

Connecting Cisco Unified Communications Manager Ver. 12.0 with BroadCloud SIP Trunk using Mediant™ SBC

Version 7.2



CallManager



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	IP-PBX Version	9
2.2	AudioCodes E-SBC Version	9
2.3	BroadCloud SIP Trunking Version.....	9
2.4	Interoperability Test Topology	10
2.4.1	Environment Setup	11
2.4.2	Known Limitations.....	11
3	Configuring Cisco CUCM	13
3.1	Log in to Cisco Unified Communications Manager	13
3.2	Create a New Trunk	13
3.3	Create a New Route Pattern.....	15
4	Configuring AudioCodes E-SBC.....	19
4.1	Step 1: IP Network Interfaces Configuration	20
4.1.1	Step 1a: Configure VLANs.....	21
4.1.2	Step 1b: Configure Network Interfaces.....	22
4.2	Step 2: Configure Media Realms	24
4.3	Step 3: Configure SIP Signaling Interfaces.....	26
4.4	Step 4: Configure Proxy Sets	27
4.5	Step 5: Configure IP Profiles	31
4.6	Step 6: Configure IP Groups.....	33
4.7	Step 7: Configure IP-to-IP Call Routing Rules	35
4.8	Step 8: Configure IP-to-IP Manipulation Rules.....	39
4.9	Step 9: Configure Message Manipulation Rules	41
4.10	Step 10: Configure Registration Accounts	46
4.11	Step 11: Miscellaneous Configuration.....	47
4.11.1	Step 11a: Configure SBC Alternative Routing Reasons	47
4.12	Step 12: Reset the E-SBC	48
A	AudioCodes INI File	49

This page is intentionally left blank.

Notice

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

This document is subject to change without notice.

Date Published: May-03-2018

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 <https://www.audiocodes.com/services-support/maintenance-and-support>.

Document Revision Record

LTRT	Description
12730	Initial document release for Version 7.2.
12731	Re-testing with Cisco CUCM 12.0 and AudioCodes Version 7.2.202

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 <https://online.audiocodes.com/documentation-feedback>.

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 BroadCloud's SIP Trunk and the Cisco CUCM environment.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and BroadCloud Partners who are responsible for installing and configuring BroadCloud's SIP Trunk and Cisco CUCM for enabling 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 IP-PBX Version

Table 2-1: IP-PBX Version

Vendor	Cisco
Model	CUCM 12.0.1
Protocol	SIP/UDP
Additional Notes	

2.2 AudioCodes E-SBC Version

Table 2-2: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none"> ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 500 Gateway & E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant SW SBC
Software Version	SIP_F7.20A.202 or later
Protocol	SIP/UDP (to the both BroadCloud SIP Trunk and IP-PBX)
Additional Notes	None

2.3 BroadCloud SIP Trunking Version

Table 2-3: BroadCloud Version

Vendor/Service Provider	BroadCloud
SSW Model/Service	BroadWorks
Software Version	21
Protocol	SIP/UDP
Additional Notes	None

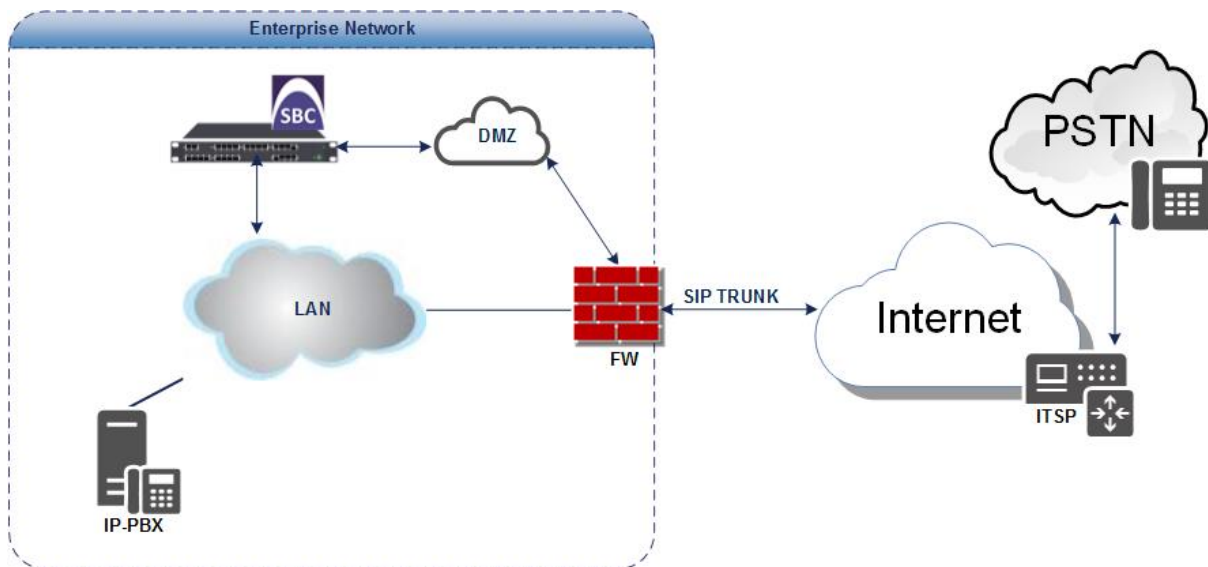
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and BroadCloud SIP Trunk with IP-PBX was done using the following topology setup:

- Enterprise deployed with IP-PBX in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using BroadCloud'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.
 - **Border:** IP-to-IP network border between IP-PBX network in the Enterprise LAN and BroadCloud'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 IP-PBX with BroadCloud 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"> ▪ IP-PBX is located on the Enterprise's LAN ▪ BroadCloud SIP Trunk is located on the WAN
Signaling Transcoding	<ul style="list-style-type: none"> ▪ IP-PBX operates with SIP-over-UDP or SIP-over-TCP transport types ▪ BroadCloud SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	<ul style="list-style-type: none"> ▪ IP-PBX supports G.711A-law, G.711U-law, and G.729 coder ▪ BroadCloud SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	<ul style="list-style-type: none"> ▪ IP-PBX operates with RTP media type ▪ BroadCloud SIP Trunk operates with RTP media type

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between IP-PBX and BroadCloud 's SIP Trunk.

This page is intentionally left blank.

3 Configuring Cisco CUCM

This section describes how to configure the Cisco Unified Communications Manager.

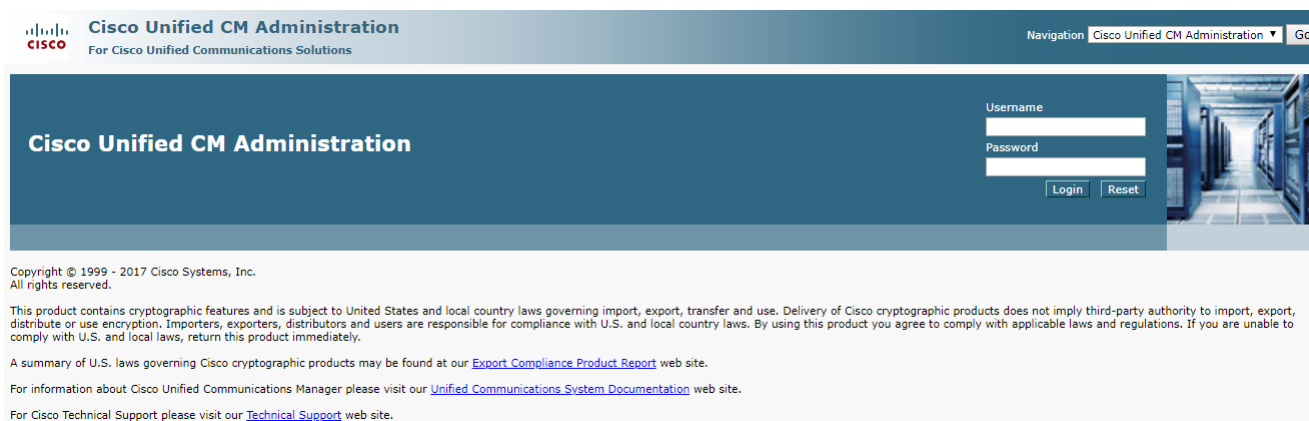
3.1 Log in to Cisco Unified Communications Manager

The procedure below describes how to log in to the Cisco CUCM Administration interface.

➤ **To log in to the Cisco Unified CM Administration interface:**

1. Log in to the Cisco Unified CM Administration by entering the IP address of the Cisco Unified Communications Manager (CUCM) in the Web browser address field.

Figure 3-1: Cisco Unified CM Administration



The screenshot shows the Cisco Unified CM Administration login page. The page has a dark blue header with the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions". On the right side of the header, there is a navigation menu with "Cisco Unified CM Administration" selected and a "Go" button. The main content area is a light blue box with the title "Cisco Unified CM Administration" and a login form. The form has two input fields: "Username" and "Password", and two buttons: "Login" and "Reset". To the right of the form is a background image of a server room. Below the form, there is a copyright notice: "Copyright © 1999 - 2017 Cisco Systems, Inc. All rights reserved." and a disclaimer: "This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately." There are also links to "Export Compliance Product Report" and "Unified Communications System Documentation" web sites, and a link to "Technical Support" web site.

2. In the 'Username' field, enter the user name.
3. In the 'Password' field, enter the password.
4. Click **Login**.

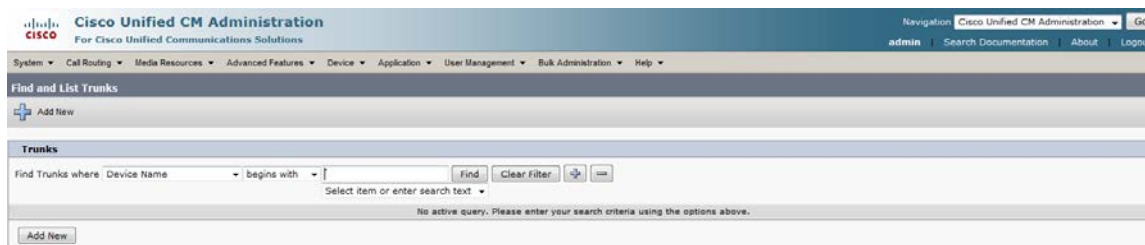
3.2 Create a New Trunk

This section describes how to create a new trunk.

➤ **To create a new trunk:**

1. From the **Device** menu drop-down list, select **Trunk**.
2. Click **Add New**.

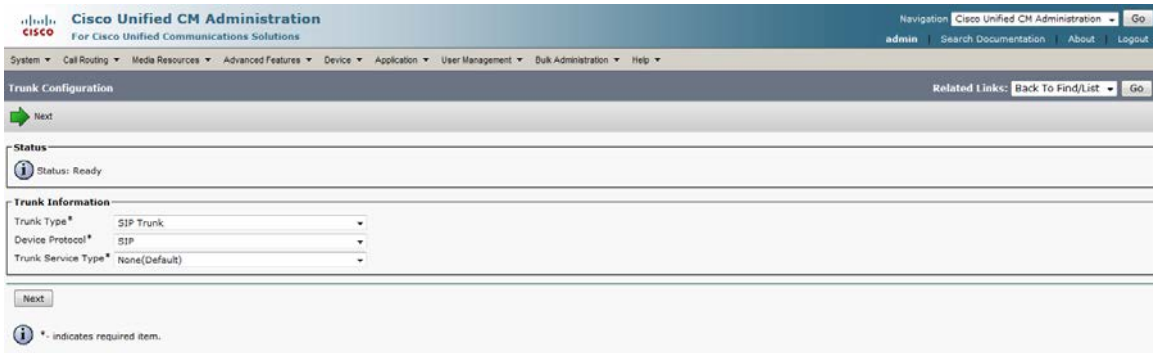
Figure 3-2: Trunk page



The screenshot shows the Cisco Unified CM Administration "Trunk" page. The page has a dark blue header with the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions". On the right side of the header, there is a navigation menu with "Cisco Unified CM Administration" selected and a "Go" button. Below the header, there is a navigation menu with "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The main content area is a light blue box with the title "Find and List Trunks" and an "Add New" button. Below the "Add New" button, there is a search form with a dropdown menu for "Find Trunks where" set to "Device Name", a "begins with" input field, and "Find", "Clear Filter", and "Reset" buttons. Below the search form, there is a message: "No active query. Please enter your search criteria using the options above." and an "Add New" button.

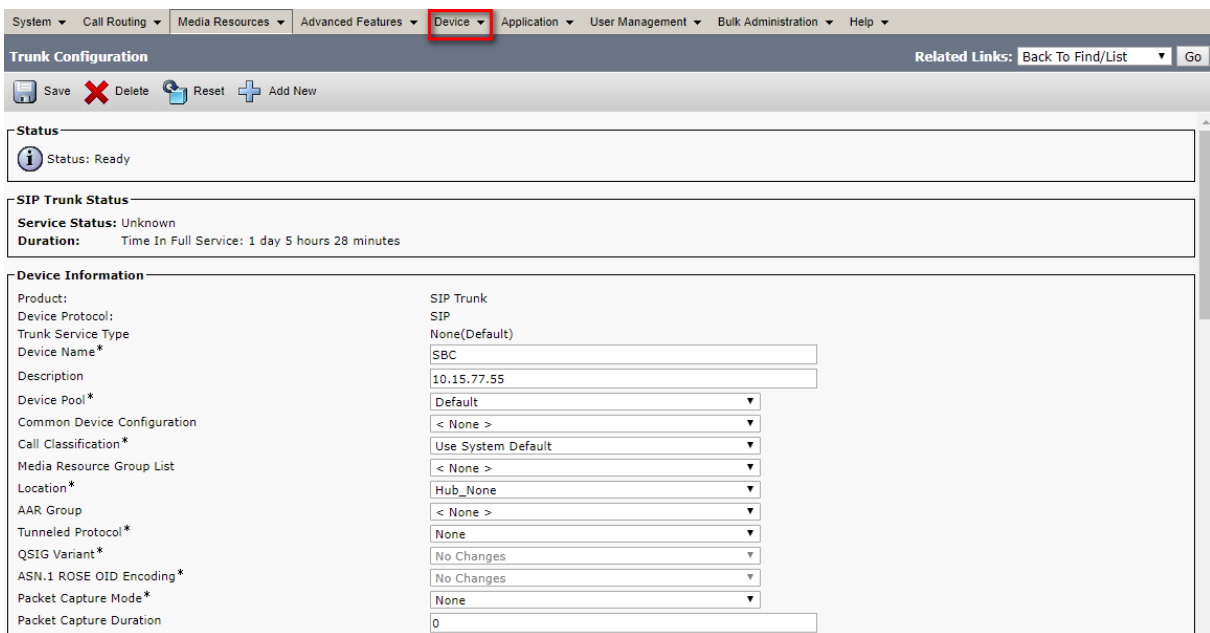
3. Select Trunk Type – **SIP Trunk**.
4. Click **Next**.

Figure 3-3: Create Trunk Page



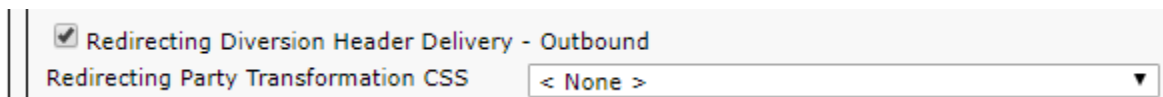
5. In the **Device Name** field, enter a unique SIP Trunk name and optionally provide a description.
6. From the **Device Pool** drop-down list, select a device pool.

Figure 3-4: SIP Trunk Settings Page



7. Select the 'Redirecting Diversion Header Delivery – Outbound' check box.

Figure 3-5: Redirecting Diversion Header Delivery



8. Enter the Destination Address and Destination Port of the AudioCodes SBC.

Figure 3-6: SIP Information Section

	Destination Address	Destination Address IPv6	Destination Port	Status
1*	10.15.77.55		5060	N/A

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Non Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* MP1xx-SIP_Profile [View Details](#)

DTMF Signaling Method* No Preference

9. From the **SIP Trunk Security** drop-down list, select a profile.
10. From the **SIP Profile** drop-down list, select a profile.
11. Click **Save**.

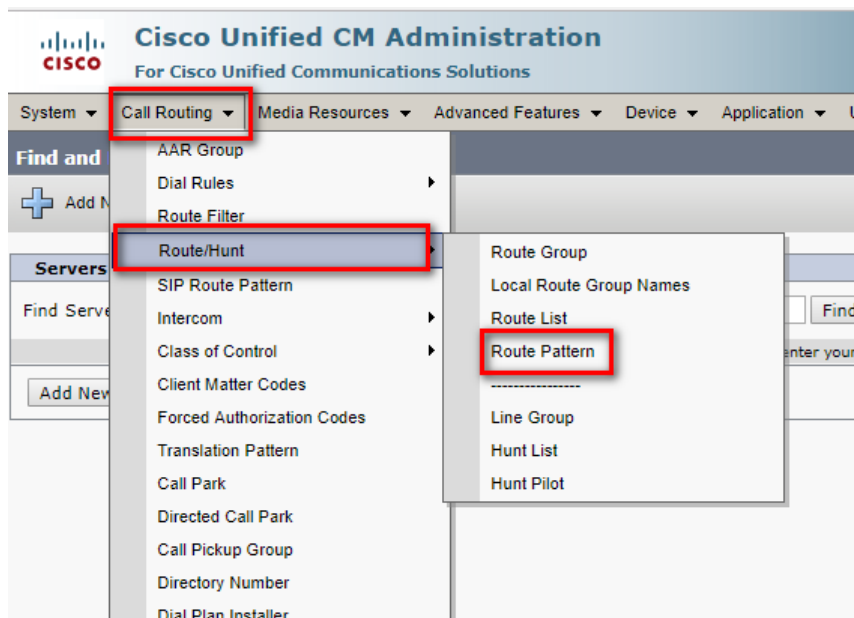
3.3 Create a New Route Pattern

This section describes how to create a new route pattern.

➤ **To create new Route Pattern:**

1. From the **Call Routing** menu drop-down list, go to the **Route/Hunt** menu and select **Route Pattern**.

Figure 3-7: Route Pattern page



2. Click **Add New**.
3. Enter a Route Pattern according to schema (optionally provide a description).
4. From the **Gateway/Route List** drop-down list, select the SIP Trunk device name.

Figure 3-8: Create Route Pattern Page

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾

Route Pattern Configuration

Save Delete Copy Add New

Status
Status: Ready

Pattern Definition

Route Pattern* 4XXX
 Route Partition < None >
 Description To SBC
 Numbering Plan -- Not Selected --
 Route Filter < None >
 MLPP Precedence* Default
 Apply Call Blocking Percentage
 Resource Priority Namespace Network Domain < None >
 Route Class* Default
Gateway/Route List* SBC (Edit)
 Route Option
 Route this pattern
 Block this pattern No Error
 Call Classification* OffNet
 External Call Control Profile < None >
 Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority
 Require Forced Authorization Code
 Authorization Level* 0
 Require Client Matter Code

5. Click **Save**.

Figure 3-9: Added Route Pattern

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List Route Patterns

Add New Select All Clear All Delete Selected

Status
7 records found

Route Patterns (1 - 7 of 7) Rows per Page 50

Find Route Patterns where Pattern begins with Find Clear Filter

Pattern	Description	Partition	Route Filter	Associated Device	Copy
1	National Calls to AT_T through AudioCodes SBC			SBC-ATT	
1#	dial # to indicate end of dialing			SBC-ATT	
19	US Numbers			SBC-ATT	
4XXX	To SBC			SBC	
972	to israel			SBC-ATT	
972!	to israel			SBC-ATT	
9XXX	to Lync			Lync	

Add New Select All Clear All Delete Selected

Figure 3-10: Added Trunk

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go
admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Find and List Trunks

+ Add New | Select All | Clear All | Delete Selected | Reset Selected

Status
7 records found

Trunks (1 - 7 of 7) Rows per Page 50

Find Trunks where Device Name begins with Find Clear Filter

	Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration	SIP Trunk Security Profile
<input type="checkbox"/>	Lync	Lync Mediation Server 10.15.25.3		Default	9XXX				SIP Trunk	Full Service	Time In Full Service: 1 day 5 hours 40 minutes	Lync Security Profile
<input type="checkbox"/>	SBC	10.15.77.55		Default	4XXX				SIP Trunk	Full Service	Time In Full Service: 1 day 5 hours 40 minutes	Non Secure SIP Trunk Profile
<input type="checkbox"/>	SBC-ATT			Default	119				SIP Trunk	Full Service	Time In Full Service: 1 day 5 hours 40 minutes	Non Secure SIP Trunk Profile
<input type="checkbox"/>	SBC-ATT			Default	11				SIP Trunk	Full Service	Time In Full Service: 1 day 5 hours 40 minutes	Non Secure SIP Trunk Profile
<input type="checkbox"/>	SBC-ATT			Default	972!#				SIP Trunk	Full Service	Time In Full Service: 1 day 5 hours 40 minutes	Non Secure SIP Trunk Profile
<input type="checkbox"/>	SBC-ATT			Default	972!				SIP Trunk	Full Service	Time In Full Service: 1 day 5 hours 40 minutes	Non Secure SIP Trunk Profile
<input type="checkbox"/>	SBC-ATT			Default	1!#				SIP Trunk	Full Service	Time In Full Service: 1 day 5 hours 40 minutes	Non Secure SIP Trunk Profile

Add New | Select All | Clear All | Delete Selected | Reset Selected



Note: An '*' indicates a mandatory field.

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

This section provides step-by-step procedures on how to configure the AudioCodes E-SBC for interworking between the IP-PBX and the BroadCloud SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.1 on page 9, and includes the following main areas:

- E-SBC WAN interface - BroadCloud SIP Trunking environment
- E-SBC LAN interface - IP-PBX environment

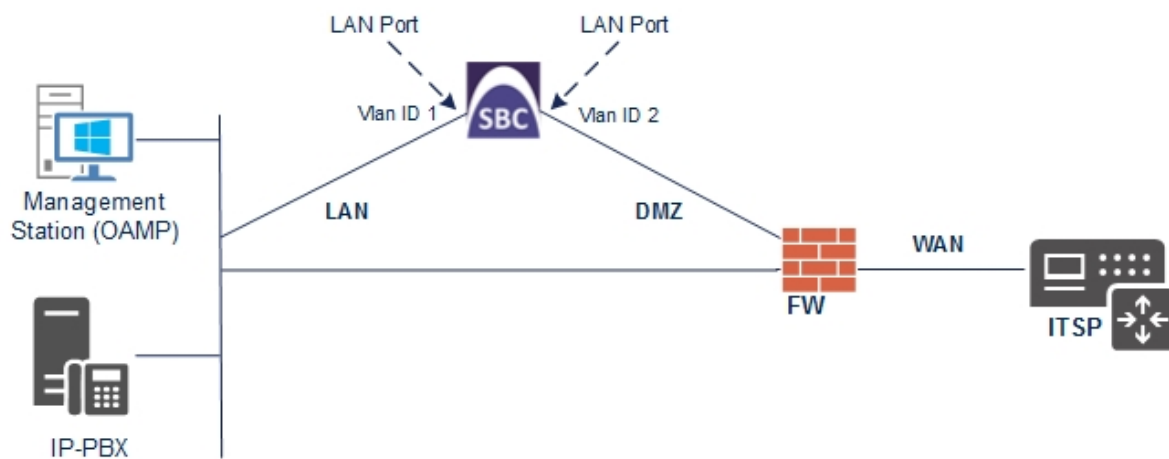
This is configured using the E-SBC's embedded Web server (hereafter, referred to as the Web interface).

4.1 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:
 - IP-PBX - located on the LAN
 - BroadCloud 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, the 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 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

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

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

➤ **To configure the VLANs:**

1. Open the Ethernet Devices Table page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).

There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.

2. 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
Tagging	Untagged

Figure 4-2: Configured VLAN IDs in Ethernet Device Table

Ethernet Devices (2)

+ New Edit | Page 1 of 1 | Show 10 records per page

INDEX ↕	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

4.1.2 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")
- WAN VoIP (assigned the name "WANSP")

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

1. Open the IP Interfaces Table page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
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
Application Type	OAMP + Media + Control
IP Address	10.15.7.8 (IP address of E-SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Default Gateway	10.15.0.1
Name	Voice (arbitrary descriptive name)
Primary DNS Server IP Address	0.0.0.0
Ethernet Device	vlan 1

3. Add a network interface for the WAN side:
 - c. Enter **1**, and then click **Add Index**.
 - d. Configure the interface as follows:



Parameter	Value
Application Type	Media + Control
IP Address	195.189.192.153 (WAN IP address)
Prefix Length	25 (for 255.255.255.128)
Default Gateway	195.189.192.129 (router's IP address)
Name	WANSP
Primary DNS Server IP Address	8.8.8.8
Secondary DNS Server IP Address	0.0.0.0
Ethernet Device	vlan 2

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

The configured IP network interfaces are shown below:

Figure 4-3: Configured Network Interfaces in IP Interfaces Table

IP Interfaces (2)

+ New Edit  Page 1 of 1 Show 10 records per page 

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	Voice	OAMP + Media	IPv4 Manual	10.15.7.8	16	0.0.0.0	0.0.0.0	0.0.0.0	vlan 1
1	WANSP	Media + Control	IPv4 Manual	195.189.19.	25	195.189.19.	8.8.8.8	0.0.0.0	vlan 2

4.2 Step 2: Configure Media Realms

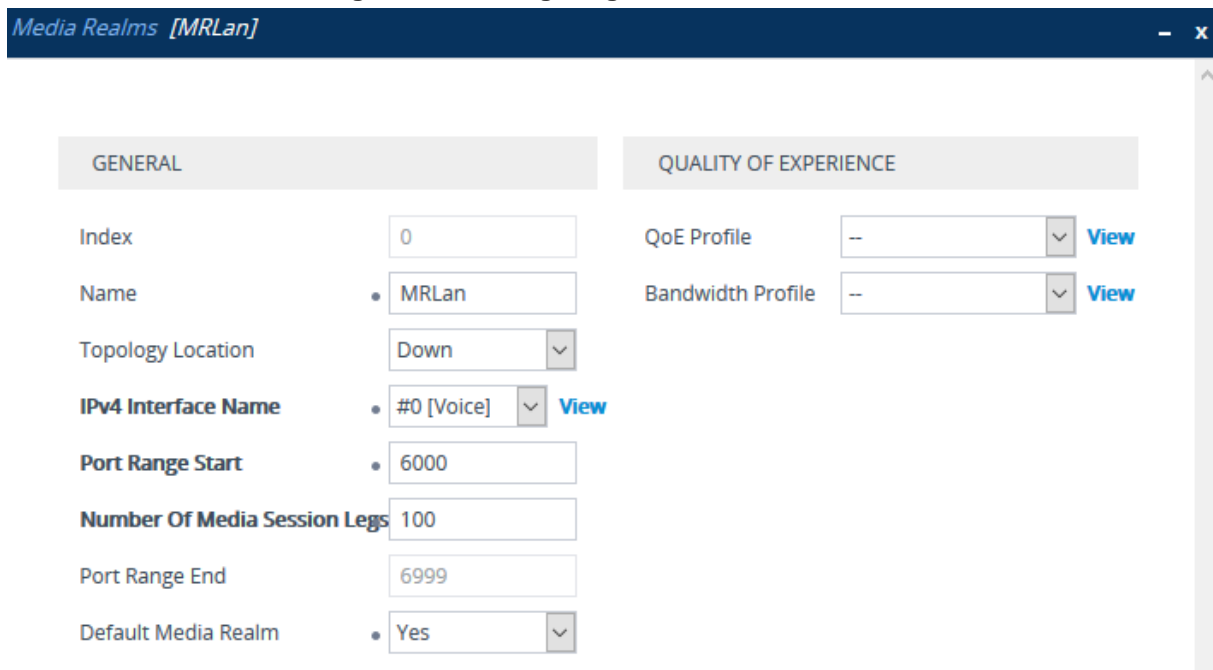
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➤ **To configure Media Realms:**

1. Open the Media Realm Table page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), but modify it as shown below:

Parameter	Value
Index	0
Name	MRLan (descriptive name)
IPv4 Interface Name	Voice
Port Range Start	6000 (as required by IP-PBX)
Number of Media Session Legs	100 (media sessions assigned with port range)

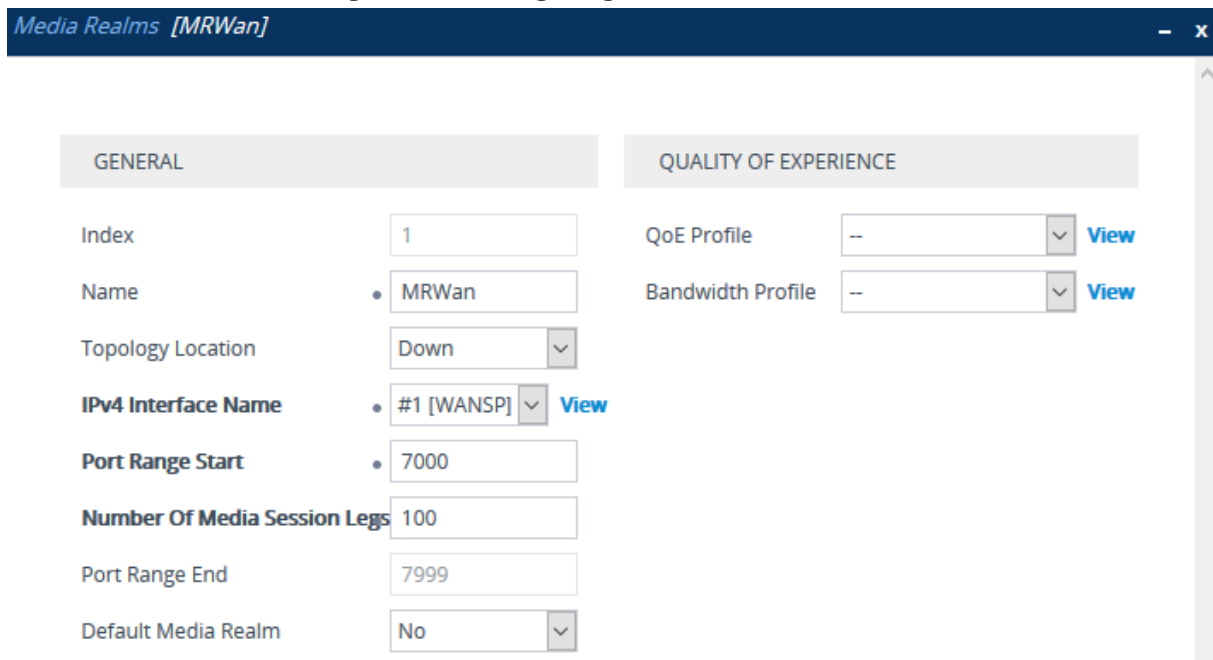
Figure 4-4: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Name	MRWan (arbitrary name)
IPv4 Interface Name	WANSP
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 4-5: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 4-6: Configured Media Realms in Media Realm Table

Media Realms (2)

+ New Edit | Page 1 of 1 | Show 10 records per page

INDEX	NAME	IPv4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MRLan	Voice	6000	100	6999	Yes
1	MRWan	WANSP	7000	100	7999	No

4.3 Step 3: 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 Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Add a SIP Interface for the LAN interface. You can use the default SIP Interface (Index 0), but modify it as shown below:

Parameter	Value
Index	0
Name	SIPInterface_LAN
Network Interface	Voice
Application Type	SBC
UDP and TCP Ports	5060
TLS Port	0
Media Realm	MRLan

3. Configure a SIP Interface for the WAN:

Parameter	Value
Index	1
Name	SIPInterface_WAN
Network Interface	WANSP
Application Type	SBC
UDP Port	5060
TCP and TLS Ports	0
Media Realm	MRWan

The configured SIP Interfaces are shown in the figure below:

Figure 4-7: Configured SIP Interfaces in SIP Interface Table

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATION PROTOCOL	MEDIA REALM
0	SIPInterface_LAN	DefaultSRD	Voice	SBC	5060	5060	0	No encapsulation	MRLan
1	SIPInterface_WAN	DefaultSRD	WANSP	SBC	5060	0	0	No encapsulation	MRWan

4.4 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:

- IP-PBX
- BroadCloud SIP Trunk

The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

➤ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Add a Proxy Set for the IP-PBX.

Parameter	Value
Index	1
Name	IP-PBX
SBC IPv4 SIP Interface	SIPInterface_LAN
Proxy Keep Alive	Using Options

Figure 4-8: Configuring Proxy Set for IP-PBX

3. Configure a Proxy Address Table for Proxy Set for IP-PBX:
 - a. Go to Proxy Address.

Parameter	Value
Index	0
Proxy Address	10.15.28.101:5060 (IP-PBX IP address / FQDN and destination port)
Transport Type	UDP

Figure 4-9: Configuring Proxy Address for IP-PBX

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	10.15.28.101:5060	UDP

4. Configure a Proxy Set for the BroadCloud SIP Trunk:

Parameter	Value
Index	2
Name	BroadCloud
SBC IPv4 SIP Interface	SIPInterface_WAN
Proxy Keep Alive	Using Options
Redundancy Mode	Homing
Proxy Hot Swap	Enable
Proxy Load Balancing Method	Disable
DNS Resolve Method	SRV

Figure 4-10: Configuring Proxy Set for BroadCloud SIP Trunk

- a. Configure a Proxy Address Table for Proxy Set 2:
- b. Go to **Proxy Address**.

Parameter	Value
Index	0
Proxy Address	nn6300southsipconnect.adpt-tech.com (IP-PBX IP address / FQDN and destination port)
Transport Type	UDP

Figure 4-11: Configuring Proxy Address for BroadCloud SIP Trunk

Proxy Sets [#1] > Proxy Address (1)

+ New Edit | Page 1 of 1 | Show 10 records per page

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	nn6300southsipconnect.adpt-tech.com	UDP

The configured Proxy Sets are shown in the figure below:

Figure 4-12: Configured Proxy Sets in Proxy Sets Table

Proxy Sets (3)

+ New Edit | Page 1 of 1 | Show 10 records per page

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#	--	SIPInterface_LAN	60		Disable
1	IP-PBX	DefaultSRD (#	--	SIPInterface_LAN	60		Disable
2	BroadCloud	DefaultSRD (#	--	SIPInterface_WAN	60	Homing	Enable

4.5 Step 5: 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:

- IP-PBX - to operate in non-secure mode using RTP and UDP
- BroadCloud SIP trunk - to operate in non-secure mode using RTP and UDP

➤ **To configure IP Profile for the IP-PBX:**

1. Open the IP Profile Settings page (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **Add**.
3. Configure the parameters as follows:

Parameter	Value
Index	1
Name	IP-PBX
SBC Media Security Mode	RTP

Figure 4-13: Configuring IP Profile for IP-PBX

The screenshot shows the configuration interface for an IP Profile. It is divided into three main sections: GENERAL, MEDIA SECURITY, and SBC SIGNALING. The GENERAL section includes fields for Index (1), Name (IP-PBX), and Created by Routing Server (No). The MEDIA SECURITY section includes dropdowns for SBC Media Security Mode (RTP), Gateway Media Security Mode (Preferable), Symmetric MKI (Disable), MKI Size (0), SBC Enforce MKI Size (Don't enforce), and SBC Media Security Method (SDES). The SBC SIGNALING section includes dropdowns for PRACK Mode (Transparent), P-Asserted-Identity Header Mode (As Is), Diversion Header Mode (As Is), History-Info Header Mode (As Is), Session Expires Mode (Transparent), Remote Update Support (Supported), Remote re-INVITE (Supported), Remote Delayed Offer Support (Supported), Remote Representation Mode (According to Operation), Keep Incoming Via Headers (According to Operation), Keep Incoming Routing Headers (According to Operation), and Keep User-Agent Header (According to Operation). At the bottom, there are Cancel and APPLY buttons.

➤ To configure an IP Profile for the BroadCloud SIP Trunk:

1. Click **Add**.
2. Configure the parameters as follows:

Parameter	Value
Index	2
Name	BroadCloud
SBC Media Security Mode	RTP
P-Asserted-Identity Header Mode	Add (required for anonymous calls)

Figure 4-14: Configuring IP Profile for BroadCloud SIP Trunk

The screenshot shows the configuration page for an IP Profile named 'BroadCloud'. The parameters are organized into three sections:

- GENERAL:**
 - Index: 2
 - Name: BroadCloud
 - Created by Routing Server: No
- MEDIA SECURITY:**
 - SBC Media Security Mode: RTP
 - Gateway Media Security Mode: Preferable
 - Symmetric MKI: Disable
 - MKI Size: 0
 - SBC Enforce MKI Size: Don't enforce
 - SBC Media Security Method: SDES
- SBC SIGNALING:**
 - PRACK Mode: Transparent
 - P-Asserted-Identity Header Mode: Add
 - Diversion Header Mode: As Is
 - History-Info Header Mode: As Is
 - Session Expires Mode: Transparent
 - Remote Update Support: Supported
 - Remote re-INVITE: Supported
 - Remote Delayed Offer Support: Supported
 - Remote Representation Mode: According to Operation
 - Keep Incoming Via Headers: According to Operation
 - Keep Incoming Routing Headers: According to Operation
 - Keep User-Agent Header: According to Operation

Buttons at the bottom: Cancel, APPLY

4.6 Step 6: 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. 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:

- IP-PBX located on LAN
- BroadCloud SIP Trunk located on WAN

➤ **To configure IP Groups:**

1. Open the IP Group Table page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Add an IP Group for the IP-PBX.

Parameter	Value
Index	1
Name	IP-PBX
Type	Server
Proxy Set	IP-PBX
IP Profile	IP-PBX
Media Realm	MRLan
SIP Group Name	interop.adpt-tech.com
Outbound Message Manipulation Set	2


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

Parameter	Value
Index	2
Name	BroadCloud
Type	Server
Proxy Set	BroadCloud
IP Profile	BroadCloud
Media Realm	MRWan
SIP Group Name	interop.adpt-tech.com (according to ITSP requirement)
Outbound Message Manipulation Set	4

The configured IP Groups are shown in the figure below:

Figure 4-15: Configured IP Groups in IP Group Table

IP Groups (3)

+ New Edit  Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_IPC	Default	Server	Not Config	ProxySet_0	--	--		Disable	-1	-1
1	IP-PBX	Default	Server	Not Config	IP-PBX	IP-PBX	MRLan	interop.ad	Enable	-1	2
2	BroadCloud	Default	Server	Not Config	BroadCloud	BroadCloud	MRWan	interop.ad	Enable	-1	4

4.7 Step 7: 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 4.6 on page 30, IP Group 1 represents IP-PBX, and IP Group 2 represents BroadCloud SIP Trunk.

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

- Terminate SIP OPTIONS messages on the E-SBC
- Calls from IP-PBX to BroadCloud SIP Trunk
- Calls from BroadCloud SIP Trunk to IP-PBX

➤ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure a rule to terminate SIP OPTIONS messages:
 - a. Click **Add**.
 - b. Configure the parameters as follows:

Parameter	Value
Index	0
Name	Terminate OPTIONS (arbitrary descriptive name)
Source IP Group	Any
Request Type	OPTIONS
Destination Type	Dest Address
Destination Address	internal

Figure 4-16: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

3. Configure a rule to route calls from IP-PBX to BroadCloud SIP Trunk:
 - a. Click **Add**.
 - b. Configure the parameters as follows:

Parameter	Value
Index	1
Name	IP-PBX to ITSP (arbitrary descriptive name)
Source IP Group	IP-PBX
Destination Type	IP Group
Destination IP Group	BroadCloud

Figure 4-17: Configuring IP-to-IP Routing Rule for IP-PBX to ITSP

4. Configure rule to route calls from BroadCloud SIP Trunk to IP-PBX:
 - a. Click **Add**.
 - b. Configure the parameters as follows:

Parameter	Value
Index	2
Name	ITSP to IP-PBX (arbitrary descriptive name)
Source IP Group	BroadCloud
Destination Type	IP Group
Destination IP Group	IP-PBX

Figure 4-18: Configuring IP-to-IP Routing Rule for ITSP to IP-PBX – Rule tab

IP-to-IP Routing
[ITSP to IP-PBX]
- X

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL

Index:

Name:

Alternative Route Options:

ACTION

Destination Type:

Destination IP Group: [View](#)

Destination SIP Interface: [View](#)

Destination Address:

Destination Port:

Destination Transport Type:

IP Group Set: [View](#)

Call Setup Rules Set ID:

Group Policy:

Cost Group: [View](#)

MATCH

Source IP Group: [View](#)

Request Type:

Source Username Prefix:

Source Host:

Source Tag:

Cancel
APPLY

The configured routing rules are shown in the figure below:

Figure 4-19: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (3)

[+ New](#) [Edit](#) [Insert](#)
Page 1 of 1
Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNAT ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAM PREFIX	DESTINATI USERNAM PREFIX	DESTINATI TYPE	DESTINATI IP GROUP	DESTINATI SIP INTERFACE	DESTINATIC ADDRESS
0	Terminate	Default_SB	Route Row	Any	OPTIONS	*	*	Dest Adre	--	--	internal
1	IP-PBX to IT	Default_SB	Route Row	IP-PBX	All	*	*	IP Group	BroadClou	--	
2	ITSP to IP-F	Default_SB	Route Row	BroadClou	All	*	*	IP Group	IP-PBX	--	



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

4.8 Step 8: 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 4.6 on page 33, IP Group 1 represents IP-PBX, and IP Group 2 represents BroadCloud SIP Trunk.



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

For example, for this interoperability test topology, a manipulation was configured to add the prefix to the destination number for calls from the IP-PBX IP Group to the BroadCloud SIP Trunk IP Group for specific destination username prefix.

➤ **To configure a number manipulation rule:**

1. Open the IP-to-IP Outbound Manipulation table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Click **Add**.
3. Configure the parameters as follows:

Parameter	Value
Index	0
Name	Add + for National Calls
Source IP Group	IP-PBX
Destination IP Group	BroadCloud
Destination Username Prefix	001
Manipulated Item	Destination URI
Remove from Left	2
Prefix to Add	+

Figure 4-20: Configuring IP-to-IP Outbound Manipulation Rule

Outbound Manipulations [Add + for National Calls]

Routing Policy: #0 [Default_SBCRoutingPolicy]

GENERAL		ACTION	
Index	0	Manipulated Item	Destination URI
Name	Add + for National Calls	Remove From Left	2
Additional Manipulation	No	Remove From Right	0
Call Trigger	Any	Leave From Right	255
MATCH		Prefix to Add	+
Request Type	All	Suffix to Add	
Source IP Group	#0 [IP-PBX] View	Privacy Restriction Mode	Transparent
Destination IP Group	#1 [BroadCloud] View		
Source Username Prefix	*		

Cancel **APPLY**

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between IP-PBX IP Group and BroadCloud SIP Trunk IP Group:

Figure 4-21: Example of Configured IP-to-IP Outbound Manipulation Rules

Outbound Manipulations (3)

+ New Edit Insert ↑ ↓ | Page 1 of 1 | Show 10 records per page

INDEX	NAME	ROUTING POLICY	ADDITIONAL MANIPULATION	SOURCE IP GROUP	DESTINATIC IP GROUP	SOURCE USERNAME PREFIX	DESTINATIC USERNAME PREFIX	MANIPULATION ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	Add + for National Calls	Default_SBC	No	IP-PBX	BroadCloud	*	001	Destination	2	0	255	+	
1	Add 011 to International	Default_SBC	No	IP-PBX	BroadCloud	*	00	Destination	2	0	255	011	
2	For Anonymity	Default_SBC	No	IP-PBX	BroadCloud	*	*	Source URI	0	0	255		

4.9 Step 9: 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 (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a manipulation rule (Manipulation Set 2) for IP-PBX. This rule applies to messages sent to the IP-PBX IP Group. This replaces the host part of the SIP Request-URI Header with the IP-PBX IP address.

Parameter	Value
Index	0
Name	Change R-URI host toward IP-PBX
Manipulation Set ID	2
Message Type	Any.Request
Action Subject	Header.Request-URI.URL.Host
Action Type	Modify
Action Value	Param.Message.Address.Dst.Address

Figure 4-22: Configuring SIP Message Manipulation Rule 0 (for IP-PBX)

The screenshot shows a configuration window titled "Message Manipulations [Change R-URI host toward IP-PBX]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
 - Index: 0
 - Name: Change R-URI host toward IP-PBX
 - Manipulation Set ID: 2
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: Header.Request-URI.URL.Host
 - Action Type: Modify
 - Action Value: Param.Message.Address.Dst.Address
- MATCH:**
 - Message Type: Any.Request
 - Condition: (empty field)

At the bottom of the window, there are "Cancel" and "APPLY" buttons.

- Configure another manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk. This rule is applied to response messages sent to the BroadCloud SIP Trunk IP Group for Rejected Calls initiated by the IP-PBX IP Group. This replaces the method type '503' with the value '486', because BroadCloud SIP Trunk not recognizes '503' method type.

Parameter	Value
Index	1
Name	Reject Cause
Manipulation Set ID	4
Message Type	any.response
Condition	header.request-uri.methodtype=='503'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'486'

Figure 4-23: Configuring SIP Message Manipulation Rule 1 (for BroadCloud SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations" with a subtitle "[Reject Responses]". The interface is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
 - Index: 1
 - Name: Reject Responses
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: header.request-uri.methodtype
 - Action Type: Modify
 - Action Value: '486'
- MATCH:**
 - Message Type: any.response
 - Condition: header.request-uri.methodtype=='503'

At the bottom of the window, there are "Cancel" and "APPLY" buttons.

4. Configure another manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk. This rule applies to messages sent to the BroadCloud SIP Trunk IP Group in a Call Forward scenario when Cisco CUCM configured to send SIP Diversion header. This replaces the user part of the SIP P-Asserted Identity Header with the value from the user part of the SIP Diversion Header.

Parameter	Value
Index	2
Name	Call Forward
Manipulation Set ID	4
Message Type	Invite
Condition	Header.Diversion exists
Action Subject	Header.P-Asserted-Identity.URL.User
Action Type	Modify
Action Value	Header.Diversion.URL.User

Figure 4-24: Configuring SIP Message Manipulation Rule 2 (for BroadCloud SIP Trunk)

The screenshot shows the configuration interface for a SIP Message Manipulation Rule. The window title is "Message Manipulations [Call Forward]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
 - Index: 2
 - Name: Call Forward
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: Header.P-Asserted-Identity.URL.User
 - Action Type: Modify
 - Action Value: Header.Diversion.URL.User
- MATCH:**
 - Message Type: Invite
 - Condition: Header.Diversion exists

At the bottom of the window, there are "Cancel" and "APPLY" buttons.



Note: Due to fact that Cisco CUCM can be configured in different ways (e.g. to use SIP REFER Message or Re-INVITE for Call Transfer scenarios), different Message Manipulation Rules may be need to be configured.

Figure 4-25: Example of Configured SIP Message Manipulation Rules

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Change R-URI host to	2	Any.Request		Header:Request-URI	Modify	Param.Message.Add	Use Current Condi
1	Reject Responses	4	any.response	header.request-uri.n	header.request-uri.n	Modify	'503'	Use Current Condi
2	Call Forward	4	Invite	Header.Diversion.ex	Header.P-Asserted-Id	Modify	Header.Diversion.UR	Use Current Condi

5. Assign Manipulation Set ID 2 to the IP-PBX IP Group:
 - a. Open the IP Groups table (**Setup menu > Signaling & Media tab > Core Entities folder > IP Groups**).
 - b. Select the row of the IP-PBX IP Group, and then click **Edit**.
 - c. Set the 'Outbound Message Manipulation Set' field to **2**.

Figure 4-26: Assigning Manipulation Set to the IP-PBX IP Group

IP Groups
[IP-PBX] - x

SRD

GENERAL

Index:

Name:

Topology Location:

Type:

Proxy Set: [View](#)

IP Profile: [View](#)

Media Realm: [View](#)

Contact User:

SIP Group Name:

Created By Routing Server:

QUALITY OF EXPERIENCE

QoE Profile: [View](#)

Bandwidth Profile: [View](#)

MESSAGE MANIPULATION

Inbound Message Manipulation Set:

Outbound Message Manipulation Set:

Message Manipulation User-Defined String 1:

Message Manipulation User-Defined String 2:

[Cancel](#) [APPLY](#)

- d. Click **Apply**.

6. Assign Manipulation Set ID 4 to the BroadCloud SIP trunk IP Group:
 - a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
 - b. Select the row of the BroadCloud SIP trunk IP Group, and then click **Edit**.
 - c. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-27: Assigning Manipulation Set 4 to the BroadCloud SIP Trunk IP Group

The screenshot shows the configuration page for an IP Group named 'BroadCloud'. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. The page is divided into several sections: 'GENERAL', 'QUALITY OF EXPERIENCE', 'MESSAGE MANIPULATION', and 'SBC REGISTRATION AND AUTHENTICATION'. The 'MESSAGE MANIPULATION' section is expanded, showing the following fields:

- Inbound Message Manipulation Set: -1
- Outbound Message Manipulation Set: 4
- Message Manipulation User-Defined String 1: (empty)
- Message Manipulation User-Defined String 2: (empty)

At the bottom of the form, there are 'Cancel' and 'APPLY' buttons.

- d. Click **Apply**.

4.10 Step 10: Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the BroadCloud SIP Trunk on behalf of the IP-PBX. The BroadCloud SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is IP-PBX IP Group and the Serving IP Group is BroadCloud SIP Trunk IP Group.

➤ **To configure a registration account:**

1. Open the Account Table page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Enter an index number (e.g., "0"), and then click **Add**.
3. Configure the account according to the provided information from , for example:

Parameter	Value
Application Type	SBC
Served IP Group	IP-PBX
Serving IP Group	BroadCloud
Username	As provided by BroadCloud
Password	As provided by BroadCloud
Host Name	interop.adpt-tech.com
Register	Regular
Contact User	8325624857 (pilot number)

4. Click **Apply**.

Figure 4-28: Configuring SIP Registration Account

INDEX	APPLICATION TYPE	SERVED TRUNK GROUP	SERVED IP GROUP	SERVING IP GROUP	USER NAME	PASSWORD	HOST NAME	REGISTER	CONTACT USER
0	SBC	-1	IP-PBX	BroadCloud	8325624857	*	interop.adpt-t	Regular	8325624857

4.11 Step 11: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

4.11.1 Step 11a: Configure SBC Alternative Routing Reasons

This step describes how to configure the E-SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case E-SBC attempts to locate an alternative route for the call.

➤ **To configure SIP reason codes for alternative IP routing:**

1. Open the SBC Alternative Routing Reasons page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons**).
2. Click **Add**; the following dialog box appears:

Figure 4-29: SBC Alternative Routing Reasons Table - Add Record

GENERAL	
Index	<input type="text" value="0"/>
Release Cause	<input type="text" value="503 Service Unavailable"/>

3. Click **Apply**.

4.12 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 (**Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**).

Figure 4-30: Resetting the E-SBC

Maintenance Actions

RESET DEVICE	LOCK / UNLOCK
Reset Device <input type="button" value="Reset"/>	Lock <input type="button" value="LOCK"/>
Save To Flash Yes <input type="button" value="v"/>	Graceful Option No <input type="button" value="v"/>
Graceful Option No <input type="button" value="v"/>	Gateway Operational State UNLOCKED

For Reset Device : If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset.

For Save Configuration: Saving configuration to flash memory may cause some temporary degradation in voice quality, therefore, it is recommended to perform this during low-traffic periods

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

A AudioCodes INI File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 3.1 on page 13, is shown below:



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

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

[SYSTEM Params]

SyslogServerIP = 10.10.10.10
EnableSyslog = 1
NTPServerUTCOffset = 7200
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.10.0.1'
;LastConfigChangeTime is hidden but has non-default value
SBCWizardFilename = 'templates4.zip'
;BarrierFilename is hidden but has non-default value
;LocalTimeZoneName is hidden but has non-default value
PM_gwINVITEDialogs = '1,475,500,15'
PM_gwSUBSCRIBEDialogs = '1,3800,4000,15'
PM_gwSBCRegisteredUsers = '1,95,100,15'
PM_gwSBCMediaLegs = '1,475,500,15'
PM_gwSBCTranscodingSessions = '1,13,15,15'

[BSP Params]

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

[Analog Params]

[ControlProtocols Params]

AdminStateLockControl = 0

[PSTN Params]

V5ProtocolSide = 0

[Voice Engine Params]

ENABLEMEDIASECURITY = 1
CallProgressTonesFilename = 'usa_tones_13.dat'
```

```

[WEB Params]

UseProductName = 1
;HTTSPKeyFileName is hidden but has non-default value
FaviconCurrentVersion = 2
Languages = 'en-US', '', '', '', '', '', '', '', ''

[SIP Params]

MEDIACHANNELS = 200
REGISTRATIONTIME = 180
GWDEBUGLEVEL = 5
USERAGENTDISPLAYINFO = 'BCLD-AudioCodes-Sip-SBCM800B'
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESEMODE = 1
MEDIACDRREPORTLEVEL = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SNMP Params]

[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging, DeviceTable_MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.77.55, 16, 10.15.0.1, "Voice",
10.15.27.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.153, 24, 195.189.192.129, "WANSP",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_CliSessionLimit, WebUsers_SessionTimeout, WebUsers_BlockTime,
WebUsers_UserLevel, WebUsers_PwNonce, WebUsers_SSHPublicKey;
    
```

```

WebUsers 0 = "Admin",
"$1$bgtDFkgQREJNFRNJHUhDGRtPTuPju+bhteClubG4vby9t7fy9fbloqfyoKmt+KP5/qz9m
ZSTlpyUkpDNzMudz54=", 1, 0, 5, -1, 15, 60, 200,
"e4064f90b5b26631d46fbcdb79f2b7a0", ".fc";
WebUsers 1 = "User",
"$1$Cj46OmhtN3ElJiolcSQnfXh4Ii5+Jn4ZRBQRHR0fHx4bTB9ITE8aVgRQVQUGAAEPXVkcD
w0GWSEgIHN0dHB2LHE=", 1, 0, 5, -1, 15, 60, 50,
"c26a27dd91a886b99de5e81b9a736232", "";

[ \WebUsers ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_DTLSVersion, TLSContexts_ServerCipherString,
TLSContexts_ClientCipherString, TLSContexts_RequireStrictCert,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse, TLSContexts_DHKeySize;
TLSContexts 0 = "default", 7, 0, "RC4:EXP", "ALL:!ADH", 0, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;

[ \TLSContexts ]

[ AudioCodersGroups ]

FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";
AudioCodersGroups 1 = "AudioCodersGroups_1";

[ \AudioCodersGroups ]

[ AllowedAudioCodersGroups ]

FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name;
AllowedAudioCodersGroups 0 = "BroadCloud Allowed Coders";
AllowedAudioCodersGroups 1 = "IP-PBX Allowed Coders";

[ \AllowedAudioCodersGroups ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ,
IpProfile_RTPRedundancyDepth, 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_SBCExtensionCodersGroupName,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,

```

```

IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCSendMultipleDTMFMethods,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionMode,
IpProfile_SBCHistoryInfoMode, IpProfile_EnableQSIGTunneling,
IpProfile_SBCFaxCodersGroupName, 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_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandlerTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWTtoVoiceCoderBW,
IpProfile_CreatedByRoutingServer, IpProfile_SBCFaxReroutingMode,
IpProfile_SBCMaxCallDuration, IpProfile_SBCGenerateRTP,
IpProfile_SBCISUPBodyHandling, IpProfile_SBCISUPVariant,
IpProfile_SBCVoiceQualityEnhancement, IpProfile_SBCMaxOpusBW,
IpProfile_SBCEnhancedPlc, IpProfile_LocalRingbackTone,
IpProfile_LocalHeldTone, IpProfile_SBCGenerateNoOp,
IpProfile_SBCRemoveUnknownCrypto;

IpProfile 1 = "IP-PBX", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "", 0, 0,
"", "", "", 0, 2, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0,
2, 2, 1, 3, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1,
-1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0;

IpProfile 2 = "BroadCloud", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24,
0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_1", 0, 0, "", "BroadCloud Allowed Coders", "", 2, 2,
0, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 3, 2, 1,
0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1,
0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0,
0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0;

[ \IpProfile ]

[ CpMediaRealm ]
    
```

```

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_RemoteIPv4IF,
CpMediaRealm_RemoteIPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile,
CpMediaRealm_TopologyLocation;
CpMediaRealm 0 = "MRLan", "Voice", "", "", "", 6000, 250, 8499, 1, "",
"", 0;
CpMediaRealm 1 = "MRWan", "WANSP", "", "", "", 6000, 250, 8499, 0, "",
"", 1;

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength,
SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName, SRD_AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "",
"";

[ \SRD ]

[ MessagePolicy ]

FORMAT MessagePolicy_Index = MessagePolicy_Name,
MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength,
MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders,
MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection,
MessagePolicy_MethodList, MessagePolicy_MethodListType,
MessagePolicy_BodyList, MessagePolicy_BodyListType,
MessagePolicy_UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;

[ \MessagePolicy ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_AdditionalUDPPorts, SIPInterface_SRDName,
SIPInterface_MessagePolicyName, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,

```

```

SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation,
SIPInterface_PreParsingManSetName, SIPInterface_AdmissionProfile;
SIPInterface 0 = "SIPInterface_LAN", "Voice", 2, 5060, 5060, 0, "",
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1,
0, 0, "", "";
SIPInterface 1 = "SIPInterface_WAN", "WANSP", 2, 5060, 0, 0, "",
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1,
0, 1, "", "";

[ \SIPInterface ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName,
ProxySet_SBCIPv6SIPInterfaceName, ProxySet_MinActiveServersLB,
ProxySet_SuccessDetectionRetries, ProxySet_SuccessDetectionInterval,
ProxySet_FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "SIPInterface_LAN", "", "", 1, 1, 10, -1;
ProxySet 1 = "IP-PBX", 1, 60, 0, 0, "DefaultSRD", 0, "default", -1, -1,
"", "", "SIPInterface_LAN", "", "", 1, 1, 10, -1;
ProxySet 2 = "BroadCloud", 1, 60, 0, 1, "DefaultSRD", 0, "default", 1, 1,
"", "", "SIPInterface_WAN", "", "", 1, 1, 10, -1;

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId, IPGroup_Tags, IPGroup_SBCUserStickiness,
IPGroup_UserUDPPortAssignment, IPGroup_AdmissionProfile;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 0, "", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "$1$gQ==", 0, "", "",
0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "";
IPGroup 1 = 0, "IP-PBX", "IP-PBX", "interop.adpt-tech.com", "", -1, 0,
"DefaultSRD", "MRLan", 1, "IP-PBX", -1, -1, 2, 0, 0, "", 0, -1, -1, "",
    
```

```

"Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1,
0, 0, 0, "", -1, "", 0, 0, "";
IPGroup 2 = 0, "BroadCloud", "BroadCloud", "interop.adpt-tech.com", "", -
1, 0, "DefaultSRD", "MRWan", 1, "BroadCloud", -1, -1, 4, 0, 0, "", 0, -1,
-1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0,
0, -1, 0, 0, 1, "", -1, "", 0, 0, "";

[ \IPGroup ]

[ SBCAlternativeRoutingReasons ]

FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

[ \SBCAlternativeRoutingReasons ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "1", 0, "10.15.28.101:5060", 0;
ProxyIp 1 = "2", 0, "nn6300southsipconnect.adpt-tech.com", 0;

[ \ProxyIp ]

[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_ContactUser,
Account_Register, Account_RegistrarStickiness,
Account_RegistrarSearchMode, Account_RegEventPackageSubscription,
Account_ApplicationType, Account_RegByServedIPG,
Account_UDPPortAssignment;
Account 0 = -1, "IP-PBX", "BroadCloud", "8325624857",
"$1$jt/69vP78vC0ruL8uA==", "interop.adpt-tech.com", "8325624857", 1, 0,
0, 0, 2, 0, 0;

[ \Account ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags,
IP2IPRouting_SrcTags, IP2IPRouting_IPGroupSetName,
IP2IPRouting_RoutingTagName, IP2IPRouting_InternalAction;

```

```

IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*, "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 1 = "IP-PBX to ITSP", "Default_SBCRoutingPolicy", "IP-PBX",
"*, "*", "*", "*", 0, "", "Any", 0, -1, 0, "BroadCloud", "", "", 0, -1,
0, 0, "", "", "", "", "default", "";
IP2IPRouting 2 = "ITSP to IP-PBX", "Default_SBCRoutingPolicy",
"BroadCloud", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "IP-PBX", "",
"", 0, -1, 0, 0, "", "", "", "", "default", "";

[ \IP2IPRouting ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Change R-URI host toward IP-PBX", 2,
"Any.Request", "", "Header.Request-URI.URL.Host", 2,
"Param.Message.Address.Dst.Address", 0;
MessageManipulations 1 = "Reject Responses", 4, "any.response",
"header.request-uri.methodtype=='486'", "header.request-uri.methodtype",
2, "'503'", 0;
MessageManipulations 2 = "Call Forward", 4, "Invite", "Header.Diversion
exists", "Header.P-Asserted-Identity.URL.User", 2,
"Header.Diversion.URL.User", 0;

[ \MessageManipulations ]

[ GwRoutingPolicy ]

FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name,
GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength,
GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ \GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]

[ MaliciousSignatureDB ]
    
```



```

FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name,
MaliciousSignatureDB_Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'";
MaliciousSignatureDB 2 = "Smapp", "Header.User-Agent.content prefix
'smapp'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix
'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix
'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content
prefix 'siparmyknife'";

[ \MaliciousSignatureDB ]

[ AllowedAudioCoders ]

FORMAT AllowedAudioCoders_Index =
AllowedAudioCoders_AllowedAudioCodersGroupName,
AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID,
AllowedAudioCoders_UserDefineCoder;
AllowedAudioCoders 2 = "BroadCloud Allowed Coders", 0, 3, "";
AllowedAudioCoders 3 = "BroadCloud Allowed Coders", 1, 1, "";
AllowedAudioCoders 4 = "BroadCloud Allowed Coders", 2, 2, "";

[ \AllowedAudioCoders ]

[ AudioCoders ]

FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId,
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,
AudioCoders_CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 2, 2, 90, -1, 1, "";
AudioCoders 1 = "AudioCodersGroups_0", 1, 1, 2, 90, -1, 1, "";
AudioCoders 2 = "AudioCodersGroups_1", 0, 3, 2, 19, -1, 0, "";
AudioCoders 3 = "AudioCodersGroups_1", 1, 1, 2, 90, -1, 0, "";
AudioCoders 4 = "AudioCodersGroups_1", 2, 2, 2, 90, -1, 0, "";

[ \AudioCoders ]

```


International Headquarters

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

AudioCodes Inc.

27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Website: <https://www.audiocodes.com/>

©2018 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-12731

