Configuration Note

AudioCodes Professional Services – Interoperability Lab

Connecting Unify OpenScape Voice with Microsoft® Teams Direct Routing Enterprise Model using AudioCodes Mediant™ SBC

Version 7.2

Microsoft Partner

Gold Communications

Microsoft Teams

Table of Contents

1 Introduction 7

1.1 Intended Audience 7
1.2 About Microsoft Teams Direct Routing 7
1.3 About AudioCodes SBC Product Series 7

2 Component Information 9

2.1 AudioCodes SBC Version 9
2.2 Unify OpenScape Voice Components and Version 9
2.3 Microsoft Teams Direct Routing Version 9
2.4 Interoperability Test Topology 10
2.4.1 Enterprise Model Implementation 10
2.4.2 Environment Setup 11
2.4.3 Infrastructure Prerequisites 11
2.4.4 Known Limitations 11

3 Configuring Teams Direct Routing 13

3.1 Prerequisites 13
3.2 SBC Domain Name in the Teams Enterprise Model 13
3.3 Example of the Office 365 Tenant Direct Routing Configuration 14
3.3.1 Online PSTN Gateway Configuration 14
3.3.2 Online PSTN Usage Configuration 14
3.3.3 Online Voice Route Configuration 14
3.3.4 Online Voice Routing Policy Configuration 14
3.3.5 Enable Online User 15
3.3.6 Assigning Online User to the Voice Route 15

4 Configuring Unify OpenScape Voice 17

4.1 OS Voice Firewall 17
4.2 Configuring Endpoints 18
4.3 Destinations & Routes 26
4.4 Translation 28
4.5 Media Server Secure Media Setting 31

5 Configuring AudioCodes SBC 33

5.1 SBC Configuration Concept in Teams Direct Routing Enterprise Model 34
5.2 IP Network Interfaces Configuration 34
5.2.1 Configure VLANs 35
5.2.2 Configure Network Interfaces 35
5.3 SIP TLS Connection Configuration 37
5.3.1 Configure the NTP Server Address 37
5.3.2 Create a TLS Context for Teams Direct Routing 38
5.3.3 Configure a Certificate 39
5.3.4 Method of Generating and Installing the Wildcard Certificate 42
5.3.5 Deploy Baltimore Trusted Root Certificate 43
5.4 Configure Media Realms 44
5.5 Configure SIP Signaling Interfaces 45
5.6 Configure Proxy Sets and Proxy Address 46
5.6.1 Configure a Proxy Address 47
5.7 Configure Coders 49

5.8 Configure IP Profiles....51
5.9 Configure IP Groups....54
5.10 Configure SRTP....56
5.11 Configuring Message Condition Rules....57
5.12 Configuring Classification Rules....58
5.13 Configure IP-to-IP Call Routing Rules....59
5.14 Configuring Firewall Settings....60
5.15 Configure Number Manipulation Rules....61
5.16 Configure Message Manipulation Rules....62
5.17 Miscellaneous Configuration....66
5.17.1 Configure Call Forking Mode....66
5.17.2 Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only)....67

A AudioCodes INI File....69

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: March-18-2020

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
39325	Initial document release for Version 7.2.

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://online.audiocodes.com/doc-feedback.

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between Unify OpenScape Voice and Microsoft's Teams Direct Routing environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the SBC based on this interoperability setup. However, it is recommended to read through this document to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including the download option, visit AudioCodes Web site at https://www.audiocodes.com/partners/sbc-interoperability-list.

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and Unify OpenScape Voice partners who are responsible for installing and configuring Unify OpenScape Voice and Microsoft's Teams Direct Routing Service in Enterprise Model for enabling VoIP calls using AudioCodes SBC.

1.2 About Microsoft Teams Direct Routing

Microsoft Teams Direct Routing allows connecting a customer-provided SBC to the Microsoft Phone System. The customer-provided SBC can be connected to almost any telephony trunk, or connect with third-party PSTN equipment. The connection allows:

- Using virtually any PSTN trunk with Microsoft Phone System
- Configuring interoperability between customer-owned telephony equipment, such as third-party PBXs, analog devices, and Microsoft Phone System

1.3 About AudioCodes SBC Product Series

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

The 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 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 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. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWS, AZURE, AWP, KVM and VMWare.

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 800C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant 9030 SBC ▪ Mediant 9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.20A.254.376 or later
Protocol	▪ SIP/UDP (to the Unify OpenScape Voice) ▪ SIP/TLS (to the Teams Direct Routing)
Additional Notes	None

2.2 Unify OpenScape Voice Components and Version

Table 2-2: Unify OpenScape Voice Components and Version

Vendor/Service Provider	Unify
SSW Model/Service	OpenScape Voice
Software Version	V9 R4.45.3
Protocol	SIP
Additional Notes	None

2.3 Microsoft Teams Direct Routing Version

Table 2-3: Microsoft Teams Direct Routing Version

Vendor	Microsoft
Model	Teams Phone System Direct Routing
Software Version	v.2019.10.29.2 i.EUWE.1
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

Microsoft Teams Direct Routing can be implemented in the *Enterprise* or *Hosting* Models.

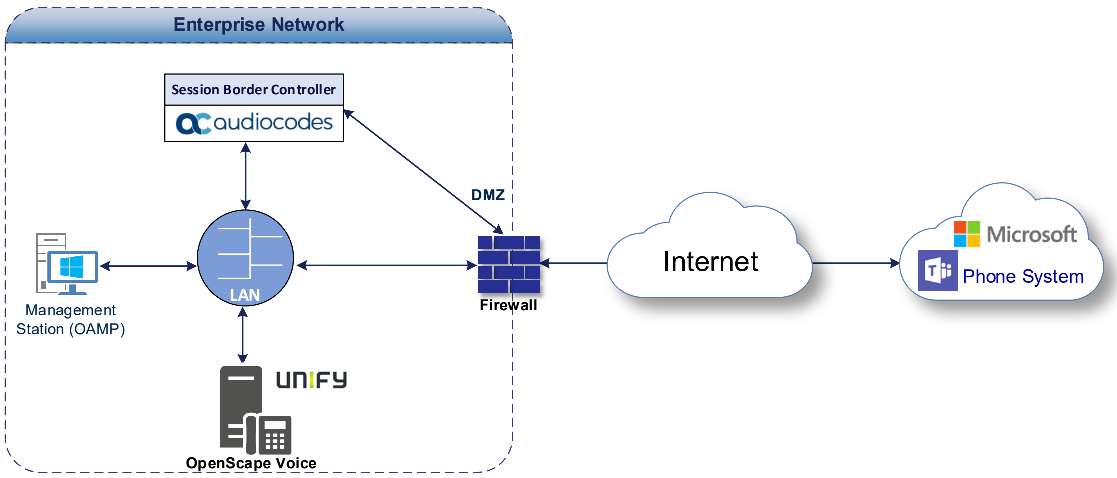
2.4.1 Enterprise Model Implementation

The interoperability testing between AudioCodes SBC and Unify OpenScape Voice with Teams Direct Routing Enterprise Model was done using the following topology setup:

- Enterprise deployed with Unify OpenScape Voice as IP-PBX, analog devices and the administrator's management station, located on the LAN
- Enterprise deployed with Microsoft Teams Phone System Direct Routing Interface located on the WAN for enhanced communication within the Enterprise
- AudioCodes SBC is implemented to interconnect between the Unify OpenScape Voice in the Enterprise LAN and Microsoft Teams on the WAN
    - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
    - **Border:** IP-to-IP network border - the Unify OpenScape Voice is located in the Enterprise LAN and the Microsoft Teams Phone Systems is located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between SBC and Microsoft Teams Direct Routing Enterprise Model with Unify OpenScape Voice



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Microsoft Teams Direct Routing environment is located on the Enterprise's (or Service Provider's) WAN ▪ Unify OpenScape Voice is located on the LAN
Signaling Transcoding	▪ Microsoft Teams Direct Routing operates with SIP-over-TLS transport type ▪ Unify OpenScape Voice operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Teams Direct Routing supports G.711A-law, G.711U-law, G.729, G.722 and SILK (NB and WB) coders ▪ Unify OpenScape Voice supports G.711A-law and G.711U-law coders
Media Transcoding	▪ Microsoft Teams Direct Routing operates with SRTP media type ▪ Unify OpenScape Voice operates with RTP media type

2.4.3 Infrastructure Prerequisites

The table below shows the list of infrastructure prerequisites for deploying Microsoft Teams Direct Routing.

Table 2-5: Infrastructure Prerequisites

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's document *Plan Direct Routing*.
SIP Trunks connected to the SBC	
Office 365 Tenant	
Domains	
Public IP address for the SBC	
Fully Qualified Domain Name (FQDN) for the SBC	
Public DNS entry for the SBC	
Public trusted certificate for the SBC	
Firewall ports for Direct Routing Signaling	
Firewall IP addresses and ports for Direct Routing Media	
Media Transport Profile	
Firewall ports for Teams Clients Media	

2.4.4 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes SBC interworking between Microsoft Teams Direct Routing and Unify OpenScape Voice.

This page is intentionally left blank.

3 Configuring Teams Direct Routing

This section describes how to configure Microsoft Teams Direct Routing to operate with AudioCodes SBC.

3.1 Prerequisites

Before you begin configuration, make sure you have the following for every SBC you want to pair:

- Public IP address
- FQDN name matching SIP addresses of the users
- Public certificate, issued by one of the supported CAs

3.2 SBC Domain Name in the Teams Enterprise Model

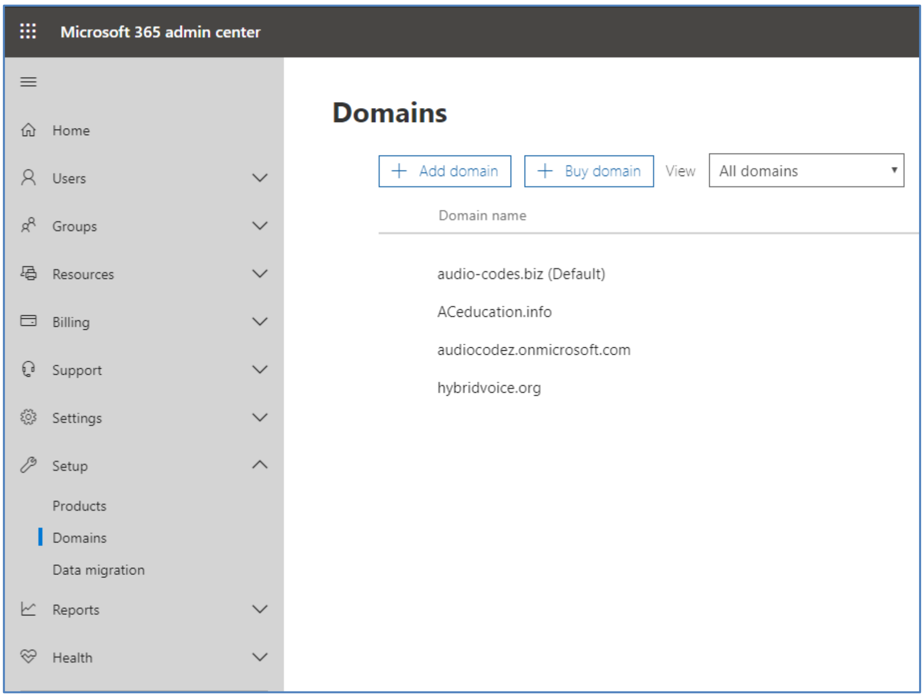
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 2-2, the administrator registered the following DNS names for the tenant:

Table 3-1: DNS Names Registered by an Administrator for a Tenant

DNS name	Can be used for SBC FQDN	Examples of FQDN names
ACeducation.info	Yes	**Valid names**: ▪ sbc.ACeducation.info ▪ ussbcs15.ACeducation.info ▪ europe.ACeducation.info **Invalid name:** sbc1.europe.ACeducation.info (requires registering domain name europe.atatum.biz in 'Domains' first)
adatumbiz.onmicrosoft.com	No	Using ***.onmicrosoft.com** domains is not supported for SBC names
hybridvoice.org	Yes	**Valid names**: ▪ sbc1.hybridvoice.org ▪ ussbcs15.hybridvoice.org ▪ europe.hybridvoice.org **Invalid name:** sbc1.europe.hybridvoice.org (requires registering domain name europe.hybridvoice.org in 'Domains' first

Users can be from any SIP domain registered for the tenant. For example, you can provide users user@ACeducation.info with the SBC FQDN **sbc1.hybridvoice.org** so long as both names are registered for this tenant.

Figure 3-1: Example of Registered DNS Names



During creation of the Domain you will be forced to create public DNS record (**sbc1.hybridvoice.org** in our example.)

3.3 Example of the Office 365 Tenant Direct Routing Configuration

3.3.1 Online PSTN Gateway Configuration

Use following PowerShell command for creating new Online PSTN Gateway:

New-CsOnlinePSTNGateway *-Identity* ***sbc1.hybridvoice.org*** *-SipSignallingPort* ***5067*** *-ForwardCallHistory $True -ForwardPai $True -MediaBypass $True -Enabled $True*

3.3.2 Online PSTN Usage Configuration

Use following PowerShell command for creating an empty PSTN Usage:

Set-CsOnlinePstnUsage *-Identity Global -Usage @{Add="**Interop**"}*

3.3.3 Online Voice Route Configuration

Use following PowerShell command for creating new Online Voice Route and associate it with PSTN Usage:

New-CsOnlineVoiceRoute *-Identity* ***"audc-interop"*** *-NumberPattern "^\+" -OnlinePstnGatewayList* ***sbc1.hybridvoice.org*** *-Priority 1 -OnlinePstnUsages* ***"Interop"***

3.3.4 Online Voice Routing Policy Configuration

Use following PowerShell command for assigning the Voice Route to the PSTN Usage:

New-CsOnlineVoiceRoutingPolicy "audc-interop" *-OnlinePstnUsages* ***"Interop"***

Note: The commands specified in Sections 3.3.5 and 3.3.6, should be run for each Teams user in the company tenant.

3.3.5 Enable Online User

Use following PowerShell command for enabling online user:

Set-CsUser *-Identity* ***user1@company.com*** *-EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:****+12345678901***

3.3.6 Assigning Online User to the Voice Route

Use following PowerShell command for assigning online user to the Voice Route:

Grant-CsOnlineVoiceRoutingPolicy *-PolicyName* ***"audc-interop"*** *-Identity* ***user1@company.com***

Use the following command on the Microsoft Teams Direct Routing Management Shell after reconfiguration to verify correct values:

- **Get-CsOnlinePSTNGateway**

```
Identity                           : sbc1.hybridvoice.org
Fqdn                               : sbc1.hybridvoice.org
SipSignallingPort                  : 5067
FailoverTimeSeconds                : 10
ForwardCallHistory                 : True
ForwardPai                         : True
SendSipOptions                     : True
MaxConcurrentSessions              :
Enabled                            : True
MediaBypass                        : True
GatewaySiteId                      :
GatewaySiteLbrEnabled              : False
FailoverResponseCodes              : 408,503,504
GenerateRingingWhileLocatingUser   : True
PidfLoSupported                    : False
MediaRelayRoutingLocationOverride  :
ProxySbc                           :
BypassMode                         : None
```

This page is intentionally left blank.

4 Configuring Unify OpenScape Voice

This section refers to OpenScape (OS) Voice related configuration for the needs of the current certification project. No reference will be made to routine OS Voice (and other Unify components) configurations because it is out of the scope of this document.

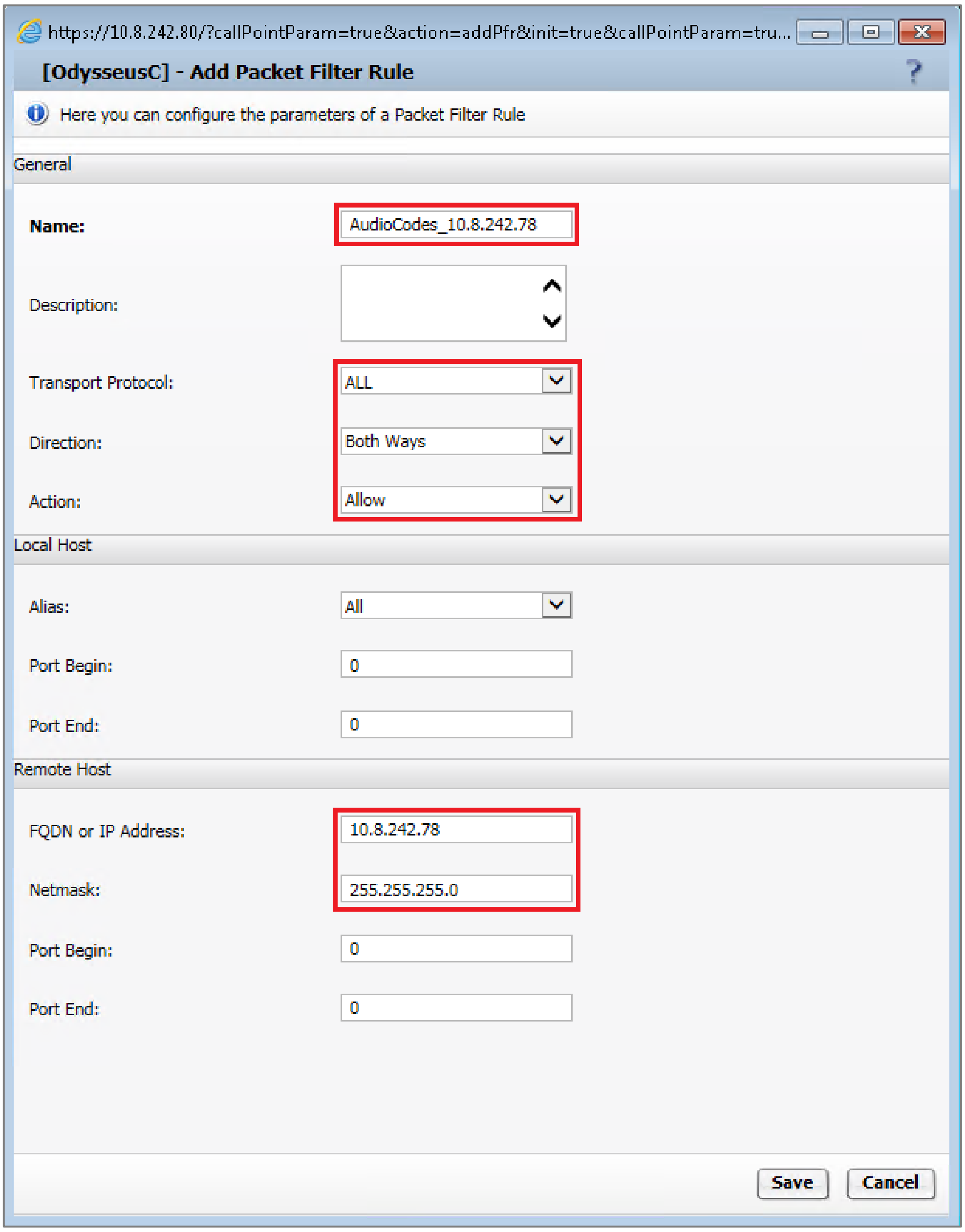
4.1 OS Voice Firewall

For the SBC to communicate with OS Voice via SIP, a firewall rule (packet filter rule) is added to OS Voice.

➢ **To add a packet filter rule:**

1. Go to **CMP** > **Configuration** > **OpenScape Voice** > **Administration** > **General Settings** > **Packet Filter Rules**.

Figure 4-1: Add Packet Filter Rule



2. Click **Add** and configure the following to allow incoming/outgoing traffic:

Parameter	Value
Name	**AudioCodes_10.8.242.64** (a common-sense name)
Transport Protocol	**ALL** (depending on customer requirements, we could configure e.g. UDP only)
Direction	**Both Ways**
Action	**Allow**
FQDN or IP Address	**10.8.242.78** (SBC LAN interface)
Netmask	**255.255.255.0**

3. Click **Save**.

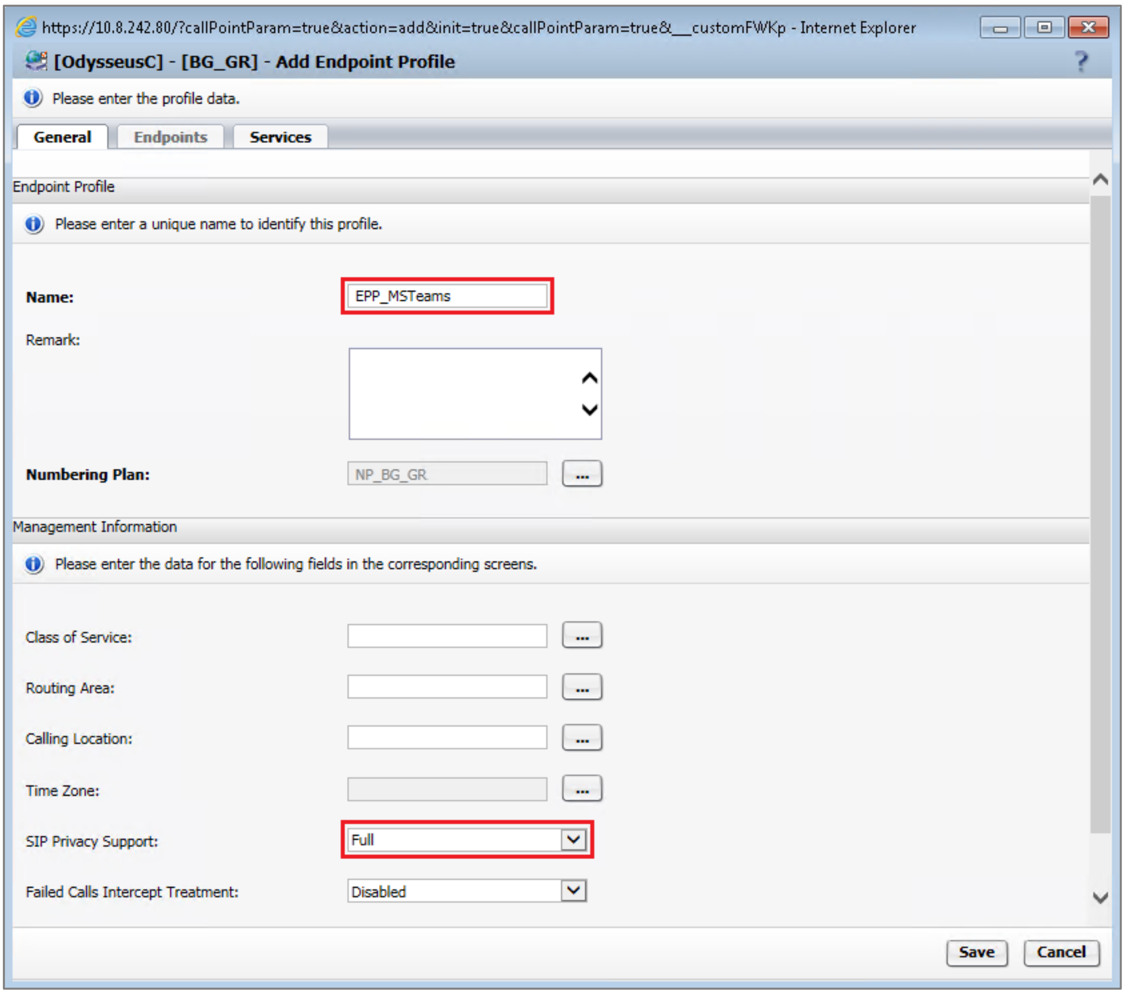
4.2 Configuring Endpoints

This section describes how to configure endpoints. An **Endpoint** is a network component, such as an originating or terminating device, and in our case the AudioCodes SBC. An endpoint can be a Directory Number (DN) that does not have a number associated with it yet. An Endpoint Profile enables the administrator to set parameters for that endpoint.

➢ **To create a new endpoint:**

1. Go to **CMP** > **Configuration** > **OpenScape Voice** > **Business Group** > **Profiles** > **Endpoint** to configure the **Endpoint Profile**.

Figure 4-2: Endpoint Profile



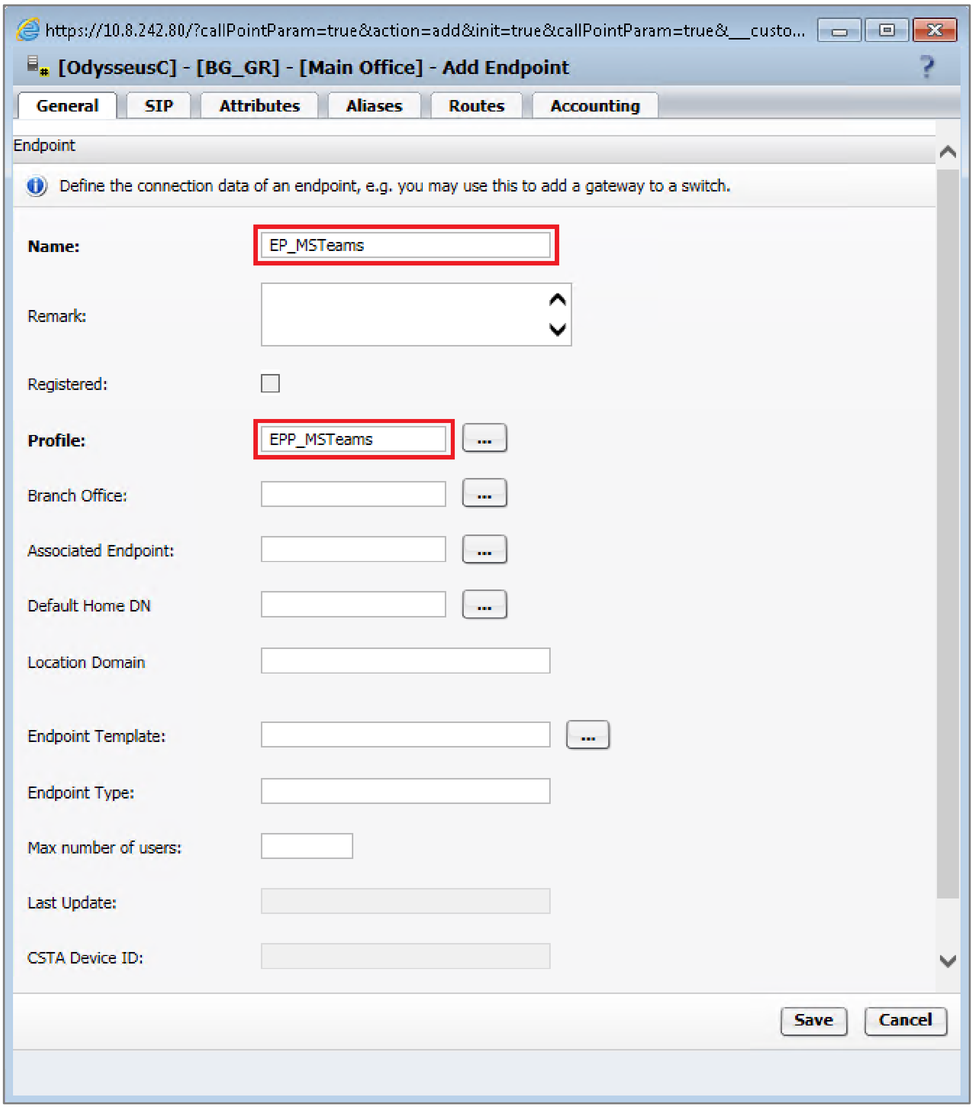
2. Click **Add** on the **General** tab, enter the following:

Parameter	Value
Name	**EPP_MSTeams** (a common-sense name)
SIP Privacy Support	**Full** (to enable RFC 3325 behavior - OS Voice sends a P-Asserted-Identity (or a to P-Preferred-Identity) header field in the messages (requests and responses) to the endpoint; the OS Voice SHALL also accept any received P-Asserted-Identity header fields).

3. Click **Save**.
4. Go to **CMP** > **Configuration** > **OpenScape Voice** > **Business Group** > **Members** > **Endpoints** to configure the Endpoint Profile.
5. Click **Add** on **General** tab, enter the following:

Parameter	Value
Name	**EP_MSTeams** (a common-sense name)
Profile	**EPP_MSTeams** (select previously created endpoint profile)

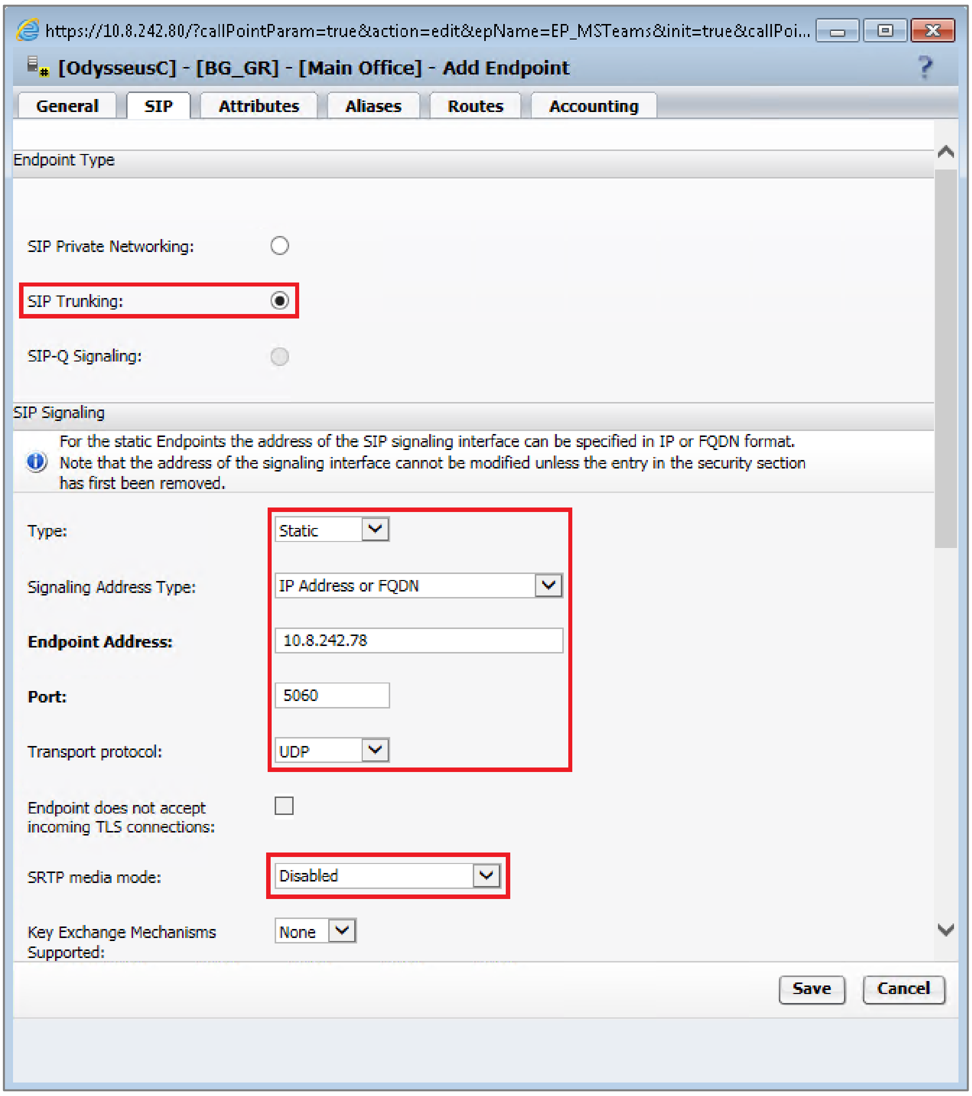
Figure 4-3: Endpoint



6. Select the **SIP** tab, and then enter the following:

Parameter	Value
SIP Trunking	**Enabled**
Type	**Static**
Signaling Address Type	**IP Address or FQDN**
Endpoint Address	**10.8.242.78** (SBC LAN interface)
Port	**5060** (default setting, as configured in SBC)
Transport protocol	**UDP** (as configured in SBC)
SRTP media mode	**Disabled**

Figure 4-4: Endpoint SIP Tab



7. Select the **Attributes** tab, and configure the following:

Parameter	Value
Send International Numbers in GNF	**Enabled** (when selected (enabled), the OS Voice adds a '+' in front of all numbers which have NPI = PUBLIC and NOA = INTERNATIONAL.To do this, both Translation and the Display Number Modification tables MUST be provisioned to send numbers with NPI = PUBLIC and NOA = INTERNATIONAL to this endpoint).
Limited PRACK Support	**Static** (the PRACK-Lite feature provides a limited form of RFC3262 PRACK within OS Voice, supporting PRACK on a half-call basis and only for SIP network-network interfaces)

Figure 4-5: Endpoint Attributes

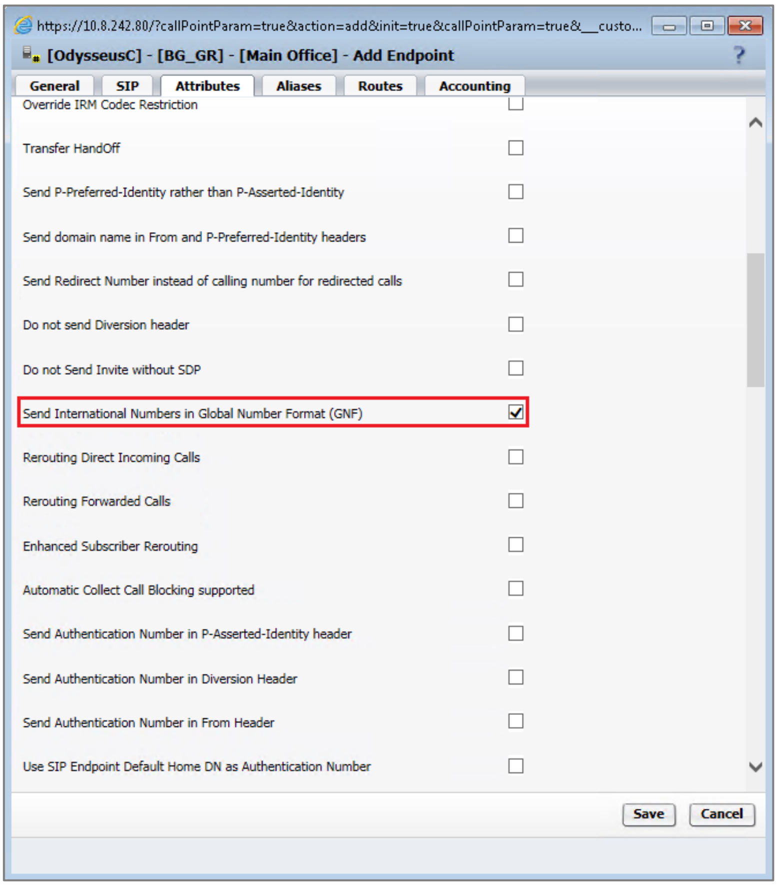
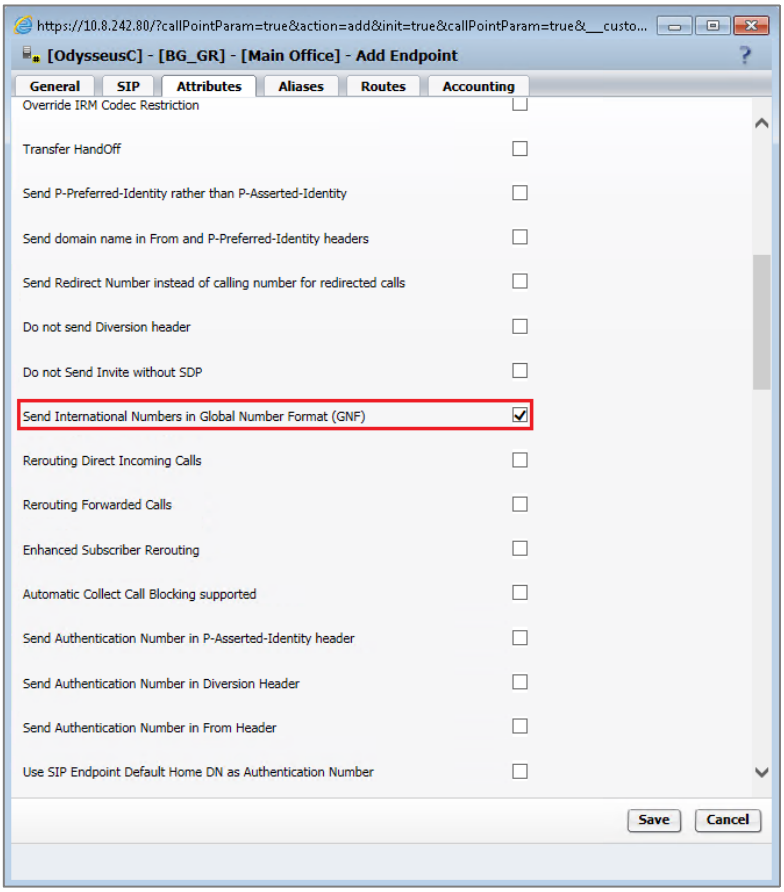
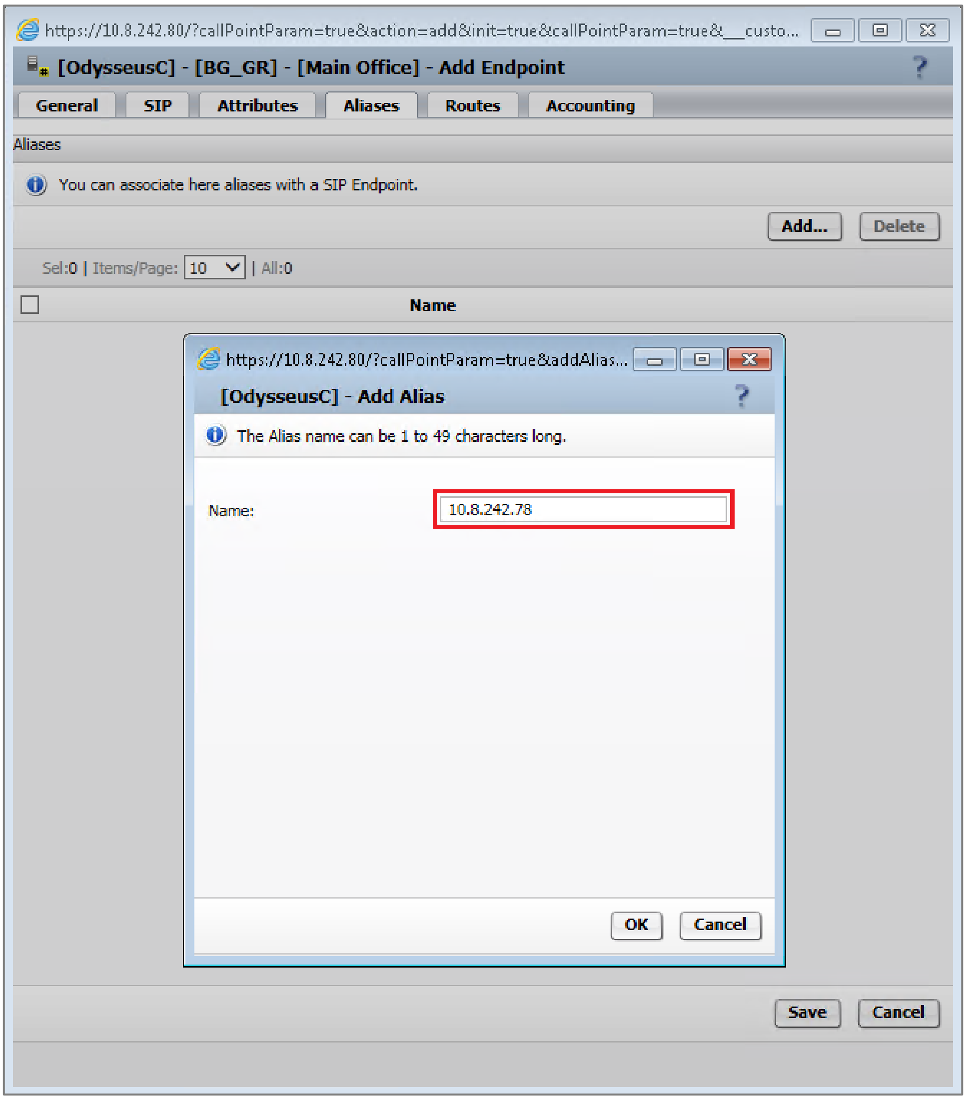


Figure 4-6: Add Endpoint



8. Select the **Aliases** tab, and then click **Add**. Enter the following:
   - **Name:** **10.8.242.78** (the SBC LAN interface for incoming SIP traffic; if there is a need to restrict the port 5060, the value 10.8.242.78:5060 should be entered, instead)

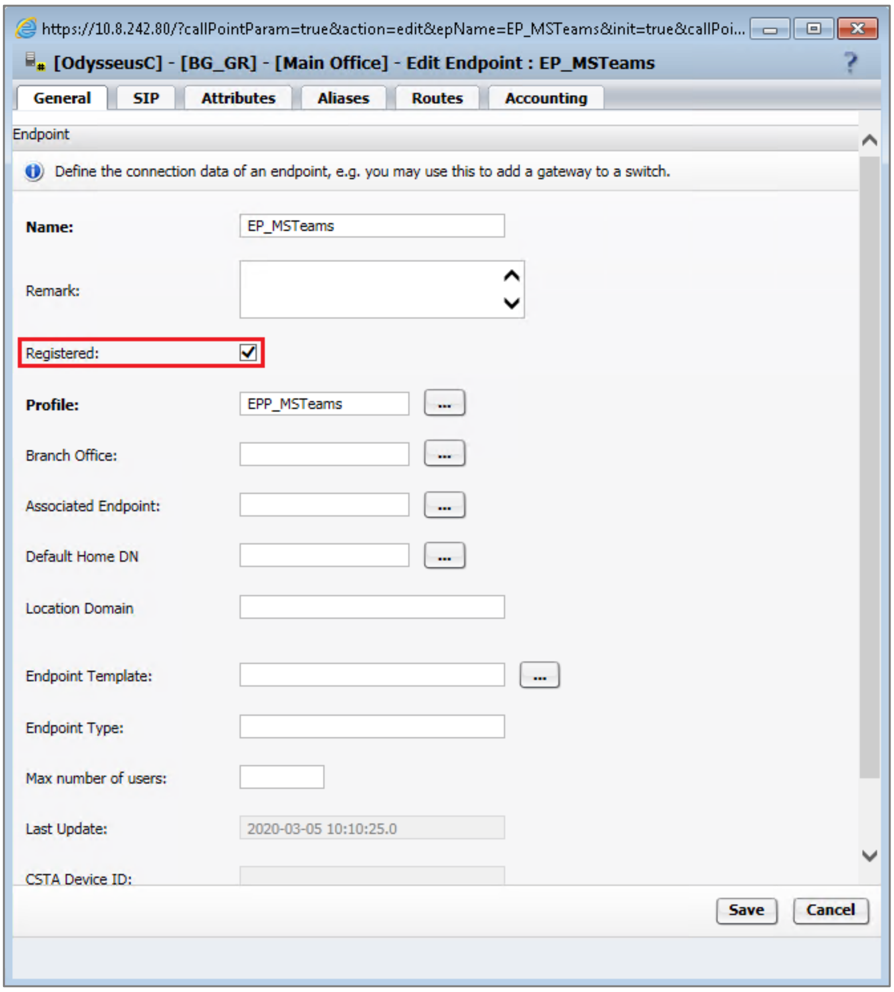
Figure 4-7: Endpoint Aliases



9. Click **OK,** and then click **Save**.

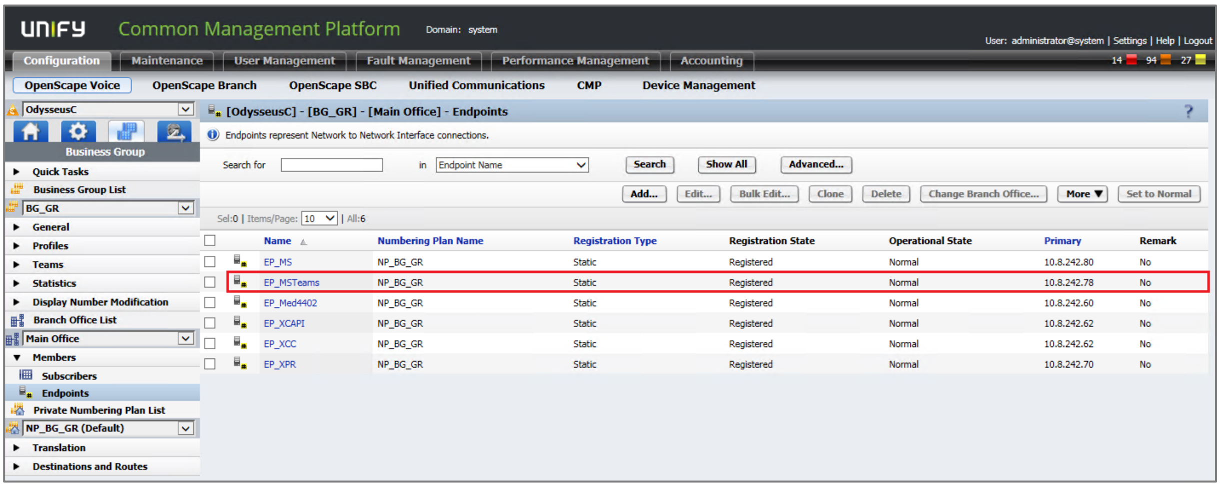
10. On **CMP** > **Configuration** > **OpenScape Voice** > **Business Group** > **Members** > **Endpoints** page, **Edit** previously created **EP_MSTeams** endpoint and select **Registered**.

Figure 4-8: Endpoint Registration



The endpoint status should look like the figure below:

Figure 4-9: Endpoint Status



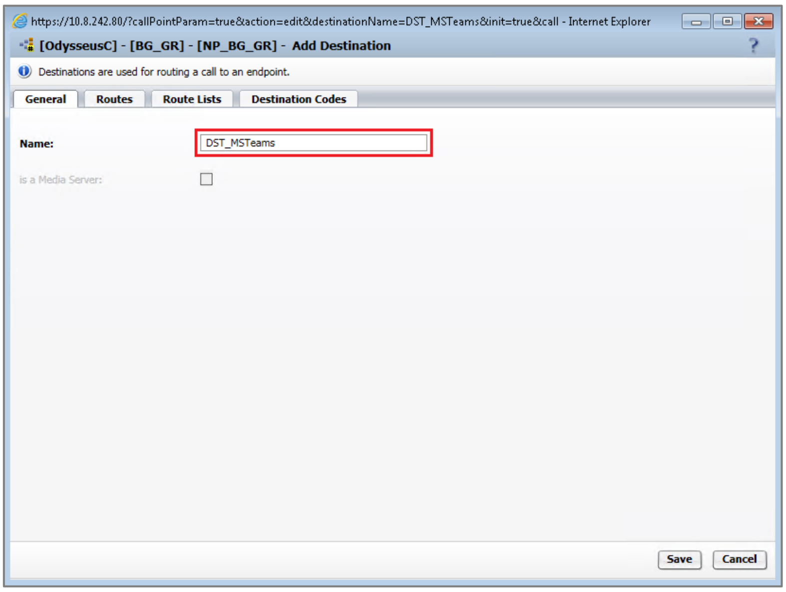
4.3 Destinations & Routes

This section describes how to create a new destinations and routes. **Destinations** are logical targets for off-net or on-net routing. When a destination is created, the name of the destination is bound to the numbering plan where the destination is created. Destinations are used to route a call to an endpoint representing a gateway. Each **Route** is a collection of groups or addresses that provide a path to a destination.

➢ **To create new Destination:**

1. Navigate to **CMP** > **Configuration** > **OpenScape Voice** > **Business Group** > **Destinations and Routes** > **Destinations**.
2. Click on **Add** and on **General** tab enter the following:
   - **Name:** **DST_MSTeams** (a common-sense name)

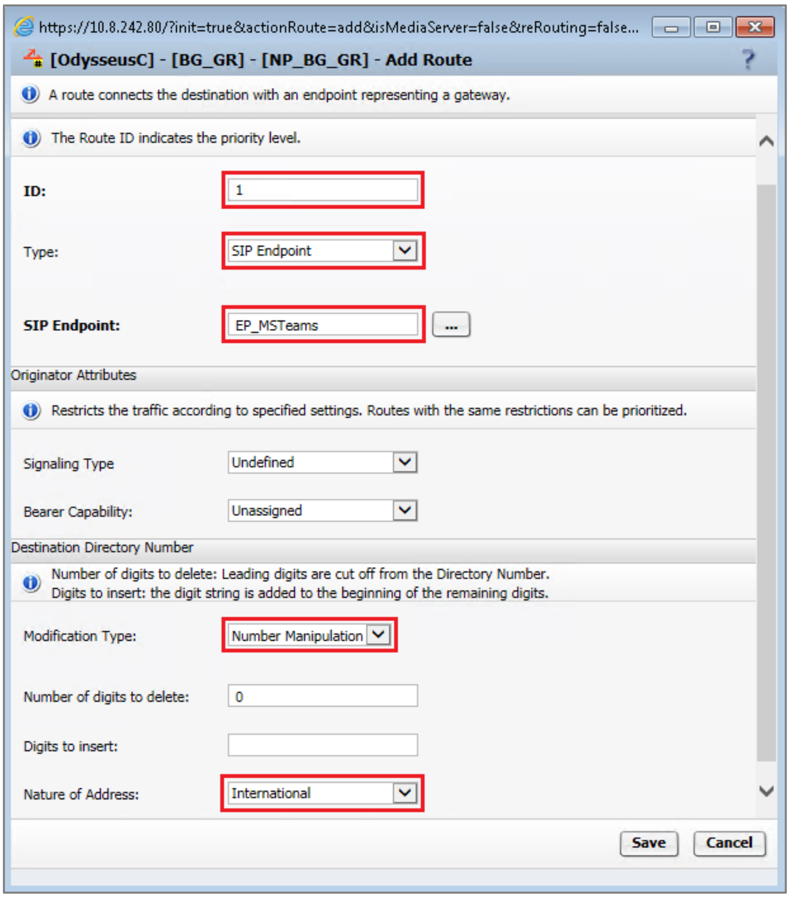
Figure 4-10: Add Destination



3. Click on **Save**.
4. On **CMP** > **Configuration** > **OpenScape Voice** > **Business Group** > **Destinations and Routes** > **Destinations** page select and **Edit** the **DST_MSTeams** destination.
5. Configure the associated Route, by clicking on **Routes tab** and entering the following:

Parameter	Value
ID	**1** (the priority of the route; if there are multiple routes to a destination, the route with the lowest numbered route ID has the highest priority, and will be selected first; we currently have one route with the SBC).
SIP Endpoint	**EP_MSTeams**
Modification Type	**Number Manipulation**
Nature of Address	**International**

Figure 4-11: Configure Route for Destination



6. Click **Save**.

> **Note:** To populate SIP Endpoint box with the **EP_MSTeams** endpoint, do the following:
>
> - Click on the corresponding button, and then select **Main Office** on the pop-up window
> - Click **Next**
> - Select **EP_MSTeams**
> - Click **OK**

4.4 Translation

This section describes how to configure translation. With **Translation,** the administrator configures to where outgoing calls per dialed digits from OS Voice subscribers are routed.

A call can only be routed if the dialed digits are matching a **PAC (Prefix Access Code)**.

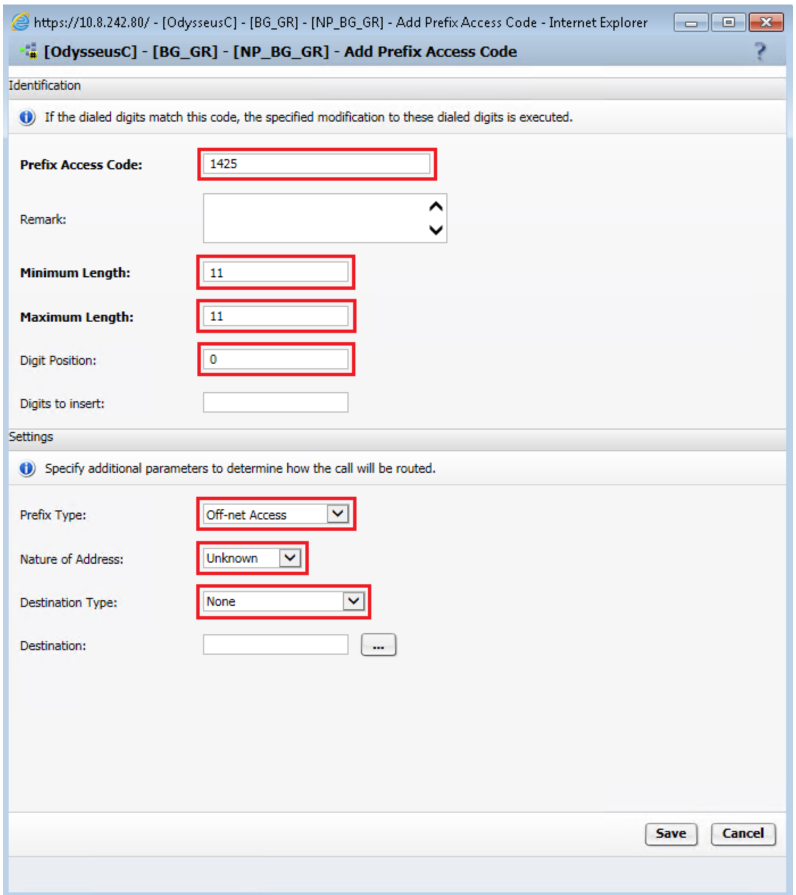
The **Destination Code** feature provides destination codes for basic telephone service. The destination code will be used for a call if the dialed or modified (in PAC) digits and the nature of address are matching.

➢ **To configure translation and destination code:**

1. Navigate to **CMP** > **Configuration** > **OpenScape Voice** > **Business Group** > **Translation** > **Prefix Access Codes**.
2. Click on **Add** and enter the following:

Parameter	Value
Prefix Access Code	**1425** (minimum expected length of Teams numbers)
Minimum Length	**11** (minimum expected length of Teams numbers)
Maximum Length	**11** (maximum expected length of Teams numbers)
Digit Position	**0** (don't remove any digits from dialed number before sending to destination)
Prefix Type	**Off-net** Access (a prefix access code to permit access to remote destinations)
Nature of Address	**Unknown**
Destination Type	**None** (the resulting digits will be processed in the user's numbering plan's destination codes table)

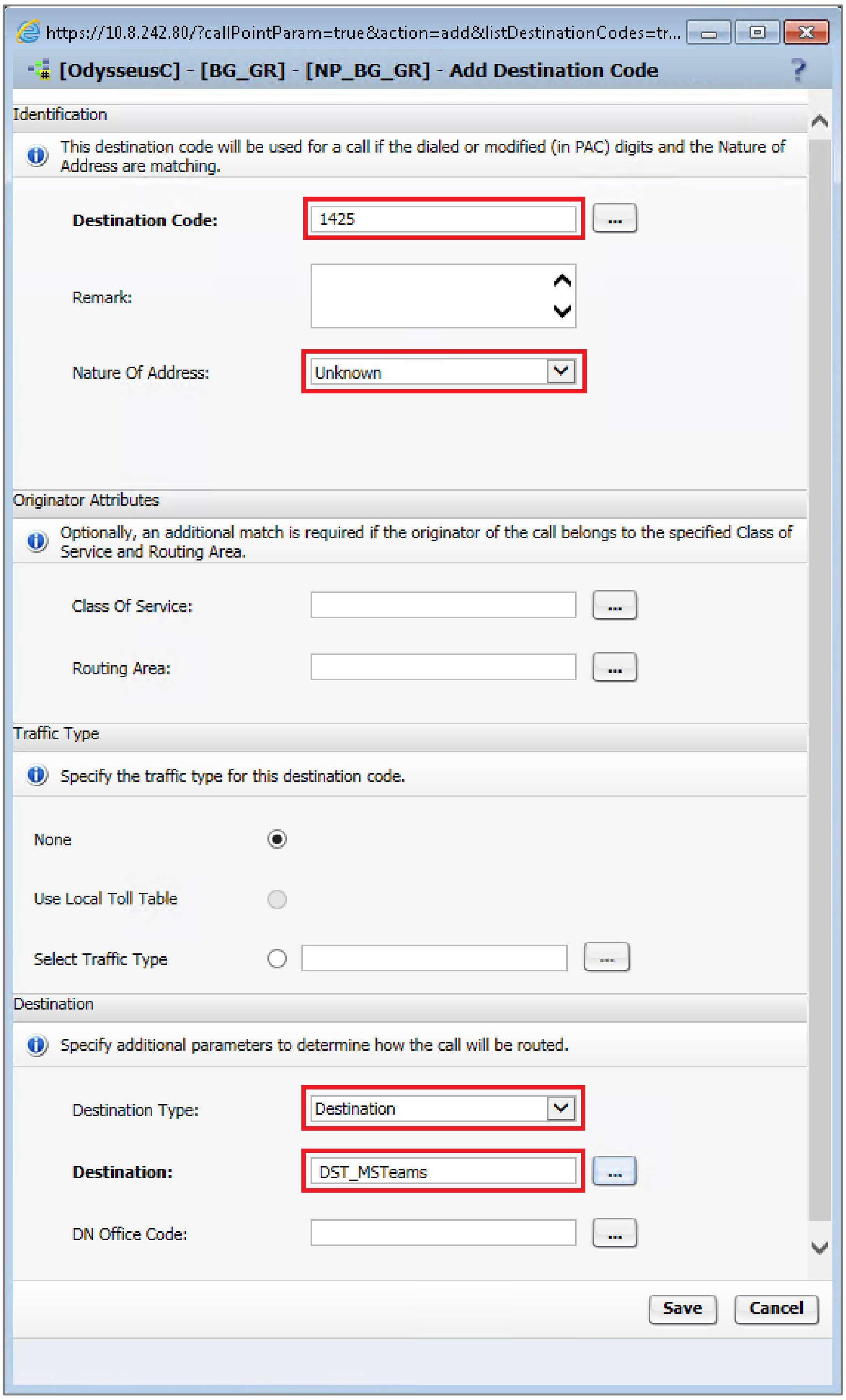
Figure 4-12: Add Prefix Access Code



3. Click **Save**.
4. Navigate to **CMP** > **Configuration** > **OpenScape Voice** > **Business Group** > **Translation** > **Destination Codes**.
5. Click on **Add** and enter the following:

Parameter	Value
Destination Code	**1425**
Nature of Address	**Unknown**
Destination Type	**Destination**
Destination	**DST_MSTeams**

Figure 4-13: Add Destination Code



6. Click **Save**.

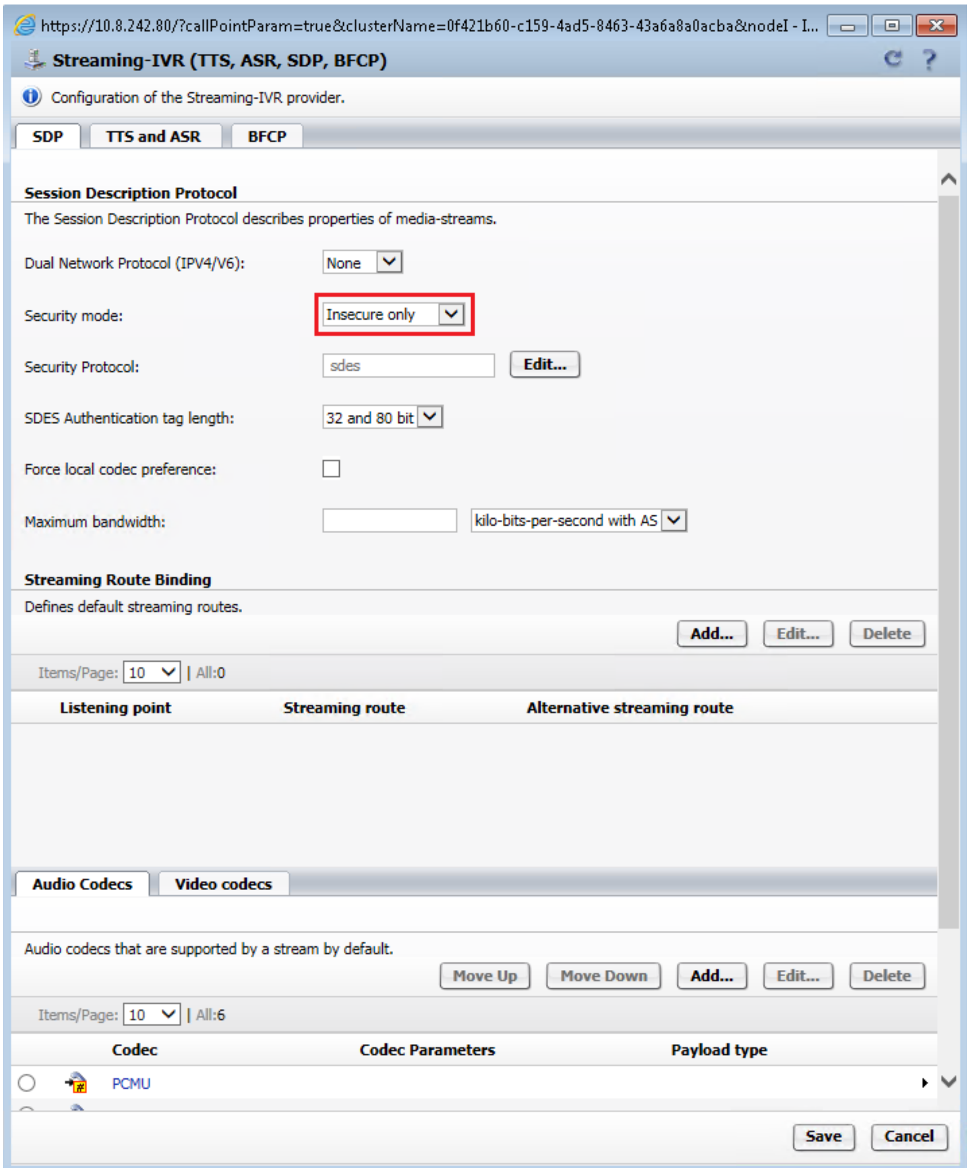
4.5 Media Server Secure Media Setting

This section describes how to configure secure media. For call transfer and large conference scenarios to work, the OpenScape Media Server should not offer SDP with secure m-line.

➢ **To configure secure media settings on media server:**

1. Navigate to **CMP > Configuration > Unified Communications > Configuration > Media Server** and click on the configured Media Server, e.g. **Backend**.
2. On the pop-up window and **Providers** tab, click on **Streaming-IVR (TTS, ASR, SDP, BFCP)** and on **SDP** tab set **Insecure only** from **Security** mode drop down list.

Figure 4-14: Configure Secure Media



3. Click **Save**.

This page is intentionally left blank.

5 Configuring AudioCodes SBC

This section provides step-by-step procedures on how to configure AudioCodes SBC for interworking between Microsoft Teams Direct Routing and the Unify OpenScape Voice. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- SBC LAN interface – Management Station and Unify OpenScape Voice
- SBC WAN interface – Teams Direct Routing environment

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

Notes:

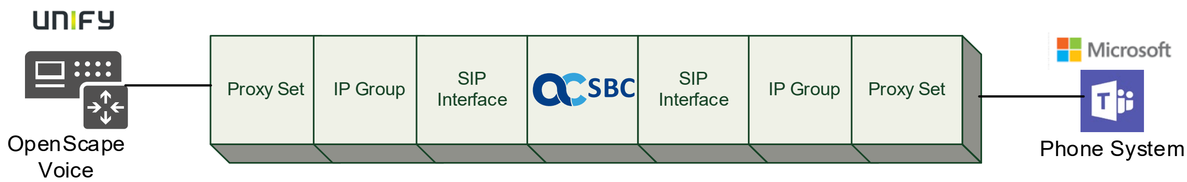
- For implementing Microsoft Teams Direct Routing and Unify OpenScape Voice based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
- **Enable Microsoft** (licensing MSFT) [All AudioCodes media gateways and SBCs are by default shipped with this license. Exceptions: MSBR products and Mediant 500 SBC or Media Gateways]
- **Microsoft TEAMS** (licensing SW/TEAMS)
- **Number of SBC sessions** [Based on requirements]
- **DSP Channels** [If media transcoding is needed]
- **Transcoding sessions** [If media transcoding is needed]

  For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this document does **not** cover all security aspects for configuring this topology. 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, which can be found at AudioCodes web site

5.1 SBC Configuration Concept in Teams Direct Routing Enterprise Model

The diagram below represents AudioCodes' device configuration concept in the Enterprise Model.

Figure 5-1: SBC Configuration Concept

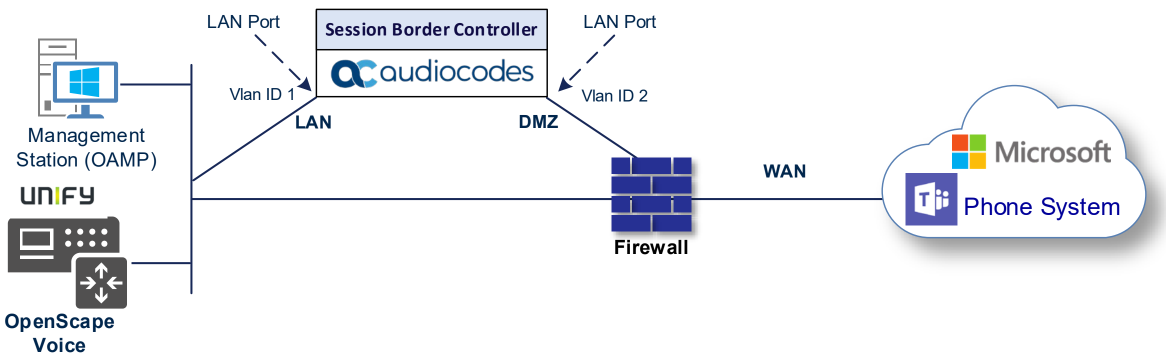


5.2 IP Network Interfaces Configuration

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

- SBC interfaces with the following IP entities:
  - Management Servers and Unify OpenScape Voice, located on the LAN
  - Microsoft Teams Direct Routing located on the WAN
- SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection depends on the method used to connect to the Enterprise's network. In the interoperability test topology, SBC connects to the LAN and DMZ using dedicated Ethernet ports
(i.e., two ports and two network cables are used).
- SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

Figure 5-2: Network Interfaces in Interoperability Test Topology



5.2.1 Configure VLANs

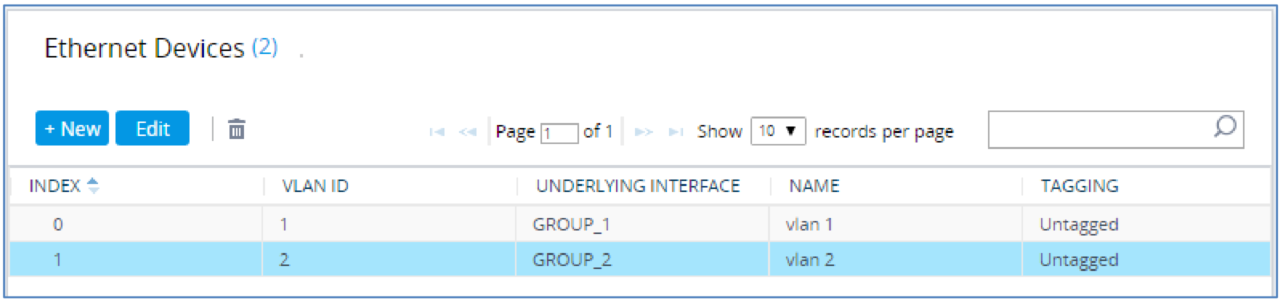
This section describes how to configure VLANs for each of the following interfaces:

- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ **To configure the VLANs:**

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

Figure 5-3: Configured VLAN IDs in Ethernet Device



5.2.2 Configure Network Interfaces

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

- LAN Interface (assigned the name "LAN_IF")
- WAN Interface (assigned the name "WAN_IF")

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

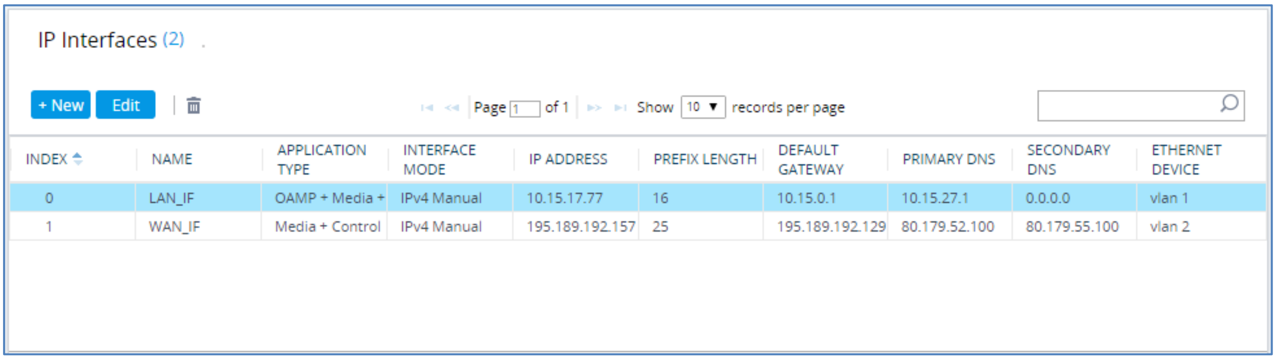
1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the IP interfaces as follows (your network parameters might be different):

Table 5-1: Configuration Example of the Network Interface Table

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	I/F Name	Ethernet Device
0	OAMP+ Media + Control	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.15.27.1	LAN_IF	vlan 1
1	Media + Control (as this interface points to the Internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.157 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	WAN_IF	vlan 2

The configured IP network interfaces are shown below:

Figure 5-4: 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	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

5.3 SIP TLS Connection Configuration

This section describes how to configure the SBC for using a TLS connection with the Microsoft Teams Direct Routing Phone System. This configuration is essential for a secure SIP TLS connection. The configuration instructions in this section are based on the following domain structure that must be implemented as part of the certificate which must be loaded to the host SBC:

- CN: sbc1.hybridvoice.org
- SAN: sbc1.hybridvoice.org

This certificate module is based on the Service Provider's own TLS Certificate. For more certificate structure options, see Microsoft Teams Direct Routing documentation.

The Microsoft Phone System Direct Routing Interface allows ***only*** TLS connections from SBCs for SIP traffic with a certificate signed by one of the Trusted Certification Authorities.

Currently, supported Certification Authorities can be found in the following link:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

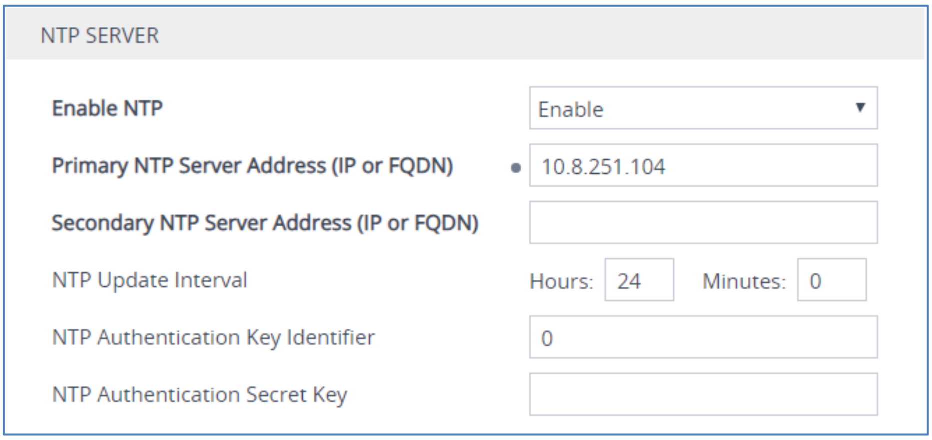
5.3.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or another global server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that NTP Server will locate on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

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

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.8.251.104**).

Figure 5-5: Configuring NTP Server Address



3. Click **Apply**.

5.3.2 Create a TLS Context for Teams Direct Routing

This section describes how to configure TLS Context in the SBC. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➢ **To configure the TLS version:**

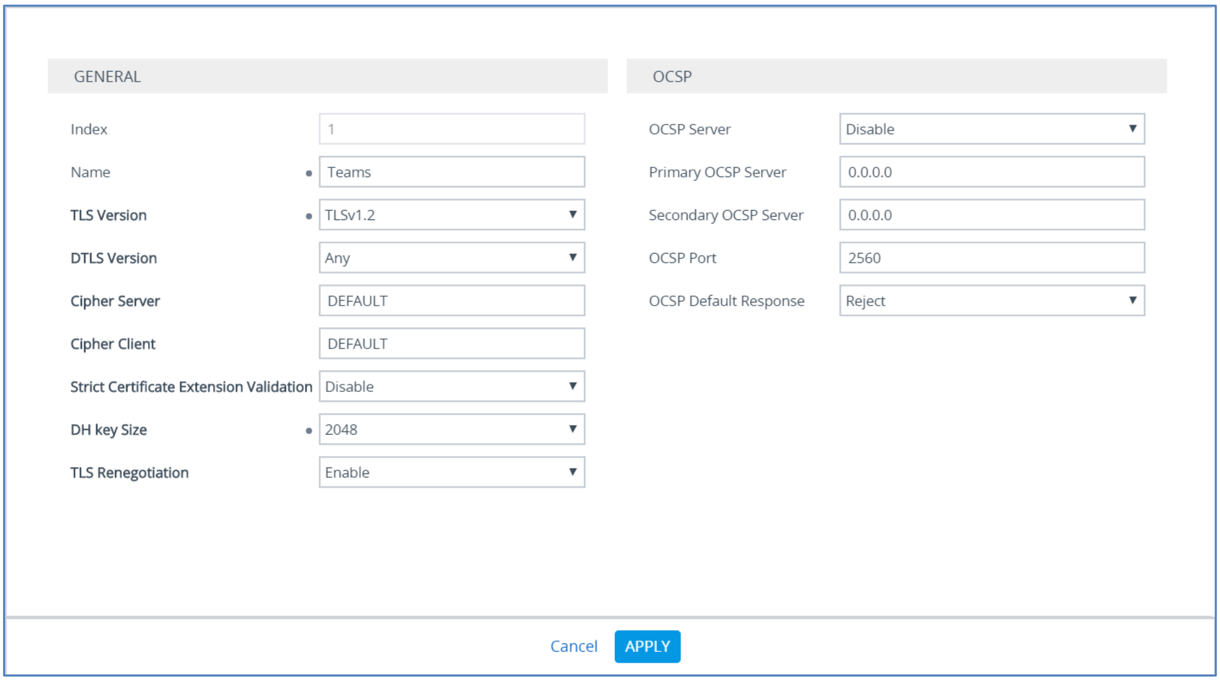
1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Create a new TLS Context by clicking **New** at the top of the interface, and then configure the parameters using the table below as reference:

Table 5-2: New TLS Context

Index	Name	TLS Version	DH key Size
1	Teams (arbitrary descriptive name)	TLSv1.2	2048
All other parameters can be left unchanged with their default values.			

Note: The table above exemplifies configuration focusing on interconnecting SIP and media. You might want to configure additional parameters according to your company's policies. For example, you might want to configure Online Certificate Status Protocol (OCSP) to check if SBC certificates presented in the online server are still valid or revoked. For more information on the SBC's configuration, see the *User's Manual*, available for download from https://www.audiocodes.com/library/technical-documents.

Figure 5-6: Configuring TLS Context for Teams Direct Routing



3. Click **Apply**.

5.3.3 Configure a Certificate

This section describes how to request a certificate for the SBC and to configure it based on the example of DigiCert Global Root CA. The certificate is used by the SBC to authenticate the connection with Microsoft Teams Direct Routing.

The procedure involves the following main steps:

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

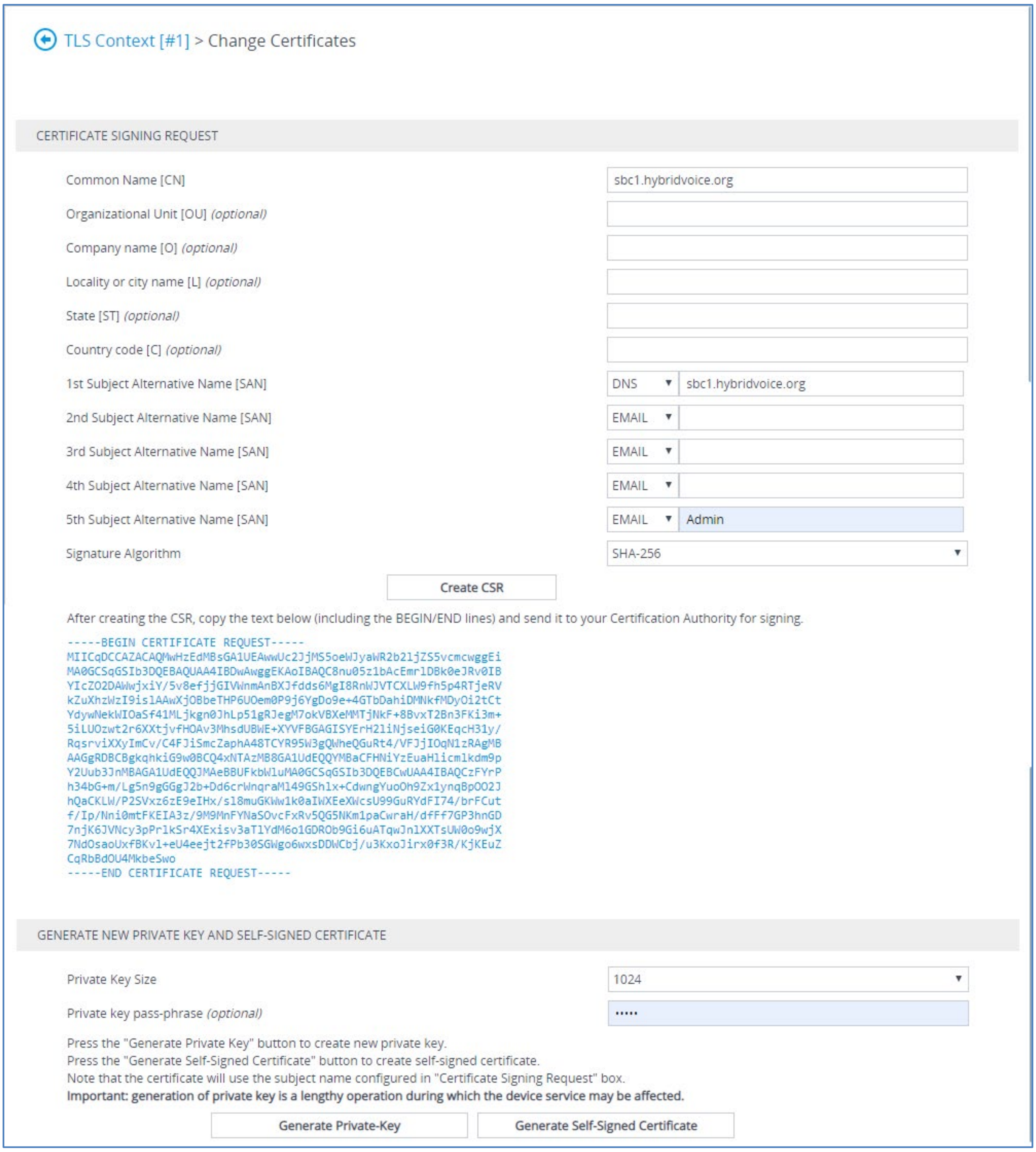
➢ **To configure a certificate:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Subject Name [CN]' field, enter the SBC FQDN name (based on example above, **sbc1.hybridvoice.org**).
   b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on example above, **sbc1.hybridvoice.org**).

Note: The domain portion of the Common Name [CN] and 1st Subject Alternative Name [SAN] must match the SIP suffix configured for Office 365 users.

   c. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024. In this case, you must change the key size to 2048.
   d. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' to **2048** and then click **Generate Private-Key**. To use **1024** as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
   e. Fill in the rest of the request fields according to your security provider's instructions.
   f. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

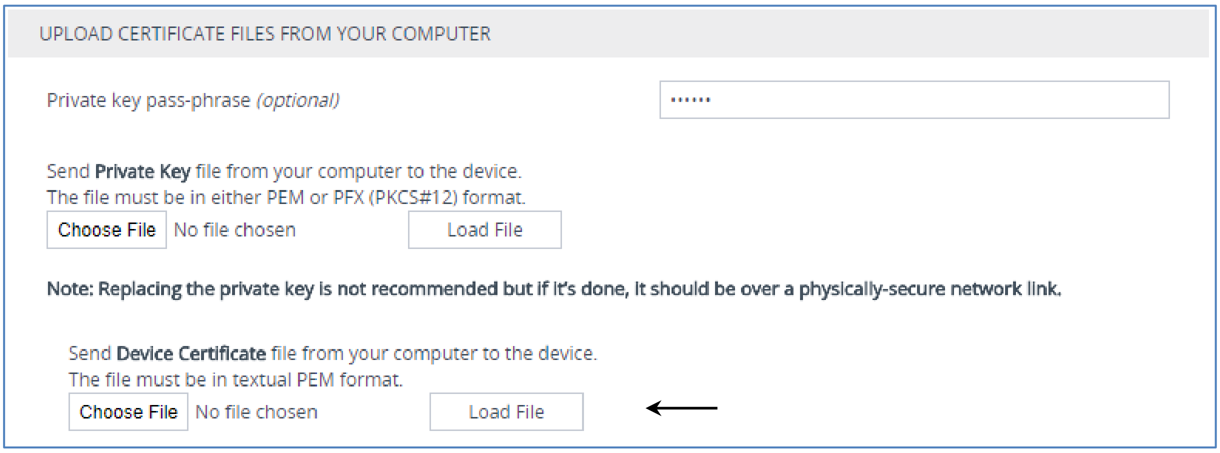
Figure 5-7: Example of Certificate Signing Request – Creating CSR



4. Copy the CSR from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----"** to a text file (such as Notepad), and then save it to a folder on your computer with the file name, for example *certreq.txt*.
5. Send *certreq.txt* file to the Certified Authority Administrator for signing.

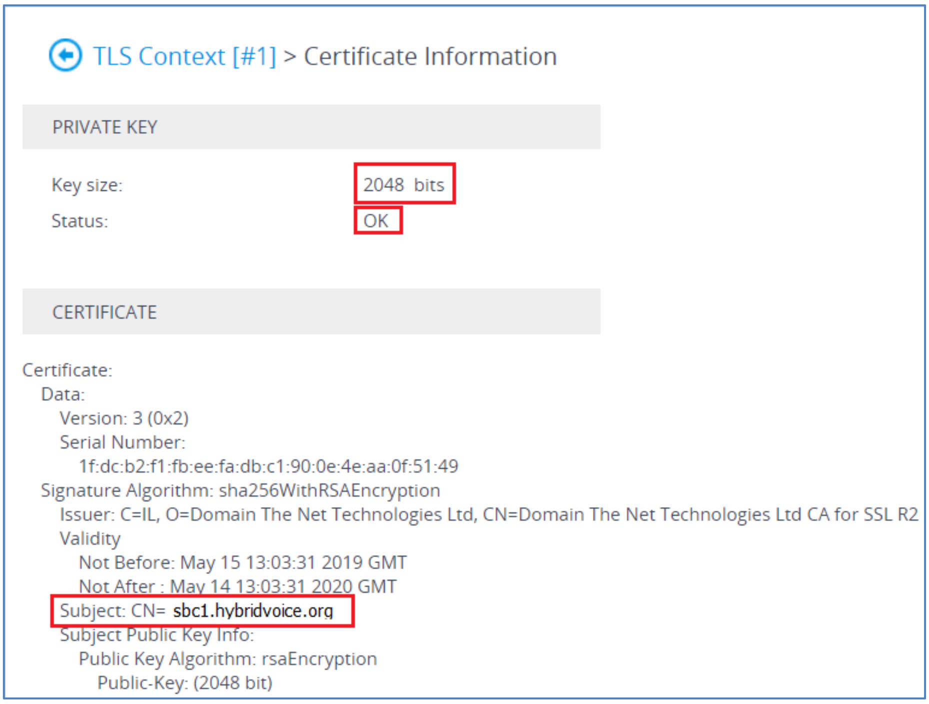
6. After obtaining an SBC signed and Trusted Root/Intermediate Certificate from the CA, in the SBC's Web interface, return to the **TLS Contexts** page and do the following:
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
   b. Scroll down to the **Upload certificates files from your computer** group, click the **Choose File** button corresponding to the '**Send Device Certificate**...' field, navigate to the certificate file obtained from the CA, and then click **Load File** to upload the certificate to the SBC.

Figure 5-8: Uploading the Certificate Obtained from the Certification Authority



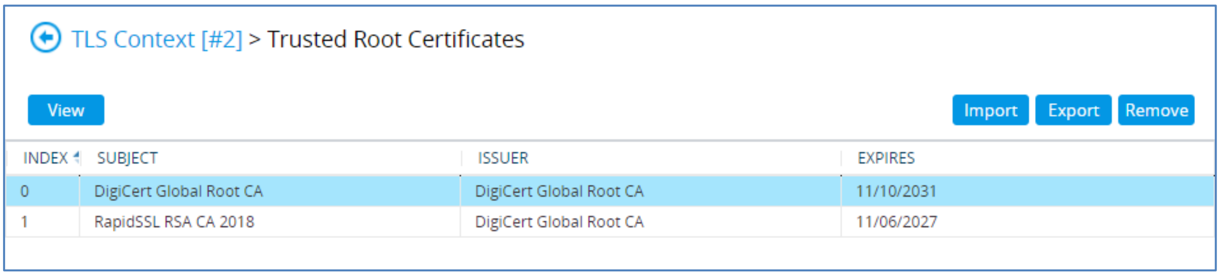
7. Confirm that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.
8. In the SBC's Web interface, return to the **TLS Contexts** page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name:

Figure 5-9: Certificate Information Example



9. In the SBC's Web interface, return to the **TLS Contexts** page.
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   b. Click the **Import** button, and then select all Root/Intermediate Certificates obtained from your Certification Authority to load.
10. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store:

Figure 5-10: Example of Configured Trusted Root Certificates



5.3.4 Method of Generating and Installing the Wildcard Certificate

To use the same certificate on multiple devices, you may prefer using 3rd party application (e.g. DigiCert Certificate Utility for Windows) to process the certificate request from your Certificate Authority on another machine, with this utility installed.

After you've processed the certificate request and response using the DigiCert utility, test the certificate private key and chain and then export the certificate with private key and assign a password.

➢ **To install the certificate:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Scroll down to the **Upload certificates files from your computer** group and do the following:
   a. Enter the password assigned during export with the DigiCert utility in the **'Private key pass-phrase'** field.
   b. Click the **Choose File** button corresponding to the 'Send **Private Key**...' field and then select the SBC certificate file exported from the DigiCert utility.

5.3.5 Deploy Baltimore Trusted Root Certificate

The DNS name of the Microsoft Teams Direct Routing interface is **sip.pstnhub.microsoft.com**. In this interface, a certificate is presented which is signed by Baltimore Cyber Baltimore CyberTrust Root with Serial Number: 02 00 00 b9 and SHA fingerprint: d4:de:20:d0:5e:66:fc: 53:fe:1a:50:88:2c:78:db:28:52:ca:e4:74.

To trust this certificate, your SBC *must* have the certificate in Trusted Certificates storage. Download the certificate from https://cacert.omniroot.com/bc2025.pem and follow the steps above to import the certificate to the Trusted Root storage.

Note: Before importing the Baltimore Root Certificate into AudioCodes' SBC, make sure it's in .PEM or .PFX format. If it isn't, you need to convert it to .PEM or .PFX format. Otherwise, you will receive a 'Failed to load new certificate' error message. To convert to PEM format, use the Windows local store on any Windows OS and then export it as 'Base-64 encoded X.509 (.CER) certificate'.

5.4 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the Unify OpenScape Voice traffic and one for the Teams traffic.

➢ **To configure Media Realms:**

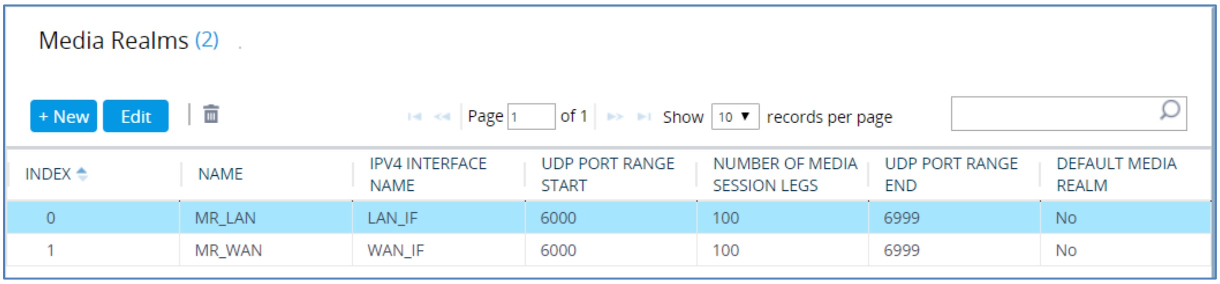
1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realms as follows (you can use the default Media Realm (Index 0), but modify it):

Table 5-3: Configuration Example Media Realms in Media Realm Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	**MR_LAN** (arbitrary name)		LAN_IF	6000	100 (media sessions assigned with port range)
1	**MR_WAN** (arbitrary name)	Up	WAN_IF	7000	100 (media sessions assigned with port range)

The configured Media Realms are shown in the figure below:

Figure 5-11: 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	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
0	MR_LAN	LAN_IF	6000	100	6999	No
1	MR_WAN	WAN_IF	6000	100	6999	No

5.5 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For the interoperability test topology, towards the SIP Trunk and towards the Teams Direct Routing SIP Interfaces must be configured for the SBC.

➢ **To configure SIP Interfaces:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Configure SIP Interfaces. You can use the default SIP Interface (Index 0), but modify it as shown in the table below. The table below shows an example of the configuration. You can change some parameters according to your requirements.

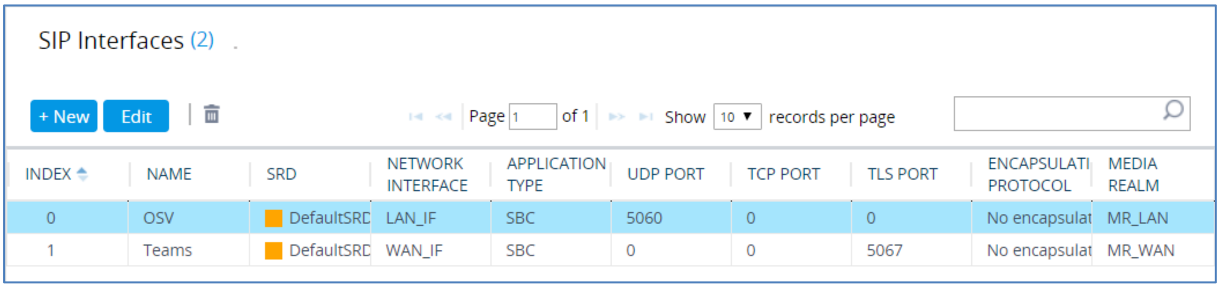
Note: The Direct Routing interface can only use TLS for a SIP port. It does not support using TCP due to security reasons. The SIP port might be any port of your choice. When pairing the SBC with Office 365, the chosen port is specified in the pairing command.

Table 5-4: Configured SIP Interfaces in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name
0	**OSV** (arbitrary name)	**LAN_IF**	**SBC**	**5060** (according to customer requirement)	**0**	**0**	**Disable** (leave default value)	**500** (leave default value)	**MR_LAN**	-
1	**Teams** (arbitrary name)	**WAN_IF**	**SBC**	**0** (Phone System does not use UDP or TCP for SIP signaling)	**0**	**5067** (as configured in the Office 365)	**Enable**	**0** (Recommended to prevent DoS attacks)	**MR_WAN**	**Teams**

The configured SIP Interfaces are shown in the figure below:

Figure 5-12: Configured SIP Interfaces in SIP Interface Table



INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATI PROTOCOL	MEDIA REALM
0	OSV	DefaultSRD	LAN_IF	SBC	5060	0	0	No encapsulat	MR_LAN
1	Teams	DefaultSRD	WAN_IF	SBC	0	0	5067	No encapsulat	MR_WAN

5.6 Configure Proxy Sets and Proxy Address

This section 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:

- Unify OpenScape Voice
- Teams Direct Routing

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

➢ **To configure Proxy Sets:**

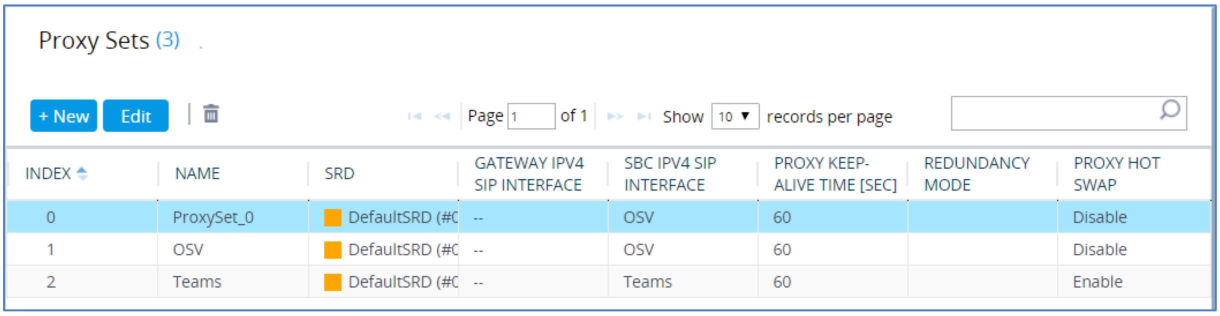
1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

Table 5-5: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap	Proxy Load Balancing Method
1	**OSV** (arbitrary name)	OSV	Default	Using Options	-	-
2	**Teams** (arbitrary name)	Teams	Teams	Using Options	Enable	Random Weights

The configured Proxy Sets are shown in the figure below:

Figure 5-13: Configured Proxy Sets in Proxy Sets Table



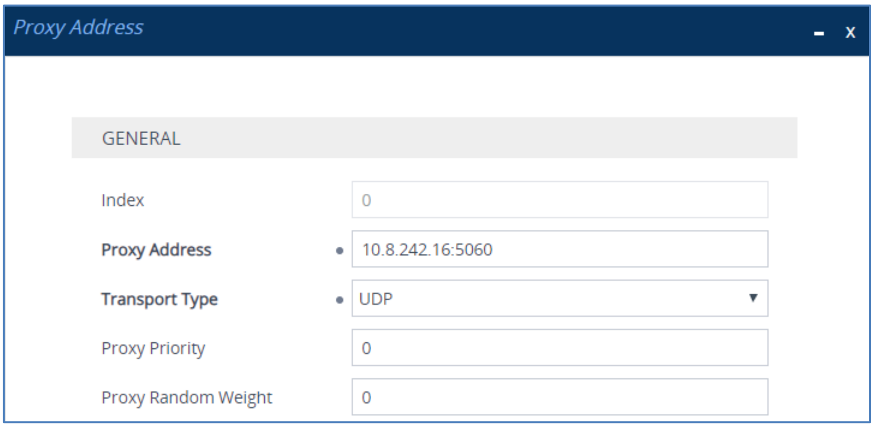
5.6.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

➢ To configure a Proxy Address for SIP Trunk:

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set **OSV**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 5-14: Configuring Proxy Address for OSV



3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 5-6: Configuration Proxy Address for SIP Trunk

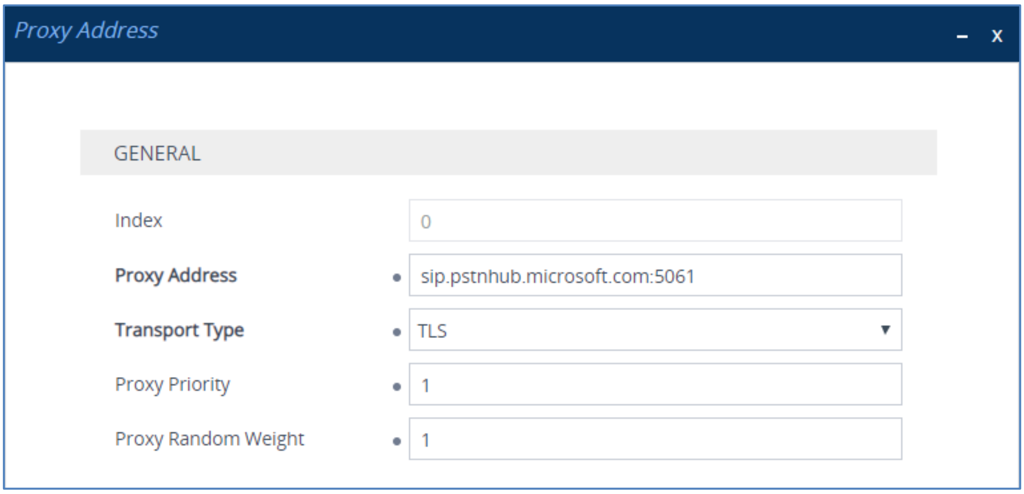
Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	10.8.242.16:5060 (OSV IP and port)	UDP	0	0

4. Click **Apply**.

➢ To configure a Proxy Address for Teams:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **Teams**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 5-15: Configuring Proxy Address for Teams Direct Routing Interface



3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 5-7: Configuration Proxy Address for Teams Direct Routing

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	sip.pstnhub.microsoft.com:5061	TLS	1	1
1	sip2.pstnhub.microsoft.com:5061	TLS	2	1
2	sip3.pstnhub.microsoft.com:5061	TLS	3	1

4. Click Appl**y**.

5.7 Configure Coders

This section describes how to configure coders (termed *Coder Group*). As Unify OpenScape Voice doesn't send a list of supported coders in the initial offer, a Coder Group with the list of supported coders for the Microsoft Teams Direct Routing leg needs to be added.

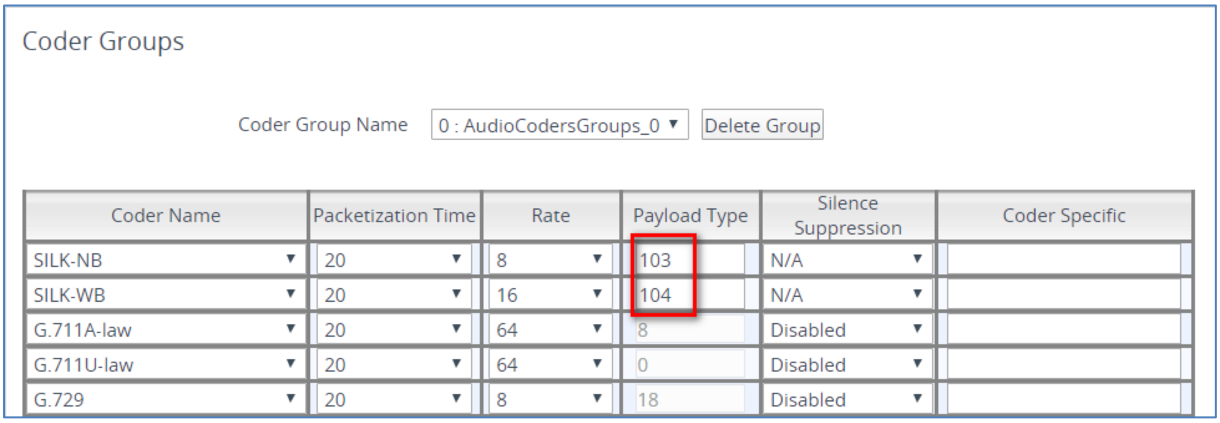
Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

➢ **To configure coders:**

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. Configure a Coder Group for Microsoft Teams Direct Routing:

Parameter	Value
Coder Group Name	**AudioCodersGroups_0**
Coder Name	▪ **SILK-NB** ▪ **SILK-WB** ▪ **G.711 A-law** ▪ **G.711 U-law** ▪ **G.729**

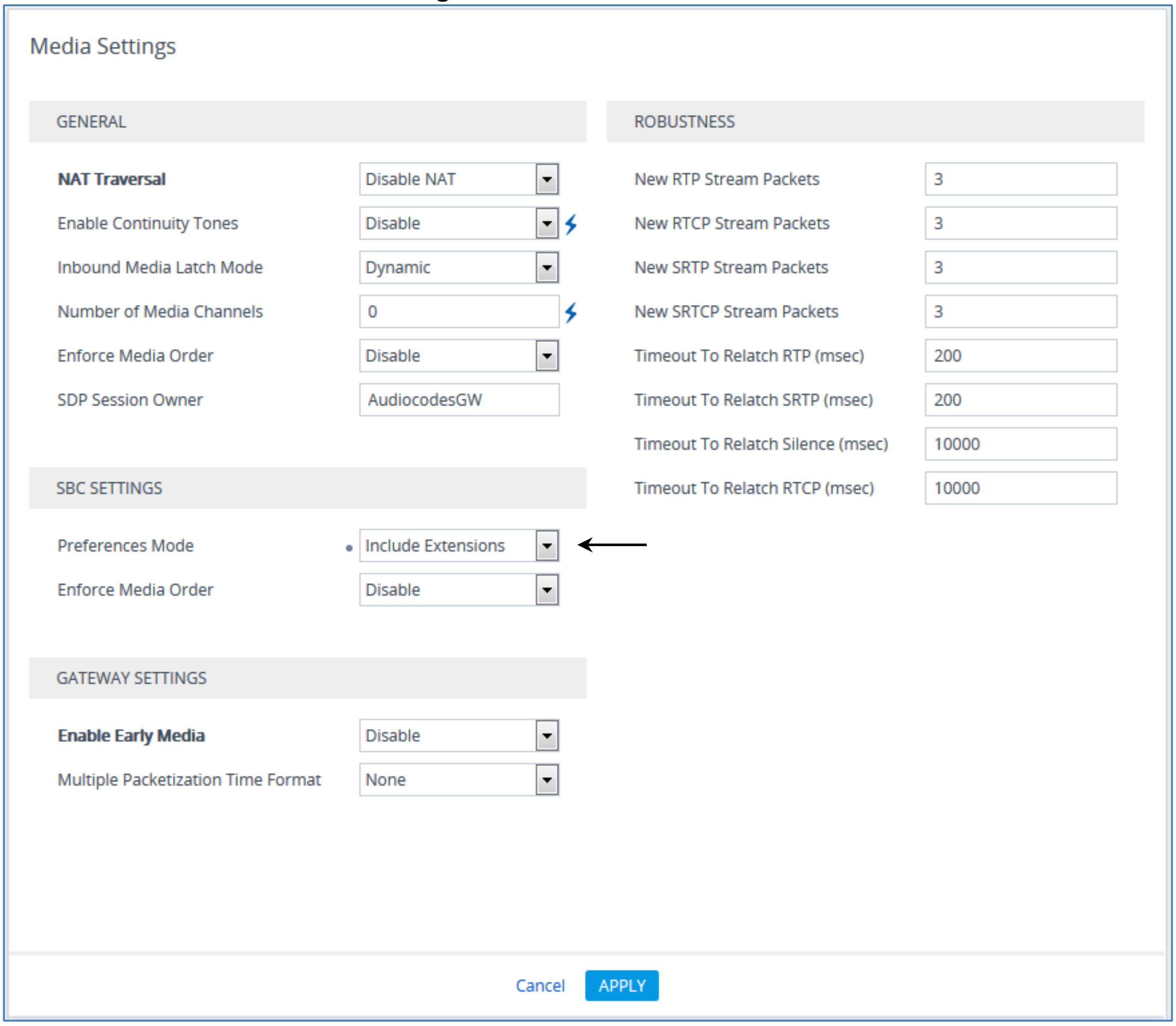
Figure 5-16: Configuring Coder Group for Microsoft Teams Direct Routing



3. Click **Apply,** and then confirm the configuration change in the prompt that pops up.

4. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).

Figure 5-17: SBC Preferences Mode



5. From the '**Preferences Mode**' drop-down list, select **Include Extensions**.
6. Click **Apply**.

5.8 Configure IP Profiles

This section 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:

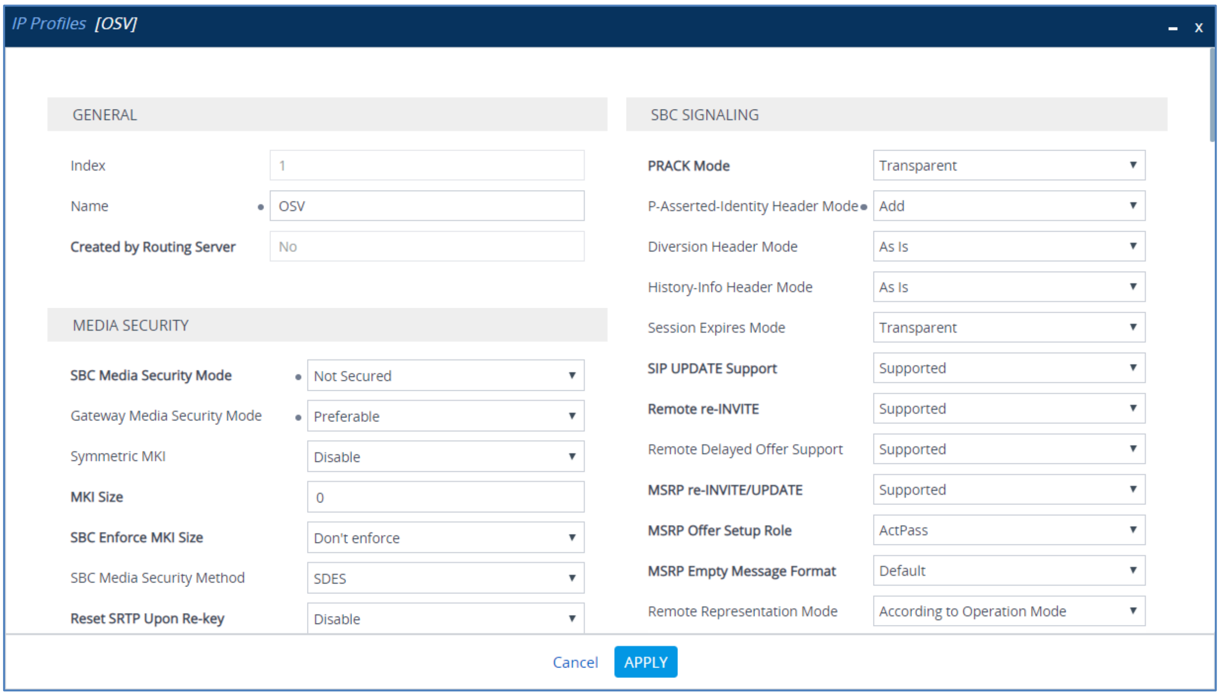
- Unify OpenScape Voice – to operate in non-secure mode using RTP and SIP over UDP
- Microsoft Teams Direct Routing – to operate in secure mode using SRTP and SIP over TLS

➢ **To configure an IP Profile for the Unify OpenScape Voice :**

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

Parameter	Value
General	
Index	**1**
Name	**OSV**
Media Security	
SBC Media Security Mode	**Not Secured**
SBC Media	
Use Silence Suppression	**Add**
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote Replaces Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**

Figure 5-18: Configuring IP Profile for Unify OpenScape Voice



3. Click **Apply**.

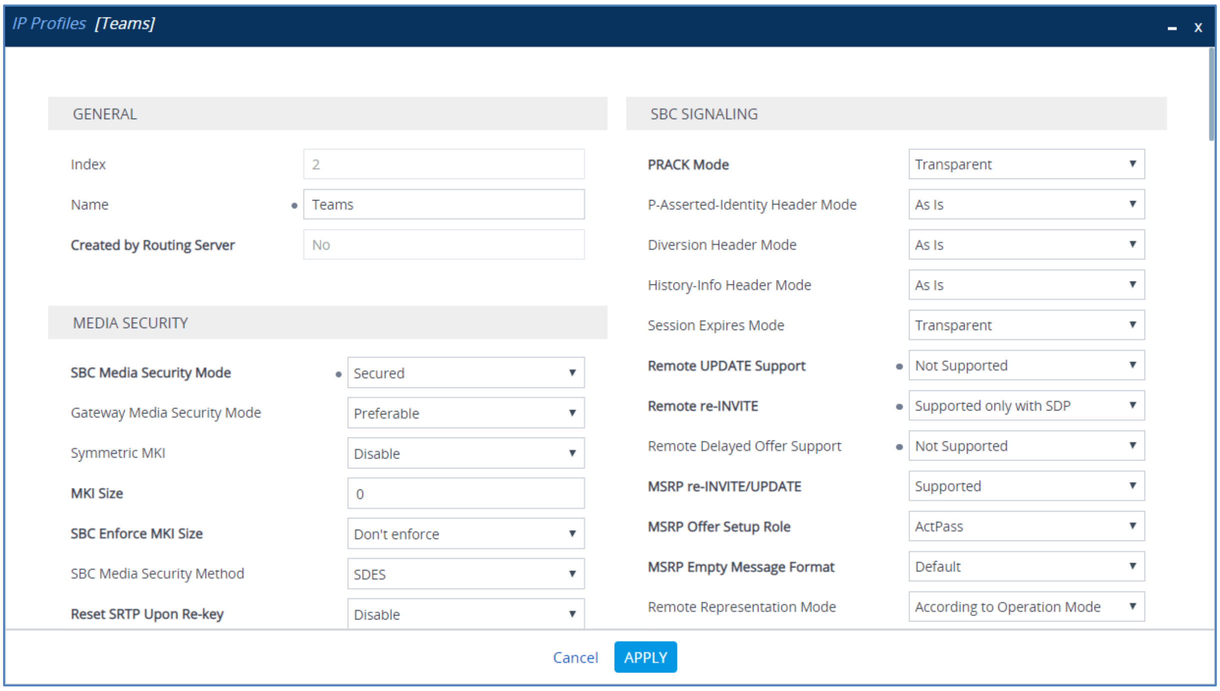
➢ To configure IP Profile for the Microsoft Teams Direct Routing:

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

Parameter	Value
General	
Index	**2**
Name	**Teams** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Early Media	
Remote Early Media RTP Detection Mode	**By Media** (required, as Microsoft Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Media	
Extension Coders Group	**AudioCodersGroups_0**
Use Silence Suppression	**Add**
RTCP Mode	**Generate Always**
ICE Mode	**Lite** (required only when Media Bypass enabled on Microsoft Teams)
SBC Signaling	

Remote Update Support	**Not Supported**
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**
SBC Hold	
Remote Hold Format	**Inactive** (some SIP Trunk may answer with a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address)

Figure 5-19: Configuring IP Profile for Microsoft Teams Direct Routing



3. Click **Apply**.

5.9 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the 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:

- Unify OpenScape Voice located on LAN
- Teams Direct Routing located on WAN

➢ **To configure IP Groups:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the Unify OpenScape Voice:

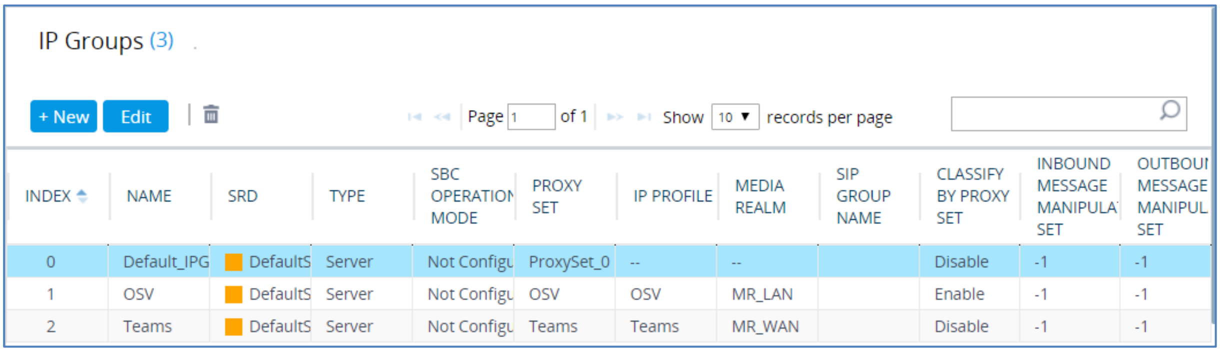
Parameter	Value
Index	**1**
Name	**OSV**
Type	**Server**
Proxy Set	**OSV**
IP Profile	**OSV**
Media Realm	**MR_LAN**
SIP Group Name	(according to requirement, for example, sbc.ACeducation.info)

3. Configure an IP Group for the Microsoft Teams Direct Routing:

Parameter	Value
Index	**2**
Name	**Teams**
Topology Location	**Up**
Type	**Server**
Proxy Set	**Teams**
IP Profile	**Teams**
Media Realm	**Teams**
Classify by Proxy Set	**Disable**
Local Host Name	**< FQDN name of your SBC in the Microsoft Teams tenant >** (For example, sbc.ACeducation.info)
Always Use Src Address	**Yes**
Proxy Keep-Alive using IP Group settings	**Enable**

The configured IP Groups are shown in the figure below:

Figure 5-20: Configured IP Groups in IP Group Table



INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULA SET	OUTBOUI MESSAGE MANIPUL SET
0	Default_IPG	DefaultS	Server	Not Configu	ProxySet_0	--	--		Disable	-1	-1
1	OSV	DefaultS	Server	Not Configu	OSV	OSV	MR_LAN		Enable	-1	-1
2	Teams	DefaultS	Server	Not Configu	Teams	Teams	MR_WAN		Disable	-1	-1

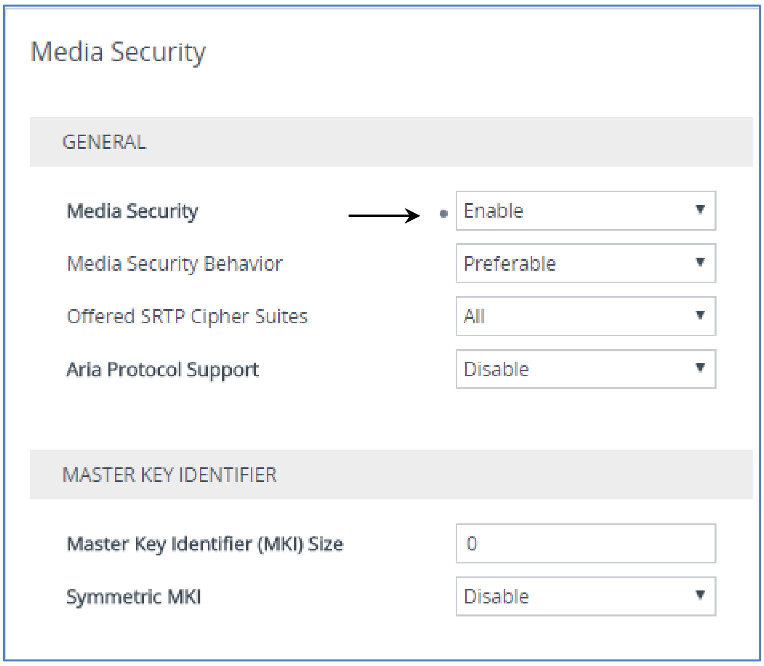
5.10 Configure SRTP

This section describes how to configure media security. The Direct Routing Interface needs to use of SRTP only, so you need to configure the SBC to operate in the same manner.

➢ **To configure media security:**

1. Open the Media Security page (**Setup menu > Signaling & Media tab > Media folder > Media Security**).
2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.

Figure 5-21: Configuring SRTP



3. Click **Apply**.

5.11 Configuring Message Condition Rules

This section describes how to configure the Message Condition Rules. A Message Condition defines special conditions (pre-requisites) for incoming SIP messages. These rules can be used as additional matching criteria for the IP-to-IP routing rules in the IP-to-IP Routing table.

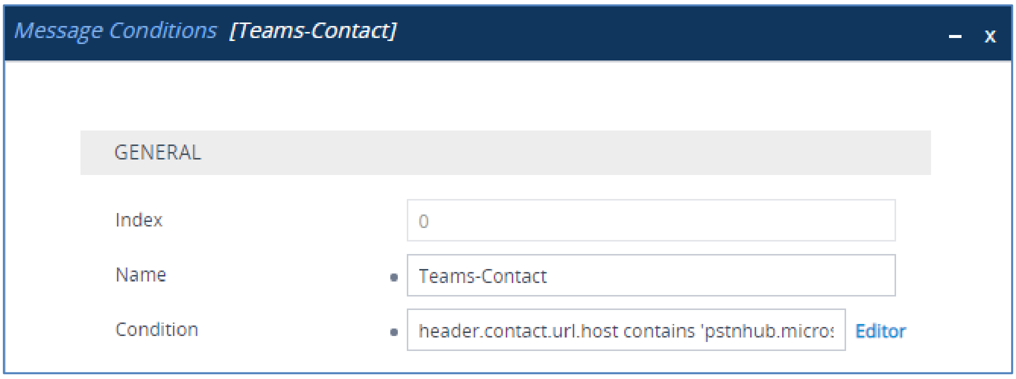
The following condition verifies that the Contact header contains Microsoft Teams FQDN.

➢ **To configure a Message Condition rule:**

1. Open the Message Conditions table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Conditions**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**0**
Name	**Teams-Contact** (arbitrary descriptive name)
Condition	**header.contact.url.host contains 'pstnhub.microsoft.com'**

Figure 5-22: Configuring Condition Table



3. Click **Apply**.

5.12 Configuring Classification Rules

This section describes how to configure Classification rules. A Classification rule classifies incoming SIP dialog-initiating requests (e.g., INVITE messages) to a 'source' IP Group. The source IP Group is the SIP entity that sent the SIP dialog request. Once classified, the device uses the IP Group to process the call (manipulation and routing).

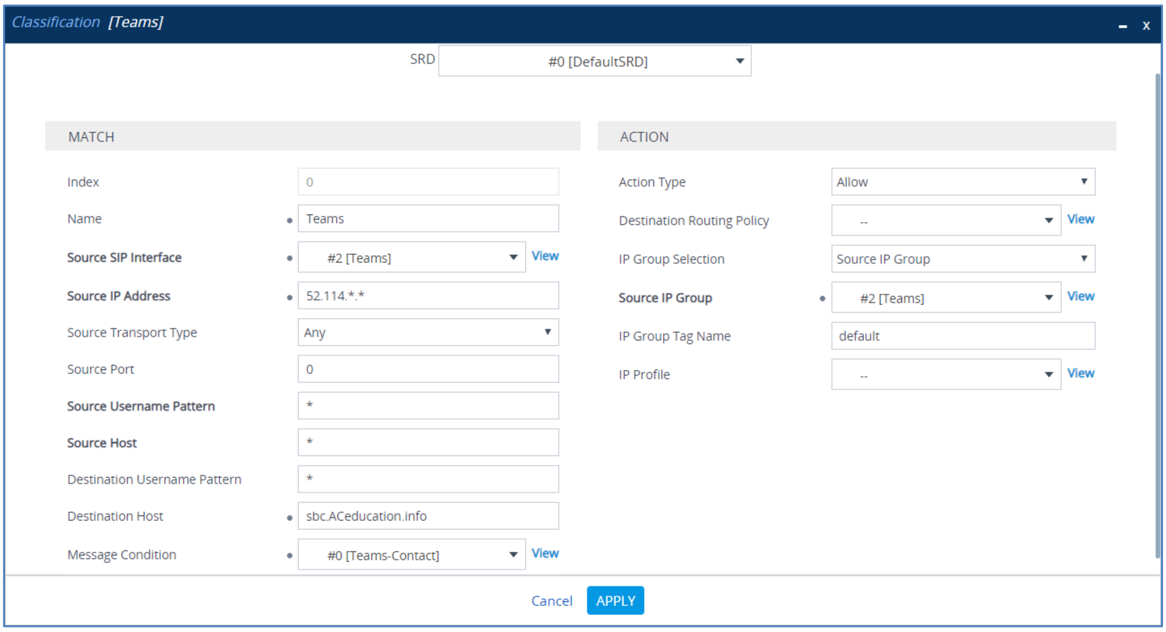
You can also use the Classification table for employing SIP-level access control for successfully classified calls, by configuring Classification rules with whitelist and blacklist settings. If a Classification rule is configured as a whitelist ("Allow"), the device accepts the SIP dialog and processes the call. If the Classification rule is configured as a blacklist ("Deny"), the device rejects the SIP dialog.

➢ **To configure a Classification rule:**

1. Open the Classification table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification Table**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**0**
Name	**Teams**
Source SIP Interface	**Teams**
Source IP Address	**52.114.*.***
Destination Host	**< FQDN name of your SBC in the Microsoft Teams tenant >** (e.g. sbc.ACeducation.info)
Message Condition	**Teams-Contact**
Action Type	**Allow**
Source IP Group	**Teams**

Figure 5-23: Configuring Classification Rule



3. Click **Apply**.

5.13 Configure IP-to-IP Call Routing Rules

This section 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 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.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Teams Direct Routing and Unify OpenScape Voice:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Terminate REFER messages to Teams Direct Routing
- Calls from Teams Direct Routing to Unify OpenScape Voice
- Calls from Unify OpenScape Voice to Teams Direct Routing

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

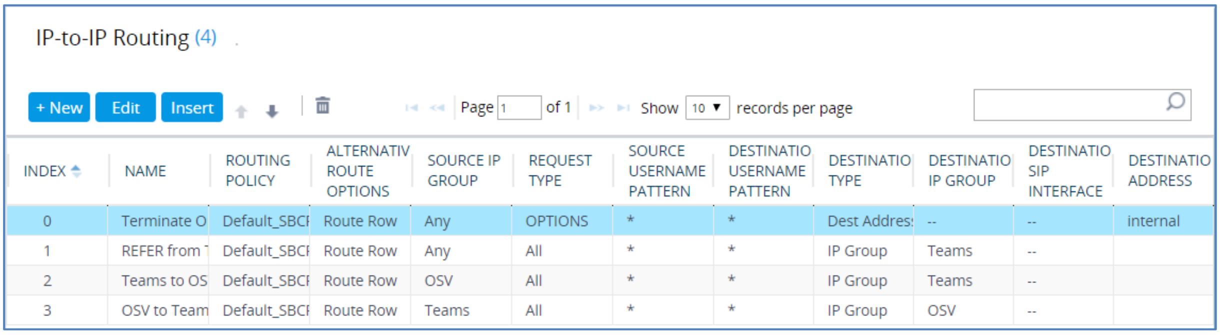
1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure routing rules as shown in the table below:

Table 5-8: Configuration IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Call Triger	ReRoute IP Group	Dest Type	Dest IP Group	Dest Address
0	Terminate OPTIONS	Any	OPTIONS			Dest Address		internal
1	Refer from Teams (arbitrary name)	Any		REFER	Teams	Request URI	Teams	
2	Teams to OSV (arbitrary name)	Teams				IP Group	OSV	
3	OSV to Teams (arbitrary name)	OSV				IP Group	Teams	

The configured routing rules are shown in the figure below:

Figure 5-24: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table


IP-to-IP Routing (4)

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

INDEX	NAME	ROUTING POLICY	ALTERNATIV ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATIO USERNAME PATTERN	DESTINATIO TYPE	DESTINATIO IP GROUP	DESTINATIO SIP INTERFACE	DESTINATIO ADDRESS
0	Terminate O	Default_SBCI	Route Row	Any	OPTIONS	*	*	Dest Addres	--	--	internal
1	REFER from T	Default_SBCI	Route Row	Any	All	*	*	IP Group	Teams	--	
2	Teams to OS	Default_SBCI	Route Row	OSV	All	*	*	IP Group	Teams	--	
3	OSV to Team	Default_SBCI	Route Row	Teams	All	*	*	IP Group	OSV	--	

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

5.14 Configuring Firewall Settings

Note: AudioCodes highly advised to configure firewall with network traffic filtering rules **in front of** WAN interface of the SBC. For detailed list of ports, which needed to be open please refer to: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-fqdns-and-firewall-ports.

As an extra security to the above note, there is option to configure traffic filtering rules (*access list*) for incoming traffic on AudioCodes SBC. For each packet received on the configured network interface, the SBC searches the table from top to bottom until the first matching rule is found. The matched rule can permit (*allow*) or deny (*block*) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted. Please note that the firewall is stateless. The blocking rules will apply to all incoming packets, including UDP or TCP responses.

➢ **To configure a firewall rule:**

1. Open the Firewall table (**Setup** menu > **IP Network** tab > **Security** folder> **Firewall**).
2. Configure the following Access list rules for Teams Direct Rout IP Interface:

Table 4-9: Firewall Table Rules

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server IP> (e.g. 8.8.8.8)	32	0	65535	Any	Enable	WAN_IF	Allow
1	52.114.148.0	32	0	65535	TCP	Enable	WAN_IF	Allow
2	52.114.132.46	32	0	65535	TCP	Enable	WAN_IF	Allow
3	52.114.75.24	32	0	65535	TCP	Enable	WAN_IF	Allow
4	52.114.76.76	32	0	65535	TCP	Enable	WAN_IF	Allow
5	52.114.7.24	32	0	65535	TCP	Enable	WAN_IF	Allow
6	52.114.14.70	32	0	65535	TCP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

Note: Be aware, that if in your configuration, connectivity to SIP Trunk (or other entities) is performed through the same IP Interface as Teams (WAN_IF in our example), you <u>must</u> add rules to allow traffic from these entities.

5.15 Configure Number Manipulation Rules

This section describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 5.9 on page 48) to denote the source and destination of the call.

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

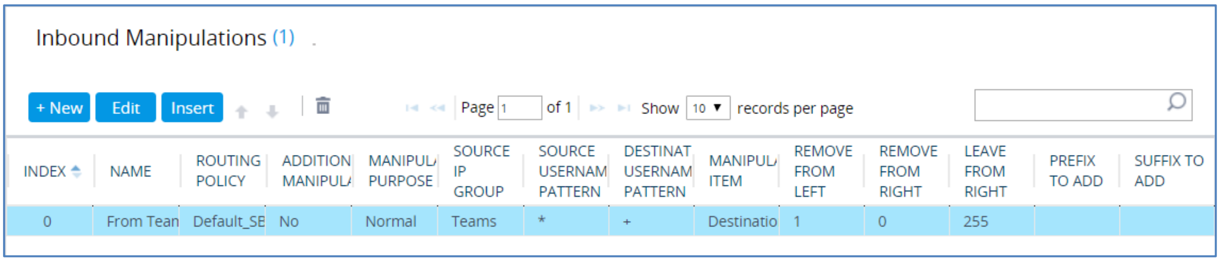
For example, for this interoperability test topology, a manipulation is configured to remove the "+" (plus sign) from the destination number for calls from the Teams Direct Routing IP Group.

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

1. Open the Inbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Inbound Manipulations**).
2. Configure the rules according to your setup.

The figure below shows an example of configured IP-to-IP inbound manipulation rules for calls from Teams Direct Routing IP Group:

Figure 5-25: Example of Configured IP-to-IP Inbound Manipulation Rules



Rule Index	Description
0	Calls from Teams IP Group with the prefix destination number "+", remove one character from left.

5.16 Configure Message Manipulation Rules

This section 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).

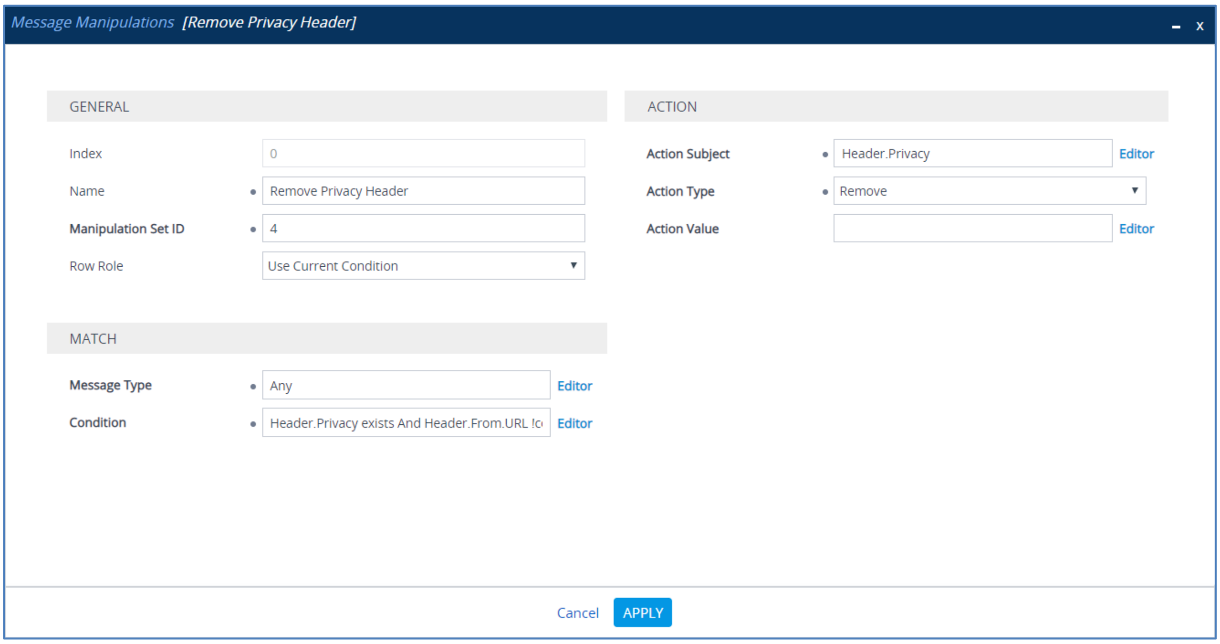
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

➢ **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 new manipulation rule (Manipulation Set 4) for Teams. This rule applies to messages received from the Teams IP Group. This remove the SIP Privacy Header in all messages, except of call with presentation restriction.

Parameter	Value
Index	**0**
Name	**Remove Privacy Header**
Manipulation Set ID	**4**
Message Type	**Any**
Condition	**Header.Privacy exists And Header.From.URL !contains 'anonymous'**
Action Subject	**Header.Privacy**
Action Type	**Remove**

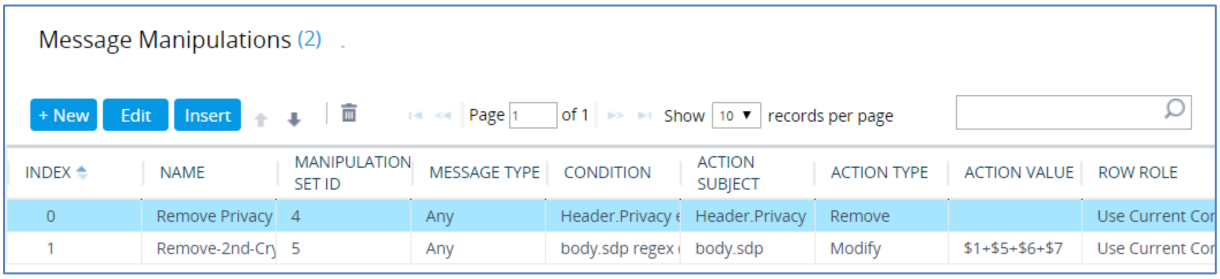
Figure 5-26: Configuring SIP Message Manipulation Rule 0 (for Teams)



3. Configure another manipulation rule (Manipulation Set 5) for Unify OpenScape Voice. This rule applies to messages sent to the Unify OpenScape Voice IP Group. This removes the second crypto line from the SDP part of the message, if it was sent in the wrong order.

Parameter	Value
Index	**1**
Name	**Remove-2nd-Crypto**
Manipulation Set ID	**5**
Message Type	**Any**
Condition	**body.sdp regex (.*)(a=crypto:2)(.*)(\r\n)(a=crypto:1)(.*)(\r\n)(.*)**
Action Subject	**body.sdp**
Action Type	**Modify**
Action Value	**$1+$5+$6+$7**

Figure 5-27: Example of Configured SIP Message Manipulation Rules



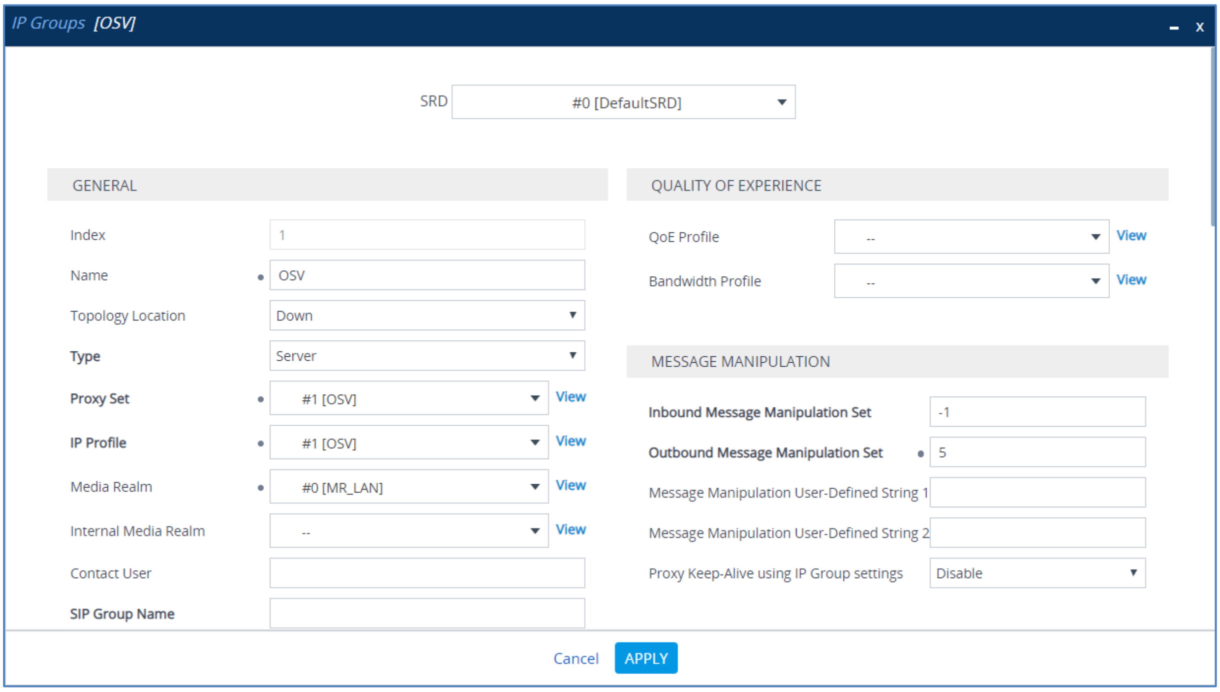
INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Remove Privacy	4	Any	Header.Privacy e	Header.Privacy	Remove		Use Current Cor
1	Remove-2nd-Cry	5	Any	body.sdp regex (	body.sdp	Modify	$1+$5+$6+$7	Use Current Cor

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set IDs (Manipulation Set IDs 4 and 5) and which are executed for messages sent to and from the Unify OpenScape Voice IP Group as well as the Teams Direct Routing IP Group. These rules are specifically required to enable proper interworking between Unify OpenScape Voice and Teams Direct Routing. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages received from the Teams IP Group. It removes the SIP Privacy Header.	Microsoft Office 365 may be configured to send a Privacy header. We recommend doing this in the SBC, for better interoperability.
1	This rule applies to messages sent to the Unify OpenScape Voice IP Group. This removes the second crypto line from the SDP part of the message, if it is sent in the wrong order.	For better interoperability with Unify OpenScape Voice.

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

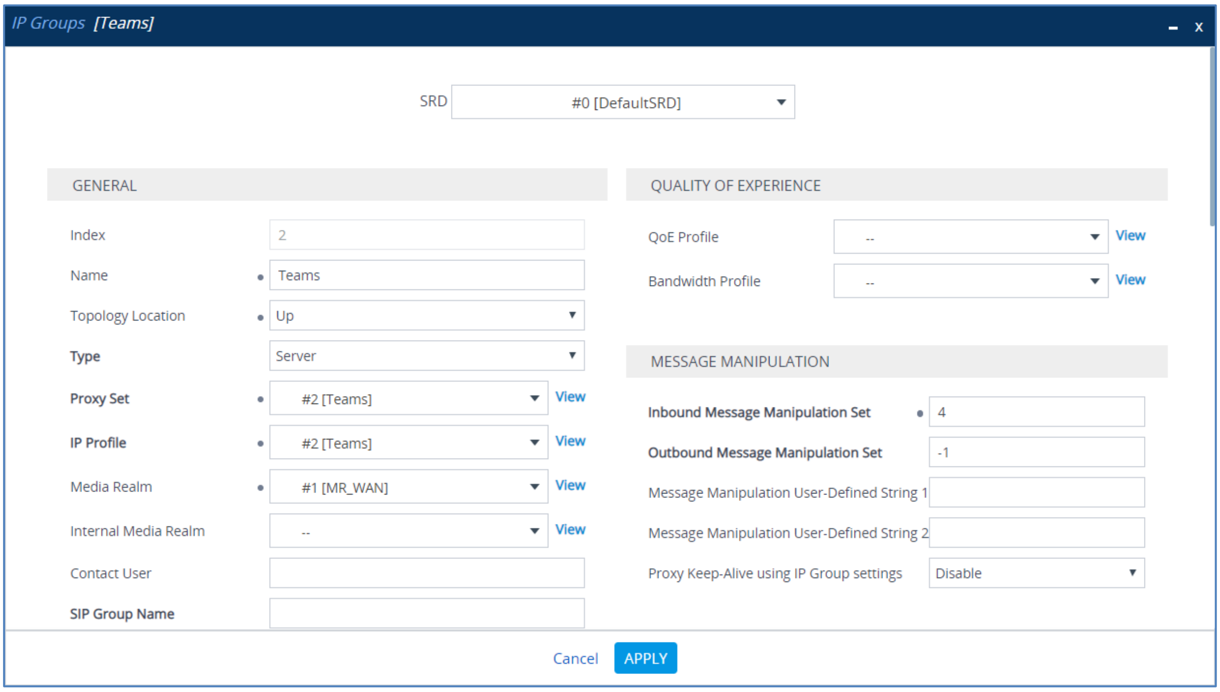
Figure 5-28: Assigning Manipulation Set to the Unify OpenScape Voice IP Group



   d. Click **Apply**.

5. Assign Manipulation Set ID 4 to the Teams Direct Routing IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the Teams Direct Routing IP Group, and then click **Edit**.
   c. Set the 'Inbound Message Manipulation Set' field to **4**.

Figure 5-29: Assigning Manipulation Set to the Teams Direct Routing IP Group



   d. Click **Apply**.

5.17 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

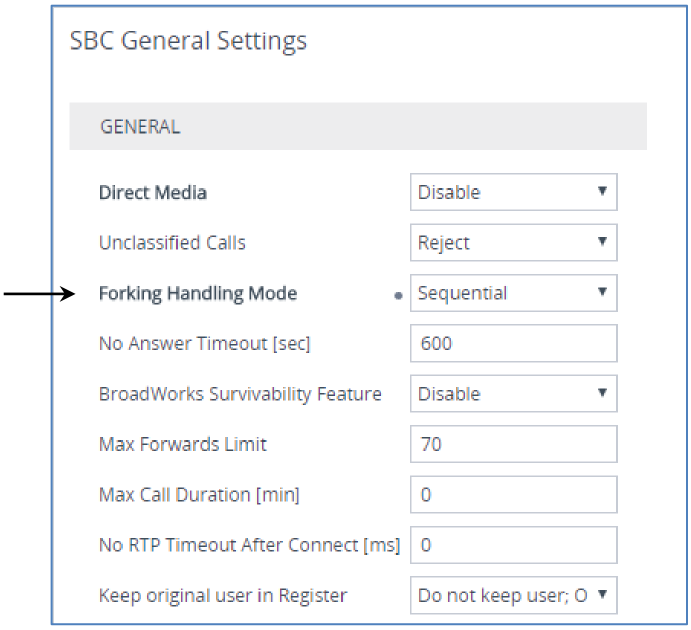
5.17.1 Configure Call Forking Mode

This section describes how to configure the SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if a SIP 18x response with SDP is received, the SBC opens a voice stream according to the received SDP. The SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if a 180 response without SDP is received. It is mandatory to set this field for the Teams Direct Routing environment.

➢ **To configure call forking:**

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

Figure 5-30: Configuring Forking Mode



3. Click **Apply**.

5.17.2 Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only)

This section describes how to optimize the SBC's CPU cores usage for a specified profile to achieve maximum capacity for that profile. The supported profiles include:

- SIP profile – improves SIP signaling performance, for example, SIP calls per second (CPS)
- SRTP profile – improves maximum number of SRTP sessions
- Transcoding profile – enables all DSP-required features, for example, transcoding and voice in-band detectors

➢ **To optimize core allocation for a profile:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'SBC Performance Profile' drop-down list, select the required profile:

3. Click **Apply**, and then reset the device with a burn-to-flash for your settings to take effect.

This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the SBC, corresponding to the Web-based configuration as described in Section 4 on page 17, is shown below:

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

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

;Board: M800B
;Board Type: 72
;Serial Number: 12197872
;Product Key: DT3465123
;Slot Number: 1
;Software Version: 7.20A.254.376
;DSP Software Version: 5014AE3_R => 710.16
;Board IP Address: 10.8.242.78
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.8.242.1
;Ram size: 512M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 3
;Num of physical LAN ports: 12
;Profile: NONE
;;;Key features:;Board Type: M800B ;IP Media: VXML ;Channel Type:
DspCh=150 ;HA ;PSTN Protocols: IUA=2 CAS ;DSP Voice features: IpmDetector
;Coders: G723 G729 GSM-FR G727 ILBC G722 SILK_NB SILK_WB OPUS_NB OPUS_WB
;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;System features: ProducrKey=DT3465123 ;Control Protocols: TEAMS MSFT
FEU=10 TestCall=10 MGCP SIP SBC=10 ;Default features:;Coders: G711 G726;

;-----  HW components -----
;
; Slot # : Module type : # of ports
;----------------------------------------------
;      1 : Empty
;      2 : Empty
;      3 : Empty
;----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.8.242.251
EnableSyslog = 1
NTPServerUTCOffset = 7200
ENABLEPARAMETERSMONITORING = 1
ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'naa', 'spc', 'll',
'cli', 'ae'
HALocalMAC = '00908fba1ff0'
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
```

```
NTPServerIP = '10.8.251.104'
SyslogLogLevel = 7
PM_VEDSPUtil = '1,135,150,15'

[BSP Params]

PCMLawSelect = 3
EnableCoreDump = 0
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0

[PSTN Params]

V5ProtocolSide = 0

[Voice Engine Params]

ENABLEMEDIASECURITY = 1
PLThresholdLevelsPerMille_0 = 5
PLThresholdLevelsPerMille_1 = 10
PLThresholdLevelsPerMille_2 = 20
PLThresholdLevelsPerMille_3 = 50
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

Languages = 'en-US', '', '', '', '', '', '', '', '', ''

[SIP Params]

GWDEBUGLEVEL = 5
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[SNMP Params]


[ PhysicalPortsTable ]

FORMAT Index = Port, Mode, SpeedDuplex, PortDescription, GroupMember;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2";
PhysicalPortsTable 4 = "FE_5_1", 1, 4, "User Port #4", "GROUP_3";
PhysicalPortsTable 5 = "FE_5_2", 1, 4, "User Port #5", "GROUP_3";
PhysicalPortsTable 6 = "FE_5_3", 1, 4, "User Port #6", "GROUP_4";
```

```
PhysicalPortsTable 7 = "FE_5_4", 1, 4, "User Port #7", "GROUP_4";
PhysicalPortsTable 8 = "FE_5_5", 1, 4, "User Port #8", "GROUP_5";
PhysicalPortsTable 9 = "FE_5_6", 1, 4, "User Port #9", "GROUP_5";
PhysicalPortsTable 10 = "FE_5_7", 1, 4, "User Port #10", "GROUP_6";
PhysicalPortsTable 11 = "FE_5_8", 1, 4, "User Port #11", "GROUP_6";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT Index = Group, Mode, Member1, Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 2, "FE_5_1", "FE_5_2";
EtherGroupTable 3 = "GROUP_4", 2, "FE_5_3", "FE_5_4";
EtherGroupTable 4 = "GROUP_5", 2, "FE_5_5", "FE_5_6";
EtherGroupTable 5 = "GROUP_6", 2, "FE_5_7", "FE_5_8";
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 0, "", "";
EtherGroupTable 8 = "GROUP_9", 0, "", "";
EtherGroupTable 9 = "GROUP_10", 0, "", "";
EtherGroupTable 10 = "GROUP_11", 0, "", "";
EtherGroupTable 11 = "GROUP_12", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

FORMAT Index = VlanID, UnderlyingInterface, DeviceName, Tagging, MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT Index = ApplicationTypes, InterfaceMode, IPAddress, PrefixLength,
Gateway, InterfaceName, PrimaryDNSServerIPAddress,
SecondaryDNSServerIPAddress, UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.8.242.78, 24, 10.8.242.1, "LAN_IF",
10.8.251.103, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.97.14.76, 27, 195.97.14.65, "WAN_IF",
8.8.8.8, 0.0.0.0, "vlan 2";

[ \InterfaceTable ]


[ ACCESSLIST ]

FORMAT Index = Source_IP, Source_Port, PrefixLen, Start_Port, End_Port,
Protocol, Use_Specific_Interface, Interface_ID, Packet_Size, Byte_Rate,
Byte_Burst, Allow_type_enum, Description;
ACCESSLIST 0 = "8.8.8.8", 0, 32, 0, 65535, "Any", 1, "WAN_IF", 0, 0, 0,
0, "8.8.8.8";
```

```
ACCESSLIST 1 = "52.114.148.0", 0, 32, 0, 65535, "TCP", 1, "WAN_IF", 0, 0,
0, 0, "52.114.148.0";
ACCESSLIST 2 = "52.114.132.46", 0, 32, 0, 65535, "TCP", 1, "WAN_IF", 0,
0, 0, 0, "52.114.132.46";
ACCESSLIST 3 = "52.114.75.24", 0, 32, 0, 65535, "TCP", 1, "WAN_IF", 0, 0,
0, 0, "52.114.75.24";
ACCESSLIST 4 = "52.114.76.76", 0, 32, 0, 65535, "TCP", 1, "WAN_IF", 0, 0,
0, 0, "52.114.76.76";
ACCESSLIST 5 = "0.0.0.0", 0, 32, 0, 65535, "TCP", 1, "WAN_IF", 0, 0, 0,
0, "52.114.7.24";
ACCESSLIST 6 = "52.114.14.70", 0, 32, 0, 65535, "TCP", 1, "WAN_IF", 0, 0,
0, 0, "52.114.14.70";
ACCESSLIST 49 = "0.0.0.0", 0, 0, 0, 65535, "Any", 1, "WAN_IF", 0, 0, 0,
1, "0.0.0.0";

[ \ACCESSLIST ]


[ WebUsers ]

FORMAT Index = Username, Password, Status, PwAgeInterval, SessionLimit,
CliSessionLimit, SessionTimeout, BlockTime, UserLevel, PwNonce,
SSHPublicKey;
WebUsers 0 = "Admin",
"$1$GioiKHt7exkTGkYWFhRGHRtJTkkeTB4AVQVQAgMDBAwLDAgJDgkPIXl2c3AmJ3NxfHktf
Sl5e2A0NmRjMGNjYW4=", 1, 0, 5, -1, 15, 60, 200,
"74685f37fe219694a700b1c59761b3eb", "";
WebUsers 1 = "User",
"$1$alxfXVlcVkFAFEQXQRVOTU5OGUxNSx2wueG24uTg4rqx6++57rjqqKWh9/Clp/WhrKuqp
aqvqpiVxMGVlMPGnJs=", 1, 0, 5, -1, 15, 60, 50,
"f5cd8f217d7fe0393122930a78e0aabf", "";

[ \WebUsers ]


[ TLSContexts ]

FORMAT Index = Name, TLSVersion, DTLSVersion, ServerCipherString,
ClientCipherString, RequireStrictCert, OcspEnable, OcspServerPrimary,
OcspServerSecondary, OcspServerPort, OcspDefaultResponse, DHKeySize;
TLSContexts 0 = "default", 0, 0, "DEFAULT", "DEFAULT", 0, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;
TLSContexts 1 = "Teams", 4, 0, "DEFAULT", "DEFAULT", 0, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 2048;

[ \TLSContexts ]


[ AudioCodersGroups ]

FORMAT Index = Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";

[ \AudioCodersGroups ]


[ IpProfile ]

FORMAT Index = ProfileName, IpPreference, CodersGroupName, IsFaxUsed,
JitterBufMinDelay, JitterBufOptFactor, IPDiffServ, SigIPDiffServ,
```

```
RTPRedundancyDepth, CNGmode, VxxTransportType, NSEMode, IsDTMFUsed,
PlayRBTone2IP, EnableEarlyMedia, ProgressIndicator2IP,
EnableEchoCanceller, CopyDest2RedirectNumber, MediaSecurityBehaviour,
CallLimit, DisconnectOnBrokenConnection, FirstTxDtmfOption,
SecondTxDtmfOption, RxDTMFOption, EnableHold, InputGain, VoiceVolume,
AddIEInSetup, SBCExtensionCodersGroupName, MediaIPVersionPreference,
TranscodingMode, SBCAllowedMediaTypes, SBCAllowedAudioCodersGroupName,
SBCAllowedVideoCodersGroupName, SBCAllowedCodersMode,
SBCMediaSecurityBehaviour, SBCRFC2833Behavior, SBCAlternativeDTMFMethod,
SBCSendMultipleDTMFMethods, SBCAssertIdentity,
AMDSensitivityParameterSuit, AMDSensitivityLevel, AMDMaxGreetingTime,
AMDMaxPostSilenceGreetingTime, SBCDiversionMode, SBCHistoryInfoMode,
EnableQSIGTunneling, SBCFaxCodersGroupName, SBCFaxBehavior,
SBCFaxOfferMode, SBCFaxAnswerMode, SbcPrackMode, SBCSessionExpiresMode,
SBCRemoteUpdateSupport, SBCRemoteReinviteSupport,
SBCRemoteDelayedOfferSupport, SBCRemoteReferBehavior,
SBCRemote3xxBehavior, SBCRemoteMultiple18xSupport,
SBCRemoteEarlyMediaResponseType, SBCRemoteEarlyMediaSupport,
EnableSymmetricMKI, MKISize, SBCEnforceMKISize, SBCRemoteEarlyMediaRTP,
SBCRemoteSupportsRFC3960, SBCRemoteCanPlayRingback, EnableEarly183,
EarlyAnswerTimeout, SBC2833DTMFPayloadType, SBCUserRegistrationTime,
ResetSRTPStateUponRekey, AmdMode, SBCReliableHeldToneSource,
GenerateSRTPKeys, SBCPlayHeldTone, SBCRemoteHoldFormat,
SBCRemoteReplacesBehavior, SBCSDPPtimeAnswer, SBCPreferredPTime,
SBCUseSilenceSupp, SBCRTPRedundancyBehavior, SBCPlayRBTToTransferee,
SBCRTCPMode, SBCJitterCompensation, SBCRemoteRenegotiateOnFaxDetection,
JitterBufMaxDelay, SBCUserBehindUdpNATRegistrationTime,
SBCUserBehindTcpNATRegistrationTime, SBCSDPHandleRTCPAttribute,
SBCRemoveCryptoLifetimeInSDP, SBCIceMode, SBCRTCPMux,
SBCMediaSecurityMethod, SBCHandleXDetect, SBCRTCPFeedback,
SBCRemoteRepresentationMode, SBCKeepVIAHeaders, SBCKeepRoutingHeaders,
SBCKeepUserAgentHeader, SBCRemoteMultipleEarlyDialogs,
SBCRemoteMultipleAnswersMode, SBCDirectMediaTag,
SBCAdaptRFC2833BWToVoiceCoderBW, CreatedByRoutingServer,
SBCFaxReroutingMode, SBCMaxCallDuration, SBCGenerateRTP,
SBCISUPBodyHandling, SBCISUPVariant, SBCVoiceQualityEnhancement,
SBCMaxOpusBW, SBCEnhancedPlc, LocalRingbackTone, LocalHeldTone,
SBCGenerateNoOp, SBCRemoveUnKnownCrypto, SBCMultipleCoders, DataDiffServ,
SBCMSRPReinviteUpdateSupport, SBCMSRPOfferSetupRole, SBCMSRPEmpMsg;
IpProfile 1 = "OSV", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "",
"", "", 0, 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, 1,
0, 0, 1, 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, 0, 0, 1, 2, 0;
IpProfile 2 = "Teams", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "", "", 0, 1, 0, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, "", 0, 0, 1, 3, 0, 0, 1, 0, 3, 2, 1, 0, 1, 0, 0, 0, 1, 0,
1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 3, 0, 0, 0, 1, 0, 0, 1, 0, 0, 300, -1, -1,
0, 0, 1, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, -1, -1, 0, 0, 0, 0, 1, 2, 0;

[ \IpProfile ]


[ CpMediaRealm ]

FORMAT Index = MediaRealmName, IPv4IF, IPv6IF, RemoteIPv4IF,
RemoteIPv6IF, PortRangeStart, MediaSessionLeg, PortRangeEnd,
TCPPortRangeStart, TCPPortRangeEnd, IsDefault, QoeProfile, BWProfile,
TopologyLocation;
CpMediaRealm 0 = "MR_LAN", "LAN_IF", "", "", "", 6000, 100, 6999, 0, 0,
0, "", "", 0;
```

```
CpMediaRealm 1 = "MR_WAN", "WAN_IF", "", "", "", 7000, 100, 7999, 0, 0,
0, "", "", 1;

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost,
LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]


[ SRD ]

FORMAT Index = Name, BlockUnRegUsers, MaxNumOfRegUsers,
EnableUnAuthenticatedRegistrations, SharingPolicy, UsedByRoutingServer,
SBCOperationMode, SBCRoutingPolicyName, SBCDialPlanName,
AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "",
"";

[ \SRD ]


[ MessagePolicy ]

FORMAT Index = Name, MaxMessageLength, MaxHeaderLength, MaxBodyLength,
MaxNumHeaders, MaxNumBodies, SendRejection, MethodList, MethodListType,
BodyList, BodyListType, UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;

[ \MessagePolicy ]


[ SIPInterface ]

FORMAT Index = InterfaceName, NetworkInterface,
SCTPSecondaryNetworkInterface, ApplicationType, UDPPort, TCPPort,
TLSPort, SCTPPort, AdditionalUDPPorts, AdditionalUDPPortsMode, SRDName,
MessagePolicyName, TLSContext, TLSMutualAuthentication,
TCPKeepaliveEnable, ClassificationFailureResponseType,
PreClassificationManSet, EncapsulatingProtocol, MediaRealm,
SBCDirectMedia, BlockUnRegUsers, MaxNumOfRegUsers,
EnableUnAuthenticatedRegistrations, UsedByRoutingServer,
TopologyLocation, PreParsingManSetName, AdmissionProfile,
CallSetupRulesSetId;
SIPInterface 0 = "OSV", "LAN_IF", "", 2, 5060, 0, 0, 0, "", 0,
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MR_LAN", 0, -1, -1, -1,
0, 0, "", "", -1;
SIPInterface 1 = "Teams", "WAN_IF", "", 2, 0, 0, 5067, 0, "", 0,
"DefaultSRD", "", "Teams", -1, 1, 0, -1, 0, "MR_WAN", 0, -1, -1, -1, 0,
1, "", "", -1;

[ \SIPInterface ]
```

```
[ ProxySet ]

FORMAT Index = ProxyName, EnableProxyKeepAlive, ProxyKeepAliveTime,
ProxyLoadBalancingMethod, IsProxyHotSwap, SRDName, ClassificationInput,
TLSContextName, ProxyRedundancyMode, DNSResolveMethod,
KeepAliveFailureResp, GWIPv4SIPInterfaceName, SBCIPv4SIPInterfaceName,
GWIPv6SIPInterfaceName, SBCIPv6SIPInterfaceName, MinActiveServersLB,
SuccessDetectionRetries, SuccessDetectionInterval,
FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "OSV", "", "", 1, 1, 10, -1;
ProxySet 1 = "OSV", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"OSV", "", "", 1, 1, 10, -1;
ProxySet 2 = "Teams", 1, 60, 2, 1, "DefaultSRD", 0, "Teams", -1, -1, "",
"", "Teams", "", "", 1, 1, 10, -1;

[ \ProxySet ]


[ IPGroup ]

FORMAT Index = Type, Name, ProxySetName, SIPGroupName, ContactUser,
SipReRoutingMode, AlwaysUseRouteTable, SRDName, MediaRealm,
ClassifyByProxySet, ProfileName, MaxNumOfRegUsers, InboundManSet,
OutboundManSet, RegistrationMode, AuthenticationMode, MethodList,
SBCServerAuthType, OAuthHTTPService, EnableSBCClientForking,
SourceUriInput, DestUriInput, TopologyHidingHeaderList, ContactName,
Username, Password, UUIFormat, QOEProfile, BWProfile,
AlwaysUseSourceAddr, MsgManUserDef1, MsgManUserDef2, SIPConnect,
SBCPSAPMode, DTLSContext, CreatedByRoutingServer, UsedByRoutingServer,
SBCOperationMode, SBCRouteUsingRequestURIPort, SBCKeepOriginalCallID,
TopologyLocation, SBCDialPlanName, CallSetupRulesSetId, Tags,
SBCUserStickiness, UserUDPPortAssignment, AdmissionProfile,
ProxyKeepAliveUsingIPG, SBCAltRouteReasonsSetName;
IPGroup 0 = 0, "Default_IPG", , , , -1, 0, "DefaultSRD", , 0, , -1, -1, -
1, 0, 0, , -1, , 0, -1, -1, , , , "$1$gQ==", 0, , , 0, 0, 0, 0, 0,
"default", 0, 0, -1, 0, 0, 0, , -1, , 0, 0, , 0, ;
IPGroup 1 = 0, "OSV", "OSV", , , -1, 0, "DefaultSRD", "MR_LAN", 1, "OSV",
-1, -1, 5, 0, 0, , -1, , 0, -1, -1, , , , "$1$gQ==", 0, , , 0, 0, 0, 0,
0, "default", 0, 0, -1, 0, 0, 0, , -1, , 0, 0, , 0, ;
IPGroup 2 = 0, "Teams", "Teams", , , -1, 0, "DefaultSRD", "MR_WAN", 0,
"Teams", -1, 4, -1, 0, 0, , -1, , 0, -1, -1, , "sbc.drtests.com", ,
"$1$gQ==", 0, , , 1, 0, 0, 0, 0, "default", 0, 0, -1, 0, 0, 1, , -1, , 0,
0, , 1, ;

[ \IPGroup ]


[ ProxyIp ]

FORMAT Index = ProxySetId, ProxyIpIndex, IpAddress, TransportType,
Priority, Weight;
ProxyIp 0 = "1", 0, "10.8.242.16:5060", 0, 0, 0;
ProxyIp 1 = "2", 0, "sip.pstnhub.microsoft.com:5061", 2, 1, 1;
ProxyIp 2 = "2", 1, "sip2.pstnhub.microsoft.com:5061", 2, 2, 1;
ProxyIp 3 = "2", 2, "sip3.pstnhub.microsoft.com:5061", 2, 3, 1;

[ \ProxyIp ]


[ ConditionTable ]
```

```
FORMAT Index = Name, Condition;
ConditionTable 0 = "Teams-Contact", "header.contact.url.host contains
'pstnhub.microsoft.com'";

[ \ConditionTable ]


[ IP2IPRouting ]

FORMAT Index = RouteName, RoutingPolicyName, SrcIPGroupName,
SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost, RequestType,
MessageConditionName, ReRouteIPGroupName, Trigger, CallSetupRulesSetId,
DestType, DestIPGroupName, DestSIPInterfaceName, DestAddress, DestPort,
DestTransportType, AltRouteOptions, GroupPolicy, CostGroup, DestTags,
SrcTags, IPGroupSetName, RoutingTagName, InternalAction;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 1 = "REFER from Teams", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 0, "", "Teams", 2, -1, 2, "Teams", "", "", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 2 = "Teams to OSV", "Default_SBCRoutingPolicy", "Teams",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "OSV", "", "", 0, -1, 0, 0,
"", "", "", "", "default", "";
IP2IPRouting 3 = "OSV to Teams", "Default_SBCRoutingPolicy", "OSV", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "Teams", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "";

[ \IP2IPRouting ]


[ Classification ]

FORMAT Index = ClassificationName, MessageConditionName, SRDName,
SrcSIPInterfaceName, SrcAddress, SrcPort, SrcTransportType,
SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost, ActionType,
SrcIPGroupName, DestRoutingPolicy, IpProfileName, IPGroupSelection,
IpGroupTagName;
Classification 0 = "Teams", "Teams-Contact", "DefaultSRD", "Teams",
"52.114.*.*", 0, -1, "*", "*", "*", "sbc.drtests.com", 1, "Teams", "",
"", 0, "default";

[ \Classification ]


[ MessageManipulations ]

FORMAT Index = ManipulationName, ManSetID, MessageType, Condition,
ActionSubject, ActionType, ActionValue, RowRole;
MessageManipulations 0 = "Remove Privacy Header", 4, "Any",
"Header.Privacy exists And Header.From.URL !contains 'anonymous'",
"Header.Privacy", 1, "", 0;
MessageManipulations 1 = "Remove-2nd-Crypto", 5, "Any", "body.sdp regex
(.*)(a=crypto:2)(.*)(\r\n)(a=crypto:1)(.*)(\r\n)(.*)", "body.sdp", 2,
"$1+$5+$6+$7", 0;

[ \MessageManipulations ]
```

```
[ GwRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost,
LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ \GwRoutingPolicy ]


[ MaliciousSignatureDB ]

FORMAT Index = Name, Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'";
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix
'smap'";
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 ]


[ AudioCoders ]

FORMAT Index = AudioCodersGroupId, AudioCodersIndex, Name, pTime, rate,
PayloadType, Sce, CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 2, 1, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_0", 3, 2, 2, 90, -1, 0, "";
AudioCoders 2 = "AudioCodersGroups_0", 0, 35, 2, 19, 103, 0, "";
AudioCoders 3 = "AudioCodersGroups_0", 1, 36, 2, 43, 104, 0, "";
AudioCoders 4 = "AudioCodersGroups_0", 4, 3, 2, 19, -1, 0, "";
AudioCoders 5 = "AudioCodersGroups_0", 5, 20, 1, 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.
200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Document #: LTRT-39325