Microsoft® Lync™ Server 2010

Survivable Branch Appliance

Mediant™ 800 SBA

SBA Installation Manual

Mediant 800 SBA

for Microsoft Lync Server 2010

HD VoIP Sounds Better

MSBG AudioCodes Multi Service Business Gateway

Microsoft® Lync™

Microsoft Partner Gold Unified Communications

AudioCodes

Version 6.4

April 2013

Document #: LTRT-39153

Table of Contents

1 Introduction 11

2 Verifying Package Contents 15

3 Mediant 800 SBA Hardware Description 17

3.1 Physical Description 17

3.1.1 Front Panel Description 17
3.1.2 Rear Panel Description 18
3.1.3 LEDs Description 20
3.1.3.1 LAN Interface LED 20
3.1.3.2 FXS LED 20
3.1.3.3 FXO LED 21
3.1.3.4 E&M LED 21
3.1.3.5 BRI LED Description 21
3.1.3.6 E1/T1 LED Description 22
3.1.3.7 Operational Status LED 22
3.1.3.8 Power LED 22

4 Assigning IP Address to PSTN Gateway 23

4.1 Initial Access PSTN Gateway with Default IP Address 23
4.2 Configuring Physical LAN Ports Pair 25
4.3 Configuring an IP Address 27

5 Pre-Configuring SBA at Datacenter 29

5.1 Adding the SBA Device to the Active Directory 29
5.2 Defining the Branch Office Topology using Topology Builder 31
5.2.1 Defining the Branch Office 31
5.2.2 Publishing the Topology 39

6 Connecting to the SBA Web-Based Tool 41

7 Installing and Configuring the SBA 45

7.1 Step 1: IP Settings 47
7.2 Step 2: Change Computer Name 50
7.3 Step 3: Change Admin Password 54
7.4 Step 4: Set Date and Time 56
7.5 Step 5: Join to a Domain 59
7.6 Step 6: Device Preparation 62
7.7 Step 7: Configuration 68
7.8 Step 8: Enable Replication 70
7.9 Step 9: Activate MCS 72
7.10 Step 10: MCS Certificate 74
7.11 Step 11: Start MCS Services 80
7.12 Step 12: Gateway Configuration 81

8 Configuring the PSTN Gateway 83

8.1 Configuring the Mediation Server 83
8.2 Restricting Communication to Mediation Server Only 88
8.3 Configuring the SIP Transport Type 90
8.3.1 Configuring TLS 90
8.3.1.1 Step 1: Enable TLS and Define TLS Port 90

8.3.1.2 Step 2: Configure the NTP Server 91
8.3.1.3 Step 3: Configure the DNS Server 92
8.3.1.4 Step 4: Configure the Gateway Name 93
8.3.1.5 Step 5: Configure a Certificate 94
8.3.1.5.1 Generate a Certificate Signing Request....94
8.3.1.5.2 Obtain Microsoft CA and Trusted Root Certificates 95
8.3.1.5.3 Load Microsoft CA and Trusted Root Certificates to PSTN Gateway 99
8.3.2 Configuring TCP Transport Type....100
8.4 Configuring Secure Real-Time Transport Protocol 101
8.5 Configuring Voice Coders (with Silence Suppression) 103
8.6 Configuring Comfort Noise and Gain Control....104
8.7 Configuring Early Media 106
8.8 Configuring PSTN Trunks....108
8.8.1 Enabling Trunks....108
8.8.2 Configuring Channel Select Method....109
8.8.3 Configuring IP-to-Trunk Group Routing....110
8.8.4 Configuring FXS Port Transfer Behavior 111
8.8.5 Configuring the Trunk 112
8.8.6 Configuring the TDM Bus 114
8.9 Configuring Normalization Rules for E.164 Format for PBX/PSTN Connectivity .115
8.9.1 Number Normalization Examples....118
8.9.1.1 Modifying E.164 Numbers to PBX / PSTN Format for Outbound Calls .118
8.9.1.2 Modifying PBX, Local, and National Calls to E.164 Format for Inbound Calls 120
9 Testing SBA Calls 121
9.1 Testing Gateway Calls....121
9.2 Testing Lync Calls 123
9.2.1 Test Prerequisites....123
9.2.2 Running the Lync Call Test 124
10 Completing SBA Setup 125
11 Miscellaneous SBA Procedures 127
11.1 Viewing General SBA Status in the Home Page....127
11.2 Starting and Stopping SBA Services 128
11.3 Updating SBA Components....129
11.4 Viewing Logged Events 133
11.5 Logging Out....133

List of Figures

Figure 1-1: Mediant 800 SBA in Lync Server 2010 Environment..12
Figure 1-2: Summary of Steps for Installing and Configuring SBA 13
Figure 3-1: Physical Description..17
Figure 3-2: LAN Port-Pair Groups and Web Interface String Names 18
Figure 3-3: Mediant 800 Rear Panel 18
Figure 4-1: Connecting Mediant 800 SBA LAN Port 1 (Front Panel)...23
Figure 4-2: Login Screen 24
Figure 4-3: Physical Ports Settings Page...25
Figure 4-4: IP Settings Screen 27
Figure 4-5: Maintenance Actions: Reset Gateway..27
Figure 5-1: New Object – Computer Dialog Box 29
Figure 5-2: RTC Universal Read Only Admins Properties 30
Figure 5-3: Menu Path to Topology Builder Program..31
Figure 5-4: Topology Builder 32
Figure 5-5: Lync Server 2010 Topology Builder..32
Figure 5-6: Identify the Site 33
Figure 5-7: Specify Site Details 34
Figure 5-8: New Branch Site Successfully Defined..34
Figure 5-9: Define the Survivable Branch Appliance FQDN 35
Figure 5-10: Select the Front End Pool 36
Figure 5-11: Select an Edge Server 37
Figure 5-12: Define the PSTN Gateway...37
Figure 5-13: Publish Topology Selection...39
Figure 5-14: Publish the Topology 39
Figure 5-15: Publish Wizard Complete..40
Figure 6-1: Connecting to the OSN Server 42
Figure 6-2: SBA Login Screen...42
Figure 6-3: SBA Home Screen 43
Figure 7-1: Setup Tab Displaying Tasks 46
Figure 7-2: Set IP Configuration Page 47
Figure 7-3: IP Settings – Login Again...48
Figure 7-4: Alert - Login..48
Figure 7-5: Login Screen 49
Figure 7-6: IP Settings - Complete 49
Figure 7-7: Change Computer Name Screen...50
Figure 7-8: Change Computer Name - Reboot 51
Figure 7-9: Change Computer Name – Applied Changes 51
Figure 7-10: Server Re-booting..52
Figure 7-11: Login Screen...52
Figure 7-12: Change Computer Name – Completed Successfully 53
Figure 7-13: Change Admin Password Screen...54
Figure 7-14: Change Admin Password – Applied Changes..54
Figure 7-15: Change Admin Password – Completed Successfully...55
Figure 7-16: Set Date and Time Screen..56
Figure 7-17: Set Date and Time - Time Zone..56
Figure 7-18: Set Date and Time – Notification Message 57
Figure 7-19: Set Date and Time – Applied Changes 57
Figure 7-20: Set Date and Time - Completed Successfully 58
Figure 7-21: Join to a Domain Screen..59
Figure 7-22: Join to a Domain – Reboot Message Box 59
Figure 7-23: Join to a Domain – Applied Changes 60
Figure 7-24: Server Rebooting 60
Figure 7-25: Welcome to SBA...61
Figure 7-26: Join to a Domain - Completed Successfully 61
Figure 7-27: Device Preparation Screen 62
Figure 7-28: Device Preparation - Started..62
Figure 7-29: Device Preparation – SQL Installation..63

Figure 7-30: Device Preparation – Ocscore Installation....63
Figure 7-31: Device Preparation – Server Installation....64
Figure 7-32: Device Preparation – Mediation Server Installation....64
Figure 7-33: Device Preparation – Restart Message Box....65
Figure 7-34: Device Preparation – Restart....65
Figure 7-35: Login Screen....66
Figure 7-36: Device Preparation – Completed Successfully....67
Figure 7-37: Configuration Screen....68
Figure 7-38: Configuration – Applied Successfully....68
Figure 7-39: Configuration – Completed Successfully....69
Figure 7-40: Enable Replication Screen....70
Figure 7-41: Enable Replication – Applied Successfully....70
Figure 7-42: Enable Replication – Completed Successfully....71
Figure 7-43: Activate MCS Screen....72
Figure 7-44: Activate MCS – Applied Successfully....72
Figure 7-45: Activate MCS – Completed Successfully....73
Figure 7-46: MCS Certificate Screen....74
Figure 7-47: Request Certificate....75
Figure 7-48: MCS Certificate – Detailed Log....76
Figure 7-49: MCS Certificate – Download Enrolled Certificate....76
Figure 7-50: MCS Certificate – Download Enrolled Certificate....77
Figure 7-51: MCS Certificate – File Download....77
Figure 7-52: MCS Certificate – File Upload....78
Figure 7-53: MCS Certificate – Detail Log....78
Figure 7-54: MCS Certificate – Complete....79
Figure 7-55: Start MCS Services Screen....80
Figure 7-56: Start MCS Services – Completed Successfully....80
Figure 7-57: Gateway Configuration Screen....81
Figure 7-58: Gateway Configuration – Manual Gateway....82
Figure 8-1: Proxy & Registration Page....84
Figure 8-2: Proxy Sets Table Page....85
Figure 8-3: Reasons for Alternative Routing Page....86
Figure 8-4: SIP General Parameters Page....87
Figure 8-5: Advanced Parameters Page....88
Figure 8-6: Outbound IP Routing Table....89
Figure 8-7: SIP General Parameters Page....90
Figure 8-8: Application Settings Page....91
Figure 8-9: DNS Server Settings....92
Figure 8-10: Proxy & Registration Page....93
Figure 8-11: Certificates Page....94
Figure 8-12: Microsoft Certificate Services Web Page....95
Figure 8-13: Request a Certificate Page....96
Figure 8-14: Advanced Certificate Request Page....96
Figure 8-15: Submit a Certificate Request or Renewal Request Page....97
Figure 8-16: Download a CA Certificate, Certificate Chain, or CRL Page....98
Figure 8-17: Certificates Page....99
Figure 8-18: SIP General Parameters Page....100
Figure 8-19: Media Security Page....101
Figure 8-20: Coders Table Page....103
Figure 8-21: RTP/RTCP Settings Page....104
Figure 8-22: IPMedia Settings Page....105
Figure 8-23: SIP General Parameters Page (1)....106
Figure 8-24: SIP General Parameters Page (2)....107
Figure 8-25: Advanced Parameters Page....107
Figure 8-26: Trunk Group Table Page....108
Figure 8-27: Trunk Group Settings Page....109
Figure 8-28: Inbound IP Routing Table Page....110
Figure 8-29: Enable Call Transfer Using Reinvites....111
Figure 8-30: Trunk Settings Page....112

Figure 8-31: TDM Bus Settings Page....114
Figure 8-32: Source Phone Number Manipulation Table for Tel-to-IP Calls....115
Figure 8-33: Destination Phone Number Manipulation Table for IP→Tel Calls....119
Figure 8-34: Destination Phone Number Manipulation Table for Tel→IP Calls....120
Figure 9-1: Enabling Telnet....121
Figure 9-2: Gateway Configuration – Calling the Phone....122
Figure 9-3: Gateway Configuration – Call Answered....122
Figure 9-4: OCS Test Call Screen....124
Figure 9-5: OCS Test Call – Logged Call Test Result....124
Figure 10-1: Complete Setup Screen....125
Figure 10-2: Complete Setup – Setup Completed....125
Figure 10-3: Complete Setup – Completed Successfully....126
Figure 11-1: Home Page....127
Figure 11-2: Start and Stop Service Page....128
Figure 11-3: Tools-System Update Menu....129
Figure 11-4:System Update Screen....130
Figure 11-5:System Update Timestamp and Message....130
Figure 11-6: System Update Message-SBA System Components....131
Figure 11-7: Login Screen after Automatic Log Out....131
Figure 11-8: Logs Screen Displaying Logged Events....133
Figure 11-9: Detailed Log Display....133

List of Tables

Table 3-1: Mediant 800 Front Panel 17
Table 3-2: Mediant 800 Rear Panel 19
Table 3-3: LAN LEDs Description 20
Table 3-4: FXS LEDs Description 20
Table 3-5: FXO LEDs Description 21
Table 3-6: E&M LEDs Description 21
Table 3-7: BRI LEDs Description 21
Table 3-8: E1/T1 LEDs Description 22
Table 3-9: STATUS LEDs Description 22
Table 3-10: POWER LEDs Description 22
Table 8-1: Number Manipulation Parameters Description 116

Notice

This document describes how to install and configure the Mediant 800 Survivable Branch Appliance (SBA), located at the remote branch office and deployed in the Microsoft Lync Server 2010 environment.

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 the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents, as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

Date Published: April-10-2013

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX 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.

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 service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact support@audiocodes.com.

Abbreviations and Terminology

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

Related Documentation

Manual Name
Mediant 800 SBA Quick Guide
Mediant 800 Enhanced Gateway and Analog Devices for Lync Installation Manual
Mediant 800 SBA Software Upgrade and Recovery for MS Lync Configuration Note
AudioCodes SCOM MP User Guide

1 Introduction

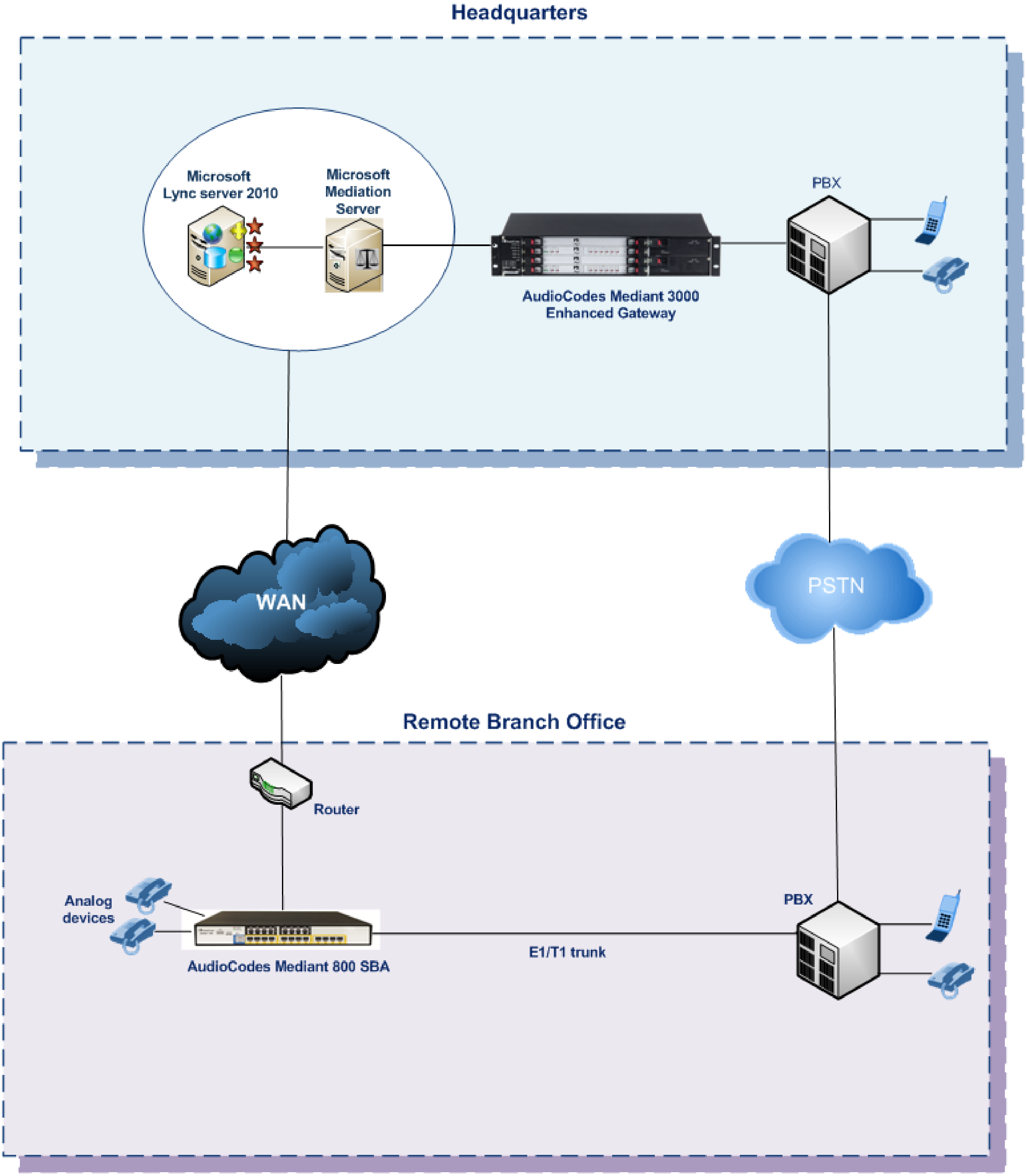
This document provides step-by-step instructions on installing and configuring the Survivable Branch Appliance (SBA) application running on AudioCodes Mediant 800 SBA, located at the remote branch office and deployed in the Lync Server 2010 environment. The Mediant 800 SBA includes an OSN Server platform with Windows Server 2008 R2 operating system, and with preinstalled Lync Server 2010 Registrar and Mediation Server software installation (MSI), and a PSTN gateway, all in a single appliance chassis.

In the Lync Server 2010 environment, given the centralized deployment model, Unified Communication (UC) users in a remote site are dependent on the servers in the enterprise's data center (typically at headquarters) for their communication, and hence are vulnerable to losing communication capabilities when the WAN is unavailable. Given the always-available expectation for voice, it is imperative that the UC solution continues to provide the ability for branch users to make and receive calls when the WAN from the branch to the primary data center is unavailable.

To provide voice services to branch users during a WAN outage, a branch office survivability solution–the Survivable Branch Appliance (SBA) application–is hosted on the OSN Server platform running on AudioCodes Mediant 800 SBA located at the branch office. During a WAN connectivity failure, Mediant 800 SBA maintains call connectivity among Microsoft users located at the branch office–Lync Server 2010 clients (for example, Microsoft Lync clients) and devices (for example, IP phones)–and between these users and the public switched telephone network (PSTN).

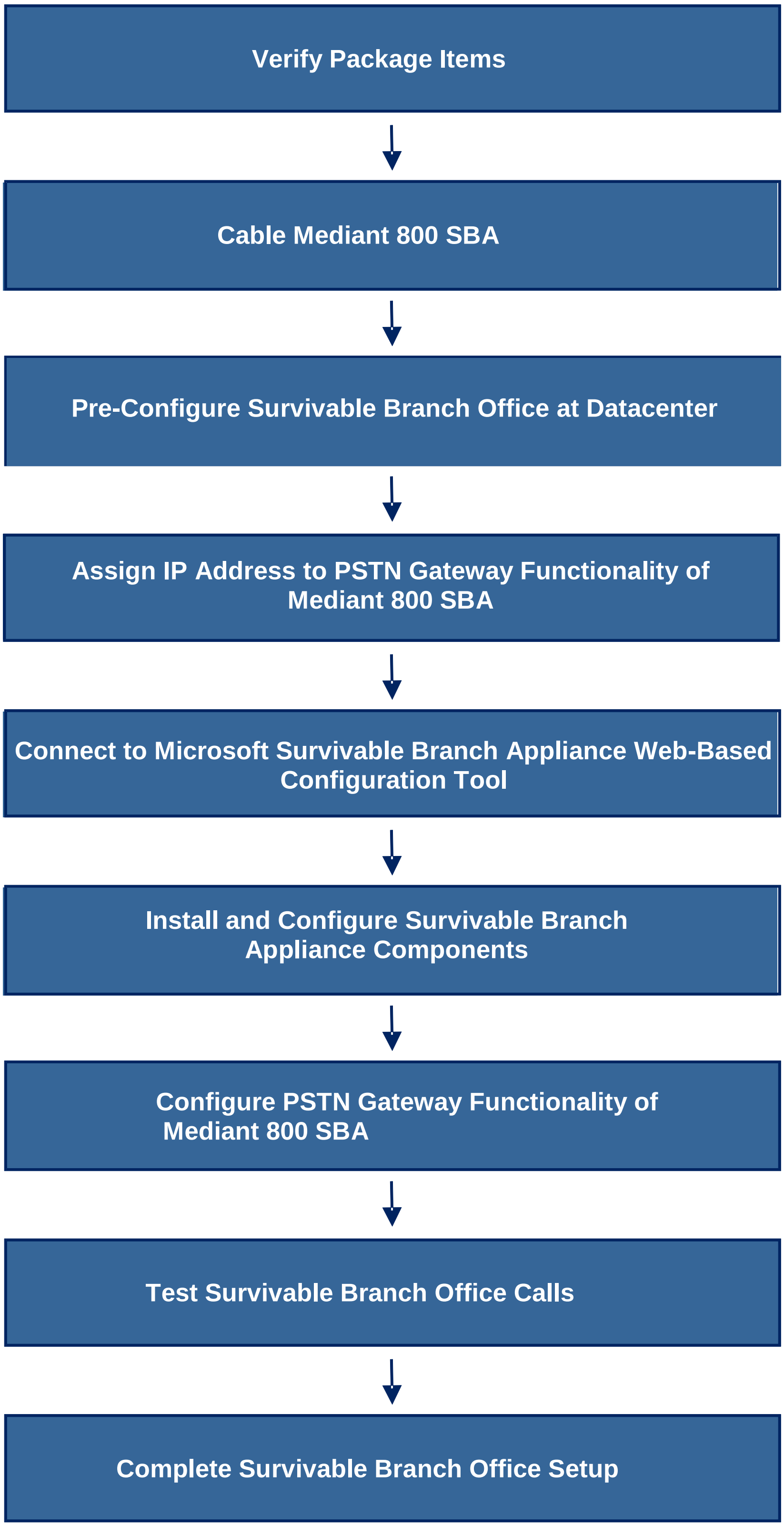
The figure below illustrates the integration of the Mediant 800 SBA in the Lync Server 2010 environment.

Figure 1-1: Mediant 800 SBA in Lync Server 2010 Environment


Headquarters
Microsoft Lync server 2010
Microsoft Mediation Server
AudioCodes Mediant 3000 Enhanced Gateway
PBX
WAN
PSTN
Remote Branch Office
Router
Analog devices
AudioCodes Mediant 800 SBA
E1/T1 trunk
PBX

The summary of the steps required to install the Mediant 800 SBA is shown in the figure below:

Figure 1-2: Summary of Steps for Installing and Configuring SBA


Verify Package Items
Cable Mediant 800 SBA
Pre-Configure Survivable Branch Office at Datacenter
Assign IP Address to PSTN Gateway Functionality of Mediant 800 SBA
Connect to Microsoft Survivable Branch Appliance Web-Based Configuration Tool
Install and Configure Survivable Branch Appliance Components
Configure PSTN Gateway Functionality of Mediant 800 SBA
Test Survivable Branch Office Calls
Complete Survivable Branch Office Setup

Reader's Notes

2 Verifying Package Contents

Ensure that your Mediant 800 SBA package is shipped with the following items:

- Four anti-slide bumpers for desktop installation
- 19-inch rack mounting kit (two flanges and six screws)
- RS-232 serial cable adaptor for serial communication between the Mediant 800 PSTN gateway functionality (flat connector) and a computer (red DB-9 connector)
- Two mounting brackets for 19-inch rack mounting
- One FXS Lifeline cable adapter (only for models with FXS interfaces)
- One AC power cable
- USB tool for SBA software upgrade and recovery procedure
- Microsoft Windows 2008 license document (envelope)

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

Reader’s Notes

3 Mediant 800 SBA Hardware Description

This section provides a hardware description overview of the Mediant 800 SBA and instructions on how to cable the Mediant 800 SBA.

3.1 Physical Description

3.1.1 Front Panel Description

The Mediant 800 front panel is shown below and described in the subsequent table:

Figure 3-1: Physical Description

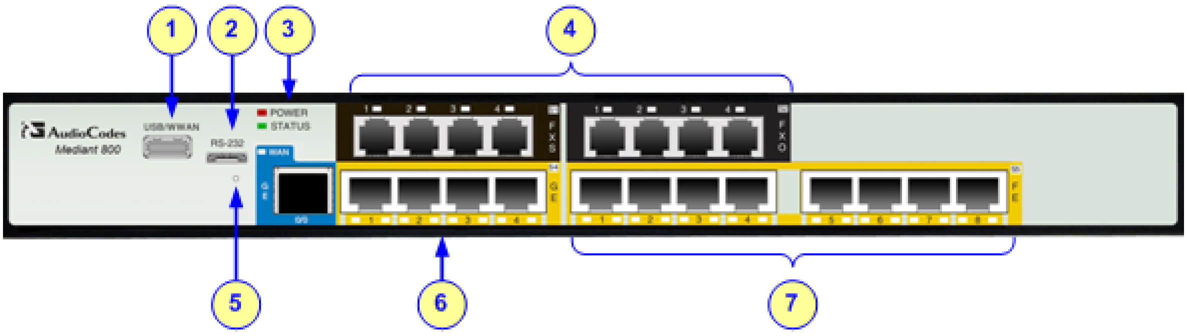


Table 3-1: Mediant 800 Front Panel

Item	Label	Description
1	USB/WWAN	Not Applicable
2	RS-232	RS-232 port for serial communication.
3	POWER / STATUS	LEDs indicating the status of the power, reboot/initialization
4	FXS / FXO / BRI / E&M / Digital	Optional telephony interfaces: ▪ FXS interfaces (RJ-11 port) ▪ FXO interfaces (RJ-11 port) ▪ BRI interfaces (RJ-45 port) ▪ E&M interfaces (RJ-45 port) ▪ E1/T1 PSTN interface (RJ-48 port)
5	**-**	Reset pinhole button for resetting the device and restoring it to factory defaults
6	GE	Up to four 10/100/1000Base-T (Gigabit Ethernet) RJ-45 LAN ports for connecting IP phones, computers, or switches. These ports support half- and full-duplex modes, auto-negotiation, straight or crossover cable detection, and Power over Ethernet (PoE). **1+1 LAN port redundancy:** These ports are grouped in pairs, where one port is active and the other redundant. When a failure occurs in the active port, a switchover is done to the redundant port.

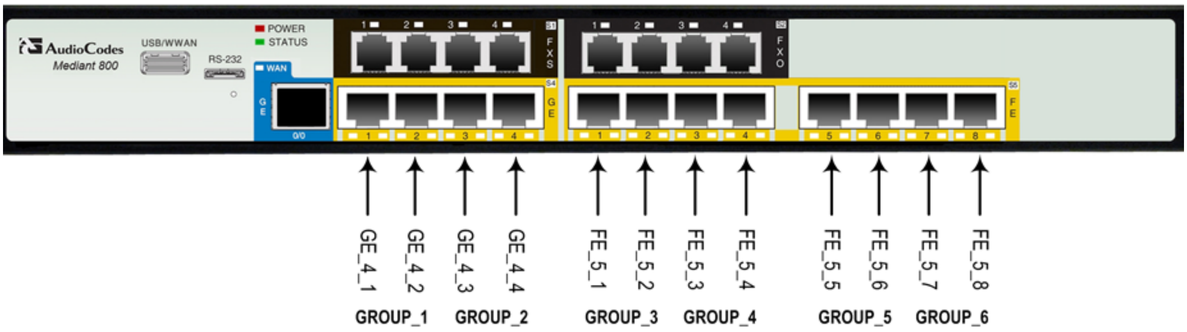
Item	Label	Description
7	FE	Eight 10/100Base-TX (Fast Ethernet) RJ-45 LAN ports for connecting IP phones, computers, or switches. These ports support half- and full-duplex modes, auto-negotiation, straight or crossover cable detection, and PoE. **1+1 LAN port redundancy:** These ports are grouped in pairs, where one port is active and the other redundant. When a failure occurs in the active port, a switchover is done to the redundant port.

The device provides up to four 10/100/1000Base-T (Gigabit Ethernet) RJ-45 ports and up to eight 10/100Base-TX (Fast Ethernet) RJ-45 ports for connection to the LAN.

These LAN ports operate in pairs (*groups*) to provide LAN port 1+1 redundancy. In each pair, one port serves as the active LAN port while the other as standby. When the active port fails, the device switches to the standby LAN port.

The figure below shows the LAN port-pair groups and the name of the ports and groups as displayed in the Web interface for configuring the port groups and assigning them to IP network interfaces (refer to the *User's Manual* for more information):

Figure 3-2: LAN Port-Pair Groups and Web Interface String Names



3.1.2 Rear Panel Description

The Mediant 800 rear panel is shown below and described in the subsequent table:

Figure 3-3: Mediant 800 Rear Panel

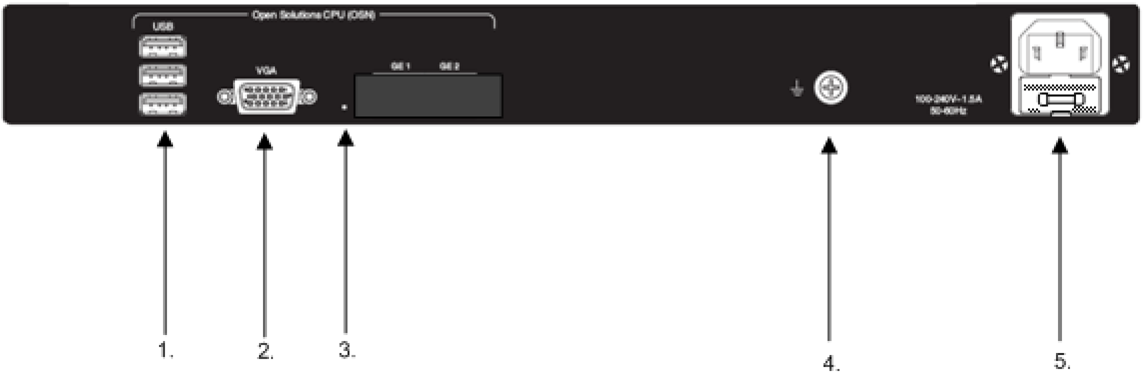


Table 3-2: Mediant 800 Rear Panel

Item	Label	Description
1	OSN USB	Three USB ports (Standard-A type) for connecting computer peripherals (e.g., mouse and keyboard) when using the OSN Server platform.
2	OSN VGA	15-Pin DB-type female VGA port for connecting to a monitor (screen) when using the OSN Server platform.
3		Reset pinhole button for resetting the OSN Server.
4	⏚	Protective earthing screw.
5	100-240V ~1.5A 50-60Hz	3-Prong AC power supply entry.

3.1.3 LEDs Description

The front panel provides various LEDs depending on the device's hardware configuration (e.g., the available telephony interfaces). These LEDs are described in the subsequent subsections.

3.1.3.1 LAN Interface LED

Each LAN port provides a LED (located on its left) for indicating LAN operating status, as described in the table below.

Table 3-3: LAN LEDs Description

LED Color	LED State	Description
Green	On	Ethernet link established.
	Flashing	Data is being received or transmitted.
-	Off	No Ethernet link.

3.1.3.2 FXS LED

Each FXS port provides a LED for indicating operating status, as described in the table below.

Table 3-4: FXS LEDs Description

LED Color	LED State	Description
Green	On	Phone is off-hooked.
	Flashing	Rings the extension line.
Red	On	Error - malfunction in line or out of service due to Serial Peripheral Interface (SPI) failure.
-	Off	Phone is on hook.
-	Off	No power received by the device.

3.1.3.3 FXO LED

Each FXO port provides a LED for indicating operating status, as described in the table below.

Table 3-5: FXO LEDs Description

LED Color	LED State	Description
Green	On	FXO line is off-hooked toward the PBX.
	Flashing	Ring signal detected from the PBX.
Red	On	Error - malfunction in line or out of service due to Serial Peripheral Interface (SPI) failure.
-	Off	Line is on hook.
-	Off	No power received by the device.

3.1.3.4 E&M LED

Each E&M port provides a LED for indicating operating status, as described in the table below.

Table 3-6: E&M LEDs Description

LED Color	LED State	Description
Green	On	Off-hook (default)
-	Off	On-hook
Red	On	Line malfunction (default)
-	Off	Normal operation

3.1.3.5 BRI LED Description

Each BRI port provides a LED for indicating operating status, as described in the table below:

Table 3-7: BRI LEDs Description

LED Color	LED State	Description
Green	On	Physical layer (Layer 1) is synchronized (normal operation).
Red	On	Physical layer (Layer 1) is not synchronized.
-	Off	Trunk is not active.

3.1.3.6 E1/T1 LED Description

Each trunk port provides a LED for indicating operating status, as described in the table below:

Table 3-8: E1/T1 LEDs Description

LED Color	LED State	Description
Green	On	Trunk is synchronized (normal operation).
Red	On	Loss due to any of the following signals: ▪ LOS - Loss of Signal ▪ LOF - Loss of Frame ▪ AIS - Alarm Indication Signal (the Blue Alarm) ▪ RAI - Remote Alarm Indication (the Yellow Alarm)
-	Off	Failure / disruption in the AC power supply or the power is currently not being supplied to the device through the AC power supply entry.

3.1.3.7 Operational Status LED

The **STATUS** LED indicates the operating status, as described in the table below.

Table 3-9: STATUS LEDs Description

LED Color	LED State	Description
Green	On	The device is operational.
	Flashing	The device is rebooting.
Red	On	Boot failure.

3.1.3.8 Power LED

The **POWER** LED indicates the operating status, as described in the table below.

Table 3-10: POWER LEDs Description

LED Color	LED State	Description
Green	On	Power is received by the device.
-	Off	No power received by the device.

4 Assigning IP Address to PSTN Gateway

The Mediant 800 SBA includes an embedded Web server (*Web interface*), providing a user-friendly graphical user interface (GUI) for configuring PSTN gateway-related functionality (*PSTN Gateway*). Before you can configure the PSTN gateway, you need to first access it with the default VoIP / Management LAN IP address, which must then be changed to suit the networking scheme in which your Mediant 800 SBA is deployed. In addition, you need to configure the LAN port redundancy.

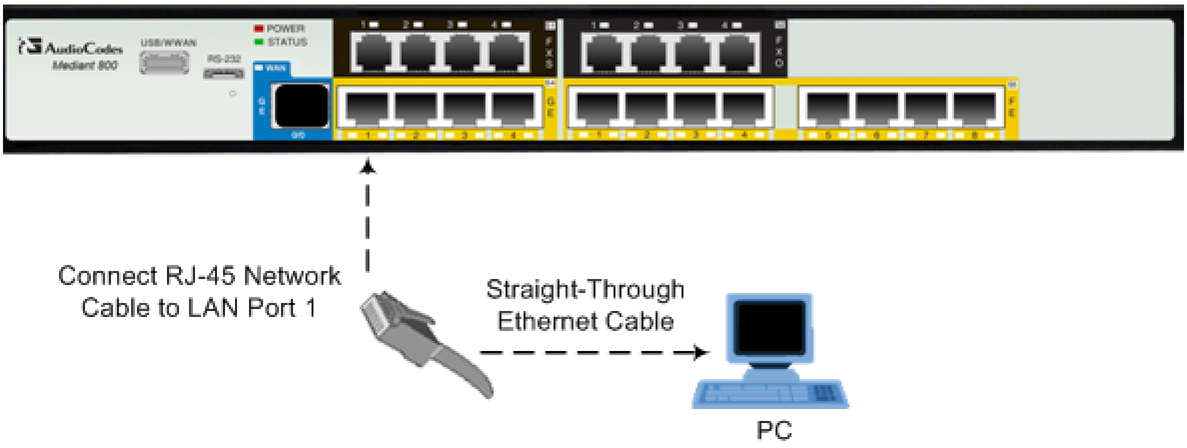
4.1 Initial Access PSTN Gateway with Default IP Address

You need to initially access the PSTN gateway with the device's default IP address.

➢ **To initially access the PSTN gateway:**

1. Connect LAN port 1 (located on the front panel of Mediant 800) directly to a computer, using a straight through Ethernet cable.

Figure 4-1: Connecting Mediant 800 SBA LAN Port 1 (Front Panel)

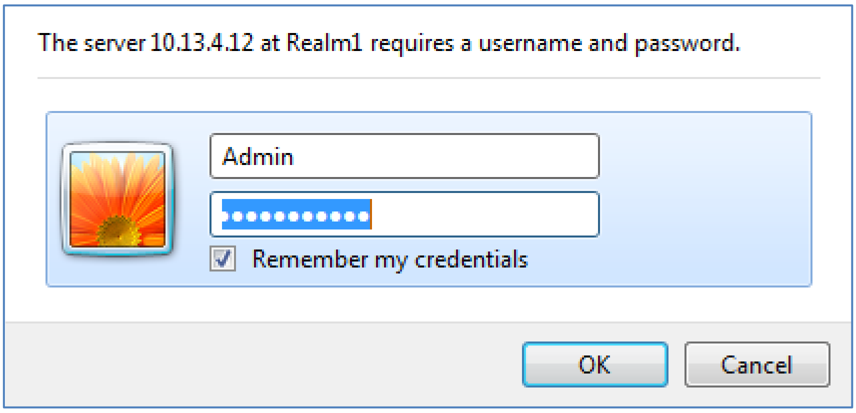

AudioCodes Mediant 800
USB/WWAN
RS-232
POWER
STATUS
WAN
GE
FXS
FXO
FE
Connect RJ-45 Network Cable to LAN Port 1
Straight-Through Ethernet Cable
PC

2. Ensure that your computer is configured to automatically obtain an IP address. The Mediant 800 embedded DHCP server (enabled by default) allocates an IP address to the computer when connected to it.
3. Open a standard Web browser, and then in the URL address field, enter the Mediant 800 default PSTN gateway LAN IP address (i.e., 192.168.0.2):

http://192.168.0.2

4. The following login screen appears, prompting you to log in with your login credentials:

Figure 4-2: Login Screen



The server 10.13.4.12 at Realm1 requires a username and password.

Admin

●●●●●●●●●●●●

☑ Remember my credentials

5. Log in with the default, case-sensitive user name (“Admin”) and password (“Admin”), and then click **OK**; the Web interface appears, displaying the Home page.

4.2 Configuring Physical LAN Ports Pair

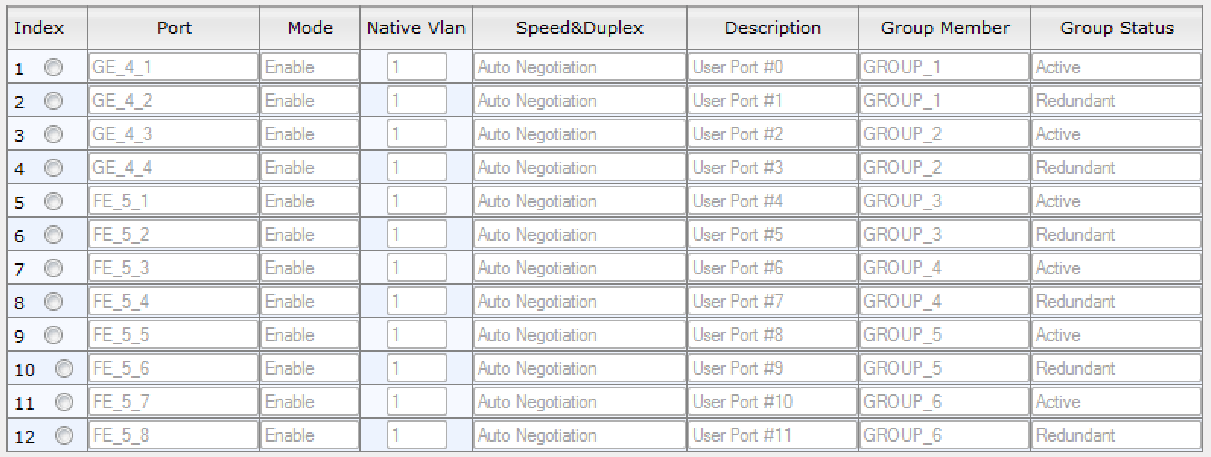
The device's physical LAN ports are grouped into pairs, where each group consists of an active port and a standby port. This provides LAN port redundancy within a group, whereby if an active port is disconnected and the other port is connected, the device switches over to the standby port, making it active and the previously active port becomes non-active. These port groups can be assigned to IP network interfaces in the Multiple Interface table, thereby allowing physical separation of network interfaces. Each port group can be assigned to up to 32 interfaces. By the means of physical separation of interfaces, the administrator can gain higher level of segregation of sub-networks. Equipment connected to different physical ports are not accessible to one other. The only connection between them can be established by cross connecting them with media stream (a VoIP call).

For each LAN port, you can configure the speed, duplex mode, native VLAN (PVID), and provide a brief description. Up to six port-pair redundancy groups are supported.

➢ **To configure the physical Ethernet ports:**

1. Open the Physical Ports Settings page (**Configuration** tab > **VoIP** menu > **Network** submenu > **Physical Ports Settings**).

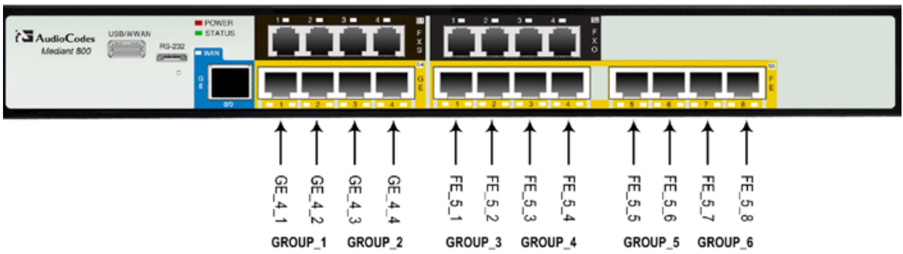
Figure 4-3: Physical Ports Settings Page



Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
1 ○	GE_4_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
2 ○	GE_4_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
3 ○	GE_4_3	Enable	1	Auto Negotiation	User Port #2	GROUP_2	Active
4 ○	GE_4_4	Enable	1	Auto Negotiation	User Port #3	GROUP_2	Redundant
5 ○	FE_5_1	Enable	1	Auto Negotiation	User Port #4	GROUP_3	Active
6 ○	FE_5_2	Enable	1	Auto Negotiation	User Port #5	GROUP_3	Redundant
7 ○	FE_5_3	Enable	1	Auto Negotiation	User Port #6	GROUP_4	Active
8 ○	FE_5_4	Enable	1	Auto Negotiation	User Port #7	GROUP_4	Redundant
9 ○	FE_5_5	Enable	1	Auto Negotiation	User Port #8	GROUP_5	Active
10 ○	FE_5_6	Enable	1	Auto Negotiation	User Port #9	GROUP_5	Redundant
11 ○	FE_5_7	Enable	1	Auto Negotiation	User Port #10	GROUP_6	Active
12 ○	FE_5_8	Enable	1	Auto Negotiation	User Port #11	GROUP_6	Redundant

2. Select the 'Index' radio button corresponding to the port that you want to configure.
3. Click the **Edit** button.
4. Configure the ports (see the table below for a description of the parameters).
5. Click **Apply** and then **Done**.

Physical Port Settings Parameters Description

Parameter	Description
Port	(Read-only field) Displays the port number. The string values displayed on the Web page represent the physical ports, as shown below:  AudioCodes Mediant 800 USB/WWAN RS-232 POWER STATUS WAN GE_4_1 GE_4_2 GE_4_3 GE_4_4 FE_5_1 FE_5_2 FE_5_3 FE_5_4 FE_5_5 FE_5_6 FE_5_7 FE_5_8 GROUP_1 GROUP_2 GROUP_3 GROUP_4 GROUP_5 GROUP_6

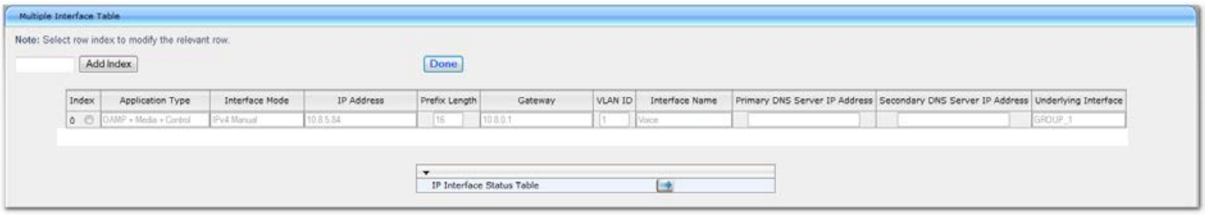
Parameter	Description
Mode	(Read-only field) Displays the mode of the port: ▪ [0] Disable ▪ [1] Enable (default)
Native Vlan	Defines the Native VLAN or PVID of the port. Incoming packets without a VLAN ID are tagged with this VLAN. For outgoing packets, if the VLAN ID as defined in the Multiple Interface table is the same as the Native VLAN ID, the device sends the packet without a VLAN; otherwise, the VLAN ID as defined in the Multiple Interface table takes precedence. The valid value range is 1 to 4096. The default is 1.
Speed & Duplex	Defines the speed and duplex mode of the port. ▪ [0] 10BaseT Half Duplex ▪ [1] 10BaseT Full Duplex ▪ [2] 100BaseT Half Duplex ▪ [3] 100BaseT Full Duplex ▪ [4] Auto Negotiation (default) ▪ [6] 1000BaseT Half Duplex ▪ [7] 1000BaseT Full Duplex
Description	Defines an arbitrary description of the port.
Group Member	(Read-only field) Displays the group to which the port belongs.
Group Status	(Read-only field) Displays the status of the port: ▪ "Active" - the active port ▪ "Redundant" - the standby (redundant) port

4.3 Configuring an IP Address

This section describes how to change the device's default IP address to match the site's IP addressing scheme.

1. Open the ‘Multiple Interface Table' page (**Configuration** tab > **VoIP** menu > **Network** sub-menu > **IP Settings**), as shown below:

Figure 4-4: IP Settings Screen



Multiple Interface Table

Note: Select row index to modify the relevant row.

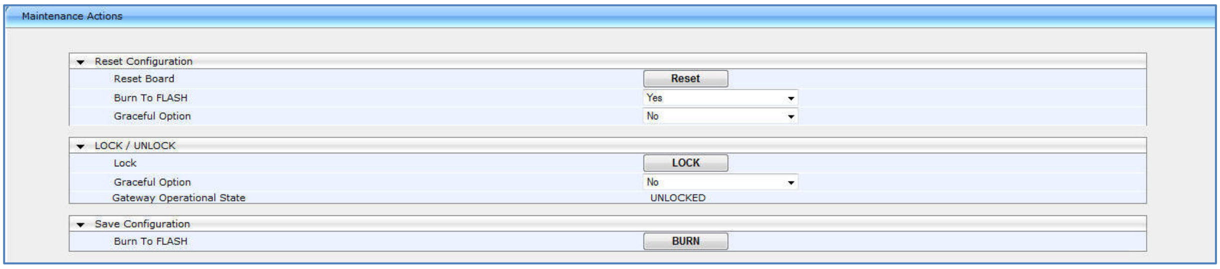
Add Index Done

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0 ○	OAMP + Media + Control	IPv4 Manual	10.8.5.84	16	10.8.0.1	1	Voice			GROUP_1

IP Interface Status Table

2. Select the 'Index' radio button corresponding to the Application Type "**OAMP + Media + Control"**(i.e., the VoIP and Management LAN interface), and then click **Edit.**
3. Configure the OAMP LAN network address so that it corresponds to your network IP addressing scheme.
4. From the 'Underlying Interface' drop-down list, select the physical LAN port group (which you configured in Section 4.2 on page 25) to which you wish to assign the OAMP interface.
5. Configure any additional required interfaces for Media and Control and assign them to the required LAN port group.
6. Click **Apply**, and then click **Done** to apply and validate your settings.
7. 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 800 resets and your settings are saved to the flash memory.

Figure 4-5: Maintenance Actions: Reset Gateway



Maintenance Actions

Reset Configuration

Reset Board	Reset
Burn To FLASH	Yes
Graceful Option	No

LOCK / UNLOCK

Lock	LOCK
Graceful Option	No
Gateway Operational State	UNLOCKED

Save Configuration

Burn To FLASH	BURN

8. Maintain the cabled connection between the Mediant 800 LAN port and the computer.

Reader's Notes

5 Pre-Configuring SBA at Datacenter

Prior to installing the SBA at the branch office (as described later in Section 7 on page 45), you must perform the following at the datacenter (typically, located at headquarters):

- Add the SBA Device to the Active Directory (AD).
- Create a user account on the AD belonging to the **RTCUniversalSBATechnicians** group. This user performs the SBA deployment (Domain Admin account can also perform SBA deployment, by default).
- Add (publish) the SBA Device to your topology.

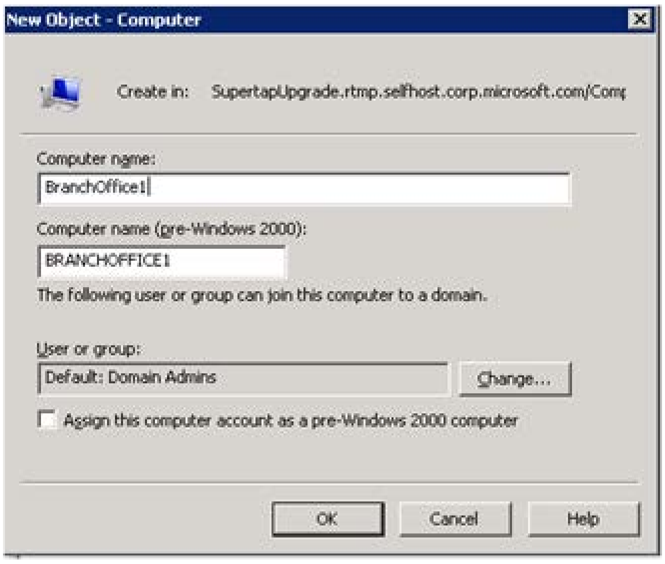
5.1 Adding the SBA Device to the Active Directory

The procedure below describes how to add the SBA device to the AD.

➢ **To add the SBA device to the Active Directory:**

1. Add the planned Survivable Branch Appliance device name to the Active Directory Domain Services:
   a. Start the Active Directory Users and Computers program (**Start** > **Administrative Tools** > **Active Directory Users and Computers**).
   b. Add the Survivable Branch Appliance device name to the domain computers (right-click **Computers**, choose **New**, and then click **Computer**).

Figure 5-1: New Object – Computer Dialog Box



New Object - Computer

Create in: SupertapUpgrade.rtmp.selfhost.corp.microsoft.com/Comp

Computer name: BranchOffice1

Computer name (pre-Windows 2000): BRANCHOFFICE1

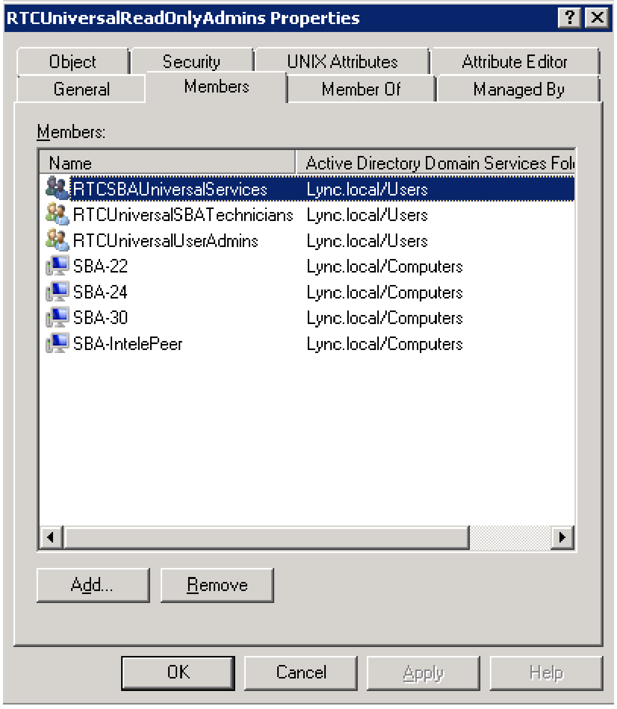
The following user or group can join this computer to a domain.

User or group: Default: Domain Admins

Change...
☐ Assign this computer account as a pre-Windows 2000 computer
OK
Cancel
Help

   c. Click **Change** to add a user or group that can insert this specific SBA server to the domain. (if you working with the Domain Administrator, do not change the “Domain Admin” group, if you working with another user, specify the name of a user or group that is allowed to join this computer to the domain.
   d. Add the Survivable Branch Appliance computer object to the **RTCUniversalReadOnlyAdmins** group (**Users > RTCUniversalReadOnlyAdmins** (right-click,and choose **Properties**, then choose the Numbers tab and **Add**).

Figure 5-2: RTC Universal Read Only Admins Properties



Members:

Name	Active Directory Domain Services Fol
RTCSBAUniversalServices	Lync.local/Users
RTCUniversalSBATechnicians	Lync.local/Users
RTCUniversalUserAdmins	Lync.local/Users
SBA-22	Lync.local/Computers
SBA-24	Lync.local/Computers
SBA-30	Lync.local/Computers
SBA-IntelePeer	Lync.local/Computers

e. Start the ADSI Edit program (**Start** > **Administrative Tools** > **ADSI Edit**).

f. Right-click the Survivable Branch Appliance computer name (that you created in step 'b' above), and then choose **Properties**.

g. In the Attributes list, set **servicePrincipalName** to "HOST/<SBA FQDN>", where *SBA FQDN* is the FQDN of your Survivable Branch Appliance (e.g., HOST/SBA.Lync.local).

2. Create a user account on Active Directory Services belonging to the **RTCUniversalSBATechnicians** group. This user performs the Survivable Branch Appliance deployment.

5.2 Defining the Branch Office Topology using Topology Builder

This section describes how to add the Survivable Branch Appliance to your topology, using Lync Server 2010 Topology Builder. This configuration includes the following main steps:

- Defining the branch office – see Section 5.2.1.
- Publishing the topology – see Section 5.2.2 on page 39.

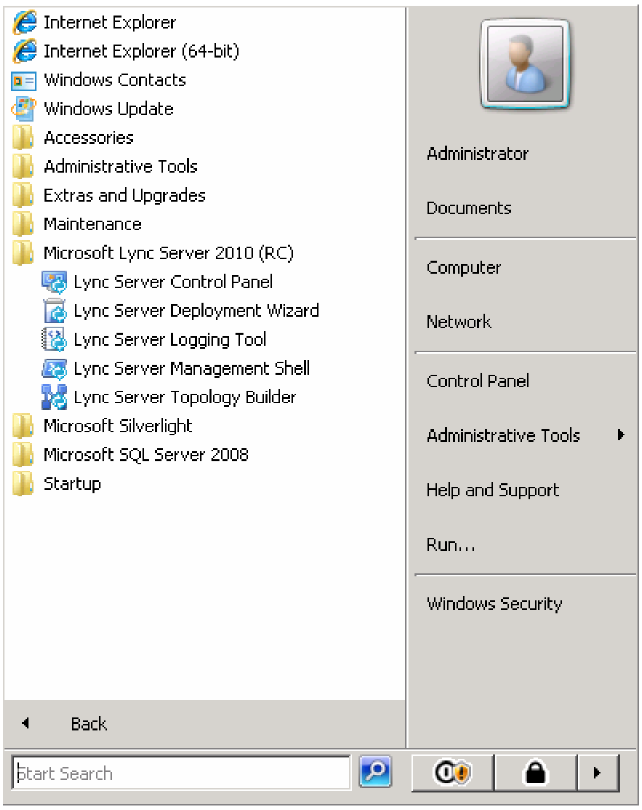
5.2.1 Defining the Branch Office

The procedure below describes how to create and define the branch office.

➢ **To create branch sites:**

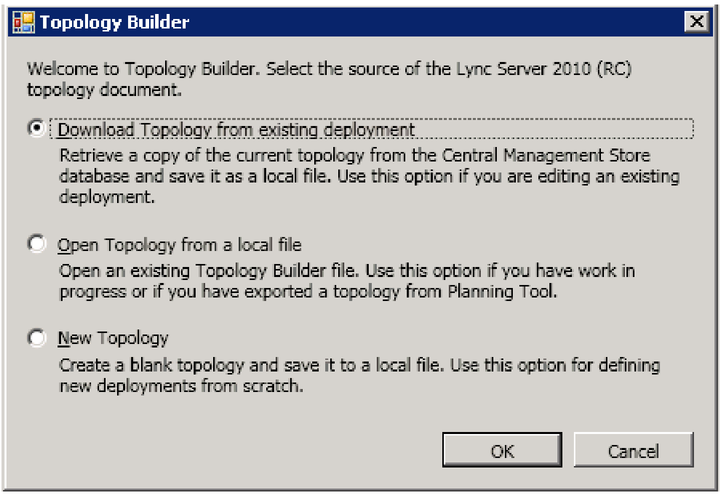
1. Start the Lync Server 2010 Topology Builder program (**Start** menu > **All Programs** > **Microsoft Lync Server 2010**, **Lync Server Topology Builder**), as shown below:

Figure 5-3: Menu Path to Topology Builder Program



Topology Builder opens, as shown below:

Figure 5-4: Topology Builder



Topology Builder

Welcome to Topology Builder. Select the source of the Lync Server 2010 (RC) topology document.

● Download Topology from existing deployment
Retrieve a copy of the current topology from the Central Management Store database and save it as a local file. Use this option if you are editing an existing deployment.

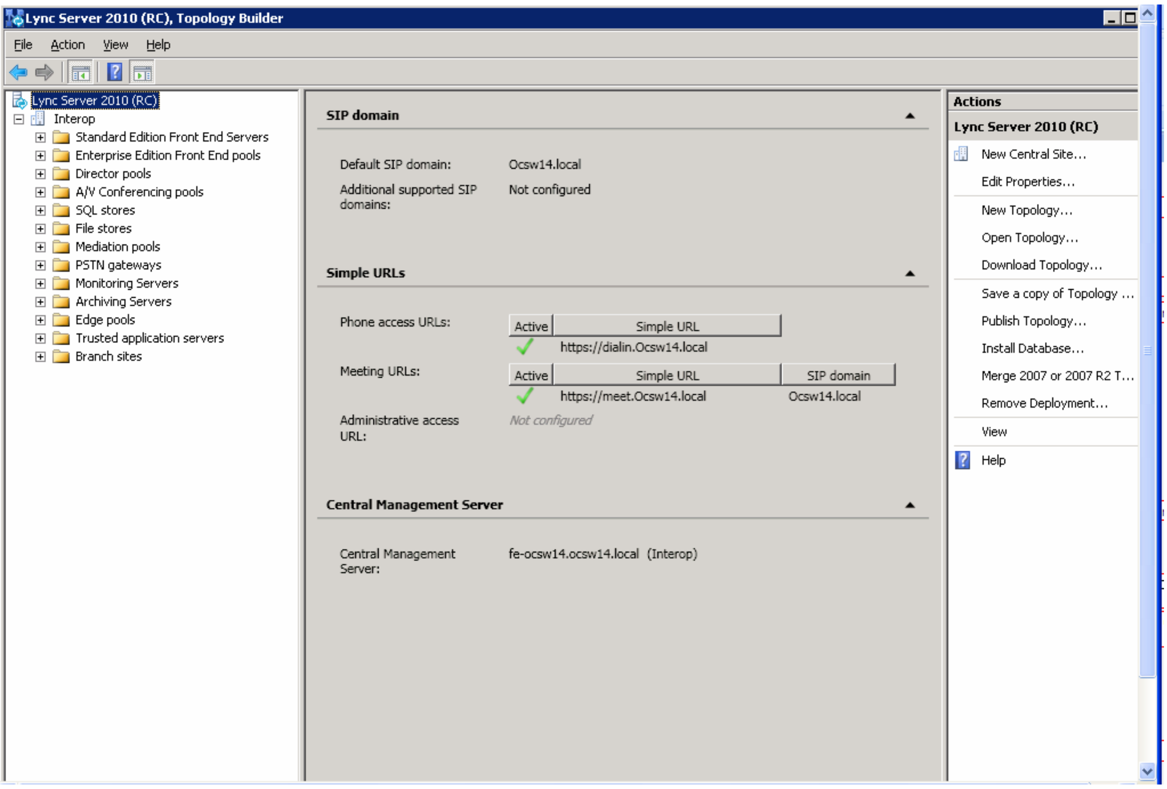
○ Open Topology from a local file
Open an existing Topology Builder file. Use this option if you have work in progress or if you have exported a topology from Planning Tool.

○ New Topology
Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.

2. Select the **Download Topology from existing deployment** option (assuming your Lync Server 2010 deployment already has a topology), and then click **OK**; a dialog box opens, prompting you to save the existing topology file.

3. Save the topology; the following screen appears:

Figure 5-5: Lync Server 2010 Topology Builder



Lync Server 2010 (RC), Topology Builder

- Lync Server 2010 (RC)
  - Interop
    - Standard Edition Front End Servers
    - Enterprise Edition Front End pools
    - Director pools
    - A/V Conferencing pools
    - SQL stores
    - File stores
    - Mediation pools
    - PSTN gateways
    - Monitoring Servers
    - Archiving Servers
    - Edge pools
    - Trusted application servers
    - Branch sites

SIP domain

Default SIP domain: Ocsw14.local

Additional supported SIP domains: Not configured

Simple URLs

Phone access URLs:

Active	Simple URL
✓	https://dialin.Ocsw14.local

Meeting URLs:

Active	Simple URL	SIP domain
✓	https://meet.Ocsw14.local	Ocsw14.local

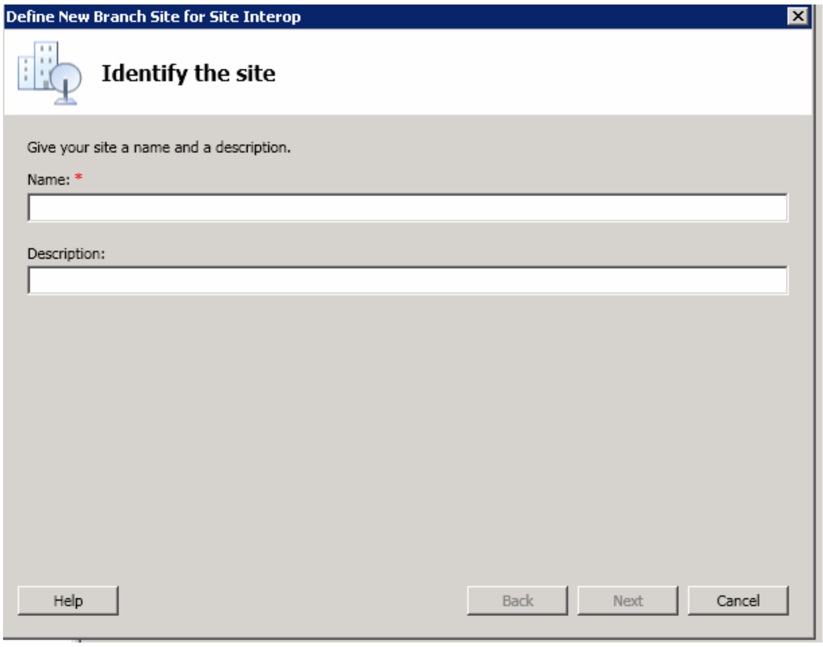
Administrative access URL: *Not configured*

Central Management Server

Central Management Server: fe-ocsw14.ocsw14.local (Interop)

4. From the Topology Builder console tree, do one of the following:
   - If you used the Planning tool to design your Enterprise Voice topology, expand the **Branch sites** node, and then expand the name of the branch site you specified in the tool. To modify each section of the branch office, right-click the branch site, and then from the shortcut menu, choose **Edit Properties**.
   - If you did not use the Planning tool, right-click the **Branch sites** node, and then from the shortcut menu, choose **New Branch Site**; the following dialog box appears:

Figure 5-6: Identify the Site



Define New Branch Site for Site Interop

Identify the site

Give your site a name and a description.

Name: *

Description:

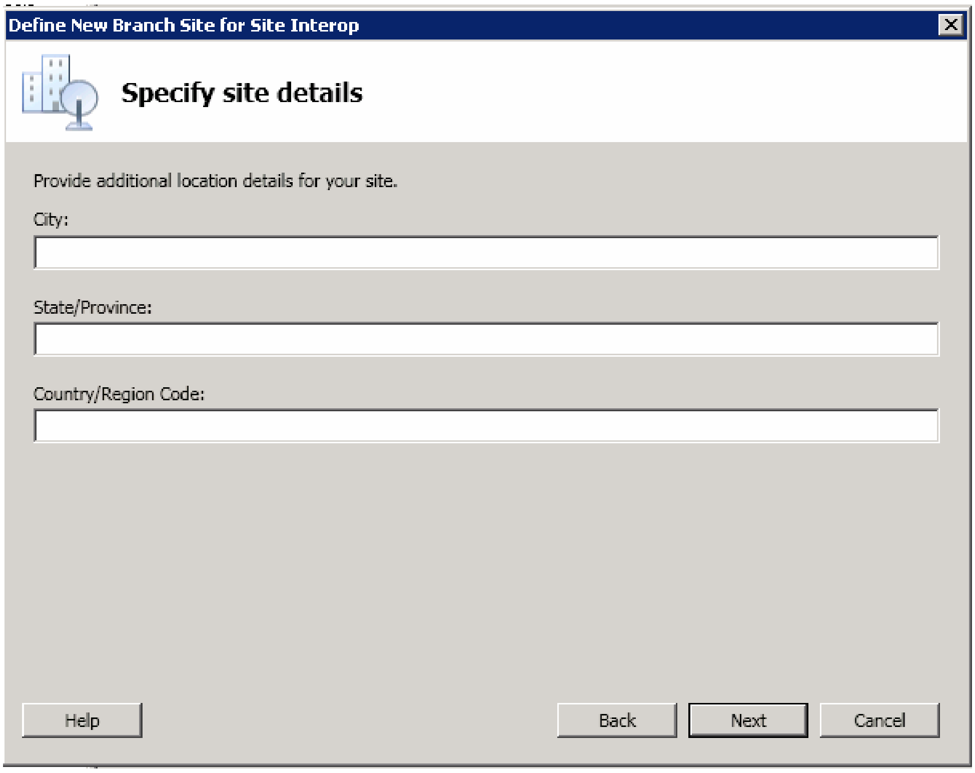
5. In the dialog box, do the following:

   a. In the ‘Name’ field, type the name of the branch site. Only this field is required, the other fields are optional.

   b. In the ‘Description’ field, type a meaningful description of the branch site.

   c. Click **Next**; the following dialog box appears:

Figure 5-7: Specify Site Details



Define New Branch Site for Site Interop

Specify site details

Provide additional location details for your site.

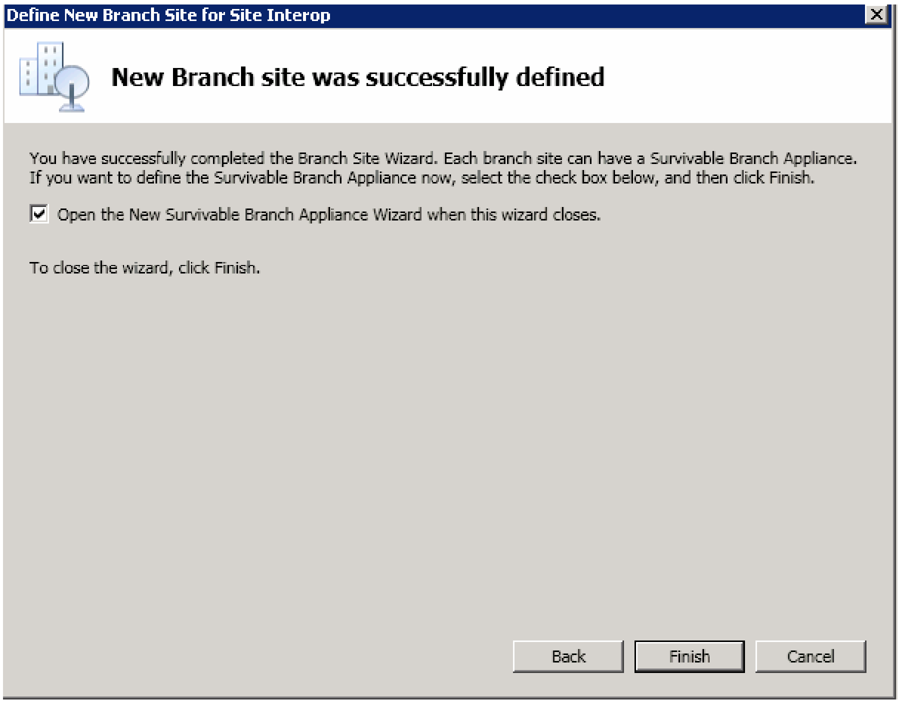
City:

State/Province:

Country/Region Code:

6. In the dialog box, do the following:
   a. In the 'City' field, type the name of the city in which the branch site is located.
   b. In the 'State/Province' field, type the name of the state or region in which the branch site is located.
   c. In the 'Country/Region Code' field, type the two-digit calling code for the country in which the branch site is located.
   d. Click **Next**; the following dialog box appears:

Figure 5-8: New Branch Site Successfully Defined



Define New Branch Site for Site Interop

New Branch site was successfully defined

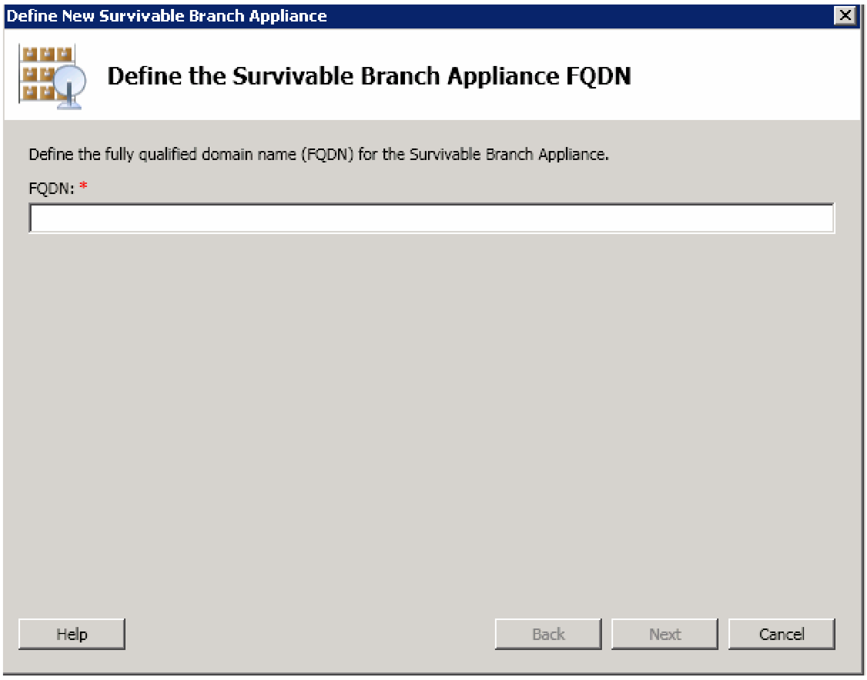
You have successfully completed the Branch Site Wizard. Each branch site can have a Survivable Branch Appliance. If you want to define the Survivable Branch Appliance now, select the check box below, and then click Finish.

☑ Open the New Survivable Branch Appliance Wizard when this wizard closes.

To close the wizard, click Finish.

7. Select the check-box, **Open the New Survivable Branch Appliance Wizard when this wizard closes**, and then click **Finish**; the following dialog box appears:

Figure 5-9: Define the Survivable Branch Appliance FQDN



Define New Survivable Branch Appliance

Define the Survivable Branch Appliance FQDN

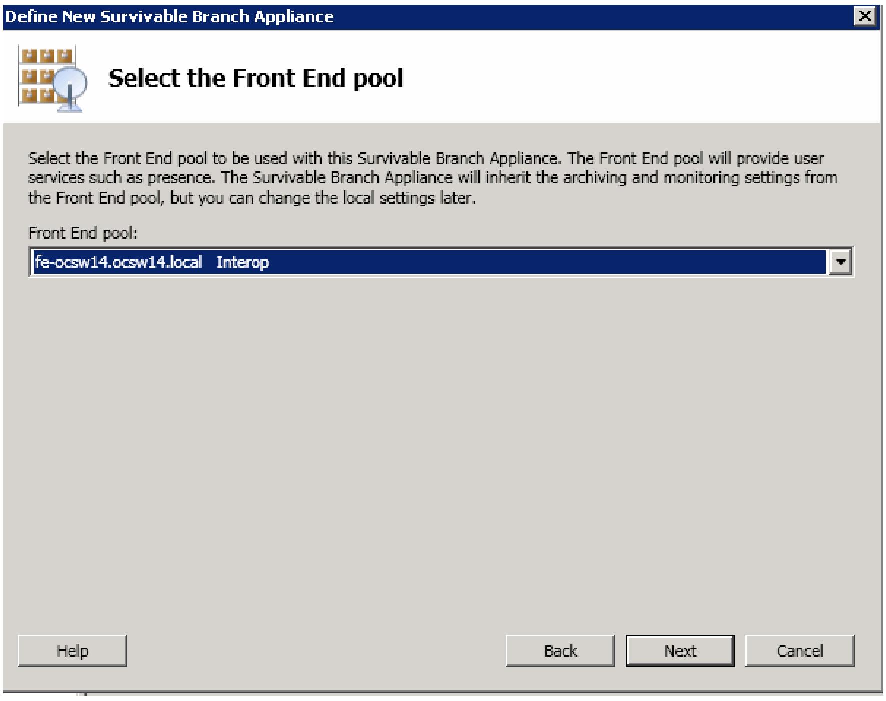
Define the fully qualified domain name (FQDN) for the Survivable Branch Appliance.

FQDN: *

8. In the ‘FQDN’ field**,** type the FQDN of the SBA, and then click **Next**; the following dialog box appears:

Note: The Survivable Branch Appliance FQDN that you configured in the ‘FQDN’ field must be the same as the FQDN that you configured using the ADSI Edit program in Section 5.1 on page 29.

Figure 5-10: Select the Front End Pool



Define New Survivable Branch Appliance

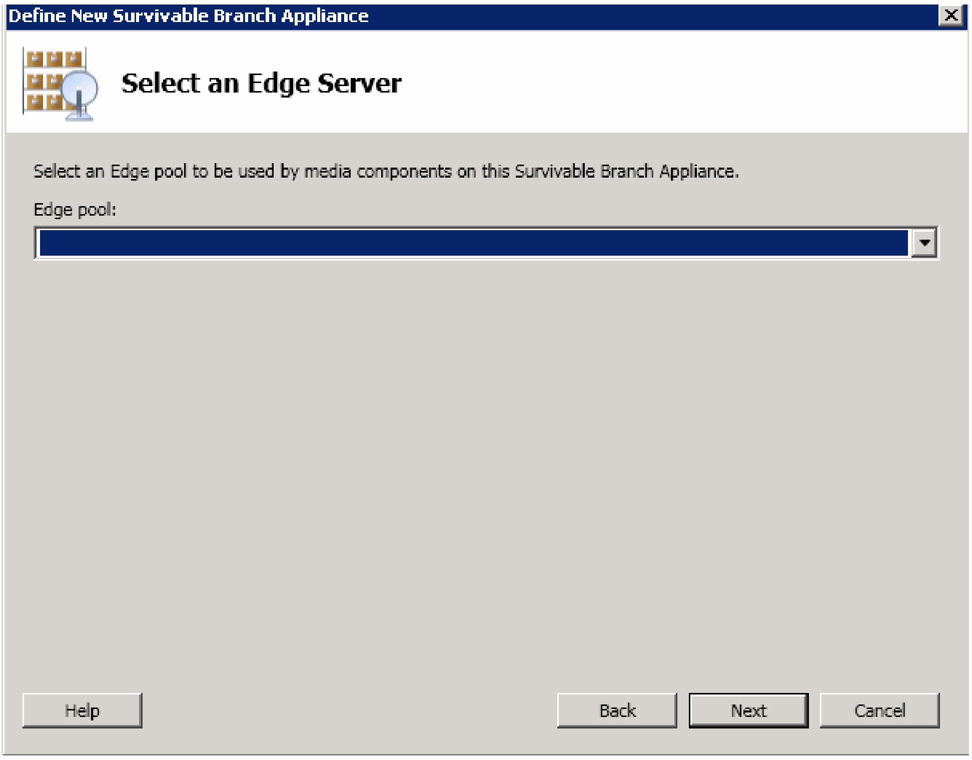
Select the Front End pool

Select the Front End pool to be used with this Survivable Branch Appliance. The Front End pool will provide user services such as presence. The Survivable Branch Appliance will inherit the archiving and monitoring settings from the Front End pool, but you can change the local settings later.

Front End pool: fe-ocsw14.ocsw14.local Interop

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

Figure 5-11: Select an Edge Server



Define New Survivable Branch Appliance

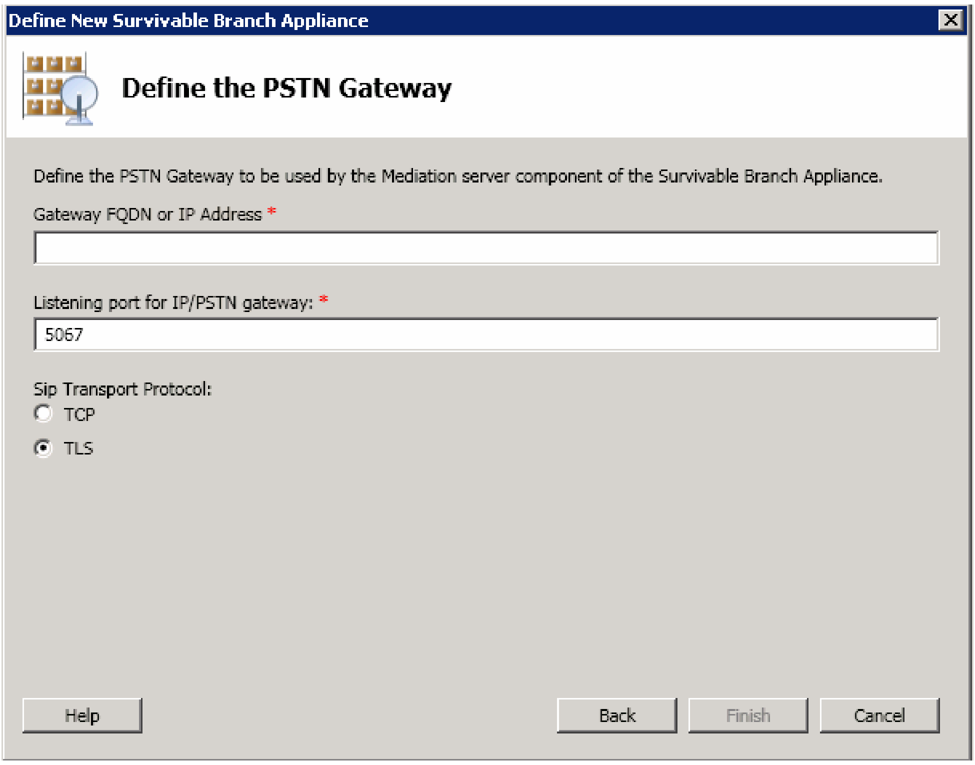
Select an Edge Server

Select an Edge pool to be used by media components on this Survivable Branch Appliance.

Edge pool:

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

Figure 5-12: Define the PSTN Gateway



Define New Survivable Branch Appliance

Define the PSTN Gateway

Define the PSTN Gateway to be used by the Mediation server component of the Survivable Branch Appliance.

Gateway FQDN or IP Address *

Listening port for IP/PSTN gateway: *

5067

Sip Transport Protocol:

○ TCP

● TLS

11. Do the following:

    a. In the ‘Gateway FQDN or IP Address’ field, type the PSTN gateway FQDN or IP address on which the Mediation Server component of the SBA is running. This is the IP address as configured for the PSTN gateway in Section 4 on page 23. If you are using FQDN, ensure that your DNS server is configured to resolve the FQDN into this IP address.

    b. In the ‘Listening port for IP/PSTN gateway’ field, type the gateway listening port. This must be the same port as configured in the PSTN gateway, as described in Section 8.3 on page 90.

    c. Under the **Sip Transport Protocol** group, select the **SIP Transport Protocol** option. This must be the same transport type as configured in the PSTN gateway, as described in Section 8.3 on page 90.

Note: For call security, it is highly recommended that you deploy a Survivable Branch Appliance using TLS.

    d. Click **Finish**.

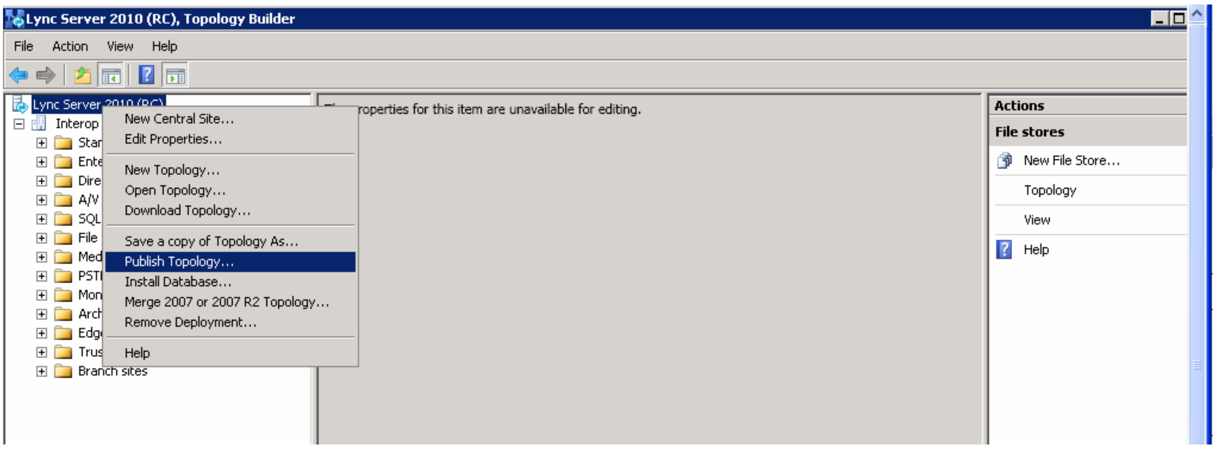
5.2.2 Publishing the Topology

Once you have defined the Branch Office (as described in the previous section), you need to publish this new topology, as described below.

➢ **To publish the topology:**

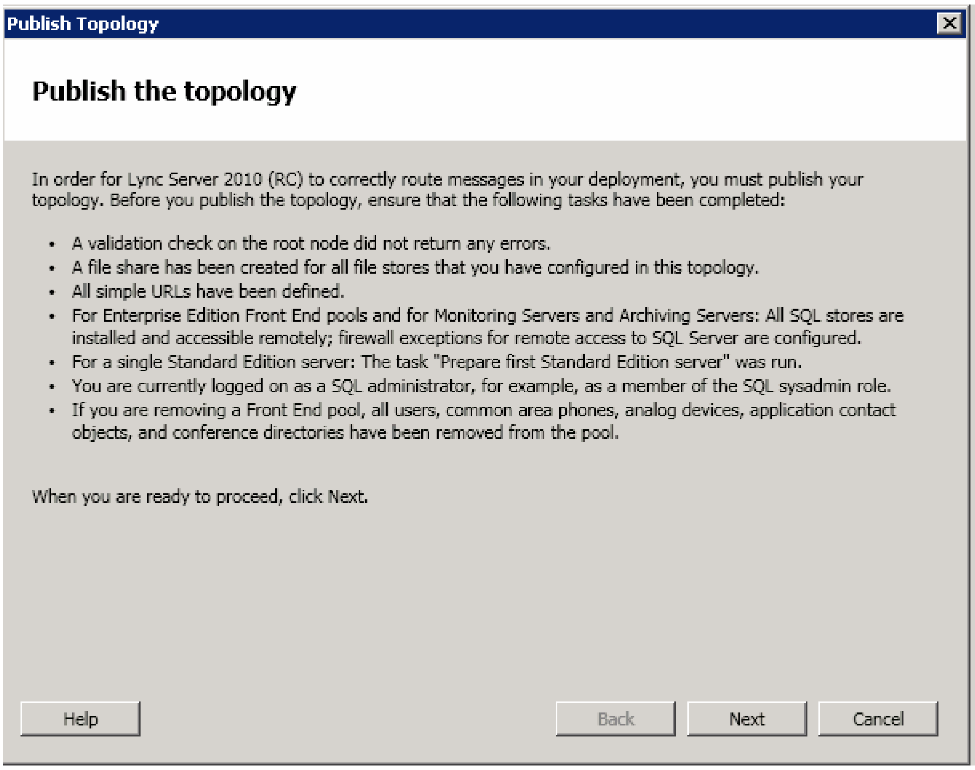
1. Right-click the root of the **Lync Server 2010** node, and then choose **Publish Topology**.

Figure 5-13: Publish Topology Selection



The following screen appears:

Figure 5-14: Publish the Topology



Publish Topology

Publish the topology

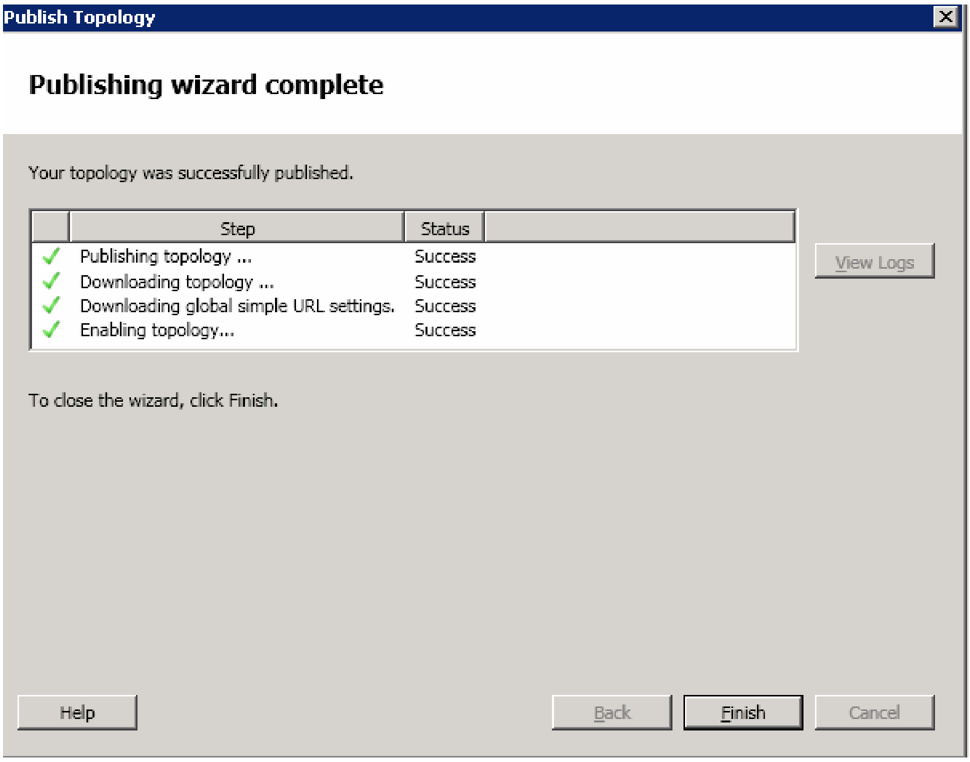
In order for Lync Server 2010 (RC) to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed:

- A validation check on the root node did not return any errors.
- A file share has been created for all file stores that you have configured in this topology.
- All simple URLs have been defined.
- For Enterprise Edition Front End pools and for Monitoring Servers and Archiving Servers: All SQL stores are installed and accessible remotely; firewall exceptions for remote access to SQL Server are configured.
- For a single Standard Edition server: The task "Prepare first Standard Edition server" was run.
- You are currently logged on as a SQL administrator, for example, as a member of the SQL sysadmin role.
- If you are removing a Front End pool, all users, common area phones, analog devices, application contact objects, and conference directories have been removed from the pool.

When you are ready to proceed, click Next.

2. Click **Next**; the following screen appears:

Figure 5-15: Publish Wizard Complete



Publish Topology

Publishing wizard complete

Your topology was successfully published.

	Step	Status
✓	Publishing topology ...	Success
✓	Downloading topology ...	Success
✓	Downloading global simple URL settings.	Success
✓	Enabling topology...	Success

To close the wizard, click Finish.

3. Verify that all steps display the 'Success' status, and then click **Finish**.

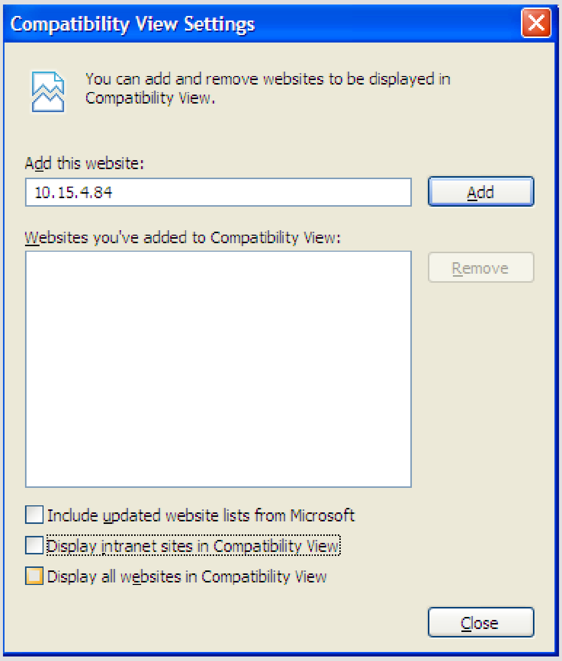
6 Connecting to the SBA Web-Based Tool

The SBA Web-based, graphical user interface (GUI) tool is used for installing and configuring the SBA application running on the Mediant 800 SBA OSN Server. You can connect and log in to the SBA Web-based tool using the default LAN IP address of the OSN Server, or by using a different IP address that suites your environment (The IP address of the OSN Server is in effect the IP address of the SBA.)

If you have recently changed the IP address of the OSN Server, then you need to use this new address to login to SBA; otherwise, you need to use the default IP address, **192.168.0.20**.

Note: The SBA Web-based tool is supported only by Internet Explorer 8 (Compatibility disabled), Firefox, and Google Chrome.

Internet Explorer 8 compatibility can be disabled by selecting **Tools** > **Compatibility View Settings**. The **Display all websites in Compatibility View** check box must be unchecked (cleared). The SBA server must not appear in the list of “Websites you’ve added to Compatibility View”.



You can add and remove websites to be displayed in Compatibility View.

Add this website: 10.15.4.84

Websites you've added to Compatibility View:

□ Include updated website lists from Microsoft

□ Display intranet sites in Compatibility View

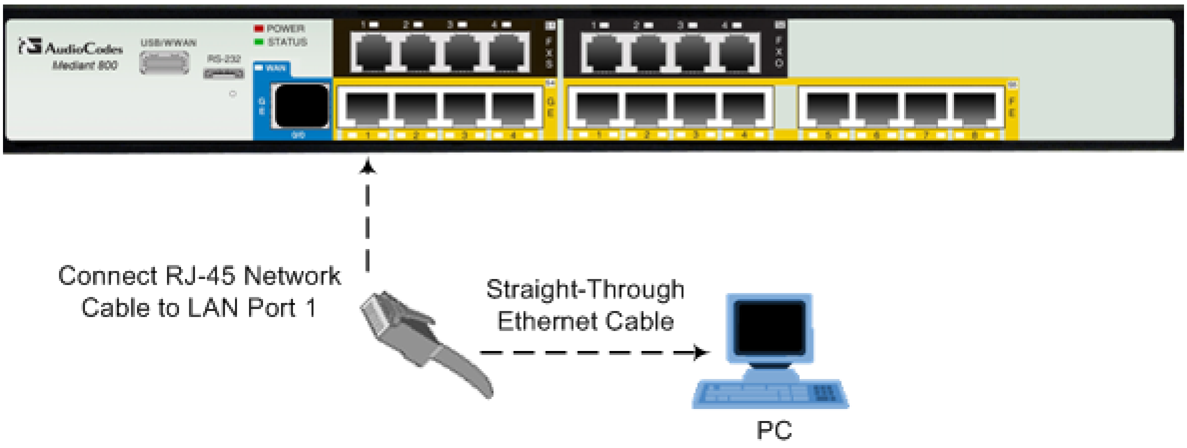
□ Display all websites in Compatibility View

Note: If the SBA was recovered or upgraded using the AudioCodes Upgrade and Recovery USB tool, the IP address of the OSN Server is received from the DHCP server and therefore, the default IP address (**192.168.0.20**) is no longer applicable.

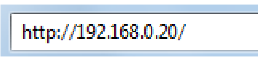
➢ To log in to the SBA wizard:

1. If not yet connected, connect LAN port **1** on the Mediant 800 front panel directly to a computer, using a straight-through Ethernet cable.

Figure 6-1: Connecting to the OSN Server


AudioCodes Mediant 800
USB/WWAN
POWER
STATUS
RS-232
WAN
Connect RJ-45 Network Cable to LAN Port 1
Straight-Through Ethernet Cable
PC

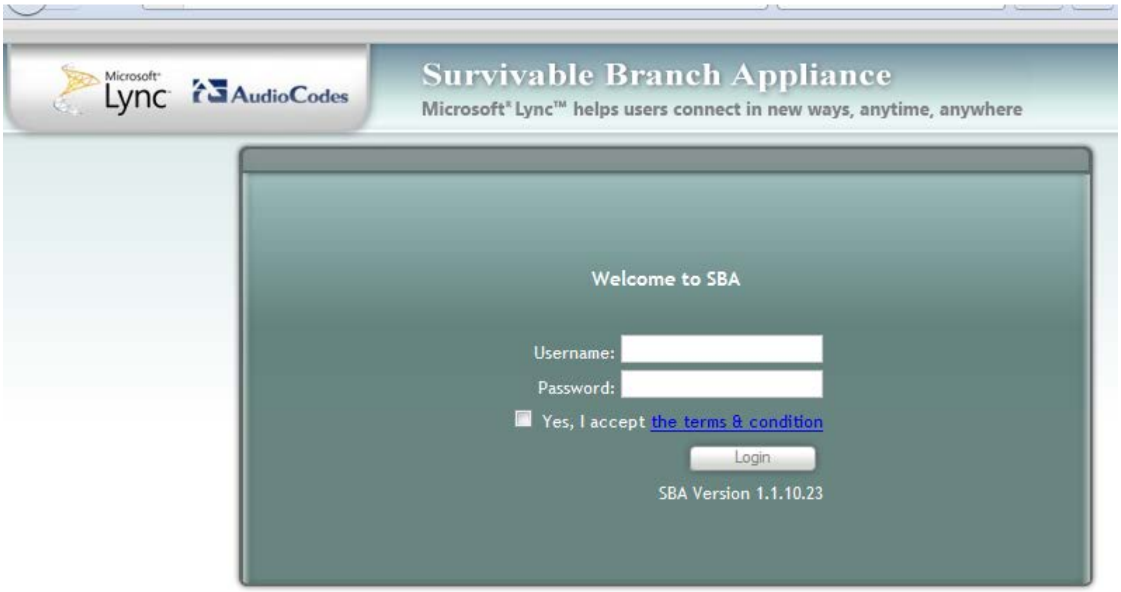
2. The default IP address of the OSN server hosting the SBA is **192.168.0.20**. If not done already, ensure that the IP address of your computer is in the same subnet as this default IP address.
3. Open a standard Web browser (Firefox, Google Chrome, or Internet Explorer 8 and later), and then in the URL address field, enter the default IP address of the OSN Server (http://192.168.0.20).



http://192.168.0.20/

The Welcome to SBA login screen appears:

Figure 6-2: SBA Login Screen



Survivable Branch Appliance

Microsoft® Lync™ helps users connect in new ways, anytime, anywhere

Welcome to SBA

Username:

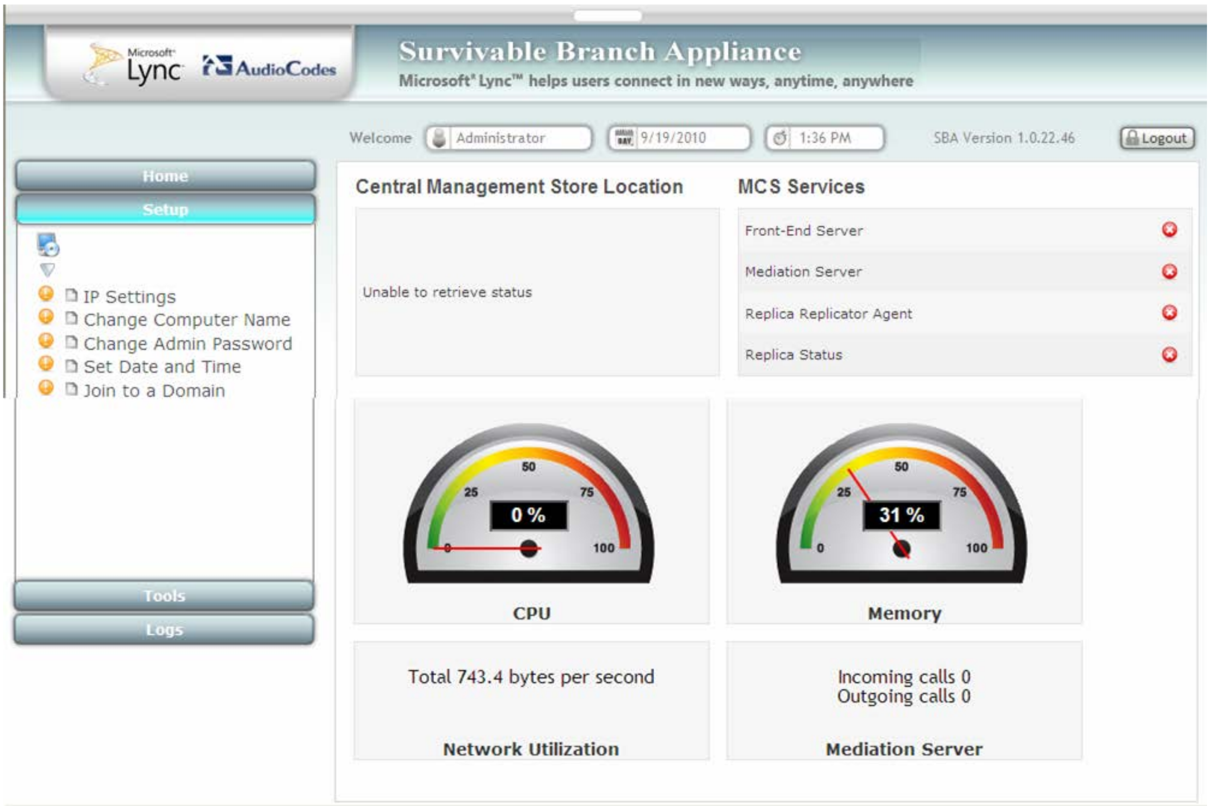
Password:

☐ Yes, I accept the terms & condition

SBA Version 1.1.10.23

4. Log in with the default username ("Administrator") and password ("Pass123"), accept the terms and conditions, and then click **Login**; the Home screen appears.

Figure 6-3: SBA Home Screen



Survivable Branch Appliance

Microsoft® Lync™ helps users connect in new ways, anytime, anywhere

Welcome Administrator 9/19/2010 1:36 PM SBA Version 1.0.22.46

Central Management Store Location

Unable to retrieve status

MCS Services

Front-End Server

Mediation Server

Replica Replicator Agent

Replica Status

0 %

CPU

31 %

Memory

Total 743.4 bytes per second

Network Utilization

Incoming calls 0
Outgoing calls 0

Mediation Server

Reader's Notes

7 Installing and Configuring the SBA

Once you are logged in to the SBA Web-based tool, you can start configuring SBA, as described in this section.

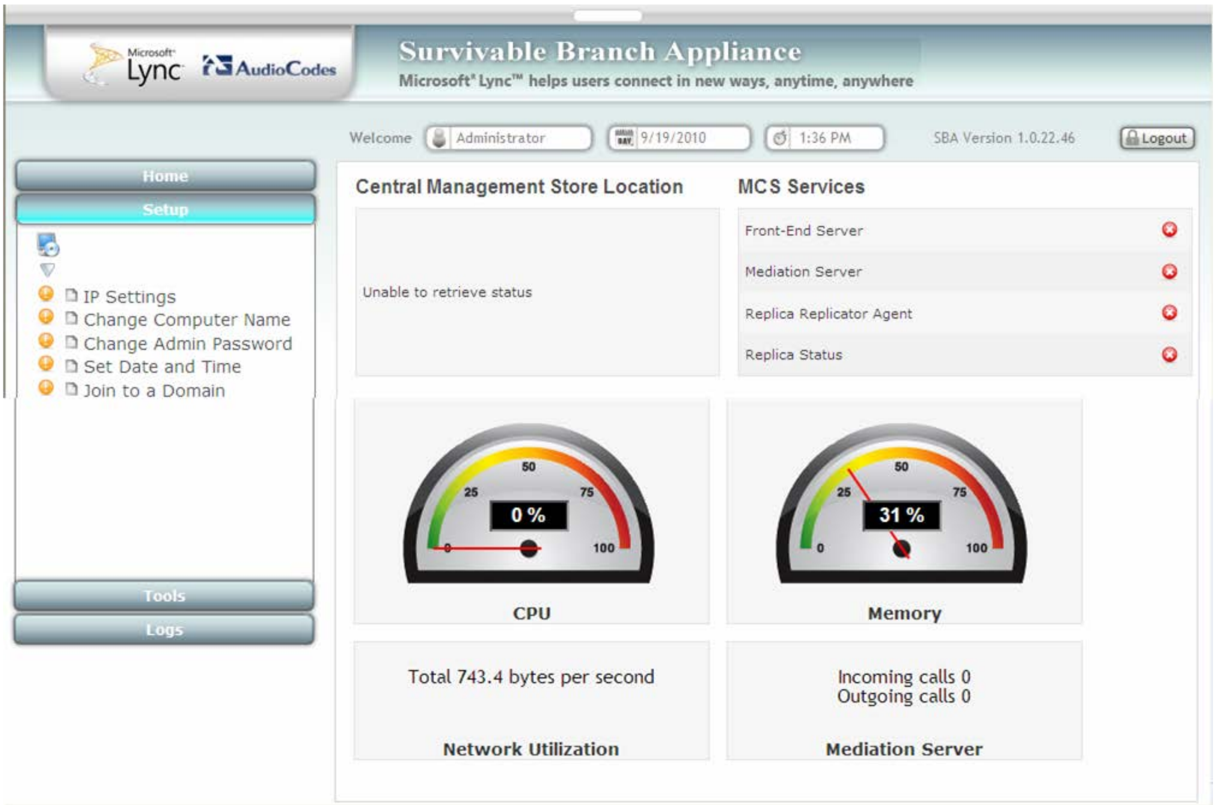
The SBA configuration is done in the **Setup** tab. For the configuration to be successful, it is imperative that all **Setup** options are performed correctly and **in sequence** (according to their order of appearance in the graphical user interface / GUI):

1. IP Settings. See Section 7.1 on page 47.
2. Change Computer Name. See Section 7.2 on page 50.
3. Change Admin Password. See Section 7.3 on page 54.
4. Set Date and Time. See Section 7.4 on page 56.
5. Join to a Domain. See Section 7.5 on page 59.
6. Device Preparation. See Section 7.6 on page 62.
7. Configuration. See Section 7.7 on page 687.7.
8. Enable Replication. See Section 7.8 on page 70.
9. Activate MCS. See Section 7.9 on page 72.
10. MCS Certificate. See Section 7.10 on page 74.
11. Start MCS Services. See Section 7.11 on page 80.
12. Gateway Configuration. See Section 7.12 on page 81.

If a task fails, ensure you correct it before continuing with additional tasks. When a task is configured successfully, a check mark (green) appears alongside the option.

Note: Initially, the **Setup** menu displays only the first few options (up till **Join to a Domain**). The remaining options appear only after you successfully define the **Joint to a Domain** option.

Figure 7-1: Setup Tab Displaying Tasks


Microsoft Lync
AudioCodes
Survivable Branch Appliance
Microsoft® Lync™ helps users connect in new ways, anytime, anywhere
Welcome
Logout
Home
Setup
Tools
Logs
0
25
50
75
100
0 %
CPU
31 %
Memory

Welcome Administrator 9/19/2010 1:36 PM SBA Version 1.0.22.46

- IP Settings
- Change Computer Name
- Change Admin Password
- Set Date and Time
- Join to a Domain

Central Management Store Location

Unable to retrieve status

MCS Services

- Front-End Server
- Mediation Server
- Replica Replicator Agent
- Replica Status

Total 743.4 bytes per second

Network Utilization

Incoming calls 0
Outgoing calls 0

Mediation Server

In each of the configuration menu screens, the current CPU and memory utilization of the OSN module is displayed. In the Setup pane, a list of all the configurable items is displayed.

Setup Pane Icon	Description
✓	Indicates a successfully configured item.
●	Indicates an item that has not yet been configured.
⊗	Indicates an item whose configuration has failed.

7.1 Step 1: IP Settings

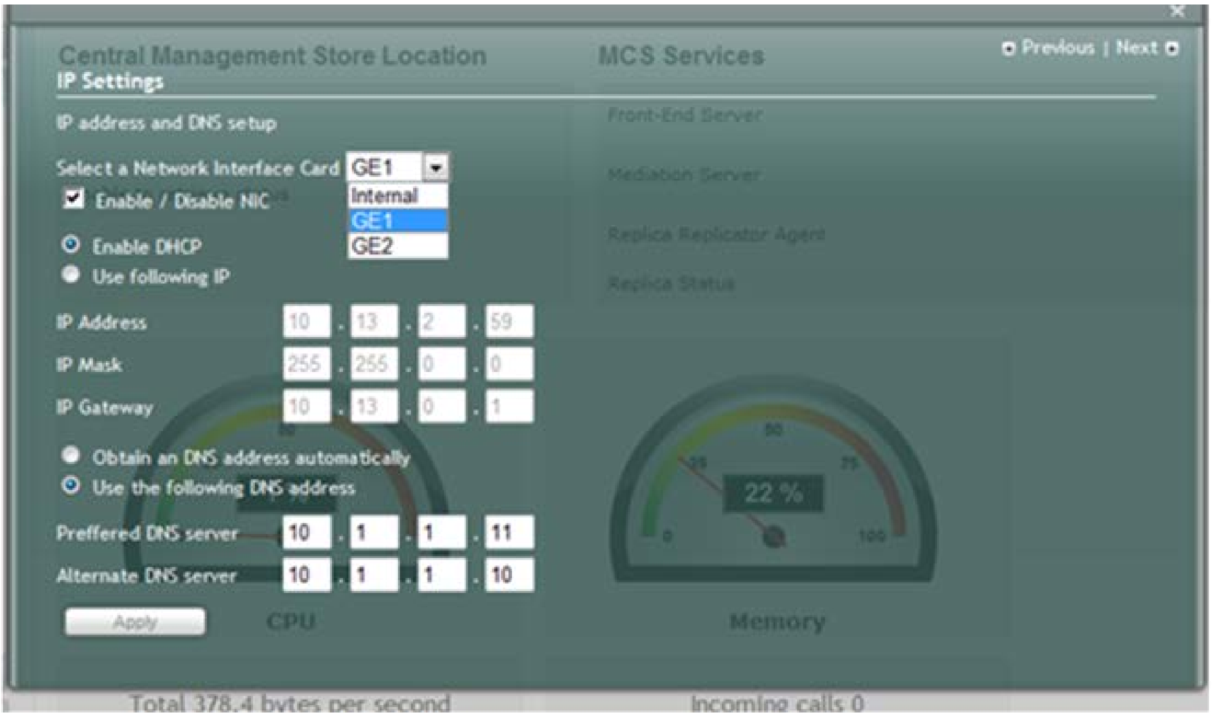
The **IP Settings** option defines the IP address and domain name server (DNS).In addition, this menu enables you to configure whether to use an internal or external NIC on the SBA device.

> **Note:** If you previously changed the IP Settings (see Section 7.1 on page 47), then you can skip this section. However, ensure that a check mark appears alongside the **IP Settings** option under the **Setup** menu. If not, you must perform the procedure described below.

➢ To set the IP address and DNS:

1. On the Setup menu, click **IP Settings**; the following screen appears:

Figure 7-2: Set IP Configuration Page



Central Management Store Location
MCS Services
○ Previous | Next ○

IP Settings

IP address and DNS setup

Select a Network Interface Card: GE1
Internal
GE1
GE2

☑ Enable / Disable NIC

● Enable DHCP
○ Use following IP

IP Address: 10 . 13 . 2 . 59
IP Mask: 255 . 255 . 0 . 0
IP Gateway: 10 . 13 . 0 . 1

○ Obtain an DNS address automatically
● Use the following DNS address

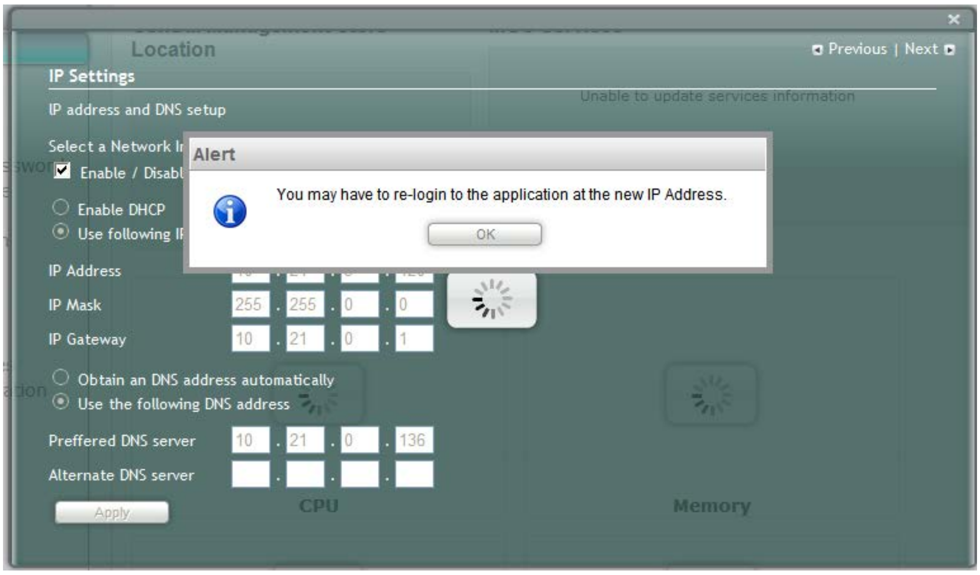
Preffered DNS server: 10 . 1 . 1 . 11
Alternate DNS server: 10 . 1 . 1 . 10

Apply

Total 378.4 bytes per second
Incoming calls 0

2. From the drop-down list, select one of the following NIC interface options:
   - Internal – Internal port that connects to the Mediant 800 switch.
   - GE1-Gigabit Ethernet Port 1
   - GE2-Gigabit Ethernet Port 2
3. Confirm/change the IP mask.
4. Confirm/change default IP gateway.
5. Click **Apply**. If the IP address has changed, you will be required to login again.

Figure 7-3: IP Settings – Login Again



Location

◘ Previous | Next ◘

IP Settings

IP address and DNS setup

Unable to update services information

Select a Network I

☑ Enable / Disabl

○ Enable DHCP

● Use following IP

Alert

You may have to re-login to the application at the new IP Address.

OK

IP Address

IP Mask 255 . 255 . 0 . 0

IP Gateway 10 . 21 . 0 . 1

○ Obtain an DNS address automatically

● Use the following DNS address

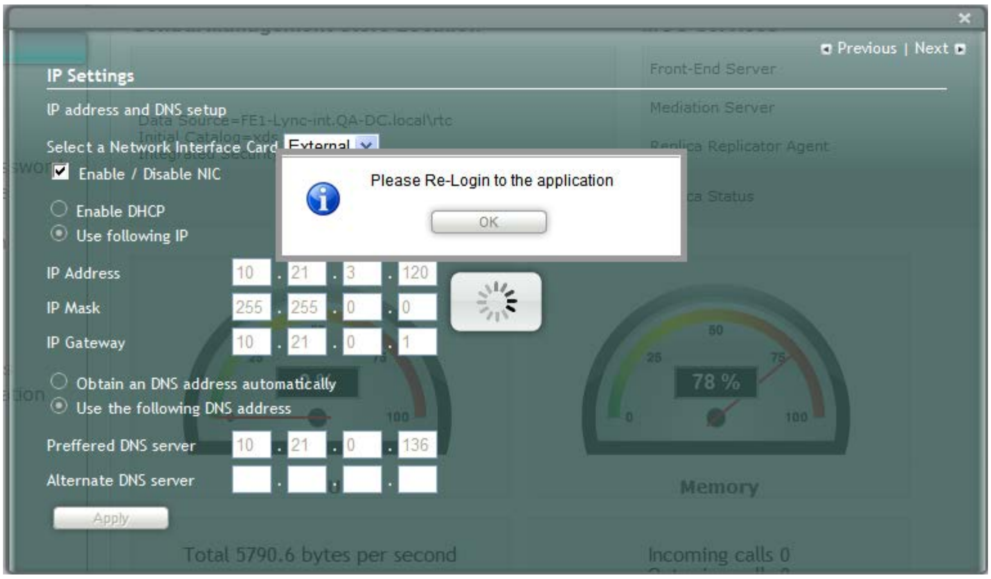
Preffered DNS server 10 . 21 . 0 . 136

Alternate DNS server . . .

Apply

6. Click **OK**; the following screen appears:

Figure 7-4: Alert - Login



◘ Previous | Next ◘

IP Settings

IP address and DNS setup

Select a Network Interface Card External

☑ Enable / Disable NIC

○ Enable DHCP

● Use following IP

Please Re-Login to the application

OK

IP Address 10 . 21 . 3 . 120

IP Mask 255 . 255 . 0 . 0

IP Gateway 10 . 21 . 0 . 1

○ Obtain an DNS address automatically

● Use the following DNS address

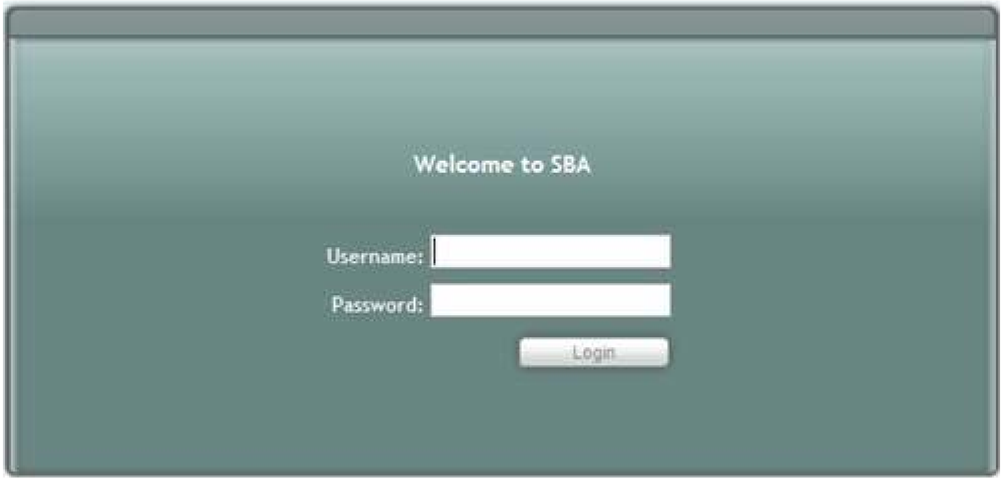
Preffered DNS server 10 . 21 . 0 . 136

Alternate DNS server . . .

Apply

7. Click **OK**.

Figure 7-5: Login Screen



Welcome to SBA

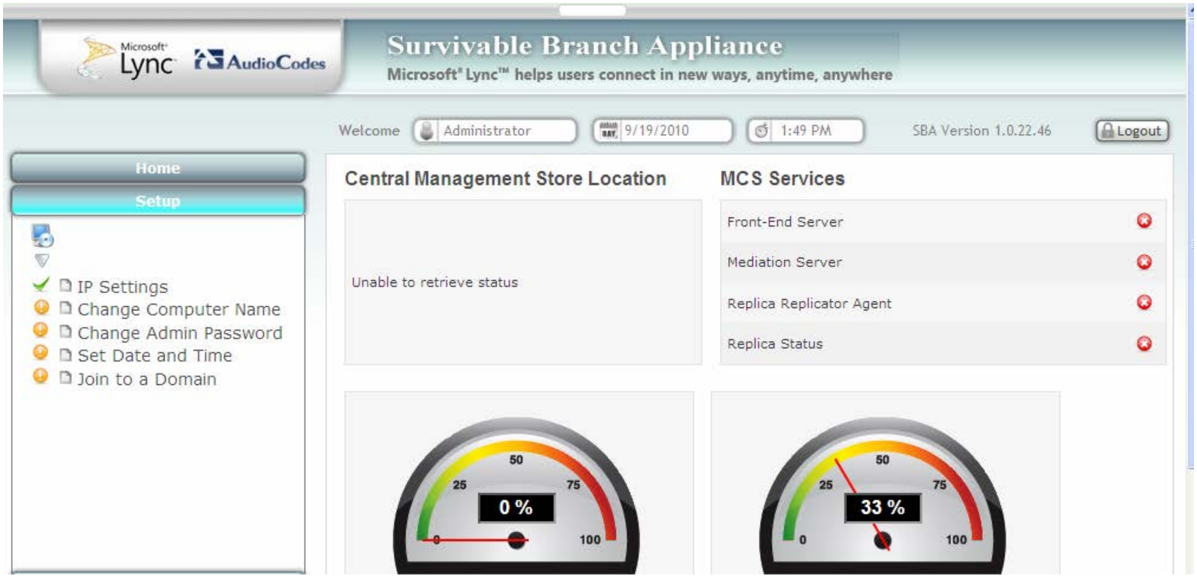
Username:

Password:

8. Enter the Username, Password and click **Login**.

Note: The system logs in with the new IP address.

Figure 7-6: IP Settings - Complete



Microsoft Lync
AudioCodes
Survivable Branch Appliance
Microsoft® Lync™ helps users connect in new ways, anytime, anywhere
Logout
Home
Setup
50
25
75
0
100
0 %
33 %

Welcome Administrator 9/19/2010 1:49 PM SBA Version 1.0.22.46

✓ IP Settings
Change Computer Name
Change Admin Password
Set Date and Time
Join to a Domain

Central Management Store Location

Unable to retrieve status

MCS Services

Front-End Server	☒
Mediation Server	☒
Replica Replicator Agent	☒
Replica Status	☒

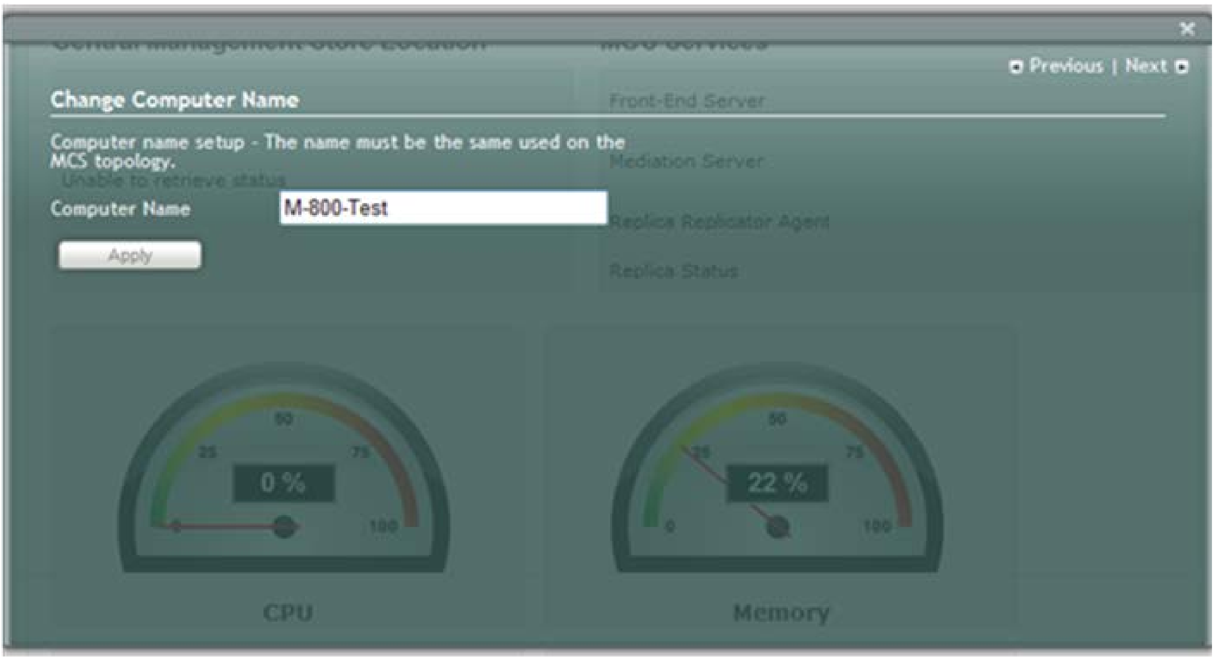
7.2 Step 2: Change Computer Name

The **Change Computer Name** option defines the computer name of the SBA.

➢ **To change the computer name:**

1. Under the **Setup** menu tab, click the **Change Computer Name** option; the following screen appears:

Figure 7-7: Change Computer Name Screen



Change Computer Name

Computer name setup - The name must be the same used on the MCS topology.

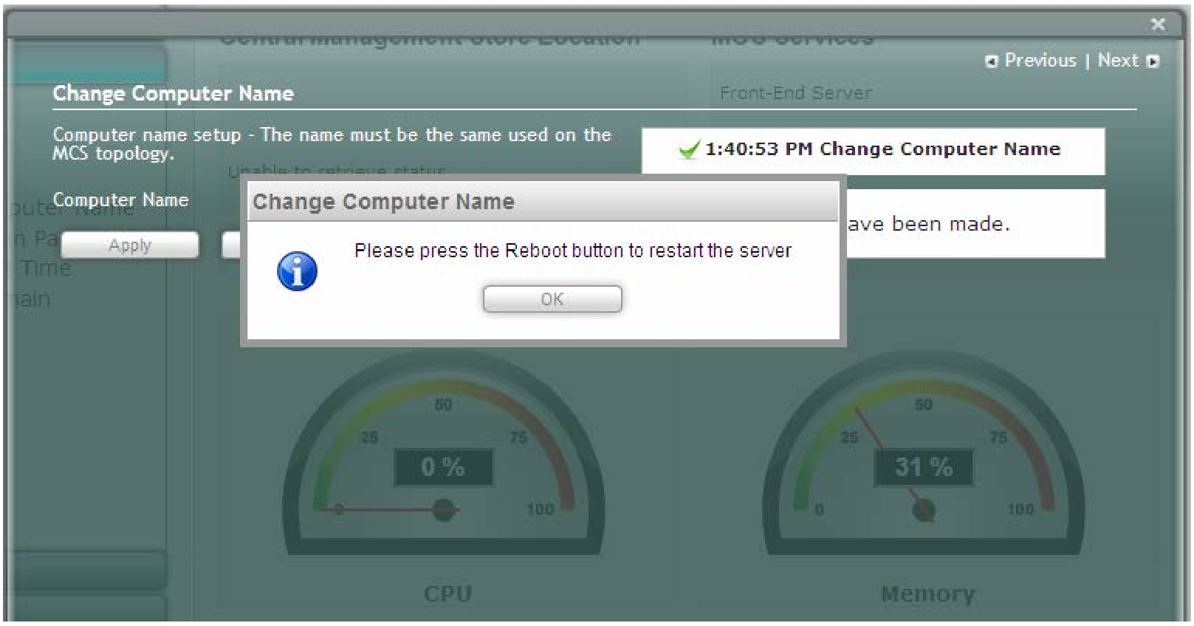
Computer Name: M-800-Test

2. In the **Computer Name** field, enter the computer name.

Note: The Computer Name must be the same as that used for the SBA in the Microsoft Active Directory (AD) and Topology during the pre-configuration steps done at the datacenter (see Section 5).

3. Click **Apply**; the “Operation Completed Successfully” message appears on the bottom of the screen. A message also appears to advise that a re-boot is necessary for the setting to take effect:

Figure 7-8: Change Computer Name - Reboot



Change Computer Name

Computer name setup - The name must be the same used on the MCS topology.

Computer Name

✓ 1:40:53 PM Change Computer Name

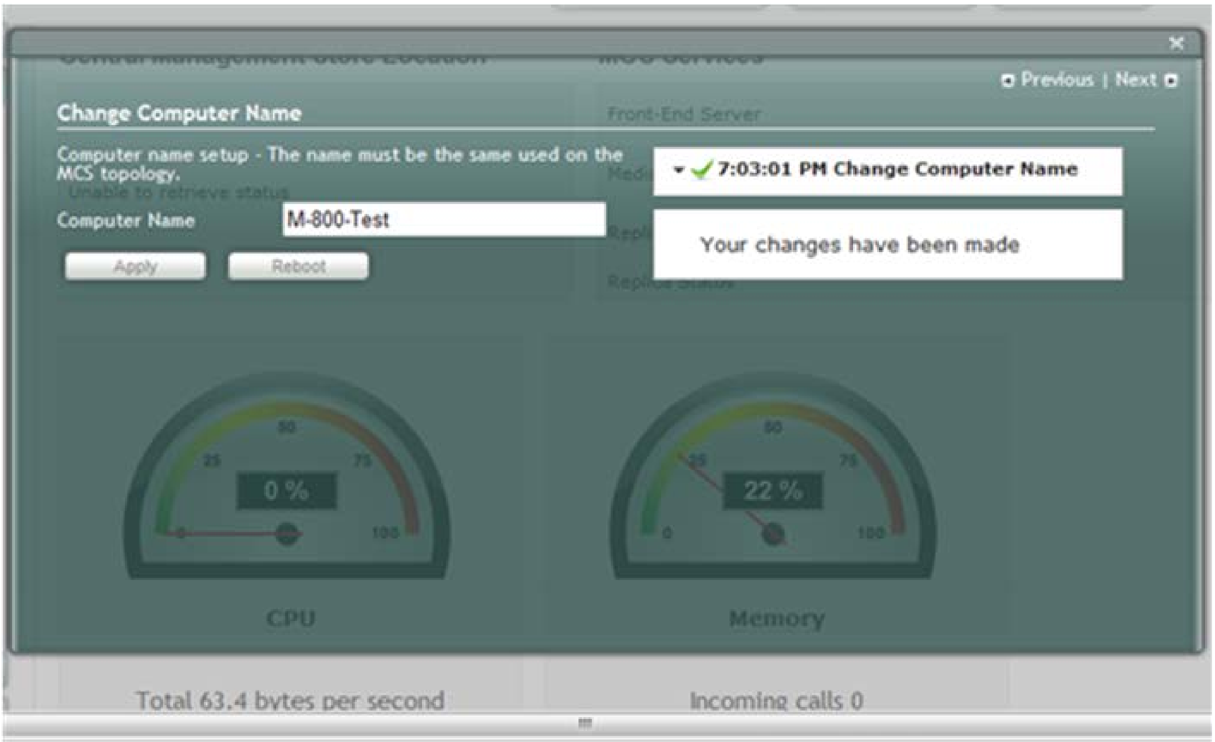
ave been made.

Change Computer Name

Please press the Reboot button to restart the server

4. Click **OK**; the following screen appears:

Figure 7-9: Change Computer Name – Applied Changes



Change Computer Name

Computer name setup - The name must be the same used on the MCS topology.

Computer Name: M-800-Test

✓ 7:03:01 PM Change Computer Name

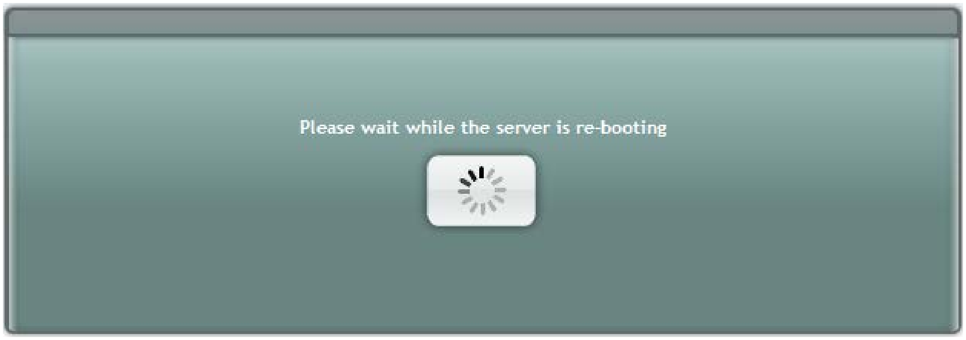
Your changes have been made

Total 63.4 bytes per second

Incoming calls 0

5. Click **Reboot**; the SBA reboots and the following screen appears:

Figure 7-10: Server Re-booting

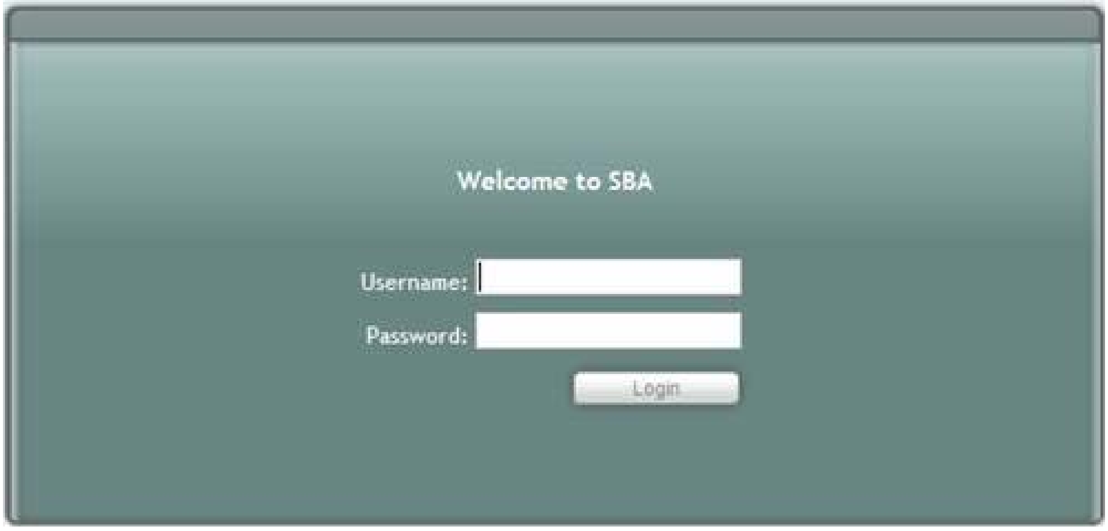


Please wait while the server is re-booting

Note: The re-boot process takes approximately five minutes.

When the SBA completes its reboot, the Welcome to SBA screen appears again.

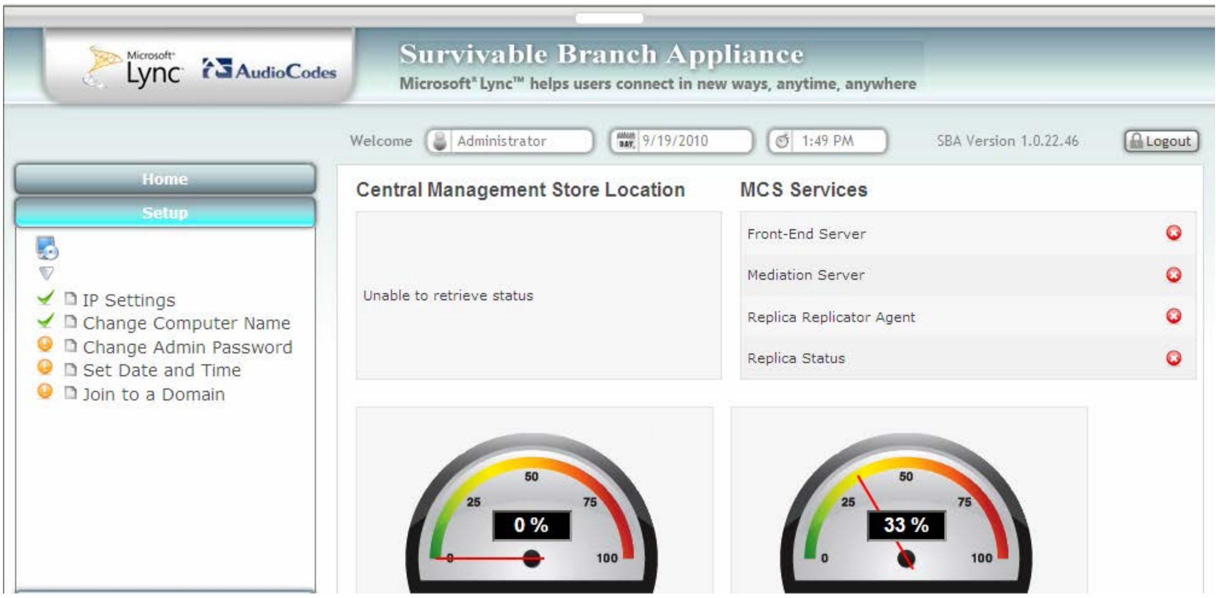
Figure 7-11: Login Screen



Welcome to SBA

6. Enter your username and password and then click **Login** to log in once again to the SBA Web-based tool; the **Setup** menu tab appears, displaying a green check mark alongside the **Change Computer Name** option, as shown below:

Figure 7-12: Change Computer Name – Completed Successfully



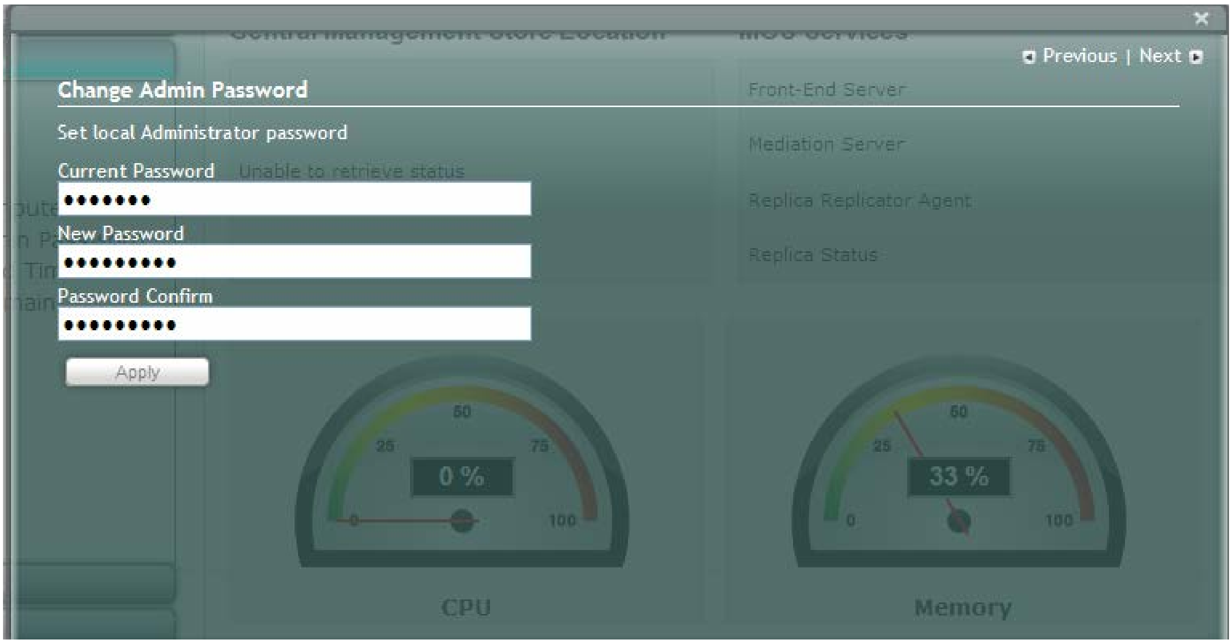
7.3 Step 3: Change Admin Password

The **Change Admin Password** option resets the local Administrator password.

➢ **To change the Administrator password:**

1. Under the **Setup** menu tab, click the **Change Admin Password** option; the following screen appears:

Figure 7-13: Change Admin Password Screen



Change Admin Password

Set local Administrator password

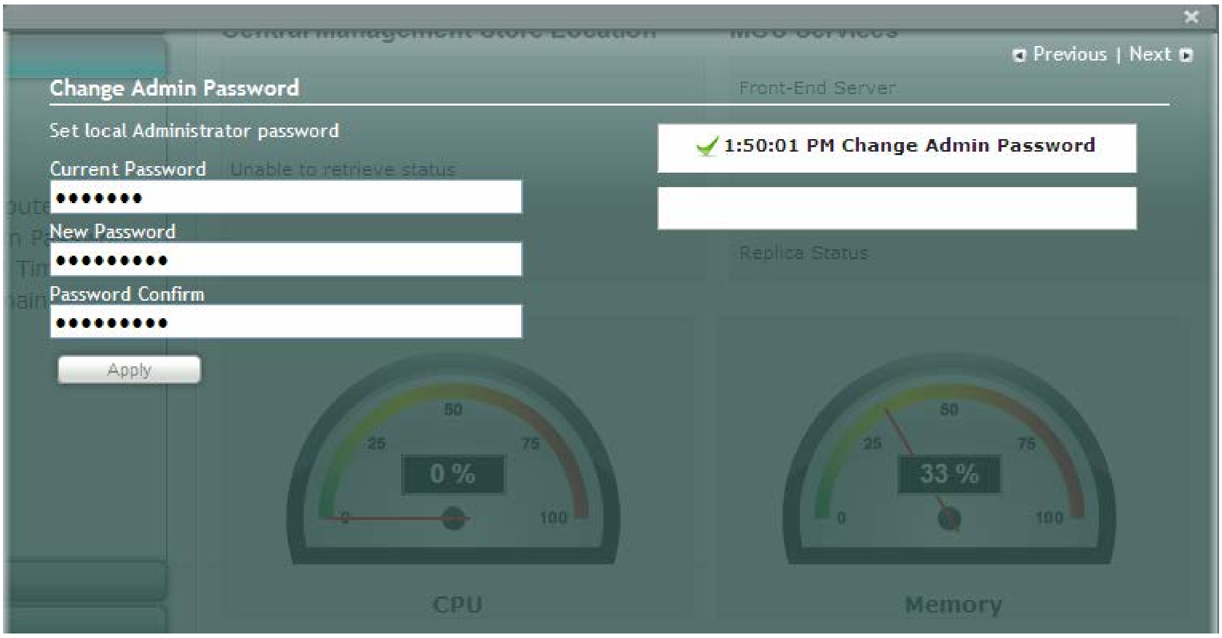
Current Password: ••••••• Unable to retrieve status

New Password: •••••••••

Password Confirm: •••••••••

2. In the 'Current Password' field, enter the current password.
3. In the 'New Password' field', enter a new password, and then in the 'Password Confirm' field, enter the new password again.
4. Click **Apply**; the following screen appears:

Figure 7-14: Change Admin Password – Applied Changes



Change Admin Password

Set local Administrator password

Current Password: ••••••• Unable to retrieve status

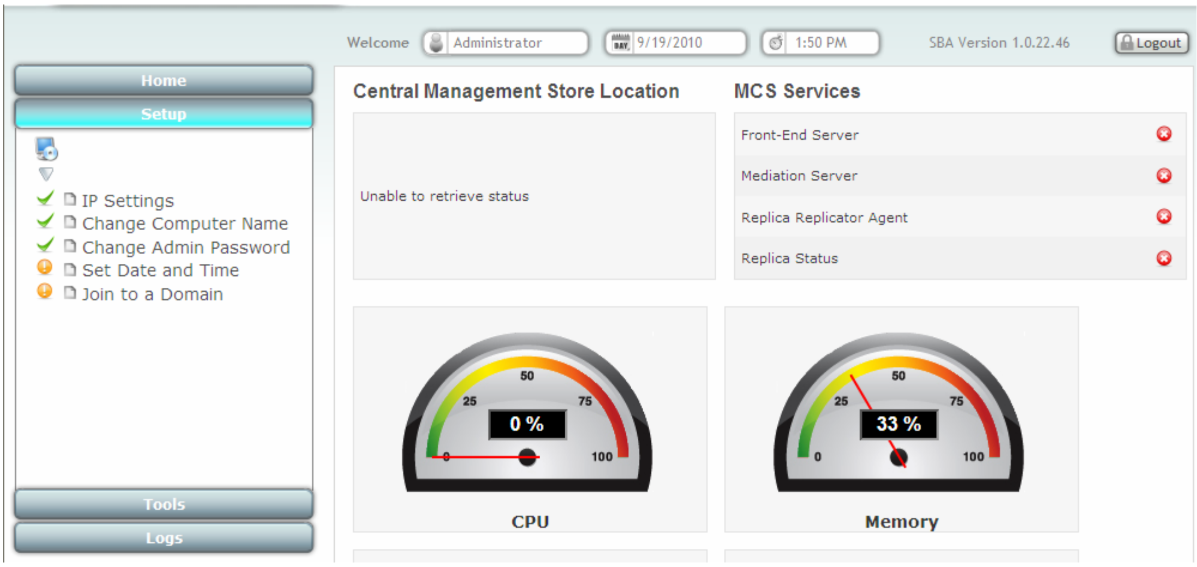
New Password: •••••••••

Password Confirm: •••••••••

✓ 1:50:01 PM Change Admin Password

5. Click **Next** to proceed to the next setup task; a green check mark appears alongside the **Change Admin Password** option under the **Setup** menu tab, as shown below:

Figure 7-15: Change Admin Password – Completed Successfully



Welcome Administrator 9/19/2010 1:50 PM SBA Version 1.0.22.46 Logout

Home

Setup

- ✓ IP Settings
- ✓ Change Computer Name
- ✓ Change Admin Password
- ● Set Date and Time
- ● Join to a Domain

Tools

Logs

Central Management Store Location

Unable to retrieve status

MCS Services	
Front-End Server	☒
Mediation Server	☒
Replica Replicator Agent	☒
Replica Status	☒

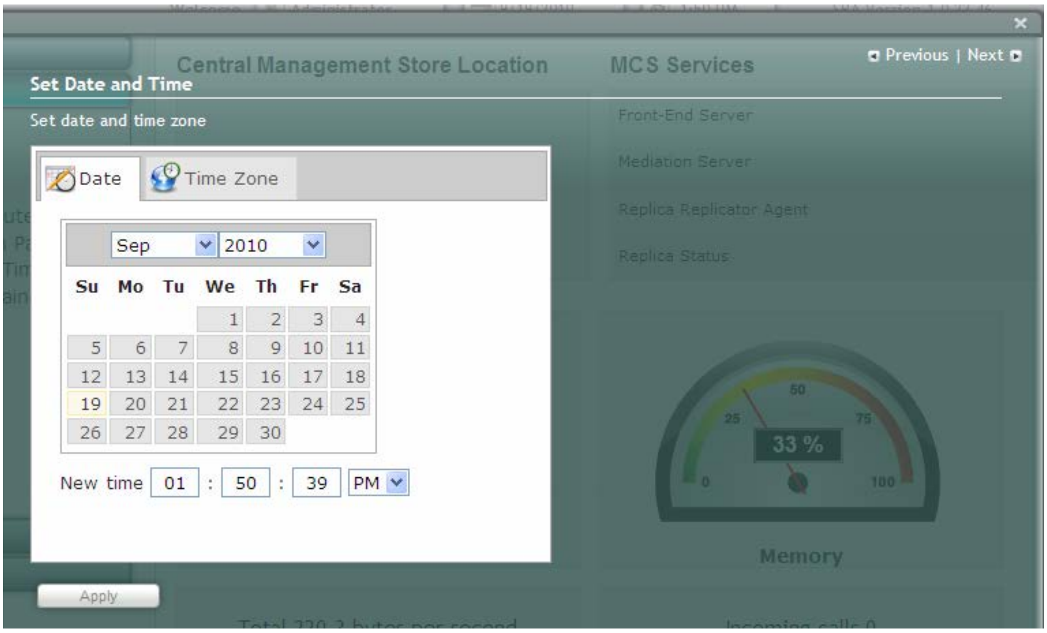
7.4 Step 4: Set Date and Time

The **Set Date and Time** option resets the date and time zone.

➢ To set the date and time:

1. Under the **Setup** menu tab, select the **Set Date and Time** option; the following screen appears:

Figure 7-16: Set Date and Time Screen



Set Date and Time

Set date and time zone

Date | Time Zone

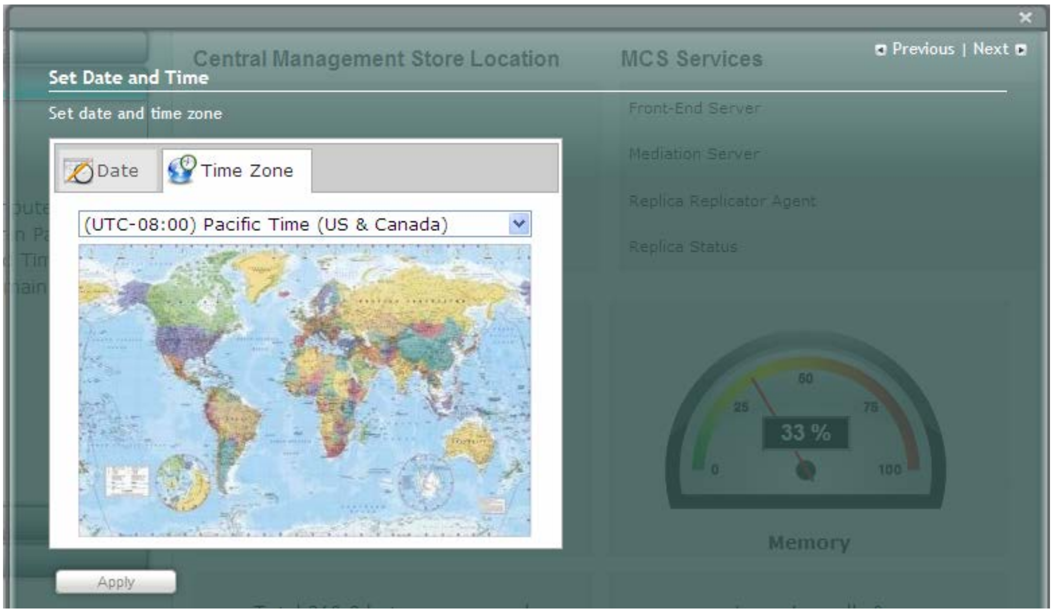
Sep 2010

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

New time 01 : 50 : 39 PM

2. Select the **Date** tab, and then define the date and time.
3. Click **Apply**; the "Operation Completed Successfully" message appears on the bottom of the screen.
4. Select the **Time Zone** tab; the following screen appears:

Figure 7-17: Set Date and Time - Time Zone



Set Date and Time

Set date and time zone

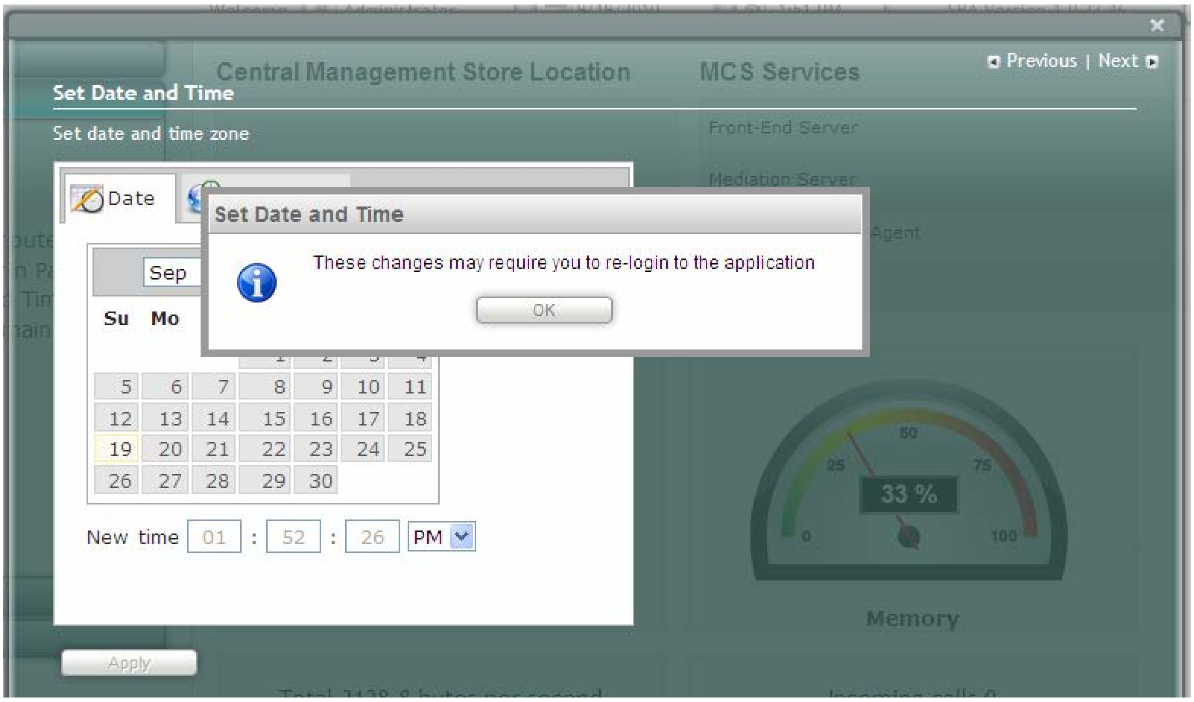
Date | Time Zone

(UTC-08:00) Pacific Time (US & Canada)

5. From the drop-down list, select the appropriate time zone.

6. Click **Apply;** a notification message box appears:

Figure 7-18: Set Date and Time – Notification Message



Set Date and Time

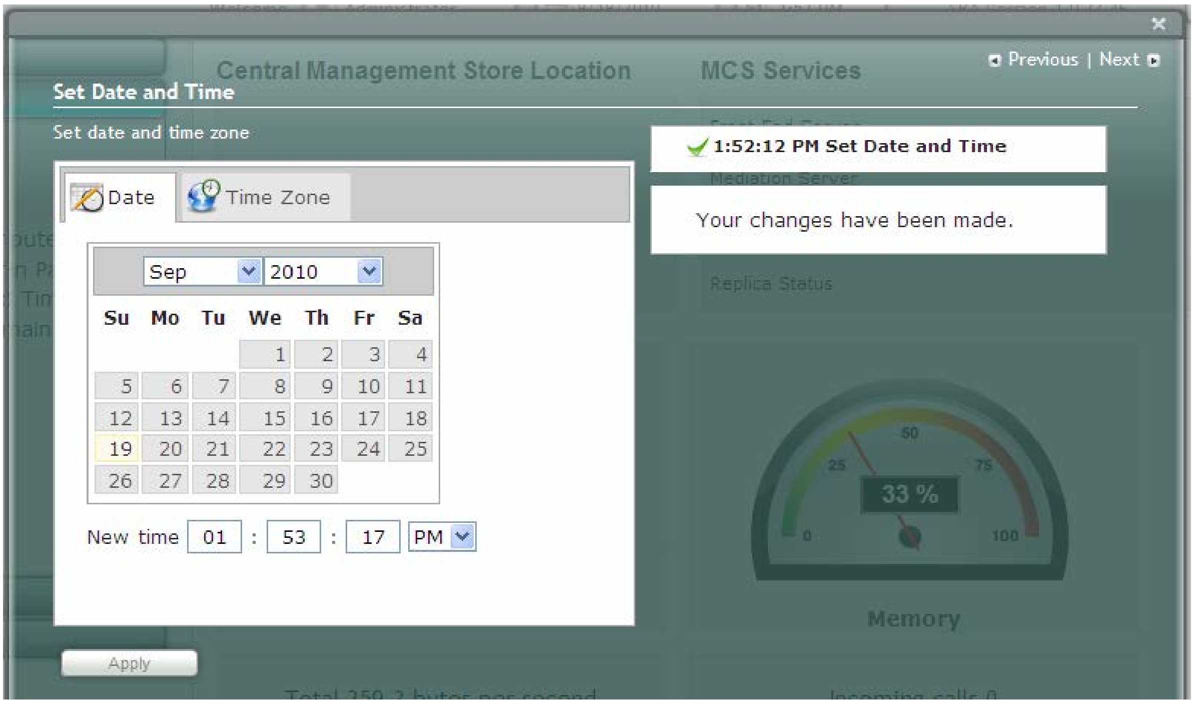
These changes may require you to re-login to the application

OK

New time 01 : 52 : 26 PM

7. Click **OK**; the following confirmation screen appears:

Figure 7-19: Set Date and Time – Applied Changes



1:52:12 PM Set Date and Time

Your changes have been made.

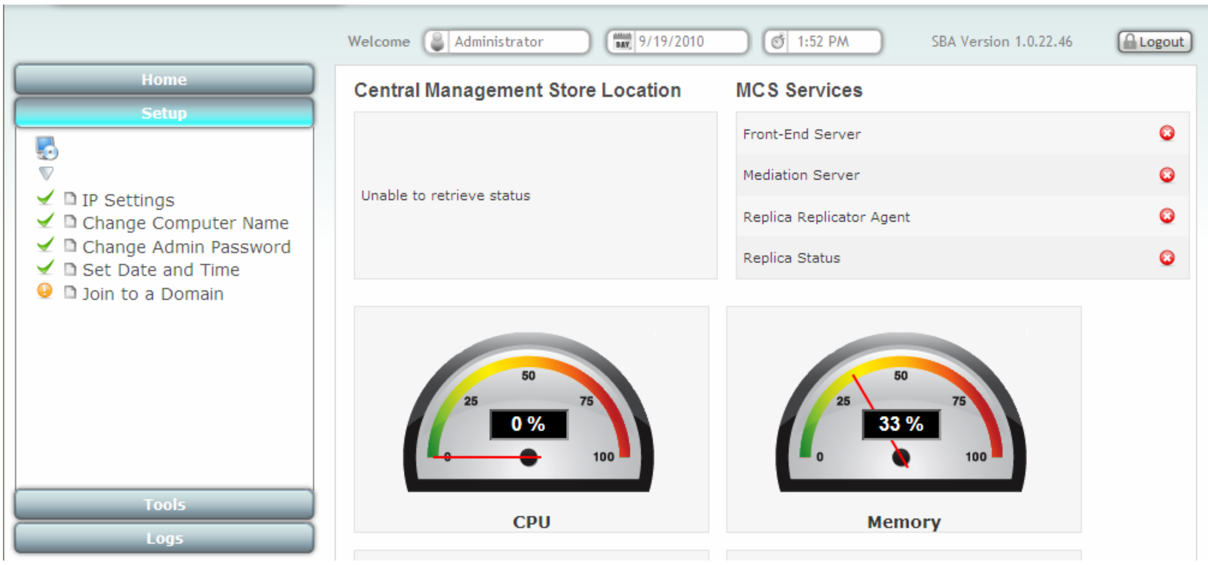
Sep 2010

New time 01 : 53 : 17 PM

8. Click **Next** to proceed to the next setup task.

A green check mark appears alongside the **Set Date and Time** option under the **Setup** menu tab, as shown below:

Figure 7-20: Set Date and Time - Completed Successfully



Welcome Administrator 9/19/2010 1:52 PM SBA Version 1.0.22.46

- ✓ IP Settings
- ✓ Change Computer Name
- ✓ Change Admin Password
- ✓ Set Date and Time
- Join to a Domain

Central Management Store Location

Unable to retrieve status

MCS Services

Front-End Server	☒
Mediation Server	☒
Replica Replicator Agent	☒
Replica Status	☒

CPU: 0 %

Memory: 33 %

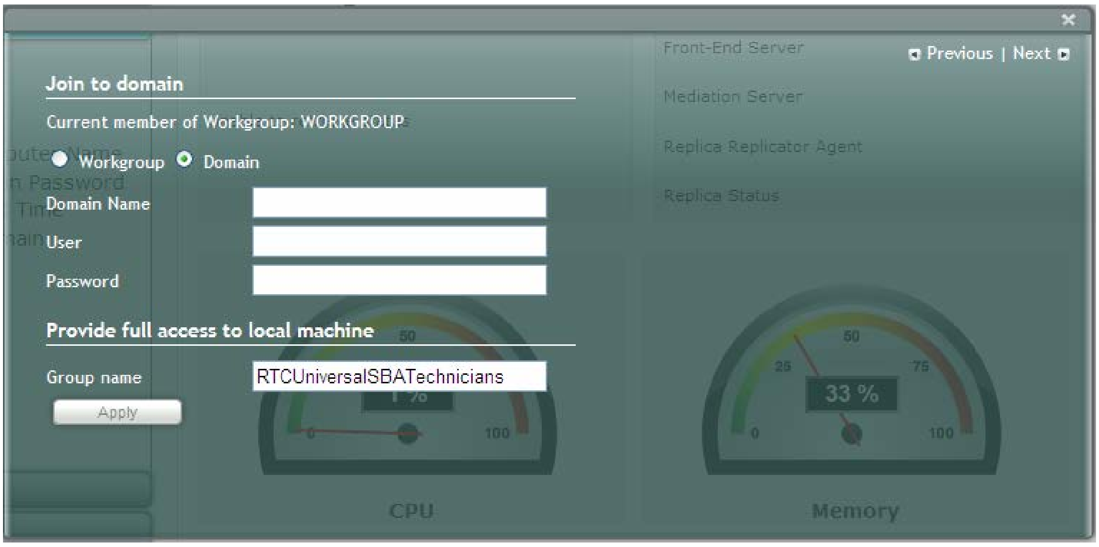
7.5 Step 5: Join to a Domain

The **Join to Domain** option enables you to join the SBA application to a domain.

➢ **To join a domain:**

1. Under the **Setup** menu, click the **Join to a Domain** option; the following screen appears:

Figure 7-21: Join to a Domain Screen



Join to domain

Current member of Workgroup: WORKGROUP

○ Workgroup ● Domain

Domain Name

User

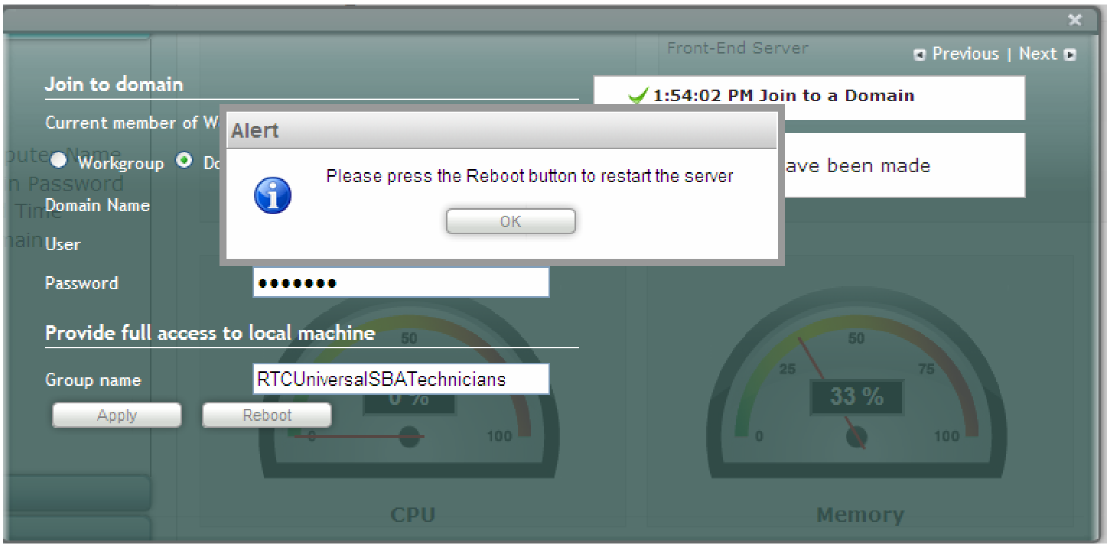
Password

Provide full access to local machine

Group name: RTCUniversalSBATechnicians

2. In the 'Domain Name' field, enter the domain name.
3. In the 'User' and 'Password' fields, enter the user and password of an account that has permission to join the SBA to the domain as configured in Section 5.1 on page 29.
4. In the 'Group name' field, ensure that the **RTCUniversalSBATechnicians** value is selected.
5. Click **Apply**; a message box appears requesting you to confirm reboot:

Figure 7-22: Join to a Domain – Reboot Message Box



Join to domain

1:54:02 PM Join to a Domain

ave been made

Alert

Please press the Reboot button to restart the server

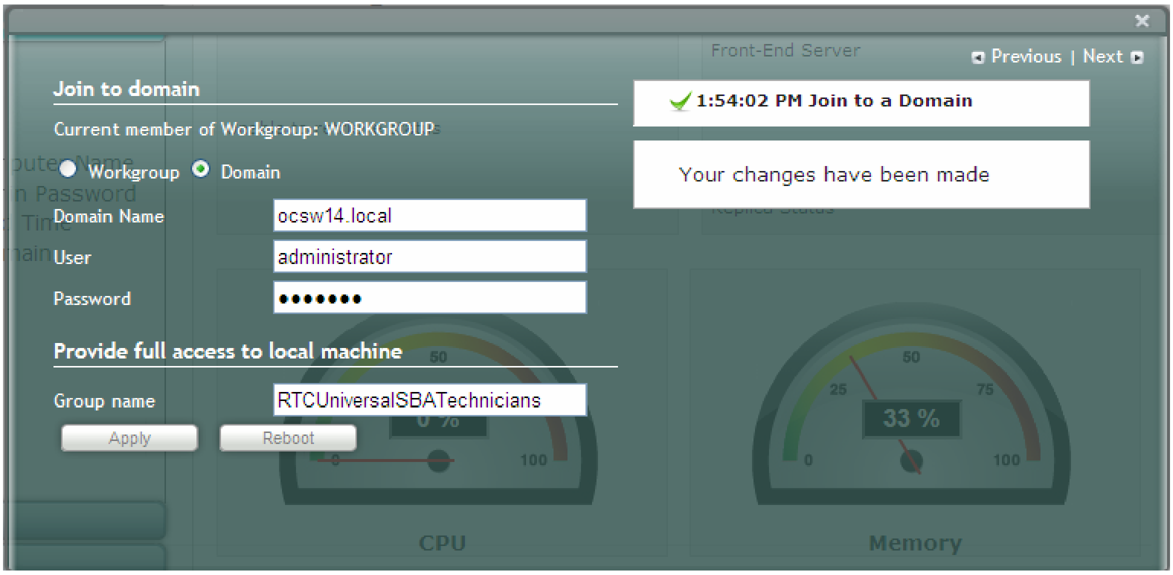
Password: •••••••

Provide full access to local machine

Group name: RTCUniversalSBATechnicians

6. Click **OK**; the following screen appears:

Figure 7-23: Join to a Domain – Applied Changes



Join to domain

Current member of Workgroup: WORKGROUP

○ Workgroup ● Domain

Domain Name: ocsw14.local

User: administrator

Password: •••••••

Provide full access to local machine

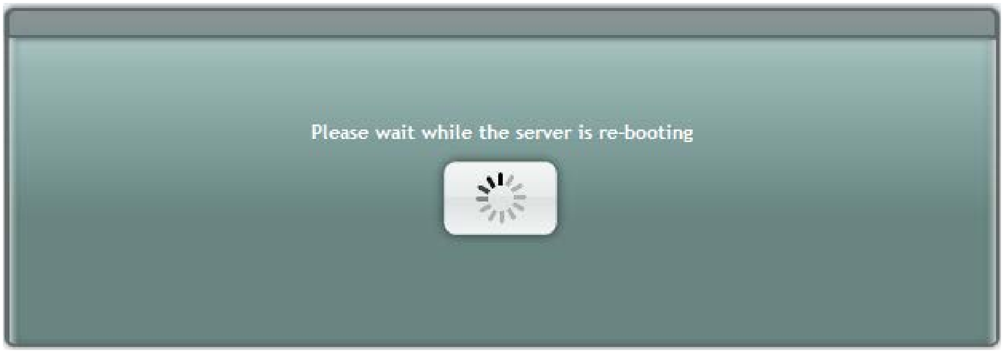
Group name: RTCUniversalSBATechnicians

✓ 1:54:02 PM Join to a Domain

Your changes have been made

7. Click **Reboot** to reboot the OSN server; the following screen appears:

Figure 7-24: Server Rebooting

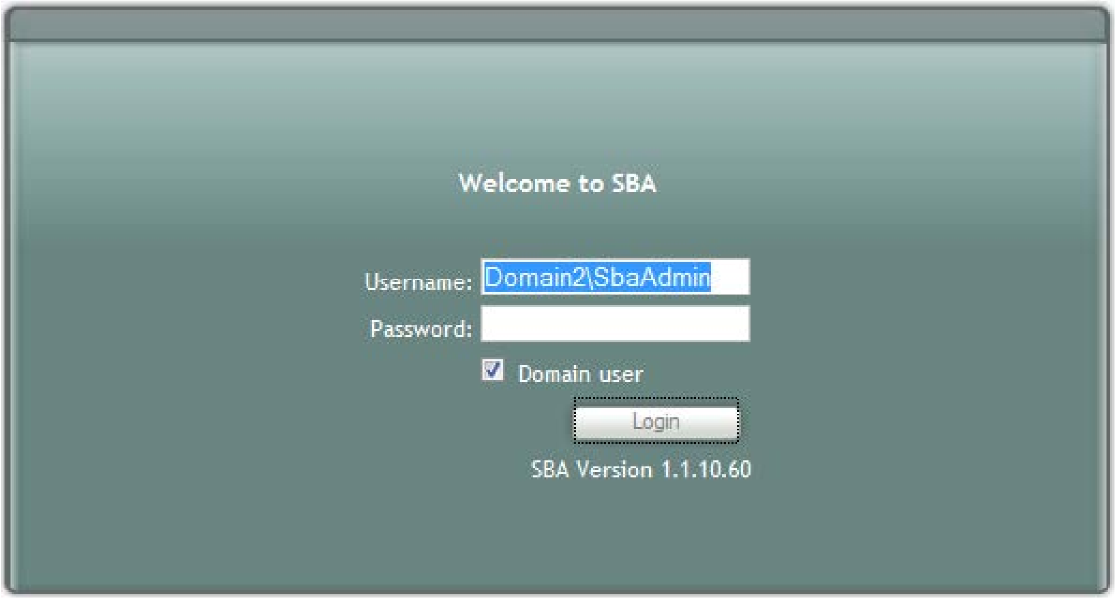


Please wait while the server is re-booting

8. When the reboot completes, the Welcome to SBA login screen appears, now displaying a **Domain user** check box (which is selected by default):

Note: When logging in to SBA with a username that belongs to a different domain than the SBA, enter domain\user as the username field in the login page.

Figure 7-25: Welcome to SBA



Welcome to SBA

Username: Domain2\SbaAdmin

Password:

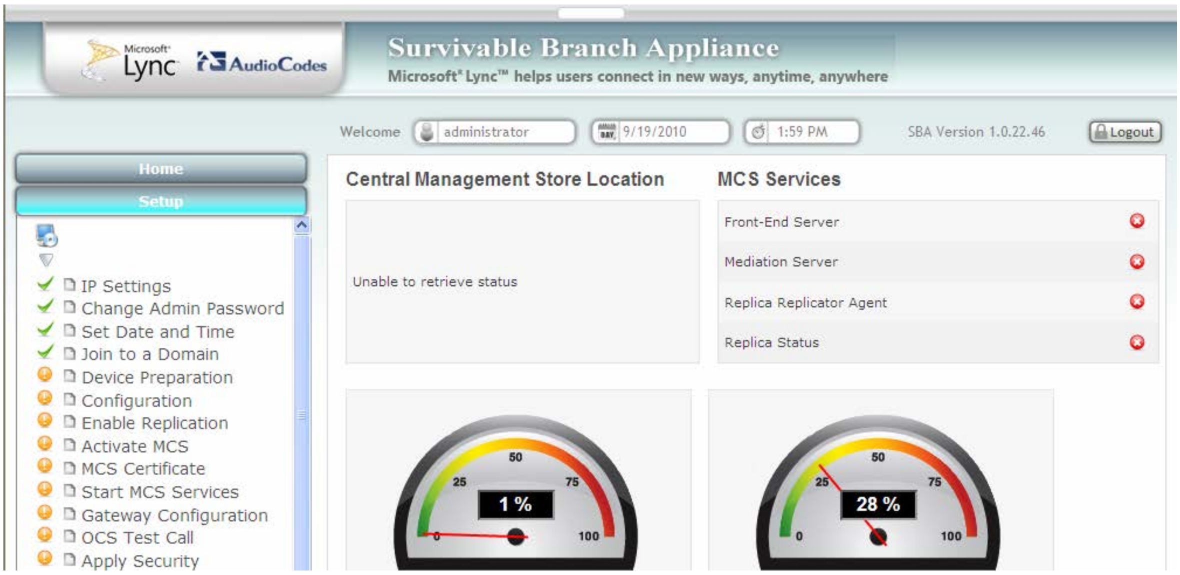
☑ Domain user

Login

SBA Version 1.1.10.60

9. Log in with the Domain user username and password, and then click **Login**; a green check mark is displayed alongside the **Join to a Domain** option under the **Setup** menu tab, as shown below. In addition, the **Setup** menu now displays the remaining menu options.

Figure 7-26: Join to a Domain - Completed Successfully



Survivable Branch Appliance

Microsoft® Lync™ helps users connect in new ways, anytime, anywhere

Welcome administrator 9/19/2010 1:59 PM SBA Version 1.0.22.46 Logout

Home

Setup

- ✓ IP Settings
- ✓ Change Admin Password
- ✓ Set Date and Time
- ✓ Join to a Domain
- ● Device Preparation
- ● Configuration
- ● Enable Replication
- ● Activate MCS
- ● MCS Certificate
- ● Start MCS Services
- ● Gateway Configuration
- ● OCS Test Call
- ● Apply Security

Central Management Store Location

Unable to retrieve status

MCS Services

Front-End Server	⊗
Mediation Server	⊗
Replica Replicator Agent	⊗
Replica Status	⊗

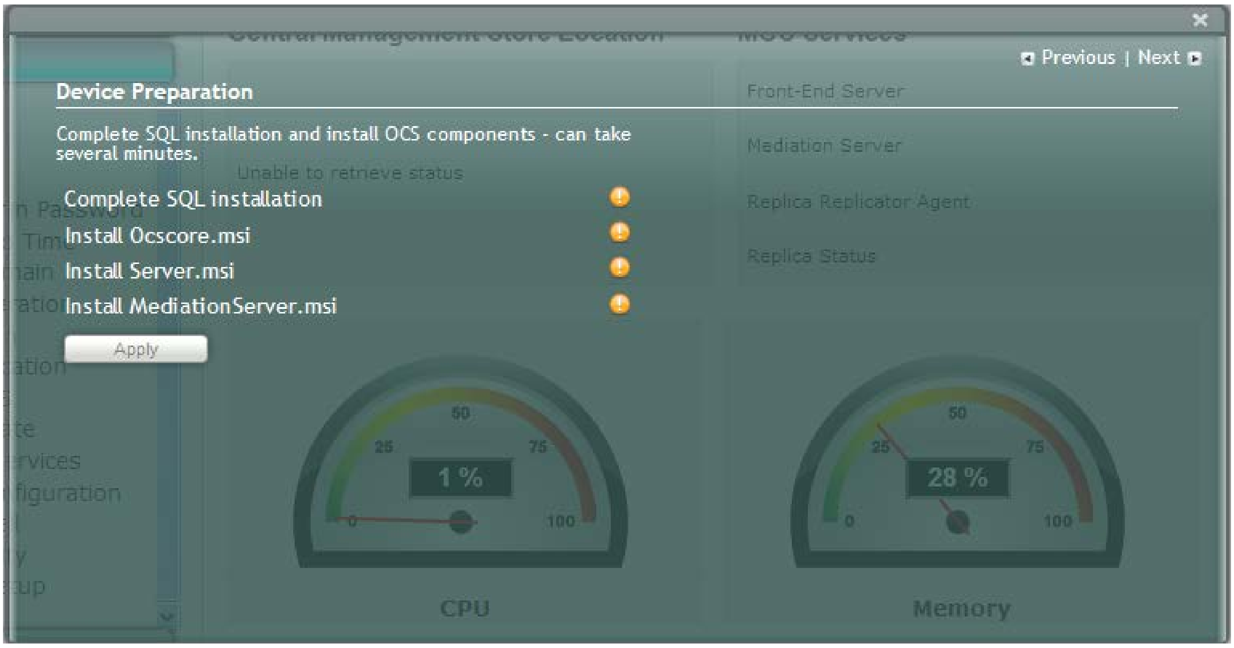
7.6 Step 6: Device Preparation

The **Device Preparation** menu option completes the SQL preparation and installs the Lync Server 2010 components.

➢ **To prepare the device:**

1. Under the **Setup** menu, click the **Device Preparation** option; the following screen appears:

Figure 7-27: Device Preparation Screen



Device Preparation

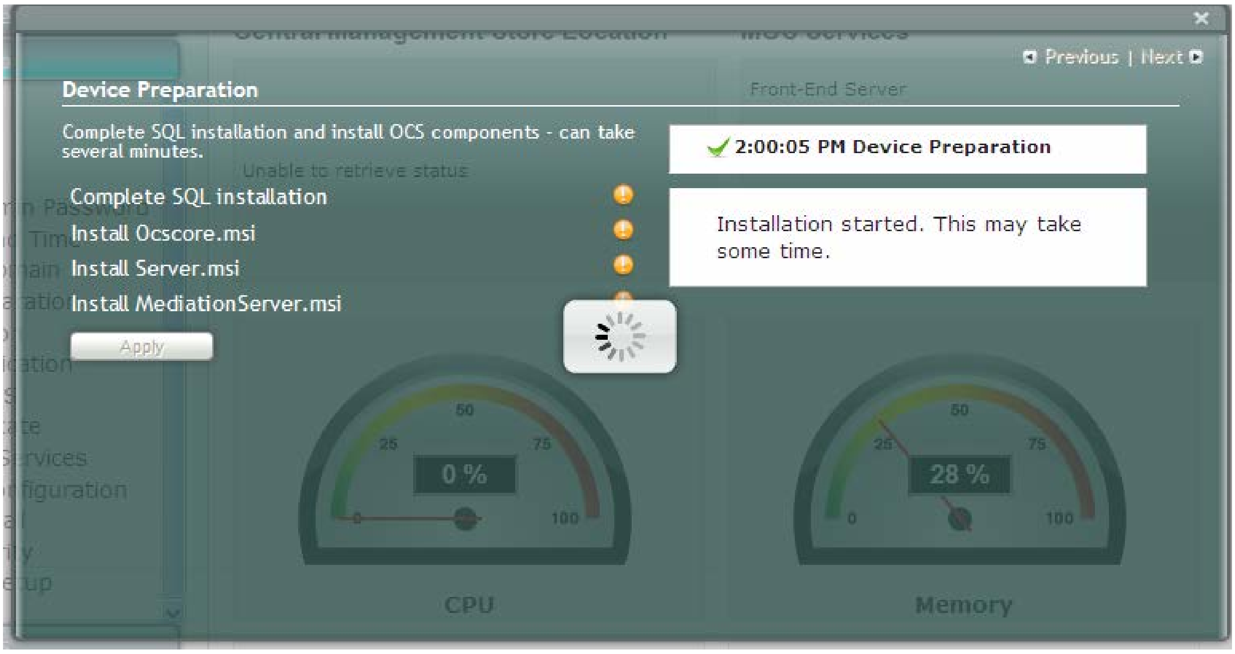
Complete SQL installation and install OCS components - can take several minutes.

Unable to retrieve status

Complete SQL installation
Install Ocscore.msi
Install Server.msi
Install MediationServer.msi

2. Click **Apply**; the SQL installation begins, and the following screens appear in sequence as the SQL installation progresses. You can view a detailed log after each installation phase, by clicking the **Detailed Log** link.

Figure 7-28: Device Preparation - Started



Device Preparation

Complete SQL installation and install OCS components - can take several minutes.

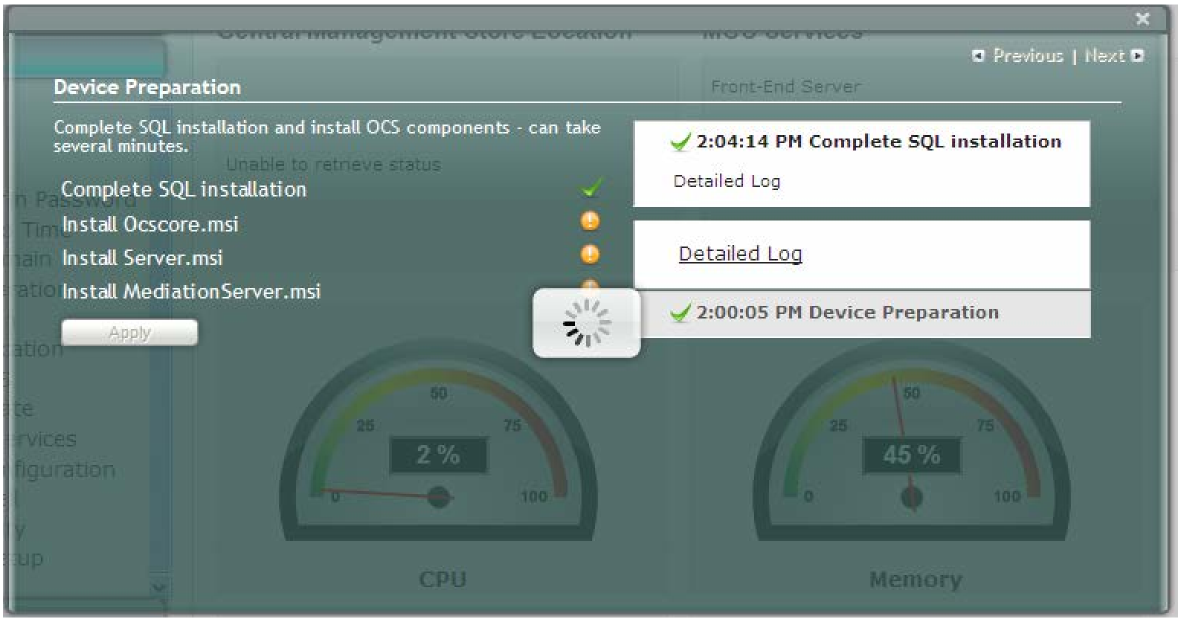
Unable to retrieve status

Complete SQL installation
Install Ocscore.msi
Install Server.msi
Install MediationServer.msi

2:00:05 PM Device Preparation

Installation started. This may take some time.

Figure 7-29: Device Preparation – SQL Installation



Device Preparation

Complete SQL installation and install OCS components - can take several minutes.

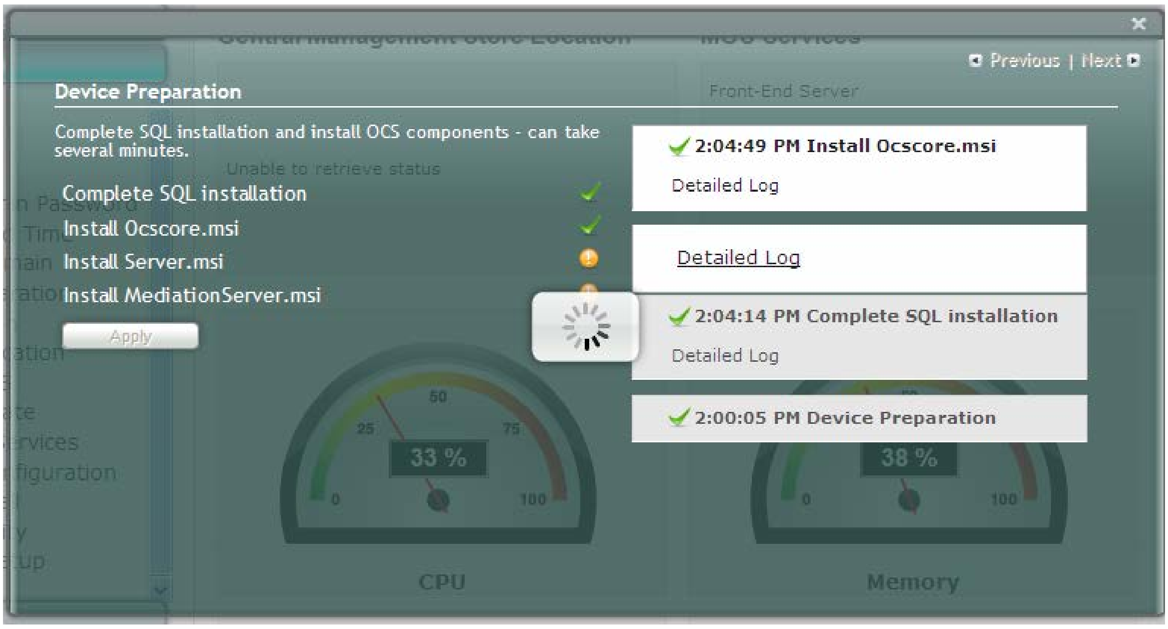
Complete SQL installation ✓
Install Ocscore.msi
Install Server.msi
Install MediationServer.msi

✓ 2:04:14 PM Complete SQL installation
Detailed Log

Detailed Log

✓ 2:00:05 PM Device Preparation

Figure 7-30: Device Preparation – Ocscore Installation



Device Preparation

Complete SQL installation and install OCS components - can take several minutes.

Complete SQL installation ✓
Install Ocscore.msi ✓
Install Server.msi
Install MediationServer.msi

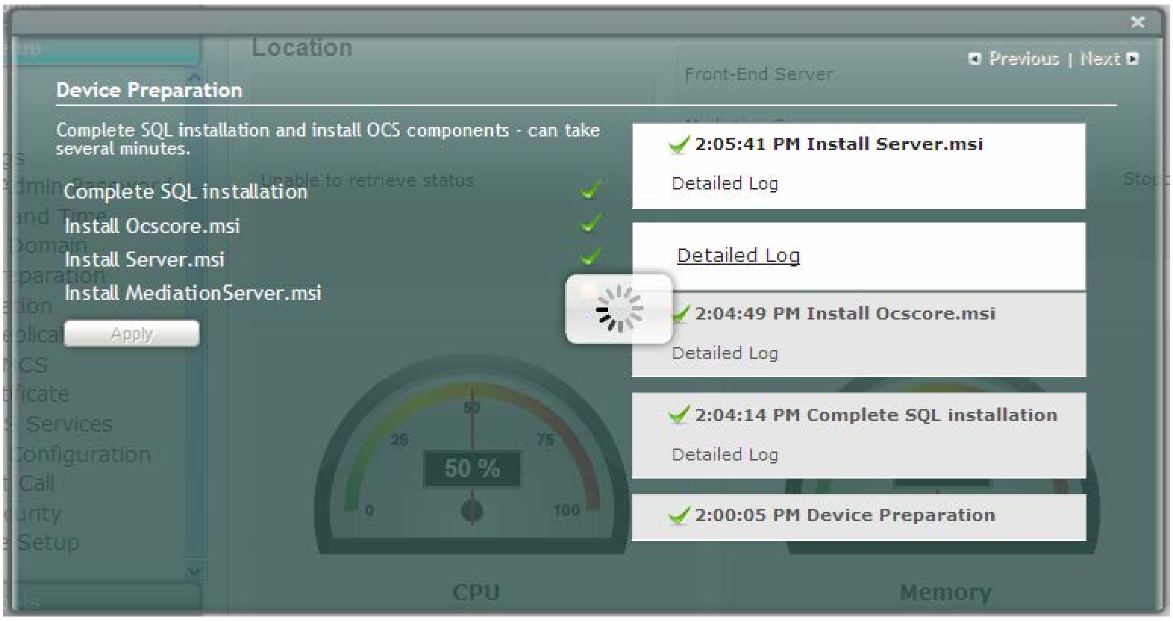
✓ 2:04:49 PM Install Ocscore.msi
Detailed Log

Detailed Log

✓ 2:04:14 PM Complete SQL installation
Detailed Log

✓ 2:00:05 PM Device Preparation

Figure 7-31: Device Preparation – Server Installation



Device Preparation

Complete SQL installation and install OCS components - can take several minutes.

Complete SQL installation ✓
Install Ocscore.msi ✓
Install Server.msi ✓
Install MediationServer.msi

✓ 2:05:41 PM Install Server.msi
Detailed Log

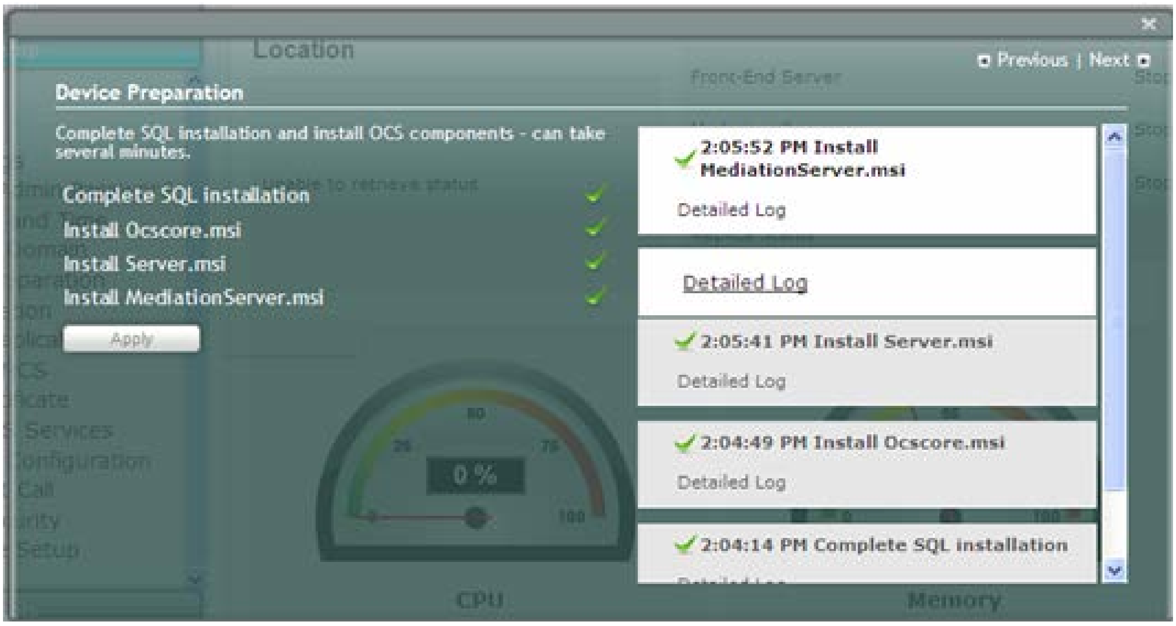
Detailed Log

✓ 2:04:49 PM Install Ocscore.msi
Detailed Log

✓ 2:04:14 PM Complete SQL installation
Detailed Log

✓ 2:00:05 PM Device Preparation

Figure 7-32: Device Preparation – Mediation Server Installation



Device Preparation

Complete SQL installation and install OCS components - can take several minutes.

Complete SQL installation ✓
Install Ocscore.msi ✓
Install Server.msi ✓
Install MediationServer.msi ✓

✓ 2:05:52 PM Install MediationServer.msi
Detailed Log

Detailed Log

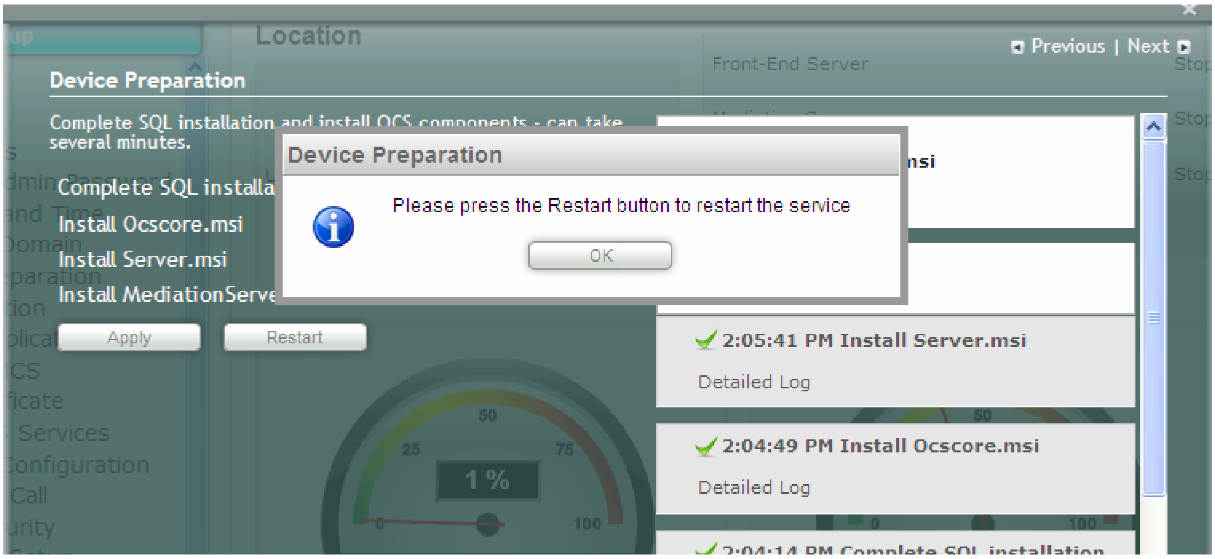
✓ 2:05:41 PM Install Server.msi
Detailed Log

✓ 2:04:49 PM Install Ocscore.msi
Detailed Log

✓ 2:04:14 PM Complete SQL installation

When installation completes, you are notified to click the **Restart** button to restart the server services:

Figure 7-33: Device Preparation – Restart Message Box



Device Preparation

Please press the Restart button to restart the service

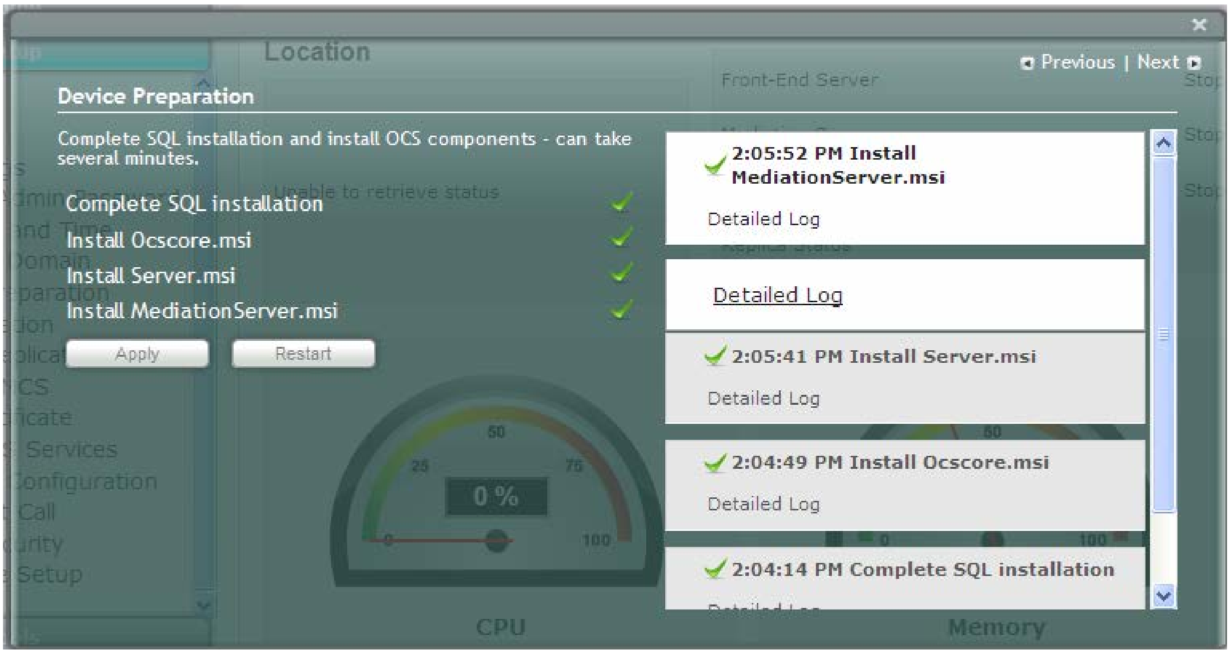
2:05:41 PM Install Server.msi
Detailed Log

2:04:49 PM Install Ocscore.msi
Detailed Log

2:04:14 PM Complete SQL installation

3. Click **OK**; the following screen appears:

Figure 7-34: Device Preparation – Restart



Device Preparation

Complete SQL installation and install OCS components - can take several minutes.

Complete SQL installation ✓
Install Ocscore.msi ✓
Install Server.msi ✓
Install MediationServer.msi ✓

2:05:52 PM Install MediationServer.msi
Detailed Log

Detailed Log

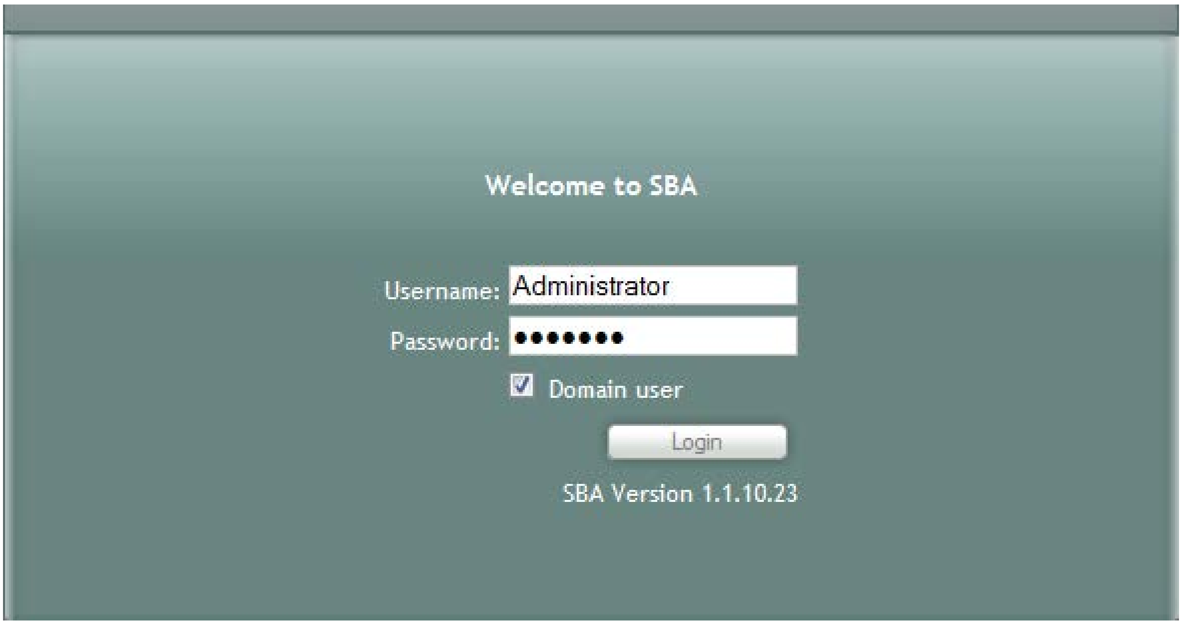
2:05:41 PM Install Server.msi
Detailed Log

2:04:49 PM Install Ocscore.msi
Detailed Log

2:04:14 PM Complete SQL installation

4. If all steps have been completed successfully, click **Restart**. If not, refer to the Detailed Log for corrective information, rectify the problem, and then click **Apply** to install the remaining components.

Figure 7-35: Login Screen



Welcome to SBA

Username: Administrator

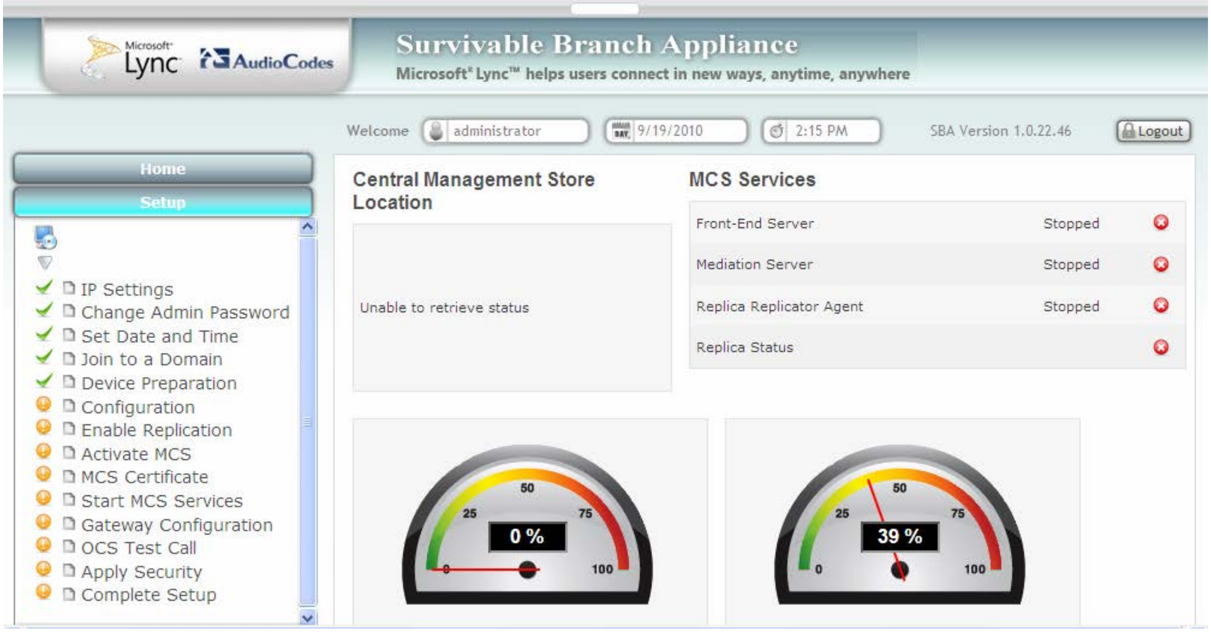
Password: •••••••

☑ Domain user

SBA Version 1.1.10.23

5. Log in with the Domain user username and password, and then click **Login**; a green check mark appears alongside the **Device Preparation** option under the Setup menu (as shown below). In addition, the **Setup** menu now displays the remaining menu options.

Figure 7-36: Device Preparation – Completed Successfully


Microsoft Lync
AudioCodes
Survivable Branch Appliance
Microsoft® Lync™ helps users connect in new ways, anytime, anywhere
Logout
Home
Setup
50
25
75
0
100

Welcome administrator 9/19/2010 2:15 PM SBA Version 1.0.22.46

- ✓ IP Settings
- ✓ Change Admin Password
- ✓ Set Date and Time
- ✓ Join to a Domain
- ✓ Device Preparation
- ● Configuration
- ● Enable Replication
- ● Activate MCS
- ● MCS Certificate
- ● Start MCS Services
- ● Gateway Configuration
- ● OCS Test Call
- ● Apply Security
- ● Complete Setup

Central Management Store Location

Unable to retrieve status

MCS Services

Front-End Server	Stopped	✗
Mediation Server	Stopped	✗
Replica Replicator Agent	Stopped	✗
Replica Status		✗

0 %

39 %

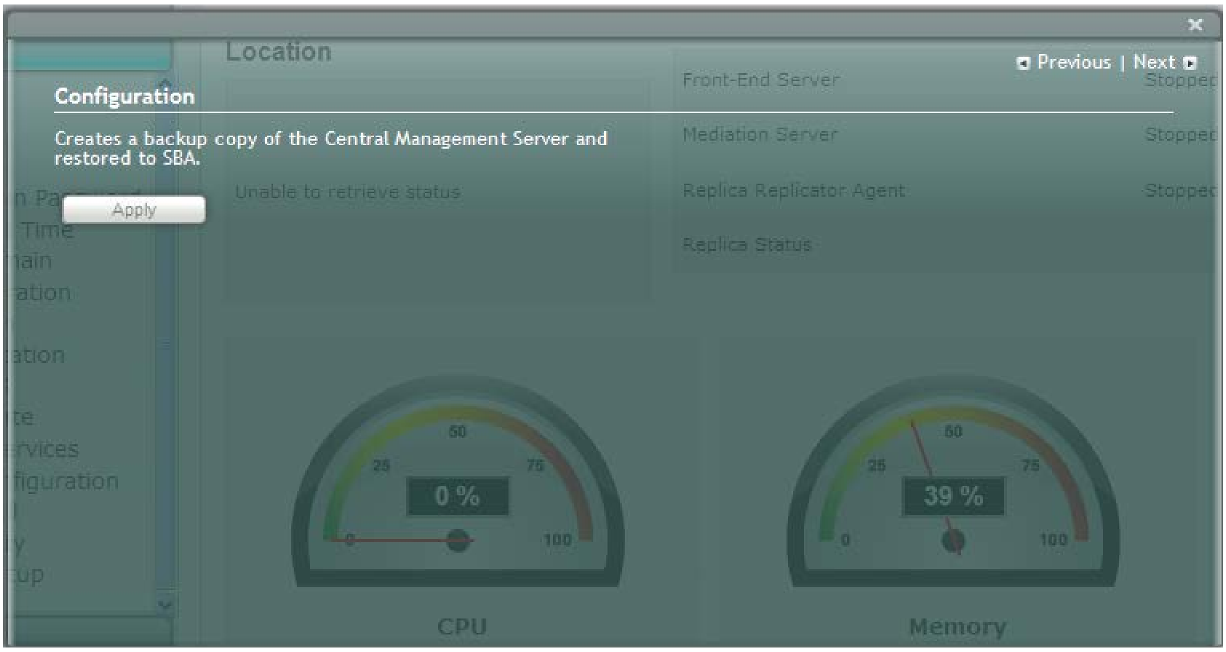
7.7 Step 7: Configuration

The **Configuration** option creates a backup copy of the Central Management Server on the SBA server.

➢ **To create a backup of the Central Management Server:**

1. Under the **Setup** menu, click the **Configuration** option; the following screen appears:

Figure 7-37: Configuration Screen



Configuration

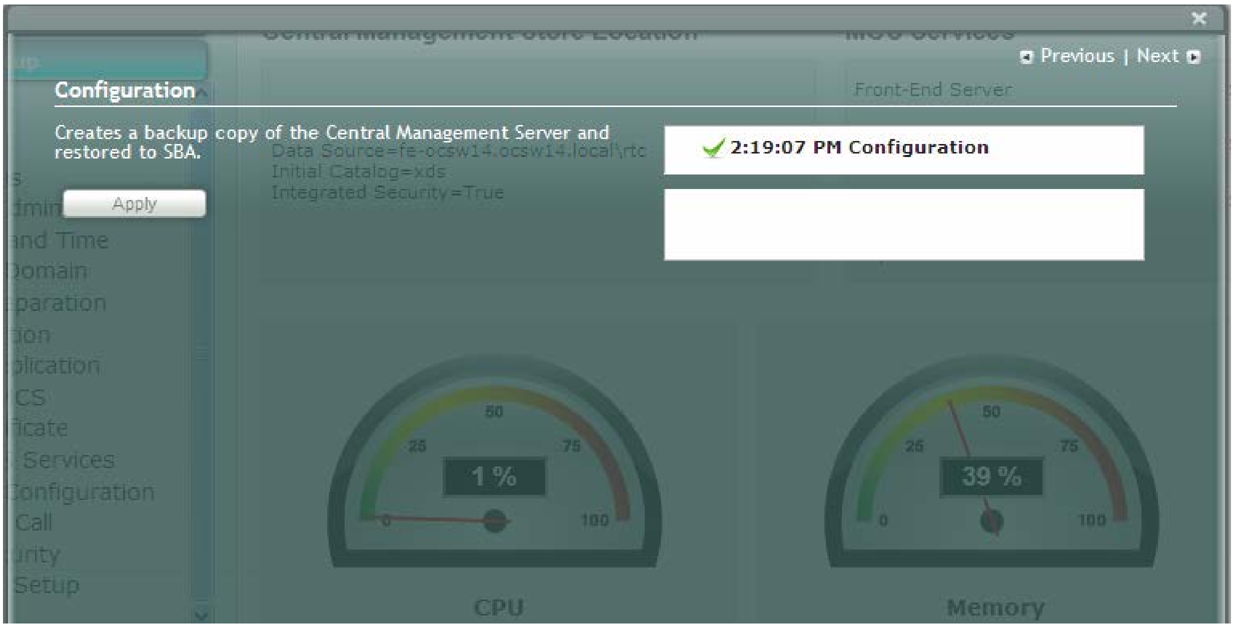
Creates a backup copy of the Central Management Server and restored to SBA.

Unable to retrieve status

Front-End Server	Stopped
Mediation Server	Stopped
Replica Replicator Agent	Stopped
Replica Status	

2. Click **Apply**; the following screen appears:

Figure 7-38: Configuration – Applied Successfully



Configuration

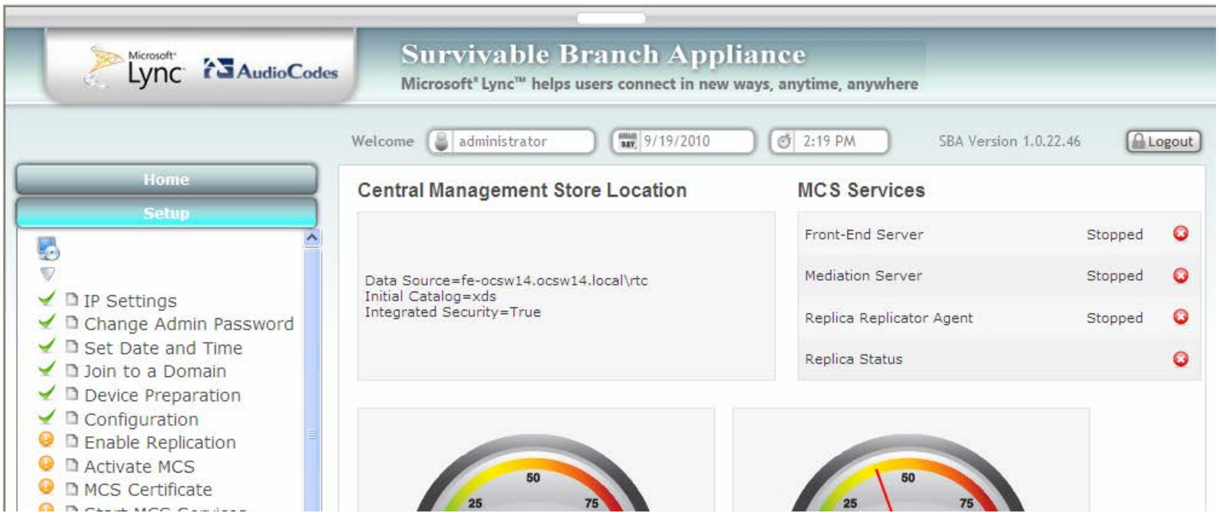
Creates a backup copy of the Central Management Server and restored to SBA.

Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True

✓ 2:19:07 PM Configuration

A green check mark appears alongside the **Configuration** option under the **Setup** menu, as shown below:

Figure 7-39: Configuration – Completed Successfully



administrator

9/19/2010

2:19 PM

SBA Version 1.0.22.46

Central Management Store Location

Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True

MCS Services

Front-End Server	Stopped	☒
Mediation Server	Stopped	☒
Replica Replicator Agent	Stopped	☒
Replica Status		☒

Note: If the backup procedure fails, reboot the SBA server manually using the **Tools** menu option (see Section 11.2 on page 128), and then repeat the procedure above.

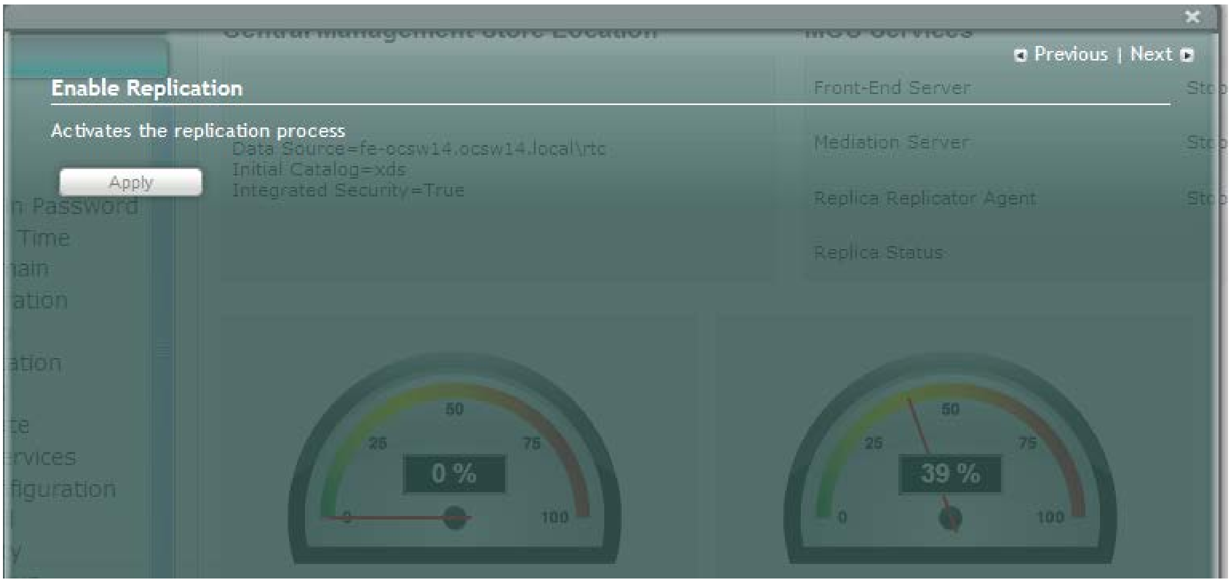
7.8 Step 8: Enable Replication

The **Enable Replication** option activates the replication process for the Lync Server 2010.

- **To enable replication:**

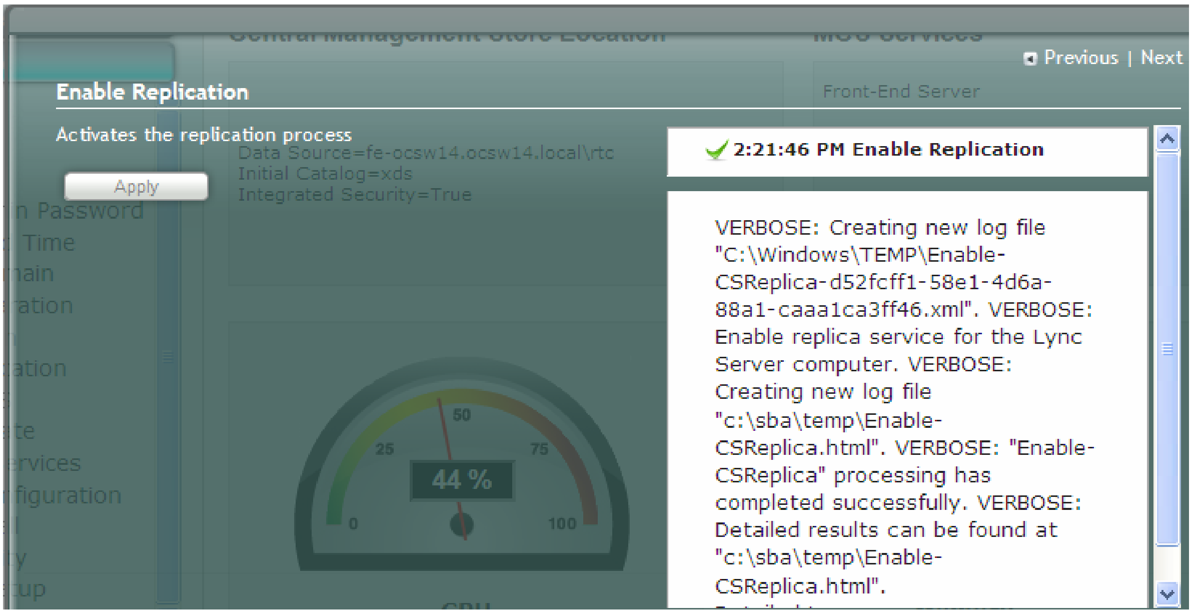
1. Under the **Setup** menu, click the **Enable Replication** option; the following screen appears:

Figure 7-40: Enable Replication Screen



2. Click **Apply**; the following screen appears:

Figure 7-41: Enable Replication – Applied Successfully

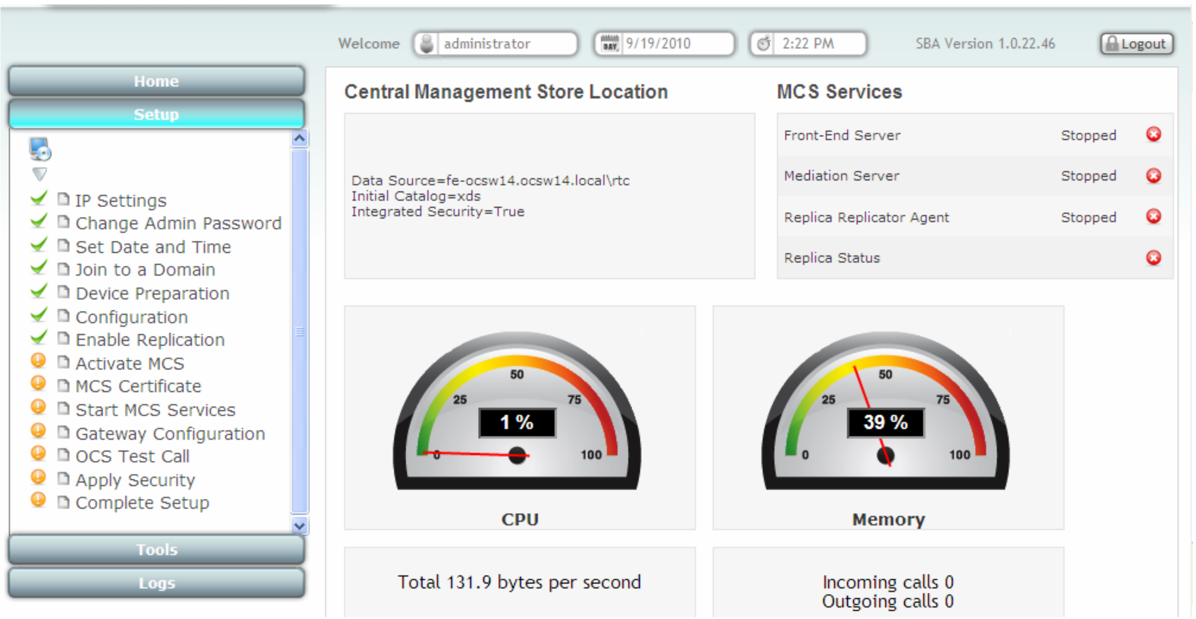


✓ 2:21:46 PM Enable Replication

```
VERBOSE: Creating new log file
"C:\Windows\TEMP\Enable-
CSReplica-d52fcff1-58e1-4d6a-
88a1-caaa1ca3ff46.xml". VERBOSE:
Enable replica service for the Lync
Server computer. VERBOSE:
Creating new log file
"c:\sba\temp\Enable-
CSReplica.html". VERBOSE: "Enable-
CSReplica" processing has
completed successfully. VERBOSE:
Detailed results can be found at
"c:\sba\temp\Enable-
CSReplica.html".
```

A green check mark appears alongside the **Enable Replication** option under the **Setup** menu, as shown below:

Figure 7-42: Enable Replication – Completed Successfully



Central Management Store Location

Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True

MCS Services

Front-End Server	Stopped	☒
Mediation Server	Stopped	☒
Replica Replicator Agent	Stopped	☒
Replica Status		☒

Total 131.9 bytes per second

Incoming calls 0
Outgoing calls 0

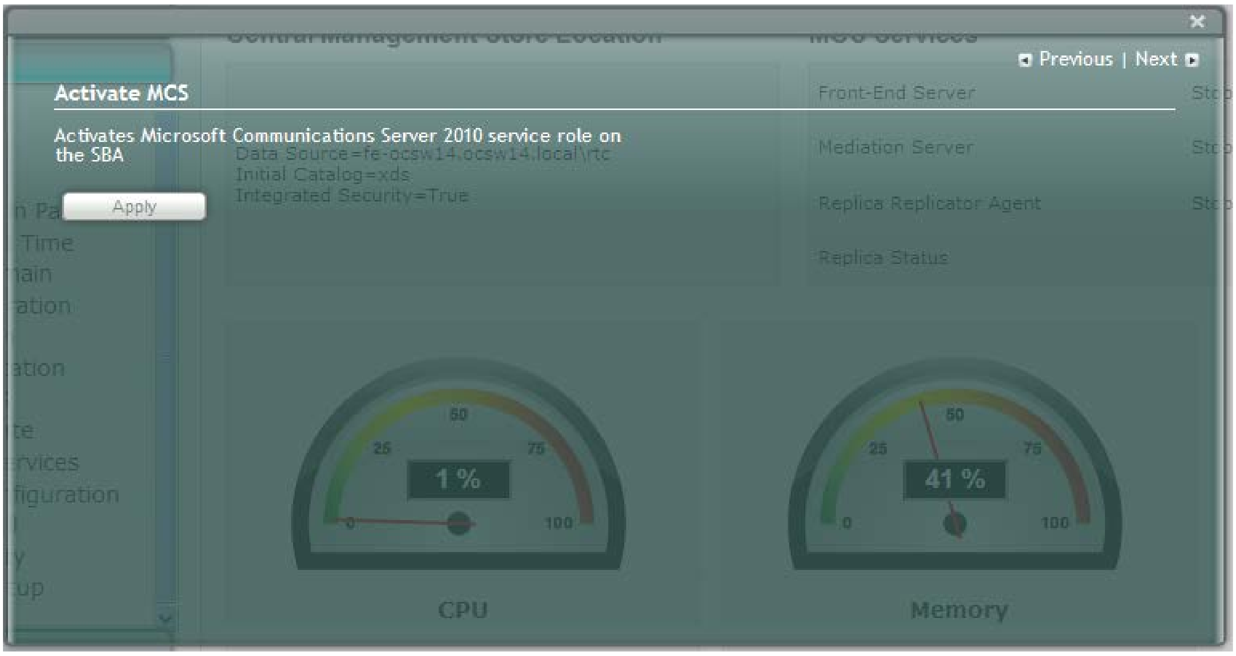
7.9 Step 9: Activate MCS

The **Activate MCS** option activates a computer running a Lync Server 2010 service role. Installing the required software does not automatically cause a computer to adopt a new service role; instead, that computer must be activated before it actually begins to function in its new role.

➢ To activate MCS:

1. Under the **Setup** menu, click the **Activate MCS** option; the following screen appears:

Figure 7-43: Activate MCS Screen

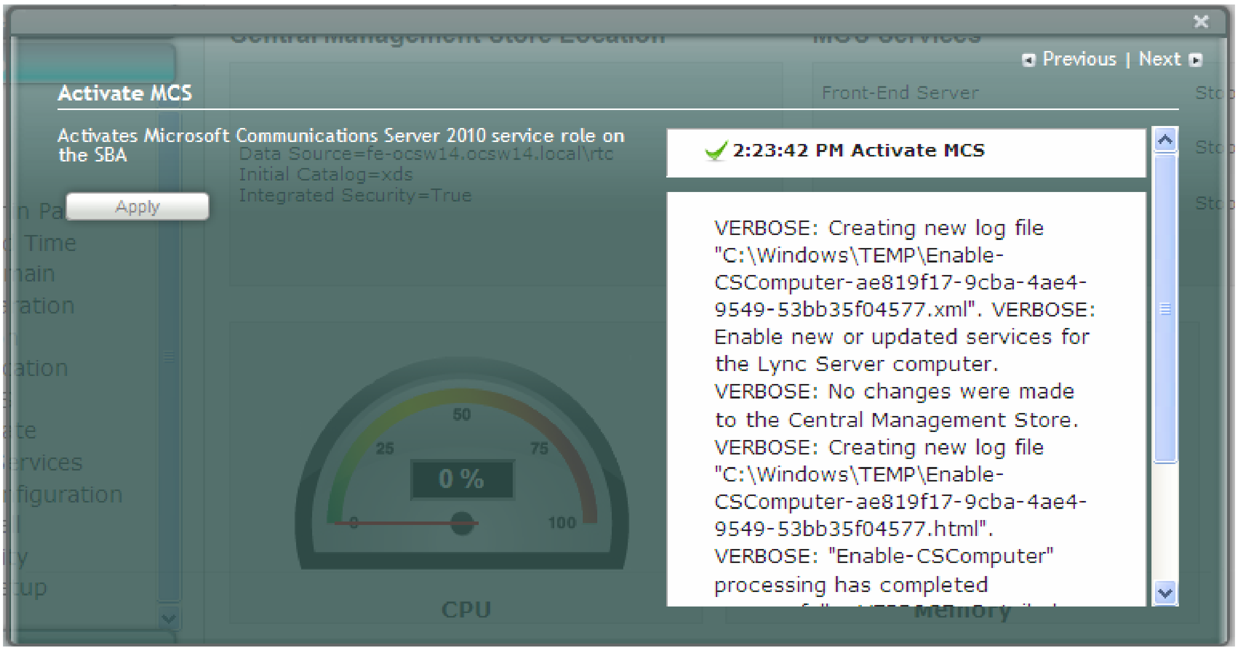


Activate MCS

Activates Microsoft Communications Server 2010 service role on the SBA

2. Click **Apply**; the following screen appears:

Figure 7-44: Activate MCS – Applied Successfully



Activate MCS

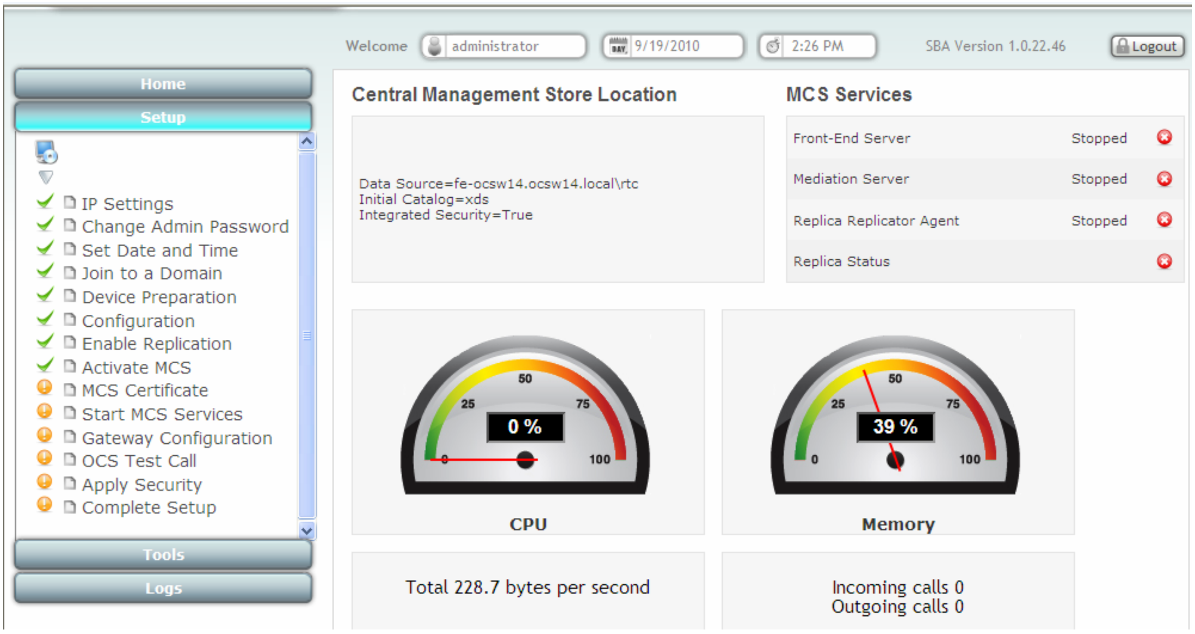
Activates Microsoft Communications Server 2010 service role on the SBA

✓ 2:23:42 PM Activate MCS

```
VERBOSE: Creating new log file
"C:\Windows\TEMP\Enable-
CSComputer-ae819f17-9cba-4ae4-
9549-53bb35f04577.xml". VERBOSE:
Enable new or updated services for
the Lync Server computer.
VERBOSE: No changes were made
to the Central Management Store.
VERBOSE: Creating new log file
"C:\Windows\TEMP\Enable-
CSComputer-ae819f17-9cba-4ae4-
9549-53bb35f04577.html".
VERBOSE: "Enable-CSComputer"
processing has completed
```

A green check mark appears alongside the **Activate MCS** option under the **Setup** menu, as shown below:

Figure 7-45: Activate MCS – Completed Successfully



Central Management Store Location

Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True

MCS Services

Front-End Server	Stopped	✗
Mediation Server	Stopped	✗
Replica Replicator Agent	Stopped	✗
Replica Status		✗

Total 228.7 bytes per second

Incoming calls 0
Outgoing calls 0

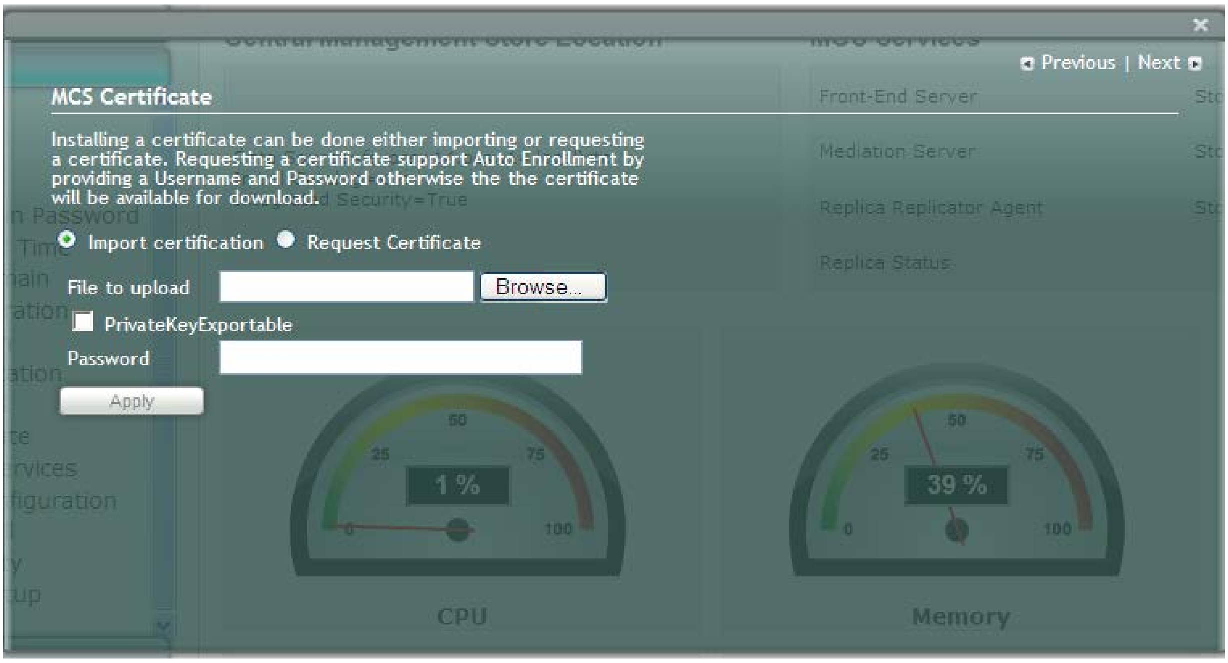
7.10 Step 10: MCS Certificate

The **MCS Certificate** option installs a certificate from the domain's certificate authority.

➢ **To install a Certificate:**

- Under the **Setup** menu, click the **MCS Certificate** option; the following screen appears:

Figure 7-46: MCS Certificate Screen



MCS Certificate

Installing a certificate can be done either importing or requesting a certificate. Requesting a certificate support Auto Enrollment by providing a Username and Password otherwise the the certificate will be available for download.

● Import certification ○ Request Certificate

File to upload

□ PrivateKeyExportable

Password

Certificates can be installed either by importing an existing certificate or requesting a new certificate.

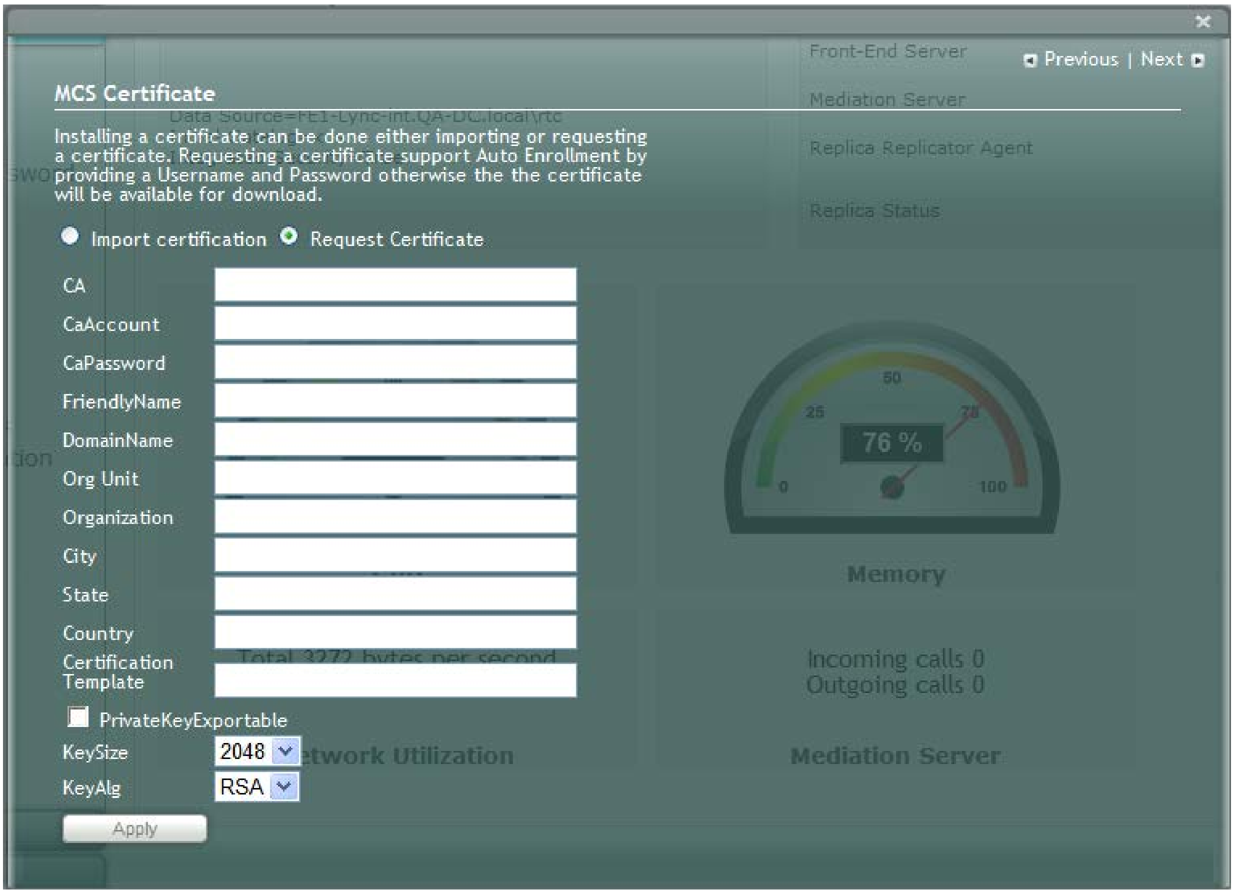
➢ **To import an existing certificate:**

1. Select the **Import Certification** radio button.
2. Click **Browse** to select the **File to Upload**.
3. Enter the **Password** (optional) of the certificates.
4. Click **Apply**.

➢ To request a new certificate:

1. Select the **Request Certificate** radio button.

Figure 7-47: Request Certificate



MCS Certificate

Installing a certificate can be done either importing or requesting a certificate. Requesting a certificate support Auto Enrollment by providing a Username and Password otherwise the the certificate will be available for download.

○ Import certification ● Request Certificate

CA	
CaAccount	
CaPassword	
FriendlyName	
DomainName	
Org Unit	
Organization	
City	
State	
Country	
Certification Template	

□ PrivateKeyExportable

KeySize 2048

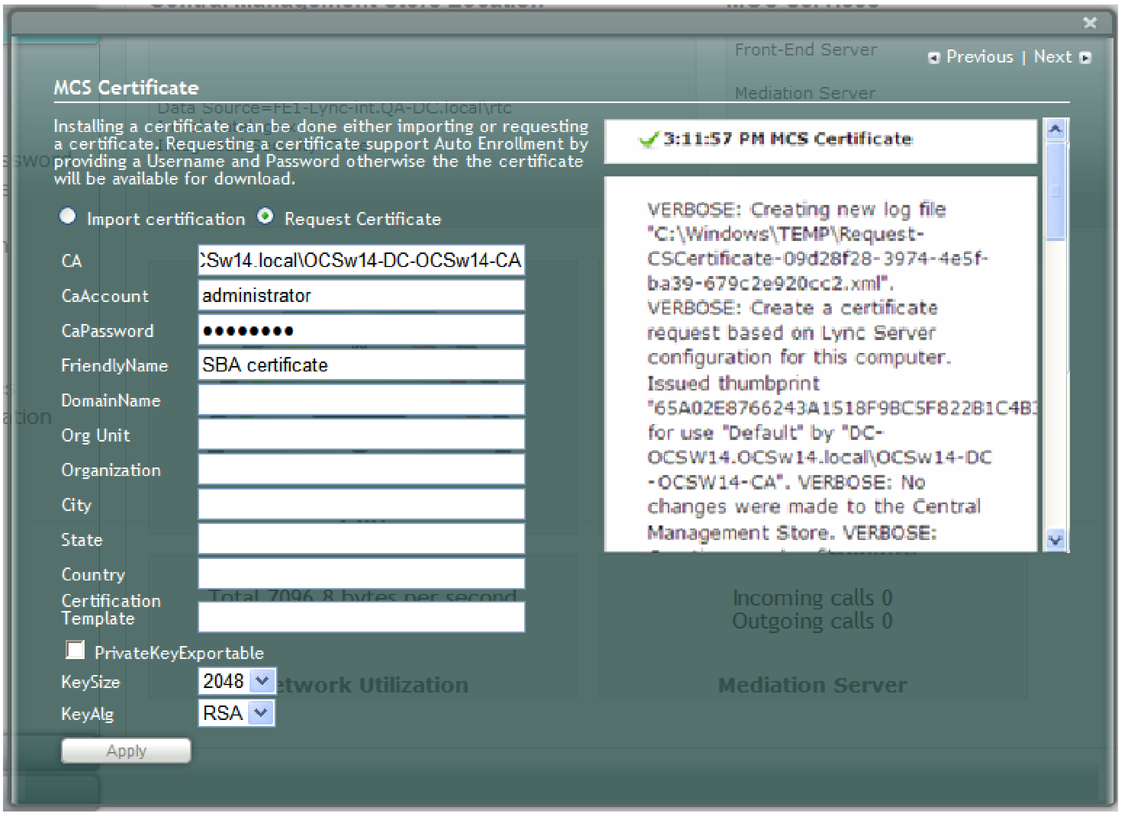
KeyAlg RSA

Apply

2. Requesting a certificate supports Auto-enrollment. Enter all fields. Those fields beginning with a CA prefix are mandatory. The correct Certificate Authority (CA), User and Password must also be supplied.

   The CA field contains the *<CA FQDN>\<CA Name> (e.g., CA.Lync.local\CA-DC-Lync-CA).*

Figure 7-48: MCS Certificate – Detailed Log



MCS Certificate

Installing a certificate can be done either importing or requesting a certificate. Requesting a certificate support Auto Enrollment by providing a Username and Password otherwise the the certificate will be available for download.

○ Import certification ● Request Certificate

CA	:Sw14.local\OCSw14-DC-OCSw14-CA
CaAccount	administrator
CaPassword	••••••••
FriendlyName	SBA certificate
DomainName	
Org Unit	
Organization	
City	
State	
Country	
Certification Template	

□ PrivateKeyExportable

KeySize 2048

KeyAlg RSA

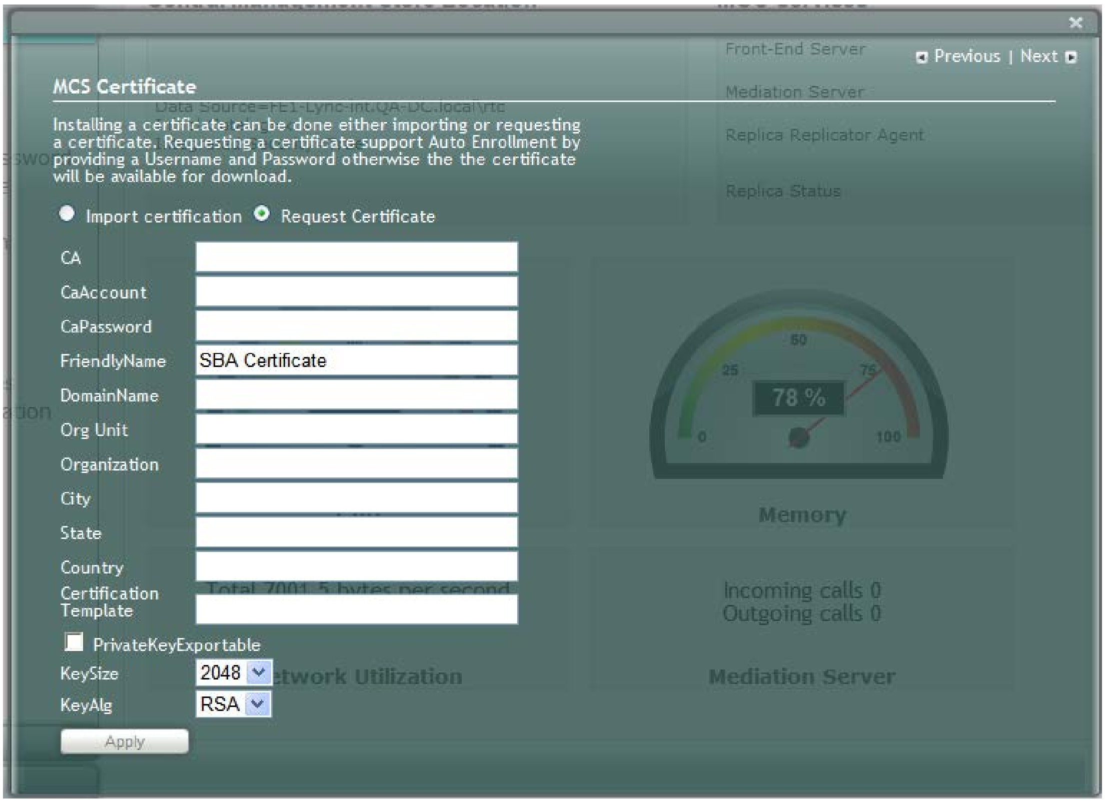
Apply

✓ 3:11:57 PM MCS Certificate

```
VERBOSE: Creating new log file
"C:\Windows\TEMP\Request-
CSCertificate-09d28f28-3974-4e5f-
ba39-679c2e920cc2.xml".
VERBOSE: Create a certificate
request based on Lync Server
configuration for this computer.
Issued thumbprint
"65A02E8766243A1518F9BC5F822B1C4B
for use "Default" by "DC-
OCSW14.OCSw14.local\OCSw14-DC
-OCSW14-CA". VERBOSE: No
changes were made to the Central
Management Store. VERBOSE:
```

3. If the CA field is not entered, the system creates an enrollment certificate, which can be downloaded.

Figure 7-49: MCS Certificate – Download Enrolled Certificate



MCS Certificate

Installing a certificate can be done either importing or requesting a certificate. Requesting a certificate support Auto Enrollment by providing a Username and Password otherwise the the certificate will be available for download.

○ Import certification ● Request Certificate

CA	
CaAccount	
CaPassword	
FriendlyName	SBA Certificate
DomainName	
Org Unit	
Organization	
City	
State	
Country	
Certification Template	

□ PrivateKeyExportable

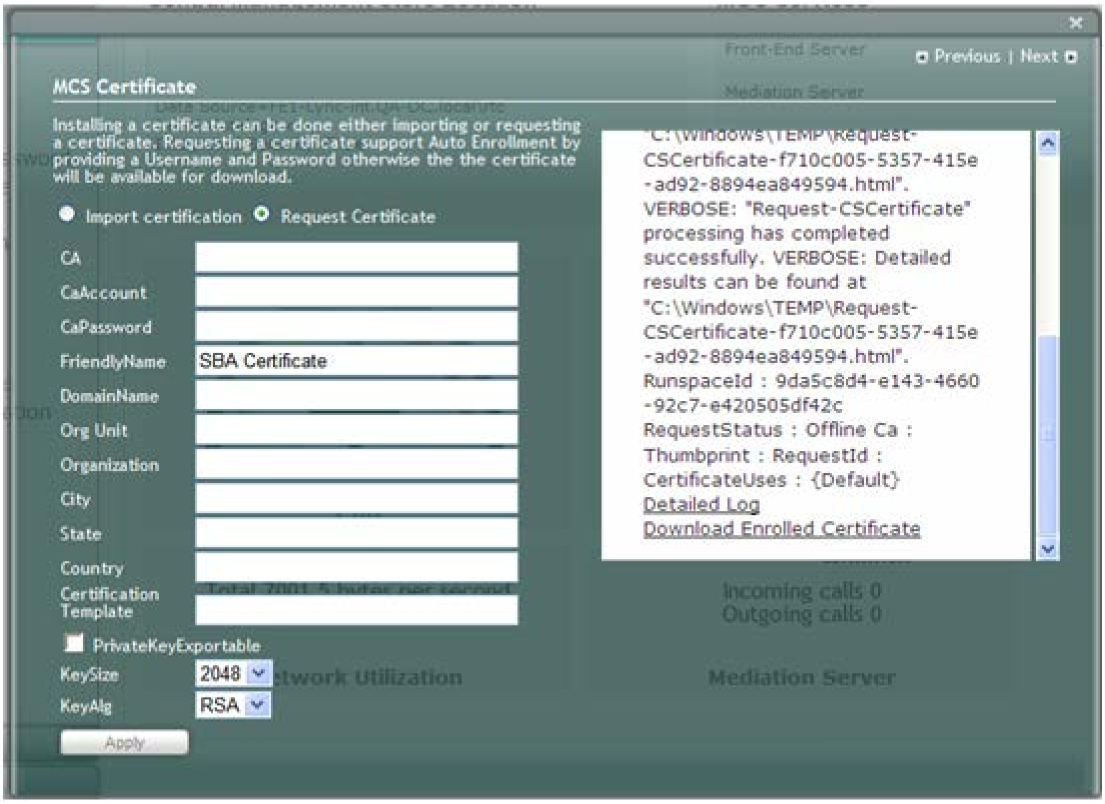
KeySize 2048

KeyAlg RSA

Apply

4. Click **Apply**; the following screen appears.

Figure 7-50: MCS Certificate – Download Enrolled Certificate



MCS Certificate

Installing a certificate can be done either importing or requesting a certificate. Requesting a certficate support Auto Enrollment by providing a Username and Password otherwise the the certificate will be available for download.

○ Import certification ● Request Certificate

CA

CaAccount

CaPassword

FriendlyName: SBA Certificate

DomainName

Org Unit

Organization

City

State

Country

Certification Template

☐ PrivateKeyExportable

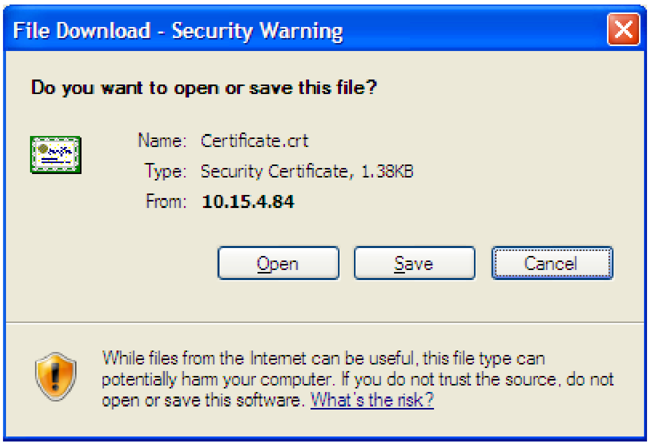
KeySize: 2048

KeyAlg: RSA

```
"C:\Windows\TEMP\Request-
CSCertificate-f710c005-5357-415e
-ad92-8894ea849594.html".
VERBOSE: "Request-CSCertificate"
processing has completed
successfully. VERBOSE: Detailed
results can be found at
"C:\Windows\TEMP\Request-
CSCertificate-f710c005-5357-415e
-ad92-8894ea849594.html".
RunspaceId : 9da5c8d4-e143-4660
-92c7-e420505df42c
RequestStatus : Offline Ca :
Thumbprint : RequestId :
CertificateUses : {Default}
Detailed Log
Download Enrolled Certificate
```

5. Click the **Download Enrolled Certificate** link**;** the following screen appears.

Figure 7-51: MCS Certificate – File Download



File Download - Security Warning

Do you want to open or save this file?

Name: Certificate.crt

Type: Security Certificate, 1.38KB

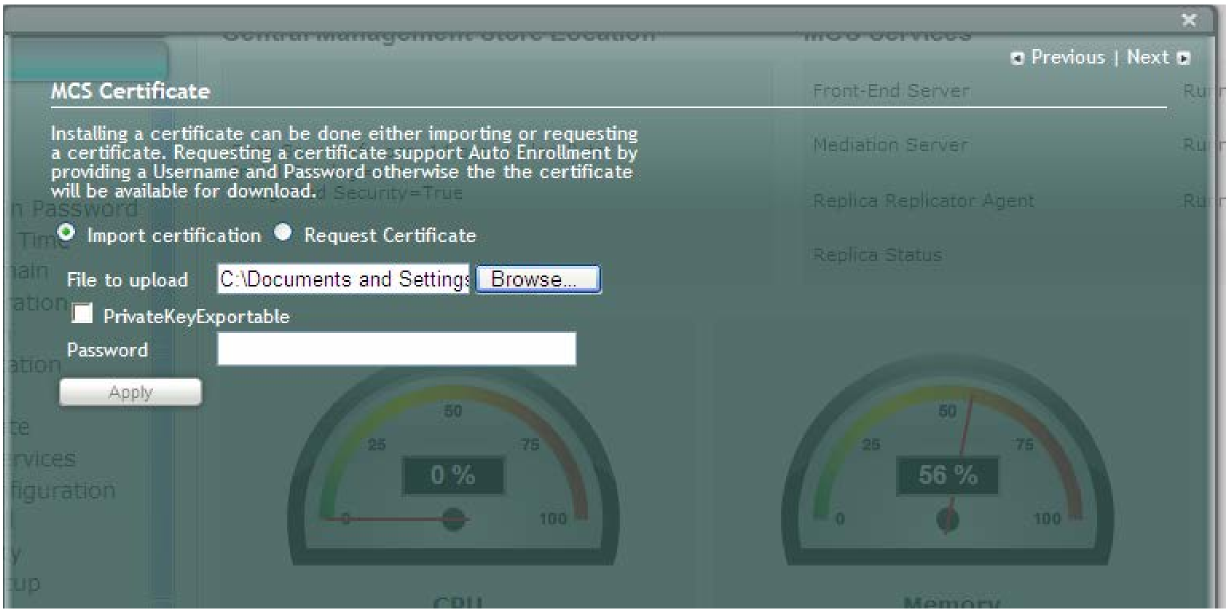
From: **10.15.4.84**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

6. Click **Save**.

7. Once the Enrollment Certificate has been signed, select the **Import Certification** radio button as shown below and upload the signed certificate to be uploaded by using the **Browse** and **File to Upload** fields.

Figure 7-52: MCS Certificate – File Upload



MCS Certificate

Installing a certificate can be done either importing or requesting a certificate. Requesting a certificate support Auto Enrollment by providing a Username and Password otherwise the the certificate will be available for download.

● Import certification ○ Request Certificate

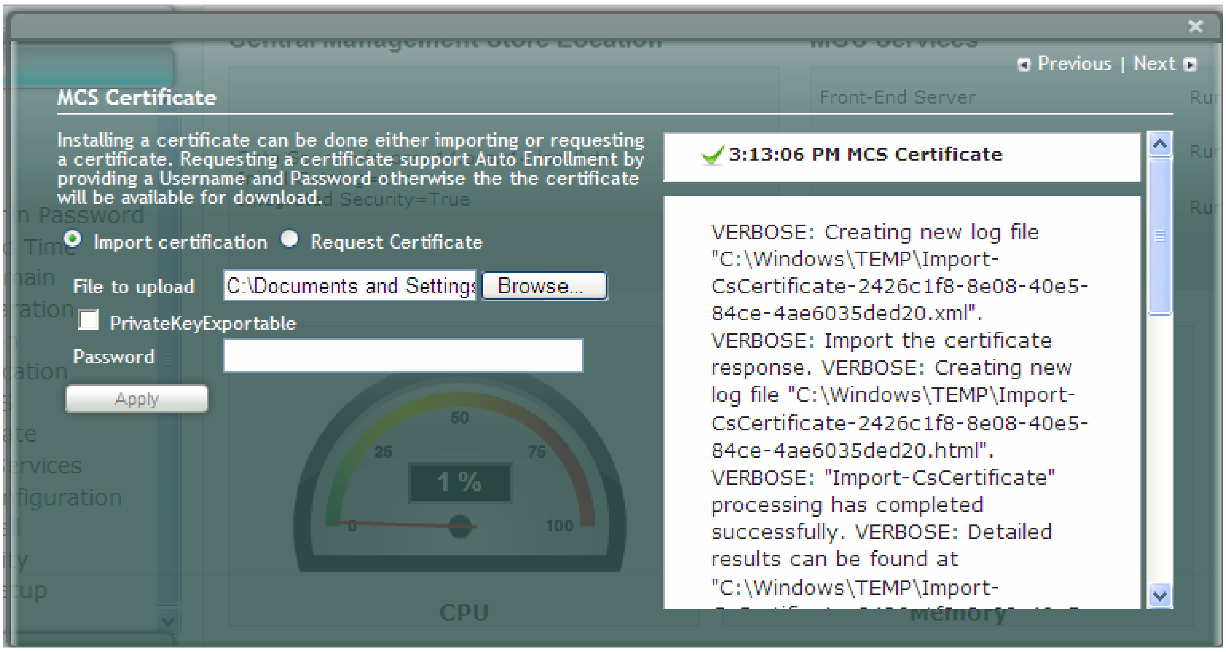
File to upload C:\Documents and Settings

□ PrivateKeyExportable

Password

8. Click **Apply**; the following screen appears:

Figure 7-53: MCS Certificate – Detail Log



MCS Certificate

Installing a certificate can be done either importing or requesting a certificate. Requesting a certificate support Auto Enrollment by providing a Username and Password otherwise the the certificate will be available for download.

● Import certification ○ Request Certificate

File to upload C:\Documents and Settings

□ PrivateKeyExportable

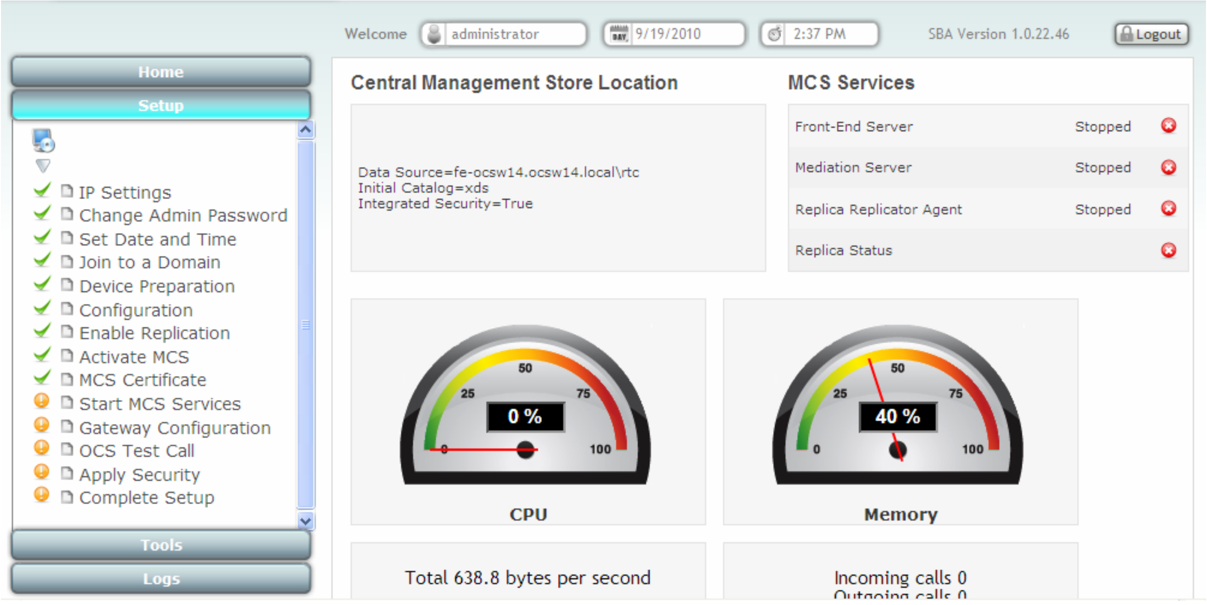
Password

✓ 3:13:06 PM MCS Certificate

```
VERBOSE: Creating new log file
"C:\Windows\TEMP\Import-
CsCertificate-2426c1f8-8e08-40e5-
84ce-4ae6035ded20.xml".
VERBOSE: Import the certificate
response. VERBOSE: Creating new
log file "C:\Windows\TEMP\Import-
CsCertificate-2426c1f8-8e08-40e5-
84ce-4ae6035ded20.html".
VERBOSE: "Import-CsCertificate"
processing has completed
successfully. VERBOSE: Detailed
results can be found at
"C:\Windows\TEMP\Import-
```

A green check mark appears adjacent to the completed menu item.

Figure 7-54: MCS Certificate – Complete



Central Management Store Location

```
Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True
```

MCS Services

Front-End Server	Stopped	✗
Mediation Server	Stopped	✗
Replica Replicator Agent	Stopped	✗
Replica Status		✗

Total 638.8 bytes per second

Incoming calls 0
Outgoing calls 0

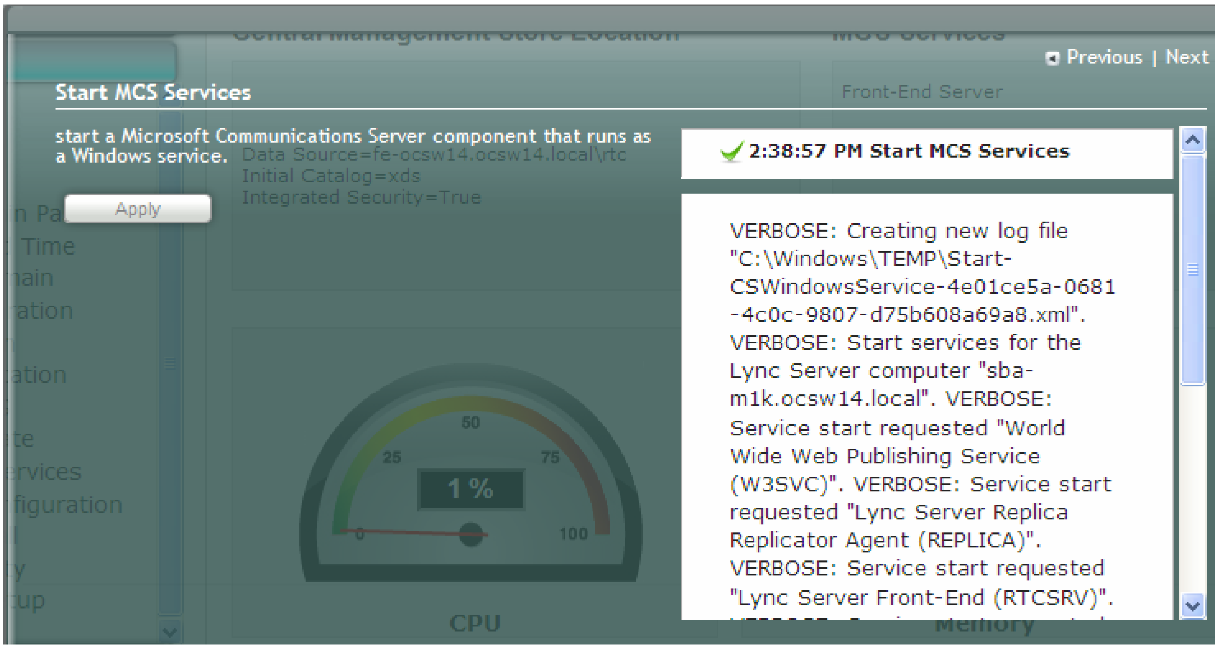
7.11 Step 11: Start MCS Services

The **Start MCS Services** option enables you to start a Lync Server 2010 (formerly, termed *Communications Server*) component that runs as a Windows service.

➢ **To start MCS services:**

1. Under the **Setup** menu, click the **Start MCS Services** option; the following screen appears:

Figure 7-55: Start MCS Services Screen



Start MCS Services

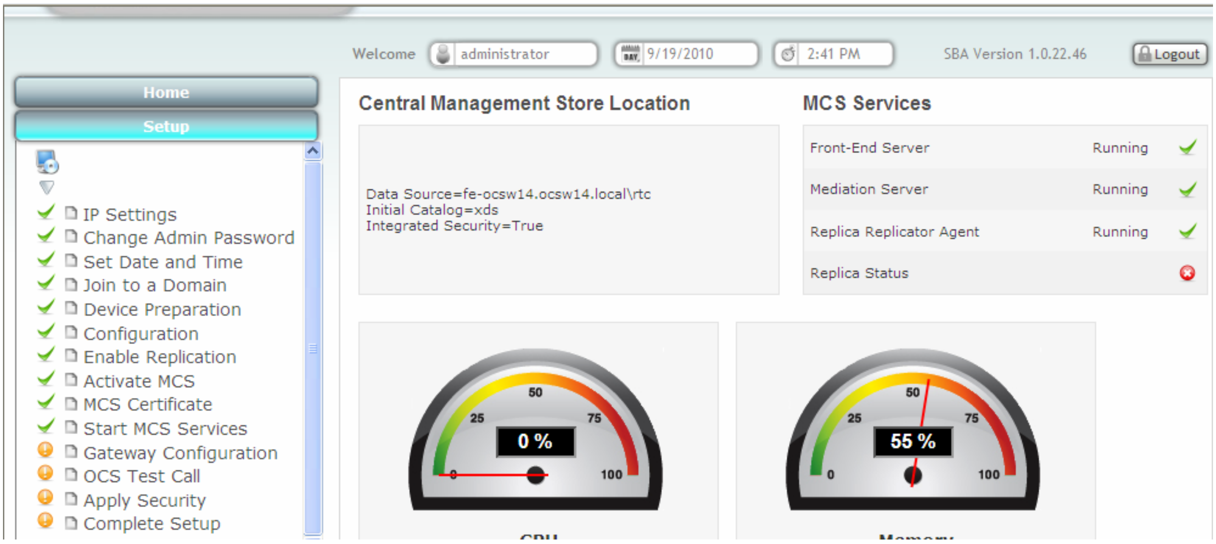
start a Microsoft Communications Server component that runs as a Windows service.

✓ 2:38:57 PM Start MCS Services

```
VERBOSE: Creating new log file
"C:\Windows\TEMP\Start-
CSWindowsService-4e01ce5a-0681
-4c0c-9807-d75b608a69a8.xml".
VERBOSE: Start services for the
Lync Server computer "sba-
m1k.ocsw14.local". VERBOSE:
Service start requested "World
Wide Web Publishing Service
(W3SVC)". VERBOSE: Service start
requested "Lync Server Replica
Replicator Agent (REPLICA)".
VERBOSE: Service start requested
"Lync Server Front-End (RTCSRV)".
```

2. Click **Apply** to start the services as per the MCS configuration settings; a green check mark appears alongside the **Start MCS Services** option under the **Setup** menu, as shown below:

Figure 7-56: Start MCS Services – Completed Successfully



Welcome administrator 9/19/2010 2:41 PM SBA Version 1.0.22.46

- ✓ IP Settings
- ✓ Change Admin Password
- ✓ Set Date and Time
- ✓ Join to a Domain
- ✓ Device Preparation
- ✓ Configuration
- ✓ Enable Replication
- ✓ Activate MCS
- ✓ MCS Certificate
- ✓ Start MCS Services
- ● Gateway Configuration
- ● OCS Test Call
- ● Apply Security
- ● Complete Setup

Central Management Store Location

Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True

MCS Services

Front-End Server	Running	✓
Mediation Server	Running	✓
Replica Replicator Agent	Running	✓
Replica Status		✗

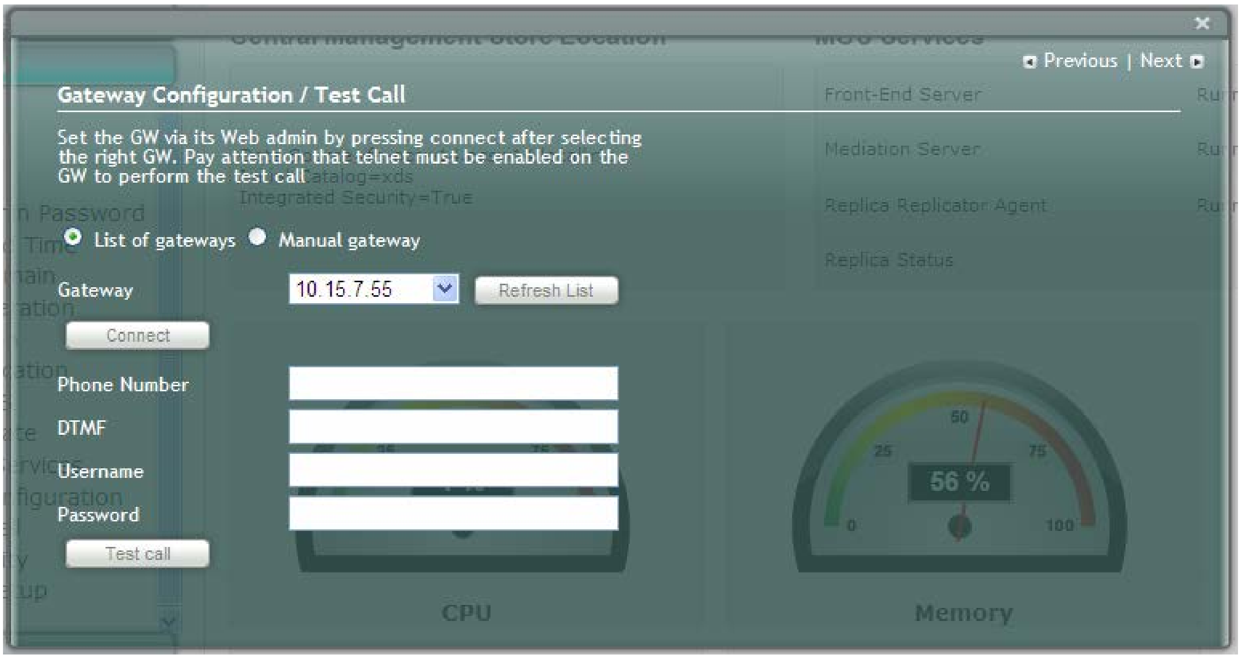
7.12 Step 12: Gateway Configuration

The **Gateway Configuration** option connects you to the Web-based interface of the PSTN gateway functionality of Mediant 800 SBA.

➢ **To configure the gateway:**

1. Under the **Setup** menu, click the **Gateway Configuration** option; the following screen appears:

Figure 7-57: Gateway Configuration Screen



Gateway Configuration / Test Call

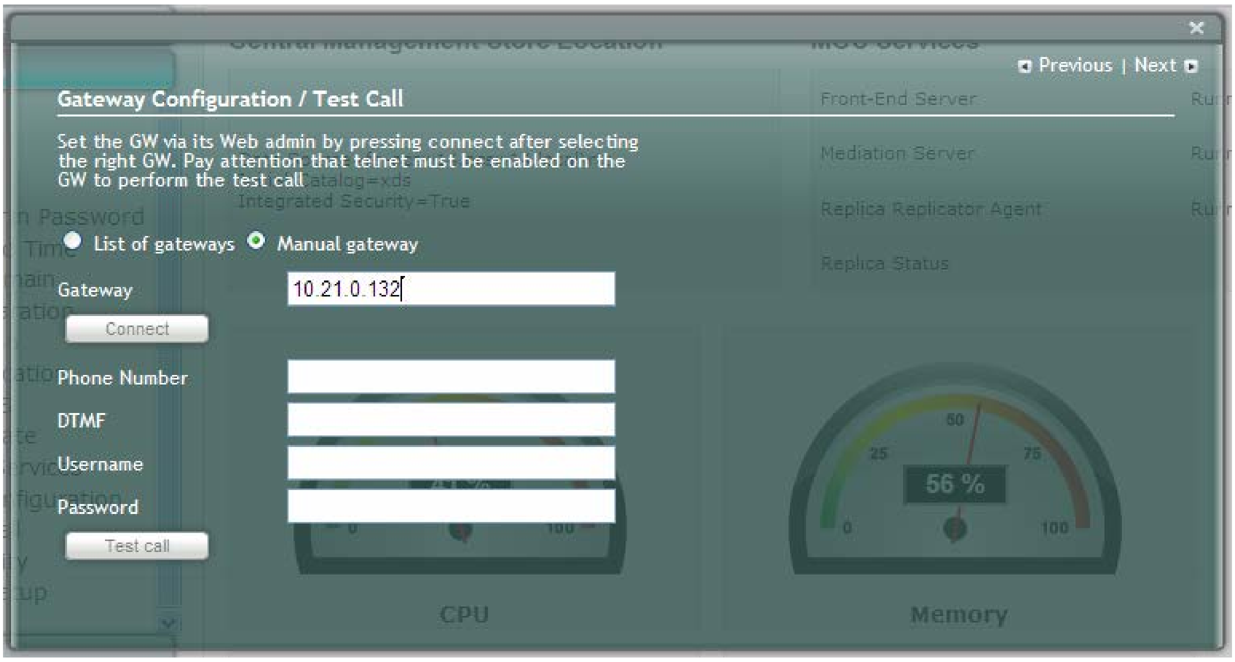
Set the GW via its Web admin by pressing connect after selecting the right GW. Pay attention that telnet must be enabled on the GW to perform the test call

● List of gateways ○ Manual gateway

Gateway: 10.15.7.55

2. Select the **Manual Gateway** option and then in the ‘Gateway’ field, enter the IP address or DNS name as shown below:

Figure 7-58: Gateway Configuration – Manual Gateway



Gateway Configuration / Test Call

Set the GW via its Web admin by pressing connect after selecting the right GW. Pay attention that telnet must be enabled on the GW to perform the test call

○ List of gateways ● Manual gateway

Gateway: 10.21.0.132

Phone Number:

DTMF:

Username:

Password:

3. Click **Connect**.

4. Configure the PSTN gateway as described in Section 8 on page 83.

8 Configuring the PSTN Gateway

This section provides step-by-step procedures for configuring the PSTN gateway functionality of the Mediant 800 SBA located at the branch office. In addition to connecting the SBA gateway to PBX\PSTN using E1/T1, this configuration also includes an embedded FXS port for analog devices. The configuration is performed through the embedded Web server (*Web interface*) of the PSTN gateway.

Note: Before configuring the PSTN gateway, ensure the following:

- The PSTN gateway is running SIP firmware version SIP_F6.40A.019.008 or later.
- The PSTN gateway must be installed with the following feature keys:
    - **MSFT** - enables working with Microsoft Lync
    - **IPSEC**, **MediaEncryption**, **StrongEncryption**, and **EncryptControlProtocol** - enable working with TLS
    - **SBC** - enables the SBC feature

8.1 Configuring the Mediation Server

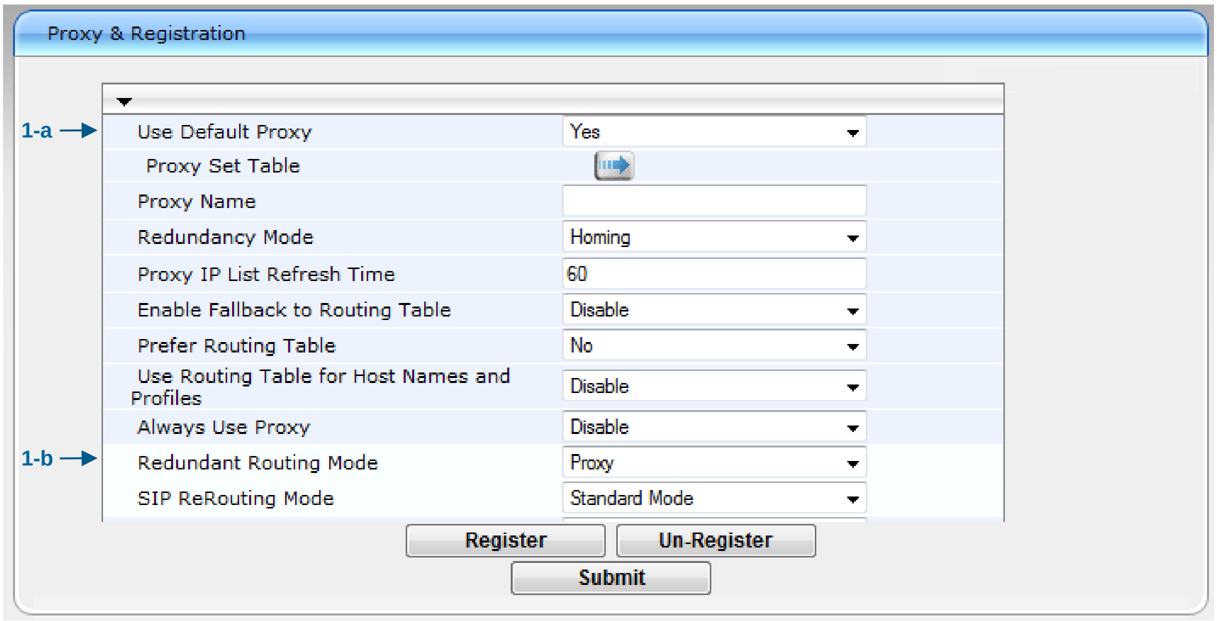
The procedure below describes how to configure the address (IP address or FQDN) of the Mediation Server through which the PSTN gateway communicates with Lync. The PSTN gateway forwards all telephone calls (PBX/PSTN and analog devices) to the Mediation Server using this configured address. The address is configured in the PSTN gateway as a proxy server. In other words, the Mediation Server acts as a proxy server (without registration) for the PSTN gateway.

If you have more than one Mediation Server in the cluster, proxy redundancy functionality can also be configured. If the Mediation Server running on the Mediant 800 SBA is unavailable (i.e., a SIP 503 is received in response to an INVITE), then the PSTN gateway re-sends the INVITE to the next Mediation Server (located at the datacenter).

➢ **To configure the Mediation Server:**

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

Figure 8-1: Proxy & Registration Page



Proxy & Registration

Use Default Proxy	Yes
Proxy Set Table	
Proxy Name	
Redundancy Mode	Homing
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Disable
Redundant Routing Mode	Proxy
SIP ReRouting Mode	Standard Mode

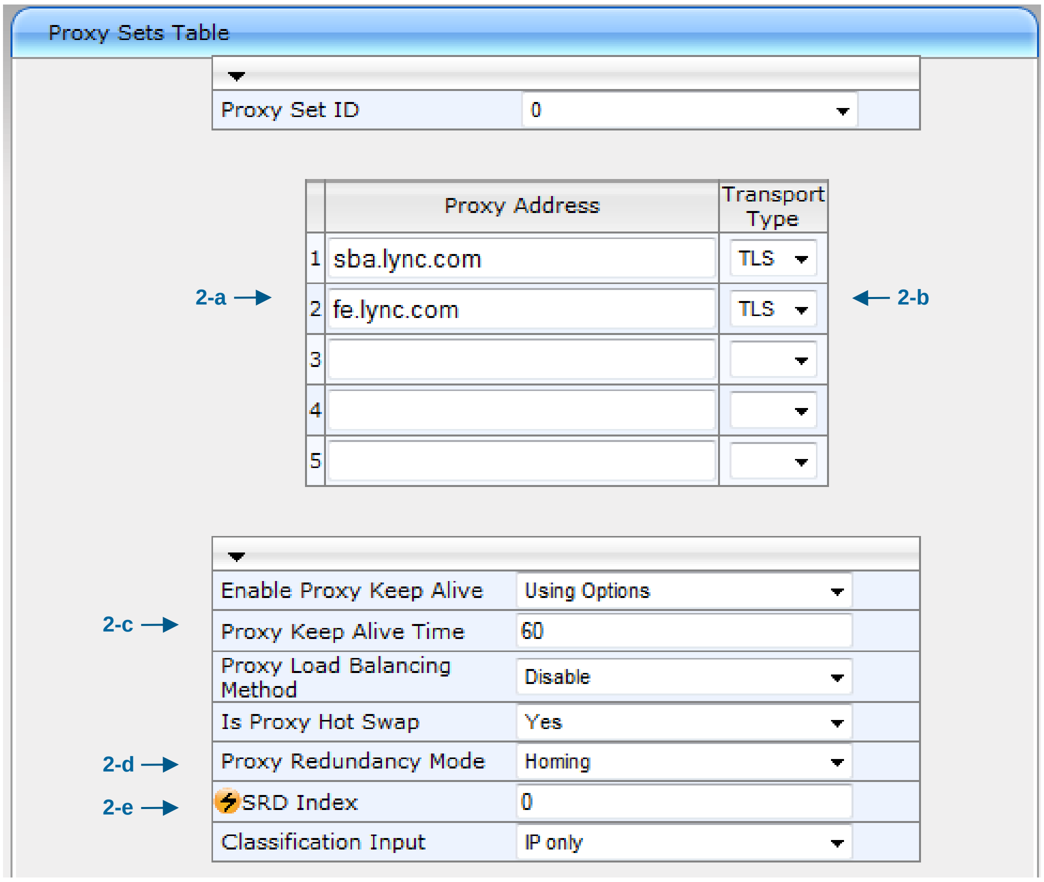
a. From the 'Use Default Proxy' drop-down list, select **Yes** to enable the Mediation Server to serve as a proxy server.

b. 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 Mediant 800 SBA), the PSTN gateway 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 Lync), see Step 3.

c. Click **Submit**.

2. Click the **Proxy Set Table** button to open the 'Proxy Sets Table' page:

Figure 8-2: Proxy Sets Table Page



Proxy Sets Table

Proxy Set ID	0

	Proxy Address	Transport Type
1	sba.lync.com	TLS
2	fe.lync.com	TLS
3		
4		
5		

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	Yes
Proxy Redundancy Mode	Homing
SRD Index	0
Classification Input	IP only

a. In the 'Proxy Address' fields, configure two proxy servers for redundancy. If the SBA application fails (at the branch office), the PSTN gateway switches over to the Mediation Server located at the datacenter.

- **Index 1:** IP address or FQDN of the Mediation Server running on the Mediant 800 SBA (configured in Section 8.3.1.4 on page 93).
- **Index 2:** IP address or FQDN of the Mediation Server running at the datacenter

Note: If you configured the Mediation Server address as an FQDN, ensure that you configure the DNS server (see Section 8.3.1.2 on page 92).

b. In the 'Transport Type' drop-down list, select the transport type (TLS or TCP) for these proxies. For more information on TLS and TCP transport type configuration, see Section 8.3 on page 90.

c. From the 'Enable Proxy Keep Alive' drop-down list, select **Using Options** to discover whether a particular Mediation Server in the cluster is available.

d. From the 'Is Proxy Hot Swap' drop-down list, select **Yes**. 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 Step 1 on page 83).

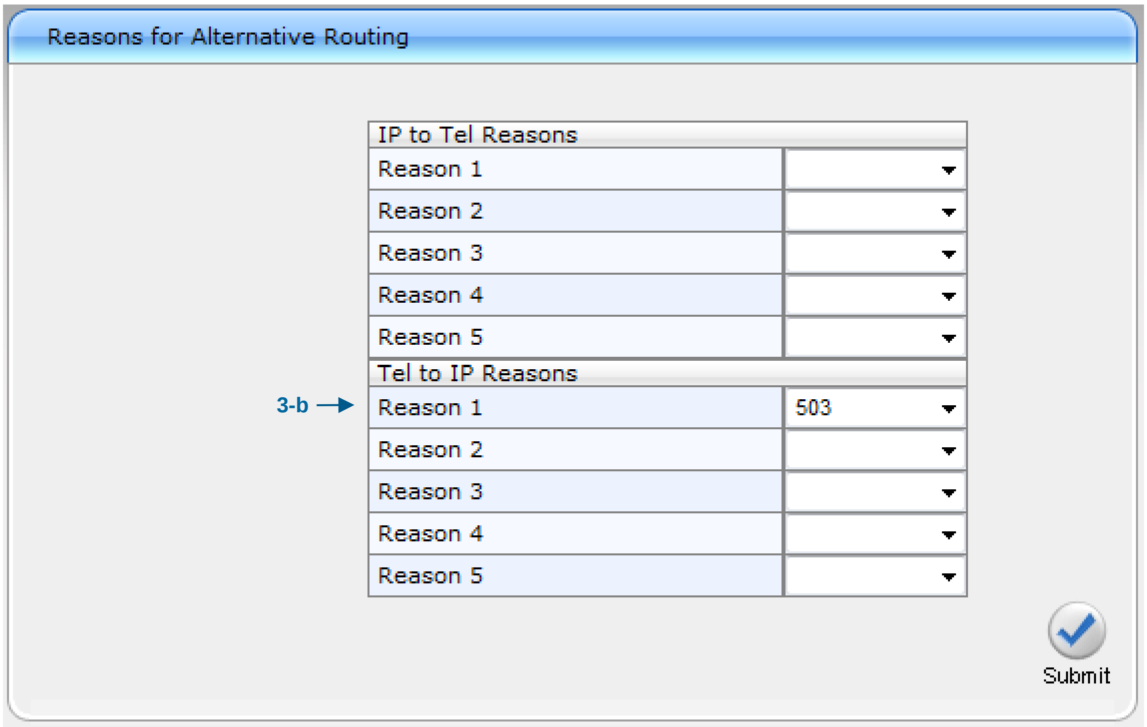
e. From the 'Proxy Redundancy Mode' drop-down list, select **Homing**. If the SBA application fails and the PSTN gateway switches over to the Mediation Server at the datacenter, then when the SBA application resumes functionality again, the PSTN gateway switches back to the Mediation Service on the SBA application.

f. Click **Submit** to apply your settings.

3. When the PSTN gateway receives a SIP 503 response from the Mediation Server in response to an INVITE, it re-sends the INVITE to the redundant Mediation Server (located at the datacenter). To achieve this, you need to configure the receipt of a SIP 503 response as a reason for IP alternative routing:

   a. Open the 'Reasons for Alternative Routing' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Routing** > **Alternative Routing Reasons**).

Figure 8-3: Reasons for Alternative Routing Page



Reasons for Alternative Routing

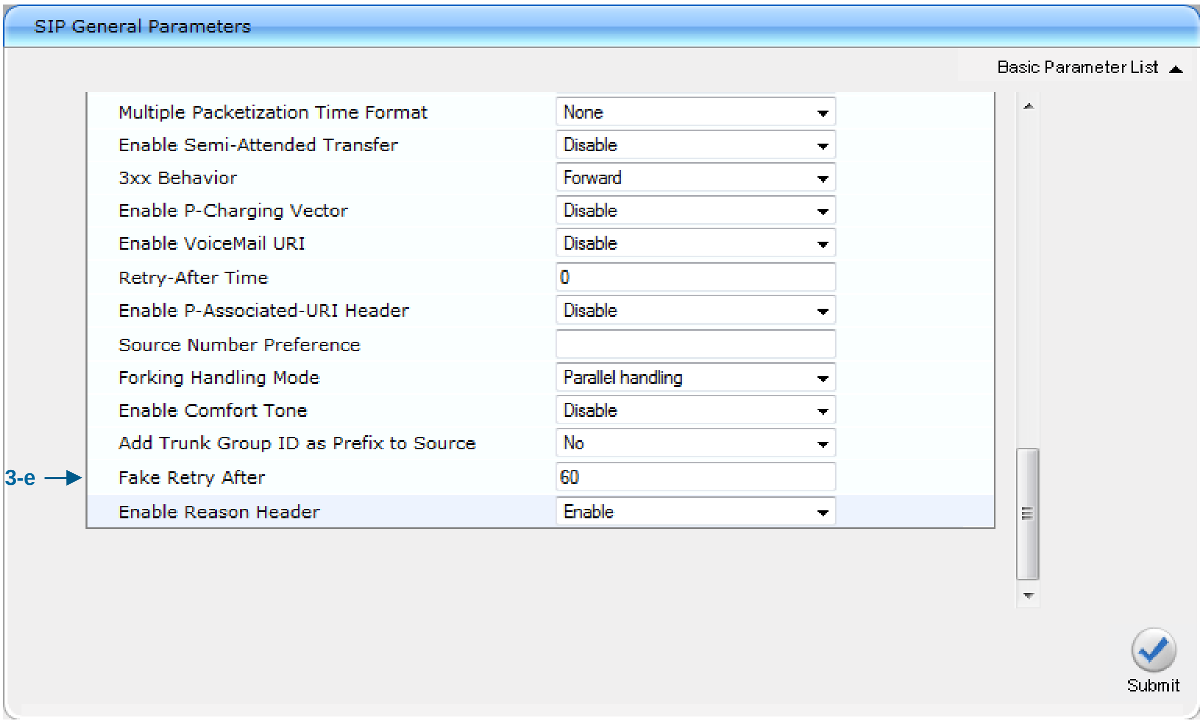
IP to Tel Reasons	
Reason 1	
Reason 2	
Reason 3	
Reason 4	
Reason 5	
Tel to IP Reasons	
Reason 1	503
Reason 2	
Reason 3	
Reason 4	
Reason 5	

   b. Under the **Tel to IP Reasons** group, from the 'Reason 1' drop-down list, select **503**.

   c. Click **Submit**.

   d. Open the 'SIP General Parameters' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** sub-menu > **General Parameters**).

Figure 8-4: SIP General Parameters Page



SIP General Parameters

Multiple Packetization Time Format	None
Enable Semi-Attended Transfer	Disable
3xx Behavior	Forward
Enable P-Charging Vector	Disable
Enable VoiceMail URI	Disable
Retry-After Time	0
Enable P-Associated-URI Header	Disable
Source Number Preference	
Forking Handling Mode	Parallel handling
Enable Comfort Tone	Disable
Add Trunk Group ID as Prefix to Source	No
Fake Retry After	60
Enable Reason Header	Enable

e. In ‘Fake Retry After’ field, enter the time '60' (in seconds). When the PSTN gateway receives a SIP 503 response (from the Mediation Server) without a Retry-After header, the PSTN gateway behaves as if the 503 response includes a Retry-After header with this user-defined period.

f. Click **Submit**.

g. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

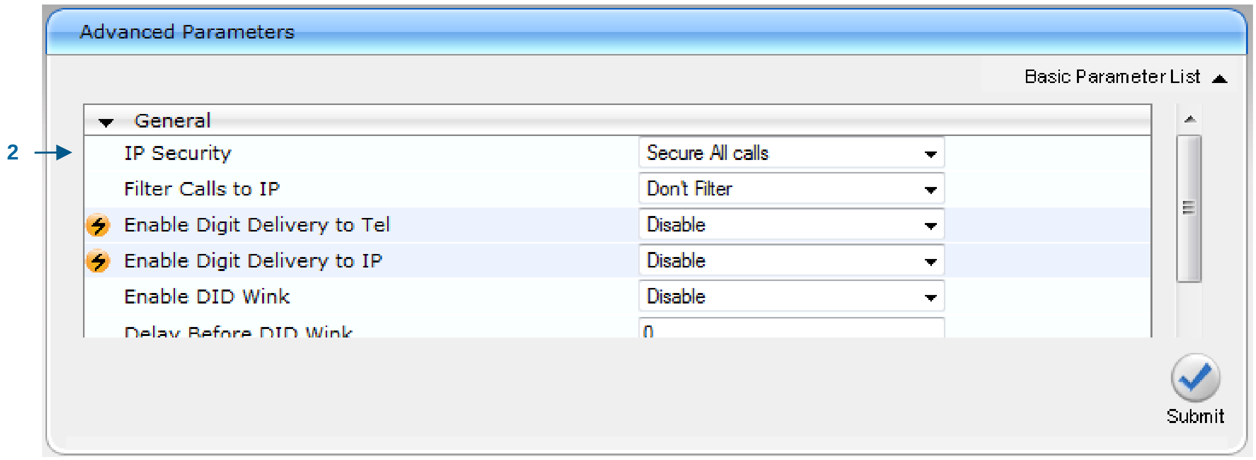
8.2 Restricting Communication to Mediation Server Only

The procedure below describes how to restrict IP communication, by allowing communication only between the PSTN gateway and the Mediation Server. This ensures that the PSTN gateway accepts and sends SIP calls **only** from and to the Mediation Server (as required by Microsoft). This is done by enabling the IP Security feature and then defining the allowed ("administrative" list) IP addresses (or FQDNs) in the Outbound IP Routing table.

➢ **To allow IP communication only between the PSTN gateway and Mediation Server:**

1. Open the 'Advanced Parameters' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** sub-menu > **Advanced Parameters**).

Figure 8-5: Advanced Parameters Page



Advanced Parameters

Basic Parameter List ▲

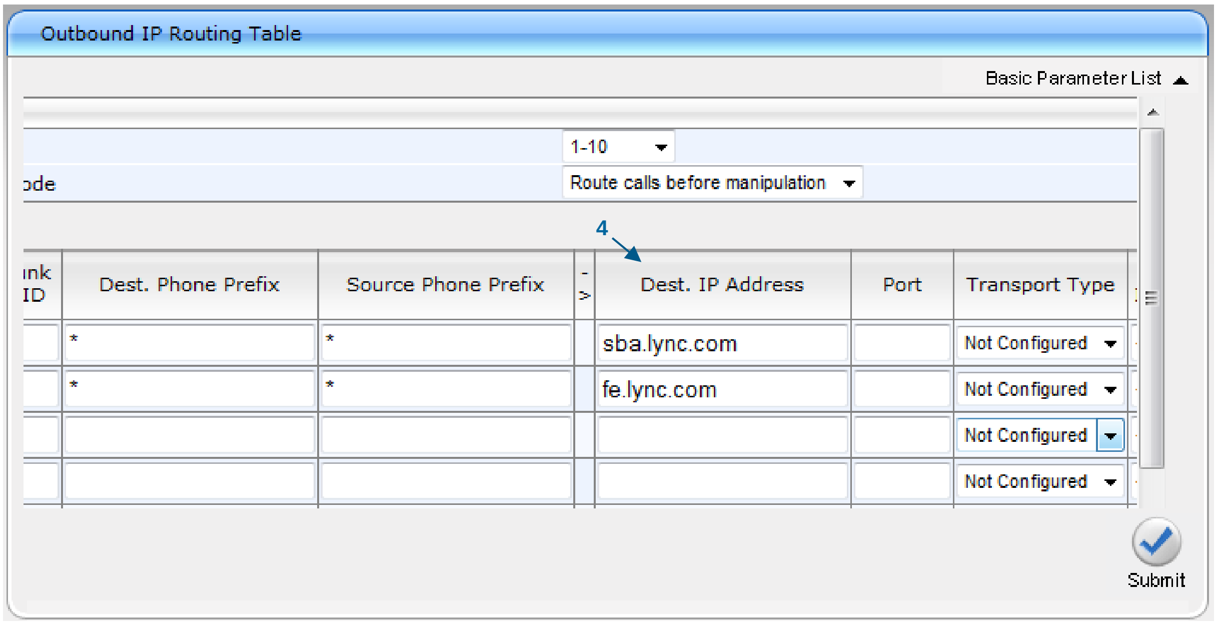
▼ General

IP Security	Secure All calls
Filter Calls to IP	Don't Filter
Enable Digit Delivery to Tel	Disable
Enable Digit Delivery to IP	Disable
Enable DID Wink	Disable
Delay Before DID Wink	0

2. From the 'IP Security' drop-down list, select **Secure All calls** to enable the security feature to accept and send SIP calls only from and to user-defined IP addresses (i.e., Mediation Server) configured in the 'Outbound Routing' table (see step below) In the event where you already have defined an IP address or FQDN in the Proxy Set table (see Section 8.1 on page 83), you do not need to proceed to the step below.

3. Open the 'Outbound IP Routing Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Routing** > **Tel to IP Routing**).

Figure 8-6: Outbound IP Routing Table



Outbound IP Routing Table

Basic Parameter List

1-10

ode Route calls before manipulation

nk ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Port	Transport Type
	*	*		sba.lync.com		Not Configured
	*	*		fe.lync.com		Not Configured
						Not Configured
						Not Configured

Note: The setting in the ‘Outbound Routing’ table concerns security only, and does not represent a routing rule.

4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.3 Configuring the SIP Transport Type

The following SIP transport types can be employed for communication between the PSTN gateway and the Mediation Server:

- **Transport Layer Security (TLS)** – enabled by default (and recommended) - see Section 8.3.1 on page 90.
- **Transmission Control Protocol (TCP)** – see Section 8.3.2 on page 100.

8.3.1 Configuring TLS

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

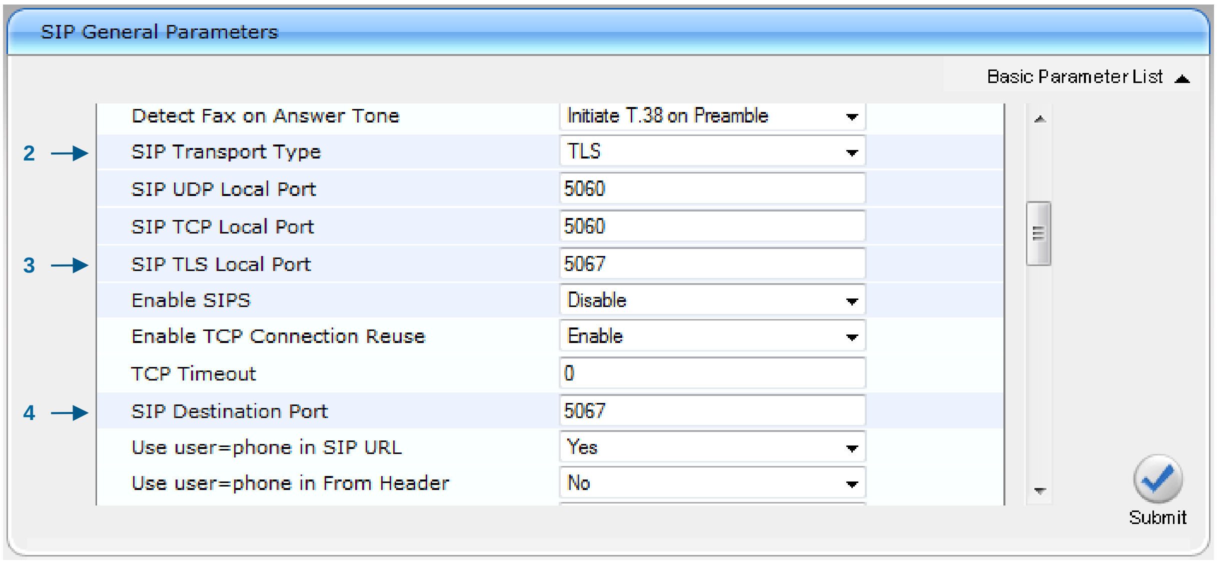
8.3.1.1 Step 1: Enable TLS and Define TLS Port

The procedure below describes how to enable TLS and configure the PSTN gateway ports used for TLS.

➢ **To enable TLS and configure TLS ports:**

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

Figure 8-7: SIP General Parameters Page



Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	TLS
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5067
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5067
Use user=phone in SIP URL	Yes
Use user=phone in From Header	No

2. From the 'SIP Transport Type' drop-down list, select **TLS**.
3. In the 'SIP TLS Local Port', enter '5067'. This port corresponds to the Mediation Server TLS transmitting port configuration.
4. In the 'SIP Destination Port', enter '5067'. This port corresponds to the Mediation Server TLS listening port configuration.
5. Click **Submit** to apply your settings.
6. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

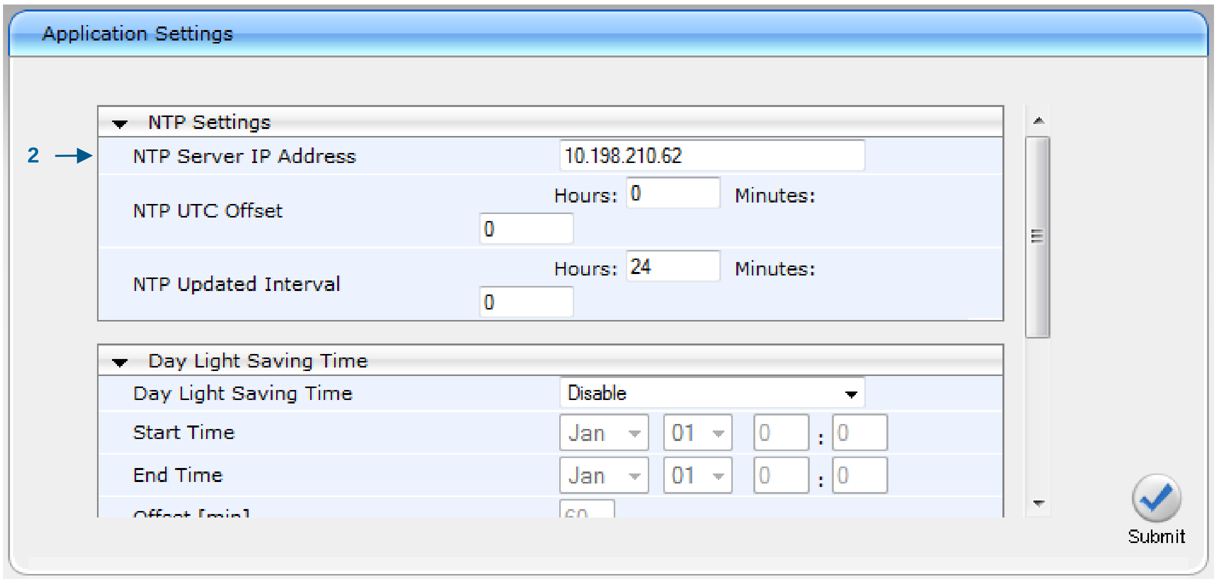
8.3.1.2 Step 2: Configure the NTP Server

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, by synchronizing it with a third-party NTP server. This ensures that the PSTN gateway has the same date and time as the Certification Authority (CA), discussed later in Section 8.3.1 on page 90.

➢ **To configure the NTP server:**

1. Open the 'Application Settings' page (**Configuration** tab > **System** menu > **Application Settings**).

Figure 8-8: Application Settings Page



Application Settings

NTP Settings

NTP Server IP Address: 10.198.210.62

NTP UTC Offset: Hours: 0 Minutes: 0

NTP Updated Interval: Hours: 24 Minutes: 0

Day Light Saving Time

Day Light Saving Time: Disable

Start Time: Jan 01 0 : 0

End Time: Jan 01 0 : 0

Offset [min]: 60

2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server.
3. Click **Submit** to apply your changes.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

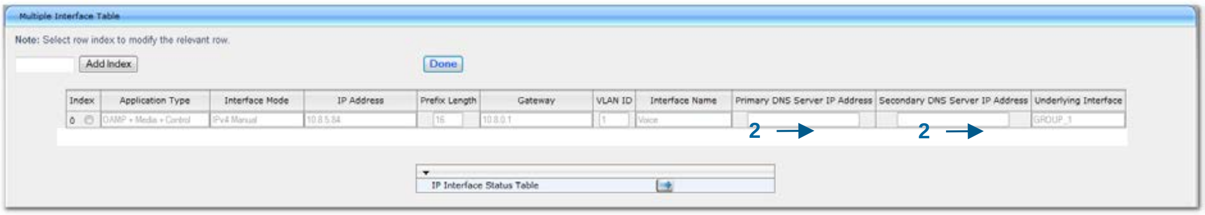
8.3.1.3 Step 3: Configure the DNS Server

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 ‘IP Settings’ page (**Configuration** tab > **VoIP** menu > **Network** sub-menu > **IP Settings**).

Figure 8-9: DNS Server Settings



Multiple Interface Table

Note: Select row index to modify the relevant row.

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0	OAMP + Media + Control	IPv4 Manual	10.8.5.84	16	10.8.0.1	1	Voice			GROUP_1

2. In the 'DNS Primary Server IP' and 'DNS Secondary Server IP' fields, enter the IP address of the primary and secondary DNS server, respectively.
3. Click **Submit** to apply your changes.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

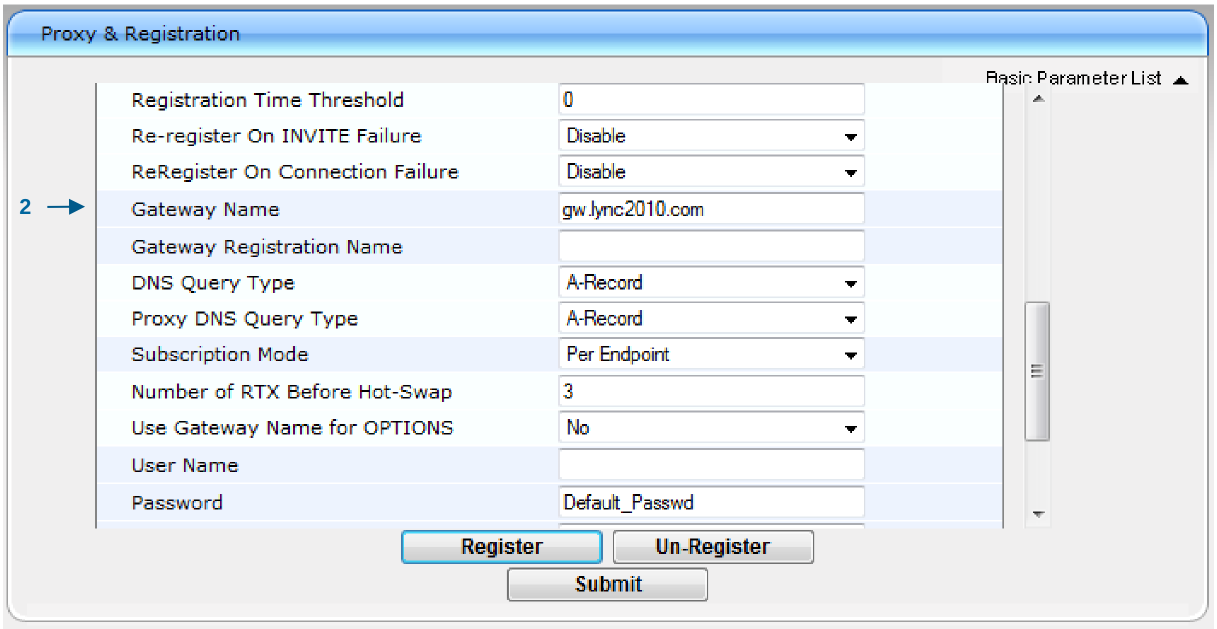
8.3.1.4 Step 4: Configure the Gateway Name

The procedure below describes how to configure the host name for the PSTN gateway. This appears as the URI host name in the SIP From header in INVITE messages sent by the PSTN gateway to the Mediation Server. This allows the Mediation Server to identify the PSTN gateway (if required), when using certificates for TLS (see Section 8.3.1.5.1 on page 94).

➢ **To configure the SIP gateway name:**

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

Figure 8-10: Proxy & Registration Page



Proxy & Registration

Basic Parameter List

Registration Time Threshold	0
Re-register On INVITE Failure	Disable
ReRegister On Connection Failure	Disable
Gateway Name	gw.lync2010.com
Gateway Registration Name	
DNS Query Type	A-Record
Proxy DNS Query Type	A-Record
Subscription Mode	Per Endpoint
Number of RTX Before Hot-Swap	3
Use Gateway Name for OPTIONS	No
User Name	
Password	Default_Passwd

2. In the 'Gateway Name' field, assign a unique FQDN name to the PSTN gateway within the domain, for example,'gw.lync2010.com'.This name is identical to the name that is configured in the Lync topology builder (see Section 5.2.1 on page 31)
3. Click **Submit** to apply your settings.

8.3.1.5 Step 5: Configure a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). It is composed of the following steps:

1. Generating a certificate signing request (CSR)
2. Obtaining CA and Trusted Root certificates from Microsoft
3. Installing Microsoft CA and Trusted Root certificates on the PSTN gateway

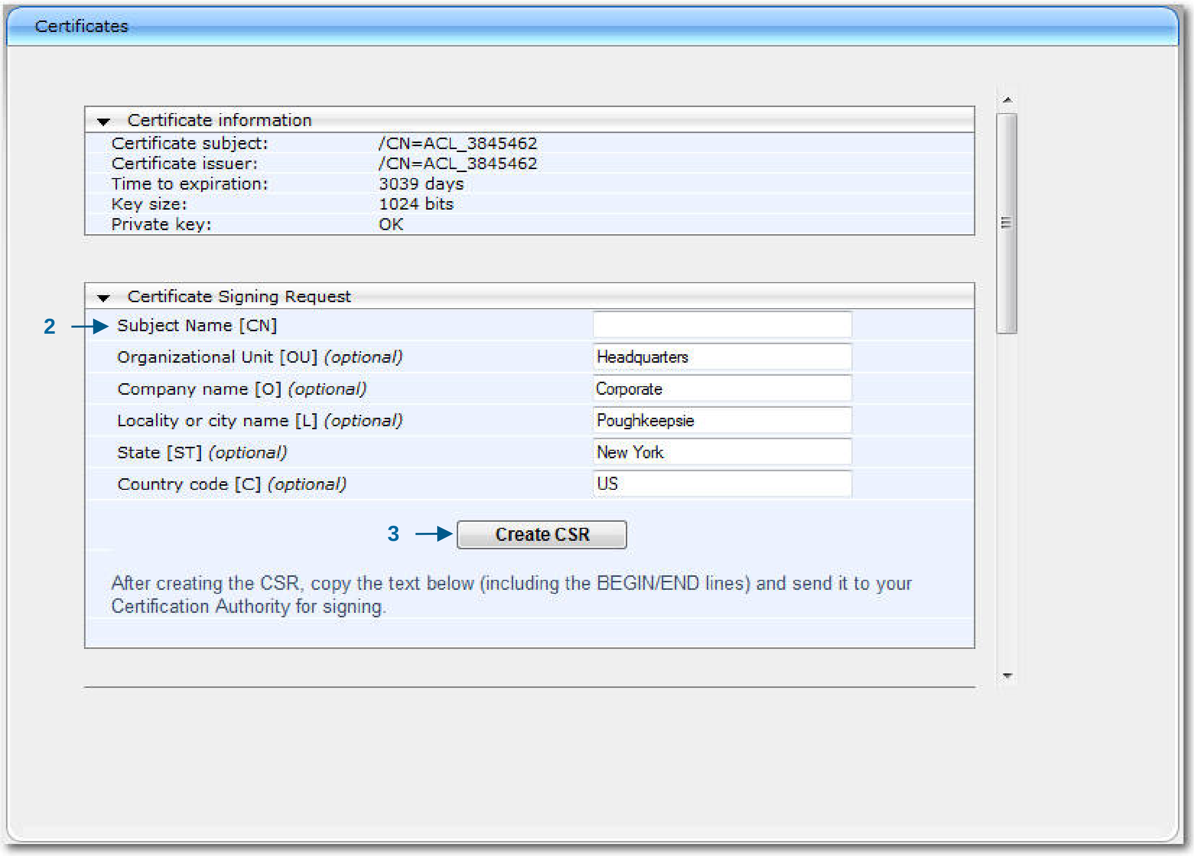
8.3.1.5.1 Generate a Certificate Signing Request

The procedure below describes how to generate a CSR by the PSTN gateway. This CSR is later sent to Microsoft CA.

➢ **To generate a CSR:**

1. Open the 'Certificates Signing Request' page (**Configuration** tab > **System** menu > **Certificates**).

Figure 8-11: Certificates Page



Certificates

▼ Certificate information

Certificate subject:	/CN=ACL_3845462
Certificate issuer:	/CN=ACL_3845462
Time to expiration:	3039 days
Key size:	1024 bits
Private key:	OK

▼ Certificate Signing Request

Subject Name [CN]	
Organizational Unit [OU] *(optional)*	Headquarters
Company name [O] *(optional)*	Corporate
Locality or city name [L] *(optional)*	Poughkeepsie
State [ST] *(optional)*	New York
Country code [C] *(optional)*	US

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

2. In the 'Subject Name' field, enter the SIP URI host name that you configured for the PSTN gateway in Section 8.3.1.4 on page 93.
3. Click **Create CSR**; a Certificate request is generated and displayed on the page.
4. Copy the certificate 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 PC with the file name *certreq.txt*.

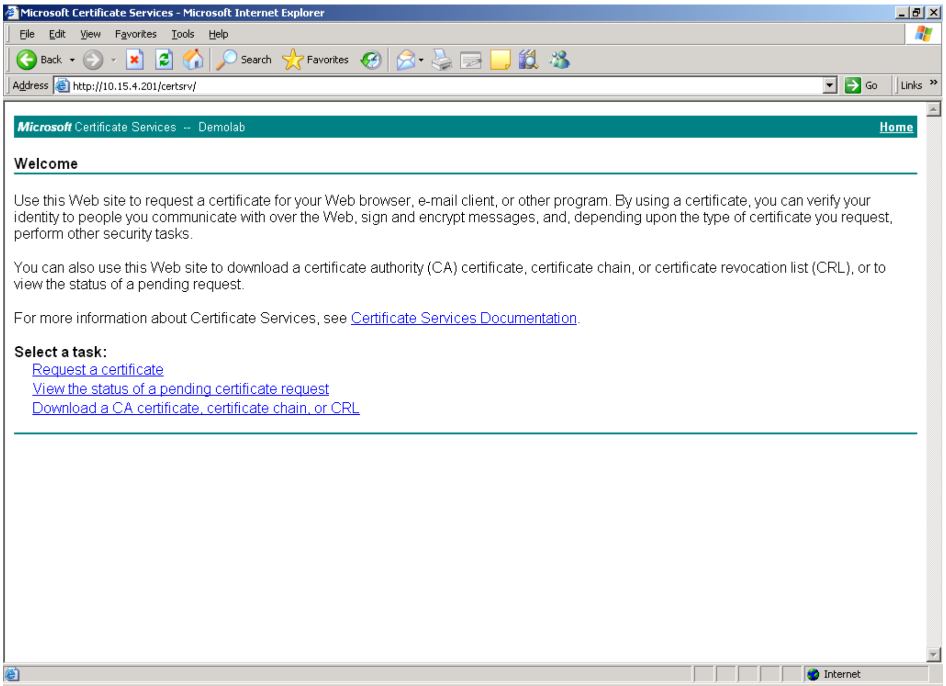
8.3.1.5.2 Obtain Microsoft CA and Trusted Root Certificates

Once you have generated a CSR (described in the previous section), you need to upload it to Microsoft Certificate server and request a CA and trusted root certificates.

➢ **To obtain Microsoft CA and trusted root certificates:**

1. Open a Web browser and then navigate to Microsoft Certificate Services at **http://< certificate server address >/certsrv**.

Figure 8-12: Microsoft Certificate Services Web Page


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.15.4.201/certsrv/
Go Links
Internet

Microsoft Certificate Services -- Demolab Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

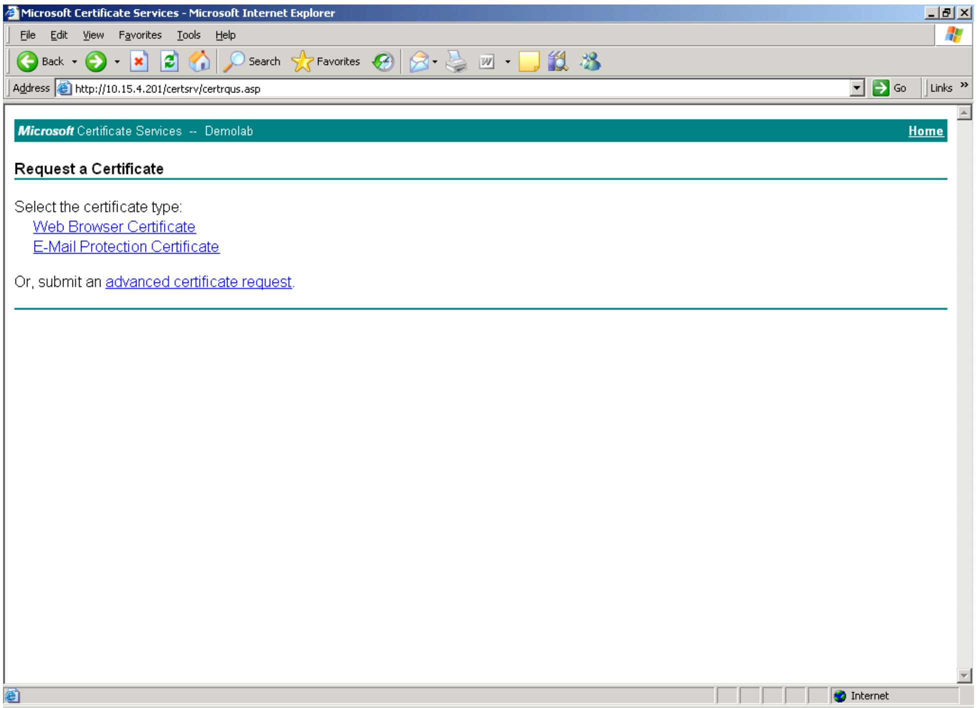
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

2. Click the **Request a certificate** link; the Request a Certificate page appears:

Figure 8-13: Request a Certificate Page


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://10.15.4.201/certsrv/certrqus.asp
Go
Links
Microsoft Certificate Services -- Demolab
Home
Internet

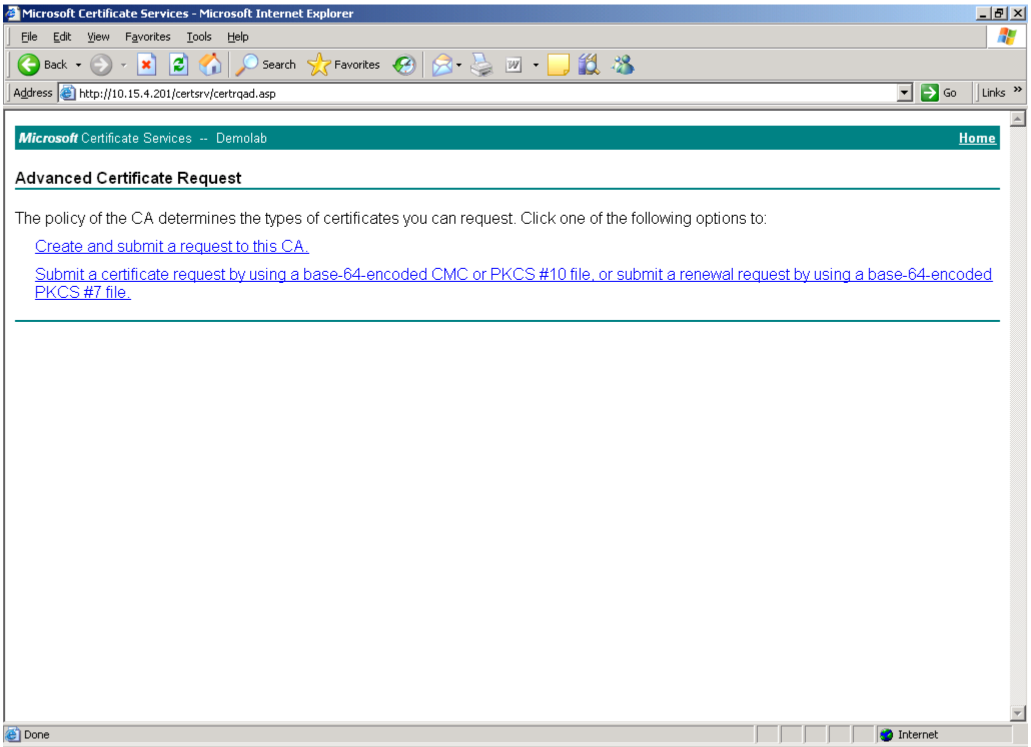
Request a Certificate

Select the certificate type:
Web Browser Certificate
E-Mail Protection Certificate

Or, submit an advanced certificate request.

3. Click the **advanced certificate request** link; the Advanced Certificate Request page appears:

Figure 8-14: Advanced Certificate Request Page


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://10.15.4.201/certsrv/certrqad.asp
Go
Links
Microsoft Certificate Services -- Demolab
Home
Done
Internet

Advanced Certificate Request

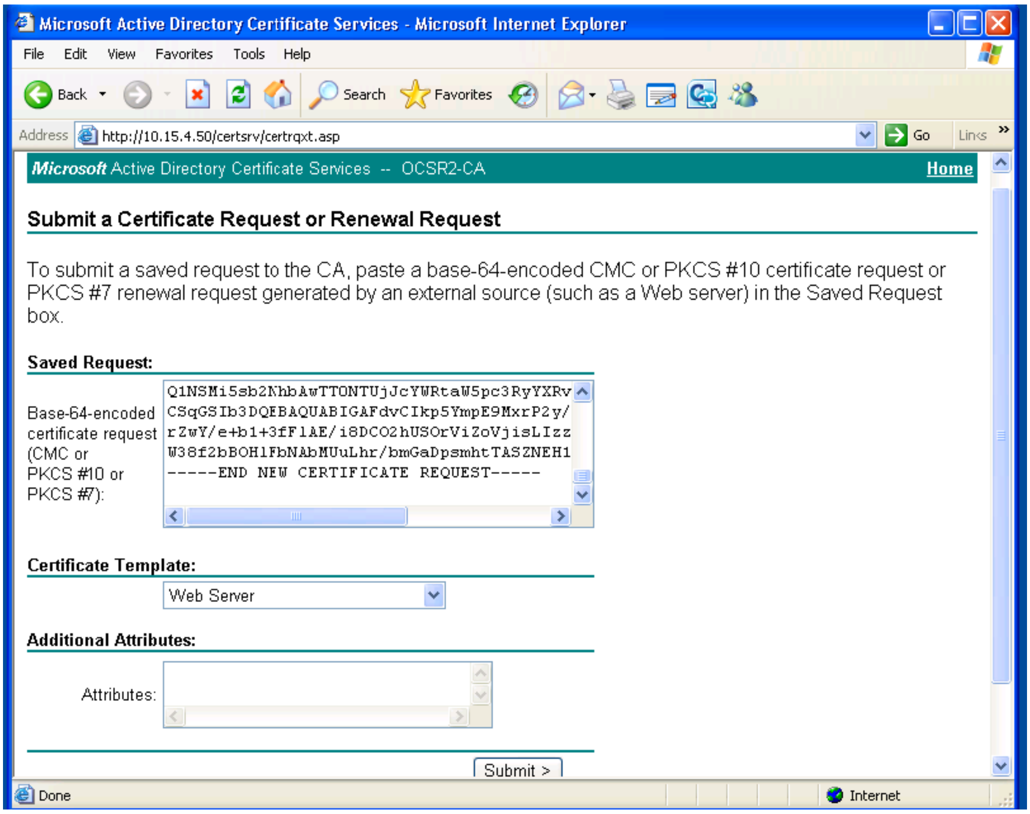
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

4. Click the **Submit a Certificate request by using base-64-encoded...** link; the Submit a Certificate Request or Renewal Request page appears:

Figure 8-15: Submit a Certificate Request or Renewal Request Page


Microsoft Active Directory Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://10.15.4.50/certsrv/certrqxt.asp
Go
Links
Microsoft Active Directory Certificate Services -- OCSR2-CA
Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
Q1NSMi5sb2NhbAwTTONTUjJcYWRtaW5pc3RyYXRv
CSqGSIb3DQEBAQUABIGAFdvCIkp5YmpE9MxrP2y/
rZwY/e+b1+3fFlAE/i8DCO2hUSOrViZoVjisLIzz
W38f2bBOHlFbNAbMUuLhr/bmGaDpsmhtTASZNEH1
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

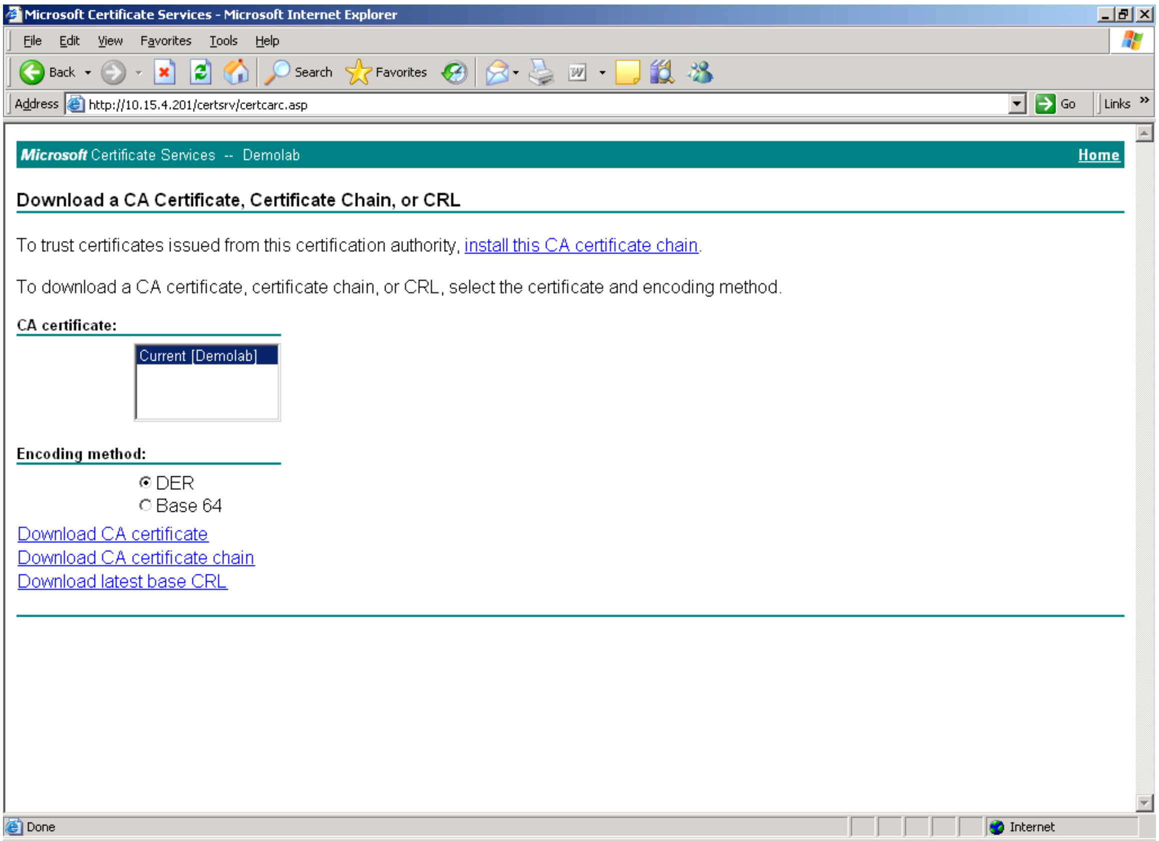
Web Server

Additional Attributes:

Attributes:

5. Open the CSR file (*certreq.txt*) that you created and saved in Section 8.3.1.5.1 on page 94, and then copy its contents to the **Saved Request** text box.
6. From the **Certificate Template** drop-down list, select “Web Server”.
7. Click **Submit**.
8. Select the **Base 64** encoding option.
9. Click the **Download CA certificate** link, and then save the file with the name, *gateway.cer* in a folder on your PC.
10. Navigate once again to the certificate server at **http://< certificate server address >/certsrv**.
11. Click the **Download a CA certificate**, **certificate chain or CRL** link; the Download a CA Certificate, Certificate Chain, or CRL page appears:

Figure 8-16: Download a CA Certificate, Certificate Chain, or CRL Page



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.15.4.201/certsrv/certcarc.asp
Go Links
Microsoft Certificate Services -- Demolab
Home
Done
Internet

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Demolab]

Encoding method:

● DER
○ Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL

12. Under the **Encoding method** group, select the **Base 64** option.
13. Click the **Download CA certificate** link, and then save the file with the name *certroot.cer* in a folder on your PC.

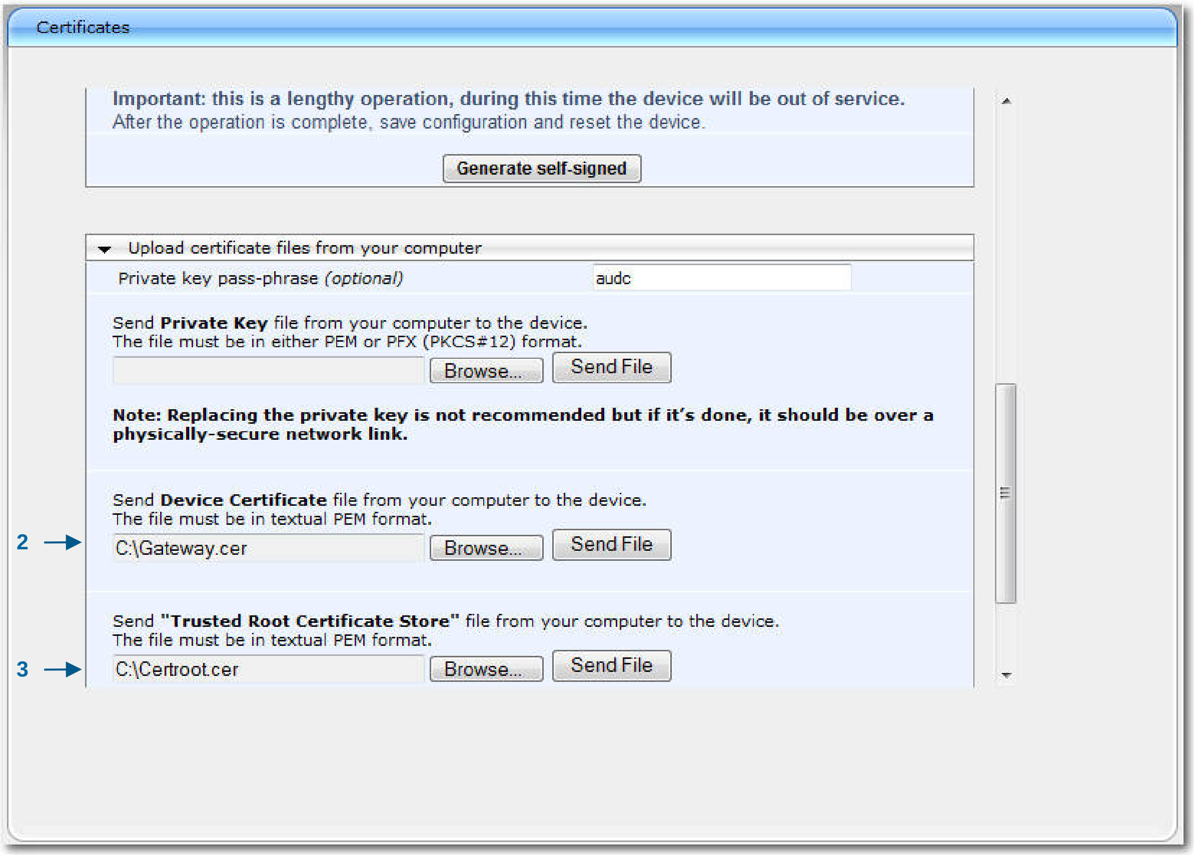
8.3.1.5.3 Load Microsoft CA and Trusted Root Certificates to PSTN Gateway

Once you have obtained the CA and trusted root certificates from Microsoft, you need to load these two certificates to the PSTN gateway.

➢ **To load certificates to the PSTN gateway:**

1. Open the 'Certificates Signing Request' page (**Configuration** tab > **System** menu > **Certificates**).

Figure 8-17: Certificates Page



Certificates

Important: this is a lengthy operation, during this time the device will be out of service.
After the operation is complete, save configuration and reset the device.

▾ Upload certificate files from your computer

Private key pass-phrase *(optional)*: audc

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

2 → C:\Gateway.cer

Send **"Trusted Root Certificate Store"** file from your computer to the device.
The file must be in textual PEM format.

3 → C:\Certroot.cer

2. In the 'Device Certificate' field, click **Browse**, select the *gateway.cer* certificate file that you saved on your local disk (see Step 9 in the previous section), and then click **Send File** to upload the certificate to the PSTN gateway.
3. In the 'Trusted Root Certificate Store' field, click **Browse** to select the *certroot.cer* certificate file that you saved on your local disk (see Step 13 in the previous section), and then click **Send File** to upload the certificate.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.3.2 Configuring TCP Transport Type

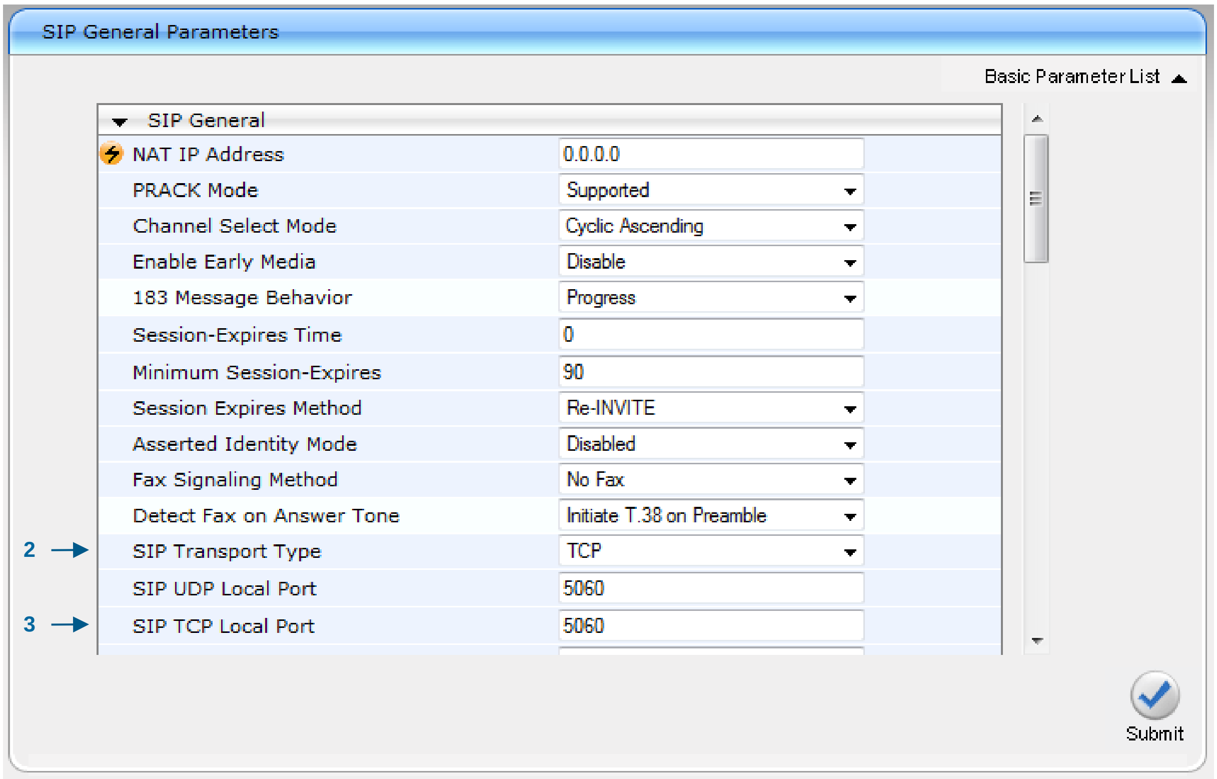
TCP provides unencrypted SIP signaling between the PSTN gateway and Mediation Server. The procedure below describes how to configure the SIP TCP transport type.

Note: Microsoft does not recommend implementing TCP for the SIP transport type between the PSTN gateway and the Mediation Server.

➢ **To set SIP transport type to TCP:**

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

Figure 8-18: SIP General Parameters Page



NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Disable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	No Fax
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	TCP
SIP UDP Local Port	5060
SIP TCP Local Port	5060

2. From the 'SIP Transport Type' drop-down list, select **TCP**.
3. In the 'SIP TCP Local Port' field, enter the same listening TCP port number as was configured on the Topology Builder for the gateway.
4. Click **Submit** to apply your changes.
5. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.4 Configuring Secure Real-Time Transport Protocol

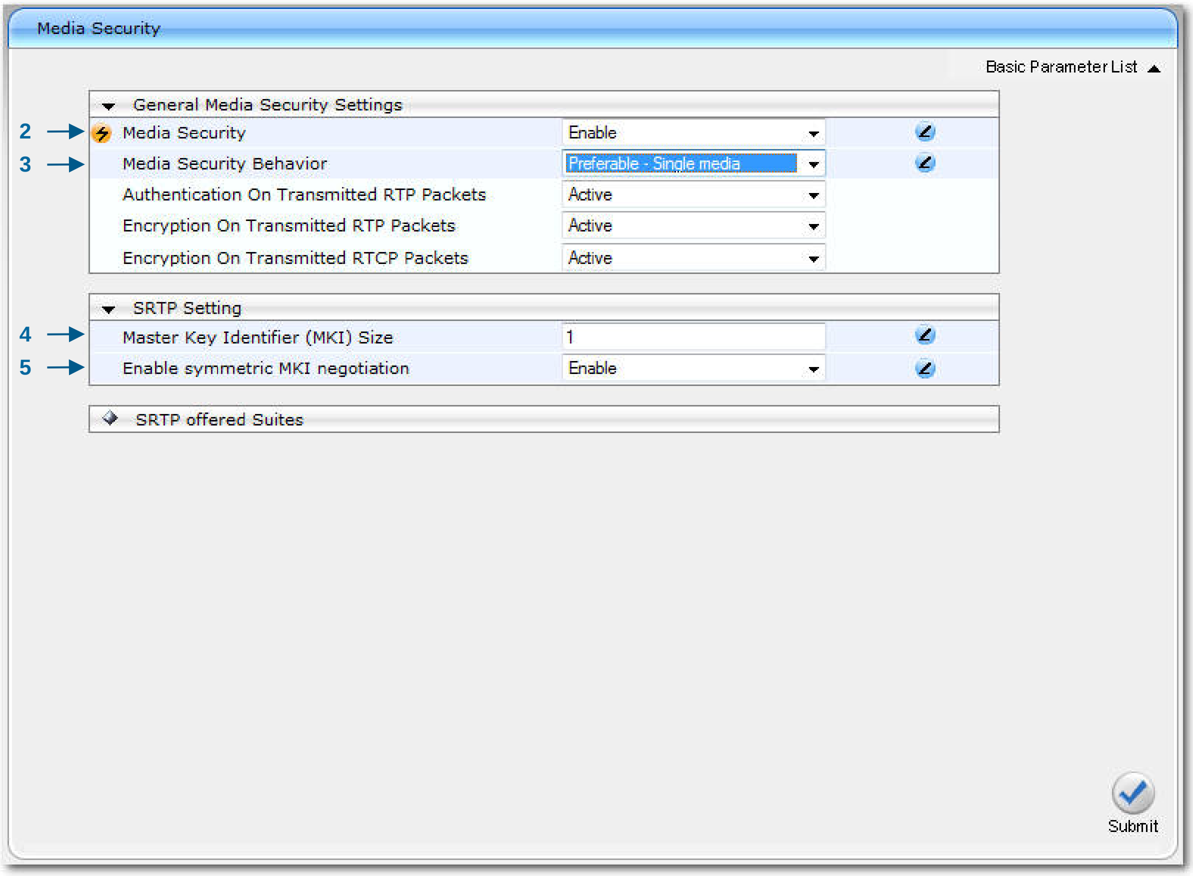
If you configure TLS as the SIP transport type between the PSTN gateway and Mediation Server, you must enable Secure RTP (SRTP) encryption and set its mode of operation to one of the following (and that which matches the SRTP supported at the Mediation Server):

- **Preferable** (default)**:** The PSTN gateway initiates encrypted calls. However, if negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted.
- **Mandatory:** The PSTN gateway initiates encrypted calls, but if negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected.
- **Preferable - Single Media:** The PSTN gateway sends SDP with a single media ('m=') line only (e.g., m=audio 6000 RTP/AVP 4 0 70 96) with RTP/AVP and crypto keys. The remote SIP user agent (UA) can respond with SRTP or RTP parameters:
    - If the remote SIP UA does not support SRTP, it uses RTP and ignores the crypto lines.
    - If the PSTN gateway receives an SDP offer with a single media, it responds with SRTP (RTP/SAVP) if the 'Media Security' parameter is set to 'Enable'. If SRTP is not supported (i.e., 'Media Security' is set to 'Disabled'), it responds with RTP.

➢ **To configure SRTP:**

1. Open the 'Media Security' page (**Configuration** tab > **VoIP** menu > **Media** sub-menu > **Media Security**).

Figure 8-19: Media Security Page



Media Security

Basic Parameter List ▲

General Media Security Settings

Media Security	Enable
Media Security Behavior	Preferable - Single media
Authentication On Transmitted RTP Packets	Active
Encryption On Transmitted RTP Packets	Active
Encryption On Transmitted RTCP Packets	Active

SRTP Setting

Master Key Identifier (MKI) Size	1
Enable symmetric MKI negotiation	Enable

SRTP offered Suites

2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. From the 'Media Security Behavior' drop-down list, select one of the following:
   - **Mandatory** if the Mediation Server is configured to SRTP “Required”.
   - **Preferable-Single media** if the Mediation server is configured to SRTP Optional.
4. In the 'Master Key Identifier (MKI) Size' field, enter '1'. This configures the size (in bytes) of the MKI in SRTP Tx packets.
5. From the 'Enable Symmetric MKI Negotiation' drop-down list, select **Enable**.
6. Click **Submit** to apply your changes.
7. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.
8. 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 800 resets and your settings are saved to the flash memory.

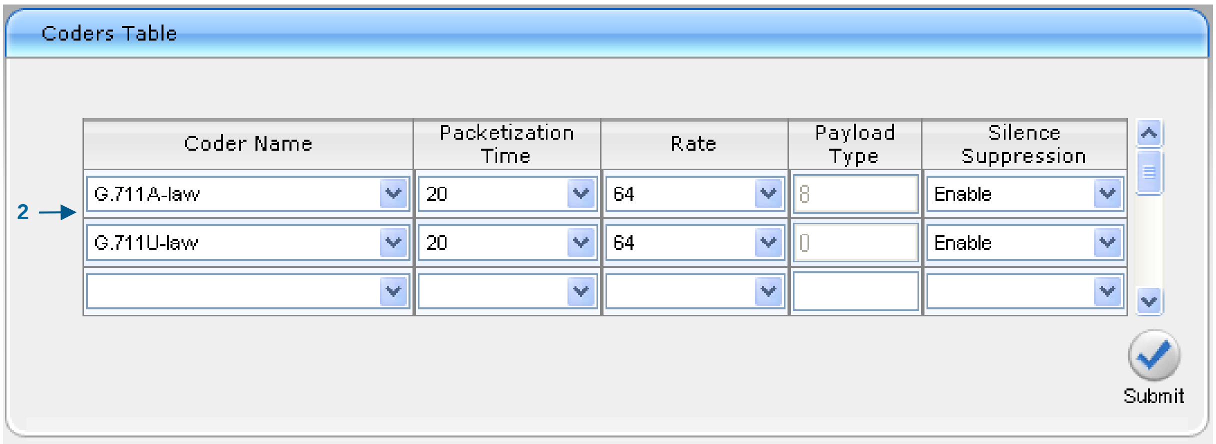
8.5 Configuring Voice Coders (with Silence Suppression)

The PSTN gateway 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 'Coders' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** sub-menu > **Coders**).

Figure 8-20: Coders Table Page



Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711A-law	20	64	8	Enable
G.711U-law	20	64	0	Enable

2. From the 'Coder Name' drop-down list, select the required coder.
3. From the 'Silence Suppression' drop-down list, select **Enable**.
4. Click **Submit**.
5. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.6 Configuring Comfort Noise and Gain Control

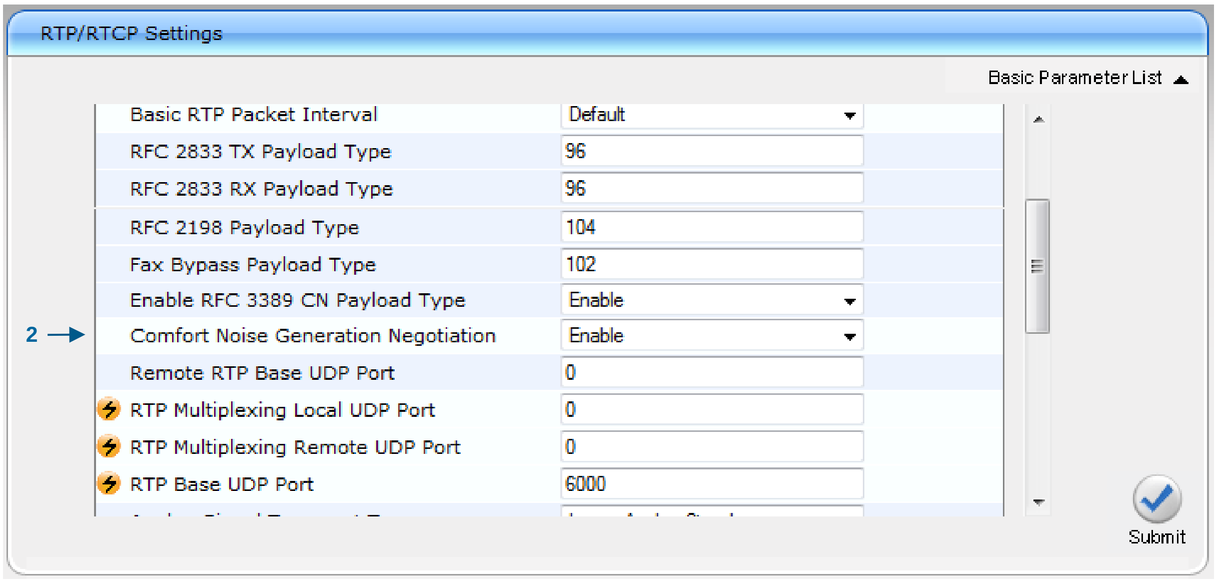
The Lync network provides high voice quality by implementing suppression of typing noise during calls and improved generation of "comfort noise," which reduces hissing and smoothes over the discontinuous flow of audio packets. You may need to configure the PSTN gateway to match these voice quality features, by enabling silence suppression, comfort noise generation, automatic gain control (AGC), and echo canceller (enabled by default).

> **Note:** Silence suppression is configured per coder type, as described in Section 8.5.

➢ **To configure voice quality:**

1. Open the 'RTP/RTCP Settings' page (**Configuration** tab > **VoIP** menu > **Media** sub-menu > **RTP/RTCP Settings**).

Figure 8-21: RTP/RTCP Settings Page



RTP/RTCP Settings

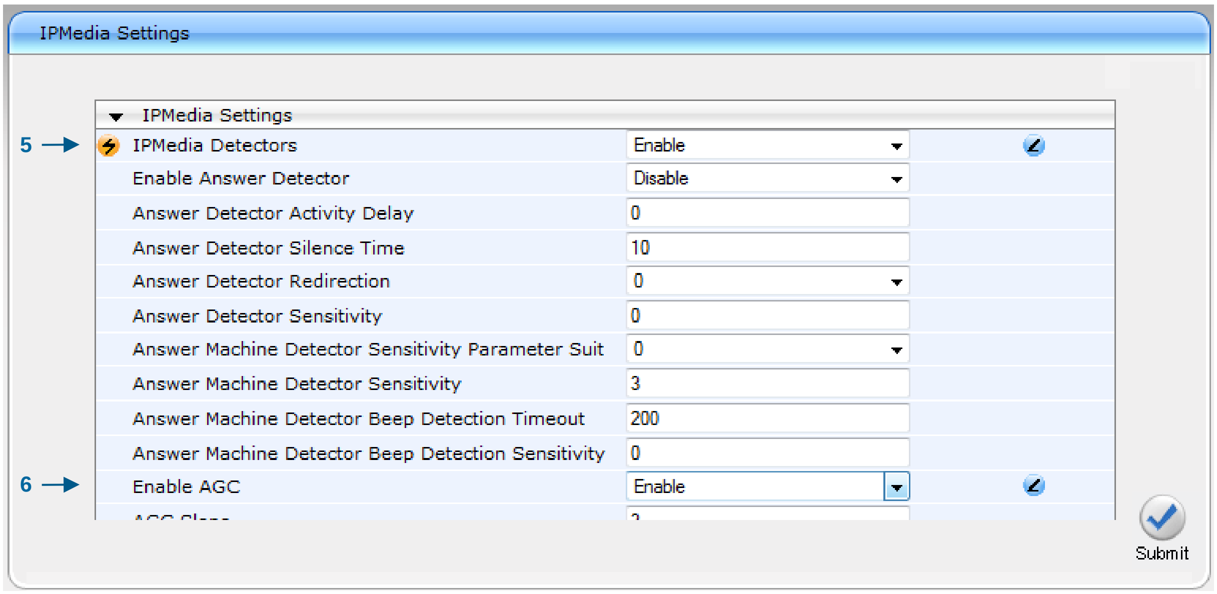
Basic Parameter List ▲

Basic RTP Packet Interval	Default
RFC 2833 TX Payload Type	96
RFC 2833 RX Payload Type	96
RFC 2198 Payload Type	104
Fax Bypass Payload Type	102
Enable RFC 3389 CN Payload Type	Enable
Comfort Noise Generation Negotiation	Enable
Remote RTP Base UDP Port	0
RTP Multiplexing Local UDP Port	0
RTP Multiplexing Remote UDP Port	0
RTP Base UDP Port	6000

2. From the 'Comfort Noise Generation Negotiation' drop-down list, select **Enable** to enable comfort noise generation.
3. Click **Submit**.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

5. Open the 'IPMedia Settings' page (**Configuration** tab > **VoIP** menu > **Media** sub-menu > **IPMedia Settings**).

Figure 8-22: IPMedia Settings Page



IPMedia Settings

IPMedia Settings

IPMedia Detectors	Enable
Enable Answer Detector	Disable
Answer Detector Activity Delay	0
Answer Detector Silence Time	10
Answer Detector Redirection	0
Answer Detector Sensitivity	0
Answer Machine Detector Sensitivity Parameter Suit	0
Answer Machine Detector Sensitivity	3
Answer Machine Detector Beep Detection Timeout	200
Answer Machine Detector Beep Detection Sensitivity	0
Enable AGC	Enable
AGC Slope	2

6. From the ‘IPMedia Detectors’ drop-down list, select **Enable**. This parameter requires a PSTN gateway reset (see Step 10 below).
7. From the ‘Enable AGC’ drop-down list, select **Enable**.
8. Click **Submit** to apply your changes.
9. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.
10. 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 800 resets and your settings are saved to the flash memory.

8.7 Configuring Early Media

Early media refers to audio and video that is exchanged before a call is accepted by the recipient. Early media generated by the caller includes voice commands or dual-tone multi frequency (DTMF) tones to activate interactive voice response (IVR) systems. Early media generated by the call recipient include ringback tones, announcements, and requests for input.

Enhanced early media support in Lync 2010 enables a caller to hear a ringback tone generated by the call recipient's mobile phone. This is also the case in team-call scenarios, where a call is routed to two team members, one of whom has configured simultaneous ringing for his or her mobile phone.

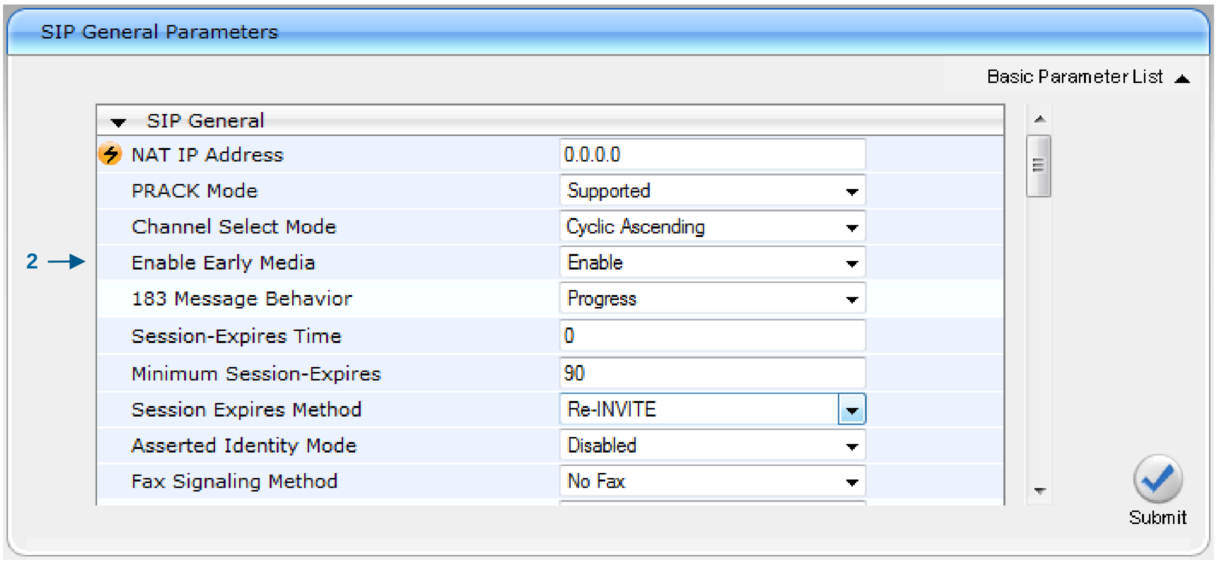
According to Lync 2010 requirements, AudioCodes PSTN gateway must send a SIP 183 with SDP immediately after it receives an INVITE. The RTP packets however, will not be sent until the PSTN gateway receives an ISDN Progress, Alerting and Progress Indicator or Connect message. For example, if the PSTN gateway receives ISDN Progress, it starts sending RTP packets according to initial negotiation, but there is no need to re-send the 183 response.

You may need to configure the PSTN gateway's early media feature to support Lync 2010 enhanced early media feature.

➢ To configure the Early Media feature:

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

Figure 8-23: SIP General Parameters Page (1)



SIP General Parameters

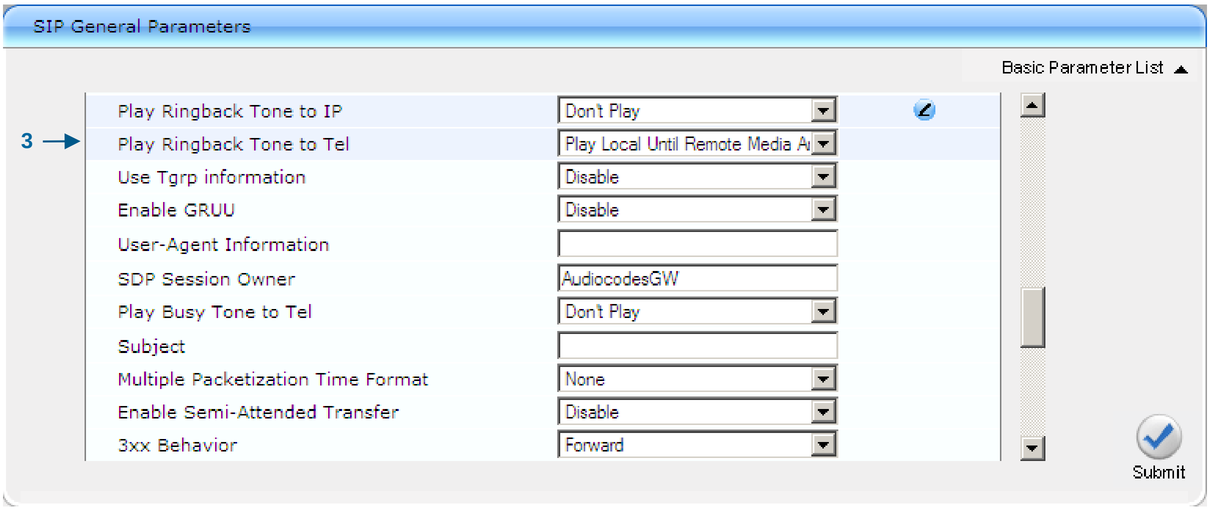
Basic Parameter List

SIP General

NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Enable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	No Fax

2. From the 'Enable Early Media' drop-down list, select **Enable**.
3. 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.

Figure 8-24: SIP General Parameters Page (2)

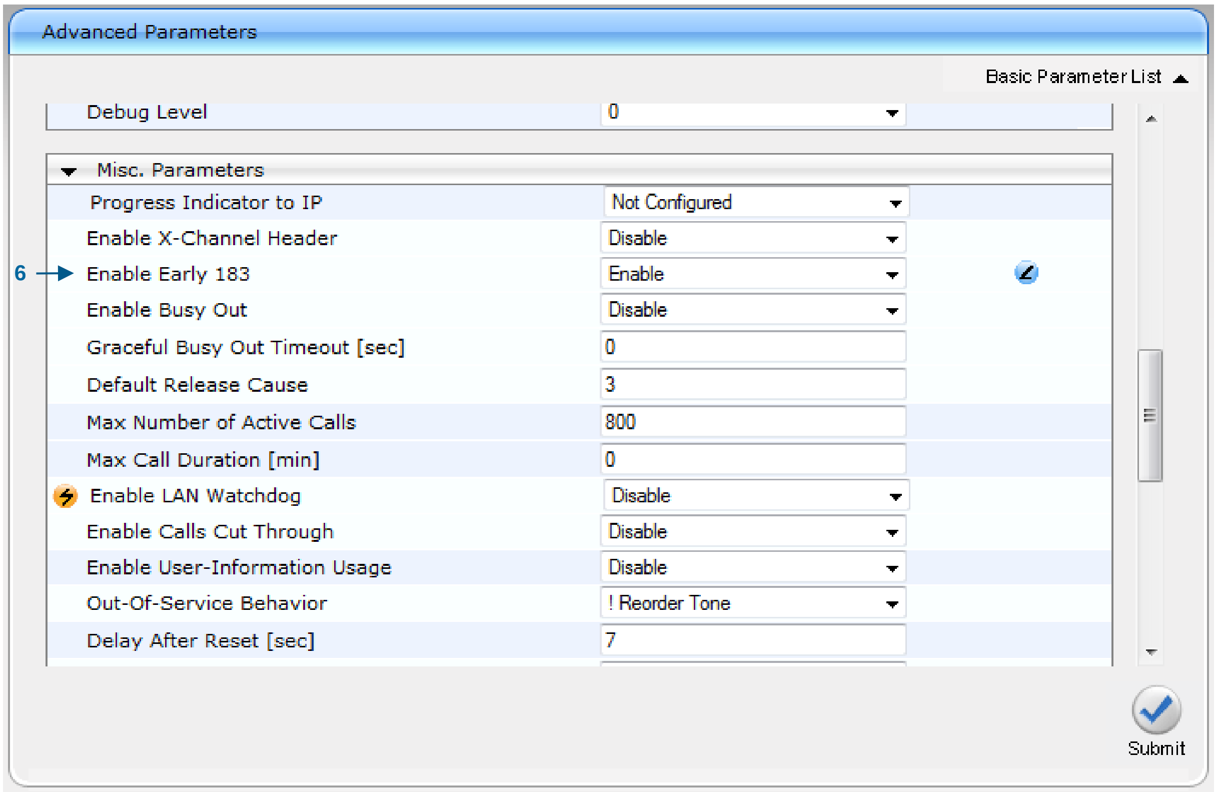


SIP General Parameters

Play Ringback Tone to IP	Don't Play
Play Ringback Tone to Tel	Play Local Until Remote Media A
Use Tgrp information	Disable
Enable GRUU	Disable
User-Agent Information	
SDP Session Owner	AudiocodesGW
Play Busy Tone to Tel	Don't Play
Subject	
Multiple Packetization Time Format	None
Enable Semi-Attended Transfer	Disable
3xx Behavior	Forward

4. Click **Submit** to apply your changes.
5. Open the 'Advanced Parameters' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** sub-menu > **Advanced Parameters**).

Figure 8-25: Advanced Parameters Page



Advanced Parameters

Debug Level	0

Misc. Parameters

Progress Indicator to IP	Not Configured
Enable X-Channel Header	Disable
Enable Early 183	Enable
Enable Busy Out	Disable
Graceful Busy Out Timeout [sec]	0
Default Release Cause	3
Max Number of Active Calls	800
Max Call Duration [min]	0
Enable LAN Watchdog	Disable
Enable Calls Cut Through	Disable
Enable User-Information Usage	Disable
Out-Of-Service Behavior	! Reorder Tone
Delay After Reset [sec]	7

6. From the ‘Enable Early 183’ drop-down list, select **Enable**.
7. Click **Submit** to apply your changes.
8. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.8 Configuring PSTN Trunks

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

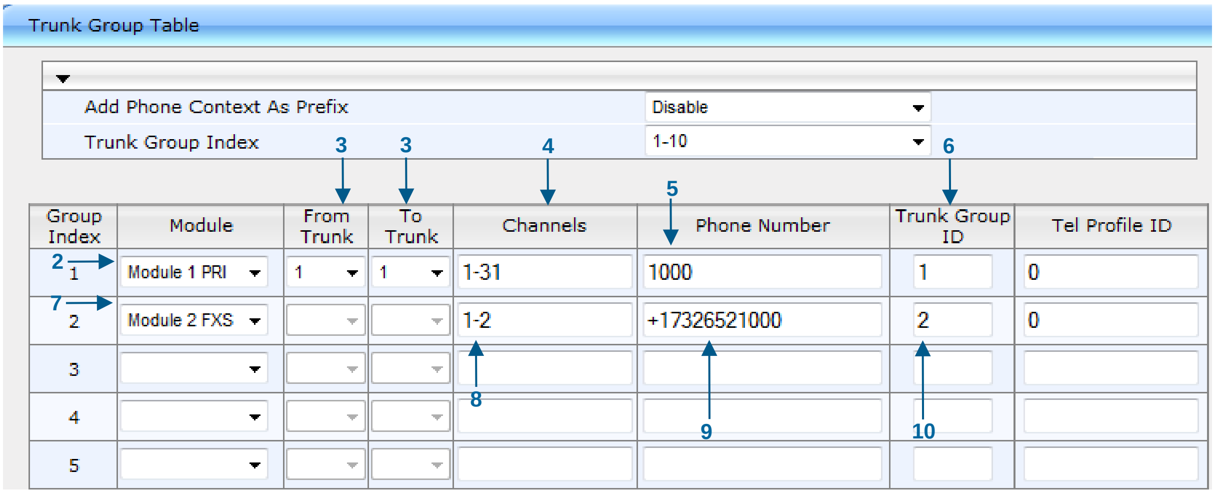
8.8.1 Enabling Trunks

To enable trunks, you need to assign them to Trunk Groups, as described below.

➢ **To enable trunks:**

1. Open the 'Trunk Group Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Trunk Group** > **Trunk Group**).

Figure 8-26: Trunk Group Table Page



Trunk Group Table

Add Phone Context As Prefix	Disable
Trunk Group Index	1-10

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-31	1000	1	0
2	Module 2 FXS			1-2	+17326521000	2	0
3							
4							
5							

2. Row index #1 - In the 'Module' column, select the module number and type (e.g., PRI) on which the trunks are located.
3. In the ‘From Trunk' and 'To Trunk' columns, select the physical trunk range.
4. In the ‘Channel(s)’ column, enter the B-channels (i.e., 1-31) that you want to enable.
5. In the 'Phone Number' column, enter the phone number (e.g., 1000) for the first channel, and then phone numbers 1001, 1002, 1003 and so on, are sequentially assigned to subsequent channels.
6. In the ‘Trunk Group ID’ column, enter the ID (i.e 1) for the Trunk Group.
7. Row index #2 - In the 'Module' column, select the module number and type (e.g., FXS) on which the FXS port are located.
8. In the ‘Channel(s)’ column, enter the channels (i.e, 1-2) that you wish to enable.
9. In the 'Phone Number' column, enter the phone number (e.g., +17326521000) for the first channel, and then phone numbers 1001, 1002, 1003 and so on, are sequentially assigned to subsequent channels.
10. In the ‘Trunk Group ID’ column, enter the ID (i.e, 2) for the Trunk Group.
11. Click **Submit** to apply your changes.
12. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

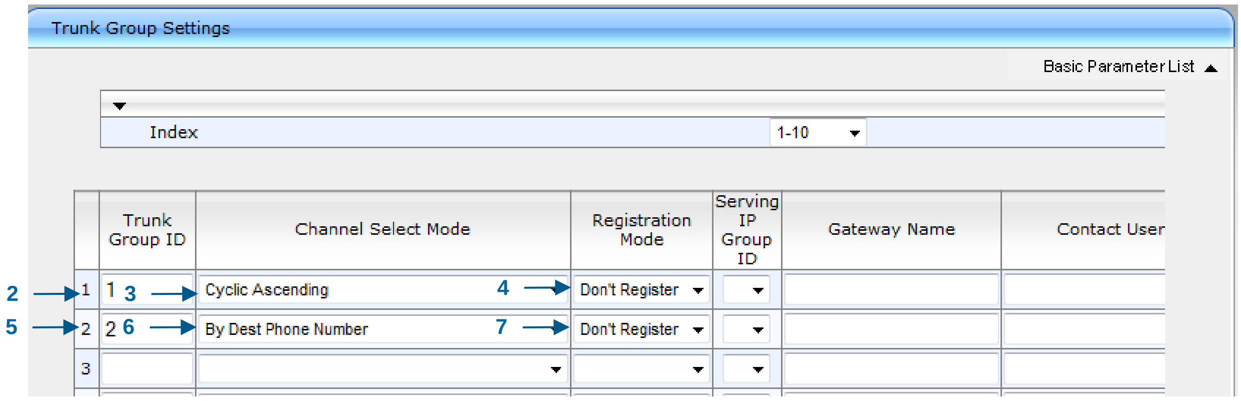
8.8.2 Configuring Channel Select Method

Once you have enabled the trunks and assigned them to Trunk Groups, you need to configure how the PSTN gateway selects trunk channels belonging to a Trunk Group for receiving IP-to-Tel calls.

➢ **To configure the channel select mode:**

1. Open the 'Trunk Group Settings' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP sub-menu** > **Trunk Group** > **Trunk Group Settings**).

Figure 8-27: Trunk Group Settings Page



Trunk Group Settings

Basic Parameter List

Index 1-10

	Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	1	Cyclic Ascending	Don't Register			
2	2	By Dest Phone Number	Don't Register			
3						

2. Row index #1 -In the 'Trunk Group ID' column, enter the Trunk Group ID that you want to configure (i.e. 1).
3. From the 'Channel Select Mode' drop-down list, select the method for which IP-to-Tel calls are assigned to channels pertaining to the Trunk Group (i.e. Cyclic Ascending).
4. From the 'Registration Mode' drop-down list, select **Don't Register**.
5. Row index #2 - In the 'Trunk Group ID' column, enter the second Trunk Group ID that you wish to configure (i.e. 2).
6. From the 'Channel Select Mode' drop-down list, select the method for which IP-to-Tel calls are assigned to channels pertaining to the Trunk Group (i.e. By Dest Phone Number).
7. From the 'Registration Mode' drop-down list, select **Don't Register**.
8. Click **Submit** to apply your changes.
9. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

8.8.3 Configuring IP-to-Trunk Group Routing

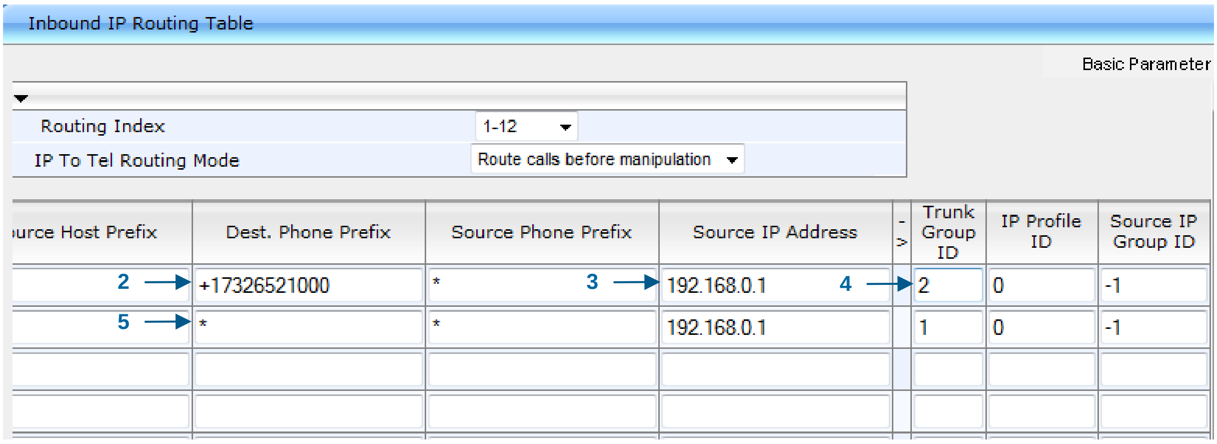
The procedure below describes how to configure an IP-to-Trunk Group routing rule, whereby all calls from the Mediation Server to any destination phone number is routed to Trunk Group 1 (that you configured in Section 8.8.1 on page 108).

Since Lync 2010 requires that the PSTN gateway must accept calls only from the Mediation Server, the routing rule must be configured with the source IP address of only the Mediation Server ("allowed Mediation Servers"). This prevents calls from un-trusted SIP entities.

➢ **To configure an IP-to-Trunk Group routing rule:**

1. Open the 'Inbound IP Routing Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Routing** > **IP to Trunk Group Routing**).

Figure 8-28: Inbound IP Routing Table Page



Inbound IP Routing Table

Basic Parameter

Routing Index: 1-12

IP To Tel Routing Mode: Route calls before manipulation

urce Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	->	Trunk Group ID	IP Profile ID	Source IP Group ID
	+17326521000	*	192.168.0.1		2	0	-1
	*	*	192.168.0.1		1	0	-1

2. In the first table entry row, enter the FXS port Phone number (i.e. +17326521000) in the 'Dest. Phone Prefix' and 'Source Phone Prefix' fields.
3. In the 'Source IP Address' field, enter the IP address of the Mediation server.
4. In the 'Trunk Group ID' field, enter the Trunk Group to where the calls must be routed (i.e. 2).
5. In the second table entry row, enter the asterisk (*) sign in the 'Dest. Phone Prefix' and 'Source Phone Prefix' fields.
6. Click **Submit** to apply your changes.
7. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.

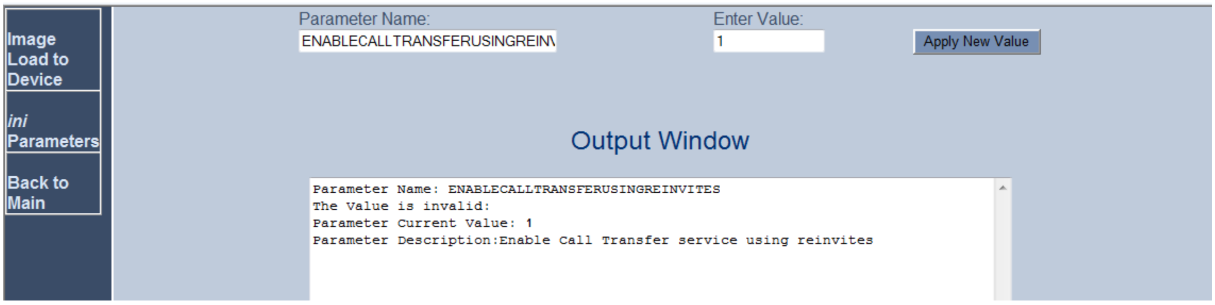
8.8.4 Configuring FXS Port Transfer Behavior

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).

➢ **To configure the Enable Call Transfer Using Reinvites parameter:**

1. Open the 'Admin" page, by appending the case-sensitive suffix ‘AdminPage’ to the Media gateway's IP address in your Web browser's URL field (e.g., http://10.15.4.22/AdminPage).
2. On the left pane, click ***ini*** Parameters.

Figure 8-29: Enable Call Transfer Using Reinvites



```
Parameter Name: ENABLECALLTRANSFERUSINGREINVITES
The Value is invalid:
Parameter Current Value: 1
Parameter Description:Enable Call Transfer service using reinvites
```

3. In the 'Parameter Name' field, enter the parameter 'EnableCallTransferUsingReinvites' and in the 'Enter Value' field, enter '1'**.**
4. Click **Apply New Value**.

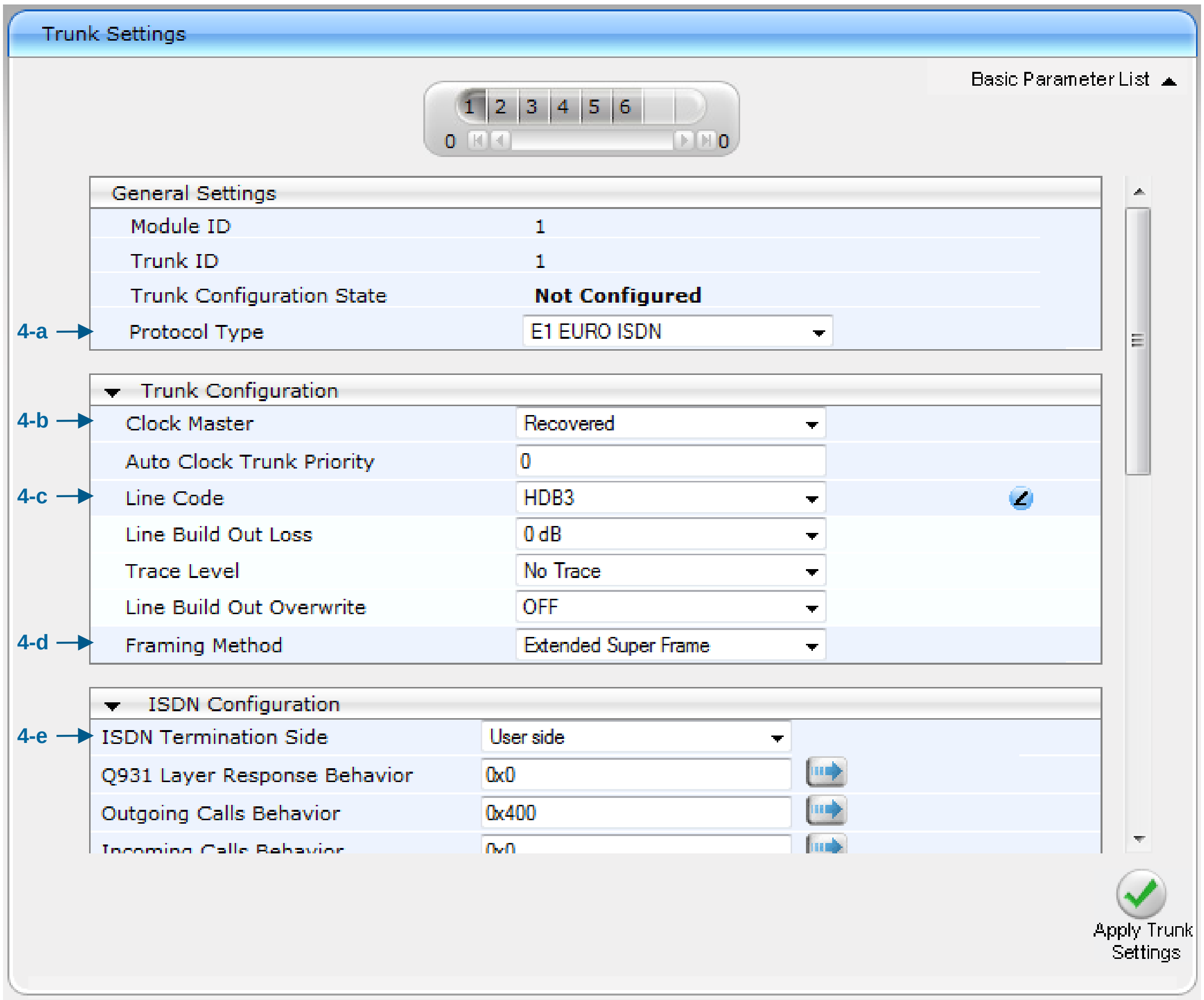
8.8.5 Configuring the Trunk

The procedure below describes basic configuration of the physical trunk.

➢ **To configure the physical trunk:**

1. Open the ‘Trunk Settings’ page (**Configuration** tab > **VoIP** menu > **PSTN** sub-menu > **Trunk Settings**).

Figure 8-30: Trunk Settings Page



Trunk Settings

General Settings	
Module ID	1
Trunk ID	1
Trunk Configuration State	**Not Configured**
Protocol Type	E1 EURO ISDN

Trunk Configuration	
Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	HDB3
Line Build Out Loss	0 dB
Trace Level	No Trace
Line Build Out Overwrite	OFF
Framing Method	Extended Super Frame

ISDN Configuration	
ISDN Termination Side	User side
Q931 Layer Response Behavior	0x0
Outgoing Calls Behavior	0x400
Incoming Calls Behavior	0x0

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.

Notes:

- 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 8.8.6).
- To delete a previously configured trunk, set the parameter 'Protocol Type' to 'None'.

   b. From the ‘Clock Master’ drop-down list, select the trunk's clock source:
      - ‘Recovered’: clock source is recovered from the trunk
      - ‘Generated’: clock source is provided by the internal TDM bus clock source (according to the parameter ‘TDM Bus Clock Source’ – see Section 8.8.6 on page 114)

   c. From the ‘Line Code’ drop-down list, select the line code:
      - ‘B8ZS’ (bipolar 8-zero substitution) for T1 trunks only
      - ‘HDB3’ (high-density bipolar 3) for E1 trunks only
      - ‘AMI’ (for E1 and T1)

   d. From the ‘Framing Method’ drop-down list, select the required framing method. For E1 trunks always set this parameter to ‘Extended Super Frame’.

   e. To configure whether the trunk connected to the PBX is User or Network side for QSIG, from the 'ISDN Termination' drop-down list, select ‘User side’ or ‘Network side’.

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.

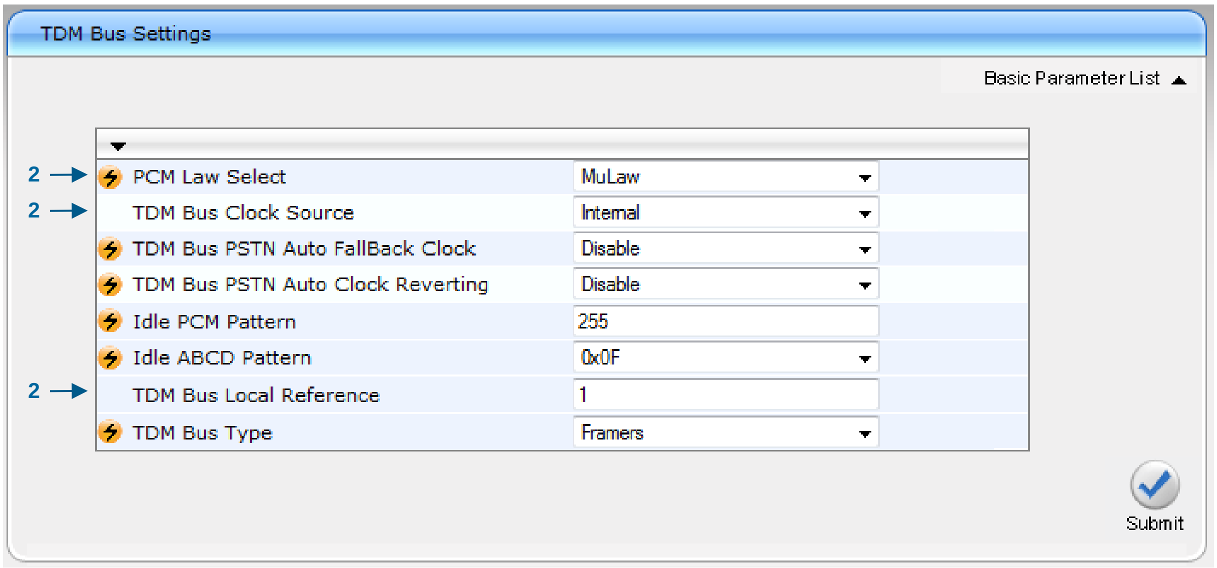
8.8.6 Configuring the TDM Bus

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 (**Configuration** tab > **VoIP** menu > **TDM** sub-menu > **TDM Bus Settings**).

Figure 8-31: TDM Bus Settings Page



TDM Bus Settings

Basic Parameter List ▲

PCM Law Select	MuLaw
TDM Bus Clock Source	Internal
TDM Bus PSTN Auto FallBack Clock	Disable
TDM Bus PSTN Auto Clock Reverting	Disable
Idle PCM Pattern	255
Idle ABCD Pattern	0x0F
TDM Bus Local Reference	1
TDM Bus Type	Framers

2. Configure the TDM bus parameters according to your deployment requirements. Below is a description of some of the main TDM parameters:
   - **PCM Law Select:** defines the type of PCM companding law in the input/output TDM bus. Typically, A-Law is used for E1 and Mu-Law for T1/J1.
   - **TDM Bus Clock Source:** defines the clock source to which the PSTN gateway synchronizes - generate clock from local source (Internal) or recover clock from PSTN line (Network).
   - **TDM Bus Local Reference:** defines the physical trunk ID from which the PSTN gateway recovers (receives) its clock synchronization when the TDM Bus Clock Source is configured to recover the clock from the PSTN line.
3. Click **Submit** to apply your changes.
4. On the toolbar, click **Burn** to save the changes to the PSTN gateway flash memory.
5. 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 800 resets and your settings are saved to the flash memory.

8.9 Configuring Normalization Rules for E.164 Format for PBX/PSTN Connectivity

Lync 2010 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 Lync 2010 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 Lync clients through Lync 2010) and inbound calls (i.e., calls destined to Lync clients).

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

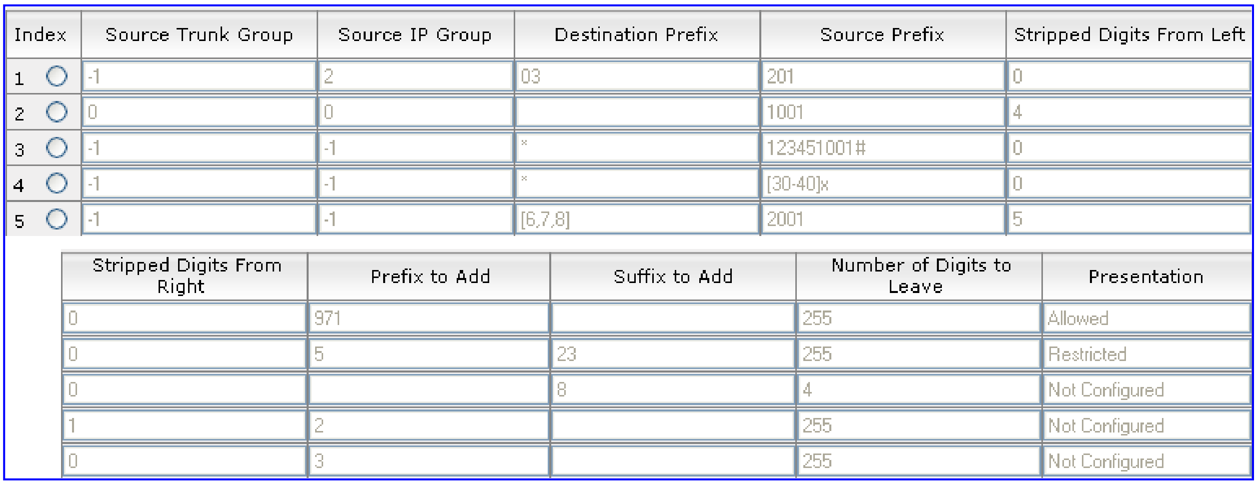
- **For Tel-to-IP calls:**
  - Destination Phone Number Manipulation Table for Tel-to-IP Calls
  - Source Phone Number Manipulation Table for Tel-to-IP Calls
- **For IP-to-Tel calls:**
  - Destination Phone Number Manipulation Table for IP-to-Tel Calls
  - Source Phone Number Manipulation Table for IP-to-Tel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

Number manipulation configuration examples are provided for inbound and outbound calls in Section 8.9.1.

➢ **To configure number manipulation rules:**

1. Open the required number Manipulation table (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Manipulations** sub-menu); the relevant Manipulation table page is displayed (e.g., 'Source Phone Number Manipulation Table for Tel→IP Calls' page).

Figure 8-32: Source Phone Number Manipulation Table for Tel-to-IP Calls



Index	Source Trunk Group	Source IP Group	Destination Prefix	Source Prefix	Stripped Digits From Left
1 ○	-1	2	03	201	0
2 ○	0	0		1001	4
3 ○	-1	-1	*	123451001#	0
4 ○	-1	-1	*	[30-40]x	0
5 ○	-1	-1	[6,7,8]	2001	5

Stripped Digits From Right	Prefix to Add	Suffix to Add	Number of Digits to Leave	Presentation
0	971		255	Allowed
0	5	23	255	Restricted
0		8	4	Not Configured
1	2		255	Not Configured
0	3		255	Not Configured

2. Configure manipulation rules as required. The figure above shows an example of the use of manipulation rules for Tel-to-IP source phone number manipulation:
   - **Index 1:** When the destination number has the prefix 03 (e.g., 035000), source number prefix 201 (e.g., 20155), and from source IP Group ID 2, the source number is changed to, for example, 97120155.
   - **Index 2:** When the source number has prefix 1001 (e.g., 1001876), it is changed to 587623.

- **Index 3:** When the source number has prefix 123451001 (e.g., 1234510012001), it is changed to 20018.
- **Index 4:** When the source number has prefix from 30 to 40 and a digit (e.g., 3122), it is changed to 2312.
- **Index 5:** When the destination number has the prefix 6, 7, or 8 (e.g., 85262146), source number prefix 2001, it is changed to 3146.

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

Table 8-1: Number Manipulation Parameters Description

Parameter	Description
Source Trunk Group	The source Trunk Group ID for Tel-to-IP calls. To denote all Trunk Groups, leave this field empty. **Notes:** ▪ The value -1 indicates that this field is ignored in the rule. ▪ This parameter is available only in the 'Source Phone Number Manipulation Table for Tel -> IP Calls' and 'Destination Phone Number Manipulation Table for Tel -> IP Calls' pages. ▪ For IP-to-IP call routing, this parameter is not required (i.e., leave the field empty).
Source IP Group	The IP Group from where the IP-to-IP call originated. Typically, this IP Group of an incoming INVITE is determined/classified using the ‘Inbound IP Routing Table'. If not used (i.e., any IP Group), simply leave the field empty. **Notes:** ▪ The value -1 indicates that this field is ignored in the rule. ▪ This parameter is available only in the 'Source Phone Number Manipulation Table for Tel -> IP Calls' and 'Destination Phone Number Manipulation Table for Tel -> IP Calls' pages. ▪ If this Source IP Group has a Serving IP Group, then all calls originating from this Source IP Group are sent to the Serving IP Group. In this scenario, this table is used only if the parameter PreferRouteTable is set to 1.
Destination Prefix	Destination (called) telephone number prefix. An asterisk (*) represents any number.
Source Prefix	Source (calling) telephone number prefix. An asterisk (*) represents any number.
Source IP Address	Source IP address of the caller (obtained from the Contact header in the INVITE message). **Notes:** ▪ This parameter is applicable only to the Number Manipulation tables for IP-to-Tel calls. ▪ The source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 to 10.8.8.99. ▪ The source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all IP addresses between 10.8.8.0 and 10.8.8.255.

Parameter	Description
Stripped Digits From Left	Number of digits to remove from the left of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 1234.
Stripped Digits From Right	Number of digits to remove from the right of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 5551.
Prefix to Add	The number or string that you want added to the front of the telephone number. For example, if you enter '9' and the phone number is 1234, the new number is 91234.
Web: Suffix to Add	The number or string that you want added to the end of the telephone number. For example, if you enter '00' and the phone number is 1234, the new number is 123400.
Number of Digits to Leave	The number of digits that you want to retain from the right of the phone number. For example, if you enter '4' and the phone number is 00165751234, then the new number is 1234.
NPI	The Numbering Plan Indicator (NPI) assigned to this entry. ▪ **[0]** Unknown (default) ▪ **[9]** Private ▪ **[1]** E.164 Public ▪ **[-1**] Not Configured = value received from PSTN/IP is used **Note:** This parameter is applicable only to Number Manipulation tables for IP-to-Tel calls.
TON	The Type of Number (TON) assigned to this entry. ▪ If you selected 'Unknown' for the NPI, you can select Unknown **[0].** ▪ If you selected 'Private' for the NPI, you can select Unknown **[0],** Level 2 Regional **[1],** Level 1 Regional **[2],** PISN Specific **[3]** or Level 0 Regional (Local) **[4].** ▪ If you selected 'E.164 Public' for the NPI, you can select Unknown **[0],** International **[1],** National **[2],** Network Specific **[3],** Subscriber **[4]** or Abbreviated **[6].** **Notes:** ▪ This parameter is applicable only to Number Manipulation tables for IP-to-Tel calls. ▪ The default is 'Unknown'.
Presentation	Determines whether Caller ID is permitted: ▪ Not Configured = Privacy is determined according to the Caller ID table. ▪ **[0]** Allowed = Sends Caller ID information when a call is made using these destination/source prefixes. ▪ **[1]** Restricted = Restricts Caller ID information for these prefixes. **Notes:** ▪ This field is applicable only to Number Manipulation tables for source number manipulation. ▪ If 'Presentation' is set to 'Restricted' and the AssertedIdMode parameter is set to 'P-Asserted', the From header in the INVITE message includes the following: From: 'anonymous' <sip: anonymous@anonymous.invalid> and 'privacy: id' header.

8.9.1 Number Normalization Examples

Two examples are provided below for number normalization. The examples are based on the following assumptions:

- PBX with prefix (local) number 333
- 4-digit extension numbers that begin with the digit 1 (i.e., 1xxx)
- National area code is 206
- Country code is 1

8.9.1.1 Modifying E.164 Numbers to PBX / PSTN Format for Outbound Calls

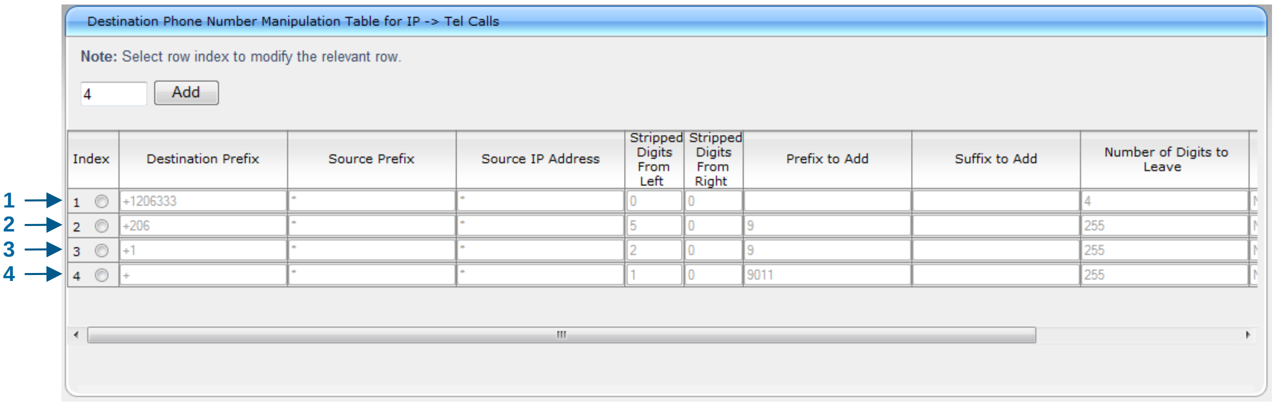
Outbound calls refer to calls made by Lync clients to a PBX / PSTN number.

1. **Local Calls within PBX:** The caller dials only the last four digits (e.g., 1212). Lync translates (normalizes) the phone number into an E.164 number format: +12063331212 (where *+1* is the country code, *206* the local area code, and *333* the PBX prefix number). The Manipulation table is configured to send only the last four digits to the PBX (i.e., 1212).
2. **National Calls to the Same Area Code:** The caller dials 9 for an external line, and then dials a 7-digit telephone number (e.g., 9-555-4321). Lync translates (normalizes) the phone number into an E.164 number format: +12065554321 (where *+1* is the country code, *206* the local area code, *5554321* the phone number). The Manipulation table is configured to remove (strip) the first five digits and add 9 as a prefix to the remaining number. Therefore, the PSTN gateway sends the number 95554321 to the PBX, and then the PBX sends the number 5554321 to the PSTN.
3. **National Calls to a Different Area Code:** The caller dials 9 for an external line, the out-of-area code, and then a 7-digit telephone number (e.g., 9-503-331-1425). Lync translates (normalizes) the phone number into an E.164 number format: +15033311425 (where *+1* is the international code, *503* the out-of area code, *3311425* the phone number). The Manipulation table is configured to remove (strip) the first two digits (i.e., *+1*), add then add 9 as a prefix to the remaining number. Therefore, the PSTN gateway sends the number 95033311425 to the PBX, and then the PBX sends the number 5033311425 to the PSTN.

4. **Dialing International Calls:** The caller dials 9 for an external line, the access code for international calls (e.g., 011 for the US), the country code (e.g., +44 for the UK), the area code (e.g., 1483), and then a 6-digit telephone number (e.g., 829827). Lync translates (normalizes) the phone number into an E.164 number format: +441483829827 (where *+44* is the country code, *1483* the area code, *829827* the phone number). The Manipulation table is configured to remove the first digit (e.g., +), and add the external line digit (e.g., 9) and the access code for international calls (e.g., 011 for the US) as the prefix. Therefore, the PSTN gateway sends the number 9011441483829827 to the PBX and the PBX, in turn, sends the number 011441483829827 to the PSTN.

The configuration of the above scenarios is shown in the Figure 8-33.

Figure 8-33: Destination Phone Number Manipulation Table for IP→Tel Calls



Destination Phone Number Manipulation Table for IP -> Tel Calls

Note: Select row index to modify the relevant row.

4

Index		Destination Prefix	Source Prefix	Source IP Address	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add	Suffix to Add	Number of Digits to Leave
1	○	+1206333	*	*	0	0			4
2	○	+206	*	*	5	0	9		255
3	○	+1	*	*	2	0	9		255
4	○	+	*	*	1	0	9011		255

8.9.1.2 Modifying PBX, Local, and National Calls to E.164 Format for Inbound Calls

Inbound calls refer to calls received by Lync clients from the PBX / PSTN.

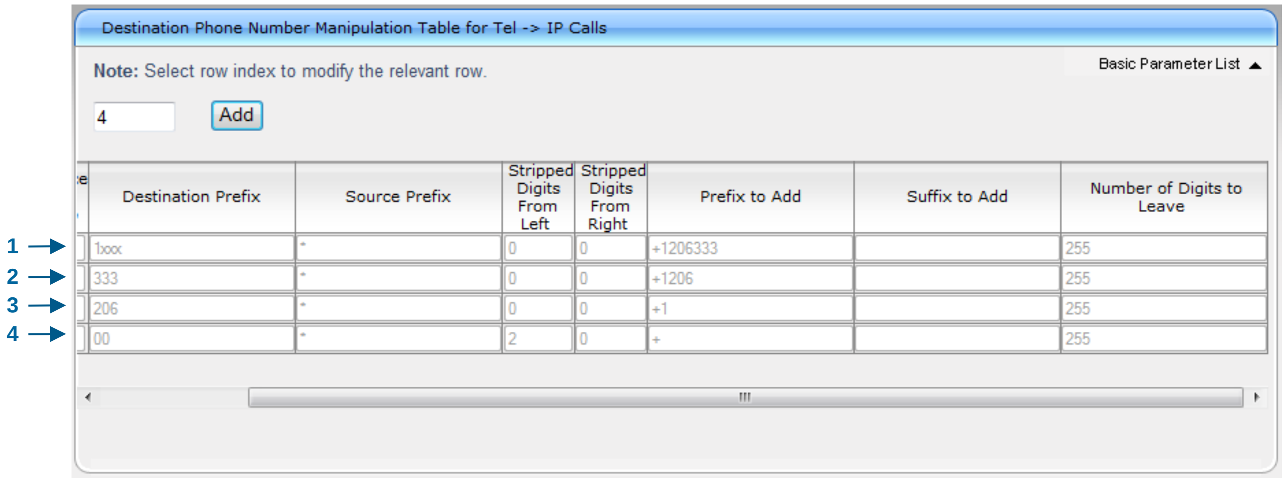
1. **Local Calls from the PBX / PSTN:** The PBX user only dials a 4-digit extension number of the Lync client (e.g., 1220). The Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1206333 to the extension number. Therefore, the PSTN gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.
2. **National Calls with the Same Area Code**: The PSTN user dials a 7-digit phone number (e.g., 333-1220), which is received by the PSTN gateway. The Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1206 to the number. Therefore, the PSTN gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.
3. **National Calls from a Different Area Code:** The PSTN user dials the national area code and then a 7-digit phone number (e.g., 206-333-1220), which is received by the PSTN gateway. The Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1 to the number. Therefore, the PSTN gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.

   Note: Whether the area code is received by the PSTN gateway depends on the country's PSTN numbering rules.
4. **International Calls:** The PSTN international (overseas) caller dials the international access and country code (e.g., 001 for the US), the national area code, and then a 7-digit phone number (e.g., 206-333-1220), which is received by the PSTN gateway. The Manipulation table is configured to normalize the number into E.164 format, by removing the first two digits (e.g., 00) and adding the prefix plus sign (+). Therefore, the PSTN gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.

   Note: Whether the international and country codes are received by the PSTN gateway depends on the country's PSTN numbering rules.

The configuration of the above scenarios is shown in the figure below:

Figure 8-34: Destination Phone Number Manipulation Table for Tel→IP Calls



Destination Phone Number Manipulation Table for Tel -> IP Calls

Note: Select row index to modify the relevant row.

	Destination Prefix	Source Prefix	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add	Suffix to Add	Number of Digits to Leave
1 →	1xxx	*	0	0	+1206333		255
2 →	333	*	0	0	+1206		255
3 →	206	*	0	0	+1		255
4 →	00	*	2	0	+		255

9 Testing SBA Calls

Once you have completed the configuration steps described in the previous sections, you can test call making at the branch office, as described in this section.

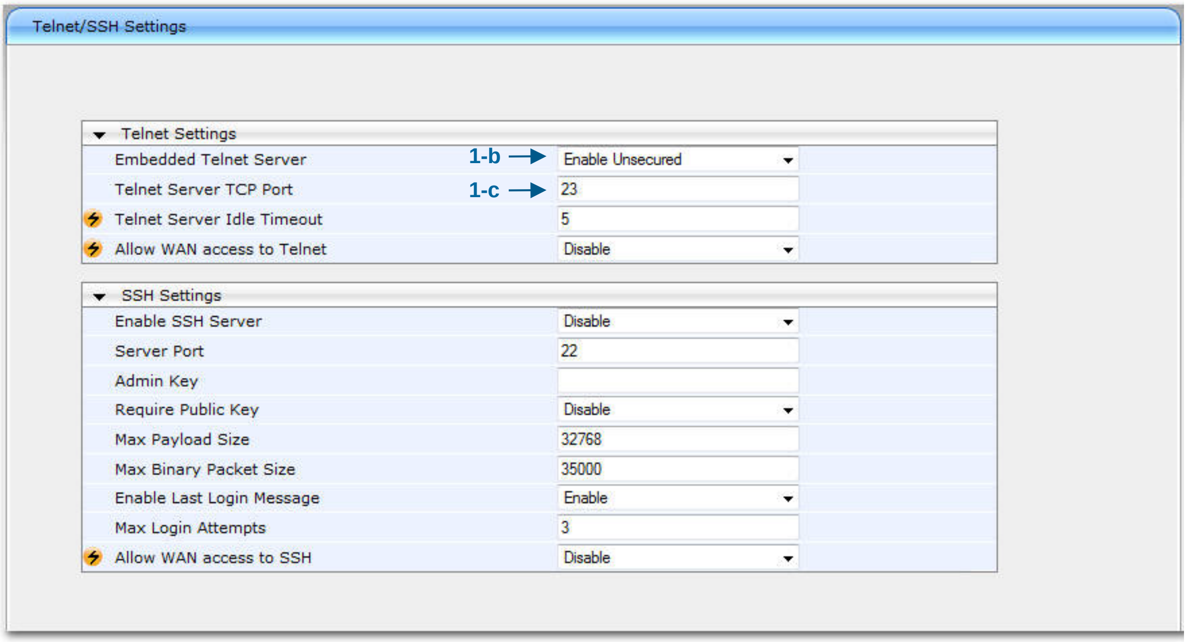
9.1 Testing Gateway Calls

The procedure below describes how to test calls on the PSTN gateway. Before you do this, you need to establish a telnet session with the PSTN gateway.

➢ **To test gateway calls:**

1. Enable Telnet on the PSTN gateway, using the PSTN gateway Web interface:
   a. Open the ‘Telnet/SSH Settings’ page (**Configuration** tab > **System** menu > **Management** sub-menu > **Telnet/SSH Settings**).
   b. From the ‘Embedded Telnet Server’ drop-down list, select **Enable Unsecured**.
   c. In the ‘Telnet Server TCP Port’ field, ensure that the port used for Telnet is '23' (default).

Figure 9-1: Enabling Telnet

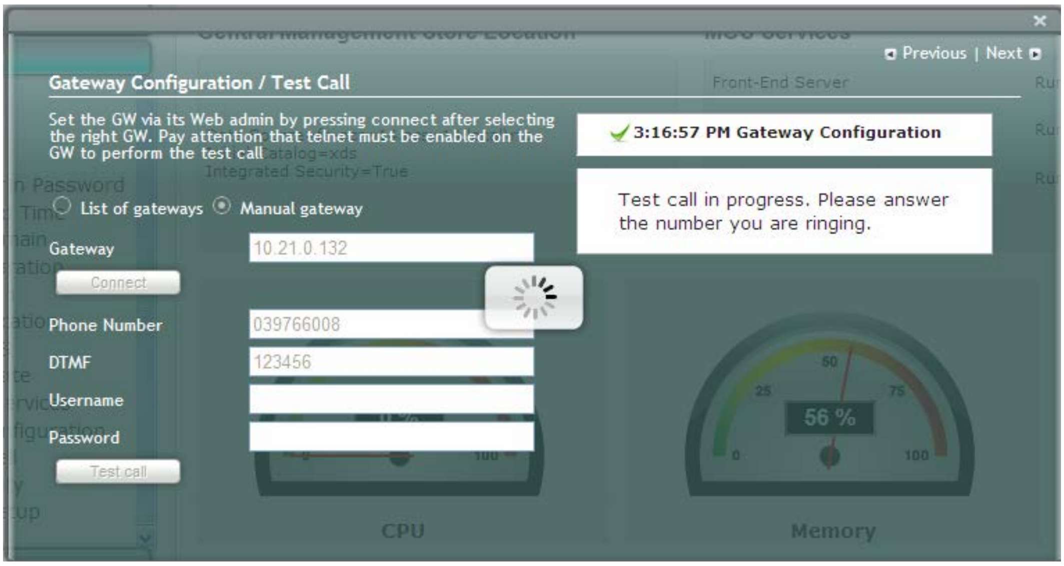


Telnet/SSH Settings

Telnet Settings	
Embedded Telnet Server	Enable Unsecured
Telnet Server TCP Port	23
Telnet Server Idle Timeout	5
Allow WAN access to Telnet	Disable
SSH Settings	
Enable SSH Server	Disable
Server Port	22
Admin Key	
Require Public Key	Disable
Max Payload Size	32768
Max Binary Packet Size	35000
Enable Last Login Message	Enable
Max Login Attempts	3
Allow WAN access to SSH	Disable

2. Establish a Telnet session with the PSTN gateway.
3. Log in to the SBA Web Setup and do the following:
   a. Under the **Setup** menu, click the **Gateway Configuration** option.
   b. Select the **Manual Gateway** radio button and enter the IPaddress or the FQDN of the gateway (as configured in Section 8.1 on page 83).
   c. In the ‘Phone Number’ field, enter a phone number.
   d. In the ‘DTMF’ field, enter any DTMF string. This DTMF string will be heard when the user picks up the phone handset.
   e. If you changed the Web/Telnet login username and password of the PSTN gateway, then enter their values in the ‘Username’ and ‘Password’ fields respectively; otherwise, leave the fields as is.
   f. Click **Test call**.

Figure 9-2: Gateway Configuration – Calling the Phone



Gateway Configuration / Test Call

Set the GW via its Web admin by pressing connect after selecting the right GW. Pay attention that telnet must be enabled on the GW to perform the test call

○ List of gateways ● Manual gateway

Gateway: 10.21.0.132

Phone Number: 039766008

DTMF: 123456

Username:

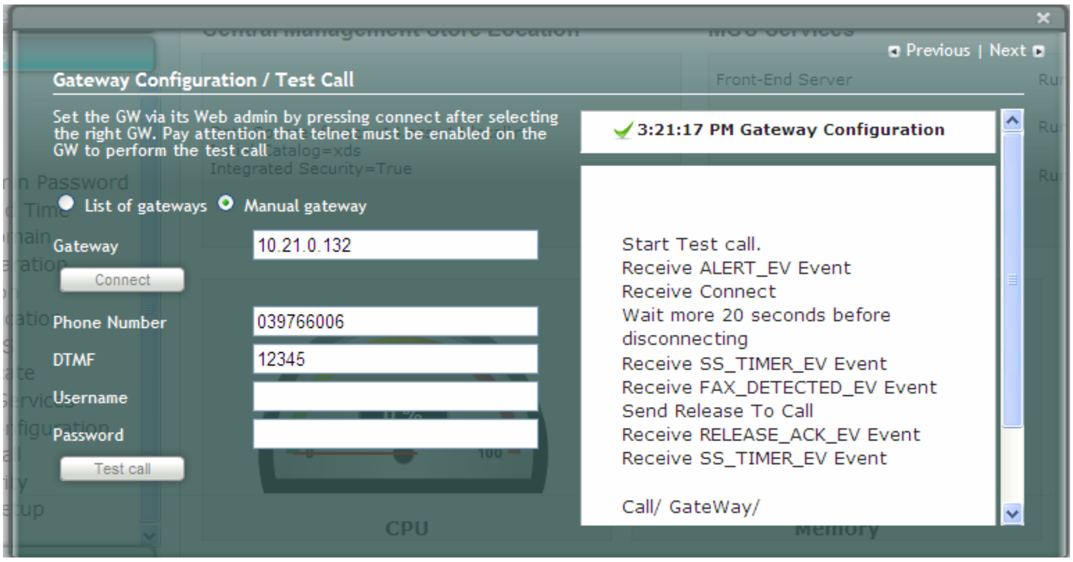
Password:

3:16:57 PM Gateway Configuration

Test call in progress. Please answer the number you are ringing.

If the phone does not ring, an error message is displayed and the call test fails. If the phone rings, lift the handset and confirm that you can hear the DTMFs. The following screen appears when you answer the phone:

Figure 9-3: Gateway Configuration – Call Answered



Gateway Configuration / Test Call

Set the GW via its Web admin by pressing connect after selecting the right GW. Pay attention that telnet must be enabled on the GW to perform the test call

○ List of gateways ● Manual gateway

Gateway: 10.21.0.132

Phone Number: 039766006

DTMF: 12345

Username:

Password:

3:21:17 PM Gateway Configuration

```
Start Test call.
Receive ALERT_EV Event
Receive Connect
Wait more 20 seconds before
disconnecting
Receive SS_TIMER_EV Event
Receive FAX_DETECTED_EV Event
Send Release To Call
Receive RELEASE_ACK_EV Event
Receive SS_TIMER_EV Event

Call/ GateWay/
```

Note: It is recommended to disable Telnet after making the test call.

9.2 Testing Lync Calls

The **OCS Test Call** option allows you test a PSTN call initiated by the Lync Server 2010. The test call succeeds if the PSTN call is routed from Lync to the PSTN through the gateway.

9.2.1 Test Prerequisites

Before running the **OCS Test Call**, the following prerequisites must be met:

- Test users have been created in the Lync Server 2010 and are voice-enabled.
- VoIP Outbound Routing configuration has been setup and the correct policies have been assigned to the test users.
- Built-in-users for OcsHealthMonitoring have been configured using the following commands:

  ```
  New-CsHealthMonitoringConfiguration -Identity
  <XdsGlobalRelativeIdentity> -FirstTestUserSipUri <String> -
  SecondTestUserSipUri <String>
  ```

  Where,

  - ***Identity*** is the FQDN of the pool where the health monitoring configuration settings are to be assigned (i.e., SBA FQDN).
  - ***FirstTestUserSipUri*** is the SIP address of the first test user to be configured for use by this collection of health monitoring settings. Note that the SIP address must include the sip: prefix, for example:

    ```
    -FirstTestUserSipUri sip:kenmyer@litwareinc.com
    ```

  - ***SecondTestUserSipUri*** is the SIP address of the second test user to be configured for use by this collection of health monitoring settings. Note that the SIP address must include the sip: prefix, for example:

    ```
    -FirstTestUserSipUri sip:jhaas@litwareinc.com
    ```

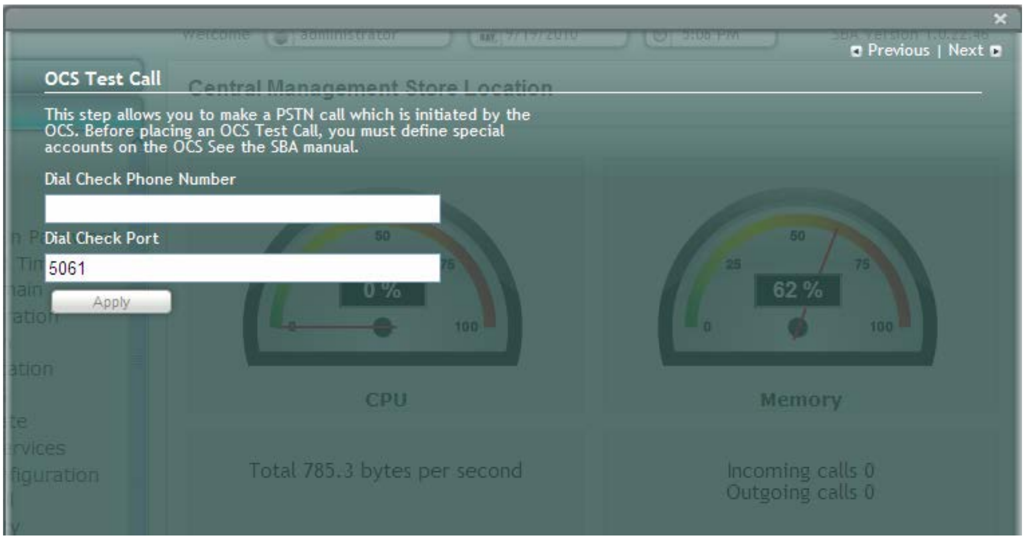
9.2.2 Running the Lync Call Test

The procedure for running the test is described below.

➢ **To run the OSC test call:**

1. Under the **Setup** menu, select the **OCS Test Call** option; the OCS Test Call screen appears:

Figure 9-4: OCS Test Call Screen



OCS Test Call

This step allows you to make a PSTN call which is initiated by the OCS. Before placing an OCS Test Call, you must define special accounts on the OCS See the SBA manual.

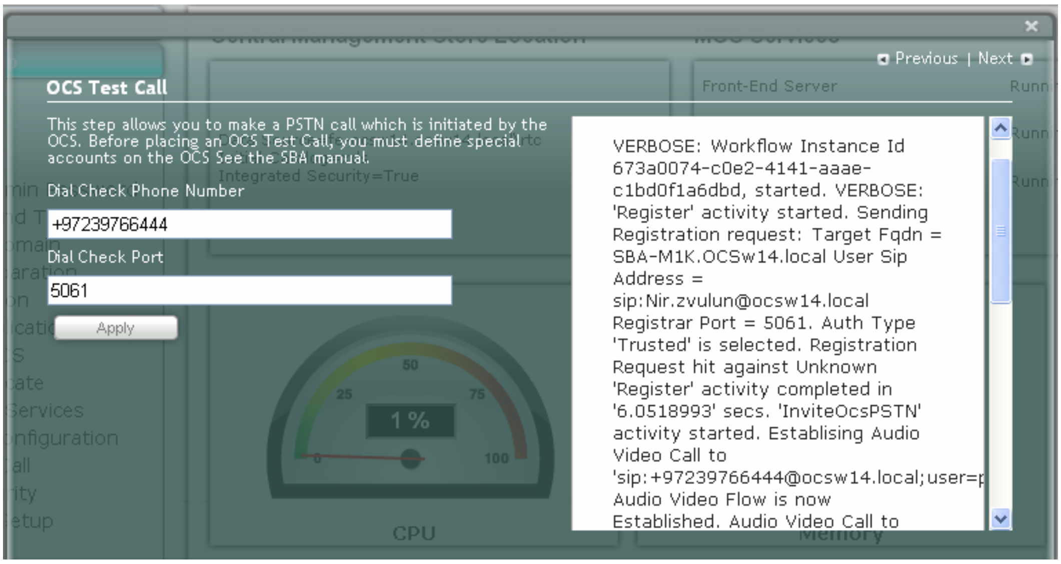
Dial Check Phone Number:

Dial Check Port: 5061

2. In the ‘Dial Check Phone Number’ field, enter the phone number to dial.
3. In the ‘Dial Check Port’ field, leave as is (i.e., 5061).
4. Click **Apply** to start the test call.

If the test is successful, the phone of the PSTN user rings and when the handset is lifted, the DTMF tones are heard. If the phone does not ring, an error message is displayed on the screen. The screen displays logged details of the call:

Figure 9-5: OCS Test Call – Logged Call Test Result



OCS Test Call

This step allows you to make a PSTN call which is initiated by the OCS. Before placing an OCS Test Call, you must define special accounts on the OCS See the SBA manual.

Dial Check Phone Number: +97239766444

Dial Check Port: 5061

```
VERBOSE: Workflow Instance Id
673a0074-c0e2-4141-aaae-
c1bd0f1a6dbd, started. VERBOSE:
'Register' activity started. Sending
Registration request: Target Fqdn =
SBA-M1K.OCSw14.local User Sip
Address =
sip:Nir.zvulun@ocsw14.local
Registrar Port = 5061. Auth Type
'Trusted' is selected. Registration
Request hit against Unknown
'Register' activity completed in
'6.0518993' secs. 'InviteOcsPSTN'
activity started. Establising Audio
Video Call to
'sip:+97239766444@ocsw14.local;user=p
Audio Video Flow is now
Established. Audio Video Call to
```

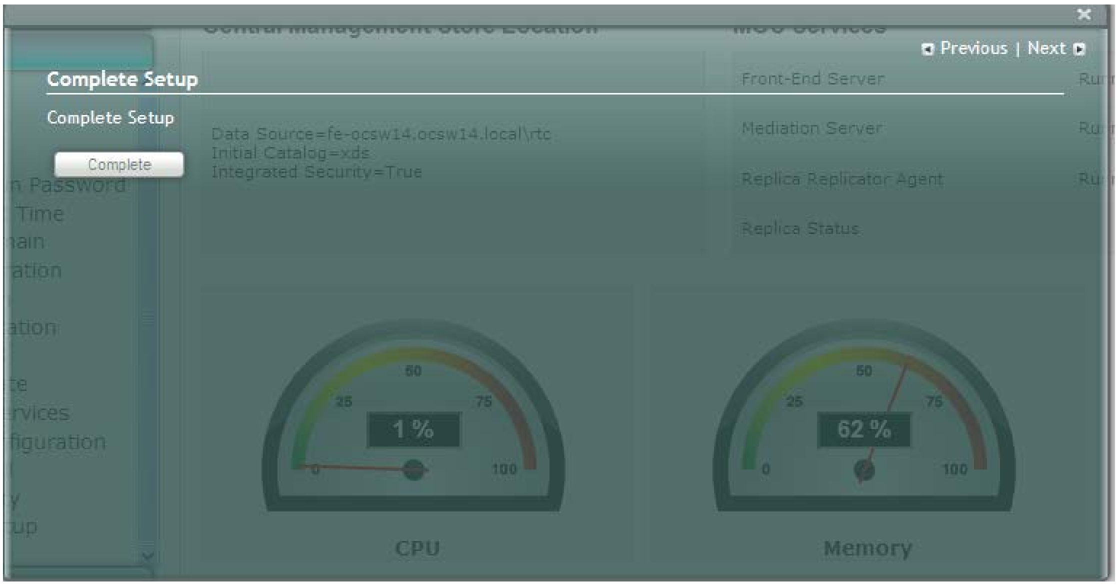
10 Completing SBA Setup

Once you have completed all configurations as described in the previous sections, you need to perform the procedure described below to complete the SBA setup.

➢ To complete SBA setup:

1. Log in to the SBA Web wizard (if not logged in already).
2. Under the **Setup** menu, select the **Complete Setup** option; the Complete Setup screen appears:

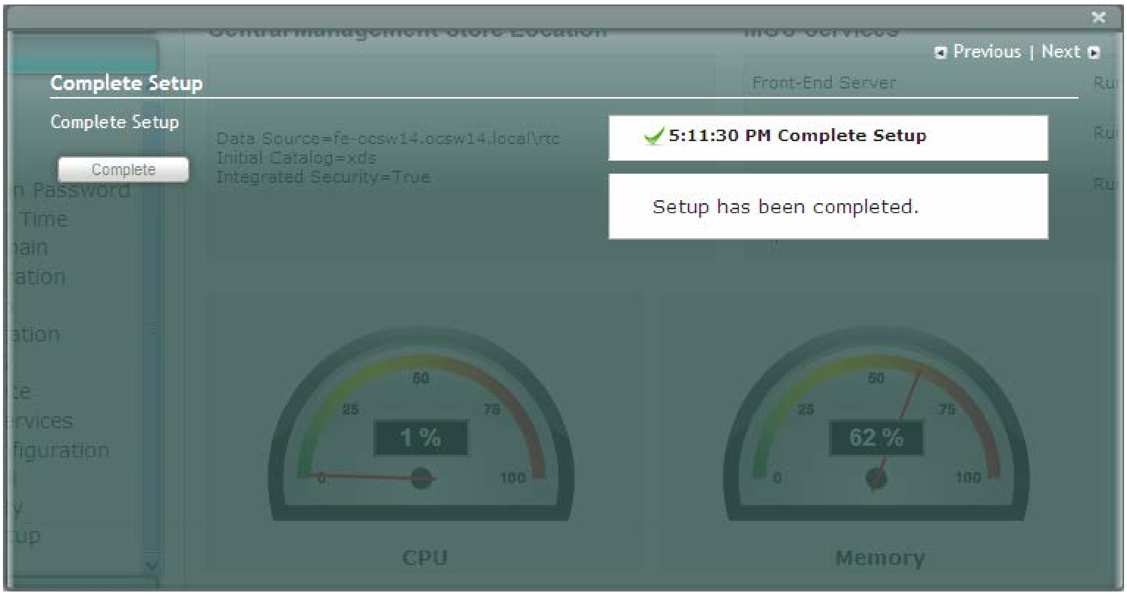
Figure 10-1: Complete Setup Screen



Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True

3. Click **Complete**; the following screen appears, indicating that the SBA setup is complete:

Figure 10-2: Complete Setup – Setup Completed



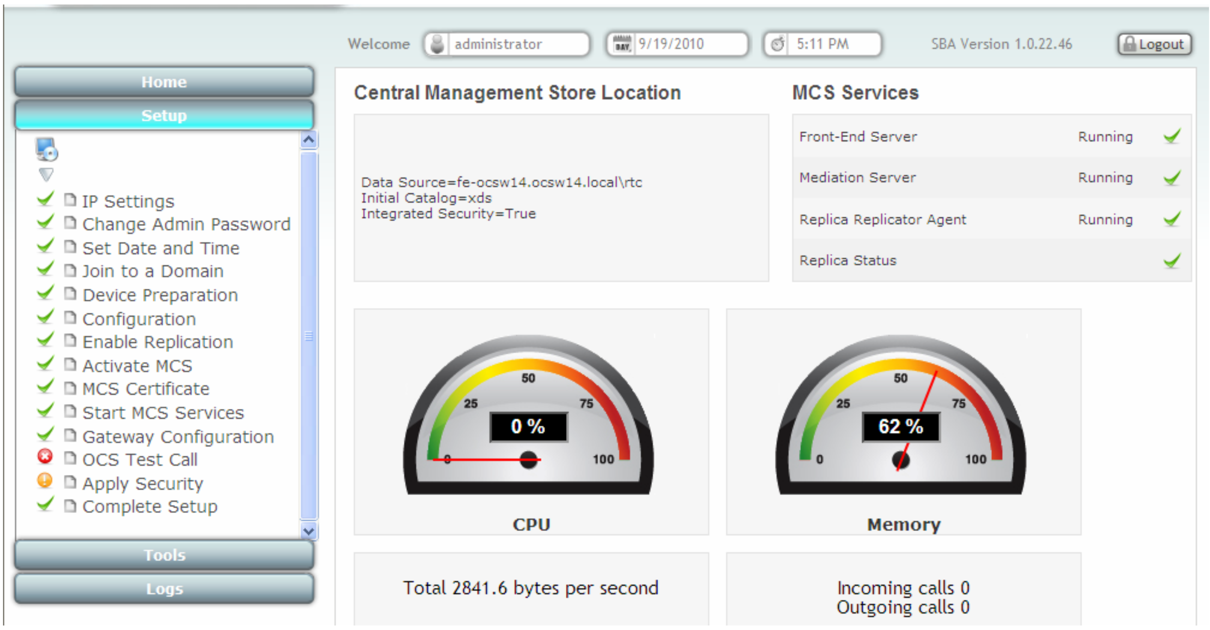
Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True

✓ 5:11:30 PM Complete Setup

Setup has been completed.

A green check mark appears alongside the **Complete Setup** option under the **Setup** menu:

Figure 10-3: Complete Setup – Completed Successfully



Welcome administrator 9/19/2010 5:11 PM SBA Version 1.0.22.46

- ✓ IP Settings
- ✓ Change Admin Password
- ✓ Set Date and Time
- ✓ Join to a Domain
- ✓ Device Preparation
- ✓ Configuration
- ✓ Enable Replication
- ✓ Activate MCS
- ✓ MCS Certificate
- ✓ Start MCS Services
- ✓ Gateway Configuration
- ☒ OCS Test Call
- ! Apply Security
- ✓ Complete Setup

Central Management Store Location

```
Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True
```

MCS Services

Front-End Server	Running	✓
Mediation Server	Running	✓
Replica Replicator Agent	Running	✓
Replica Status		✓

Total 2841.6 bytes per second

Incoming calls 0
Outgoing calls 0

11 Miscellaneous SBA Procedures

This section describes various procedures that can be performed using the SBA Web-based tool.

11.1 Viewing General SBA Status in the Home Page

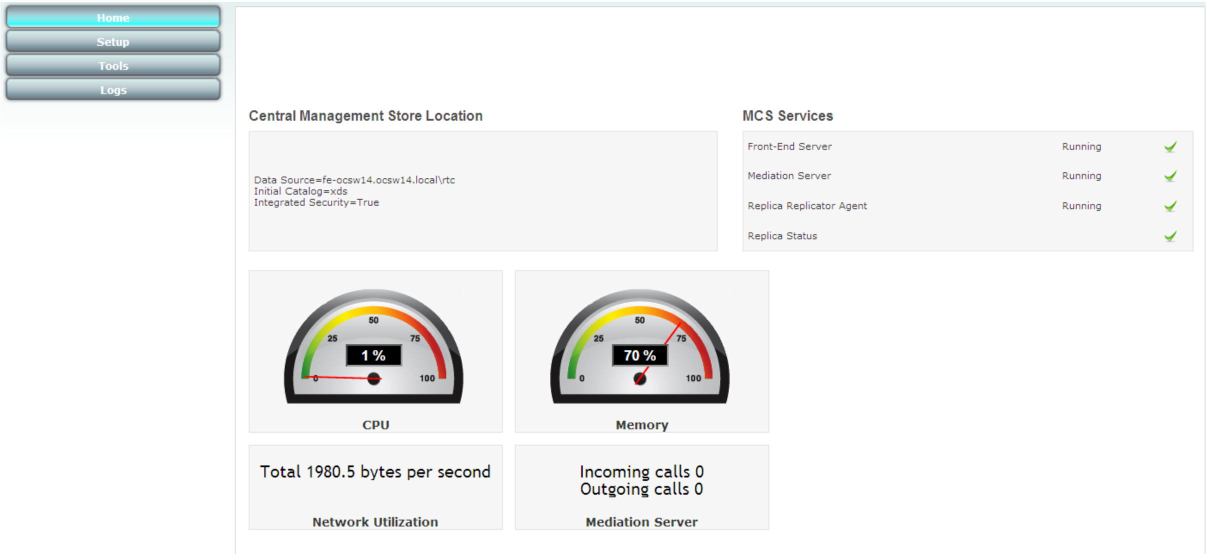
The general operating status of the SBA can be viewed in the Home page. This displays the following:

- Central management store location
- SBA services status (stopped or running)
- CPU, memory, and network usages
- Number of incoming and outgoing calls

➢ To view the Home page:

- Select the **Home** menu tab:

Figure 11-1: Home Page



Central Management Store Location

Data Source=fe-ocsw14.ocsw14.local\rtc
Initial Catalog=xds
Integrated Security=True

MCS Services

Front-End Server	Running	✓
Mediation Server	Running	✓
Replica Replicator Agent	Running	✓
Replica Status		✓

CPU

Memory

Total 1980.5 bytes per second

Network Utilization

Incoming calls 0
Outgoing calls 0

Mediation Server

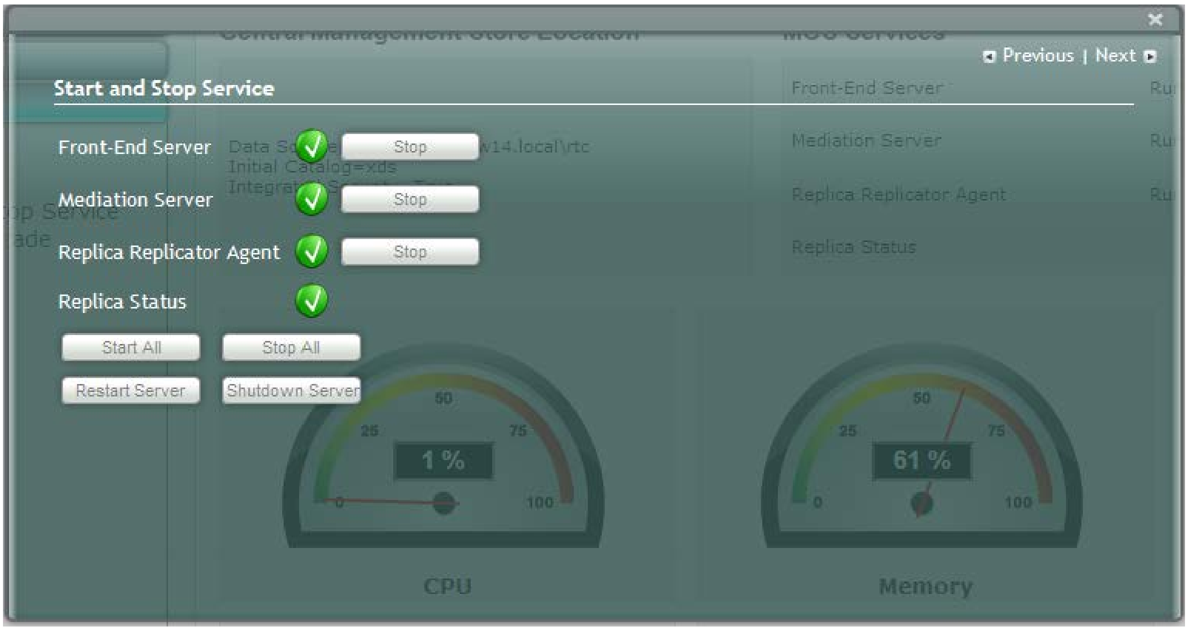
11.2 Starting and Stopping SBA Services

You can stop and start SBA services as described in the procedure below.

➢ **To start and stop services:**

1. Select the **Tools** menu tab, and then click the **Start and Stop Service** option; the Start and Stop Service page appears:

Figure 11-2: Start and Stop Service Page



2. Click one of the following as required:
   - **Start All:** Starts the services on the SBA
   - **Stop All:** Stops the services on the SBA
   - **Restart Server:** Restarts the server
   - **Shutdown Server:** Shuts down the server

11.3 Updating SBA Components

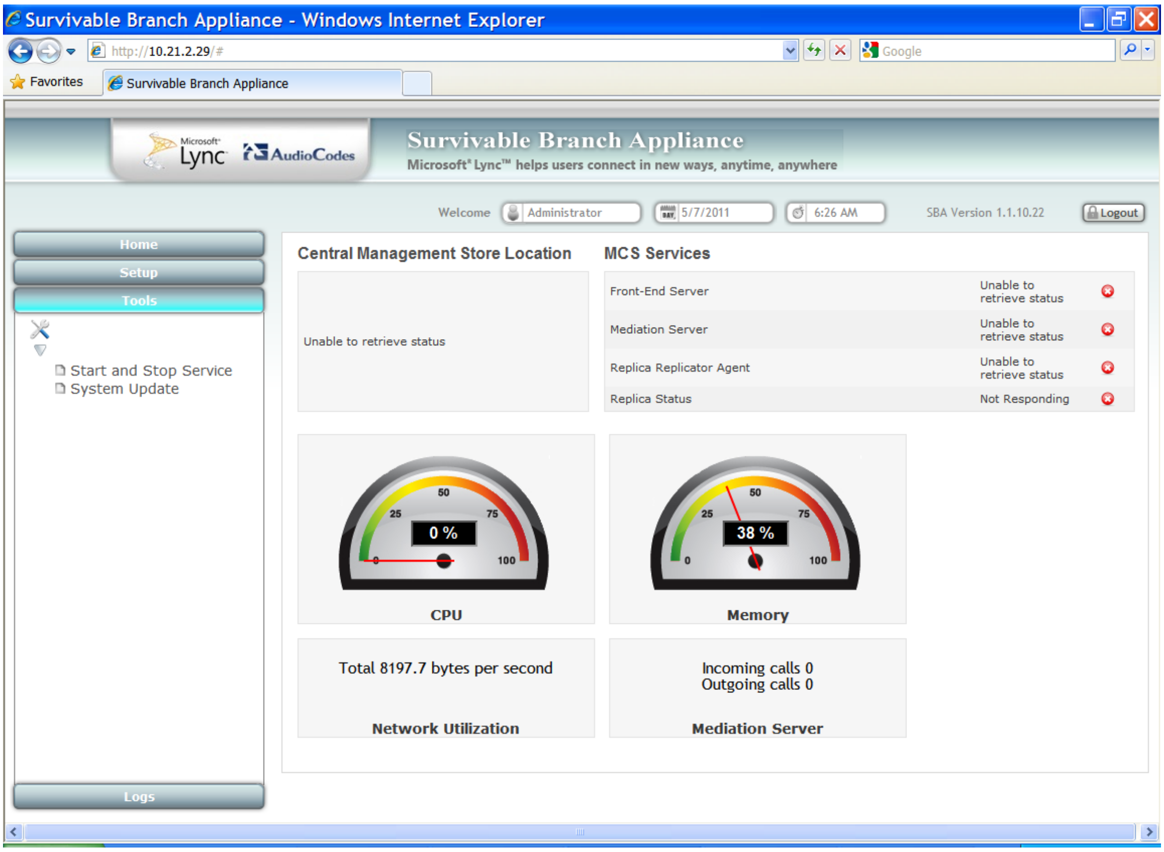
This section describes how to update SBA components using the SBA interface. The following components can be updated:

- SBA GUI components
- Microsoft Lync Server 2010 components

➢ To update SBA components:

1. In the Tools pane, select the **System Update** checkbox.

Figure 11-3: Tools-System Update Menu


Survivable Branch Appliance - Windows Internet Explorer
http://10.21.2.29/#
Google
Favorites
Survivable Branch Appliance
Microsoft Lync
AudioCodes
Survivable Branch Appliance
Microsoft® Lync™ helps users connect in new ways, anytime, anywhere
Logout
Home
Setup
Tools
Logs
50
25
75
0
100
CPU
Memory

Welcome Administrator 5/7/2011 6:26 AM SBA Version 1.1.10.22

Start and Stop Service
System Update

Central Management Store Location

Unable to retrieve status

MCS Services

Front-End Server	Unable to retrieve status
Mediation Server	Unable to retrieve status
Replica Replicator Agent	Unable to retrieve status
Replica Status	Not Responding

CPU: 0 %

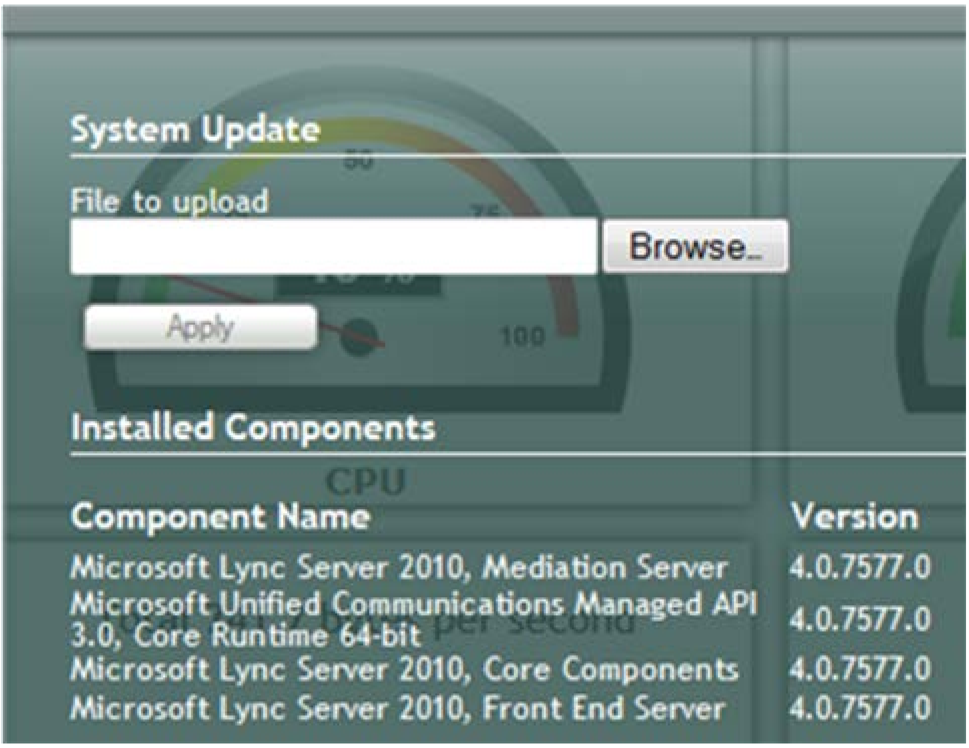
Memory: 38 %

Network Utilization: Total 8197.7 bytes per second

Mediation Server: Incoming calls 0 Outgoing calls 0

The System Update screen is displayed:

Figure 11-4:System Update Screen



System Update

File to upload

Installed Components

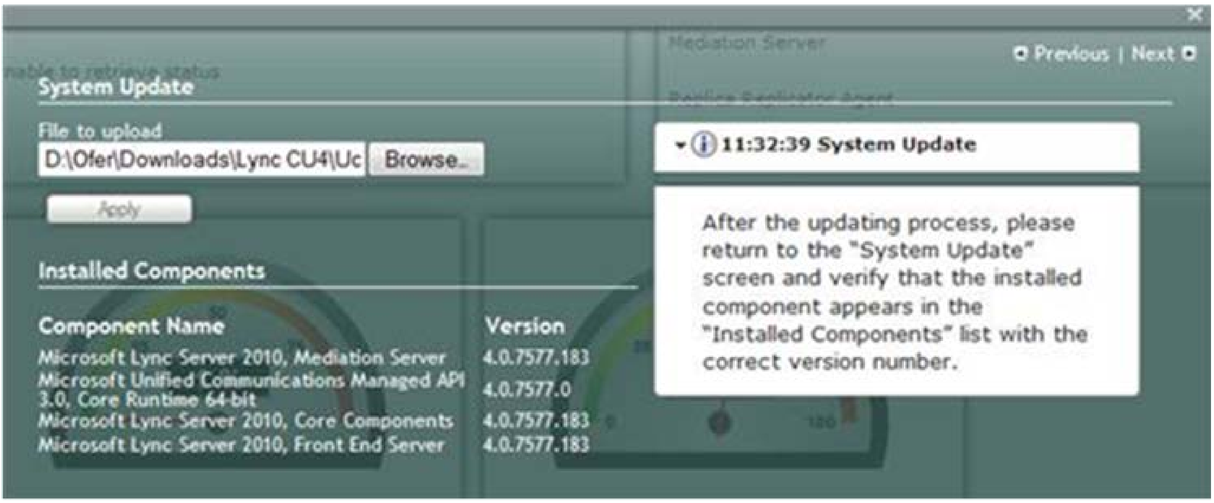
Component Name	Version
Microsoft Lync Server 2010, Mediation Server	4.0.7577.0
Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit	4.0.7577.0
Microsoft Lync Server 2010, Core Components	4.0.7577.0
Microsoft Lync Server 2010, Front End Server	4.0.7577.0

The currently installed SBA components are listed in the **Installed Components** pane.

2. In the ‘File to upload’ field, click **Browse** to select the file to upload and then click **Apply**.

   Choose either the SBA GUI file or the Microsoft Lync Server 2010 Components file; the following screen is displayed:

Figure 11-5:System Update Timestamp and Message



System Update

File to upload: D:\Ofer\Downloads\Lync CU4\Uc

Installed Components

Component Name	Version
Microsoft Lync Server 2010, Mediation Server	4.0.7577.183
Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit	4.0.7577.0
Microsoft Lync Server 2010, Core Components	4.0.7577.183
Microsoft Lync Server 2010, Front End Server	4.0.7577.183

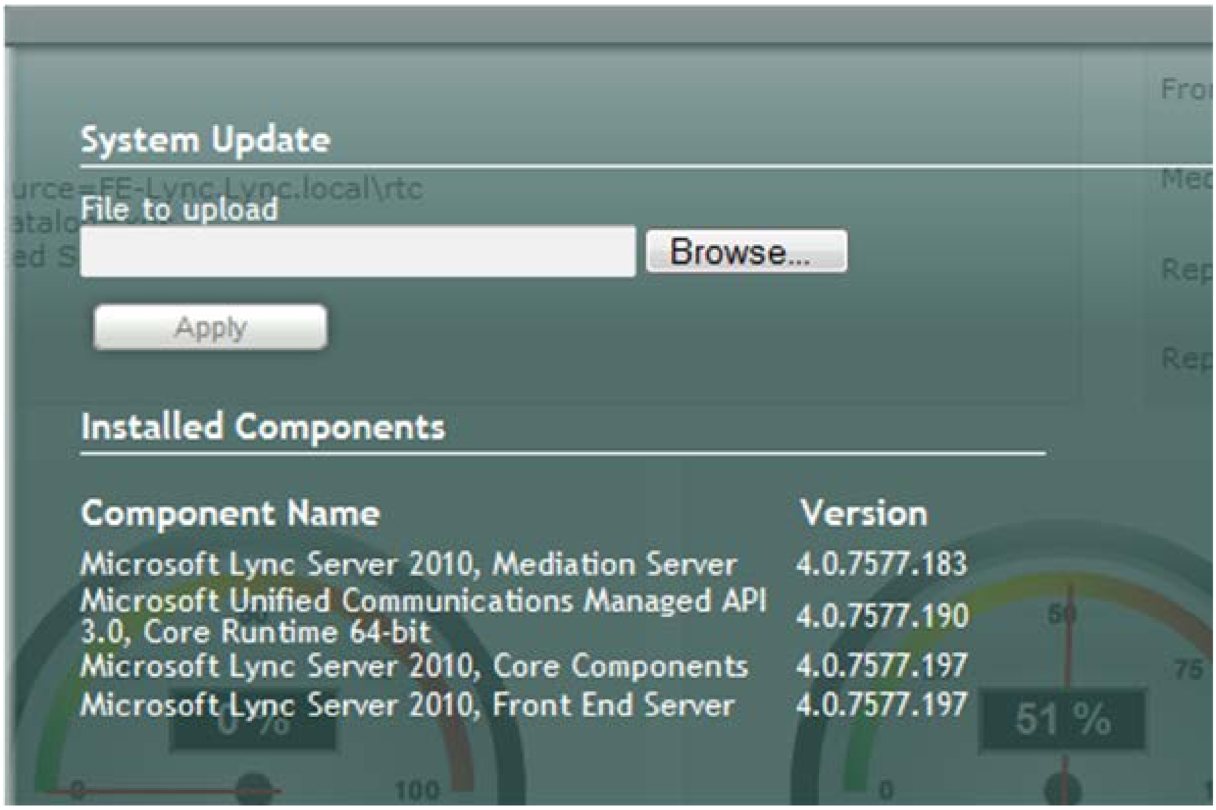
11:32:39 System Update

After the updating process, please return to the "System Update" screen and verify that the installed component appears in the "Installed Components" list with the correct version number.

A time-stamp of the time that you commenced the System Update is displayed in the right-hand pane.

3. Close the System Update screen and then reopen it; the following screen is displayed:

Figure 11-6: System Update Message-SBA System Components



System Update

File to upload

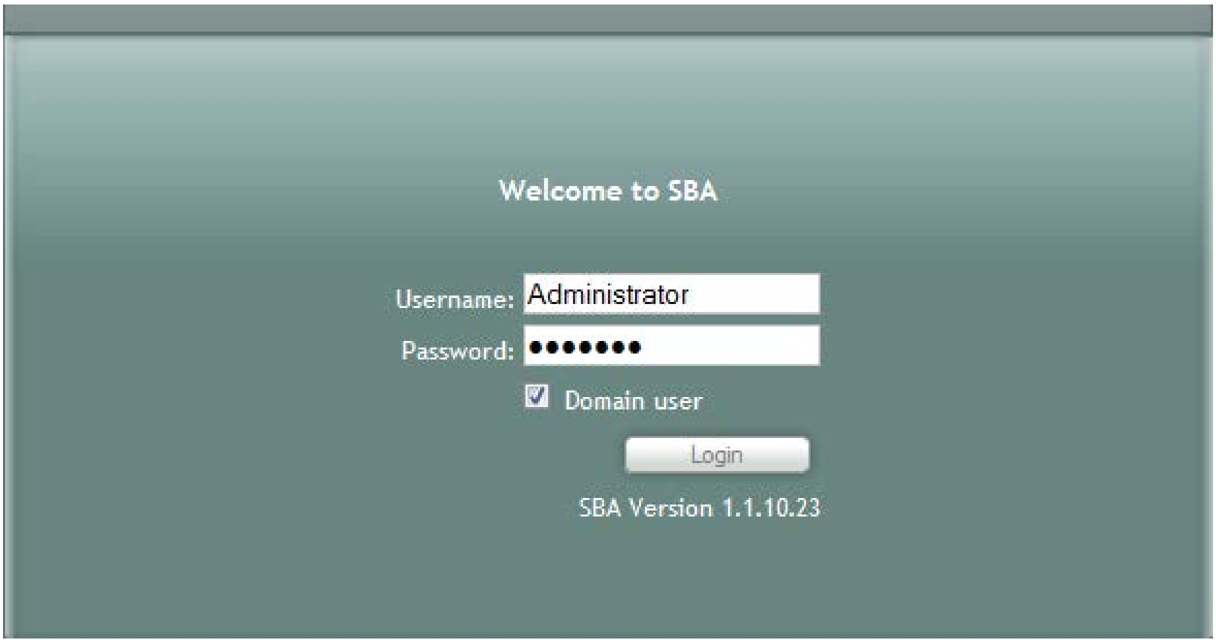
Installed Components

Component Name	Version
Microsoft Lync Server 2010, Mediation Server	4.0.7577.183
Microsoft Unified Communications Managed API 3.0, Core Runtime 64-bit	4.0.7577.190
Microsoft Lync Server 2010, Core Components	4.0.7577.197
Microsoft Lync Server 2010, Front End Server	4.0.7577.197

Note that in the above example, the version numbers have changed for the "Managed API" "Core Components" and the "Front End Server" components.

Wait a few minutes for the update to apply. At the end of the process, the System Logs out automatically and the login screen is displayed.

Figure 11-7: Login Screen after Automatic Log Out



Welcome to SBA

Username: Administrator

Password: •••••••

☑ Domain user

SBA Version 1.1.10.23

4. Do one of the following:
   - If you are updating SBA GUI components:
     a. In the Login screen, verify that the new SBA version number is displayed (if it does not appear, see step 'd' below).
     b. Enter your login and password details, and then click **Login**.
     c. Ensure that the new SBA version number is displayed in the SBA Home Page.
     d. Logout and Login again, and then ensure that the new SBA version number is displayed in the Login screen.
   - If you are updating Microsoft Lync Server 2010 components:
     a. Enter your login and password details, and then click **Login**.
     b. In the Tools menu, select the **System Update** checkbox.
     c. Verify that the new component and respective version number is displayed in the **Installed Components** pane.

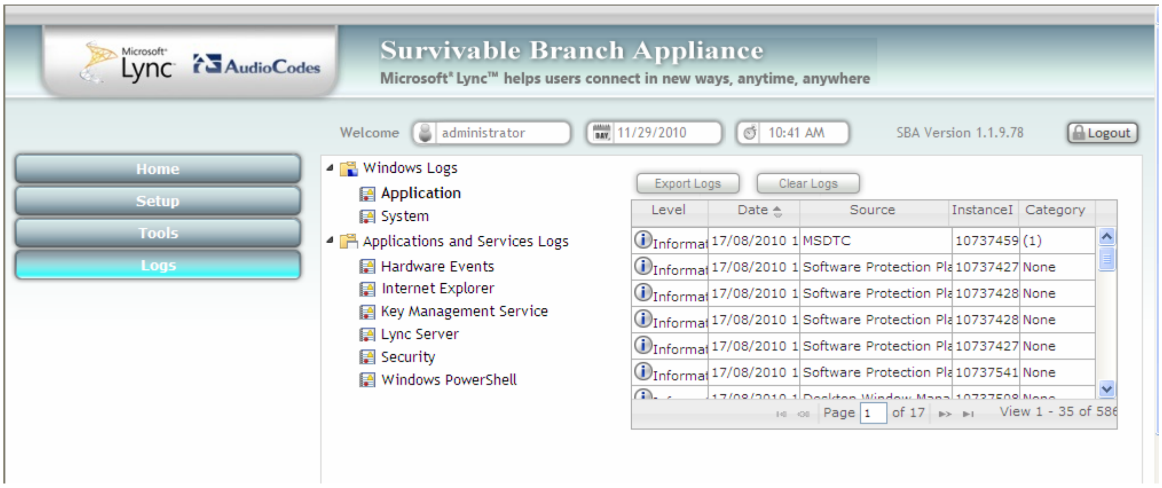
11.4 Viewing Logged Events

The procedure below describes how to view and handle logged events.

➢ To view and handle logged events:

1. Select the **Logs** menu tab; the Logs screen appears displaying logged events:

Figure 11-8: Logs Screen Displaying Logged Events

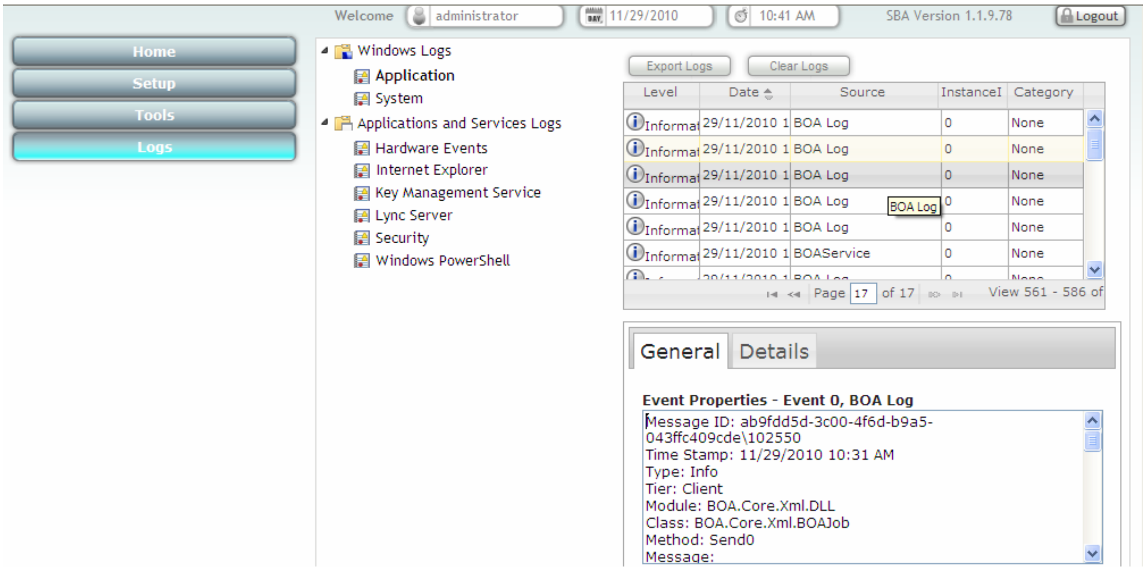


Level	Date	Source	InstanceI	Category
Informat	17/08/2010 1	MSDTC	10737459	(1)
Informat	17/08/2010 1	Software Protection Pla	10737427	None
Informat	17/08/2010 1	Software Protection Pla	10737428	None
Informat	17/08/2010 1	Software Protection Pla	10737428	None
Informat	17/08/2010 1	Software Protection Pla	10737427	None
Informat	17/08/2010 1	Software Protection Pla	10737541	None

Page 1 of 17 View 1 - 35 of 586

2. To view details of a logged event, select the event.

Figure 11-9: Detailed Log Display



Level	Date	Source	InstanceI	Category
Informat	29/11/2010 1	BOA Log	0	None
Informat	29/11/2010 1	BOA Log	0	None
Informat	29/11/2010 1	BOA Log	0	None
Informat	29/11/2010 1	BOA Log	0	None
Informat	29/11/2010 1	BOA Log	0	None
Informat	29/11/2010 1	BOAService	0	None

Page 17 of 17 View 561 - 586 of

Event Properties - Event 0, BOA Log

Message ID: ab9fdd5d-3c00-4f6d-b9a5-043ffc409cde\102550
Time Stamp: 11/29/2010 10:31 AM
Type: Info
Tier: Client
Module: BOA.Core.Xml.DLL
Class: BOA.Core.Xml.BOAJob
Method: Send0
Message:

3. To clear the displayed log, click the **Clear Logs** button. To export the logged events, click the **Export Logs**.

11.5 Logging Out

The procedure below describes how to log out the SBA wizard.

➢ To log out the SBA Web wizard:

- Click the **Logout** button.

SBA Installation Manual

www.audiocodes.com