

Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Avaya Aura™ Session Manager and Nortel CS1000 with
Vodafone SIP Trunk using Mediant E-SBC



AVAYA



July 2014

Document # LTRT-38130

 **AudioCodes**

Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	AudioCodes E-SBC Version	9
2.2	Vodafone SIP Trunking Version.....	9
2.3	Avaya Aura Version.....	9
2.4	Interoperability Test Topology	10
2.4.1	Environment Setup	11
2.4.2	Known Limitations.....	11
3	Configuring AudioCodes E-SBC.....	13
3.1	Step 1: IP Network Interfaces Configuration	14
3.1.1	Step 1a: Configure VLANs.....	15
3.1.2	Step 1b: Configure Network Interfaces.....	15
3.1.3	Step 1c: Configure the Native VLAN ID.....	17
3.2	Step 2: Enable the SBC Application	17
3.3	Step 3: Signaling Routing Domains Configuration	18
3.3.1	Step 3a: Configure Media Realms.....	18
3.3.2	Step 3b: Configure SRDs	20
3.3.3	Step 3c: Configure SIP Signaling Interfaces	22
3.4	Step 4: Configure Proxy Sets	23
3.5	Step 5: Configure IP Groups.....	25
3.6	Step 6: Configure IP Profiles	26
3.7	Step 7: Configure Maximum IP Media Channels	31
3.8	Step 8: Configure IP-to-IP Call Routing Rules	32
3.9	Step 9: Configure IP-to-IP Manipulation Rules.....	38
3.10	Step 10: Configure Message Manipulation Rules	40
3.11	Step 11: Miscellaneous Configuration.....	45
3.11.1	Step 11a: Configure Max-Forwards.....	45
3.12	Step 12: Reset the E-SBC	46
A	AudioCodes INI File	48
B	Configuring Avaya Session Manager.....	56

This page is intentionally left blank

Notice

This document describes how to connect the Avaya Session Manager and the Nortel CS1000 with Vodafone SIP Trunk using AudioCodes Mediant E-SBC product series.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published, nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2014 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: July-24-2014

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

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

Customer Support

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

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at <http://www.audiocodes.com/downloads>.

This page is intentionally left blank

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between Vodafone's SIP Trunk and Avaya Aura environment.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Vodafone Partners who are responsible for installing and configuring Vodafone's SIP Trunk and Avaya's Aura for VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

AudioCodes' family of E-SBC devices enables reliable connectivity and security between the Enterprise's and the service provider's VoIP networks.

The E-SBC provides perimeter defense as a way of protecting Enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the E-SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security and manageability. The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes E-SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware.

This page is intentionally left blank

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none"> ▪ Mediant 500 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC
Software Version	SIP_6.80A.227.005
Protocol	<ul style="list-style-type: none"> ▪ SIP/UDP (to the Vodafone SIP Trunk) ▪ SIP/UDP (to the Avaya Session Manager)
Additional Notes	None

2.2 Vodafone SIP Trunking Version

Table 2-2: Vodafone Version

Vendor/Service Provider	Vodafone
SSW Model/Service	
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Avaya Aura Version

Table 2-3: Avaya Aura Version

Vendor	Avaya/Nortel
Model	CS1000/SM
Software Version	Nortel CS 1000: SIP GW release_7.0 version_ssLinux-7.65.16 Avaya Session Manager : AVAYA-SM-6.3.6.0.636005
Protocol	SIP
Additional Notes	

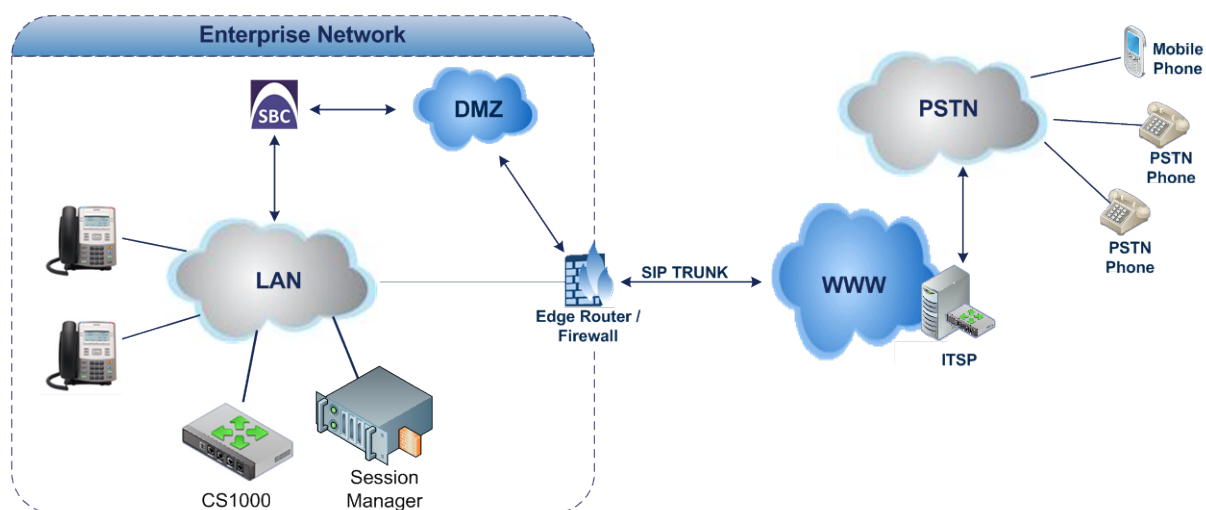
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and Vodafone SIP Trunk with Avaya Aura was done using the following topology setup:

- Enterprise deployed with Nortel CS1000 and Avaya Session Manager in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to connect the Enterprise to the PSTN network using Vodafone's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
 - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
 - **Border:** IP-to-IP network border between Avaya network in the Enterprise LAN and Vodafone's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between E-SBC and Avaya Aura with Vodafone SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	<ul style="list-style-type: none">▪ Avaya Aura environment is located on the Enterprise's LAN▪ Vodafone SIP Trunk is located on the WAN
Signaling Transcoding	<ul style="list-style-type: none">▪ Avaya Aura operates with SIP-over-UDP transport type▪ Vodafone SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	<ul style="list-style-type: none">▪ Avaya Aura supports G.711A-law and G.711U-law coders▪ Vodafone SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	<ul style="list-style-type: none">▪ Avaya Aura operates with RTP media type▪ Vodafone SIP Trunk operates with RTP media type

2.4.2 Known Limitations

The section described in this document describes the limitation that occurred in the Interoperability test plan:

- **Force Transcoding** is enabled on the E-SBC; meaning that the device's SBC application interworks the media by implementing DSP transcoding. This feature enabled due to that Vodafone SIP trunk expects to receive the first incoming RTP packet from the IP PBX. This issue occurs in a Call Forward Scenario to a PSTN Number. The Forwarder IP Phone isn't responsible for passing the RTP, so it is sent out from the SBC that closes the RTP path within it.

This page is intentionally left blank

3 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Avaya Aura and the Vodafone SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- E-SBC WAN interface - Vodafone SIP Trunking environment
- E-SBC LAN interface - Avaya environment

This configuration is done using the E-SBC's embedded Web server (hereafter, referred to as *Web interface*).

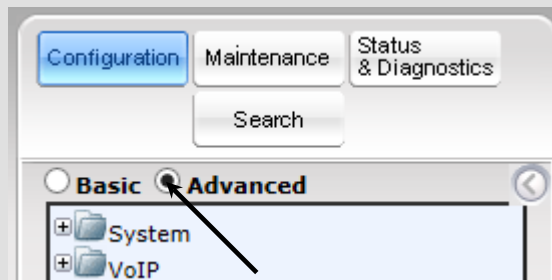
Notes:

- For implementing Avaya Aura and Vodafone SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:

- ✓ **SBC**
- ✓ **Security**
- ✓ **DSP**
- ✓ **RTP**
- ✓ **SIP**

For more information about the Software License Key, contact your AudioCodes sales representative.

- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the Avaya environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document.
- Before you begin configuring the E-SBC, ensure that the E-SBC's Web interface Navigation tree is in Full-menu display mode. To do this, select the **Full** option, as shown below:



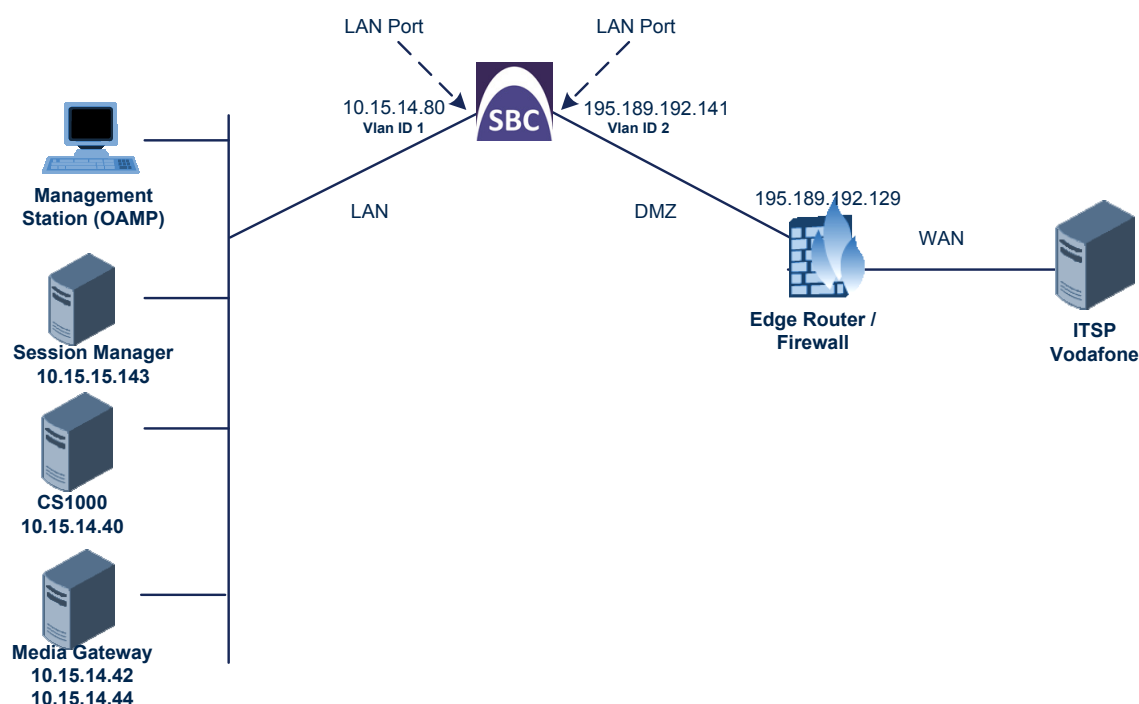
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

3.1 Step 1: IP Network Interfaces Configuration

This step describes how to configure the E-SBC's IP network interfaces. There are several ways to deploy the E-SBC; however, this interoperability test topology employs the following deployment method:

- E-SBC interfaces with the following IP entities:
 - Avaya servers, located on the LAN
 - Vodafone SIP Trunk, located on the WAN
- E-SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In the interoperability test topology, E-SBC connects to the LAN and WAN using dedicated LAN ports (i.e., two ports and two network cables are used).
- E-SBC also uses two logical network interfaces:
 - LAN (VLAN ID 1)
 - WAN (VLAN ID 2)

Figure 3-1: Network Interfaces in Interoperability Test Topology



3.1.1 Step 1a: Configure VLANs

This step describes how to define VLANs for each of the following interfaces:

- LAN VoIP (assigned the name "Voice-LAN")
- WAN VoIP (assigned the name "X2-LAN")

➤ **To configure the VLANs:**

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).
2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side as follows:

Parameter	Value
Index	1
VLAN ID	2
Underlying Interface	GROUP_2 (Ethernet port group)
Name	vlan 2

Figure 3-2: Configured VLAN IDs in Ethernet Device Table

Index	VLAN ID	Underlying Interface	Name
0	1	GROUP_1	vlan 1
1	2	GROUP_2	vlan 2

3.1.2 Step 1b: Configure Network Interfaces

This step describes how to configure the IP network interfaces for each of the following interfaces:

- LAN VoIP (assigned the name "Voice-LAN")
- WAN VoIP (assigned the name "X2-LAN")

➤ **To configure the IP network interfaces:**

1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
2. Modify the existing LAN network interface:
 - a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.

- b. Configure the interface as follows:

Parameter	Value
IP Address	10.15.14.80 (IP address of E-SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Gateway	10.15.0.1
Interface Name	Voice-LAN (arbitrary descriptive name)
Primary DNS Server IP Address	10.15.25.1
Underlying Device	vlan 1

3. Add a network interface for the WAN side:

- a. Enter **1**, and then click **Add Index**.

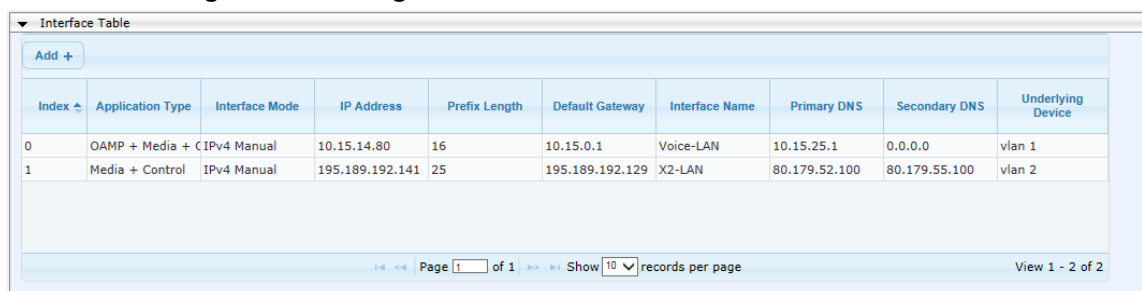
- b. Configure the interface as follows:

Parameter	Value
Application Type	Media + Control
IP Address	195.189.192.141 (WAN IP address)
Prefix Length	25 (for 255.255.255.128)
Gateway	195.189.192.129 (router's IP address)
Interface Name	X2-LAN
Primary DNS Server IP Address	0.0.0.0
Secondary DNS Server IP Address	0.0.0.0
Underlying Device	vlan 2

4. Click **Apply**, and then **Done**.

The configured IP network interfaces are shown below:

Figure 3-3: Configured Network Interfaces in IP Interfaces Table



Interface Table									
Add +									
Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media + C	IPv4 Manual	10.15.14.80	16	10.15.0.1	Voice-LAN	10.15.25.1	0.0.0.0	vlan 1
1	Media + Control	IPv4 Manual	195.189.192.141	25	195.189.192.129	X2-LAN	80.179.52.100	80.179.55.100	vlan 2

Page 1 of 1 Show 10 records per page View 1 - 2 of 2

3.1.3 Step 1c: Configure the Native VLAN ID

This step describes how to configure the Native VLAN ID for the LAN and WAN interfaces.

➤ **To configure the Native VLAN ID for the IP network interfaces:**

1. Open the Physical Ports Settings page (**Configuration** tab > **VoIP** menu > **Network** > **Physical Ports Table**).
2. For the **GROUP_1** member ports, set the 'Native Vlan' field to **1**. This VLAN was assigned to network interface "Voice-LAN".
3. For the **GROUP_2** member ports, set the 'Native Vlan' field to **2**. This VLAN was assigned to network interface "X2-LAN".

Figure 3-4: Configured Port Native VLAN

Physical Ports Settings							
Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_4_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_4_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
2	GE_4_3	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
3	GE_4_4	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant

3.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➤ **To enable the SBC application:**

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

Figure 3-5: Enabling SBC Application

⚡ SAS Application	Disable
⚡ SBC Application	Enable
⚡ IP to IP Application	Disable

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 3.12 on page 46).

3.3 Step 3: Signaling Routing Domains Configuration

This step describes how to configure Signaling Routing Domains (SRD). The SRD represents a logical VoIP network. Each logical or physical connection requires an SRD, for example, if the E-SBC interfaces with both the LAN and WAN, a different SRD would be required for each one.

The SRD is composed of the following:

- Media Realm: defines a UDP port range for RTP/SRTP (media) traffic on a specific logical IP network interface of the E-SBC.
- SIP Interface: defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface of the E-SBC.

3.3.1 Step 3a: Configure Media Realms

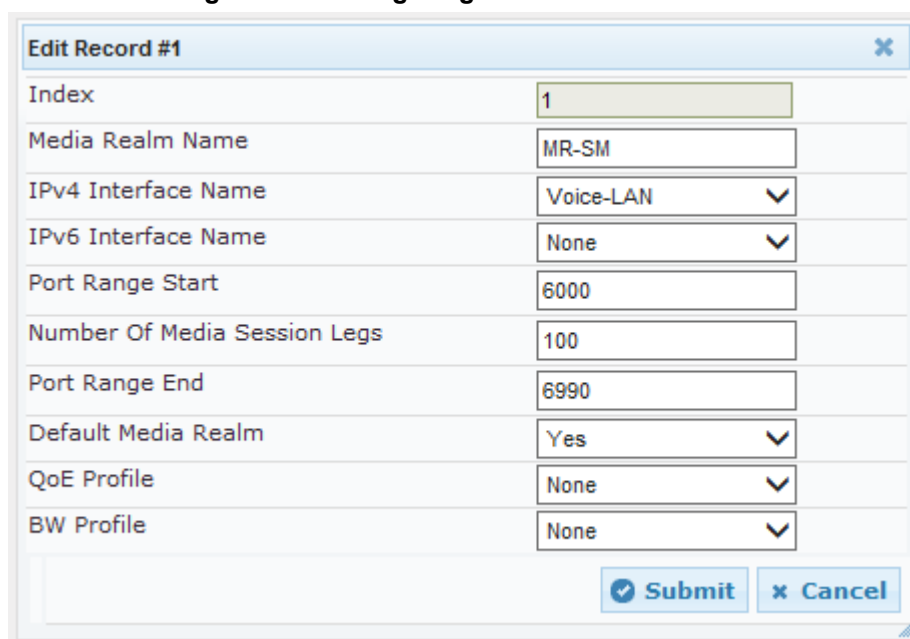
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➤ To configure Media Realms:

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
2. Modify the existing Media Realm for LAN traffic:

Parameter	Value
Index	0
Media Realm Name	MR-SM (descriptive name)
IPv4 Interface Name	Voice-LAN
Port Range Start	6000 (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 3-6: Configuring Media Realm for LAN



Edit Record #1	
Index	1
Media Realm Name	MR-SM
IPv4 Interface Name	Voice-LAN
IPv6 Interface Name	None
Port Range Start	6000
Number Of Media Session Legs	100
Port Range End	6990
Default Media Realm	Yes
QoE Profile	None
BW Profile	None
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Media Realm Name	MR-VF (arbitrary name)
IPv4 Interface Name	X2-LAN
Port Range Start	7000 (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 3-7: Configuring Media Realm for WAN

Edit Record #2

Index	2
Media Realm Name	MR-VF
IPv4 Interface Name	X2-LAN
IPv6 Interface Name	None
Port Range Start	7000
Number Of Media Session Legs	100
Port Range End	7990
Default Media Realm	No
QoE Profile	None
BW Profile	None

The configured Media Realms are shown in the figure below:

Figure 3-8: Configured Media Realms in Media Realm Table

Media Realm Table

Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
1	MR-SM	Voice-LAN	None
2	MR-VF	X2-LAN	None

Page 1 of 1 Show 10 records per page View 1 - 2 of 2

3.3.2 Step 3b: Configure SRDs

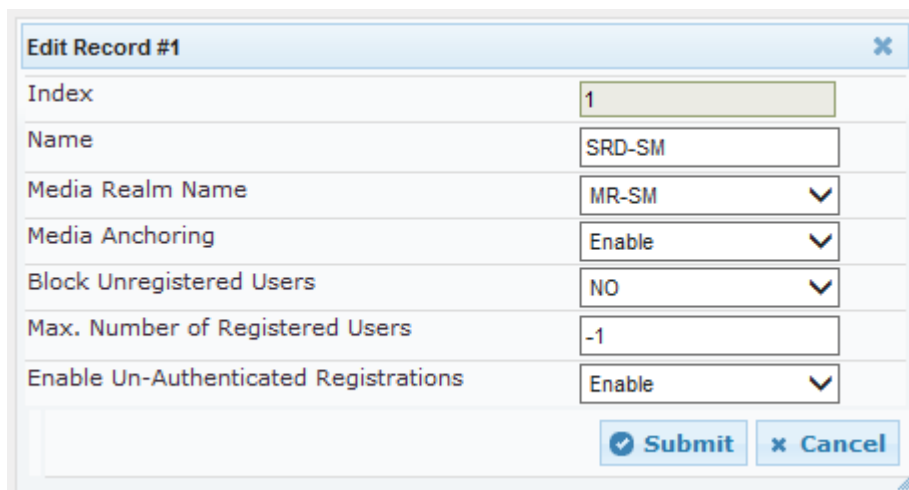
This step describes how to configure the SRDs. You create two SRDs, one for the E-SBC's internal interface and one for the E-SBC's external interface.

➤ **To configure SRDs:**

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SRD Table**).
2. Configure an SRD for the E-SBC's internal interface (toward Avaya SM):

Parameter	Value
SRD Index	1
SRD Name	SRD-SM (descriptive name for SRD)
Media Realm	MR-SM (associates SRD with Media Realm)

Figure 3-9: Configuring LAN SRD



Edit Record #1	
Index	1
Name	SRD-SM
Media Realm Name	MR-SM
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure an SRD for the E-SBC's external interface (toward the Vodafone SIP Trunk):

Parameter	Value
SRD Index	2
SRD Name	SRD-VF
Media Realm	MR-VF

Figure 3-10: Configuring WAN SRD

Edit Record #2

Index	2
Name	SRD-VF
Media Realm Name	MR-VF
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable

The configured SRDs are shown in the figure below:

Figure 3-11: Configured SRDs in SRD Table

SRD Table

Index	Name	Media Realm Name	Media Anchoring
1	SRD-SM	MR-SM	Enable
2	SRD-VF	MR-VF	Enable

Page 1 of 1 Show 10 records per page View 1 - 2 of 2

3.3.3 Step 3c: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, an internal and external SIP Interface must be configured for the E-SBC.

➤ **To configure SIP Interfaces:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Configure a SIP interface for the LAN:

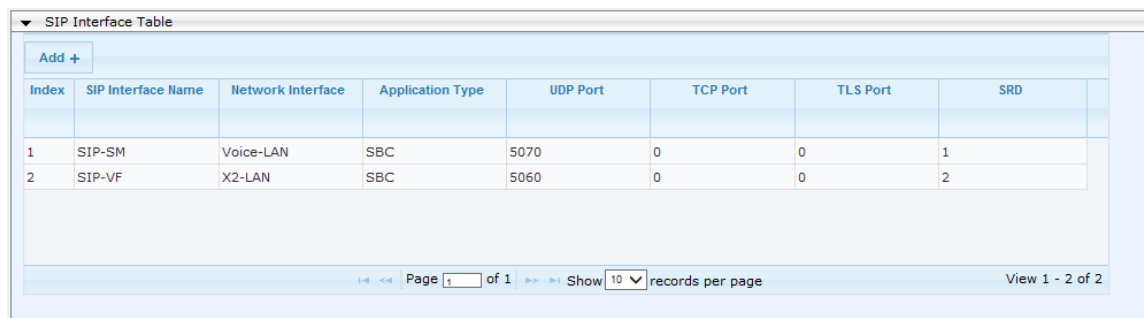
Parameter	Value
Index	1
Interface Name	SIP-SM (arbitrary descriptive name)
Network Interface	Voice
Application Type	SBC
UDP Port	5070
TCP and TLS	0
SRD	1

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	2
Interface Name	SIP-VF (arbitrary descriptive name)
Network Interface	X2-LAN
Application Type	SBC
UDP Port	5060
TCP and TLS	0
SRD	2

The configured SIP Interfaces are shown in the figure below:

Figure 3-12: Configured SIP Interfaces in SIP Interface Table



SIP Interface Table							
Add +							
Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	SIP-SM	Voice-LAN	SBC	5070	0	0	1
2	SIP-VF	X2-LAN	SBC	5060	0	0	2

Page 1 of 1 Show 10 records per page View 1 - 2 of 2

3.4 Step 4: Configure Proxy Sets

This step describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- Avaya Aura
- Vodafone SIP Trunk

These Proxy Sets will later be associated with IP Groups.

➤ To configure Proxy Sets:

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Configure a Proxy Set for Avaya SM:

Parameter	Value
Proxy Set ID	1
Proxy Address	10.15.15.143:5070 (Avaya Session Manager IP address / FQDN and destination port)
Transport Type	UDP
Proxy Name	SM (arbitrary descriptive name)
SRD Index	1

Figure 3-13: Configuring Proxy Set for Avaya Aura

Proxy Set ID: 1

	Proxy Address	Transport Type
1	10.15.15.143:5070	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name: SM

Enable Proxy Keep Alive: Disable

3. Configure a Proxy Set for the Vodafone SIP Trunk:

Parameter	Value
Proxy Set ID	2
Proxy Address	212.144.52.96:5060 (Vodafone IP address / FQDN and destination port)
Transport Type	UDP
Proxy Name	Vodafone (arbitrary descriptive name)
SRD Index	2 (enables classification by Proxy Set for SRD of IP Group belonging to Vodafone SIP Trunk)

Figure 3-14: Configuring Proxy Set for Vodafone SIP Trunk

Proxy Set ID
2

	Proxy Address	Transport Type
1	212.144.52.96:5060	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name

SM

Enable Proxy Keep Alive

Disable

Proxy Keep Alive Time

60

KeepAlive Failure responses

- Reset the E-SBC with a burn to flash for these settings to take effect (see Section 3.12 on page 46).

3.5 Step 5: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E-SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. A typical deployment consists of multiple IP Groups associated with the same SRD. For example, you can have two LAN IP PBXs sharing the same SRD, and two ITSPs / SIP Trunks sharing the same SRD. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In this interoperability test topology, IP Groups must be configured for the following IP entities:

- Avaya SM and CS1K located on LAN
- Vodafone SIP Trunk located on WAN

➤ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Configure an IP Group for the Avaya SM and CS1K :

Parameter	Value
Index	1
Type	Server
Description	SM (arbitrary descriptive name)
Proxy Set ID	1
SIP Group Name	etkn.de (according to ITSP requirement)
SRD	1
Media Realm Name	MR-SM
IP Profile ID	1

3. Configure an IP Group for the Vodafone SIP Trunk:

Parameter	Value
Index	2
Type	Server
Description	Vodafone (arbitrary descriptive name)
Proxy Set ID	2
SIP Group Name	vodafone.com (according to ITSP requirement)
SRD	2
Media Realm Name	MR-VF
IP Profile ID	2

The configured IP Groups are shown in the figure below:

Figure 3-15: Configured IP Groups in IP Group Table

IP Group Table					
Add +					
Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User
1	Server	SM	1	etkn.de	
2	Server	VF	2	vodafone.com	
Page 1 of 1 Show 10 records per page View 1 - 2 of 2					

3.6 Step 6: Configure IP Profiles

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

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

- Avaya SM
- Vodafone SIP trunk

Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 3.5 on page 25).

➤ To configure IP Profiles:

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Add**.
3. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Profile Name	SM (arbitrary descriptive name)

Figure 3-16: Configuring IP Profile for Avaya SM – Common Tab

Common	
Index	1
Profile Name	SM
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
RTP Redundancy Depth	0
Echo Canceled	Line
Disconnect on Broken Connection	No
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0
Media IP Version Preference	Only IPv4
Symmetric MKI	Disable
MKI Size	0
Reset SRTP Upon Re-key	Disable
Generate SRTP keys mode	Only If Required
Jitter Buffer Max Delay [msec]	300
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

4. Click the **SBC** tab, and then validate the parameter as follows:

Parameter	Value
Media Security Behavior	As Is

Figure 3-17: Configuring IP Profile for Avaya Aura – SBC Tab

Common GW SBC	
Index	1
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	
Allowed Coders Group ID	None
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction
SBC Media Security Behavior	As Is
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
P-Asserted-Identity	As Is
Diversion Mode	As Is
History-Info Mode	As Is
Fax Coders Group ID	None
Fax Behavior	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
PRACK Mode	Transparent
Session Expires Mode	Transparent
Remote Update Support	Supported
Remote re-INVITE	Supported
Remote Delayed Offer Support	Supported

5. Configure an IP Profile for the Vodafone SIP Trunk:
6. Click **Add**.
7. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Profile Name	VF (arbitrary descriptive name)

Figure 3-18: Configuring IP Profile for Vodafone SIP Trunk – Common Tab

Parameter	Value
Index	2
Profile Name	VF
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
RTP Redundancy Depth	0
Echo Canceler	Line
Disconnect on Broken Connection	Yes
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0
Media IP Version Preference	Only IPv4
Symmetric MKI	Disable
MKI Size	0
Reset SRTP Upon Re-key	Disable
Generate SRTP keys mode	Only If Required
Jitter Buffer Max Delay [msec]	300

Submit Cancel

8. Click the **SBC** tab, and then configure the parameters as follows:

Parameter	Value
Transcoding Mode	Force (this parameter is required to send first RTP packet towards VF SIPT)
Media Security Behavior	As Is
Remote Update Support	Supported Only After Connect (this parameter is required by the VF SIPT)

Figure 3-19: Configuring IP Profile for Vodafone SIP Trunk – SBC Tab

Common GW SBC	
Index	2
Extension Coders Group ID	None ▼
Transcoding Mode	Force ▼
Allowed Media Types	
Allowed Coders Group ID	None ▼
Allowed Video Coders Group ID	None ▼
Allowed Coders Mode	Restriction ▼
SBC Media Security Behavior	As Is ▼
RFC 2833 Behavior	As Is ▼
Alternative DTMF Method	As Is ▼
P-Asserted-Identity	As Is ▼
Diversion Mode	As Is ▼
History-Info Mode	As Is ▼
Fax Coders Group ID	None ▼
Fax Behavior	As Is ▼
Fax Offer Mode	All coders ▼
Fax Answer Mode	Single coder ▼
PRACK Mode	Transparent ▼
Session Expires Mode	Transparent ▼
Remote Update Support	Supported Only After ▼
Remote re-INVITE	Supported ▼

3.7 Step 7: Configure Maximum IP Media Channels

This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.



Note: This step is required due to the **Force Transcoding** parameter setting in the Vodafone IP Profile.

➤ **To configure the maximum number of IP media channels:**

1. Open the IP Media Settings page (**Configuration** tab > **VoIP** menu > **IP Media** > **IP Media Settings**).

Figure 3-20: Configuring Number of IP Media Channels

⚡ Number of Media Channels	30
⚡ Voice Streaming	Disable
NetAnn Announcement ID	annc
MSCML ID	ivr
Transcoding ID	trans

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 3.12 on page 46).

3.8 Step 8: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 3.5 on page 25, IP Group 1 represents Avaya Aura, and IP Group 2 represents Vodafone SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Avaya Aura (LAN) and Vodafone SIP Trunk (WAN):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Avaya Aura to Vodafone SIP Trunk
- Calls from Vodafone SIP Trunk to Avaya Aura

➤ To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:
3. Click **Add**.
4. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	0
Route Name	OPTIONS termination (arbitrary descriptive name)
Source IP Group ID	1
Request Type	OPTIONS
Destination Type	Dest Address
Destination Address	internal

Figure 3-21: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab

The screenshot shows the 'Rule' tab of a configuration window. The 'Rule' tab is selected, and the 'Action' tab is also visible. The configuration parameters are as follows:

Parameter	Value
Index	0
Route Name	OPTIONS termination
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any

At the bottom right, there are 'Submit' and 'Cancel' buttons.

5. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 3-22: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab

The screenshot shows the 'Action' tab of the configuration window. The 'Rule' tab is also visible. The configuration parameters are as follows:

Parameter	Value
Index	0
Destination Type	Dest Address
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	internal
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None
Rules Set Id	-1

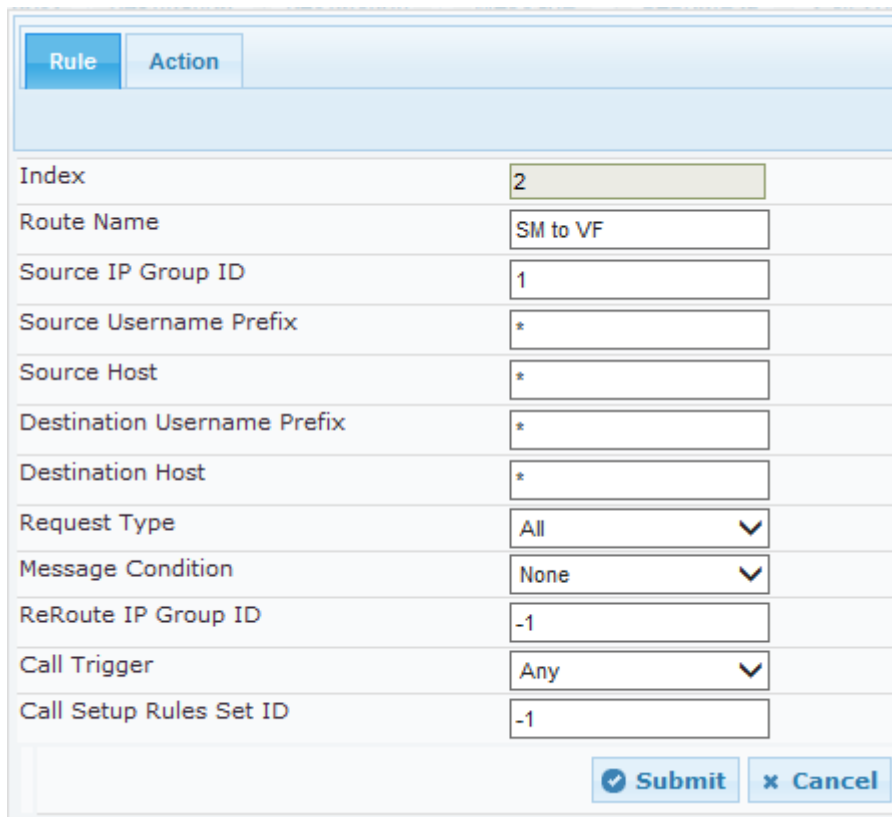
At the bottom right, there are 'Submit' and 'Cancel' buttons.

6. Configure a rule to route calls from Avaya Aura to Vodafone SIP Trunk:
 7. Click **Add**.

8. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	SM to VF (arbitrary descriptive name)
Source IP Group ID	1

Figure 3-23: Configuring IP-to-IP Routing Rule for SM to VF – Rule tab



Rule	Action
Index	2
Route Name	SM to VF
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

Submit Cancel

9. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	2
Destination SRD ID	2

Figure 3-24: Configuring IP-to-IP Routing Rule for SM to VF – Action tab

Index	1
Destination Type	IP Group
Destination IP Group ID	2
Destination SRD ID	2
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None
Rules Set Id	-1

10. Configure a rule to route calls from Vodafone SIP Trunk to Avaya Aura:
11. Click **Add**.
12. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	VF to SM (arbitrary descriptive name)
Source IP Group ID	2

Figure 3-25: Configuring IP-to-IP Routing Rule for VF to SM – Rule tab

Rule	Action
Index	5
Route Name	VF to SM
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

13. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	1
Destination SRD ID	1

Figure 3-26: Configuring IP-to-IP Routing Rule for VF to SM – Action tab

Rule		Action	
Index	2		
Destination Type	IP Group		
Destination IP Group ID	1		
Destination SRD ID	1		
Destination Address			
Destination Port	0		
Destination Transport Type			
Alternative Route Options	Route Row		
Group Policy	None		
Cost Group	None		
Rules Set Id	-1		
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>			

The configured routing rules are shown in the figure below:

Figure 3-27: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing Table										
Add +		Insert +								
Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Call Setup Rules Set ID	Destination Type	Destination SRD ID
1	Terminate Opti	*	*	*	None	-1	Any	-1	Dest Address	None
2	SM to VF	*	*	*	None	-1	Any	-1	IP Group	2
3	VF to SM	*	*	*	None	-1	Any	-1	IP Group	1

Page 1 of 1 Show 10 records per page View 1 - 3 of 3



Note: The routing configuration may change according to your specific deployment topology.

3.9 Step 9: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 3.5 on page 25, IP Group 1 represents Avaya environment, and IP Group 2 represents Vodafone SIP Trunk.



Note: Adapt the manipulation table according to your environment dial plan.

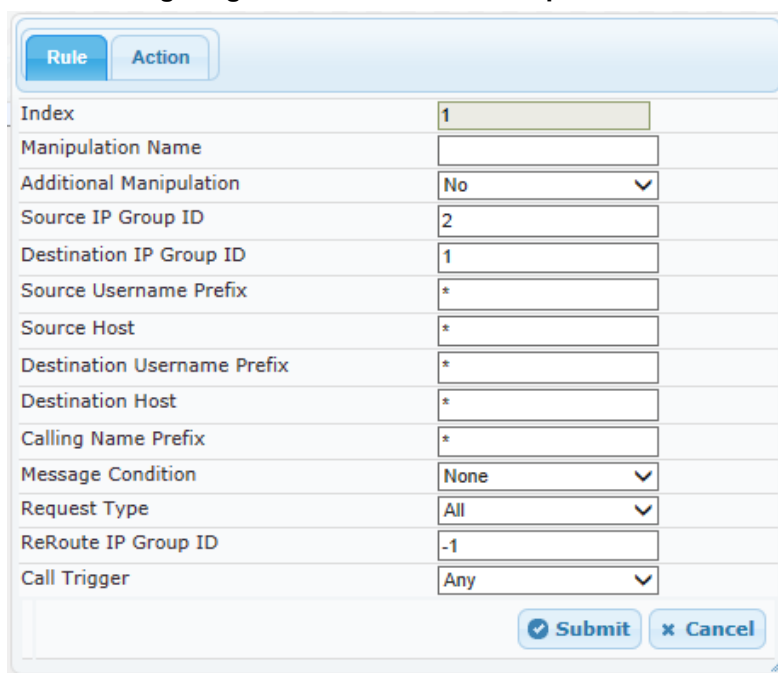
For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from IP Group 2 (Vodafone SIP Trunk) to IP Group 1 (i.e., Avaya CS1K) for any destination username prefix.

➤ To configure a number manipulation rule:

1. Open the IP-to-IP Outbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC > Manipulations SBC > IP-to-IP Outbound**).
2. Click **Add**.
3. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Source IP Group	2
Destination IP Group	1
Destination Username Prefix	* (asterisk sign)

Figure 3-28: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



Rule	
Index	1
Manipulation Name	
Additional Manipulation	No
Source IP Group ID	2
Destination IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Calling Name Prefix	*
Message Condition	None
Request Type	All
ReRoute IP Group ID	-1
Call Trigger	Any

Submit Cancel

4. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)

Figure 3-29: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

5. Click **Submit**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between IP Group 1 (i.e., Avaya Aura) and IP Group 2 (i.e., Vodafone SIP Trunk):

Figure 3-30: Example of Configured IP-to-IP Outbound Manipulation Rules

IP to IP Outbound Manipulation												
Index	Manipulation Name	Additional Manipulation	Source IP Group ID	Destination IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Request Type	Manipulated Item	Prefix to Add	Suffix to Add
1		No	2	1	*	*	*	*	All	Destination	+	
2		No	1	2	*	*	+	*	All	Destination		
3		No	1	2	+	*	*	*	All	Source URI		

Page 1 of 1 Show 10 records per page View 1 - 3 of 3

Rule Index	Description
1	Calls from IP Group 2 to IP Group 1 with any destination number (*), add "+" to the prefix of the destination number.
2	Calls from IP Group 1 to IP Group 2 with the prefix destination number "+", remove "+" from this prefix.
3	Calls from IP Group 1 to IP Group 2 with source number prefix "+", remove the "+" from this prefix.

3.10 Step 10: Configure Message Manipulation Rules

This step describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

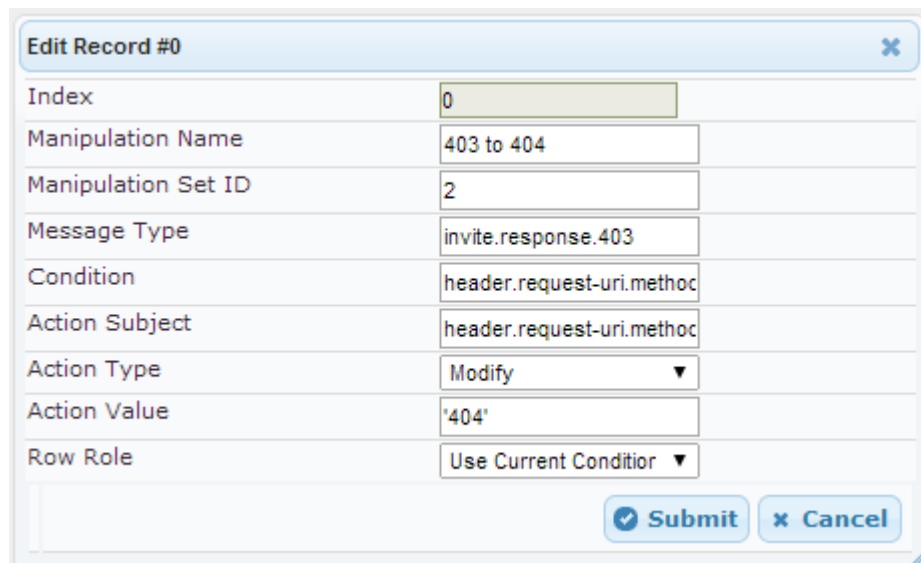
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

➤ **To configure SIP message manipulation rule:**

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure manipulation rule (Manipulation Set 0) for Vodafone SIP Trunk. This rule is applied to response messages sent to the Vodafone SIP Trunk (IP Group 2) for Rejected Calls initiated by the Avaya CS1K (IP Group 1). This replaces the method type '403' with the value '404', because Vodafone SIP Trunk retransmits '403' method type when the call originates from an international source.

Parameter	Value
Index	0
Manipulation Set ID	2
Message Type	Invite.response.403
Condition	header.request-uri.methodtype=='403'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'404'
Row Role	Use Current Condition

Figure 3-31: Configuring SIP Message Manipulation Rule 0 (for Vodafone SIP Trunk)



Edit Record #0	
Index	0
Manipulation Name	403 to 404
Manipulation Set ID	2
Message Type	invite.response.403
Condition	header.request-uri.methoc
Action Subject	header.request-uri.methoc
Action Type	Modify
Action Value	'404'
Row Role	Use Current Condition
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure another manipulation rule (Manipulation Set 2) from Vodafone SIP Trunk. This rule is applied to incoming Options messages received from the Vodafone SIP Trunk (IP Group 2) in an Active Calls. This replaces the method type '18' (i.e., Options) with the value '18' (i.e., Update) to avoid the E-SBC to terminate those Options.

Parameter	Value
Index	2
Manipulation Set ID	2
Message Type	Options
Condition	header.request-uri.methodtype=='8'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'18'
Row Role	Use Current Condition

Figure 3-32: Configuring SIP Message Manipulation Rule 2 (from Vodafone SIP Trunk)

The screenshot shows a web-based configuration interface for SIP Message Manipulation Rule 2. The dialog box is titled 'Edit Record #2'. It contains the following fields and values:

- Index: 2
- Manipulation Name: Options to Update
- Manipulation Set ID: 2
- Message Type: Options
- Condition: header.request-uri.methodtype=='8'
- Action Subject: header.request-uri.methodtype
- Action Type: Modify (selected from a dropdown)
- Action Value: '18'
- Row Role: Use Current Condition (selected from a dropdown)

At the bottom right, there are two buttons: 'Submit' and 'Cancel'.

4. Configure another manipulation rule (Manipulation Set 1) to Avaya CS1K. This rule is applied to above messages manipulation sent from the Vodafone SIP Trunk (IP Group 2) for Options type messages. This replaces the method type '18' (i.e., Update) back to the value '8' (i.e., Options).

Parameter	Value
Index	3
Manipulation Set ID	1
Message Type	Update
Condition	header.request-uri.methodtype=='18'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'8'
Row Role	Use Current Condition

Figure 3-33: Configuring SIP Message Manipulation Rule 3 (for CS1K)

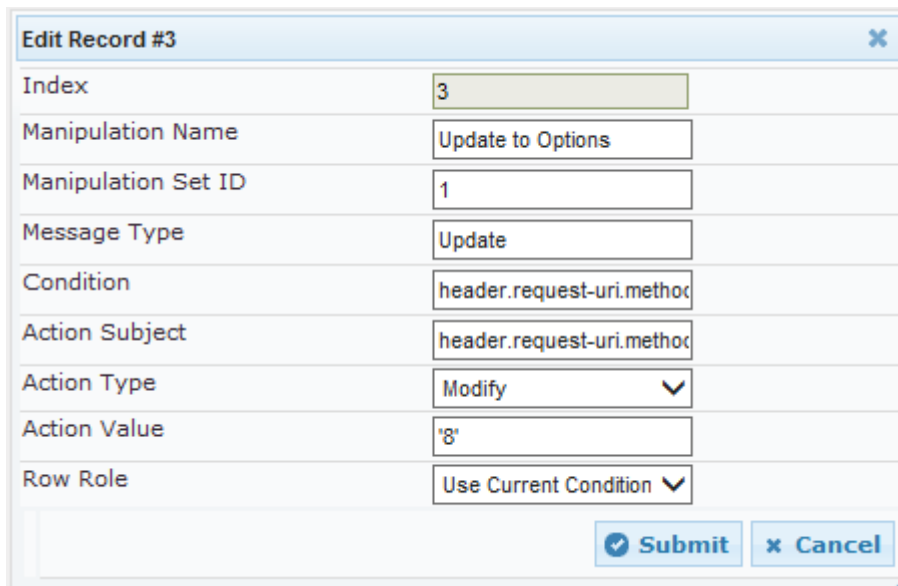
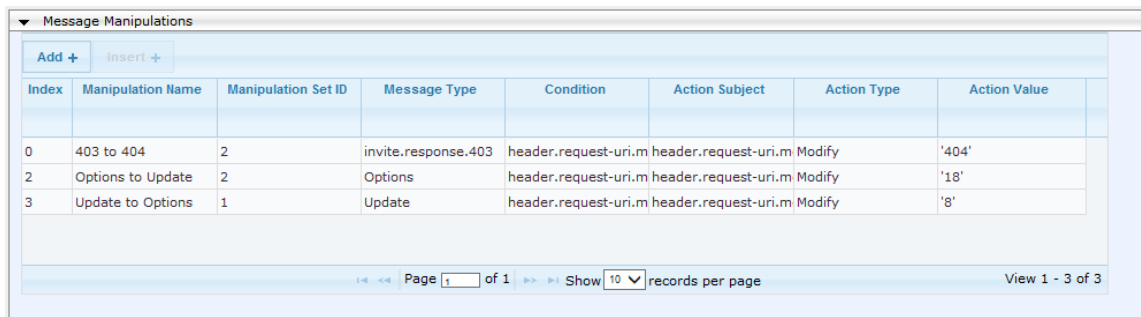


Figure 3-34: Configured SIP Message Manipulation Rules



Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0	403 to 404	2	invite.response.403	header.request-uri.m header.request-uri.m	Modify		'404'
2	Options to Update	2	Options	header.request-uri.m header.request-uri.m	Modify		'18'
3	Update to Options	1	Update	header.request-uri.m header.request-uri.m	Modify		'8'

The table displayed below includes SIP message manipulation rules which are bound together by commonality via the Manipulation Set IDs (Manipulation Set IDs 1, 2) which are executed for messages sent to and from the Vodafone SIP Trunk (IP Group 2) as well as the Avaya CS1K (IP Group 1). These rules are specifically required to enable proper interworking between Vodafone SIP Trunk and Avaya CS1K. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Message Manipulation Rules

Rule Index	Reason	Description
0	Vodafone SIP Trunk doesn't disconnect the call immediately when responded with '403' method type.	This rule is applied to response messages sent to the Vodafone SIP Trunk (IP Group 2) for Unregistered Phone. This replaces the method type '403' with the value '404'.
2	Vodafone SIP Trunk sends Options every 60 seconds in a live call. To avoid this termination on the E-SBC need to convert those Options messages into Update	This rule is applied to Options messages sent from Vodafone SIP Trunk (IP Group 2) in an active call session. This convert the method type '8' (Options) with the value '18' (Update).
3	and flip them back towards Avaya CS1K.	This rule is applied to Convert back the messages sent from Vodafone SIP Trunk (IP Group 2) to Options. This convert the method type '18' (Update) with the value '8 (Options)'.

5. Assign Manipulation Set IDs 1 to IP Group 1:
 - a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
 - b. Select the row of IP Group 1, and then click **Edit**.
 - c. Click the **SBC** tab.
 - d. Set the 'Outbound Message Manipulation Set' field to 1.

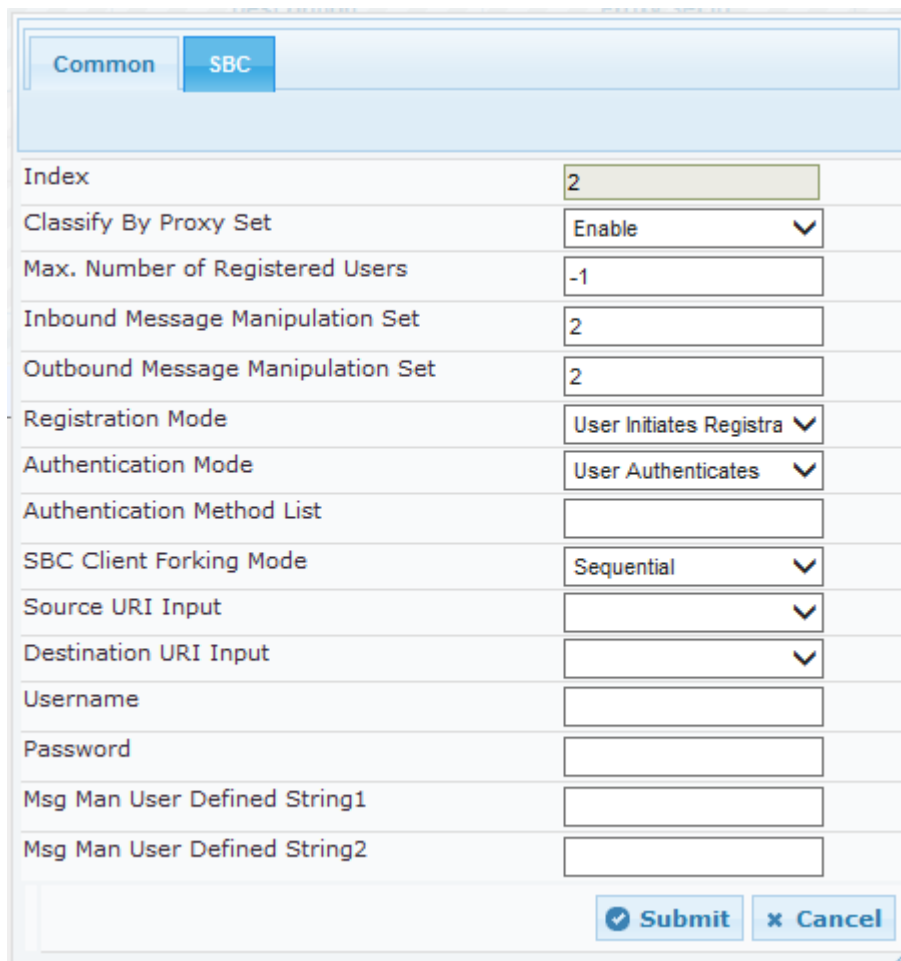
Figure 3-35: Assigning Manipulation Set 1 to IP Group 1

The screenshot shows the 'SBC' configuration tab for IP Group 1. The 'Outbound Message Manipulation Set' field is set to '1'. Other fields include 'Index' (1), 'Classify By Proxy Set' (Enable), 'Max. Number of Registered Users' (-1), 'Inbound Message Manipulation Set' (-1), 'Registration Mode' (User Initiates Registration), 'Authentication Mode' (User Authenticates), 'Authentication Method List' (empty), 'SBC Client Forking Mode' (Sequential), 'Source URI Input' (empty), 'Destination URI Input' (empty), 'Username' (empty), 'Password' (empty), 'Msg Man User Defined String1' (empty), and 'Msg Man User Defined String2' (empty). At the bottom are 'Submit' and 'Cancel' buttons.

- e. Click **Submit**.

6. Assign Manipulation Set ID 2 to IP Group 2:
 - a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
 - b. Select the row of IP Group 2, and then click **Edit**.
 - c. Click the **SBC** tab.
 - d. Set the 'Inbound Message Manipulation Set' field to **2**.
 - e. Set the 'Outbound Message Manipulation Set' field to **2**.

Figure 3-36: Assigning Manipulation Set 2 to IP Group 2



Common		SBC
Index	2	
Classify By Proxy Set	Enable	
Max. Number of Registered Users	-1	
Inbound Message Manipulation Set	2	
Outbound Message Manipulation Set	2	
Registration Mode	User Initiates Registra	
Authentication Mode	User Authenticates	
Authentication Method List		
SBC Client Forking Mode	Sequential	
Source URI Input		
Destination URI Input		
Username		
Password		
Msg Man User Defined String1		
Msg Man User Defined String2		

- f. Click **Submit**.

3.11 Step 11: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

3.11.1 Step 11a: Configure Max-Forwards

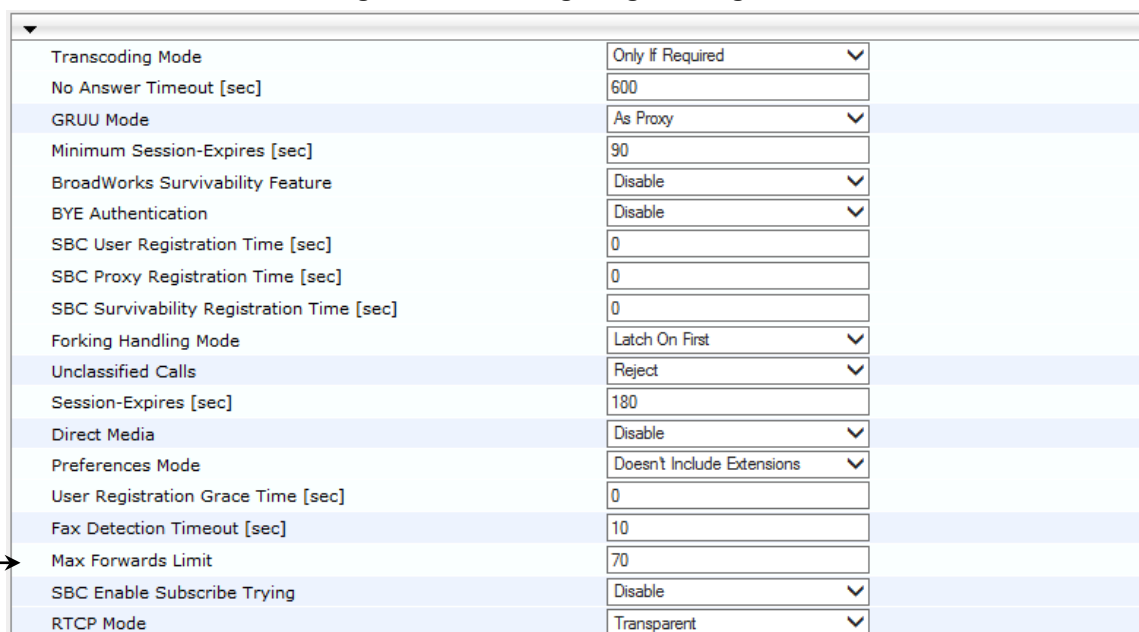
This step describes how to configure the Max-Forwards header. The Max-Forwards header is used to limit the number of servers (such as proxies) that can forward the SIP request. The Max-Forwards value indicates the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request.

➤ **To configure Max-Forwards SIP header:**

1. Open the General Settings page (**Configuration** tab > **VoIP** menu > **SBC** > **General Settings**).
2. In the 'Max Forwards Limit' Enter **70**.

Note: The Default sends Max-Forwards with a value of 10. Avaya CS1K and Session Manager decrement each one by 4 so in Call Forwarding scenario no Max-forwards left.

Figure 3-37: Configuring Forking Mode



Transcoding Mode	Only If Required
No Answer Timeout [sec]	600
GRUU Mode	As Proxy
Minimum Session-Expires [sec]	90
BroadWorks Survivability Feature	Disable
BYE Authentication	Disable
SBC User Registration Time [sec]	0
SBC Proxy Registration Time [sec]	0
SBC Survivability Registration Time [sec]	0
Forking Handling Mode	Latch On First
Unclassified Calls	Reject
Session-Expires [sec]	180
Direct Media	Disable
Preferences Mode	Doesn't Include Extensions
User Registration Grace Time [sec]	0
Fax Detection Timeout [sec]	10
Max Forwards Limit	70
SBC Enable Subscribe Trying	Disable
RTCP Mode	Transparent

3. Click **Submit**.

3.12 Step 12: Reset the E-SBC

After you have completed the configuration of the E-SBC described in this chapter, save ("burn") the configuration to the E-SBC's flash memory with a reset for the settings to take effect.

➤ **To save the configuration to flash memory:**

1. Open the Maintenance Actions page (**Maintenance** tab > **Maintenance** menu > **Maintenance Actions**).

Figure 3-38: Resetting the E-SBC

▼ Reset Configuration	
Reset Board	<input type="button" value="Reset"/>
Burn To FLASH	Yes ▼
Graceful Option	No ▼
▼ LOCK / UNLOCK	
Lock	<input type="button" value="LOCK"/>
Graceful Option	No ▼
Gateway Operational State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	<input type="button" value="BURN"/>

2. Ensure that the 'Burn to FLASH' field is set to **Yes** (default).
3. Click the **Reset** button.

This page is intentionally left blank

A AudioCodes INI File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 3 on page 13, is shown below:



Note: To load and save an ini file, use the Configuration File page (**Maintenance** tab > **Software Update** menu > **Configuration File**).

```
;*****
; ** Ini File **
;*****

;Board: Mediant 4000
;Board Type: 70
;Serial Number: 5928360
;Slot Number: 1
;Software Version: 6.80A.227.005
;DSP Software Version: 5039AE3_R => 680.22
;Board IP Address: 10.15.14.80
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 2048M Flash size: 252M
;Num of DSP Cores: 24 Num DSP Channels: 1000
;Num of physical LAN ports: 8
;Profile: NONE
;Key features;;Board Type: Mediant 4000 ;Coders: G723 G729 G727 ;IP
Media: VXML ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;Channel Type: RTP DspCh=1000 ;HA ;Control
Protocols: MSFT CLI SIP SBC=500 ;Default features;;Coders: G711 G726;

;----- Mediant 4000 HW components-----
;
; Slot # : LAN Ports : DSP's # : Module type
;-----
;1 |0 |0 |Empty |
;2 |0 |0 |Empty |
;3 |0 |0 |Empty |
;4 |0 |0 |Empty |
;5 & 6 |1 - 8 |4 |CSM |
;7 |0 |0 |Empty |
;8 |0 |0 |Empty |

;MAC Addresses in use:
;-----
;GROUP_1 - 00:90:8f:5a:75:ab
;GROUP_2 - 00:90:8f:5a:75:ab
;GROUP_3 - 00:90:8f:5a:75:a9
;GROUP_4 - 00:90:8f:5a:75:a9
;-----

[SYSTEM Params]
```



```
SyslogServerIP = 10.15.16.153
EnableSyslog = 1
DebugRecordingDestIP = 10.15.16.153
;VpFileLastUpdateTime is hidden but has non-default value
DebugRecordingStatus = 0
NTPServerIP = '0.0.0.0'
LDAPSEARCHDNSINPARALLEL = 0
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

FarEndDisconnectType = 7

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]

[MEGACO Params]

EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[Voice Engine Params]

[WEB Params]

WebLogoText = 'Interop Test'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
HTTPSCipherString = 'RC4:EXP'

[SIP Params]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
SBCDirectMedia = 0
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCMAXFORWARDSLIMIT = 70
SBCFORKINGHANDLINGMODE = 0
```

```
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[IPsec Params]

[SNMP Params]

[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_1", 1, 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_2", 1, 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_3", 1, 2, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4", 1, 2, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "GE_5", 1, 1, 4, "User Port #4", "GROUP_3",
"Active";
PhysicalPortsTable 5 = "GE_6", 1, 1, 4, "User Port #5", "GROUP_3",
"Redundant";
PhysicalPortsTable 6 = "GE_7", 1, 1, 4, "User Port #6", "GROUP_4",
"Active";
PhysicalPortsTable 7 = "GE_8", 1, 1, 4, "User Port #7", "GROUP_4",
"Redundant";

[ \PhysicalPortsTable ]

[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_1", "GE_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_3", "GE_4";
EtherGroupTable 2 = "GROUP_3", 2, "GE_5", "GE_6";
EtherGroupTable 3 = "GROUP_4", 2, "GE_7", "GE_8";
EtherGroupTable 4 = "GROUP_5", 0, "", "";
EtherGroupTable 5 = "GROUP_6", 0, "", "";
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 0, "", "";

[ \EtherGroupTable ]

[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName;
DeviceTable 0 = 1, "GROUP_1", "vlan 1";
DeviceTable 2 = 2, "GROUP_2", "vlan 2";
```

```

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.14.80, 16, 10.15.0.1, 1, "Voice-LAN",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.141, 25, 195.189.192.129, 2, "X2-
LAN", 0.0.0.0, 0.0.0.0, "vlan 2";

[ \InterfaceTable ]

[ DspTemplates ]

;
; *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \DspTemplates ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 1 = "MR-SM", "Voice-LAN", "", 6000, 100, 6990, 1, "", "";
CpMediaRealm 2 = "MR-VF", "X2-LAN", "", 7000, 100, 7990, 0, "", "";

[ \CpMediaRealm ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "SRD-SM", "MR-SM", 0, 0, -1, 1;
SRD 2 = "SRD-VF", "MR-VF", 0, 0, -1, 1;

[ \SRD ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IPAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "10.15.15.143:5070", 0, 1;

```

```

ProxyIp 1 = "212.144.52.96:5060", 0, 2;

[ \ProxyIp ]

[ IpProfile ]

; ** NOTE: Changes were made to active configuration.
; ** The data below is different from current values.
FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCEExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPptimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay;

IpProfile 1 = "SM", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0, -
1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 0, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1,
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300;

IpProfile 2 = "VF", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0, -
1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 1, "", -1, -1, 0, 0, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 1, 2, 1, 0, 0, 1, 0, 1,
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300;

```

```
[ \IpProfile ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_TLSContext,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp;
ProxySet 0 = "", 0, 60, 0, 0, 0, 0, "-1", -1, -1, "";
ProxySet 1 = "SM", 0, 60, 0, 0, 1, 0, "-1", -1, -1, "";
ProxySet 2 = "SM", 0, 60, 0, 0, 2, 0, "-1", -1, -1, "";

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2;
IPGroup 1 = 0, "SM", 1, "etkn.de", "", 0, -1, -1, 0, -1, 1, "MR-SM", 1,
1, -1, -1, 1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "", 0,
"", "";
IPGroup 2 = 0, "VF", 2, "vodafone.com", "", 0, -1, -1, 0, -1, 2, "MR-VF",
1, 2, -1, 2, 2, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "", 0,
"", "";

[ \IPGroup ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix,
IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 1 = "Terminate Options", -1, "", "etkn.de", "", "", 6,
"", -1, 0, -1, 1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 2 = "SM to VF", 1, "", "", "", "", 0, "", -1, 0, -1, 0,
2, "2", "", 0, -1, 0, 0, "";
IP2IPRouting 3 = "VF to SM", 2, "", "", "", "", 0, "", -1, 0, -1, 0,
1, "1", "", 0, -1, 0, 0, "";
```

```
[ \IP2IPRouting ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 0, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;

[ \TLSContexts ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPSPort, SIPInterface_TLSPort,
SIPInterface_SRD, SIPInterface_MessagePolicy, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet;
SIPInterface 1 = "SIP-SM", "Voice-LAN", 2, 5070, 0, 0, 1, "", "", -1, 0,
500, -1;
SIPInterface 2 = "SIP-VF", "X2-LAN", 2, 5060, 0, 0, 2, "", "", -1, 0,
500, -1;

[ \SIPInterface ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageCondition,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID, IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 2 = "Remove Calling Name", 0, -1, 2, "*", "*",
"*, "*", "", 0, -1, 0, 2, 0, 0, 0, "", "", 0;

[ \IPOutboundManipulation ]

[ CodersGroup0 ]
```

```
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0;

[ \CodersGroup0 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "403 to 404", 2, "invite.response.403",
"header.request-uri.methodtype=='403'", "header.request-uri.methodtype",
2, "'404'", 0;
MessageManipulations 2 = "Options to Update", 2, "Options",
"header.request-uri.methodtype=='8'", "header.request-uri.methodtype", 2,
"'18'", 0;
MessageManipulations 3 = "Update to Options", 1, "Update",
"header.request-uri.methodtype=='18'", "header.request-uri.methodtype",
2, "'8'", 0;

[ \MessageManipulations ]

[ RoutingRuleGroups ]

FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable,
RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost;
RoutingRuleGroups 0 = 0, 0, 1;

[ \RoutingRuleGroups ]

[ LoggingFilters ]

FORMAT LoggingFilters_Index = LoggingFilters_FilterType,
LoggingFilters_Value, LoggingFilters_Syslog, LoggingFilters_CaptureType;
LoggingFilters 0 = 1, "", 1, 2;

[ \LoggingFilters ]

[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 0;
ResourcePriorityNetworkDomains 2 = "dod", 0;
ResourcePriorityNetworkDomains 3 = "drsn", 0;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 0;

[ \ResourcePriorityNetworkDomains ]
```

B Configuring Avaya Session Manager

This step shows example configuration screenshots on how to configure the Avaya Session Manager to interwork with the AudioCodes SBC.



Note: This is configuration is partial for the entire Avaya Aura environment.

Figure B-1: Configuring the SBC on the Session Manager

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

CommProfile Type Preference:

Loop Detection

Loop Detection Mode:

SIP Link Monitoring

SIP Link Monitoring:

Figure B-2: Configuring the SBC on the Session Manager

Adaptation Details Commit Cancel

General

* **Adaptation Name:**

Module Name:

Module Parameter Type:

Add Remove

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	MIME	no
<input type="checkbox"/>	odstd	etkn.de
<input type="checkbox"/>	psrcd	etkn.de

Select : All, None Page 2

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

3 Items

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	* 0	* 1	* 36		* 1	+49	destination	
<input type="checkbox"/>	* 0	* 1	* 36		* 0	0	origination	
<input type="checkbox"/>	* 00	* 2	* 36		* 2	+	destination	

Select : All, None

This page is intentionally left blank



Configuration Note

