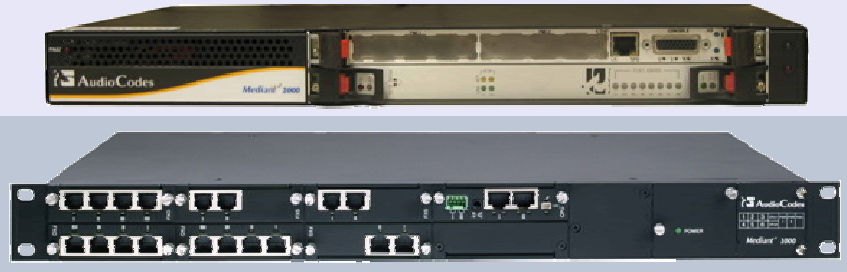
Mediant™ 1000, Mediant 1000 MSBG & Mediant 2000

AudioCodes Enhanced Media Gateway and SBA for Microsoft® Lync™

# Installation and Configuration Manual



Version 1.3

December 2010

Document # LTRT-18206

# Table of Contents

# List of Figures

# List of Tables

**Reader's Notes**

## Notice

This document describes the installation and configuration of AudioCodes' Enhanced Media Gateway and SBA for integration with Microsoft® Lync™ Server 2010.

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 can be viewed at http://www.audiocodes.com/downloads.



Date Published: December-8-2010

## Trademarks



## 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 provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com.

## Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used, and only Industry standard terms are used throughout this manual.

**Note:** Throughout this guide, the term *Media Gateway* refers to AudioCodes' Mediant 1000, Mediant 1000 MSBG, and Mediant 2000 devices.

**Reader's Notes**

# 1 Introduction

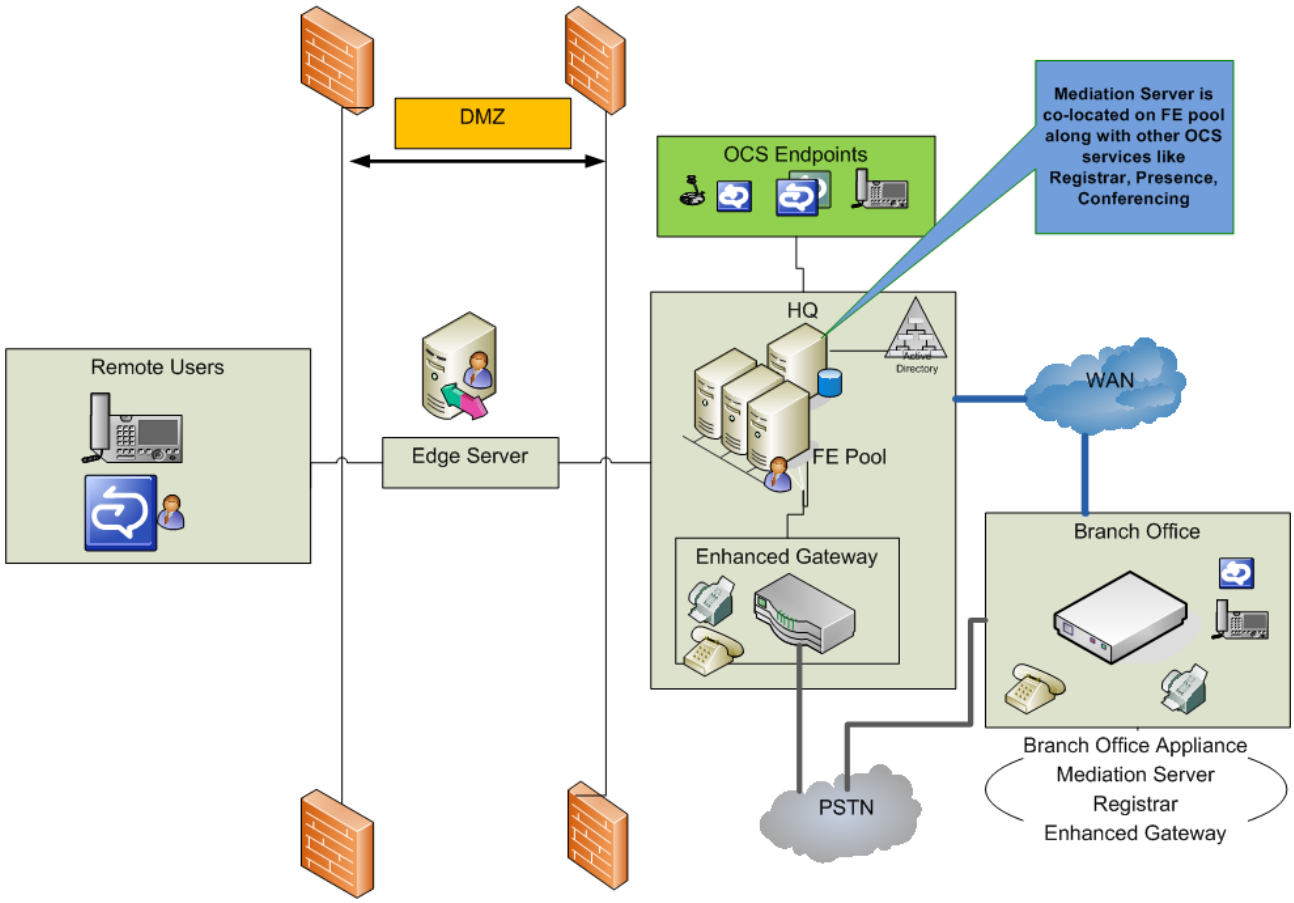
This document describes the configuration of AudioCodes Enhanced Media Gateway and its Survivable Branch Appliance (SBA) application hosted on AudioCodes Media Gateway, for integration with Microsoft® Lync™ Server 2010 (Lync Server 2010). The AudioCodes gateways that support this application include the Mediant 1000, Mediant 1000 MSBG, and Mediant 2000.

One of the components in the Lync Server 2010 network is the Microsoft Communication Server 2010 Mediation Server (*Mediation Server*). The Mediation Server can be deployed either on a standalone physical server or co-located with the Front End server pool. The latter is a new enhancement in Lync Server 2010. The Mediation Server is the Lync Server 2010 edge entity responsible for interfacing the Lync Server 2010 network with an Enhanced Media Gateway that provides legacy connections to the PSTN.

This solution is comprised of three main areas:

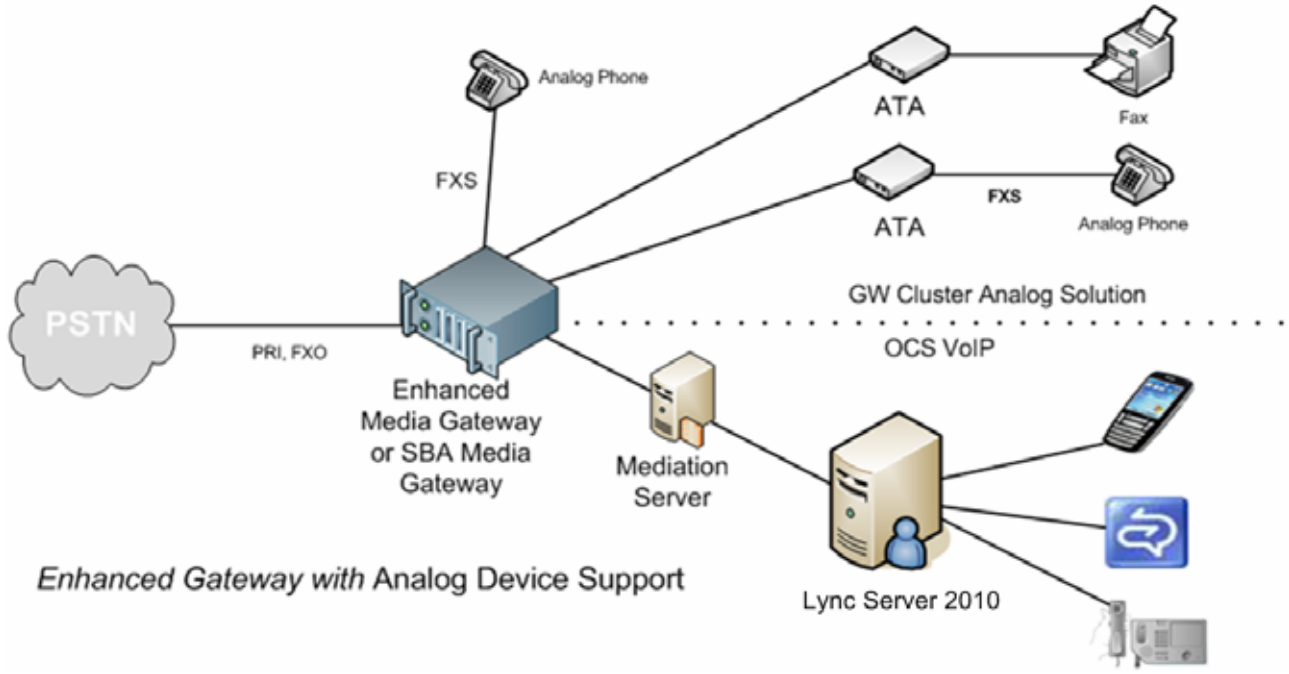
- **Enhanced Media Gateway:** The Enhanced Media Gateway is co-located at the enterprise's headquarters with Mediation Server and Lync Server 2010. The Enhanced Media Gateway interfaces between Mediation Server, analog devices and the PBX/PSTN.

**Figure 1-1: Unified Communication Network Topology with Enhanced Media Gateway for Connectivity to PSTN**



- **Support for Analog Devices:** In the Lync Server 2010 environment, the Enhanced Media Gateway provides support for analog devices such as analog phones and fax machines. The figure below illustrates the high-level architecture of such an environment:

**Figure 1-2: High-Level Architecture of Enhanced Media Gateway with Analog Devices**



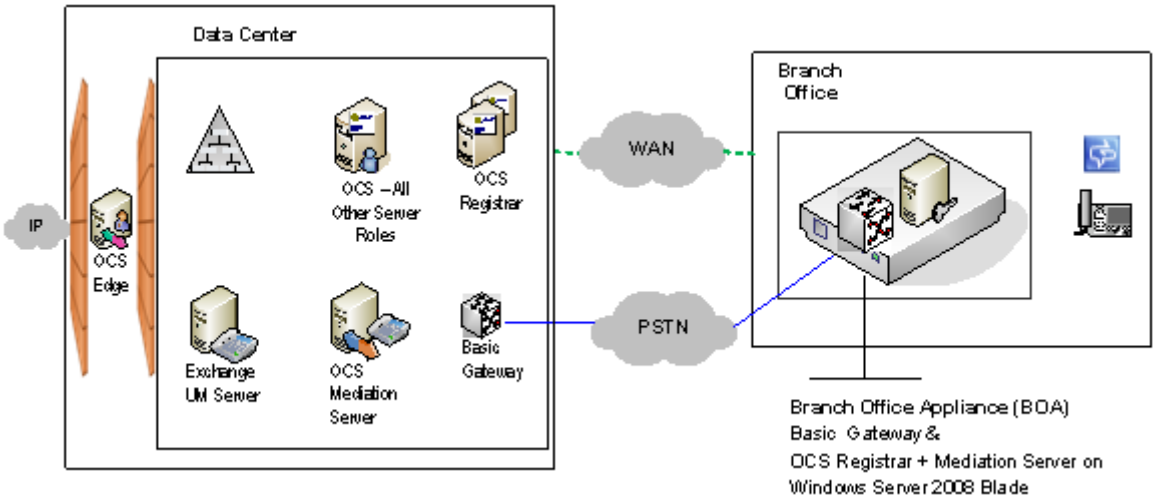

- **Survivable Branch Appliance (SBA):** In Office Communications Server 2007/R2 (OCS 2007), given the centralized deployment model, Unified Communication (UC) enabled users in a remote site are dependent on the servers in the data center for their communication and collaboration needs, and hence are 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 basic voice services to branch users during a WAN outage, a branch office survivability solution – the Survivable Branch Appliance (SBA) application - is hosted by AudioCodes Media Gateway at the branch office. The SBA provides call survivability when IP network connectivity fails, by maintaining call connectivity between Microsoft's Office Communicator (OC) clients themselves at the branch office, and between OC clients and the PSTN. This solution includes an **AudioCodes SBA Media Gateway** for PSTN termination.

The SBA Media Gateway hosting the SBA application is located at the enterprise's branch office. The hosting method for the SBA application depends on the Media Gateway:

- **Mediant 1000 and Mediant 1000 MSBG:** hosted on the OSN3 Server platform
- **Mediant 2000:** hosted on the Single Board Computer (SBC) blade

**Figure 1-3: AudioCodes SBA Media Gateway Solution at Branch Office**



## 1.1 How to Read this Document

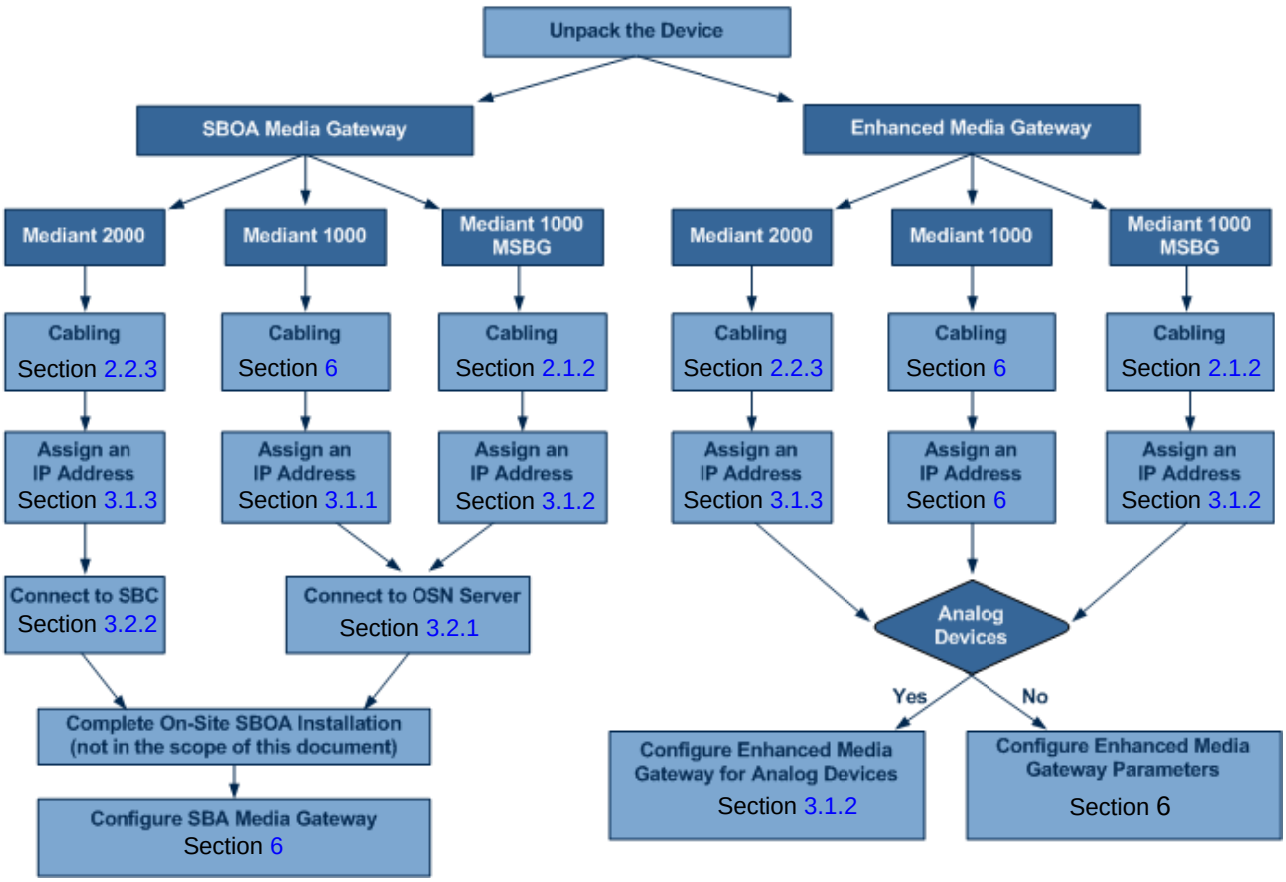
This document provides step-by-step procedures for configuring AudioCodes Enhanced Media Gateway and Survivable Branch Appliance (SBA) application hosted on AudioCodes SBA Media Gateway, deployed in the Lync 2010 environment.

**Note:** This document applies to AudioCodes Media Gateways running software version 6.0A.021 or later.

This document is organized into the following sections:

- **Section 2:** describes the hardware installation of AudioCodes Mediant 1000, Mediant 1000 MSBG and Mediant 2000 Media Gateways.
- **Section 3:** describes how to initialize the Media Gateway by assigning IP addresses as well as how to connect to the OSN server hosting the SBA application to complete the SBA on-site/on-domain installation.
- **Section 4:** provides step-by-step procedures for configuring the Enhanced Media Gateway to operate with Mediation Server.
- **Section 5**: provides step-by-step procedures for configuring the Enhanced Media Gateway to support the required analog devices.
- **Section 6:** provides a description for configuring the SBA Media Gateway to support the SBA application.

**Figure 1-4: Configuration Flowchart**



# 2 Hardware Installation

This section describes the hardware installation procedures for the following AudioCodes gateways:

- Mediant 1000/Mediant 1000 MSBG
- Mediant 2000

## 2.1 Mediant 1000/Mediant 1000 MSBG

The Mediant 1000B chassis is provided only if support for OSN3 is required. The Mediant 1000B chassis provides eight Advanced Mezzanine Card (AMC) or AdvancedMC form-factor modules for housing the OSN3 server AMC-based modules (single and mid-sized AMC modules) on its rear panel. The OSN3 can also be provided with dual SATA hard-disk drives (HDD).

**Note:** Any usage of additional AMC modules that are not described or mentioned in this document requires approval by AudioCodes.

### 2.1.1 Physical Description

This section provides a physical description of the Mediant 1000.

#### 2.1.1.1 Front-Panel Description

The Mediant 1000B chassis' front panel is displayed in the figure below and described in Table 2-1.

**Figure 2-1: Front-Panel Components**

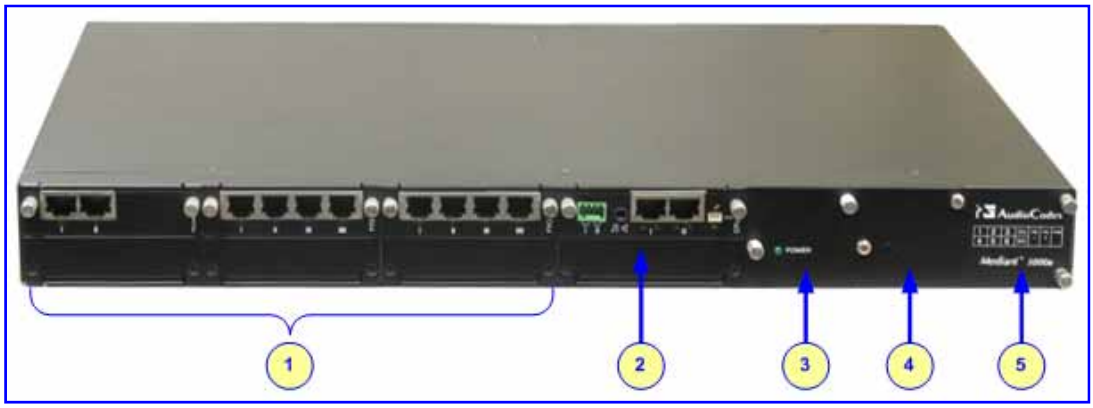



**Table 2-1: Front-Panel Component Description**

| Item # | Label | Description |
|---|---|---|
| 1 | **FXS**, **FXO**, **TRUNKS**, **BRI**, **MPM** | Telephony modules. |
| 2 | **CRMX** or **CMX** | Hosts either the CRMX module (for data routing) or the CMX module (CPU for VoIP gateway functionality) |
| 3 | **Power 1** | (Optional) Spare Power Supply module slot |
| 4 | **Power 2** | Main Power Supply module |
| 5 | - | Extractable Fan Tray module with a schematic displayed showing the chassis' slot numbers |

### 2.1.1.2 Rear-Panel Description

The Mediant 1000B chassis' front panel is displayed in the figure below and described in Table 2-2.

**Figure 2-2: Rear-Panel Components**

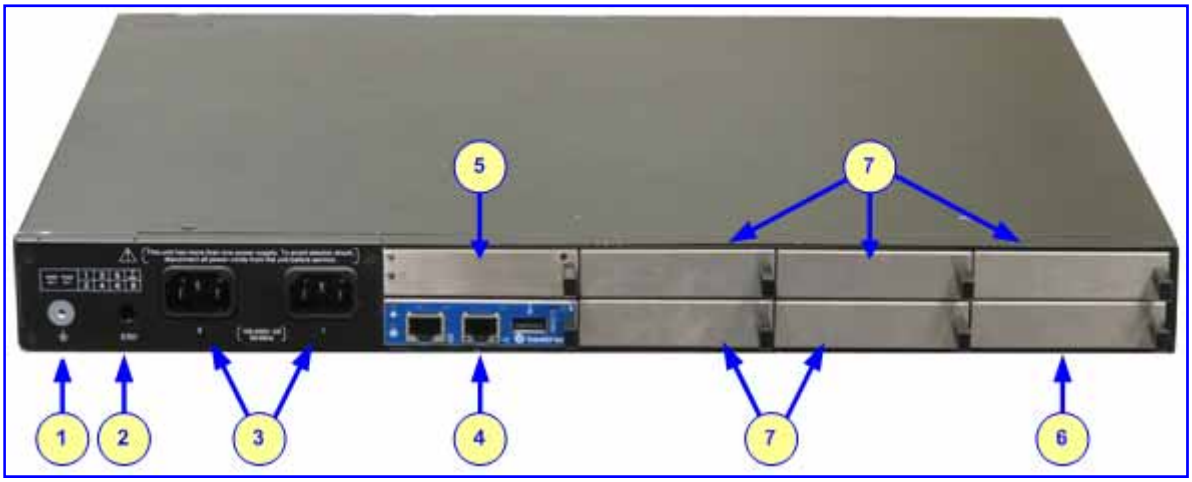



**Table 2-2: Rear-Panel Component Descriptions**

| Item # | Label | Description |
|---|---|---|
| **1** | ⏚ | Protective earthing screw. |
| **2** | ESD | Electrostatic Discharge (ESD) socket. |
| **3** | 100-240V~1A | Dual AC Power Supply Entries. |
| **4** | OSN3 | OSN3 AMC module. |
| **5** | HDD | Main Hard-disk drive (HDD) AMC module for OSN3 platform. |
| **6** | HDD | Second, optional HDD for OSN3 platform. |
| **7** | - | Empty AMC module slots. |

### 2.1.1.3 OSN3 Modules (for SBA Media Gateway)

The OSN3 platform consists of two main AMC modules:

- OSN3, providing the port connector interfaces (refer to Section 2.1.1.3 on page 19)
- HDMX, providing the hard-disk drive (refer to Section 2.1.1.3.2 on page 22)

The table below lists the specifications of the OSN3 server platform:

**Table 2-3: OSN3 Specifications**

| Parameter | Specification |
|---|---|
| CPU | Intel® Core™ 2 Duo 1.5 GHz processors L7400 with Intel 3100 Chipset (64-bit) |
| RAM Memory | 2 G or 4 G DDR2 with ECC |
| Storage | Single or Dual hard-disk drive of 80 G SATA |
| Bus/Chipset | 64 Bit |
| L2 Cache | 2 M |
| Interfaces | ▪ Gigabit Ethernet<br>▪ USB 2.0 via Connection Module<br>▪ RS-232 COM |

#### 2.1.1.3.1 OSN3 Module

The OSN3 module connector ports are shown in the figure below and described in Table 2-4.

**Figure 2-3: OSN3 Module Ports**

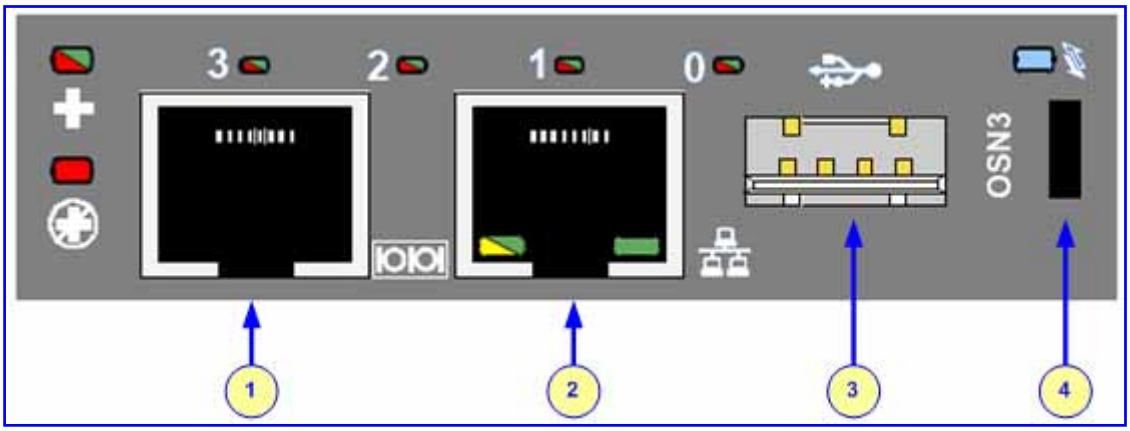



**Table 2-4: OSN3 Module Component Description**

| Item # | Description |
|---|---|
| **1** | RJ-45 port for RS-232 serial interface (COM1) |
| **2** | RJ-45 port for Gigabit Ethernet. The interface provides automatic detection and switching between 10Base-T, 100Base-TX and 1000Base-T data transmission (Auto-Negotiation). Auto-wire switching for crossed cables is also supported (Auto-MDI/X). |
| **3** | USB 2.0 port |
| **4** | Insertion/extraction handle |

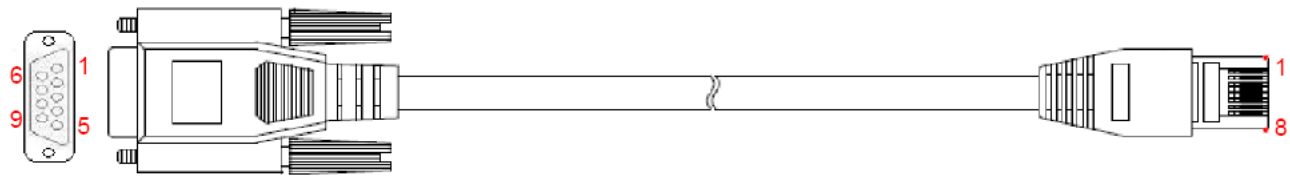
The RJ-45 connector pinouts for Gigabit Ethernet interface are listed in the table below:

**Table 2-5: Gigabit Ethernet Interface (RJ-45) Connector Pinouts**

| Pin | 100Base-Tx | | 1000Base-T | |
|---|---|---|---|---|
| | I/O | Signal | Signal | Function |
| **1** | O | Tx+ | I/O | BI_DA+ |
| **2** | 0 | Tx- | I/O | BI_DA- |
| **3** | I | Rx+ | I/O | BI_DB+ |
| **4** | | | I/O | BI_DC+ |
| **5** | | | I/O | BI_DC- |
| **6** | **I** | Rx- | I/O | BI_DB- |
| **7** | | | I/O | BI_DD+ |
| **8** | | | I/O | BI_DD- |

Serial cabling uses an RJ-45 to DB-9 female cable adapter (supplied), as shown below:

**Figure 2-4: RJ-45 to DB-9 Serial Cable Adapter**




The RJ-45 connector pinouts for RS-232 interface are listed in the table below:

**Table 2-6: RS-232 Serial Interface (Connector Pinouts**

| RJ-45 | | | DB-9 |
|---|---|---|---|
| **Pin** | **Signal** | **Function** | **Pin** |
| **1** | RTS | Request to send | 8 |
| **2** | DTR | Data terminal ready | 6 |
| **3** | TXD | Transmit data | 2 |
| **4** | GND | Signal ground | 5 |
| **5** | GND | Signal ground | 5 |
| **6** | RXD | Receive data | 3 |
| **7** | DSR | Data send ready | 4 |
| **8** | CTS | Clear to send | 7 |

The OSN3 LEDs are shown in the figure below and described Table 2-7.

**Figure 2-5: OSN3 LEDs**

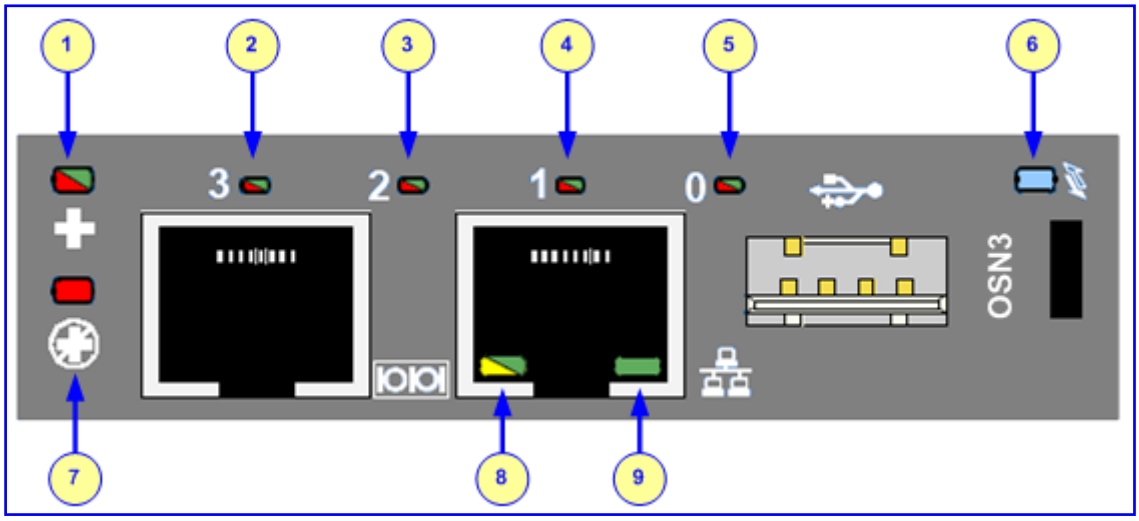



**Table 2-7: OSN3 Module LED Description**

| Item # | Color | State | Description |
|---|---|---|---|
| 1 | **Red** | On | Damaged hardware |
| | **-** | Off | Normal operation |
| 2 | **Red** | On | When lit during boot-up, indicates power failure. |
| | | Flashing | Processor over-temperature above 125°C and processor over-temperature above 100°C. |
| | **-** | Off | Normal operation. |
| 3 | **Red** | On | When lit during boot-up, indicates clock failure. |
| | | Flashing | Processor over-temperature above 125°C and chipset over-temperature above 105°C. |
| | **-** | Off | Normal operation. |
| 4 | **Red** | On | When lit during boot-up, indicates a hardware reset. |
| | | Flashing | Processor over-temperature above 125°C. |
| | **-** | Off | Normal operation. |
| 5 | **Red** | On | When lit up during boot-up, indicates a BIOS boot failure. |
| | | Flashing | Processor over-temperature above 125°C. |
| | **-** | Off | Normal operation. |

| Item # | Color | State | Description |
|---|---|---|---|
| 6 | Blue | Flashing | Module undergoing shutdown sequence when module pulled out to first extraction position. |
| | | On | Module shutdown sequence complete and the module can be extracted from the chassis slot. |
| | | Off | Module correctly inserted in chassis slot |
| 7 | Red | On | Out of Service |
| | | Flashing | Upgrade |
| | - | Off | Normal operation |
| 8 | Green | On | 100Base-TX connection. |
| | Yellow | On | 1000Base-T connection |
| | - | Off | 10Base-T connection if ACT LED active. |
| 9 | Green | On | Valid Ethernet link (cable connection) has been established. |
| | - | Off | The LED goes temporarily off if network packets are being sent or received through the RJ-45 port. When this LED remains off, a valid link has not been established due to a missing or a faulty cable connection. |

### 2.1.1.3.2 HDMX (Hard-Disk Drive) Module

The components of the HDMX module is shown in the figure below and described in Table 2-7.

**Figure 2-6: HDMX Module Components**


**Table 2-8: HDMX Module LED Description**

| Item # | Color | State | Description |
|---|---|---|---|
| 1 | Green | On | Power received by HDD. |
| | - | Off | No power received by HDD. |
| 2 | Blue | Flashing | Module undergoing shutdown sequence when module pulled out to first extraction position. |
| | | On | Module shutdown sequence complete and the module can be extracted from the chassis slot. |
| | | Off | Module correctly inserted in chassis slot |
| 1 | Red | Flashing | The OSN server's hard disk drive (HDD) is in use (active). |
| | - | Off | Hard disk drive not in use. |

### 2.1.1.3.3 Inserting and Extracting AMC Modules

The OSN3 modules are designed for hot-swappable operation. Hot swapping allows the coordinated insertion and extraction of modules without disrupting other operational elements within the system. This allows for identified faulty elements to be removed and replaced without taking the entire device out of service. In addition, the AMC module's insertion-extraction handle allows for quick-and-easy replacement of faulty modules.

The following procedure describes how to insert an AMC module into the chassis slot.

➢ **To insert the module:**

1. Carefully insert the module into the slot until it makes contact with the AMC card-edge connector located on the backplane.
2. Connect all external interfacing cables to the module as required.
3. Using the handle on the front panel, engage the module with the chassis backplane.
4. When the handle is locked, the module is engaged; the HS LED turns off.

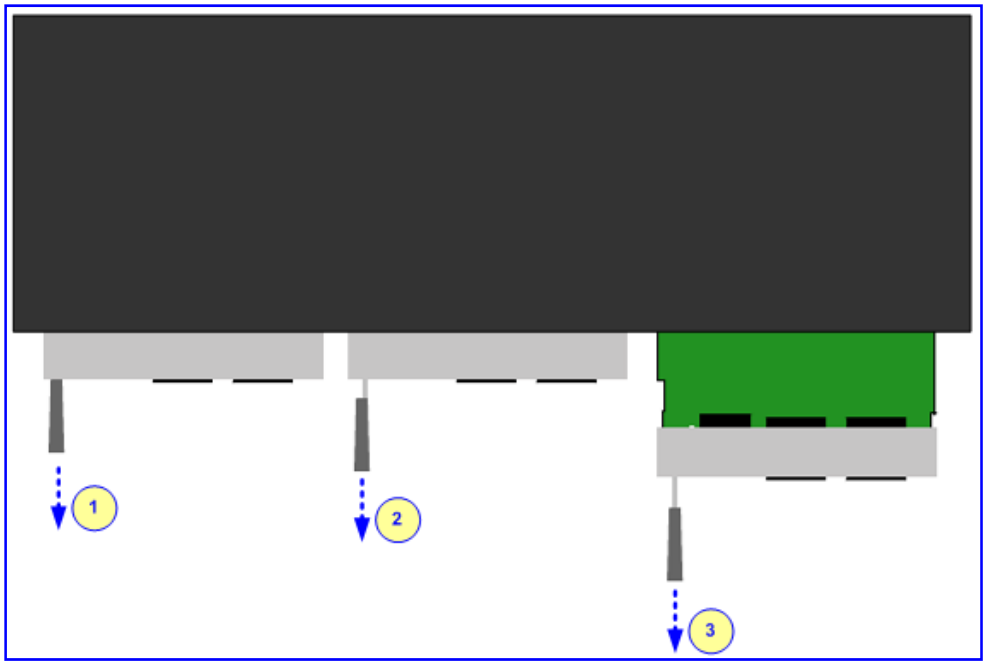
The following procedure describes how to extract an AMC module from the chassis.

**Note:** Before extracting the HDMX module (if required), you must perform a hard-disk drive dismount (i.e., a logical disconnection of the hard drive).

➢ **To extract the module:**

1. Pull the handle on the module's front panel and semi extract the module to the first "click"; the module performs a shutdown sequence indicated by the flashing blue **Hot Swap** LED (see stages 1 and 2 in the figure below).
2. When the LED stops flashing and remains constantly on, disconnect any interfacing cables that may be connected to the module.
3. Using the module's handle, pull the module out of the slot (see stage 3 in the figure below).

**Figure 2-7: Extracting AMC Modules**



## 2.1.2 Cabling

### 2.1.2.1 Connecting to Earth (Ground)

The device must be permanently connected to earth (ground), using an equipment-earthing conductor.

**Protective Earthing**

The equipment is classified as Class I EN60950 and UL60950 and must be earthed at all times.

➢ **To earth the device:**

1. Connect an electrically earthed strap of 16 AWG wire (minimum) to the chassis' earthing screw (located on the rear panel), using the supplied washer.
2. Connect the other end of the strap to a protective earthing. This should be in accordance with the regulations enforced in the country of installation.

**Figure 2-8: Earthing the Device**


### 2.1.2.2 Connecting to Network

The connection to the network depends on the module housed in the device's chassis:

- CMX (refer to Section 2.1.2.2.1)
- CRMX (refer to Section 2.1.2.2.2)

#### 2.1.2.2.1 CMX Module

The device's CPU module provides two 10/100Base-TX RJ-45 ports for connectivity to the Ethernet network (IP network). The dual ports provide Ethernet redundancy.

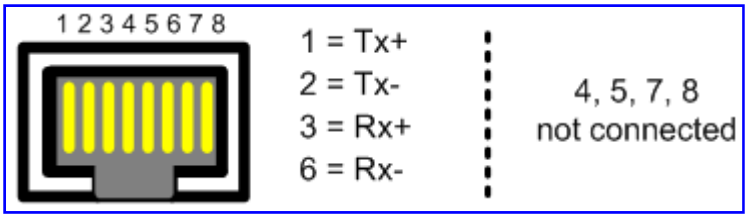
**Figure 2-9: CMX Module**


➢ **To connect the device to the IP/Ethernet network:**

1. On the CPU module, connect the first Ethernet port (labeled **I**) directly to the Ethernet network, using a straight-through RJ-45 Ethernet cable.
2. Optionally, for Ethernet redundancy, connect the second Ethernet port (labeled **II**) to the Ethernet network.

The RJ-45 connector pinouts are shown in the figure below:

**Figure 2-10: RJ-45 Connector Pinouts**




**Notes:**

- For Ethernet redundancy, it's recommended to connect each of the Ethernet ports to a different switch.
- When assigning an IP address to the device using HTTP (refer to 'Assigning an IP Address Using HTTP' on page 47), you may be required to cable the Ethernet port differently.

### 2.1.2.2.2 CRMX Module

The type of WAN port interface depends on the CRMX module installed in the chassis:

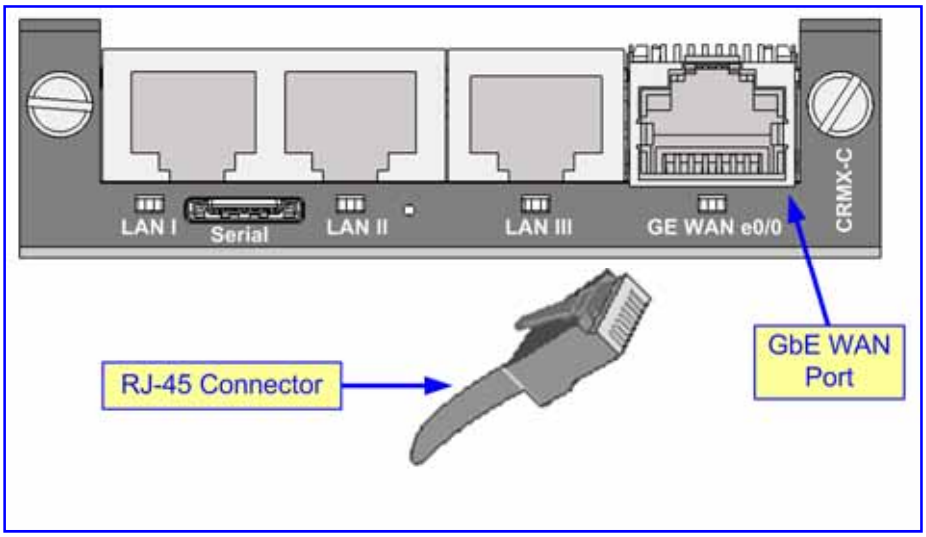
- **CRMX-C:** RJ-45 port (4-twisted pair copper cabling) providing 1 Gigabit Ethernet (GbE) interface for connection to the Internet
- **CRMX-S:** 1000Base-SX optical multi-mode fiber port
- **CRMX-L:** 1000Base-LX optical single-mode fiber port
- **CRMX-T:** RJ-48c (2-twisted pairs copper cabling) Channel Service Unit/Data Service Unit (DSU/CSU) T1 WAN port, for connecting to a T1 line

**Gigabit Ethernet Copper Cabling:** The CRMX-C module provides a 100/1000Base-TX Gigabit Ethernet RJ-45 port for connection to the Wide Area Network (WAN).

➢ **To connect the device to the WAN using the GbE port:**

1. Attach one end of a straight-through RJ-45 Ethernet Cat 6 or Cat 5e (two-pair Category 5 UTP) cable to the module's WAN port (labeled **GE WAN**).

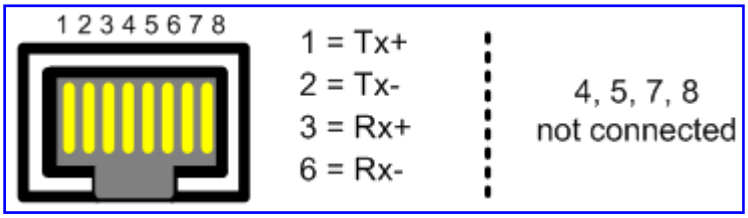
**Figure 2-11: Connecting the GbE WAN Port**




2. Attach the other end of the cable directly to the WAN network (e.g., to a ADSL or Cable modem).

The RJ-45 connector pinouts are shown in the figure below:

**Figure 2-12: RJ-45 Connector Pinouts**




**Optical Fiber Cabling:** The CRMX-S and CRMX-L modules provide a 1000Base-SX and 1000Base-LX Gigabit Ethernet optical fiber port (multi- or single-mode fiber) respectively.

This WAN port provides a 1.25 Gbps optical small form-factor pluggable (SFP) transceiver. To interface with this SFP transceiver, you need to provide (i.e., not supplied) the following items:

- **Cable:** twin, single-mode or multi-mode optic fiber
  - Single-Mode Fiber 1000Base-LX:
    - Input Sensitivity: -20 dBm maximum
    - Output Power: -9 dBm minimum; -3 dBm maximum
  - Multi-Mode Fiber 1000Base-SX:
    - Input Sensitivity: -18 dBm maximum
    - Output Power: -9 dBm minimum; -3 dBm maximum
- **Connector:** LC-type plug

## Caution Laser

If the CRMX module's WAN port is ordered for optical fiber interface, then the device is a Class 1 LED/Laser emitting device, as defined by 21CFR 1040 and IEC825.

Do not stare directly into the beam or into fiber optic terminations as this can damage your eyesight. Avoid exposure to laser radiation by ensuring that you insert dust / EMI plugs into SFP transceiver modules to which no cables are connected. Laser radiation may be emitted from the aperture of the SFP transceiver modules when no cables are connected.

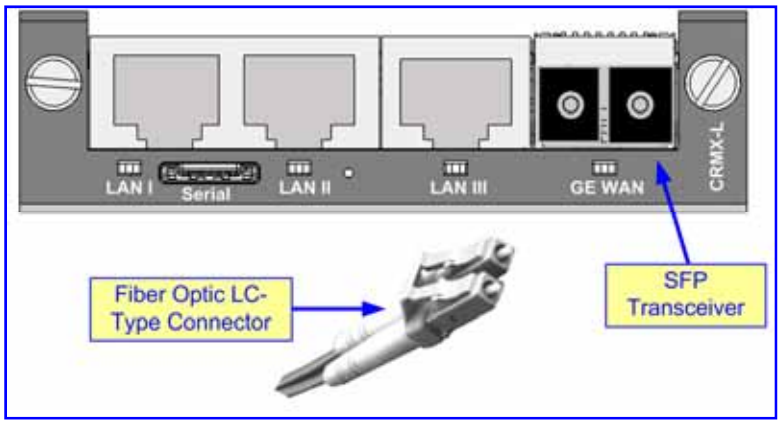
## Care in Handling Fiber Optic Cabling

- When handling fiber optic cables, be sure to implement the following:
  - Excessive bending of the Fiber Optic Cable can cause distortion and signal losses.
  - Ensure the minimum bending radius recommended by the Fiber Optic Cable supplier.
  - Maximum Fiber Optic cable length for multimode fiber is 550 m.
- Preserve the minimum-bending ratio indicated by the cable manufacturer.

➢ **To connect the device to the WAN using optical fiber cabling:**

1. Remove the protective dust plug covering the WAN port's SFP transceiver.
2. Connect the LC-type plugs at the end of the fiber optic cable to the WAN port's SFP transceiver (labeled **GE WAN**).

**Figure 2-13: Connecting the SFP Fiber Optic WAN Port**




3. Connect the other end of the cable to the fiber network.

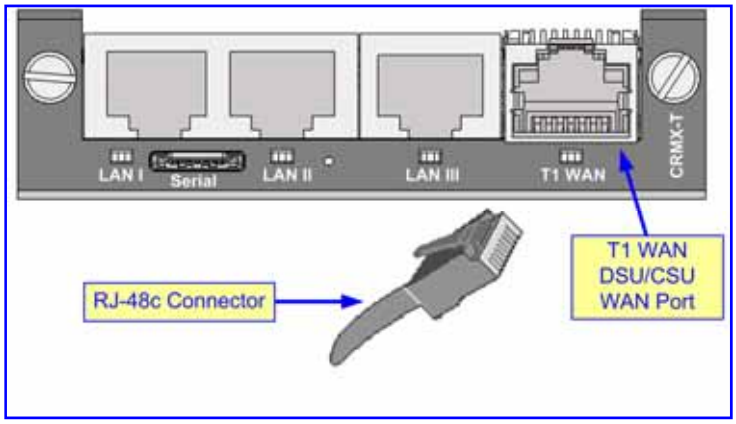
**T1 WAN DSU/CSU Cabling:** The CRMX-T module provides a WAN connection through a T1 line interface (according to ANSI T1.403-1999). The module's T1 WAN DSU/CSU port interface transmits and receives (1.544 Mbps) data using IP over Point-to-Point Protocol (PPP) or IP over High-Level Data Link Control (HDLC) framing.

**Warning:** To protect against electrical shock and fire, use a 26 AWG min wire to connect the T1 WAN port.

➢ **To connect the device's T1 WAN DSU/CSU port to a T1 line:**

1. Connect the RJ-48c T1 trunk cable to the device's T1 WAN port (labeled **T1 WAN**).

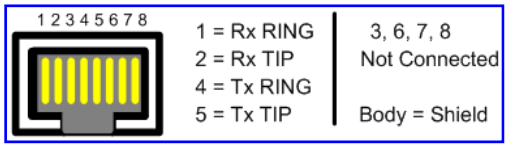
**Figure 2-14: Connecting the T1 WAN DSU/CSU Port**




2. Connect the other end of the cable to the T1 line.

RJ-48c trunk connectors are wired according to the figure below:

**Figure 2-15: RJ-48c Connector Pinouts for E1/T1**



### 2.1.2.3 Connecting to the LAN

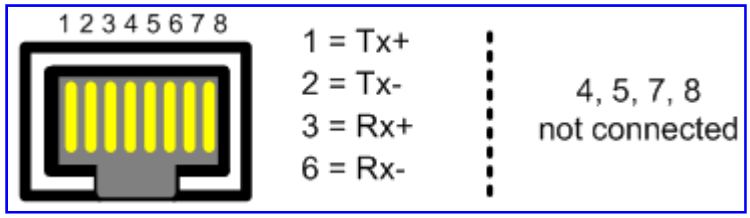
The device's CRMX/CMX module provides 10/100/1000Base-T Gigabit Ethernet RJ-45 ports for connection to the Local Area Network (LAN).

➢ **To connect the device to the LAN:**

- Using a straight-through RJ-45 Ethernet Cat 6 or Cat 5e (two-pair Category 5 UTP) cable, connect the CRMX/CMX module's LAN port/s to the LAN (e.g., PC or switch).

The RJ-45 connector pinouts are shown in the figure below:

**Figure 2-16: RJ-45 Connector Pinouts**




### 2.1.2.4 Connecting to FXS/FXO Interfaces

The procedure below describes the cabling of the device's FXS and FXO module analog interfaces.

**Warnings:**

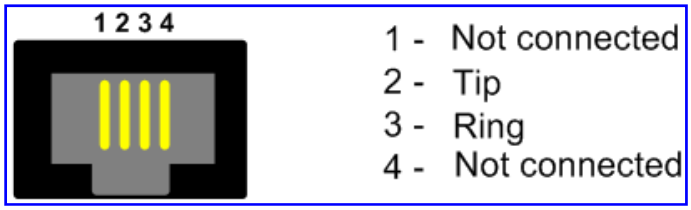
- To protect against electrical shock and fire, use a 26 AWG min wire to connect FXO ports to the PSTN.
- Ensure that FXS and FXO ports are connected to the appropriate, external devices; otherwise, damage to the device can occur.

➢ **To connect the FXS /FXO interfaces:**

- Using the device's RJ-11 connectors on the FXS/FXO module, connect the device to the required telephone interfaces:
  - **FXS:** connect the FXS module's ports to fax machines, modems, and/or telephones.
  - **FXO:** connect the FXO module's ports to telephone exchange analog lines or PBX extensions.

The RJ-11 connector pinouts are shown in the figure below:

**Figure 2-17: RJ-11 Connector Pinouts**



### 2.1.2.5 Connecting to E1/T1 Trunks

The procedure below describes the cabling of the device's TRUNKS module interfaces (i.e., E1/T1 trunks).

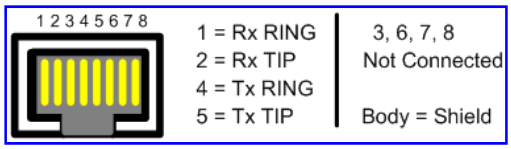
**Warning:** To protect against electrical shock and fire, use a 26 AWG min wire to connect T1 or E1 ports to the PSTN.

➢ **To connect the digital trunk interfaces:**

1. Connect the E1/T1 trunk cables to the ports on the device's **TRUNKS** module(s).
2. Connect the other ends of the trunk cables to your PBX/PSTN switch.

RJ-48c trunk connectors are wired according to the figure below:

**Figure 2-18: RJ-48c Connector Pinouts for E1/T1**




### 2.1.2.6 Connecting to Power

The device can house up to two extractable power supply modules (Power 1 and Power 2), each providing an AC power connector on the device's rear panel. The dual power option provides the device with power redundancy.

**Warnings:**

- Units must be connected (by service personnel) to a socket-outlet with a protective earthing connection.
- Use only the AC power cord supplied with the device.

➢ **To connect the device to the power supply:**

- On the device's rear panel, connect the left (active) 100-240V~50-60 Hz power socket to a standard electrical outlet using the supplied AC power cord.

The front panel of the power supply module provides a LED (labeled **POWER**) that is lit green when the device is powered up. If this LED is off, a power supply problem may be present.

**Notes:**

- If both power units are used (for load sharing - failure protection / redundancy), ensure that you connect each power supply unit to a different AC supply circuit.
- The two AC power sources must have the same ground potential.

# 2.2 Mediant 2000

This section provides a hardware description of and cabling procedures for the Mediant 2000 Single Board Computer (SBC) blade/server, which hosts Mediation Server. This SBC blade is housed in the second, optional slot on the Mediant 2000 chassis' front panel.

## 2.2.1 Physical Description

The SBC blade provides the following port interfaces:

- One 10/100/1000BaseTX RJ-45 port
- DB-26 female port, supporting interfaces for USB 2.0, RS 232, console screen, keyboard, and mouse.

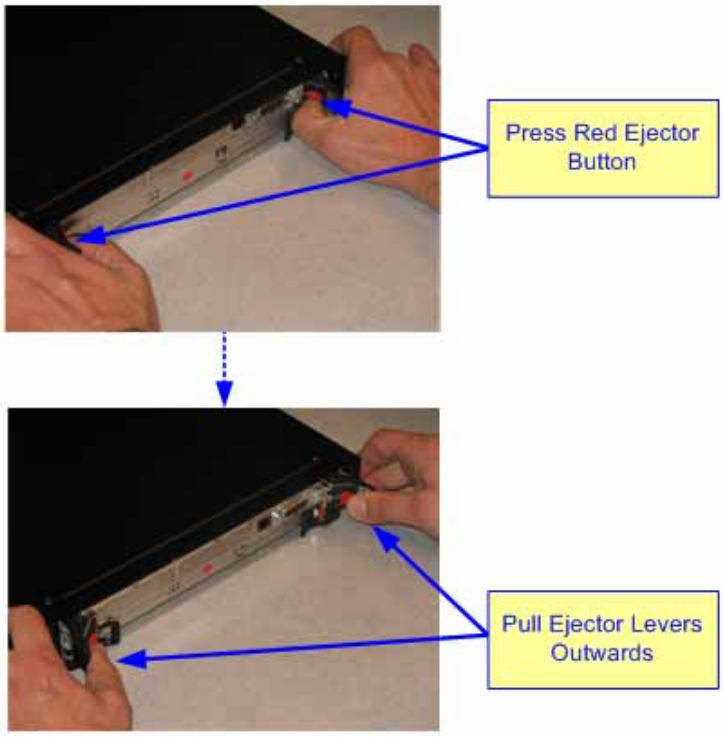
## 2.2.2 Removing / Inserting the SBC Blade

The SBC blade provides two ejector levels on either side for inserting and removing the blade into and from the Mediant 2000 chassis' front-panel slot.

➢ **To remove the blade:**

1. Disconnect all cables from the blade.
2. Unfasten the screws located at both ends of the blade, which secure the blade to the chassis.
3. Press the blade's red ejector buttons located on each of the two black ejector/injector levers.
4. Pull the two ejector/injector levers and gently ease the blade out of the slot.

**Figure 2-19: Removing the Blade**

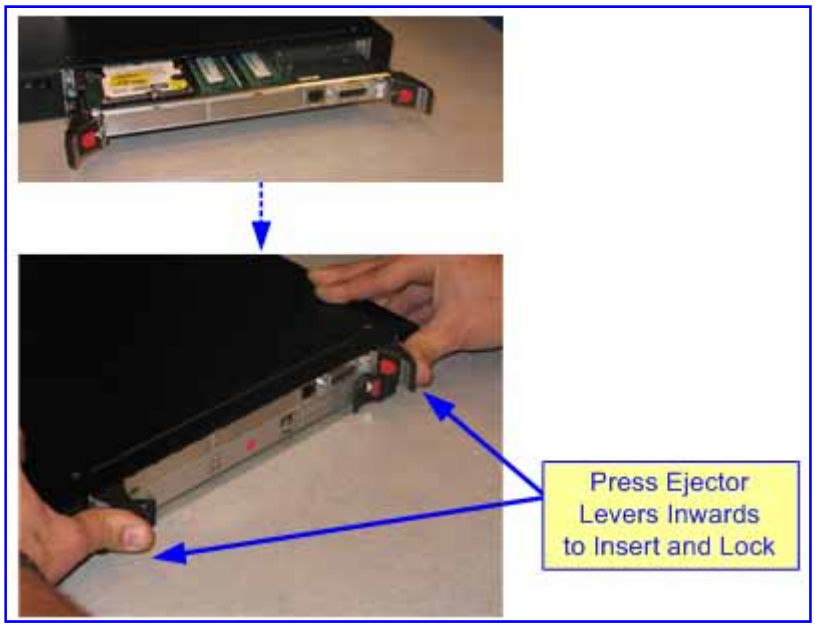



➢ **To insert a blade:**

1. Ensure that the blade's red ejector buttons are pressed-in (i.e., black ejector/injector latches in the open, pulled out position).
2. Hold the blade horizontally and insert the blade into the slot, aligning the blade edges with the groves inside the slot.
3. Ease the blade all the way into the slot until the ejector/injector levers touch the chassis.

4. Lock the blade into place by pressing the two black ejector/injector levers on both ends inward, until you hear a click.
5. Fasten the screws on the front of the blade to secure the blade to the chassis.

**Figure 2-20: Inserting Blade**



## 2.2.3 Cabling the Standard Interfaces

This section describes the cabling of the device.

**Electrical Earthing**

The device must be permanently connected to the earth using the screw provided on the rear panel. Use 14-16 AWG wire and a proper ring terminal for the earthing.

➢ **To cable the device:**

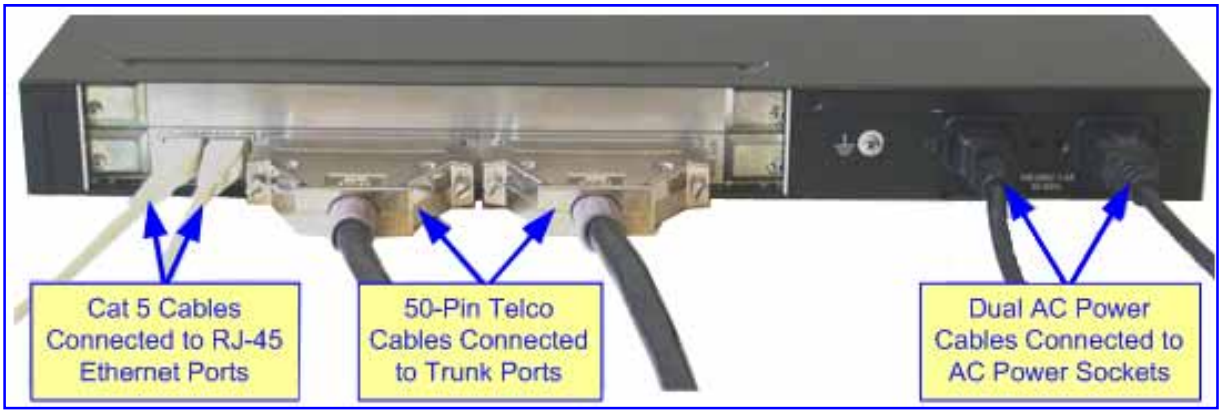
1. Permanently earth (ground) the device (refer to 'Earthing (Grounding) the Device' on page 33).
2. Connect the E1/T1 trunk interfaces (refer to 'Connecting the E1/T1 Trunk Interfaces' on page 33).
3. Connect the Ethernet interface (refer to 'Connecting the Ethernet Interface' on page 34).
4. Connect the power supply (refer to 'Connecting to the Power Supply' on page 34).

Once you have completed the above hardware installation steps, after powering-up the device the **Ready** and **LAN** LEDs on the front panel turn green (after a self-testing period of about three minutes). Any malfunction changes the **Ready** LED to red.

The cabling method of the device (performed on the rear panel), depends on the number of supported trunks (and power socket type):

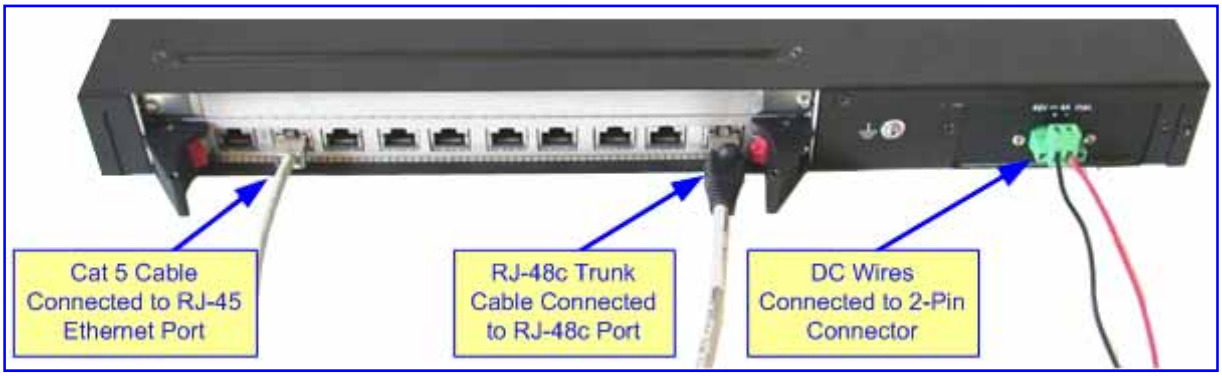
- Cabling for 16 trunks and dual AC power:

**Figure 2-21: Rear-Panel Cabling for 16 Trunks (Dual AC)**




- Cabling for eight trunks and DC power:

**Figure 2-22: Rear-Panel Cabling for 8 Trunks (DC Power)**



### 2.2.3.1 Earthing (Grounding) the Device

The device must be permanently connected to earth (ground), using an equipment-earthing conductor.

**Protective Earthing**

The equipment is classified as Class I EN60950 and UL60950 and must be earthed at all times.

➢ **To earth the device:**

1. Connect an electrically earthed strap of 16 AWG wire (minimum) to the chassis' earthing screw (located on the rear panel), using the supplied washer.
2. Connect the other end of the strap to a protective earthing. This should be in accordance with the regulations enforced in the country of installation.

### 2.2.3.2 Connecting the E1/T1 Trunk Interfaces

Connect the E1/T1 Trunk interfaces using either Telco (for devices with 16 spans) or RJ-48c (for devices with 1, 2, 4, or 8 spans) connectors.

➢ **To connect E1/T1 trunks using 50-pin Telco connectors (16-trunk device):**

1. Attach the Trunk cable's (of at least 26 AWG UTP) 50-pin male Telco connector to the 50-pin female Telco port (labeled **TRUNKS 1-8**) on the device's rear panel.
2. Connect the other end of the Trunk cable to the PBX/PSTN switch.
3. Repeat steps 1 through 2 for the second Trunk cable, but this time, connect it to the connector labeled **TRUNKS 9-16**.

The 50-pin male Telco cable connector must be wired according to the pinouts in the table below, and to mate with the female connector illustrated in the figure below.

**Figure 2-23: 50-pin Female Telco Board-Mounted Connector**

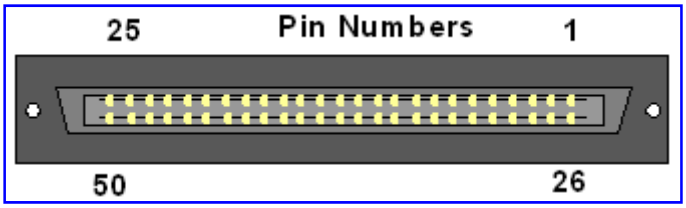



**Table 2-9: E1/T1 Connector Pinouts for Each 50-pin Telco Connector**

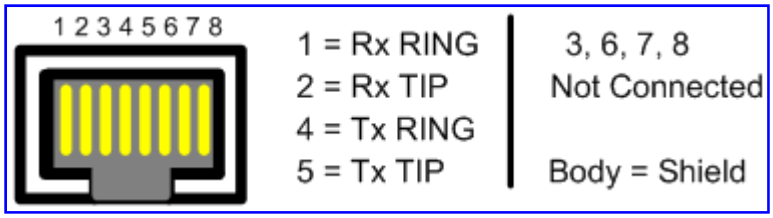
| E1/T1 Trunk Number | | Tx Pins (Tip/Ring) | Rx Pins (Tip/Ring) |
|---|---|---|---|
| 1 to 8 | 9 to 16 | | |
| 1 | 9 | 27/2 | 26/1 |
| 2 | 10 | 29/4 | 28/3 |
| 3 | 11 | 31/6 | 30/5 |
| 4 | 12 | 33/8 | 32/7 |
| 5 | 13 | 35/10 | 34/9 |
| 6 | 14 | 37/12 | 36/11 |
| 7 | 15 | 39/14 | 38/13 |
| 8 | 16 | 41/16 | 40/15 |

➢ **To connect E1/T1 trunks using RJ-48c connectors (1-, 2-, 4-, 8-trunk device):**

1. Connect the E1/T1 trunk cables to the ports labeled **PSTN 1 to 8** (in the case of the 8-trunk device) on the device's rear panel.
2. Connect the other ends of the Trunk cables to the PBX/PSTN switch.

RJ-48c trunk connectors are wired according to the connector pinouts shown in the figure below:

**Figure 2-24: RJ-48c Connector Pinouts**




### 2.2.3.3 Connecting the Ethernet Interface

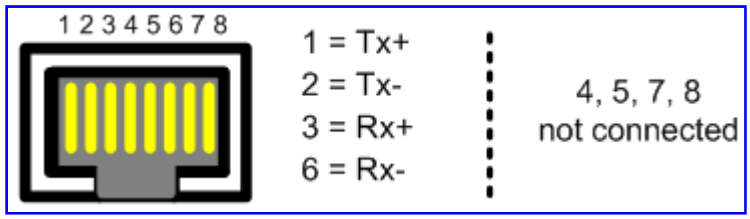
The device provides two 10/100Base-TX RJ-45 ports for connection to the Ethernet network. The dual ports provide Ethernet redundancy.

➢ **To connect the Ethernet interface:**

1. Connect a standard Category 5 network cable to the Ethernet RJ-45 port (labeled **ETH**) on the device's rear panel.
2. Connect the other end of the Category 5 network cable to your IP network.
3. For Ethernet redundancy/backup, repeat steps 1 through 2 for the second Ethernet port.

The RJ-45 connectors are wired according to the figure below:

**Figure 2-25: RJ-45 Connector Pinouts**




**Notes:**

- For Ethernet redundancy, it's recommended to connect each of the Ethernet connectors to a different switch.
- When assigning an IP address to the device using HTTP (refer to 'Assigning an IP Address Using HTTP' on page 47), you may be required to disconnect the Ethernet cable and re-cable it differently.

### 2.2.3.4 Connecting the Power Supply

The connection to the power supply depends on the supported hardware configuration:

- Single or dual AC power (refer to 'Connecting the AC Power Supply' on page 35).
- DC power (refer to 'Connecting the DC Power Supply' on page 35).

#### 2.2.3.4.1 Connecting the AC Power Supply

The device can support up to two AC power interfaces (single or dual).

**Warnings:**

- Units must be connected (by service personnel) to a socket-outlet with a protective earthing connection.
- Use only the AC power cord supplied with the device.

➢ **To connect the AC power cable:**

1. Attach one end of the 100/240 VAC power cable (supplied) to the rear AC socket.
2. Connect the other end of the power cable to an earthed AC power supply.
3. For connecting the second AC power socket (if power supply redundancy is supported), follow steps 1 through 2, but connect this second power cable to a separate earthed mains circuits.

**Note:** For dual AC power supply, please note the following:

- The LED on the left side of the chassis only functions when the dual AC is used. It is not relevant to the single AC power connection.
- If only one power socket is connected to the AC power (i.e., the other plug is left unconnected), the chassis' LED (on the left side) is lit red, indicating that one of the dual power inlets is disconnected.
- When both the AC power cables are connected, one of the plugs can be disconnected under power without affecting operation, in which case the chassis' left LED is lit red.
- A UPS can be connected to either (or both) of the AC connections.
- The dual AC connections operate in a 1+1 configuration and provide load-sharing redundancy.
- Each of the dual power cables can be connected to different AC power phases.

### 2.2.3.4.2 Connecting the DC Power Supply

The device can connect to a DC power supply using one of the following methods:

- DC terminal block with a screw connection type.
- DC terminal block with a crimp connection type.

➢ **To connect power using a DC terminal block screw connector:**

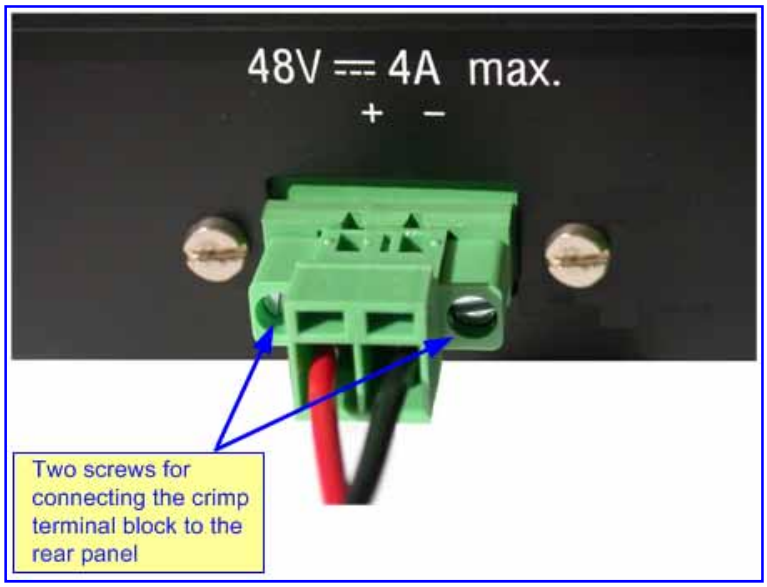
1. Create a DC cable by inserting two 14-16 AWG insulated wires into the supplied terminal block adaptor (refer to the figure below), and then fasten the two screws, each one located directly above each wire.
2. Connect the two insulated wires to the correct DC power supply. Ensure that the connections to the DC power supply maintain the correct polarity.
3. Insert the terminal block into the DC inlet located on the device's rear panel.

**Figure 2-26: DC Power Terminal Block Screw Connector**


➢ **To connect power using a DC terminal block crimp connector:**

1. Remove the DC adaptor (screw connection type) that is attached to the device's rear panel.
2. Connect the two insulated wires to the correct DC power supply. Ensure that the connections to the DC power supply maintain the correct polarity.
3. Insert the terminal block into the DC inlet located on the device's rear panel.

**Figure 2-27: DC Power Terminal Block Crimp Connector**



# 3 Initialization

This section describes the initial configuration required:

- Assigning an IP address to the gateways (refer to Section 3.1)
- Connecting to the SBA application (refer to Section 3.2)

## 3.1 Assigning the Gateway an IP Address

This section describes how to assign an IP address to the Media Gateway:

- Mediant 1000 (refer to Section 3.1.1)
- Mediant 1000 MSBG (refer to Section 3.1.2)
- Mediant 2000 (refer to Section 3.1.3)

### 3.1.1 Mediant 1000

This section describes how to change the device's default IP address so that it corresponds with your network environment. The table below lists the device's default IP address.

**Table 3-1: Default IP Addresses**

| Parameter | Default Value |
|---|---|
| **IP Address** | 10.1.10.10 |
| **Subnet Mask** | 255.255.0.0 |
| **Default Gateway IP Address** | 0.0.0.0 |

To assign an IP address to the device, use one of the following methods:

- Device's HTTP-based embedded Web server `accessed using a Web browser (refer to 'Assigning an IP Address using HTTP' on page 47).
- BootP (refer to 'Assigning an IP Address using BootP' on page 48).
- Voice Menu using a standard touch-tone telephone connected to one of the FXS analog ports (refer to 'Assigning an IP Address using the Voice Menu Guidance' on page 40).
- Embedded Command Line Interface (CLI), accessed using RS-232 or Telnet (refer to 'Assigning an IP Address using the CLI' on page 50).
- Dynamic Host Control Protocol (DHCP) - refer to the *User's Manual*.

**Tip:** If at a later stage after re-defining the IP address, your IP address is unknown (e.g., forgotten), use the BootP/TFTP utility to access the device (refer to the Product Reference Manual).

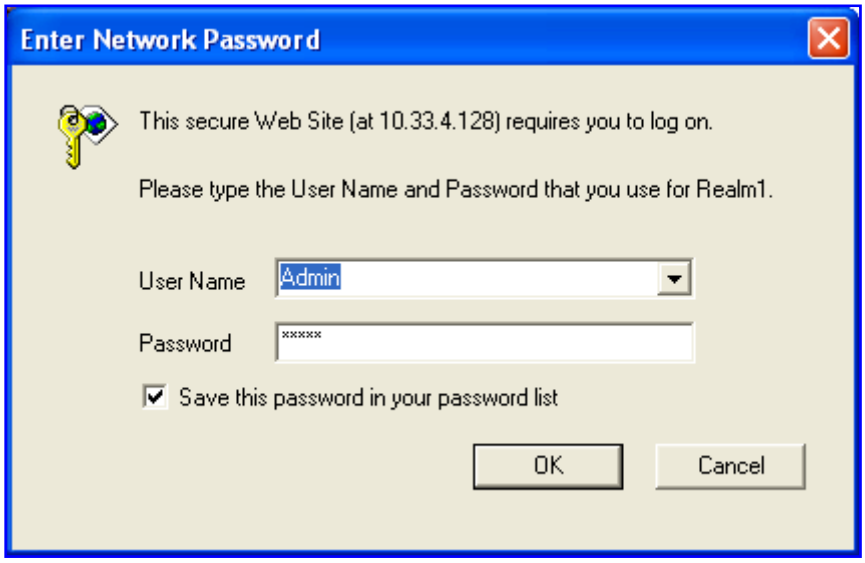
### 3.1.1.1 Assigning an IP Address using HTTP

You can assign an IP address to the device, using the device's Web interface.

➢ **To assign an IP address using HTTP:**

1. Disconnect the device from the network and reconnect it to a PC using one of the following methods:
   - **Using a hub or switch between a PC and the device:** Connect the network interface on your PC to a port on a network hub / switch, using a standard Ethernet cable. Connect the device to another port on the same network hub / switch, using another standard Ethernet cable.
   - **Direct connection between a PC and the device:** Connect the network interface on your PC directly to the device, using an Ethernet crossover cable.
2. Change your PC's IP address and subnet mask to correspond with the device's factory default IP address and subnet mask.
3. Access the device's Web interface:
   a. Open a standard Web browser application and in the Uniform Resource Locator (URL) field, enter the device's default IP address (e.g., http://10.1.10.10); the Web interface's 'Enter Network Password' dialog box appears, as shown in the figure below**:**

**Figure 3-1: Enter Network Password Screen**




   b. Enter the device's default login, case-sensitive user name ('Admin') and password ('Admin'), and then click **OK**; the Web interface is accessed, displaying the Web interface's 'Home' page.
4. Change the device's IP address, by performing the following:
   a. Open the 'Multiple Interface Table' page, (**Configuration** tab > **Network Settings** menu > **IP Settings**).
   b. Define the device's IP address, subnet mask, and default Gateway IP address (for "OAMP + Media + Control" application type) so that they correspond to your network IP scheme.
   c. Click **Apply**.
   d. Save your settings to the flash memory and reset the device.
5. Disconnect your PC from the device or from the hub/switch (depending on the connection method used in Step 1).
6. Reconnect the device and PC (if necessary) to the network.
7. Restore your PC's IP address and subnet mask to their original settings. If necessary, restart your PC and re-access the device via the Web interface with its newly assigned IP address.

### 3.1.1.2 Assigning an IP Address using BootP

You can assign an IP address to the device, using the supplied AudioCodes' BootP/TFTP Server application.

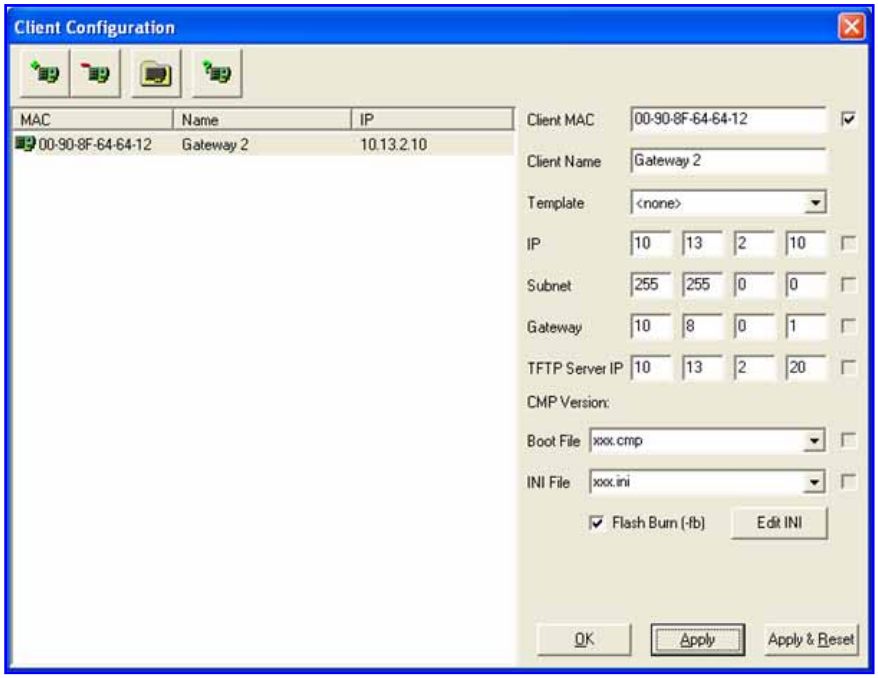
**Notes:**

- BootP procedure can also be performed using any standard compatible BootP server.
- For a detailed description of BootP, refer to the *Product Reference Manual.*

➢ **To assign an IP address using BootP:**

1. Start the BootP application.
2. From the Edit menu, choose **Preferences,** and then in the 'Preferences' dialog box, set the 'Timeout' field to 50.
3. From the Services menu, choose **Clients**; the 'Client Configuration' dialog box appears.
4. Click the **Add New Client** icon; a client with blank parameters is displayed.
5. In the 'Client MAC' field, enter the device's MAC address. The MAC address is printed on the label located on the underside of the device. Ensure that the check box to the right of the field is selected - this enables the client in the BootP tool (if the client is disabled, no replies are sent to BootP requests).
6. In the 'IP' field, enter the IP address (in dotted-decimal notation) that you want to assign to the device.
7. In the 'Subnet' field, enter the subnet mask (in dotted-decimal notation) that you want to assign to the device. Ensure that the subnet mask is valid, otherwise, the device may not function.
8. In the 'Gateway' field, enter the IP address of the default Media Gateway (if any).
9. Click **Apply** to save the new client.
10. Click **OK**; the 'Client Configuration' screen closes.
11. Physically reset the device using the hardware reset button (or power down and then power up the device). This causes the device to use BootP; the device changes its network parameters to the values provided by BootP.

**Figure 3-2: BootP Client Configuration Screen**



### 3.1.1.3 Assigning an IP Address using the Voice Menu Guidance

Initial configuration of the device can be performed using a standard touch-tone telephone connected to one of the FXS ports. The voice menu can also be used to query and modify basic configuration parameters.

**Note:** Assigning an IP address using voice menu guidance is only relevant when the device houses an FXS module.

➢ **To assign an IP address using the voice menu guidance:**

1. Connect a telephone to one of the FXS ports.
2. Lift the handset and dial ***12345** (three stars followed by the digits 1, 2, 3, 4, and 5).
3. Wait for the 'configuration menu' voice prompt to be played.
4. To change the IP address:
   a. Press **1** followed by the pound key (#); The current IP address of the device is played.
   b. Press the # key.
   c. Dial the new IP address. Use the star (*) key instead of periods (.), e.g., 192*168*0*4, and then press # to finish.
   d. Review the new IP address, and then press **1** to save.
5. To change the subnet mask:
   a. Press **2** followed by the # key; The current subnet mask of the device is played.
   b. Press the # key.
   c. Dial the new subnet mask (e.g., 255*255*0*0), and then press # to finish.
   d. Review the new subnet mask, and then press **1** to save.
6. To change the default Gateway IP address:
   a. Press **3** followed by the # key; The current default Gateway address is played.
   b. Press the # key.
   c. Dial the new default Gateway address (e.g., 192*168*0*1), and then press # to finish.
   d. Review the new default Gateway address, and then press **1** to save.
7. Hang up the handset.
8. Access the device's Web interface with the new IP address you assigned.

Alternatively, initial configuration may be performed using an HTTP server, as discussed in the *Product Reference Manual* ('Automatic Update Facility'). The Voice Menu may be used to specify the configuration URL.

➢ **To set a configuration URL:**

1. Obtain the IP address of the configuration HTTP server (e.g., 36.44.0.6).
2. Connect a telephone to one of the FXS ports.
3. Lift the handset and dial ***12345** (three stars followed by the digits 1, 2, 3, 4, and 5).
4. Wait for the 'configuration menu' voice prompt to be played.
5. Dial **31** followed by the # key; the current IP address is played.
6. To change the IP address, perform the following:
   a. Press the # key.
   b. Dial the configuration server's IP address. Use the star (*) key instead of dots ("."), e.g., 36*44*0*6, and then press # to finish.
   c. Review the configuration server's IP address, and then press **1** to save.
7. Dial **32** followed by the # key, and then perform the following to change the configuration file name pattern:
   a. Press the # key.

**b.** Select one of the patterns listed in the table below (*aa.bb.cc.dd* denotes the IP address of the configuration server):

| # | Configuration File Name Pattern | Description |
|---|---|---|
| 1 | http://aa.bb.cc.dd/config.ini | Standard config.ini. |
| 2 | https://aa.bb.cc.dd/config.ini | Secure HTTP. |
| 3 | http://aa.bb.cc.dd/audiocodes/<MAC>.ini | The device's MAC address is appended to the file name (e.g., http://36.44.0.6/audiocodes/00908f012300.ini). |
| 4 | http://aa.bb.cc.dd:8080/config.ini | HTTP on port 8080. |
| 5 | http://aa.bb.cc.dd:1400/config.ini | HTTP on port 1400. |
| 6 | http://aa.bb.cc.dd/cgi-bin/acconfig.cgi?mac=<MAC>&ip=<IP> | Generating configuration per IP/MAC address dynamically, using a CGI script. See perl example below. |

**c.** Press the selected pattern code, and then press # to finish.

**8.** Press **1** to save, and then hang up the handset. The device retrieves the configuration from the HTTP server.

The following is an example perl CGI script, suitable for most Apache-based HTTP servers for generating configuration dynamically per pattern #6 above. Copy this script to /var/www/cgi-bin/acconfig.cgi on your Apache server and edit it as required:

```
#!/usr/bin/perl
use CGI;
$query = new CGI;
$mac = $query->param('mac');
$ip = $query->param('ip');
print "Content-type: text/plain\n\n";
print "; INI file generator CGI\n";
print "; Request for MAC=$mac IP=$ip\n\n";
print <<"EOF";
SyslogServerIP = 36.44.0.15
EnableSyslog = 1
SSHServerEnable = 1
EOF
```

The table below lists the configuration parameters that can be queried or modified using the voice menu:

**Table 3-2: Configuration Parameters Available via the Voice Menu**

| Item Number at Menu Prompt | Description |
|---|---|
| **1** | IP address. |
| **2** | Subnet mask. |
| **3** | Default Gateway IP address. |
| **4** | Primary DNS server IP address. |
| **7** | DHCP enable / disable. |
| **31** | Configuration server IP address. |
| **32** | Configuration file name pattern. |
| **99** | Voice menu password (initially 12345).<br>**Note:** The voice menu password can also be changed using the Web interface or *ini* file parameter VoiceMenuPassword (refer to the *User's Manual*). |

### 3.1.1.4 Assigning an IP Address Using the CLI

You can assign an IP address to the device, using command-line interface (CLI).

➢ **To assign an IP address via the CLI:**

1. Connect the device's RS-232 port to either COM1 or COM2 communication port on your PC.
2. Use a serial communication software (e.g., HyperTerminal™) to establish a serial communication link with the device, using the following communications port settings:
   - **Baud Rate:** 115,200 bps
   - **Data Bits:** 8
   - **Parity:** None
   - **Stop Bits:** 1
   - **Flow Control:** None

   The CLI prompt appears.
3. At the prompt, type **`conf`**, and then press <Enter>; the configuration folder is accessed.
4. To view the current network parameters, at the prompt, type **`GCP IP`**, and then press <Enter>; the current network settings are displayed.
5. Change the network settings by typing the following:

   ```
   SCP IP [ip_address] [subnet_mask] [default_gateway]
   ```

   For example,

   ```
   SCP IP 10.13.77.7 255.255.0.0 10.13.0.1
   ```

   The new settings take effect on-the-fly and connectivity to the device is active at the new IP address.
   **Note:** This command requires you to enter all three network parameters (each separated by a space).
6. To save the configuration, at the prompt, type **SAR**, and then press <Enter>; the device restarts with the new network settings.

## 3.1.2 Mediant 1000 MSBG

You need to assign the following IP addresses to the device and in the order listed below:

- LAN IP address
- WAN IP address

### 3.1.2.1 Assigning LAN IP Addresses

You need to define LAN IP addresses for the following interface services:

- VoIP and management (OAMP, Media, and Control) - refer to "VoIP and Management LAN Interface" on page 43
- Data-routing (with security) - refer to "Data-Routing LAN Interface" on page 44

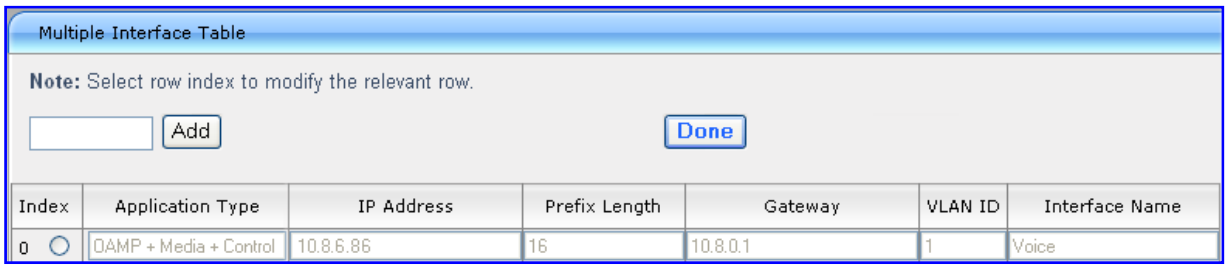
#### 3.1.2.1.1 VoIP and Management LAN Interface

The procedure below describes how to assign an IP address to the LAN VoIP and Management interface.

➢ **To assign a LAN VoIP and Management IP address:**

1. Open the 'IP Settings' page (**Configuration** tab > **VoIP** menu > **Network Settings** > **IP Settings**).
2. Select the 'Index' radio button corresponding to the Application Type "**OAMP + Media + Control** (i.e., VoIP and management interface), and then click **Edit**.
3. Configure the new IP address and prefix length so that it corresponds to your network IP addressing scheme (e.g., 10.8.6.86).
4. Configure additional IP interfaces, if required.

**Figure 3-3: Multiple Interface Table Page**




5. Click **Apply**, and then **Done** to apply and validate settings. If validation fails, the device does not reboot.
6. Save your settings to flash memory and reset the device.

**Notes:**

- The VoIP and Management interface must be in the same subnet as the data-routing interface.
- When operating with VoIP and data-routing functionalities, it is recommended to define the Default Gateway IP address for the VoIP network interfaces in the same subnet and with the same VLAN ID as the IP address defined later for the data-routing LAN interface.

#### 3.1.2.1.2 Data-Routing LAN Interface

The default IP address of the LAN data-routing interface is listed in the table below:

**Table 3-3: Default LAN Data-Routing IP Address**

| Parameter | Default Value |
|---|---|
| **IP Address** | 192.168.0.1 |
| **Subnet Mask** | 255.255.255.0 |
| **Default Gateway** | 0.0.0.0 |

**Note:** The data-routing interface must be in the same subnet as the VoIP and Management interface.

➢ **To define the device's LAN data-routing IP address:**

1. Access the device's Web interface with the IP address that you assigned to the VoIP and Management interface (refer to "VoIP and Management LAN Interface" on page 43).
2. Access the 'Connections' page (**Configuration** tab > **Data Settings** menu > **Data System** > **Connections**).

**Figure 3-4: Connections Page**


3. Click the "LAN Switch VLAN 1" connection, and then click the **Settings** tab.
4. In the 'IP Address' and 'Subnet Mask' fields, enter the required IP address (e.g., 10.8.6.85) and subnet respectively, and then click **OK**.

**Figure 3-5: Defining LAN Data-Routing IP Address**

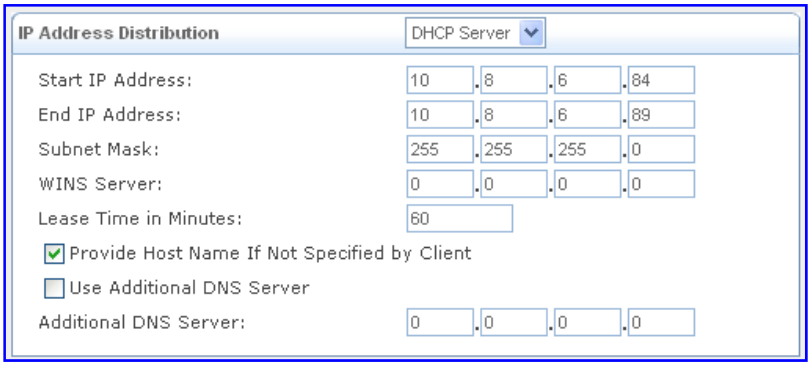
### 3.1.2.2 Configuring the Device's DHCP Server

The device is supplied with an enabled internal DHCP server for the LAN and with default IP pool addresses relating to the default subnet LAN. After reconfiguring the LAN IP addresses, the IP pool addresses are changed accordingly. You can either disable the DHCP server or modify the IP address pool. The device (acting as a DHCP server), uses this setting to allocate IP addresses to all the computers connected to its LAN interface.

➢ **To configure DHCP on the device:**

1. Access the device's Web interface, using the device's name ("msbg.home") or Voice and Management IP address that you assigned in 'Assigning a LAN IP Address' on page 43.
2. Access the 'DHCP Server' page (**Configuration** tab > **Data Settings** menu > **Services** submenu > **DHCP Server**).
3. Click the **LAN Hardware Ethernet Switch** link; the following page appears:

**Figure 3-6: Configuring the DHCP Server**




4. From the 'IP Address Distribution' drop-down list, select "DHCP Server".
5. Define the IP address pool using the fields under the 'IP Address Distribution' group.
6. Click **OK**.
7. If required, refresh the address by disconnecting the cable and then reconnecting it again, or by performing the following in the Windows' command line interface:

```
ipconfig /release
ipconfig /renew
```

### 3.1.2.3 Assigning a WAN IP Address

Once you have configured the device's LAN interfaces, you can then define the device's WAN interface (for connecting to the Internet). The WAN interface connection type can be one of the following:

- **Manual IP address:** defines a single, static IP address for connection to the WAN
- **Automatic IP address:** the device obtains its WAN IP settings from a remote DHCP server
- **Point-to-Point Protocol over Ethernet (PPPoE):** requires login user name and password (supplied by your Internet Service Provider - ISP)
- **Point-to-Point Tunneling Protocol (PPTP):** similar to PPPoE, and requires PPTP server IP address etc. (supplied by your ISP)
- **Layer 2 Tunneling Protocol (L2TP):** similar to PPTP

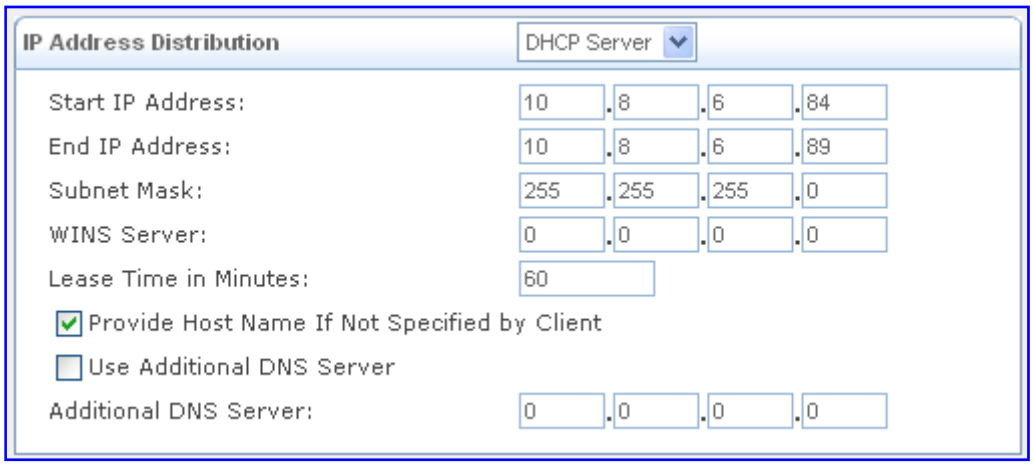
**Notes:**

- Before you configure the WAN interface connection, ensure that you have all the required information from your ISP.
- Once you have configured the WAN IP address, you must define the SIP WAN IP address with this same IP address in the Voice and Management interface.

➢ **To assign a WAN IP address:**

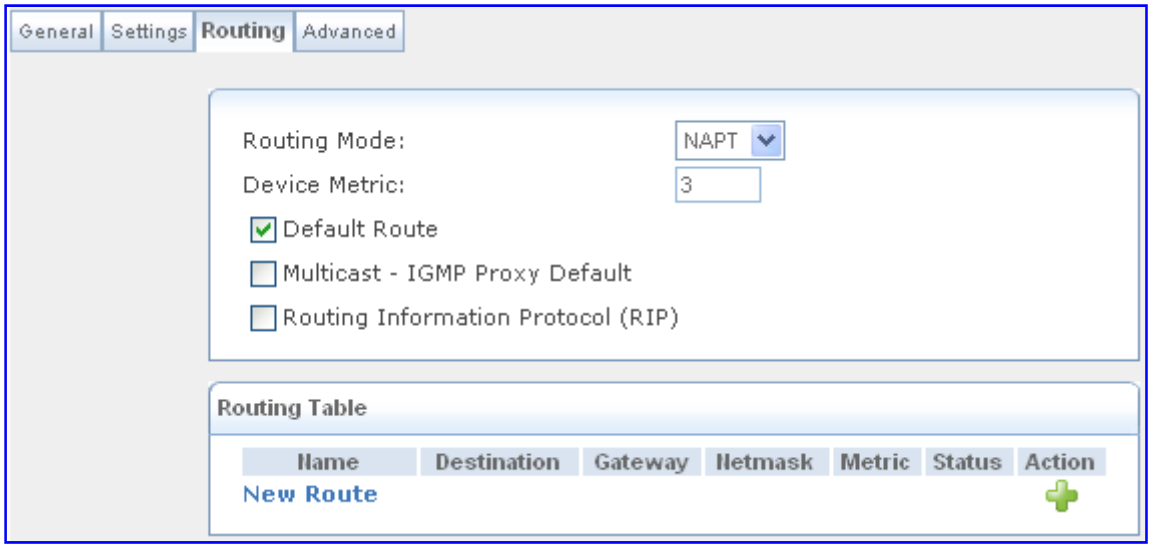
1. Cable the device to the WAN network (i.e., ADSL or Cable modem), using the WAN port (refer to 'Connecting to WAN' on page 24).
2. Access the device's Web interface, using the device's name ("msbg.home") or Voice and Management IP address.
3. Access the 'Settings' page (**Configuration** tab > **Data Settings** menu > **WAN Access** submenu > **Settings**).

**Figure 3-7: Configuring the DHCP Server**




4. From the 'Connection Type' drop-down lists, select the required connection type for the WAN, and then configure the subsequent, available fields for the selected connection type.
5. Configure the WAN interface operating mode for Network Address Port Translation (NAPT):
   a. Click the **Click here for Advanced Settings** link, and then select the **Routing** tab; the 'Routing' page appears.

**Figure 3-8: Routing Tab**




   b. From the 'Routing Mode' drop-down list, select 'NAPT'.
   c. Select the 'Default Route' check box.
   d. Click **OK**.

### 3.1.3 Mediant 2000

This section describes how to change the device's default IP address so that it corresponds with your network environment. The table below lists the device's default IP address.

**Table 3-4: Default IP Addresses**

| Parameter | Default Value |
|---|---|
| **IP Address** | ▪ Device with a single module (trunks 1-8): 10.1.10.10<br>▪ Device's second module (trunks 9-16): 10.1.10.11 |
| **Subnet Mask** | 255.255.0.0 |
| **Default Gateway IP Address** | 0.0.0.0 |

**Note:** The device can include one or two identical modules. These modules are fully independent, each possessing its own MAC and IP address. If the device includes two modules, the IP addresses assigned to these modules must be in the same subnet.

To assign an IP address to the device, use one of the following methods:

- Device's HTTP-based embedded Web server `accessed using a Web browser (refer to 'Assigning an IP Address using HTTP' on page 47).
- BootP (refer to 'Assigning an IP Address using BootP' on page 48).
- Embedded Command Line Interface (CLI), accessed using RS-232 (if supported) or Telnet (refer to 'Assigning an IP Address using the CLI' on page 50).
- Dynamic Host Control Protocol (DHCP) - refer to the *User's Manual*.

**Tip:** If at a later stage after re-defining the IP address, your IP address is unknown (e.g., forgotten), use the BootP/TFTP utility to access the device (refer to the Product Reference Manual).

#### 3.1.3.1 Assigning an IP Address using HTTP

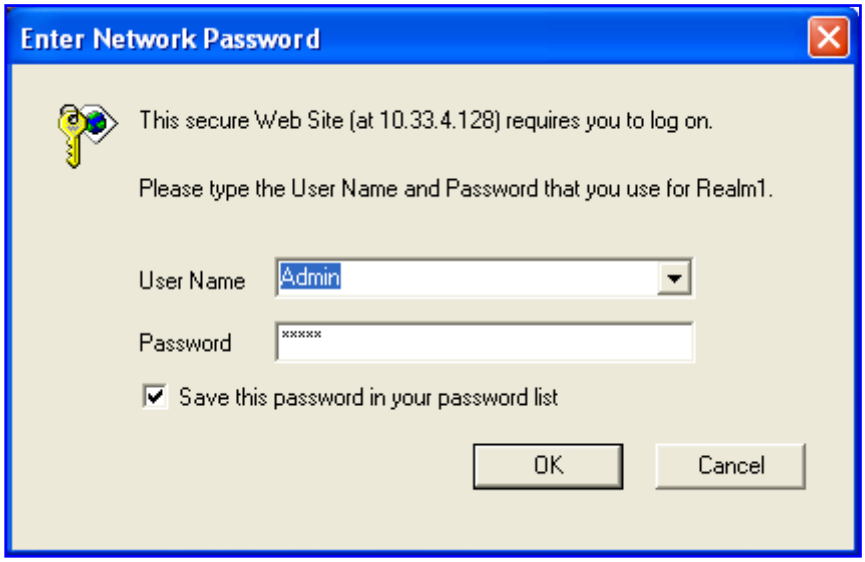
You can assign an IP address to the device, using the device's Web interface.

➢ **To assign an IP address using HTTP:**

1. Disconnect the device from the network and reconnect it to a PC using one of the following methods:
   - **Using a hub or switch between a PC and the device:** Connect the network interface on your PC to a port on a network hub / switch, using a standard Ethernet cable. Connect the device to another port on the same network hub / switch, using another standard Ethernet cable.
   - **Direct connection between a PC and the device:** Connect the network interface on your PC directly to the device, using an Ethernet crossover cable.
2. Change your PC's IP address and subnet mask to correspond with the device's factory default IP address and subnet mask.

3. Access the device's Web interface:
   a. Open a standard Web browser application and in the Uniform Resource Locator (URL) field, enter the device's default IP address (e.g., http://10.1.10.10); the Web interface's 'Enter Network Password' dialog box appears, as shown in the figure below**:**

**Figure 3-9: Enter Network Password Screen**




   b. Enter the device's default login, case-sensitive user name ('Admin') and password ('Admin'), and then click **OK**; the Web interface is accessed, displaying the Web interface's 'Home' page.
4. Change the device's IP address, by performing the following:
   a. Open the 'Multiple Interface Table' page, (**Configuration** tab > **Network Settings** menu > **IP Settings**).
   b. Define the device's IP address, subnet mask, and default Gateway IP address (for "OAMP + Media + Control" application type) so that they correspond to your network IP scheme.
   c. Click **Apply**.
   d. Save your settings to the flash memory and reset the device.
5. When implementing a device with two modules, repeat steps 2 through 3 for the second module; otherwise, skip to Step 6.
6. Disconnect your PC from the device or from the hub/switch (depending on the connection method used in Step 1).
7. Reconnect the device and PC (if necessary) to the network.
8. Restore your PC's IP address and subnet mask to their original settings. If necessary, restart your PC and re-access the device via the Web interface with its newly assigned IP address.

### 3.1.3.2 Assigning an IP Address using BootP

You can assign an IP address to the device, using the supplied AudioCodes' BootP/TFTP Server application.

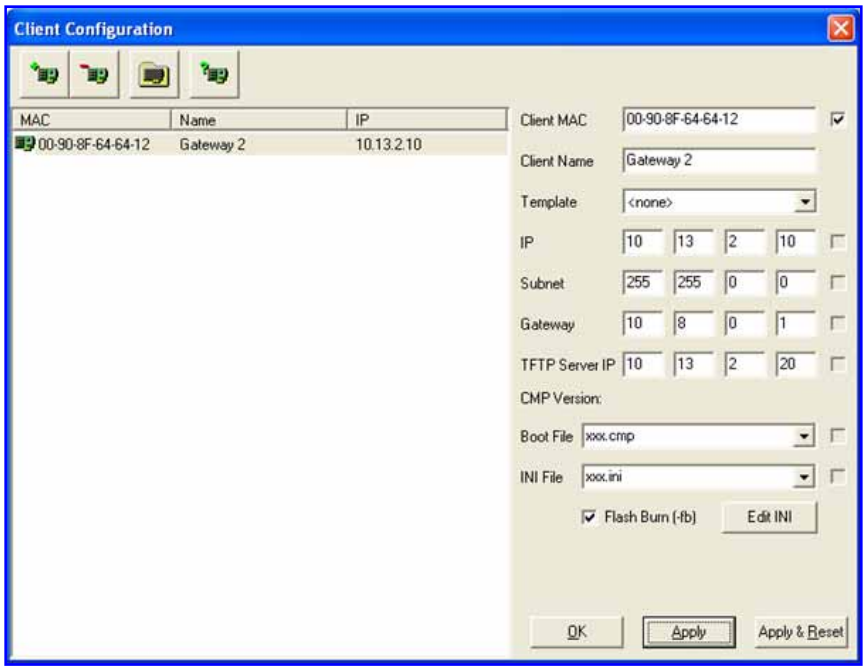
**Notes:**

- BootP procedure can also be performed using any standard compatible BootP server.
- For a detailed description of BootP, refer to the *Product Reference Manual.*

➢ **To assign an IP address using BootP:**

1. Start the BootP application.
2. From the Edit menu, choose **Preferences,** and then in the 'Preferences' dialog box, set the 'Timeout' field to 50.
3. From the Services menu, choose **Clients**; the 'Client Configuration' dialog box appears.
4. Click the **Add New Client** icon; a client with blank parameters is displayed.
5. In the 'Client MAC' field, enter the device's MAC address. The MAC address is printed on the label located on the underside of the device. Ensure that the check box to the right of the field is selected - this enables the client in the BootP tool (if the client is disabled, no replies are sent to BootP requests).
6. In the 'IP' field, enter the IP address (in dotted-decimal notation) that you want to assign to the device.
7. In the 'Subnet' field, enter the subnet mask (in dotted-decimal notation) that you want to assign to the device. Ensure that the subnet mask is valid, otherwise, the device may not function.
8. In the 'Gateway' field, enter the IP address of the default gateway (if any).
9. Click **Apply** to save the new client.
10. Click **OK**; the 'Client Configuration' screen closes.
11. Physically reset the device using the hardware reset button (or power down and then power up the device). This causes the device to use BootP; the device changes its network parameters to the values provided by BootP.
12. Repeat steps 2 through 11 for the device's second module (if used).

**Figure 3-10: BootP Client Configuration Screen**



### 3.1.3.3 Assigning an IP Address using the CLI

You can assign an IP address to the device, using command-line interface (CLI).

➢ **To assign an IP address via the CLI (if supported):**

1. Connect the device's RS-232 port to either COM1 or COM2 communication port on your PC.
2. Use a serial communication software (e.g., HyperTerminal™) to establish a serial communication link with the device, using the following communications port settings:
   - **Baud Rate:** 115,200 bps
   - **Data Bits:** 8
   - **Parity:** None
   - **Stop Bits:** 1
   - **Flow Control:** None

   The CLI prompt appears.
3. At the prompt, type **conf**, and then press <Enter>; the configuration folder is accessed.
4. To view the current network parameters, at the prompt, type **GCP IP**, and then press <Enter>; the current network settings are displayed.
5. Change the network settings by typing the following:

   ```
   SCP IP [ip_address] [subnet_mask] [default_gateway]
   ```

   For example,

   ```
   SCP IP 10.13.77.7 255.255.0.0 10.13.0.1
   ```

   The new settings take effect on-the-fly and connectivity to the device is active at the new IP address.
   **Note:** This command requires you to enter all three network parameters (each separated by a space).
6. To save the configuration, at the prompt, type **SAR**, and then press <Enter>; the device restarts with the new network settings.

# 3.2 Connecting to the SBA Application

This section describes how to connect to the Survivable Branch Appliance (SBA) application:

- Mediant 1000/Mediant 1000 MSBG - refer to Section 3.2.1
- Mediant 2000 - refer to Section 3.2.2

## 3.2.1 Mediant 1000 and Mediant 1000 MSBG

The OSN Server hosting the SBA application is provided pre-installed with Microsoft Windows® Server 2008 R2 operating system (OS). You can connect to the OSN Server using Microsoft's Remote Desktop Connection program.

**Notes:**

- To connect remotely to the OSN server running Windows, ensure that Remote Desktop is enabled.
- The remote PC must be in the same subnet as the OSN server (default IP address is 10.1.10.12).

### 3.2.1.1 Cabling

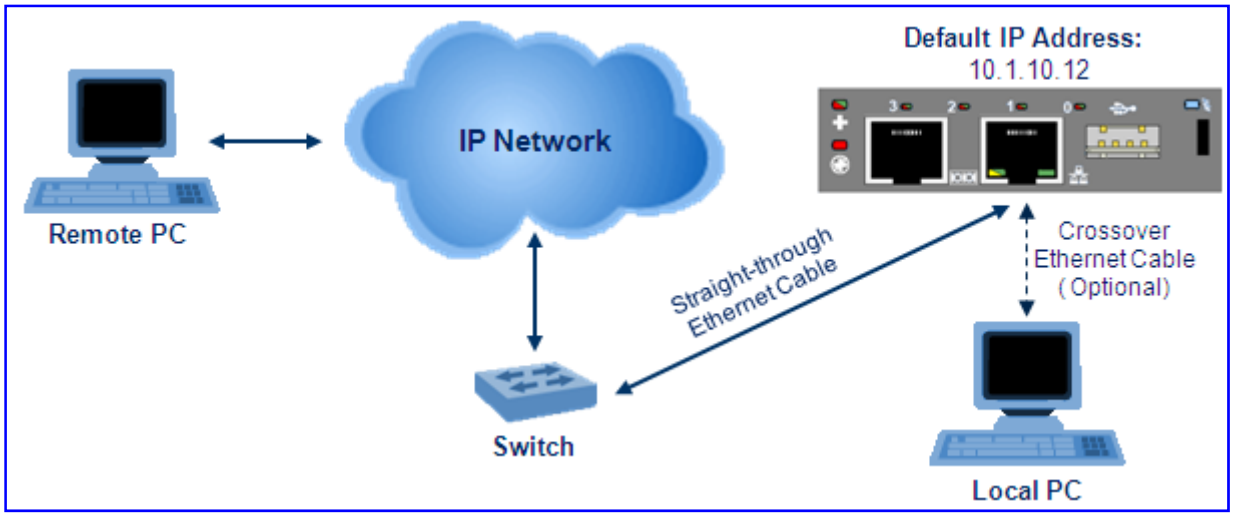
Before you can connect remotely to the OSN Server, you need to cable a PC (running Remote Desktop Connection) to the OSN Server's IP network interface.

The OSN3 server connects initially to the IP network through the LAN port of the OSN3 module.

➢ **To cable OSN3 for Remote Desktop Connection:**

- Connect the Ethernet LAN port of the OSN3 module to the LAN network, by performing one of the following:
  - **Remote PC connection:** using a straight-through cable, connect the LAN port to a switch that is connected to the IP network.
  - **Local PC connection:** using a crossover cable, connect the LAN port directly to the PC's LAN port.

**Figure 3-11: Cabling OSN3 for Remote Desktop Connection from PC with Windows XP**



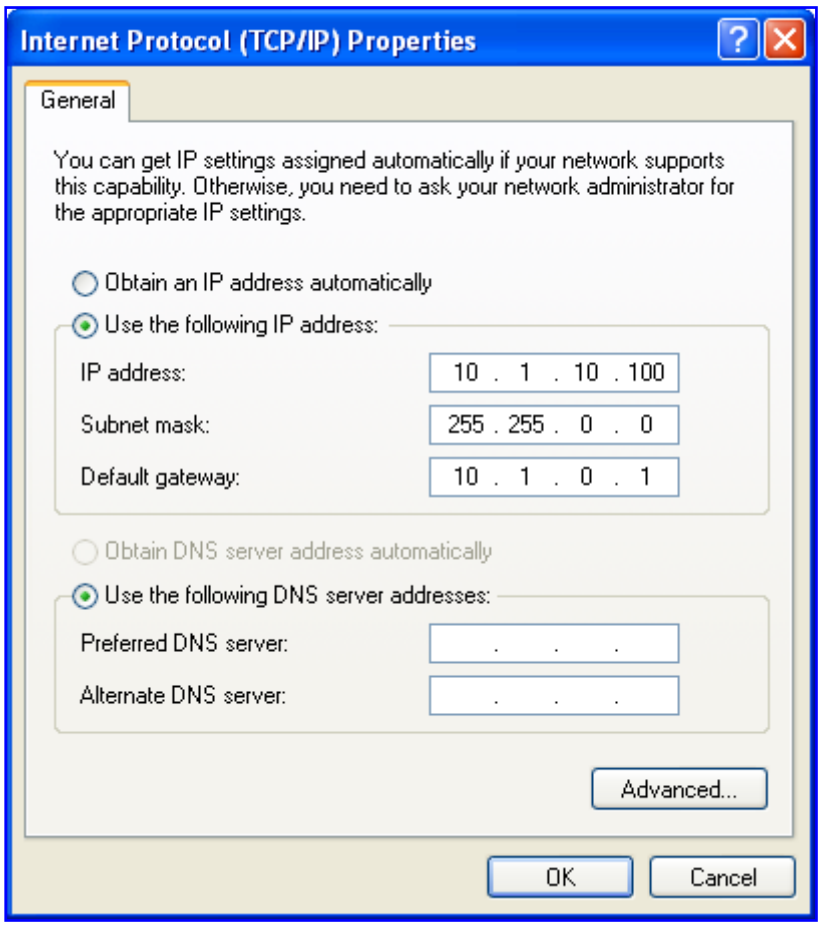
### 3.2.1.2 Connecting using Remote Desktop Connection

Once you have cabled the PC to the OSN Server, perform the procedure below for connecting the PC remotely to the OSN Server (running Windows) using the Remote Desktop Connection program.

➢ **To remotely connect a PC to the OSN Server running Windows:**

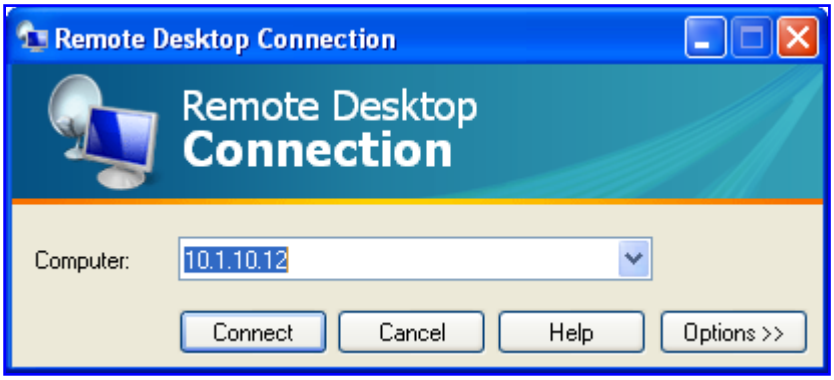
1. Change the PC's IP address so that it is in the same subnet as the default OSN Server's IP address (i.e., 10.1.10.12). The figure below displays an example of a changing a PC's IP address:

**Figure 3-12: Changing the PC's IP Address**



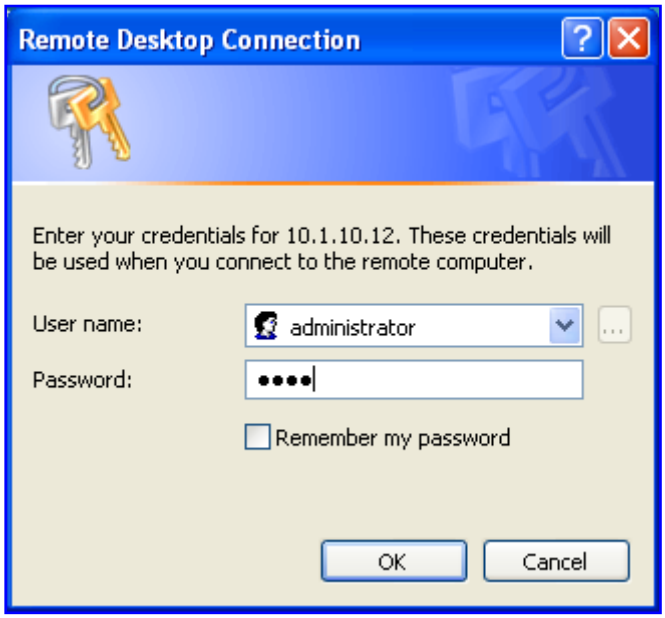

2. Start Microsoft's Remote Desktop Connection program - from the **Start** menu, point to **Programs**, to **Accessories**, to **Communications**, and then click **Remote Desktop Connection**.

**Figure 3-13: Entering IP Address in Remote Desktop Connection**



3. In the 'Computer' field, enter the OSN Server's default IP address (i.e., 10.1.10.12).
4. Click **Connect**.

**Figure 3-14: Entering User Name and Password in Remote Desktop Connection**




5. Enter the OSN Server's default user name (i.e., "Administrator") and password (i.e., "Pass123").
6. Click **OK**; Remote Desktop Connection connects you to the desktop of the device's OSN server.

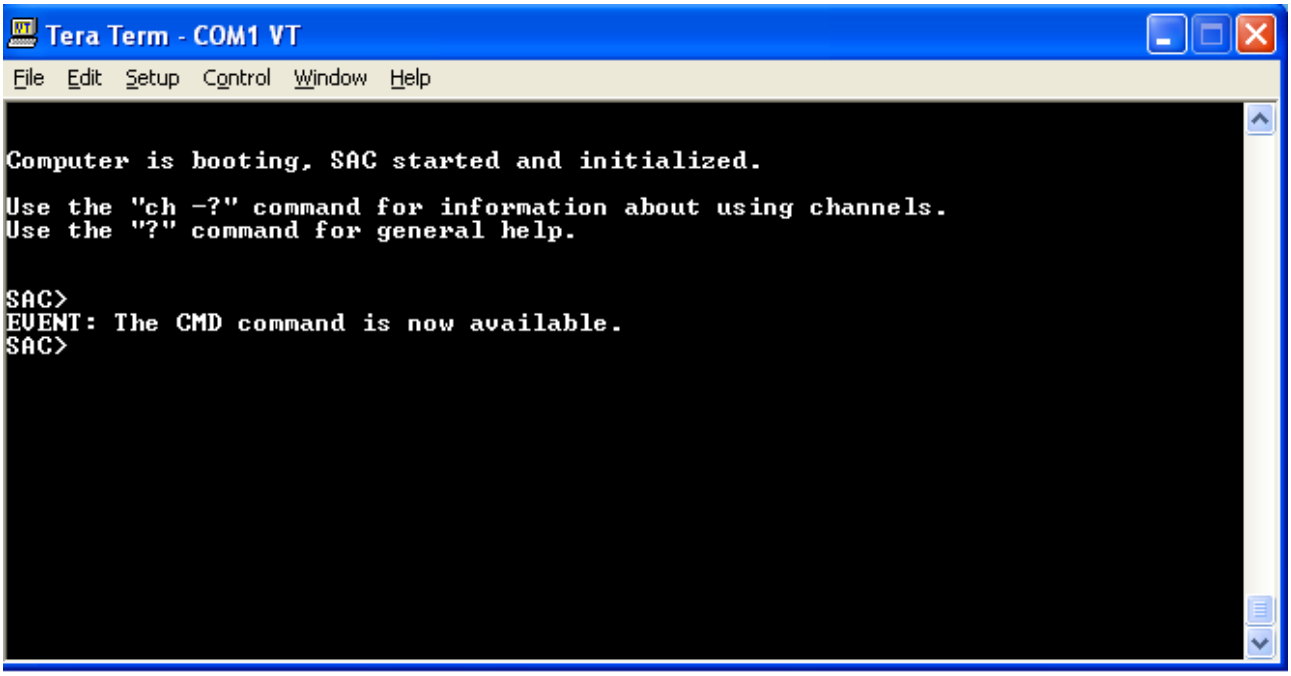
### 3.2.1.3 Connecting using Serial Port

To verify (or configure) the IP address of the OSN3 server, you can use the serial port as described below:

➢ **To connect to the Mediant 1000 OSN server using the serial port:**

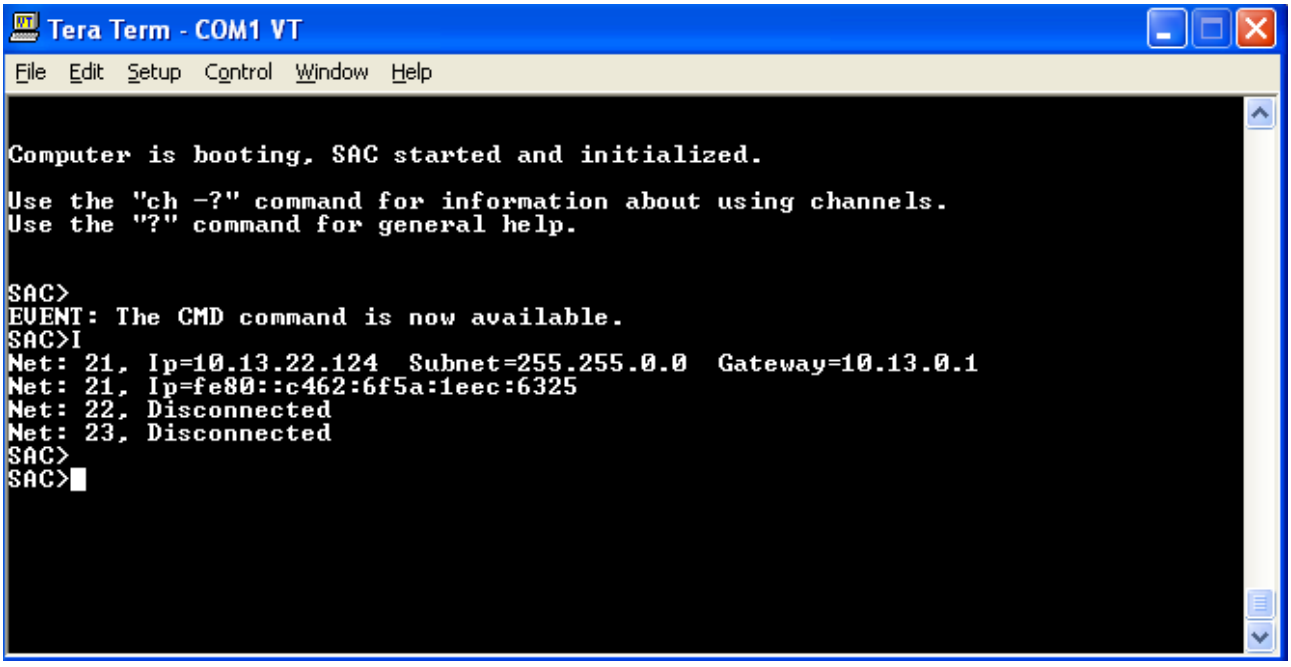
1. Connect one end of the serial cable (refer to Section 2.1.1.3.1) to the OSN serial port and the other end to the PC serial port.
2. Start HyperTerminal and set the port to 115200 (bits per second), 8 (data bits), N (parity), 1 (stop bits); the following prompt appears:

**Figure 3-15: Terminal Prompt**




3. At the prompt, enter 'I' to list all the IP network numbers and their IP addresses.

**Figure 3-16: List of IP Addresses**



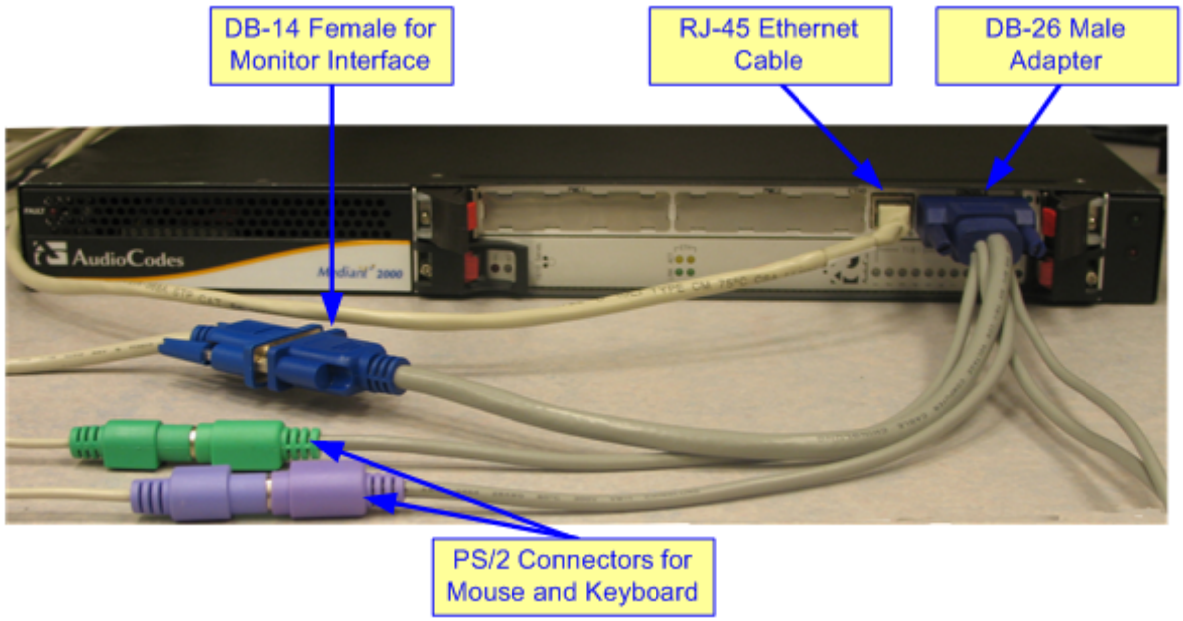
## 3.2.2 Mediant 2000

The connection to the SBC blade is performed through the graphic (monitor) interface, which is provided by the DB-26 port. The SBC blade running Microsoft Windows Server 2008 R2 is accessed using the default user name "Administrator" and password "Pass123".

➢ **To connect to the Mediant 2000 SBC server:**

1. Connect the DB-26 female adapter cable to the DB-26 male port on the SBC blade.
2. Connect the DB-26 cable extensions to their respective interfaces:
   - DB-14 connector to the monitor
   - Two PS/2 connectors to the mouse and keyboard
3. Connect the SBC blade's RJ-45 port to your network.

**Figure 3-17: Cabling of the SBC Blade**




4. Power on Mediant 2000; Microsoft Windows Server 2008 starts.
5. Log in to the server using the default user name ("Administrator) and password ("Pass123").

**Note:** As an alternative, you can access the SBC server using Microsoft's Remote Desktop Connection program. The default IP address is 10.1.10.12/24.

**Reader's Notes**

# 4 Configuring the Enhanced Media Gateway

This section provides step-by-step procedures for configuring AudioCodes Enhanced Media Gateway.

**Notes:** .**Before starting configuring the Gateway please ensure the following:**

1. The Media Gateway is running SIP firmware Version 6.0A.021 or later.
2. The Media Gateway must be installed with the following special Feature Keys:
   - MSFT - enable working with Microsoft Lync.
   - IPSEC, MediaEncryption, StrongEncryption and EncryptControlProtocol - enable working with TLS transport type.
   - SBC (for Mediant 1000B MSBG) or IP2IP (for Mediant 1000B and Mediant 2000) - enable the IP-to-IP feature.

## 4.1 Defining Mediation Server's IP Address, Redundancy and Load Balancing

As the IP address of Mediation Server (through which the AudioCodes Media Gateway communicates with Lync 2010) is specific to deployment, you must define this parameter. The Media Gateway forwards all telephone calls (PBX/PSTN and analog devices) to this IP address (i.e., to Mediation Server).

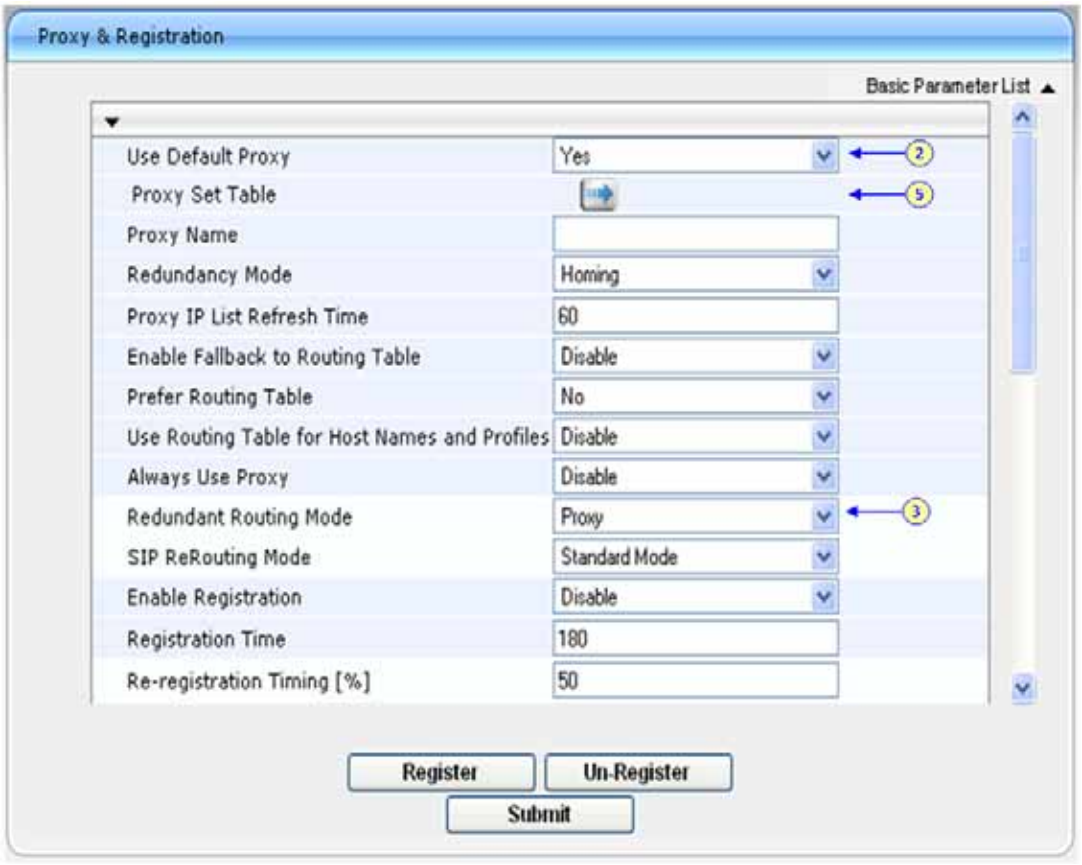
The IP address is defined in the Media Gateway's embedded Web server as the proxy server's IP address. In other words, Mediation Server acts as a proxy server (without registration).

If you have more than one Mediation Server in the cluster, load balancing and proxy redundancy functionality should apply also, to achieve the Lync 2010 requirement.

➢ **To define Mediation Server's IP address or FQDN:**

1. Open the 'Proxy & Registration' page (**Configuration** tab > **Protocol Configuration** menu > **Proxies/IpGroups/Registration** submenu > **Proxy & Registration**).

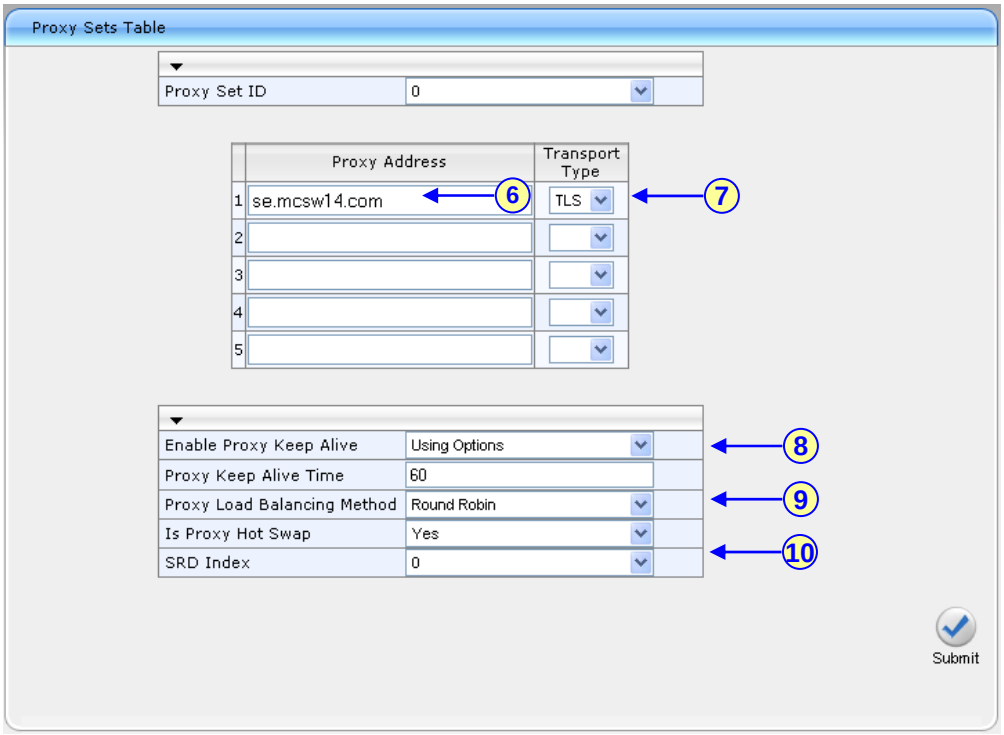
**Figure 4-1: Proxy & Registration Page**




2. From the 'Use Default Proxy' drop-down list, select 'Yes'. This allows Mediation Server to act as a proxy server.
3. From the 'Redundant Routing Mode' drop-down list, select 'Proxy'. This parameter determines that if a 5xx response is received for an INVITE message to the primary proxy, the Gateway will attempt to send it to the redundant proxy. To configure 503 for the Reason for Alternative Routing (as required by Lync 2010), refer to Section 4.2.
4. Click **Submit**.

5. Click the **Proxy Set Table** button to open the 'Proxy Sets Table' page for configuring groups of proxy addresses.

**Figure 4-2: Proxy Sets Table Page**




6. Configure Mediation Server's IP address (or FQDN).

   **Note:** When using FQDN, ensure that you define the DNS server's IP address ('Application Settings' page - **Configuration** tab > **Network Settings** menu > **Application Settings** > **DNS Settings**) or Mediation Server's domain name and corresponding IP address ('Internal DNS Table' page - **Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Internal DNS Table**). Refer to Section 4.3.2.

7. From the 'Transport Type' drop-down list, select the transport type (TCP or TLS) according to your deployment. For additional details for transport type configuration, refer to the following sections:

   - For TLS, Section 4.3
   - For TCP, Section 4.4

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

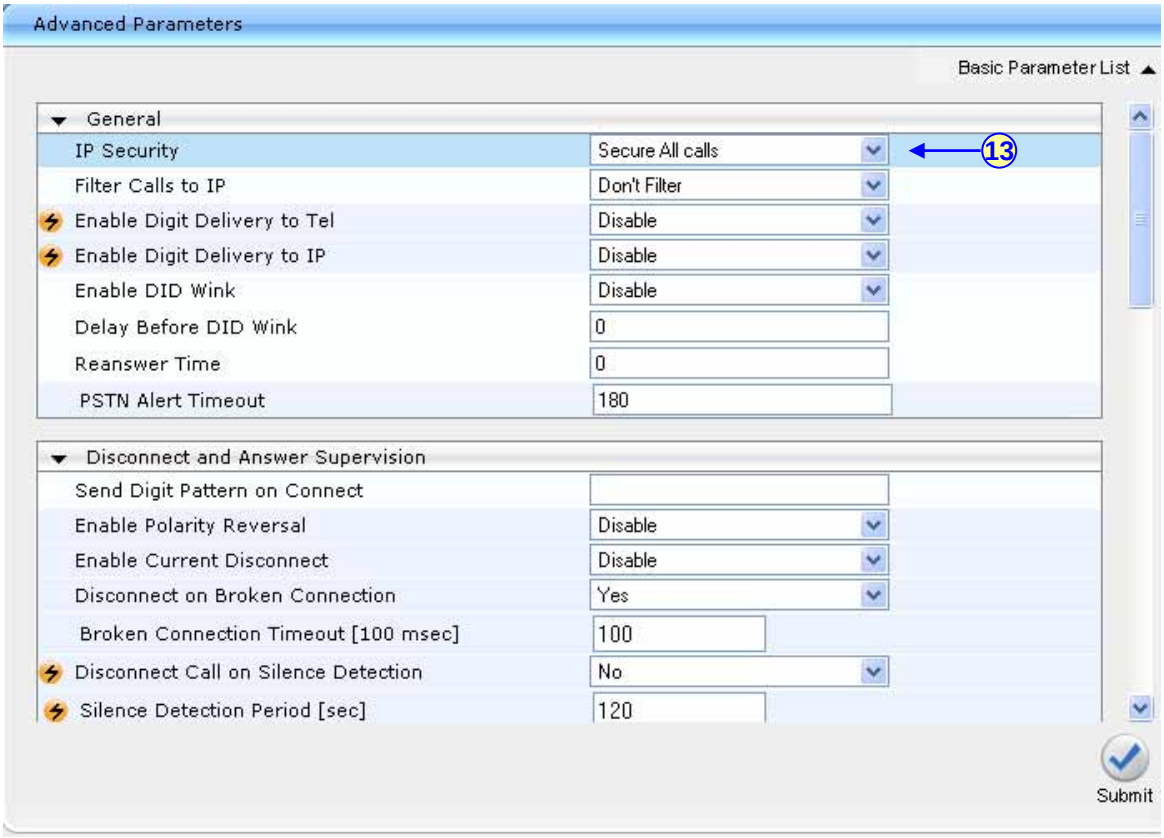
9. If your environment has multiple Mediation Servers, you need to configure load balancing. From the "Proxy Load Balancing Method" drop-down list, select 'Round Robin' to enable round-robin Proxy Load Balancing mechanism.

10. From the 'Is Proxy Hot Swap' drop-down list, select 'Enable'. If there is no response from the first Mediation Server after a specific number of retransmissions (configured by the parameter HotSwapRtx), the INVITE message is resent to the next redundant Mediation Server.

11. Click **Submit**.

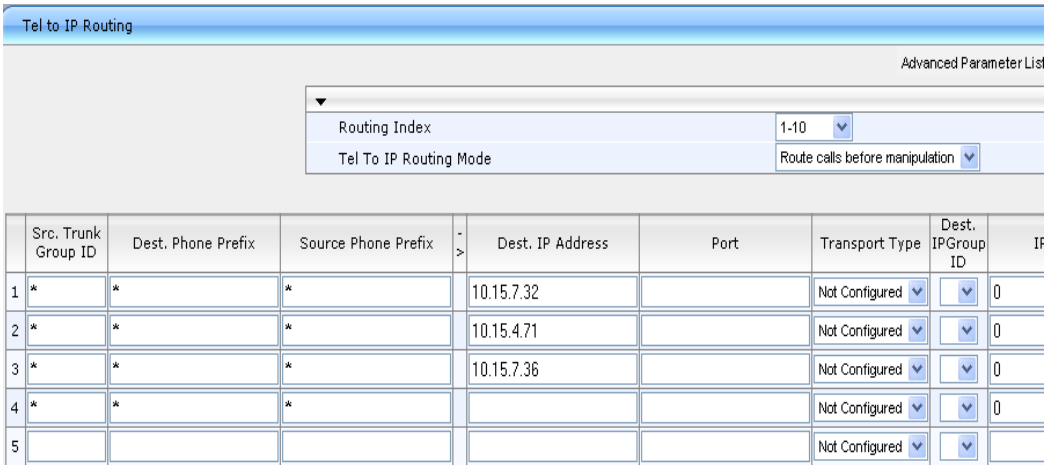
12. Open the 'Advanced Parameters' page (**Configuration** tab > **Protocol Configuration** menu > **SIP Advanced Parameters** submenu > **Advanced Parameters** page item).

**Figure 4-3: Advanced Parameters**




13. From 'IP Security' drop-down list, select 'Secure All calls'. To ensure security, Gateways must honor or send requests from/to the Mediation Server only if the Mediation server appears in an administrative list, under **Dest. IP Address** in the 'Tel to IP Routing Table' (refer to the next step), The 'IP Security' parameter determines whether the device accepts/sends SIP calls only from/to the configured IP addresses defined in the 'Tel to IP Routing Table'.
14. Open the 'Tel to IP Routing Table' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Tel to IP Routing**) and specify the IP address of the trusted Mediation Servers as follows:

**Figure 4-4: Tel to IP Routing Table**




15. Save the changes to flash memory, by clicking the **Burn** button on the toolbar.

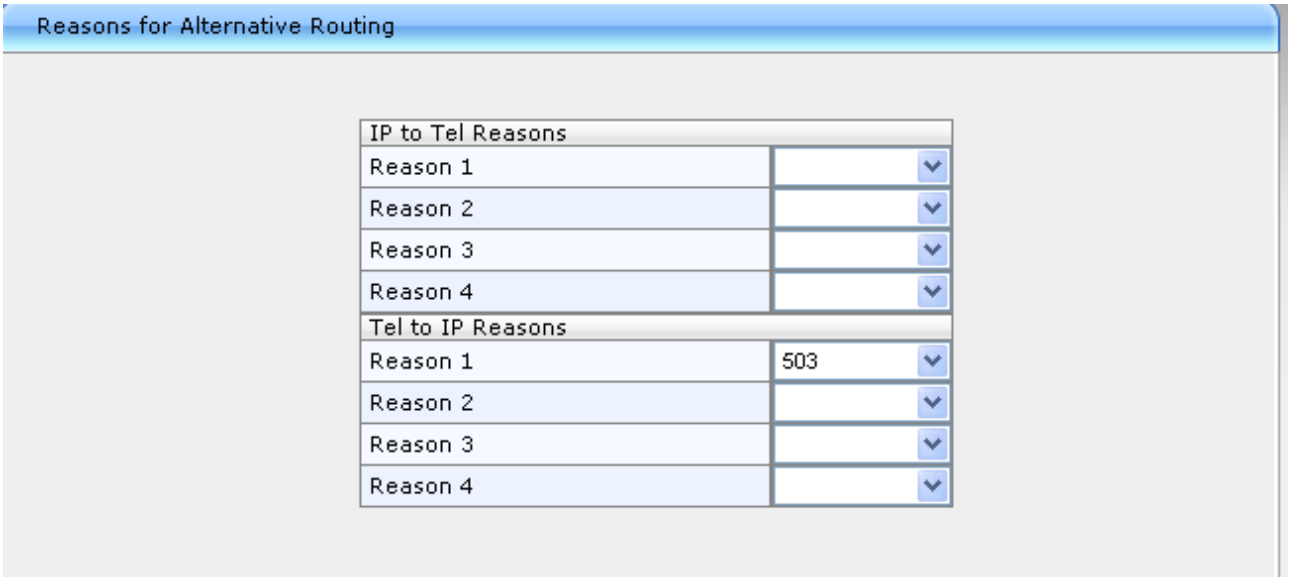
## 4.2 Defining Reasons for Alternative Routing

A 503 SIP response from the Mediation Server to an INVITE must cause the Media Gateway to perform a failover. To achieve this requirement, you need to configure the Reasons for Alternative Routing for Tel-to-IP calls to be a 503 SIP response.

➢ **To define SIP Reason for Alternative Routing:**

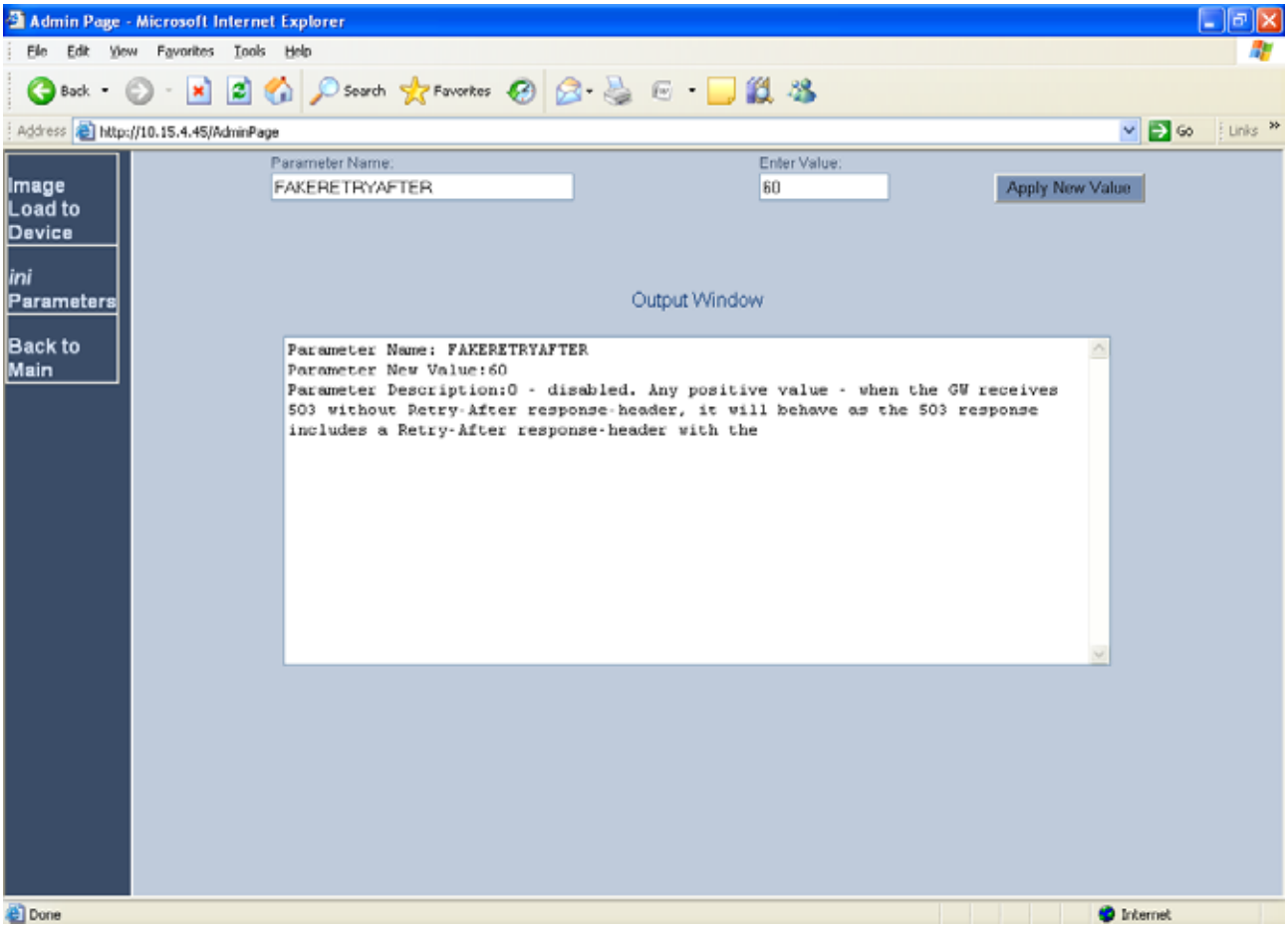
1. Open the 'Reasons for Alternative Routing' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Reasons for Alternative Routing**).

**Figure 4-5: Reasons for Alternative Routing Page**




2. Under the Tel to IP Reasons group, for Reason 1 select '503'.
3. Click **Submit**.
4. 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://10.15.4.15/AdminPage).

**Figure 4-6: Admin Page**




5. On the left pane, click **ini Parameters**.
6. In the 'Parameter Name' field, enter the parameter **FakeRetryAfter**. When the Gateway receives 503 without Retry-After response-header, it will behave as if the 503 response includes a Retry-After response-header with the period specified by the parameter FakeRetryAfter.
7. In the 'Enter Value' field, enter “60”.
8. Click **Apply New Value**.
9. Save the changes to flash memory, by clicking the **Burn** button on the toolbar.

# 4.3 Defining SIP TLS Transport Type

The SIP transport types that can be used for communicating between Mediation Server and AudioCodes gateways include the following:

- **Transport Layer Security (TLS):** this is the default and the recommended setting of Mediation Server. This setting provides encrypted signaling between Mediation Server and the Media Gateway (which is connected to the PSTN). If you configure your Media Gateway link for TLS, then signaling of calls to and from the PSTN are encrypted end to end.
- **Transmission Control Protocol (TCP):** In this transport type, the SIP signaling between Mediation Server and the Media Gateway uses SIP over TCP, which is unencrypted signaling.

If the SIP transport type for the link between the Enhanced Media Gateway and Mediation Server is set to TLS, the Media Gateway must be configured with a certificate for authentication during the TLS handshake with Mediation Server.

This section describes how to configure AudioCodes gateways for implementing a TLS connection with Mediation Server. To configure the Media Gateway to work with TCP, refer to Section 4.4.

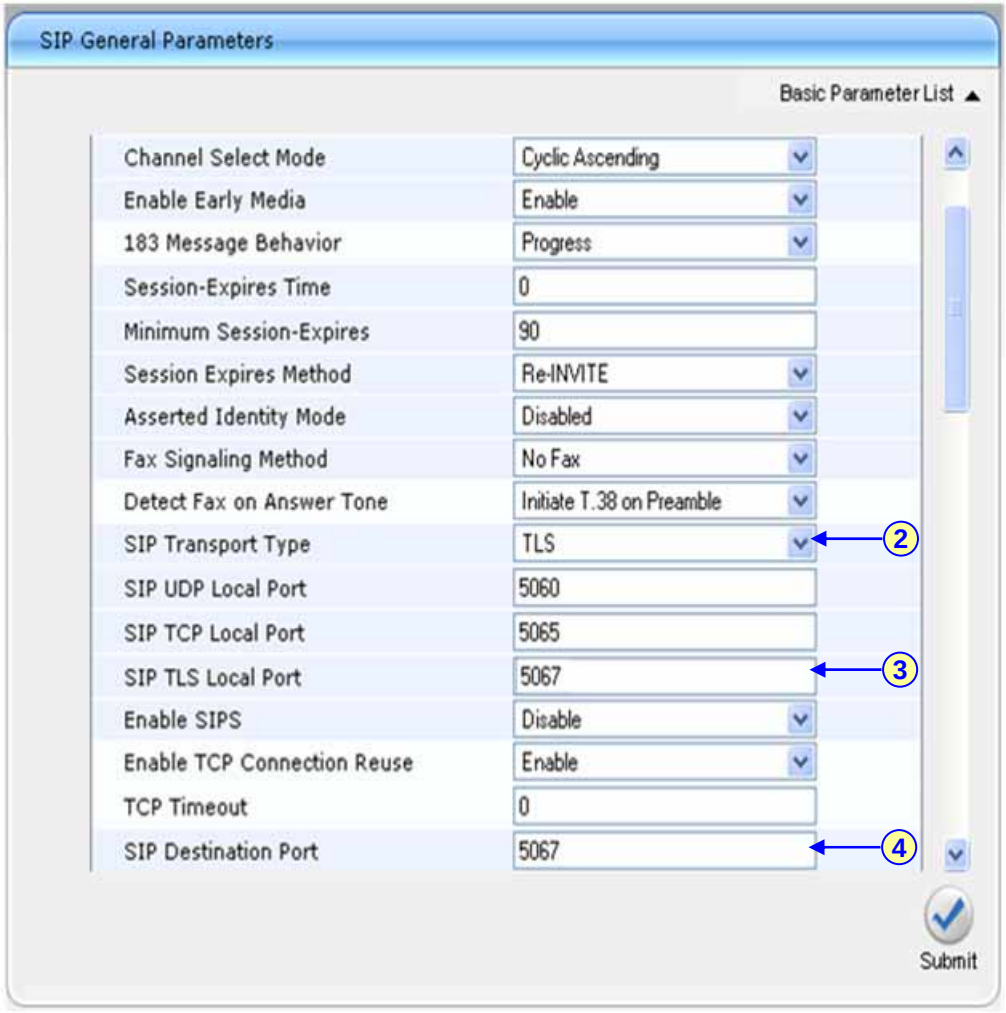
### 4.3.1 Step 1: Configure General SIP Parameters

The procedure below configures general SIP parameters.

➢ **To configure general SIP parameters:**

1. Open the 'SIP General Parameters' page (**Protocol Configuration** > **Protocol Definition** > **SIP General Parameters**).

**Figure 4-7: SIP General Parameters Page**




2. From the 'SIP Transport Type' drop-down list, select "TLS".
3. In the 'SIP TLS Local Port', enter "5067" (Corresponding to Mediation Server TLS transmitting port configuration).
4. In the 'SIP Destination Port', enter "5067" (Corresponding to Mediation Server TLS listening port configuration).

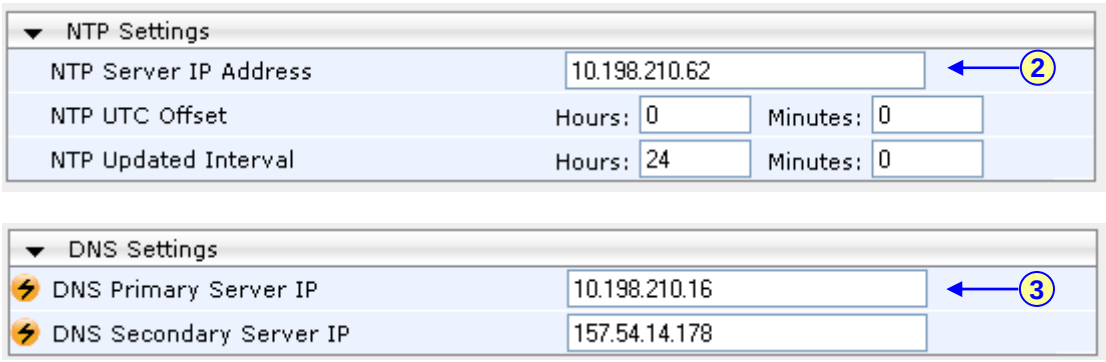
### 4.3.2 Step 2: Configure NTP and DNS Server

The procedure below configures the NTP Server IP address or FQDN and the Domain Name System (DNS) servers.

➢ **To configure the NTP and DNS servers:**

1. Open the 'Application Settings' page (**Network Settings** > **Application Settings**).

**Figure 4-8: Application Settings Page**




2. Define the NTP server's IP address so that it corresponds to your network environment.
3. In the 'DNS Primary Server IP' and 'DNS Secondary Server IP' fields, set the primary and secondary DNS server's IP addresses with the IP address of your DNS server.
4. Click the **Submit** button to save your changes.
5. Save the changes to flash memory, by clicking the **Burn** button on the toolbar. The changes take effect after restart.

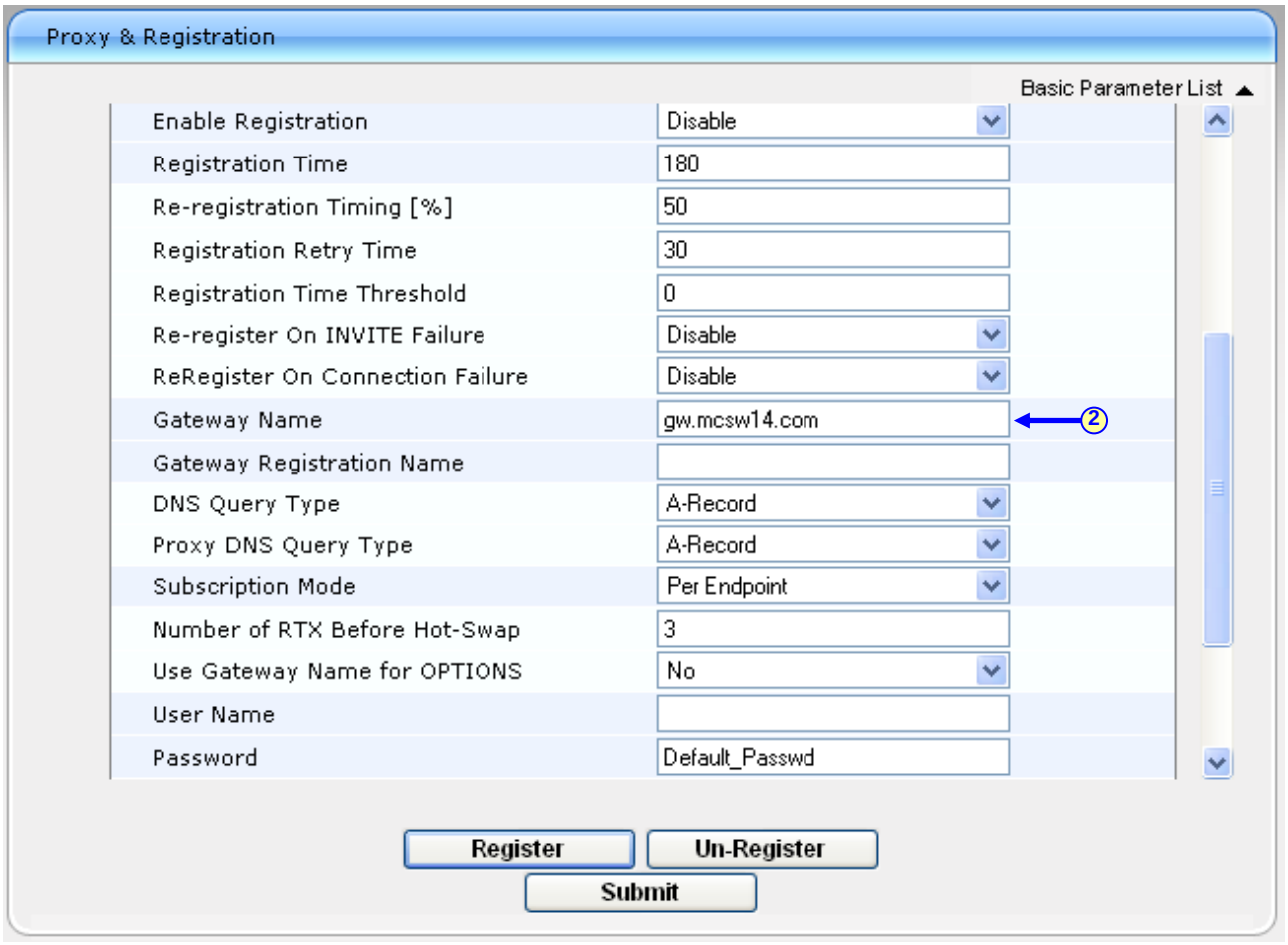
### 4.3.3 Step 3: Configure the Gateway Name

The procedure below configures the Media Gateway name.

➢ **To configure the Media Gateway name:**

1. Open the **'Proxy & Registration'** page (**Configuration** tab > **Protocol Configuration** menu > **Proxies/IpGroups/Registration** submenu > **Proxy & Registration**).

**Figure 4-9: Proxy & Registration Page**




2. In the 'Gateway Name' field, assign a unique FQDN name to the Media Gateway within the domain, for example, gw.mcsw14.com.

### 4.3.4 Step 4: Configure a Certificate

The procedure below describes how to exchange a certificate with Microsoft Certificate Authority.

➢ **To configure a certificate:**

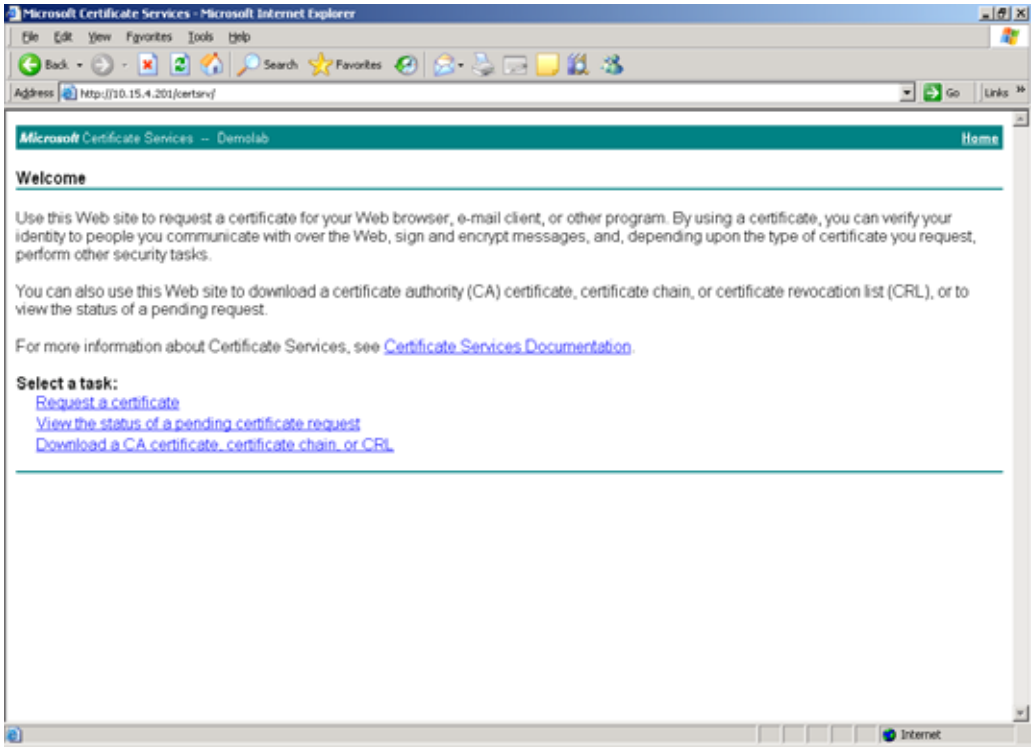
1. Open the 'Certificates' page (**Security Setting**s menu > **Certificates**).

**Figure 4-10: Certificates Page**


2. In the 'Subject Name' field, enter the Media Gateway name as configured in the previous step (refer to Section 4.3.3), and then click **Generate CSR**; a Certificate request is generated.
3. 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 as *certreq.txt*.

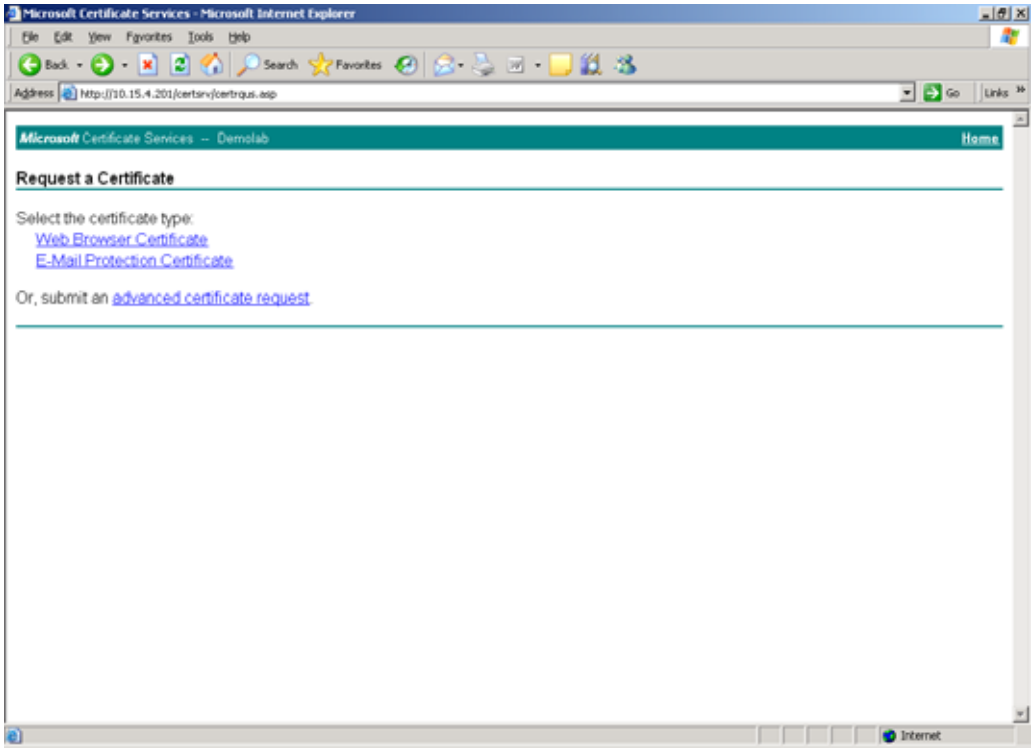
4. Navigate to the certificate Server http://<Certificate Server>/CertSrv.

**Figure 4-11: Microsoft Certificate Services Web Page**



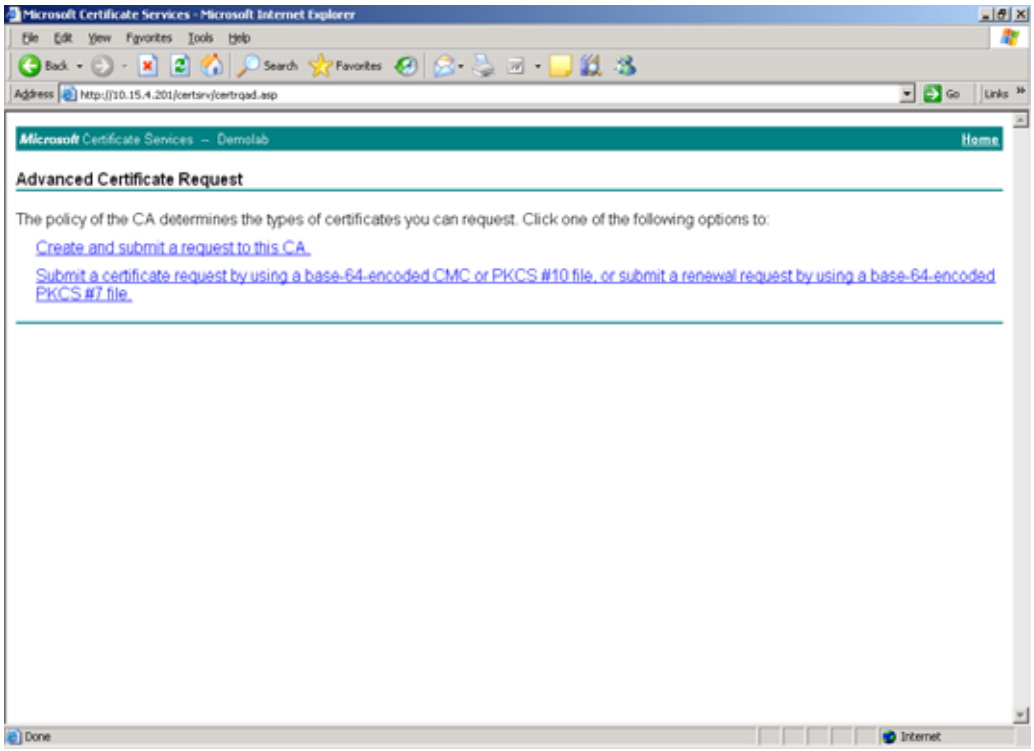

5. Click the link **Request a certificate**.

**Figure 4-12: Request a Certificate Page**



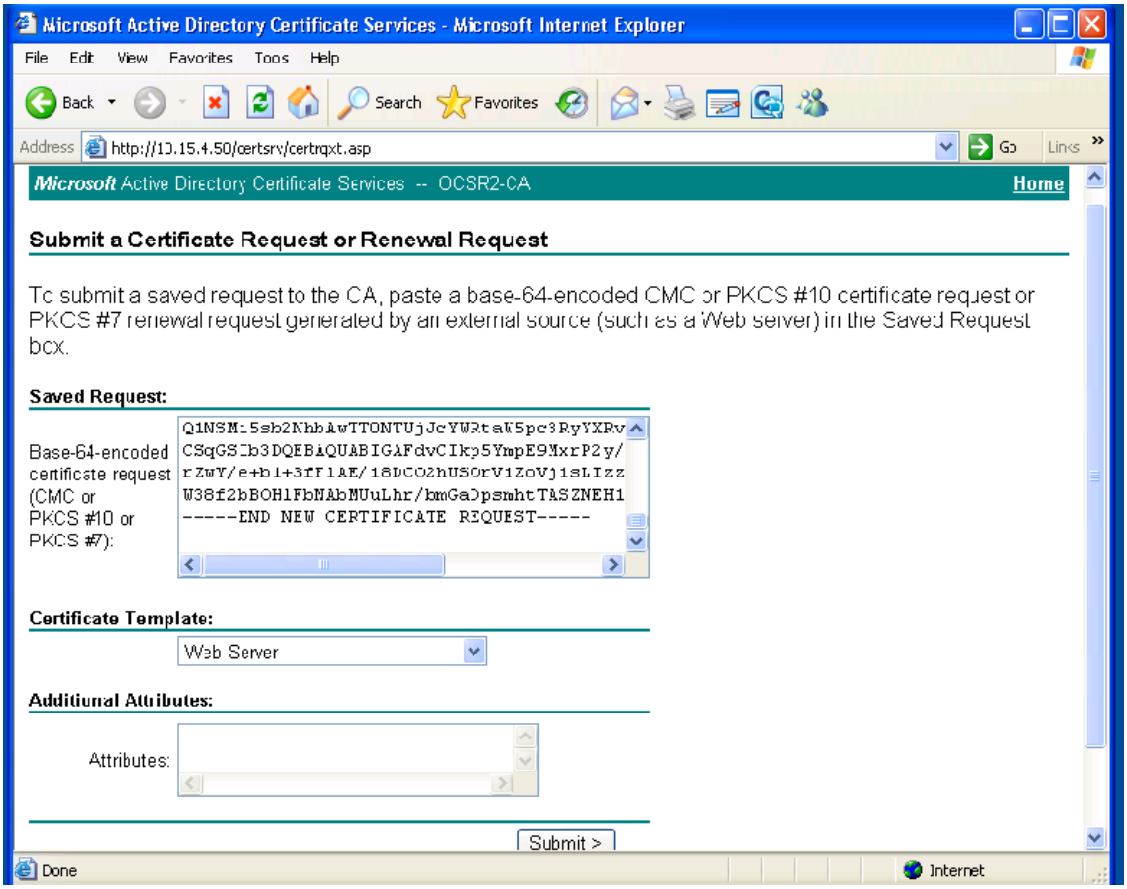
6. Click the link **advanced certificate request**, and then click **Next**.

**Figure 4-13: Advanced Certificate Request Page**



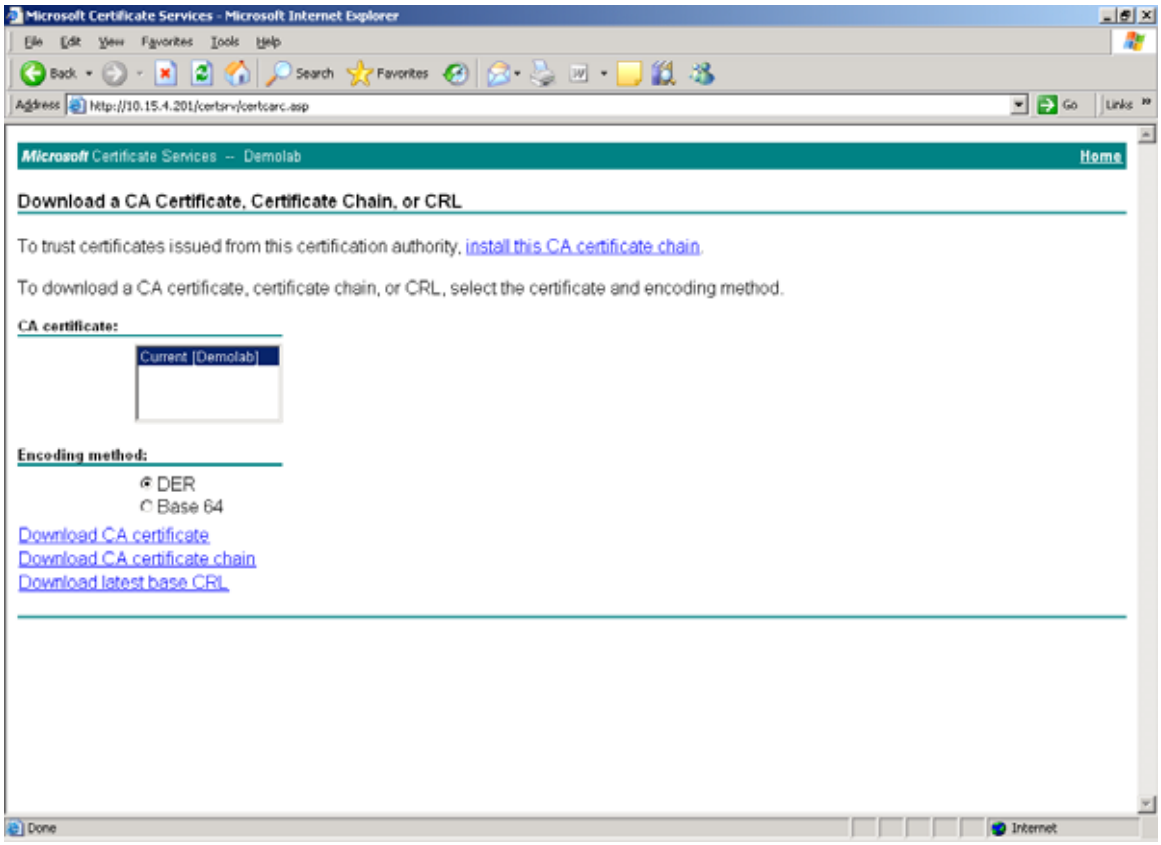

7. Click the link **Submit a Certificate request by using base64 encoded...**, and then click **Next**.

**Figure 4-14: Submit a Certificate Request or Renewal Request Page**



8. Open the *certreq.txt* file that you created and saved (in Step 3), and then copy its contents to the 'Base64 Encoded Certificate Request' text box.
9. Select "Web Server" from the **Certificate Template:**.drop-down box.
10. Click **Submit**.
11. Choose the 'Base 64' encoding option, and then click the link **Download CA certificate**.
12. Save the file as *gateway.cer* in a folder on your PC.
13. Navigate to the certificate Server http://<Certificate Server>/CertSrv.
14. Click the link **Download a CA Certificate, Certificate Chain or CRL**.

**Figure 4-15: Download a CA Certificate, Certificate Chain, or CRL Page**




15. Under the Encoding method group, perform the following:
    a. Select the 'Base 64' encoding method option.
    b. Click the link **Download CA certificate.**
16. Save the file as *certroot.cer* in a folder on your PC.
17. Navigate back to the 'Certificates' page (Step 1).
18. In the 'Server Certificate' field, click **Browse** and select the *gateway.cer* certificate file that you saved on your local disk (see Step 12), and then click **Send File** to upload the certificate.

**19.** In the 'Trusted Root Certificate Store' field, click **Browse** and select the *certroot.cer* certificate file that you saved on your local disk (see Step 16), and then click **Send File** to upload the certificate.

**Figure 4-16: Certificates Page**


**20.** Save (burn) the Media Gateway configuration and reset the Media Gateway, using the Web interface's 'Maintenance Actions' page (**Management Configuration** menu > **Maintenance Actions**).

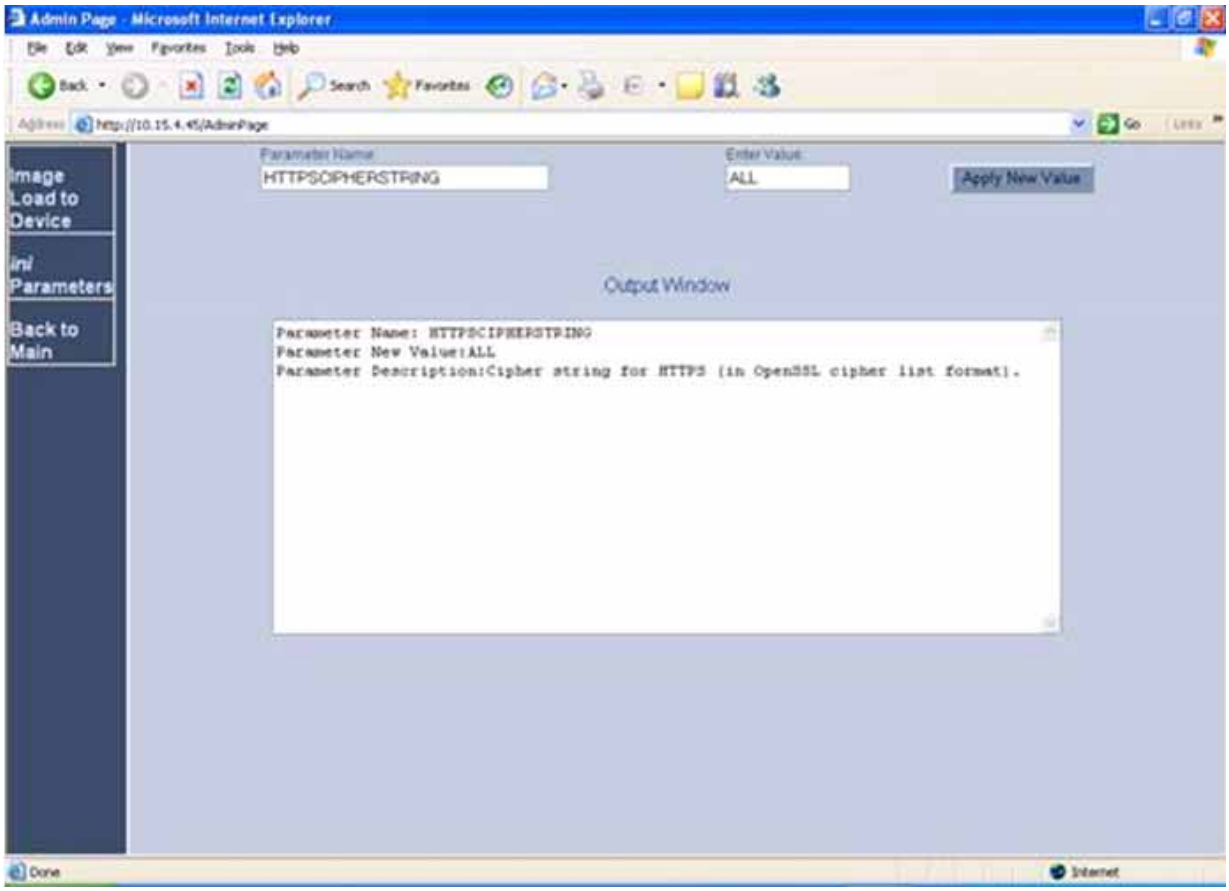
### 4.3.5 Step 5: Define the Cipher String for HTTPS

The procedure below describes how to define the cipher string for HTTPS.

➢ **To define the cipher string for HTTPS:**

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://10.15.4.15/AdminPage).

**Figure 4-17: Admin Page**




2. On the left pane, click **ini Parameters**.
3. In the 'Parameter Name' field, enter the parameter "HTTPSCipherString".
4. In the 'Enter Value' field, enter “ALL”.
5. Click **Apply New Value**.

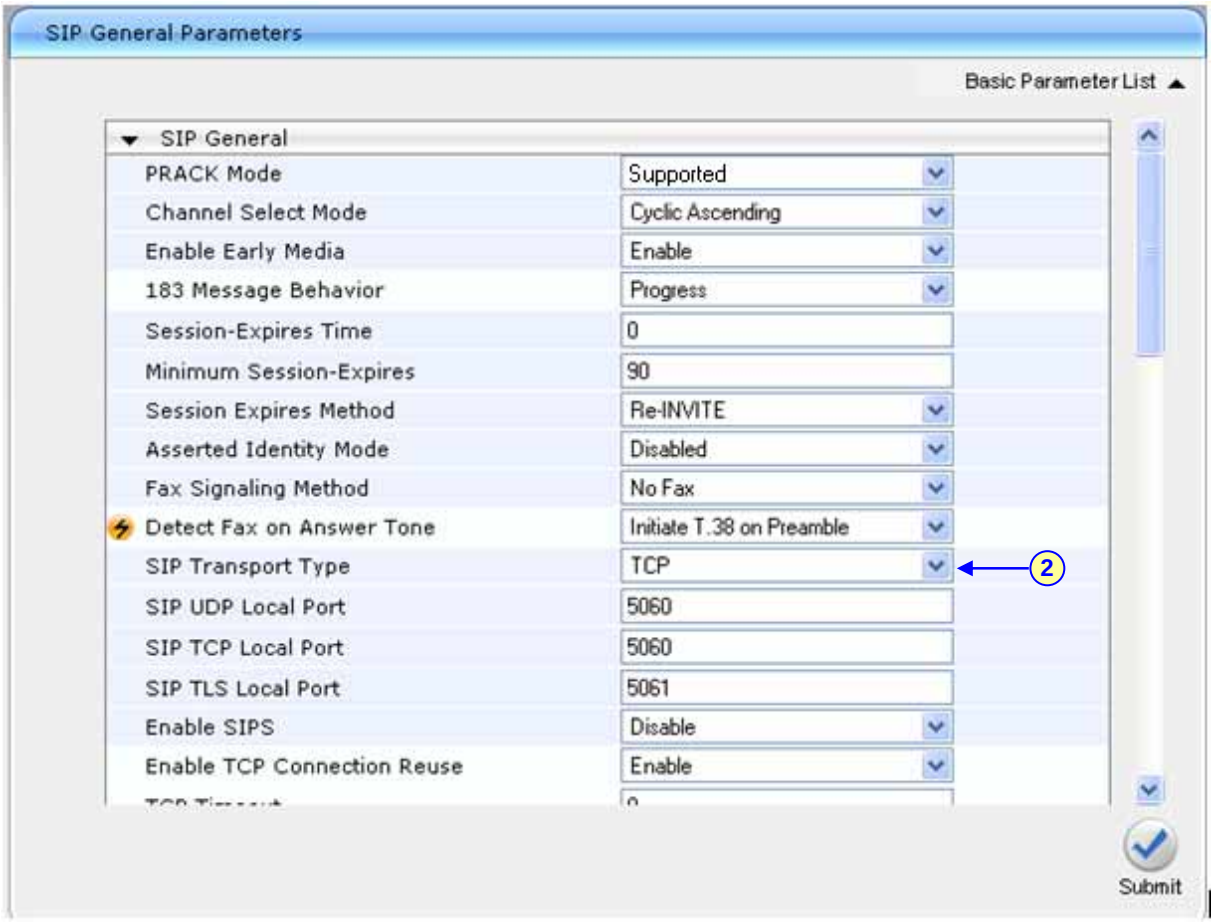
# 4.4 Defining SIP TCP Transport Type

The procedure below describes how to configure the SIP TCP transport type. Basically, you can configure the Mediation Server to operate with TCP, which is not recommended by Microsoft.

➢ **To define the SIP transport type for TCP:**

1. Open the 'SIP General Parameters' page (**Configuration** tab > **Protocol Configuration** menu > **Protocol Definition** submenu > **SIP General Parameters**).

**Figure 4-18: SIP General Parameters Page**




2. From the 'SIP Transport Type' drop-down list, select 'TCP'.
3. Click the **Submit** button to save your changes.
4. Save the changes to flash memory, by clicking the **Burn** button on the toolbar.

# 4.5 Configure Secure Real-Time Transport Protocol (SRTP)

If you configure TLS for the SIP transport link between the Media Gateway and the Mediation Server, you must specify whether Secure RTP (SRTP) encryption is:

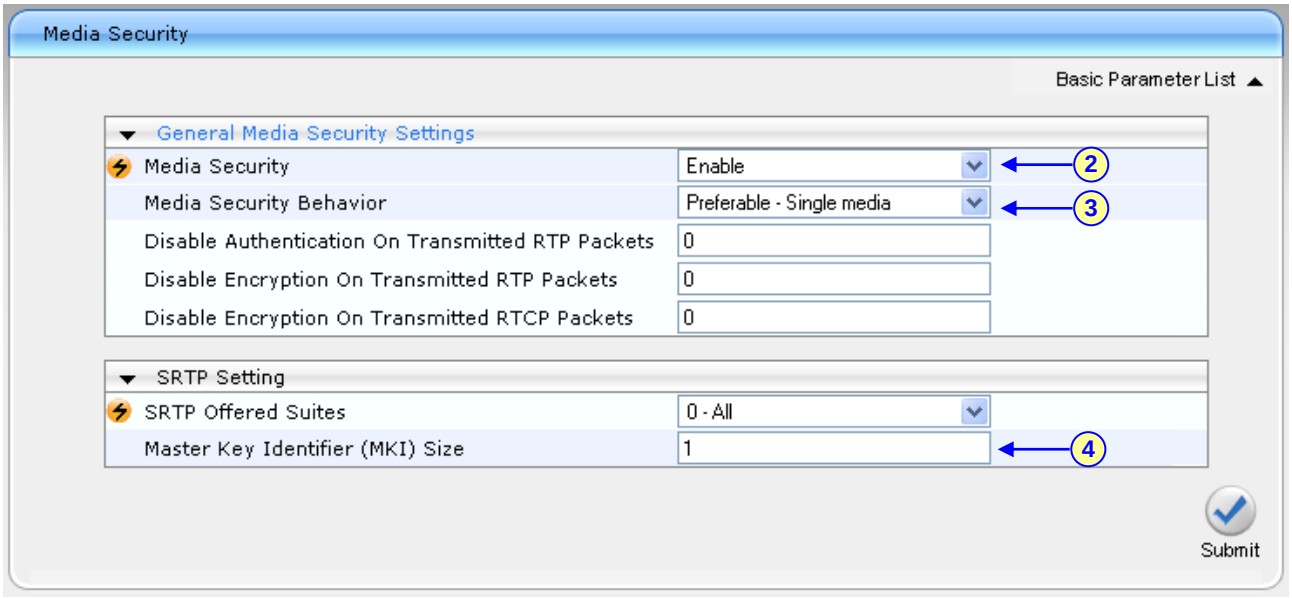
- **Required:** SRTP should be attempted, but do not use encryption if negotiation for SRTP is unsuccessful.
- **Optional:** Attempt to negotiate the use of SRTP to secure media packets. Use RTP if SRTP cannot be negotiated.
- **Not used:** Send media packets using RTP.

If you choose to configure the Mediation Server to use SRTP (Required or Optional), you need to configure the Media Gateway to operate in the same manner.

➢ **To configure the media security:**

1. Open the 'Media Security' page (**Configuration** tab > **Media Settings** menu > **Media Security**).

**Figure 4-19: Media Security Page**




2. From the ‘Media Security’ drop-down list, select “Enable”, to enable SRTP.
3. From the ‘Media Security Behavior’ drop-down list, select:
   - “Mandatory” if Mediation Server is configured to SRTP Required
   - ”Preferable-Single media” if Mediation Server is configured to SRTP Optional.
4. In the ‘Master Key Identifier (MKI) Size’ field, enter ‘1’.
5. Click **Submit**.
6. Save (burn) the Media Gateway configuration and reset the Media Gateway, using the Web interface’s ‘Maintenance Actions’ page (**Management Configuration** menu > **Maintenance Actions**).

# 4.6 Defining E1/T1/BRI Trunk Settings

The 'Trunk Group Table' page allows you to enable the Media Gateway's channels by assigning them telephone numbers and other attributes (e.g., Trunk Groups and Profiles). Trunk Groups are used for routing IP-to-Tel calls with common rules. Channels that are not defined are disabled.

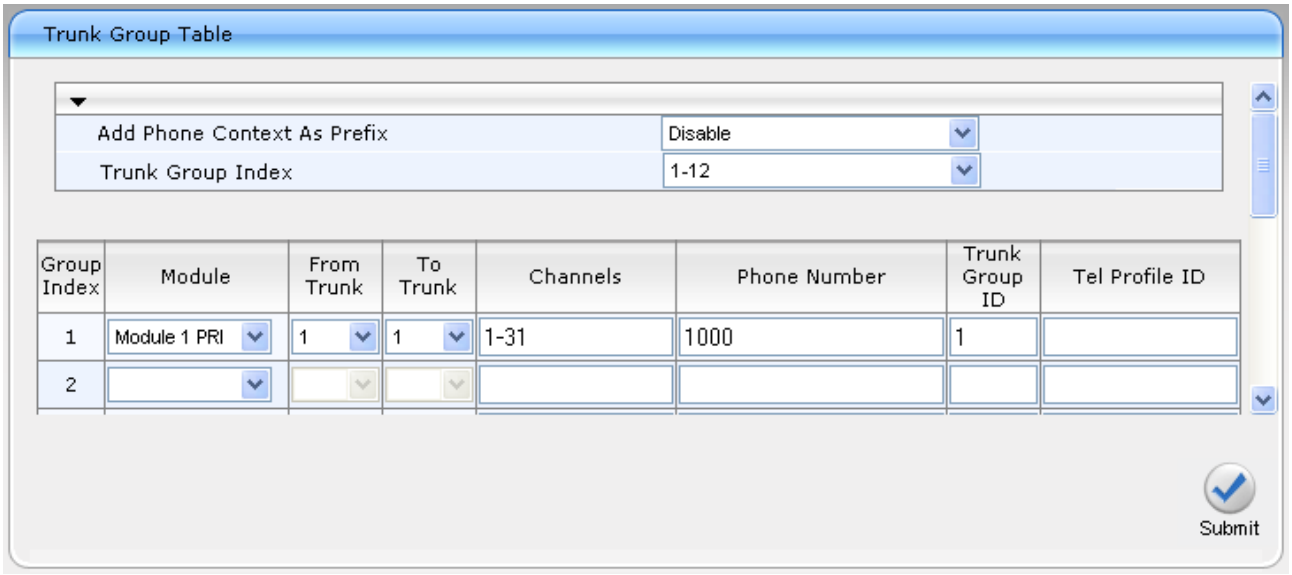
## 4.6.1 Configuring the Trunk Group Table

The procedure below configures Trunk Groups.

➢ **To configure the Trunk Group table:**

1. Open the 'Trunk Group Table' page (**Configuration** tab > **Protocol Configuration** menu > **Trunk Group** submenu > **Trunk Group**).

**Figure 4-20: Trunk Group Table Page**




2. Configure the Trunk Group Table as follows:
   a. In the 'Module' column, select the module type (i.e., FXS/FXO/BRI/PRI) for which you want to define the Trunk Group.
   b. In the 'From Trunk' and 'To Trunk' columns, select the starting and the ending physical Trunk number in the Trunk Group. (Applicable only to PRI and BRI modules.)
   c. In the 'Channel(s)' column, enter the Media Gateway's channels or ports (analog module), or Trunk B-channels (digital module, i.e. 1-31).
   d. Enter the phone number (e.g., 1000) for the first channel in the 'Phone Number' column. Phone numbers 1001, 1002, 1003 and so on are sequentially assigned to subsequent channels (i.e., 2 through 31).
   e. In the 'Trunk Group ID' column, enter the Trunk ID (i.e. 1).
3. Click **Submit** to save your changes.
4. Save the changes to flash memory, by clicking the **Burn** button on the toolbar.

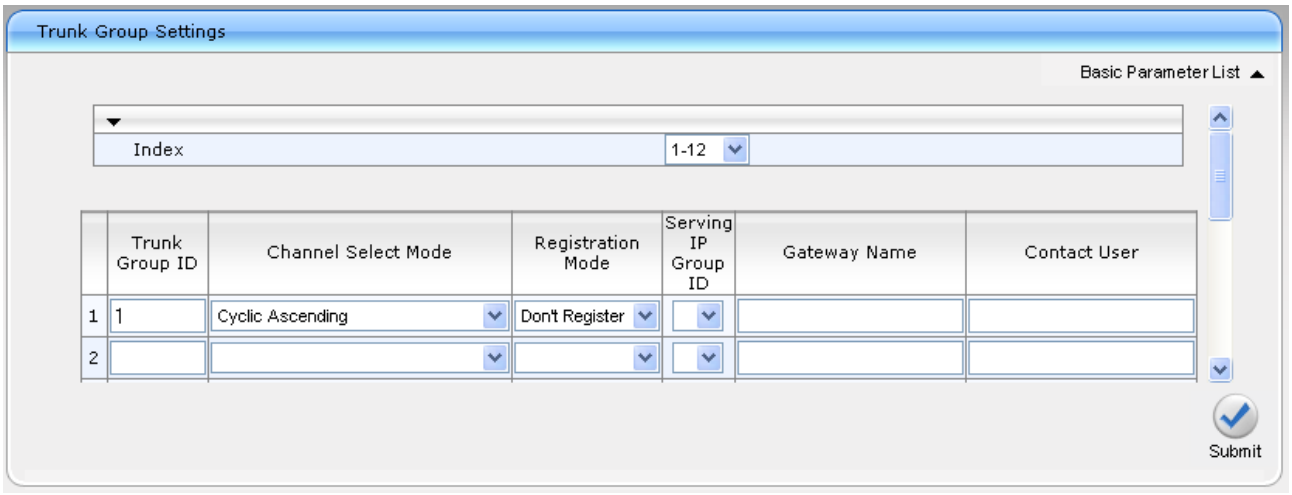
## 4.6.2 Configuring the Trunk Group setting Table

The 'Trunk Group Settings' page is used to select the method for which IP-to-Tel calls are assigned to channels within each Trunk Group.

➢ **To configure the Trunk Group settings:**

1. Open the 'Trunk Group Settings' page (**Configuration** tab > **Protocol Configuration** menu > **Trunk Group** submenu > **Trunk Group Settings**).

**Figure 4-21: Trunk Group Settings Page**




2. In the 'Trunk Group ID' column, enter the Trunk Group ID that you want to configure.
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'.

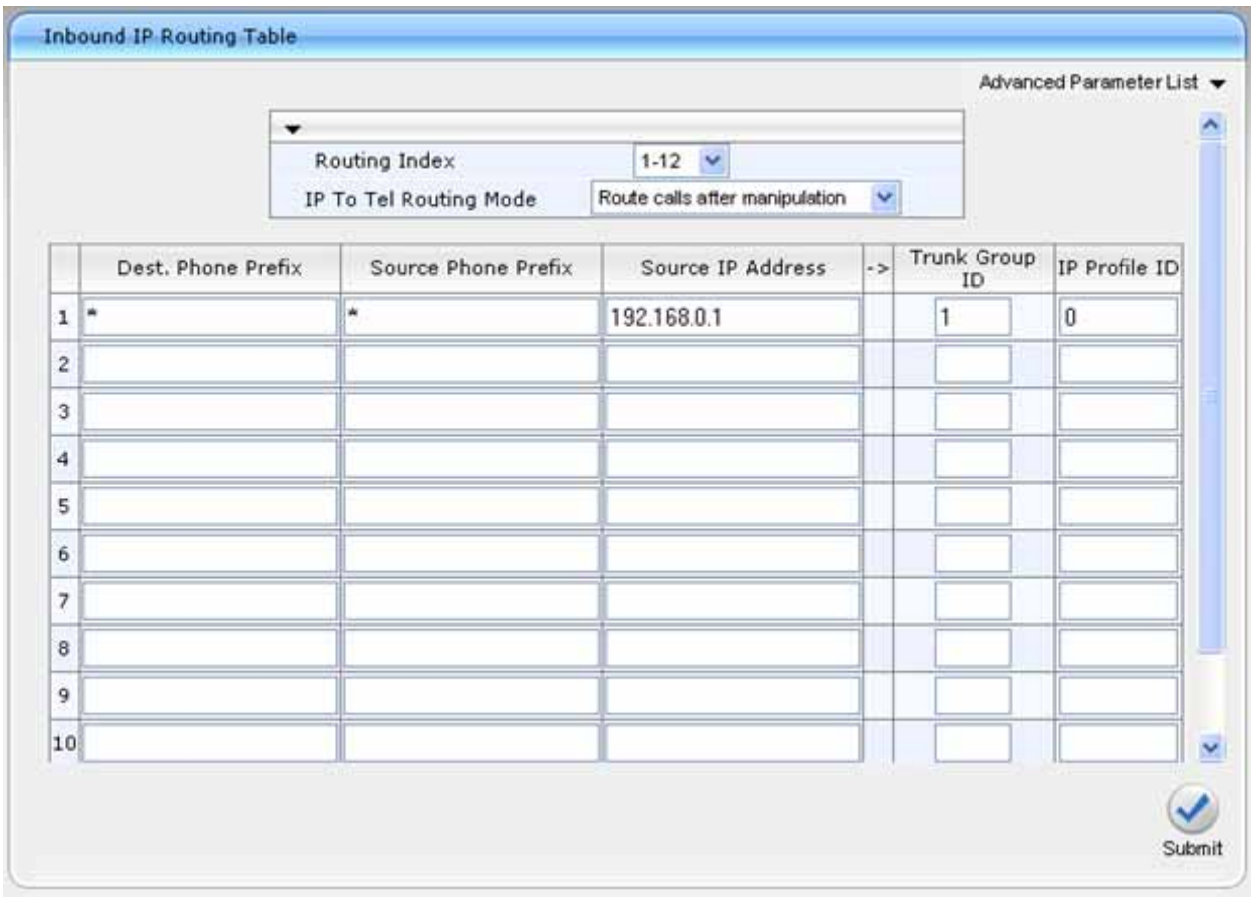
## 4.6.3 Configuring IP-to-Trunk Group Routing

This step defines how to configure the Media Gateway's IP to Trunk Group Routing table.

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

1. Open the 'IP to Trunk Group Routing' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **IP to Trunk Group Routing**).

**Figure 4-22: IP to Trunk Group Routing Page**




2. **Index #1** – all calls from source IP address of the Mediation Server, for any destination phone number and from any source phone number is routed to Trunk Group 1 (defined in the previous step).

**Note:** Since Lync 2010 requires that the Gateways must honor requests from Mediation Server if and only if the Mediation Server is listed in the allowed Mediation Servers, you must configure in the 'Source IP Address' column the IP Addresses of the Mediation Servers to avoid accepting calls from un-trusted SIP entity.

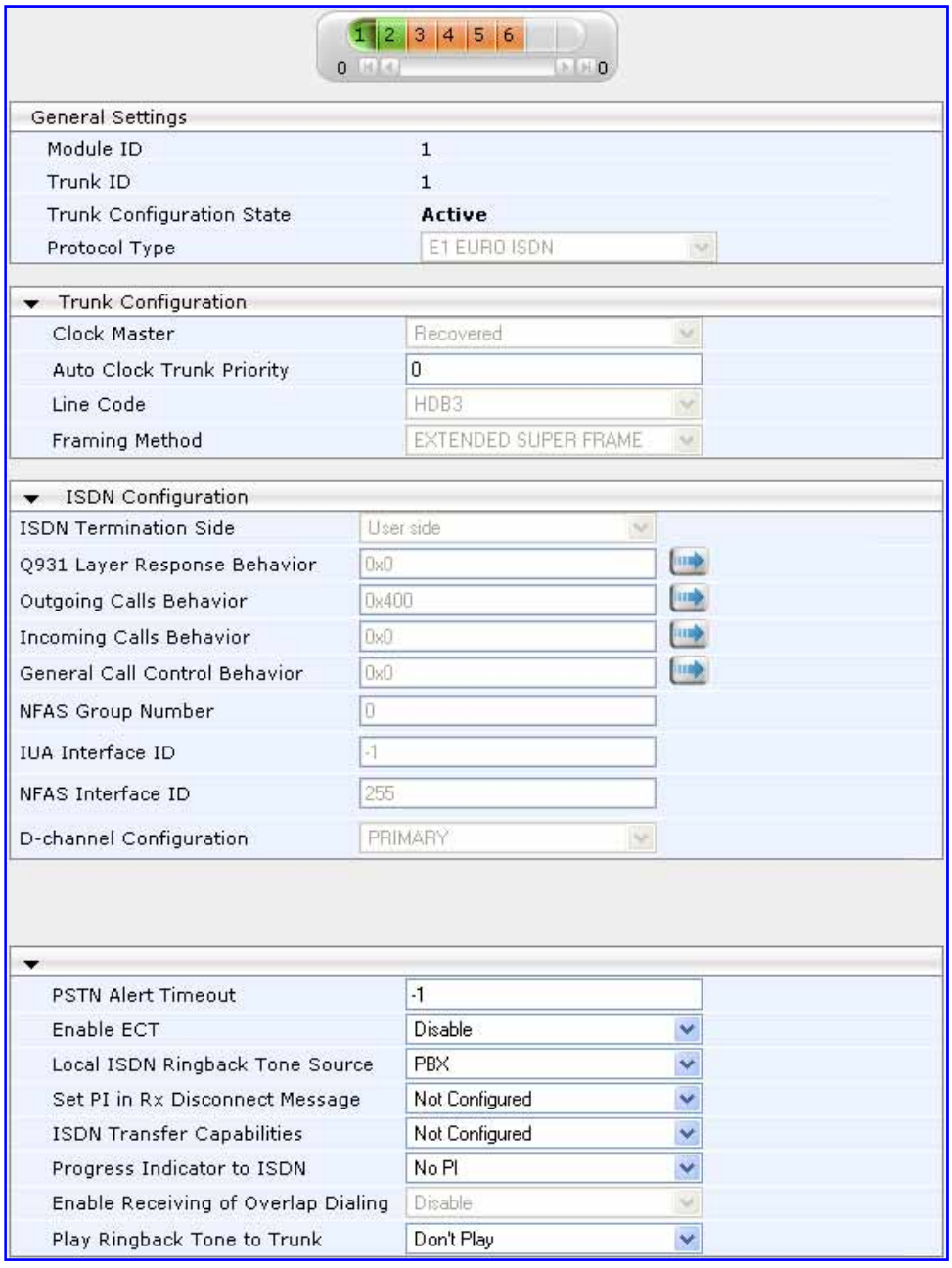
## 4.6.4 Configuring the Trunk Settings

The procedure below configures the Trunk settings.

➢ **To configure the Trunk settings:**

1. Open the 'Trunk Settings' page (**Configuration** tab > **PSTN Settings** menu > **Trunk Settings**).

**Figure 4-23: Trunk Settings Page**




On the top of the page, a bar with Trunk number icons displays the status of each trunk, according to the following color codes:

- Grey: Disabled
- Green: Active
- Yellow: RAI alarm
- Red: LOS / LOF alarm
- Blue: AIS alarm
- Orange: D-channel alarm (ISDN only)

2. Select the Trunk that you want to configure, by clicking the desired Trunk number icon. The bar initially displays the first eight Trunk number icons (i.e., trunks 1 through 8). To scroll through the Trunk number icons (i.e., view the next/last or previous/first group of eight Trunks),

   After you have selected a trunk, the following is displayed:

   - The read-only 'Module ID' field displays the module number to which the trunk belongs.
   - The read-only 'Trunk ID' field displays the selected trunk number.
   - The read-only 'Trunk Configuration State' displays the state of the trunk (e.g., 'Active' or 'Inactive').
   - The parameters displayed in the page pertain to the selected trunk only.

3. Click the **Stop Trunk** button (located at the bottom of the page) to de-activate the trunk so that you can configure currently grayed out (unavailable) parameters.(Skip this step if you want to configure parameters that are also available when the trunk is active). The stopped trunk is indicated by the following:

   - The 'Trunk Configuration State' field displays 'Inactive'.
   - The **Stop Trunk** button is replaced by the **Apply Trunk Settings** button. (When all trunks are stopped, the **Apply to All Trunks** button also appears.)
   - All the parameters are available and can be modified.

4. Configure the required trunk parameters.
5. Click the **Apply Trunk Settings** button to apply the changes to the selected trunk (or click **Apply to All Trunks** to apply the changes to all trunks); the **Stop Trunk** button replaces **Apply Trunk Settings** and the 'Trunk Configuration State' displays 'Active'.
6. Save (burn) the Media Gateway configuration and reset the Media Gateway, using the Web interface's 'Maintenance Actions' page (**Management Configuration** menu > **Maintenance Actions**).

**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 device.
- The displayed parameters on the page depend on the protocol selected in the 'Protocol Type' field.
- All trunks must be of the same line type (i.e., either 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 device's Release Notes).
- If the trunk protocol type is CAS, you can assign or modify a dial plan (in the 'Dial Plan' field) and perform this without stopping the trunk.
- If the trunk can't be stopped because it provides the device's clock (assuming the device is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the device's clock or enable 'TDM Bus PSTN Auto Clock' in the 'TDM Bus Settings' page (refer to Section 4.6.5).
- To delete a previously configured trunk, set the parameter 'Protocol Type' to 'None'.

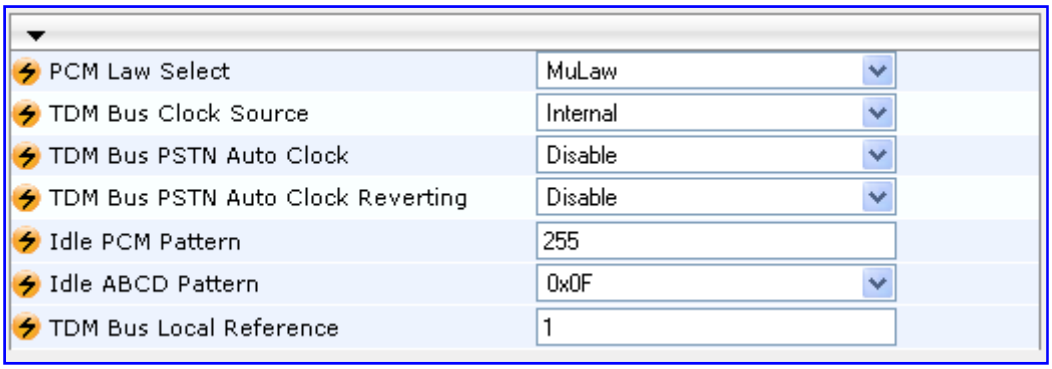
## 4.6.5 Defining TDM Bus Settings

The procedure below describes how to define TDM bus settings.

➢ **To define the TDM bus settings:**

1. Open the 'TDM Bus Settings' page (**Configuration** tab > **TDM Configuration** menu > **TDM Bus Settings**).

**Figure 4-24: TDM Bus Settings Page**




2. Configure the TDM bus parameters according to your deployment as required.
   - **PCM Law Select** - determines the type of PCM companding law in input/output TDM bus. Typically, A-Law is used for E1 spans and Mu-Law for T1/J1 spans.
   - **TDM Bus Clock Source** – determines the clock source to which the Media Gateway synchronizes. Generate clock from local source (Internal) or Recover clock from PSTN line (Network).
   - **TDM Bus Local Reference** – determine the Physical Trunk ID from which the Media Gateway recovers (receives) its clock synchronization when the TDM Bus Clock Source is configured to recover the clock from PSTN line.
3. Click **Submit** to save your changes.
4. Save (burn) the Media Gateway configuration and reset the Media Gateway, using the Web interface's 'Maintenance Actions' page (**Management Configuration** menu > **Maintenance Actions**).

## 4.6.6 Uploading CAS Files and Assigning to Trunks

If your deployment supports Channel Associated Signaling (CAS), you need to upload the CAS configuration file from your PC to the Media Gateway and then assign the CAS file to the trunk that is connected to the PBX. You can upload up to eight CAS files and assign different files to different trunks. The CAS file is downloaded from the Web in the same ZIP file as the *ini* configuration file.

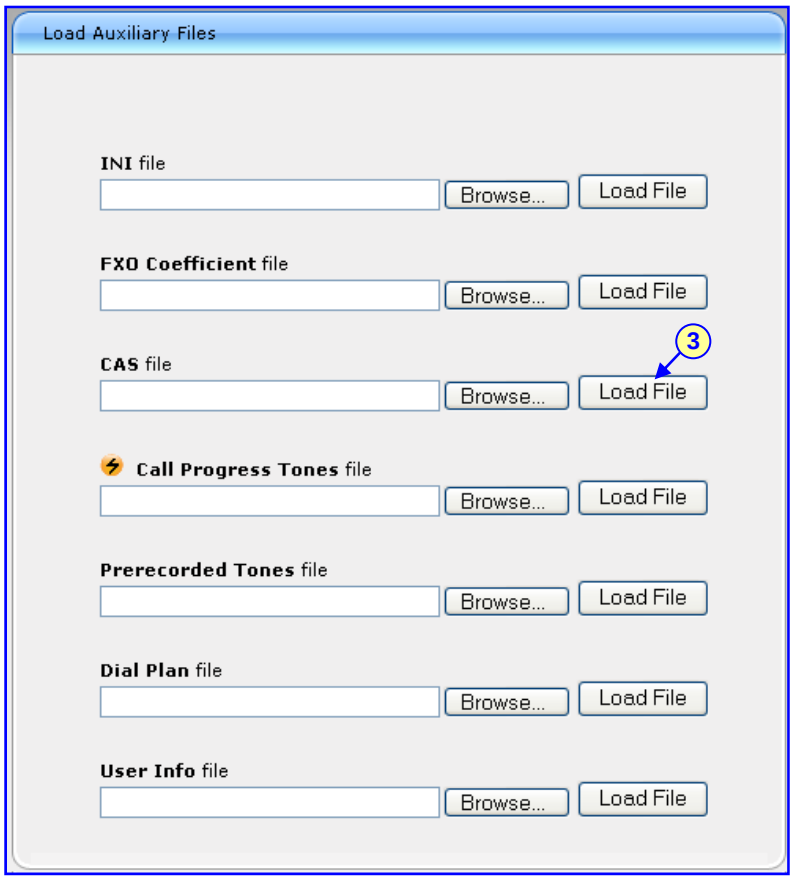
The CAS files contain the CAS Protocol definitions for CAS-terminated trunks. The Media Gateway supports different variants of CAS protocols for E1 and T1 spans, including MFC R2, E&M immediate start, E&M delay dial/start, loop start, and ground start.

**Note:** Ensure that the CAS table is applicable for operating with the deployed PBX/PSTN interfaces.

➢ **To upload CAS files and assign to Trunks:**

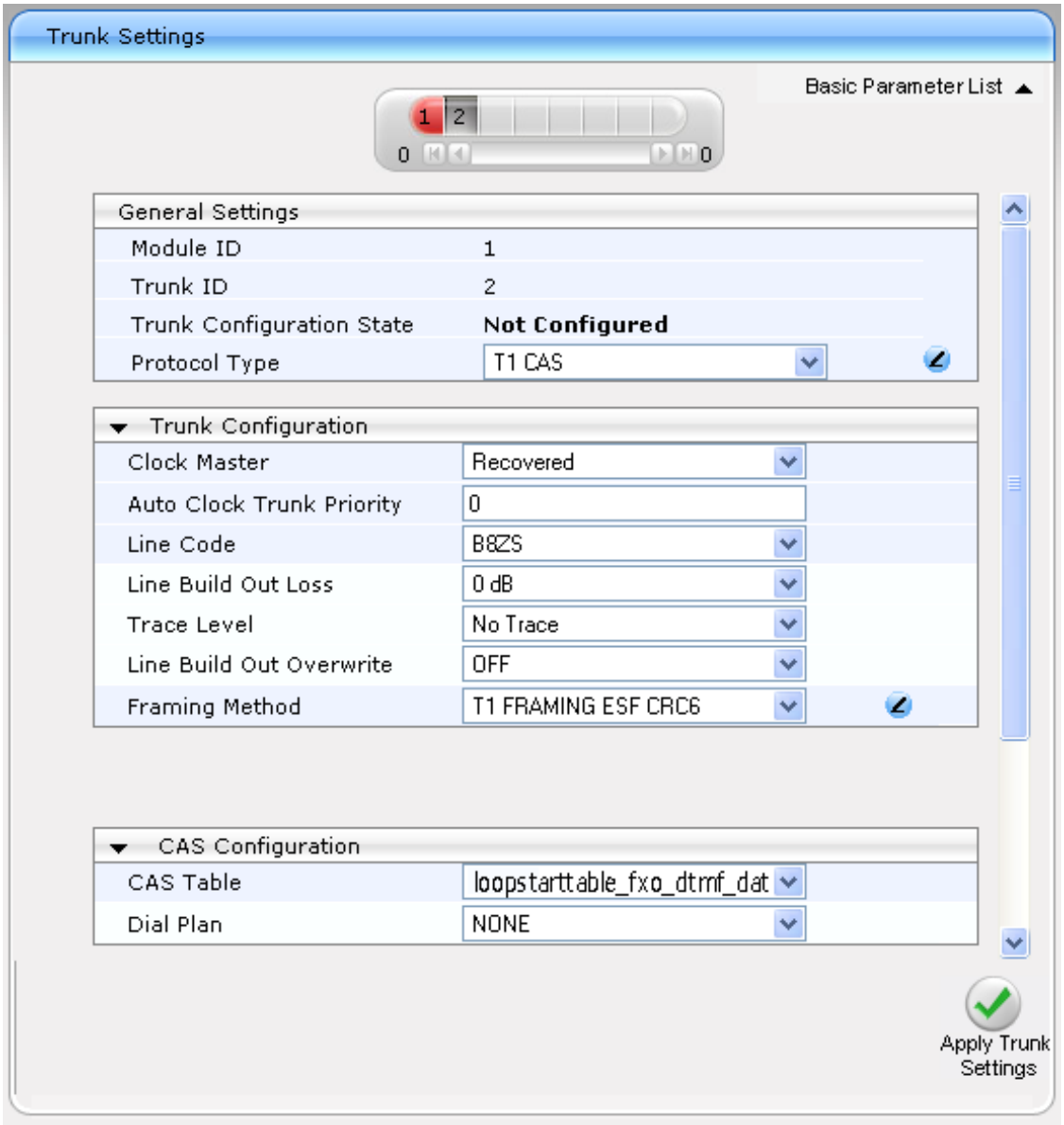
1. Open the 'Load Auxiliary Files' page (**Management** tab > **Software Update** menu > **Load Auxiliary Files**).

**Figure 4-25: Load Auxiliary Files Page**




2. Click the **Browse** button corresponding to the 'CAS file 'field, and then navigate to the CAS file you want uploaded to the Media Gateway. Select the file, and then click **Open**; the file name and path appear in the field beside the **Browse** button.
3. Click the **Load File** button corresponding to the ' CAS file' field; the file's loading takes effect on-the-fly.
4. Save (burn) the Media Gateway configuration and reset the Media Gateway, using the Web interface's 'Maintenance Actions' page (**Management Configuration** menu > **Maintenance Actions**).
5. Open the 'Trunk Settings' page (**Configuration** tab > **PSTN Settings** menu > **Trunk Settings**).

**Figure 4-26: Trunk Settings Page**




6. Click the **Trunk Status** icon to which you want to assign the CAS file, and then click **Stop Trunk** to de-activate the trunk.
7. From the 'CAS Table' drop-down list, select the CAS file (that you uploaded to the Media Gateway).
8. Click **Apply Trunk Settings** to apply the settings.
9. Save (burn) the Media Gateway configuration and reset the Media Gateway, using the Web interface's 'Maintenance Actions' page (**Management Configuration** menu > **Maintenance Actions**).

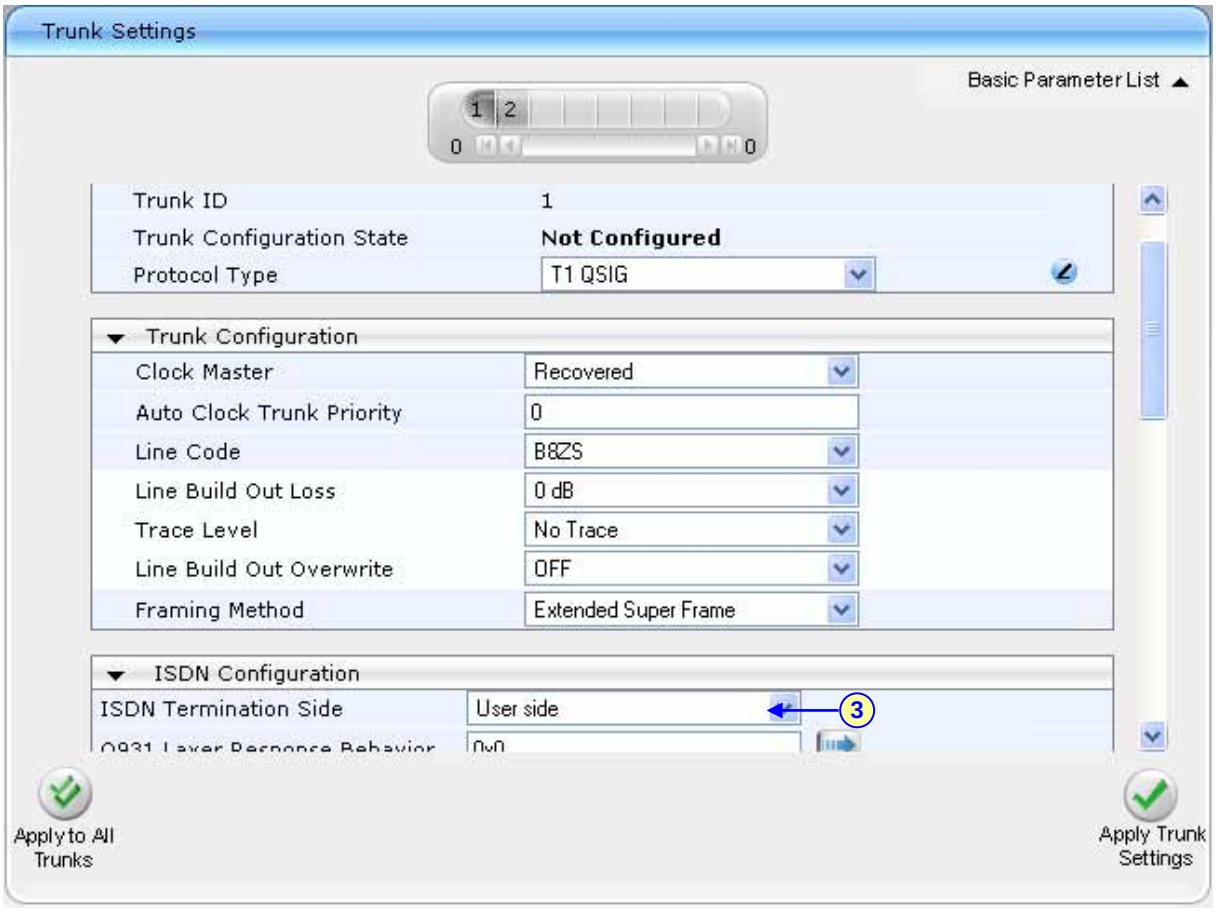
## 4.6.7 Defining ISDN Trunk Termination Side for QSIG

The procedure below describes how to change the ISDN termination side (User or Network side) for QSIG settings.

➢ **To define the Trunk ISDN termination side:**

1. Open the 'Trunk Settings' page (**Configuration** tab > **PSTN Settings** menu > **Trunk Settings**).

**Figure 4-27: Trunk Settings Page**




2. Click the **Trunk** icon pertaining to the trunk you want to configure, and then click **Stop Trunk** to de-activate the Trunk.
3. From the 'ISDN Termination' drop-down list, select whether the Trunk connected to the PBX is User or Network side.
4. Click **Apply Trunk Settings** to apply the settings.
5. Save (burn) the Media Gateway configuration and reset the Media Gateway, using the Web interface's 'Maintenance Actions' page (**Management Configuration** menu > **Maintenance Actions**).

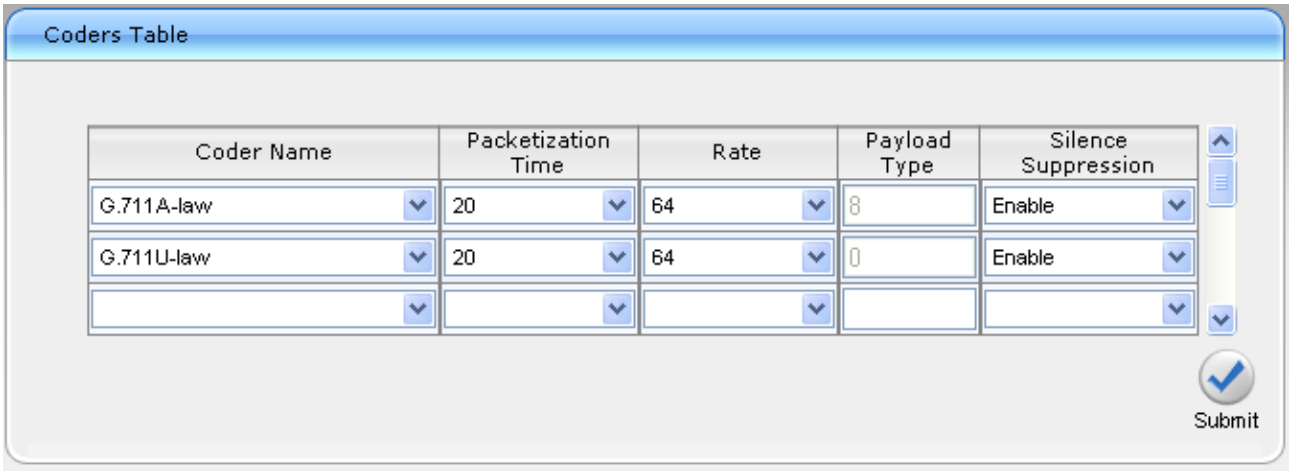
# 4.7 Defining Voice Coders

The Media Gateway communicates with Mediation Server using either the G.711 A-law or G.711 μ-law (Mu-Law) voice coder. It is recommended to use Silence Suppression to improve the performance of Mediation Server. The procedure below shows how you can change the default coder.

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

1. Open the 'Coders' page (**Configuration** tab > **Protocol Configuration** menu > **Coders And Profile Definition** submenu > **Coders** page item).

**Figure 4-28: Coders Table Page**




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**.

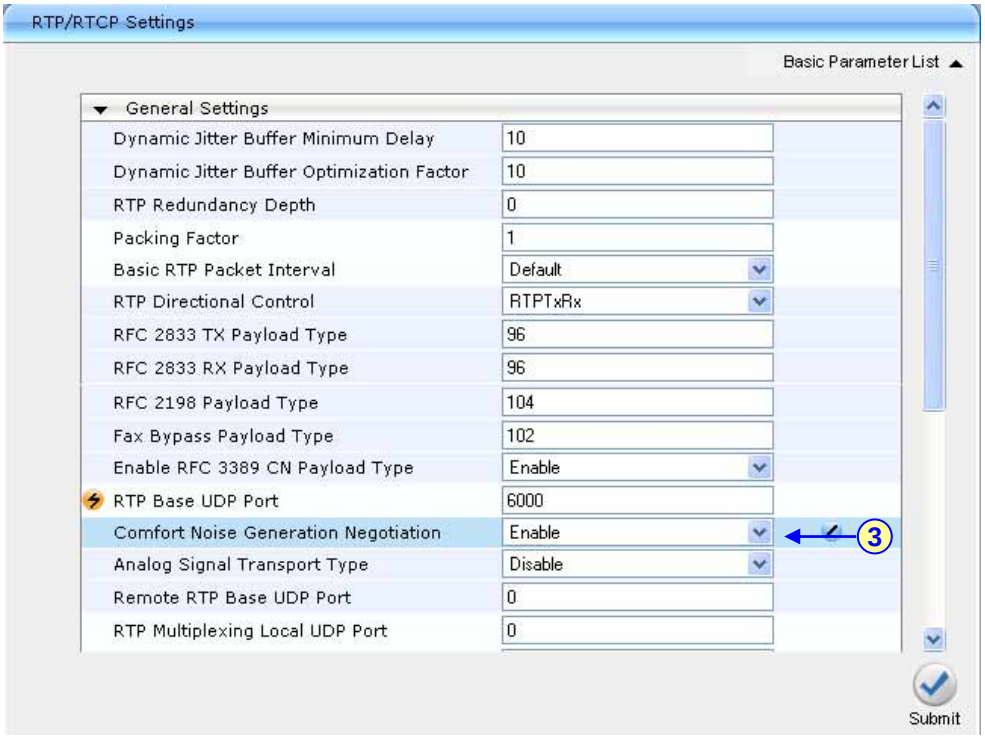
# 4.8 Define Silence Suppression, Comfort Noise and AGC

Overall voice quality is significantly better for Lync 2010. These improvements include 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 change the Media Gateway Silence Suppression, Comfort Noise and Automatic Gain Control (AGC) parameters to achieve this goal. Please note that the Echo canceller is enabled by default.

➢ **To configure silence suppression parameters:**

1. Silence Suppression is configured per coder type. (Refer to Section 4.7 above to enable Silence Suppression per coder.)
2. Open the 'RTP/RTCP Settings' page (**Configuration** tab > **Media Settings** menu > **RTP / RTCP Settings**).

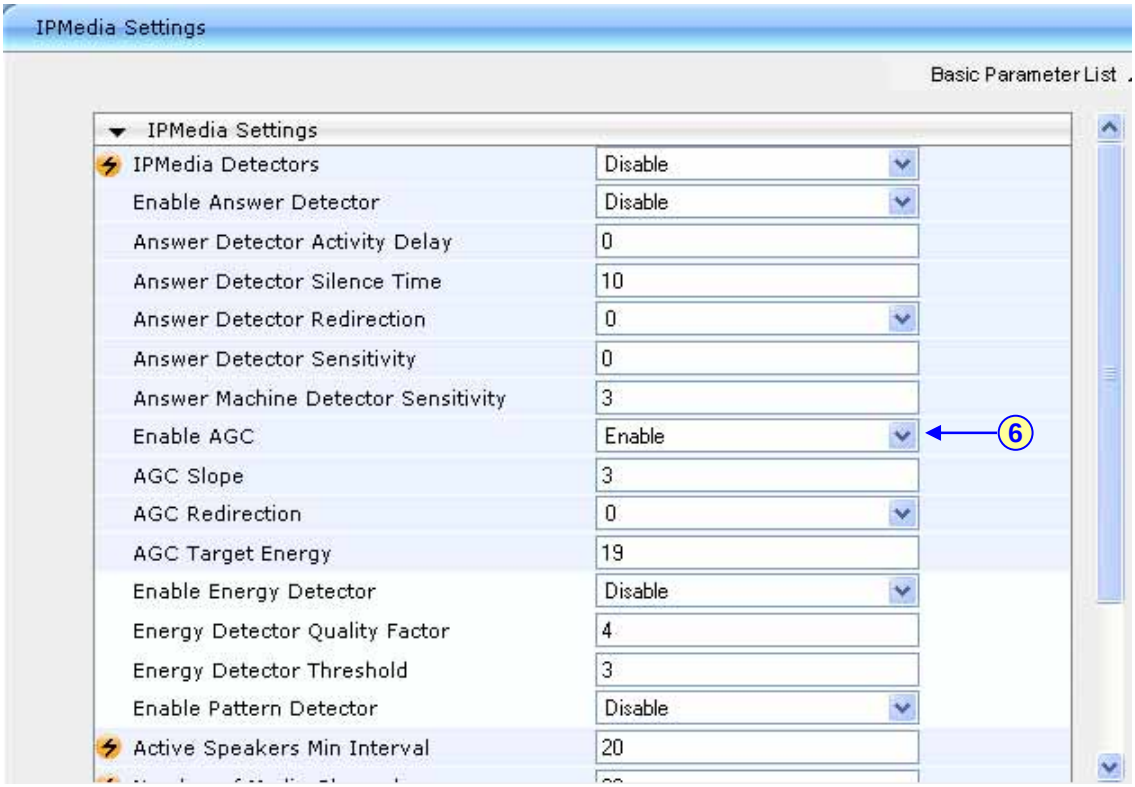
**Figure 4-29: RTP/RTCP Settings Page**




3. From the 'Comfort Noise Generation Negotiation' drop-down list, select 'Enable'. This enables negotiation and usage of Comfort Noise (CN).
4. Click **Submit**.

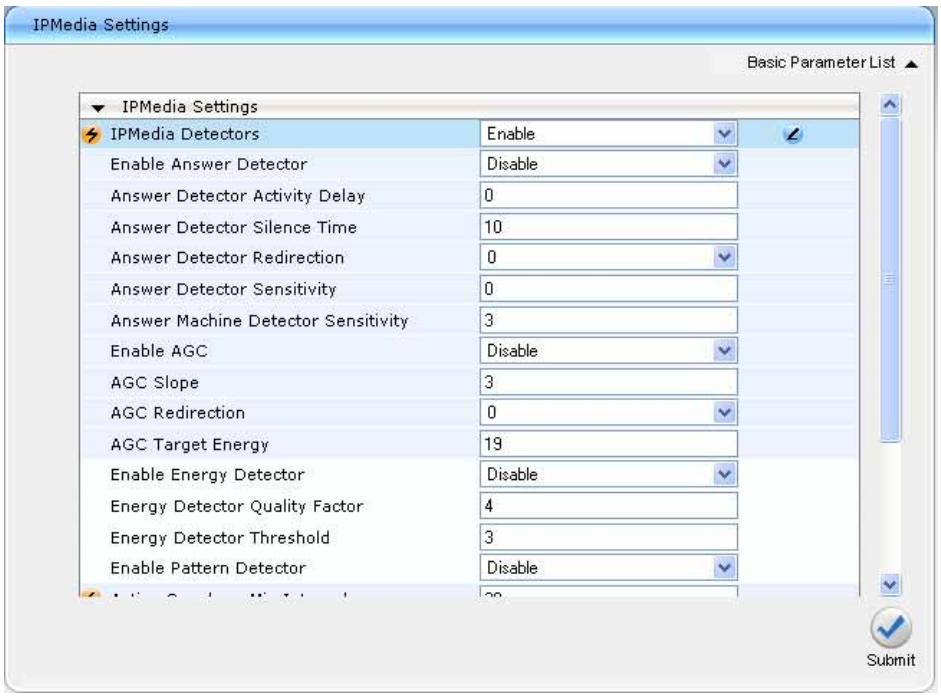
5. Open the 'IPMedia Settings' page (**Configuration** tab > **Media Settings** menu > **IPmedia Settings**).

**Figure 4-30: IPMedia Settings Page**




6. From the 'Enable AGC' drop-down list, select 'Enable'.
7. Click **Submit**.
8. Open the 'IPMedia Settings' page (**Configuration** tab > **Media Settings** menu > **IPMedia Settings** page item.
9. From the 'IPMedia Detectors' drop-down list, select 'Enable'.

**Figure 4-31: IPMedia Settings**



# 4.9 Defining 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.

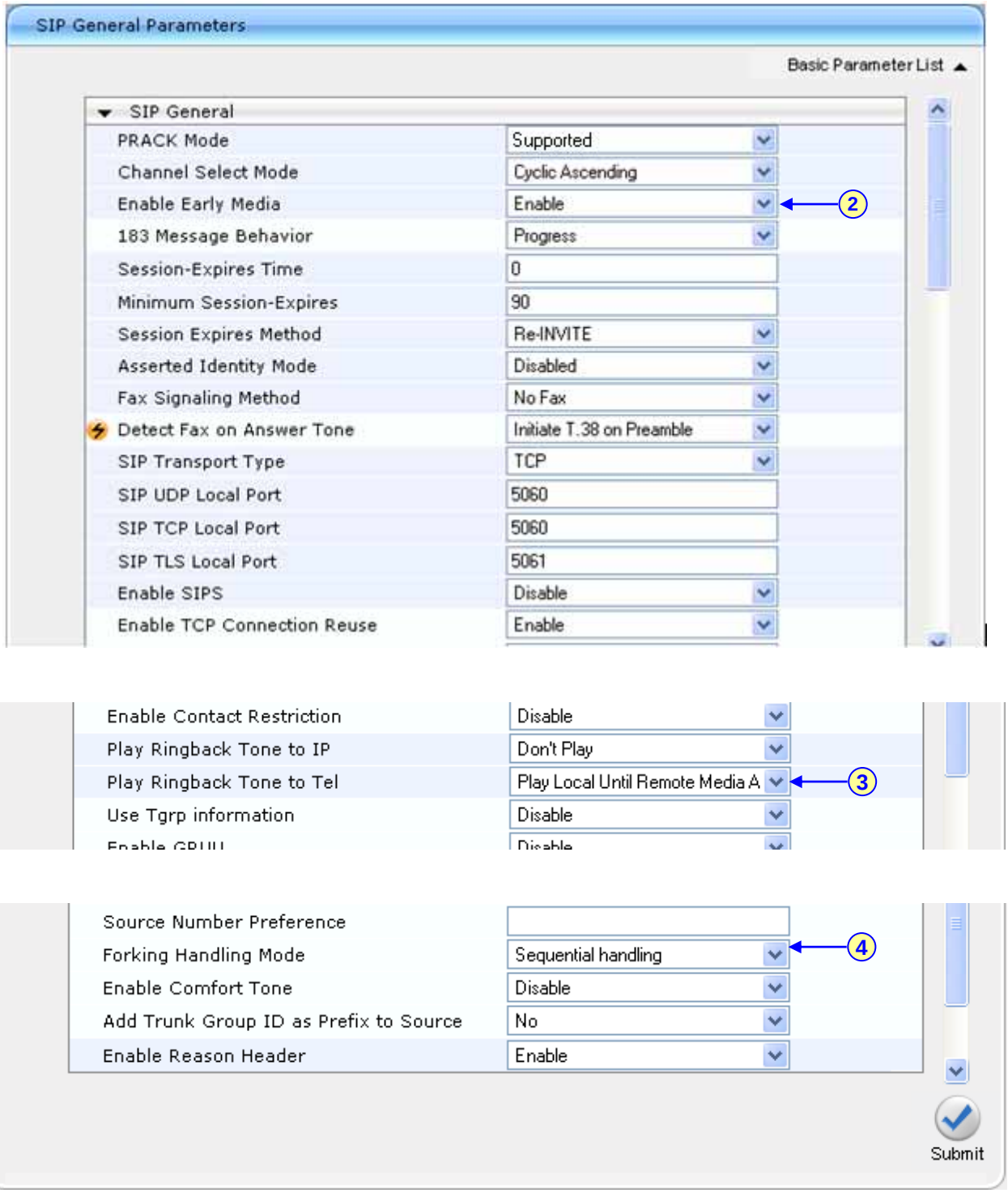
According to Lync 2010 requirements, the AudioCodes Media Gateway should send 183 with SDP, immediately after it receives an INVITE. The RTP packets however, will not be sent until the Media Gateway receives Progress, Alerting + Progress Indicator or Connect from ISDN. For example, if the Media Gateway receives ISDN Progress, it starts sending RTP packets according to initial negotiation, but there is no need to send again the 183 response.

You may need to change the Media Gateway's early media parameter to support Lync 2010 enhanced early media feature.

➢ **To define the Early Media parameters:**

1. Open the **'SIP General Parameters'** page (**Configuration** tab > **Protocol Configuration** menu > **Protocol Definition** submenu > **SIP General Parameters**).

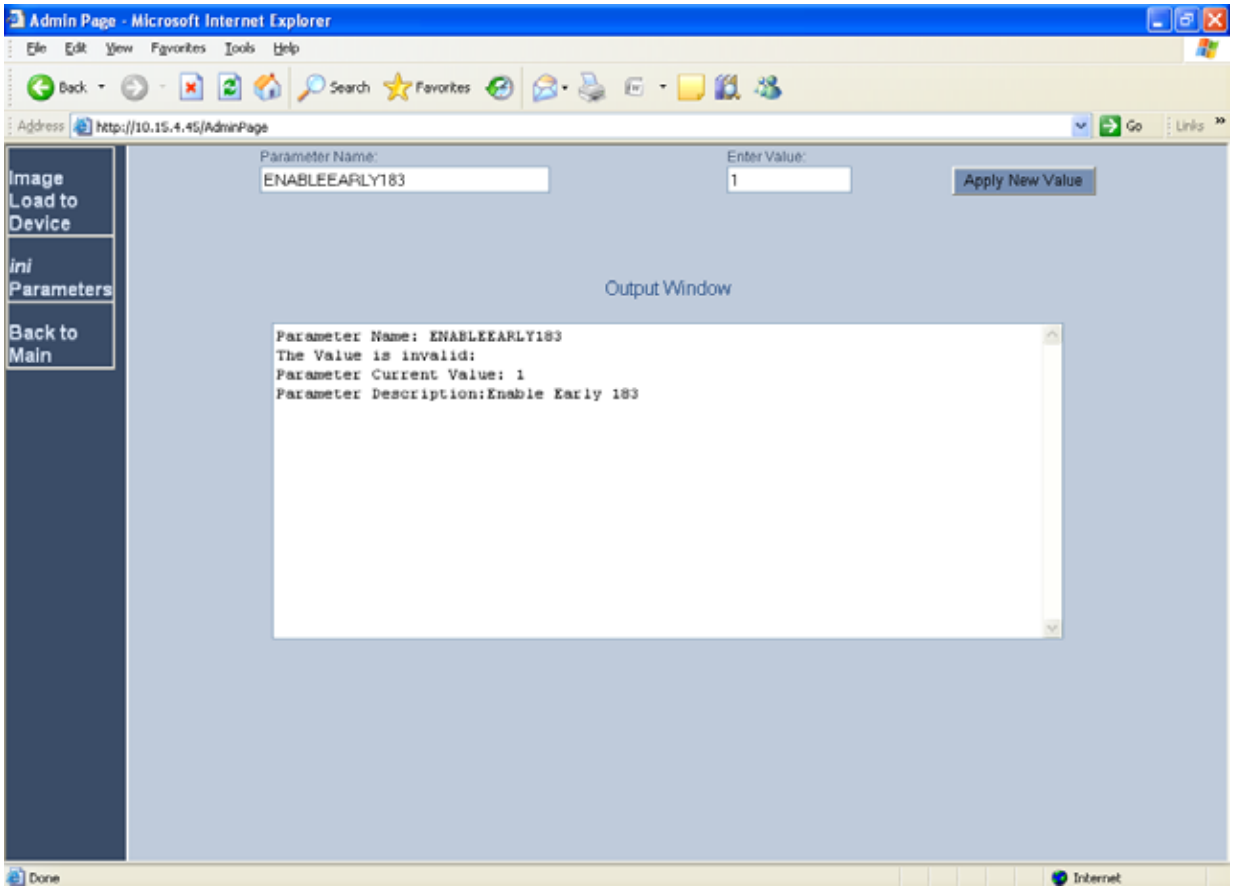
**Figure 4-32: SIP General Parameters Page**




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

4. From the 'Forking Handling Mode' drop-down list, select 'Sequential handling'. The Media Gateway opens a voice stream toward the first 18x SIP response that includes an SDP and disregards any 18x response with an SDP received thereafter.
5. Click **Submit** to save your changes.
6. 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://10.15.4.15/AdminPage).

**Figure 4-33: Admin Page Settings**




7. In the Admin Page, on the left pane, click **ini Parameters**.
8. In the 'Parameter Name' field, enter the parameter "ENABLEEARLY183".
9. In the 'Enter Value' field, enter "1".
10. Click **Apply New Value**.
11. Save the changes to flash memory, by clicking the **Burn** button on the toolbar.

# 4.10 Translating Numbers From/To E.164 Using Manipulation Tables for PBX/PSTN Connectivity

The Manipulation tables provide the ability to translate (normalize) numbers dialed in standard E.164 format to various formats and vice versa. Manipulation is necessary for your dial plan as Lync 2010 uses the standard E.164 format while your PBX or PSTN implements other number formats for dialing.

Due to Lync 2010 normalization rules, the Media Gateway may need to perform number manipulation for outbound calls (i.e., calls received from OC clients/endpoints through Lync 2010) and inbound calls (i.e., calls destined for OC clients). If the Media Gateway is connected to a PBX or directly to the PSTN, the Media Gateway may need to perform number manipulations for the called and/or calling number to match the PBX or PSTN interfaces dialing rules or to match Lync 2010 E.164 format.

## 4.10.1 Manipulation Tables

The **Manipulation Tables** submenu allows you to configure number manipulation and mapping of NPI/TON to SIP messages. The number manipulation rules are configured in the following 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

Manipulation number configuration examples are provided for inbound and outbound calls in Section 4.10.4.

➢ **To configure the Number Manipulation tables:**

1. Open the Number Manipulation page you want to configure (**Configuration** tab > **Protocol Configuration** menu > **Manipulation Tables** submenu > **Dest Number IP->Tel**, **Dest Number Tel->IP**, **Source Number IP->Tel**, or **Source Number Tel->IP**); the relevant Manipulation table page is displayed (e.g., 'Source Phone Number Manipulation Table for Tel→IP Calls' page).

**Figure 4-34: Source Phone Number Manipulation Table for Tel-to-IP Calls**

| | Destination Prefix | Source Prefix | Stripped Digits Number | Prefix (Suffix) to Add | Number of Digits to Leave | Presentation |
|---|---|---|---|---|---|---|
| 1 | 03 | 201 | 0 | 971 | | Allowed |
| 2 | | 1001 | 4 | 5(23) | | Restricted |
| 3 | | 123451001# | 0 | (8) | 4 | Not Configured |
| 4 | | [30-40]xx | (1) | 2 | | Not Configured |
| 5 | [6,7,8] | 2001 | 5 | 3 | | Not Configured |
| 6 | | | | | | Not Configured |

The figure above shows an example of the use of manipulation rules in the 'Source Phone Number Manipulation Table for Tel→IP Calls':

- When the destination number is 035000 and source number is 20155, the source number is changed to 97120155.
- When the source number is 1001876, it is changed to 587623.
- When the source number is 1234510012001, it is changed to 20018.
- When the source number is 3122, it is changed to 2312.

2. From the 'Table Index' drop-down list, select the range of entries that you want to edit (up to 20 entries can be configured for Source Number IP-to-Tel Manipulation, up to 120 entries can be configured for Source Number Tel-to-IP Manipulation, and up to 100 entries for Destination Number Manipulation).

3. Configure the Number Manipulation table according to the table below.
4. Click **Submit** to save your changes.
5. Save the changes to flash memory, by clicking the **Burn** button.

**Notes:**

- The manipulation rules are executed in the following order:
  1. Number of stripped digits.
  2. Number of digits to leave.
  3. Prefix / suffix to add.
- The manipulation rules can be applied to any incoming call whose source IP address (if applicable), source Trunk Group (if applicable), source IP Group (if applicable), destination number prefix and source number prefix matches the values defined in the 'Source IP Address', 'Source Trunk Group', 'Source IP Group', 'Destination Prefix', and 'Source Prefix' fields respectively. The number manipulation can be performed using a combination of each of the above criteria, or using each criterion independently.
- For available notations that represent multiple numbers, refer to Section 4.10.2 on page 93.

**Table 4-1: Number Manipulation Parameters Description**

| Parameter | Description |
|---|---|
| Source Trunk Group | The source Trunk Group (1-99) for Tel-to-IP calls. To denote any Trunk Group, leave this field empty.<br>**Notes:**<br>▪ 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.<br>▪ 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.<br>**Notes:**<br>▪ This parameter is available only in the 'Source Phone Number Manipulation Table for Tel -> IP Calls' page.<br>▪ If this Source IP Group has a Serving IP Group, then all calls originating from this Source IP Group is 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. |

| Parameter | Description |
|---|---|
| Source IP | Source IP address of the caller (obtained from the Contact header in the INVITE message).<br>**Notes:**<br>▪ This parameter is applicable only to the Number Manipulation tables for IP-to-Tel calls.<br>▪ 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.<br>▪ 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. |
| 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. |
| 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. |
| NPI | The Numbering Plan Indicator (NPI) assigned to this entry.<br>▪ **[0]** Unknown (default)<br>▪ **[9]** Private<br>▪ **[1]** E.164 Public<br>▪ **[-1]** Not Configured = value received from PSTN/IP is used<br>**Notes:**<br>▪ This parameter is applicable only to Number Manipulation tables for IP-to-Tel calls.<br>▪ For a detailed list of the available NPI/TON values, refer to 4.10.3 on page 94. |
| TON | The Type of Number (TON) assigned to this entry.<br>▪ If you selected 'Unknown' for the NPI, you can select Unknown [0].<br>▪ 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].<br>▪ 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].<br>**Notes:**<br>▪ This parameter is applicable only to Number Manipulation tables for IP-to-Tel calls.<br>▪ The default is 'Unknown'. |

| Parameter | Description |
|---|---|
| Presentation | Determines whether Caller ID is permitted:<br>▪ Not Configured = privacy is determined according to the Caller ID table.<br>▪ Allowed = sends Caller ID information when a call is made using these destination / source prefixes.<br>▪ Restricted = restricts Caller ID information for these prefixes.<br>**Notes:**<br>▪ Only applicable to Number Manipulation tables for source number manipulation.<br>▪ If 'Presentation' is set to 'Restricted' and 'Asserted Identity Mode' 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. |

## 4.10.2 Dialing Plan Notation

The dialing plan notation applies to the Number Manipulation tables, 'Tel to IP Routing' table and 'IP to Trunk Group Routing'. The dialing notation applies to digits entered for the destination and source prefixes to represent multiple numbers.

**Table 4-2: Dialing Plan Notations**

| Notation | Description | Example |
|---|---|---|
| **[n-m]** | Represents a range of numbers.<br>**Note:** Range of letters is not supported. | ▪ **[5551200-5551300]#:** represents all numbers from 5551200 to 5551300.<br>▪ **123[100-200]#:** represents all numbers from 123100 to 123200. |
| **[n,m,...]** | Represents multiple numbers. Up to three digits can be used to denote each number. | ▪ **[2,3,4,5,6]#:** represents a one-digit number that starts with 2, 3, 4, 5, or 6.<br>▪ **[11,22,33]xxx#:** represents a five-digit number that starts 11, 22, or 33.<br>▪ **[111,222]xxx#:** represents a six-digit number that starts 111 or 222. |
| **x** | Represents any single digit. | **54324:** represents any number that starts with 54324. |
| **Pound sign (#) at the end of a number** | Represents the end of a number. | **54324xx#:** represents a 7-digit number that starts with 54324. |
| **A single asterisk (*)** | Represents any number. | ***:** represents any number (i.e., all numbers). |

The device matches the rules starting at the top of the table (i.e., top rules take precedence over lower rules). For this reason, enter more specific rules above more generic rules. For example, if you enter 551 in entry 1 and 55 in entry 2, the device applies rule 1 to numbers that start with 551 and applies rule 2 to numbers that start with 550, 552, 553, 554, 555, 556, 557, 558 and 559. However, if you enter 55 in entry 1 and 551 in entry 2, the device applies rule 1 to all numbers that start with 55 including numbers that start with 551.

### 4.10.3 Numbering Plans and Type of Number

Numbers are classified by their Numbering Plan Indication (NPI) and their Type of Number (TON). The Media Gateway supports all NPI/TON classifications used in the standard. The list of ISDN ETSI NPI/TON values is shown in the following table:

**Table 4-3: NPI/TON Values for ISDN ETSI**

| NPI | TON | Description |
|---|---|---|
| Unknown [0] | Unknown [0] | A valid classification, but one that has no information about the numbering plan. |
| E.164 Public [1] | Unknown [0] | A public number in E.164 format, but no information on what kind of E.164 number. |
| | International [1] | A public number in complete international E.164 format, e.g., 16135551234. |
| | National [2] | A public number in complete national E.164 format, e.g., 6135551234. |
| | Subscriber [4] | A public number in complete E.164 format representing a local subscriber, e.g., 5551234. |
| Private [9] | Unknown [0] | A private number, but with no further information about the numbering plan. |
| | Level 2 Regional [1] | |
| | Level 1 Regional [2] | A private number with a location, e.g., 3932200. |
| | PISN Specific [3] | |
| | Level 0 Regional (local) [4] | A private local extension number, e.g., 2200. |

For NI-2 and DMS-100 ISDN variants, the valid combinations of TON and NPI for calling and called numbers include (Plan/Type):

- **0/0** - Unknown/Unknown
- **1/1** - International number in ISDN/Telephony numbering plan
- **1/2** - National number in ISDN/Telephony numbering plan
- **1/4** - Subscriber (local) number in ISDN/Telephony numbering plan
- **9/4** - Subscriber (local) number in Private numbering plan

## 4.10.4 Number Normalization Examples

Two examples are provided below for number normalization. The examples are based on the following assumptions: a PBX with prefix (local) number 333 and a 4-digit extension number that begins with the digit 1 (i.e., 1xxx); National area code 206; Country code 1.

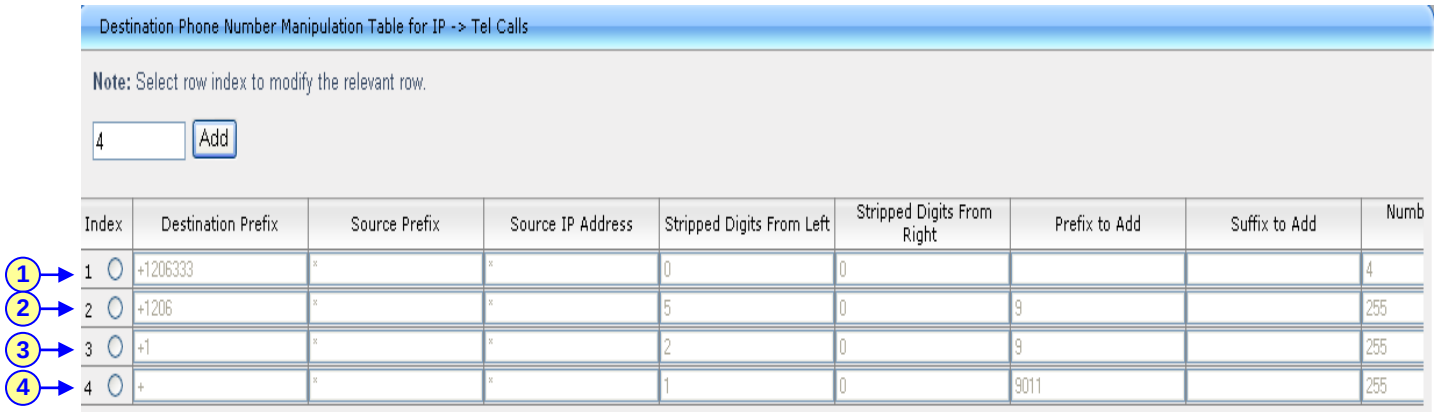
- **Modifying E.164 Numbers to PBX Format for Outbound Calls**

  Outbound calls refer to calls made by Lync 2010 users (OC clients) connected through IP to the Lync 2010.

  1. **Local calls within the PBX:** The caller dials only the last four digits (e.g., 1212). Lync 2010 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 Media Gateway's 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 2010 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 Media Gateway's Manipulation table is configured to remove (strip) the first five digits and add 9 as a prefix to the remaining number. Therefore, the Media 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 2010 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 Media Gateway's 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 Media Gateway sends the number 95033311425 to the PBX, and then the PBX sends the number 5033311425 to the PSTN.
  4. **Making 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 2010 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 Media Gateway's 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 Media 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 below:

**Figure 4-35: Phone Number Manipulation Table for IP→Tel Calls**



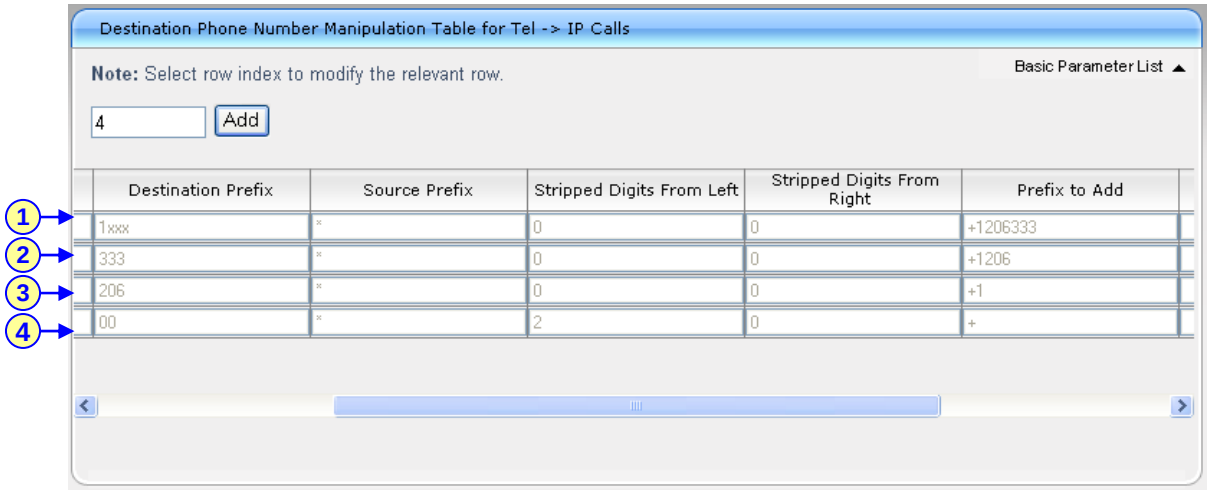
- **Modifying PBX, Local, and National Calls to E.164 Format for Inbound Calls**

Inbound calls refer to calls received by OC clients connected through IP to the Lync 2010.

1. **Local calls from the PBX or PSTN:** the PBX user only dials a 4-digit extension number of the OC client (e.g., 1220). The Media Gateway's Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1206333 to the extension number. Therefore, the Media Gateway sends the number +12063331220 to Lync 2010, which relays the call to the OC 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 Media Gateway. The Media Gateway's Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1206 to the number. Therefore, the Media Gateway sends the number +12063331220 to Lync 2010, which relays the call to the OC 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 Media Gateway. The Media Gateway's Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1 to the number. Therefore, the Media Gateway sends the number +12063331220 to Lync 2010, which relays the call to the OC client. **Note:** Whether the area code is received by the Media 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 Media Gateway. The Media Gateway's 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 Media Gateway sends the number +12063331220 to Lync 2010, which relays the call to the OC client. **Note:** Whether the international and country codes are received by the Media Gateway depends on the country's PSTN numbering rules.

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

**Figure 4-36: Phone Number Manipulation Table for Tel→IP Calls**



# 5 Connecting Analog Devices to Lync 2010

This section describes how to connect analog devices deployed in the Lync 2010 environment, using AudioCodes Enhanced Media Gateway.

In such a network architecture, the routing of calls is performed as follows:

1. Calls originating from the analog devices or from the PSTN toward the Media Gateway are routed to Microsoft's Mediation Server.
2. The Mediation Server (using the Lync 2010 Front End server) determines whether the call is routed to one of the OC clients or routed back to the central, AudioCodes Media Gateway toward one of the analog devices or to the PSTN.
3. The Mediation Server routes the calls to the single, central Media Gateway.
4. The Media Gateway routes the call to various media gateways, to any other SIP entity that serves these analog devices (such as fax machines, modems, Teletypewriter/TTY, text phones, and analog phones), or to the PSTN.

**Notes:**

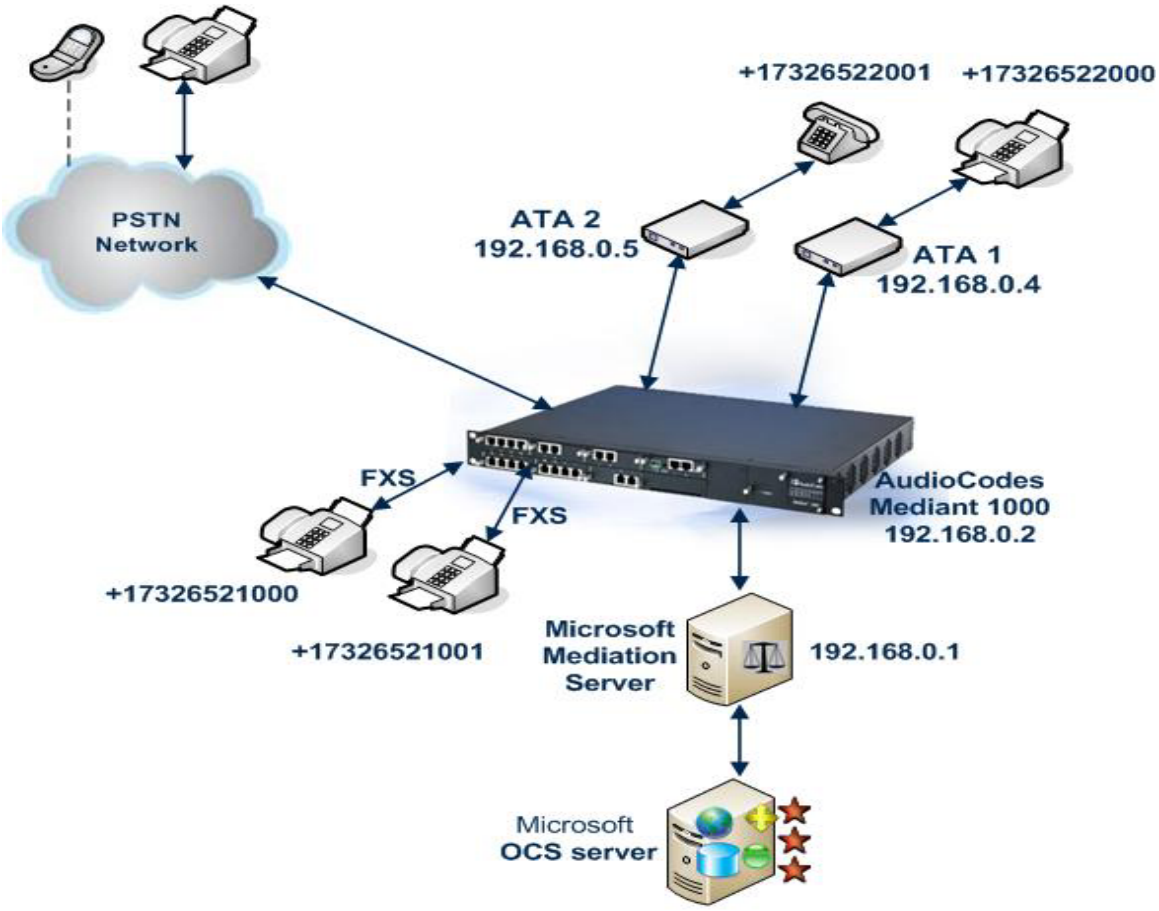
- The connection to the PSTN can be provided using embedded Trunk (E1/T1) cards or embedded analog (FXO) cards.
- The SIP entities that serve the analog devices can be either external ATA SIP devices, or embedded analog (FXS) cards.

The Media Gateway implements static routing decisions to route calls to the analog devices. This routing is based on the Media Gateway's internal IP-to-IP routing tables, which uses the analog devices' phone numbers and IP addresses.

To better understand the advantages of implementing the Media Gateway's IP-to-IP feature in the Lync 2010 environment, assume the following example scenario (refer to Figure 5-1):

- The enterprise has a deployed Lync 2010 at its headquarters and OC clients connected to Lync 2010.
- The enterprise has a deployed AudioCodes' Mediant 1000 Media Gateway. This Media Gateway is connected with several trunks to the legacy PBX\PSTN, and provides an integrated analog (FXS ports) card that serves analog fax machines.
- The enterprise has several SIP entities serving various analog devices that work with TCP/RTP transport type.

**Figure 5-1: Connecting Analog Devices in Lync 2010 Environment using AudioCodes Gateway**



# 5.1 Enhanced Media Gateway Configuration

The procedures described in this section for implementing analog devices in the Lync 2010 environment using AudioCodes gateways, assumes the setup example illustrated in Figure 5-1.

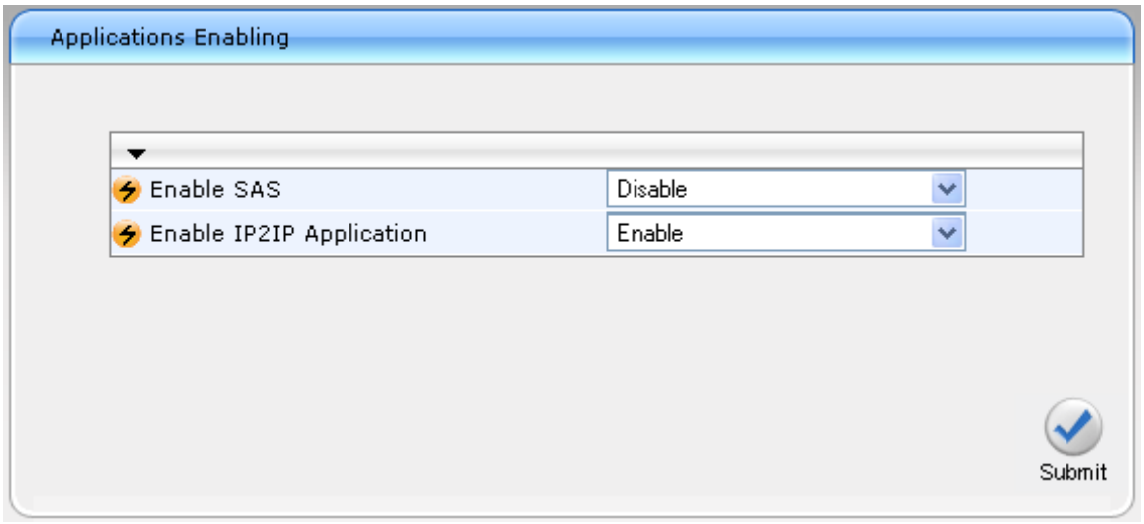
## 5.1.1 Step 1: Enable IP-to-IP Application

This step defines how to enable the Media Gateway's IP-to-IP (IP2IP) application.

➢ **To enable IP-to-IP application:**

1. Open the 'Applications Enabling' page (**Configuration** tab > **Protocol Configuration** menu > **Applications Enabling**).

**Figure 5-2: Applications Enabling Page**




2. From the 'Enable IP2IP Application' drop-down list, select "Enable".
3. Reset the Media Gateway.

**Note:** This page displays the application only if the Media Gateway is installed with the relevant Software Upgrade Key supporting the IP-to-IP application.

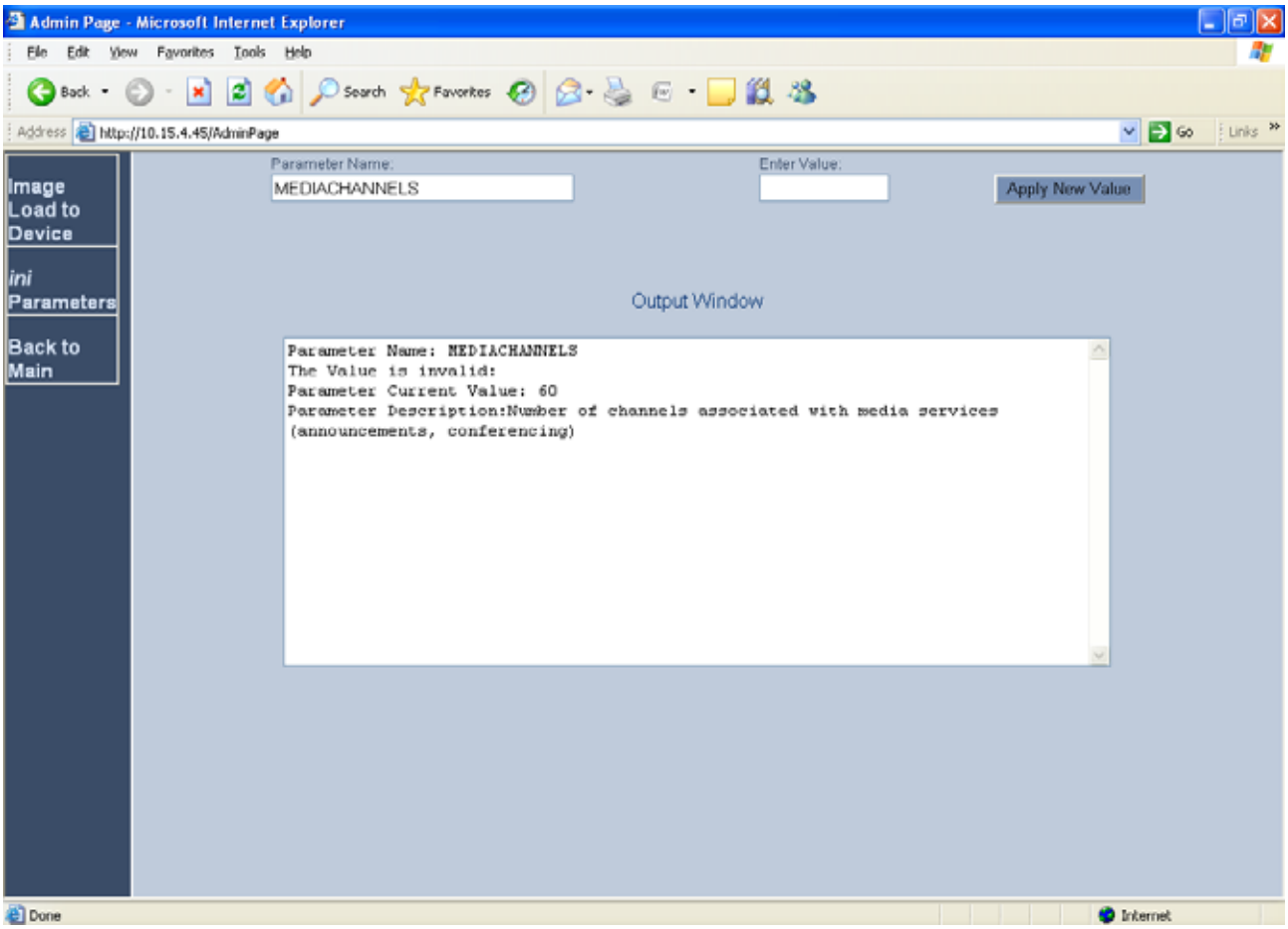
### 5.1.2 Step 2: Configure the Number of Media Channels

The number of media channels represents the number of digital signaling processors (DSP) channels that the Media Gateway allocates for IP-to-IP calls (the remaining DSP channels can be used for PSTN calls). Two IP media channels are used per IP-to-IP call session. The maximum number of media channels available on the Media Gateway is 120 (i.e., up to 60 IP-to-IP calls).

➢ **To configure the number of the media channels:**

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://10.15.4.45/AdminPage).

**Figure 5-3: Admin Page for IP Media Channels Settings**




2. On the left pane, click **ini Parameters**.
3. In the 'Parameter Name' field, enter the parameter "MEDIACHANNELS".
4. In the 'Enter Value' field, enter the number of required IP-to-IP sessions multiplied by two. For example, enter “60” to enable up to 30 IP-to-IP calls.
5. Click **Apply New Value**.

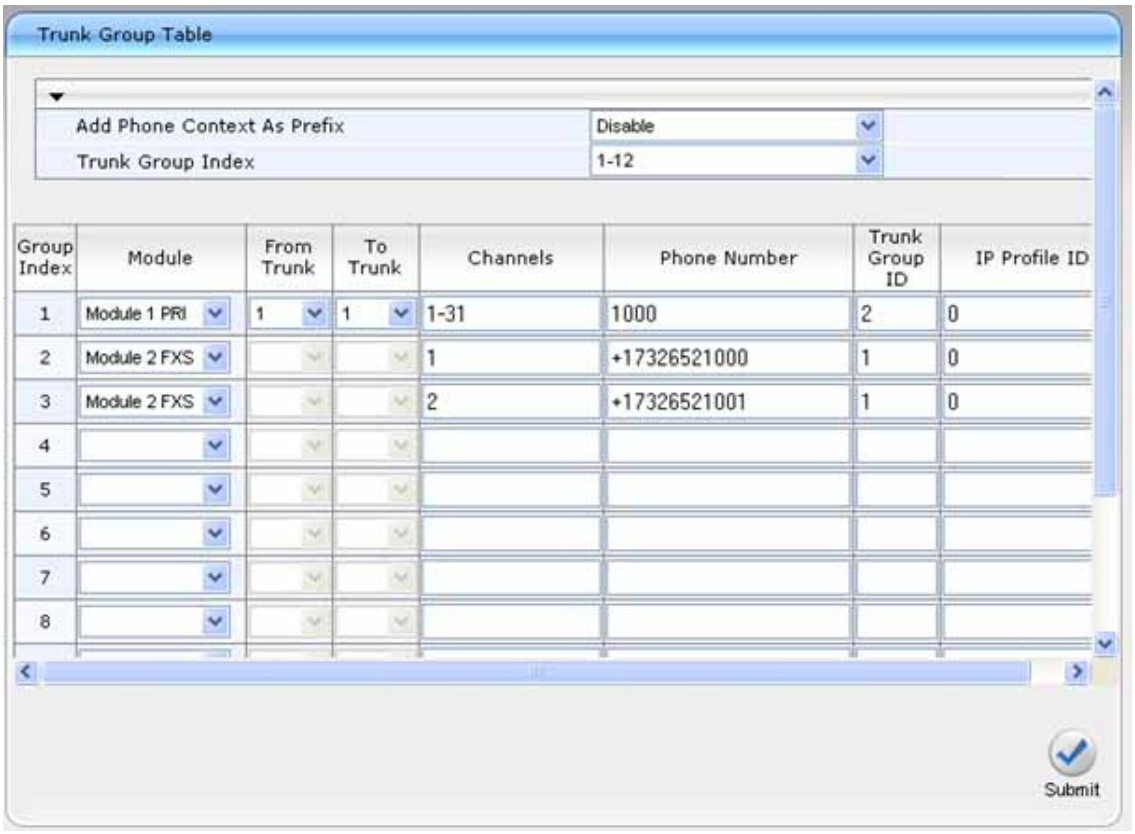
### 5.1.3 Step 3: Configure Trunk Group Table

This step defines how to enable the Media Gateway's FXS port PSTN trunk channels. The 'Trunk Group Table' page allows you to enable the device's channels by assigning them telephone numbers and other attributes (e.g., Trunk Groups and Profiles).

➢ **To configure the Trunk Group table:**

1. Open the 'Trunk Group Table' page (**Configuration** tab > **Protocol Configuration** menu > **Trunk Group** submenu > **Trunk Group**).

**Figure 5-4: Trunk Group Table Page**




2. Configure the Trunk Group according to the figure above. To ensure correct routing of IP-to-Tel calls, assign a different Trunk Group ID for the digital trunk and the FXS module.

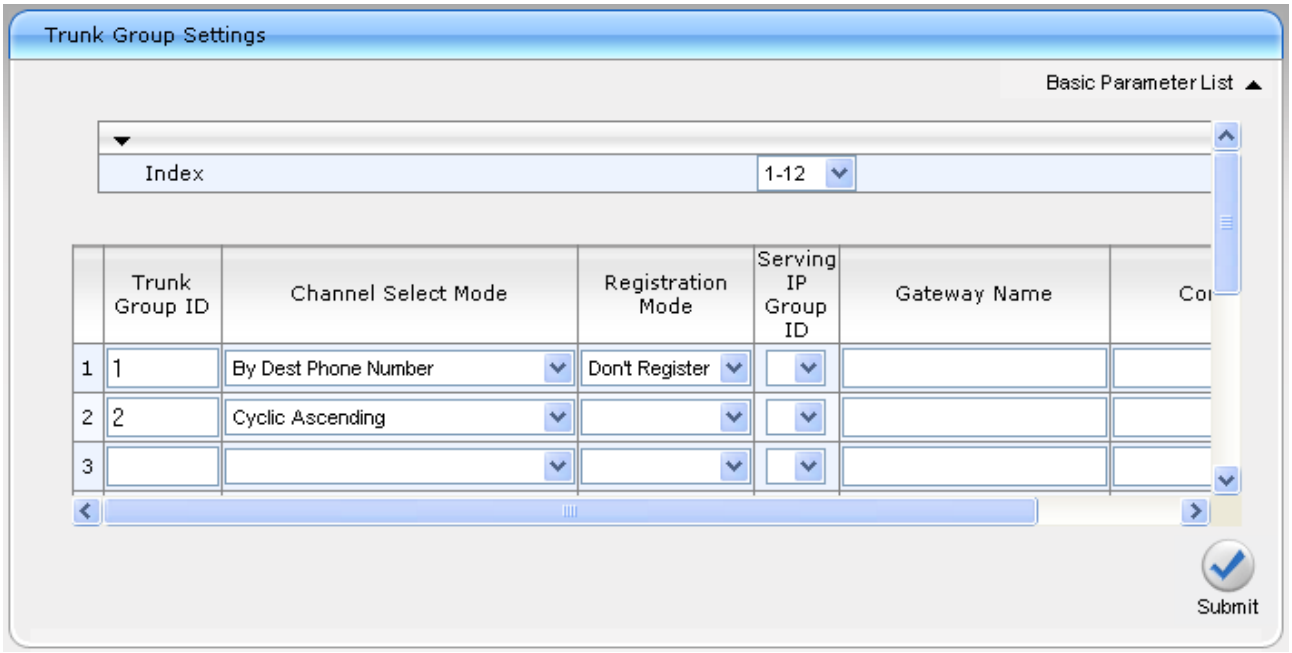
### 5.1.4 Step 4: Configure Trunk Group Settings Table

This step defines how to configure the method for which IP-to-Tel calls are assigned to channels within each Trunk Group. This is done in the 'Trunk Group Settings' page.

➢ **To configure the Trunk Group Settings table:**

1. Open the 'Trunk Group Settings' page (**Configuration** tab > **Protocol Configuration** menu > **Trunk Group** submenu > **Trunk Group Settings**).

**Figure 5-5: Trunk Group Setting Table Page**




2. Configure the Trunk Group according to the figure above:
   - The Channel Select Mode of the FXS port (Trunk Group ID 1) should be set to 'By Dest Phone Number'.
   - The Channel Select Mode of the digital trunk should be set to 'Cyclic Ascending'.

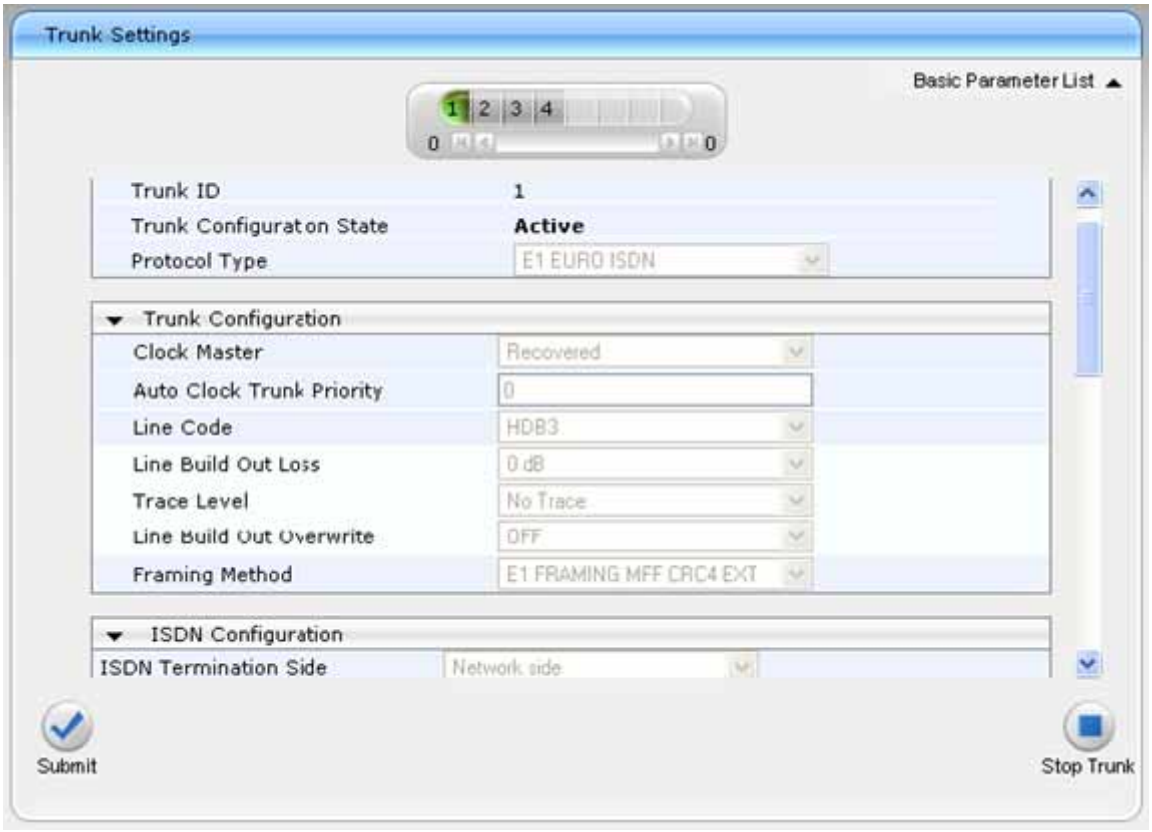
### 5.1.5 Step 5: Configure Trunk Settings

This step describes how to configure the PBX/PSTN Trunk that is connected to the Media Gateway.

➢ **To configure the Trunk Setting:**

1. Open the 'Trunk Settings' page (**PSTN Settings** menu > **Trunk Settings**).

**Figure 5-6: Trunk Setting Page**




2. Use the page above to configure the Trunk parameters according to your PBX/PSTN Trunk connection.

## 5.1.6 Step 6: Configure Secure Real-Time Transport Protocol (SRTP)

## 5.1.7 Step 6-a: Configure the Gateway for SRTP

To configure the Gateway for SRTP please refer to Section 4.5.

From the **Media Security Behavior** drop-down list, select:

- "Mandatory" - if Mediation Server is configured to SRTP Required
- "Preferable-Single media" - if Mediation Server is configured to SRTP Optional

## 5.1.8 Step 6-b: Configure IP Profile for Analog Device

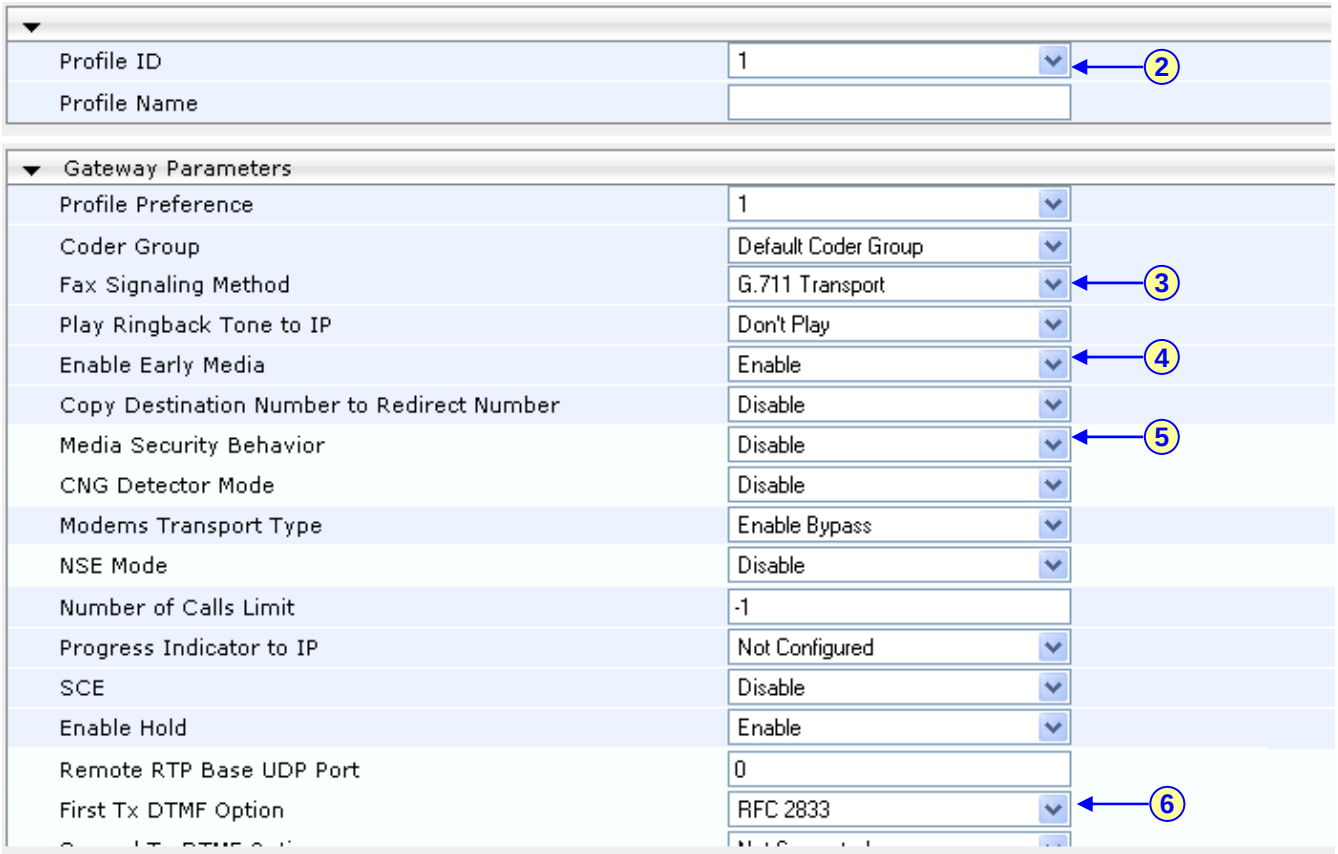
As described in the introduction to this section, the ATA's analog device uses the TCP/RTP transport type, while the Mediation server uses TLS/SRTP for security settings.

Therefore, you must configure an IP Profile for the analog device (which will disable the SRTP behavior in case the call should route to the ATA's device). This IP Profile will be used later in the Routing table.

➢ **To configure the IP Profile settings:**

1. Open the 'IP Profile Settings' page (**Configuration** tab > **Protocol Configuration** menu > **Coders And Profile Definition** submenu > **IP Profile Settings**).

**Figure 5-7: IP Group Table Page**




2. From the 'Profile ID' drop-down list, select '1' to indicate the number for the IP Profile.
3. From the 'Fax Signaling Method' drop-down list, select '*G.711 Transport*'
4. From the 'Enable Early Media' drop-down list, select '*Enable'*.
5. From the 'Media Security Behavior' drop-down list, select *'Disable'* if the Analog Device is configured to use RTP.
6. From the 'First Tx DTMF Option' drop-down list, select *'RFC 2833'*.

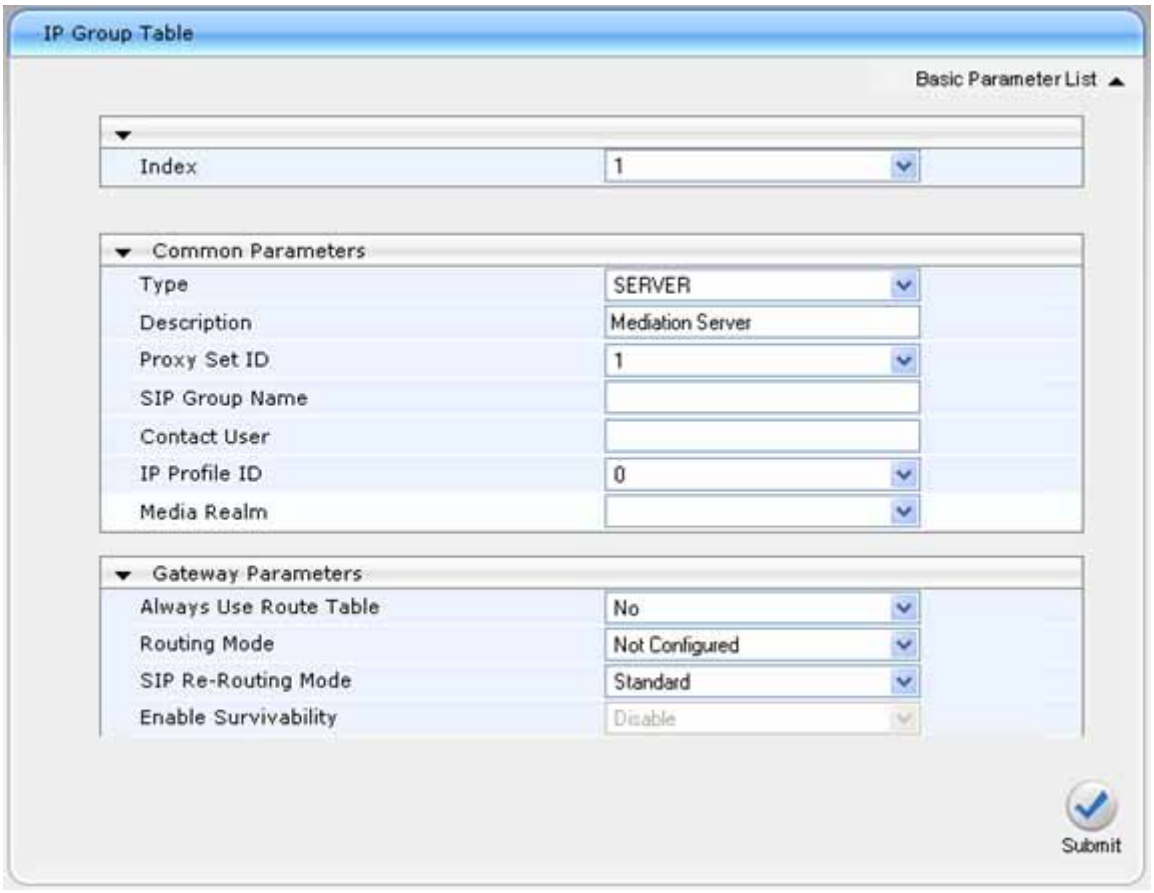
## 5.1.9 Step 7: Configure IP Group Table

The 'IP Group Table' page allows you to create up to nine logical IP entities called *IP Groups*. These IP Groups are used for call routing. This step describes how to configure the IP Group table for the Mediation Server.

➢ **To configure IP Groups:**

1. Open the 'IP Group Table' page (**Configuration** tab > **Protocol Configuration** menu > **Proxies/IpGroups/Registration** submenu > **IP Group Table).**

**Figure 5-8: IP Group Table Page**




2. Define IP Group #**1** for Mediation Server as follows:
   - **Index** = “1” - represent the ID for this IP Group.
   - **Type** = “SERVER” - used when the destination address (configured by the Proxy Set in Step 7, Section 5.1.10) of the IP Group is known.
   - **Description** = "Mediation Sever" - arbitrary name.
   - **Proxy Set ID** = “1” - represents the IP address (configured in Step 7, Section 5.1.10) for communicating with this IP Group.

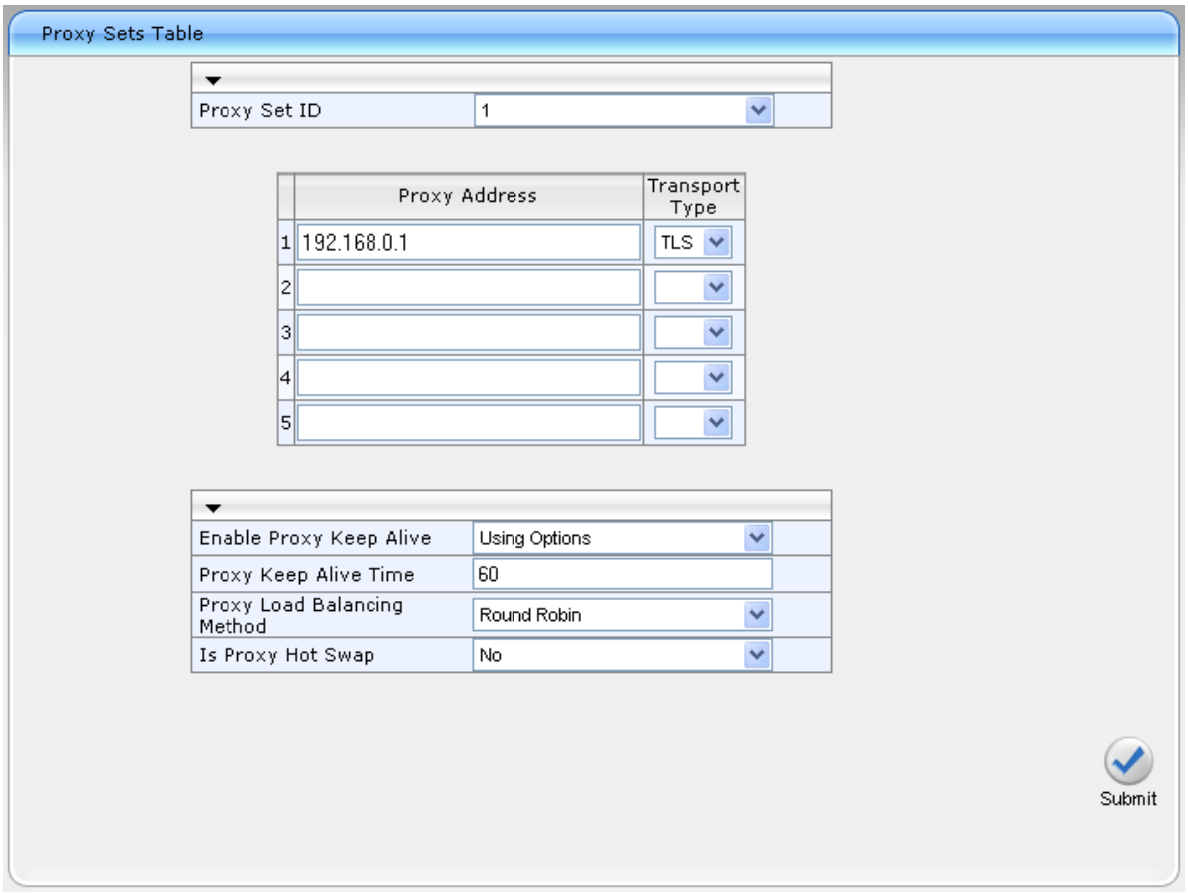
## 5.1.11 Step 8: Configure Proxy Set Table

This step describes how to configure the Proxy Sets. The Proxy Sets represent the IP addresses (or FQDN), required for communicating with the Mediation Server.

➢ **To configure the Proxy set:**

1. Open the 'Proxy Sets Table' page (**Configuration** tab > **Protocol Configuration** menu > **Proxies/IpGroups/Registration** submenu > **Proxy Sets Table**).

**Figure 5-9: Proxy Sets Table Page**




2. From the 'Proxy Set ID' drop-down list, select *'1'*.
3. In the 'Proxy Address' column, enter the IP address (or FQDN) of Mediation Server (192.168.0.1 in our example).
4. From the 'Transport Type' drop-down list corresponding to the IP address entered above, select *'TLS'*.

**Note:** If the SIP transport type for the link between the Enhance Gateway and Mediation Server is set to TLS, the Media Gateway must be configured with a certificate for authentication during the TLS handshake with Mediation Server. Refer to Section 4.3 for configuring TLS transport type including certification process to work with Mediation server.

5. From the 'Enable Proxy Keep Alive' drop-down list select *'Using Options'*. This parameter must be set to *'Using Options'* when Mediation server redundancy is used.
6. From the 'Proxy Load Balancing Method' drop-down list, select *'Round Robin'* to enable the Round Robin Proxy Load Balancing mechanism.

## 5.1.12 Step 9: Routing Setup

The Media Gateway's IP-to-IP call routing capabilities is performed in two stages:

1. **Inbound IP Routing:** Recognizes the received call as an IP-to-IP call or IP-to-Tel call based on the call's source IP address or/and Dest. Phone Prefix and /or the Source Phone Prefix. This stage is configured in the 'IP To Trunk Group Routing Table'.
2. **Outbound IP Routing:** Once recognized as an IP-to-IP call in the first stage (see above), the call is routed to the appropriate destination (i.e., IP address). This stage is configured in the 'Tel to IP Routing Table'.

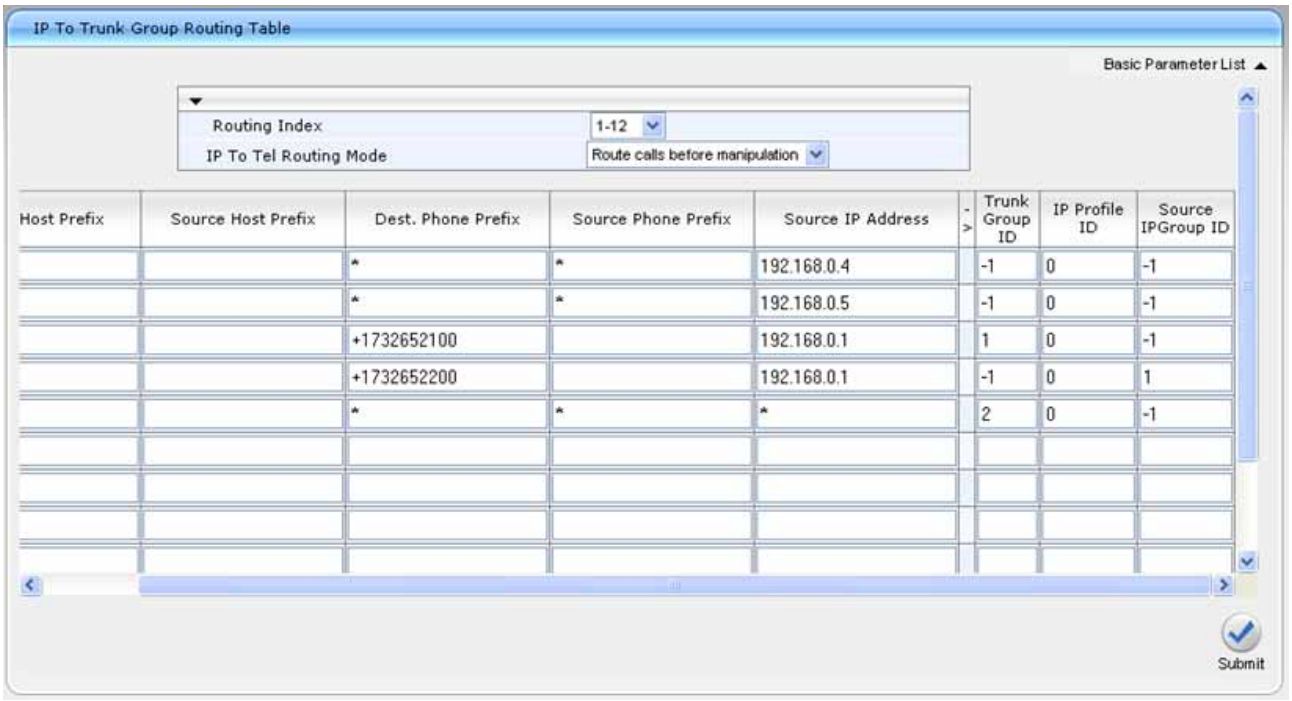
## 5.1.13 Step 9-a: Configure Inbound IP Routing

This step defines how to configure the Media Gateway's IP to Trunk Group Routing Table.

➢ **To configure Inbound Routing:**

1. Open the 'IP to Trunk Group Routing' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **IP to Trunk Group Routing**).

**Figure 5-10: IP to Trunk Group Routing Page**




2. Configure the following routing rules:
   - **Row 1** – calls from source IP address 192.168.0.4 (i.e., ATA 1) are assigned to Trunk Group ID '-1', identifying them as inbound IP-to-IP calls. These calls are later routed to the Mediation Server (Section 5.1.14).
   - **Row 2** - calls from source IP address 192.168.0.5 (i.e., ATA 2) are assigned to Trunk Group ID '-1', identifying them as inbound IP-to-IP calls. These calls are later routed to the Mediation Server (Section 5.1.14).
   - **Row 3** – calls from IP address 192.168.0.1 (i.e. Mediation Server) and the destination number prefix is +1732652100 (i.e. one of the embedded Media Gateway FXS ports) are routed to Trunk Group ID 1 (configured in Section 5.1.3).
   - **Row 4** – calls from IP address 192.168.0.1 (i.e. Mediation Server) and the destination number prefix is +1732652200 (i.e. one external ATA devices) are assigned to Trunk Group ID '-1', identifying them as inbound IP-to-IP calls. These calls are also assigned to the IP Group pertaining to Mediation Server (configured in Section 5.1.9).
   - **Row 5** – all other calls (that do not match any of the above rules) are routed to Trunk Group ID 2 (i.e., the PSTN).

## 5.1.14 Step 9-b: Configure Outbound IP Routing

This step defines how to configure the Media Gateway's Tel to IP Routing Table.

➢ **To configure Outbound IP Routing:**

1. Open the 'Tel to IP Routing Table' page (**Configuration** tab > **Protocol Configuration** menu > **Routing Tables** submenu > **Tel to IP Routing**).

**Figure 5-11: Tel to IP Routing page**

| | Src. IPGroupID | Src. Host Prefix | Dest Host Prefix | Src. Trunk Group ID | Dest. Phone Prefix | Source Phone Prefix | -> | Dest. IP Address | Port | Transport Type | Dest. IPGroup ID | IP Profile ID |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | | | * | 17326522000 | * | | 192.168.0.4 | | TCP | | 1 |
| 2 | 1 | | | * | 17326522001 | * | | 192.168.0.5 | | TCP | | 1 |
| 3 | | | | * | * | * | | | | TLS | 1 | 0 |
| 4 | | | | | | | | | | Not Configured | | 0 |
| 5 | | | | | | | | | | Not Configured | | 0 |
| 6 | | | | | | | | | | Not Configured | | 0 |
| 7 | | | | | | | | | | Not Configured | | 0 |
| 8 | | | | | | | | | | Not Configured | | |
| 9 | | | | | | | | | | Not Configured | | |
| 10 | | | | | | | | | | Not Configured | | |

2. Configure the following routing rules:
   - **Row Index 1** – calls from source IP Group 1 (i.e. Mediation Server) and the destination phone number is +17326522000 are routed to IP address 192.168.0.4 (i.e. ATA 1), using 'TCP' transport type and IP Profile ID '1'.
   - **Row Index 2** - calls from source IP Group 1 (i.e. Mediation Server) and the destination phone number is +17326522001 are routed to IP address 192.168.0.5 (i.e. ATA 2), using 'TCP' transport type and IP Profile ID '1'.
   - **Row Index 3** – all other calls (that do not match the rules above), meaning calls from PSTN (Tel-to-IP calls), ATA's (IP-to-IP calls) and embedded Media Gateway FXS port (Tel–to-IP calls) are routed to destination IP Group 1 (i.e. Mediation Server), using 'TLS' transport type.

**Note:** To ensure security, Gateways must honor or send requests from/to the Mediation Server only if the Mediation Server is in an administrative list. The list should appear in the 'Tel to IP Routing' Table, Please refer to Section 4.1, Steps 1212 ,13 and 14 in order to add the list of the trusted Mediation Servers IP address to this table.

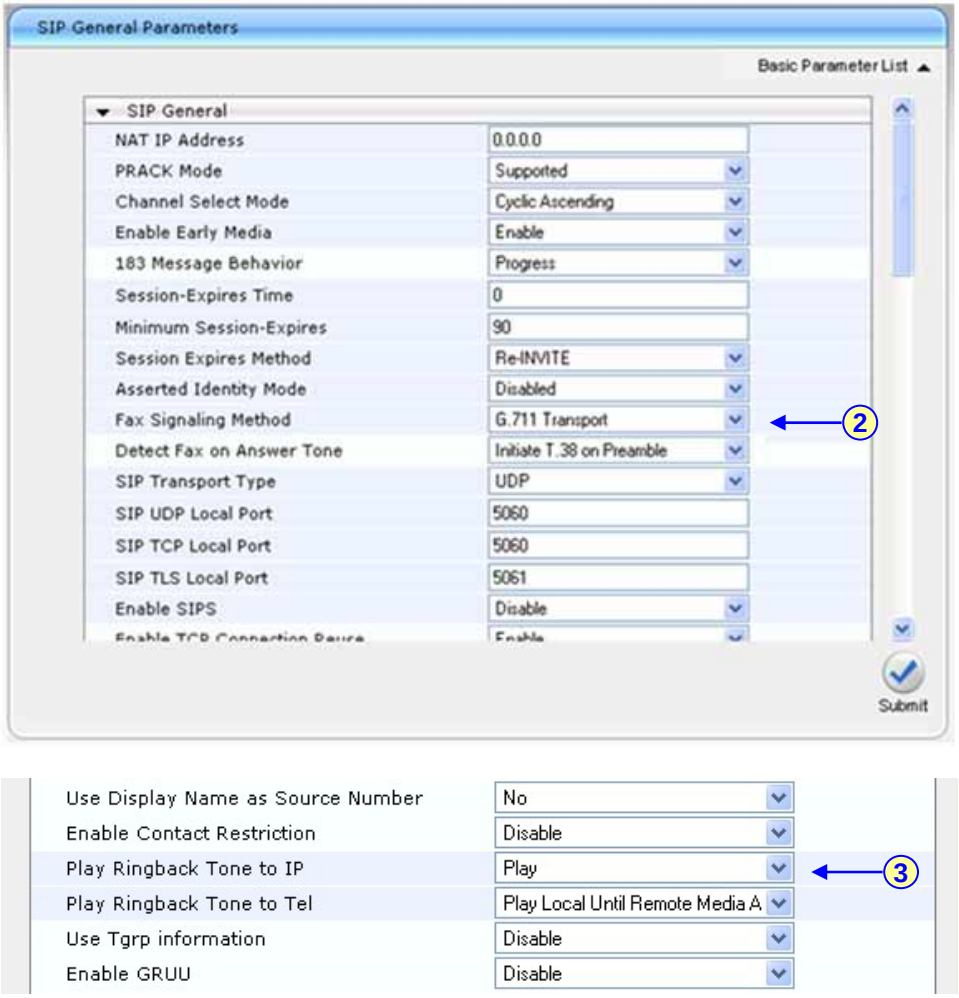
## 5.1.15 Step 10: Configure Fax Signaling Method

This step defines how to configure the Fax Signaling Method to G.711 Transport for the calls between the Media Gateway and the analog devices (ATA's and embedded Media Gateway FXS ports).

➢ **To configure the Fax Signaling Method parameters:**

1. Open the 'SIP General Parameters' page (**Configuration** tab > **Protocol Configuration** menu > **Protocol Definition** submenu > **SIP General Parameters**).

**Figure 5-12: SIP General Parameters Page**




2. From the **FAX Signaling Method** drop-down list, select *'G.711 Transport'*.
3. From **Play Ringback Tone to IP** drop-down list, select *'Play'* to provide a ringback tone to the analog device in case it transferred to another IP user.

## 5.1.16 Step 11: Configure General Parameters

Configure general parameters as described in the following sections:

- Section 4.6, Defining E1/T1/BRI Trunk Settings
- Section 4.7, Defining Voice Coder
- Section 4.8, Define Silence Suppression, Comfort Noise and AGC
- Section 4.9, Defining Early Media

# 5.2 Analog Devices (ATA's) Configuration

This section defines how to configure the analog device entity to route its calls to AudioCodes Media Gateway. The analog device entity must be configured to send all calls to Media Gateway without undergoing any registration process.

Assuming the ATA devices are AudioCodes MP-11x series, the following configurations should be made:

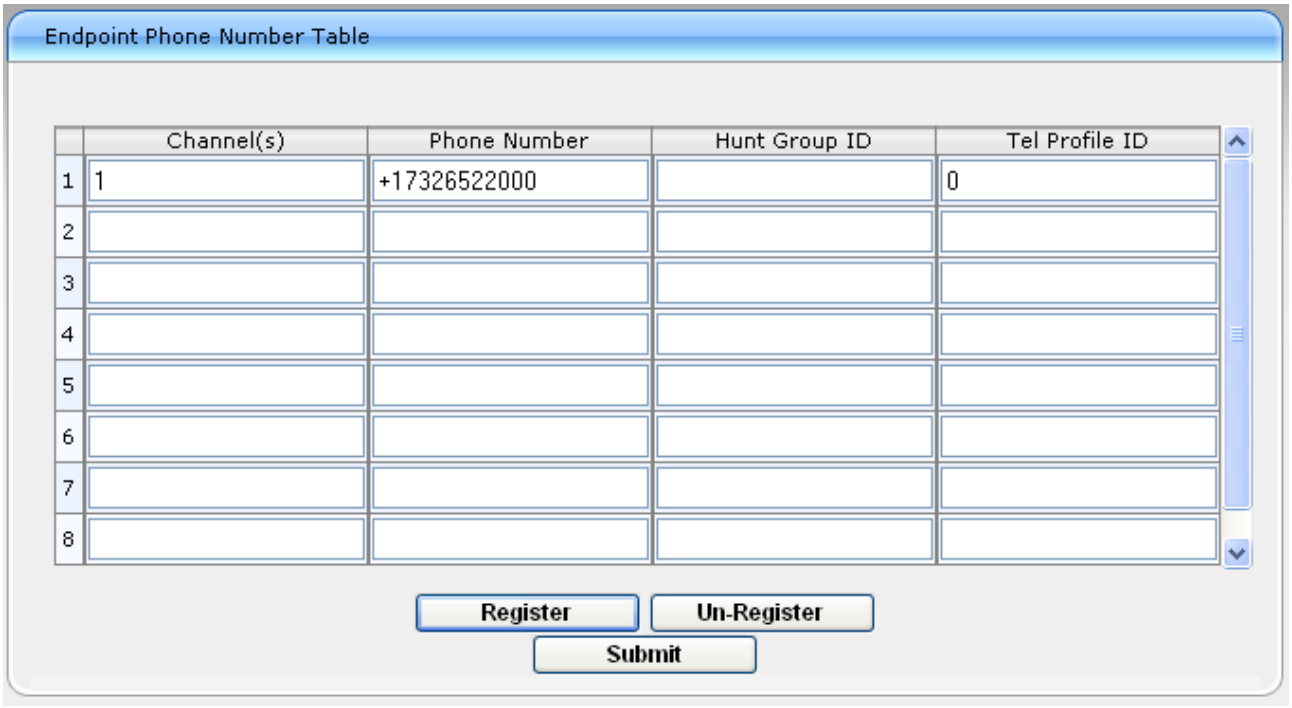
## 5.2.1 Step 1: Configure the Endpoint Phone Number Table

The 'Endpoint Phone Number Table' page allows you to activate the MP-11x ports (endpoints), by defining telephone numbers. The configuration below uses the example of ATA1 destination phone number +17326522000 (IP address 192.168.0.4).

➢ **To configure the Endpoint Phone Number table:**

- Open the 'Endpoint Phone Number Table' page (**Configuration** tab > **Protocol Configuration** menu > **Endpoint Number** submenu > **Endpoint Phone Number**).

**Figure 5-13: Endpoint Phone Number Table Page**



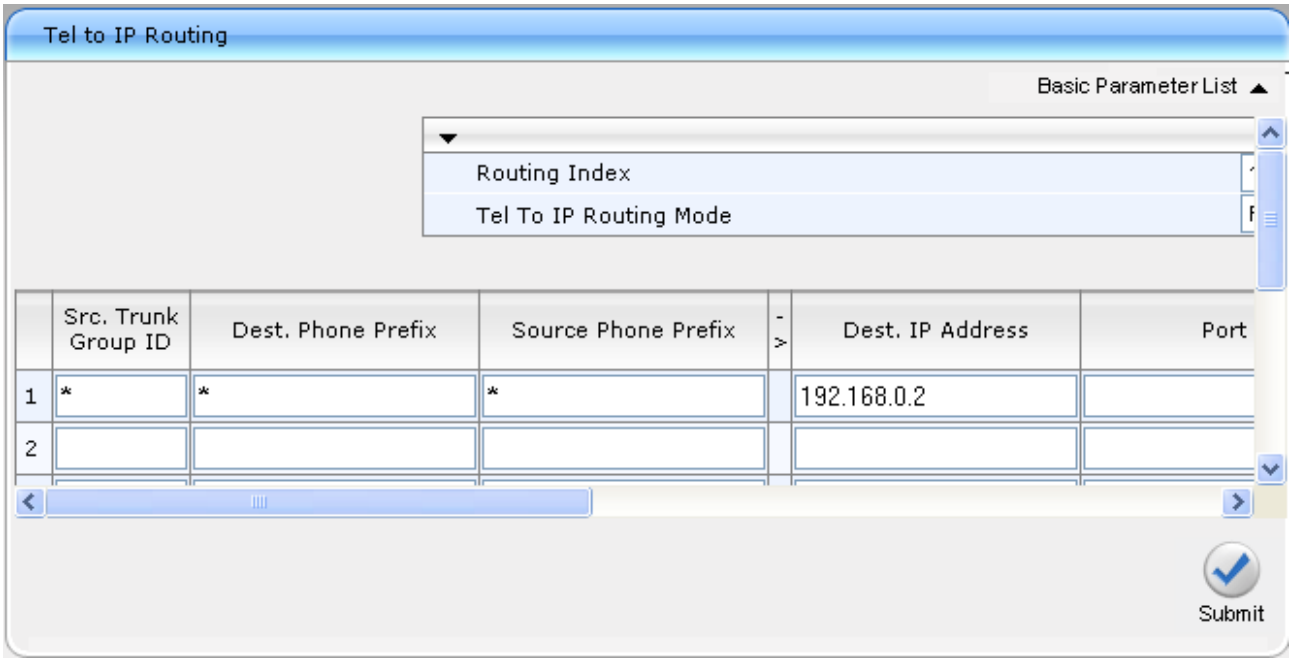
### 5.2.2 Step 2: Configure Tel to IP Routing Table

This step describes how to configure the Tel-to-IP routing rules to ensure that the MP-11x sends all calls to AudioCodes central Media Gateway.

➢ **To configure the Tel to IP Routing table:**

- Open the 'Tel to IP Routing' page (**Configuration** tab > **Protocol Configuration** menu> **Routing Tables** submenu > **Tel to IP Routing**).

**Figure 5-14: Tel to IP Routing Page**



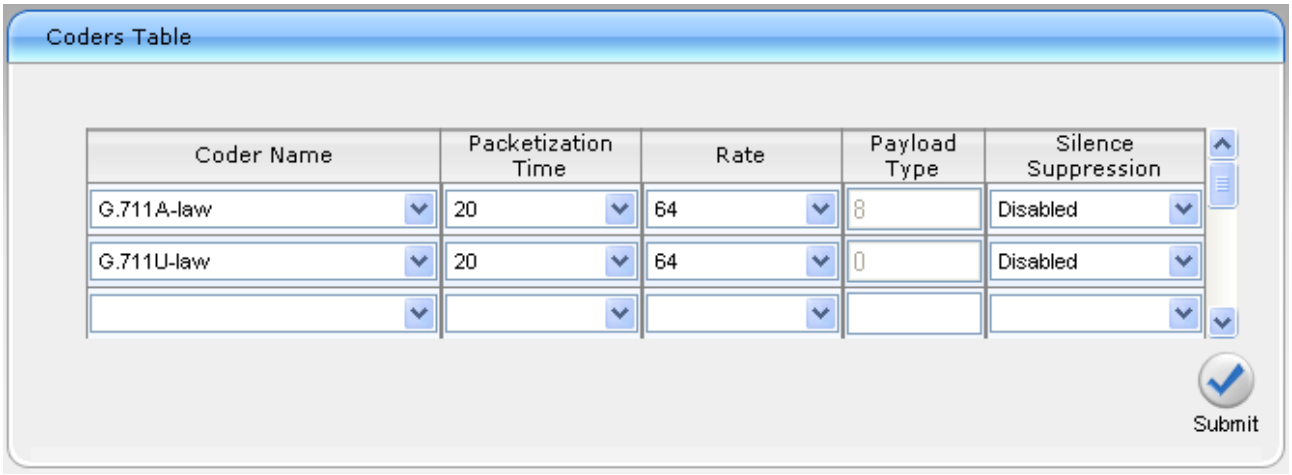

### 5.2.3 Step 3: Configure Coders Table

This step describes how to configure the coders for MP-11x.

➢ **To configure MP-11x coders:**

- Open the 'Coders' page (**Configuration** tab > **Protocol Configuration** menu > **Coders And Profile Definition** submenu > **Coders**).

**Figure 5-15: Coders Table Page**



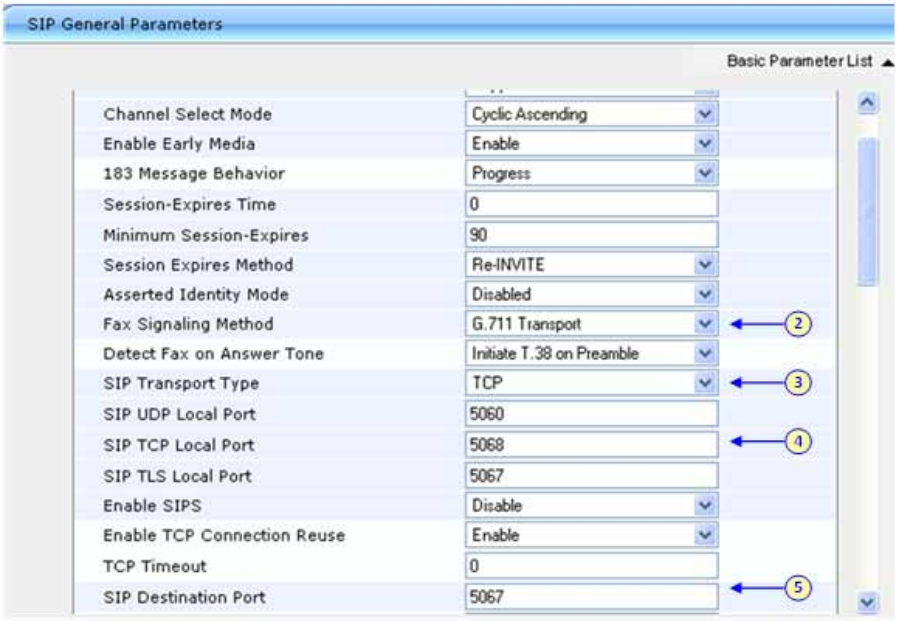
### 5.2.4 Step 4: Configure SIP TCP Transport Type and Fax Signaling Method

This step describes how to configure the fax signaling method for MP-11x.

➢ **To configure the fax signaling method:**

1. Open the 'SIP General Parameters' page (**Configuration** tab > **Protocol Configuration** menu > **Protocol Definition** submenu > **SIP General Parameters**).

**Figure 5-16: SIP General Parameters Page**




2. From the 'FAX Signaling Method' drop-down list, select *'G.711 Transport'*.
3. From the 'SIP Transport Type' drop-down list, select *'TCP'.*
4. In the 'SIP TCP Local Port' field, enter *'5068'* (corresponding to the Central Gateway TLS transmitting port configuration).
5. In the 'SIP Destination Port', enter *'5067'* (corresponding to the Central Gateway TLS listening port configuration).

# 6 Configuring Survivable Branch Appliance

As described in the Introduction (refer to Section 1), the Survivable Branch Appliance (SBA) application solution, hosted by AudioCodes' SBA Media Gateway is deployed at the branch office and provides basic voice services to branch users during a WAN outage.

The SBA application is installed on the SBA Media Gateways as follows:

- Mediant 1000 and Mediant 1000 MSBG on the OSN server
- Mediant 2000: on the SBC blade

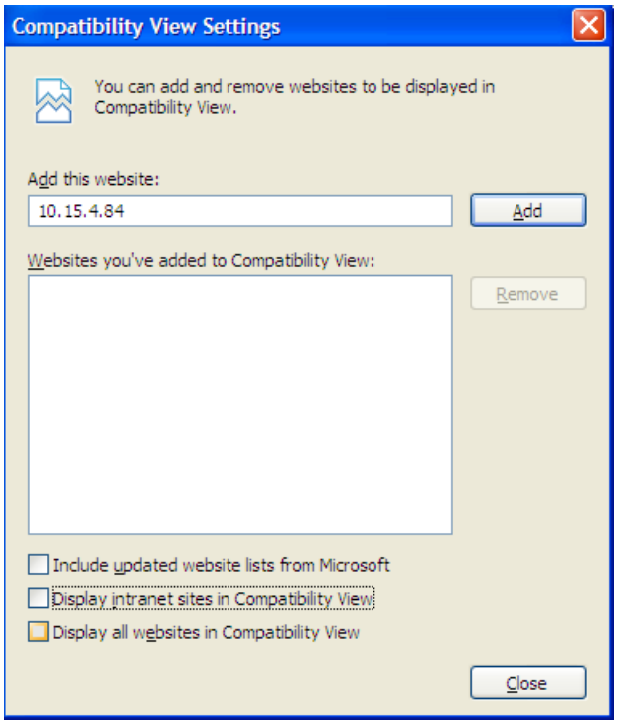
These hosting platforms are pre-installed with Microsoft Windows Server 2008 R2.

**Notes:** Before configuring the SBA, you must perform the following steps, which are detailed in Section 6.1. These steps contain the following:

- Adding the SBA Device to the Active Directory
- Creating a user account on the Active Directory belonging to the *RTCUniversalSBATechnicians* group. This user will perform the SBA deployment (Domain Admin account can perform SBA deployment too by default).
- Adding the SBA Device to your topology
- To establish CS test calls from the SBA GUI, you will need to define special accounts on the OCS.
- The SBA GUI only works with Internet Explorer 8 (Compatibility disabled), Firefox and Google Chrome.
- Internet Explorer 8 compatibility can be disabled by selecting **Tools** > **Compatibility View Settings** (see below):
  - **"Display all websites in Compatibility View"** must be unchecked.

    The SBA GUI server must not appear on the list of **"Websites you've added to Compatibility View"**.

**Figure 6-1: Compatibility View Settings**



# 6.1 Preparation

This sub-section was written for the RC version. For the Beta Refresh version, the dialogs are different but the process is similar.

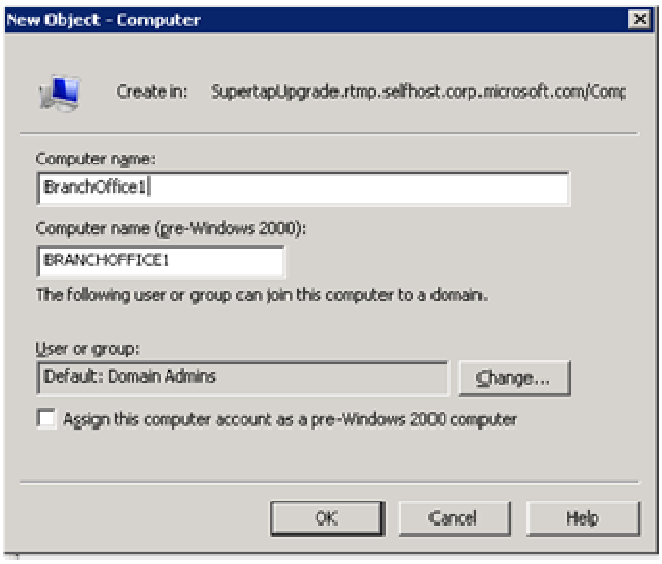
## 6.1.1 Datacenter Workflow

The steps in this sub-section must be performed at the datacenter.

### 6.1.1.1 Adding the Survivable Branch Appliance Device to Active Directory

1. Add the planned Survivable Branch Appliance device name to the Active Directory Domain Services.
   a. Add the Survivable Branch Appliance device name to the domain computers.

**Figure 6-2: New Object - Computer**




   b. In New Object - Computer, click **Change** to add a user or group that can add this specific device to the domain. The branch site technician will need to perform this step in the branch site at a later stage.

   c. Specify the name of a user or group that is allowed to join this computer to the domain.

   d. Open up ADSI Edit. Open up the properties for the Survivable Branch Appliance, and then set **servicePrincipalName** to be "HOST/<SBA FQDN>" where <SBA FQDN> is the FQDN of your Survivable Branch Appliance.

   e. Add the Survivable Branch Appliance computer object to the **RTCUniversalReadOnlyAdmins** group.
2. Create a user account on Active Directory Services belonging to the *RTCUniversalSBATechnicians* group. This user will perform the Survivable Branch Appliance deployment.

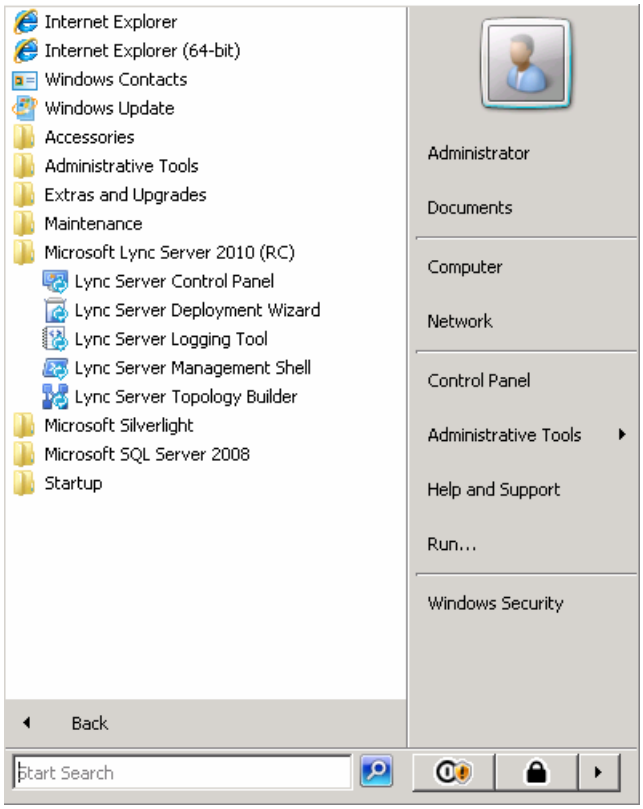
### 6.1.1.2 Defining the Branch Office Topology Through Topology Builder

This sub-section explains how to add the Survivable Branch Appliance to your topology using Topology Builder, and publish the topology.

➢ **To create branch sites:**

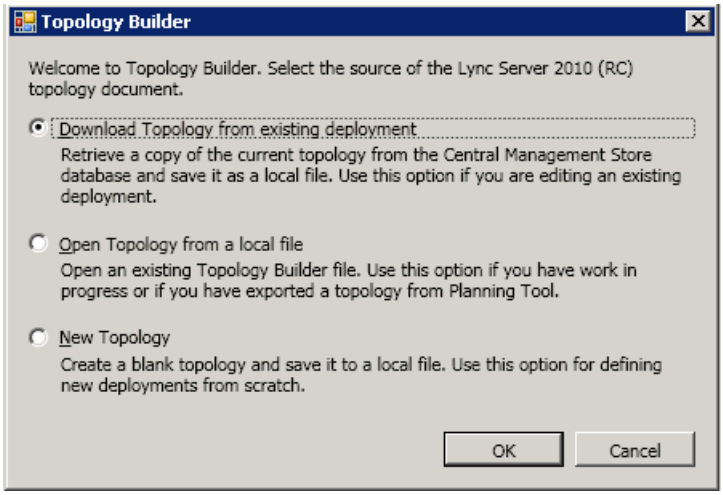
1. Open the Topology Builder: Click **Start** > **All** Programs > **Microsoft Lync Server 2010 (RC)**, and then click **Lync Server Topology Builder**.

**Figure 6-3: Topology Builder Menu**



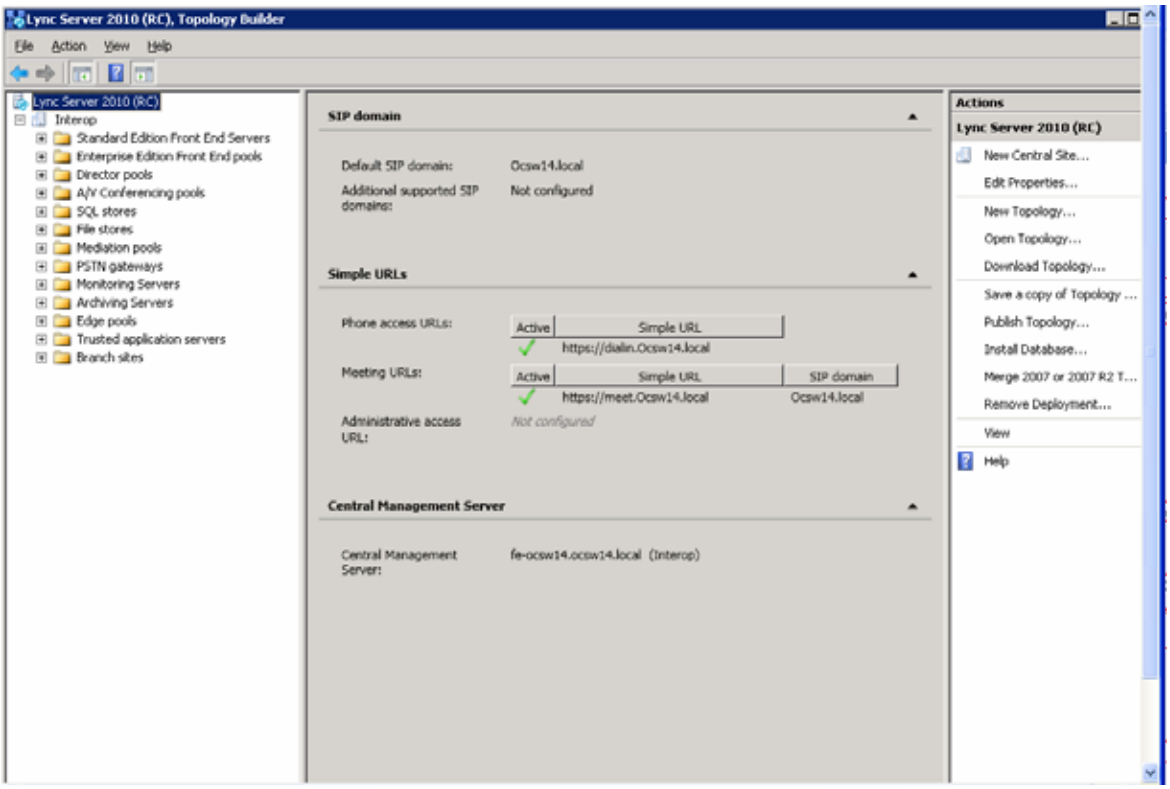

2. On the screen below, select **Download Topology from existing deployment** (assuming your Lync Server deployment already has a topology); a dialog to save the existing topology will open. Select a filename for the topology.

**Figure 6-4: Topology Builder**



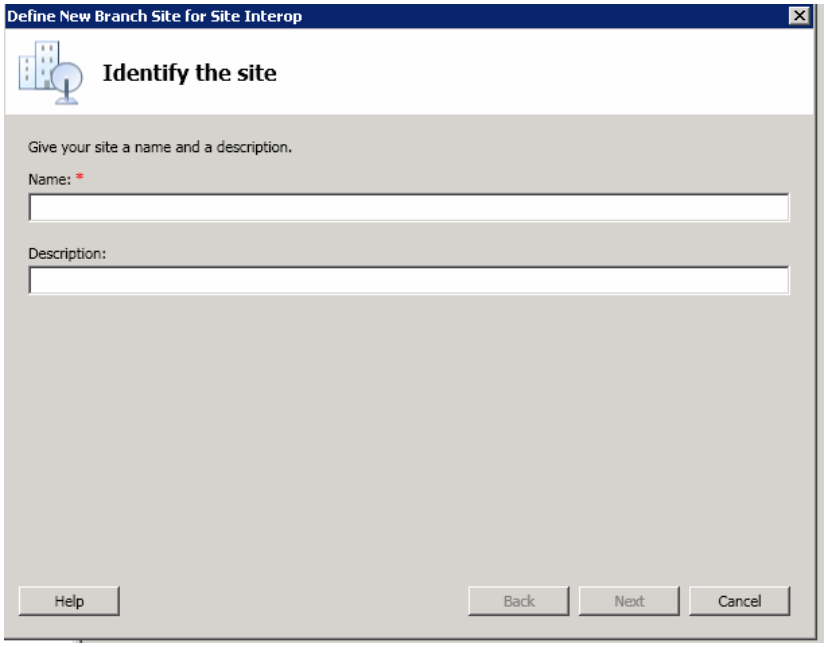
3. From the console tree, do one of the following:
   - If you used the planning tool to design your Enterprise Voice topology, expand the **Branch Office Sites** node, and then expand the name of the branch site you specified in the tool. By right- clicking, you can select the edit option for every section of the branch office.
   - If you did not use the planning tool, right-click the **Branch Office Sites** node, and then click **Define Branch Site**. Continue to the next step.

**Figure 6-5: Lync Server 2010 Topology Builder**




4. In the dialog box, do the following:
   - Click **Name**, and then type the name of the branch site. Only this field is Required, the other fields are optional.
   - Click **Description**, and then type a meaningful description for the branch site.
   - Click **Next**.

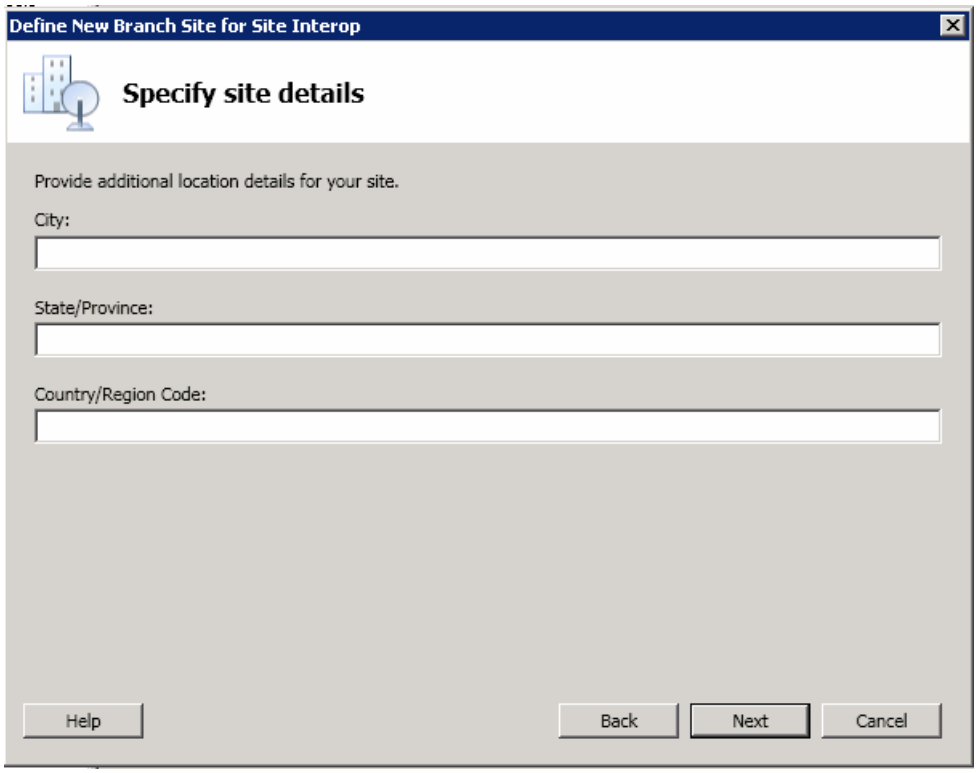
**Figure 6-6: Lync Server 2010 Topology Builder**




**5.** In the following dialog box, do the following:

- Click **City**, and then type the name of the city in which the branch site is located.
- Click **State/Province**, and then type the name of the state or region in which the branch site is located.
- Click **Country/Region Code**, and then type the two-digit calling code for the country in which the branch site is located.
- Click **Next**.

**Figure 6-7: Specify Site Details**



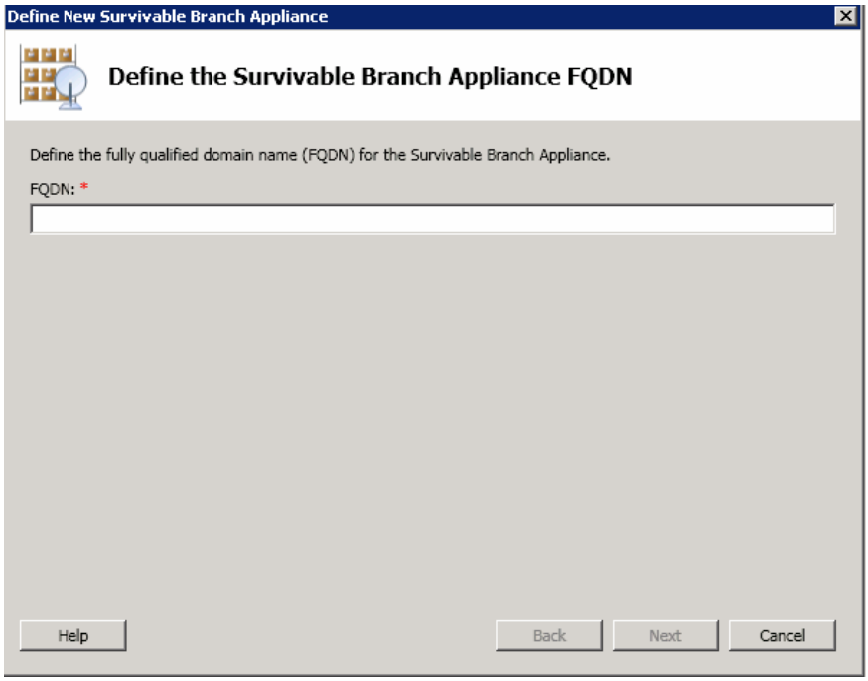
6. Check the "**Open the New Survivable Branch Appliance Wizard when this wizard is closes**" check-box and click **Finish**.

**Figure 6-8: Define New Branch Site for Site Interop**


7. Click **FQDN,** and then type the SBA FQDN.

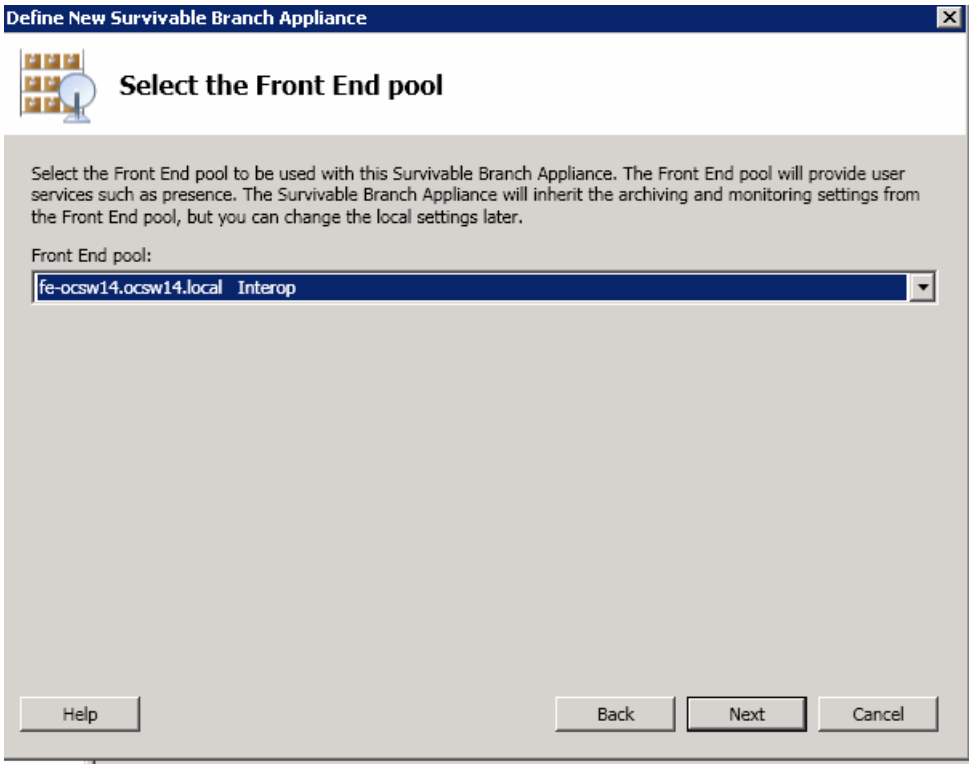
**Note:** If this is a Survivable Branch Appliance, the name you enter in the System FQDN must be the same FQDN as the Survivable Branch Appliance FQDN you entered using ADSI edit above.

**Figure 6-9: Define SBA FQDN**



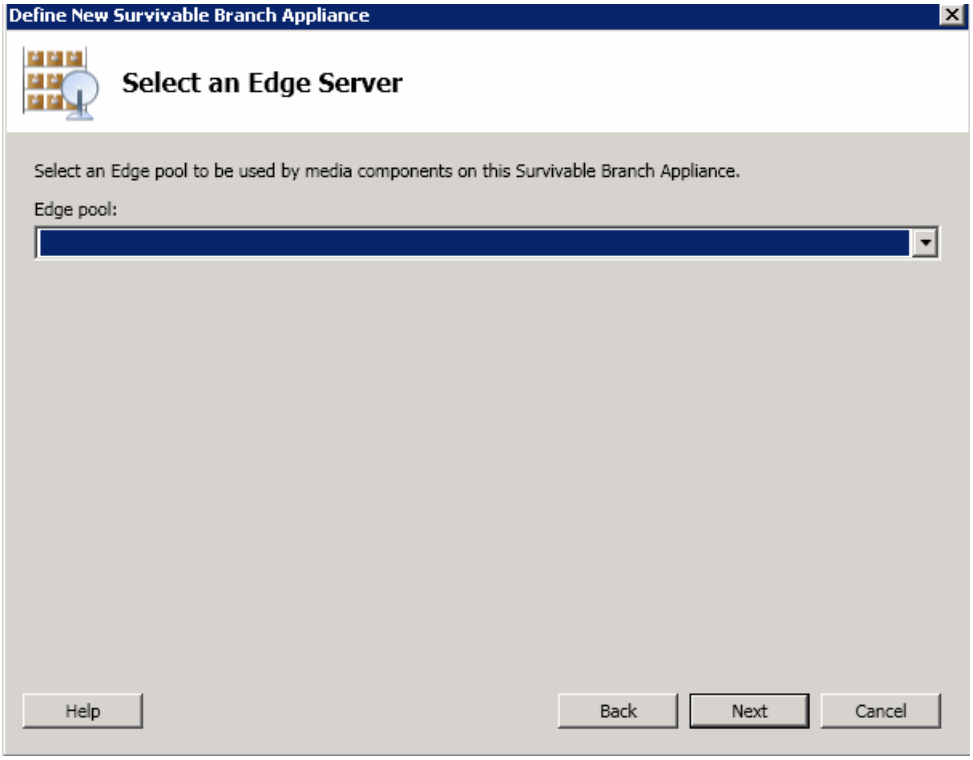
8. Select the **Front End Pool** to be used with this SBA.

**Figure 6-10: Front End Pool**




9. Select the **Edge Pool** to be used with this SBA (optional).

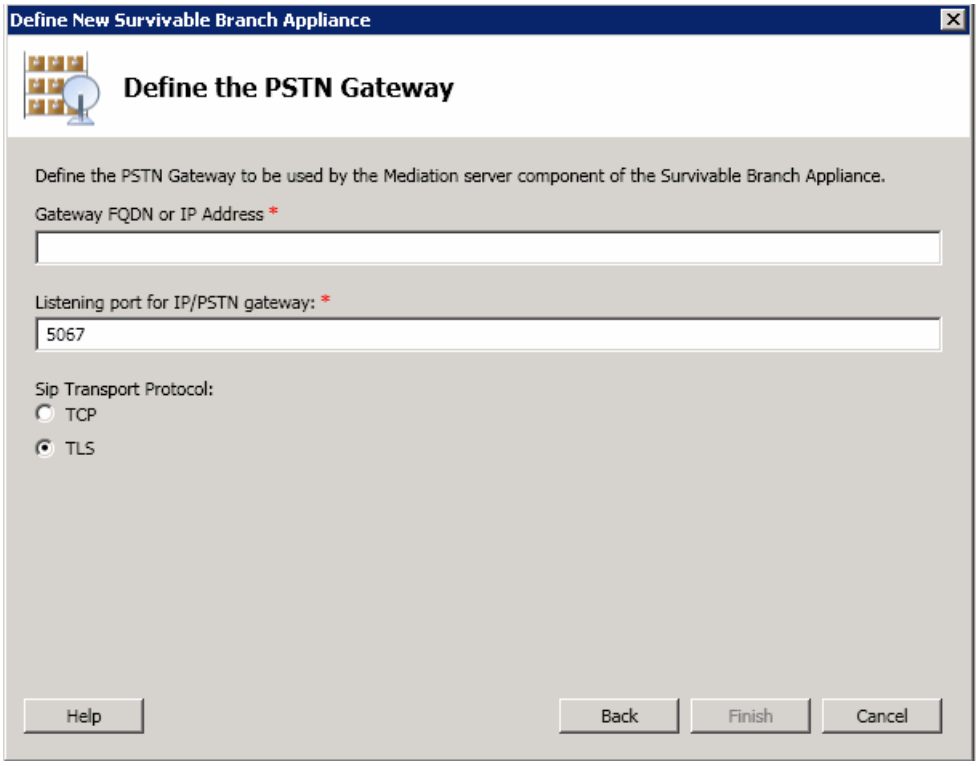
**Figure 6-11: Edge Pool**




10. Do the following:
    - Click **Gateway FQDN op IP Address**, and then type the Gateway FQDN or IP to be used by the Mediation Server component of the SBA.
    - Click **Listening port for IP/PSTN Gateway**, and type the Gateway listening port.
    - Select the **SIP Transport Protocol**.

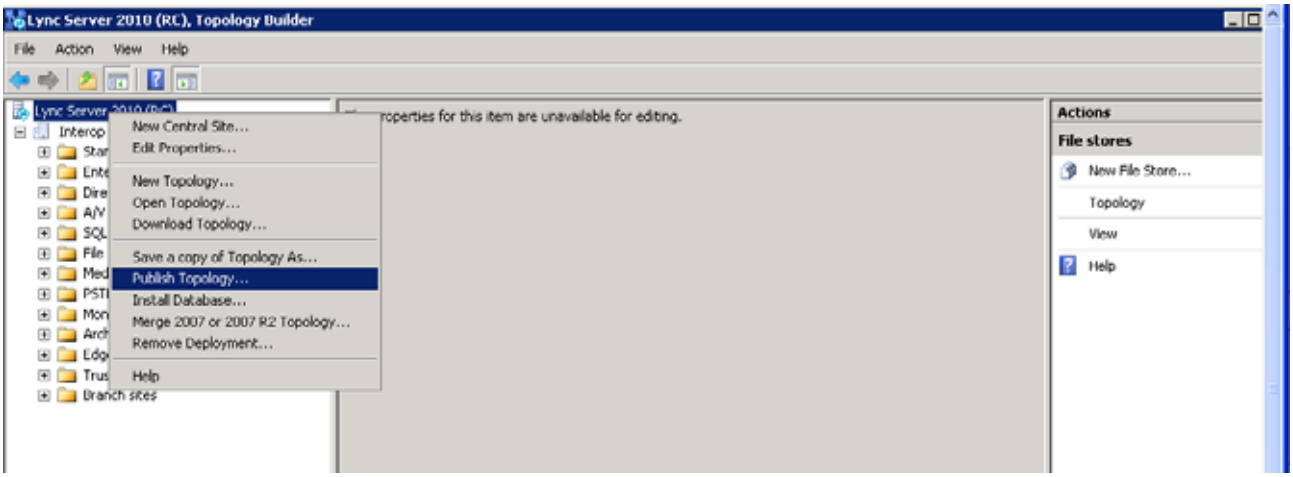
11. For security reasons, we strongly recommend that if you deploy a Survivable Branch Appliance, that you use TLS.

**Figure 6-12: Define the PSTN Gateway**



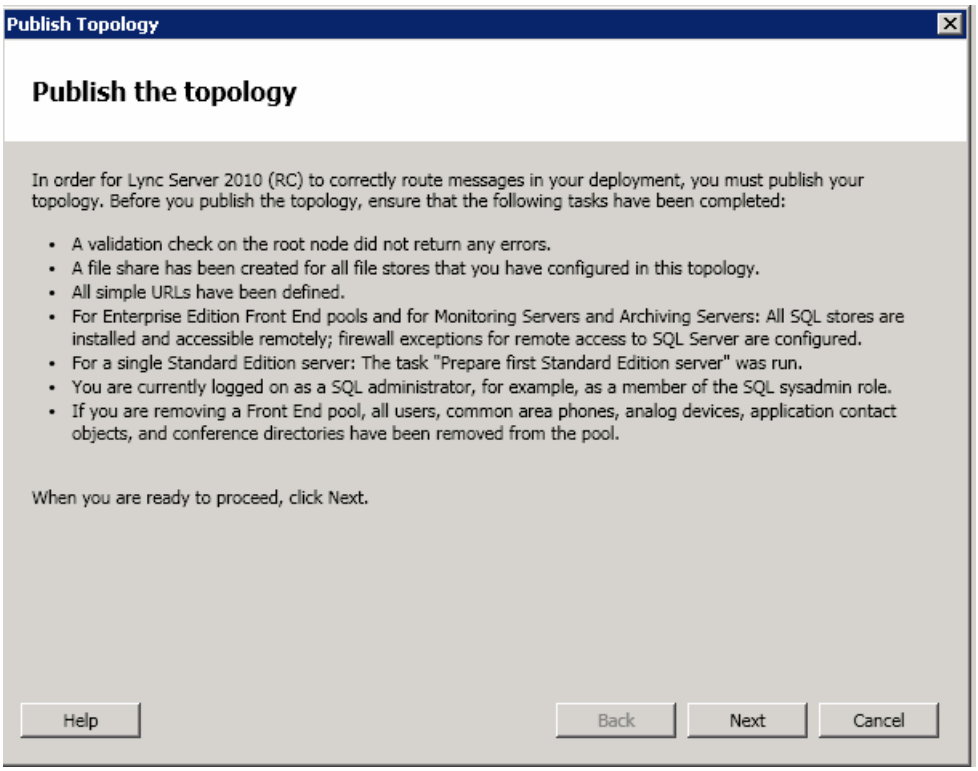

12. Click **Finish**.
13. Publish the new topology by right-clicking on the root of the **Lync Server 2010 (RC)** menu bar, and select the **Publish Topology** action.

**Figure 6-13: Publish Topology Selection**



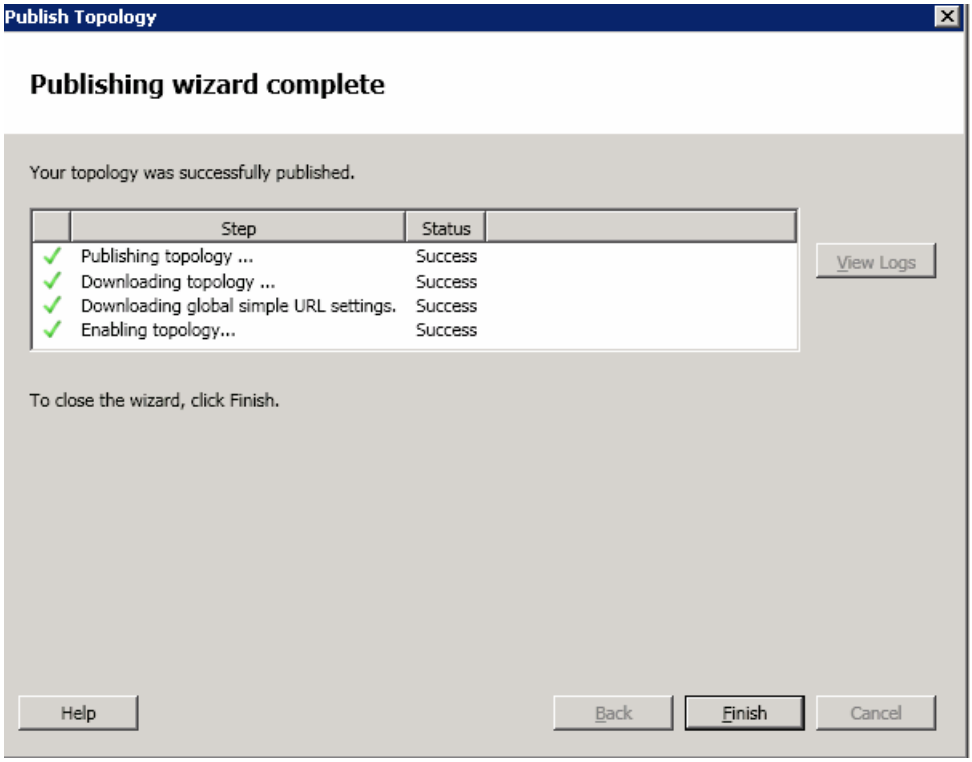
14. Click **Next**.

**Figure 6-14: Publish Topology – Confirm Tasks**




15. Confirm that all steps were succeeded, and click **Finish**.

**Figure 6-15: Publish Wizard Complete**



## 6.2 Installing and Configuring SBA

The following section describes the steps required to install and configure the SBA application.

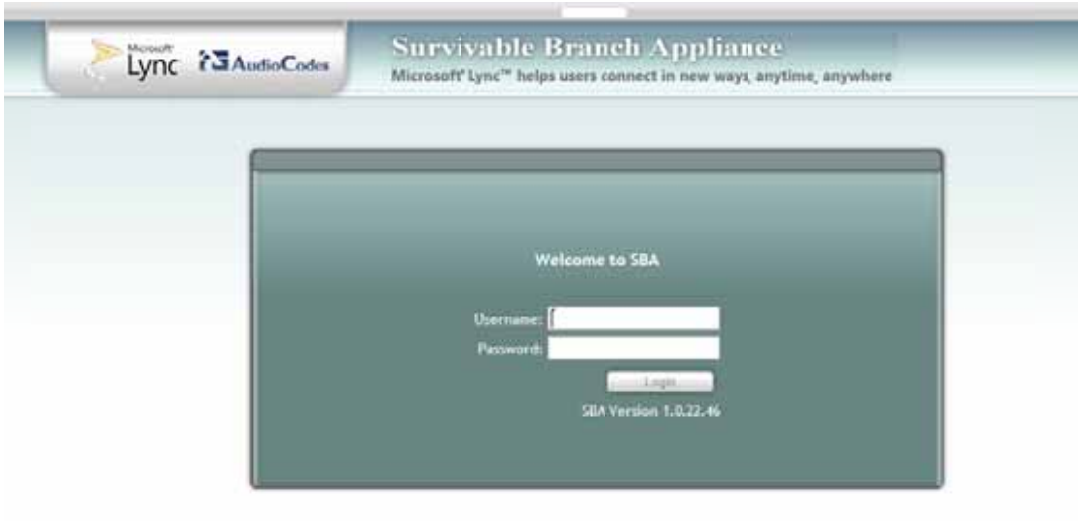
➢ **To install and configure SBA:**

1. Open your internet browser (Firefox, Chrome or Internet Explorer 8 and above is the preferred browser) with **http://10.1.10.12** to start the SBA application; the **Survivable Branch Application** login page appears.

**Notes:**

- Only when opening the **Login** page before the system is up will the **System is starting please wait** message appear. Refresh this page till this message disappears before logging in.
- In case the SBA was recovered or upgrade by using the AudioCodes recovery USB, the IP will be from the DHCP and not 10.1.10.12.

**Figure 6-16: Survivable Branch Appliance Page**




2. Enter the **Username** as 'Administrator' and **Password** as 'Pass123', and then click **Login**; the **Setup Menu** page appears.

**Note:** If the local Administrator password was changed via the Set Password menu, use the new password, instead of the default 'Pass123'.

**Figure 6-17: Setup Menu**


**Note:** Only a few Setup menu options are active when first entering the application.

## 6.2.1 Main Functions

The main functions of this application are included in the following menu tabs and are described below.

- Home
- Setup
- Tools
- Logs

**Notes:**

- For documentation, the **Setup** menu options are described first. **Home**, **Tools** and **Logs** are described later in this section.
- For the installation and configuration process to succeed, it is imperative that all **Setup** tasks are performed correctly, **in sequence**. If a task fails, ensure it is rectified, before continuing with additional tasks.

## 6.2.2 Setup

Perform the following steps in sequence to setup the SBA application.

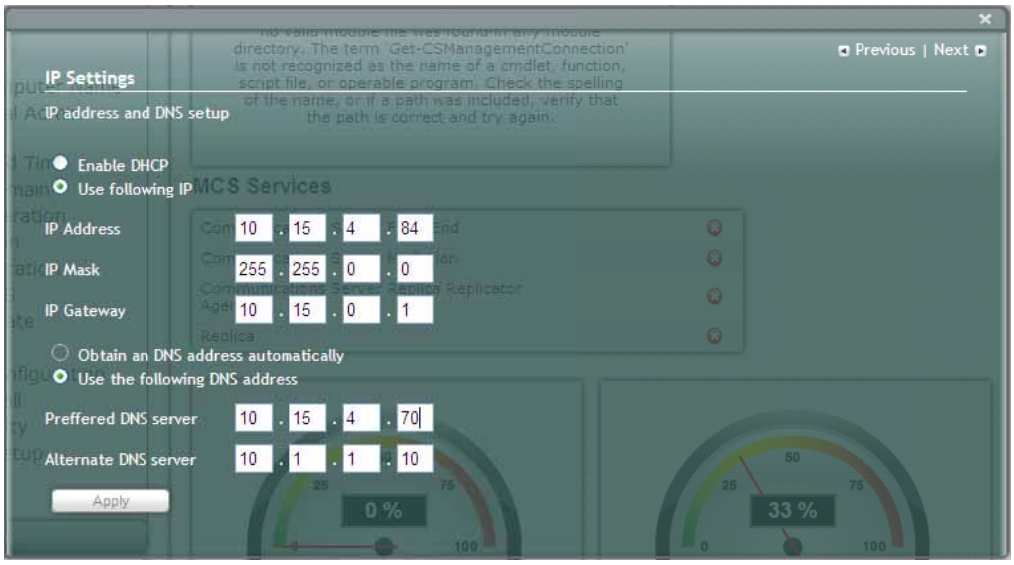
### 6.2.2.1 IP Settings

This menu option sets the IP address and DNS.

➢ **To set the IP address and DNS:**

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

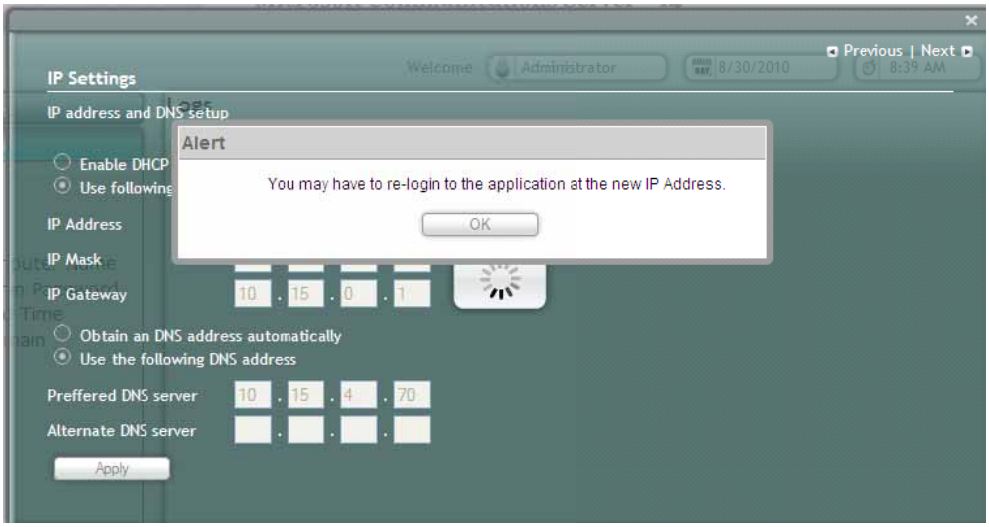
**Figure 6-18: Set IP Configuration Page**




2. Confirm the IP Address, IP Mask and IP Gateway fields and click **Apply**. If the IP address has changed, you will be required to login again.

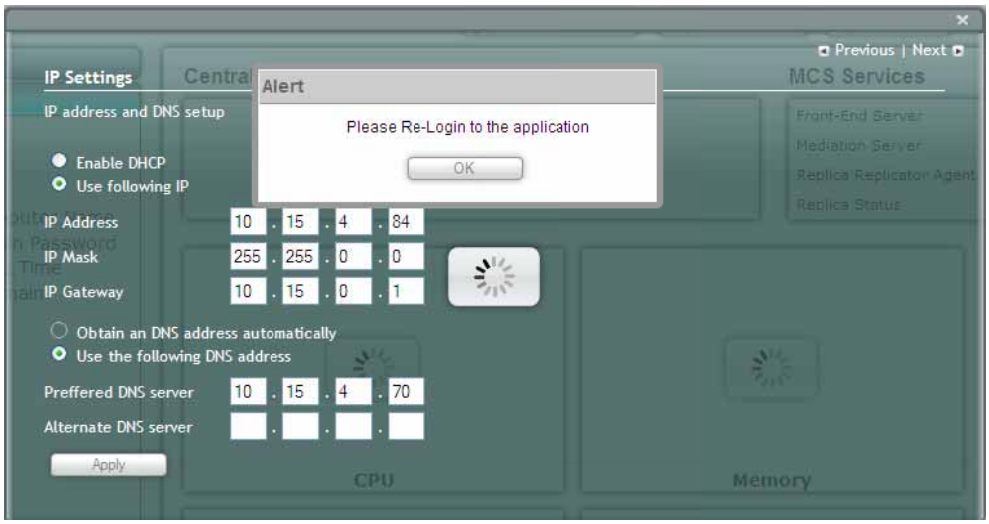
**Note:** For the Beta Refresh version, providing only one DNS server does not work. If you wish to provide only one, put the same server on the preferred and alternate DNS, or set only one via RDT..

**Figure 6-19: IP Settings – Login Again**




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

**Figure 6-20: Alert - Login**

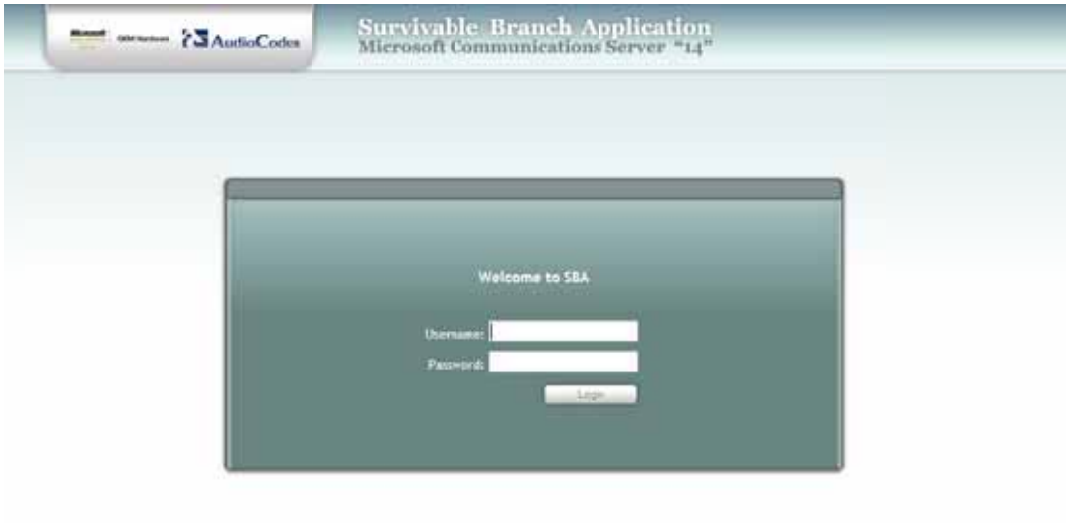



**4.** Click **OK**.

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

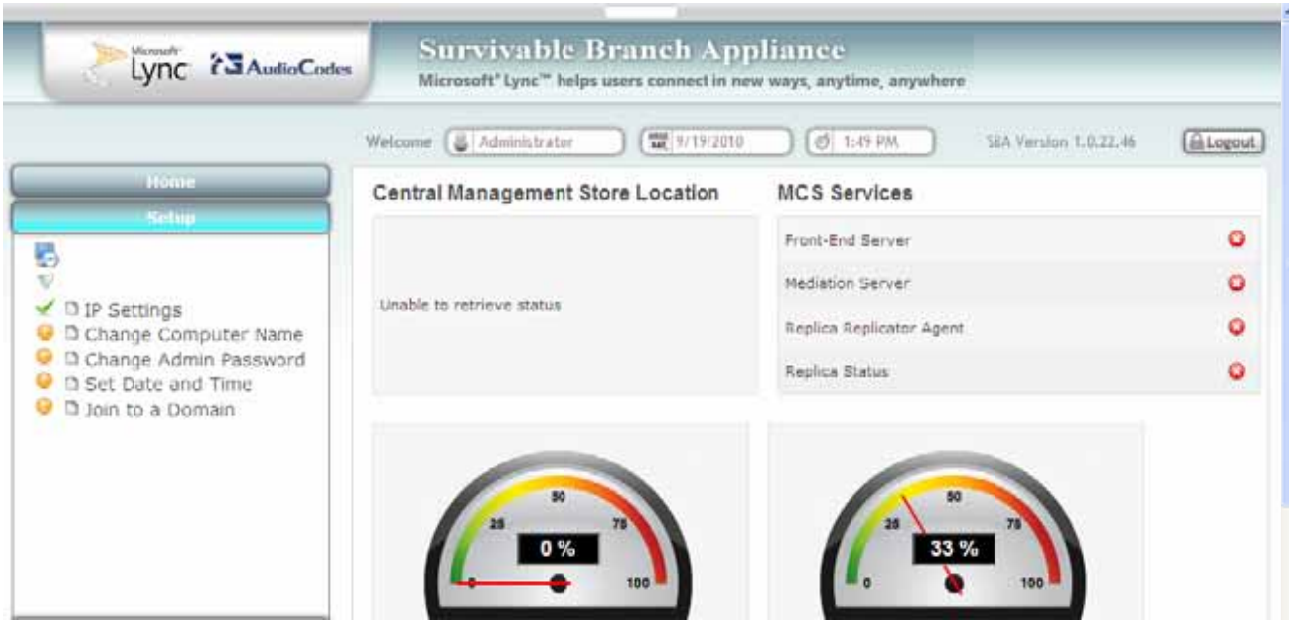
**Note:** The system logs in with the new IP address.

**Figure 6-21: Login Screen**




**Note:** As each menu item has been completed, a green check mark appears by the item.

**Figure 6-22: IP Settings - Complete**



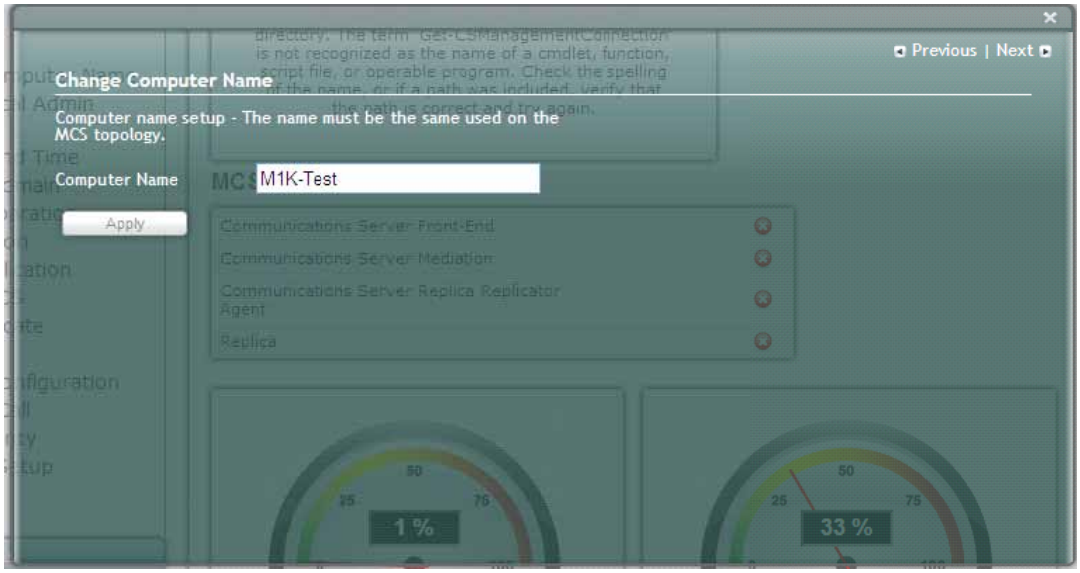
### 6.2.2.2 Change Computer Name

This menu option changes the computer name.

➢ **To change the computer name:**

1. On the Setup menu, select the **Change Computer Name** link; the following screen appears:

**Figure 6-23: Change Computer Name**

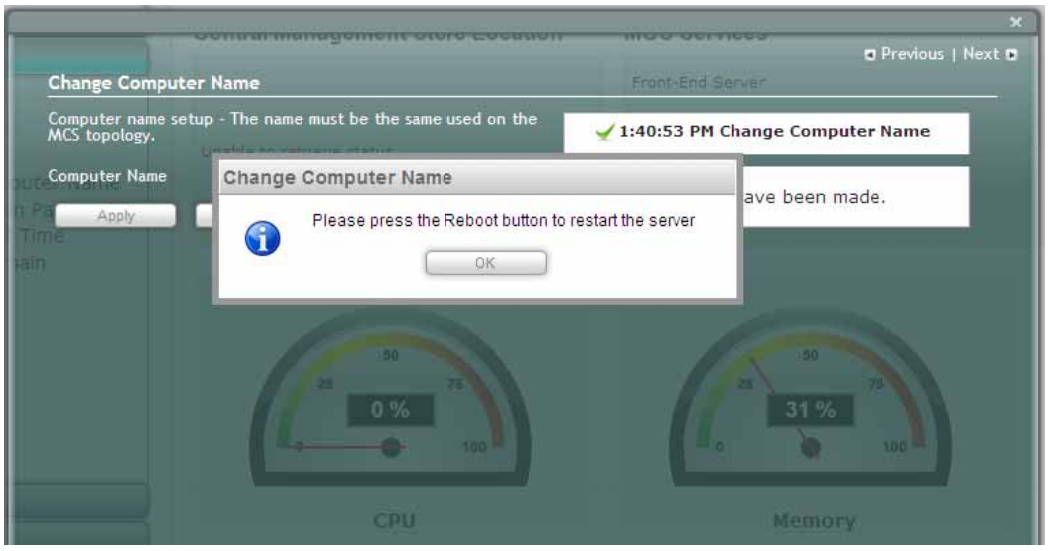



2. Enter the new computer name in the **Computer Name** field.

**Note:** You must use the same Computer Name which was used for the SBA on the Active Directory (AD) and on the Topology on the pre-configuration steps on the datacenter.

3. Click **Apply**; an "**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 rename to be effective.

**Figure 6-24: Change Computer Name - Reboot**



4. Click **OK** and then click **Reboot** to restart the server.

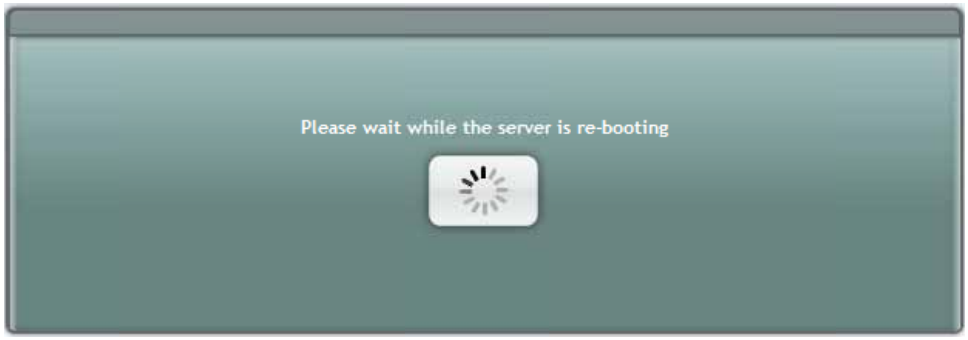
**Note:** The re-boot process can take a few minutes.

5. The following screen appears.

**Figure 6-25: Change Computer Name – Saving Changes**

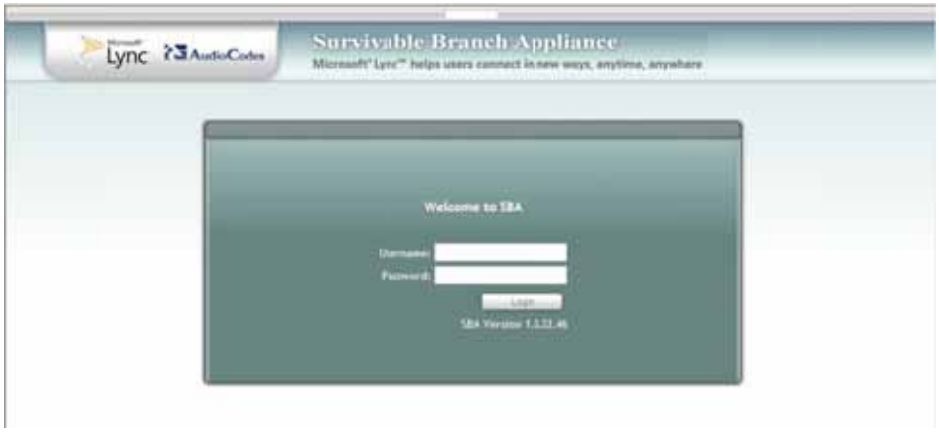

6. Click **Reboot**; the following screen appears.

**Figure 6-26: Server Re-booting**



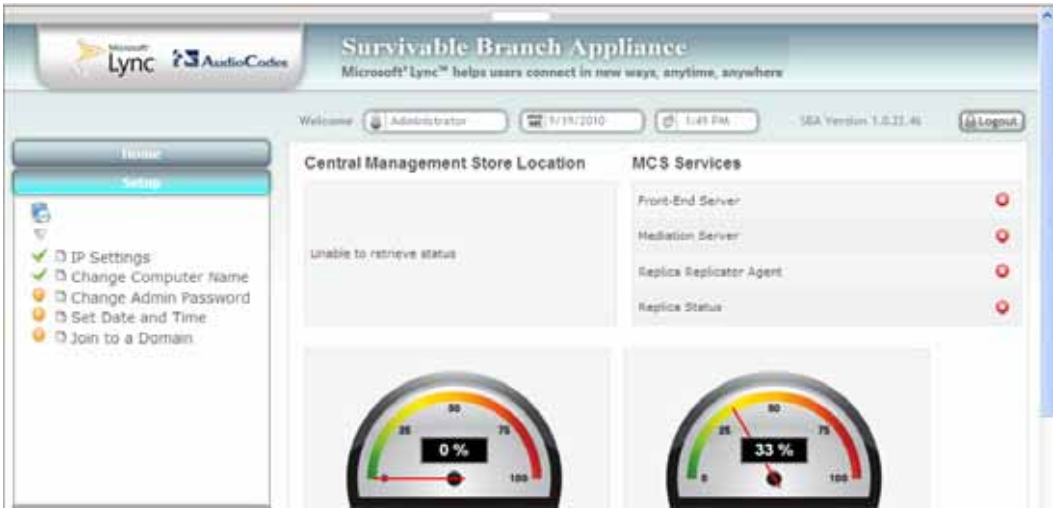

7. Login again when the following screen appears.

**Figure 6-27: Login Screen**



**8.** A green check mark appears by the completed menu item.

**Figure 6-28: Change Computer Name - Completed**



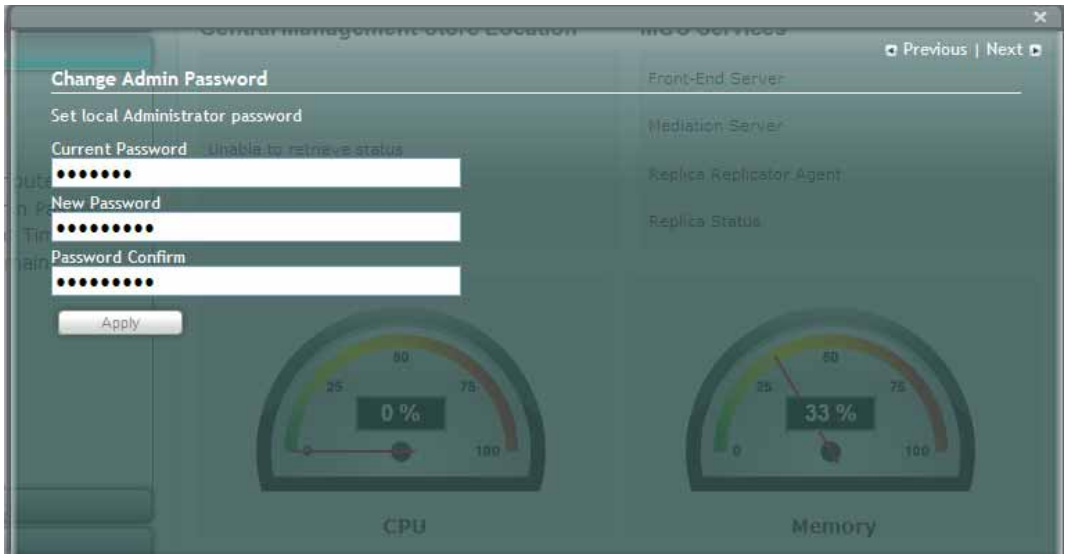
### 6.2.2.3 Change Admin Password

This menu option resets the local Administrator password.

➢ **To change the Admin password:**

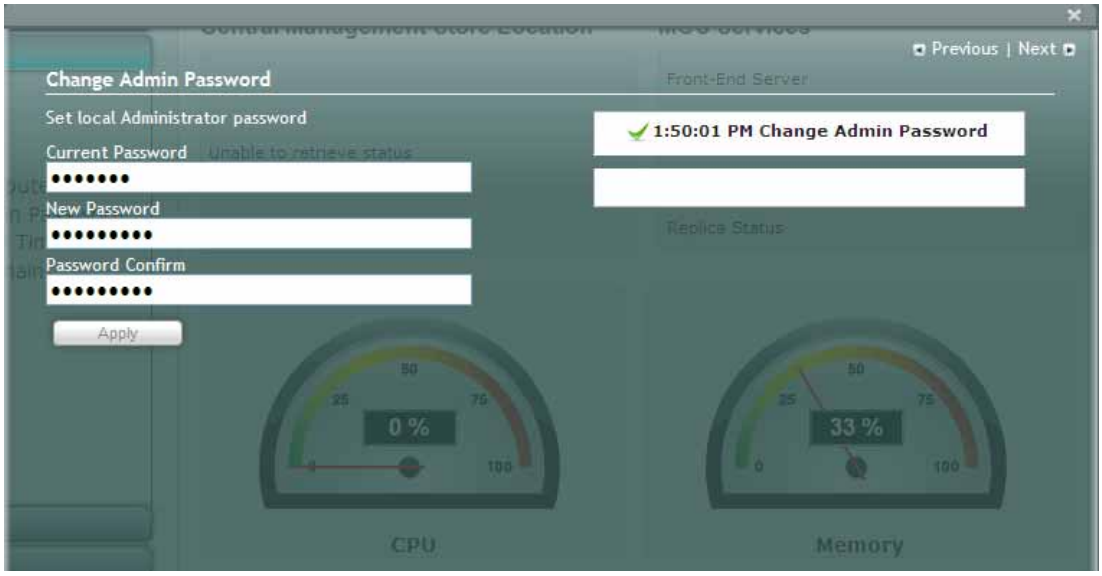
1. On the Setup menu, select the **Change Admin Password** link; the following screen appears

**Figure 6-29: Set Local Administrator Password**




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

**Figure 6-30: Change Admin Password – Saving Changes**



**6.** A green check mark appears by the completed menu item.

**Figure 6-31: Change Admin Password – Completed**

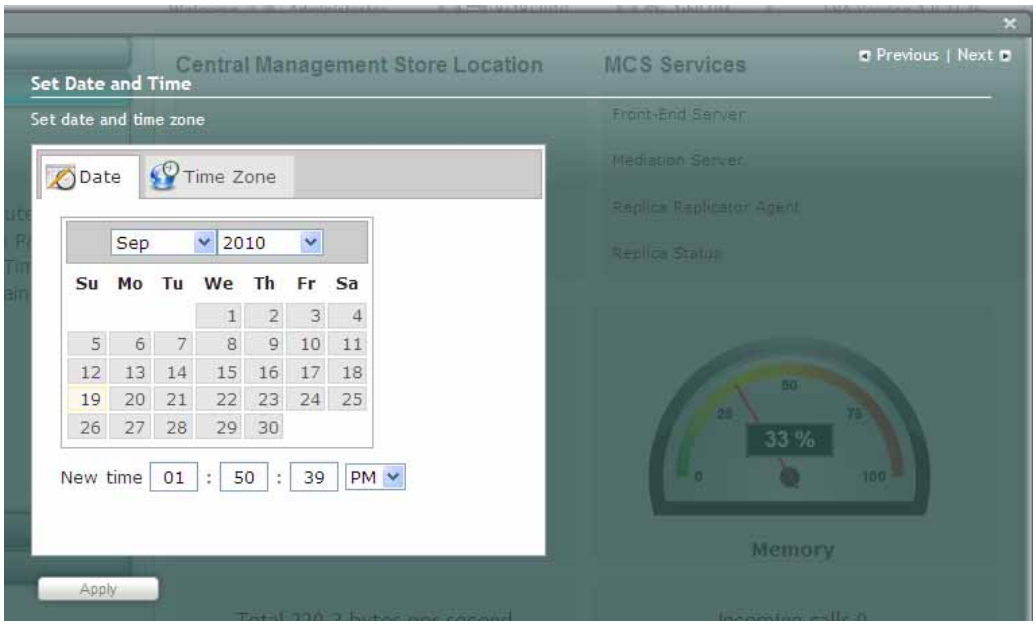
### 6.2.2.4 Set Date and Time

This menu option resets the date and time zone.

➢ **To set the date and time:**

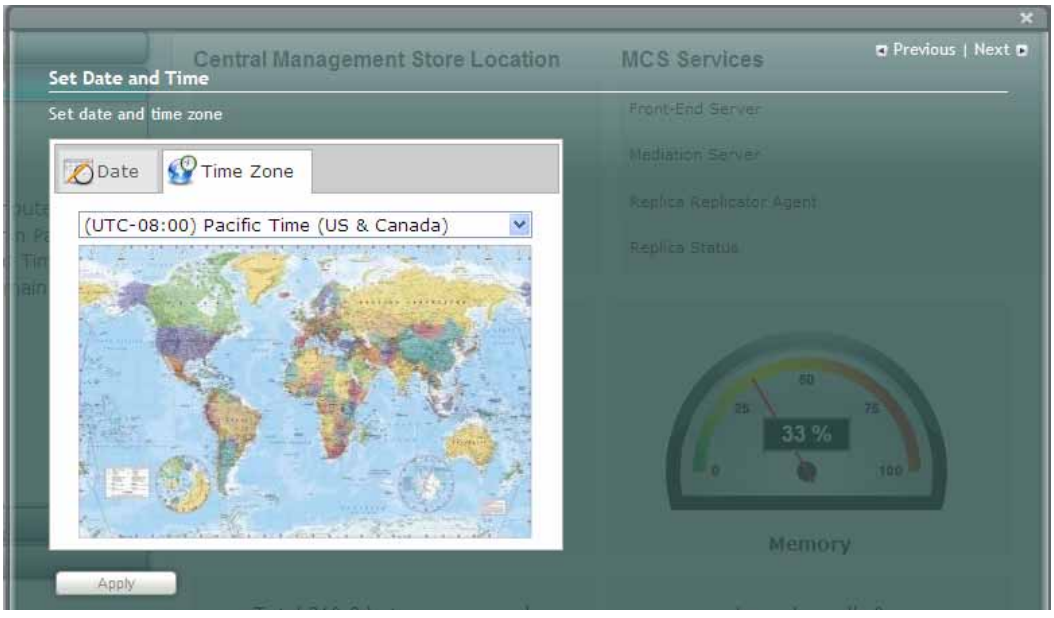
1. On the Setup menu, select the **Set Date and Time** link; the following screen appears:

**Figure 6-32: Date & Time Page**



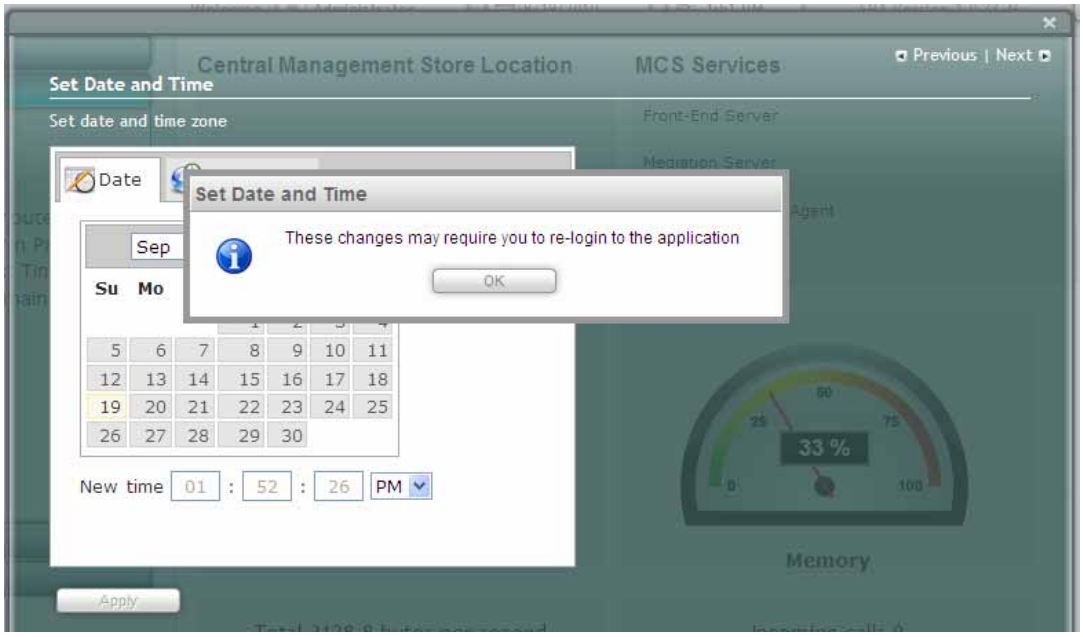

2. Select the **Date** tab and set the date and new time.
3. Click **Apply**; an "**Operation Completed Successfully**" message appears on the bottom of the screen.
4. Click **Time Zone** tab; the following screen appears.

**Figure 6-33: Set Time Zone Page**



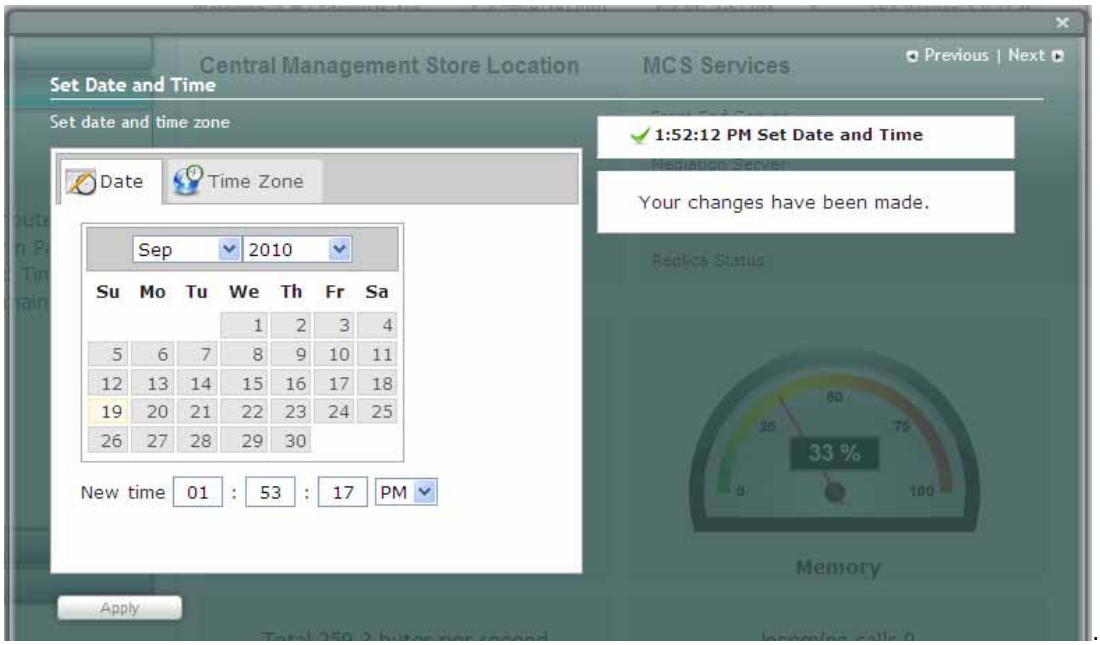

5. Open the drop-down list and select the appropriate Time Zone.
6. Click **Apply;** the following screen appears.

**Figure 6-34: Set Date and Time**



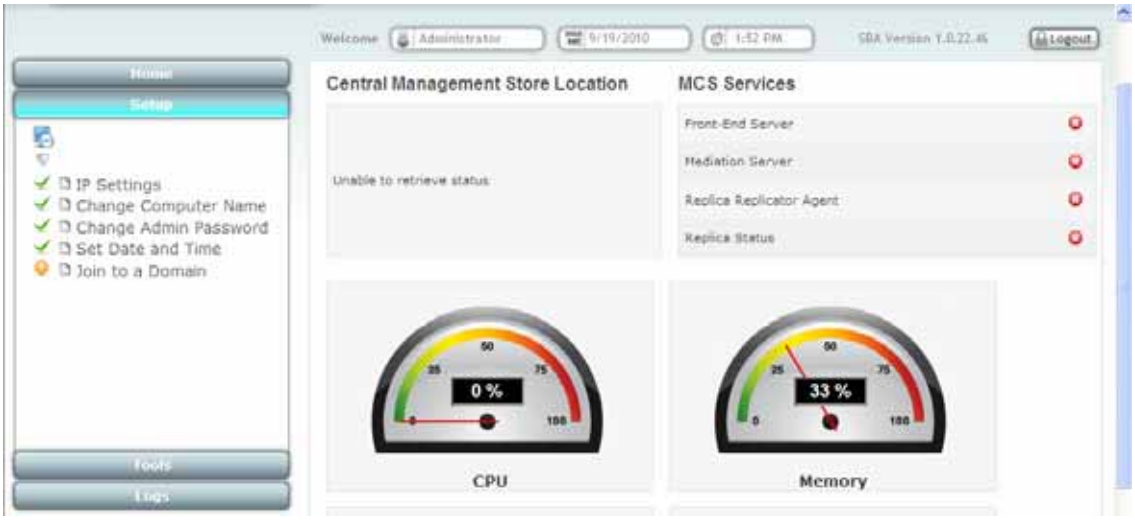

**7.** The following confirmation screen appears:

**Figure 6-35: Set Time Zone Page - Confirmation**




**8.** A green check mark appears by the completed menu item.

**Figure 6-36: Set Date and Time - Completed**



### 6.2.2.5 Join to Domain

This menu option enables join to domain.

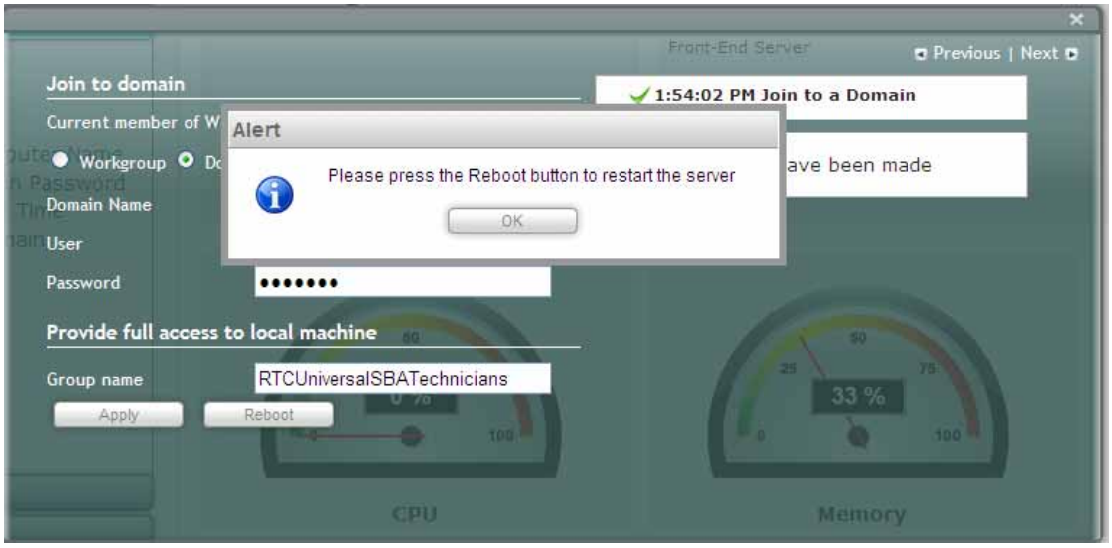
➢ **To join to the domain:**

1. On the **Setup** menu, click **Join to Domain**; the following screen appears.

**Figure 6-37: Join Domain**


2. Enter the **Domain Name**.
3. Enter the **User** and **Password** of an account that has permissions to join the SBA to the domain.
4. Click **Apply**; the following screen appears.

**Figure 6-38: Join Domain - Alert**

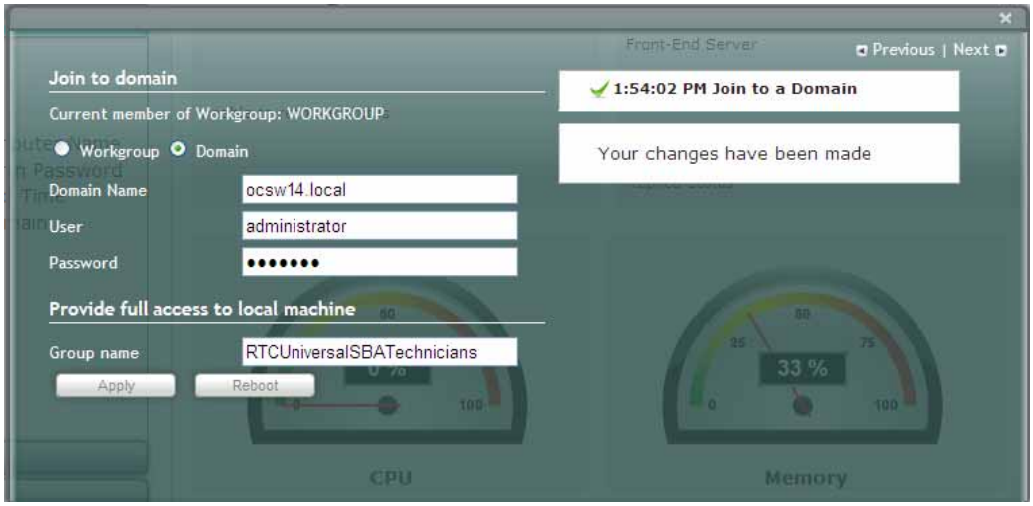



5. Click **OK**; the following screen appears.

**Note:** **Join to Domain** requires a computer re-boot which is done at the end of the next menu option.

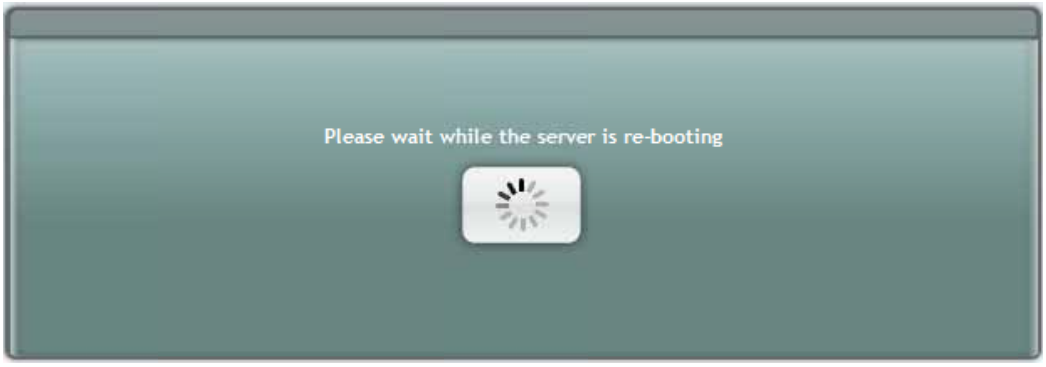
6. Click **Re-boot** on the following screen.

**Figure 6-39: Join Domain - Confirmation**




7. The following screen appears.

**Figure 6-40: Server Re-booting**




8. After re-booting, login as the Domain User.

**Note:** The Domain User check box is selected.

9. The login screen appears.

**Figure 6-41: Welcome to SBA**

**10.** After logging in as the Domain User, the following screen appears.

**Figure 6-42: Join to a Domain - Completed**


**11.** A green check mark appears by the completed menu item.

**Note:** The remaining menu options now appear in the **Setup** menu..

### 6.2.2.6 Device Preparation

This menu option completes the SQL preparation and installs the OCS components.

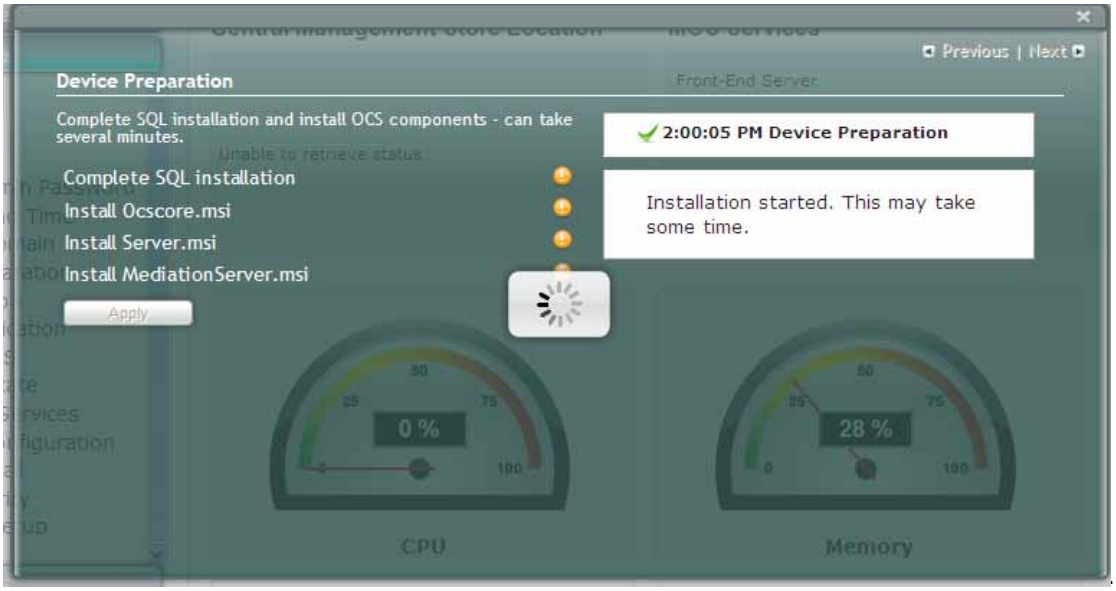
➢ **To prepare the device:**

1. On the Setup menu, click **Device Preparation**; the following screen appears.

**Figure 6-43: Device Preparation**


2. Click **Apply.**

**Figure 6-44: Device Preparation - Start**



**3.** The following screens appear**.**

**Figure 6-45: Device Preparation - Wait**

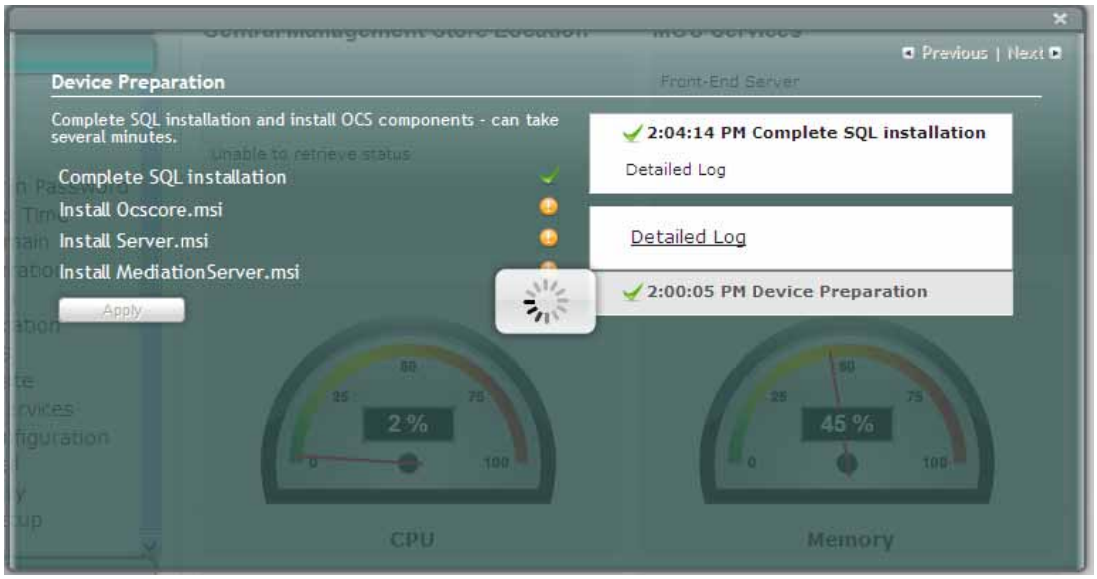
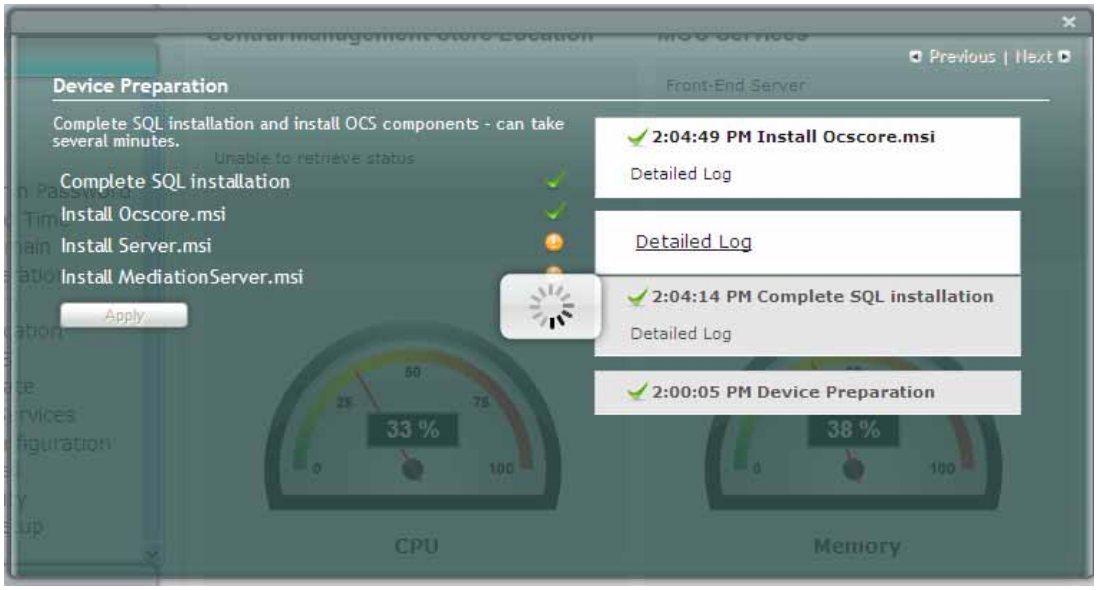



**Figure 6-46: Device Preparation – PM Install Ocscore.msi**




**Note:** A Detailed Log can be viewed after each phase has been completed. Click on the **Detailed Log** link to view the log.

**Figure 6-47: Device Preparation – PM Install Server.msi**

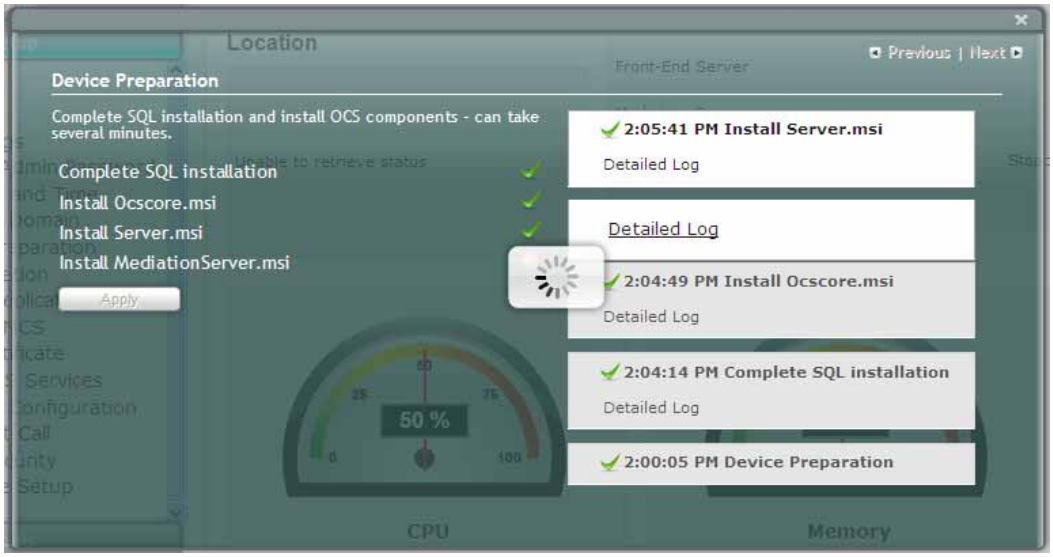
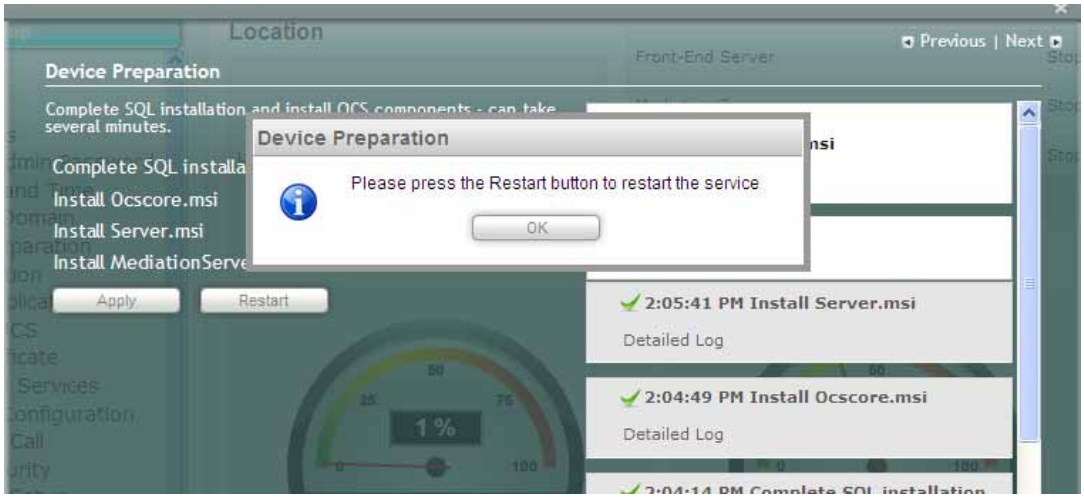
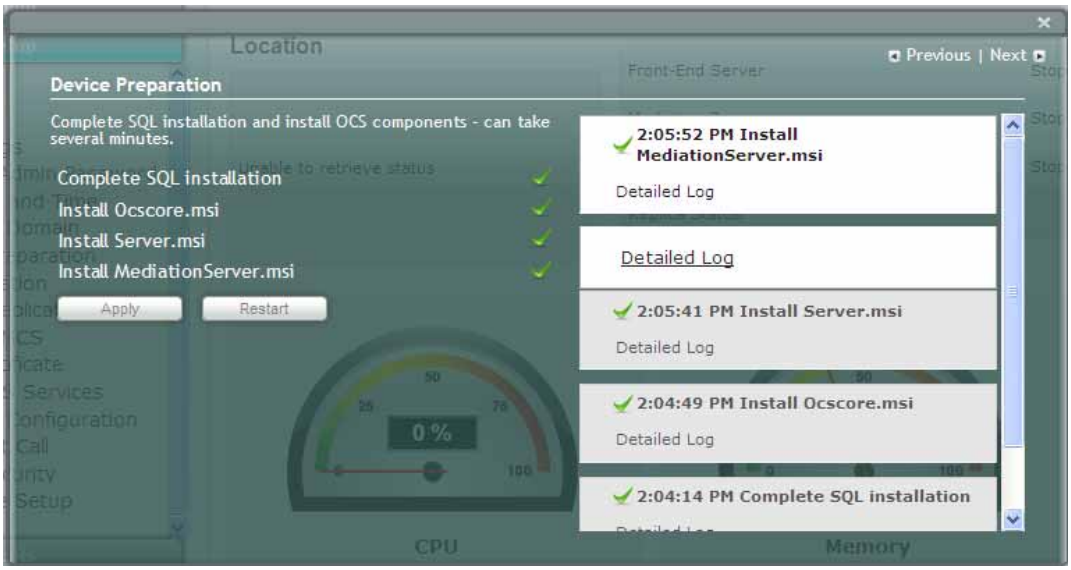



**Figure 6-48: Device Preparation - Restart**




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

**Figure 6-49: Device Preparation – PM Install MediationServer.ini**



5. Click **Restart** if all steps have been successfully completed. If not, refer to the Detailed Log for more information.

**Note:** **For the Beta Refresh version** - In case you are not prompted to restart the service after the device preparation has finished, you will need to restart the server manually via the Tools Menu or RDT.

**Note:** If one of the installation steps have failed, rectify the problem as described in the Detailed Log. Clicking **Apply** on the Device Preparation page, will try to install the remaining components.

6. A green check mark appears by the completed menu item.

**Figure 6-50: Device Preparation – Completion**

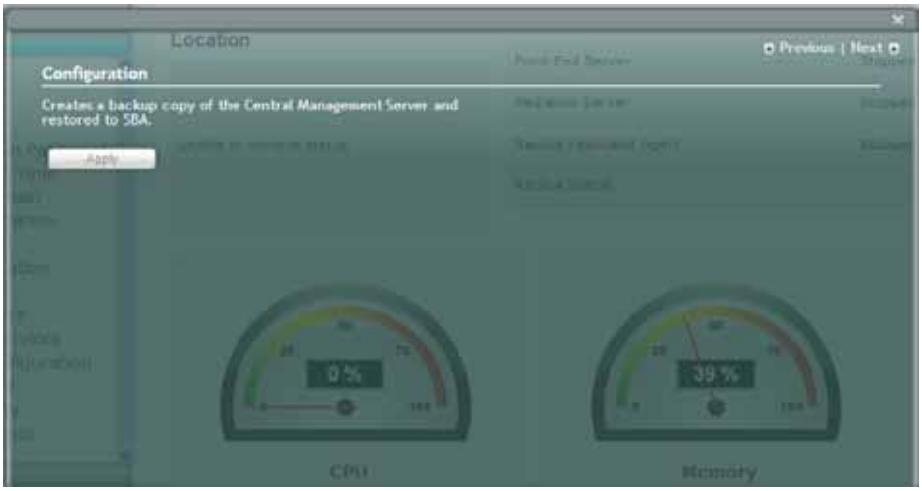
### 6.2.2.7 Configuration

This menu option creates a backup copy of the Central Management Server to be stored on the SBA server.

➢ **To run configuration:**

1. On the **Setup** menu, click **Configuration**; the following screen appears.

**Figure 6-51: Configuration**

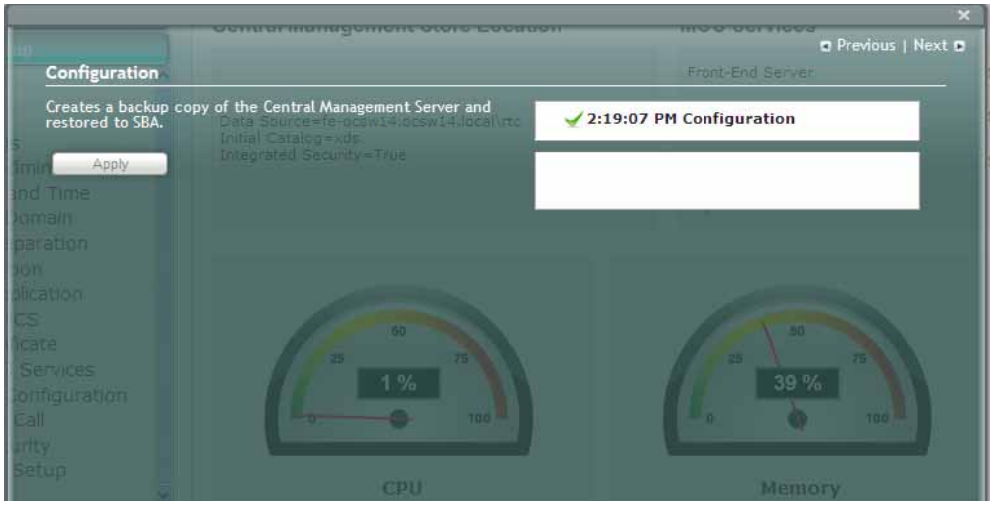



2. Click **Apply**.

**Note:** If the Configuration step fails immediately after the Device Preparation phase, re-boot the server manually using the **Tools** menu option.

3. The following screen appears..

**Figure 6-52: Configuration Start**



**4.** A green check mark appears by the completed menu item.

**Figure 6-53: Configuration - Completion**

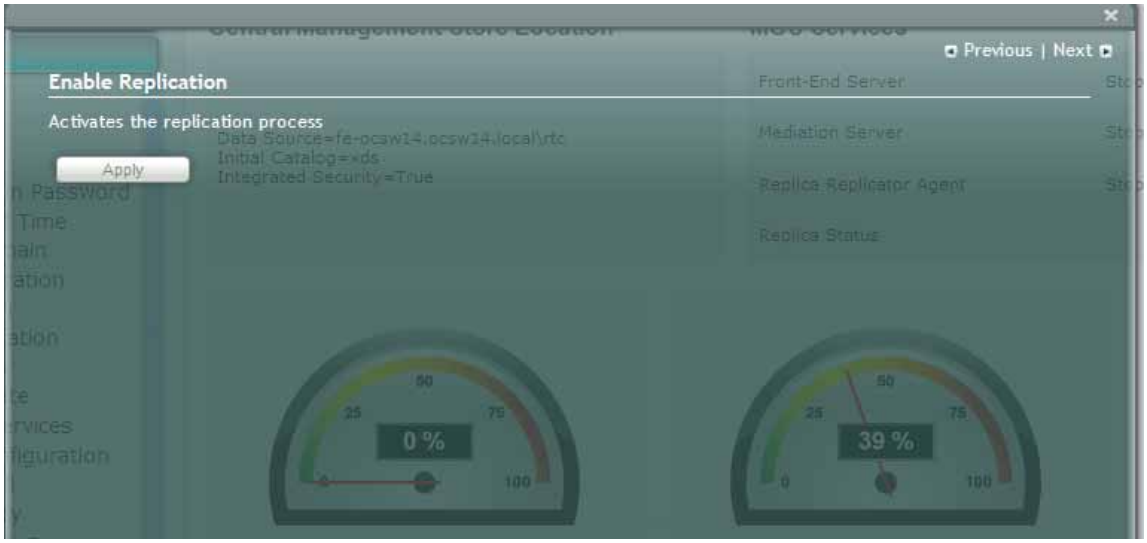
### 6.2.2.8 Enable Replication

This menu option activates the replication process.

➢ **To enable replication:**

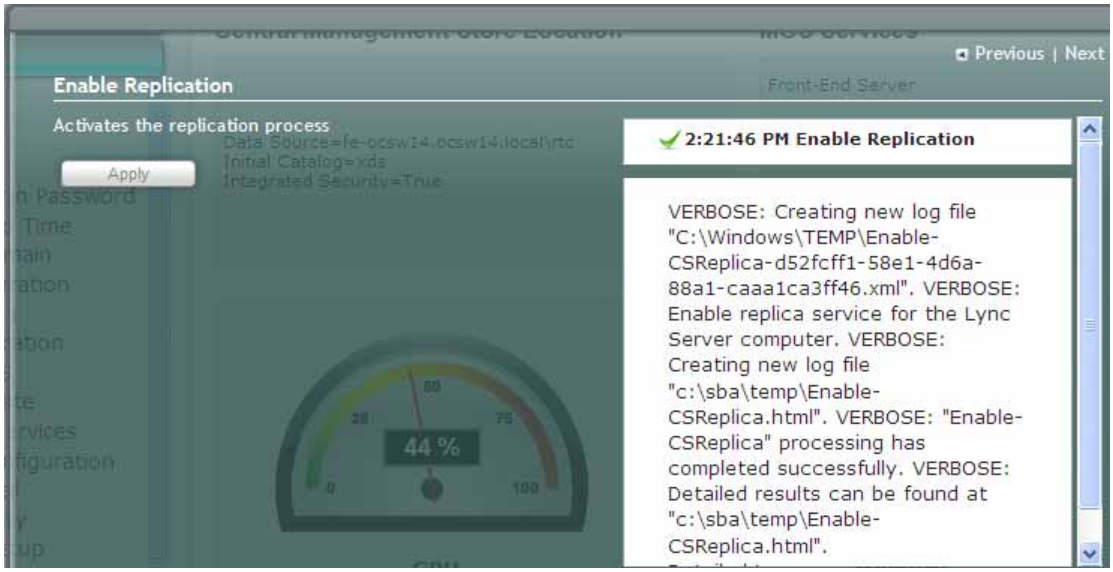
1. On the **Setup** menu, click **Enable Replication**; the following screen appears.

**Figure 6-54: Enable Replication**



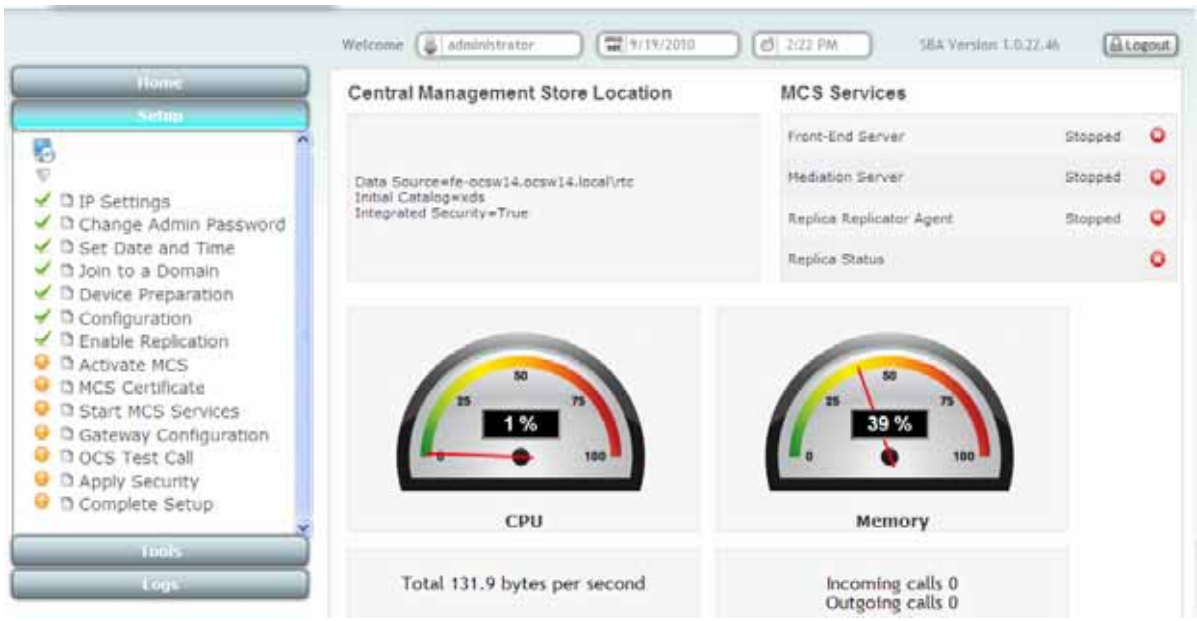

2. Click **Apply**; the following screen appears.

**Figure 6-55: Enable Replication**



**3.** A green check mark appears by the completed menu item.

**Figure 6-56: Enable Replication - Completion**



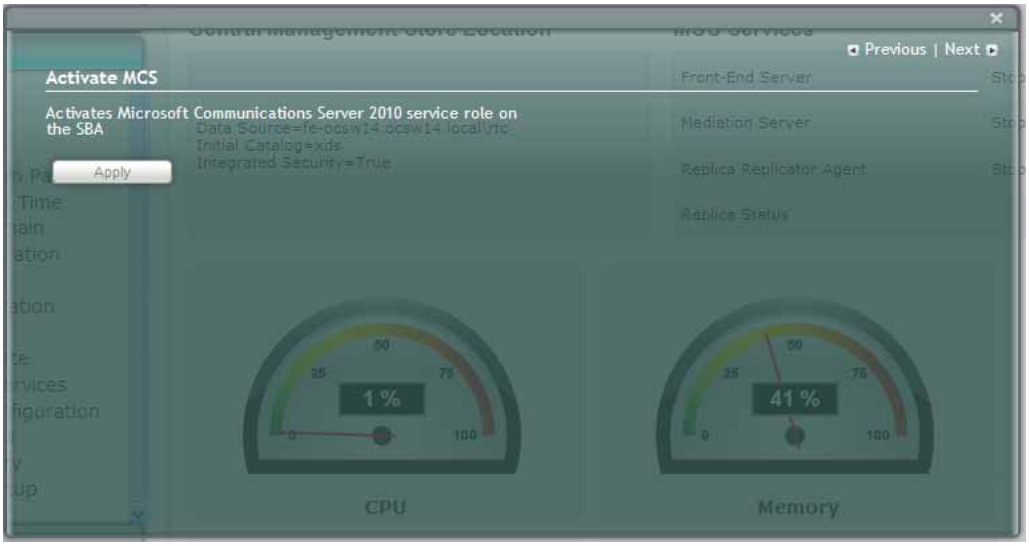
### 6.2.2.9 Activate MCS

This menu option activates a computer running a Microsoft 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:**

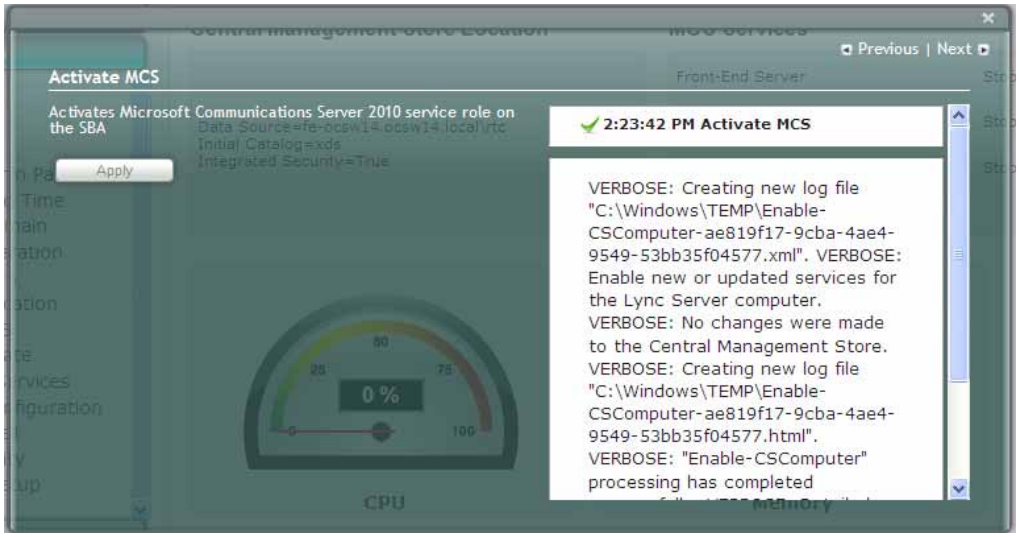
1. On the **Setup** menu, click **Activate MCS**; the following screen appears.

**Figure 6-57: Activate MCS**



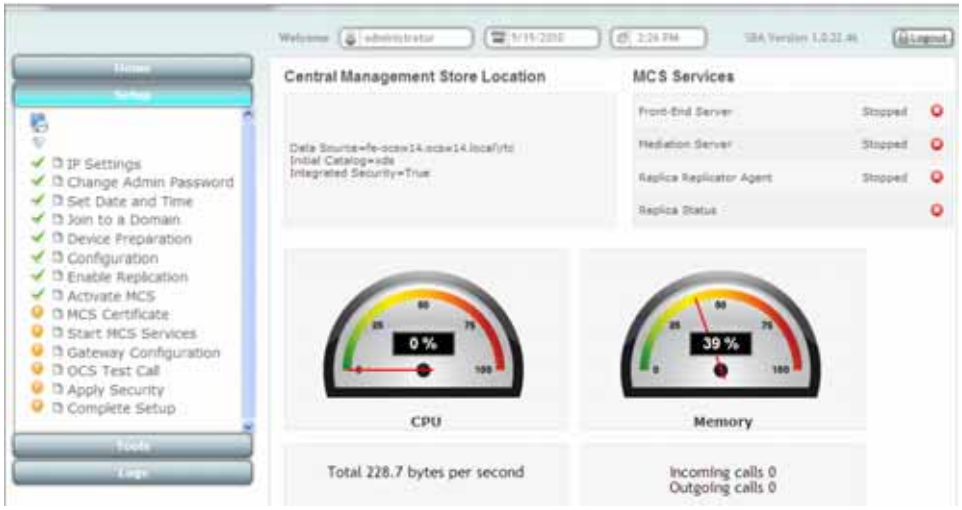

2. Click **Apply**; the following screen appears.

**Figure 6-58: Activate MCS – Processing**



**3.** A green check mark appears by the completed menu item.

**Figure 6-59: Activate MCS - Completion**



### 6.2.2.10 MCS Certificate

This menu option installs a certificate from the domain's certificate authority. On the **Setup** menu, click **MCS Certificate**; the following screen appears.

**Figure 6-60: Import Certification**


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

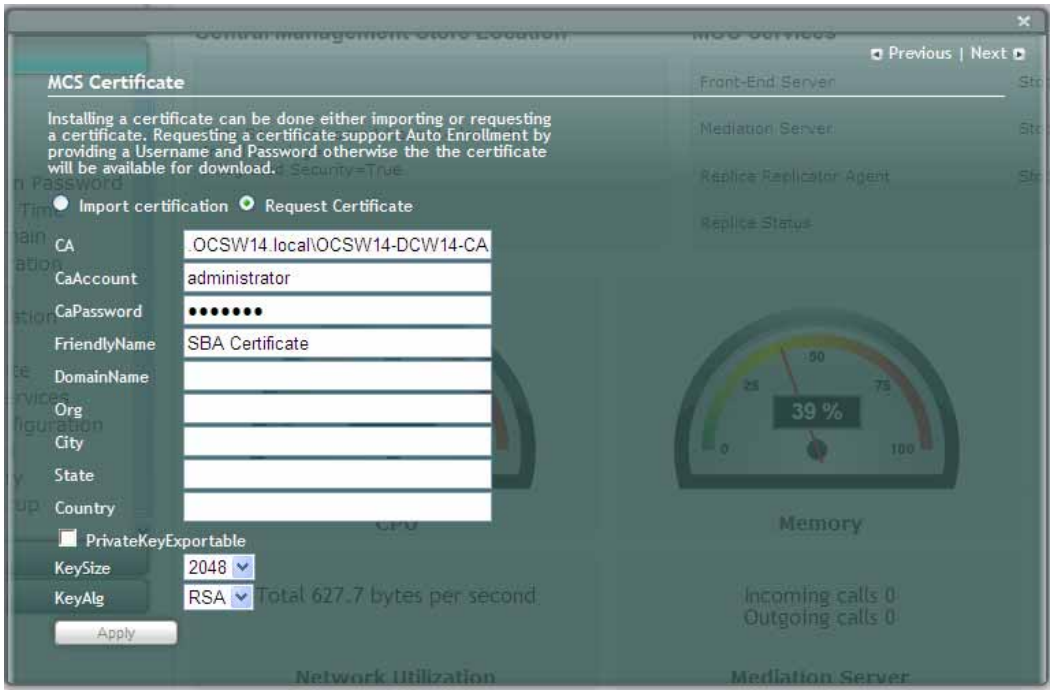
➢ **To import a certificate:**

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 certificate:**

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

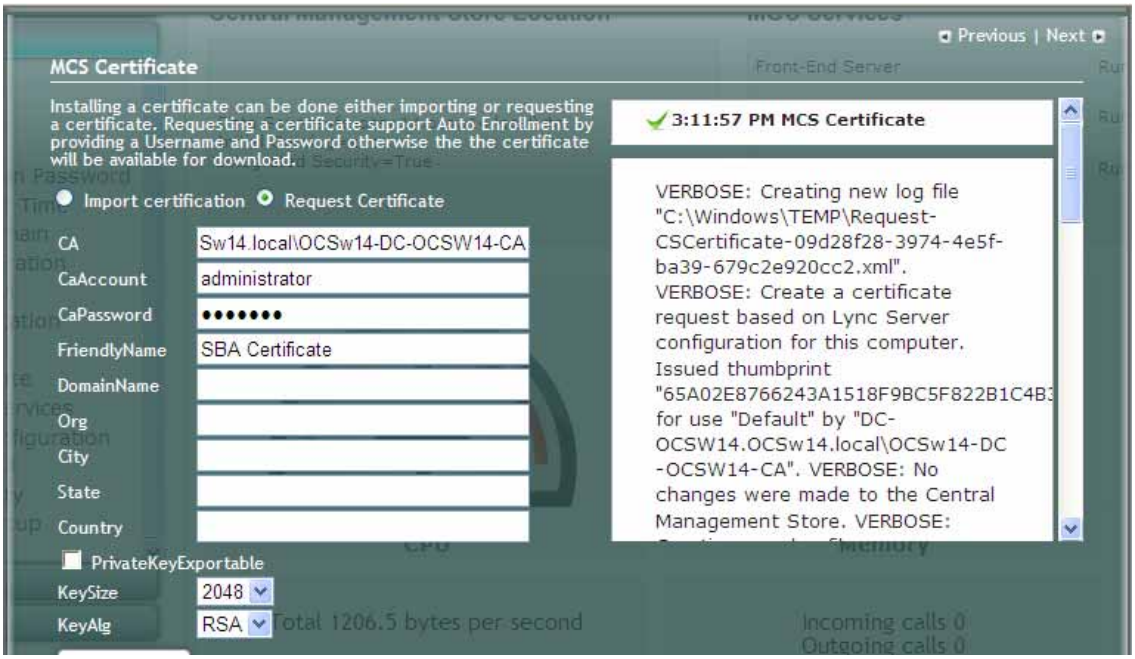
**Figure 6-61: Request Certificate**



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.

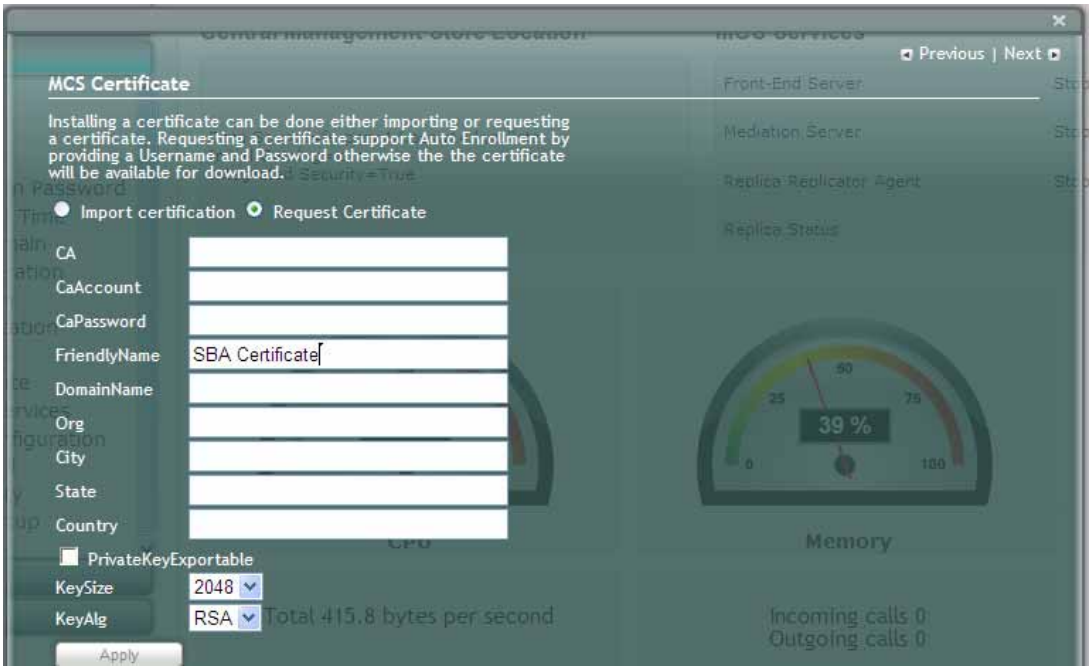
   The CA field contains the *CA FQDN\CA Name.*

**Figure 6-62: MCS Certificate – Detailed Log**



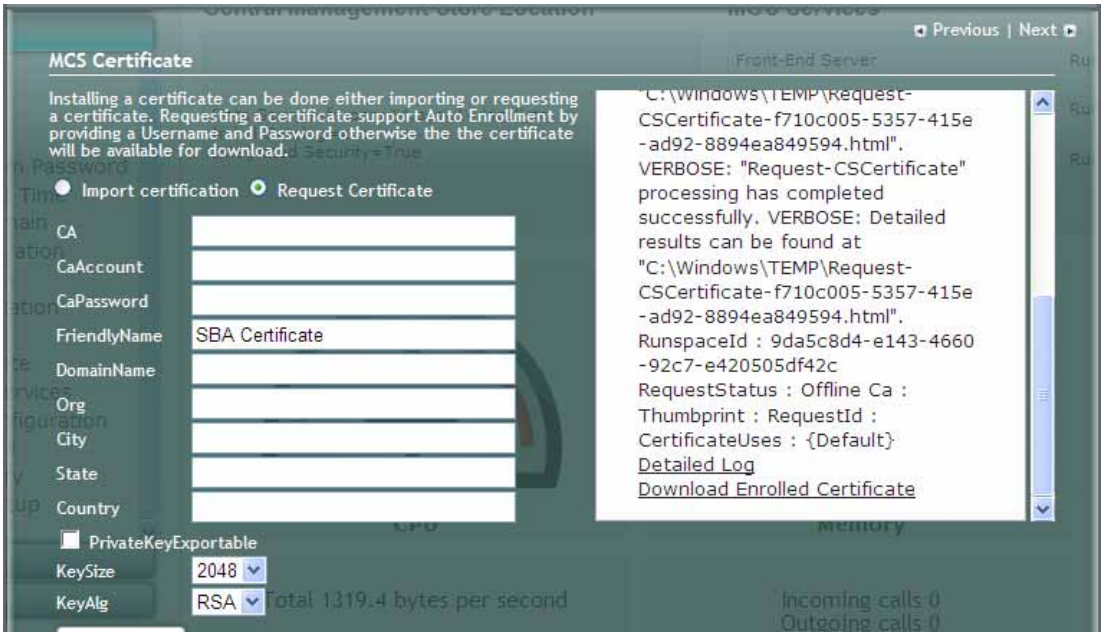

3. If the CA field is not entered, the system will create an enrollment certificate which can be downloaded.

**Figure 6-63: MCS Certificate – Download Enrolled Certificate**



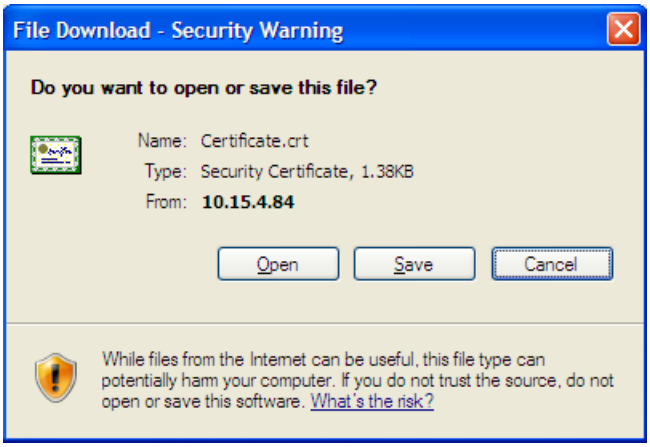

4. Click **Apply**; the following screen appears.

**Figure 6-64: MCS Certificate – Download Enrolled Certificate**




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

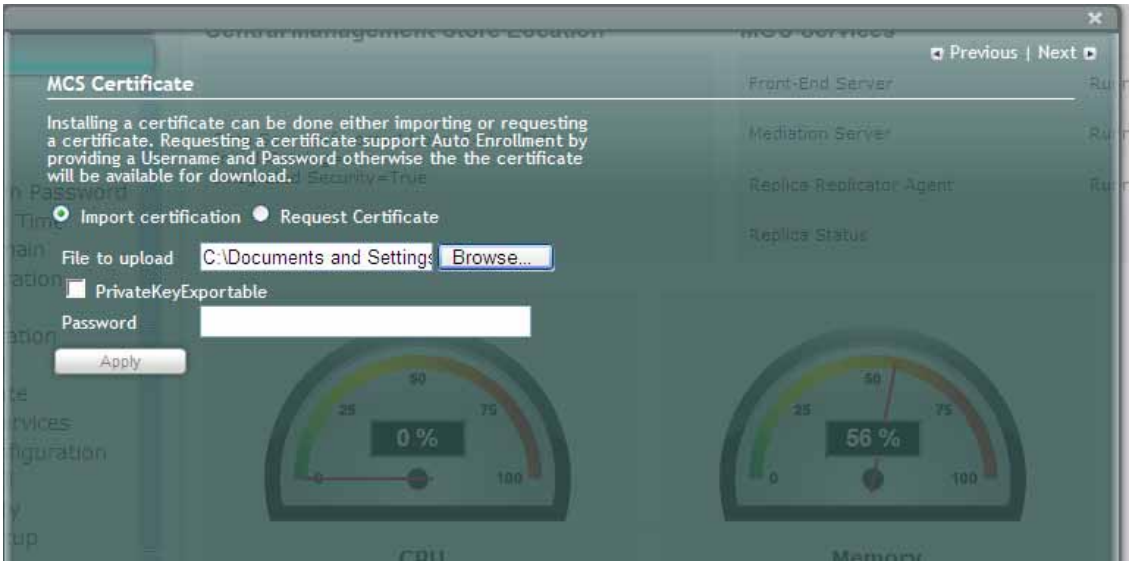
**Figure 6-65: MCS Certificate – File Download**




6. Click **Save**.

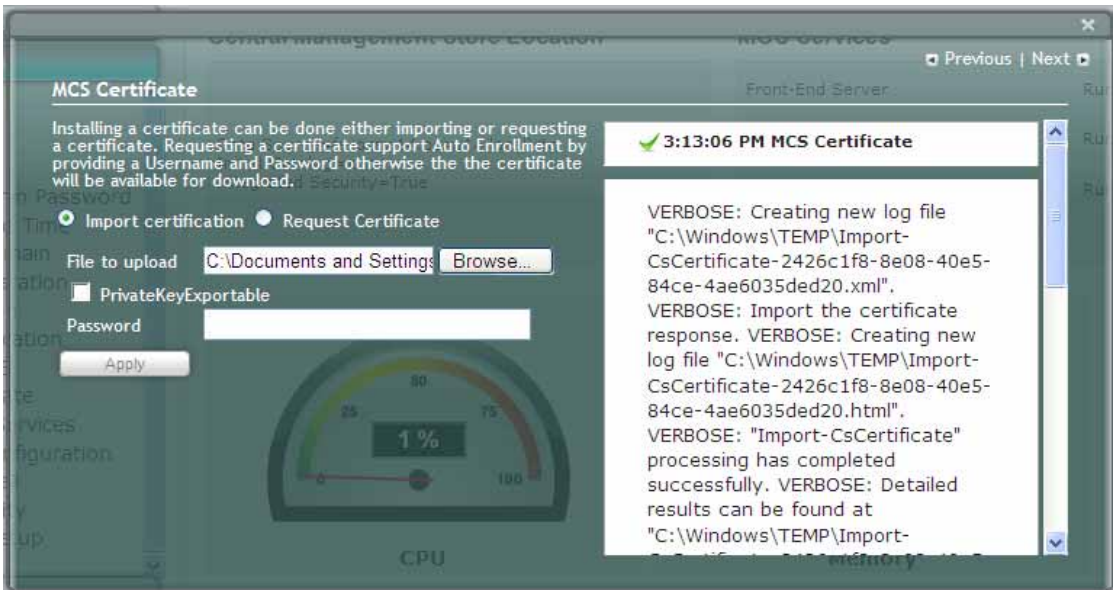
7. Once the Enrollment Certificate has been signed, select the **Import Certification** radio-button as shown below and upload the signed certificate to be uploaded by using the **Browse** and **File to Upload** fields.
8. Click **Apply**.

**Figure 6-66: MCS Certificate – File Upload**



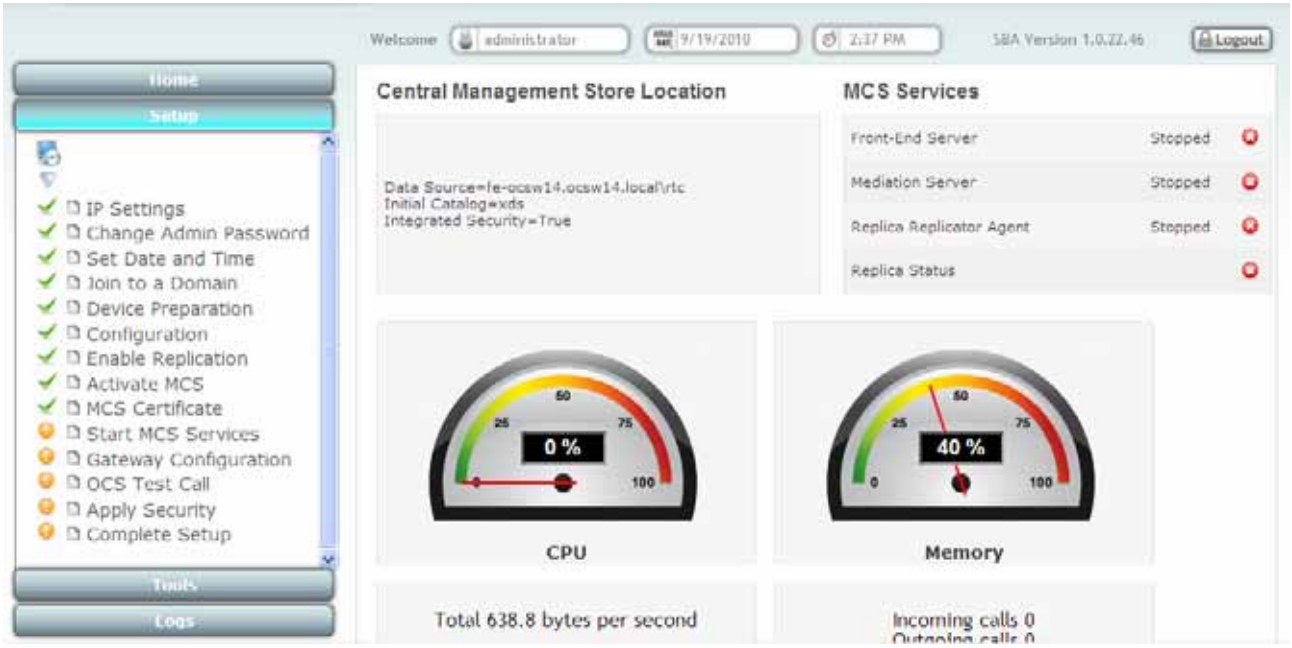

9. The following screen appears.

**Figure 6-67: MCS Certificate – Detail Log**



**10.** A green check mark appears by the completed menu item.

**Figure 6-68: MCS Certificate – Complete**



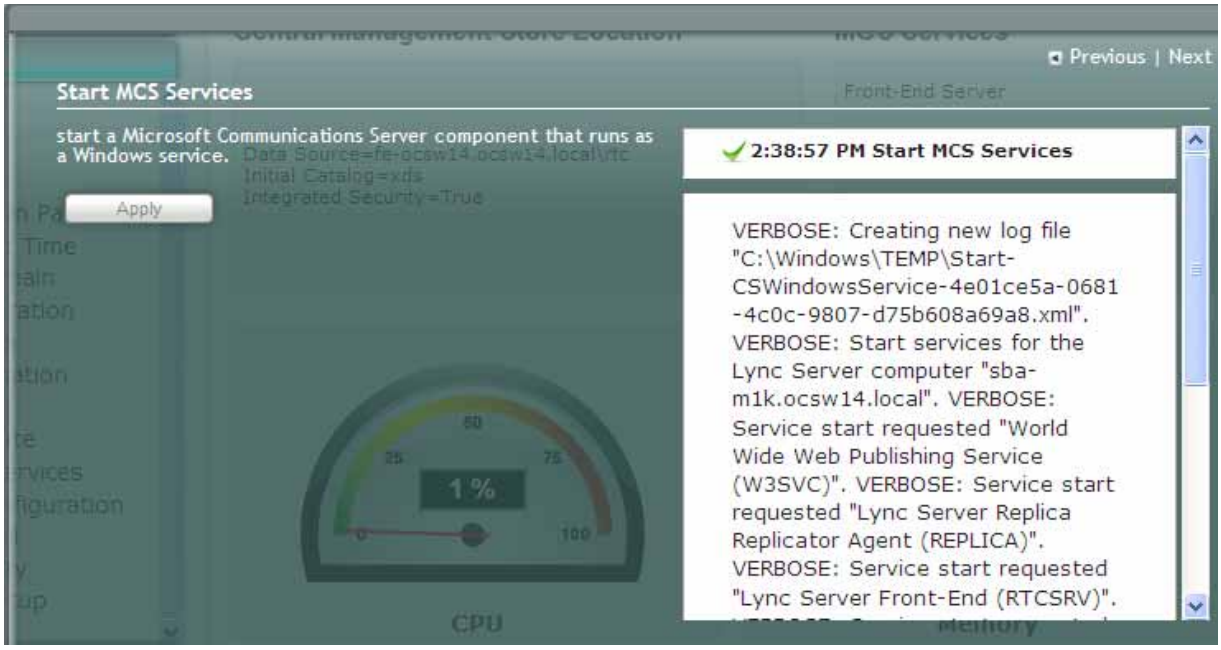
### 6.2.2.11 Start MCS Services

This menu option enables you to start a Microsoft Communications Server component that runs as a Windows service.

➢ **To start MCS Services:**

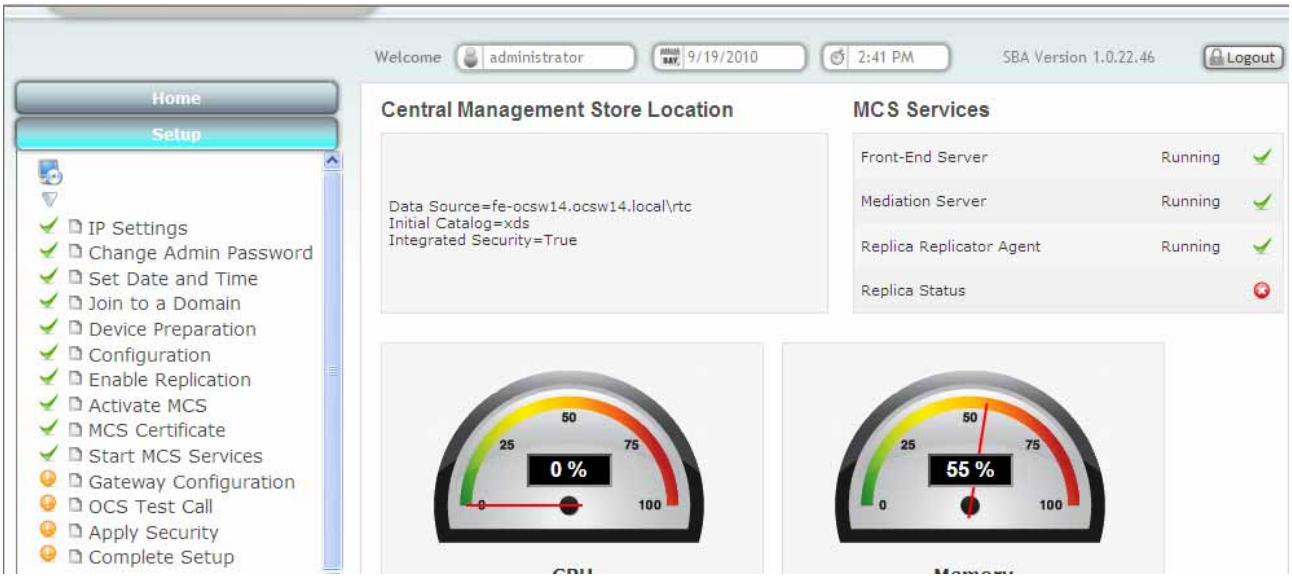
1. On the **Setup** menu, click **Start MCS Services**; the following screen appears.

**Figure 6-69: Start MCS Services**




2. Click **Apply** to start the services as per the MCS configuration settings.
3. A green check mark appears by the completed menu item.

**Figure 6-70: Start MCS Services - Completion**



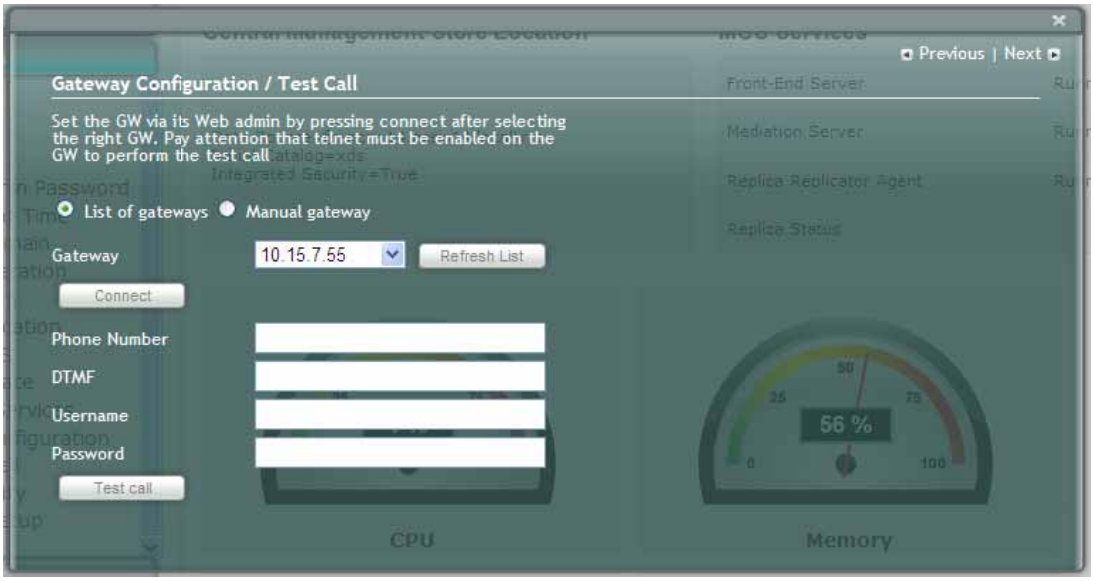
### 6.2.2.12 Gateway Configuration

This menu option sets the Gateway via its Web Administrator. Telnet must be enabled on the gateway to perform the Test Call..

➢ **To configure the gateway:**

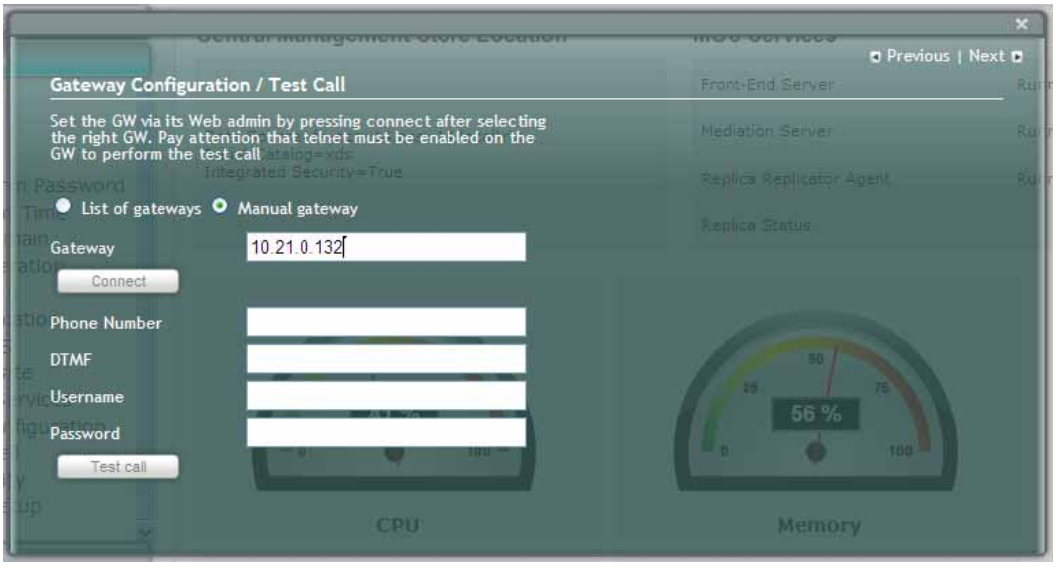
1. On the **Setup** menu, click **Gateway Configuration**; the following screen appears.

**Figure 6-71: Gateway Configuration**




2. Using the **List of Gateways** (default) option, select a gateway from the gateway drop-down box. In case your gateway is not displayed in the list, select the **Manual gateway** radio-button and enter an **IP Address** or **DNS Name** in the **Gateway** field.
3. Click **Connect** and setup the gateway.

**Figure 6-72: Gateway Configuration – Manual Gateway**



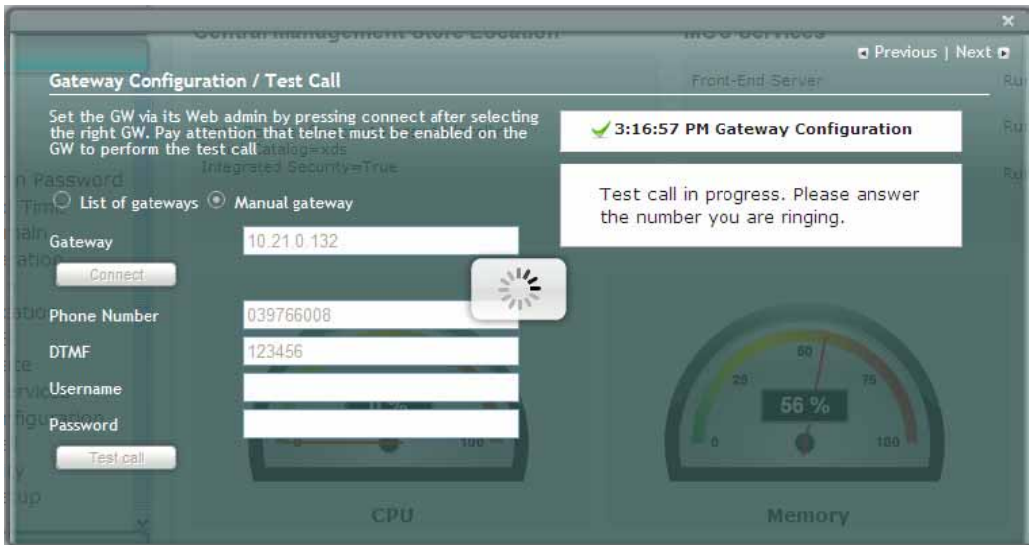

**Note:** At this point, enable Telnet.

4. Please refer to Section 6.3 for instructions on how to configure the gateway.

### ➢ To perform a Test Call

1. Enter a **Phone Number**.
2. Enter a **DTMF**.
3. Telnet needs to be enabled on default Port 23. Refer to the Web Interface – **Management** > **Telnet/SSH Settings**. Set **Embedded Telnet Server** to **"Enable".** Set **Telnet Server TCP Port** to **"23".**
4. **Username** and **Password** are not mandatory. If you changed the Username and Password of the gateway, use it in this step.
5. Click **Test call**.

**Figure 6-73: Gateway Configuration – Test Call in Progress**




**Note:** If the test fails, the phone will not ring. If the phone does ring, lift the handset and confirm that you can hear the DTMFs.

6. The following screen appears when you answer the phone. If the phone does not ring, an error message will appear.

**Figure 6-74: Gateway Configuration – Test Call in Progress**

### 6.2.2.13 OCS Test Call

The **OCS Test Call** option allows you to make a PSTN call which is initiated by the OCS.

Before placing an OC Test Call, you must define special accounts on the OCS:

The following are the prerequisites for the cmdlets to run. These tasks will be performed by the MCS Admin.

- Test Users are already created in MCS and they are voice enabled.
- VoIP Outbound Routing configuration is setup, and the correct policies are assigned to the Test Users.

You need to set up the built-in-users for OcsHealthMonitoring in advance with the following commands:

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

**Identity** - Fully qualified domain name of the pool where the health monitoring configuration settings are to be assigned.

**FirstTestUserSipUri** - 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.

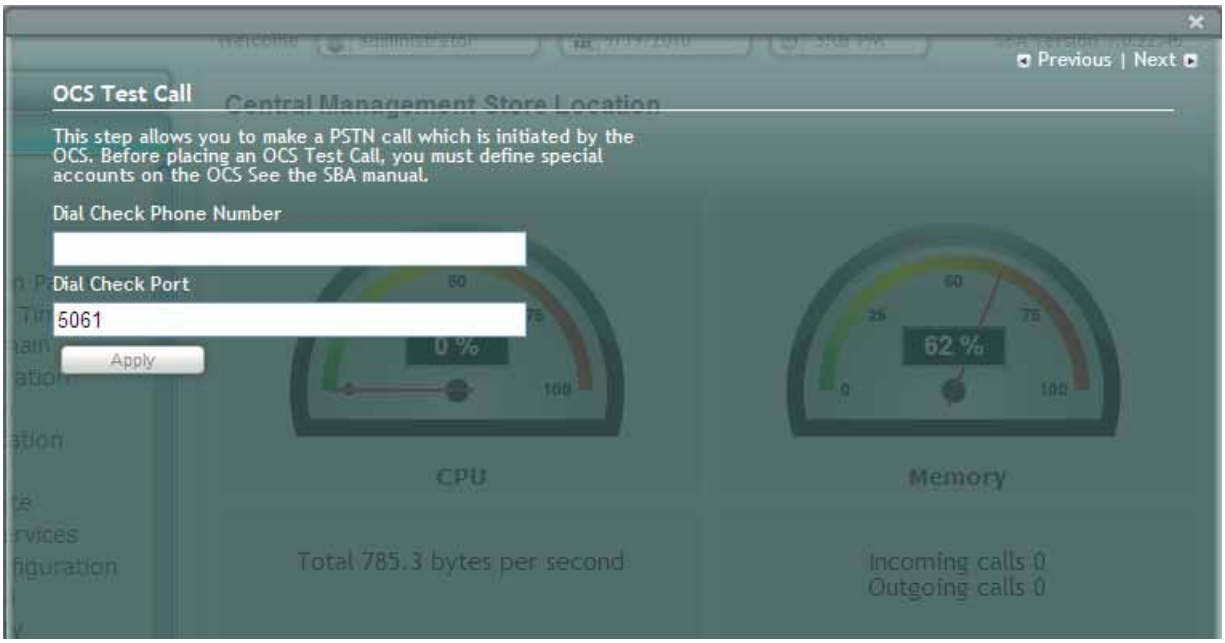
**SecondTestUserSipUri** - SIP address of the second test user to be configured for use by this collection of health monitoring settings. Note that the SIP address must include the sip: prefix. For example: -FirstTestUserSipUri sip:jhaas@litwareinc.com.

➢ **To place a call:**

1. Enter the **Dial Check Phone Number**.
2. Enter **Dial Check Port**.
3. Click **Apply**.

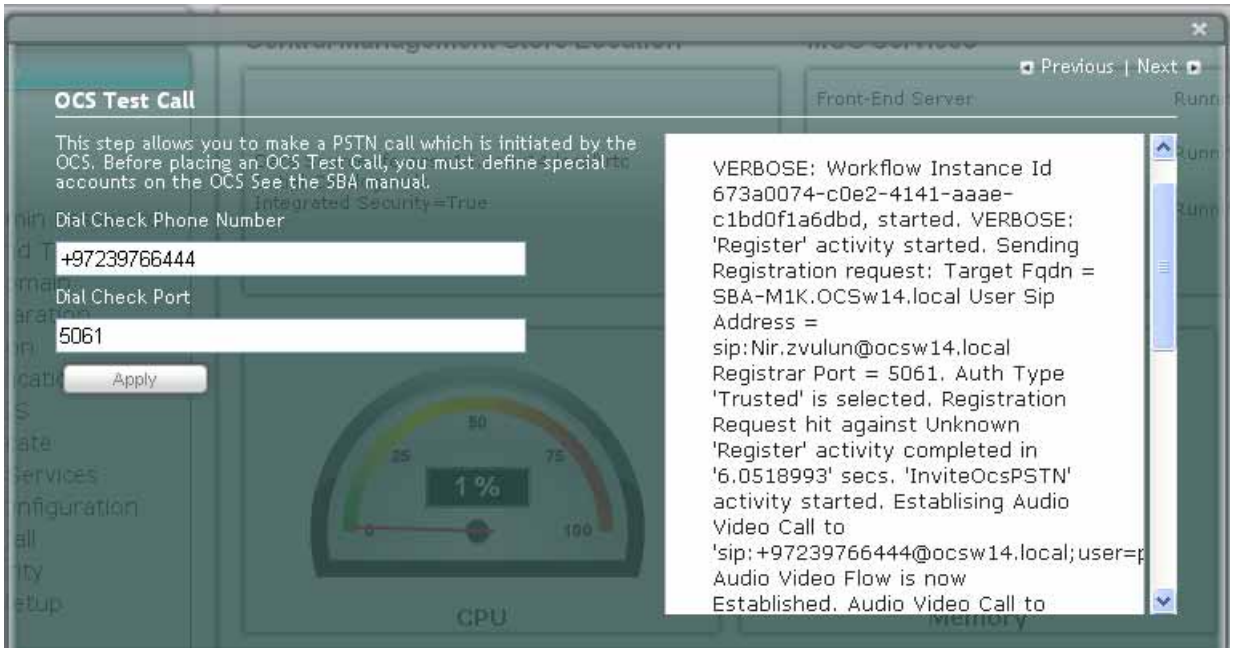
**Note:** **For the Beta Refresh version** - enter 5061 on the dial check port.

**Figure 6-75: OCS Test Call**




**4.** The following screen appears.

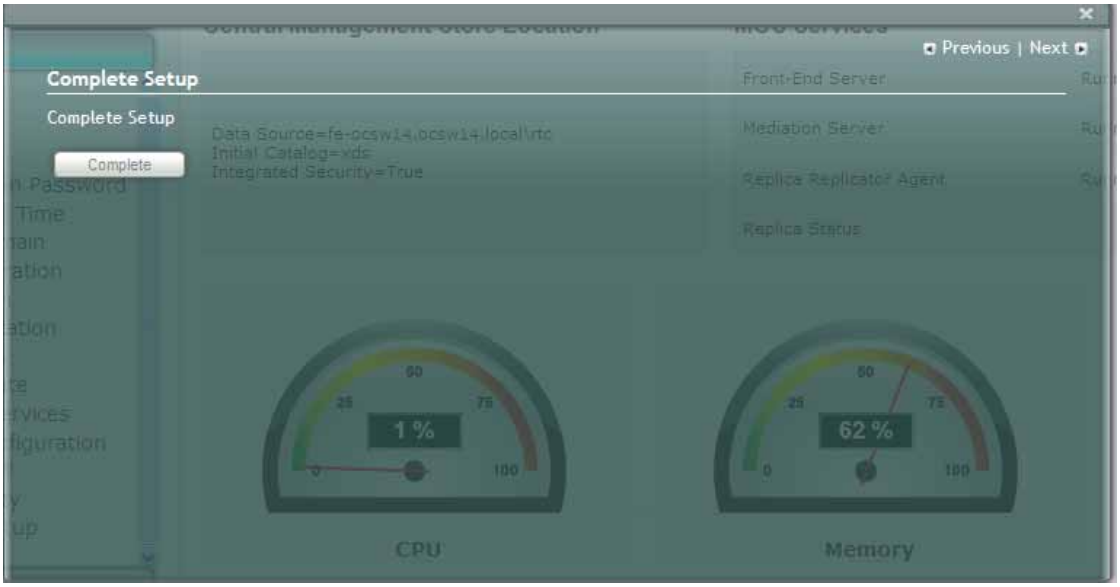
**Figure 6-76: OCS Test Call**



### 6.2.2.14 Complete Setup

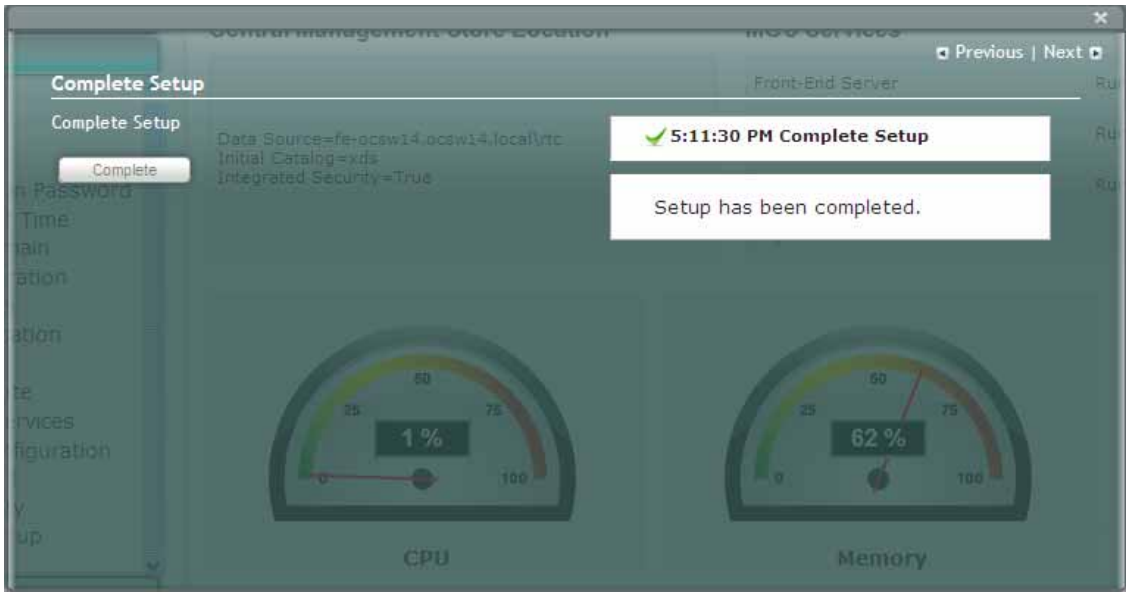
1. After completing all SBA settings, click **Complete**. When you log in, the **Home** tab will be displayed and not **Setup**.

**Figure 6-77: Complete Setup**



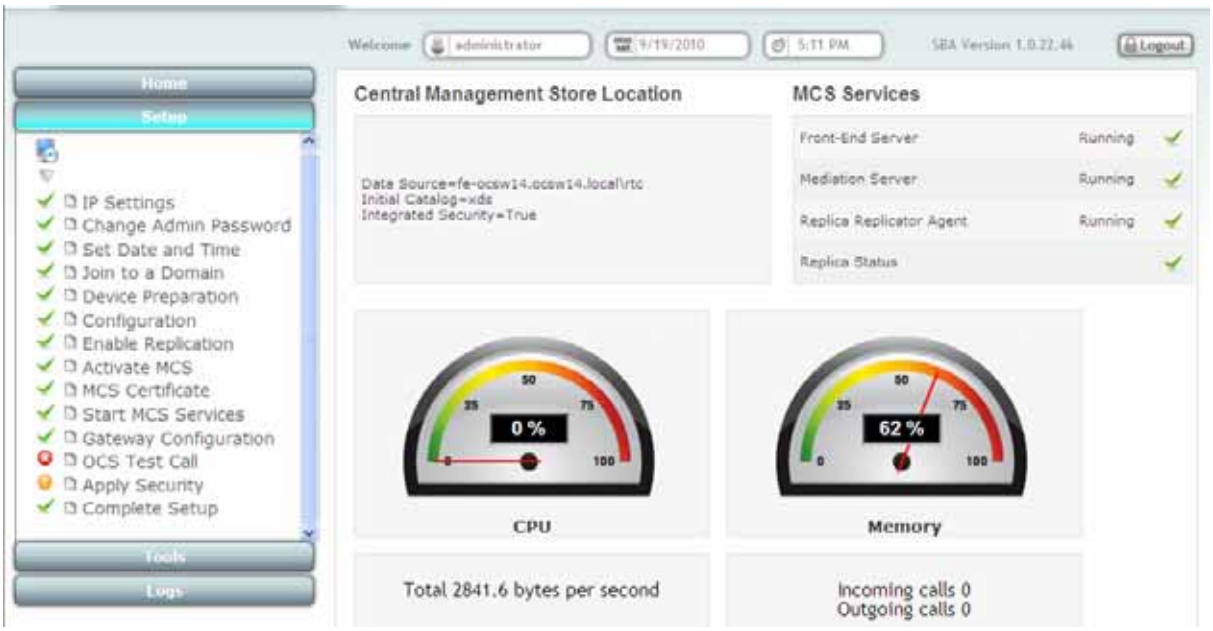

2. The following screen appears.

**Figure 6-78: Complete Setup – Setup Completed**



**3.** A green check mark appears by the completed menu item.

**Figure 6-79: Complete Setup**



## 6.2.3 Home

The **Home** tab displays the **Home** page as shown below:

**Figure 6-80: Home Page**

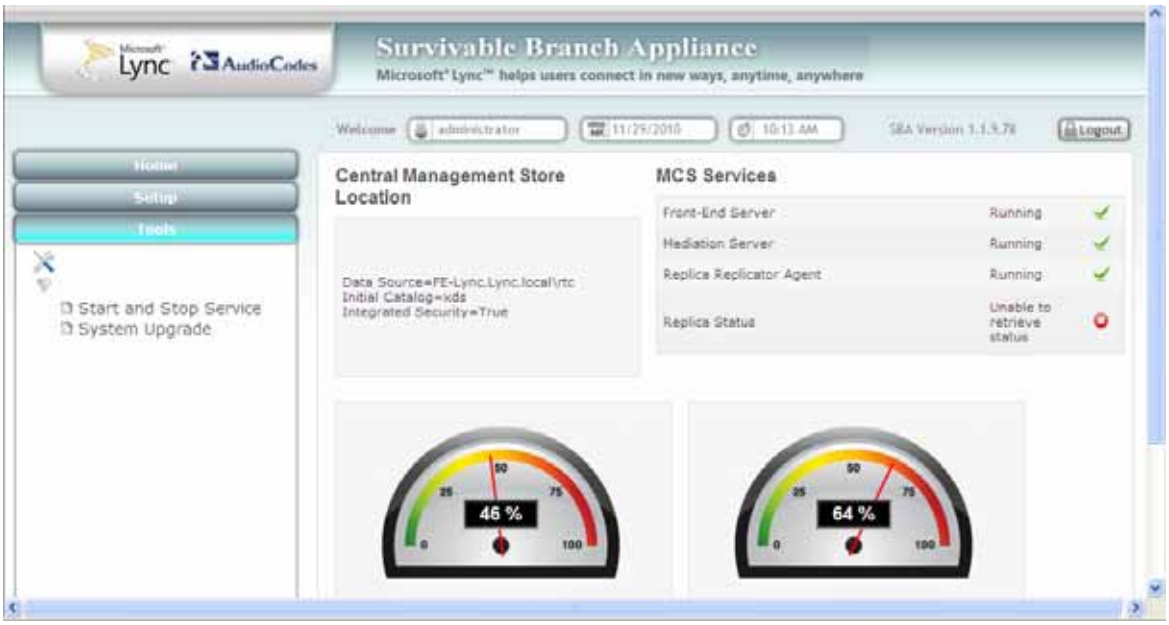

## 6.2.4 Tools

The **Tools** tab displays two sub-menus:

- **Start and Stop Service**
- **System update**

as shown below.

**Figure 6-81: Tools Page**



## 6.2.5 Start and Stop Service

The Start and Stop Service page appears as shown below:

**Figure 6-82: Start and Stop Service Page**


- **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.

## 6.2.6 System Update

The **System Update** menu provides the ability to:

- Update the GUI software via a ZIP file
- Install an update as an MSU file from Microsoft

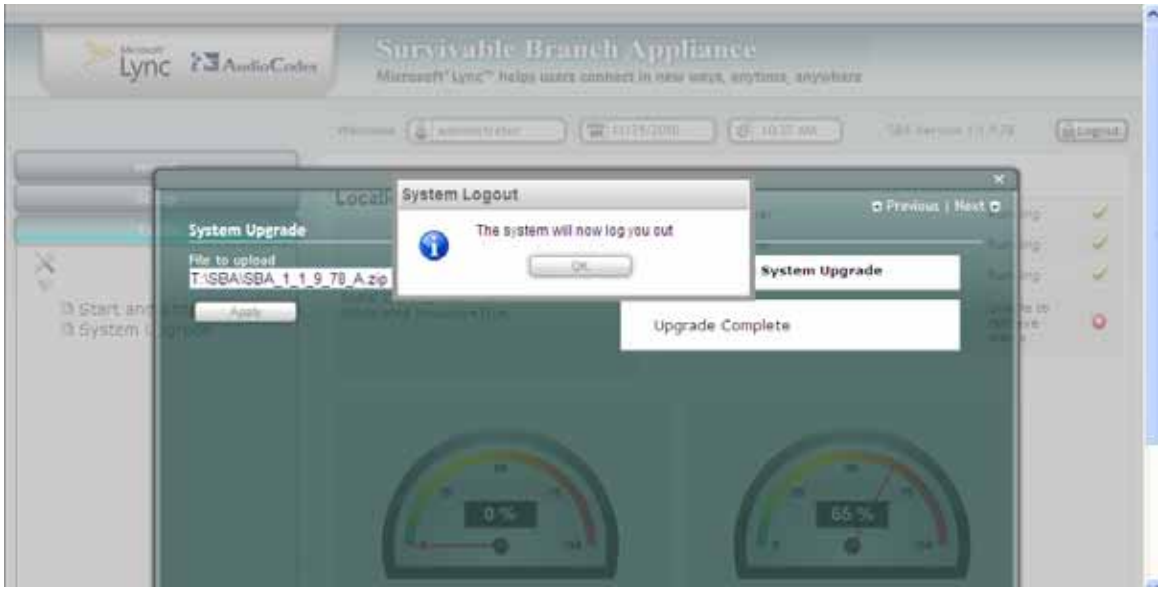
➢ **To perform a system update:**

1. Click **Browse** and select the file to upload.
2. Click **Apply**.

**Figure 6-83: System Update Page**


3. The following message appears.

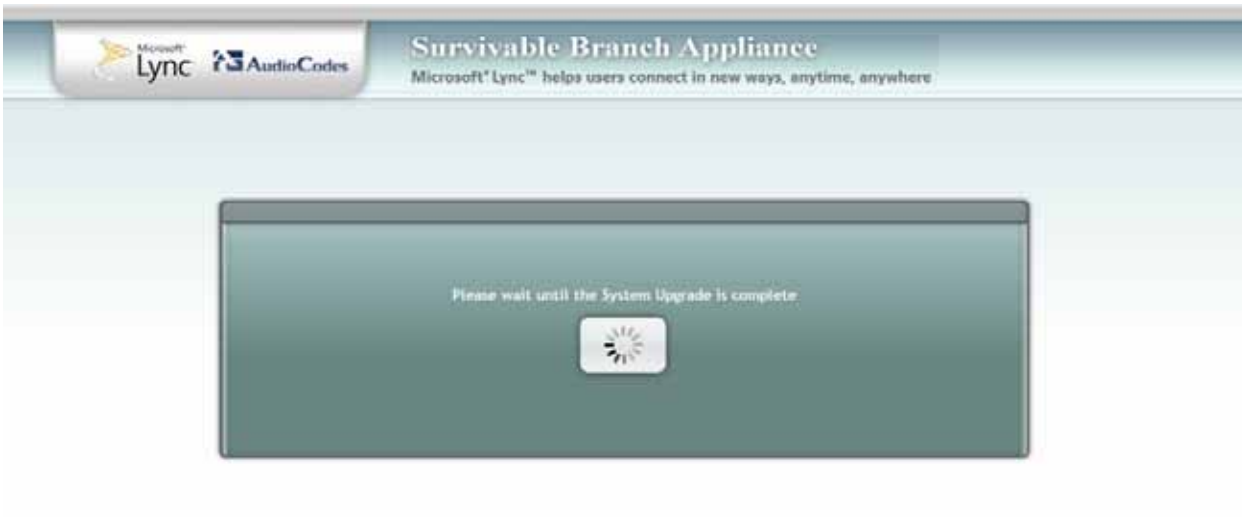
**Figure 6-84: System Logout Message**




4. Click **OK**.

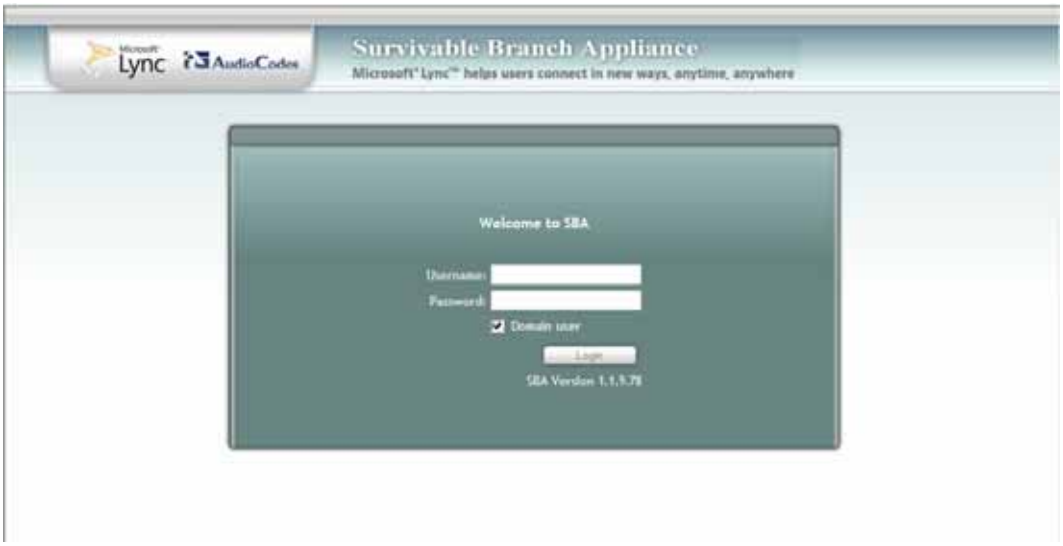
5. The following message is displayed to inform you that you need to wait till the update has been completed.

**Figure 6-85: "Please Wait" Message**




6. The following Login page appears.If you update the GUI software, you will see the new version number on this login page.

**Figure 6-86: Login Page with New Version Number**



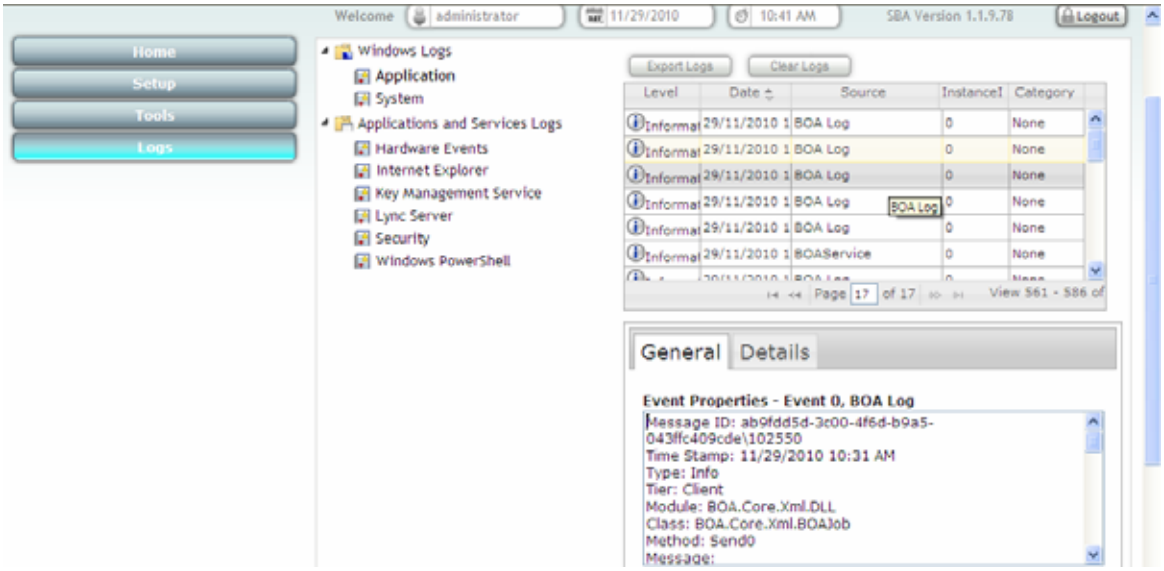
## 6.2.7 Logs

The Log page displays the Server Event Viewer log as shown in the figure below.

**Figure 6-87: Logs Page**


1. To delete a log, click on the event to view the detailed log section. You can also clear or export the logs.These two operations work only on the active log section.

**Figure 6-88: Detailed Log Page**




## 6.2.8 Logout

The Logout option logs you out from the application.

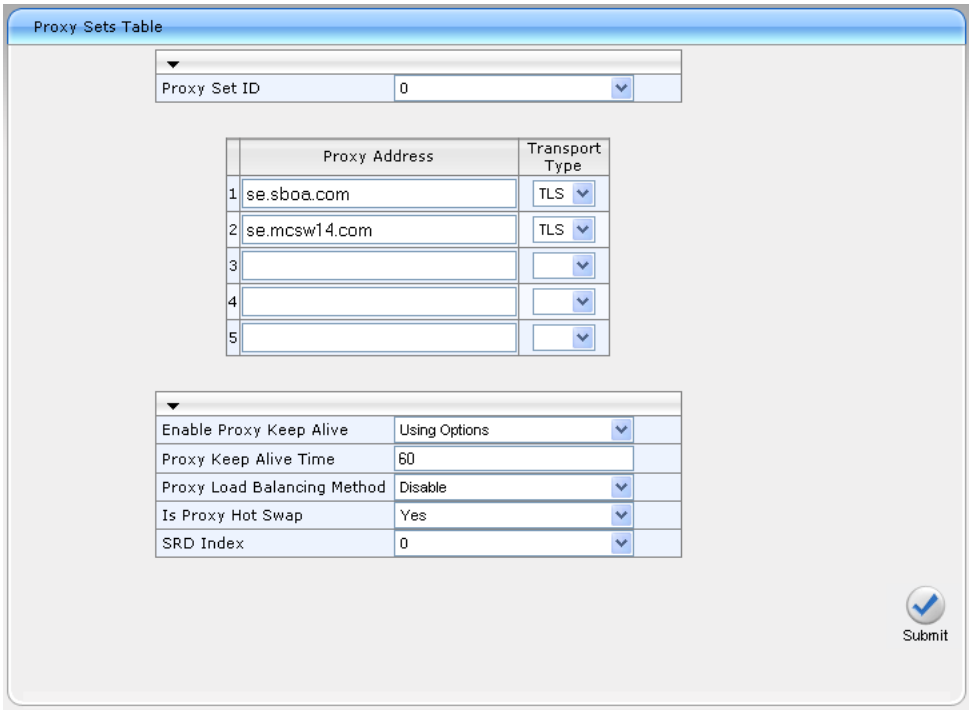
# 6.3 Configuring SBA Media Gateway

Once the SBA application is installed and configured as described in the previous sub-section, you can begin configuring the SBA media gateway as described below.

➢ **To configure the SBA Media Gateway:**

1. Connect to the OSN/SBC (refer to Section 3.2), and then complete the on-site/on-domain SBA application installation.
2. **Configure the SBA Media Gateway:** Since the SBA application is running the Mediation Server, most of the configuration of the Enhanced Media Gateway described in Section 4 also applies to the SBA Media Gateway deployed at the branch office.
   a. **Exception 1:** The DNS load balancing configuration is not required as this functionality interfaces with only one Mediation Server which is co-located on the same hardware chassis as the SBA Media Gateway. Therefore, follow the procedures in Section 4, but skip Step 9 of Section 4.1.
   b. **Exception 2:** According to the SBA specification, if the SBA application fails, the SBA Media Gateway must switchover to the Mediation Server at the Data Center. Therefore, you should configure the Proxy Sets Table (refer to Section 4.1) with two proxies:
      - **Index 1:** The IP address/FQDN of the Mediation Server running on the SBA.
      - **Index 2:** The IP address/FQDN of the Mediation Server running at the Data Center.

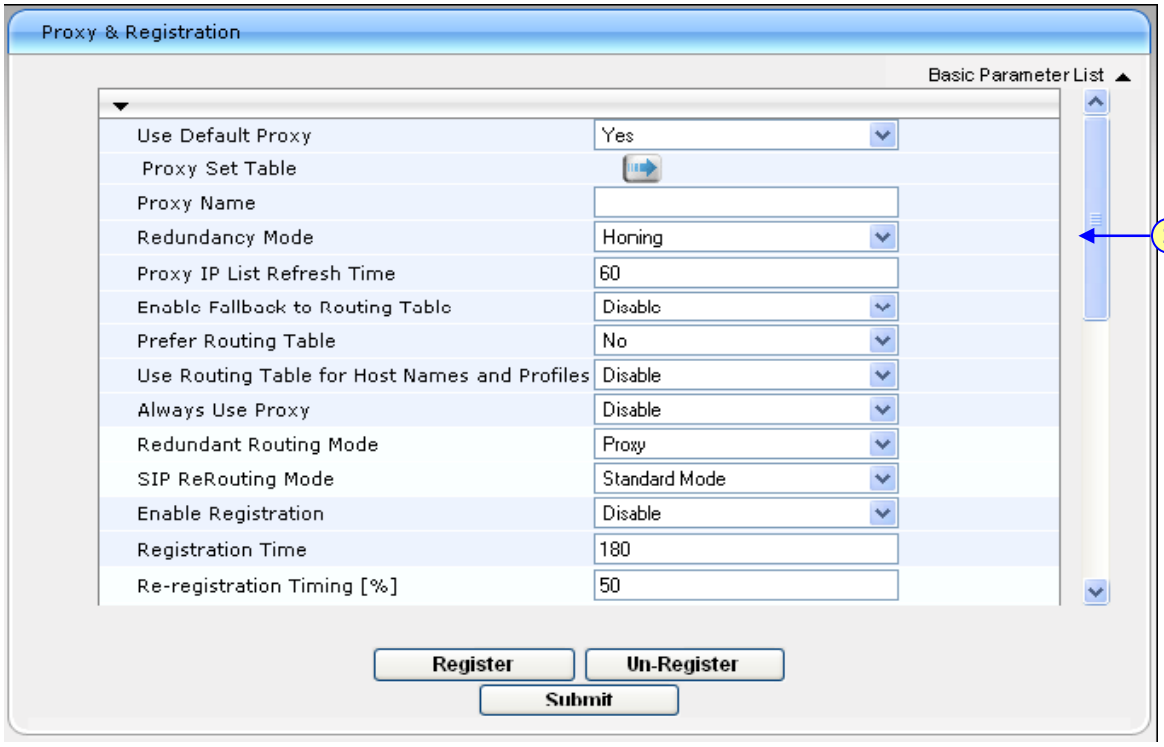
**Figure 6-89: Defining Proxy Sets for SBA Media Gateway**




   c. **Exception 3:** If the SBA application fails and the Media Gateway switches over to the Mediation Server at the Data Center, when the SBA application resumes functionality, the Gateway should switch back the Mediation Service on the SBA application. Therefore, the **Homing** mode should be configured on the gateway.

3. Open the '**Proxy & Registration**' page (**Configuration** tab > **Protocol Configuration** menu > **Proxies/IpGroups/Registration** submenu > **Proxy & Registration**), and configure the 'Redundancy Mode' parameter to '**Homing**'.

**Figure 6-90: Defining Homing Mode for SBA Media Gateway**



## Reader's Notes

# Installation and Configuration Manual Ver. 1.3

www.audiocodes.com