

Microsoft® Teams Direct Routing Enterprise Model and VoIP.ms SIP Trunk using AudioCodes Mediant™ SBC

Version 7.2

Microsoft Partner

Gold Communications

VOIP.ms



Microsoft Teams

ac audiocodes

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	VoIP.ms SIP Trunking 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 AudioCodes SBC	17
4.1	SBC Configuration Concept in Teams Direct Routing Enterprise Model	18
4.2	IP Network Interfaces Configuration	18
4.2.1	Configure VLANs	19
4.2.2	Configure Network Interfaces.....	19
4.3	SIP TLS Connection Configuration	21
4.3.1	Configure the NTP Server Address	21
4.3.2	Create a TLS Context for Teams Direct Routing.....	22
4.3.3	Configure a Certificate	23
4.3.4	Method of Generating and Installing the Wildcard Certificate	26
4.3.5	Deploy Baltimore Trusted Root Certificate	27
4.4	Configure Media Realms	28
4.5	Configure SIP Signaling Interfaces	29
4.6	Configure Proxy Sets and Proxy Address.....	30
4.6.1	Configure a Proxy Address.....	31
4.7	Configure Coders	33
4.8	Configure IP Profiles.....	36
4.9	Configure IP Groups.....	39
4.10	Configure SRTP	40
4.11	Configuring Message Condition Rules.....	41
4.12	Configuring Classification Rules	42
4.13	Configure IP-to-IP Call Routing Rules	43
4.14	Configuring Firewall Settings.....	44

4.15	Configure Number Manipulation Rules	45
4.16	Configure Message Manipulation Rules	46
4.17	Configure Registration Accounts (optional).....	58
4.18	Miscellaneous Configuration.....	59
4.18.1	Configure Call Forking Mode.....	59
4.18.2	Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only)	60
A	AudioCodes INI File	61

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: January-09-2020

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
29355	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 VoIP.ms's SIP Trunk 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 VoIP.ms partners who are responsible for installing and configuring VoIP.ms's SIP Trunk 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 to 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	<ul style="list-style-type: none"> ▪ 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.254.565 or later
Protocol	<ul style="list-style-type: none"> ▪ SIP/UDP (to the VoIP.ms SIP Trunk) ▪ SIP/TLS (to the Teams Direct Routing)
Additional Notes	None

2.2 VoIP.ms SIP Trunking Version

Table 2-2: VoIP.ms Version

Vendor/Service Provider	VoIP.ms
SSW Model/Service	
Software Version	
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	Release v.2019.11.28.2
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

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

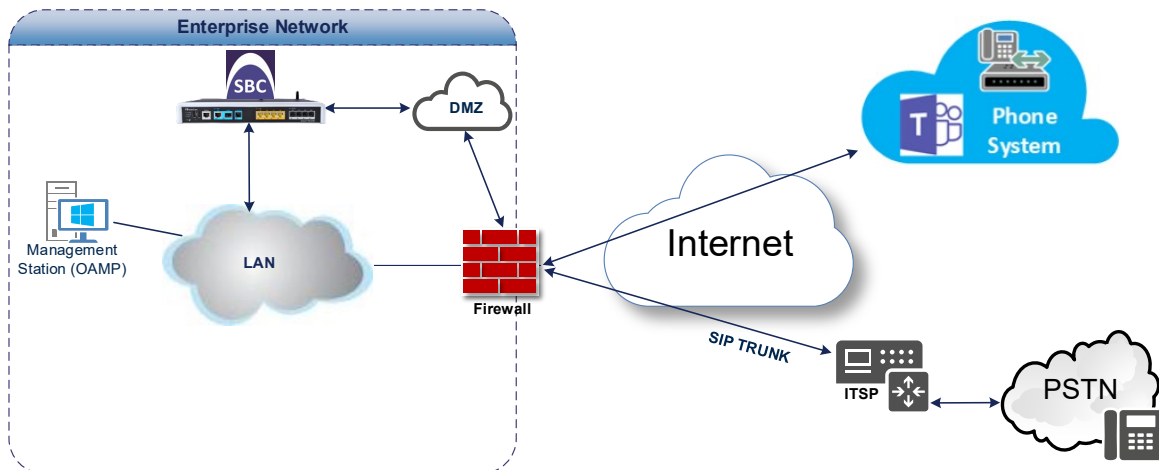
2.4.1 Enterprise Model Implementation

The interoperability testing between AudioCodes SBC and VoIP.ms SIP Trunk with Teams Direct Routing Enterprise Model was done using the following topology setup:

- Enterprise deployed with third-party 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
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using VoIP.ms's SIP Trunking service
- AudioCodes SBC is implemented to interconnect between the SIP Trunk 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 VoIP.ms's SIP Trunk 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 VoIP.ms SIP Trunk



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	<ul style="list-style-type: none"> Microsoft Teams Direct Routing environment and VoIP.ms SIP Trunk are located on the Enterprise's (or Service Provider's) WAN
Signaling Transcoding	<ul style="list-style-type: none"> Microsoft Teams Direct Routing operates with SIP-over-TLS transport type VoIP.ms SIP Trunk operates with SIP-over-UDP or SIP-over-TCP or SIP-over-TLS transport types
Codecs Transcoding	<ul style="list-style-type: none"> Microsoft Teams Direct Routing supports G.711A-law, G.711U-law, G.729, G.722, SILK (NB and WB) and OPUS coders VoIP.ms SIP Trunk supports G.711A-law, G.711U-law, and G.729 coders
Media Transcoding	<ul style="list-style-type: none"> Microsoft Teams Direct Routing operates with SRTP media type VoIP.ms SIP Trunk operates with RTP or SRTP media types

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 VoIP.ms's SIP Trunk.

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

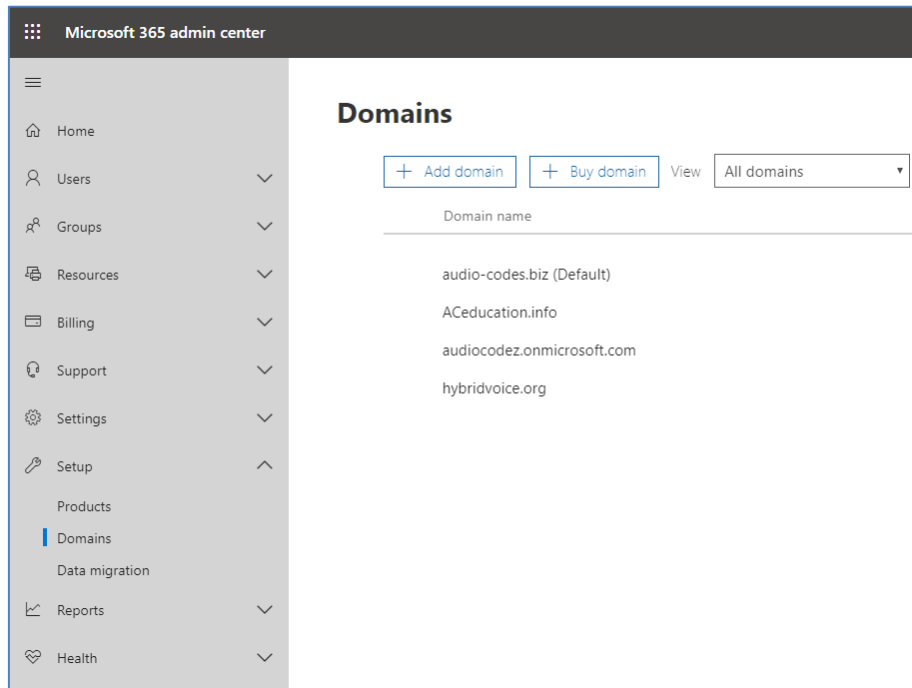
3.2 SBC Domain Name in the Teams Enterprise Model

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	<p>Valid names:</p> <ul style="list-style-type: none"> ▪ sbc.ACeducation.info ▪ ussbcs15.ACeducation.info ▪ europe.ACeducation.info <p>Invalid name: sbc1.europe.ACeducation.info (requires registering domain name europe.atatum.biz in 'Domains' first)</p>
adatumbiz.onmicrosoft.com	No	Using *.onmicrosoft.com domains is not supported for SBC names
hybridvoice.org	Yes	<p>Valid names:</p> <ul style="list-style-type: none"> ▪ sbc1.hybridvoice.org ▪ ussbcs15.hybridvoice.org ▪ europe.hybridvoice.org <p>Invalid name: sbc1.europe.hybridvoice.org (requires registering domain name europe.hybridvoice.org in 'Domains' first)</p>

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 (**sb1.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 5068 -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       : 5068
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 AudioCodes SBC

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

- SBC LAN interface – Management Station
- SBC WAN interface - VoIP.ms SIP Trunking and 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 VoIP.ms SIP Trunk 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



4.1 SBC Configuration Concept in Teams Direct Routing Enterprise Model

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

Figure 4-1: SBC Configuration Concept

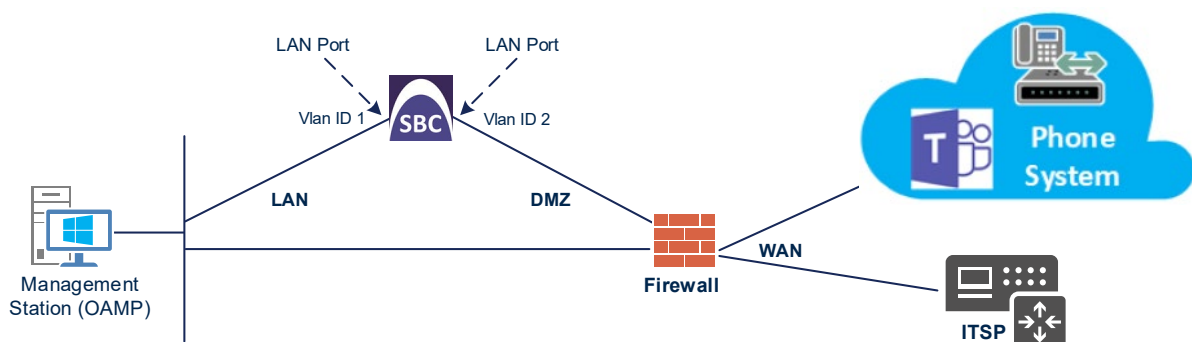


4.2 IP Network Interfaces Configuration

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, located on the LAN
 - Microsoft Teams Direct Routing and VoIP.ms SIP Trunk, 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 4-2: Network Interfaces in Interoperability Test Topology



4.2.1 Configure VLANs

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

- LAN (assigned the name "LAN_IF")
- WAN (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 4-3: Configured VLAN IDs in Ethernet Device

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

4.2.2 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 4-1: 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 4-4: 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

4.3 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>

4.3.1 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., **10.15.28.1**).

Figure 4-5: Configuring NTP Server Address

NTP SERVER	
Enable NTP	Enable
Primary NTP Server Address (IP or FQDN)	10.15.28.1
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

3. Click **Apply**.

4.3.2 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 4-2: New TLS Context

Index	Name	TLS Version
1	Teams (arbitrary descriptive name)	TLSv1.2
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 4-6: Configuring TLS Context for Teams Direct Routing

TLS Contexts [Teams]
- x

GENERAL	OCSP
Index <input style="width: 80%;" type="text" value="1"/>	OCSP Server <input style="width: 80%;" type="text" value="Disable"/>
Name <input style="width: 80%;" type="text" value="Teams"/>	Primary OCSP Server <input style="width: 80%;" type="text" value="0.0.0.0"/>
TLS Version <input style="width: 80%;" type="text" value="TLSv1.2"/>	Secondary OCSP Server <input style="width: 80%;" type="text" value="0.0.0.0"/>
DTLS Version <input style="width: 80%;" type="text" value="Any"/>	OCSP Port <input style="width: 80%;" type="text" value="2560"/>
Cipher Server <input style="width: 80%;" type="text" value="RC4:AES128"/>	OCSP Default Response <input style="width: 80%;" type="text" value="Reject"/>
Cipher Client <input style="width: 80%;" type="text" value="DEFAULT"/>	
Strict Certificate Extension Validation <input style="width: 80%;" type="text" value="Disable"/>	
DH key Size <input style="width: 80%;" type="text" value="1024"/>	

Cancel APPLY

3. Click **Apply**.

4.3.3 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 4-7: Example of Certificate Signing Request – Creating CSR

➔
TLS Context [#1] > Change Certificates

CERTIFICATE SIGNING REQUEST

Common Name [CN]	<input type="text" value="sbc1.hybridvoice.org"/>
Organizational Unit [OU] (optional)	<input type="text"/>
Company name [O] (optional)	<input type="text"/>
Locality or city name [L] (optional)	<input type="text"/>
State [ST] (optional)	<input type="text"/>
Country code [C] (optional)	<input type="text"/>
1st Subject Alternative Name [SAN]	DNS ▾ sbc1.hybridvoice.org
2nd Subject Alternative Name [SAN]	EMAIL ▾ <input type="text"/>
3rd Subject Alternative Name [SAN]	EMAIL ▾ <input type="text"/>
4th Subject Alternative Name [SAN]	EMAIL ▾ <input type="text"/>
5th Subject Alternative Name [SAN]	EMAIL ▾ Admin
Signature Algorithm	SHA-256 ▾

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

```

-----BEGIN CERTIFICATE REQUEST-----
MIICDCCAZACQwHzEdMBsGA1UEAwUzZjJMS5oelhJyahR2b2ljZS55cmVmcwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAAoIBAQC8nu05z1bAcEmr1DBk0eJRv0IB
YIcZ02DAWwixiY/5v8efjjGIVlnmAnBXJfdds6MgI8RnWJVTXCLW9fh5p4RTjeRV
kZuXhzWzI9is1AAwXj08beTHP6U0em0P9j6YgDo9e+4GTbDah1DMNkFMDy0i2tCt
YdywNeklIOa5f41MLjkgv07hLp51gRjEgM7okVBXeMMTjNkF+8BvxT2Bn3FKi3m+
5iLU0zwt2r6XXtjvFH0Av3MhsdUBWE+XYVFBGAGISYErH21iNjseiG0KEqcH31y/
RqsrviXXyImCv/C4Fj1SmcZaph448TCYR95h3gQmheQGuRt4/VFJjIOqN1zRagMB
AAgRDBCBgkqhkiG9w0BCQ4xNTAzMjB8GA1UdEQYMBaCFHniYzEuaH1cm1kdm9p
Y2Uub3JnBAGA1UdEQYMAeBBUFkbW1uMA0GCSqGSIb3DQEBCwUAA4IBAQCzFYrP
h34bG+m/Lg5n9gGGj2b+Dd6crWnqraM149G5h1x+CdwngYuo0h9Zx1ynq8p00Zj
hQaCKLW/P25Vxz6zE9eIHx/s18muGKlw1k0aIWXEeXivcsU99GuRYdFI74/brFCut
f/Ip/Hn10mtFKEIA3z/9M9MnFYNasOvcFxrV5QG5Nkm1paCwraH/dFFF7GP3hngD
7njK6JVNcy3pPr1KsR4XEX1sv3aT1YdM6o1GDR0b9G16uATqwJn1XXTsUw0o9wjX
7Nd0saoUxvFKv1+eU4eejt2Fpb305Gwigo6wxsDDmCbJ/u3KxoJ1rx0f3R/KjKEuZ
CqRbD0U4MkbeSwo
-----END CERTIFICATE REQUEST-----
    
```

GENERATE NEW PRIVATE KEY AND SELF-SIGNED CERTIFICATE

Private Key Size	<input type="text" value="1024"/>
Private key pass-phrase (optional)	<input type="password" value="....."/>

Press the "Generate Private Key" button to create new private key.
 Press the "Generate Self-Signed Certificate" button to create self-signed certificate.
 Note that the certificate will use the subject name configured in "Certificate Signing Request" box.
 Important: generation of private key is a lengthy operation during which the device service may be affected.

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 4-8: Uploading the Certificate Obtained from the Certification Authority

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase (optional)

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

No file chosen

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

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

No file chosen ←

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 4-9: Certificate Information Example

← TLS Context [#1] > Certificate Information

PRIVATE KEY

Key size: 2048 bits

Status: OK

CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number:
1f:dc:b2:f1:fb:ee:fa:db:c1:90:0e:4e:aa:0f:51:49

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=IL, O=Domain The Net Technologies Ltd, CN=Domain The Net Technologies Ltd CA for SSL R2

Validity

Not Before: May 15 13:03:31 2019 GMT

Not After: May 14 13:03:31 2020 GMT

Subject: CN= sbc1.hybridvoice.org

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

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 4-10: Example of Configured Trusted Root Certificates

INDEX	SUBJECT	ISSUER	EXPIRES
0	DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031
1	RapidSSL RSA CA 2018	DigiCert Global Root CA	11/06/2027

4.3.4 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.

4.3.5 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'.

4.4 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the SIP Trunk 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 4-3: 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-VoIP.ms (arbitrary name)		WAN_IF	10000	100 (media sessions assigned with port range)
1	MR-Teams (arbitrary name)	Up	WAN_IF	7000	100 (media sessions assigned with port range)

The configured Media Realms are shown in the figure below:

Figure 4-11: Configured Media Realms in Media Realm Table

INDEX	NAME	IPv4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
0	MR-VoIP.ms	WAN_IF	10000	100	10999	No
1	MR-Teams	WAN_IF	7000	100	7999	No

4.5 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 4-4: 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	VoIP.ms (arbitrary name)	WAN_IF	SBC	5060 (according to VoIP.ms account configuration)	5060 (according to VoIP.ms account configuration)	5081 (according to VoIP.ms account configuration)	Disable (leave default value)	500 (leave default value)	MR-VoIP.ms	default
1	Teams (arbitrary name)	WAN_IF	SBC	0 (Phone System does not use UDP or TCP for SIP signaling)	0	5061 (as configured in the Office 365)	Enable	0 (Recommended to prevent DoS attacks)	MR-Teams	Teams

The configured SIP Interfaces are shown in the figure below:

Figure 4-12: Configured SIP Interfaces in SIP Interface Table

SIP Interfaces (2)

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

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATION PROTOCOL	MEDIA REALM
0	VoIP.ms	DefaultSRD	WAN_IF	SBC	5060	5060	5081	No encapsulat	MR-VoIP.ms
1	Teams	DefaultSRD	WAN_IF	SBC	0	0	5061	No encapsulat	MR-Teams

4.6 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:

- VoIP.ms SIP Trunk
- 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 4-5: 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	VoIP.ms (arbitrary name)	VoIP.ms	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 4-13: Configured Proxy Sets in Proxy Sets Table

Proxy Sets (3)

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

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#)	--	VoIP.ms	60		Disable
1	VoIP.ms	DefaultSRD (#)	--	VoIP.ms	60		Disable
2	Teams	DefaultSRD (#)	--	Teams	60		Enable

4.6.1 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 **VoIP.ms**, 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 4-14: Configuring Proxy Address for SIP Trunk

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

Table 4-6: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	montreal1.voip.ms:5060 (VoIP.ms POP FQDN and port)	UDP	0	0

- 4. Click **Apply**.



Note: The Transport Type can be configured as UDP or TCP or TLS, according to VoIP.ms account configuration.

➤ **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 4-15: 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 4-7: 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 **Apply**.

4.7 Configure Coders

This section describes how to configure coders (termed *Coder Group*). As Microsoft Teams Direct Routing supports the SILK and OPUS coders while the network connection to VoIP.ms SIP Trunk may restrict operation with a dedicated coders list, you need to add a Coder Group with the supported coders for each leg, the Microsoft Teams Direct Routing and the VoIP.ms SIP Trunk.

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_1
Coder Name	<ul style="list-style-type: none"> ▪ SILK-NB ▪ SILK-WB ▪ G.711 A-law ▪ G.711 U-law ▪ G.729

Figure 4-16: Configuring Coder Group for Microsoft Teams Direct Routing

Coder Groups

Coder Group Name: 1 : AudioCodersGroups_1 Delete Group

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
SILK-NB	20	8	103	N/A	
SILK-WB	20	16	104	N/A	
G.711A-law	20	64	8	Disabled	
G.711U-law	20	64	0	Disabled	
G.729	20	8	18	Disabled	

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

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the VoIP.ms SIP Trunk uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the VoIP.ms SIP Trunk in the next step.

➤ **To set a preferred coder for the VoIP.ms SIP Trunk:**

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New** and configure a name for the Allowed Audio Coders Group for VoIP.ms SIP Trunk.

Figure 4-17: Configuring Allowed Coders Group for VoIP.ms SIP Trunk

Allowed Audio Coders Groups [ITSP Allowed Coders]

GENERAL

Index: 0

Name: ITSP Allowed Coders

3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Index	Coder
0	G.711 U-law
1	G.729

Figure 4-18: Configuring Allowed Coders for VoIP.ms SIP Trunk

Allowed Audio Coders Groups [#0] > Allowed Audio Coders (2)

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

INDEX	CODER	USER-DEFINED CODER
0	G.711 U-law	
1	G.729	

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

Figure 4-19: SBC Preferences Mode

Media Settings

GENERAL		ROBUSTNESS	
NAT Traversal	Disable NAT	New RTP Stream Packets	3
Enable Continuity Tones	Disable	New RTCP Stream Packets	3
Inbound Media Latch Mode	Dynamic	New SRTP Stream Packets	3
Number of Media Channels	0	New SRTCP Stream Packets	3
Enforce Media Order	Disable	Timeout To Relatch RTP (msec)	200
SDP Session Owner	AudiocodesGW	Timeout To Relatch SRTP (msec)	200
		Timeout To Relatch Silence (msec)	10000
		Timeout To Relatch RTCP (msec)	10000
SBC SETTINGS			
Preferences Mode	<input checked="" type="radio"/> Include Extensions <input type="radio"/> Disable		
Enforce Media Order	Disable		
GATEWAY SETTINGS			
Enable Early Media	Disable		
Multiple Packetization Time Format	None		

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

4.8 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:

- VoIP.ms SIP trunk – to operate in non-secure mode using RTP or secure mode using SRTP
- Microsoft Teams Direct Routing – to operate in secure mode using SRTP

➤ **To configure an IP Profile for the VoIP.ms SIP Trunk:**

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	VoIP.ms
Media Security	
SBC Media Security Mode	Not Secured or Secured (according to connectivity mode)
SBC Media	
Allowed Audio Coders	ITSP Allowed Coders
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 4-20: Configuring IP Profile for VoIP.ms SIP Trunk

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_1
RTCP Mode	Generate Always (required, as some ITSPs do not send RTCP packets during while in Hold mode, but Microsoft expected to them)

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 4-21: Configuring IP Profile for Microsoft Teams Direct Routing

The screenshot shows the configuration interface for an IP Profile. It is organized into three main sections: GENERAL, MEDIA SECURITY, and SBC SIGNALING. The GENERAL section contains fields for Index (2), Name (Teams), and Created by Routing Server (No). The MEDIA SECURITY section includes SBC Media Security Mode (Secured), Gateway Media Security Mode (Preferable), Symmetric MKI (Disable), MKI Size (0), SBC Enforce MKI Size (Don't enforce), SBC Media Security Method (SDS), and Reset SRTP Upon Re-key (Disable). The SBC SIGNALING section contains a list of signaling options, each with a dropdown menu: PRACK Mode (Transparent), P-Asserted-Identity Header Mode (As Is), Diversion Header Mode (As Is), History-Info Header Mode (As Is), Session Expires Mode (Transparent), Remote UPDATE Support (Not Supported), Remote re-INVITE (Supported only with SDP), Remote Delayed Offer Support (Not Supported), MSRP re-INVITE/UPDATE (Supported), MSRP Offer Setup Role (ActPass), MSRP Empty Message Format (Default), and Remote Representation Mode (According to Operation Mode). At the bottom of the window, there are 'Cancel' and 'APPLY' buttons.

3. Click **Apply**.

4.9 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:

- VoIP.ms SIP Trunk
- Teams Direct Routing

➤ 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 VoIP.ms SIP Trunk:

Parameter	Value
Index	1
Name	VoIP.ms
Type	Server
Proxy Set	VoIP.ms
IP Profile	VoIP.ms
Media Realm	MR-VoIP.ms
SIP Group Name	<VoIP.ms POP server> (For example, montreal1.voip.ms)

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	MR-Teams
SIP Group Name	<VoIP.ms POP server> (For example, montreal1.voip.ms)
Classify By Proxy Set	Disable
Local Host Name	<FQDN name of your SBC in the Microsoft Teams tenant> (For example, sbc1.customers.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 4-22: 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 MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_IPC	Default	Server	Not Config	ProxySet_0	--	--		Disable	-1	-1
1	VoIP.ms	Default	Server	Not Config	VoIP.ms	VoIP.ms	MR-VoIP.m	montreal1.	Enable	-1	4
2	Teams	Default	Server	Not Config	Teams	Teams	MR-Teams	montreal1.	Disable	1	-1

4.10 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 4-23: Configuring SRTP

Media Security

GENERAL

Media Security → • Enable ▼

Media Security Behavior Preferable ▼

Offered SRTP Cipher Suites All ▼

Aria Protocol Support Disable ▼

MASTER KEY IDENTIFIER

Master Key Identifier (MKI) Size 0

Symmetric MKI Disable ▼

3. Click **Apply**.

4.11 Configuring Message Condition Rules

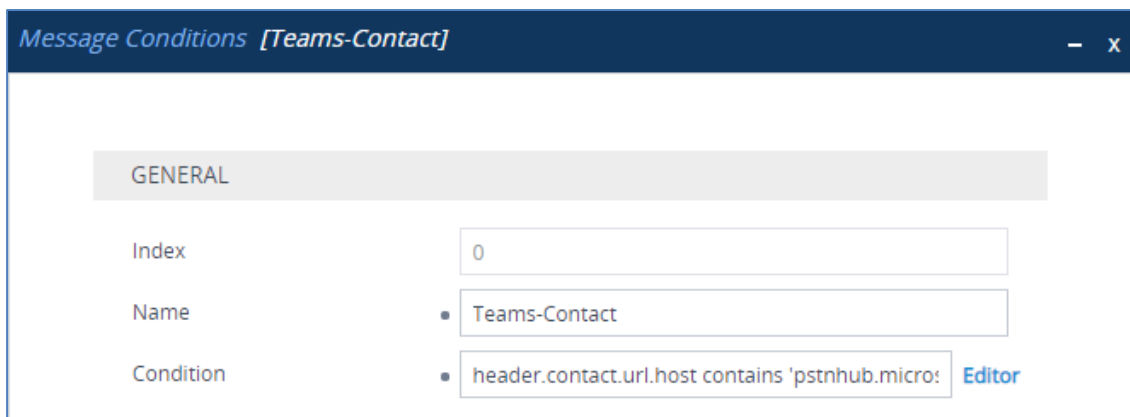
This section describes how to configure the Message Condition Rules. A Message Condition defines special conditions (pre-requisites) for incoming SIP messages. These rules can be used as additional matching criteria for the IP-to-IP routing rules in the IP-to-IP Routing table. The following condition 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 4-24: Configuring Condition Table



3. Click **Apply**.

4.12 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 4-25: Configuring Classification Rule

The screenshot shows a configuration window titled "Classification [Teams]". At the top, there is a dropdown for "SRD" set to "#0 [DefaultSRD]". The window is divided into two main sections: "MATCH" and "ACTION".

MATCH Section:

- Index: 0
- Name: Teams
- Source SIP Interface: #2 [Teams]
- Source IP Address: 52.114.*.*
- Source Transport Type: Any
- Source Port: 0
- Source Username Pattern: *
- Source Host: *
- Destination Username Pattern: *
- Destination Host: sbc.ACeducation.info
- Message Condition: #0 [Teams-Contact]

ACTION Section:

- Action Type: Allow
- Destination Routing Policy: ..
- IP Group Selection: Source IP Group
- Source IP Group: #2 [Teams]
- IP Group Tag Name: default
- IP Profile: ..

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

3. Click **Apply**.

4.13 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 VoIP.ms SIP Trunk:

- 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 VoIP.ms SIP Trunk
- Calls from VoIP.ms SIP Trunk 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 4-8: 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 VoIP.ms (arbitrary name)	Teams				IP Group	VoIP.ms	
3	VoIP.ms to Teams (arbitrary name)	VoIP.ms				IP Group	Teams	

The configured routing rules are shown in the figure below:

Figure 4-26: 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	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATIC USERNAME PATTERN	DESTINATIC TYPE	DESTINATIC IP GROUP	DESTINATIC SIP INTERFACE	DESTINATIC ADDRESS
0	Terminate C	Default_SBC	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	Refer from T	Default_SBC	Route Row	Any	All	*	*	Request URI	Teams	--	
2	Teams to Vo	Default_SBC	Route Row	Teams	All	*	*	IP Group	VoIP.ms	--	
3	VoIP.ms to T	Default_SBC	Route Row	VoIP.ms	All	*	*	IP Group	Teams	--	



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

4.14 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 must add rules to allow traffic from these entities.

4.15 Configure Number Manipulation Rules

This section describes how to configure IP-to-IP number 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 4.9 on page 32) 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 add the "+" (plus sign) to the destination number (if it not exists) for calls from the VoIP.ms SIP Trunk IP Group to the Teams Direct Routing IP Group for any destination username pattern.

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

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

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between Teams Direct Routing IP Group and VoIP.ms SIP Trunk IP Group:

Figure 4-27: Example of Configured IP-to-IP Outbound Manipulation Rules

INDEX	NAME	ROUTING POLICY	ADDITIONAL MANIPULATION	SOURCE IP GROUP	DESTINATION IP GROUP	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	MANIPULATE ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	Dst To Teams	Default_SBCR	No	Any	Teams	*	XXXXXXXXXX#	Destination U	0	0	255	+1	
1	Src To Teams	Default_SBCR	No	Any	Teams	XXXXXXXXXX#	*	Source URI	0	0	255	+1	
2	Src to Teams	Default_SBCR	No	Any	Teams	*	*	Source URI	0	0	255	+	

Rule Index	Description
0	Calls to Microsoft Teams IP Group with the 10 digits destination number (national format), add "+1" to the prefix of the destination number.
1	Calls to Microsoft Teams IP Group with the 10 digits source number (national format), add "+1" to the prefix of the source number.
2	Calls to Microsoft Teams IP Group with any source number (international format), add "+" to the prefix of the source number.

4.16 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 1) for Teams. This rule applies to messages received from the Teams IP Group. This removes the SIP P-Asserted-Identity Header.

Parameter	Value
Index	0
Name	Remove PAI
Manipulation Set ID	1
Action Subject	Header.P-Asserted-Identity
Action Type	Remove

Figure 4-28: Configuring SIP Message Manipulation Rule 0 (for Teams)

The screenshot shows a configuration window titled "Message Manipulations [Remove PAI]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
 - Index: 0
 - Name: Remove PAI
 - Manipulation Set ID: 1
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: Header.P-Asserted-Identity
 - Action Type: Remove
 - Action Value: (empty field)
- MATCH:**
 - Message Type: Any
 - Condition: (empty field)

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

- Configure another manipulation rule (Manipulation Set 4) for VoIP.ms SIP Trunk. This rule applies to messages sent to the VoIP.ms SIP Trunk IP. This removes the SIP Privacy Header in all messages, with the exception of the call with the presentation restriction.

Parameter	Value
Index	1
Name	Remove Privacy Header
Manipulation Set ID	4
Condition	Header.Privacy exists And Header.From.URL !contains 'anonymous'
Action Subject	Header.Privacy
Action Type	Remove

Figure 4-29: Configuring SIP Message Manipulation Rule 1 (for VoIP.ms SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Remove Privacy Header]". It is organized into three main sections: GENERAL, ACTION, and MATCH. Each section contains several input fields and dropdown menus, many with "Editor" links next to them. At the bottom of the window, there are "Cancel" and "APPLY" buttons.

Section	Field	Value
GENERAL	Index	1
	Name	Remove Privacy Header
	Manipulation Set ID	4
	Row Role	Use Current Condition
ACTION	Action Subject	Header.Privacy
	Action Type	Remove
	Action Value	
MATCH	Message Type	Any
	Condition	Header.Privacy exists And Header.Fron

- Configure another manipulation rule (Manipulation Set 1) for Teams. This rule applies to messages received from the Teams IP Group. This removes the SIP History-Info.1 Header in all messages.

Parameter	Value
Index	2
Name	Remove History-Info.1
Manipulation Set ID	1
Action Subject	Header.History-Info.1
Action Type	Remove

Figure 4-30: Configuring SIP Message Manipulation Rule 2 (for Teams)

Message Manipulations [Remove History-Info.1]
- x

<div style="background-color: #f2f2f2; padding: 2px; margin-bottom: 5px;">GENERAL</div> <p>Index <input style="width: 100%;" type="text" value="2"/></p> <p>Name <input style="width: 100%;" type="text" value="Remove History-Info.1"/></p> <p>Manipulation Set ID <input style="width: 100%;" type="text" value="1"/></p> <p>Row Role <input style="width: 100%;" type="text" value="Use Current Condition"/></p>	<div style="background-color: #f2f2f2; padding: 2px; margin-bottom: 5px;">ACTION</div> <p>Action Subject <input style="width: 100%;" type="text" value="Header.History-Info.1"/> Editor</p> <p>Action Type <input style="width: 100%;" type="text" value="Remove"/></p> <p>Action Value <input style="width: 100%;" type="text"/> Editor</p>
<div style="background-color: #f2f2f2; padding: 2px; margin-bottom: 5px;">MATCH</div> <p>Message Type <input style="width: 100%;" type="text"/> Editor</p> <p>Condition <input style="width: 100%;" type="text"/> Editor</p>	

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

- Configure another manipulation rule (Manipulation Set 4) for the VoIP.ms SIP Trunk. This rule applies to messages sent to the VoIP.ms SIP Trunk IP Group in a Call Forward scenario. This adds the SIP Diversion Header with the value of the SIP History-Info Header, if it exists.

Parameter	Value
Index	3
Name	Call Forward
Manipulation Set ID	4
Condition	Header.History-Info exists
Action Subject	Header.Diversion
Action Type	Add
Action Value	Header.History-Info

Figure 4-31: Configuring SIP Message Manipulation Rule 3 (for VoIP.ms SIP Trunk)

The screenshot shows the configuration interface for a SIP message manipulation rule. The window title is "Message Manipulations [Call Forward]".

- GENERAL Section:**
 - Index: 3
 - Name: Call Forward
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- ACTION Section:**
 - Action Subject: Header.Diversion
 - Action Type: Add
 - Action Value: Header.History-Info
- MATCH Section:**
 - Message Type: (empty)
 - Condition: Header.History-Info exists

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

- Configure a new manipulation rule (Manipulation Set 4) for the VoIP.ms SIP Trunk. This rule applies to messages sent to the VoIP.ms SIP Trunk IP Group in a Call Forward scenario. This removes the '+1' from the user part of the SIP Diversion.

Parameter	Value
Index	4
Name	Call Forward
Manipulation Set ID	4
Action Subject	Header.Diversion.URL.User
Action Type	Remove Prefix
Action Value	'+1'

Figure 4-32: Configuring SIP Message Manipulation Rule 4 (for VoIP.ms SIP Trunk)

The screenshot shows the configuration interface for a SIP Message Manipulation Rule. The window title is "Message Manipulations: [Call Forward]".

GENERAL

- Index: 4
- Name: Call Forward
- Manipulation Set ID: 4
- Row Role: Use Current Condition

ACTION

- Action Subject: Header.Diversion.URL.User
- Action Type: Remove Prefix
- Action Value: '+1'

MATCH

- Message Type: (empty)
- Condition: (empty)

Buttons: Cancel, APPLY

7. Configure a new manipulation rule (Manipulation Set 4) for the VoIP.ms SIP Trunk. This rule applies to messages sent to the VoIP.ms SIP Trunk IP Group in a Call Forward scenario. This replaces the host name of the SIP Diversion with the value from SIP To Header.

Parameter	Value
Index	5
Name	Call Forward
Manipulation Set ID	4
Action Subject	Header.Diversion.URL.Host.Name
Action Type	Modify
Action Value	Header.To.URL.Host.Name

Figure 4-33: Configuring SIP Message Manipulation Rule 5 (for VoIP.ms SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Call Forward]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
 - Index: 5
 - Name: Call Forward
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: Header.Diversion.URL.Host.Name
 - Action Type: Modify
 - Action Value: Header.To.URL.Host.Name
- MATCH:**
 - Message Type: (empty field)
 - Condition: (empty field)

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

8. Configure another manipulation rule (Manipulation Set 4) for the VoIP.ms SIP Trunk. This rule applies to messages sent to the VoIP.ms SIP Trunk IP Group in a Call Forward scenario. This removes the SIP History-Info Header in all messages.

Parameter	Value
Index	6
Name	Call Forward
Manipulation Set ID	4
Action Subject	Header.History-Info
Action Type	Remove

Figure 4-34: Configuring SIP Message Manipulation Rule 6 (for VoIP.ms SIP Trunk)

The screenshot shows a configuration window titled "Message Manipulations [Call Forward]". It is divided into three main sections: GENERAL, ACTION, and MATCH.

- GENERAL:**
 - Index: 6
 - Name: Call Forward
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- ACTION:**
 - Action Subject: Header.History-Info
 - Action Type: Remove
 - Action Value: (empty)
- MATCH:**
 - Message Type: (empty)
 - Condition: (empty)

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

9. Configure another manipulation rule (Manipulation Set 4) for the VoIP.ms SIP Trunk. This rule applies to messages sent to the VoIP.ms SIP Trunk IP Group in a Call Transfer scenario. This replaces the host name of the SIP Referred-By Header, with the value from the SIP To Header.

Parameter	Value
Index	7
Name	Call Transfer
Manipulation Set ID	4
Condition	Header.Referred-By exists
Action Subject	Header.Referred-By.URL.Host.Name
Action Type	Modify
Action Value	Header.To.URL.Host.Name

Figure 4-35: Configuring SIP Message Manipulation Rule 7 (for VoIP.ms SIP Trunk)

The screenshot shows the configuration interface for a SIP message manipulation rule. It is titled "Message Manipulations [Call Transfer]".

- GENERAL Section:**
 - Index: 7
 - Name: Call Transfer
 - Manipulation Set ID: 4
 - Row Role: Use Current Condition
- MATCH Section:**
 - Message Type: (empty)
 - Condition: Header.Referred-By exists
- ACTION Section:**
 - Action Subject: Header.Referred-By.URL.Host.Name
 - Action Type: Modify
 - Action Value: Header.To.URL.Host.Name

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

- Configure another manipulation rule (Manipulation Set 4) for VoIP.ms SIP Trunk. This rule applies to messages sent to the VoIP.ms SIP Trunk IP Group in a Call Transfer scenario. This removes the '+1' from the user part of the SIP Referred-By Header.

Parameter	Value
Index	8
Name	Call Transfer
Manipulation Set ID	4
Condition	Header.Referred-By exists
Action Subject	Header.Referred-By.URL.User
Action Type	Remove Prefix
Action Value	'+1'

Figure 4-36: Configuring SIP Message Manipulation Rule 8 (for VoIP.ms SIP Trunk)

Figure 4-37: 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 PAI	1	Any		Header.P-Asserted-Id	Remove		Use Current Condition
1	Remove Privacy Head	4	Any	Header.Privacy exists	Header.Privacy	Remove		Use Current Condition
2	Remove History-Info.	1			Header.History-Info.1	Remove		Use Current Condition
3	Call Forward	4		Header.History-Info €	Header.Diversion	Add	Header.History-Info	Use Current Condition
4	Call Forward	4			Header.Diversion.UR	Remove Prefix	'+1'	Use Current Condition
5	Call Forward	4			Header.Diversion.UR	Modify	Header.To.URL.Host	Use Current Condition
6	Call Forward	4			Header.History-Info	Remove		Use Current Condition
7	Call Transfer	4		Header.Referred-By €	Header.Referred-By.t	Modify	Header.To.URL.Host	Use Current Condition
8	Call Transfer	4		Header.Referred-By €	Header.Referred-By.t	Remove Prefix	'+1'	Use Current Condition

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set IDs (Manipulation Set IDs 1 and 4) and which are executed for messages sent to and from the VoIP.ms SIP Trunk IP Group as well as the Teams Direct Routing IP Group. These rules are specifically required to enable proper interworking between VoIP.ms SIP Trunk 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. This removes the SIP P-Asserted-Identity Header.	Microsoft Office 365 may be configured to send a PAI header. We recommend doing this in the SBC, for better interoperability.
1	This rule applies to messages sent to the VoIP.ms SIP Trunk IP. This remove the SIP Privacy Header in all messages, except of call with presentation restriction.	The same as in previous rule.
2	This rule applies to messages received from the Teams IP Group. This remove the SIP History-Info.1 Header in all messages.	
3	This rule applies to messages <u>sent</u> to the nexVortex SIP Trunk IP Group in a Call Forward scenario. This add the SIP Diversion Header with the value of the SIP History-Info Header, if it exists.	For Call Forward scenarios, the VoIP.ms SIP Trunk requires the SIP Diversion Header. To do this, the SIP Diversion Header is added with the value from the SIP History-Info Header and the SIP History-Info Header is removed.
4	This rule applies to messages sent to the nexVortex SIP Trunk IP Group in a Call Forward scenario. This removes the '+1' from the user part of the SIP Diversion.	
5	This rule applies to messages sent to the nexVortex SIP Trunk IP Group in a Call Forward scenario. This replaces the Host Name of the SIP Diversion with the value from SIP To Header.	
6	This rule applies to messages sent to the nexVortex SIP Trunk IP Group in a Call Forward scenario. This removes the SIP History-Info Header in all messages.	
7	This rule applies to messages sent to the nexVortex SIP Trunk IP Group in a Call Transfer scenario. This replaces the host name of the SIP Referred-By Header with the value from the SIP To Header.	For Call Transfers initiated by Teams Direct Routing, the VoIP.ms SIP Trunk needs to replace the Host Name of the SIP Referred-By Header with the value from the SIP To Header.
8	This rule applies to messages sent to the VoIP.ms SIP Trunk IP Group in a Call Transfer scenario. This removes the '+1' from the user part of the SIP Referred-By Header.	

11. Assign Manipulation Set IDs 1 and 2 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 **1**.

Figure 4-38: Assigning Manipulation Set to the Teams Direct Routing IP Group

The screenshot shows the 'IP Groups [Teams]' configuration window. At the top, there is an SRD dropdown menu set to '#0 [DefaultSRD]'. The window is divided into several sections: 'GENERAL', 'QUALITY OF EXPERIENCE', and 'MESSAGE MANIPULATION'. In the 'GENERAL' section, fields include Index (2), Name (Teams), Topology Location (Up), Type (Server), Proxy Set (#2 [Teams]), IP Profile (#2 [Teams]), Media Realm (#1 [MR-Teams]), Internal Media Realm (--), Contact User, and SIP Group Name. In the 'QUALITY OF EXPERIENCE' section, there are QoE Profile and Bandwidth Profile dropdowns. In the 'MESSAGE MANIPULATION' section, the 'Inbound Message Manipulation Set' is set to '1' (highlighted with a red box), 'Outbound Message Manipulation Set' is set to '-1', and 'Proxy Keep-Alive using IP Group settings' is set to 'Enable'. At the bottom, there are 'Cancel' and 'APPLY' buttons.

- d. Click **Apply**.

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

Figure 4-39: Assigning Manipulation Set 4 to the VoIP.ms SIP Trunk IP Group

The screenshot shows the configuration interface for an IP Group named 'VoIP.ms'. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. Below this are two main sections: 'GENERAL' and 'QUALITY OF EXPERIENCE'. The 'GENERAL' section includes fields for Index (1), Name (VoIP.ms), Topology Location (Down), Type (Server), Proxy Set (#1 [VoIP.ms]), IP Profile (#1 [VoIP.ms]), Media Realm (#0 [MR-VoIP.ms]), Internal Media Realm (--), Contact User, and SIP Group Name. The 'QUALITY OF EXPERIENCE' section includes QoE Profile and Bandwidth Profile, both set to '--'. Below these is the 'MESSAGE MANIPULATION' section, which contains 'Inbound Message Manipulation Set' (-1), 'Outbound Message Manipulation Set' (4, highlighted with a red box), 'Message Manipulation User-Defined String 1', 'Message Manipulation User-Defined String 2', and 'Proxy Keep-Alive using IP Group settings' (Disable). At the bottom, there are 'Cancel' and 'APPLY' buttons.

- d. Click **Apply**.

4.17 Configure Registration Accounts (optional)

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the VoIP.ms SIP Trunk on behalf of Teams Direct Routing.



Note: This section is only relevant when the VoIP.ms account is configured with username/password authentication. This section is not relevant if you implement Static IP Authentication.

In the interoperability test topology, the Served IP Group is Teams Direct Routing IP Group and the Serving IP Group is VoIP.ms SIP Trunk IP Group.

➤ **To configure a registration account:**

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New**.
3. Configure the account according to the provided information from , for example:

Parameter	Value
Application Type	SBC
Served IP Group	Teams
Serving IP Group	VoIP.ms
Host Name	VoIP.ms POP Server
Contact User	1234567890 (account username)
Register	Regular
Username	As configured in the VoIP.ms account
Password	As configured in the VoIP.ms account

Figure 4-40: Configuring a SIP Registration Account

4. Click **Apply**.

4.18 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

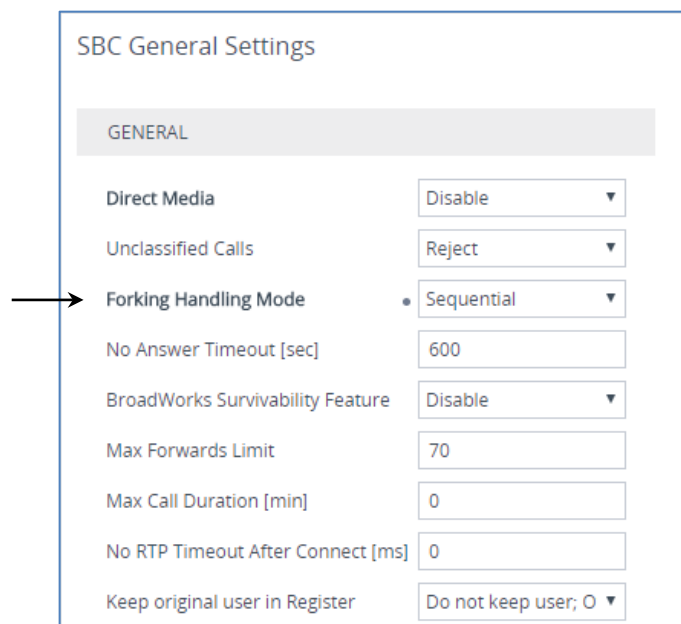
4.18.1 Configure Call Forking Mode

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 4-41: Configuring Forking Mode



The screenshot shows the 'SBC General Settings' configuration page. A grey header bar at the top contains the word 'GENERAL'. Below this, several settings are listed in a table-like format. The 'Forking Handling Mode' setting is highlighted with a blue arrow pointing to its dropdown menu, which is currently set to 'Sequential'. Other settings include 'Direct Media' (Disable), 'Unclassified Calls' (Reject), 'No Answer Timeout [sec]' (600), 'BroadWorks Survivability Feature' (Disable), 'Max Forwards Limit' (70), 'Max Call Duration [min]' (0), 'No RTP Timeout After Connect [ms]' (0), and 'Keep original user in Register' (Do not keep user; 0).

SBC General Settings	
GENERAL	
Direct Media	Disable ▼
Unclassified Calls	Reject ▼
Forking Handling Mode	Sequential ▼
No Answer Timeout [sec]	600
BroadWorks Survivability Feature	Disable ▼
Max Forwards Limit	70
Max Call Duration [min]	0
No RTP Timeout After Connect [ms]	0
Keep original user in Register	Do not keep user; 0 ▼

3. Click **Apply**.

4.18.2 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:

SBC Performance Profile

• Optimized for transcoding ▼ ⚡

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

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 **
;*****

[SYSTEM Params]

SyslogServerIP = 10.10.10.10
EnableSyslog = 1
NTPServerUTCOffset = 7200
TLSPkeySize = 2048
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.15.28.1'
SBCWizardFilename = 'templates4.zip'

[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'
SBCPREFERENCESMODE = 1
MEDIACDRREPORTLEVEL = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[SNMP Params]

[ 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, 10.15.77.77, 16, 10.15.0.1, "LAN_IF",
10.15.27.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.157, 24, 195.189.192.129, "WAN_IF",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]

[ WebUsers ]

FORMAT Index = Username, Password, Status, PwAgeInterval, SessionLimit,
CliSessionLimit, SessionTimeout, BlockTime, UserLevel, PwNonce,
SSHPublicKey;
WebUsers 0 = "Admin",
"$1$bgtDFkgQREJNFRNJHUhDGRtPTuPju+bhteClubG4vby9t7fy9fbloqfyoKmt+KP5/qz9m
ZSTlpyUkpDNzMudz54=", 1, 0, 5, -1, 15, 60, 200,
"e4064f90b5b26631d46fbcdb79f2b7a0", ".fc";
WebUsers 1 = "User",
"$1$Cj46OmhtN3ElJiolcSQnfXh4Ii5+Jn4ZRBQRHR0fHx4bTB9ITE8aVgRQVQUGAAEPXVxCD
w0GWSEgIHN0dHB2LHE=", 1, 0, 5, -1, 15, 60, 50,
"c26a27dd91a886b99de5e81b9a736232", "";

[ \WebUsers ]

[ TLSContexts ]

FORMAT Index = Name, TLSVersion, DTLSVersion, ServerCipherString,
ClientCipherString, RequireStrictCert, TlsRenegotiation, OcspEnable,
OcspServerPrimary, OcspServerSecondary, OcspServerPort,
OcspDefaultResponse, DHKeySize;
TLSContexts 0 = "default", 0, 0, "DEFAULT", "DEFAULT", 0, 1, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;
TLSContexts 1 = "Teams", 4, 0, "RC4:AES128", "DEFAULT", 0, 1, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;

[ \TLSContexts ]

[ AudioCodersGroups ]

FORMAT Index = Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";
AudioCodersGroups 1 = "AudioCodersGroups_1";

[ \AudioCodersGroups ]

[ AllowedAudioCodersGroups ]
    
```

```

FORMAT Index = Name;
AllowedAudioCodersGroups 0 = "ITSP Allowed Coders";

[ \AllowedAudioCodersGroups ]

[ 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,
SBCSendEchoMultipleDTMFMethods, SBCAssertIdentity,
AMDSensitivityParameterSuit, AMDSensitivityLevel, AMDMaxGreetingTime,
AMDMaxPostSilenceGreetingTime, SBCDiversionsMode, 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,
SBCRemoteCryptoLifetimeInSDP, 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 = "VoIP.ms", 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,
"", "ITSP Allowed Coders", "", 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, 1, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0,
0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, -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_1", 0, 0, "", "", "", 0, 1, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, "", 0, 0, 1, 1, 0, 0, 1, 0, 3, 2, 1, 0, 1, 0, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 1, 0, 0, 3, 1, 0, 0, 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-VoIP.ms", "WAN_IF", "", "", "", 10000, 100, 10999,
0, 0, 0, "", "", 0;
CpMediaRealm 1 = "MR-Teams", "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 = "VoIP.ms", "WAN_IF", "", 2, 5060, 5060, 0, 0, "", 0,
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MR-VoIP.ms", 0, -1, -1,
-1, 0, 0, "", "", -1;
SIPInterface 1 = "Teams", "WAN_IF", "", 2, 0, 0, 5061, 0, "", 0,
"DefaultSRD", "", "Teams", -1, 1, 0, -1, 0, "MR-Teams", 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", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "VoIP.ms", "", "", 1, 1, 10, -1;
ProxySet 1 = "VoIP.ms", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"VoIP.ms", "", "", 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,
InternalMediaRealm, ClassifyByProxySet, ProfileName, MaxNumOfRegUsers,
InboundManSet, OutboundManSet, RegistrationMode, AuthenticationMode,
MethodList, SBCServerAuthType, OAuthHTTPService, EnableSBCCClientForking,
SourceUriInput, DestUriInput, ContactName, Username, Password, UIFormat,
QOEProfile, BWProfile, AlwaysUseSourceAddr, MsgManUserDef1,
MsgManUserDef2, SIPConnect, SBCPSAPMode, DTLContext,
CreatedByRoutingServer, UsedByRoutingServer, SBCOperationMode,
SBCRouteUsingRequestURIPort, SBCKeepOriginalCallID, TopologyLocation,
SBCDialPlanName, CallSetupRulesSetId, Tags, SBCUserStickiness,
UserUDPPortAssignment, AdmissionProfile, ProxyKeepAliveUsingIPG,
SBCAltRouteReasonsSetName, TeamsMediaOptimization;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", "", 0, "", -1, -1, -1, 0, 0, "", -1, "", 0, -1, -1, "", "",
"$1$gQ==", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "",
-1, "", 0, 0, "", 0, "", 0;
IPGroup 1 = 0, "VoIP.ms", "VoIP.ms", "montreal1.voip.ms", "", -1, 0,
"DefaultSRD", "MR-VoIP.ms", "", 1, "VoIP.ms", -1, -1, 4, 0, 0, "", -1,
"", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", 0, "", "", 0, 0, "default",
0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 0, "", 0;
IPGroup 2 = 0, "Teams", "Teams", "montreal1.voip.ms", "", -1, 0,
"DefaultSRD", "MR-Teams", "", 0, "Teams", -1, 1, -1, 0, 0, "", -1, "", 0,
-1, -1, "int-sbc2.audctrunk.aceducation.info", "", "$1$gQ==", 0, "", "",
1, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 1, "", -1, "", 0, 0, "", 1,
"", 0;

[ \IPGroup ]

```

```

[ ProxyIp ]

FORMAT Index = ProxySetId, ProxyIpIndex, IpAddress, TransportType,
Priority, Weight;
ProxyIp 0 = "1", 0, "montreall.voip.ms: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 ]

[ Account ]

FORMAT Index = AccountName, ServedTrunkGroup, ServedIPGroupName,
ServingIPGroupName, Username, Password, HostName, ContactUser, Register,
RegistrarStickiness, RegistrarSearchMode, RegEventPackageSubscription,
ApplicationType, RegByServedIPG, UDPPortAssignment,
ReRegisterOnInviteFailure;
Account 0 = "", -1, "Teams", "VoIP.ms", "user", "password",
"montreall.voip.ms", "user", 1, 0, 0, 0, 2, 0, 0, 0;

[ \Account ]

[ 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 VoIP.ms", "Default_SBCRoutingPolicy", "Teams",
"*,*',*',*', 0, "", "Any", 0, -1, 0, "VoIP.ms", "", "", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 3 = "VoIP.ms to Teams", "Default_SBCRoutingPolicy",
"VoIP.ms", "*", "*", "*", "*", 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, "*", "*", "*", "int-
sbc2.audctrunk.aceducation.info", 1, "Teams", "", "", 0, "default";

[ \Classification ]

[ IPInboundManipulation ]

FORMAT Index = ManipulationName, RoutingPolicyName,
IsAdditionalManipulation, ManipulationPurpose, SrcIPGroupName,
SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost, RequestType,
ManipulatedURI, RemoveFromLeft, RemoveFromRight, LeaveFromRight,
Prefix2Add, Suffix2Add;
IPInboundManipulation 0 = "Dst from Teams (national)",
"Default_SBCRoutingPolicy", 0, 0, "Teams", "*", "*", "+1", "*", 0, 1, 2,
0, 255, "", "";
IPInboundManipulation 1 = "Dst from Teams (international)",
"Default_SBCRoutingPolicy", 0, 0, "Teams", "*", "*", "+[2-9]", "*", 0, 1,
1, 0, 255, "00", "";
IPInboundManipulation 2 = "Src from Teams (national)",
"Default_SBCRoutingPolicy", 0, 0, "Teams", "+1", "*", "*", "*", 0, 0, 2,
0, 255, "", "";

[ \IPInboundManipulation ]

[ IPOutboundManipulation ]

FORMAT Index = ManipulationName, RoutingPolicyName,
IsAdditionalManipulation, SrcIPGroupName, DestIPGroupName,
SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost,
CallingNamePrefix, MessageConditionName, RequestType, ReRouteIPGroupName,
Trigger, ManipulatedURI, RemoveFromLeft, RemoveFromRight, LeaveFromRight,
Prefix2Add, Suffix2Add, PrivacyRestrictionMode, DestTags, SrcTags;
IPOutboundManipulation 0 = "Dst from VoIP.ms",
"Default_SBCRoutingPolicy", 0, "VoIP.ms", "Any", "*", "*", "XXXXXXXXXX#",
"*, "*", "", 0, "Any", 0, 1, 0, 0, 255, "+1", "", 0, "", "";
IPOutboundManipulation 1 = "Src from VoIP.ms (national)",
"Default_SBCRoutingPolicy", 0, "VoIP.ms", "Any", "XXXXXXXXXX#", "*", "*",
"*, "*", "", 0, "Any", 0, 0, 0, 255, "+1", "", 0, "", "";
IPOutboundManipulation 2 = "Src from VoIP.ms (international)",
"Default_SBCRoutingPolicy", 0, "VoIP.ms", "Any", "*", "*", "*", "*", "*",
"*, 0, "Any", 0, 0, 0, 255, "+", "", 0, "", "";

[ \IPOutboundManipulation ]

[ MessageManipulations ]

FORMAT Index = ManipulationName, ManSetID, MessageType, Condition,
ActionSubject, ActionType, ActionValue, RowRole;
MessageManipulations 0 = "Remove PAI", 1, "Any", "", "Header.P-Asserted-
Identity", 1, "", 0;

```

```

MessageManipulations 1 = "Remove Privacy Header", 4, "Any",
"Header.Privacy exists And Header.From.URL !contains 'anonymous'",
"Header.Privacy", 1, "", 0;
MessageManipulations 2 = "Remove History-Info.1", 1, "", "",
"Header.History-Info.1", 1, "", 0;
MessageManipulations 3 = "Call Forward", 4, "", "Header.History-Info
exists", "Header.Diversion", 0, "Header.History-Info", 0;
MessageManipulations 4 = "Call Forward", 4, "", "",
"Header.Diversion.URL.User", 6, "'+1'", 0;
MessageManipulations 5 = "Call Forward", 4, "", "",
"Header.Diversion.URL.Host.Name", 2, "Header.To.URL.Host.Name", 0;
MessageManipulations 6 = "Call Forward", 4, "", "", "Header.History-
Info", 1, "", 0;
MessageManipulations 7 = "Call Transfer", 4, "", "Header.Referred-By
exists", "Header.Referred-By.URL.Host.Name", 2,
"Header.To.URL.Host.Name", 0;
MessageManipulations 8 = "Call Transfer", 4, "", "Header.Referred-By
exists", "Header.Referred-By.URL.User", 6, "'+1'", 0;

[ \MessageManipulations ]

[ GwRoutingPolicy ]

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

[ \GwRoutingPolicy ]

[ LoggingFilters ]

FORMAT Index = FilterType, Value, LogDestination, CaptureType, Mode;
LoggingFilters 0 = 1, "", 1, 2, 0;

[ \LoggingFilters ]

[ ResourcePriorityNetworkDomains ]

FORMAT Index = Name, Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ \ResourcePriorityNetworkDomains ]

[ 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 ]

[ AllowedAudioCoders ]

FORMAT Index = AllowedAudioCodersGroupName, AllowedAudioCodersIndex,
CoderID, UserDefineCoder;
AllowedAudioCoders 0 = "ITSP Allowed Coders", 0, 2, "";
AllowedAudioCoders 1 = "ITSP Allowed Coders", 1, 3, "";

[ \AllowedAudioCoders ]

[ AudioCoders ]

FORMAT Index = AudioCodersGroupId, AudioCodersIndex, Name, pTime, rate,
PayloadType, Sce, CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_1", 0, 35, 2, 19, 103, 0, "";
AudioCoders 2 = "AudioCodersGroups_1", 1, 36, 2, 43, 104, 0, "";
AudioCoders 3 = "AudioCodersGroups_1", 2, 1, 2, 90, -1, 0, "";
AudioCoders 4 = "AudioCodersGroups_1", 3, 2, 2, 90, -1, 0, "";
AudioCoders 5 = "AudioCodersGroups_1", 4, 3, 2, 19, -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>

©2020 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-29335

