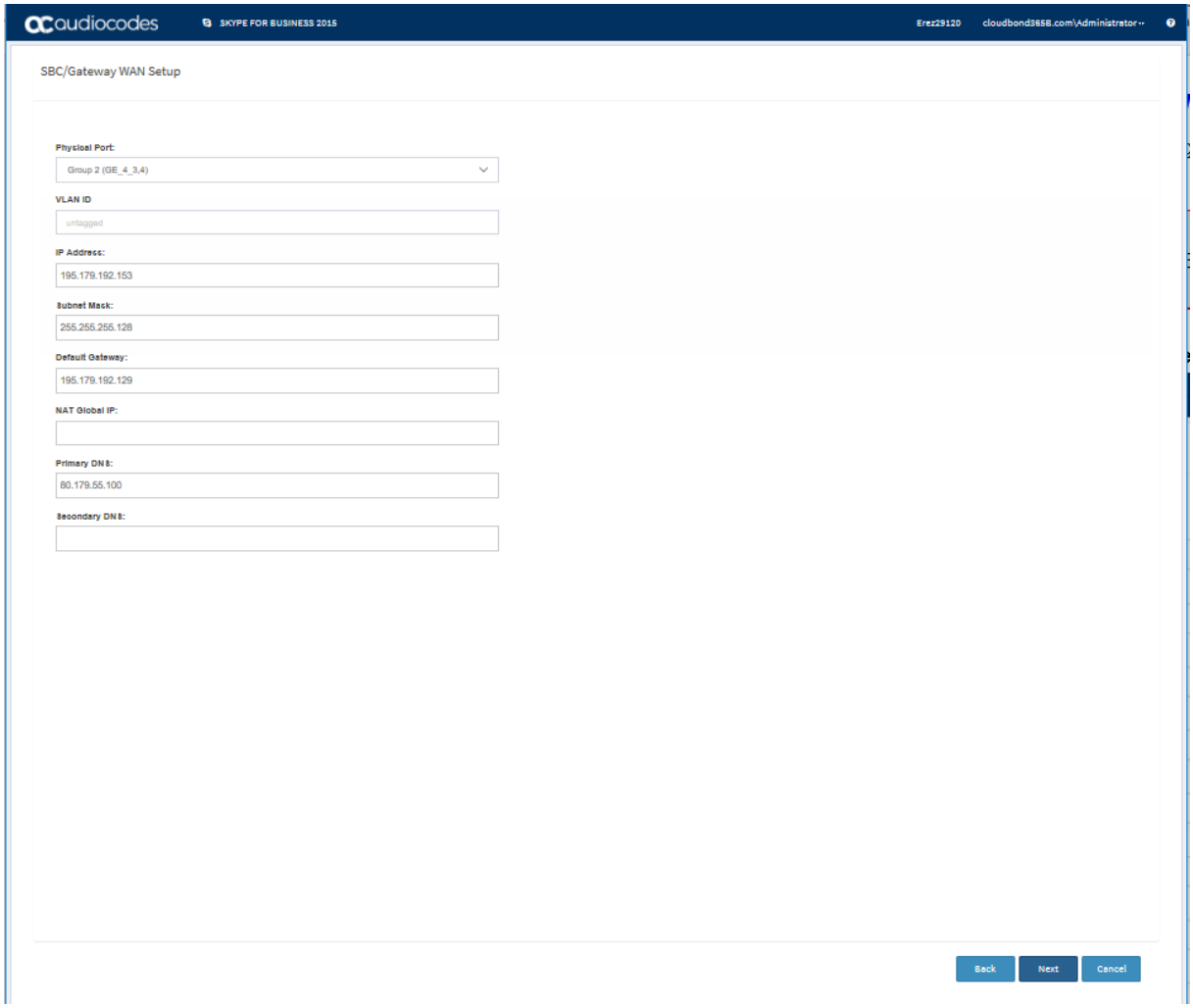
- **Physical Port:** Defines the physical port that should be used for connecting the SBC to the Enterprise LAN (typically to the Ethernet switch). On most devices, two physical ports may be used for Ethernet link redundancy. For example on the Mediant 1000B , the first LAN link should be connected to the Gigabit Ethernet 0/1 port and the backup link should be connected to the Gigabit Ethernet 0/2 port.
- **VLAN ID:** Defines the VLAN ID used on the LAN network interface. When set to empty (untagged) or 1, traffic on the LAN network interface is untagged.
- **IP Address:** Defines the SBC's IP address on the LAN network interface. The IP address should be part of Enterprise LAN and therefore is typically "private" IP address. This address is used for communicating with the IP-PBX and/or Users that reside inside the LAN, as well as for the management (OAM) traffic.
- **Subnet Mask:** Defines the subnet mask of the Enterprise LAN.
- **Default Gateway:** Defines the default gateway of the Enterprise LAN.
- **NAT Global IP** (Target IP Address in NAT Translation Table)**:** This is applicable only when SBC is connected via enterprise router that performs Network Address Translation (NAT). Defines the global IP address (of the Enterprise router) used by SBC when communicating with ITSP (for SIP Trunk application) or IP-PBX (for Hosted IP-PBX application).
- **Primary DNS:** Defines the primary DNS server of the Enterprise LAN. This parameter is mandatory if you use hostname / FQDN for IP-PBX address.
- **Secondary DNS:** Defines the secondary DNS server of the Enterprise LAN. This parameter is mandatory if you use hostname / FQDN for IP-PBX address.

9.2.2 Step 2-2: Configure E-SBC and Gateway WAN Connection

This step describes how to setup the connection of the gateway/SBC application to the Enterprise WAN.

Note: This step is only relevant if you are configuring the E-SBC/gateway parameters.

Figure 9-3: E-SBC and Gateway WAN Setup



➢ **This step defines the following parameters:**

- **Physical Port:** Defines the physical port that should be used for connecting the to the DMZ port on the Enterprise router. On most devices, two physical ports may be used for Ethernet link redundancy. For example, on Mediant 1000B, for "Two ports: LAN and WAN" network topology, the first WAN link should be connected to the Gigabit Ethernet 7/1 port and the backup link should be connected to the Gigabit Ethernet 7/2 port.
- **VLAN ID:** Defines the VLAN ID that is used on the WAN network interface. When set to empty (untagged) or 1, traffic on the WAN network interface is untagged.
- **IP Address:** Defines the IP address on the WAN network interface. The IP address

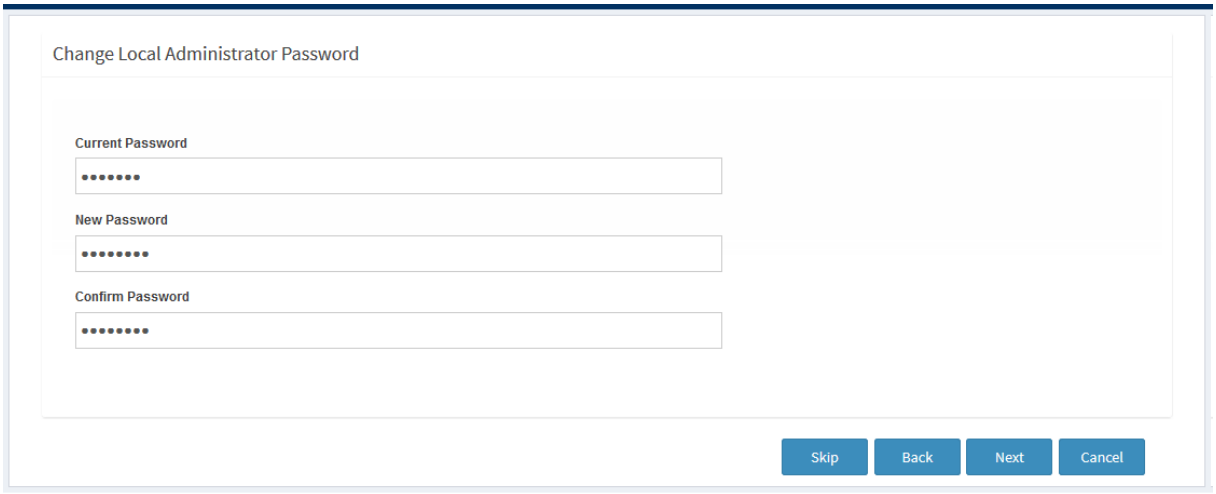
should be "public" (globally routable) and is used for communicating with ITSP and/or IP-PBX that resides outside the LAN. When the WAN network interface is the only interface that exists, it's also used for the management (OAM) traffic.

- **Subnet Mask:** Defines the subnet mask of the WAN network interface.
- **Default Gateway:** Defines the default gateway of the WAN network interface.
- **NAT Global IP** (Target IP Address in NAT Translation Table)**:** This is applicable only when is connected via enterprise router that performs Network Address Translation (NAT). Defines the global IP address (of the Enterprise router) used by when communicating with ITSP (for SIP Trunk application) or IP-PBX (for Hosted IP-PBX application).
- **Primary DNS:** Defines the primary DNS server of the WAN network interface. This parameter is mandatory if you use hostname / FQDN for ITSP / IP-PBX address
- **Secondary DNS:** Defines the secondary DNS server of the WAN network interface. Leave it as empty if there is only one DNS server available.

9.3 Step 3: Change Local Administrator Password

This step describes how to change the password of the local administrator on the SBA.

Figure 9-4: SBA Setup Wizard - Change Local Administrator Password



➢ **To change the local administrator password:**

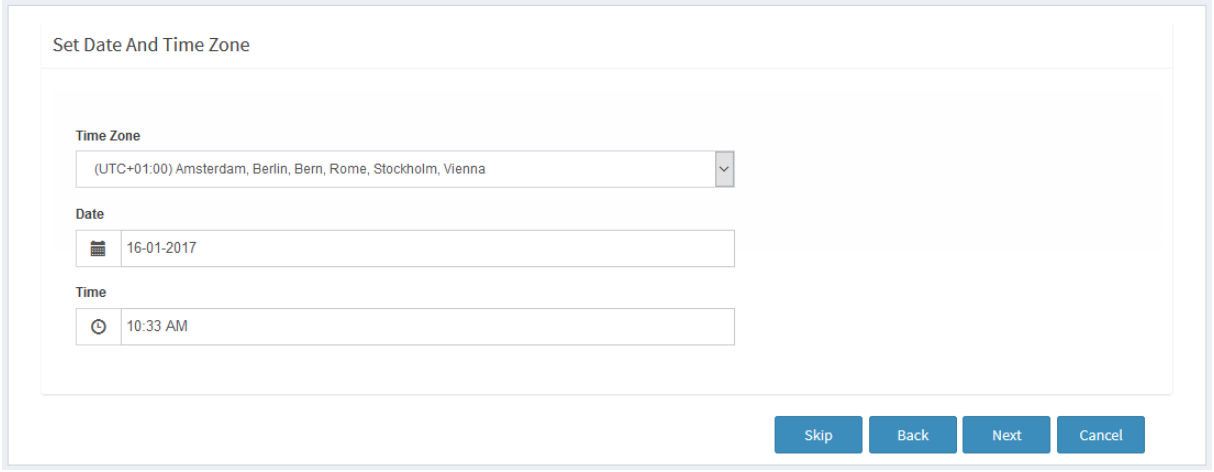
1. Enter the current password of the local administrator.
2. Enter the new password.
3. Confirm the new password.

9.4 Step 4: Set Date and Time Zone

This step describes how to set the date and time zone for the OSN server.

Note: These settings are not synchronized with the E-SBC/gateway clock settings.

Figure 9-5: SBA Setup Wizard - Set Date and Time Zone



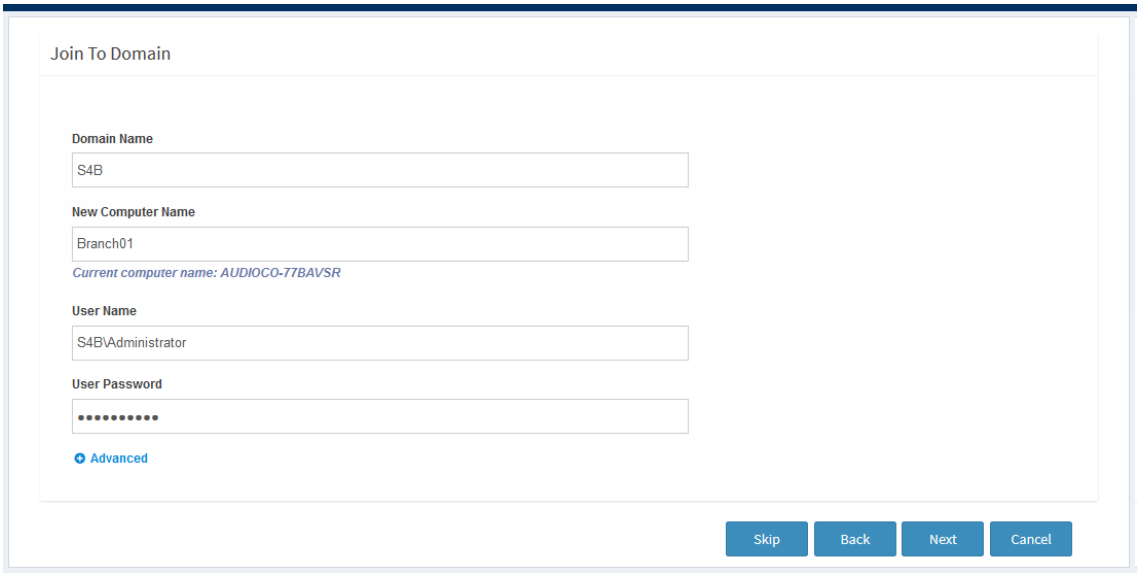
➢ **To set the date and time zone of the SBA server:**

1. Select the Time Zone of the SBA branch device that you are configuring.
2. Set the date and time of the SBA branch device.

9.5 Step 5: Join to the Domain

This step describes how to join the SBA branch to the domain.

Figure 9-6: SBA Setup Wizard - Join to Domain



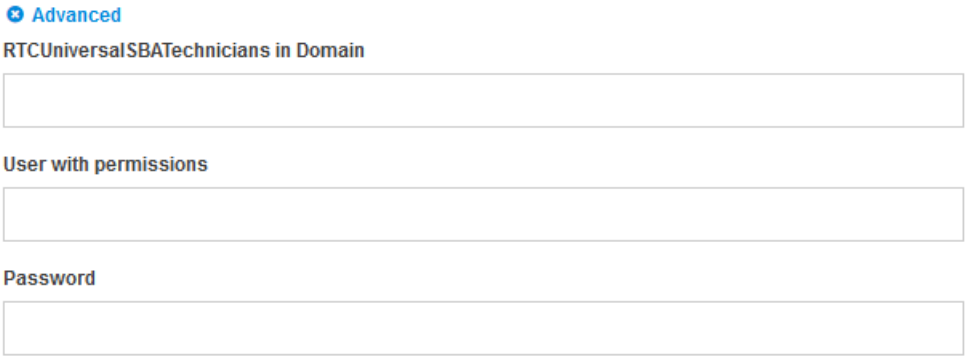
➢ **To join to the domain:**

1. In the 'Domain Name' field, enter the domain name of the SBA branch site.
2. In the 'New Computer Name' field, enter the desired name for the SBA branch site device. The Computer Name string "AUDC" is by default used to identify the appliance.

Note: The computer name must be identical to the Computer Name configured in the AD (see Section 5, Adding SBA to Active Directory).

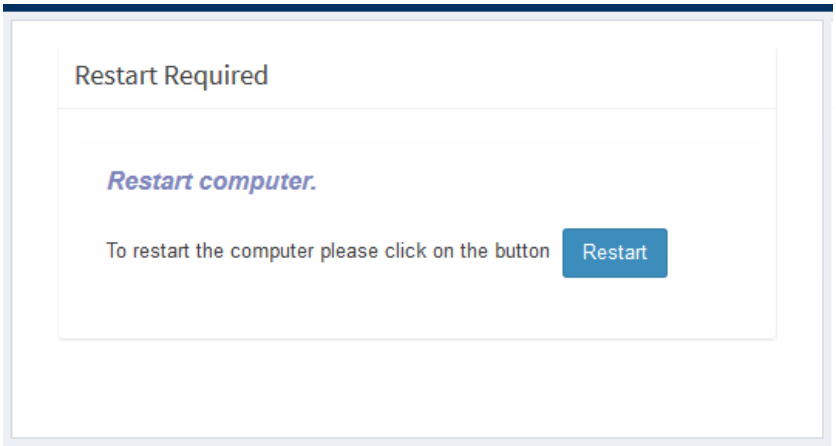
3. In the 'User Name' and 'User Password' fields, enter the domain username and password of the administrator who is authorized for the domain.
4. If you want to add the RTCUniversalSBATechnicians group domain, do the following:
   a. Click **Advanced**:

Figure 9-7: SBA Setup Wizard - Join to Domain (Advanced)



   b. In the 'RTCUniversalSBATechnicians in Domain' field, enter the group domain name.
   c. In the 'User with permissions' field, enter the username.
   d. In the 'Password' field, enter the password.
5. Click **Next**; you are prompted to restart the server:

Figure 9-8: SBA Setup Wizard - Restart SBA Server

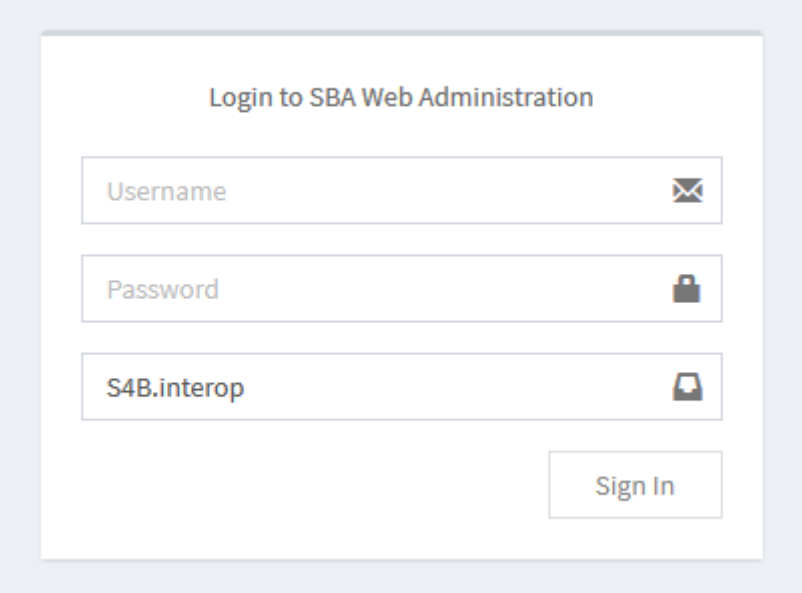


6. Click **Restart** to restart the SBA server; a message appears informing you that the SBA server is restarting.

9.6 Step 6: Login to Domain

This step describes how to login to the domain.

Figure 9-9: SBA Setup Wizard - Login to Domain

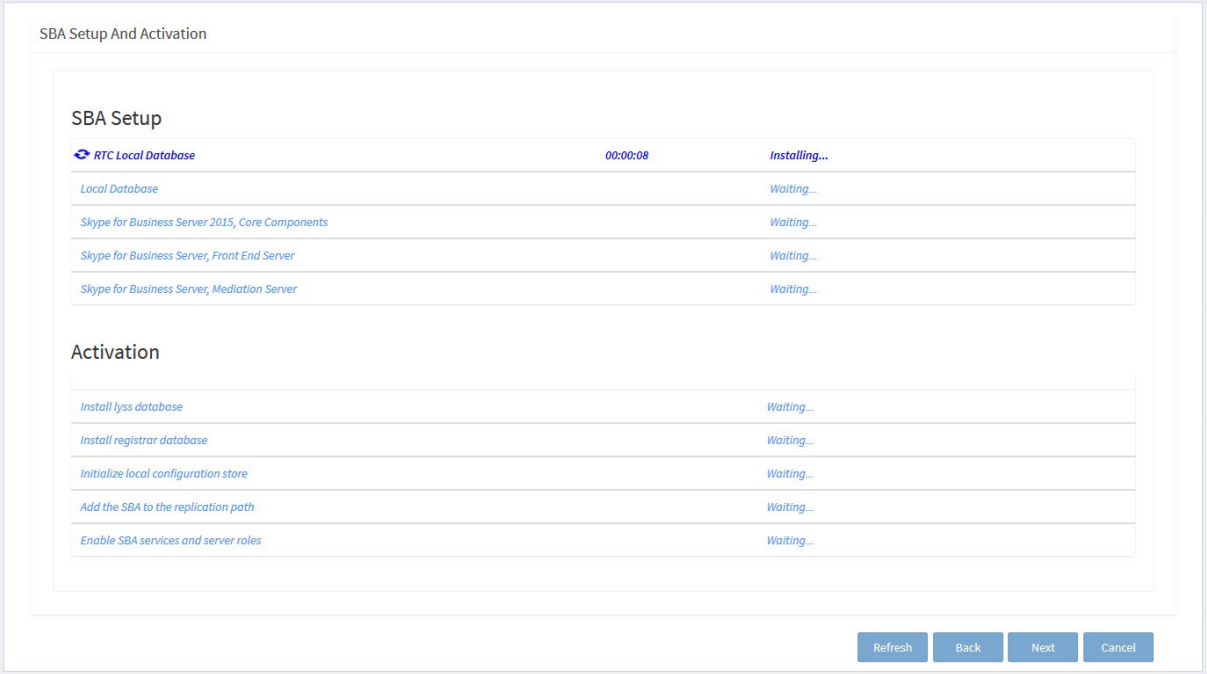


➢ **To login to the domain:**

1. Enter the domain administrator credentials, as configured in Section 9.5.
2. Click **Sign In**.

   Once you login to the domain the following screen is displayed showing the progress of the installation of the components of the SBA setup:

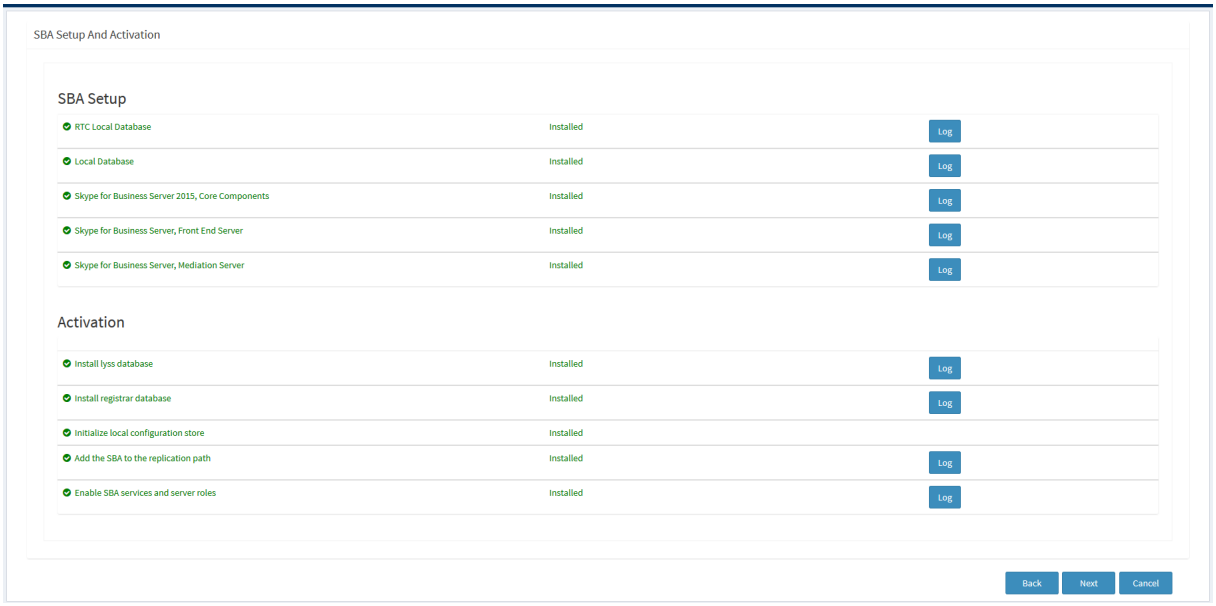
Figure 9-10: SBA Setup Wizard - Installation Progress



A timer adjacent to each component shows how long the installation process has taken.

Once all of the SBA components have been successfully installed, they are all displayed as shown in the screen below:

Figure 9-11: SBA Setup Wizard - Installation Completed



Note that you can view logs and reports at each stage of the installation.

3. Once the SBA branch appliance has installed of the components (all components are displayed in green as shown in the screen above), click **Next**.

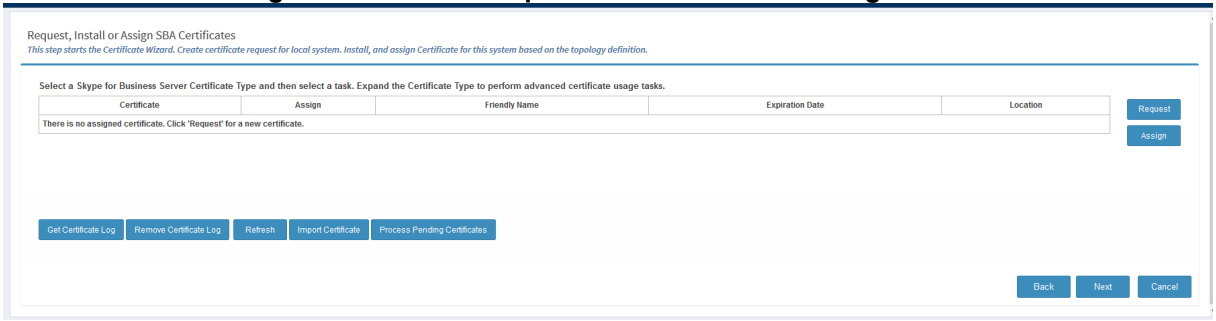
9.7 Step 7: Configure SBA Certificates

This step describes how to configure the certificates that are used to secure the connection between the SBA branch appliance and the Skype for Business server in the Data center.

You can implement certificates by using one of the following methods:

- Generating a Certificate Signing Request (CSR)
- Importing an existing certificate. See Importing an Existing Certificate on page 64.

Figure 9-12: SBA Setup Wizard - Certificate Configuration



The main certificate configuration screen above includes the following options:

- **Request:** Send a CSR request to a CA.
- **Assign:** Assign an existing certificate to the SBA appliance.
- **Get Certificate Log:** Open the log file for the selected certificate which includes the processing information for the certificate's deployment on the Skype for Business server.
- **Remove Certificate Log:** Remove the log file for the selected certificate from the installation certificate directory.
- **Refresh:** updates the list of certificates in the certificate list.
- **Import certificate:** import an existing certificate that has been processed by your enterprise's CA

9.7.1 Generating a Certificate Signing Request (CSR)

There are two methods that you can use to generate a certificate request:

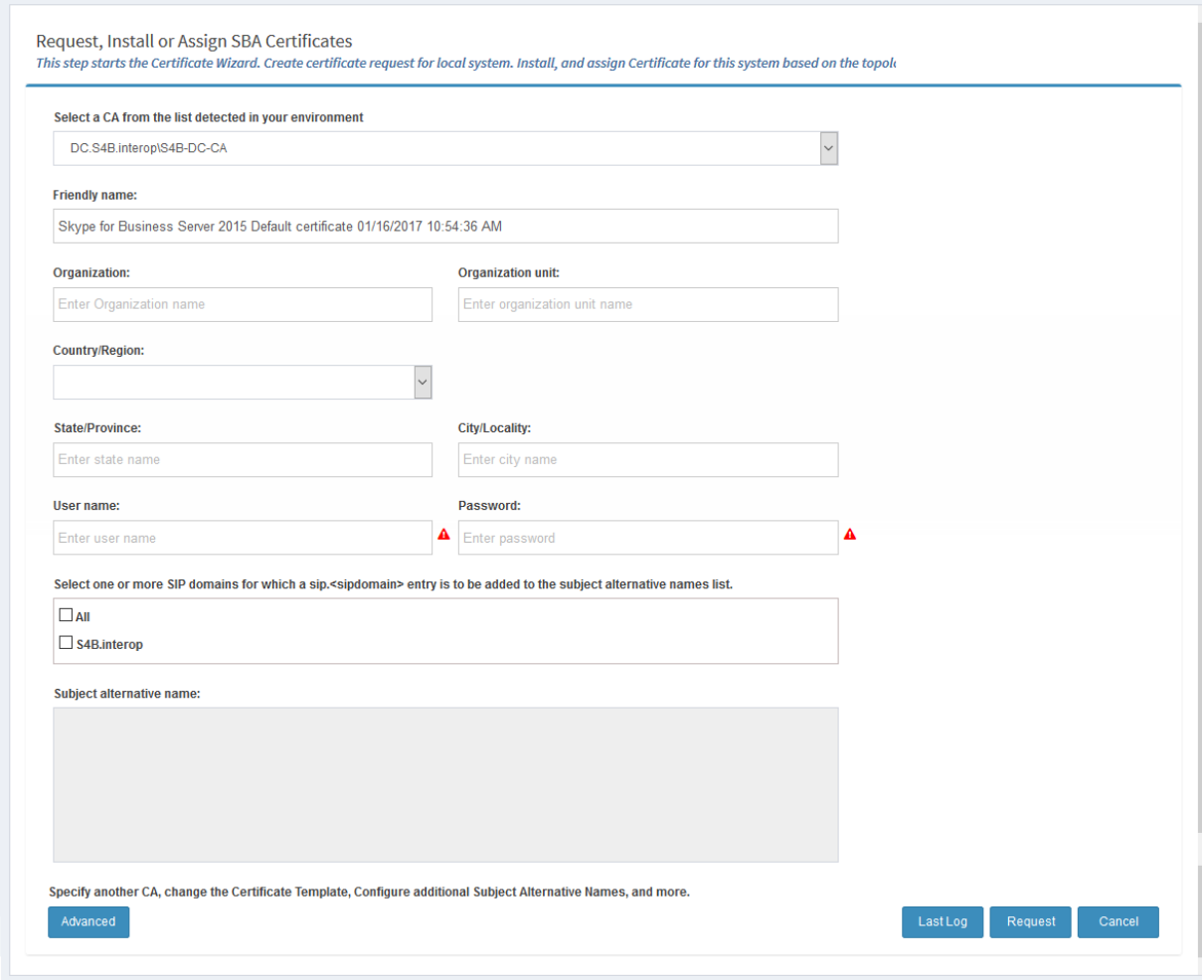
- Send the request immediately to an Online Certificate Authority.
- Prepare the request Offline and then send the requests later.

When both options are selected, you can monitor the status of the requests in the Wizard.

➢ **To generate a Certificate Signing Request (CSR) :**

1. Click **Request** to send a CSR request to the Microsoft CA authority.

Figure 9-13: SBA Setup Wizard - Certificate Signing Request (CSR)



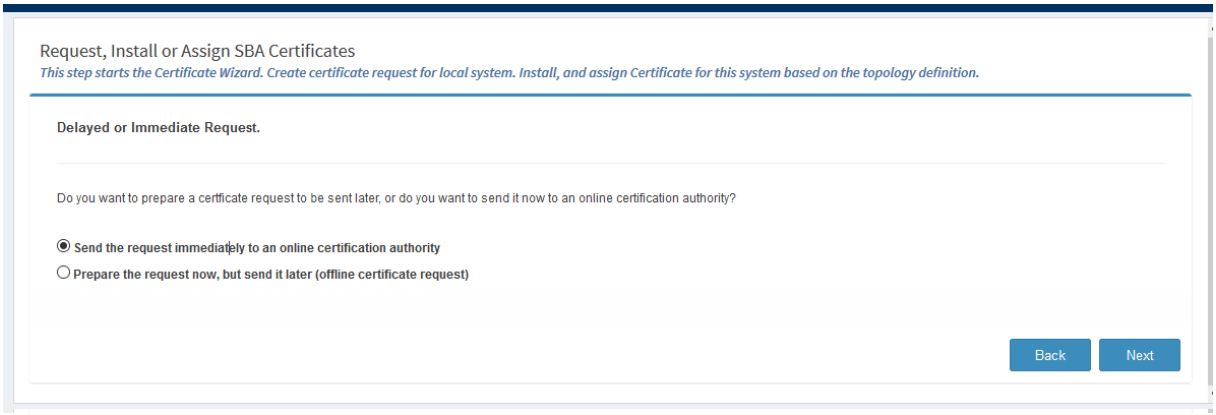
2. Enter the details of the CSR request:
   - **Friendly Name:** The name through which the certificate will be accessed (usually the fully-qualified domain name, e.g., www.domain.com or mail.domain.com).
   - **Organization:** The legally registered name of your organization/company.
   - **Organizational unit:** The name of your department within the organization (frequently this entry will be listed as "IT," "Web Security," or is simply left blank).
   - **City/locality:** The city in which your organization is located.
   - **State/province:** The state in which your organization is located.
   - **Country/region:** If needed, you can find your two-digit country code in our list.
   - **User name** and **Password** for the user who is authorized to request an online certificate.
   - **SIP Domain:** The SIP domain name is used when communicating with the Skype for Business Server. The domain name is used in the following SIP message headers when communicating with the SBC or Gateway application:
     - Subject name
     - Subject alternative name
     - Subject Alternative Name -Alternative name for the SBA appliance in the domain.

     This name is the Fully Qualified Domain Name (FQDN) of the E-SBC (also configured in the Topology Builder in Section 6).
3. Do one of the following:

a. If you wish to send the request immediately to an Online Certificate Authority, proceed to step 6.
b. If you wish to prepare the request and send it offline using Microsoft Windows or other tools, click the **Advanced** button and proceed to Step 4 below.

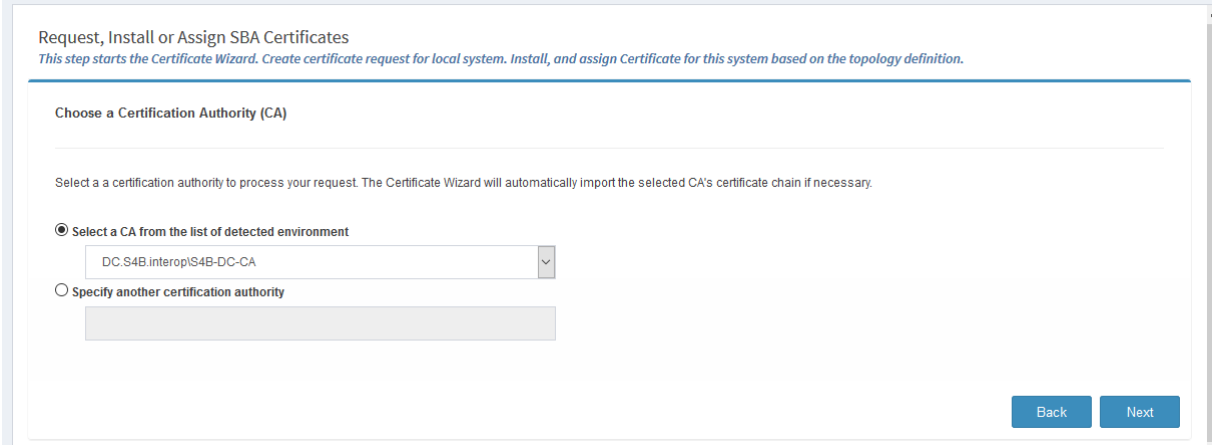
4. Click **Advanced.**

Figure 9-14: SBA Setup Wizard - Advanced Certificate Options



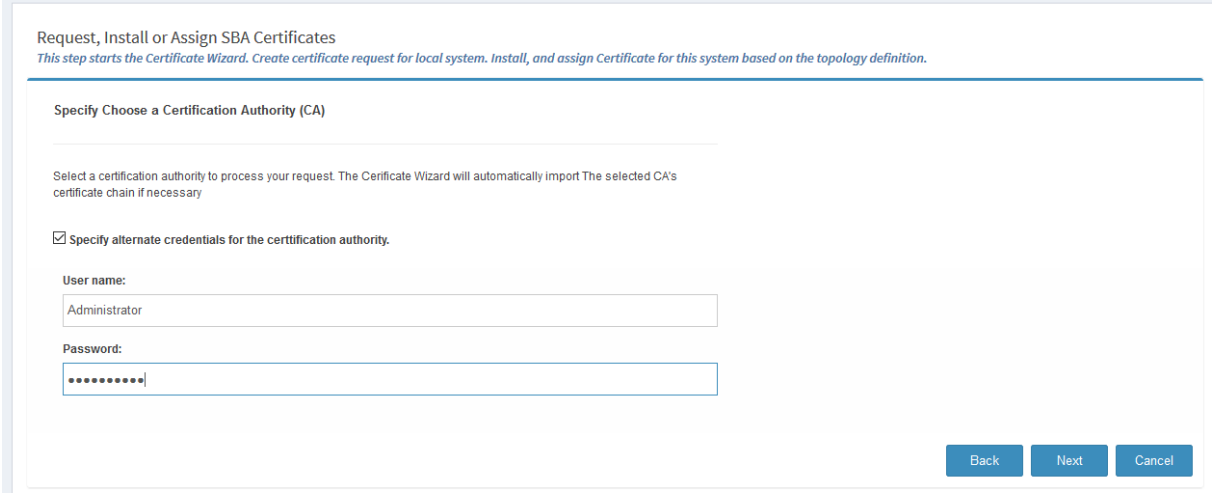
5. Select the option **Prepare the request now; however send it later (offline certificate request)**; the CSR request is sent manually by the administrator (Skip to Step 8).
6. Click **Next**; if you selected to request the certificate immediately, the following screen is displayed:

Figure 9-15: Online Certificate Request



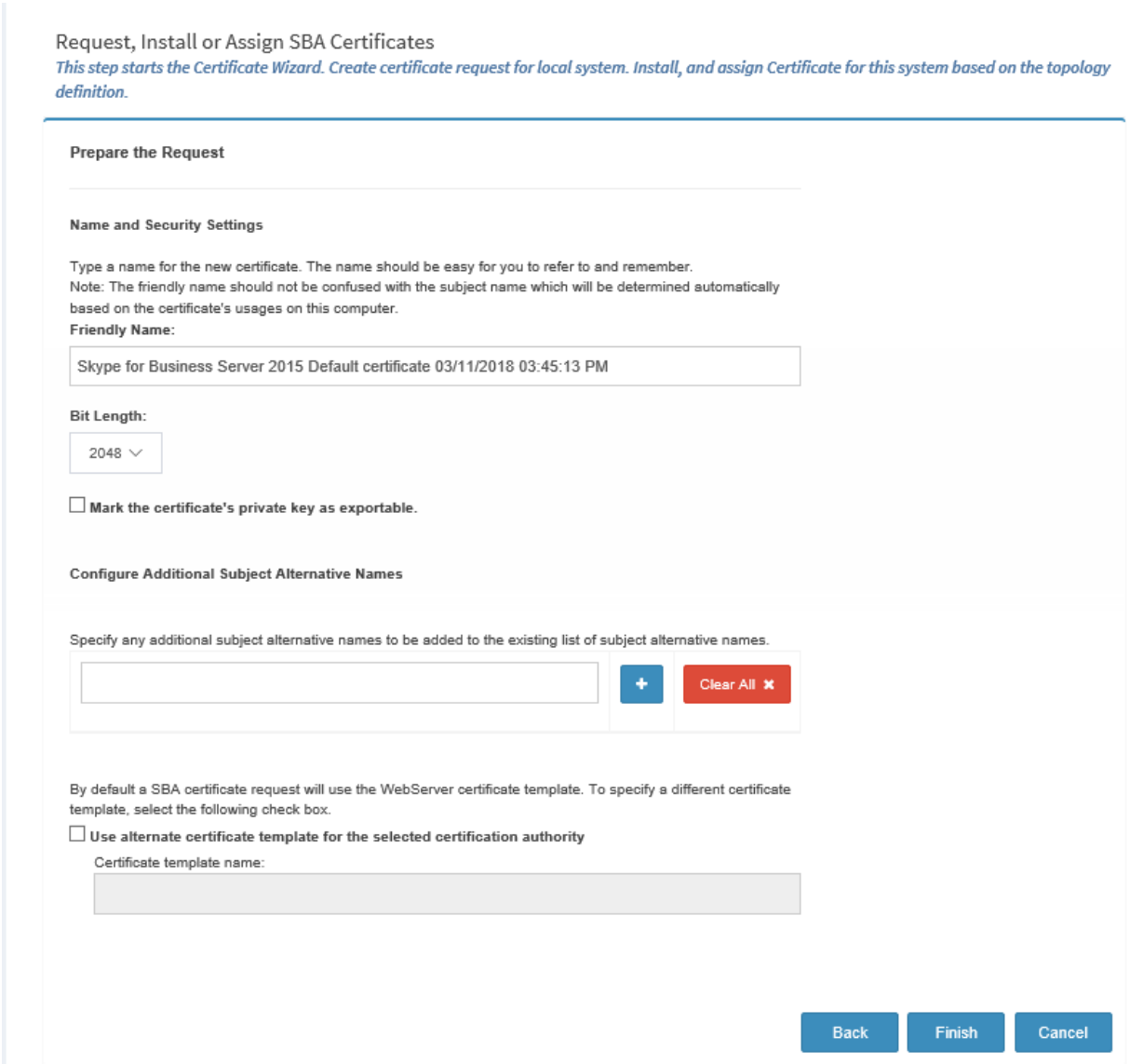
7. From the drop-down list box, select the desired CA from which to request a certificate or specify another CA in the text box and click **Next**.

Figure 9-16: Select CA

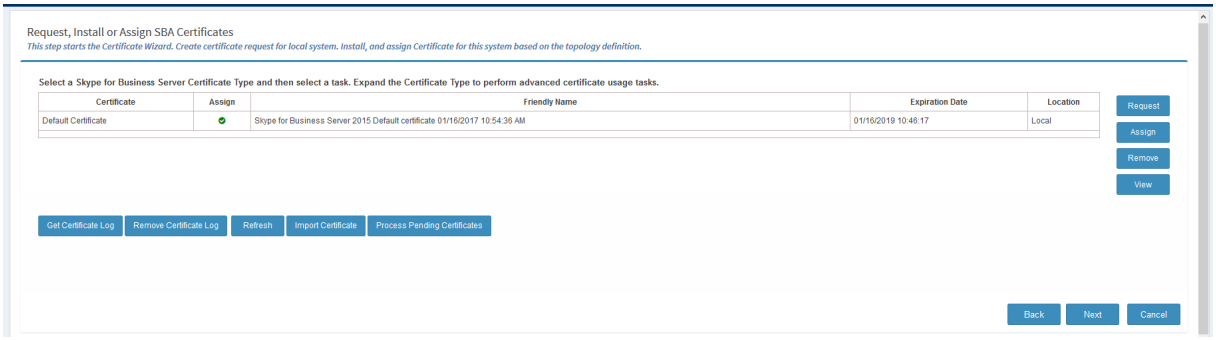


8. Enter the user name and Password for the administrator who is authorized to request a certificate, select the "Specify alternate credentials authority" check box, and click **Next**; the following screen is displayed:

Figure 9-17: Prepare the Request



9. Enter the Friendly Name and Security Settings for the certificate:
   - Enter the Bit Length
   - Mark the certificate's private key as exportable
   - Configure additional alternative names
   - Enter the Certificate Template name if the default is not used
10. Click **Finish**; a summary of the certificate request is displayed:



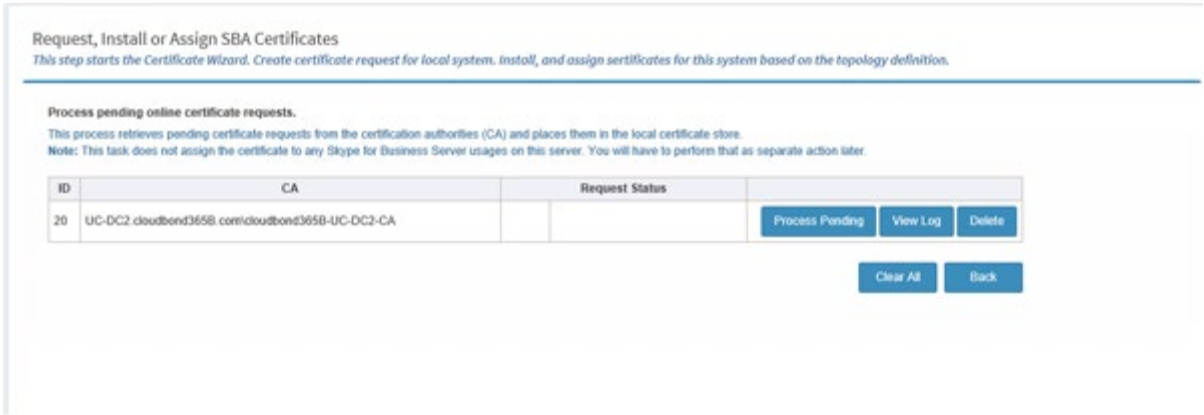
9.7.1.1 Pending Requests

When the Certificate Authority has not yet processed the Certificate request, it is in the pending state. When the pending certificate is processed, it is retrieved from the CA and copied to the local certificate store on the SBA server.

➢ **To view currently pending certificates and process them:**

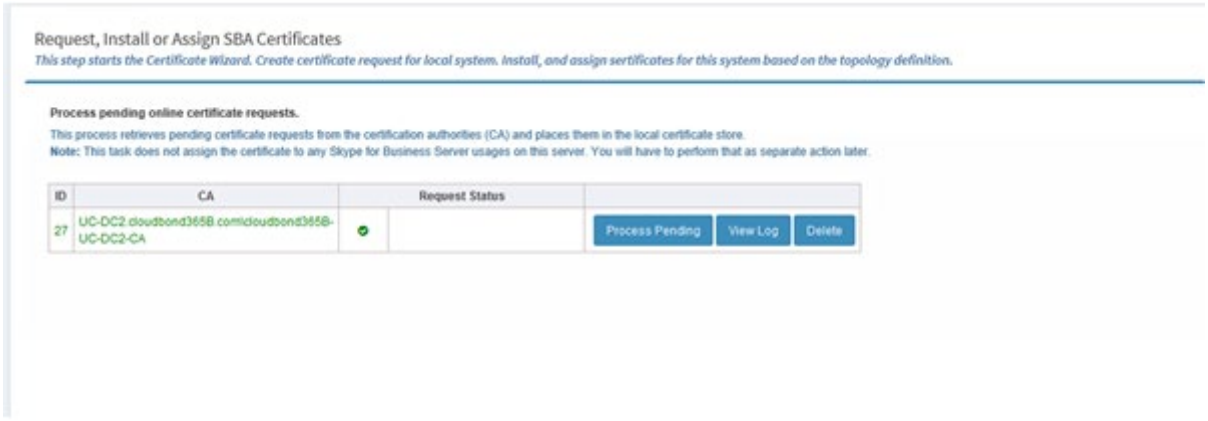
1. Click **Process Pending Certificates**.

Figure 9-18: CSR Pending



2. Click **Process Pending** button to process the pending certificate as described above.

Figure 9-19: Certificate Process Pending



Once the pending request has been processed, it is highlighted in green as shown in the figure above.

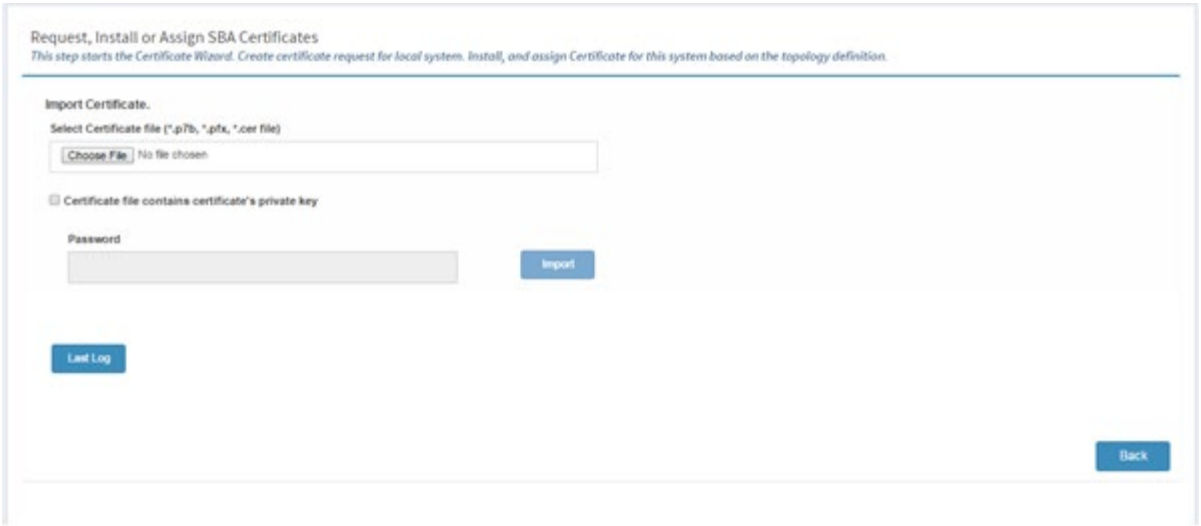
9.7.2 Importing an Existing Certificate

This procedure describes how to import a certificate that you generated offline with an external CA and saved to your PC.

➢ **To import an existing certificate:**

1. Click the **Import Certificate** button; the following screen is displayed:

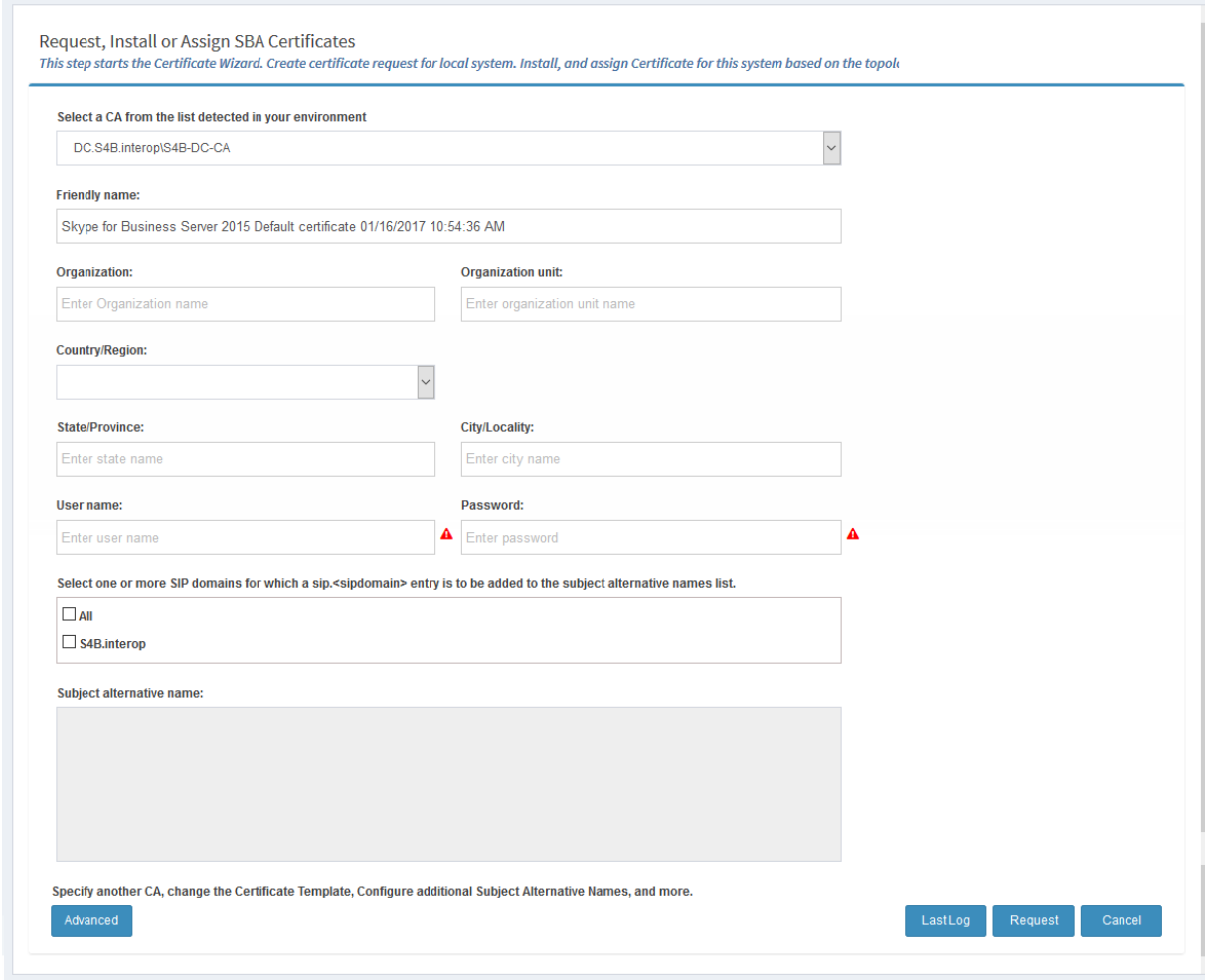
Figure 9-20: Importing Certificates



2. Click **Browse** to browse to the certificate that you wish to import. The valid formats for importing are .p7b, .pfx and .cer files.
3. (Optional) Select the "Certificate file contains certificate's private key" check box to include a private key with the certificate and then enter the Password (passphrase) key for the private key.

4. Click **Import**.

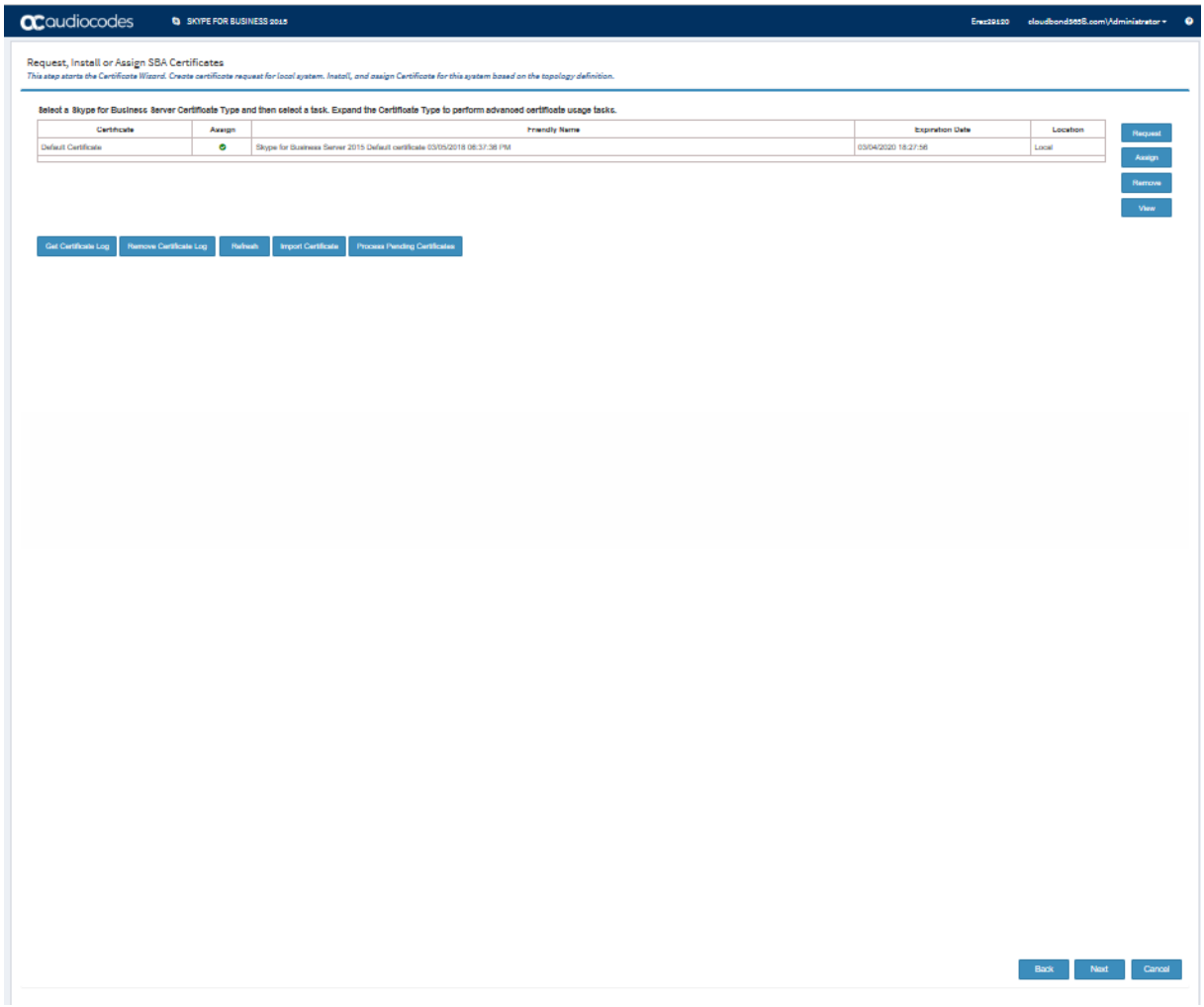
Figure 9-21: Import Certificate File



9.7.3 Assigning a Certificate

Once you have issued a CSR request to a Certificate Authority and the request has been processed (as shown in the figure below), it is automatically assigned. If however, you already have a list of other certificates that you later wish to reassign to the SBA, see the procedure below.

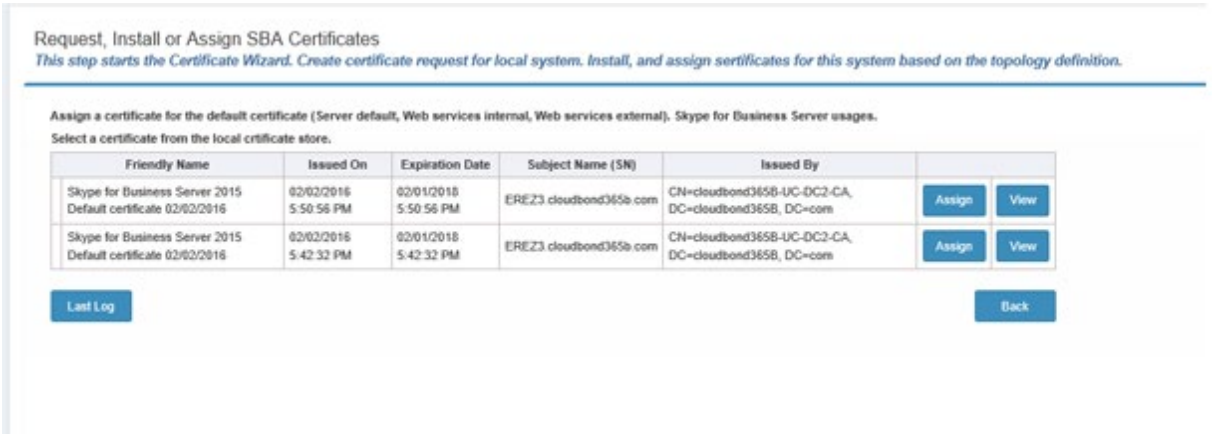
Figure 9-22: Assigning a Certificate



➢ **To assign a certificate to the SBA installation:**

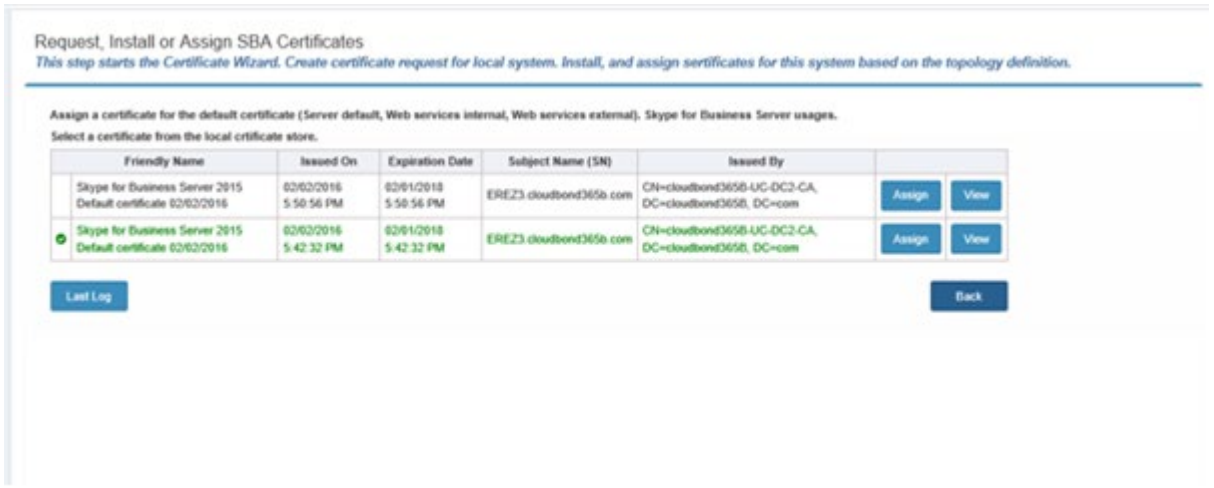
1. Click **Assign**; the following screen is displayed:

Figure 9-23: Assigning a Certificate



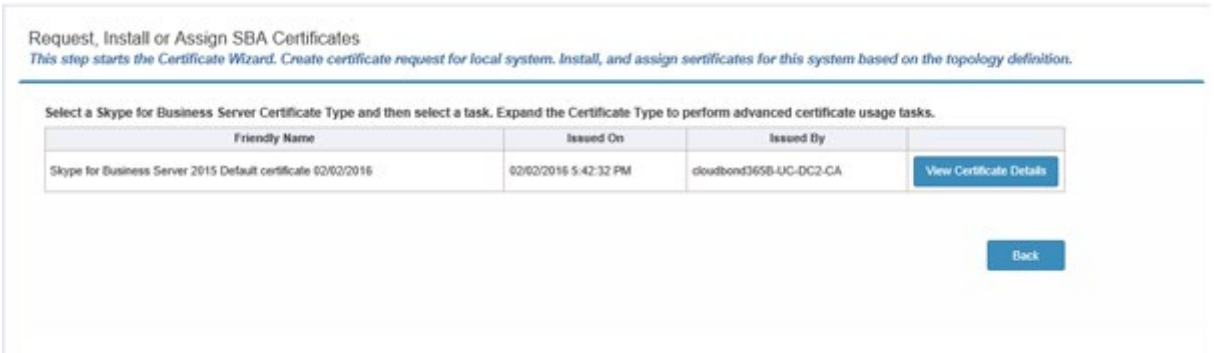
2. Click the **Assign** button adjacent to the certificate that you wish to install on the SBA; the assigned certificate is displayed in green as shown in the figure below:

Figure 9-24: Assigned Certificate



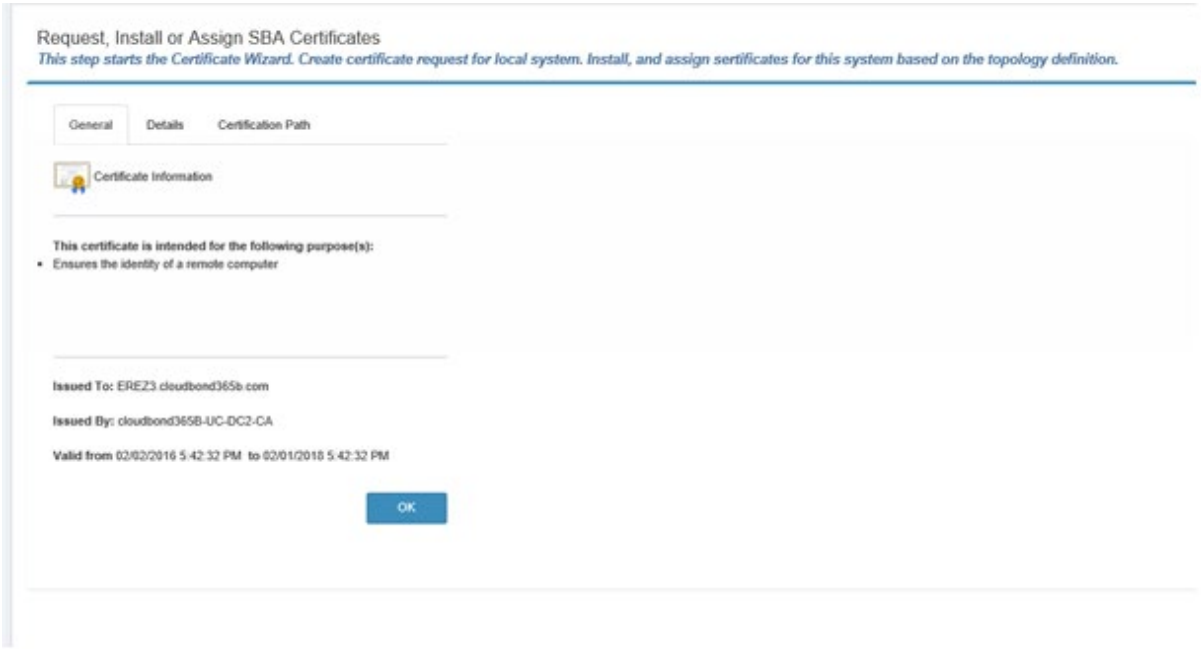
3. Click **View** to view the details of the certificate.

Figure 9-25: View Certificate Details Button



4. Click the **View Certificate Details** button to view the details of the certificate.

Figure 9-26: View Certificate Details

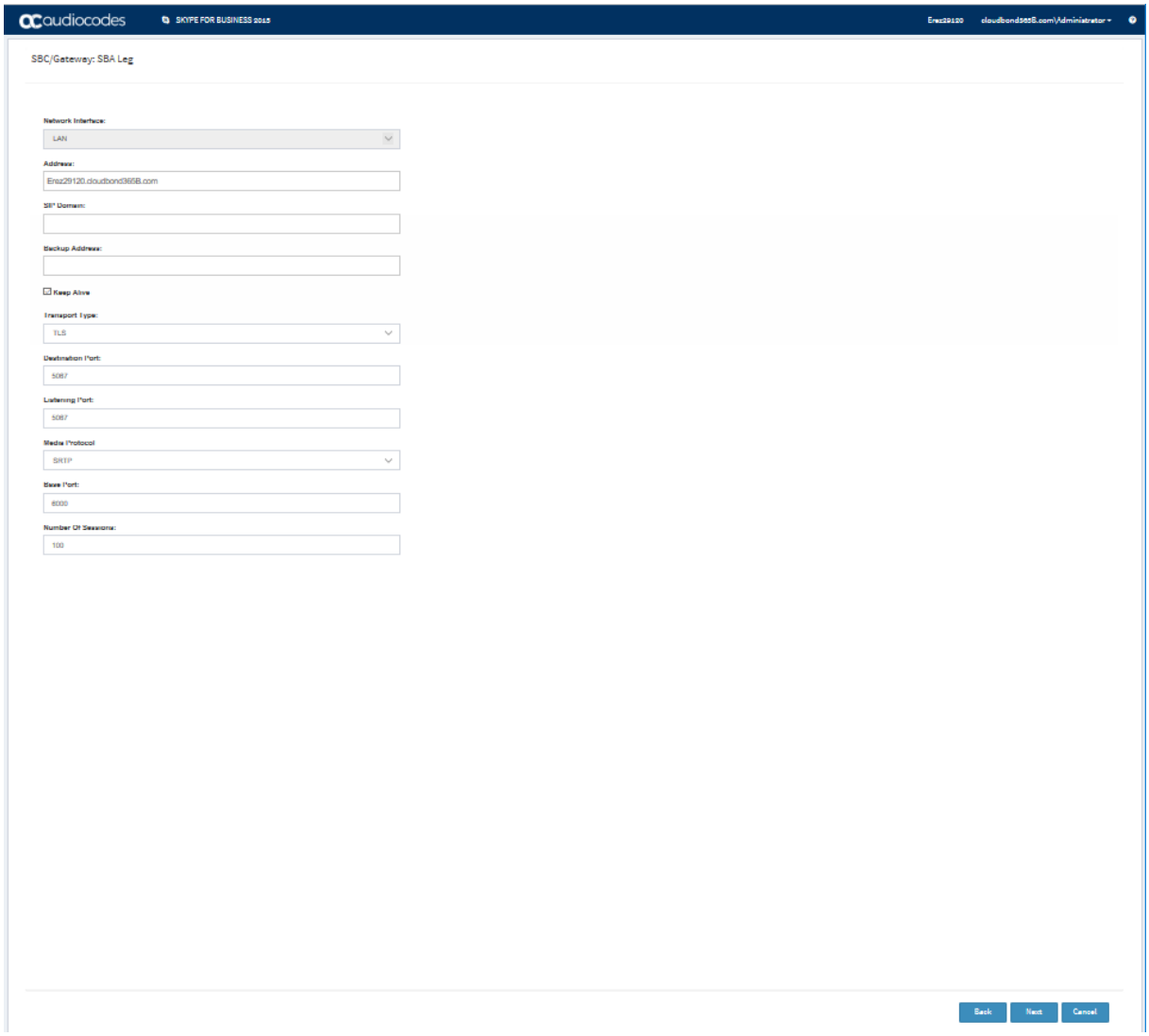


9.8 Step 8: Configure SBC/Gateway SBA Leg

This step describes how to configure the connection between the SBA and the E-SBC/gateway application. This step creates the Proxy Set and IP Group for the SBA connection with the E-SBC/gateway application.

Note: This step is only relevant if you chose to configure the SBC/gateway at the beginning of the wizard.

Figure 9-27: SBC/Gateway SBA Leg



➢ **This step includes the configuration of the following parameters:**

(Note that the equivalent parameter in the device's Web server is indicated in brackets).

- **Network Interface:** Shows the Network Interface that is used for communicating with the SIP Trunk.
- **Address** (Proxy Address table)**:** Defines the IP address or FQDN of the SBA device. This address is configured in the Proxy Sets "Proxy Address" table.
- **SIP Domain:** (SIP Group Name or Gateway Name)**:** Defines the SIP domain name that is used when communicating between the SBA and SBC. The domain name is used in the following SIP message headers when communicating with the Gateway and :
  - for outbound calls: in Request-URI and To headers
  - for inbound calls: in From header

  This name is the Fully Qualified Domain Name (FQDN) of the E-SBC (also configured in the Topology Builder in Section 6, Step 9).
- **Backup Address:** Defines the FQDN of the Skype for Business Front End server. If the Front End has only one address, leave this field empty. Used in the event where the SBA device Address (defined above) does not respond.
- **Keep Alive** (Proxy Keep-alive)**:** Enables the periodic keep-alive check of multiple SIP Trunk addresses.
- **Transport Type** (SIP Transport Type)**:** Defines the SIP transport type for SBA-E-SBC/gateway connection.
- **Destination Port** (SIP Destination Port)**:** Defines the SIP port used by the SBA-E-SBC/gateway connection.
- **Listening Port** (TLS Port)**:** Defines the port used for SBA-E-SBC/gateway connection.
- **Media Protocol** (Media Security)**:** Defines the media protocol type ("SRTP" is equivelant to Media Security enabled in device Web).
- **Base Port** (Port Range Start)**:** Defines the first media port.
- **Number of Sessions** (Number of Media Session Legs)**:** Defines the number of media sessions supported by the E-SBC. Note: The E-SBC allocates 10 media ports for each session. For example, if the base media port is 6000 and 100 sessions are supported, actual "range" of media ports allocated by the E-SBC is 6000-6999.

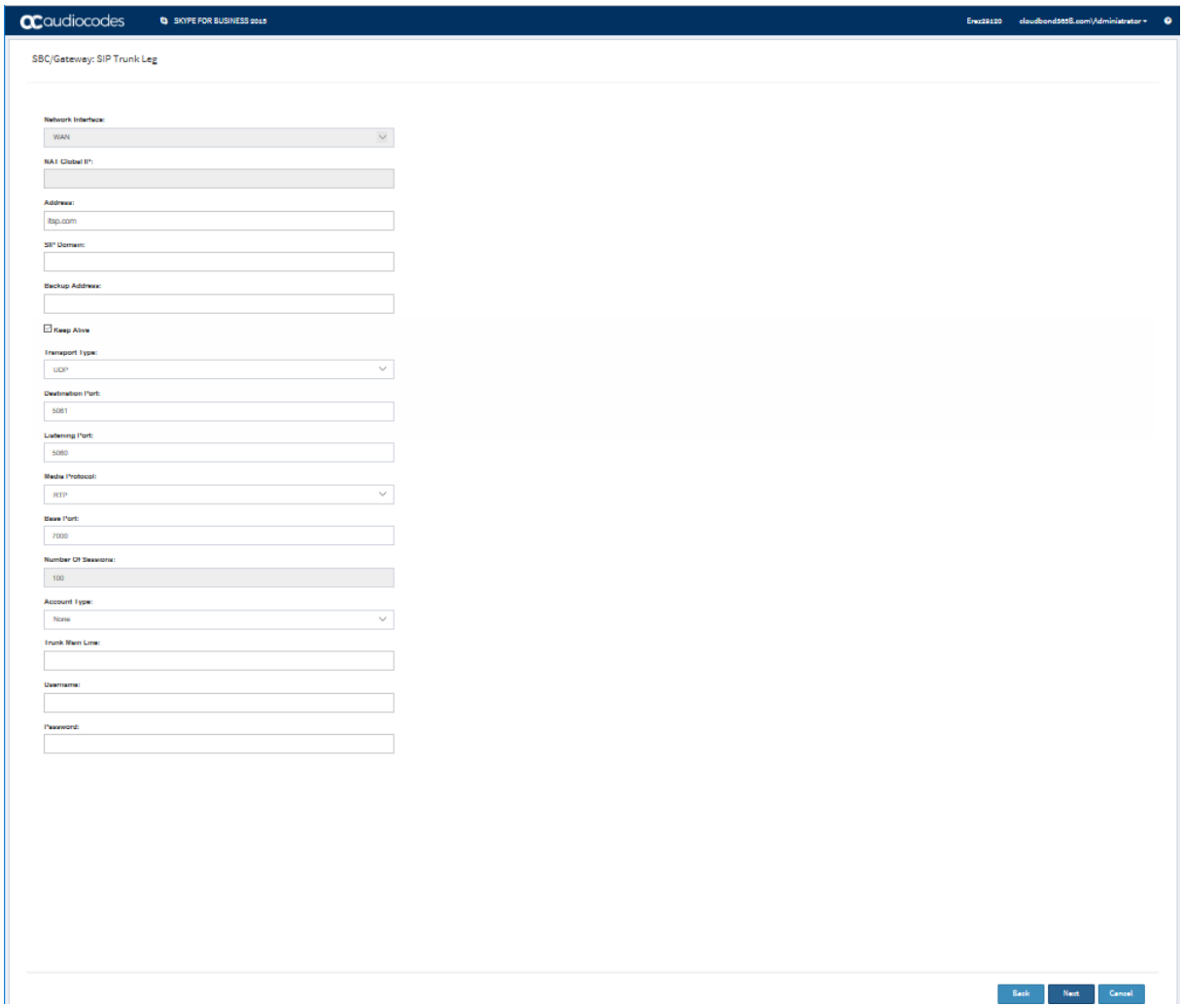
9.9 Step 9: Configure SIP Trunk/IP-PBX Leg

This step describes how to configure the connection between the E-SBC and the SIP trunk or IP-PBX. The example figure below shows a SIP Trunk configuration.

Note: This step is only relevant if you are configuring the E-SBC/gateway parameters and have applied either a SIP Trunk or IP-PBX template in the network topology (see Section 11.2).

The figure below shows an example for a SIP Trunk Configuration (for IP-PBX templates this screen is titled "SBC: SIP Trunk Leg".

Figure 9-28: SIP Trunk Configuration



➢ **This step includes the configuration of the following parameters:**

(Note that the equivalent parameter in the device's Web server is indicated in brackets.)

- The following parameters configure the SIP Trunk address and communication protocol details:
  - **Network Interface:** Shows the Network Interface that is used for communicating with the SIP Trunk.
  - **NAT Global IP:** Shows the global IP address (of the Enterprise router) used

when communicating with the SIP Trunk. Applicable only when E-SBC is connected to the router that performs Network Address Translation (NAT).

Note: The Enterprise router must be configured to "port forward" all VoIP traffic from the SIP Trunk (that resides in WAN) to the E-SBC. The exact port forwarding configuration is shown in the ini file configuration summary at the end of the Wizard process. This consists of the E-SBC address, SIP listening port (e.g. 5060) and a range of media ports defined below (e.g. 6000-6999).

- **Address** (Proxy Address table)**:** Defines the IP address or FQDN of the SIP Trunk.
- **Backup Address**: The Backup Address is the FQDN of the Skype for Business FE server. Used in the event where the SIP Trunk address (defined above) does not respond.
- **SIP Domain** (SIP Group Name or Gateway Name)**:** Defines the SIP domain name that is used when communicating between the E-SBC and the SIP Trunk or IP-PBX. The domain name is used in the following SIP message headers:
  - for outbound calls: in Request-URI and To headers
  - for inbound calls: in From header

  This name is the Fully Qualified Domain Name (FQDN) of the E-SBC (also configured in the Topology Builder in Section 6).
- **Keep Alive** (Proxy Keep-alive)**:** Enables the periodic keep-alive check of multiple SIP Trunk addresses.

- The following parameters configure SIP ports and transport type used when communicating with the SIP Trunk.
  - **Transport Type** (SIP Transport Type)**:** Defines the SIP transport type for SIP Trunk.
  - **Destination Port** (SIP Destination Port)**:** Defines the SIP port used by the SIP Trunk.
  - **Listening Port** (TLS Port)**:** Defines the SIP port used by the E-SBC when communicating with SIP Trunk.

  Note: For the "One port: WAN" network topology, the E-SBC must use different Listening Ports when communicating with the IP-PBX and SIP Trunk.
- The following parameters configure Media protocol type (RTP/SRTP) and ports used by the E-SBC when communicating with the IP-PBX:
  - **Media Protocol** (Media Security)**:** Defines the media protocol type ("SRTP" is equivelant to Media Security enabled in device Web).
  - **Base Port** (Port Start Range)**:** Defines the first media port.
  - **Number Of Sessions** (Number of Media Session Legs)**:** Defines the number of media sessions supported by the E-SBC.

  Note: The E-SBC allocates 10 media ports for each session. For example, if the base media port is 6000 and 100 sessions are supported, actual "range" of media ports allocated by the E-SBC is 6000-6999.
- The following parameters configure E-SBC registration on the SIP Trunk:
  - **Enable Registration** (Enable Registration)**:** Defines whether the E-SBC should perform registration on the SIP Trunk.
  - **Trunk Main Line:** Defines "leading number" assigned by the SIP Trunk. Many SIP Trunks use the same value for Trunk Main Line and Username parameters. For example, the IP-PBX registers this number on the softswitch on behalf of all its users.
  - **Username** (User Name)**:** Defines the SIP authentication username (as provided by the SIP Trunk).
  - **Password** (Password)**:** Defines SIP authentication password (as provided by the SIP Trunk).

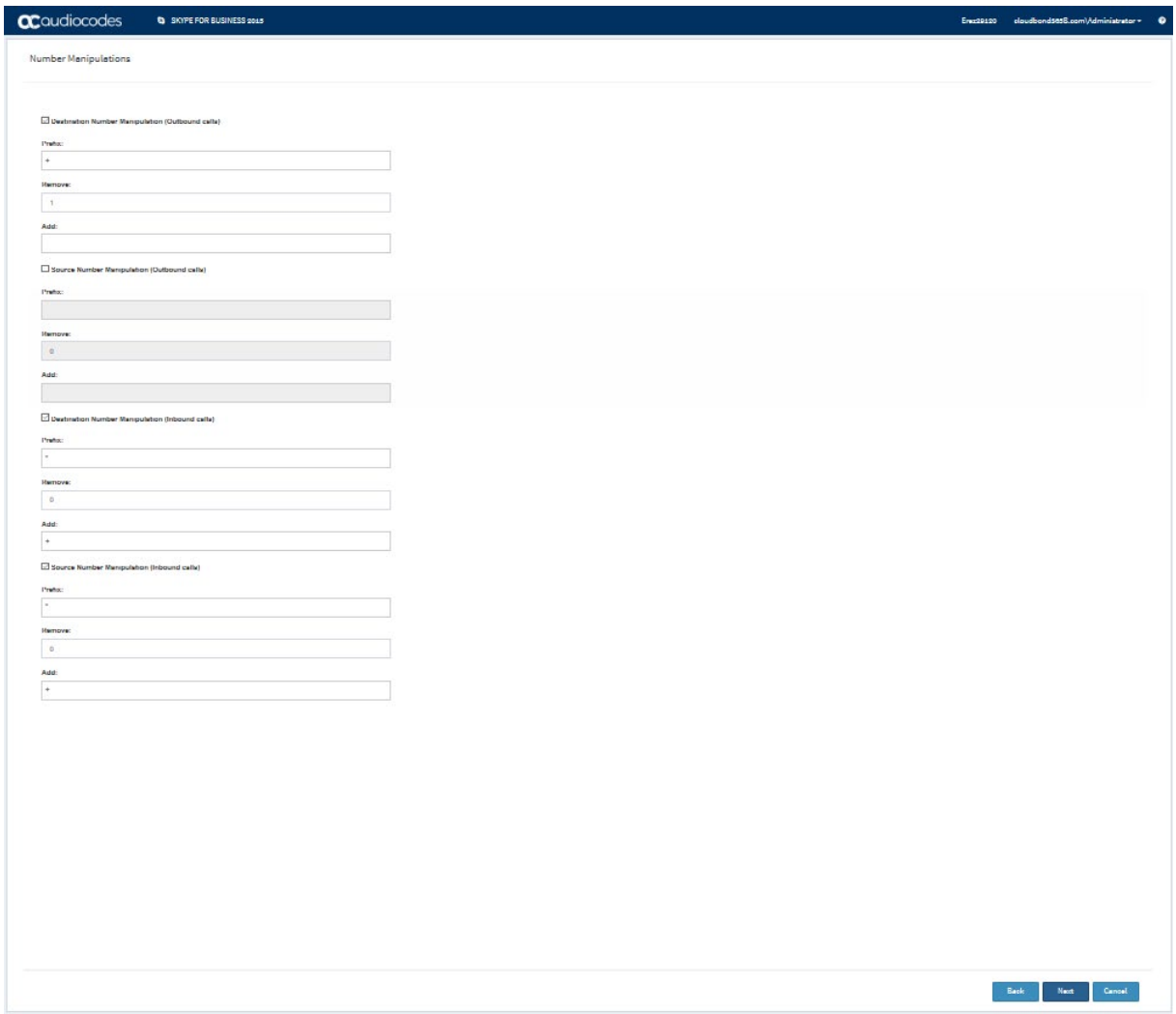
9.10 Step 10: Configure Number Manipulation

This step configures number manipulations that modify caller / callee number for calls that pass through the E-SBC. This step is very important and must be adapted to your specific setup, because typically IP-PBX and ITSP use different numbering plans (e.g. IP-PBX may use 10-digit number format while ITSP uses a 7-digit format).

For each call "direction" (outbound / inbound), you may define different manipulation rules for caller (source) and callee (destination) numbers.

Note: This step is only relevant if you are configuring the E-SBC/gateway parameters.

Figure 9-29: Number Manipulations



You can configure number manipulation rules for the following (select the check box adjacent to the desired set):

- Destination Number (Outbound calls)
- Source Number (Outbound calls)
- Destination Number (Inbound calls)
- Source Number (Inbound calls)

➢ **Each of the above manipulation rules consists of the following three parameters:**

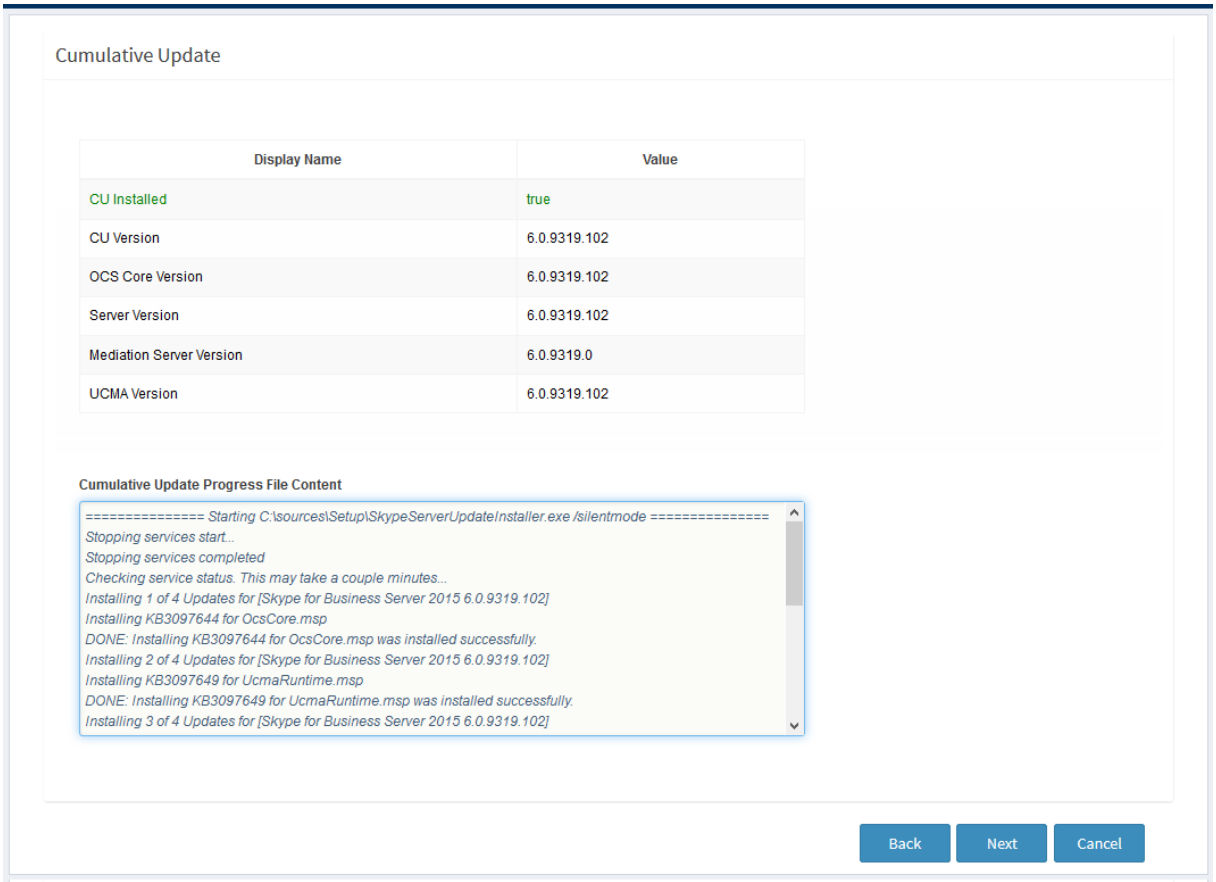
- **Prefix:** Defines a prefix (digits in the beginning of the number) for which manipulation is applied. If set to "*", manipulation is applied to all numbers.
- **Remove:** Defines the number of digits to be removed from the beginning of the number. If set to "0", no digits are removed.
- **Add:** Defines a new "prefix" to be added to the beginning of the number. If set to empty, no prefix is added.

  For example, if Prefix is "+972", Remove (digits) is "4" and Add is "0", then:
  - number "+97239764000" is changed to "039764000"
  - number "039764001" is left unchanged

9.11 Step 11: Run Cumulative Updates

The Wizard process includes the installation of Microsoft Skype for Business Server Cumulative Updates (CUs). When the Wizard completes, a, a screen similar to the following is displayed:

Figure 9-30: SBA Setup Wizard - Cumulative Updates

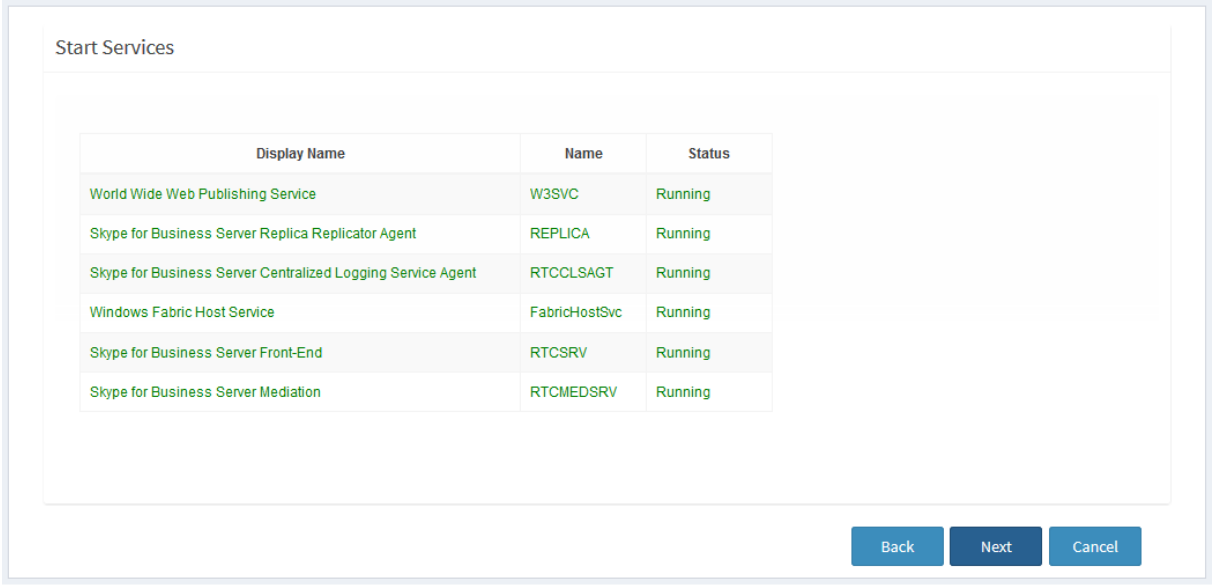


9.12 Step 12: Start Services

This step describes the process for startup of the SBA services.

The following example screen shows the beginning of the startup process where one service has been started (indicated in green).

Figure 9-31: SBA Setup Wizard - Start Services

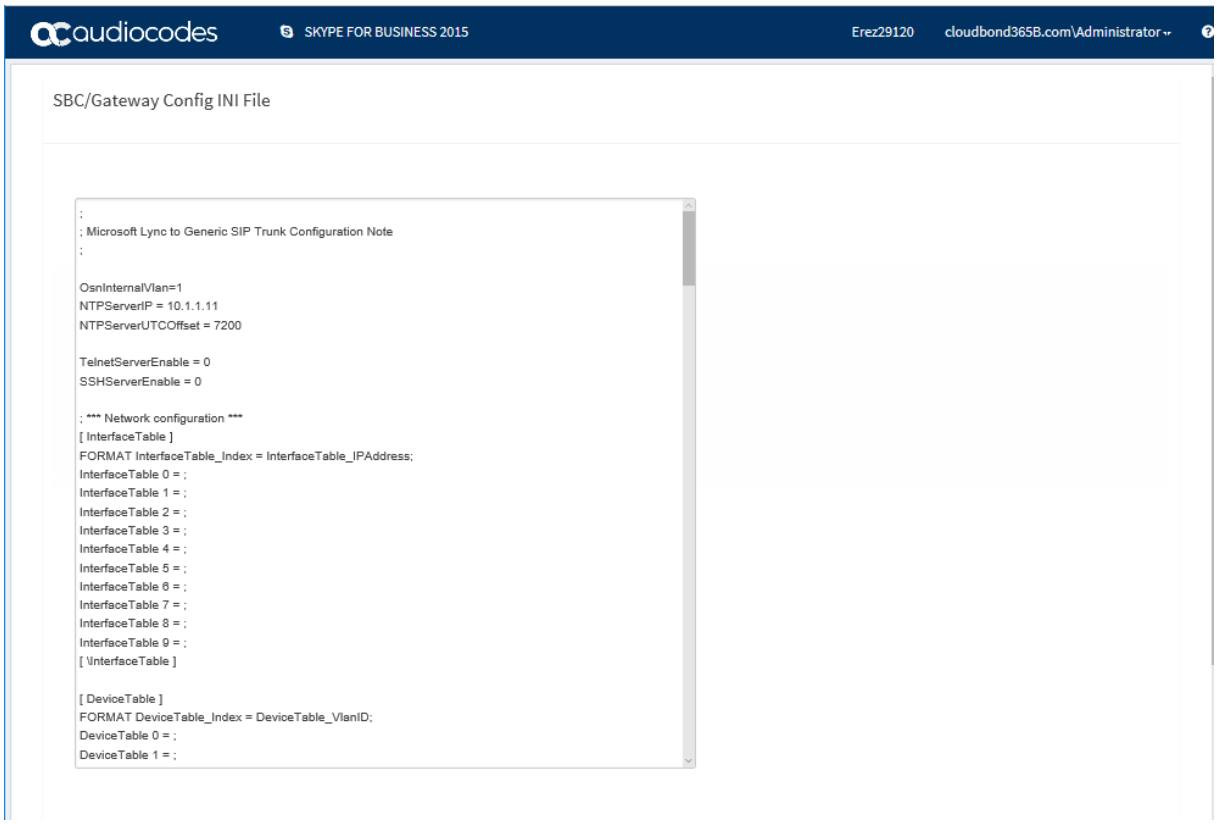


9.13 Step 13: Complete Wizard

At the conclusion of the Wizard process, one of the following is displayed:

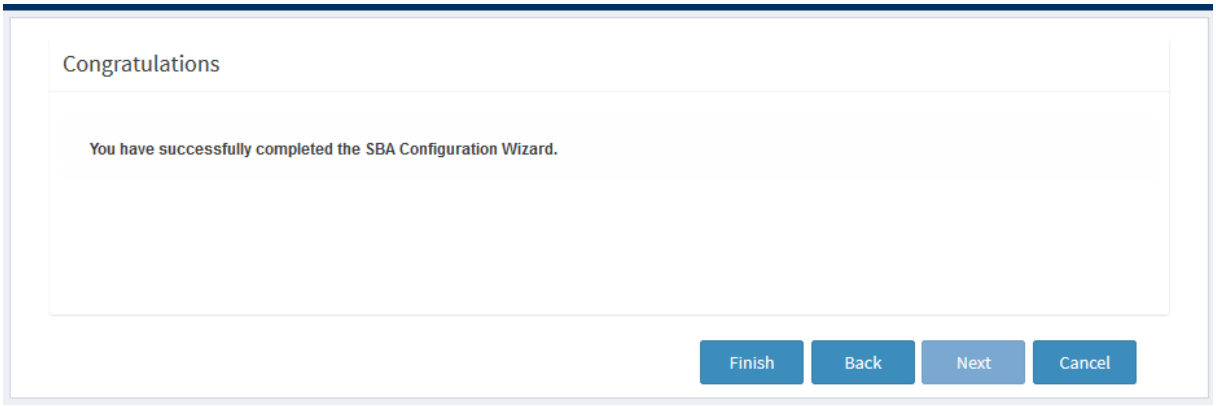
- If you have configured the E-SBC/gateway device, the generated gateway/E-SBC ini configuration file is displayed (note that you cannot edit this output until you save the ini file or load it to your device).

Figure 9-32: Wizard Complete- E-SBC/gateway Configuration



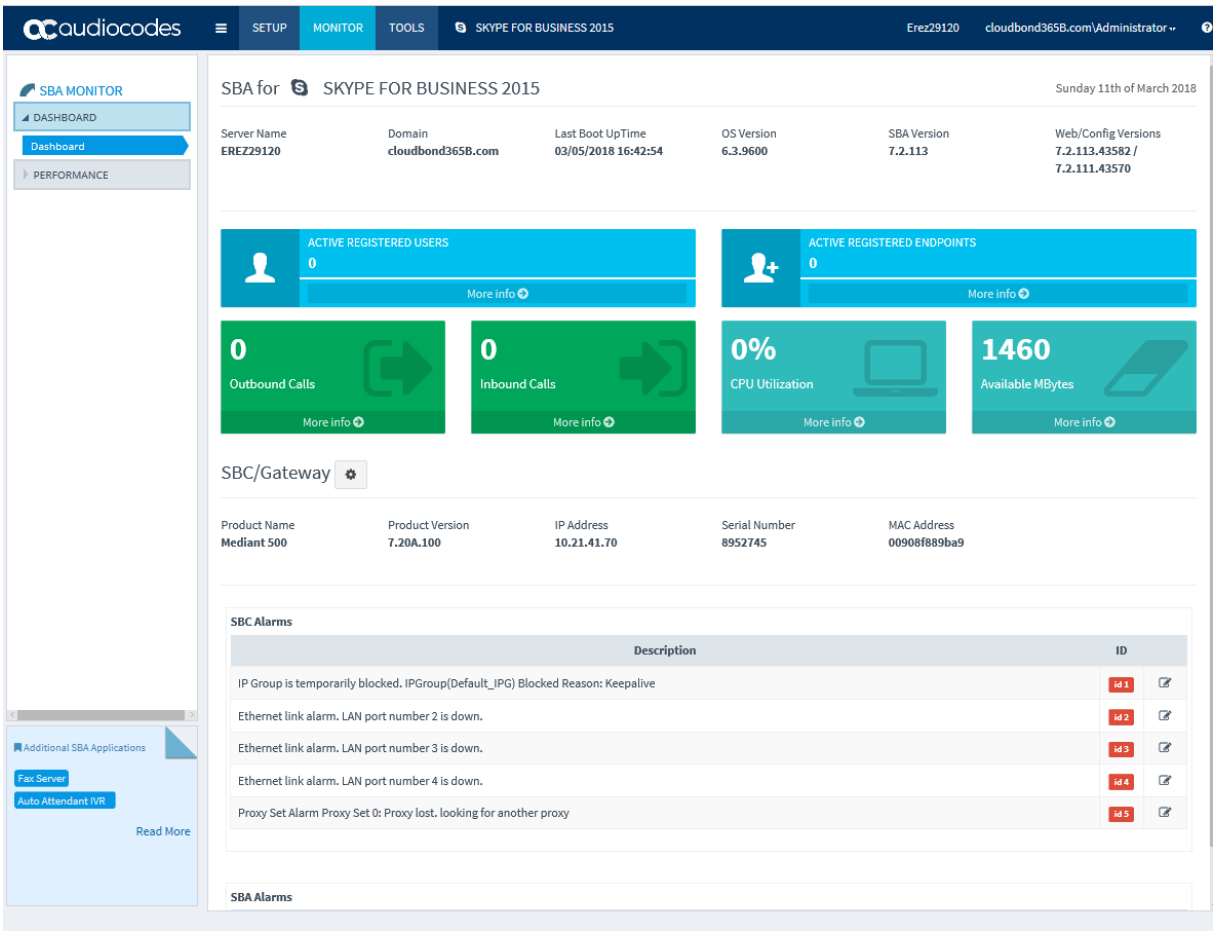
- If you have only configured the SBA, a successful notification screen is displayed.

Figure 9-33: SBA Setup Wizard - Wizard Complete



- Click **Finish**; the SBA Setup Wizard closes and you are returned to the dashboard of the SBA Management Interface:

Figure 9-34: SBA Management Interface - Dashboard

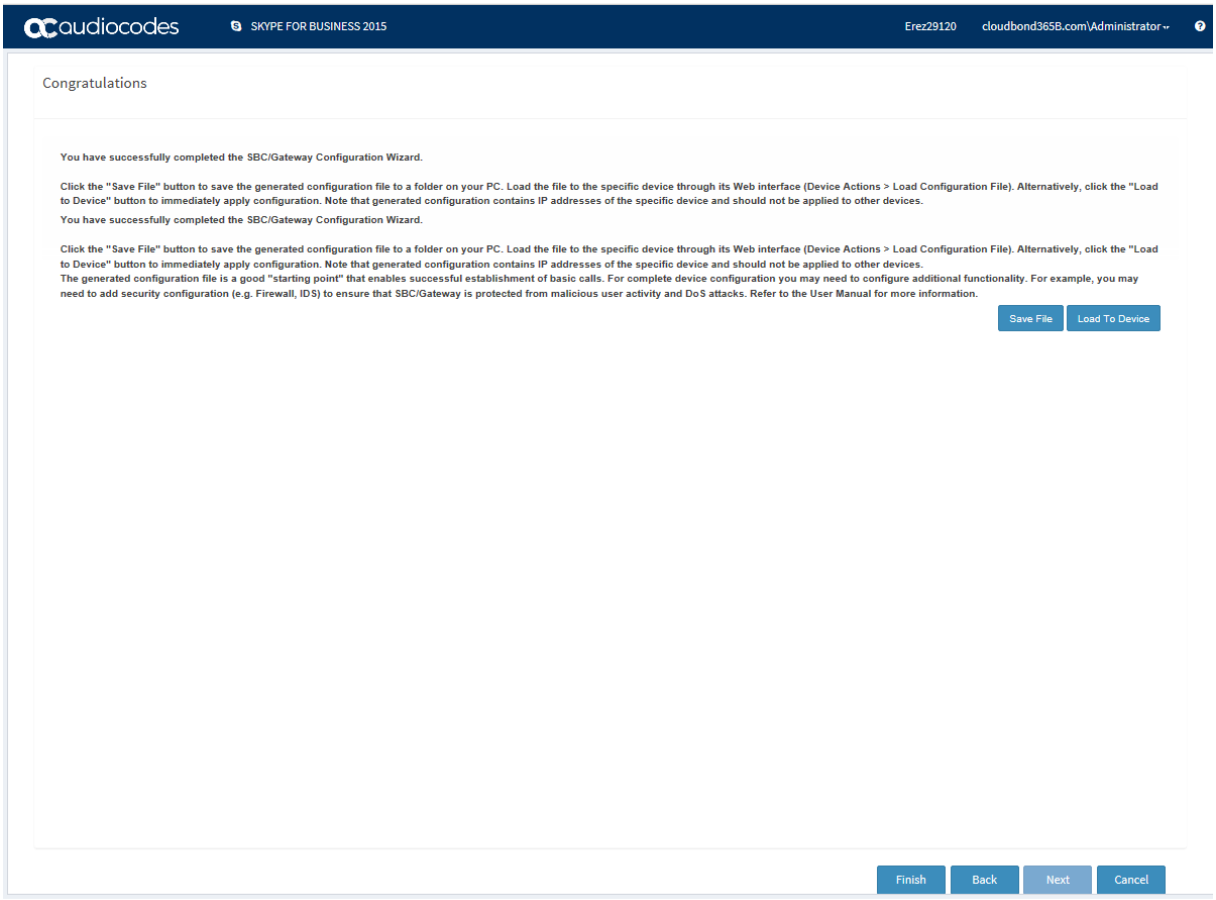


9.14 Step 14: Apply INI File to Device

At the conclusion of the Wizard process, you can either save the E-SBC/gateway ini file to your PC or load it to your device.

Note: This step is only relevant if you are configuring the E-SBC/gateway parameters.

Figure 9-35: Loading and Saving INI File



The wizard generates an ini file which includes the basic configuration of the E-SBC/gateway device. You can now perform one of the following actions:

- **Load to Device:** Load the configuration INI file immediately to the device.
- **Save File:** Save the INI file to your desired location and then later load it using the Embedded Web server tool for the device.

9.15 Step 15: Post Wizard Actions

Once you have completed the Wizard, click **Finish** to return to the SBA Management Interface Main Dashboard. You should now do the following:

- Uses the SBA Management Interface to perform various actions, such as connect to the E-SBC/gateway device from the SBA Management Interface dashboard link (see Chapter 12).
- Perform post-wizard configuration and fine-tuning such as configure PSTN trunks (see Part "Configuring Gateway and E-SBC (Manually) and Post-wizard Tuning on page 109).

Note:

- If you have deployed the "Local Gateway" template in your Network Topology, then specific parameters must be manually configured, such as the PSTN trunk configuration.
- For both the Gateway and E-SBC deployments, you need to use the device's Web server to manually configure and load the TLS certificates used to secure the connection between the Gateway and E-SBC and the Mediation server.

This page is intentionally left blank.

10 Using the SBA Management Interface

Once you have initially set up the SBA through the SBA Management Interface's SBA Setup Wizard, as described in Section 9, you can use the SBA Management Interface for full configuration, maintenance and monitoring of the SBA. In addition, if your SBA device is also employing gateway functionality (i.e., PSTN Gateway and/or SBC), you can use the SBA Management Interface for viewing basic monitoring of the gateway and for accessing the gateway's Web interface (single sign-on) for full gateway configuration.

Note: The SBA Management Interface supports the following Web browsers:

- Internet Explorer 10 and later (with HTML 5 support and with Compatibility View mode disabled)
- Mozilla Firefox 35.01 or later
- Google Chrome 40.0.2214 or later

The figure below shows the main areas of the SBA Management Interface:

Figure 10-1: Main Areas of SBA Management Interface

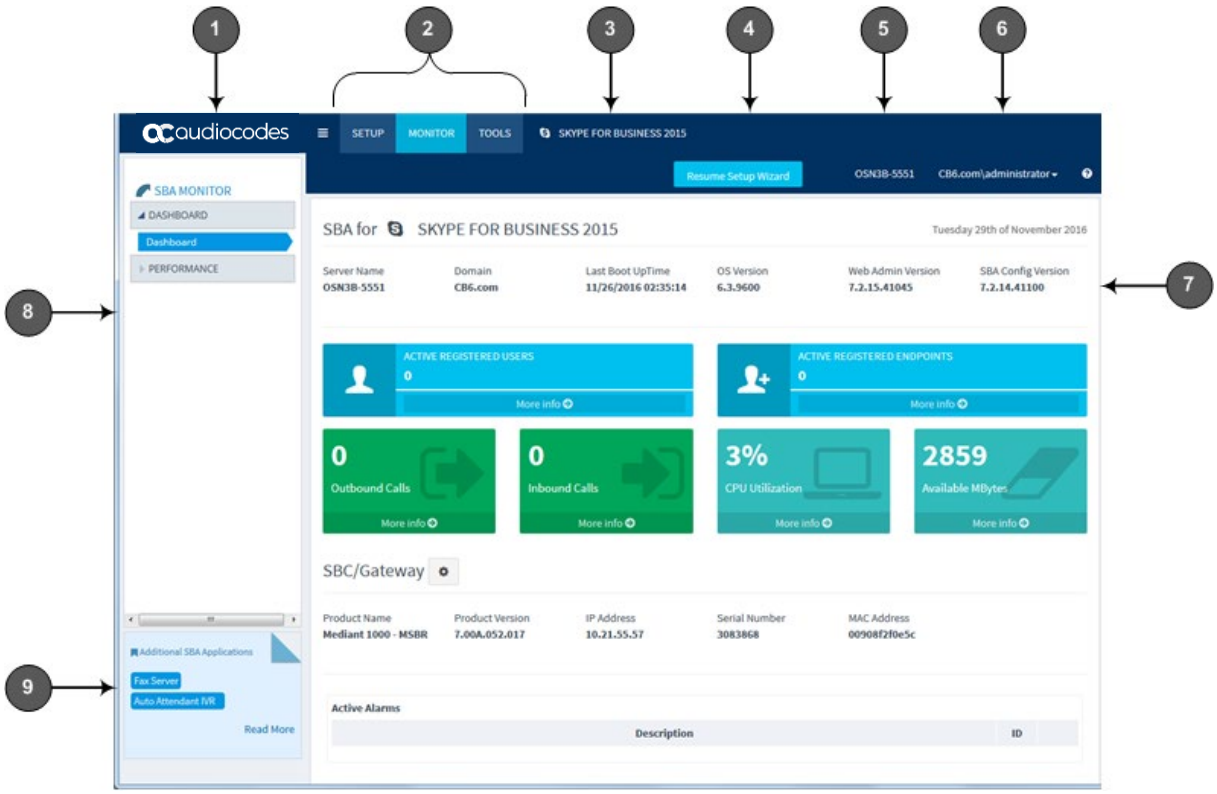


Table 10-1: Main Areas of SBA Management Interface

Item #	Description
1	When clicked, displays the Dashboard.
2	Menu bar with menus (Setup, Monitor and Tools).
3	Opens AudioCodes website, displaying the page on products for Microsoft.
4	**Resume Setup Wizard** button. If you exit the SBA Setup Wizard before its completion, you can later resume from the same wizard page, by clicking the button.

Item #	Description
5	Displays the SBA computer name (defined when joining the domain). If clicked, a pop-up appears displaying system information.
6	Displays the currently logged-in username. When clicked, a drop-down menu appears with the **Logout** command, which if clicked, logs you out of the SBA Management interface.
7	Displays the properties of the SBA for Skype for Business. For more information, see Section 0.
8	Navigation pane containing folders and page items, which depend on the menu selected from the menu bar.
9	Opens AudioCodes website, showing a page with additional SBA applications (Fax Server and Auto Attendant IVR).

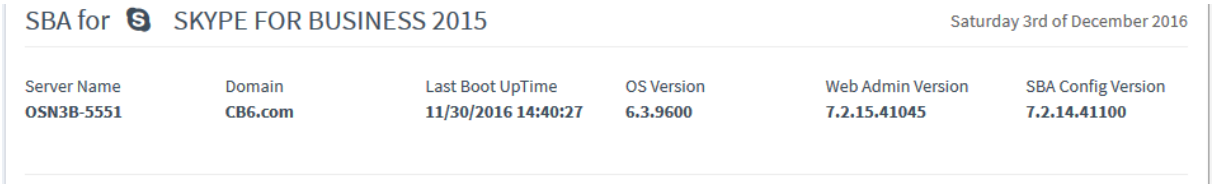
10.1 Viewing General SBA Details

The following procedure describes how to view general SBA details.

➢ **To view general SBA details:**

1. From the **Monitor** menu, select the **Dashboard** folder, and then click **Dashboard**.
2. Under the SBA section, the following information is displayed:

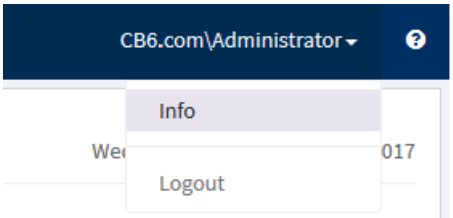
Figure 10-2: Viewing General SBA Details



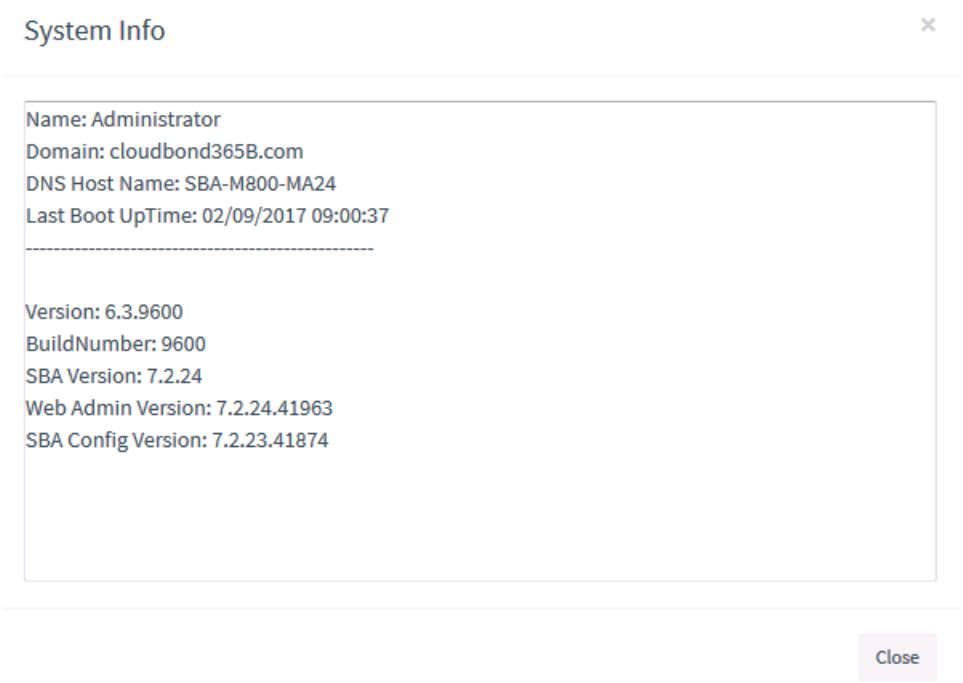
The following information is displayed:

- **Server Name:** Name of the SBA
- **Domain:** Domain name to which the SBA is joined
- **Last Boot Up Time:** Date and time at which the SBA server was last restarted
- **OS Version:** Version of the Windows Server 2012 R2 operating system
- **We Admin Version:** Version number of the SBA Management Interface
- **SBA Config Version:** Version of the SBA service

You can also view general SBA details, by clicking the arrow next to the logged-in username, and then choosing **Info**:



The System Info window appears:



The following information is displayed:

- **Name:** Username of the currently logged-in user
- **Domain:** Domain name to which the SBA is joined
- **DNS Host Name:** Name of the SBA
- **Last Boot Up Time :** Date and time at which the SBA server was last restarted
- **Version:** Version of the Windows Server 2012 R2 operating system
- **Build Number:** Build version of the Windows Server 2012 R2 operating system
- **SBA Version:** Software version of the SBA
- **Web Admin Version:** Version number of the SBA Management Interface
- **SBA Config Version:** Version of the SBA service

10.2 SBA Configuration

This section describes SBA configuration operations that you can do through the SBA Management Interface (in addition to configuration through the SBA Setup Wizard).

10.2.1 Viewing and Configuring Network Interfaces

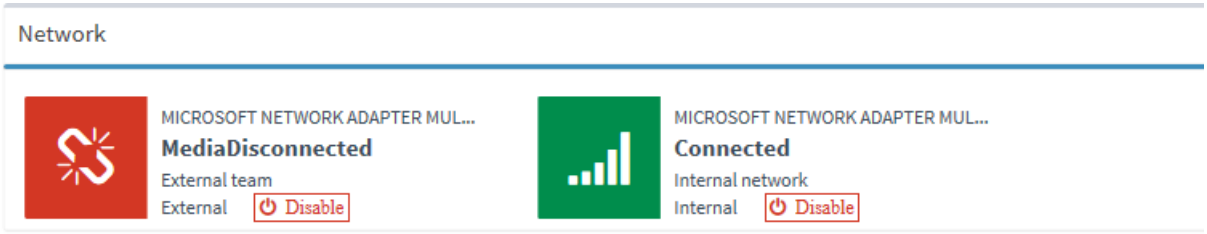
The device includes the following network interface cards (NIC) on the OSN module:

- **External Ethernet Ports:**
  - From Version 7.2.213: If there are two external interfaces, NIC teaming is used.
    - **External Team:** By default, the NIC is enabled (192.168.0.20)
  - For previous versions:
    - **GE I:** By default, the NIC is enabled (192.168.0.20).
    - **GE II:** By default, the NIC is disabled.
- **Internal Ethernet Port:**
  - Internal Network: By default, the NIC is enabled and enabled for DHCP

➢ **To view and configure network interfaces:**

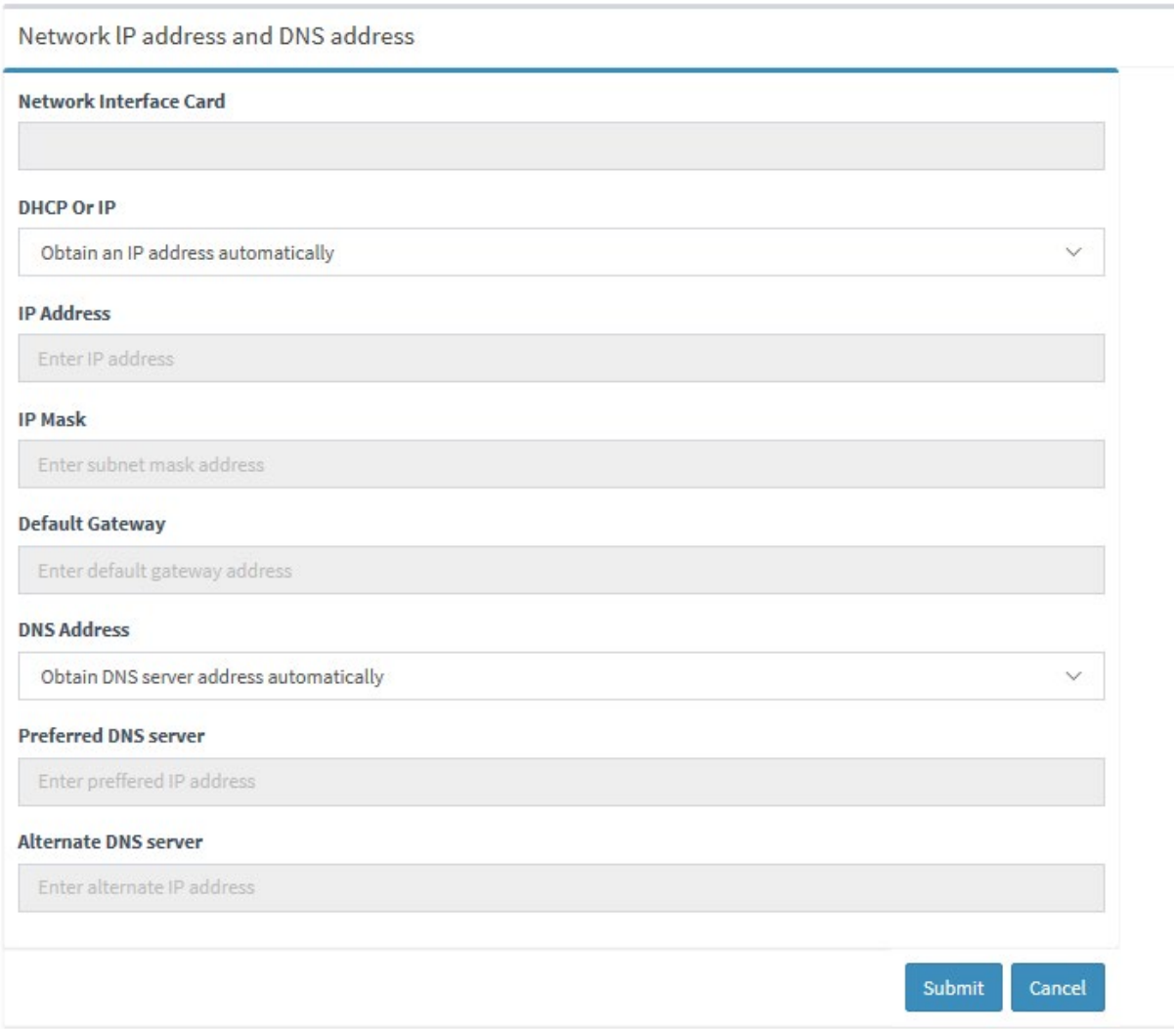
1. From the **Setup** menu, select the **Setup** folder, and then click **Network**:

Figure 10-3: Viewing Network Interfaces



2. To disable a network interface, click **Disable**; to enable a network interface, click **Enable**.
3. To configure a network interface, click the required network icon; the following appears:

Figure 10-4: Configuring a Network Interface (e.g., External NIC Team)



4. As network configuration is explained in detail in the SBA Wizard section, see Section 8.1 for more information.

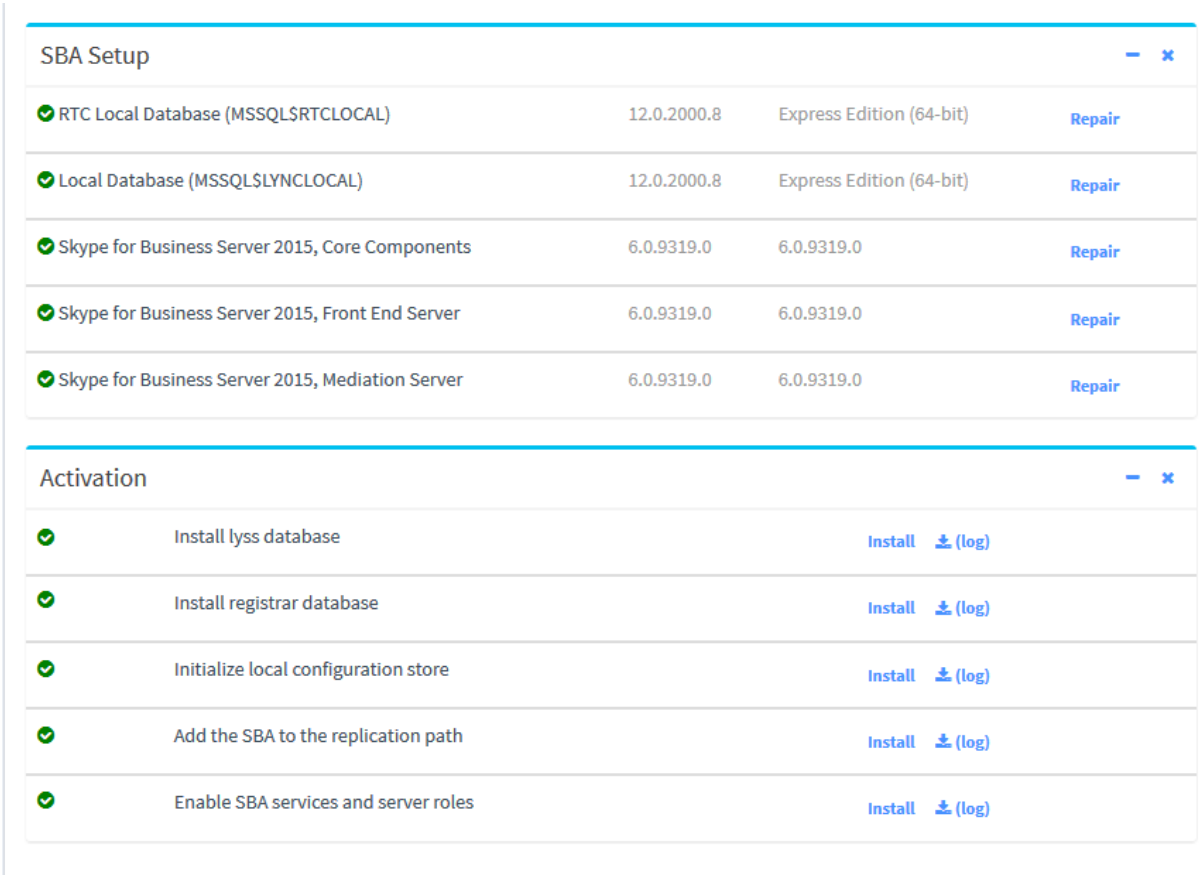
10.2.2 Viewing Installed SBA Components

You can view the status of the installed SBA for Skype for Business components. The icon means that the component is installed and running normally; the icon means that a problem exists with the component. If a problem exists, you can view a logged file, by clicking (log) corresponding to the component, and also install the component again by clicking **install**.

➢ **To view status of installed SBA components:**

- From the **Setup** menu, select the **Setup** folder, and then click **SBA Setup**:

Figure 10-5: Viewing Installed SBA Components



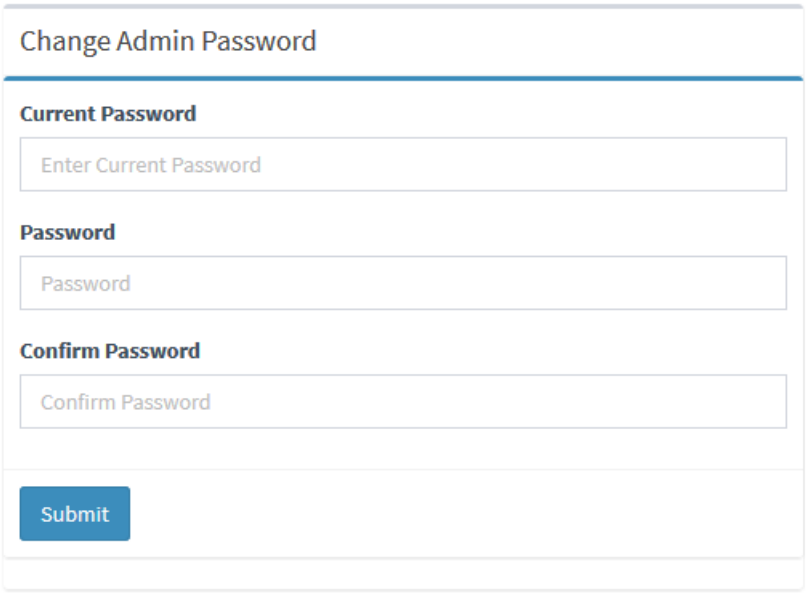
10.2.3 Changing the Login Password

The following procedure describes how to change the login password of the administrator who is currently logged into the SBA Management Interface.

➢ **To change the login password:**

1. From the **Setup** menu, select the **Setup** folder, and then click **Change Admin Password**; the following appears:

Figure 10-6: Changing Login Password



2. In the 'Current Password' field, enter the current password.
3. In the 'New Password' field, enter the new password.
4. In the 'Confirm Password' field, enter the new password again.
5. Click **Submit**.

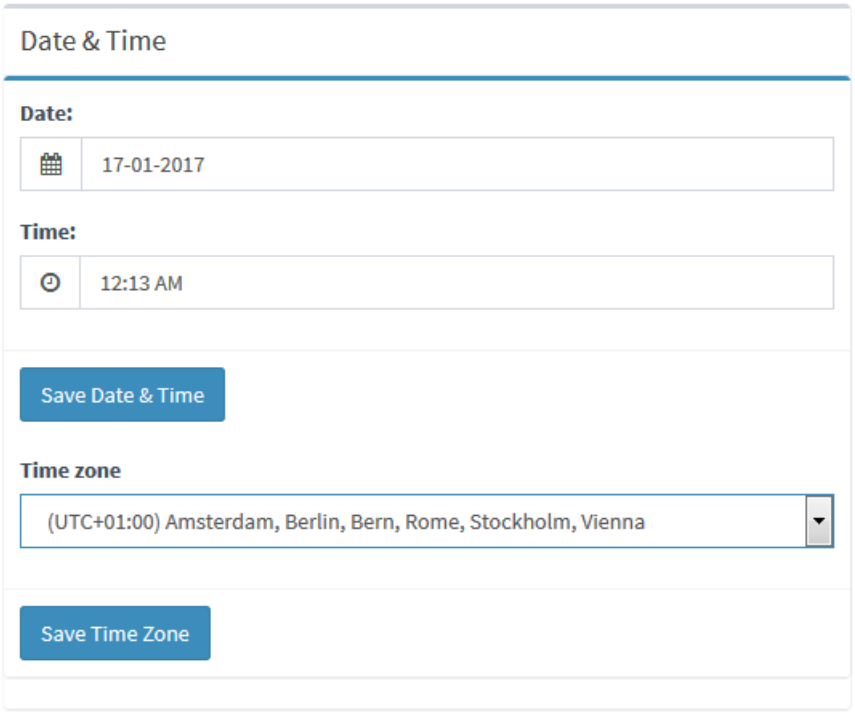
10.2.4 Configuring Date and Time

The following procedure describes how to configure the SBA server's date and time.

➢ **To configure the date and time:**

1. From the **Setup** menu, select the **Setup** folder, and then click **Date & Time**; the following appears:

Figure 10-7: Configuring Date and Time



2. Click the 'Date' field, and then select the date using the pop-up calendar.
3. Click the 'Time' field, and then select the time using the pop-up time box.
4. Click **Save Date & Time**.
5. From the 'Time Zone' drop-down list, select the UTC time zone in which the SBA is located, and then click **Save Time Zone**; the date in the 'Date' field is automatically adjusted according to the selected time zone.

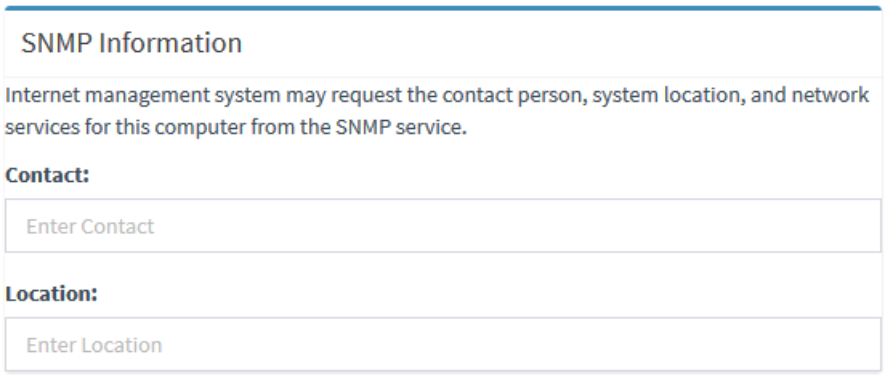
10.2.5 Configuring SNMP

The following procedure describes how to configure SNMP-based communication between the SBA and AudioCodes One Voice Operations Center (OVOC) such as the EMS.

➢ **To configure SNMP:**

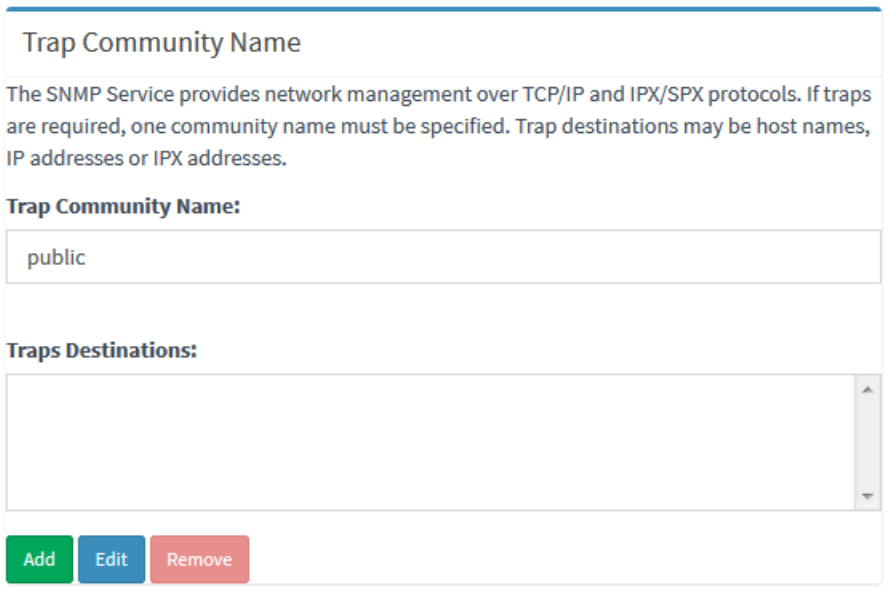
1. From the **Setup** menu, select the **Setup** folder, and then click **SNMP**.
2. Under the SNMP Information group, in the 'Contact' and 'Location' fields, enter the contact person and physical location respectively:

Figure 10-8: Configuring SNMP Information



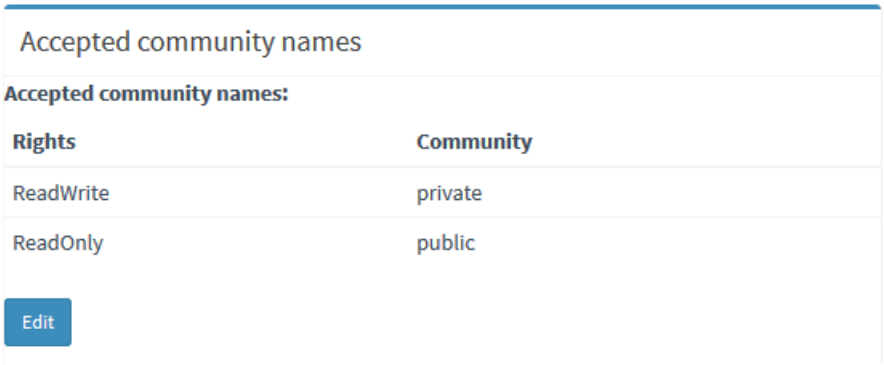
3. Under the Trap Community Name group, do the following:
   a. In the 'Trap Community Name' field, enter the trap community string for the SNMPv2 user. Alternatively, you can use the default "public" string.
   b. Click **Add**, and then in the dialog box, enter destinations to send the traps (e.g., the EMS server's IP address), and then click **Add** to apply your destinations and to close the dialog box.

Figure 10-9: Configuring Trap Community String and Destinations



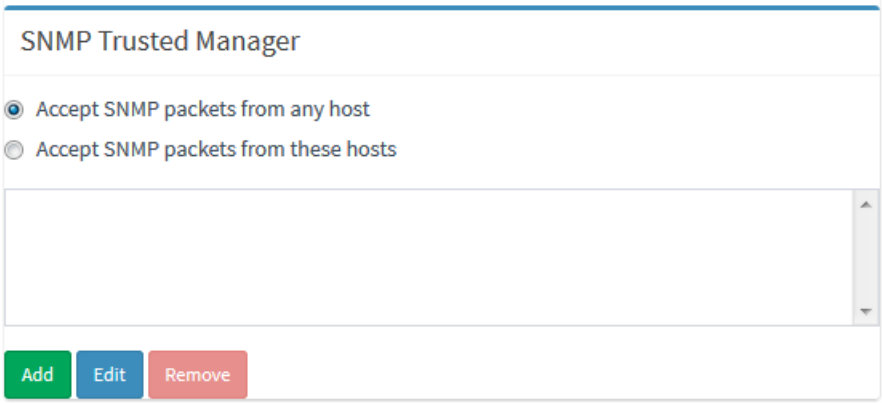
4. Under the Accepted community names group, select the required privilege right (ReadWrite or ReadOnly), and then click **Edit** to configure the community name whose SNMP hosts are allowed to send SNMP requests to the SBA.

Figure 10-10: Configuring Read-Write Privileges per Community Name



5. Under the SNMP Trusted Manager group, configure from whom to accept SNMP packets:
   - **Accept SNMP packets from any host:** All SNMP packets from all SNMP hosts belonging to any community listed in Accepted community names are processed. No SNMP packets are rejected on the basis of the host name or IP address of the source host or the list of acceptable hosts.
   - **Accept SNMP packets from these hosts:** SNMP hosts and SNMP management systems that can send SNMP requests to this SNMP host. Click **Add** to add the trusted managers. This setting provides a higher level of security than use of a community name, which can contain a large group of hosts. You can add the names of any SNMP host or SNMP management system that belong to any community listed in Accepted community names. Only SNMP packets received from the hosts in this list are accepted. All other SNMP messages are rejected, and then authentication traps are sent.

Figure 10-11: Configuring Trusted Managers



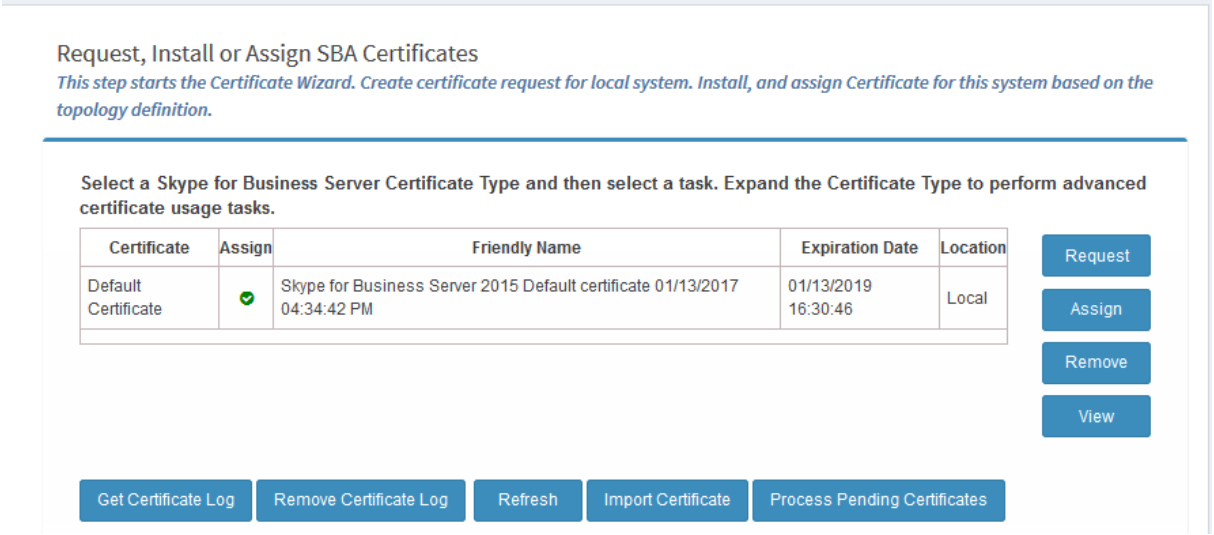
10.2.6 Configuring Certificates

The following procedure describes how to configure the certificates that are used to secure communication between the SBA and the datacenter.

➢ **To configure certificates:**

1. From the **Setup** menu, select the **Setup** folder, and then click **SBA Certificate**.

Figure 10-12: Configuring Certificates



2. As certificate configuration is explained in detail in the SBA Wizard section, see Section 9.7 for more information.

10.2.7 SBC/Gateway Certificate

The following procedure describes how to configure the SBC/Gateway certificates that are used to secure communication between the SBA and the SBC/Gateway. SBC/Gateway certificate is needed only if TLS is used between the SBC/Gateway and the SBA. If TCP is used, there is no need for signing the SBC/Gateway with a certificate.

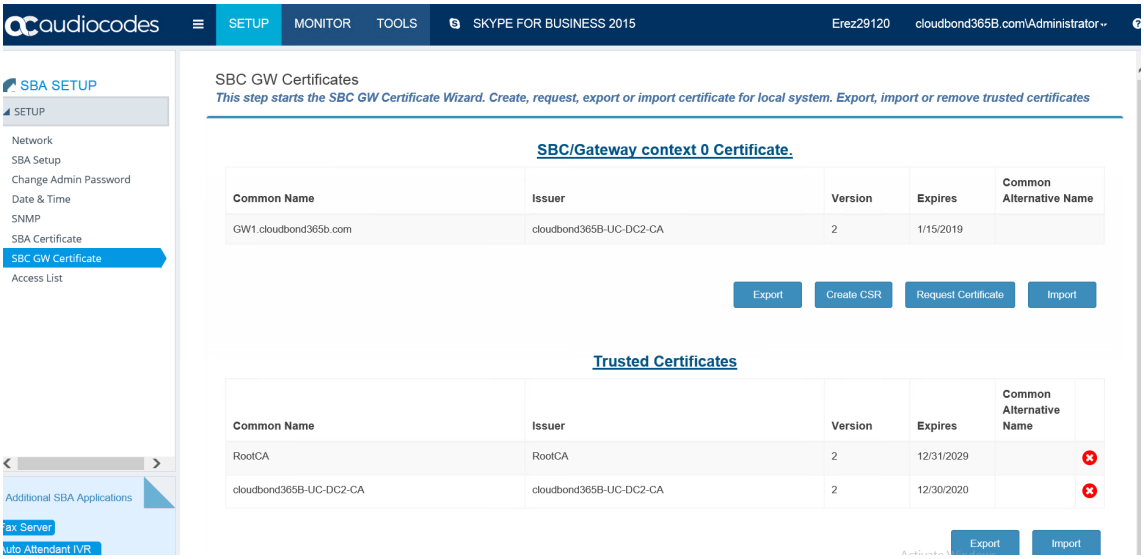
The SBC/Gateway can hold several certificates (TLS Contexts). The SBA GUI handles only TLS Context 0 of the SBC/Gateway certificate, which is the default certificate context.

Note: The SBC/Gateway certificate can also be managed through the SBC/Gateway Web interface. If you wish to change the private key or use a different certificate context (instead of TLS Context 0), then use the SBC/Gateway Web interface.

➢ **To configure certificates:**

1. From the **Setup** menu, select the **Setup** folder, and then click **SBC GW Certificate**.

Figure 10-13: Configuring SBC/GW Certificates

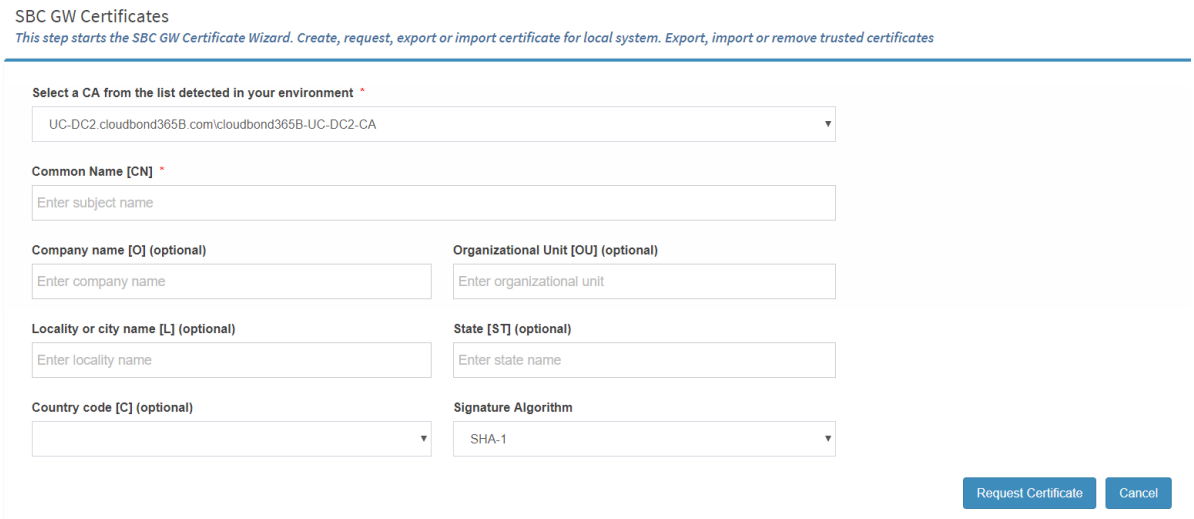


2. The upper part manages the SBC/Gateway certificate and the lower part manages the CA root certificates. For creating a certificate, you can have two options -- automatic enrolment or manual:
   - Automatic enrolment: Click **Request Certificate**.
   - Manual: First create a CSR (click **Create CSR**) and after the certificate is ready, import it (click **Import**).

   If you wish to export the certificate, click **Export**. This exports the SBC/Gateway certificate without the private key.

➢ Request Certificate – automatic certificate enrolment

1. Click **Request Certificate**; the following appears:

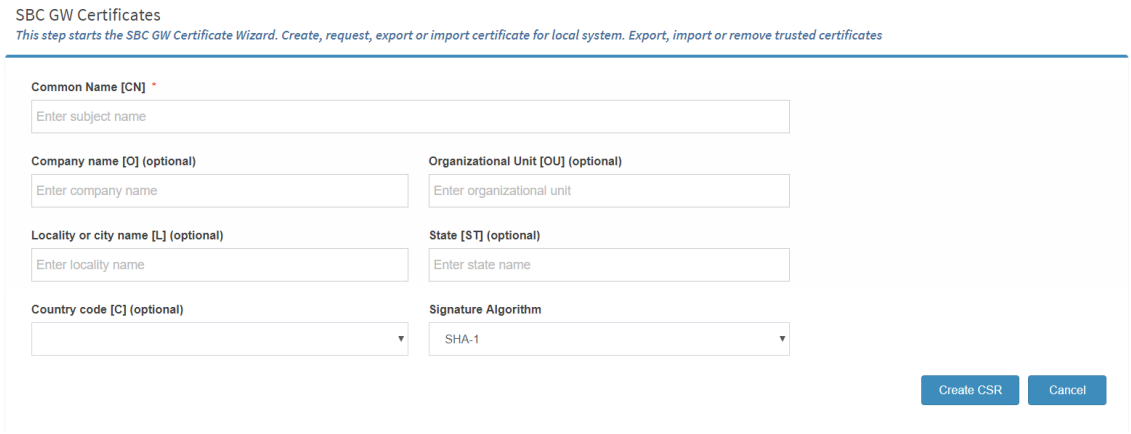


2. Fill in the information, and then click **Request Certificate**.

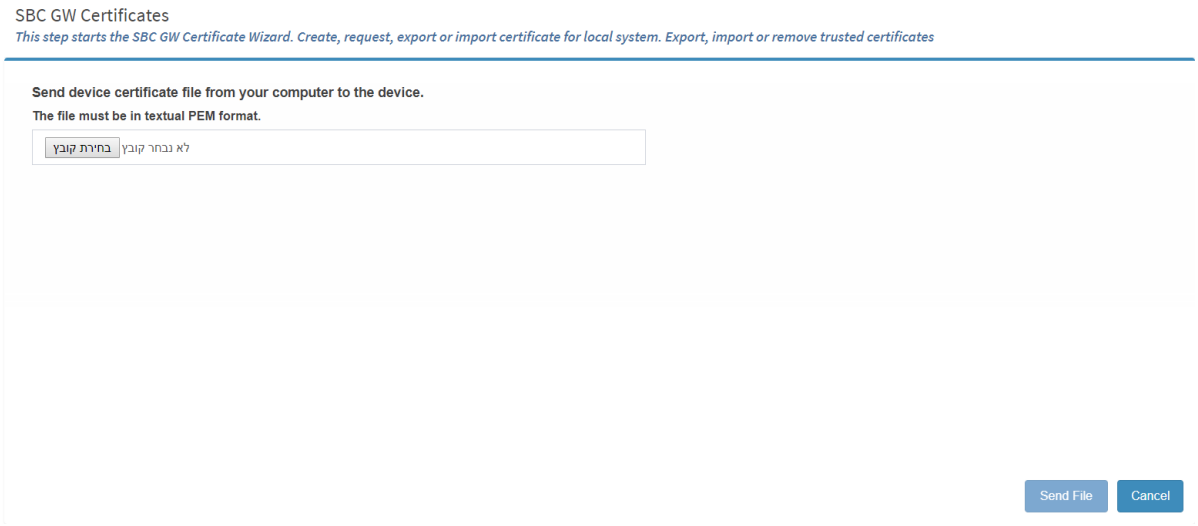
Note: SBC/Gateway automatic enrolment does not support pending certificate. If it is needed, use the manual procedure by creating a CSR and then importing the signed certificate..

➢ CSR – import – manual certificate

1. Create a CSR by clicking **Create CSR**; the following appears:



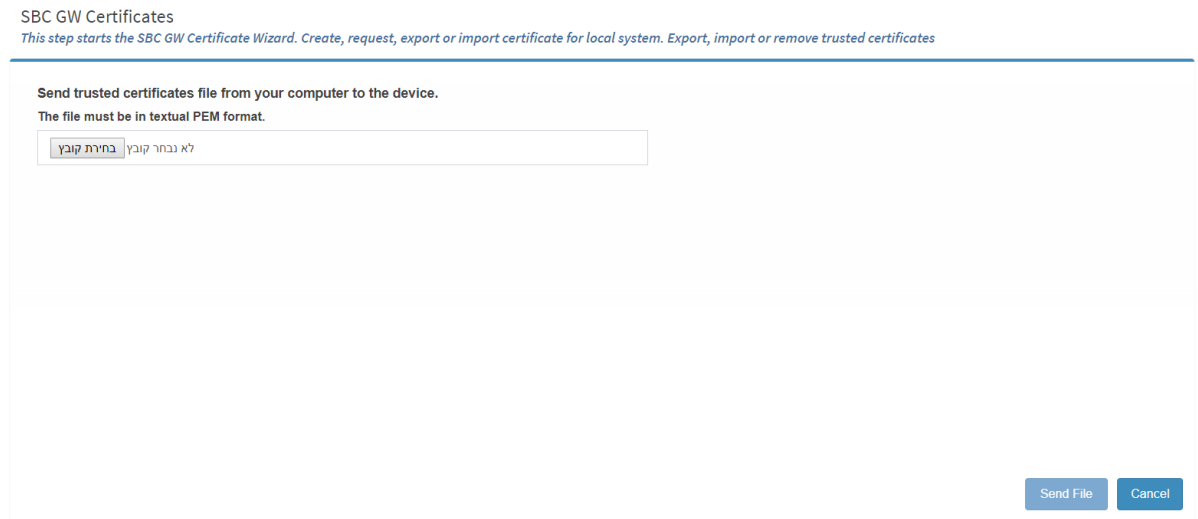
2. Fill in the information, and then click **Create CSR**.
3. Download the CSR that is signed by your CA.
4. Click **Import**; the following appears:



5. Select the signed certificate, and then click **Send File**.

➢ CA Root – Trusted Certificate

1. The CA root of your CA must be loaded to the SBC/Gateway. To import the CA root, obtain it from your CA in PEM format and then use the **Import** button on the Trusted Certificate section; the following appears:



2. Select the CA root certificate, and then click **Send File**.

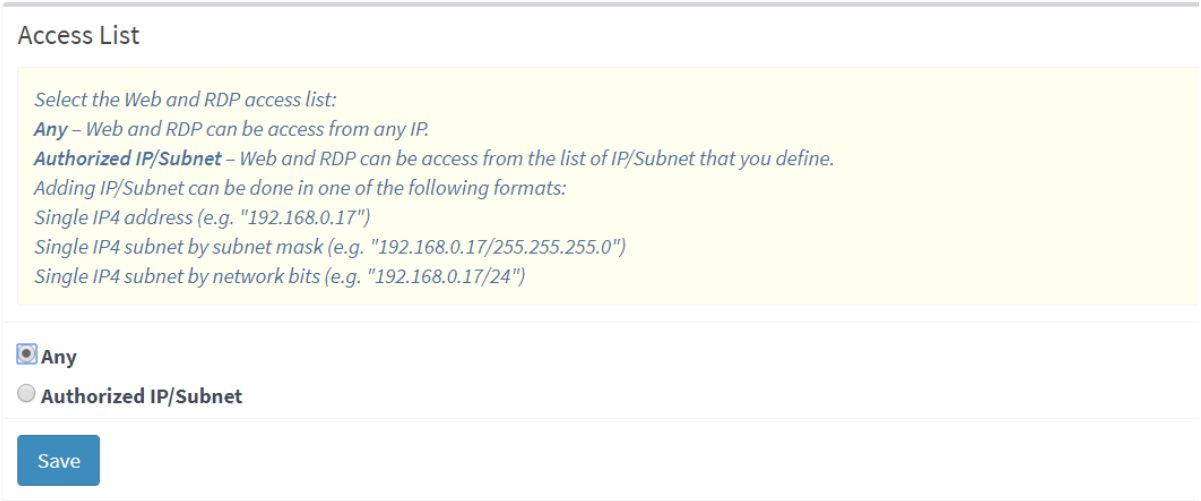
10.2.8 Access List

The following procedure describes how to configure which IP addresses are allowed to access the SBA Web and RDP. This setup limits access to the SBA part only and not to the SBC/Gateway part (for the SBC/Gateway access list, use the SBC/Gateway Web interface).

Note: Pay attention to which IP address/subnet you specify. You can mistakenly block yourself to the SBA. If this occurs, use the screen and keyboard to connect to the SBA locally and open the Web interface locally to fix the access list.

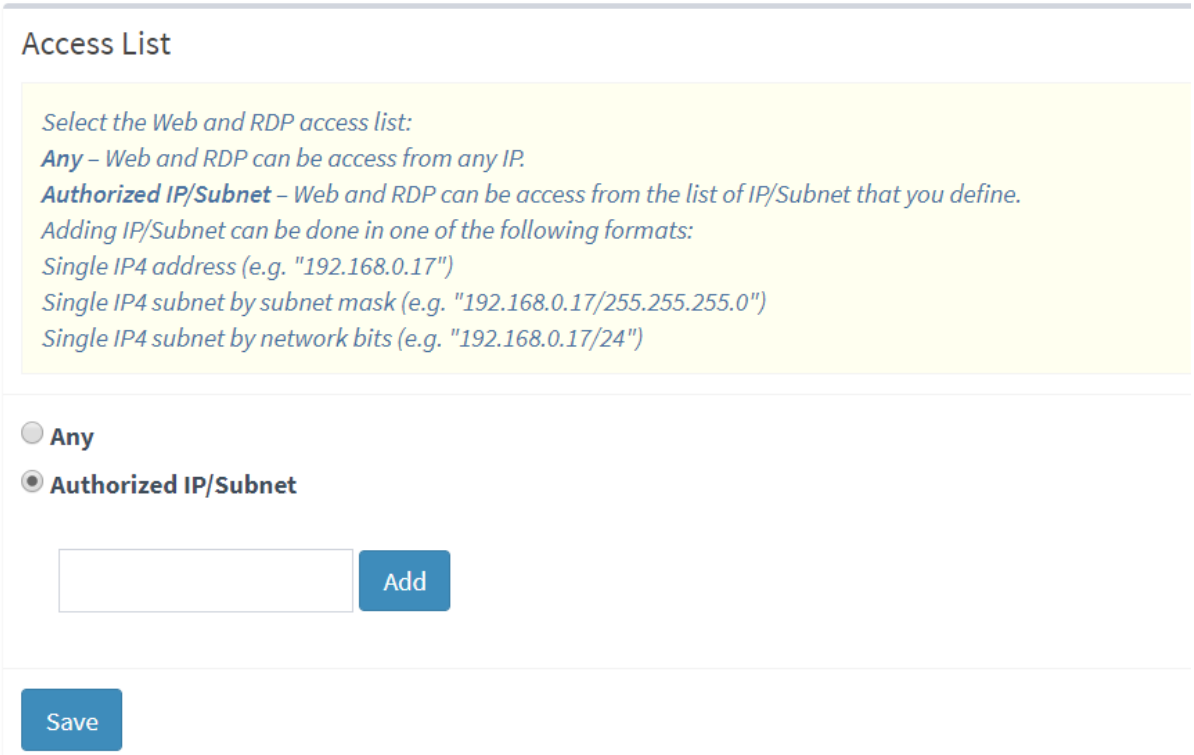
➢ **To configure the Access List:**

1. From the **Setup** menu, select the **Setup** folder, and then click **Access List**.



2. By default, any IP address can access the Web and RDP (**Any** option).

3. To allow SBA management from a specific IP/Subnet, select the **Authorized IP/Subnet** option; the following appears:



4. You can add an IP address/subnet in one of the following formats:
   - Single IPv4 address (e.g. "192.168.0.17")
   - Single IPv4 subnet by subnet mask (e.g. "192.168.0.17/255.255.255.0")
   - Single IPv4 subnet by network bits (e.g. "192.168.0.17/24")
5. Click **Add**
6. Click **Save** to save your changes.

10.3 Gateway-Related Operations

If you are also using your device for Gateway functionality (i.e., PSTN Gateway and/ or SBC), you can use the SBA Management Interface for various Gateway-related operations, as described in this section.

Note: To enable communication between the SBA Management Interface and the Gateway's Web interface, ensure the following:

- Internal VLAN is enabled (OSNInternalVLAN=1).
- Gateway/SBC software version (.cmp) is 7.00A.053.006 or later.

10.3.1 Viewing Gateway Information

The following subsections describe how to view various information relating to the Gateway.

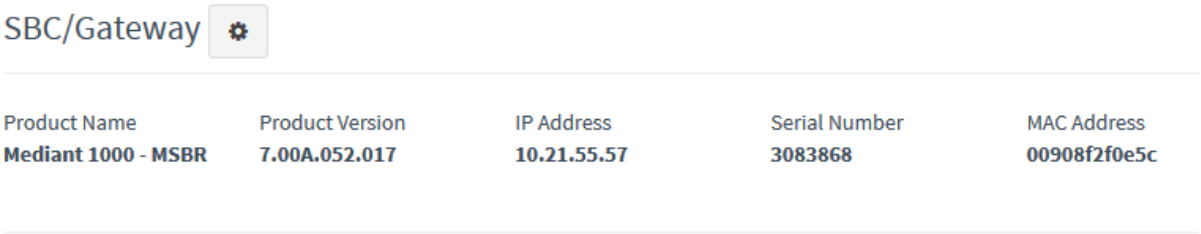
10.3.1.1 Viewing Gateway Details

The following procedure describes how to view details about the Gateway.

➢ **To view gateway details:**

1. From the **Monitor** menu, select the **Dashboard** folder, and then click **Dashboard**.
2. Scroll down the page to the SBC/Gateway section:

Figure 10-14: Viewing Gateway Details



The following information is displayed:

- **Product Name:** Name of the Gateway model
- **Product Version:** Software version currently running on the Gateway
- **IP Address:** IP address of the Gateway's OAMP interface
- **Serial Number:** Serial number of the Gateway's CPU
- **MAC Address:** MAC address of the Gateway

10.3.1.2 Viewing Gateway Alarms

The following procedure describes how to view active alarms raised by the Gateway.

➢ **To view active gateway alarms:**

1. From the **Monitor** menu, select the **Dashboard** folder, and then click **Dashboard**.
2. Scroll down the page to the Active Alarms section:

Figure 10-15: Viewing Active Gateway Alarms

10.3.2 Accessing Gateway's Web Interface

If required, you can access the Gateway's Web interface from the SBA Management Interface. The Gateway's Web interface allows you to fully configure Gateway functionality.

➢ **To access the gateway's Web interface:**

1. From the **Monitor** menu, select the **Dashboard** folder, and then click **Dashboard**.
2. Scroll down the page to the SBC/Gateway section, and then click ; the Web interface of the Gateway opens.

For more information on using the Gateway's Web interface, refer to the Gateway's *User's Manual*.

10.4 Performance Monitoring

The SBA Management Interface allows you to monitor the SBA.

10.4.1 Viewing Call Statistics

The following procedure describes how to view call statistics.

➢ **To view call statistics:**

1. From the **Monitor** menu, select the **Performance** folder, and then click **Calls**.
2. Click **On** to enable statistics or **Off** to disable.

Figure 10-16: Viewing Call Statistics

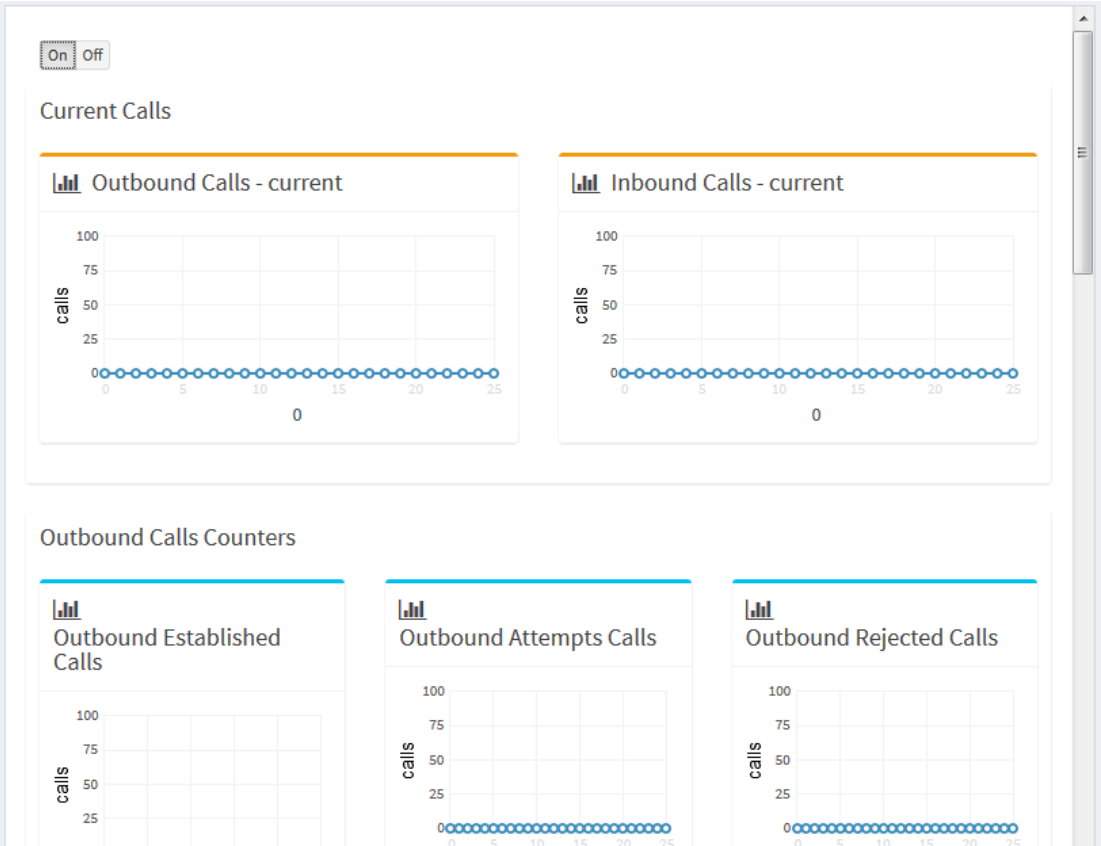


Table 10-2: Call Statistics Description

Graph	Description
Current Calls	
Outbound Calls - current	Number of current outbound calls
Inbound Calls - current	Number of current inbound calls
Outbound Calls Counters	
Outbound Established Calls	Number of outbound established calls
Outbound Attempts Calls	Numbers of outbound call attempts
Outbound Rejected Calls	Number of outbound calls that were rejected
Outbound Invites Calls	Number of sent SIP INVITE messages

Graph	Description
Active Outbound Priority Calls	Number of currently active outbound priority calls
Active Outbound Media Bypass Calls	Number of currently active outbound media bypass calls
Outbound Media Bypass Calls	Number of outbound media bypass calls
Inbound Calls Counters	
Inbound Established Calls	Number of inbound established calls
Inbound Attempts Calls	Numbers of inbound call attempts
Inbound Rejected Calls	Number of inbound calls that were rejected
Inbound Invites Calls	Number of received SIP INVITE messages
Active Inbound Priority Calls	Number of currently active inbound priority calls
Active Inbound Media Bypass Calls	Number of currently active inbound media bypass calls
Inbound Media Bypass Calls	Number of inbound media bypass calls

10.4.2 Viewing Registered Users Statistics

The following procedure describes how to view active registered user statistics, which includes users and endpoints.

➢ **To view registered user statistics:**

1. From the **Monitor** menu, select the **Performance** folder, and then click **Active Users**.
2. Click **On** to enable statistics or **Off** to disable.

Figure 10-17: Viewing Active Users

10.4.3 Viewing General SBA Server Statistics

The following procedure describes how to view general statistics of the SBA server.

➢ **To view SBA server statistics:**

1. From the **Monitor** menu, select the **Performance** folder, and then click **Key Health Indicators**.
2. Click **On** to enable statistics or **Off** to disable.

Figure 10-18: Viewing SBA Server Statistics

Table 10-3: SBA Server Statistics

Graph	Description
General Server Health	
Available Bytes	Available physical memory (in MBytes) for running processes
CPU Utilization	Current utilization of CPU (in %)
Avg. Disk Sec/Read	Average time of disk-read latency
Avg. Disk Sec/Write	Average time of disk-write latency

Graph	Description
SQL Server	
MSSQL RTC Page Life Expectancy	Number of seconds that the SQL server (RTC Local) expects a data page to remain in the cache
MSSQL Lync Page Life Expectancy	Number of seconds that the SQL server (Lync Local) expects a data page to remain in the cache
Front-end Server	
Database – Queue Latency	Average time a request is held in the request queue to RTCDyn database
Database – Sproc Latency	Average time to execute a sproc call against RTCDyn database
Database – Throttled	Number of requests rejected with a retry since the database queue latency was high
REG Database – Queue Latency	Average time a request is held in the request queue to RTC database
REG Database – Sproc Latency	Average time to execute a sproc call against RTC database
REG Database – Throttled	Number of requests rejected with a retry since the database queue latency was high
Shared Database – Queue Latency	Average time a request is held in the request queue to RTCShared database
Shared Database – Sproc Latency	Average time to execute a sproc call against RTCShared database
Shared Database – Throttled	Number of requests rejected with a retry since the database queue latency was high

10.5 Maintenance

This section describes various maintenance operations.

10.5.1 Upgrading SBA Software and Cumulative Updates

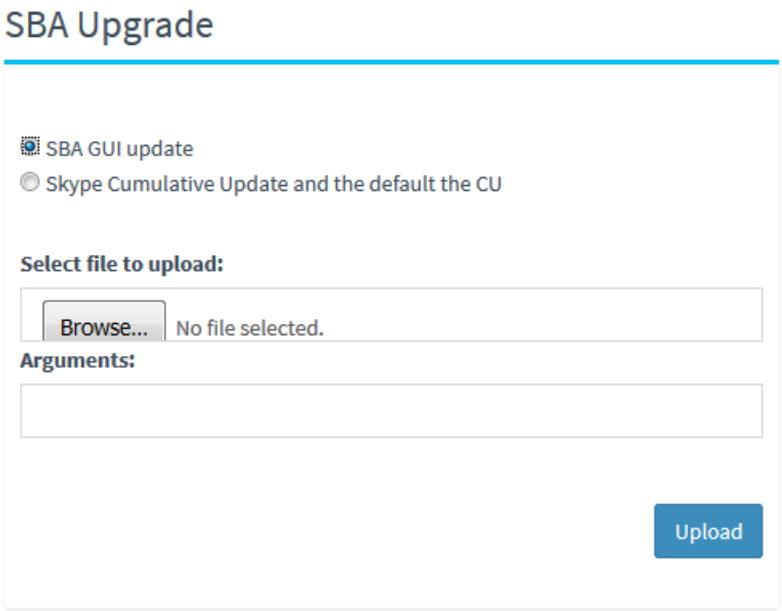
The following procedure describes how to upgrade the SBA Management Interface and Cumulative Updates (CU).

Note: During the CU update process, one or more Skype for Business services are temporarily stopped (e.g., Front End service) and as a result, currently active traffic is terminated. Therefore, it is recommended to perform this update during low-traffic periods. For more information on updating CU, see Section 19.

➢ **To upgrade SBA software and CU:**

1. From the **Tools** menu, click **SBA Software Upgrade**; the following appears:

Figure 10-19: Upgrading SBA Software and CU



2. Depending on what you want to upgrade, select one of these options:
   - **SBA GUI update** to update the SBA Management Interface.
   - **Skype Cumulative Update** to update the CU.
3. Click **Browse** to select the file that you want to load, and then click **Upload**.

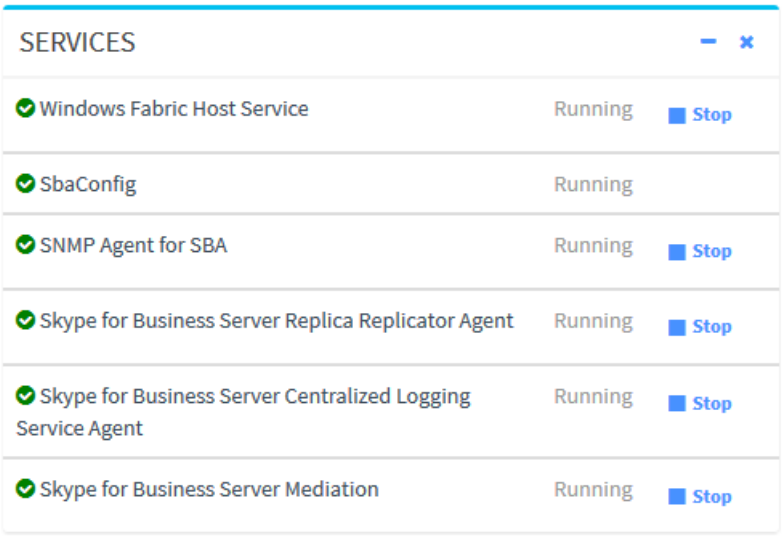
10.5.2 Stopping and Starting SBA Services

The following procedure describes how to stop and start SBA services.

➢ **To stop and start SBA services:**

1. From the **Tools** menu, click **SBA Services**; the following appears:

Figure 10-20: Stopping and Starting SBA Services



2. Do one of the following:
   - To stop a service, click the corresponding **Stop** button; the service displays the "Stopped" status message.
   - To start a service, click the corresponding **Start** button; the service displays the "Running" status message.

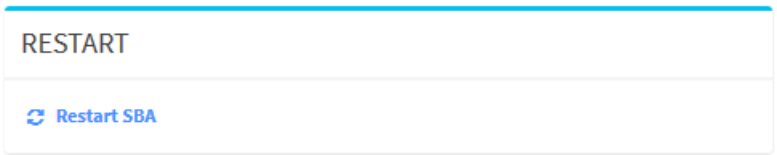
10.5.3 Restarting SBA Server

The following procedure describes how to reset the SBA.

➢ **To restart the SBA:**

1. From the **Tools** menu, click **SBA Services**; the following appears:

Figure 10-21: Restarting SBA



2. Click **Restart SBA**.

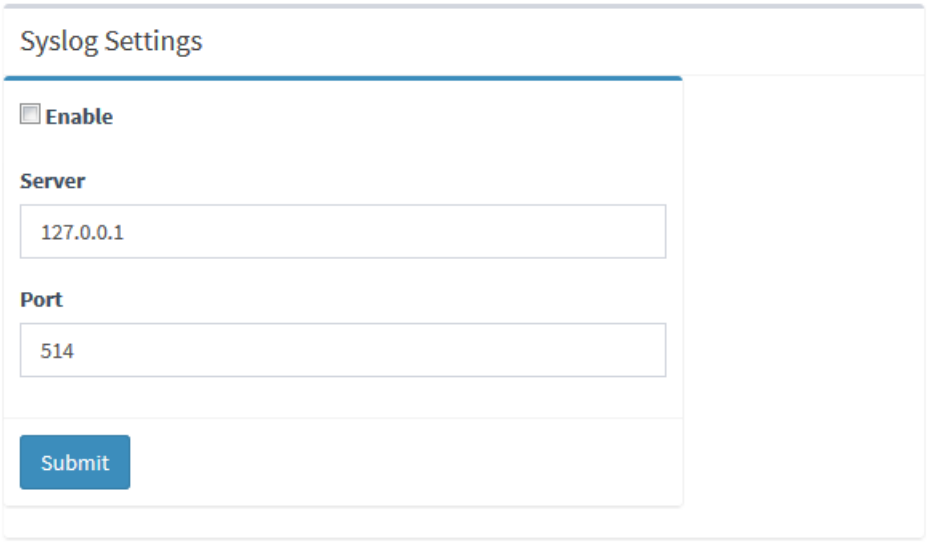
10.5.4 Configuring Syslog

The following procedure describes how to enable the SBA to send SBA configuration logs (see SBA Configuration Logs on page 105) to a Syslog server (for diagnostics).

➢ **To configure Syslog:**

1. From the **Tools** menu, click **SBA Syslog**; the following appears:

Figure 10-22: Configuring Syslog



2. Select the **Enable** check box.
3. In the 'Server' field, enter the Syslog server's IP address.
4. In the 'Port' field, enter the Syslog server's port.
5. Click **Submit**.

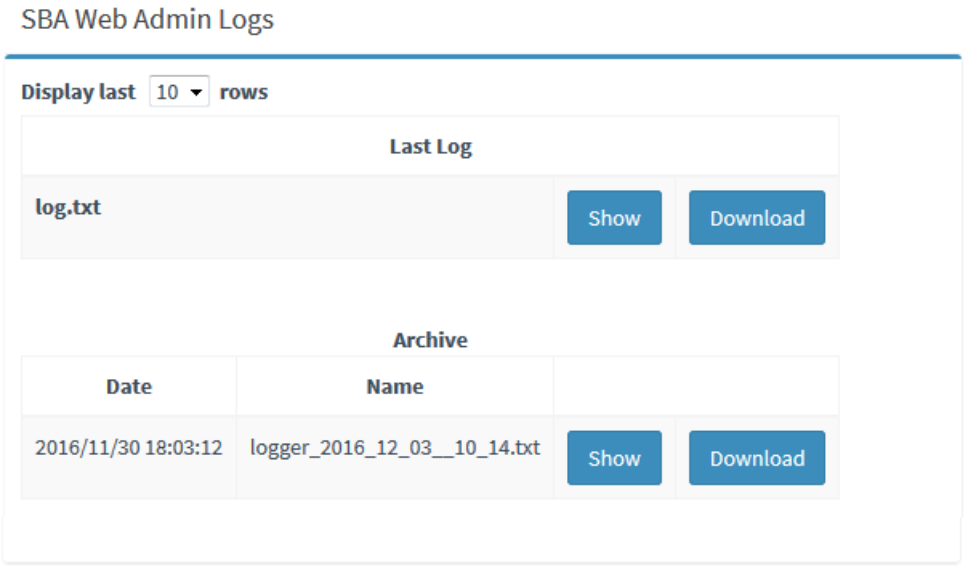
10.5.5 Viewing Logged SBA Management Interface Activities

The following procedure describes how to view logged activities performed in the SBA Management interface such as logging in and out of the GUI.

➢ **To view logged activities:**

1. From the **Tools** menu, click **Web Admin Logs**; the following appears:

Figure 10-23: Viewing Logged SBA Management Activities



2. From the 'Display last' drop-down list, select the number of row records to display.
3. Click **Show** to view the contents of the logged file or **Download** to save the logged file to your PC.

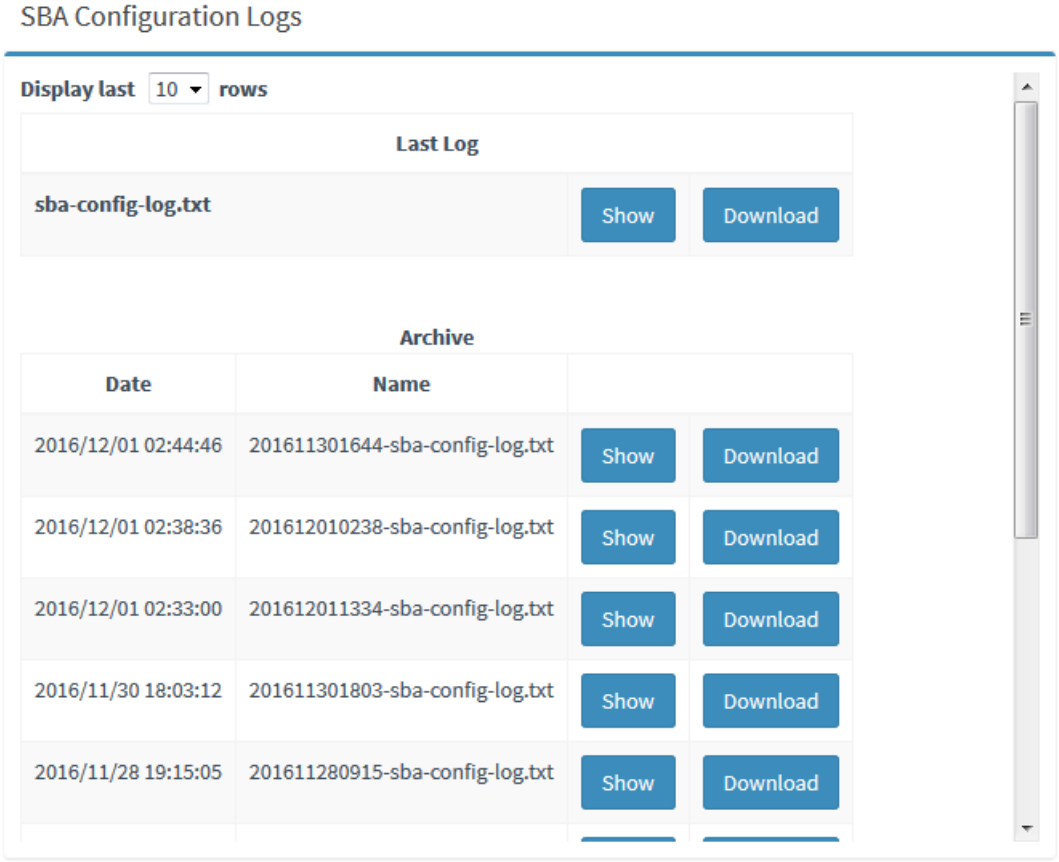
10.5.6 Viewing Logged SBA Configuration Activities

The following procedure describes how to view logged SBA configuration operations.

➢ **To view logged SBA configuration:**

1. From the **Tools** menu, click **SBA Configuration Logs**; the following appears:

Figure 10-24: Viewing Logged SBA Configuration Operations



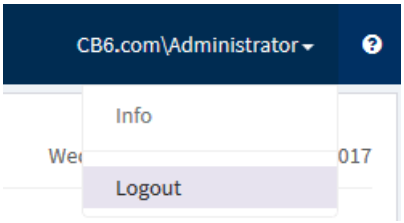
2. From the 'Display last' drop-down list, select the number of rows to display.
3. Click **Show** to view the contents of the logged file or click **Download** to save the logged file to your PC.

10.6 Logging out of SBA Management Interface

The following procedure describes how to log out SBA Management Interface.

➢ **To log out SBA Management Interface:**

1. Click the arrow located next to the logged-in username:



2. Choose **Logout**.

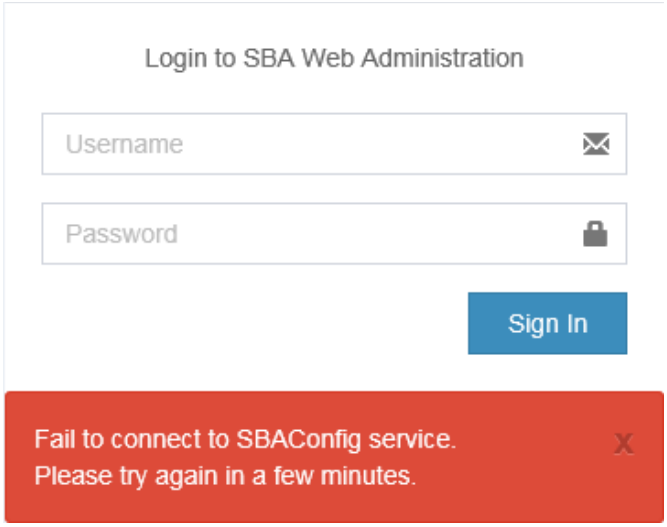
10.7 Troubleshooting

The following table lists troubleshooting SBA Management Interface

10.7.1 Login Failure due to Connection Failure with SBA Service

If you manually restart the SBA server and then attempt to login before the SBA Configuration service has restarted, the following message may appear:

Figure 10-25: Fail to Connect to SBA Configuration Service

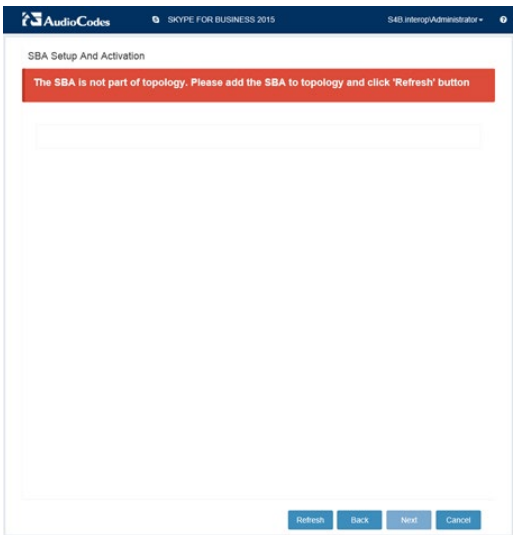


To resolve the problem, wait a few minutes and then try logging in again.

10.7.2 SBA Topology not Created

If the SBA Topology has not been configured, the following message is displayed after joining the SBA to the domain (see Section 11.8):

Figure 10-26: Topology Not Defined



Part IV

Configuring Gateway/SBC Manually and Post-Wizard Tuning

11 Introduction

When you deployed network topology using the SBA Wizard tool, Gateway and E-SBC parameters were either directly configured in the Wizard or the deployed Wizard template included parameters with pre-configured default values. This part is designed to assist you to verify and supplement the configuration of these parameters. This is done using step-by-step procedures for manually configuring the Gateway and E-SBC device residing on the SBA Branch appliance. The configuration is done through the embedded Web server (Web interface) of the Mediant 1000B Gateway and E-SBC. The following summarizes these configuration scenarios:

- Verifying or running the equivalent to the basic Gateway and E-SBC setup that was performed using the SBA Wizard (see Chapter 11).
- Performing supplementary configuration for fine-tuning the basic SBA Wizard configuration setup (see note below) and configuring parameters that cannot be configured using the SBA Wizard.

Note:. Supplementary configuration is required for specific settings as follows (also indicated by footnotes throughout this chapter):

- The TLS certificates used to authenticate the connection between the AudioCodes device and the Mediation server must be configured manually using the procedures described in Section 13.8.
- The Voice coders must be configured manually.
- The FXS ports and PSTN trunks configuration (see Chapter 18) are not configured by the SBA Wizard, therefore you must perform this configuration manually.
- The Normalization Rules for Gateway (PSTN) and E-SBC (see Chapter 19) describe supplementary information for advanced configuration (the basic configuration was performed in the SBA Wizard in Section 11.12).
- The configuration examples shown in this section show the configuration of the Gateway and E-SBC Skype for Business leg. Examples are not provided for the configuration of the SIP Trunk or IP-PBX legs (for more information, refer to the appropriate SIP Vendor or IP-PBX interoperability documentation).
- If you wish to configure the SBA Branch appliance as both a Gateway and E-SBC, you need to manually configure the device to support the second Application type i.e. to support both Tel-to-IP and IP-to-IP calls. For more information, refer to *Mediant SBC Configuration Examples*.

This page is intentionally left blank.

12 Configuring the Connection with the Mediation Server

The procedure below describes how to configure the address (IP address or FQDN) of the Mediation Server through which the Gateway communicates with Skype for Business. If you have more than one Mediation Server in the cluster, proxy redundancy functionality can also be configured.

12.1 Step 1: Configure Gateway Name

This step describes the configuration of the Proxy and Registration mechanism for the Mediation Server connection.

➢ **To configure the Proxy and Registration:**

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).

Figure 12-1: Proxy and Registration Page

2. In the 'Gateway Name' field, assign a unique FQDN name to the Gateway or E-SBC within the domain, for example,'gw.SkypeForBusiness.com'.This name is identical to the name that is configured in the Skype for Business Topology Builder (see Section 9.1).

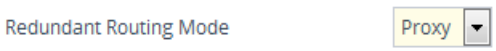
Note: The Gateway and SBC FQDN name is included in the SIP messages and is retrieved from either the 'Gateway Name' or the 'SIP Group Name' (in the IP Group). For more information on the use of these parameters, refer to the *Mediant 1000B Gateway & E-SBC User's Manual*.

3. Click **Apply** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the devices flash memory.

12.2 Step 2: Configure Routing Mode

1. Open the Routing Settings screen (**Setup** menu > **Signalling & Media** tab > **Routing** > **Routing Settings**).

Figure 12-2: Routing Settings Page



2. From the 'Redundant Routing Mode' drop-down list, select **Proxy**. This setting ensures that if a SIP 5xx message is received in response to an INVITE message sent to the primary proxy (i.e., Mediation Server on the device), the PSTN Gateway or E-SBC re-sends it to the redundant proxy (i.e., Mediation Server at the datacenter). To configure alternative routing upon receipt of a SIP 503 response (as required by Skype for Business), see Section 12.4.
3. Click **Apply** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the devices flash memory.

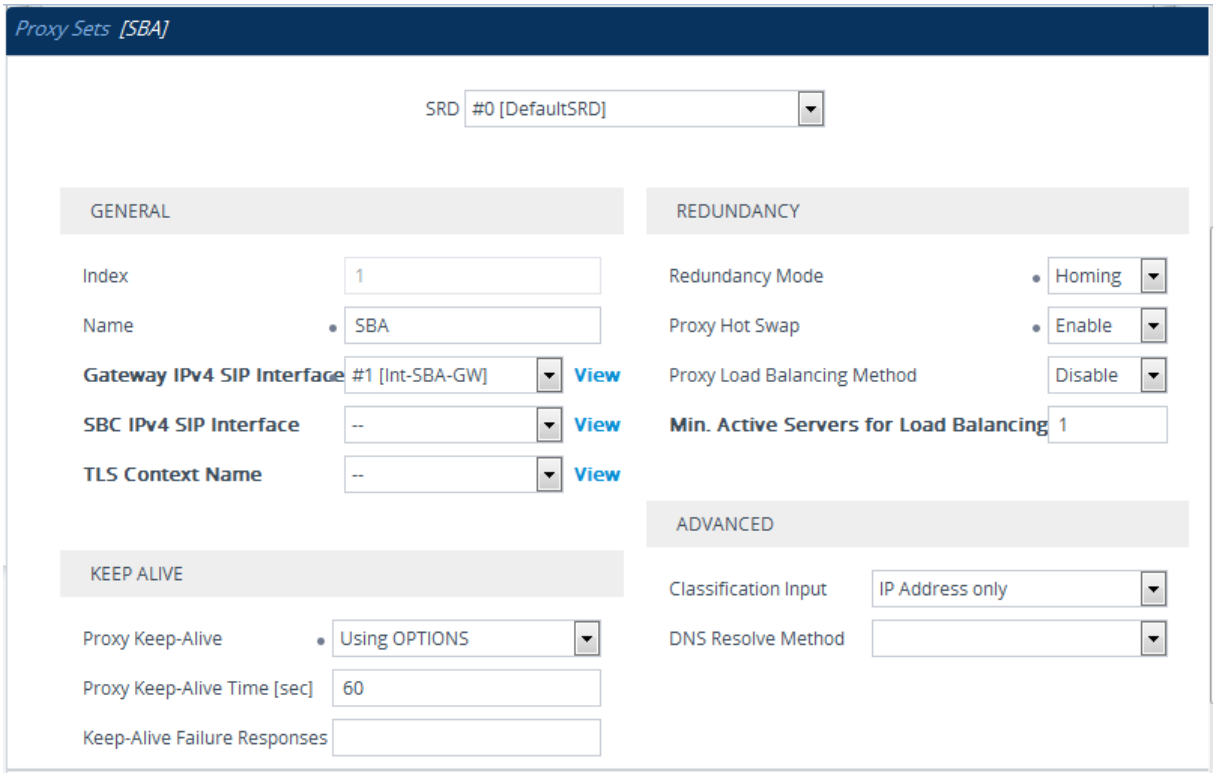
12.3 Step 3: Proxy Sets

This step describes the configuration of the Proxy Set for the Mediation server connection.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets table (**Setup** menu > **Signalling & Media** tab > **Core Entities** > **Proxy Sets**).

Figure 12-3: Proxy Sets Table

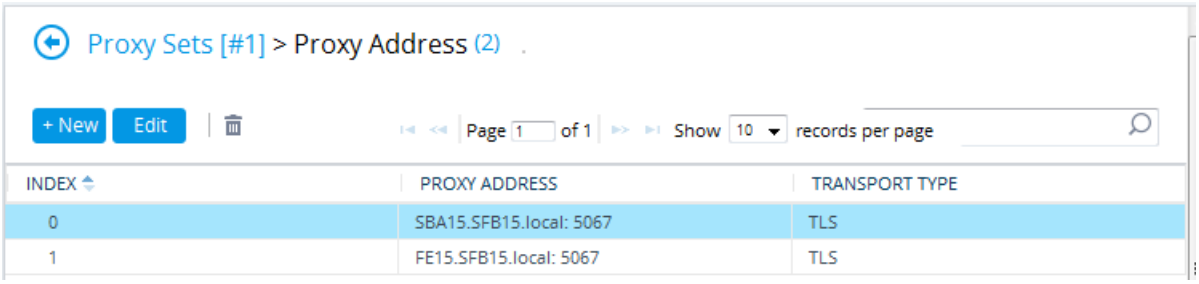


   a. Click the **Add** button to create a Proxy Set for PSTN calls.
   b. From the 'Proxy Keep-Alive' drop-down list, select **Using OPTIONS** to discover whether a particular Mediation Server in the cluster is available.
   c. From the 'Proxy Hot Swap' drop-down list, select **Enable**. If there is no response from the first Mediation Server after a user-defined number of retransmissions, the INVITE message is sent to the redundant Mediation Server. The number of retransmissions is configured by the Number of RTX Before Hot-Swap parameter in the 'Proxy & Registration' page (see Section 13.1).
   d. From the 'Redundancy Mode' drop-down list, select **Homing**. If the SBA application fails and the PSTN Gateway or E-SBC switches over to the Mediation Server at the datacenter, then when the SBA application resumes functionality again, the PSTN Gateway or E-SBC switches back to the Mediation Service on the SBA application.
   e. Click **Apply** to apply your settings.
2. Click the **Proxy Address Table** link at the bottom of the screen.
3. Click the **New** button and configure two proxy servers for redundancy. If the SBA application fails (at the branch office), the PSTN Gateway or E-SBC switches over to the Mediation Server located at the datacenter:
   - Index 0: IP address or FQDN of the Mediation Server running on the device and configure **TLS** Transport type with port **5067**.

- Index 1: IP address or FQDN of the Mediation Server running at the datacenter and configure **TLS** Transport type with port **5067**.

Note: If you configured the Mediation Server address as an FQDN, ensure that you configure the DNS server (see Section 13.8.3).

Figure 12-4: Proxy Sets Address List



4. Click **Apply** to apply your settings.
5. On the toolbar, click **Burn** to save the changes to the devices flash memory.

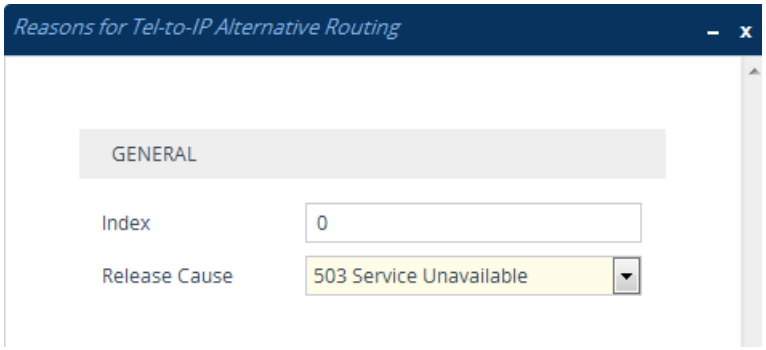
12.4 Step 4: Reasons for Alternative Routing

This step describes how to configure reasons for alternative routing for Tel-to-IP calls.

➢ **To configure reasons for Alternative Tel-to-IP Routing:**

1. Open the 'Reasons for Alternative Routing' page (**Setup** menu > **Signalling & Media** tab > **Gateway** > **Routing** > **Alternative Routing Reasons > Reasons for Tel-to-IP**).
2. Click **New** to add a new entry with the Release Cause **503 Service Unavailable**.

Figure 12-5: Add Alternative Reason

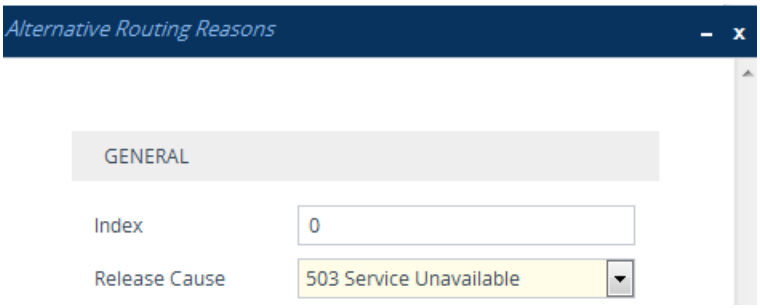


3. Click **Apply** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the devices flash memory.

➢ **To configure reasons for Alternative SBC Routing:**

1. Open the 'SBC Alternative Routing' page (**Setup** menu > **Signalling & Media** tab > **SBC** > **Routing** > **Alternative Reasons**).
2. Click **New** to add a new entry with the Release Cause **503 Service Unavailable**.

Figure 12-6: Add Alternative Reason



3. Click **Apply** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the devices flash memory.

➢ To Configure Fake Retry After (for both Gateway and SBC):

1. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

Figure 12-7: SIP Definitions General Settings

2. In 'Fake Retry After' field, enter the time **60** (in seconds). When the PSTN Gateway or E-SBC receives a SIP 503 response (from the Mediation Server) without a Retry-After header, the PSTN Gateway or E-SBC behaves as if the 503 response includes a Retry-After header with this user-defined period.
3. Click **Apply** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the devices flash memory.

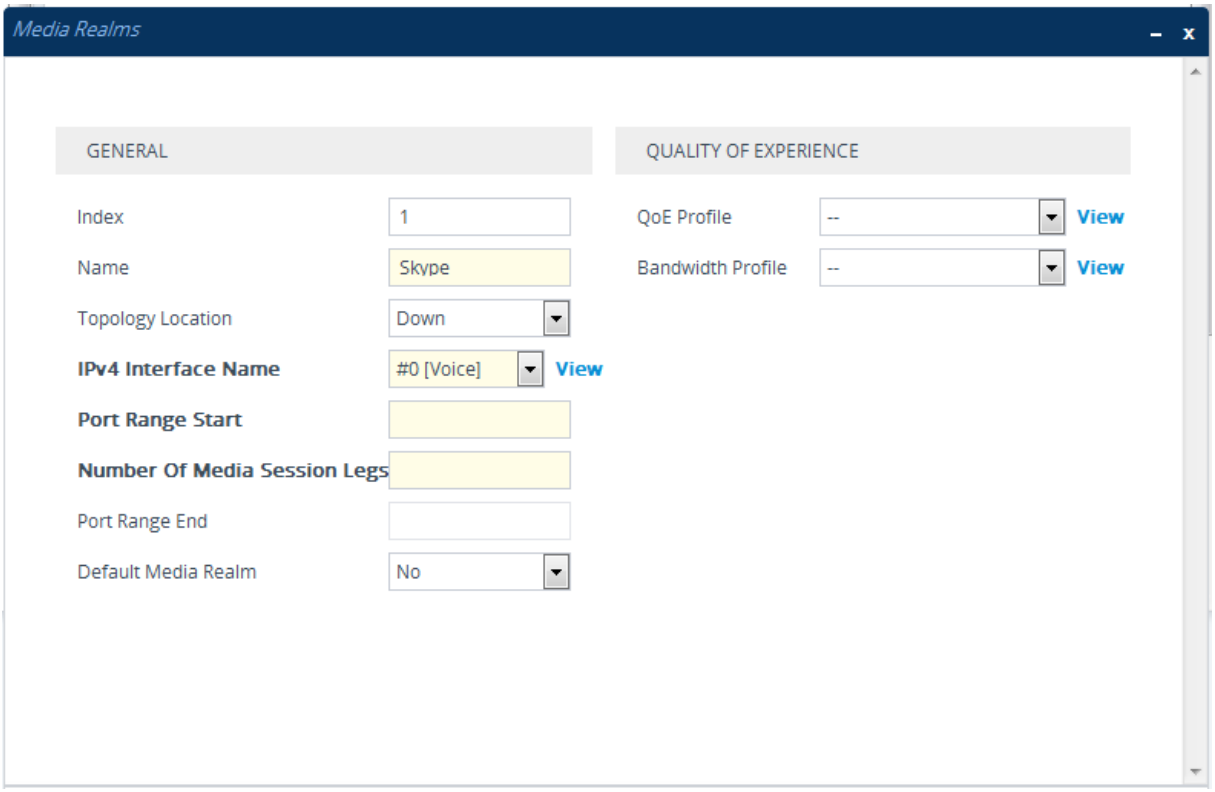
12.5 Step 5: Media Realms

This step describes how to create a Media Realm for the PSTN and SBC media.

➢ **To create a Media Realm:**

1. Open the Media Realms table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realms** table).

Figure 12-8: Media Realm-LAN



2. Click **New** to add a Media Realm for LAN:
   a. Configure the Port Start Range.
   b. Ensure that the Number of Media Session Legs is configured according to the feature key.
   c. Click **Save**.
3. (SBC only) Click **New** to add a Media Realm for WAN:
   a. Configure the Port Start Range.
   b. Ensure that the Number of Media Session Legs is configured according to the feature key.
   c. Click **Save**.

Figure 12-9: Media Realm-WAN

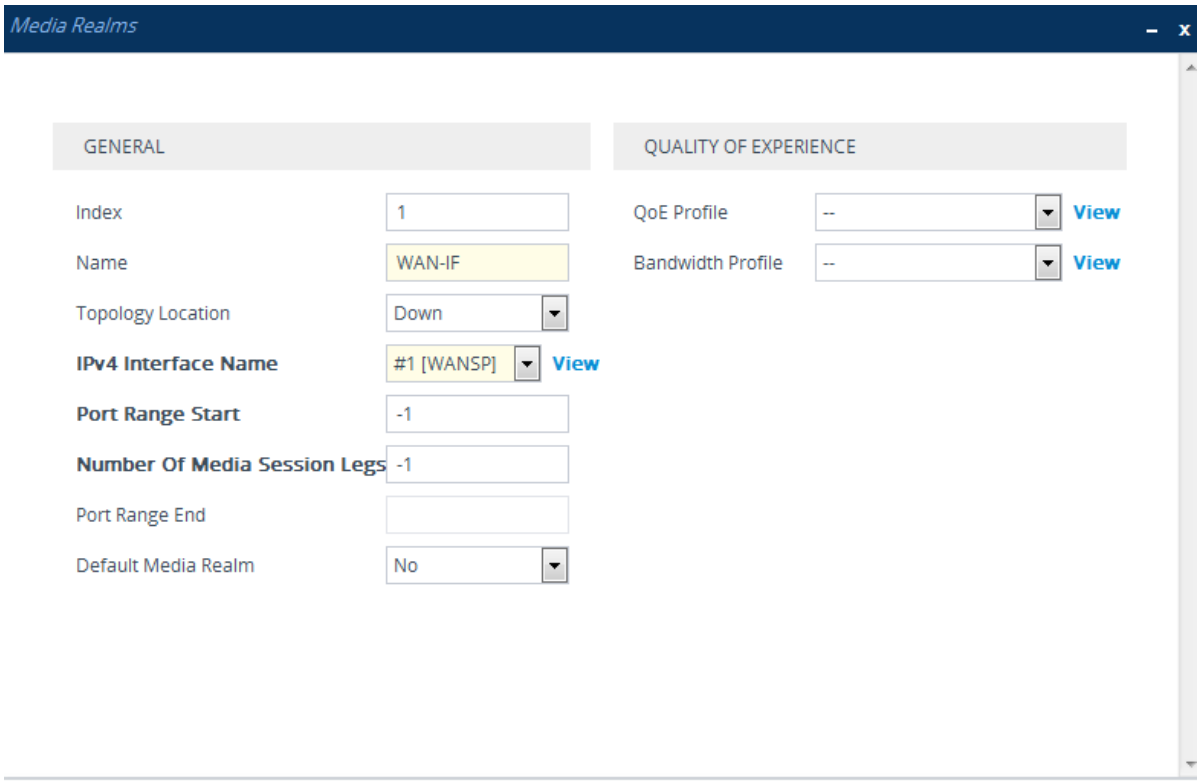
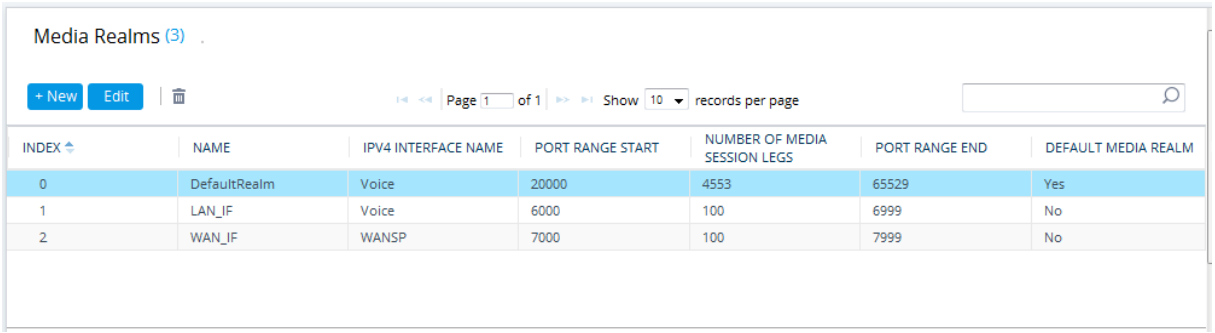


Figure 12-10: Configured Media Realms



4. Click **Apply** to apply your settings.
5. On the toolbar, click **Burn** to save the changes to the devices flash memory.

12.6 Step 6: SIP Interfaces (SBC Only)

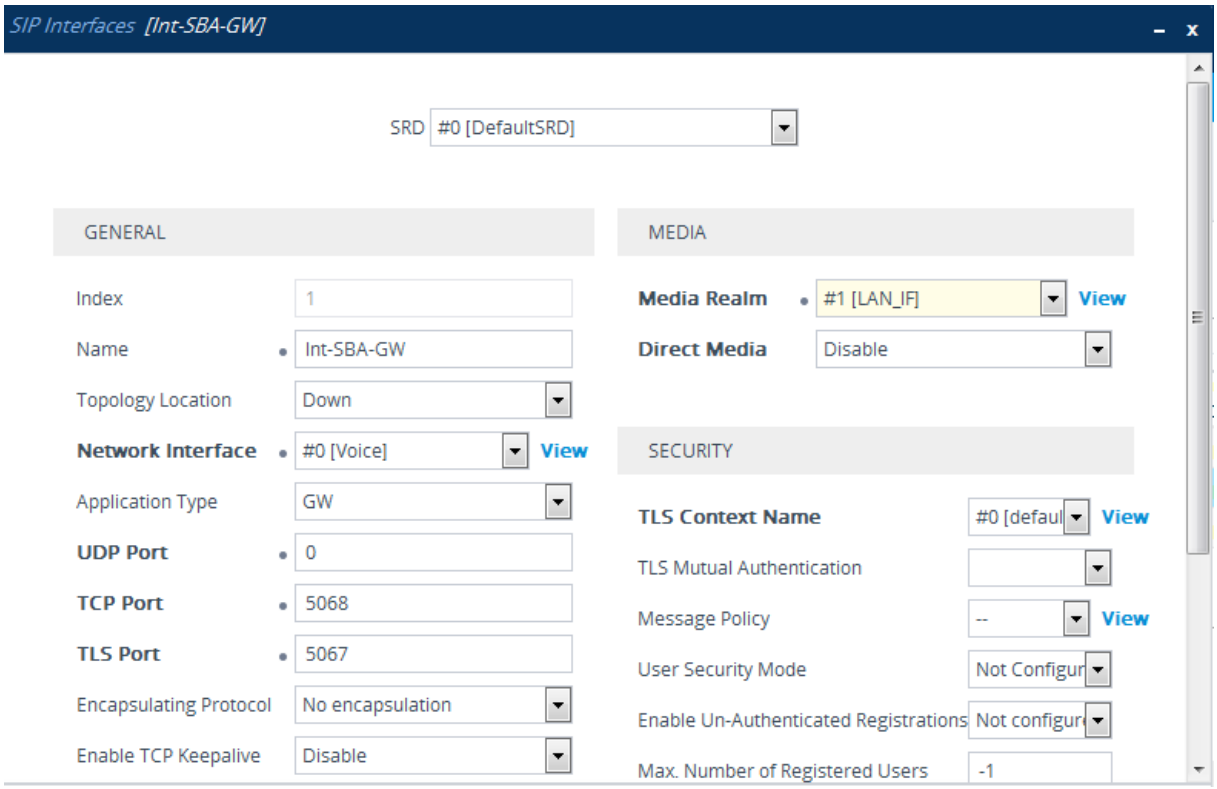
This step.describes how to configure the SIP interfaces for the SBC calls.

Note: The gateway application uses the default SIP interface (you later configure this interface for TLS see Section 12.9). However, you may create a new SIP interface for the gateway application if you wish to change default settings.

➢ **To configure SIP interfaces:**

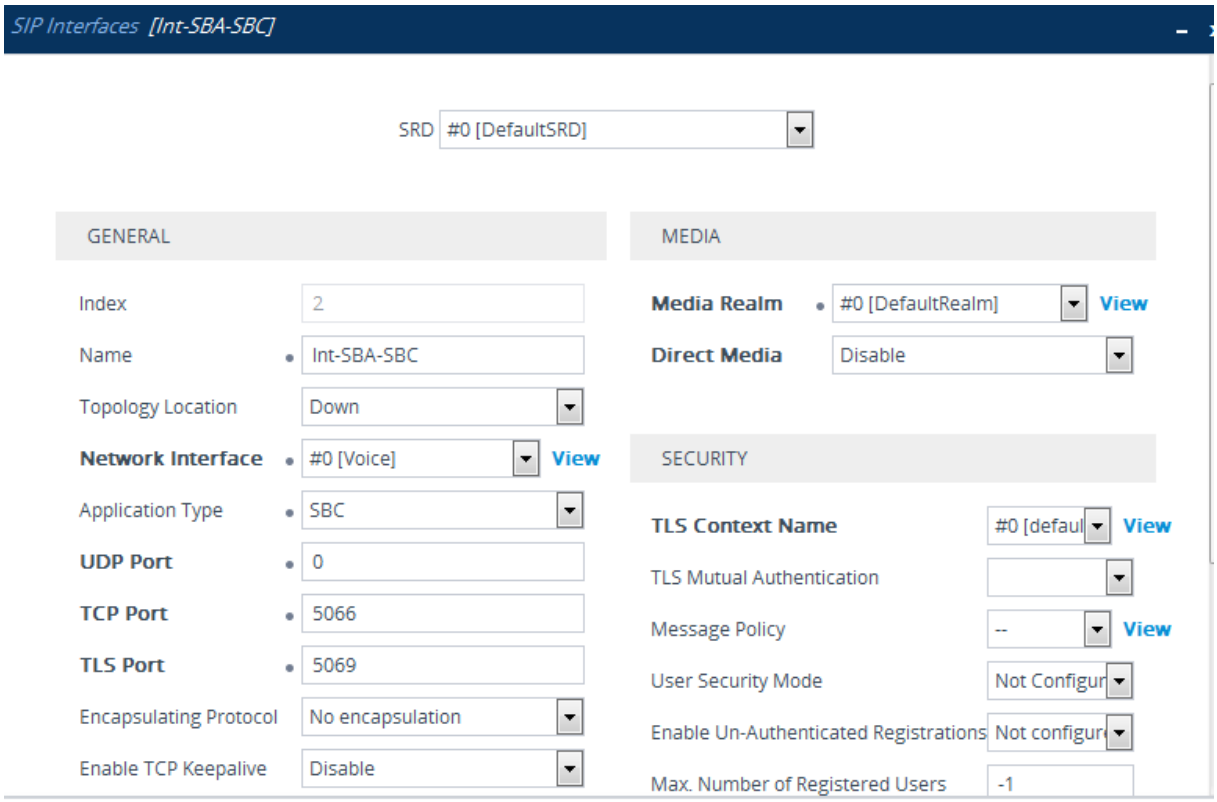
1. Open the SIP Interfaces table page (**Configuration** tab > **VoIP** menu > **VoIP Network**> **SIP Interface Table**).
2. Click **New** to add a SIP Interface for the LAN SBC calls:

Figure 12-11: Gateway SIP Interface



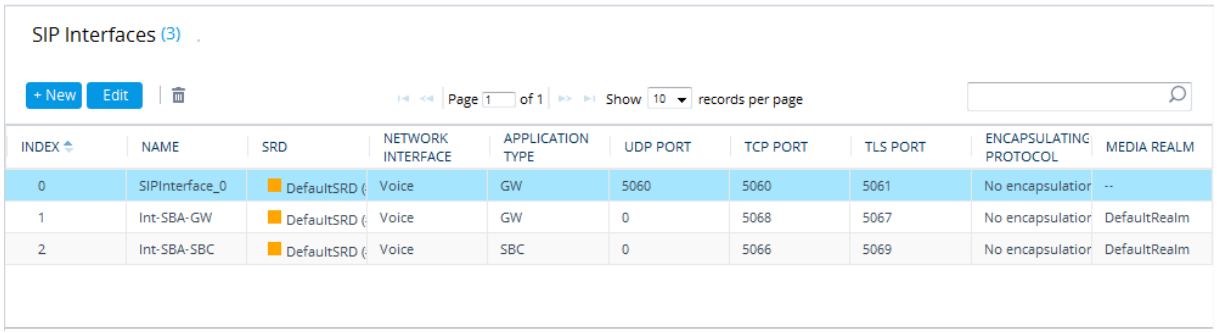
   a. From the Application Type drop-down list, select the GW application type.
   b. From the Media Realm drop-down list, select the Media Realm for the LAN that you configured above.
   c. In the 'TLS Port' field, enter **5067**.
   d. Click **Apply** to apply your settings.
3. Click **New** to add a SIP Interface for the LAN SBC calls:
   a. From the Application Type drop-down list, select the GW application type.
   b. From the Media Realm drop-down list, select the Media Realm for the LAN that you configured above.
   c. In the 'TLS Port' field, enter **5067**.
   d. Click **Apply** to apply your settings.

Figure 12-12: SBC SIP Interface



4. Repeat the above steps if you are configuring a connection with a remote IP-PBX or SIP trunk interface.
5. On the toolbar, click **Burn** to save the changes to the devices flash memory.

Figure 12-13: Configured SIP Interfaces



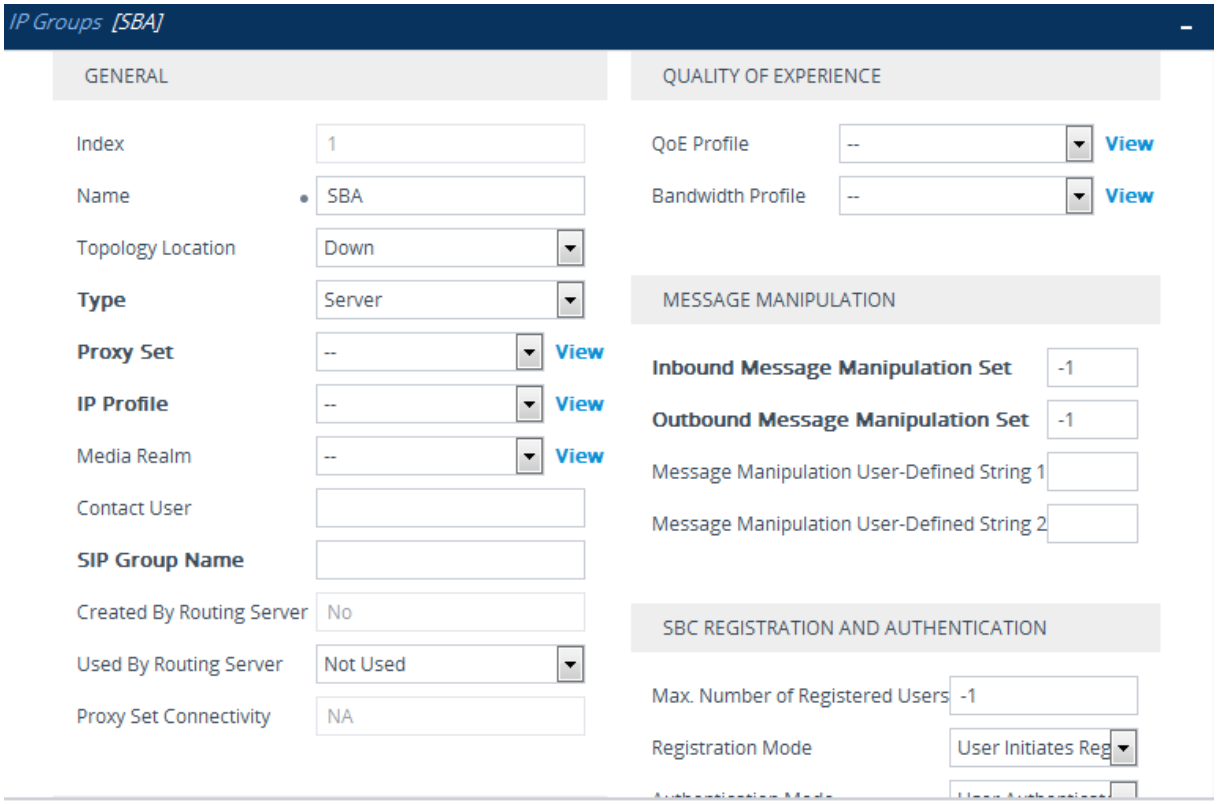
12.7 Step 7: IP Groups

This step describes how to create an IP Group for the PSTN calls and SBC calls.

➢ **To add IP Groups:**

1. Open the IP Group table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   a. Click **New** to create an IP Group of Type 'Server' for the PSTN calls.
   b. Click **Apply** to apply your settings.

Figure 12-14: IP Group-Gateway



12.7.1 SBC

This step describes how to configure an SBC IP Group. The IP Group represents an IP entity on the network with which the SBC communicates. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In the SBA and SBC topology, IP Groups must be configured for the following IP entities:

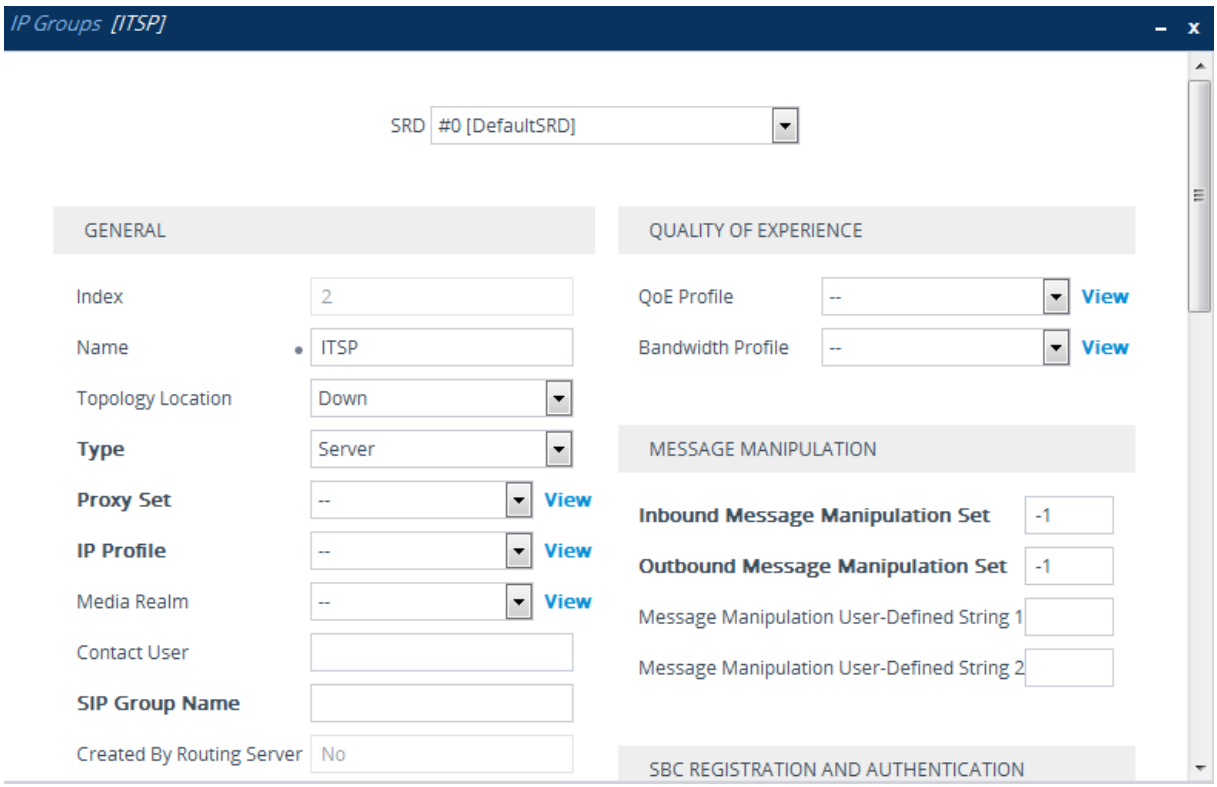
- SBC Mediation Server located on LAN (see example configuration below)
- Vendor SIP Trunk or IP-PBX located on WAN (refer to the relevant AudioCodes Interop documentation).

➢ **To create an IP Group for the Skype for Business Server 2015:**

1. Open the IP Group table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**.

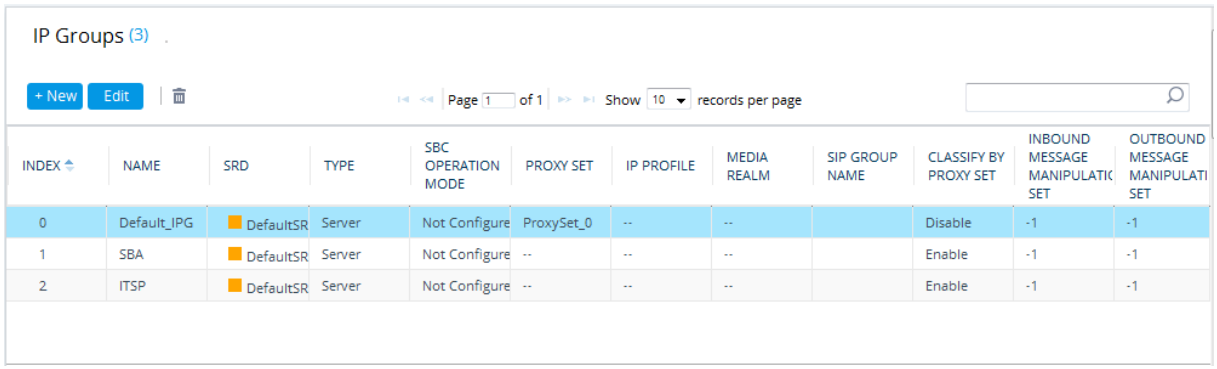
2. Click **New** to create an IP Group of Type 'Server'.

Figure 12-15: IP Group-SIP Trunk/IP-PBX



a. Configure the Skype for Business Proxy Set that you created in Section 12.3.
b. Configure the Skype for Business Media Realm that you configured in Step 0.
c. Click **Apply** to apply your settings.

Figure 12-16: Configured IP Groups



12.8 Step 8: Routing

This step describes how to configure Tel-to-IP and IP-to-IP Routing.

12.8.1 IP-to-Tel Routing

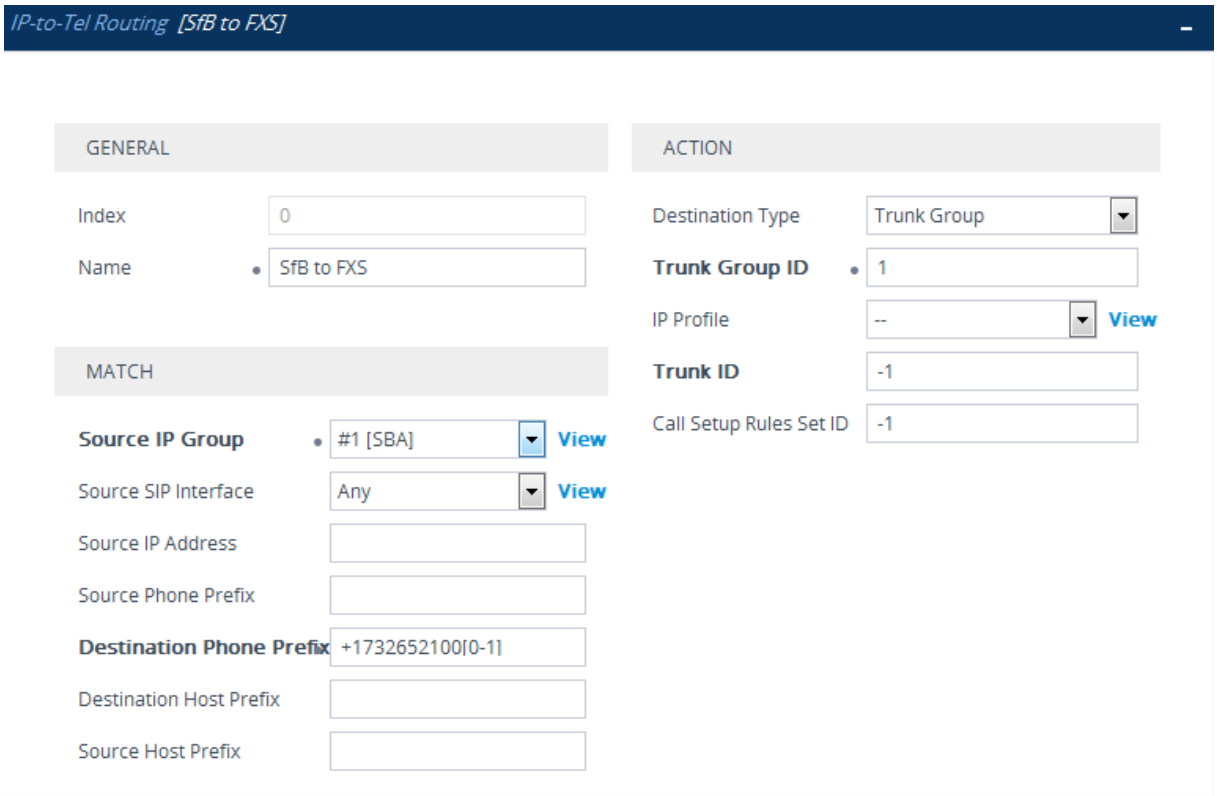
This step describes how to configure IP-to-Tel routing for the gateway calls.

➢ **To configure IP-to-Tel routing:**

1. Open the IP-to-Tel Routing page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing** >**IP-to-Tel Routing**).

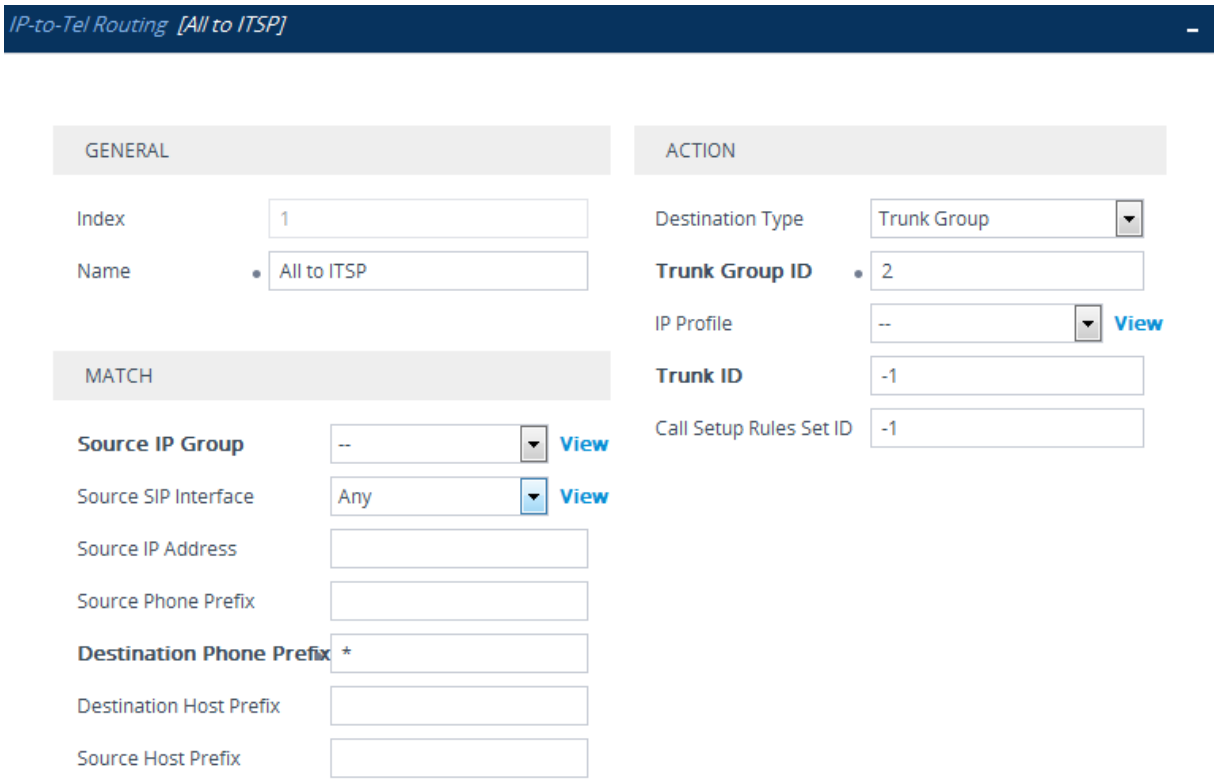
2. Click **New** to create an IP-to-Tel Routing rule for Skype for Business to FXS gateway calls.

Figure 12-17: IP-to-Tel Routing Rule (Skype for Business to FXS)



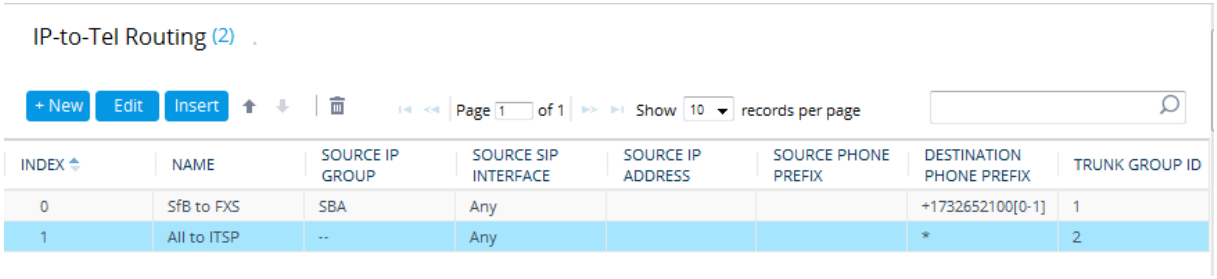
3. Click **Apply** to apply your settings.
4. Click **New** to create an IP-to-Tel Routing rule for ITSP calls.

Figure 12-18: IP-to-Tel Routing Rule (All to ITSP)



5. Click **Apply** to apply your settings.
6. On the toolbar, click **Burn** to save the changes to the devices flash memory.

Figure 12-19:Configured IP-to-Tel Routing Rules



12.8.2 IP-to-IP Routing

This step describes how to configure IP-to-IP call routing rules.

For the SBA topology, the following IP-to-IP routing rules need to be configured to route calls between Skype for Business Server 2015 (LAN) and Vendor SIP Trunk or IP-PBX (WAN):

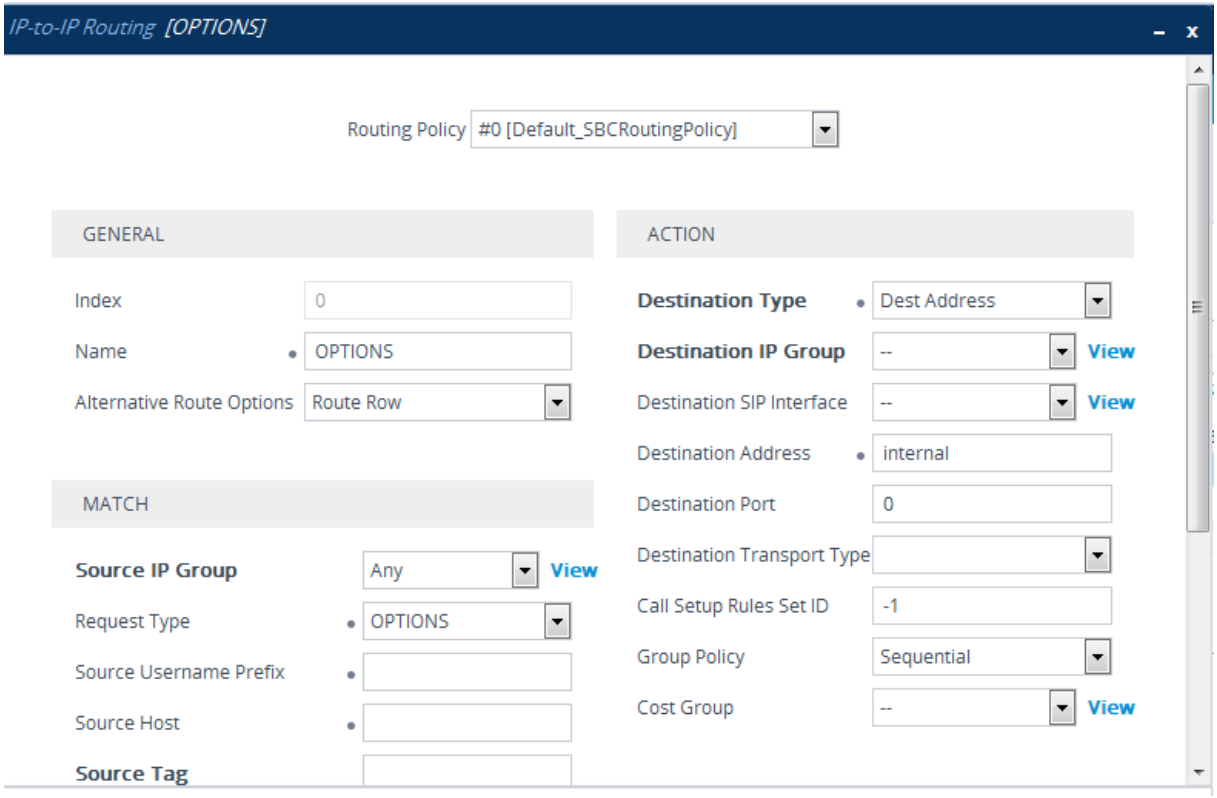
- Calls from Skype for Business Server 2015 to Vendor SIP Trunk or IP-PBX (see example below)
- Calls from Vendor SIP Trunk or IP-PBX to Skype for Business Server 2015 (refer to relevant AudioCodes Interop documentation).

➢ **To configure IP-to-IP routing for Skype for Business Server 2015:**

1. Open the IP-to-IP Routing page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Create a new IP-to-IP Routing OPTIONS rule:

a. Click **New** to create a new rule.

Figure 12-20: IP-to-IP Routing Options Rule

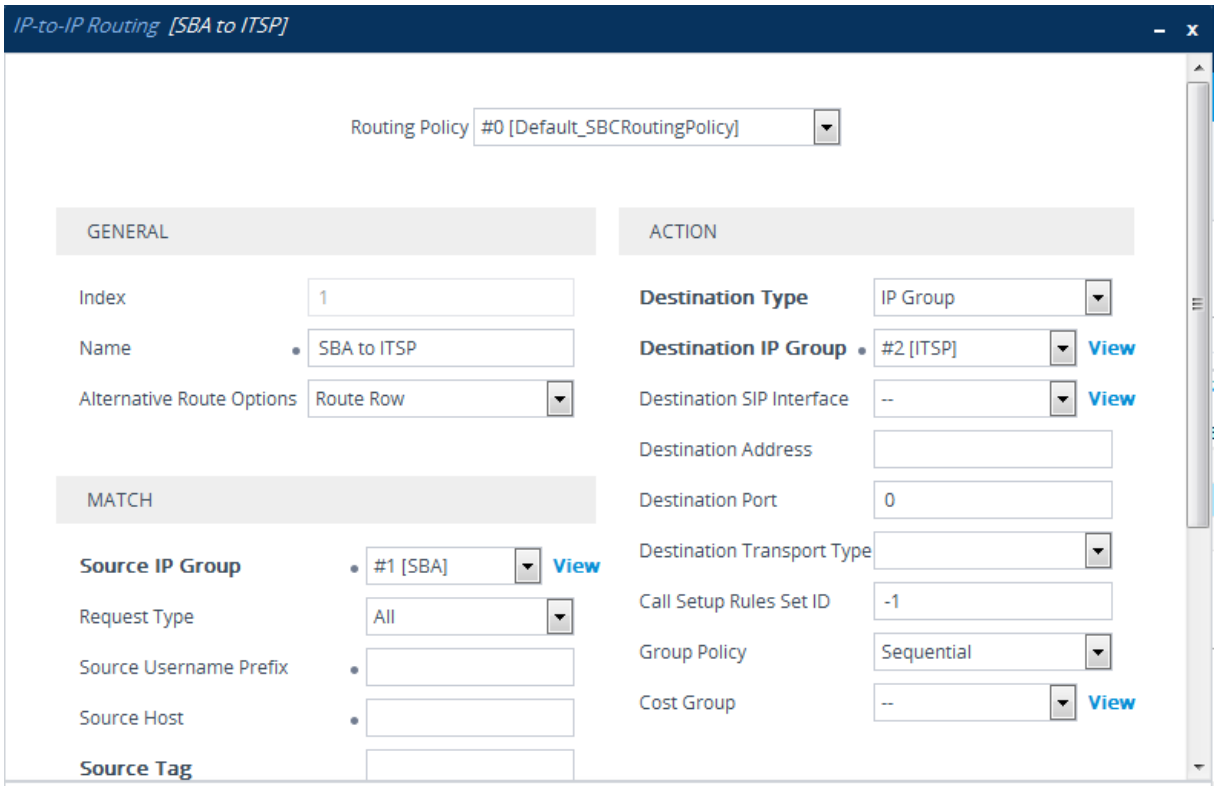


b. Click **Apply** to apply your settings.

3. Create a new IP-to-IP Routing rule for SBA to ITSP calls.

a. Click **New** to create a new rule.

Figure 12-21: SBA to ITSP Routing Rule

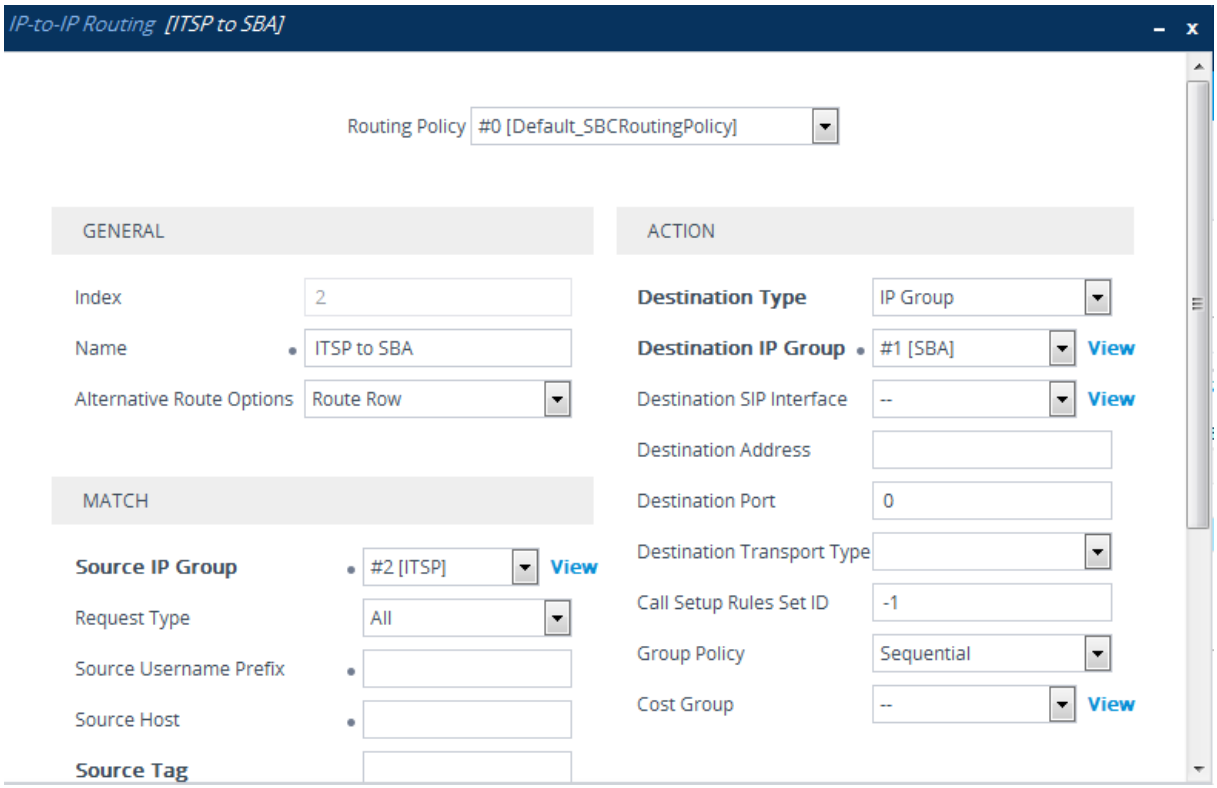


b. Click **Apply** to apply your settings.

4. Create a new IP-to-IP Routing rule for ITSP to SBA calls:

a. Click **New** to create a IP-to-IP Routing rule for SBA to ITSP calls.

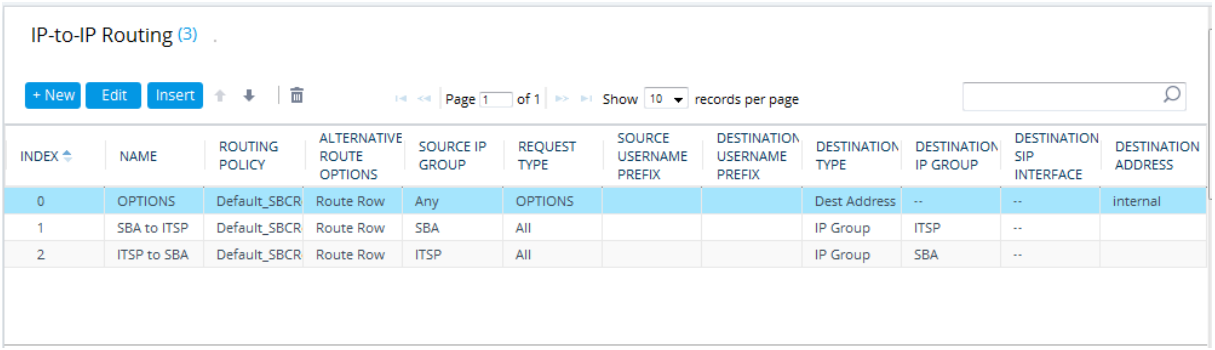
Figure 12-22: ITSP to SBA Routing Rule



b. Click **Apply** to apply your settings.

5. On the toolbar, click Burn to save the changes to the devices flash memory.

Configured IP-to-IP Routing Rules



12.9 Step 9: SIP TLS Connection

TLS provides encrypted SIP signaling between the PSTN Gateway or E-SBC and the Mediation Server. When using TLS, you also need to configure the Gateway or E-SBC with a certificate for authentication during the TLS handshake with the Mediation Server.

12.9.1 Step 9-1: Enable SIP TLS Listening Port

This step describes how to configure the SIP TLS listening port (see Section 0).

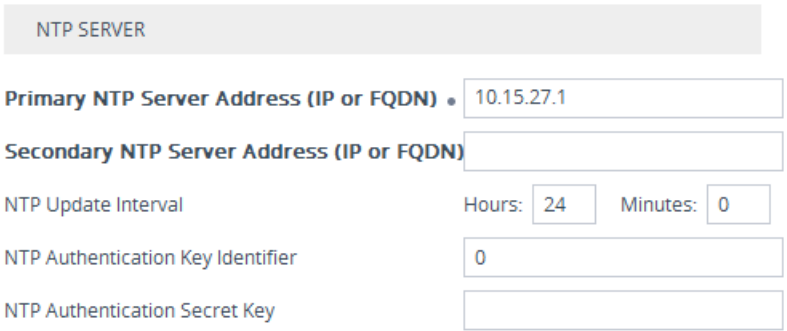
12.9.2 Step 9-2: Configure the NTP Server Address

The procedure below describes how to configure the Network Time Protocol (NTP) server. This is important for maintaining the correct time and date on the PSTN Gateway or E-SBC, by synchronizing it with a third-party NTP server. This ensures that the PSTN Gateway or E-SBC has the same date and time as the Certification Authority (CA).

➢ **To configure the NTP server address:**

1. Open the Time & Date page (**Setup** tab > **Time And Date**).

Figure 12-23: Configuring NTP Server Address



2. In the 'Primary NTP Server Address (IP or FQDN)' field, enter the IP address of the NTP server.
(e.g., **10.15.27.1**).
3. Configure the appropriate Time Zone.

Note: If you configured the NTP address as an FQDN, ensure that you configure the DNS server (see Section 13.8.3).

4. Click **Apply** to apply your settings.
5. On the toolbar, click **Burn** to save the changes to the devices flash memory.

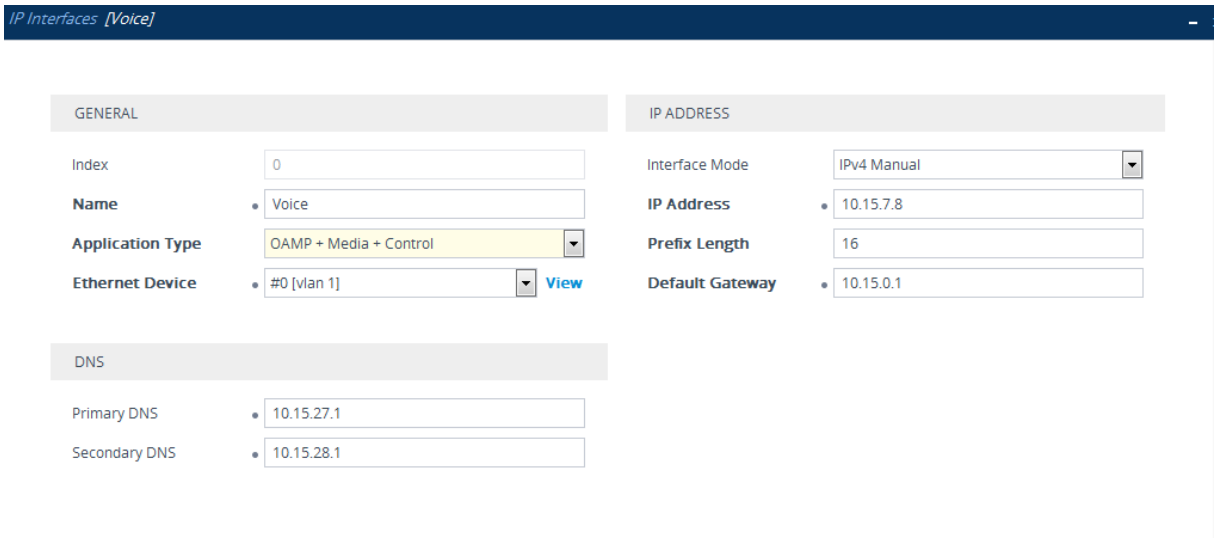
12.9.3 Step 9-3: Configure the DNS Server

The procedure below describes how to configure the IP address of the Domain Name System (DNS) servers. This is required if the Mediation Server is configured with an FQDN, in which case, the DNS is used to resolve it into an IP address.

➢ **To configure the DNS servers:**

1. Open the Interface Table page (**Setup** tab > **IP Network** menu > **Core Entities** folder> I**P Interfaces**).
2. Create a new IP interface for the Voice interface:
   a. Click **New** to create a new interface.
   b. In the 'Primary DNS' and 'Secondary DNS' fields, enter the IP address of the Primary and Secondary DNS server respectively.

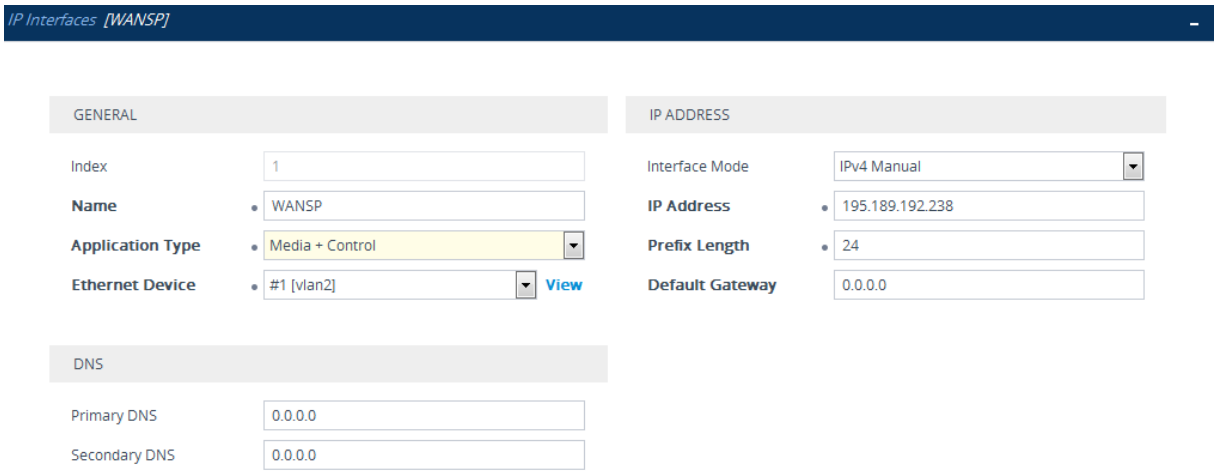
Figure 12-24: IP Interface-Voice



   c. Click **Apply** to apply your changes.

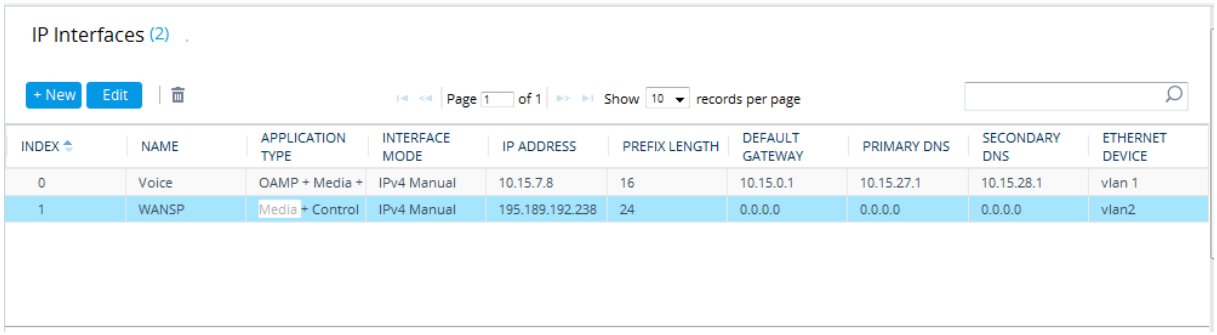
3. Create a new IP interface for the WAN interface:
   a. Click **New** to create a new interface.

Figure 12-25: IP Interface-WAN



   b. Click **Apply** to apply your changes
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

Figure 12-26: Configured IP Interfaces



12.9.4 Step 9-4: Configure Gateway or E-SBC Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the device to authenticate the connection with Skype for Business Server 2015.[1]

The procedure involves the following main steps:

a. Generating a Certificate Signing Request (CSR).
b. Requesting Device Certificate from CA.
c. Obtaining Trusted Root Certificate from CA.
d. Deploying Device and Trusted Root Certificates on E-SBC.

Note: The Subject Name (CN) field parameter should be identically configured in the DNS Active Directory and Topology Builder (see Chapters 8 and 9).

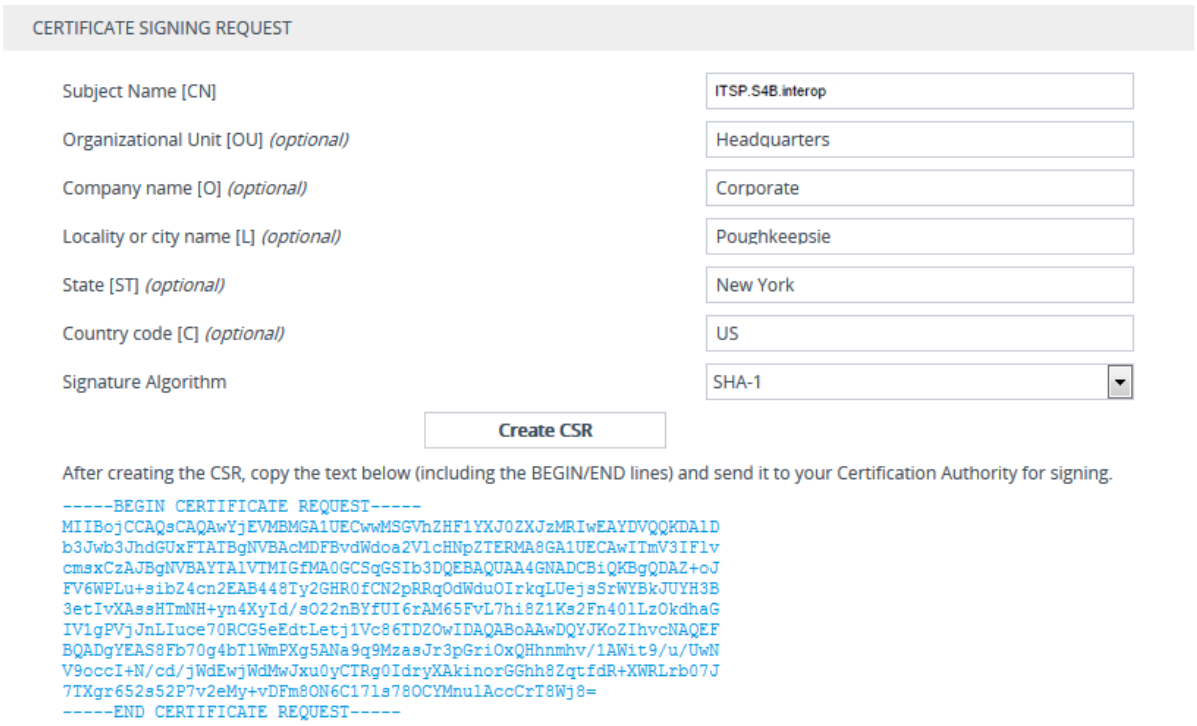
➢ **To configure a certificate:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click the **Change Certificate** link, located at the bottom of the TLS Contexts page; the Change Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Subject Name [CN]' field, enter the E-SBC FQDN name (e.g., **Gateway.S4B.interop**).
      This FQDN is also configured in the Topology Builder.
   b. Fill in the rest of the request fields according to your security provider's instructions.

[1] You cannot load certificates to the device for the Gateway and SBC TLS context using the SBA Wizard.

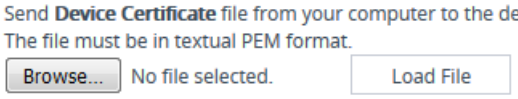
4. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 12-27: Certificate Signing Request – Creating CSR



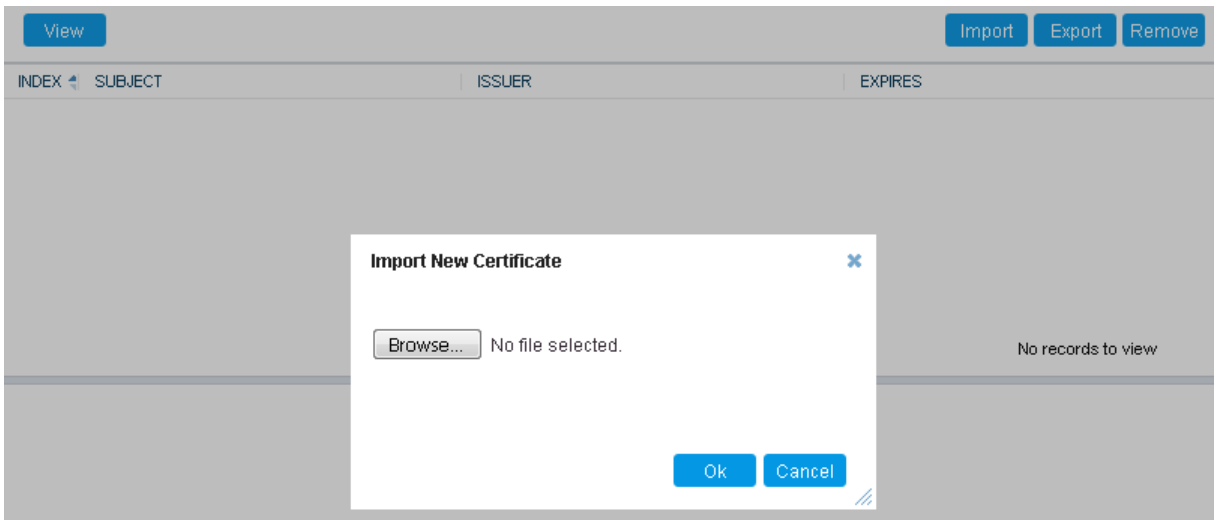
5. Copy the CSR from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----"** to a text file (such as Notepad), and then save it to a folder on your computer with the file name *certreq.txt*.
6. Send the *certreq.txt* to your system administrator.
7. Save the file you received from your system administrator as *certroot.cer* to a folder on your computer.
8. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
   a. In the TLS Contexts table, select the required TLS Context index row (typically, the default TLS Context at Index 0 is used), and then click the **Change Certificates** link, located at the bottom of the TLS Contexts page; the Change Certificates page appears.
   b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 1414, and then click **Send File** to upload the certificate to the E-SBC.

Figure 12-28: Upload Device Certificate Files from your Computer Group



   c. In the E-SBC's Web interface, return to the **TLS Contexts** page.
   d. In the TLS Contexts table, select the required TLS Context index row, and then click the **Trusted-Roots Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   e. Click the **Import** button, and then select the certificate file to load.

Figure 12-29: Importing Root Certificate into Trusted Certificates Store



9. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
10. Click **Submit** to apply your changes.
11. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.
12. On the toolbar, from the Device Actions drop-down list, choose **Reset**, and then in the'Maintenance Actions' page, click the **Reset** button; the Mediant 1000B resets and your settings are saved to the flash memory.

13 Configure IP Profile

This step describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In the SBA and SBC topology, IP Profiles need to be configured for the following IP entities:

- Microsoft Skype for Business Server 2015 - to operate in secure mode using SRTP and TLS (see example below)
- Vendor SIP trunk or IP-PBX- to operate in non-secure mode using RTP and UDP (refer to relevant AudioCodes Interop documentation).
- Connection to analog device.

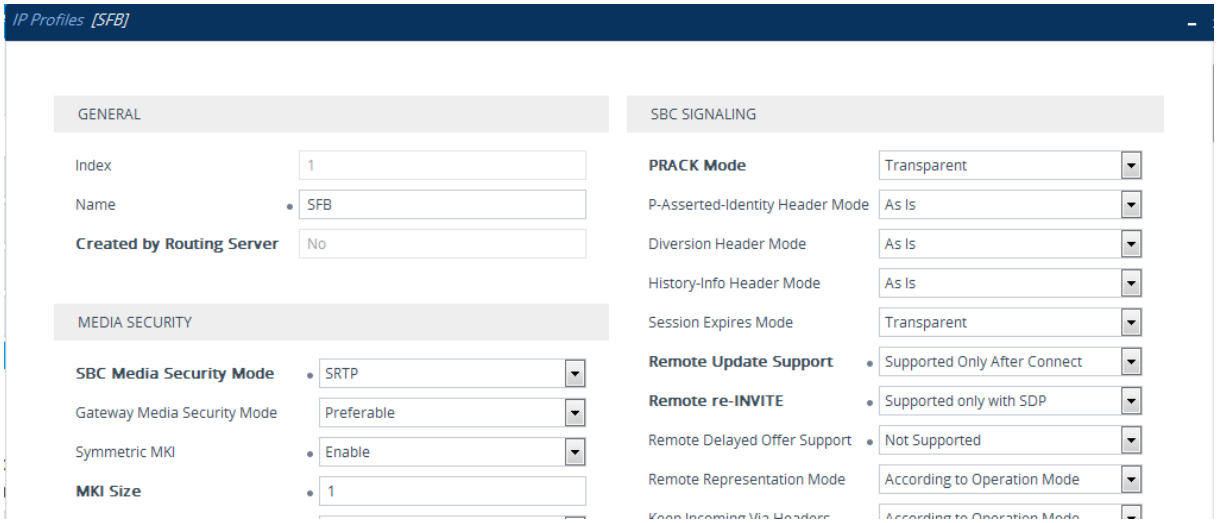
➢ **To configure IP Profile for the Skype for Business Server 2015:**

1. Open the IP Profile Settings page (**Setup** tab > **Signaling & Media** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	**1**
Name	**S4B**
Media Security	
SBC Media Security Mode	**SRTP** (set to **RTP** if the Skype for Business site does not support SRTP i.e. if the 'Encryption Support Level' parameter is set to "Not Supported" in the Trunk Configuration in the Skype for Business Topology.
Symmetric MKI	**Enable**
MKI Size	**1**
SBC Enforce MKI Size	**Enforce**
Reset SRTP State Upon Re-key	**Enable**
Generate SRTP Keys Mode:	**Always**
SBC Early Media	
Remote Early Media RTP Detection Mode	**By Media** (required, as Skype for Business Server 2015 does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
Use Silence Suppression	**Transparent** or **Add**
SBC Signaling	
Remote Update Support	**Supported Only After Connect**
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**

SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally** (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)
Remote 3xx Mode	**Handle Locally** (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)

Figure 13-1: Skype for Business IP Profile



3. Click **Apply** to apply your settings.

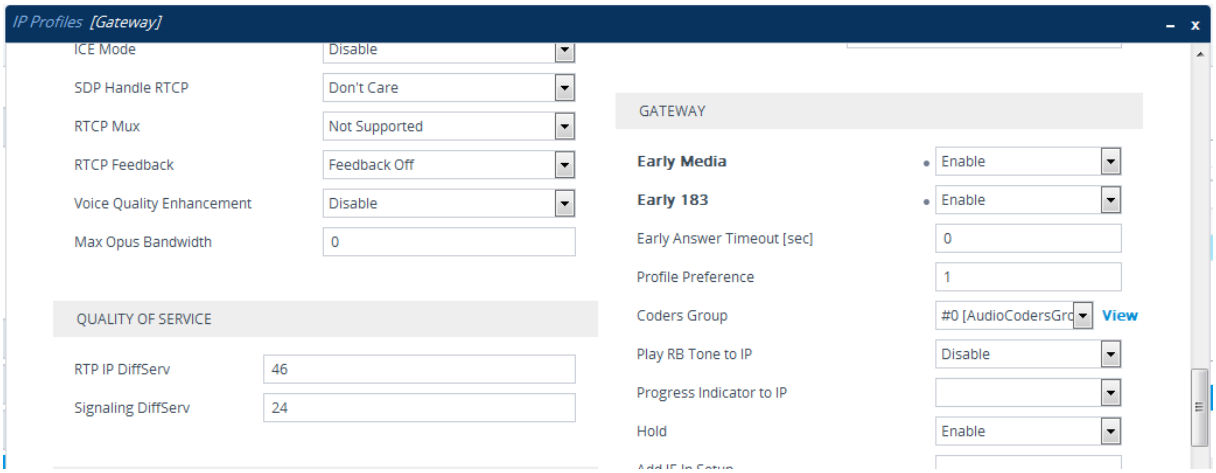
➢ To configure IP Profile for the Skype for Gateway:

1. Open the IP Profile Settings page (**Setup** tab > **Signaling & Media** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	**1**
Name	**Gateway**
Media Security	
Gateway Media Security Mode	**Mandatory** (set to **Preferable-Single media** if SRTP is not supported i.e. if the 'Encryption Support Level' parameter is set to "Not Supported" in the Trunk Configuration in the Skype for Business Topology.
Symmetric MKI	**Enable**
MKI Size	**1**
SBC Enforce MKI Size	**Enforce**
Reset SRTP State Upon Re-key	**Enable**
Generate SRTP Keys Mode:	**Always**
Gateway	

Early Media	**Enable** Enables the Early Media feature for sending media (e.g., ringing) before the call is established per specific calls. This parameter can also be configured globally (see Section 13.1.1).
Early 183	**Enable** Enables the device to send SIP 183 responses with SDP to the IP upon receipt of INVITE messages per specific calls. This parameter can also be configured globally (see Section 13.1.1)

Figure 13-2: Gateway IP Profile



3. Click **Apply** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the devices flash memory.

13.1 Configuring Early Media (Global Settings)

Early media refers to audio and video that is exchanged before a call is accepted by the recipient. In the IP Profile configuration (see above in Section 13), you can configure early media settings according to specific calls. These parameters can also be configured globally and in addtion, there are also other global settings.

13.1.1 PSTN Gateway

According to Skype for Business requirements, AudioCodes PSTN Gateway must send a SIP 183 with SDP immediately after it receives an INVITE. The RTP packets however, will not be sent until the PSTN Gateway receives an ISDN Progress, Alerting and Progress Indicator or Connect message. For example, if the PSTN Gateway receives ISDN Progress, it starts sending RTP packets according to initial negotiation, but there is no need to re-send the 183 response.

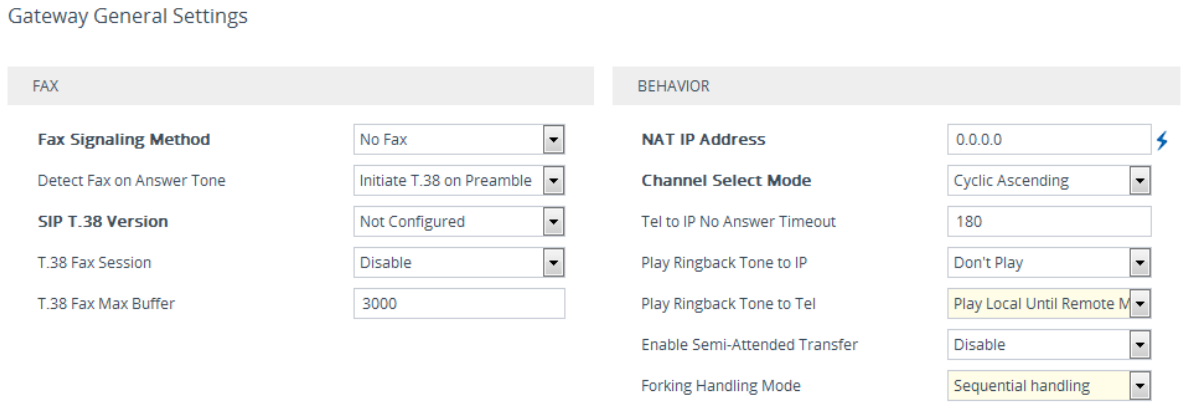
➢ **To configure the Early Media feature for the gateway:**

1. Open the Gateway General Settings page (**Setup** tab > **Signaling & Media** > **Gateway** menu > **Gateway General Settings**).
2. From the 'Play Ringback Tone to Tel' drop-down list, select **Play Local Until Remote Media Arrive**. If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current

180 response), the PSTN Gateway plays a local ringback tone if there are no prior received RTP packets. The PSTN Gateway stops playing the local ringback tone as soon as it starts receiving RTP packets. At this stage, if the PSTN Gateway receives additional 18x responses, it does not resume playing the local ringback tone.

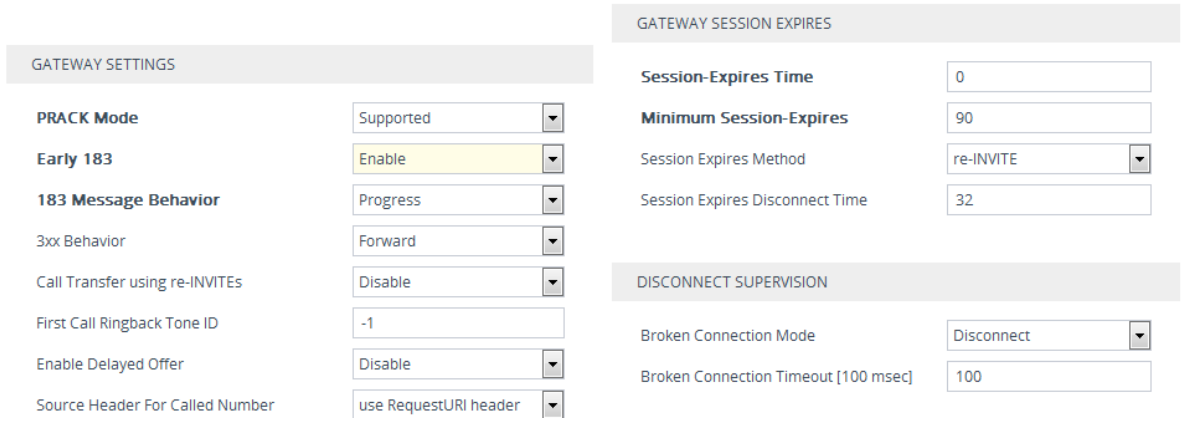
3. From the 'Forking Handling Mode' drop-down list, select **Sequential handling**. The PSTN Gateway opens a voice stream toward the first 18x SIP response that includes an SDP and disregards any 18x response with an SDP received thereafter.

Figure 13-3: Gateway General Settings Page



4. Click **Apply** to apply your settings.
5. Open the SIP Definitions General Settings page (**Setup** tab > **Signaling & Media** > **SIP Definitions** menu > **SIP Definitions General Settings**).

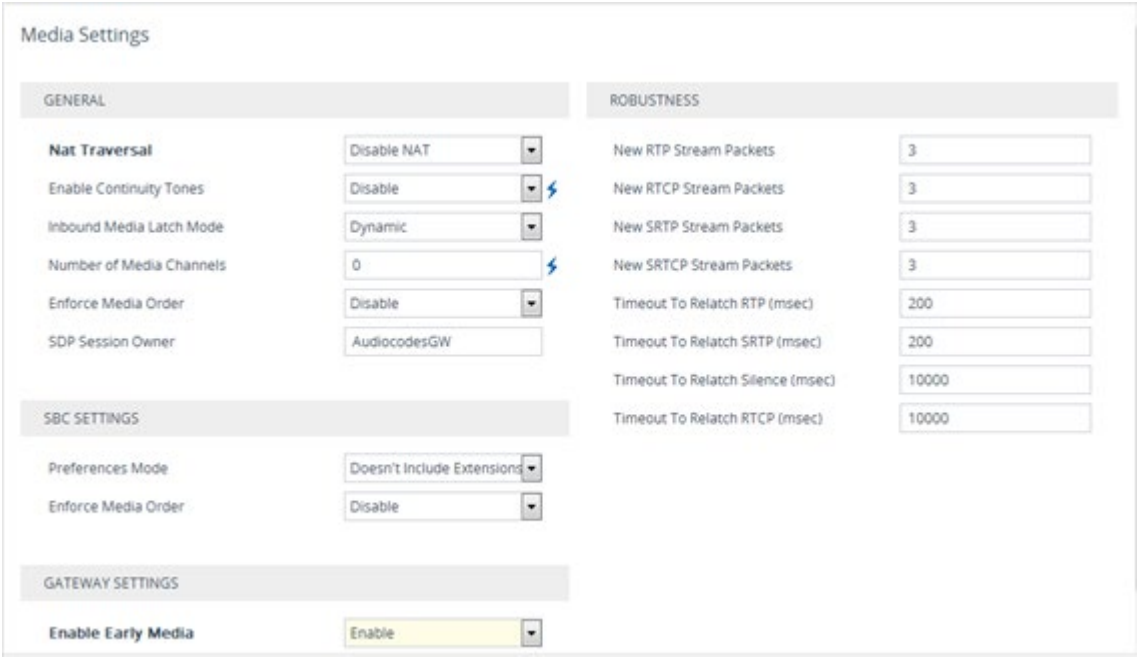
Figure 13-4: SIP Definitions General Settings



6. From the 'Early 183' drop-down list, select **Enable**.

   You can also configure this parameter per call in the IP Profile (see Section 13).
7. Click **Apply** to apply your settings.
8. Open the Media Settings page (**Setup** tab > **Signaling & Media** > **Media** > **Media Settings**.

Figure 13-5: Media Settings-Enable Early Media



9. From the 'Enable Early Media' drop-down list, select **Enable**.
   You can also configure this parameter per call in the IP Profile (see Section 13).

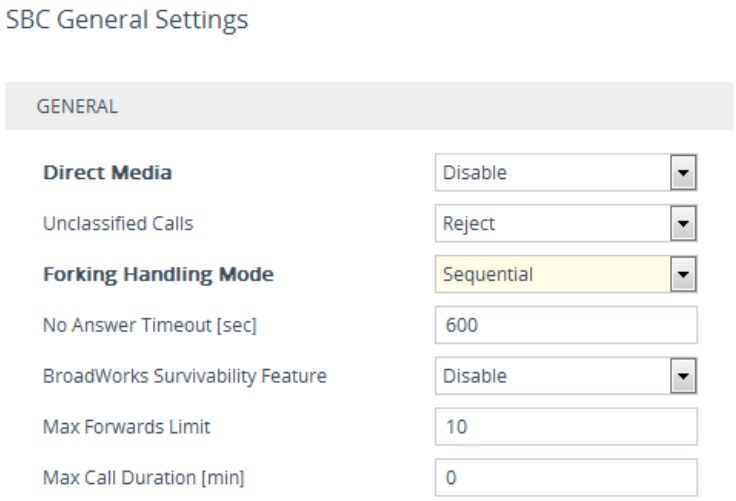
13.1.2 Forking Handling-SBC

You should configure the SBC forking handling so that the SBC opens a voice stream toward the first 18x SIP response that includes an SDP and disregards any 18x response with an SDP received thereafter.

➢ **To configure Forking Handling Mode for the SBC:**

1. Open the SBC General Settings page (**Setup** tab > **Signaling & Media** > **SBC** menu > **SBC General Settings**.
2. From the 'Forking Handling Mode' drop-down list, select **Sequential**.

Figure 13-6: SBC General Setting



3. Click **Apply** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the devices flash memory.

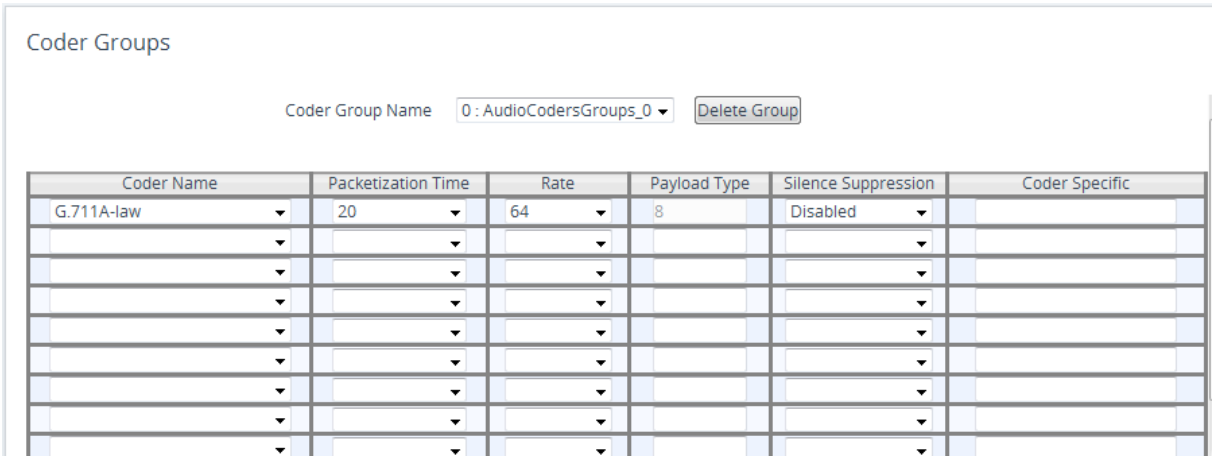
14 Configuring Voice Coders (with Silence Suppression)

The PSTN Gateway or E-SBC communicates with the Mediation Server using either the G.711 A-law or G.711 μ-law (Mu-Law) voice coder. In addition, silence suppression can be enabled per coder, which is recommended for improving the performance of the Mediation Server. The procedure below shows how you can change the default coder.

➢ **To configure the voice coder and silence suppression:**

1. Open the Coder Groups page (**Setup** tab > **Signaling & Media** > **Coders and Profiles** > **Coder Groups**).

Figure 14-1: Coder Groups Page



2. From the 'Coder Name' drop-down list, select the required coder (the Wizard only configures the G711A-law coder by default)[2].
3. From the 'Silence Suppression' drop-down list, select **Enable**[3].
4. Click **Apply** to apply your settings.
5. On the toolbar, click **Burn** to save the changes to the devices flash memory.

[2] Only the G711A-law coder is configured in the SBA Wizard
[3] Not configured by the SBA Wizard

This page is intentionally left blank.

15 Configuring Comfort Noise and Gain Control

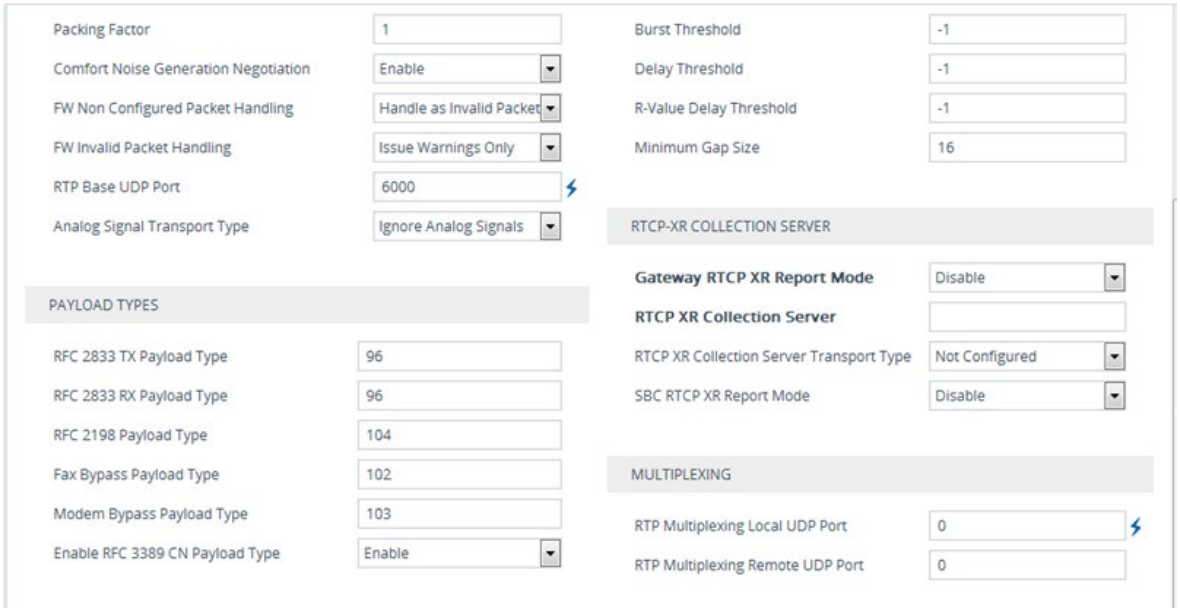
The Skype for Business network provides high voice quality by implementing suppression of typing noise during calls and improved generation of "comfort noise," which reduces hissing and smoothens over the discontinuous flow of audio packets. You may need to configure the PSTN Gateway or E-SBC to match these voice quality features, by enabling silence suppression, comfort noise generation and echo canceller (enabled by default).

Note: Silence suppression is configured per coder type, as described in Chapter 15.

➢ **To configure voice quality:**

1. Open the RTP/RTCP Settings page (**Setup** tab > **Signaling & Media** > **Media** > **RTP/RTCP Settings**).

Figure 15-1: RTP RTCP Settings Page



2. (Gateway Only) From the 'Comfort Noise Generation Negotiation' drop-down list, set **Enable** to enable comfort noise generation.

   For SBC devices, configure parameter 'Use Silence Suppression' in IP Profile (see Chapter 13).
3. From the 'Enable RFC 3389 CN payload Type' drop-down list, verify that this parameter is set to **Enable**.
4. Click **Apply** to apply your settings.
5. On the toolbar, click **Burn** to save the changes to the devices flash memory.

This page is intentionally left blank.

16 Configuring FXS Ports and PSTN Trunks (Gateway Only)

This section describes how to configure FXS ports and PRI (i.e., E1/T1) or BRI trunks connected to the PSTN Gateway.

Note: The SBA Wizard only configures a default Trunk Group, therefore you must perform the configuration described in this section.

16.1 Step 1: Enabling FXS Ports and PSTN Trunks

The procedure below describes how to enable the FXS ports and PSTN trunk (E1/T1) channels of the Enhanced gateway. This is done by defining telephone numbers for the channels and assigning them to Trunk Groups. To ensure correct routing of IP-to-Tel calls, you need to define different Trunk Groups for the digital trunk and the FXS module.

➢ **To enable the FXS ports and PSTN trunks:**

1. Open the Trunk Group Table page (**Setup** tab > **Signaling & Media** > **Gateway** menu > **Trunk** & **Groups** > **Trunk Groups**.

Figure 16-1: Trunk Group Table Page

Trunk Group Table

Add Phone Context As Prefix: Disable
Trunk Group Index: 1-12

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 1 PRI	1	1	1-31	1000	2	None
2	Module 2 FXS			1	17326521000	1	None
3	Module 2 FXS			2	17326521001	1	None
4							None
5							None
6							None
7							None
8							None

2. Define the following Trunk Groups:
   - Trunk Group #2: PRI module (E1/T1) with one span (1-31 channels)
   - Trunk Group #1: FXS module with two FXS channels – Channel 1 with phone number +17326521000 and Channel 2 with phone number +17326521001
   - Those numbers need to be configured as TelUri numbers for analog devices in Skype for Business environment using the powershell command New-CsAnalogDevice.
3. Click **Apply** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the devices flash memory.

16.2 Step 2: Configuring the Channel Select Method

Once you have enabled the PSTN trunk and FXS ports, and assigned them to Trunk Groups, you need to configure the method for which IP-to-Tel calls are assigned to channels within each Trunk Group.

➢ **To configure the channel select method for each Trunk Group:**

1. Open the Trunk Group Settings page (**Setup** tab > **Signaling & Media** > **Gateway** menu > **Trunk** & **Groups** > **Trunk Group Settings**.

Figure 16-2: Trunk Group Setting Page-Trunk Group #1

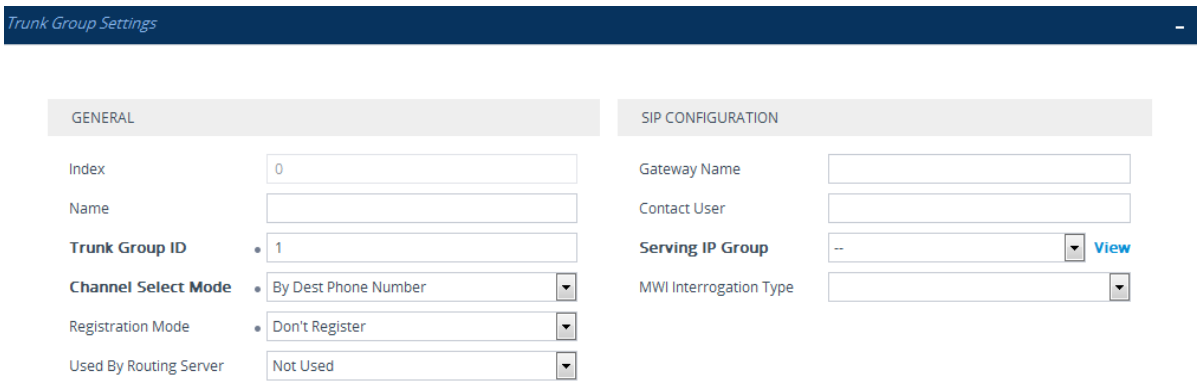


Figure 16-3: Trunk Group Setting Page-Trunk Group #2

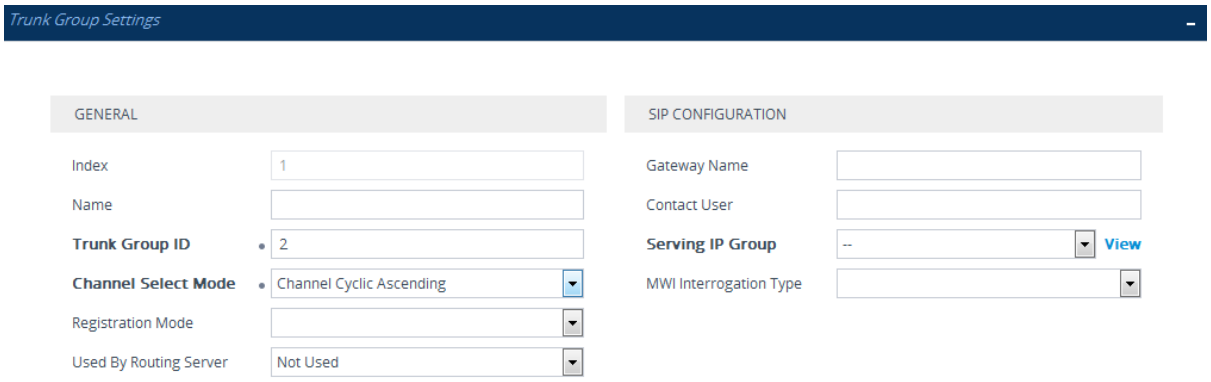
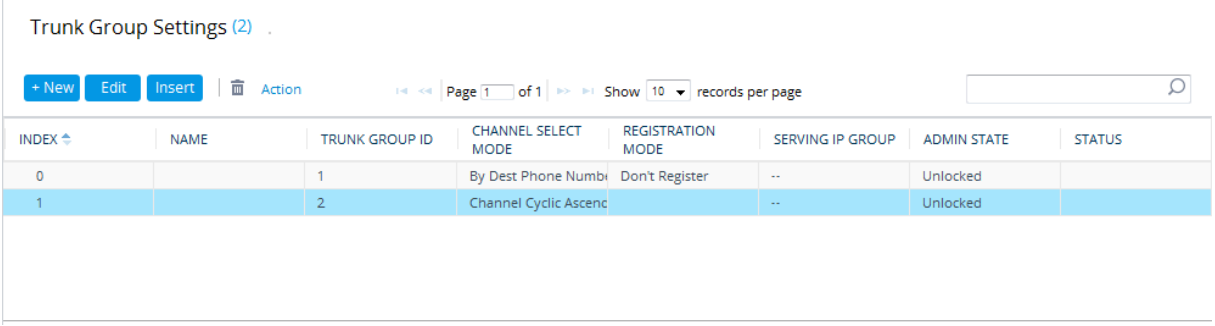


Figure 16-4: Trunk Group Settings Configured



2. For the FXS ports (i.e., Trunk Group #1), from the 'Channel Select Mode' drop-down list, select By Dest Phone Number. This setting sends the call to a specific FXS user according to the called (destination) number.
3. For the PSTN trunk (i.e., Trunk Group #2), from the 'Channel Select Mode' drop-down select Cyclic Ascending. This setting sends the call to the next available channel, in ascending cyclic order.
4. Click **Apply** to apply your settings.
5. On the toolbar, click **Burn** to save the changes to the device's flash memory.

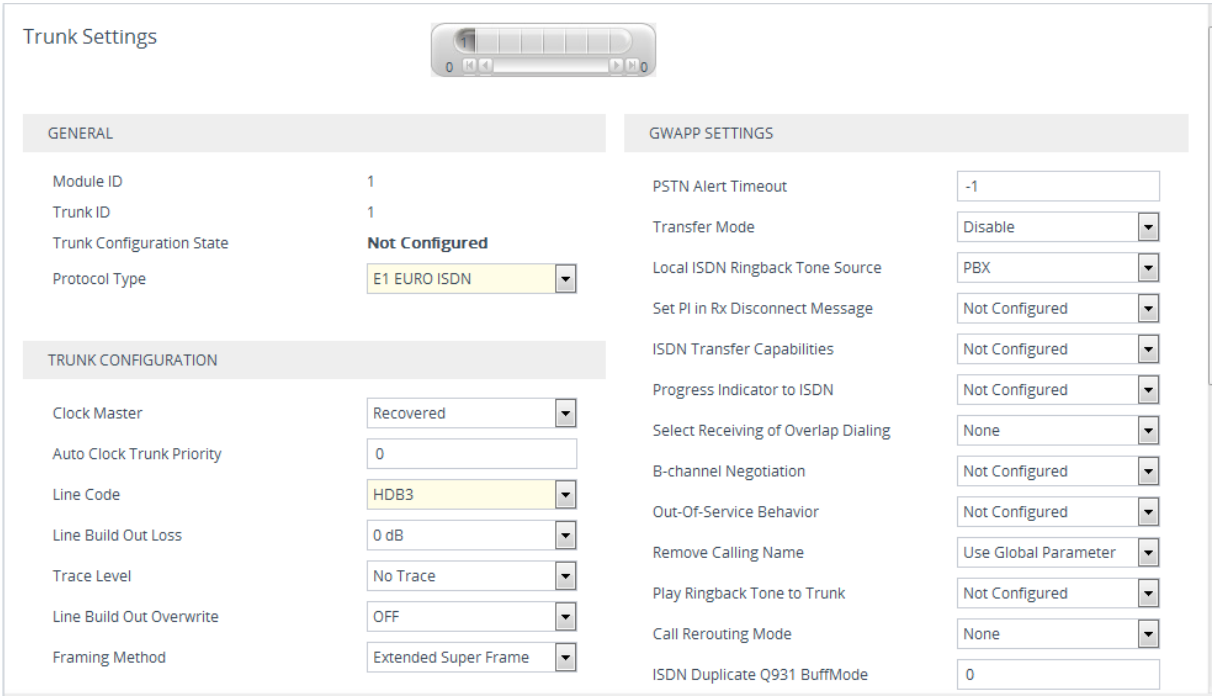
16.3 Step 3: Configuring the Trunk

The procedure below describes basic configuration of the physical trunk.

➢ **To configure the physical trunk:**

1. Open the Trunk Settings page (**Setup** tab > **Signaling & Media** > **Gateway** menu > **Trunks**).

Figure 16-5: Trunk Settings Page



2. On the top of the page, a bar with trunk number icons displays the status of each trunk:
   - Grey - disabled
   - Green - active
   - Yellow - RAI alarm
   - Red - LOS / LOF alarm
   - Blue - AIS alarm
   - Orange - D-channel alarm (ISDN only)

   Select the Trunk that you want to configure, by clicking the desired trunk number icon.
3. If the trunk is new, configure the trunk as required. If the trunk was previously configured, click the Stop Trunk button to de-activate the trunk.
4. Basic trunk configuration:
   a. From the 'Protocol Type' drop-down list, select the required trunk protocol.

Note:

- If the 'Protocol Type' field displays 'NONE' (i.e., no protocol type selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the PSTN Gateway.
- All PRI trunks of the PSTN Gateway must be of the same line type - E1 or T1. However, different variants of the same line type can be configured on different trunks, for example, E1 Euro ISDN and E1 CAS (subject to the constraints in the Release Notes).
- BRI trunks can operate with E1 or T1 trunks.
- If the trunk can't be stopped because it provides the clock (assuming the PSTN Gateway is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the clock or enable 'TDM Bus PSTN Auto Clock' in the 'TDM Bus Settings' page (see Section Configuring the TDM Bus on page 147).
- To delete a previously configured trunk, set the Protocol Type parameter to **NONE**.

5. Continue configuring the trunk according to your requirements.
6. When you have completed configuration, click the **Apply Trunk Settings** button to apply the changes to the selected trunk.
7. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

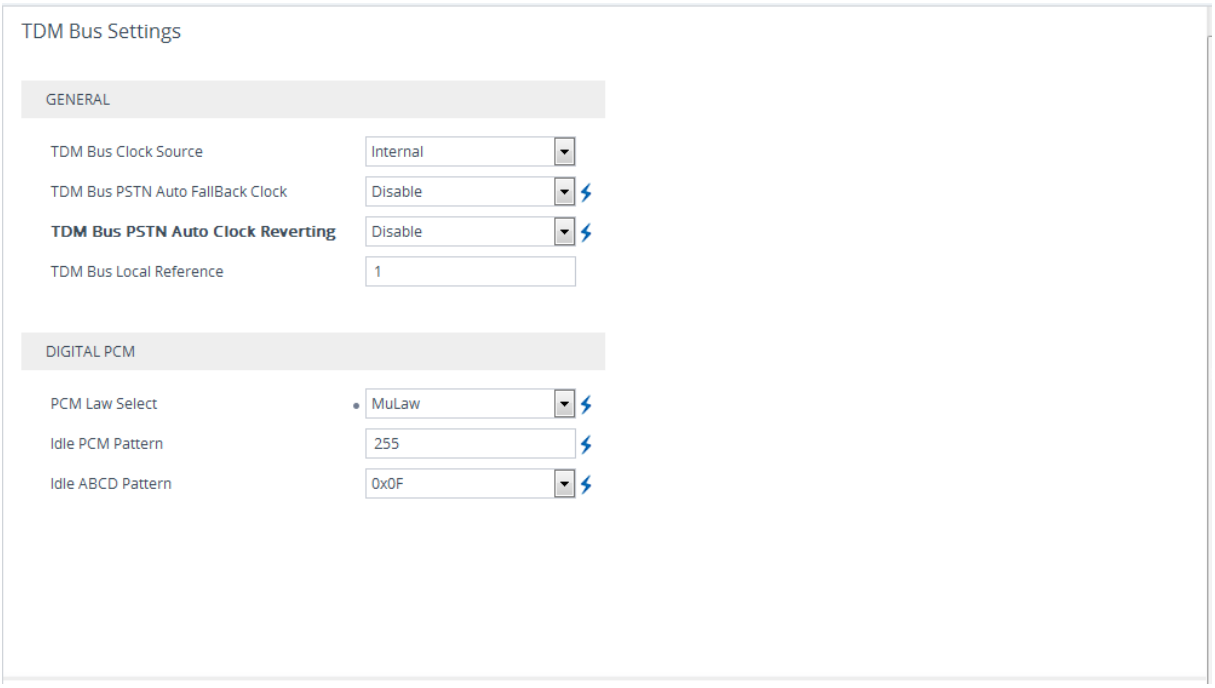
16.4 Step 4: Configuring the TDM Bus

The procedure below describes how to configure the TDM bus of the PSTN Gateway.

➢ **To configure the TDM bus:**

1. Open the TDM Bus Settings page (**Setup** tab > **Signaling & Media** > **Gateway** menu > **Media** > **TDM Bus Settings**).

Figure 16-6: TDM Bus Settings Page



2. Configure the TDM bus parameters according to your deployment requirements.
3. Click **Apply** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

16.5 Step 5: Configuring FXS Port Transfer Behavior

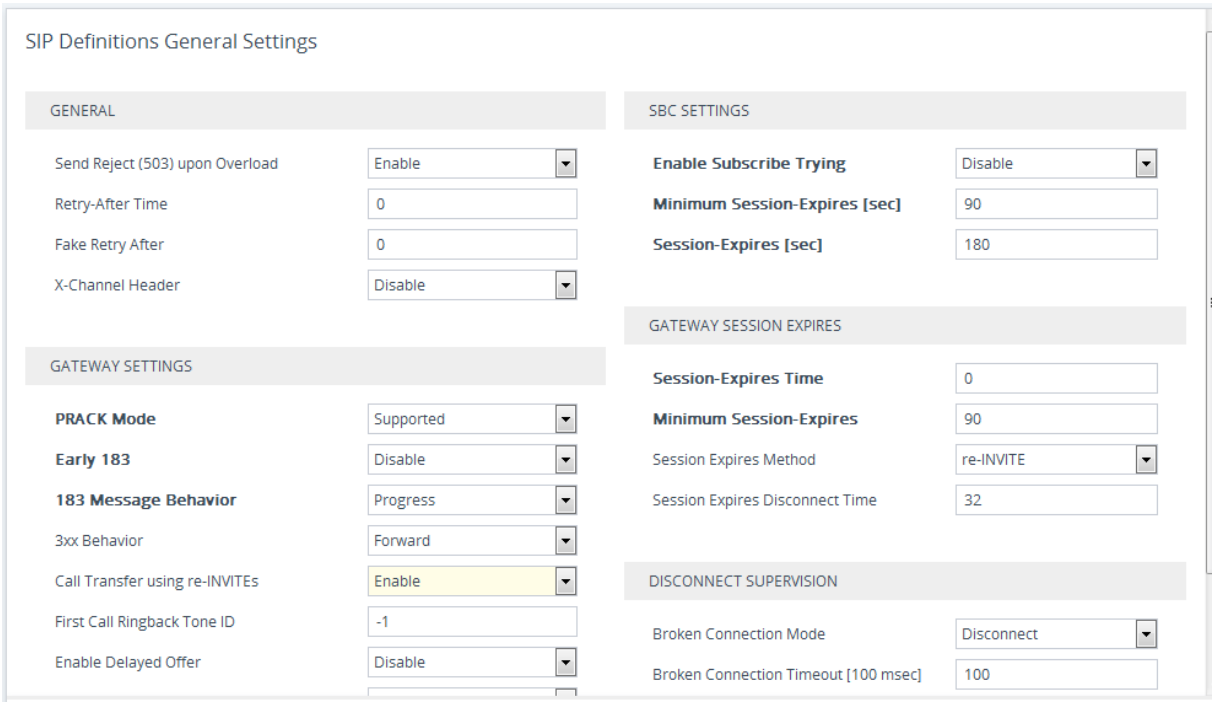
Since the Mediation server does not support receiving SIP Refer messages, you must configure the Enhanced gateway FXS port to send INVITE messages (in the event when call transfer is initiated from the FXS port).

Note: For this feature to work, an MPM module is required, and media channels should be configured according to the number of FXS ports (see below).

➢ **To configure the FXS port transfer feature using the re-invites parameter:**

1. Open the SIP Definitions General Settings page (**Setup** tab > **Signaling & Media** > **SIP Definitions > SIP Definitions General Settings**).
2. From the 'Call Transfer using re-INVITEs' drop-down list, select **Enable**

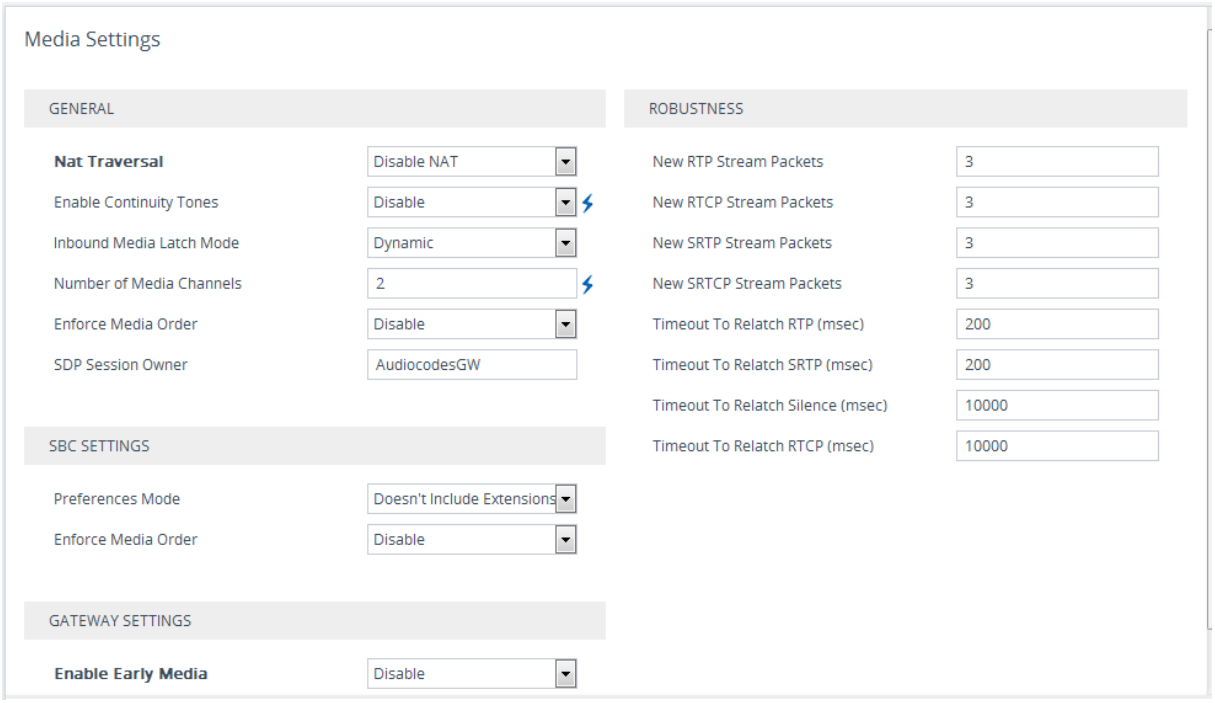
Figure 16-7: Enable Call Transfer Using Re-invites



Note: The above screen reflects a device with the MPM module configured and therefore the Call Transfer using re-INVITEs parameter is visible and configurable.

3. Open the Media Settings page (**Setup** tab > **Signaling & Media** > **Media > Media Settings**).
4. In the 'Number of Media Channels' field, enter the number of media channels; two media channels for each FXS port (device reset required).

Figure 16-8: Media Settings



5. Click **Apply** to apply the changes.
6. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

17 Configuring Number Manipulation Rules

This chapter describes in detail how to configure both gateway and SBC number manipulation rules.

17.1 Configuring Gateway Number Manipulation

Skype for Business implements the standard E.164 format, while the PBX or PSTN implements other number formats for dialing. If the PSTN Gateway is connected to a PBX or directly to the PSTN, the PSTN Gateway may need to perform number manipulations for the called and/or calling number to match the PBX or PSTN dialing rules or to match Skype for Business E.164 format.

Therefore, the PSTN Gateway must be configured with manipulation rules to translate (i.e., normalize) numbers dialed in standard E.164 format to various formats, and vice versa. Manipulation needs to be done for outbound calls (i.e., calls received from Skype for Business clients through Skype for Business) and inbound calls (i.e., calls destined to Skype for Business clients).

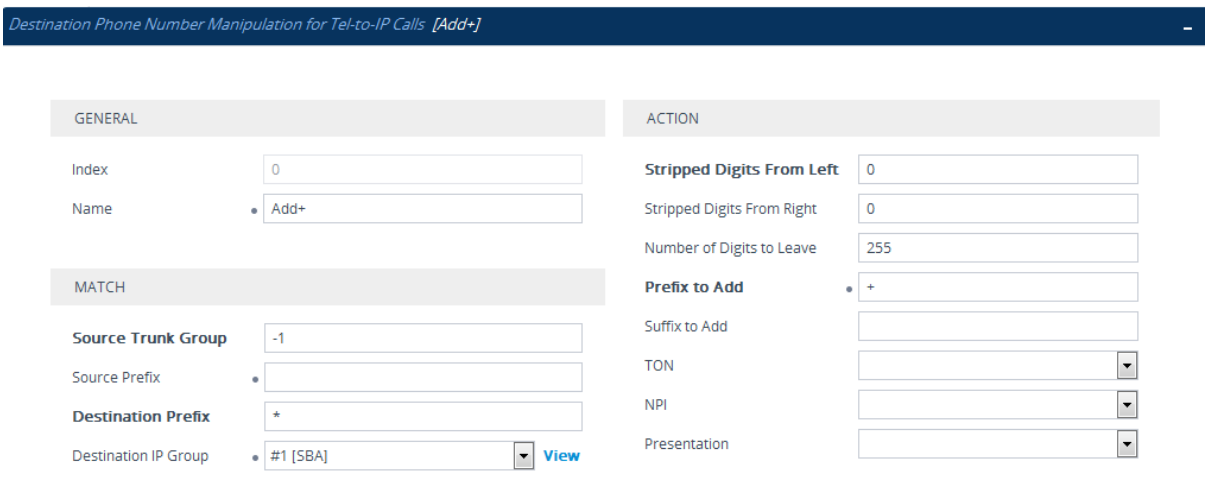
Number manipulation (and mapping of NPI/TON to SIP messages) rules are configured in the following Manipulation tables:

- For Tel-to-IP calls:
  - Destination Phone Number Manipulation Table for Tel-to-IP Calls
  - Source Phone Number Manipulation Table for Tel-to-IP Calls
- For IP-to-Tel calls:
  - Destination Phone Number Manipulation Table for IP-to-Tel Calls
  - Source Phone Number Manipulation Table for IP-to-Tel Calls

➢ **To configure gateway number manipulation rules:**

1. Open the Tel to IP Manipulation table (**Setup** tab > **Signaling & Media** > **Gateway** > **Manipulation > Dest Number Tel->IP**).
2. Click the **New** button to create a new manipulation rule.

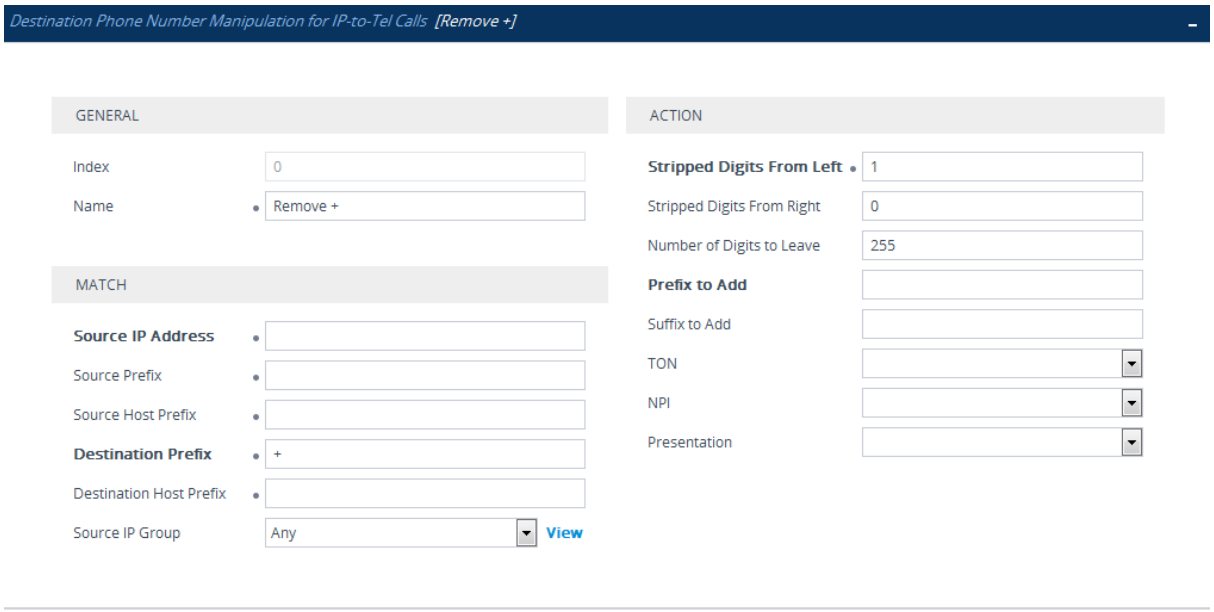
Figure 17-1: Destination Phone Number Manipulation Table for Tel-to-IP Calls



3. Click **Apply** to apply your settings.
4. Open the IP to Tel Manipulation table (**Setup** tab > **Signaling & Media** > **Gateway** >

Manipulation > Dest Number IP->Tel).

Figure 17-2: Destination Phone Number Manipulation Table for IP-to-Tel Calls



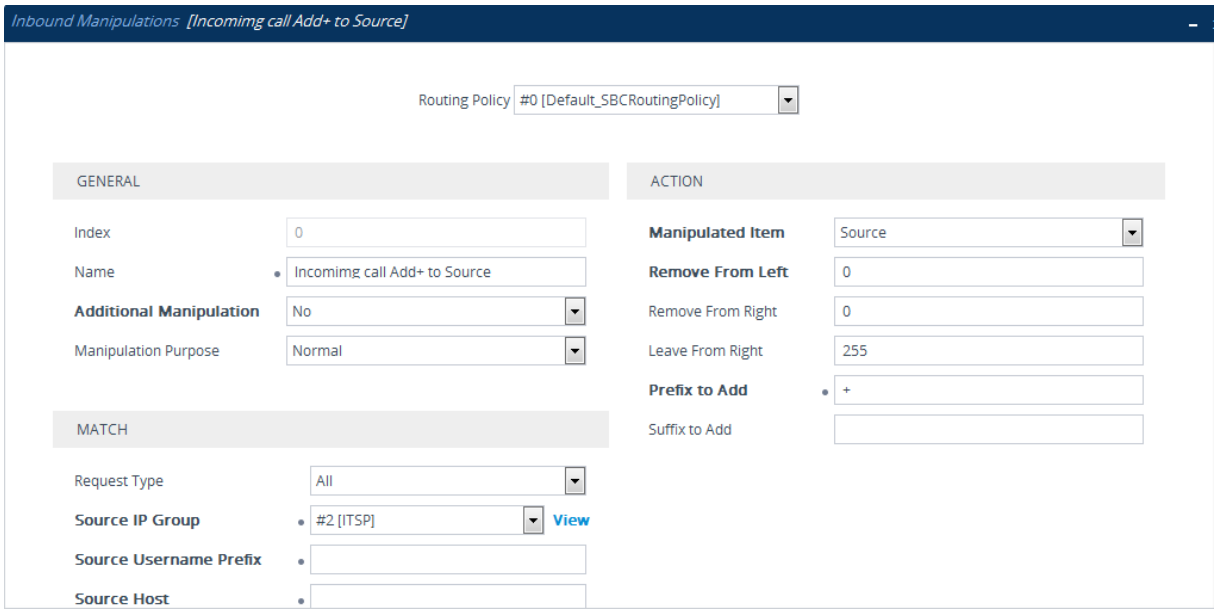
5. Click the **New** button to create a new manipulation rule.
6. On the toolbar, click **Burn** to save the settings to the device; the device resets, saving the settings to flash memory.

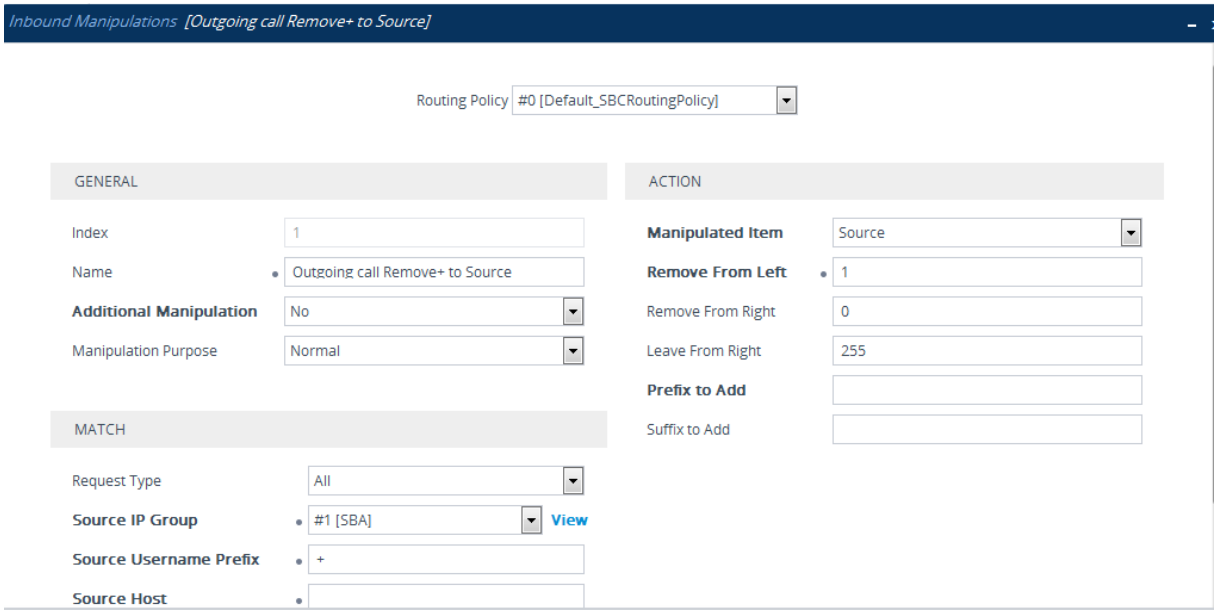
17.2 Configuring SBC Manipulation

➢ **To configure SBC inbound manipulation rules:**

1. Open the Inbound Manipulations table (**Setup** tab > **Signaling & Media** > **SBC** > **Manipulation** > **Inbound Manipulations**).
2. Click **New** to create new rules (see examples below).

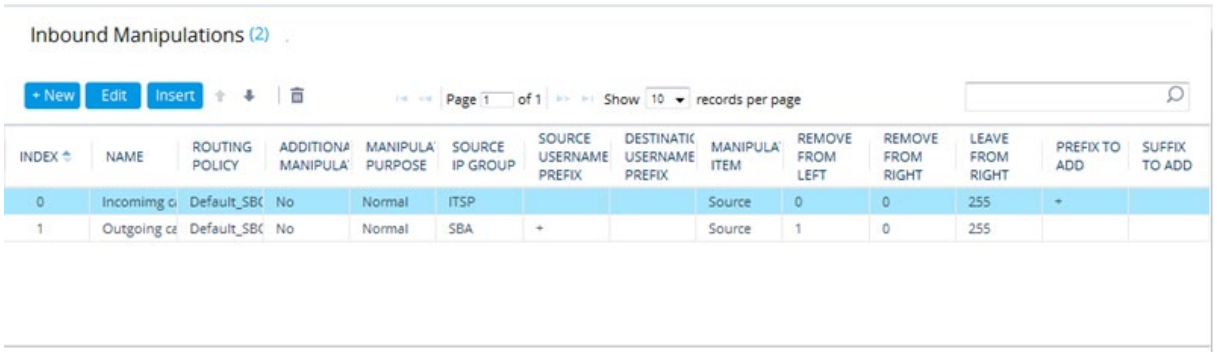
Figure 17-3: SBC Inbound Manipulations





The configured inbound manipulation rules are shown below:

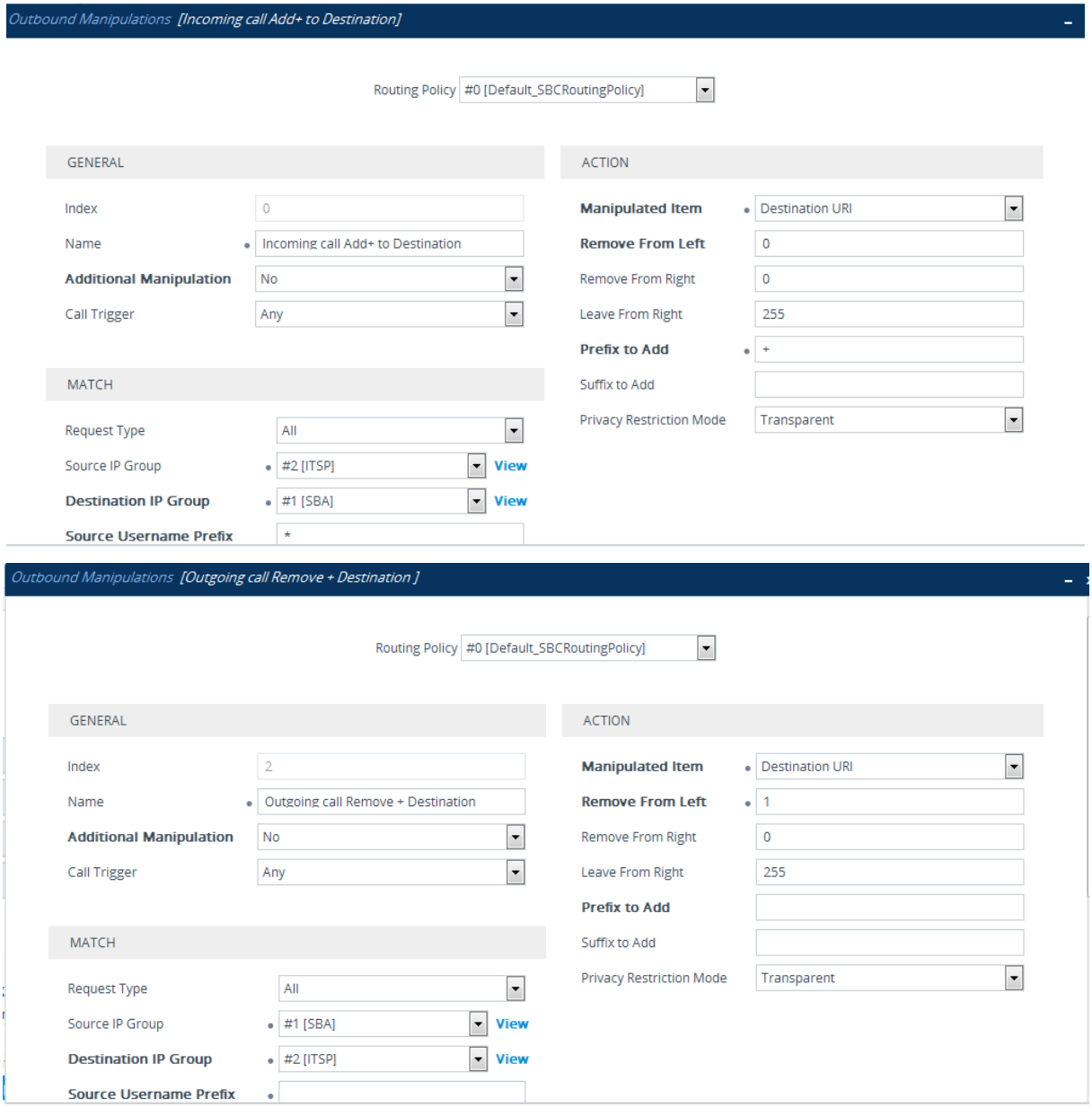
Figure 17-4: Configured SBC Inbound Manipulation Rules



➢ **To configure SBC outbound manipulation rules:**

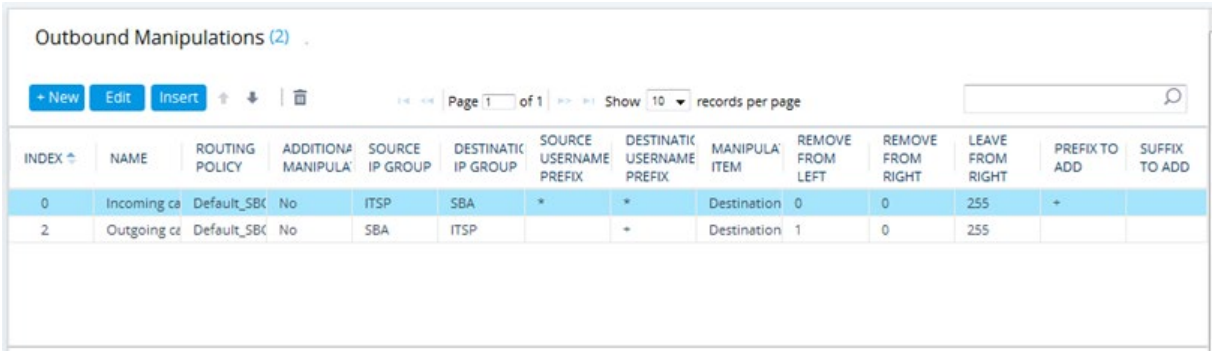
1. Open the Outbound Manipulations table (**Setup** tab > **Signaling & Media** > **SBC** > **Manipulation** > **Outbound Manipulations**).
2. Click **New** to create new rules (see examples below).

Figure 17-5: SBC Outbound Manipulations



The configured outbound manipulation rules are shown below:

Figure 17-6: Configured SBC Outbound Manipulation Rules



Part V

Maintenance

18 Upgrading SBA to Skype for Business

This chapter describes how to upgrade your device from Microsoft Lync Server (2010 / 2013) to Skype for Business and includes the following steps:

- SBA Upgrade Kits on page 157
- Upgrading HDMX Module from HDD to SSD on page 158
- Installing the SBA Skype for Business Image on page 160
- Configuring the SBA on page 166

Note: SBA Skype for Business is compatible with Gateway/SBC software version (.cmp) 7.00A.053.006 and later.

18.1 SBA Upgrade Kits

The following table lists the different Mediant 1000B SBA platforms with Microsoft Lync and their corresponding SBA upgrade kits for Skype for Business.

Mediant 1000B SBA Platforms with Lync and Required SBA Upgrade Kit for Skype for Business

SBA Platform with Lync		Required H/W Changes	SBA Upgrade Kit for Skype for Business
CPN	Description		
M1KB-XXX-SBA	OSN3 2G-RAM with HDD	Replace HDMX module (HDD to SSD)	**M1KB-SBA-SFB-UP-HW** • 120G SSD pre-installed with Windows Server 2012 R2 and Microsoft Skype for Business SBA • License for Windows 2012 R2 OS • License for Skype for Business SBA • Dongle with Skype for Business image (for backup)
M1KB-XXX-SBA-ES or M1KB-XXX-SBA-SSD	OSN3 2G-RAM with SSD	n/a	**M1KB-SBA-SFB-UP-SW** • License for Windows Server 2012 R2 OS • License for Skype for Business SBA • Dongle with Skype for Business image (for backup)
M1KB-XXX-4G-SBA	OSN3 4G-RAM with HDD	Replace HDMX module (HDD to SSD)	**M1KB-SBA-SFB-UP-HW** • 120G SSD pre-installed with Windows Server 2012 R2 and Microsoft Skype for Business SBA • License for Windows 2012 R2 OS • License for Skype for Business SBA • Dongle with Skype for Business image (for backup)

SBA Platform with Lync		Required H/W Changes	SBA Upgrade Kit for Skype for Business
CPN	Description		
M1KB-XXX-4G-SBA-SSD	OSN3 4G-RAM with SSD	n/a	**M1KB-SBA-SFB-UP-SW** • License for Windows Server 2012 R2 OS • License for Skype for Business SBA • Dongle with Skype for Business image (for backup)
M1KB-XXX-SBA-ES	OSN3B	n/a	**M1KB-SBA-SFB-UP-SW** • License for Windows Server 2012 R2 OS • License for Skype for Business SBA • Dongle with Skype for Business image (for backup)
M1KB-XXX-SBA-EO or M1KB-XXX-SBA-EO-X	OSN4	n/a	**M1KB-SBA-SFB-UP-SW** • License for Windows Server 2012 R2 OS • License for Skype for Business SBA • Dongle with Skype for Business image (for backup)

18.2 Upgrading HDMX Module from HDD to SSD

This section describes how to upgrade your HDMX module from a hard disk drive (HDD) to a Solid-State Drive (SSD).

Note:

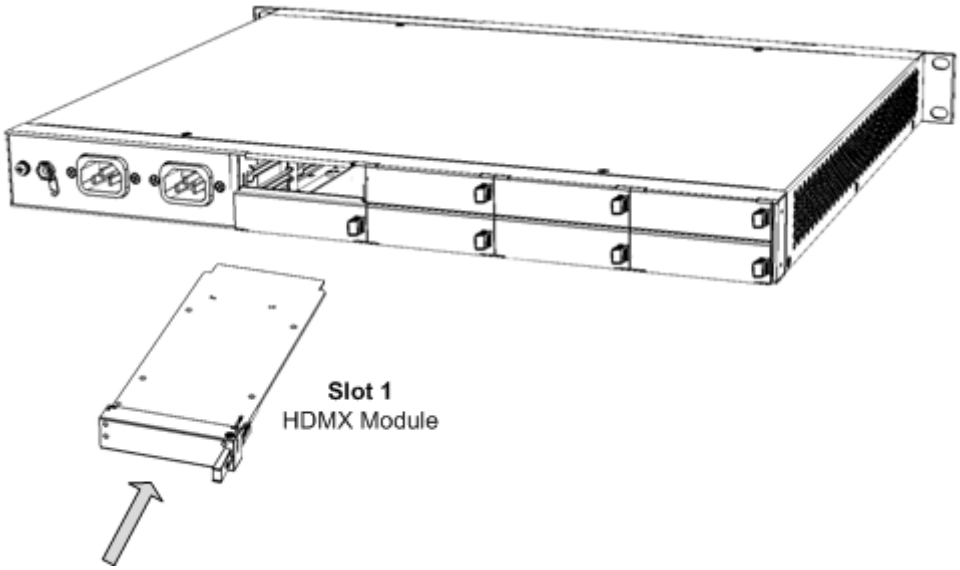
- Please refer to Section 18.1 to check whether this procedure is applicable to your SBA upgrade.
- When you replace the HDMX module, your SBA application becomes unavailable. The SBA application becomes available only after you install the new SBA for Skype for Business software.

➢ **To upgrade the HDMX module from HDD to SSD:**

1. Maintain power to the device chassis.
2. Shutdown the SBA server (see Section 10.5.2).
3. Remove the current HDMX module from the chassis:
   a. Gently pull the HDMX module's handle out to the first notch; the handle is now partially pulled out and the module undergoes a shutdown sequence, indicated by the slow-flashing LED on the module.
   b. When the LED stops flashing and is constantly lit, indicating that the shutdown sequence is complete, grip and gently pull the HDMX module's handle to slide the module out of the slot.
4. Insert the new HDMX module:
   a. Take the HDMX module out of the box in which it was shipped and remove it from the protective plastic packet.

b. Hold the new HDMX module in the correct orientation, as shown in the figure below, and gently insert the module into the slot, sliding it along the slot's guide rails until it makes contact with the card-edge connector located on the backplane.

Figure 18-1: Installing HDMX Module



c. Push-in the HDMX module's handle until it clicks firmly into the slot.

18.3 Installing the SBA Skype for Business Image

The SBA Skype for Business application is provided on the USB dongle that is shipped in your ordered SBA upgrade kit. The image also includes Microsoft Windows Server 2012 R2 installation.

Warning:

- **Before installing** the SBA Skype for Business image, make sure that your OSN server (SBA server) is running a **compatible BIOS version** – make sure that the last **three** digits of the Project Version field is 216 (e.g., 5603E216) or greater. If not, you need to upgrade the BIOS. For more information, see Section 24 on page 183.
- When you install the SBA Skype for Business image, all previous SBA settings are restored to default settings.

Note:

- HDMI-based connections are applicable only to OSN3B, OSN3C, OSN4, and OSN4B modules.
- For upgrading Microsoft Skype for Business Server on your device, you can also use AudioCodes SBA ProConnect tool, which is designed for remote management of multiple SBA devices. For more information, refer to the *SBA ProConnect User's Manual* and contact your AudioCodes representative.

➢ **To install the SBA Skype for Business image:**

1. Establish a connection with the OSN server:
   - **Direct connection through HDMI:** See Section 22.1.
   - **Serial connection:** See Section 22.2.
2. Connect the SBA USB dongle:
   - **Direct connection through HDMI:** Plug the SBA dongle into one of the available USB ports on the USB hub:

Figure 18-2: Connecting SBA Dongle for HDMI Connectivity - OSN3C and OSN4B Modules

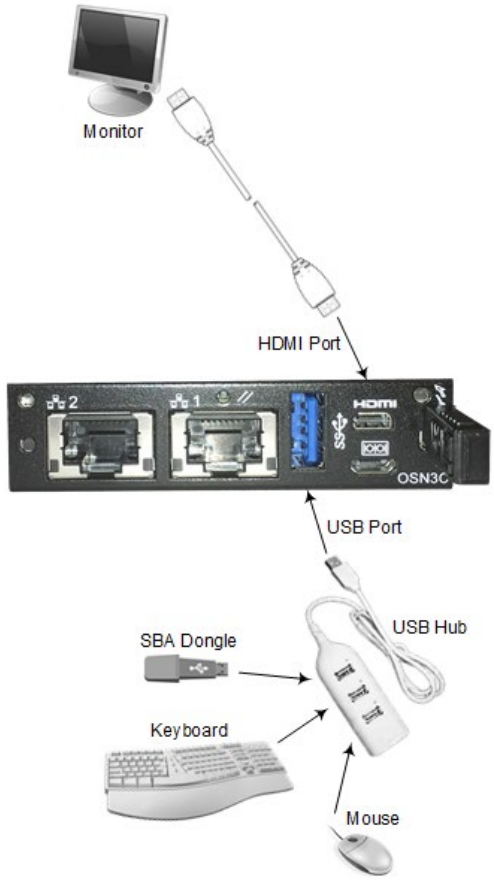
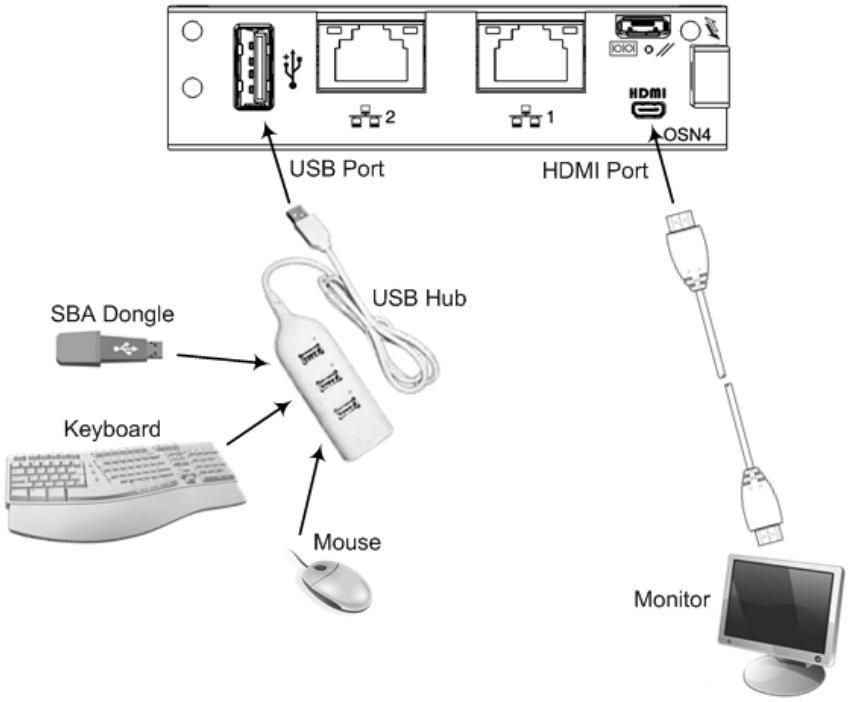


Figure 18-3: Connecting SBA Dongle for HDMI Connectivity - OSN3B and OSN4 Modules



- **Serial connection:** Plug the SBA dongle into the USB port on the OSN module:

Figure 18-4: Connecting SBA Dongle - OSN3C and OSN4B Modules

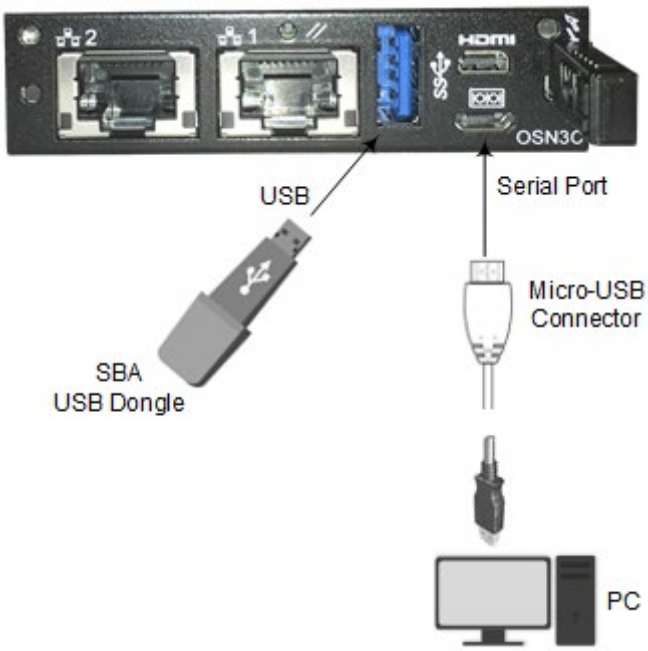


Figure 18-5: Connecting SBA Dongle - OSN3B and OSN4 Modules

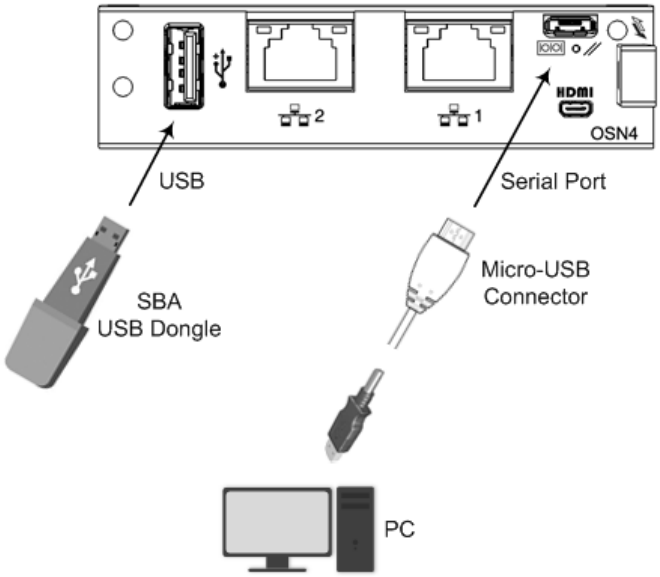
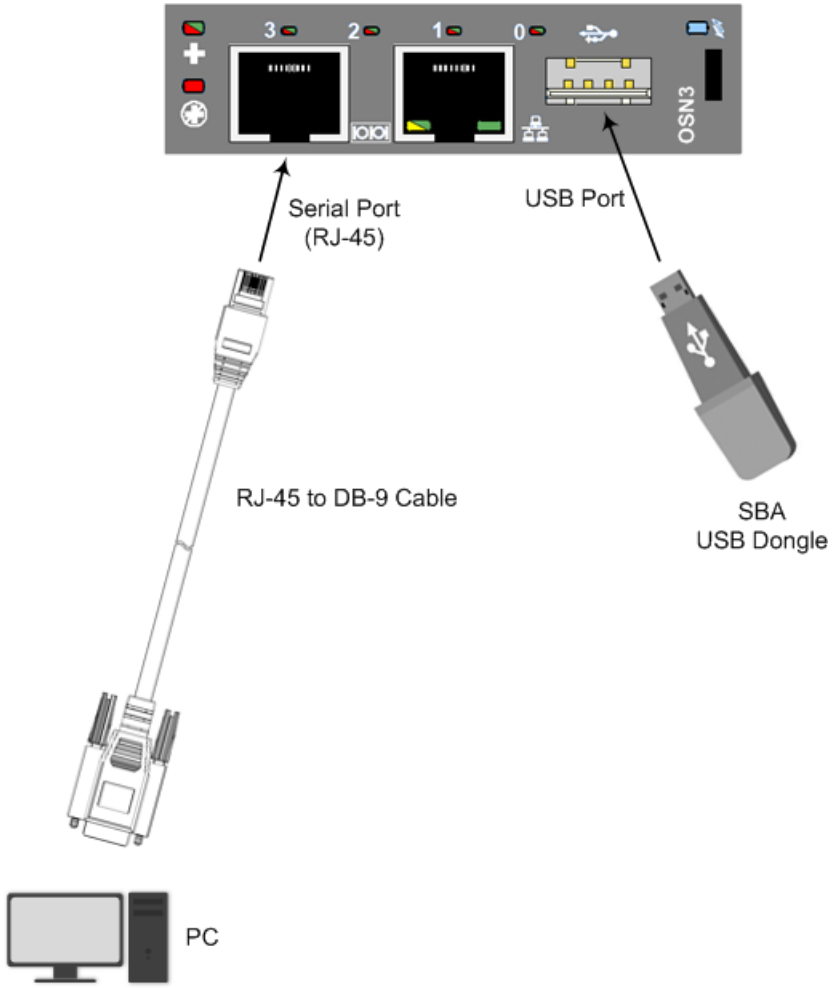


Figure 18-6: Connecting SBA Dongle - OSN3 Module



3. Reset the OSN server using the OSN module's handle, as described in Section 23.1.
4. **For Serial Connection Only:**
   a. Wait until the following prompt appears in the command-line interface (CLI):
   ```
   SAC>
   EVENT: The CMD command is now available.
   ```
   b. At the prompt, type the following:
   ```
   SAC>cmd
   ```
   c. At the prompt, type the following:
   ```
   SAC>ch -sn Cmd0001
   ```
   The channel number (shown above as "Cmd0001") may be different; it is displayed above the prompt.

5. At the prompt, type the following:

```
X:\windows\system32>gorecover.bat
```

The following appears:

```
X:\windows\system32>gorecover.bat

X:\windows\system32>X:"\Program Files\RecoveryUtil\RecoveryUt
********************  RECOVERY UTIL LOG  ********************
INFO:  *************** Reading INI file parameters... *******
The filename, directory name, or volume label syntax is incor
The filename, directory name, or volume label syntax is incor
      *************** Configure remote desktop server *******
CONFIRM: Do you want to run recovery utility? (Y/N)
```

6. At the confirmation prompt, type the following:

```
X:\windows\system32>Y
```

The Skype for Business and Windows installation begins. When complete, the following appears:

Figure 18-7: Installation Complete

```
Copyright (C) Microsoft Corp. All rights reserved.
Version: 6.1.7600.16385


[ 100% ] Applying progress

Successfully applied image.

Total elapsed time: 5 min 55 sec



INFO: *************** Set boot to be from image ***************
bcdboot.exe C:\Windows  /s C: /vBoot files successfully created.
The operation completed successfully.
The operation completed successfully.
The operation completed successfully.
INFO: Copying recovery image to second partition.
copy E:\imageM1K.wim D:\imageM1K.wim
        1 file(s) copied.

X:\windows\system32>
                    _
```

7. Unplug the SBA dongle from the USB port.
8. At the prompt, type the following:

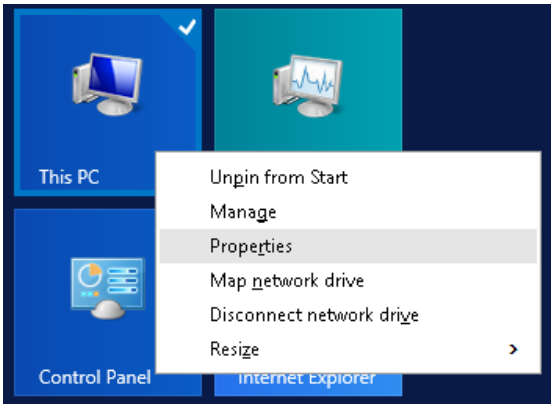
```
X:\windows\system32>exit
```

- **For HDMI Connection:** The SBA server restarts to complete installation.
- **For Serial Connection:** You are returned to the *SAC*> prompt. At the prompt, type the following to restart the SBA server and complete installation:

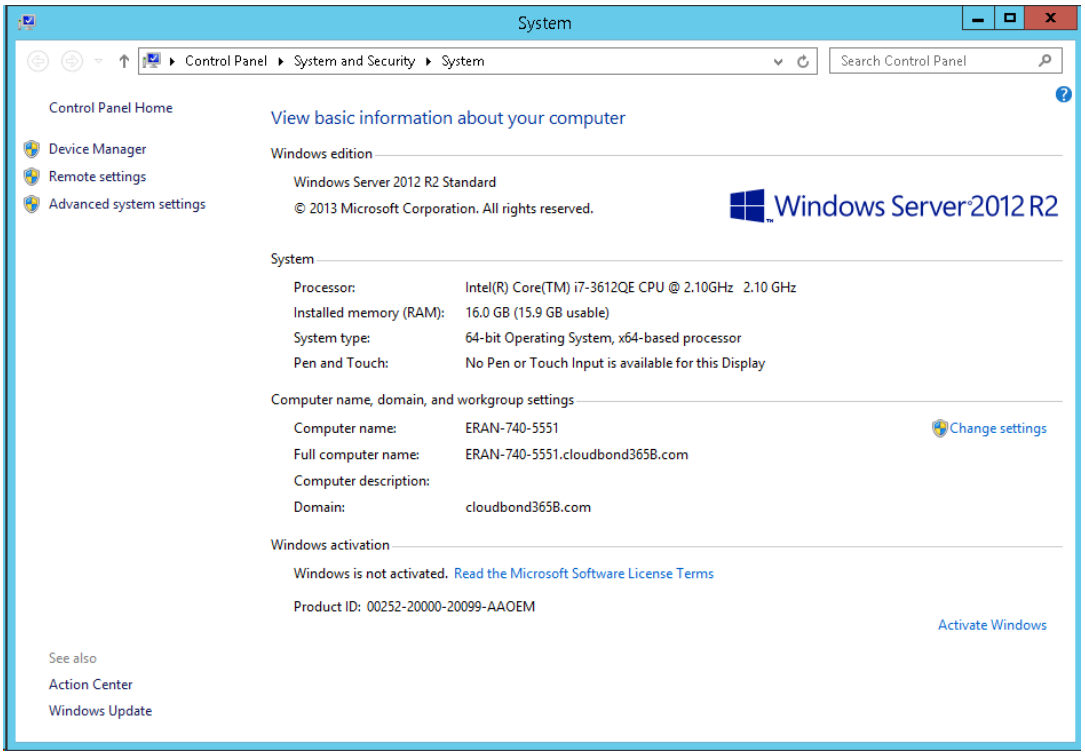
```
SAC>restart
```

9. **(For OSN3 Module Only)** Activate Windows Server 2012 R2:
   a. Connect to the SBA server installed on the OSN3 module through Windows Remote Desktop (see Section 22.4).

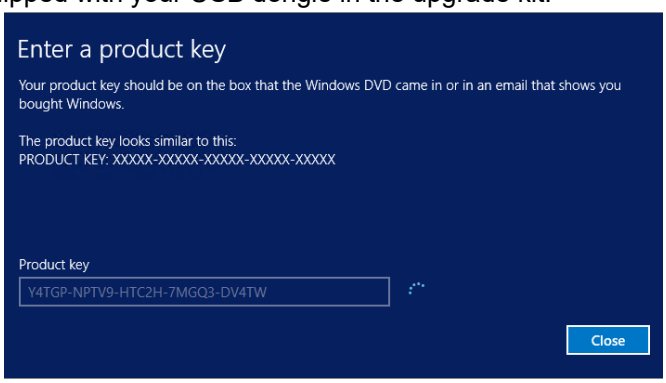
b. Click the Windows **Start** button, right-click **This PC**, and then from the shortcut-menu, choose **Properties**:



The following window appears:



c. Click **Activate Windows**, and then in the 'Product key' field, enter your Windows Server product key (license). The product key is located on the sticker that is shipped with your USB dongle in the upgrade kit.



18.4 Configuring the SBA

Configure the SBA through the Web-based (HTTP) SBA Management interface's SBA wizard as described in Chapter 9.

19 Installing Microsoft Cumulative Updates

This chapter describes how to install Microsoft Cumulative Updates (CU) for SBA Skype for Business on your device. Installation is done through the device's Web-based (HTTP) SBA Management interface.

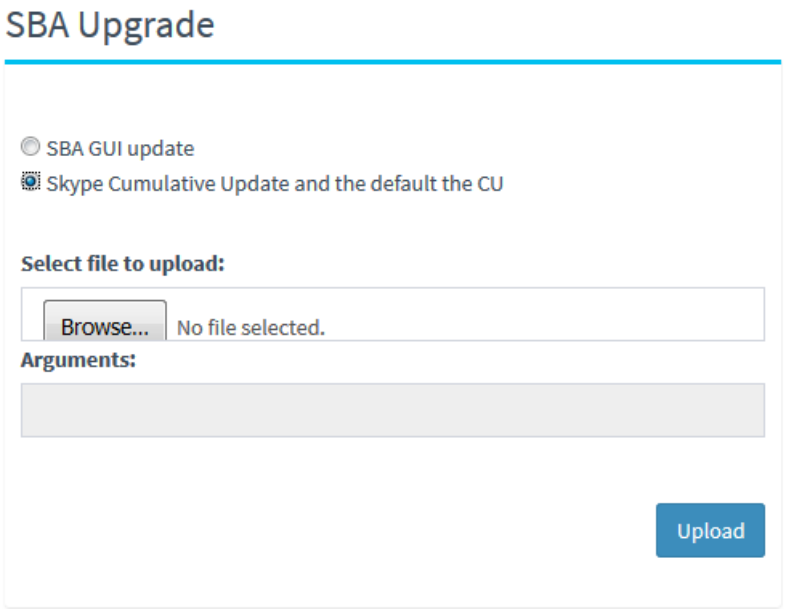
Note:

- During the CU update process, one or more Skype for Business services are temporarily stopped (e.g., Front End service) and as a result, currently active traffic is terminated. Therefore, it is recommended to perform this update during low-traffic periods.
- For installing Microsoft Cumulative Updates (CU) on the device, you can also use AudioCodes SBA ProConnect tool, which is designed for remote management of multiple SBA devices. For more information, refer to the *SBA ProConnect User's Manual* and contact your AudioCodes representative.

➢ **To install Microsoft CU:**

1. Download the CU file (Skype*ServerUpdateInstaller.exe*) from AudioCodes' website at https://audiocodes.sharefile.com/d-s8a84c39bff6446da.
2. Log in to the SBA Management interface.
3. Open the SBA Upgrade page (**Tools** menu > **SBA Software Upgrade**).
4. Select the **Skype Cumulative Update** option:

Figure 19-1: SBA Upgrade Page



5. Click **Browse** to select the downloaded Microsoft CU file.
6. Click **Upload**.

This page is intentionally left blank.

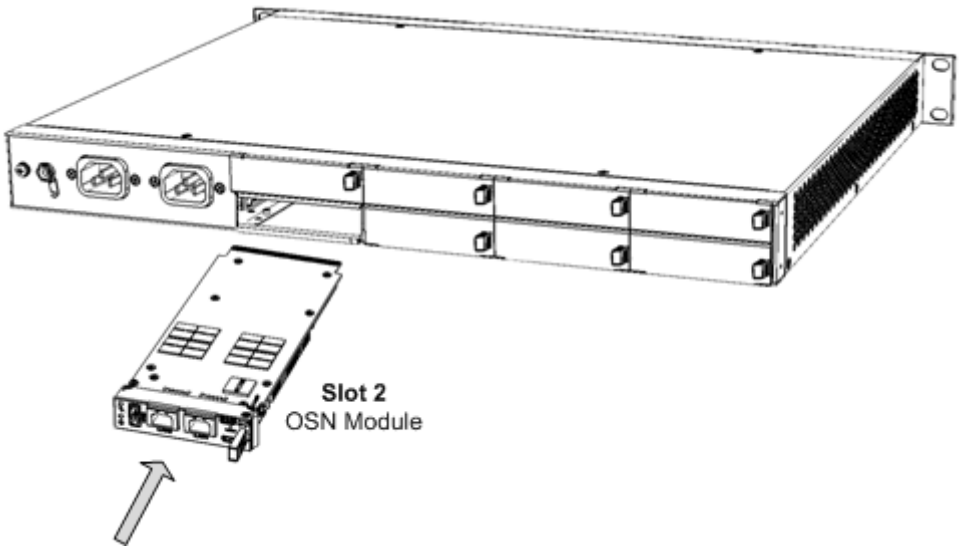
20 Upgrading the OSN Module

This chapter describes how to upgrade the OSN3 module to OSN3B, OSN3C, OSN4, or OSN 4B.

➢ **To upgrade the OSN module to OSN3B or OSN4:**

1. Shutdown the SBA server.
2. Remove the old OSN module:
   a. Gently pull the OSN module's handle until the **first** notch; the handle is now partially pulled out and the module undergoes a shutdown sequence indicated by the slow-flashing LED on the module.
   b. When the LED stops flashing and is constantly lit, indicating that the shutdown sequence is complete, disconnect any cables that may be connected to the module.
   c. Grip and gently pull the module's handle to slide the module out of the slot.
3. Insert the new OSN module:
   a. Hold the new OSN module in the correct orientation, as shown in the figure below, and gently insert the module into the slot, sliding it along the slot's guide rails until it makes contact with the card-edge connector located on the backplane.

Figure 20-1: Installing OSN Module



   a. Push the module's handle until it clicks firmly into the slot; the SBA server on the OSN module starts up.

This page is intentionally left blank.

21 SBA Skype for Business Recovery

If you experience an SBA Skype for Business system failure, you need to re-install the SBA Skype for Business image, as described in Section 18.3 on page160.

This page is intentionally left blank.

22 Connection Methods to SBA Server

You can connect to the SBA server using the following connectivity methods:

- Direct connection through HDMI (see Section 22.1)
- Serial connection (see Section 22.2)
- HTTP/S connection (see Section 22.3)
- Remote Desktop connection (see Section 22.4)

22.1 Direct Connection through HDMI

The following procedure describes how to connect to the SBA server through a direct connection using the HDMI.

Note: The HDMI-based connection is applicable only to OSN3B, OSN3C, OSN4, and OSN4B modules.

➢ **To connect to SBA through an HDMI-based connection:**

1. On the OSN module, connect a USB hub to the USB port, and then connect the following computer peripherals to the USB hub:
   - Mouse
   - Keyboard

Figure 22-1: Connecting USB Hub and USB Devices - OSN3C and OSN4B Modules

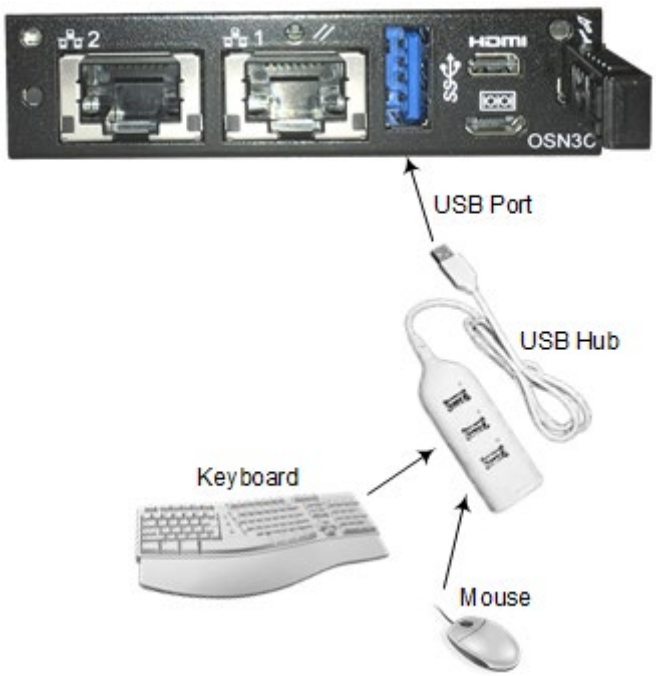
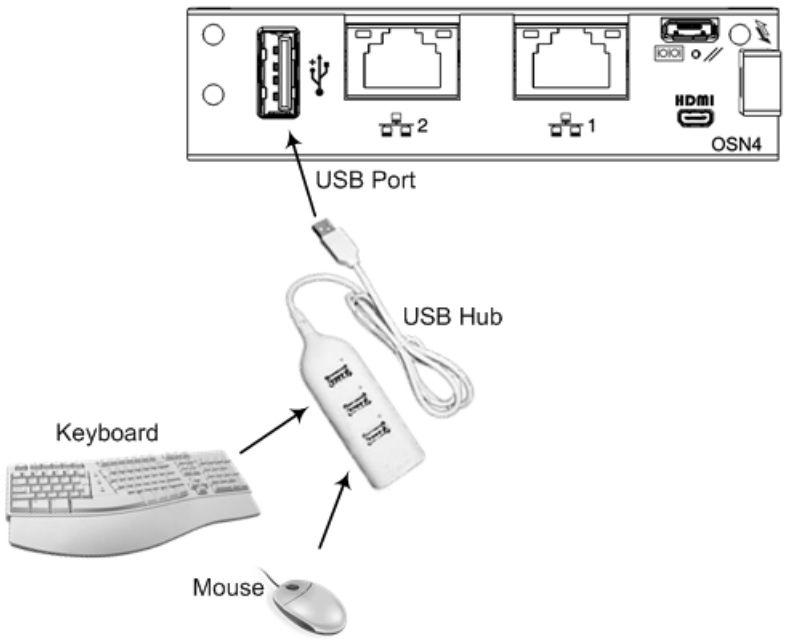


Figure 22-2: Connecting USB Hub and USB Devices - OSN3B and OSN4 Modules



2. On the OSN module, connect a monitor, using the mini HDMI-to-HDMI cable (supplied):
   a. Connect one end of the cable to the micro-HDMI port (19-pin Type D) on the OSN module
   b. Connect the other end of the cable to the HDMI port on your monitor.

Figure 22-3: Connecting Monitor to HDMI Port - OSN3C and OSN4B Modules

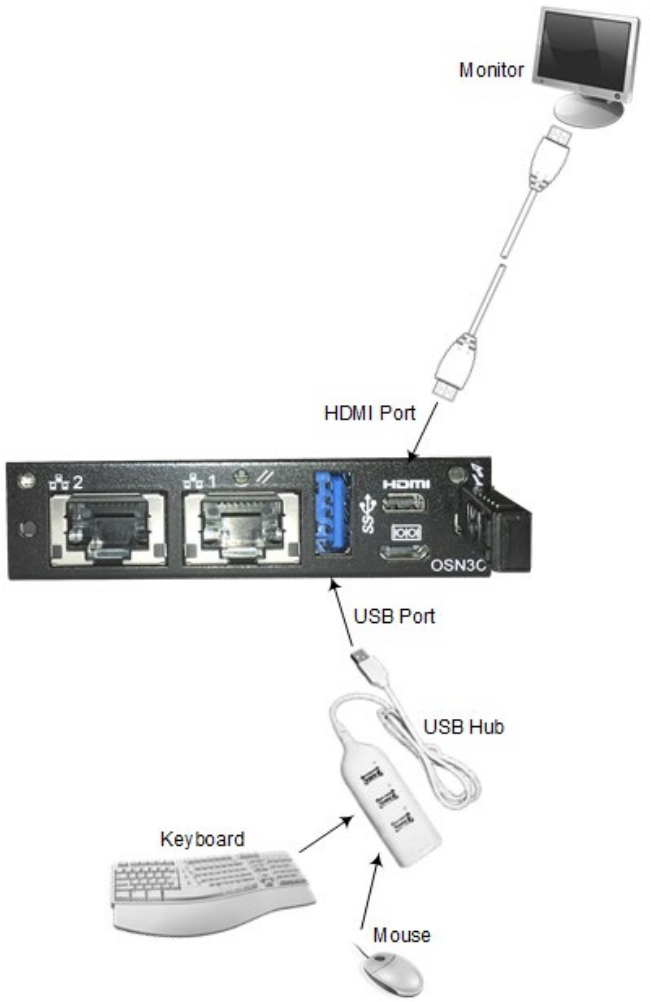
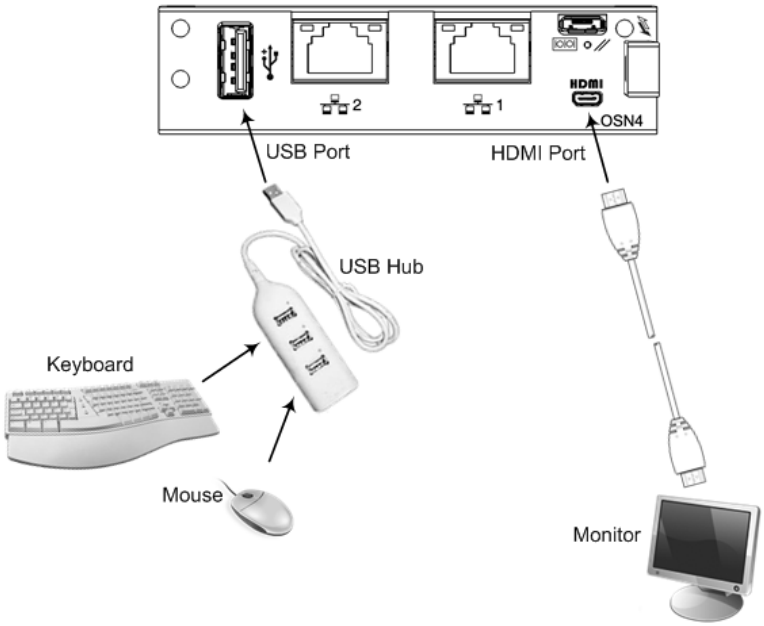


Figure 22-4: Connecting Monitor to HDMI Port - OSN3B and OSN4 Modules



3. Reset the SBA by powering off and then powering on the chassis.

22.2 Serial Connection

The following procedure describes how to connect to the SBA through a serial (console) connection.

➢ **To connect to SBA through a serial connection:**

1. Perform the following cable setup:
   - **OSN3B and OSN4 Modules:**
     a. Connect the micro-USB connector, located on one end of the USB-to-USB cable adapter (supplied), to the serial (console) port (labeled **|O|O|**) on the OSN module.
     b. Connect the USB connector, on the other end of the cable adapter, to the serial port of your PC.

Figure 22-5: Serial Cabling - OSN3C and OSN4B Modules

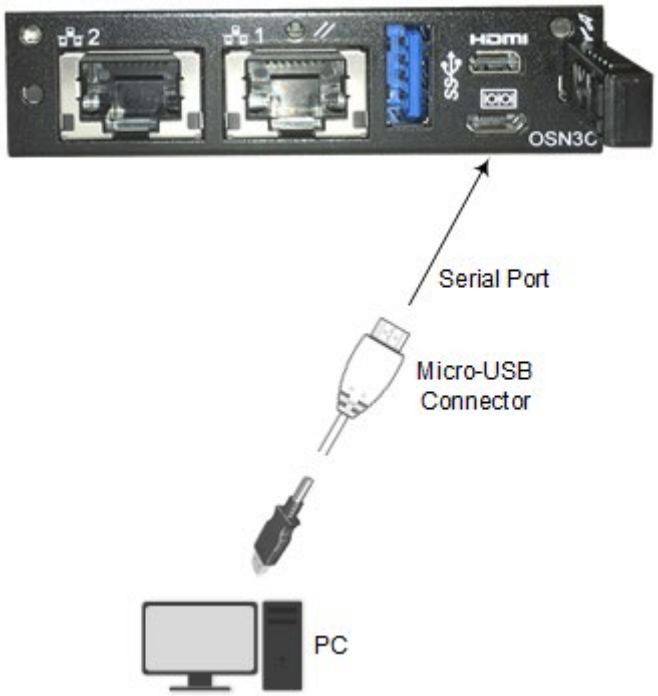
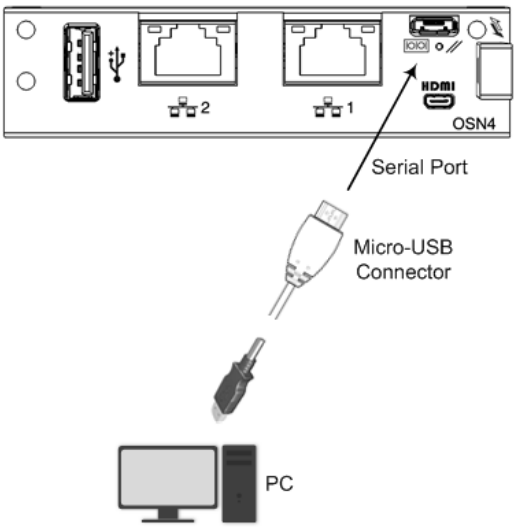
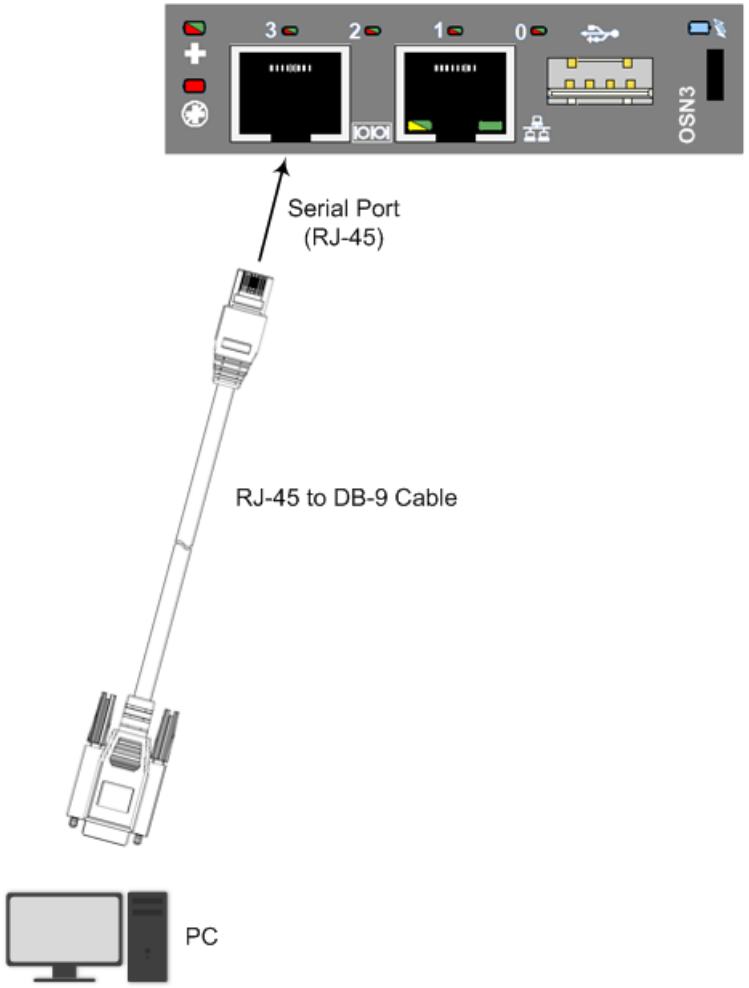


Figure 22-6: Serial Cabling - OSN3B and OSN4 Modules



- **OSN3 Module:**
  a. Connect the RJ-45 connector, located on one end of an RJ-45 to DB-9 cable adapter (not supplied), to the RJ-45 serial port (labeled **|O|O|**) on the OSN module.
  b. Connect the DB-9, on the other end of the cable adapter, to the serial port of your PC.

Figure 22-7: Serial Cabling of OSN3 Module to PC



2. Using a terminal emulation program such as HyperTerminal, establish a serial communication session with the following port settings:
   - Bits per second: 115200
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

22.3 Connecting through HTTP/S

The following procedure describes how to connect remotely to the SBA server through HTTP/S.

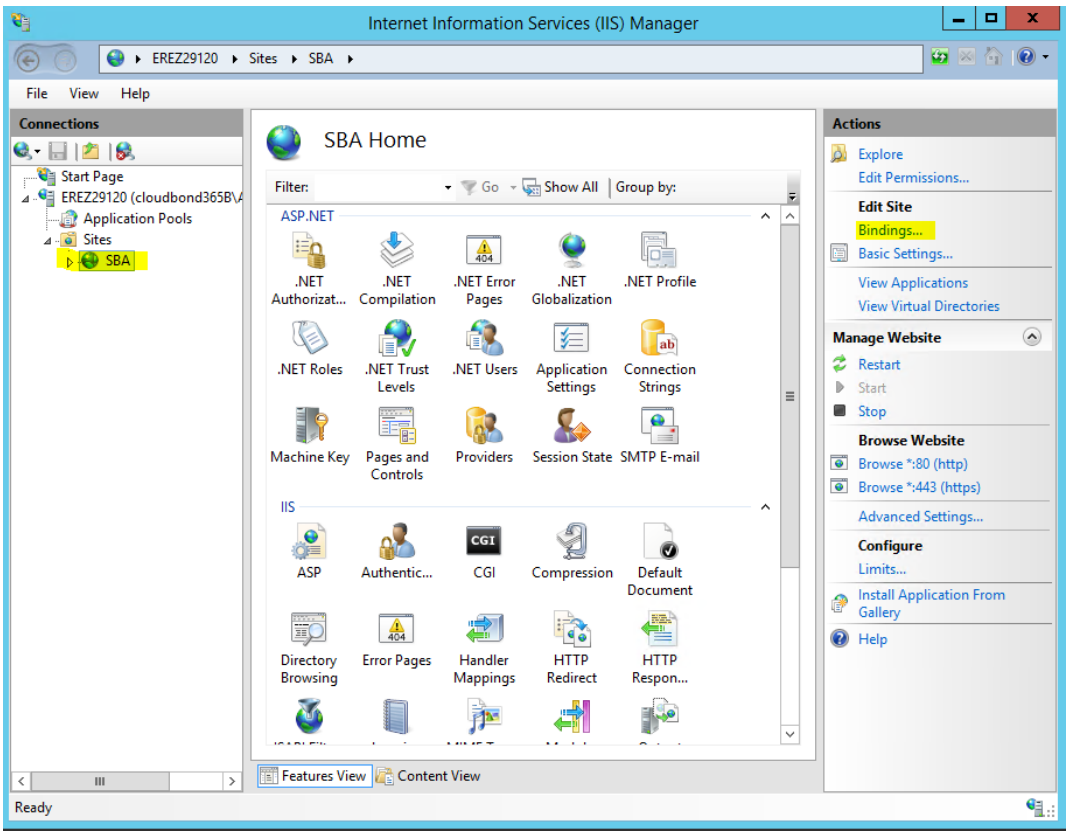
➢ **To connect to SBA through HTTP/S:**

1. Cable the OSN module to your network, as described in Section 8.1.
2. On your PC, open a Web browser, and then enter the IP address of the SBA Management interface.

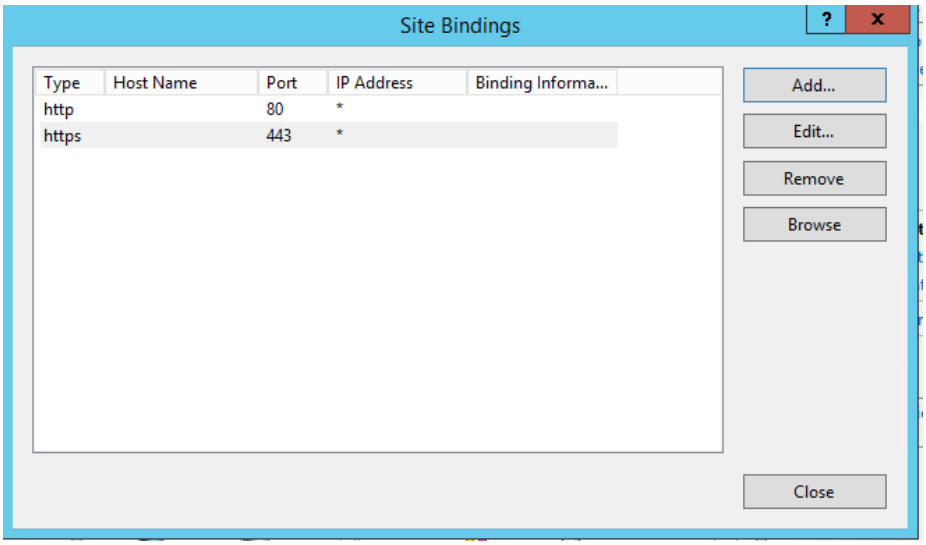
If you require HTTPS for the Web interface, the easiest way to do this is to finish the SBA setup through HTTP, and then configure HTTPS support. This is done because in the setup procedure, a certificate is added to the SBA and it can be used by the Web server. If you wish to implement HTTPS from the beginning, you need to create a certificate for the server and use it for the Web.

➢ **To configure HTTPS for SBA Web interface:**

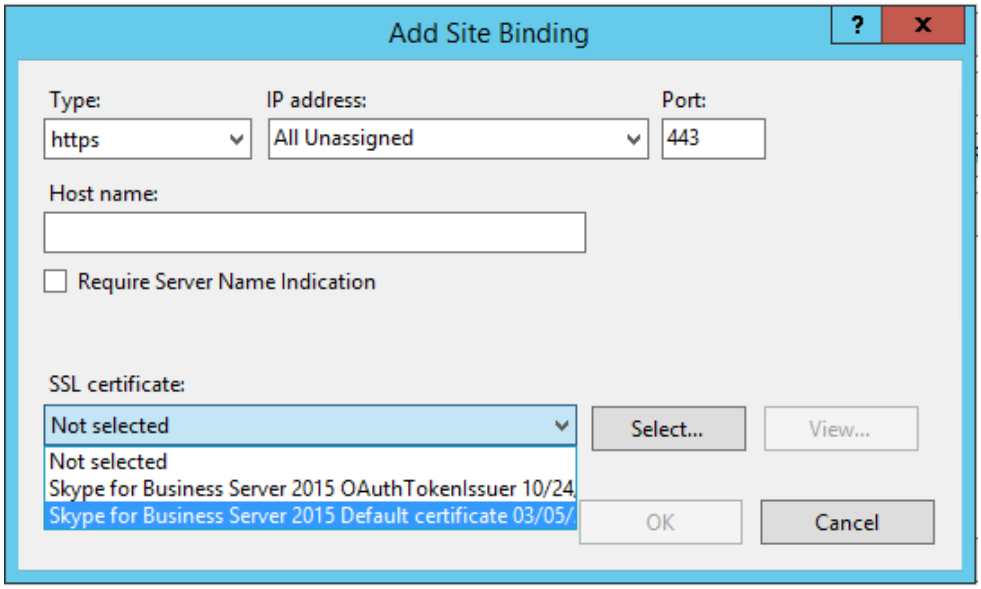
1. Install a certificate for the SBA (through the normal SBA setup procedure, or added manually).
2. Open Microsoft Internet Information Services (IIS).
3. Open the SBA site and then click **Bindings**:



The following appears:



4. If you don't have a binding line for HTTPS, click **Add**. If you have the HTTPS line, click **Edit**; the following appears:



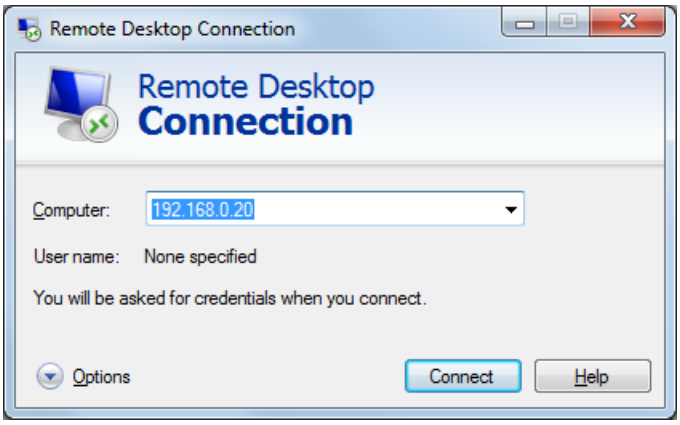
5. From the 'Type' drop-down list, select **https.**
6. From the 'SSL certificate' drop-down list, select the certificate created by the SBA setup (or use the certificate that you added for the Web interface). **Note:** Don't select the OAuth certificate.
7. For the certificate created by the SBA, use the SBA FQDN as the Subject Name (SN). (When you access the SBA's Web interface using this as the Web certificate, you need to enter the SBA's FQDN as the URL.)
8. You can add this like as note for the previse item
9. By default, binding to port 80 is available. If you want to enable access only through HTTPS (and block HTTP), you need to delete this HTTP binding. Before doing this, check that HTTPS is functioning.

22.4 Connecting to SBA through Remote Desktop

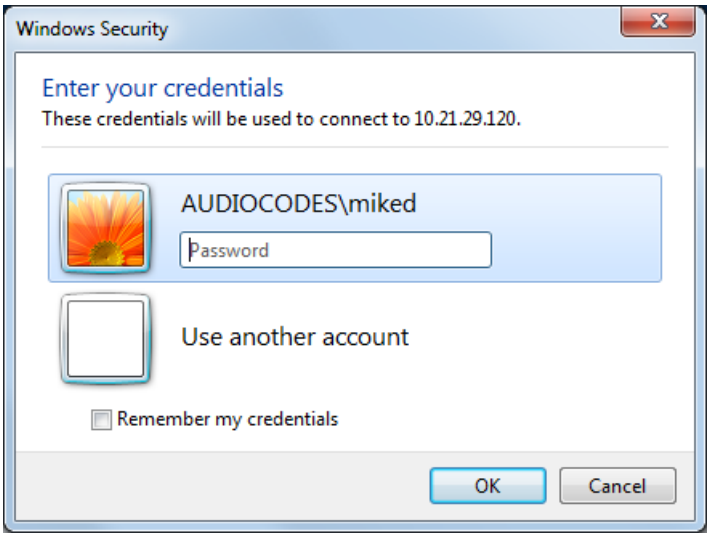
The following procedure describes how to connect remotely to the SBA server through Windows Remote Desktop.

➢ **To connect to SBA through Remote Desktop:**

1. Cable the OSN module to your network, as described in Section 8.1.
2. Start the Remote Desktop Connection program on your PC, and then in the 'Computer' field, enter the IP address of the SBA:



3. Click **Connect**:



4. Enter the SBA's password, and then click **OK**; you are connected to the SBA server.
5. Open the Web browser, and then enter the IP address of the SBA management server.

23 Resetting the SBA Server

You can reset the SBA server using the following methods:

- OSN module handle (see Section 23.1)
- Windows restart (see Section 23.2)
- SBA Management interface (see Section 23.3)
- CLI (see Section 23.4)

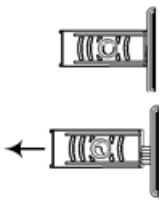
23.1 Resetting SBA using OSN Module Handle

The following procedure describes how to reset the SBA server using the OSN module's handle.

➢ **To reset the SBA server using the OSN module's handle:**

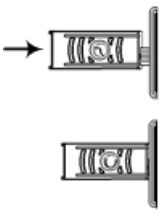
1. Even though the handle can be pulled out two notches, gently pull it out **only** to the **first notch**; the LED light starts **flashing blue**:

Figure 23-1: Pulling OSN Module Handle to First Notch



2. Wait until the LED light changes to **solid blue**, indicating that the SBA server has shut down.
3. Gently push the handle all the way back into the module; the LED switches off, indicating that the SBA server is undergoing a reset:

Figure 23-2: Pushing-in OSN Module Handle



23.2 Resetting SBA through Windows

The following procedure describes how to reset the SBA server through Windows on which the SBA server is running.

➢ **To reset SBA by shutting down Windows:**

1. Connect to the SBA server (Remote Desktop or direct through HDMI).
2. Perform a Windows restart (e.g., from the **Start** menu, click **Restart**).

23.3 Resetting SBA through SBA Management Interface

You can reset the SBA through the SBA Management interface, as described in Section 10.5.3 on page 103.

23.4 Resetting SBA through CLI

The following procedure describes how to reset the SBA through CLI.

➢ **To reset SBA through CLI:**

1. Establish a serial connection with the SBA, as described in 22.2.
2. At the prompt, type the following:

```
>restart
```

24 Upgrading the BIOS on SBA Server

This chapter describes how to upgrade the BIOS of your SBA server running on the OSN module. This is necessary only if you are running an old BIOS version.

Note: This section is applicable only to the OSN3B and OSN4 modules.

24.1 Verifying the Current BIOS Version

This section describes how to view the current BIOS version. You can do this through a serial connection or a direct connection to the SBA Windows server.

24.1.1 Viewing BIOS Version through Serial Connection

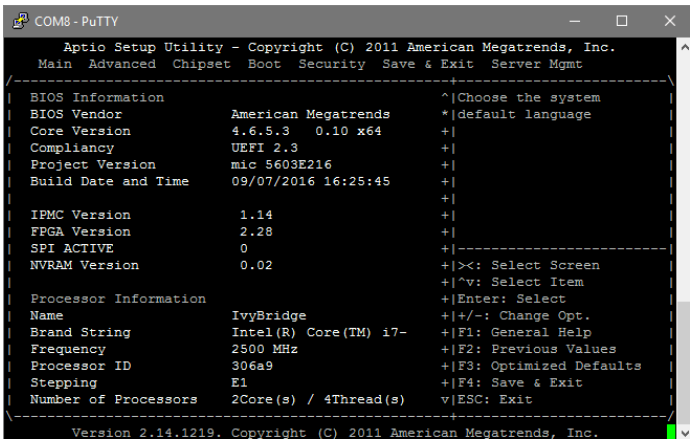
The following procedure describes how to view the BIOS version through a serial connection.

➢ **To view BIOS version through serial connection:**

1. Establish a serial connection with the OSN module, as described in 22.2.
2. At the prompt, type the following to reset the server:

```
>restart
```

3. Access the BIOS, by pressing the Delete key or F2 function key.
4. In the BIOS Main menu, check the value of the **Build Date and Time** field.

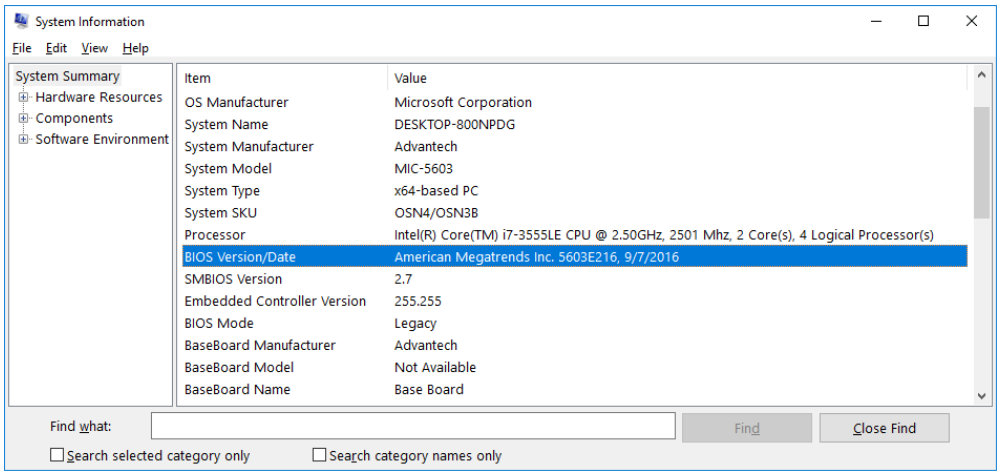


24.1.2 Viewing BIOS Version through Desktop Connection

The following procedure describes how to view the BIOS version through a Desktop connection.

➢ **To view BIOS version through Desktop connection:**

1. Access the SBA server.
2. Click the Windows **Start** button, and then in the search box, type "msinfo32"; the System information window appears and the BIOS version is displayed in the BIOS Version/Date field, as shown in the example below:



24.2 Upgrading BIOS

The upgrade procedure includes the following main steps:

1. Obtaining the latest BIOS image
2. Creating a Bootable BIOS file from a USB Dongle
3. Installing new BIOS

24.2.1 Obtain the BIOS Image File

Obtain the BIOS image file (.img) from AudioCodes. You can download the file from AudioCodes ShareFile portal at https://audiocodes.sharefile.com/d-s4fe8b2599144db8b. Save it on a folder on your PC.

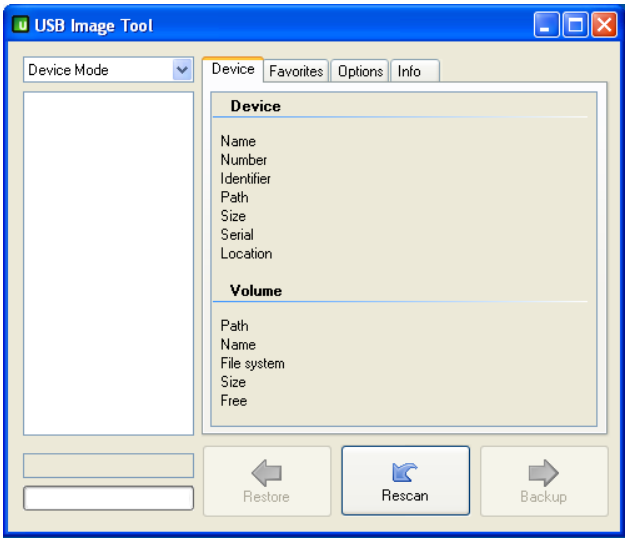
24.2.2 Create a Bootable BIOS File from a USB Dongle

The following procedure describes how to create a bootable file of the BIOS image file (which you downloaded) from a USB dongle. The procedure uses the third-party, USB Image Tool program as an example.

➢ **To create a bootable file of BIOS image from a USB dongle:**

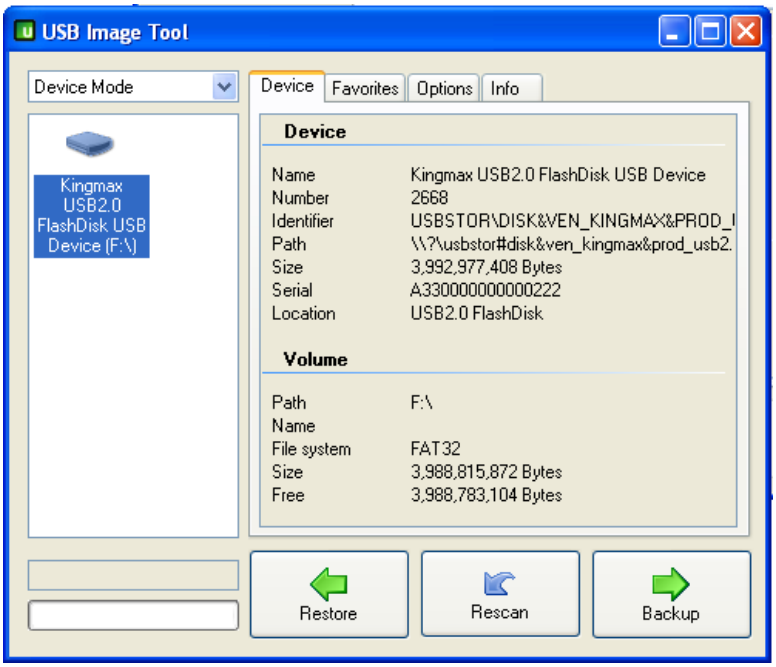
1. Open a USB burn application, for example, USB Image Tool:

Figure 24-1: USB Image Tool - Main Window



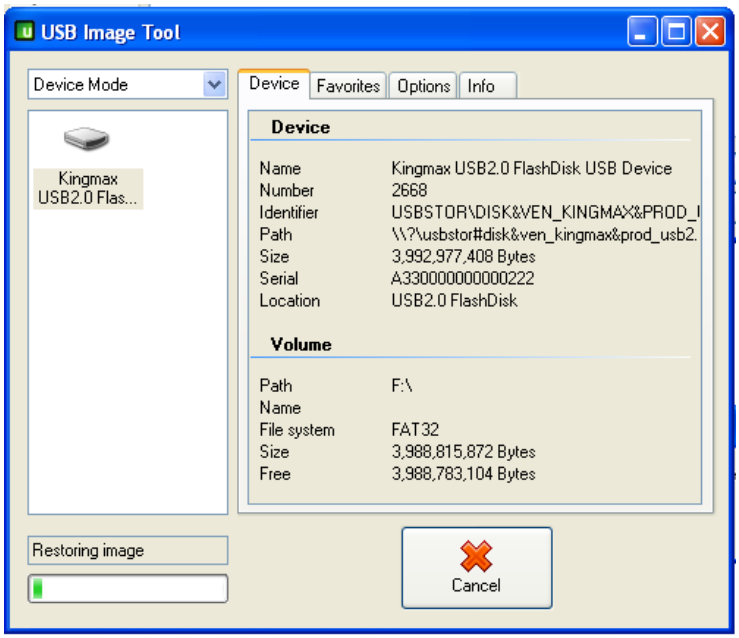
2. Plug the USB dongle into the USB port on your PC where you saved your downloaded BIOS image file.
3. When the dongle is recognized, select its' icon:

Figure 24-2: USB Device Recognition



4. Click **Restore**, select the downloaded BIOS file (.img), and then click **Open**; you are prompted to approve the restore action.
5. Click **Yes**; the restore process starts and the progress is displayed on the bottom-left side progress bar:

Figure 24-3: Restore Image Process



6. When the restore process finishes, perform a "Safely Remove Hardware" on your PC, and then unplug the USB dongle from the PC.

24.2.3 Upgrade the BIOS on the OSN

The following procedure describes how to upgrade the BIOS on the OSN module from the USB dongle on which you created a bootable BIOS file.

➢ **To upgrade the OSN BIOS:**

1. Download the latest BIOS version from AudioCodes ShareFile portal at https://audiocodes.sharefile.com/d-s0cc960a278a437da.
2. Copy the downloaded folder to the bootable USB dongle that you prepared in Section 24.2.2.
3. Shutdown the SBA server.
4. Remove the HDMX module from the chassis slot. (This ensures that the BIOS first boots from the USB.)
5. Plug the USB dongle into the USB port on the OSN module.
6. Establish a serial connection with the OSN, as described in Section 22.2.
7. Reset the SBA sever, using the OSN module handle (see Section 181).
8. When the *DOS C/* prompt appears, navigate to the folder on the USB dongle where you copied the BIOS version in Step 2.
9. Type the following to back up the LAN1 MAC address:

```
>fpt -gbe -d 579.bin
```

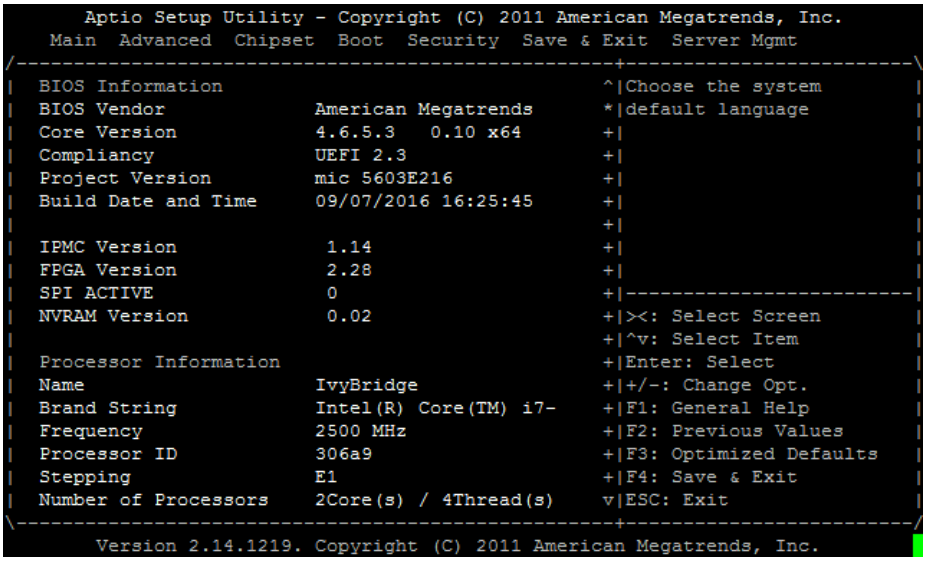
10. When the FPT operation passes successfully, at the DOS prompt, type the following to upgrade the BIOS:

```
>fpt -f <BIOS file name>.bin (e.g., fpt -f 5603E216.bin)
```

11. When the FPT operation passes successfully, at the DOS prompt, type the following to restore the LAN1 MAC address:

```
>fpt -gbe -f 579.bin
```

12. Insert the HDMX module back into the chassis slot.
13. Remove the USB dongle from the USB port on the OSN module.
14. Restart the SBA server, using the OSN module handle (see Section 181).
15. To view the upgraded BIOS version, press the F2 key and then Del key consecutively until you enter the BIOS. The BIOS version is displayed in the Project Version field, as shown in the example below:



25 Monitoring through SNMP

This chapter describes the monitoring of the SBA through SNMP.

25.1 SNMP Trap Alarms

This section describes the SNMP trap alarms of the SBA.

25.1.1 SBA Services Status Alarm

Table 25-1: acSBAServicesStatusAlarm

Alarm	acSBAServicesStatusAlarm		
OID	1.3.6.1.4.1.5003.9.30.2.2.0.1		
Description	Services status alarm. The services are Front End Server, Mediation Server, Replica Server, and Centralized Logging Service for Microsoft Skype for Business (Centralized Logging is not available for Lync 2010).		
Source Varbind Text	SBA Server		
Alarm Text	Indicates which of the above-mentioned services is down.		
Event Type	Other		
Probable Cause	Other		
Additional Info	When an SBA is configured, displays the 'SBA Description' field.		
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Critical	Service is down	"SERVICE_STOPPED"	Start the service and check why the service stopped, using the event viewer.
Major	Service is paused	"SERVICE_PAUSED"	Start the service and check why the service paused, using the event viewer.
Cleared	Service is running	"SERVICE_RUNNING"	-
Indeterminate	Service in indeterminate state	"SERVICE_CONTINUE_PENDING" "SERVICE_PAUSE_PENDING" "SERVICE_START_PENDING" "SERVICE_STOP_PENDING"	Start the service and check why the service is in indeterminate state, using the event viewer.

25.1.2 SBA Disk Space Alarm

Table 25-2: acSBADiskSpaceAlarm

Alarm	acSBADiskSpaceAlarm		
OID	1.3.6.1.4.1.5003.9.30.2.2.0.4		
Description	Sent if the disk (C) usage level exceeds configured thresholds. Thresholds can be configured in the snmp_sba.ini under C:\SBA (requires service restart for the changes to take effect).		
Source Varbind Text	SBA Server		
Event Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Critical	Disk usage level is over 90%	"Disk space usage Critical !!! (over 90%)"	Remove unnecessary files from disk. Clean log files.
Major	Disk usage level is between 80% and 90%	"Disk space usage Major (80 - 90%)"	Remove unnecessary files from disk. Clean log files.
Cleared	Disk usage level is below 80%	"Disk space usage is OK (0 - 80%)"	-

25.1.3 SBA CPU Status Alarm

Table 25-3: acSBACpuStatusAlarm

Alarm	acSBACpuStatusAlarm		
OID	1.3.6.1.4.1.5003.9.30.2.2.0.2		
Description	Sent if the SBA server's CPU utilization is above the threshold.		
Source Varbind Text	Processor Information/%Processor Time/_Total		
Event Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Critical	CPU is greater than 90%	"High CPU usage Above 90%"	Using the task manager, check if the CPU load is constant or not. Locate the process that is causing the high CPU usage and check if high CPU is reasonable (for example, high CPU when performing Windows updates or running traces on the SBA). If there isn't a reason for the high CPU, reset the SBA and if this doesn't solve the issue, contact AudioCodes support.
Major	CPU greater than 80%	"High CPU usage Above 80%"	See corrective action above.
Cleared	CPU is less than 76%	-	-

25.1.4 SBA Memory Status Alarm

Table 25-4: acSBAMemorytatusAlarm

Alarm	acSBAMemorytatusAlarm		
OID	1.3.6.1.4.1.5003.9.30.2.2.0.3		
Description	Sent when the level of available physical memory om the SBA server is below the threshold.		
Source Varbind Text	Memory/% Available MByte		
Event Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Critical	Available memory is less than 4%	"High memory usage, available memory is Below 4%"	Using the task manager, locate the process that is causing the high memory usage. The SQL process can use a huge amount of memory, which is normal. If you install extra tools on the SBA, remove or disable them and check if this solves the high memory usage. On 2G RAM SBAs, memory usage can be high, but it should not have any impact on the service that the SBA provides. Perform a Windows update and SQL server update. If there isn't a reason for the high memory, reset the SBA and if this doesn't solve the issue, contact AudioCodes support.
Major	Available memory is less than 7%	"High memory usage, available memory is Below 7%"	See corrective action above.
Cleared	Available memory is less than 8%	-	-

25.1.5 SBA Certificate Expired Alarm

Table 25-5: acSbaCertificateExpiredAlarm

Alarm	acSbaCertificateExpiredAlarm		
OID	1.3.6.1.4.1.5003.9.30.2.2.0.5		
Description	Sent when the certificate that is used to secure the connection between the SBA and the Datacenter is about to expire. The alarm is sent when the number of days to certificate expiration is below the threshold.		
Source Varbind Text	-		
Event Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Critical	Number of days to certificate expiration is less than 2 days	"Certificate will expire in 2 days."	Using Windows mmc tool, check the expiration date of the certificates and locate the expired certificate. Sign the expired certificate and install it on the machine.
Major	Number of days to certificate expiration is less than 30 days	"Certificate will expire in 30 days."	See corrective action above.
Cleared	New valid certificate is installed.	-	-

25.1.6 SBA Performance Counter Alarm

Table 25-6: acSbaPerfCounterAlarm

Alarm	acSbaPerfCounterAlarm		
OID	1.3.6.1.4.1.5003.9.30.2.2.0.6		
Description	Sent when the configured performance counter's value is above or below the configured threshold.		
Source Varbind Text	(Performance counter full path)		
Event Type	Other		
Probable Cause	Other		
Additional Info	-		
Alarm Severity	**Condition**	**Text**	**Corrective Action**
Critical	Monitored value crossed the "Critical" threshold	"Performance counter <Full Path of Performance Counter> is <Above or Below> <Threshold Value>"	-
Major	Monitored value crossed the "Major" threshold	"Performance counter <Full Path of Performance Counter> is <Above or Below> <Threshold Value>"	-
Cleared	Monitored value falls below the "Major" threshold	-	-

25.2 SNMP Performance Monitoring MIBs

The following table lists the SNMP MIBs that provide performance monitoring status of the SBA.

Table 25-7: Performance Monitoring MIBs for SBA Status

MIB Name	Description
acSBAFrontEndServerStatus	Displays the status of the SBA Front End Server: ▪ service_continue_pending: The service is about to continue. ▪ service_pause_pending: The service is pausing. ▪ service_paused: The service has paused. ▪ service_running: The service is running. ▪ service_start_pending: The service is starting. ▪ service_stop_pending: The service is stopping. ▪ service_stopped: The service has stopped. ▪ service_not_installed: The service is not installed or has installation errors.
acSBAMediationServerStatus	Displays the status of the SBA Mediation Server: ▪ service_continue_pending: The service is about to continue. ▪ service_pause_pending: The service is pausing. ▪ service_paused: The service has paused. ▪ service_running: The service is running. ▪ service_start_pending: The service is starting. ▪ service_stop_pending: The service is stopping. ▪ service_stopped: The service has stopped. ▪ service_not_installed: The service is not installed or has installation errors.
acSBAReplicaServerStatus	Displays the status of the SBA Replica Server: ▪ service_continue_pending: The service is about to continue. ▪ service_pause_pending: The service is pausing. ▪ service_paused: The service has paused. ▪ service_running: The service is running. ▪ service_start_pending: The service is starting. ▪ service_stop_pending: The service is stopping. ▪ service_stopped: The service has stopped. ▪ service_not_installed: The service is not installed or has installation errors.

MIB Name	Description
AcSBACentLoggingAgentStatus	Displays the status of the SBA Central Logging agent: ▪ Skype for Business: ✓ service_continue_pending: The service is about to continue. ✓ service_pause_pending: The service is pausing. ✓ service_paused: The service has paused. ✓ service_running: The service is running. ✓ service_start_pending: The service is starting. ✓ service_stop_pending: The service is stopping. ✓ service_stopped: The service has stopped. ✓ service_not_installed: The service is not installed or has installation errors. ▪ Lync 2010: ✓ service_non_available: The service is not supported by Lync 2010.
acSBASetupStatus	Displays the SBA setup status: ▪ setup_not_done: No step has been done. ▪ setup_done: All steps have been successful. ▪ setup_partial: At least one step is successful, not completed or returns an error.

Part VI

Appendix

26 Running Anti-Virus Software

When Anti-Virus software is run on SBA components, make sure that the Antivirus file scanning exclusions are based on the Microsoft recommendations at https://technet.microsoft.com/EN-US/library/mt629173.aspx?f=255&MSPPError=-2147217396.

This page is intentionally left blank.

27 Configuring RAID

This section describes how to set up and enable RAID 1 (**R**edundant **A**rray of **I**ndependent **D**isks) on the device.

RAID 1 is achieved by using two solid-state drives (SSD) in a master-slave configuration, where the slave disk has an exact copy (or mirror) of the data on the master disk. Thus, RAID 1 provides redundancy for the SBA in case of failure of one of the disks.

SSD functionality is provided by the HDMX module of the device. Therefore, for RAID 1, you need to install two HDMX modules.

27.1 Prerequisites

Before configuring RAID, make sure the following prerequisites are met:

- SBA installation and configuration is complete.
- Second HDMX module is available (for slave):
  - Installed in Slot #8 on the rear panel (see figure below).
  - Unallocated (without a volume allocated).
  - Storage capacity is identical to the main HDMX module in Slot #1 (e.g., both are 256-GB RAM SSD).

Figure 27-1: HDMX Module Slot Assignment

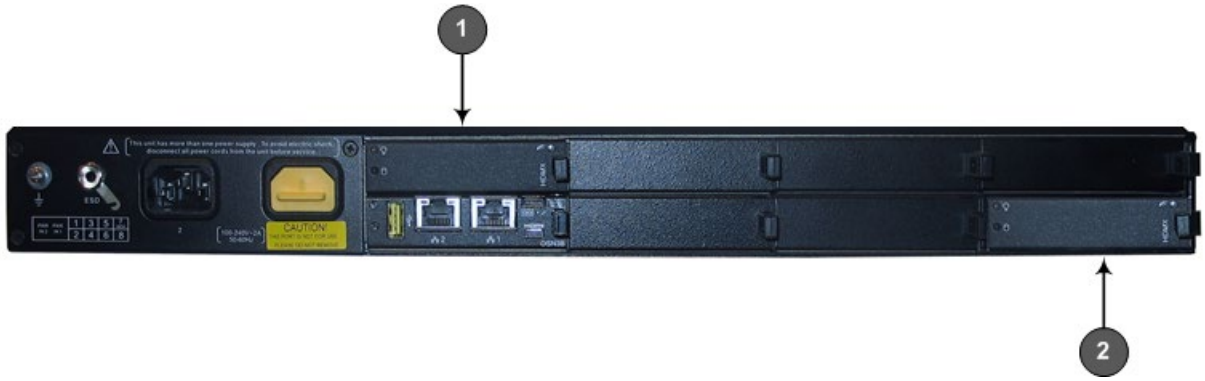


Table 27-1: HDMX Module Slot Assignment

Item #	Description
1	Primary (master) HDMX module in Slot #1
2	Secondary (slave) HDMX module in Slot #8

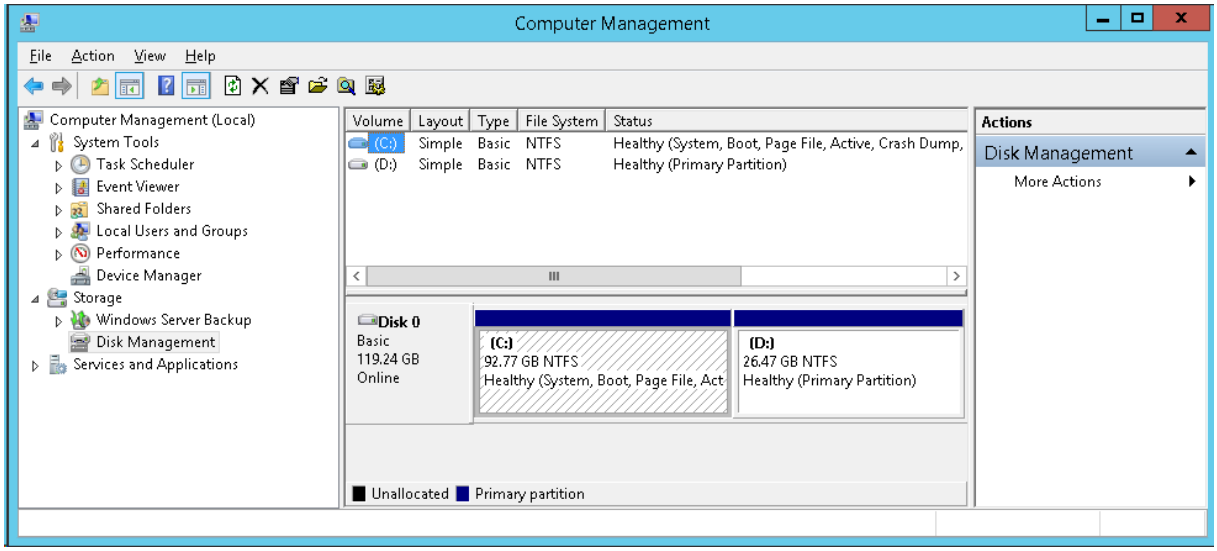
27.2 Configuring RAID 1

The procedure below describes how to configure RAID 1, where a mirrored volume is created for partition C.

➢ **To configure RAID 1:**

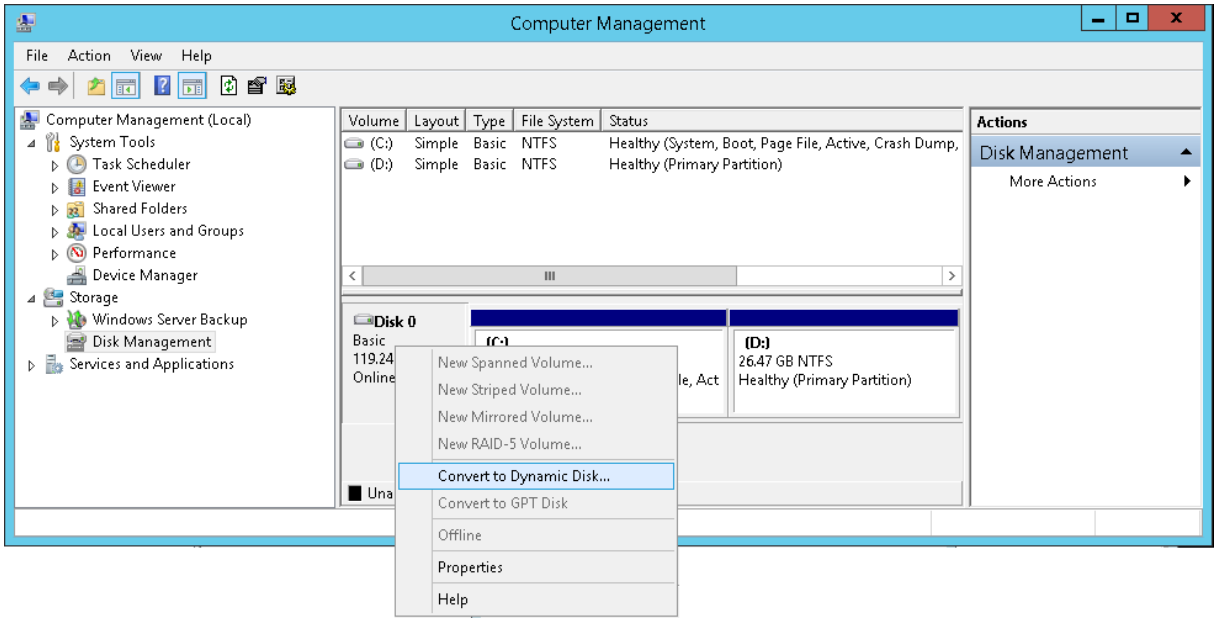
1. Connect to the SBA server through a Remote Desktop Connection (see Section 22.4).
2. Open the Computer Management window, and then navigate to the **Disk Management** item (**Storage** > **Disk Management**):

Figure 27-2: Disk Management



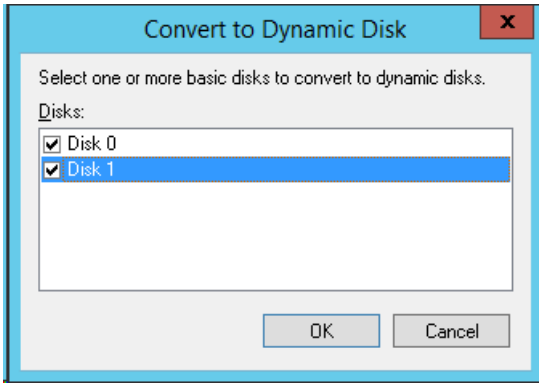
3. Right-click **Disk 0** (HDMX module in Slot #1), and then from the shortcut menu, choose **Convert to Dynamic Disk**:

Figure 27-3: Convert to Dynamic Disk



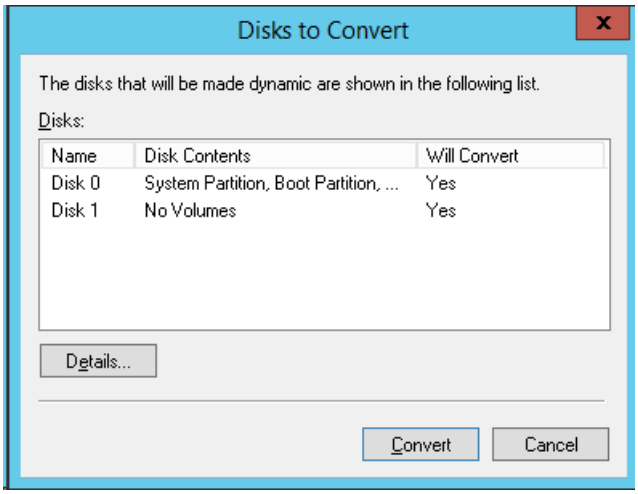
4. Select both disks:

Figure 27-4: Convert to Dynamic Disk Selection



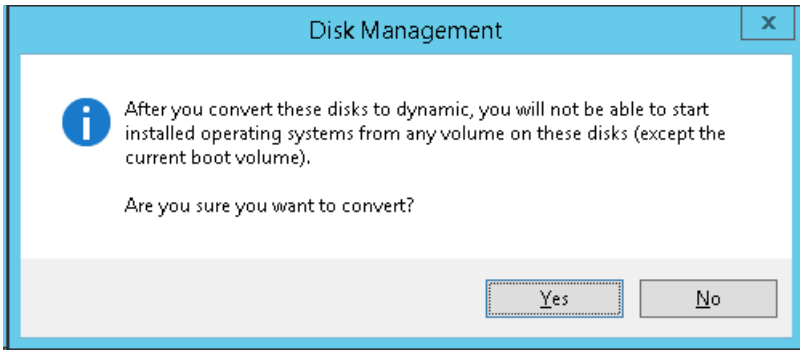
5. Click **OK**.

Figure 27-5: Disks to Convert



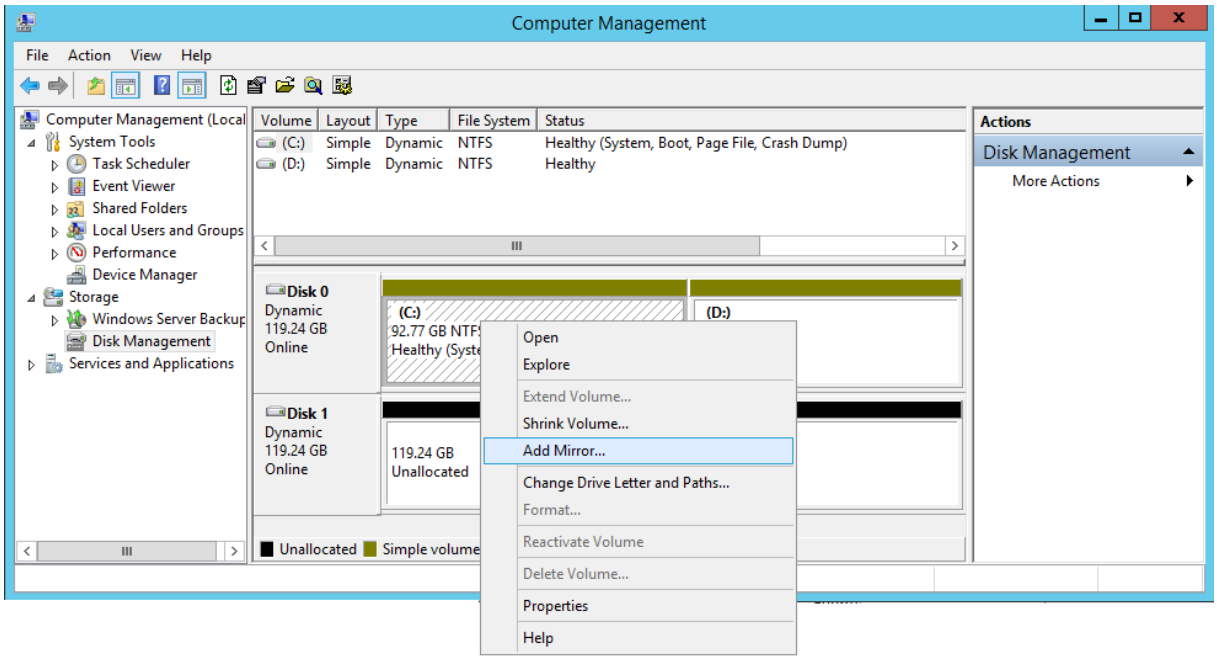
6. Click **Convert**.

Figure 27-6: Disk Management



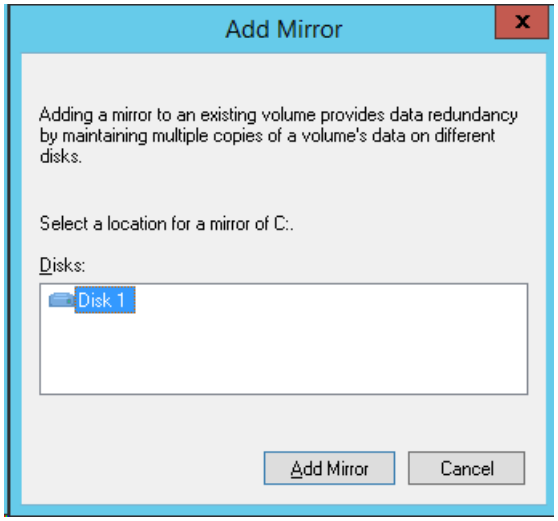
7. Click **Yes**.
8. Right-click volume (partition) **C**, and then from the shortcut menu, choose **Add Mirror**:

Figure 27-7: Add Mirror to Volume C



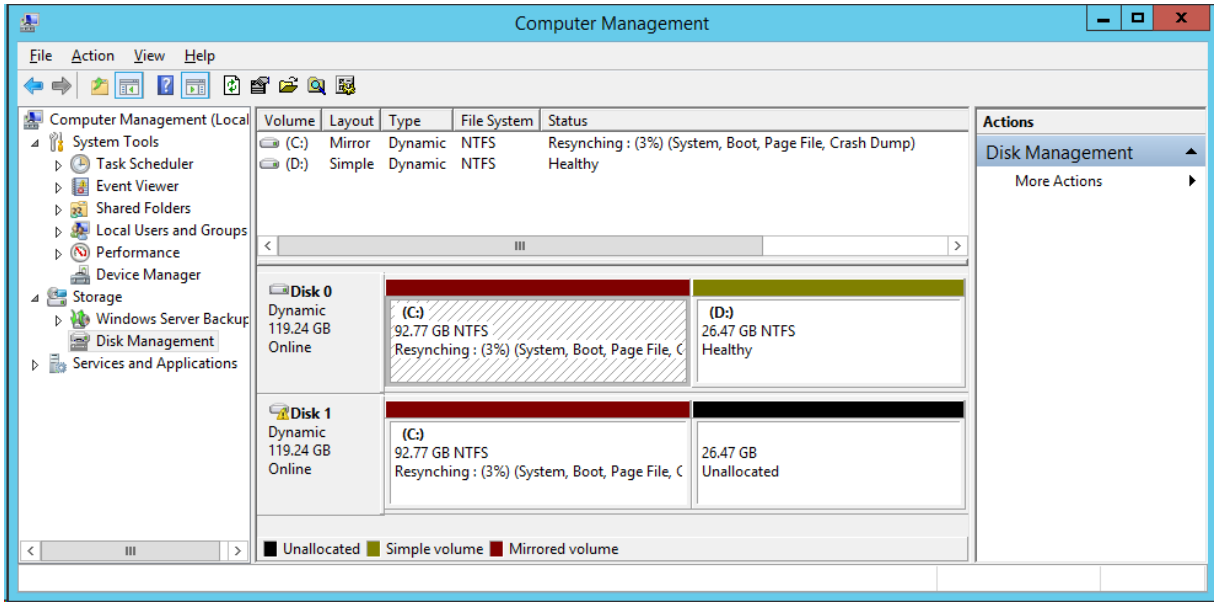
9. Select **Disk 1** (HDMX module in Slot #8) as the location for a mirror of volume C of Disk 0:

Figure 27-8: Add Mirror Disk 1



10. Click **Add Mirror**; the progress is displayed:

Figure 27-9: Disk Management - Resynchronization



Note: If you need to replace (for whatever reason) one of the HDMX modules, do the following:

1. Replace the HDMX modules.
2. Reset the SBA server (see Section 23).
3. Connect to the SBA server through a Remote Desktop Connection.
4. Open the Computer Management window, and then remove the mirrored disk volume.
5. Configure RAID to re-create a mirrored volume, as described in this section.

This page is intentionally left blank.

28 Configuring NIC Teaming

If you want to have network redundancy or network load balancing for the SBA server, you can configure two NIC interfaces on the OSN server as a team, so that the SBA server will be reachable on both interfaces through the same IP address.

Note: NIC teaming is supported only on the device's OSN3B, OSN3C, OSN4, and OSN4B modules. The support also assumes that an appropriate Intel network driver is installed.

28.1 Prerequisites

The following lists the prerequisites for creating NIC teaming:

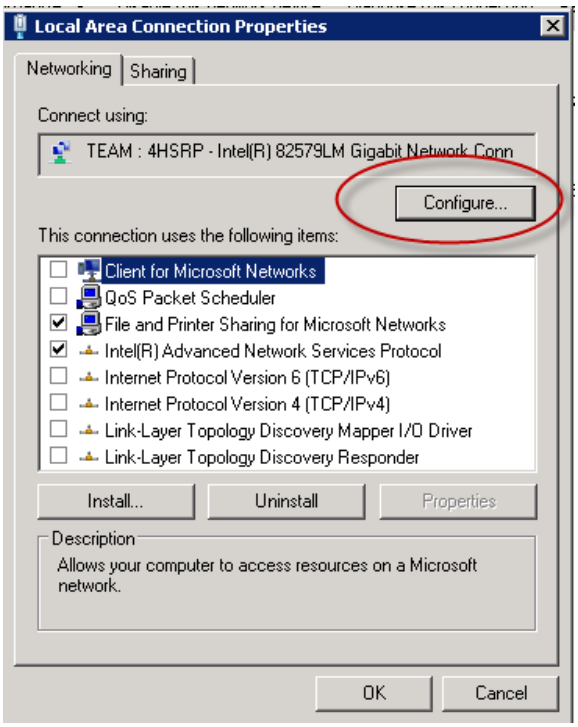
- The NIC interface driver must be updated with the May 2013 driver version or later. The recommended driver for NIC teaming can be downloaded from http://support.advantech.com.tw/Support/DownloadSRDetail_New.aspx?SR_ID=1-ND3LPH&Doc_Source=Download
- As a precaution, make sure that you have established serial communication with the SBA server. It is possible that after NIC teaming has been created, the SBA server will acquire an IP address from a DHCP server (you can configure a static IP address only afterwards).

28.2 Creating a Team for the Network Adapters

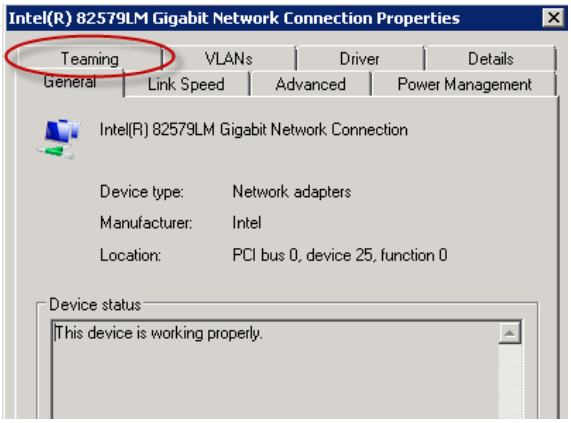
The following procedure describes how to create a team for the OSN server's network adapters.

➢ **To create a NIC team:**

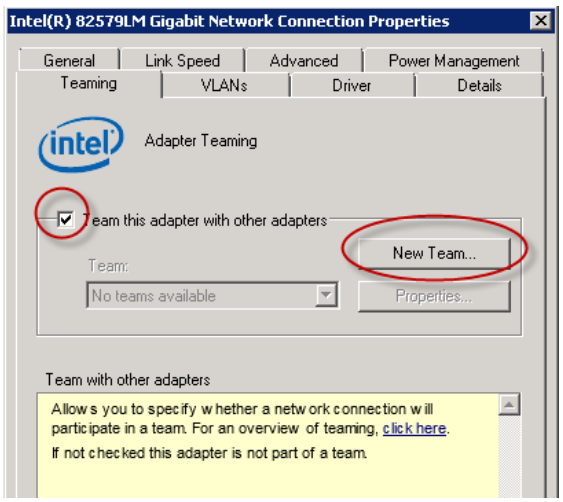
1. Right-click the NIC's properties, and then click **Configure**:



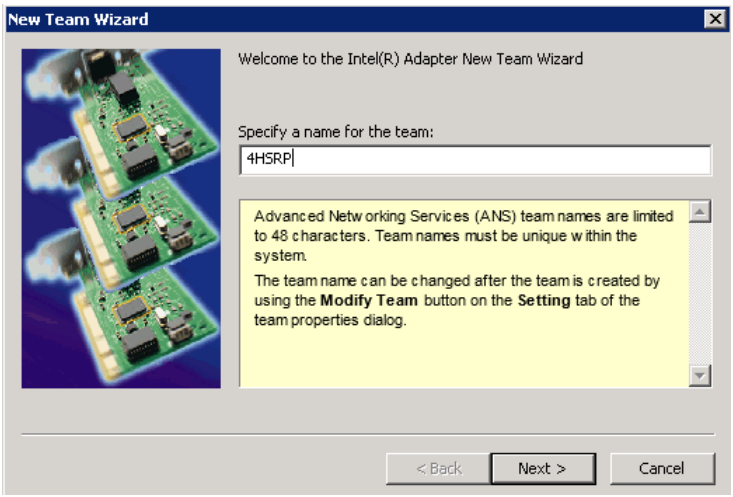
2. Click the **Teaming** tab:



3. Select the **Team this adapter with other adapters** check box, and then click **New Team**:

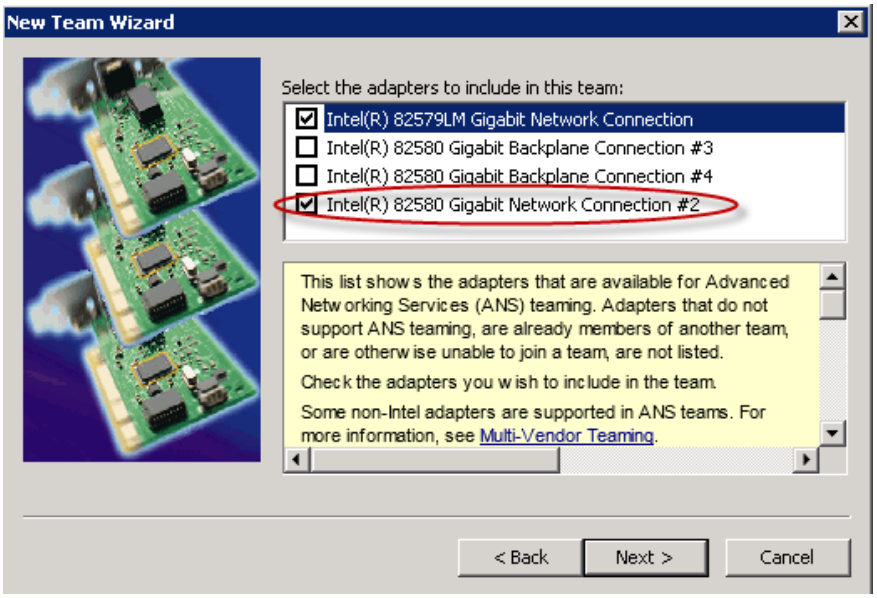


4. In the 'Specify a name for the team' field, enter a name for the team:



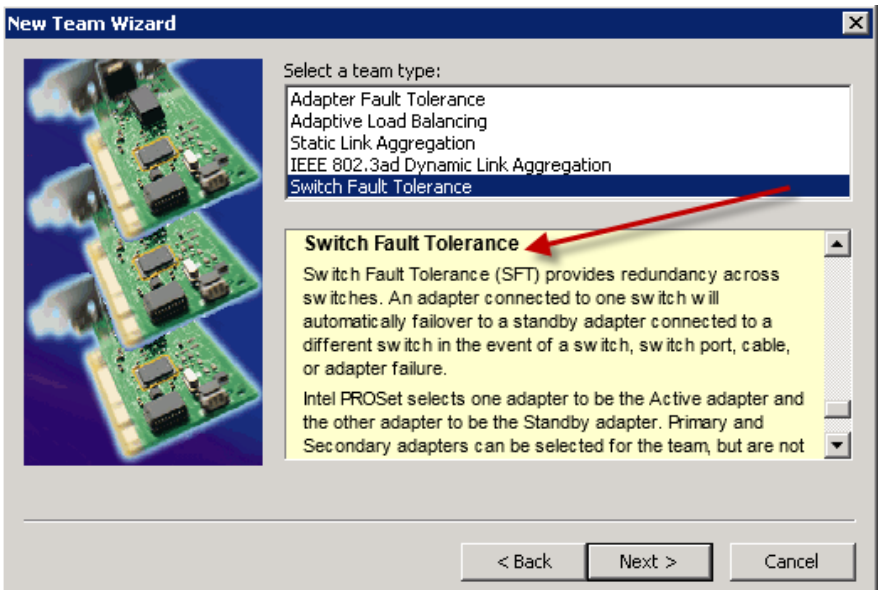
5. Click **Next**.

6. Select the adapters to include in the team. Make sure that you select the correct interfaces (in our case, physical interfaces and not backplane interfaces):

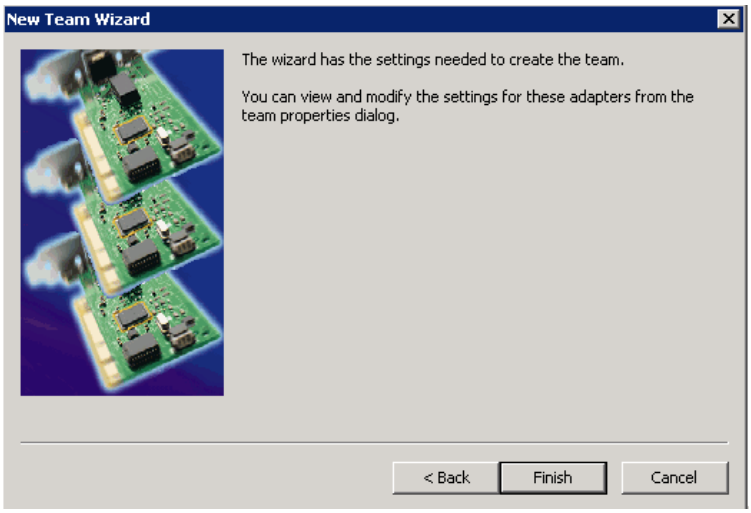


7. Click **Next**.

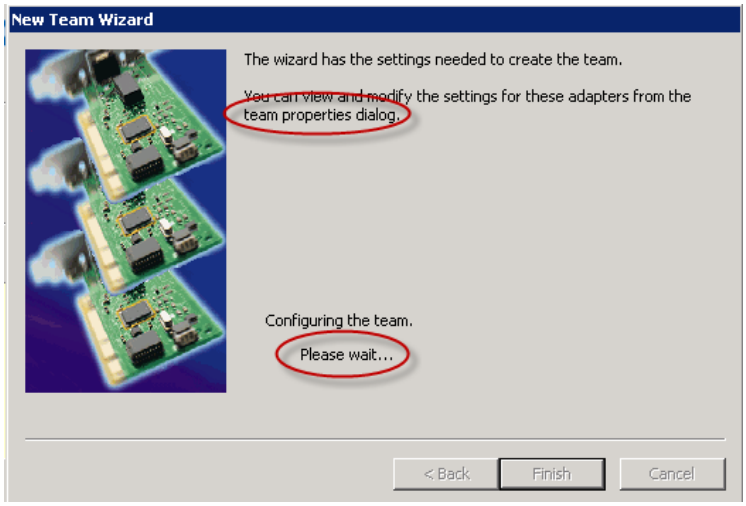
8. Select the team type. An explanation of each team type is shown in the pane below. Select the type most suitable for your NIC teaming:



9. Click **Next**:



10. Click **Finish**; the wizard begins creating the team (this may take a few minutes). At this stage, you may lose connectivity with the SBA server.



11. View the IP address assigned to the NIC team:
    a. Open the serial interface.
    b. At the prompt, type the following:

```
i
```

```
SAC>
SAC>
SAC>
SAC>i
Net: 29, Disconnected
Net: 32, Disconnected
Net: 35, Ip=10.21.2.15  Subnet=255.255.0.0  Gateway=10.21.0.1
Net: 35, Ip=fe80::a46d:dce4:dba5:ac25
```

28.3 Post Installation

Once you have created the NIC team, check that the SBA server is accessible from both NICs:

1. Disconnect the first cable.
2. Verify that you still have connectivity to the server.
3. Reconnect the first cable.
4. Disconnect the second cable.
5. Verify that you still have connectivity to the server.
6. Reconnect the second cable.

If required, you can right-click the team's properties and modify its settings.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
200 Cottontail Lane
Suite A101E
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com

©2019 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice

Document #: LTRT-40162