

Microsoft® Teams Direct Routing Enterprise Model and Virgin Media SIP Trunk using AudioCodes Mediant™ SBC

Version 7.2



Microsoft Partner

Gold Communications



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	Virgin Media 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.....	12
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	15
3.3.1	Add New SBC to Direct Routing.....	16
3.3.2	Add Voice Route and PSTN Usage.....	17
3.3.3	Add Voice Routing Policy	19
3.3.4	Enable Online User.....	20
3.3.5	Assigning Online User to the Voice Routing Policy.....	20
4	Configuring AudioCodes SBC	21
4.1	SBC Configuration Concept in Teams Direct Routing Enterprise Model	22
4.2	IP Network Interfaces Configuration	22
4.2.1	Configure VLANs	23
4.2.2	Configure Network Interfaces	23
4.3	SIP TLS Connection Configuration	25
4.3.1	Configure the NTP Server Address	25
4.3.2	Create a TLS Context for Teams Direct Routing.....	26
4.3.3	Configure a Certificate	27
4.3.4	Method of Generating and Installing the Wildcard Certificate	30
4.3.5	Deploy Baltimore Trusted Root Certificate	31
4.4	Configure Media Realms	32
4.5	Configure SIP Signaling Interfaces	33
4.6	Configure Proxy Sets and Proxy Address.....	34
4.6.1	Configure a Proxy Address.....	35
4.7	Configure Coders	39
4.8	Configure IP Profiles.....	42
4.9	Configure SBC Alternative Routing Reasons.....	45
4.10	Configure IP Groups.....	46
4.11	Configure IP Group Sets	48
4.12	Configure SRTP	49
4.13	Configuring Message Condition Rules.....	50
4.14	Configuring Classification Rules	51
4.15	Configure IP-to-IP Call Routing Rules	52

4.16	Configuring Firewall Settings (Optional).....	54
4.17	Configure Number Manipulation Rules	55
4.18	Configure Message Manipulation Rules	56
4.19	Configure Registration Accounts	66
4.20	Miscellaneous Configuration.....	68
4.20.1	Configure Call Forking Mode.....	68
4.20.2	Configure SBC Max Retransmission Time.....	69
4.20.3	Configure Session Expires and Broken Connection Timeouts.....	70
4.20.4	Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only)	71
A	AudioCodes INI File	73
B	Configuring Analog Devices (ATAs) for Fax Support.....	85
B.1	Step 1: Configure the Endpoint Phone Number Table	85
B.2	Step 2: Configure Tel to IP Routing Table	86
B.3	Step 3: Configure Coders Table	86
B.4	Step 4: Configure SIP UDP Transport Type and Fax Signaling Method.....	87

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: April-20-2021

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
39344	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 <https://online.audiocodes.com/documentation-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 Virgin Media'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 Virgin Media partners who are responsible for installing and configuring Virgin Media'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 connect with third-party PSTN equipment. The connection allows:

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

1.3 About AudioCodes SBC Product Series

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

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

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

AudioCodes SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWS, AZURE, AWP, KVM and VMWare.

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B/C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000/B SBC ▪ Mediant 9000, 9030, 9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.20A.258.457 or later
Protocol	▪ SIP/UDP (to the Virgin Media SIP Trunk) ▪ SIP/TLS (to the Teams Direct Routing)
Additional Notes	None

2.2 Virgin Media SIP Trunking Version

Table 2-2: Virgin Media Version

Vendor/Service Provider	Virgin Media
Manufacture	Ribbon
Hardware/Software Version	Soft switch C20 / R20
Hardware/Software Version	SBC 3 Ribbon Q20 / v9.4.4.0
Hardware/Software Version	SBC 4 Ribbon Q20 / v9.4.4.0
Protocol	SIP
Additional Notes	None

2.3 Microsoft Teams Direct Routing Version

Table 2-3: Microsoft Teams Direct Routing Version

Vendor	Microsoft
Model	Teams Phone System Direct Routing
Software Version	v.2021.3.1.6
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

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

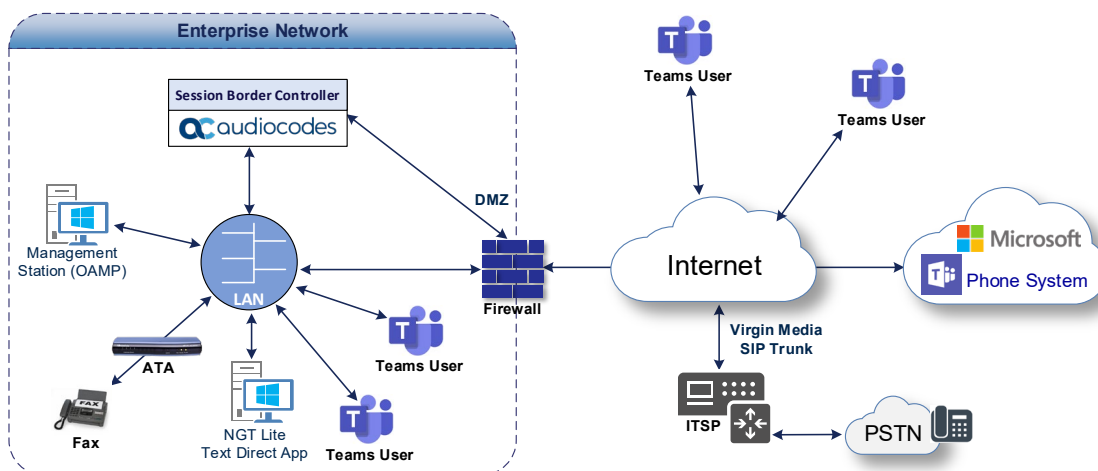
2.4.1 Enterprise Model Implementation

The interoperability testing between AudioCodes SBC and Virgin Media 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 Virgin Media'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 Virgin Media's SIP Trunk is located in the Enterprise LAN (or WAN) 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 Virgin Media SIP Trunk



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	Both, Virgin Media SIP Trunk and Microsoft Teams Direct Routing environment are located on the Enterprise's (or Service Provider's) WAN
Signaling Transcoding	- Microsoft Teams Direct Routing operates with SIP-over-TLS transport type - Virgin Media SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	- Microsoft Teams Direct Routing supports G.711A-law, G.711U-law, G.729, G.722, SILK (NB and WB) and OPUS coders - Virgin Media SIP Trunk supports both G711 A-Law and G711 U-law. The testing was only conducted using G711 A-law as this is Virgin Media SIP Trunk preferred codec for interoperability testing
Media Transcoding	- Microsoft Teams Direct Routing operates with SRTP media type - Virgin Media SIP Trunk operates with RTP media type

2.4.3 Infrastructure Prerequisites

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

Table 2-5: Infrastructure Prerequisites

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

2.4.4 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes SBC interworking between Microsoft Teams Direct Routing and Virgin Media's SIP Trunk.

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

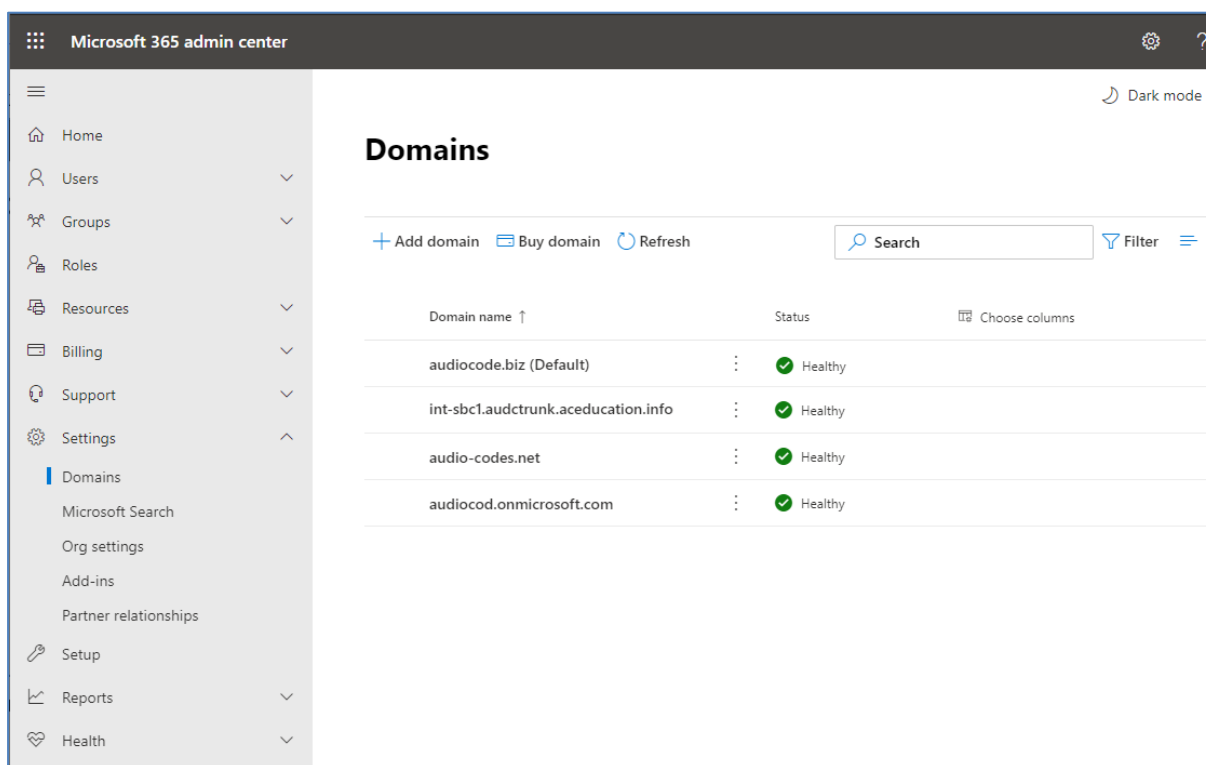
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, in Figure 3-1, the administrator registered the following DNS names for the tenant:

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

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

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

Figure 3-1: Example of Registered DNS Names

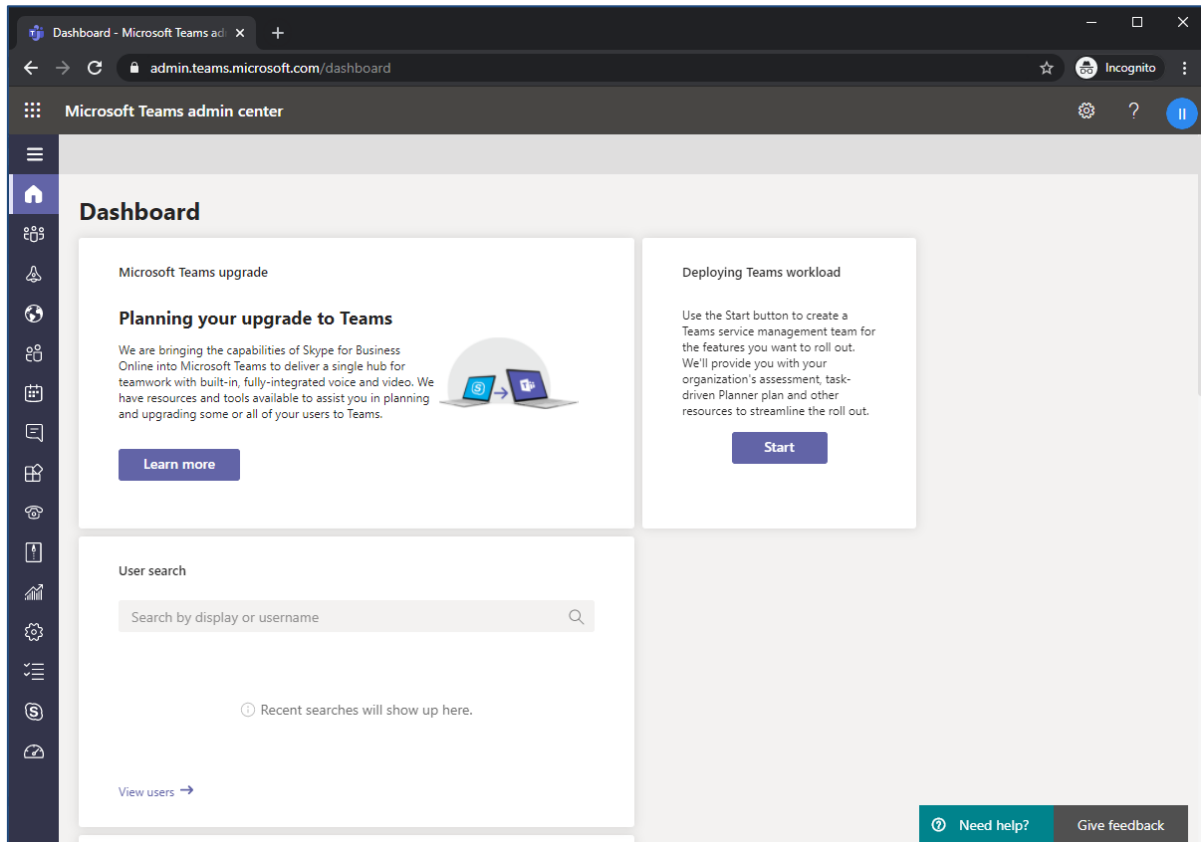


During creation of the Domain you will be forced to create public DNS record (**int-sbc1.audctrunk.aceducation.info** in our example) .

3.3 Example of the Office 365 Tenant Direct Routing Configuration

Configuration can be performed using the web or with PowerShell. For the web, login to the Teams Admin Center (<https://admin.teams.microsoft.com>) with Tenant Administrator credentials.

Figure 3-2: Teams Admin Center



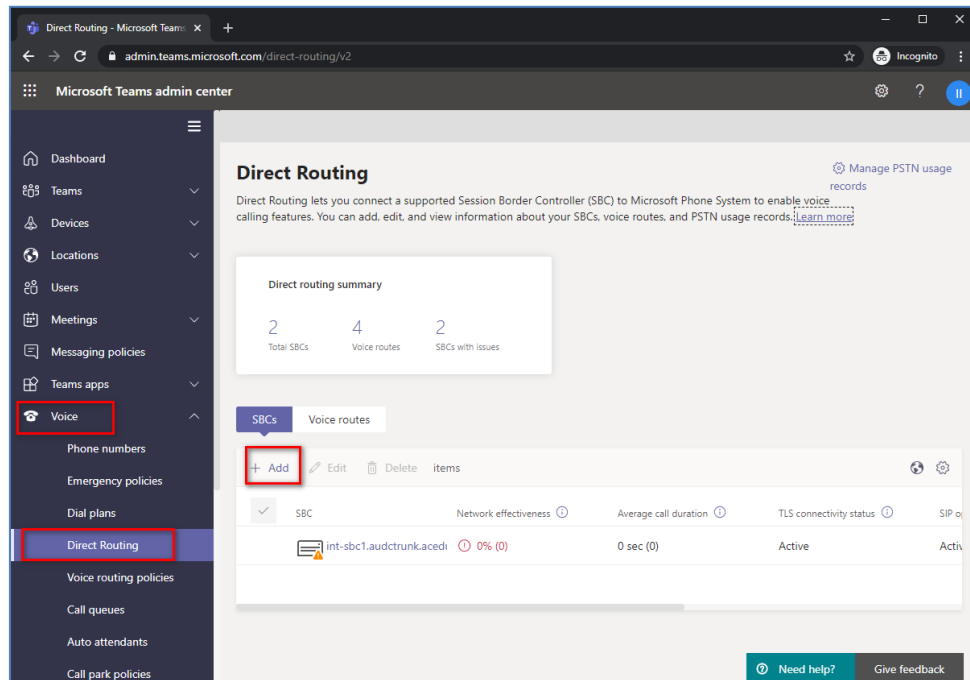
3.3.1 Add New SBC to Direct Routing

The procedure below describes how add a new SBC to Direct Routing.

➤ To add New SBC to Direct Routing:

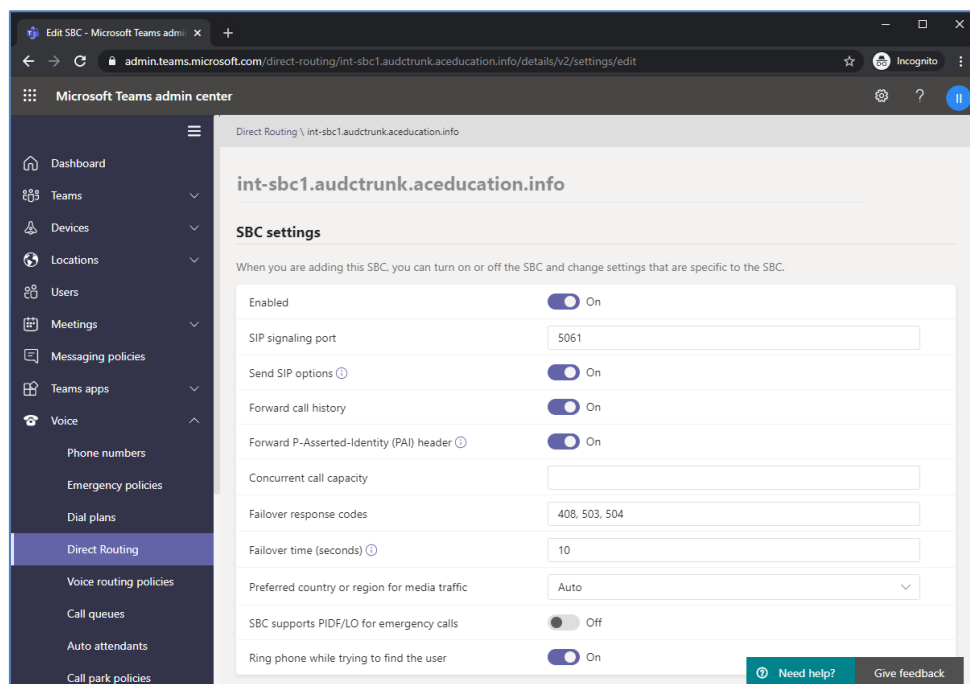
1. In the web interface, select **Voice**, and then click **Direct Routing**.
2. Under SBCs click **Add**.

Figure 3-3: Add new SBC to Direct Routing



3. Configure SBC.

Figure 3-4: Configure new SBC



You can use the following PowerShell command for creating a new Online PSTN Gateway:

```
New-CsOnlinePSTNGateway -Identity int-sbc1.audctrunk.aceducation.info -SipSignallingPort 5061 -ForwardCallHistory $True -ForwardPai $True -MediaBypass $True -Enabled $True
```



Note: Currently, enabling MediaBypass is available only through PowerShell.

3.3.2 Add Voice Route and PSTN Usage

The procedure below describes how add a voice route and PSTN usage.

➤ **To add voice route and PSTN usage:**

1. In the web interface, under **Direct Routing**, select **Voice routes**, and then click **Add**.

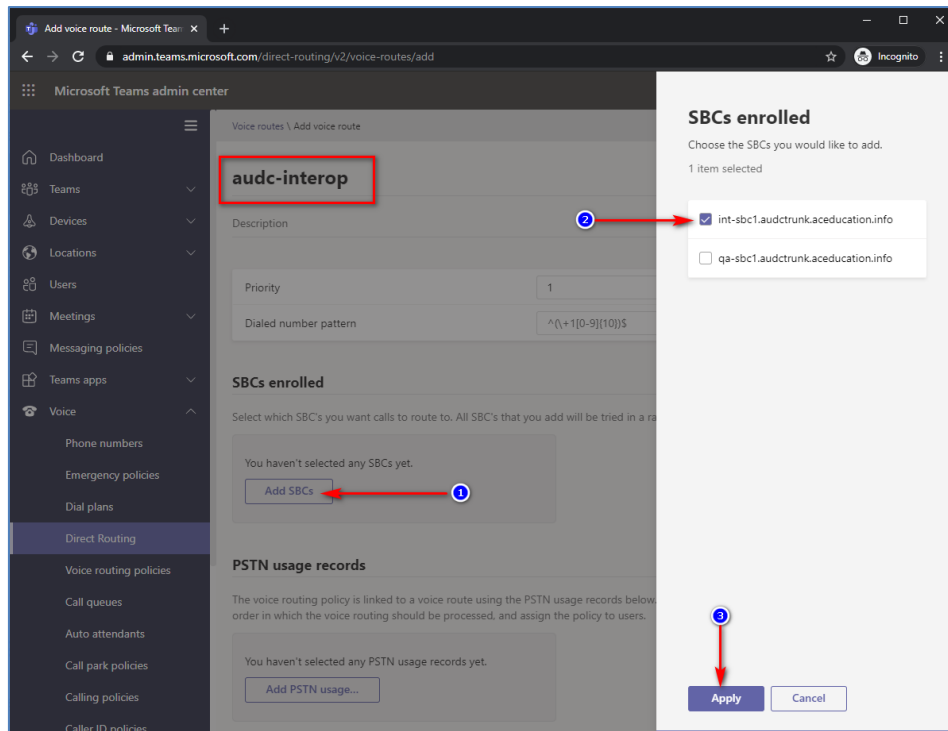
Figure 3-5: Add New Voice Route

The screenshot shows the Microsoft Teams admin center interface. The left sidebar has 'Voice' and 'Direct Routing' highlighted. The main content area is titled 'Direct Routing' and includes a summary card showing 2 Total SBCs, 4 Voice routes, and 2 SBCs with issues. Below this, the 'Voice routes' tab is active, showing a table of existing routes. The 'Add' button is highlighted with a red box.

✓	Priority	Voice route	Description	Dialed number pattern	PSTN
	1	int-il		^\+	Inte
	2	Israel		^\+972(\d{8})	Isra
	3	AC-SBCaaS-Any		\d+	SBC
	4	Test1	Only Testing		

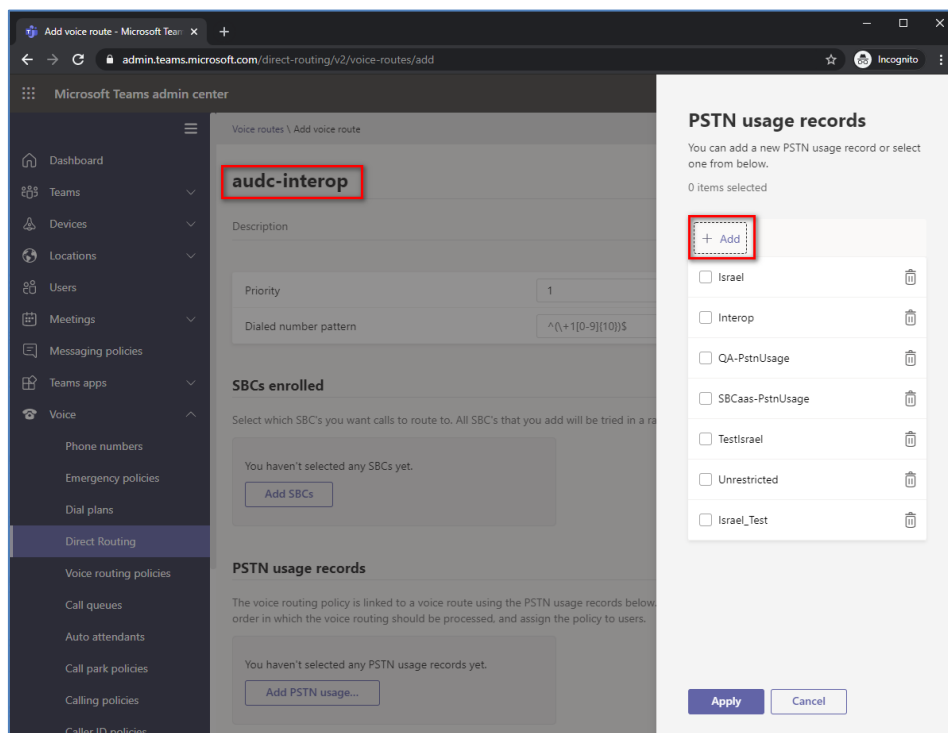
2. Create a new Voice Route and associate it with the SBC, configured in the previous step.

Figure 3-6: Associate SBC with new Voice Route



3. Add new (or associate existing) PSTN usage.

Figure 3-7: Associate PSTN Usage with New Voice Route



The same operations can be done using following PowerShell commands:

4. Creating an empty PSTN Usage:

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

5. Creating new Online Voice Route and associating it with PSTN Usage:

```
New-CsOnlineVoiceRoute -Identity "audc-interop" -NumberPattern
"^\\+" -OnlinePstnGatewayList int-
sbc1.audctrunk.aceducation.info -Priority 1 -OnlinePstnUsages
"Interop"
```

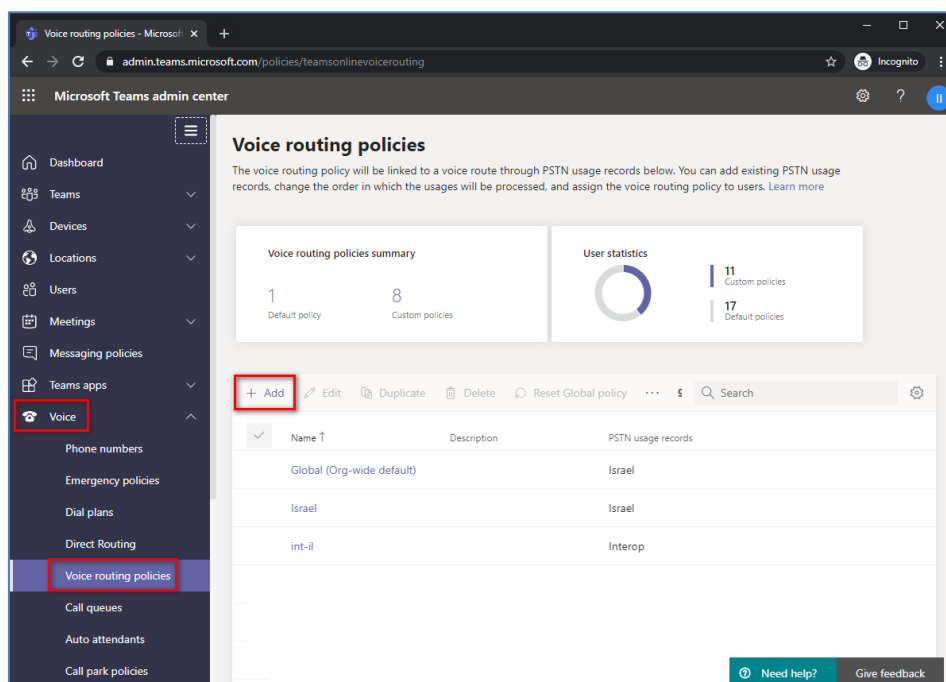
3.3.3 Add Voice Routing Policy

The procedure below describes how to add a voice routing policy

➤ To add voice routing policy:

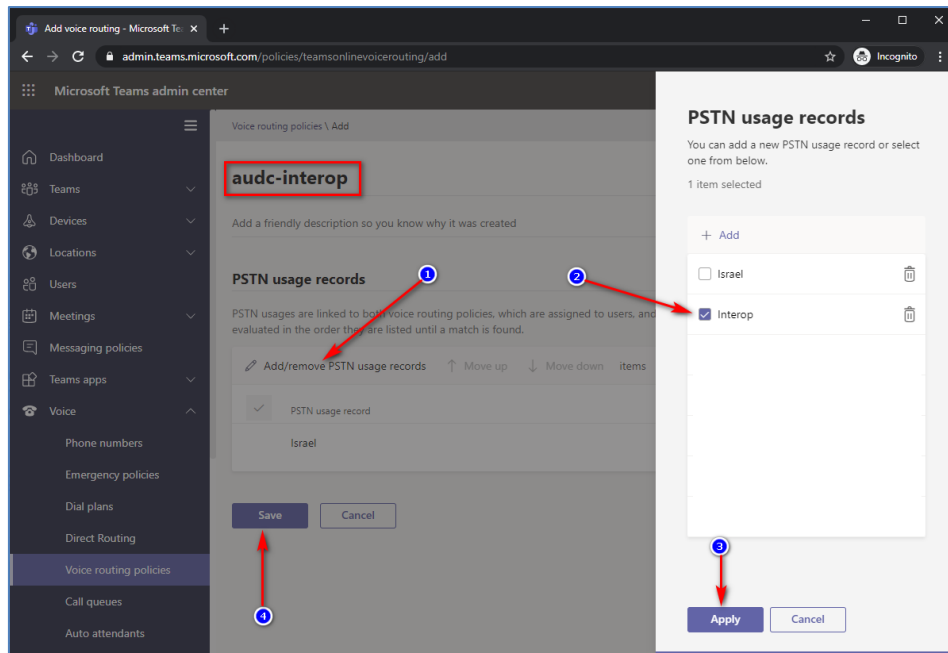
1. In the web interface, under **Voice**, select **Voice routing policies** and click **Add**.

Figure 3-8: Add New Voice Routing Policy



2. Create a new Voice Routing Policy and associate it with PSTN Usage, configured in the previous step.

Figure 3-9: Associate PSTN Usage with New Voice Routing Policy



The same operations can be done using following PowerShell command:

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



Note: The commands specified in Sections 3.3.4 and 3.3.5, should be run **for each** Teams user in the company tenant. They are currently available through PowerShell **only**.

3.3.4 Enable Online User

Use the following PowerShell command for enabling online user:

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

3.3.5 Assigning Online User to the Voice Routing Policy

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

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

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 Virgin Media 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 - Virgin Media 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 Virgin Media 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:
 - **MSFT** (general Microsoft license)
Note: By default, all AudioCodes media gateways and SBCs are shipped with this license (except MSBR products, Mediant 500 SBC, and Mediant 500 Media Gateway).
 - **SW/TEAMS** (Microsoft Teams license)
 - **Number of SBC sessions** (based on requirements)
 - **Transcoding sessions** (only if media transcoding is needed)
 - **Coders** (based on requirements)
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

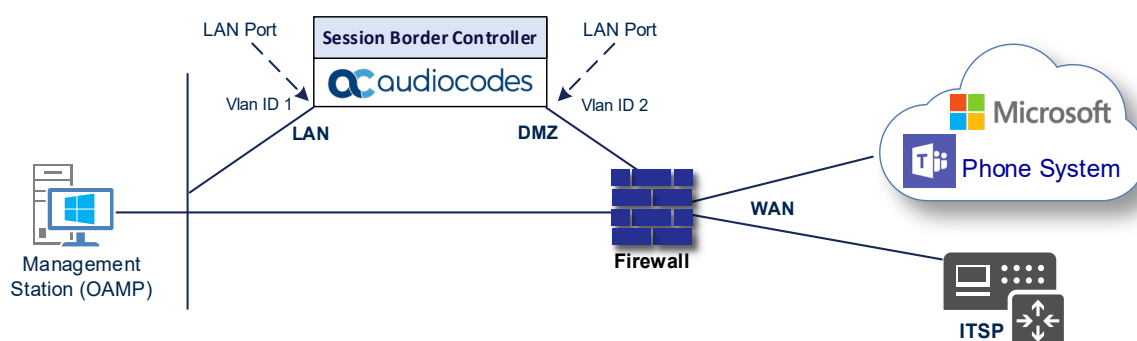


4.2 IP Network Interfaces Configuration

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 Virgin Media 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

Ethernet Devices (2)				
+ New Edit 🗑️ Page 1 of 1 Show 10 records per page				
INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

4.2.2 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: int-sbc1.audctrunk.aceducation.info
- SAN: int-sbc1.audctrunk.aceducation.info

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 the remote parties. It is important, that the NTP server is configured on the same network as the OAMP IP Interface (in our case LAN_IF) 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., **10.15.27.1**).

Figure 4-5: Configuring NTP Server Address

NTP SERVER	
Enable NTP	Enable
Primary NTP Server Address (IP or FQDN)	10.15.27.1
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]

GENERAL

Index: 1

Name: Teams

TLS Version: TLSv1.2

DTLS Version: Any

Cipher Server: DEFAULT

Cipher Client: DEFAULT

Cipher Server TLS1.3: TLS_AES_256_GCM_SHA384:TLS_CHACH

Cipher Client TLS1.3: TLS_AES_256_GCM_SHA384:TLS_CHACH

Key Exchange Groups: X25519:P-256:P-384:X448

Strict Certificate Extension Validation: Disable

DH key Size: 2048

TLS Renegotiation: Enable

OCSP

OCSP Server: Disable

Primary OCSP Server: 0.0.0.0

Secondary OCSP Server: 0.0.0.0

OCSP Port: 2560

OCSP Default Response: Reject

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:

1. Generating a Certificate Signing Request (CSR).
2. Requesting Device Certificate from CA.
3. Obtaining Trusted Root/ Intermediate Certificate from CA.
4. 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, **int-sbc1.audctrunk.aceducation.info**).
 - b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on example above, **int-sbc1.audctrunk.aceducation.info**).



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.
- d. To change the key size on TLS Context, go to: **Generate New Private Key**, change the 'Private Key Size' to the value required by your CA and then click **Generate Private-Key**. To use **2048** 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]

int-sbc1.audctrunk.aceducation.info

Organizational Unit [OU] (optional)

Company name [O] (optional)

Locality or city name [L] (optional)

State [ST] (optional)

Country code [C] (optional)

1st Subject Alternative Name [SAN]

DNS int-sbc1.audctrunk.aceducation.info

2nd Subject Alternative Name [SAN]

EMAIL

3rd Subject Alternative Name [SAN]

EMAIL

4th Subject Alternative Name [SAN]

EMAIL

5th Subject Alternative Name [SAN]

EMAIL

Signature Algorithm

SHA-256

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.

Generate Self-Signed Certificate

Create CSR

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-----
MIICtDCCAZwCAQwLjEsMCoGA1UEAwVjZmF0aW9uLm1uZm8wggE1MA0GCQsGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDBAdaD
iQKgtqr39RL7bY1RxtX9Zu80JUp9e1f1H3IEY6nY+kqfYSTIVFhm3SEsYU1sBd
J/p6EA6e0UaWLeZs1324VP+1nctA6a00Mz7uc+11p89ywNpk3+5rZNNXGZKKqpnF
P2Hw4h0px/dXX0IvEwv+4Uf1St0072bZLppDIYDqQZcxDT1r1ZzRqP5mqATaTAI
zaFayjrB0wB0n5NOH6M09u+557eJ3UQxX+36rTRxU0o+qbdjiuMFP+dXrkzA5dBY
bIrmqB27DA6RUXhwj3pw/sBSQn9FZuZpu3mZrth/EUCMEQ2tjjm96P/37mx358Fh
4CnrgXsu4HrXS6QxAgHBAAGQTA/BgkqhkiG9w0BQC4xMjAwMCA4G1udEQnMCwC
I21udC1zYmF0aW9uLm1uZm8wcnVuaY5hY2VkdmlhdG1vb15pbmZvMA0GCQsGSIb3DQEBAQUAA4IBAQJroPaX2yF/DSNJdRT+sZTEu2GnkgaorhV3hzwOaK3pLw8Hmw6upk9
UKv6E9/2Glnh1cmR20oGkFvMmRnYL8xerjTdhRjch1q/RP+1eJpm1N73xmD1sW/MVx
skirw8G52jge18rQEBZIU70R48PM/xhCV3Te4ZyEkdM3JHqoG1HyS5ud7wlyDUYHA
7x3wG1wFCHsf+CFAkw5vtAxVI6F9VOY1OGty71xhNMG1McYP8P3U215QyQoFyOC
jktQ8UEkDeHbyfig1H7S11A6g5fSHU1Y0AAKfhwvEoXU34kAMXxfn57DAShTxFwulw
pRSjw21C88DHj1FZgOC+OoxC1Va8HOEJ
-----END CERTIFICATE REQUEST-----

```

GENERATE NEW PRIVATE KEY

Private Key Size

2048

Press the "Generate Private Key" button to create new private key.

Important: generation of private key is a lengthy operation during which the device service may be affected.

Generate Private-Key

- Copy the CSR from the line "**-----BEGIN 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*.
- Send *certreq.txt* file to the Certified Authority Administrator for signing.

AudioCodes Mediant SBC

28

Document #: LTRT-39344

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:
45:be:53:11:ad:89:63:80:3b:ab:14:5e:34:34:57:53
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 4 14:24:51 2020 GMT
Not After: May 4 14:24:51 2022 GMT
Subject: CN= int-sbc1.audctrunk.aceducation.info
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA 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

TLS Context [#2] > Trusted Root Certificates			
View		Import Export Remove	
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	SIPTrunk (arbitrary name)		WAN_IF	6000	100 (media sessions assigned with port range)
1	Teams (arbitrary name)	Up	WAN_IF	7000	100 (media sessions assigned with port range)
2	MRLan (arbitrary name)		LAN_IF	6000	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

Media Realms (3)						
+ New Edit Page 1 of 1 Show 10 records per page						
INDEX	NAME	IPv4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
0	SIPTrunk	WAN_IF	6000	100	6999	No
1	Teams	WAN_IF	7000	100	7999	No
2	MRLan	LAN_IF	6000	100	6999	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), however 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	SIPTrunk (arbitrary name)	WAN_IF	SBC	5060 (according to Service Provider requirement)	0	0	Disable (leave default value)	0 (Recommended to prevent DoS attacks)	SIPTrunk	-
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)	Teams	Teams
2	SI-LAN	LAN_IF	SBC	5060	5060	5061	Disable	Leave Default	MRLan	-

The configured SIP Interfaces are shown in the figure below:

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

SIP Interfaces (3)									
+ 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	SIPTrunk	DefaultSRD	WAN_IF	SBC	5060	0	0	No encapsulation	SIPTrunk
1	Teams	DefaultSRD	WAN_IF	SBC	0	0	5061	No encapsulation	Teams
2	SI-LAN	DefaultSRD	LAN_IF	SBC	5060	5060	5061	No encapsulation	MRLan

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:

- Virgin Media SIP Trunk A
- Virgin Media SIP Trunk B
- Teams Direct Routing
- Fax supporting ATA device (if required)

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	Keep-Alive Failure Responses	Proxy Hot Swap	Proxy Load Balancing Method
1	VM Trunk A (arbitrary name)	SIPTrunk	Default	Using Options	503	-	-
1	VM Trunk B (arbitrary name)	SIPTrunk	Default	Using Options	503	-	-
3	Teams (arbitrary name)	Teams	Teams	Using Options	-	Enable	Random Weights
4	MP-Fax (arbitrary name)	SI-LAN	Default	Using Options	-	-	-

The configured Proxy Sets are shown in the figure below:

Figure 4-13: Configured Proxy Sets in Proxy Sets Table

Proxy Sets (5)							
+ 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 (#0)	--	SIPTrunk	60		Disable
1	VM Trunk A	DefaultSRD (#0)	--	SIPTrunk	60		Disable
2	VM Trunk B	DefaultSRD (#0)	--	SIPTrunk	60		Disable
3	Teams	DefaultSRD (#0)	--	Teams	60		Enable
4	MP-Fax	DefaultSRD (#0)	--	SI-LAN	60		Disable

4.6.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.



Note: When the connection is to the VM production network, the Proxy address (Signaling IP address) needs to be obtained from the VM production network. The Proxy address (Signaling IP address) reflected in the configuration below for VM Trunk A and B is for the purpose of connecting to the VM test environment and not to the production network.

➤ **To configure a Proxy Address for VM Trunk A:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**), click the Proxy Set **VM Trunk A**, 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 VM Trunk A

The screenshot shows a 'Proxy Address' configuration window. It has a title bar with 'Proxy Address' and standard window controls. Below the title bar is a 'GENERAL' tab. The configuration fields are as follows:

Field	Value
Index	0
Proxy Address	81.97.95.188:5060
Transport Type	UDP
Proxy Priority	0
Proxy Random Weight	0

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

Table 4-6: Configuration Proxy Address for VM Trunk A

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	81.97.95.188:5060	UDP	0	0

4. Click **Apply**.

➤ **To configure a Proxy Address for VM Trunk B:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**), click the Proxy Set **VM Trunk B**, 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 VM Trunk B

The screenshot shows a 'Proxy Address' configuration window. It has a dark blue title bar with the text 'Proxy Address' and standard window controls. Below the title bar is a light gray header with the word 'GENERAL'. The main area contains five configuration fields, each with a label on the left and a text input field on the right. The fields are: 'Index' with value '0', 'Proxy Address' with value '82.14.171.242:5060', 'Transport Type' with a dropdown menu showing 'UDP', 'Proxy Priority' with value '0', and 'Proxy Random Weight' with value '0'.

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

Table 4-7: Configuration Proxy Address for VM Trunk B

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	82.14.171.242:5060	UDP	0	0

4. Click **Apply**.

➤ **To configure a Proxy Address for Teams:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**), 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 4-16: Configuring Proxy Address for Teams Direct Routing Interface

The screenshot shows a 'Proxy Address' configuration window. It has a title bar with the text 'Proxy Address' and standard window controls. Below the title bar is a 'GENERAL' tab. The configuration fields are as follows:

Field	Value
Index	0
Proxy Address	sip.pstnhub.microsoft.com:5061
Transport Type	TLS
Proxy Priority	1
Proxy Random Weight	1

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

Table 4-8: 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**.

- To configure a Proxy Address for Fax supporting ATA device (if required):
- 1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**), click the Proxy Set **MP-Fax**, 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 4-17: Configuring Proxy Address for Fax ATA device

The screenshot shows a 'Proxy Address' configuration window. It has a dark blue title bar with the text 'Proxy Address' and standard window controls. The main content area has a light gray background. At the top, there is a tab labeled 'GENERAL'. Below the tab, there are three configuration fields: 'Index' with a text input containing '0', 'Proxy Address' with a text input containing '10.15.77.14:5060', and 'Transport Type' with a dropdown menu currently showing 'UDP'.

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

Table 4-9: Configuration Proxy Address for Fax ATA device

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	10.15.77.14:5060	UDP	0	0

- 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 Virgin Media SIP Trunk may restrict operation with the G.711A-law coder whenever possible, you need to add a Coder Group with the supported coders for each leg, the Microsoft Teams Direct Routing and the Virgin Media 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	▪ SILK-NB ▪ SILK-WB ▪ G.711 A-law ▪ G.711 U-law ▪ G.729

Figure 4-18: 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 Virgin Media 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 Virgin Media SIP Trunk in the next step.

➤ **To set a preferred coder for the Virgin Media 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 Virgin Media SIP Trunk.

Figure 4-19: Configuring Allowed Coders Group for Virgin Media SIP Trunk

Allowed Audio Coders Groups [VM Allowed Coders]

GENERAL

Index: 0

Name: • VM 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:

Parameter	Value
Index	0
Coder	G.711A-law

Figure 4-20: Configuring Allowed Coders for Virgin Media SIP Trunk

Allowed Audio Coders

GENERAL

Index: 0

Coder: • G.711 A-law ▼

User-defined Coder:

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

Figure 4-21: SBC Preferences Mode

Media Settings

GENERAL

NAT Traversal

Enable Continuity Tones

Inbound Media Latch Mode

Number of Media Channels

Enforce Media Order

SDP Session Owner

SBC SETTINGS

Preferences Mode ←

Enforce Media Order

GATEWAY SETTINGS

Enable Early Media

Multiple Packetization Time Format

ROBUSTNESS

New RTP Stream Packets

New RTCP Stream Packets

New SRTP Stream Packets

New SRTCP Stream Packets

Timeout To Relatch RTP (msec)

Timeout To Relatch SRTP (msec)

Timeout To Relatch Silence (msec)

Timeout To Relatch RTCP (msec)

Cancel

7. From the '**Preferences Mode**' drop-down list, select **Include Extensions**.
8. 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:

- Virgin Media SIP trunk – to operate in non-secure mode using RTP and SIP over UDP
- Microsoft Teams Direct Routing – to operate in secure mode using SRTP and SIP over TLS

➤ To configure an IP Profile for the Virgin Media 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	VM
Media Security	
SBC Media Security Mode	Not Secured
SBC Early Media	
Remote Multiple 18x	Not Supported
SBC Media	
Allowed Audio Coders	VM Allowed Coders
Use Silence Suppression	Remove
RTP Redundancy Mode	Disable
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
Session Expires Mode	Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote Replaces Mode	Handle Locally
Remote 3xx Mode	Handle Locally

Figure 4-22: Configuring IP Profile for Virgin Media 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 while in Hold mode, however Microsoft expected this behavior)
ICE Mode	Lite (required only when Media Bypass is enabled on Microsoft Teams)
SBC Signaling	

SIP 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 Replaces 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 does not support this format, therefore the SBC will replace 0.0.0.0 with its IP address).

Figure 4-23: Configuring IP Profile for Microsoft Teams Direct Routing

IP Profiles [Teams]

GENERAL

Index: 2

Name: Teams

Created by Routing Server: No

MEDIA SECURITY

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: SDES

Reset SRTP Upon Re-key: Disable

SBC SIGNALING

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

SIP 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

Remote Representation Mode: According to Operation Mode

Cancel APPLY

3. Click Apply.

4.9 Configure SBC Alternative Routing Reasons

This section describes how to configure the SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case, the SBC attempts to locate an alternative route for the call. The Alternative Reasons Set Table is used for this purpose. To apply your configured alternative routing reason rules, you need to assign the Alternative Reasons Set for which you configured the rules to the relevant IP Group in the IP Groups table, using the 'SBC Alternative Routing Reasons Set' parameter.

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

1. Open the Alternative Reasons Set table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons Set**).
2. Click **New** and configure a name for the Alternative Reasons Set.

Figure 4-24: Configuring Alternative Reasons Set for Virgin Media SIP Trunk

Alternative Reasons Set [503 Response] - x

GENERAL

Index: 0

Name: 503 Response

Description:

3. Click **Apply**.
4. Select the new row that you configured, and then click the **Alternative Reasons Rules** link located below the table; the Alternative Reasons Rules table opens.
5. Click **New**.
6. From the 'Release Cause' drop-down list, select 503 Service Unavailable:

Figure 4-25: Configuring Alternative Reasons Rule for Virgin Media SIP Trunk

Alternative Reasons Rules - x

GENERAL

Index: 0

Release Cause Code: 503 Service Unavailable

7. Click **Apply**.

4.10 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network to which the SBC communicates. This entity 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 the source and destination of the call.

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

- Virgin Media SIP Trunk (A and B)
- Teams Direct Routing
- Fax supporting ATA device (if required)

➤ 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 Virgin Media SIP Trunk A:

Parameter	Value
Index	1
Name	VM Trunk A
Type	Server
Proxy Set	VM Trunk A
IP Profile	VM
Media Realm	SIPTrunk
SIP Group Name	(according to ITSP requirement)
SBC Alternative Routing Reasons Set	503 Response (as configured in Section 4.9 on page 45)
Proxy Keep-Alive using IP Group settings	Enable

3. Configure an IP Group for the Virgin Media SIP Trunk B:

Parameter	Value
Index	2
Name	VM Trunk B
Type	Server
Proxy Set	VM Trunk B
IP Profile	VM
Media Realm	SIPTrunk
SIP Group Name	(according to ITSP requirement)
SBC Alternative Routing Reasons Set	503 Response (as configured in Section 4.9 on page 45)
Proxy Keep-Alive using IP Group settings	Enable

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

Parameter	Value
Index	3
Name	Teams
Topology Location	Up
Type	Server
Proxy Set	Teams
IP Profile	Teams
Media Realm	Teams
SIP Group Name	(according to ITSP requirement)
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

5. Configure an IP Group for the Fax supporting ATA device:

Parameter	Value
Index	4
Name	MP-Fax
Type	Server
Proxy Set	MP-Fax
Media Realm	MRLan
SIP Group Name	(according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-26: Configured IP Groups in IP Group Table

IP Groups (5)											
+ New Edit		Page 1 of 1						Show 10 records per page			
INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default.JPG	DefaultSRD	Server	Not Configured	ProxySet_0	--	--		Disable	-1	-1
1	VM Trunk A	DefaultSRD	Server	Not Configured	VM Trunk A	VM	SIPTrunk	81.97.95.188	Enable	-1	4
2	VM Trunk B	DefaultSRD	Server	Not Configured	VM Trunk B	VM	SIPTrunk	82.14.171.242	Enable	-1	4
3	Teams	DefaultSRD	Server	Not Configured	Teams	Teams	Teams	195.189.192.154	Disable	1	-1
4	MP-Fax	DefaultSRD	Server	Not Configured	MP-Fax	--	MRLan		Enable	-1	-1

4.11 Configure IP Group Sets

This section describes how to configure an IP Group Set for the Virgin Media SIP Trunk. We will use IP Group Set for alternative routing within the IP Group Set. If a chosen destination IP Group responds with a reject response that is configured for an Alternative Reasons Set that is assigned to the IP Group, or doesn't respond at all (i.e., Keep-alive with its' associated Proxy Set fails), the SBC attempts to send the call to another IP Group in the IP Group Set.

➤ **To configure IP Group Set:**

1. Open the IP Group Set table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP Group Set**).
2. Click **New** and configure a name for the Alternative Reasons Set.
3. From the 'Policy' drop-down list, select **Homing**. Therefore, the SBC always attempts to send all calls to the first IP Group in the table (i.e., lowest index). If unavailable, it will then send the calls to the next consecutive, available IP Group. However, if the first IP Group later becomes available again, the SBC will select to work with it.



Note: If the customer requires load sharing, the **Policy** parameter should be configured with **Round-Robin** value. Therefore, the SBC will select the next consecutive, available IP Group for each call.

Figure 4-27: Configuring IP Group Set for Virgin Media SIP Trunk

The screenshot shows a configuration window titled "IP Group Set [Virgin Media]". Inside, there is a "GENERAL" tab. The fields are as follows:

- Index:** 0
- Name:** Virgin Media
- Policy:** Homing (selected from a dropdown menu)
- Tags:** (empty text field)

4. Click **Apply**.
5. Select the new row that you configured, and then click the **IP Group Set Member** link located below the table; the IP Group Set Member table opens.
6. Click **New**.
7. Configure IP Group Set members:

Figure 4-28: IP Group Set Members for Virgin Media SIP Trunk

The screenshot shows the "IP Group Set Member" table. The breadcrumb is "IP Group Set [#0] > IP Group Set Member (2)". The table has the following data:

INDEX	IP GROUP	WEIGHT
0	VM Trunk A	1
1	VM Trunk B	1

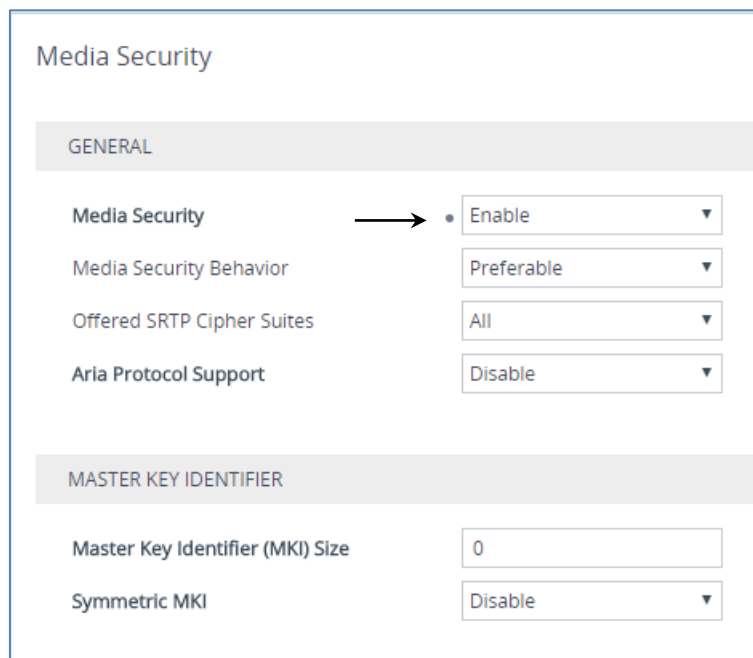
4.12 Configure SRTP

This section describes how to configure media security. The Direct Routing Interface needs to use 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 4-29: Configuring SRTP



The screenshot shows the 'Media Security' configuration page. The 'GENERAL' tab is selected. The 'Media Security' dropdown menu is set to 'Enable', indicated by an arrow. Other settings include 'Media Security Behavior' set to 'Preferable', 'Offered SRTP Cipher Suites' set to 'All', and 'Aria Protocol Support' set to 'Disable'. The 'MASTER KEY IDENTIFIER' section shows 'Master Key Identifier (MKI) Size' set to '0' and 'Symmetric MKI' set to 'Disable'.

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**.

4.13 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 4-30: Configuring Condition Table

The screenshot shows a web interface titled "Message Conditions [Teams-Contact]". It features a "GENERAL" tab. Under this tab, there are three configuration fields: "Index" with a value of "0", "Name" with a value of "Teams-Contact", and "Condition" with a value of "Header.Contact.URL.Host contains 'pstnhub.microsoft.com'". An "Editor" button is located next to the condition field.

3. Click **Apply**.

4.14 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. int-sbc1.audctrunk.aceducation.info)
Message Condition	Teams-Contact
Action Type	Allow
Source IP Group	Teams

Figure 4-31: Configuring Classification Rule

Classification [Teams]

SRD: #0 [DefaultSRD]

MATCH		ACTION	
Index	0	Action Type	Allow
Name	Teams	Destination Routing Policy	-- View
Source SIP Interface	#0 [SIPInterface_0] View	IP Group Selection	Source IP Group
Source IP Address	52.114.*.*	Source IP Group	#2 [Teams] View
Source Transport Type	Any	IP Group Tag Name	default
Source Port	0	IP Profile	-- View
Source Username Pattern	*		
Source Host	*		
Destination Username Pattern	*		
Destination Host	int-sbc1.audctrunk.aceducation.info		

Cancel APPLY

3. Click **Apply**.

4.15 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 Virgin Media 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 Virgin Media SIP Trunk
- Calls from Fax supporting ATA device to Virgin Media SIP Trunk (if required)
- Calls from Virgin Media SIP Trunk to Fax supporting ATA device (if required)
- Calls from Virgin Media 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 4-10: Configuration IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Call Trigger	ReRoute IP Group	Dest Username Pattern	Dest Type	Dest IP Group	IP Group Set	Internal Action
0	Terminate OPTIONS	Any	OPTION S				Internal			Reply (Response = '200')
1	Refer from Teams (arbitrary name)	Any		REFER	Teams		Request URI	Teams		
2	Teams to SIP Trunk (arbitrary name)	Teams					IP Group Set		Virgin Media	
3	MP-Fax to SIP Trunk (arbitrary name)	MP-Fax					IP Group Set		Virgin Media	
4	SIP Trunk to MP-Fax (arbitrary name)	Any				+44118 337412 5	IP Group	MP-Fax		
5	SIP Trunk to Teams (arbitrary name)	Any					IP Group	Teams		

The configured routing rules are shown in the figure below:

Figure 4-32: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (6)											
+ 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	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Terminate OPTIC	Default_SBCRout	Route Row	Any	OPTIONS	*	*	Internal	--	--	
1	Refer from Team	Default_SBCRout	Route Row	Any	All	*	*	Request URI	Teams	--	
2	Teams to SIP Tru	Default_SBCRout	Route Row	Teams	All	*	*	IP Group Set	--	--	
3	MP-Fax to SIP Tri	Default_SBCRout	Route Row	MP-Fax	All	*	*	IP Group Set	--	--	
4	SIP Trunk to MP-	Default_SBCRout	Route Row	Any	All	*	+441183374125	IP Group	MP-Fax	--	
5	SIP Trunk to Teal	Default_SBCRout	Route Row	Any	All	*	*	IP Group	Teams	--	



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

4.16 Configuring Firewall Settings (Optional)

As an extra security measure, there is an 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 the Teams Direct Routing IP Interface:

Table 4-11: 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
7	81.97.95.188	32	0	65535	UDP	Enable	WAN_IF	Allow
8	82.14.171.242	32	0	65535	UDP	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. See an example in the rows of index 7 and 8.

4.17 Configure Number Manipulation Rules

This section describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.10 on page 46) 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 does not exist) for calls from any IP Group for any destination username pattern; and remove the "+" (plus sign) from the destination number for emergency calls.

➤ **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 Virgin Media SIP Trunk:

Figure 4-33: Example of Configured IP-to-IP Outbound Manipulation Rules

Outbound Manipulations (5)													
+ New Edit Insert ↓ ↑ 🗑 Page 1 of 1 Show 10 records per page													
INDEX	NAME	ROUTING POLICY	ADDITIONAL MANIPULATION	SOURCE IP GROUP	DESTINATION IP GROUP	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	MANIPULATION ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	To Emergen	Default_SBC	No	Any	VM Trunk A	*	[999,112,18000]	Destination	0	0	255		
1	To Emergen	Default_SBC	No	Any	VM Trunk B	*	[999,112,18000]	Destination	0	0	255		
2	To Emergen	Default_SBC	No	Any	VM Trunk A	*	[+999,+112,-	Destination	1	0	255		
3	To Emergen	Default_SBC	No	Any	VM Trunk B	*	[+999,+112,-	Destination	1	0	255		
4	Add +	Default_SBC	No	Any	Any	*	[1-9]	Destination	0	0	255	+	

Rule Index	Description
0	For calls to emergency numbers (999, 112, 18000) through Virgin Media SIP Trunk A without the prefix destination number "+", no action is required.
1	For calls to emergency numbers (999, 112, 18000) through Virgin Media SIP Trunk B without the prefix destination number "+", no action is required.
2	For calls to emergency numbers (999, 112, 18000) through Virgin Media SIP Trunk A with the prefix destination number "+", remove this digit "+".
3	For calls to emergency numbers (999, 112, 18000) through Virgin Media SIP Trunk B with the prefix destination number "+", remove this digit "+".
4	For calls with any destination number [1-9], add "+" to the prefix of the destination number.

4.18 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 rule 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 4-34: Configuring SIP Message Manipulation Rule 0 (for Teams)

The screenshot shows the 'Message Manipulations [Remove PAI]' window. 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, there are 'Cancel' and 'APPLY' buttons.

3. Configure another manipulation rule (Manipulation Set 1) for Teams. This rule applies to messages received from the Teams IP Group. This rule removes the SIP Privacy Header in all messages, except for calls with presentation restrictions.

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

Figure 4-35: Configuring SIP Message Manipulation Rule 1 (for Teams)

Message Manipulations [Remove Privacy Header]

GENERAL

Index

1

Name

Remove Privacy Header

Manipulation Set ID

1

Row Role

Use Current Condition

MATCH

Message Type

Editor

Condition

Header.Privacy exists And Header.From

Editor

ACTION

Action Subject

Header.Privacy

Editor

Action Type

Remove

Action Value

Editor

Cancel

APPLY

4. Configure another manipulation rule (Manipulation Set 4) for Virgin Media SIP Trunk. This rule is applied to all SIP request messages sent to the Virgin Media SIP Trunk. This rule removes port from the host part of the SIP From Header, according to the Virgin Media request.

Parameter	Value
Index	2
Name	Remove Port from From Header
Manipulation Set ID	4
Message Type	Any.Request
Action Subject	Header.From.URL.Host.Port
Action Type	Modify
Action Value	'0'

Figure 4-36: Configuring SIP Message Manipulation Rule 2 (for Virgin Media SIP Trunk)

Message Manipulations [Remove Port from From Header]

GENERAL

Index

2

Name

Remove Port from From Header

Manipulation Set ID

4

Row Role

Use Current Condition

MATCH

Message Type

Any.Request

Condition

ACTION

Action Subject

Header.From.URL.Host.Port

Action Type

Modify

Action Value

'0'

Cancel

APPLY

5. Configure another manipulation rule (Manipulation Set 4) for Virgin Media SIP Trunk. This rule is applied to all SIP request messages sent to the Virgin Media SIP Trunk. This rule replaces the SIP Contact Header with the value from the SIP From Header, according to Virgin Media request.

Parameter	Value
Index	3
Name	Change Contact
Manipulation Set ID	4
Message Type	Any.Request
Action Subject	Header.Contact.URL
Action Type	Modify
Action Value	Header.From.URL

Figure 4-37: Configuring SIP Message Manipulation Rule 3 (for Virgin Media SIP Trunk)

Message Manipulations [Change Contact]

GENERAL		ACTION	
Index	3	Action Subject	Header.Contact.URL Editor
Name	Change Contact	Action Type	Modify
Manipulation Set ID	4	Action Value	Header.From.URL Editor
Row Role	Use Current Condition		

MATCH	
Message Type	Any.Request Editor
Condition	Editor

Cancel **APPLY**

6. Configure another manipulation rule (Manipulation Set 4) for Virgin Media SIP Trunk. This rule is applied to all SIP request messages sent to the Virgin Media SIP Trunk. This rule adds UPDATE and PRACK methods to the SIP Allow Header, according to Virgin Media request.

Parameter	Value
Index	4
Name	Add UPDATE and PRACK to Allow
Manipulation Set ID	4
Message Type	Any.Request
Condition	Header.Allow regex (.*)
Action Subject	Header.Allow
Action Type	Modify
Action Value	'UPDATE,PRACK,' +\$1

Figure 4-38: Configuring SIP Message Manipulation Rule 4 (for Virgin Media SIP Trunk)

Message Manipulations [Add UPDATE and PRACK to Allow]

GENERAL

Index
4
Name
Add UPDATE and PRACK to Allow
Manipulation Set ID
4
Row Role
Use Current Condition

ACTION

Action Subject
Header.Allow
Action Type
Modify
Action Value
'UPDATE,PRACK,' +\$1

MATCH

Message Type
Any.Request
Condition
Header.Allow regex (.*)

Cancel
APPLY

7. Configure another manipulation rule (Manipulation Set 4) for Virgin Media SIP Trunk. This rule is applied to all SIP request messages sent to the Virgin Media SIP Trunk. This rule removes a=maxptime header from the SDP part of the message, according to the Virgin Media request.

Parameter	Value
Index	5
Name	Remove a=maxptime from SDP
Manipulation Set ID	4
Message Type	Any.Request
Condition	Body.sdp regex (.*)(a=maxptime:200)(.*)
Action Subject	Body.sdp
Action Type	Modify
Action Value	\$1+\$3

Figure 4-39: Configuring SIP Message Manipulation Rule 5 (for Virgin Media SIP Trunk)

Message Manipulations [Remove a=maxptime from SDP]

GENERAL		ACTION	
Index	5	Action Subject	Body.sdp Editor
Name	Remove a=maxptime from SDP	Action Type	Modify
Manipulation Set ID	4	Action Value	\$1+\$3 Editor
Row Role	Use Current Condition		

MATCH	
Message Type	Any.Request Editor
Condition	Body.sdp regex (.*)(a=maxptime:200)(.*) Editor

Cancel [APPLY](#)

8. Configure another manipulation rule (Manipulation Set 4) for Virgin Media SIP Trunk. This rule is applied on all SIP request messages with SIP P-Asserted-Identity header, sent to the Virgin Media SIP Trunk IP Group. This rule replaces the user part of the SIP P-Asserted-Identity header with the pre-defined 'pilot' number.



Note: Adapt the pre-defined 'pilot' number according to your environment dial plan.

Parameter	Value
Index	6
Name	For test 27
Manipulation Set ID	4
Message Type	Any.Request
Condition	Header.P-Asserted-Identity exists
Action Subject	Header.P-Asserted-Identity.URL.User
Action Type	Modify
Action Value	'+441183374122'

Figure 4-40: Configuring SIP Message Manipulation Rule 6 (for Virgin Media SIP Trunk)

Message Manipulations [For test 27]

GENERAL

Index

6

Name

For test 27

Manipulation Set ID

4

Row Role

Use Current Condition

MATCH

Message Type

Any.Request

Condition

Header.P-Asserted-Identity exists

ACTION

Action Subject

Header.P-Asserted-Identity.URL.User

Action Type

Modify

Action Value

'+441183374122'

Cancel

APPLY

Figure 4-41: Example of Configured SIP Message Manipulation Rules

Message Manipulations (7)								
+ New Edit Insert ↑ ↓ 🗑️ ⏪ ⏩ Page 1 of 1 ⏪ ⏩ Show 10 records per page								
INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Remove PAI	1			Header.P-Asserted-	Remove		Use Current Condi
1	Remove Privacy	1		Header.Privacy exists	Header.Privacy	Remove		Use Current Condi
2	Remove Port from	4	Any.Request		Header.From.URL	Modify	'0'	Use Current Condi
3	Change Contact	4	Any.Request		Header.Contact.UR	Modify	Header.From.URL	Use Current Condi
4	Add UPDATE and P	4	Any.Request	Header.Allow regex	Header.Allow	Modify	'UPDATE,PRACK,' +'	Use Current Condi
5	Remove a=maxptin	4	Any.Request	Body.sdp regex (.*)	Body.sdp	Modify	\$1+\$3	Use Current Condi
6	For test 27	14	Any.Request	Header.P-Asserted-	Header.P-Asserted-	Modify	'+441183374122'	Use Current Condi

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 Virgin Media SIP Trunk IP Group, as well as the Teams Direct Routing IP Group. These rules are specifically required to enable proper interworking between Virgin Media SIP Trunk and Teams Direct Routing. Refer to the *User's Manual* for further details regarding 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 rule removes the SIP P-Asserted-Identity Header.	
1	This rule applies to messages sent to the Teams IP Group. This rule removes the SIP Privacy Header in all messages, except for calls with presentation restrictions.	
2	This rule is applied to all SIP request messages sent to the Virgin Media SIP Trunk. This rule removes port from the host part of the SIP From Header.	According to Virgin Media request
3	This rule is applied to all SIP request messages sent to the Virgin Media SIP Trunk. This rule replaces the SIP Contact Header with the value from the SIP From Header.	According to Virgin Media request
4	This rule is applied to all SIP request messages sent to the Virgin Media SIP Trunk. This rule adds UPDATE and PRACK methods to the SIP Allow Header.	According to Virgin Media request
5	This rule is applied to all SIP request messages sent to the Virgin Media SIP Trunk. This rule removes a=maxptime header from the SDP part of the message.	According to Virgin Media request
6	This rule is applied on all SIP request messages with SIP P-Asserted-Identity header, sent to the Virgin Media SIP Trunk IP Group. This rule replaces the user part of the SIP P-Asserted-Identity header with the pre-defined 'pilot' number.	

9. Assign Manipulation Set ID 1 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 4-42: Assigning Manipulation Set to the Teams Direct Routing IP Group

IP Groups [Teams]

SRD #0 [DefaultSRD]

GENERAL

Index 3

Name Teams

Topology Location Up

Type Server

Proxy Set #3 [Teams] View

IP Profile #2 [Teams] View

Media Realm #1 [Teams] View

Internal Media Realm -- View

Contact User

SIP Group Name 195.189.192.156

QUALITY OF EXPERIENCE

QoE Profile -- View

Bandwidth Profile -- View

MESSAGE MANIPULATION

Inbound Message Manipulation Set 1

Outbound Message Manipulation Set -1

Message Manipulation User-Defined String 1

Message Manipulation User-Defined String 2

Proxy Keep-Alive using IP Group settings Enable

Cancel APPLY

- d. Click **Apply**.

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

Figure 4-43: Assigning Manipulation Set 4 to the Virgin Media SIP Trunk A IP Group

The screenshot shows the 'IP Groups [VM Trunk A]' configuration window. At the top, there is an 'SRD' dropdown menu set to '#0 [DefaultSRD]'. The window is divided into two main sections: 'GENERAL' and 'QUALITY OF EXPERIENCE'. The 'GENERAL' section includes fields for Index (1), Name (VM Trunk A), Topology Location (Down), Type (Server), Proxy Set (#1 [VM Trunk A]), IP Profile (#1 [VM]), Media Realm (#0 [SIPTrunk]), Internal Media Realm (--), Contact User, and SIP Group Name (81.97.95.188). The 'QUALITY OF EXPERIENCE' section includes QoE Profile and Bandwidth Profile dropdowns, both set to '--'. Below these is the 'MESSAGE MANIPULATION' section, which contains 'Inbound Message Manipulation Set' (-1), 'Outbound Message Manipulation Set' (4), 'Message Manipulation User-Defined String 1', 'Message Manipulation User-Defined String 2', and 'Proxy Keep-Alive using IP Group settings' (Enable). At the bottom right, there are 'Cancel' and 'APPLY' buttons.

- d. Click **Apply**.
- e. Repeat the same procedure for the Virgin Media SIP Trunk B IP Group.

4.19 Configure Registration Accounts

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the Virgin Media SIP Trunk on behalf of Teams Direct Routing. The Virgin Media SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is Teams Direct Routing IP Group and the Serving IP Group is Virgin Media 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 Virgin Media, for Teams, serving by VM Trunk A:

Parameter	Value
Served IP Group	Teams
Application Type	SBC
Serving IP Group	VM Trunk A
Register	No
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

4. Click **Apply**.
5. Configure the account according to the provided information from Virgin Media, for Teams, serving by Virgin Media Trunk B:

Parameter	Value
Served IP Group	Teams
Application Type	SBC
Serving IP Group	VM Trunk B
Register	No
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

6. Click **Apply**.
7. Configure the account according to the provided information from Virgin Media for Fax ATA Device, serving by VM Trunk A:

Parameter	Value
Served IP Group	MP-Fax
Application Type	SBC
Serving IP Group	VM Trunk A
Register	No
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

8. Click **Apply**.
9. Configure the account according to the provided information from Virgin Media for Fax ATA Device, serving by VM Trunk B:

Parameter	Value
Served IP Group	MP-Fax
Application Type	SBC
Serving IP Group	VM Trunk B
Register	No
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

Figure 4-44: Configuring a SIP Registration Accounts

Accounts (4)									
+ New Edit Action Page 1 of 1 Show 10 records per page									
INDEX	APPLICATION TYPE	SERVED TRUNK GROUP	SERVED IP GROUP	SERVING IP GROUP	USER NAME	PASSWORD	HOST NAME	REGISTER	CONTACT USER
0	SBC	-1	S4B	VM Trunk A	virginpbx01_011	*		No	
1	SBC	-1	S4B	VM Trunk B	virginpbx01_011	*		No	
2	SBC	-1	MP-Fax	VM Trunk A	virginpbx01_011	*		No	
3	SBC	-1	MP-Fax	VM Trunk B	virginpbx01_011	*		No	

10. Click **Apply**.

4.20 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

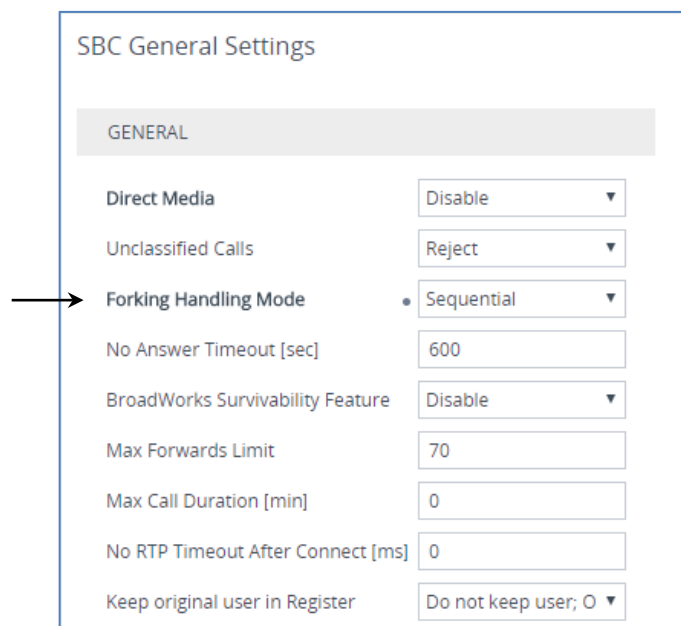
4.20.1 Configure Call Forking Mode

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 4-45: Configuring Forking Mode



The screenshot shows the 'SBC General Settings' configuration page. A tab labeled 'GENERAL' is selected. The 'Forking Handling Mode' is set to 'Sequential' via a dropdown menu, which is highlighted by an arrow from the left. 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**.

4.20.2 Configure SBC Max Retransmission Time

This section describes how to configure the SBC's maximum retransmission attempts. In this case, the SBC attempts to locate an alternative route for the call after three attempts.

➤ **To configure SIP SBC Max Retransmission Time:**

1. Open the Transport Settings (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Transport Settings**).
2. Click **New**.
3. In the 'SIP Maximum RTX' field, enter **3** (retransmission will be stopped after 3 attempts).

Figure 4-46: SBC Max Retransmission Time

Transport Settings

GENERAL	TCP CONNECTION
SIP NAT Detection: Enable	TCP/TLS Connection Reuse: Enable
Enable SIPs: Disable	TCP Timeout: 0
SIP Transport Type: UDP	Reliable Connection Persistent Mode: Disable
ENUM Resolution: e164.arpa	
SIP 408 Response upon non-INVITE: Enable	
DNS Query Type: A-Record	

SBC SETTINGS	RETRANSMISSION
WebSocket Keep-Alive Period [sec]: 0	SIP T1 Retransmission Timer [msec]: 500
	SIP T2 Retransmission Timer [msec]: 4000
	SIP Maximum RTX: 3

4. Click **Apply**.

4.20.3 Configure Session Expires and Broken Connection Timeouts

This section describes how to configure SBC's Session Expires and broken connection timeouts. Increasing broken connection timeout is required for proper behavior during fax transmission.

➤ **To configure SIP Session Expires and Broken Connection Timeouts:**

1. Open the SIP Definitions General Settings (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **SIP Definitions General Settings**).
2. In the 'Minimum Session-Expires [sec]' field, enter **600**.
3. In the 'Session-Expires [sec]' field, enter **1800**.
4. In the 'Broken Connection Timeout' field, enter **1000**.

Figure 4-47: SBC Session Expires and Broken Connection Timeouts

The screenshot shows the 'SIP Definitions General Settings' configuration page. It is divided into several sections:

- GENERAL**: Includes 'Send Reject (503) upon Overload' (Enable), 'Retry-After Time' (0), 'Fake Retry After' (0), 'Remote Management by SIP NOTIFY' (Disable), and 'X-Channel Header' (Disable).
- GATEWAY SETTINGS**: Includes 'PRACK Mode' (Supported), 'Early 183' (Disable), '183 Message Behavior' (Progress), '3xx Behavior' (Forward), 'Call Transfer using re-INVITEs' (Disable), 'First Call Ringback Tone ID' (-1), and 'Delayed Offer' (Disable).
- SBC SETTINGS**: Includes 'SUBSCRIBE Trying' (Disable), 'Minimum Session-Expires [sec]' (600), and 'Session-Expires [sec]' (1800).
- GATEWAY SESSION EXPIRES**: Includes 'Session-Expires Time' (0), 'Minimum Session-Expires' (90), 'Session Expires Method' (re-INVITE), and 'Session Expires Disconnect Time' (32).
- DISCONNECT SUPERVISION**: Includes 'Broken Connection Mode' (Disconnect) and 'Broken Connection Timeout [100 msec]' (1000).

Arrows indicate the configuration steps: from 'Minimum Session-Expires [sec]' in SBC SETTINGS to 'Session-Expires [sec]', and from 'Broken Connection Timeout [100 msec]' in DISCONNECT SUPERVISION.

5. Click **Apply**.

4.20.4 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 this 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.

This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the SBC, corresponding to the Web-based configuration as described in Section 4 on page 21, is shown below:



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

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

;Board: M800B
;Board Type: 72
;Serial Number: 5299378
;Software Version: 7.20A.258.457
;DSP Software Version: 5014AE3_R => 723.11
;Board IP Address: 10.15.77.55
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;CPU: Cavium Networks Octeon V0.1 @ 500Mhz, total 2 cores, 2 cpus, 1
sockets
;Cores mapping:
;core #0, on cpu #0, on socket #0
;core #1, on cpu #1, on socket #0
;Memory: 512 MB
;Flash size: 64 MB
;Num of DSP Cores: 3
;Num of physical LAN ports: 4
;;Key features;;Board Type: M800B ;Coders: G723 G729 G728 NETCODER GSM-
FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711 MS_RTA_NB
MS_RTA_NB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB OPUS_WB EVS
;ElTrunks=1 ;TlTrunks=1 ;FXSPorts=4 ;FXOPorts=0 ;BRITrunks=4 ;Channel
Type: DspCh=30 IPMediaDspCh=30 ;HA ;QOE features: VoiceQualityMonitoring
MediaEnhancement ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;DSP Voice features: RTCP-XR ;IP Media: Conf VXML
;DATA features: NQM ;Control Protocols: MSFT FEU=100 TestCall=100
SIPRec=10 CODER-TRANSCODING=100 SBC-SIGNALING=100 ELIN HttpProxy TEAMS
MGCP SIP SBC=100 ;Default features;;Coders: G711 G726;

;----- HW components -----
;
; Slot # : Module type : # of ports
;-----
; 1 : FALC56 : 1
; 2 : FXS : 4
; 3 : BRI : 4
;-----

;USB Port 1: Empty
;USB Port 2: Empty
;-----

[SYSTEM Params]
```

```

SyslogServerIP = 10.15.77.100
EnableSyslog = 1
NTPServerUTCOffset = 7200
HALocalMAC = '00908f50dcb2'
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.15.27.1'
Tr069VerifyCommonName = 0
SBCWizardFilename = 'templates4.zip'

[BSP Params]

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

[Analog Params]

[ControlProtocols Params]

AdminStateLockControl = 0

[PSTN Params]

V5ProtocolSide = 0

[Voice Engine Params]

BrokenConnectionEventTimeout = 1000
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
SIPMAXRTX = 3
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCMINSE = 600
SBCPREFERENCESENTRYMODE = 1
MEDIACDRREPORTLEVEL = 1
SBCFORKINGHANDLINGMODE = 1
SBCSESSIONEXPIRES = 1800
ANSWERDETECTORCMD = 10486144

[IPsec Params]

```

```

[SNMP Params]

[ PhysicalPortsTable ]

FORMAT Index = Port, Mode, SpeedDuplex, PortDescription, GroupMember;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2";

[ \PhysicalPortsTable ]

[ EtherGroupTable ]

FORMAT Index = Group, Mode, Member1, Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]

[ DeviceTable ]

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

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT Index = ApplicationTypes, InterfaceMode, IPAddress, PrefixLength,
Gateway, InterfaceName, PrimaryDNSServerIPAddress,
SecondaryDNSServerIPAddress, UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.77.55, 16, 10.15.0.1, "LAN_IF",
10.15.27.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.156, 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,
"e4064f90b5b26631d46fbcd79f2b7a0", ".fc";

```

```

WebUsers 1 = "User",
"$1$Cj46OmhtN3ElJio1cSQnfXh4Ii5+Jn4ZRBQRHR0fHx4bTB9ITE8aVgRQVQUGAAEPXvKCD
w0GWSEgIHN0dHB2LHE=", 1, 0, 5, -1, 15, 60, 50,
"c26a27dd91a886b99de5e81b9a736232", "";

[ \WebUsers ]

[ TLSContexts ]

FORMAT Index = Name, TLSVersion, DTLSVersion, ServerCipherString,
ClientCipherString, ServerCipherTLS13String, ClientCipherTLS13String,
KeyExchangeGroups, RequireStrictCert, TlsRenegotiation,
MiddleboxCompatMode, OcsEnable, OcsServerPrimary, OcsServerSecondary,
OcsServerPort, OcsDefaultResponse, DHKeySize;
TLSContexts 0 = "default", 0, 0, "DEFAULT", "DEFAULT",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56", "X25519:P-256:P-384:X448", 0, 1, 0, 0, 0.0.0.0, 0.0.0.0, 2560, 0,
2048;
TLSContexts 1 = "Teams", 4, 0, "DEFAULT", "DEFAULT",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56",
"TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA2
56", "X25519:P-256:P-384:X448", 0, 1, 0, 0, 0.0.0.0, 0.0.0.0, 2560, 0,
2048;

[ \TLSContexts ]

[ AudioCodersGroups ]

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

[ \AudioCodersGroups ]

[ AllowedAudioCodersGroups ]

FORMAT Index = Name;
AllowedAudioCodersGroups 0 = "VM 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,

```

```

SBCSendMultipleDTMFMethods, SBCAssertIdentity,
AMDSensitivityParameterSuit, AMDSensitivityLevel, AMDMaxGreetingTime,
AMDMaxPostSilenceGreetingTime, SBCDiversioMode, SBCHistoryInfoMode,
EnableQSIGTunneling, SBCFaxCodersGroupName, SBCFaxBehavior,
SBCFaxOfferMode, SBCFaxAnswerMode, SbcPrackMode, SBCSessionExpiresMode,
SBCRemoteUpdateSupport, SBCRemoteReinviteSupport,
SBCRemoteDelayedOfferSupport, SBCRemoteReferBehavior,
SBCRemote3xxBehavior, SBCRemoteMultiple18xSupport,
SBCRemoteEarlyMediaResponseType, SBCRemoteEarlyMediaSupport,
EnableSymmetricMKI, MKISize, SBCEnforceMKISize, SBCRemoteEarlyMediaRTP,
SBCRemoteSupportsRFC3960, SBCRemoteCanPlayRingback, EnableEarly183,
EarlyAnswerTimeout, SBC2833DTMFPayloadType, SBCUserRegistrationTime,
ResetSRTPStateUponRekey, AmdMode, SBCReliableHeldToneSource,
GenerateSRTPKeys, SBCPlayHeldTone, SBCRemoteHoldFormat,
SBCRemoteReplacesBehavior, SBCSDPptimeAnswer, SBCPreferredPTime,
SBCUseSilenceSupp, SBCRTPRedundancyBehavior, SBCPlayRBTToTransferee,
SBCRTCPMode, SBCJitterCompensation, SBCRemoteRenegotiateOnFaxDetection,
JitterBufMaxDelay, SBCUserBehindUdpNATRegistrationTime,
SBCUserBehindTcpNATRegistrationTime, SBCSDPHandlerTCPAttribute,
SBCRemoveCryptoLifetimeInSDP, SBCIceMode, SBCRTCPMux,
SBCMediaSecurityMethod, SBCHandleXDetect, SBCRTCPFeedback,
SBCRemoteRepresentationMode, SBCKeepVIAHeaders, SBCKeepRoutingHeaders,
SBCKeepUserAgentHeader, SBCRemoteMultipleEarlyDialogs,
SBCRemoteMultipleAnswersMode, SBCDirectMediaTag,
SBCAdaptRFC2833BWToVoiceCoderBW, CreatedByRoutingServer,
SBCFaxReroutingMode, SBCMaxCallDuration, SBCGenerateRTP,
SBCISUPBodyHandling, SBCISUPVariant, SBCVoiceQualityEnhancement,
SBCMaxOpusBW, SBCEnhancedPlc, LocalRingbackTone, LocalHeldTone,
SBCGenerateNoOp, SBCRemoveUnknownCrypto, SBCMultipleCoders, DataDiffServ,
SBCMSRPreinviteUpdateSupport, SBCMSRPOfferSetupRole, SBCMSRPEmpMsg,
SBCRenumberMID;

IpProfile 1 = "VM", 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, "", "VM
Allowed Coders", "", 0, 2, 0, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, "", 0, 0,
1, 3, 3, 2, 2, 1, 3, 2, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1,
0, 0, 0, 1, 0, 0, 2, 2, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1,
-1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0, 0, 0,
1, 2, 0, 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, "", "", 0, 0, "",
"", "", 0, 1, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 0,
1, 0, 3, 2, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 3, 1,
0, 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, 0, -1, -1, 0, 0, 0, 0, 1, 2, 0, 0;

[ \IpProfile ]

[ CpMediaRealm ]

FORMAT Index = MediaRealmName, IPv4IF, IPv6IF, RemoteIPv4IF,
RemoteIPv6IF, PortRangeStart, MediaSessionLeg, PortRangeEnd,
TCPPortRangeStart, TCPPortRangeEnd, IsDefault, QoeProfile, BWProfile,
TopologyLocation, UsedByRoutingServer;

CpMediaRealm 0 = "SIPTrunk", "WAN_IF", "", "", "", 6000, 100, 6999, 0, 0,
0, "", "", 0, 0;

CpMediaRealm 1 = "Teams", "WAN_IF", "", "", "", 7000, 100, 7999, 0, 0, 0,
"", "", 1, 0;

CpMediaRealm 2 = "MRLan", "LAN_IF", "", "", "", 6000, 100, 6999, 0, 0, 0,
"", "", 0, 0;

[ \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 = "SIPTrunk", "WAN_IF", "", 2, 5060, 0, 0, 0, "", 0,
"DefaultSRD", "", "default", -1, 0, 0, -1, 0, "SIPTrunk", 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, "Teams", 0, -1, -1, -1, 0, 1,
"", "", -1;
SIPInterface 2 = "SI-LAN", "LAN_IF", "", 2, 5060, 5060, 5061, 0, "", 0,
"DefaultSRD", "", "SPOT", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1, 0,
0, "", "", -1;

[ \SIPInterface ]


[ ProxySet ]
```

```

FORMAT Index = ProxyName, EnableProxyKeepAlive, ProxyKeepAliveTime,
ProxyLoadBalancingMethod, IsProxyHotSwap, SRDName, ClassificationInput,
TLSContextName, ProxyRedundancyMode, DNSResolveMethod,
KeepAliveFailureResp, GWIPv4SIPInterfaceName, SBCIPv4SIPInterfaceName,
GWIPv6SIPInterfaceName, SBCIPv6SIPInterfaceName, MinActiveServersLB,
SuccessDetectionRetries, SuccessDetectionInterval,
FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "SIPTrunk", "", "", 1, 1, 10, -1;
ProxySet 1 = "VM Trunk A", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1,
"503", "", "SIPTrunk", "", "", 1, 1, 10, -1;
ProxySet 2 = "VM Trunk B", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1,
"503", "", "SIPTrunk", "", "", 1, 1, 10, -1;
ProxySet 3 = "Teams", 1, 60, 2, 1, "DefaultSRD", 0, "Teams", -1, -1, "",
"", "Teams", "", "", 1, 1, 10, -1;
ProxySet 4 = "MP-Fax", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"SI-LAN", "", "", 1, 1, 10, -1;

[ \ProxySet ]

[ SBCAltRoutingReasonsSet ]

FORMAT Index = Name, Description;
SBCAltRoutingReasonsSet 0 = "503 Response", "";

[ \SBCAltRoutingReasonsSet ]

[ IPGroup ]

FORMAT Index = Type, Name, ProxySetName, VoiceAIconnector, 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, DTLSContext,
CreatedByRoutingServer, UsedByRoutingServer, SBCOperationMode,
SBCRouteUsingRequestURIPort, SBCKeepOriginalCallID, TopologyLocation,
SBCDialPlanName, CallSetupRulesSetId, Tags, SBCUserStickiness,
UserUDPPortAssignment, AdmissionProfile, ProxyKeepAliveUsingIPG,
SBCAltRouteReasonsSetName, TeamsLocalMediaOptimization,
TeamsLocalMOInitialBehavior, SIPSourceHostName, TeamsDirectRoutingMode;
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, 0, "", 0;
IPGroup 1 = 0, "VM Trunk A", "VM Trunk A", "", "81.97.95.188", "", -1, 0,
"DefaultSRD", "SIPTrunk", "", 1, "VM", -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, "", 1, "503 Response", 0, 0, "", 0;
IPGroup 2 = 0, "VM Trunk B", "VM Trunk B", "", "82.14.171.242", "", -1,
0, "DefaultSRD", "SIPTrunk", "", 1, "VM", -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, "", 1, "503 Response", 0, 0, "", 0;
IPGroup 3 = 0, "Teams", "Teams", "", "195.189.192.156", "", -1, 0,
"DefaultSRD", "Teams", "", 0, "Teams", -1, 1, -1, 0, 0, "", -1, "", 0, -
1, -1, "int-sbcl.audctrunk.aceducation.info", "", "$1$gQ=", 0, "", "",
1, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 1, "", -1, "", 0, 0, "", 1,
"", 0, 0, "", 0;

```

```

IPGroup 4 = 0, "MP-Fax", "MP-Fax", "", "", "", -1, 0, "DefaultSRD",
"MRlan", "", 1, "", -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, 0, "", 0;

[ \IPGroup ]

[ ProxyIp ]

FORMAT Index = ProxySetId, ProxyIpIndex, IpAddress, TransportType,
Priority, Weight;
ProxyIp 0 = "1", 0, "81.97.95.188:5060", 0, 0, 0;
ProxyIp 1 = "2", 0, "82.14.171.242:5060", 0, 0, 0;
ProxyIp 2 = "3", 0, "sip.pstnhub.microsoft.com:5061", 2, 1, 1;
ProxyIp 3 = "3", 1, "sip2.pstnhub.microsoft.com:5061", 2, 2, 1;
ProxyIp 4 = "3", 2, "sip3.pstnhub.microsoft.com:5061", 2, 3, 1;
ProxyIp 5 = "4", 0, "10.15.77.14:5060", 0, 0, 0;

[ \ProxyIp ]

[ Account ]

FORMAT Index = AccountName, ServedTrunkGroup, ServedIPGroupName,
ServingIPGroupName, Username, Password, HostName, ContactUser, Register,
RegistrarStickiness, RegistrarSearchMode, RegEventPackageSubscription,
ApplicationType, RegByServedIPG, UDPPortAssignment,
ReRegisterOnInviteFailure;
Account 0 = "Teams to VM Trunk A", -1, "Teams", "VM Trunk A",
"virginpbx01_01183374120", "$1$+7+4zc3ONzJEOj1BMD8+SzhKND46", "", "", 0,
0, 0, 0, 2, 0, 0, 0;
Account 1 = "Teams to VM Trunk B", -1, "Teams", "VM Trunk B",
"virginpbx01_01183374120", "$1$+7+4zc3ONzJEOj1BMD8+SzhKND46", "", "", 0,
0, 0, 0, 2, 0, 0, 0;
Account 2 = "MP-Fax to VM Trunk A", -1, "MP-Fax", "VM Trunk A",
"virginpbx01_01183374120", "$1$+7+4zc3ONzJEOj1BMD8+SzhKND46", "", "", 0,
0, 0, 0, 2, 0, 0, 0;
Account 3 = "MP-Fax to VM Trunk B", -1, "MP-Fax", "VM Trunk B",
"virginpbx01_01183374120", "$1$+7+4zc3ONzJEOj1BMD8+SzhKND46", "", "", 0,
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 ]

[ IPGroupSet ]

FORMAT Index = Name, Policy, Tags;
IPGroupSet 0 = "Virgin Media", 2, "";

```

```
[ \IPGroupSet ]

[ 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,
ModifiedDestUserName, SrcTags, IPGroupSetName, RoutingTagName,
InternalAction;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*, *, *, *, 6, "", "Any", 0, -1, 13, "", "", "", 0, -1, 0, 0, "",
"", "", "", "", "default", "Reply (Response='200')";
IP2IPRouting 1 = "Refer from Teams", "Default_SBCRoutingPolicy", "Any",
"*, *, *, *, 0, "", "Teams", 2, -1, 2, "Teams", "", "", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 2 = "Teams to SIP Trunk", "Default_SBCRoutingPolicy",
"Teams", "*", *, *, *, 0, "", "Any", 0, -1, 11, "", "", "", 0, -1,
0, 0, "", "", "", "", "Virgin Media", "default", "";
IP2IPRouting 3 = "MP-Fax to SIP Trunk", "Default_SBCRoutingPolicy", "MP-
Fax", "*", *, *, *, 0, "", "Any", 0, -1, 11, "", "", "", 0, -1, 0,
0, "", "", "", "", "Virgin Media", "default", "";
IP2IPRouting 4 = "SIP Trunk to MP-Fax", "Default_SBCRoutingPolicy",
"Any", "*", *, *, "+441183374125", "*", 0, "", "Any", 0, -1, 0, "MP-Fax",
"", "", 0, -1, 0, 0, "", "", "", "", "default", "";
IP2IPRouting 5 = "SIP Trunk to Teams", "Default_SBCRoutingPolicy", "Any",
"*, *, *, *, 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-
sbcl.audctrunk.aceducation.info", 1, "Teams", "", "", 0, "default";

[ \Classification ]

[ 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 = "To Emergency do nothing",
"Default_SBCRoutingPolicy", 0, "Any", "VM Trunk A", "*", *,
"[999,112,18000]", "*", *, "", 0, "Any", 0, 1, 0, 0, 255, "", "", 0,
"", "";
IPOutboundManipulation 1 = "To Emergency do nothing",
"Default_SBCRoutingPolicy", 0, "Any", "VM Trunk B", "*", *,
```

```

"[999,112,18000]", "*", "*", "", 0, "Any", 0, 1, 0, 0, 255, "", "", 0,
"", "";

IPOutboundManipulation 2 = "To Emergency strip +",
"Default_SBCRoutingPolicy", 0, "Any", "VM Trunk A", "*", "*",
"[+999,+112,+18000]", "*", "*", "", 0, "Any", 0, 1, 1, 0, 255, "", "", 0,
"", "";

IPOutboundManipulation 3 = "To Emergency strip +",
"Default_SBCRoutingPolicy", 0, "Any", "VM Trunk B", "*", "*",
"[+999,+112,+18000]", "*", "*", "", 0, "Any", 0, 1, 1, 0, 255, "", "", 0,
"", "";

IPOutboundManipulation 4 = "Add +", "Default_SBCRoutingPolicy", 0, "Any",
"Any", "*", "*", "[1-9]", "*", "*", "", 0, "Any", 0, 1, 0, 0, 255, "+",
"", 0, "", "";

[ \IPOutboundManipulation ]

[ MessageManipulations ]

FORMAT Index = ManipulationName, ManSetID, MessageType, Condition,
ActionSubject, ActionType, ActionValue, RowRole;
MessageManipulations 0 = "Remove PAI", 1, "", "", "Header.P-Asserted-
Identity", 1, "", 0;
MessageManipulations 1 = "Remove Privacy Header", 1, "", "Header.Privacy
exists And Header.From.URL !contains 'anonymous'", "Header.Privacy", 1,
"", 0;
MessageManipulations 2 = "Remove Port from From Header", 4,
"Any.Request", "", "Header.From.URL.Host.Port", 2, "'0'", 0;
MessageManipulations 3 = "Change Contact", 4, "Any.Request", "",
"Header.Contact.URL", 2, "Header.From.URL", 0;
MessageManipulations 4 = "Add UPDATE and PRACK to Allow", 4,
"Any.Request", "Header.Allow regex (.*)", "Header.Allow", 2,
"'UPDATE,PRACK,' +$1", 0;
MessageManipulations 5 = "Remove a=maxptime from SDP", 4, "Any.Request",
"Body.sdp regex (.*) (a=maxptime:200) (.*)", "Body.sdp", 2, "$1+$3", 0;
MessageManipulations 6 = "For test 27", 14, "Any.Request", "Header.P-
Asserted-Identity exists", "Header.P-Asserted-Identity.URL.User", 2,
"'441183374122'", 0;

[ \MessageManipulations ]

[ GwRoutingPolicy ]

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

[ \GwRoutingPolicy ]

[ 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 = "Smapp", "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 = "VM Allowed Coders", 0, 1, "";

[ \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 6 = "AudioCodersGroups_0", 1, 2, 2, 90, -1, 0, "";

[ \AudioCoders ]

[ IPGroupSetMember ]
```

```
FORMAT Index = IPGroupSetId, IPGroupSetMemberIndex, IPGroupName, Weight;  
IPGroupSetMember 0 = "0", 0, "VM Trunk A", 1;  
IPGroupSetMember 1 = "0", 1, "VM Trunk B", 1;
```

```
[ \IPGroupSetMember ]
```

```
[ SBCAltRoutingReasonsList ]
```

```
FORMAT Index = SBCAltRoutingReasonsSet, SBCAltRouteIndex,  
ReleaseCauseCode;  
SBCAltRoutingReasonsList 0 = "503 Response", 0, 503;
```

```
[ \SBCAltRoutingReasonsList ]
```

B Configuring Analog Devices (ATAs) for Fax Support

This section describes how to configure the analog device entity to route its calls to the AudioCodes SBC for supporting faxes. The analog device entity must be configured to send all calls to the AudioCodes SBC.



Note: The configuration described in this section is for ATA devices configured for AudioCodes MP-11x series.

B.1 Step 1: Configure the Endpoint Phone Number Table

The 'Endpoint Phone Number Table' page allows you to activate the MP-11x ports (endpoints) by defining telephone numbers. The configuration below uses the example of ATA destination phone number "+441183374125" with all routing directed to the SBC device (10.15.77.77).

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

1. Open the Endpoint Phone Number Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Hunt Group** sub-menu > **Endpoint Phone Number**).

Figure B-1: Endpoint Phone Number Table Page

Endpoint Phone Number Table				
	Channel(s)	Phone Number	Hunt Group ID	Tel Profile ID
1	1	+441183374125		0
2	2			0
3	3			0
4	4			0

B.2 Step 2: Configure Tel to IP Routing Table

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

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

1. Open the Tel to IP Routing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Routing** sub-menu > **Tel to IP Routing**).

Figure B-2: Tel to IP Routing Page

	Src. Hunt Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address	Port	Transport Type	Dest. IP Group ID	IP Profile ID	Cost Group ID
1	*	*	*	10.15.77.77		Not Configured	-1	0	None
2						Not Configured	-1		None
3						Not Configured	-1		None

B.3 Step 3: Configure Coders Table

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

➤ **To configure MP-11x coders:**

1. Open the Coders page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** sub-menu > **Coders**).

Figure B-3: Coders Table Page

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711A-law	20	64	8	Disabled
G.711U-law	20	64	0	Disabled

B.4 Step 4: Configure SIP UDP Transport Type and Fax Signaling Method

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

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

1. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).

Figure B-4: SIP General Parameters Page

SIP General Parameters	
Basic Parameter List ▲	
▼ SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Supported ▼
Channel Select Mode	By Dest Phone Number ▼
Enable Early Media	Disable ▼
183 Message Behavior	Progress ▼
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	re-INVITE ▼
Asserted Identity Mode	Disabled ▼
Fax Signaling Method	T.38 Relay ▼
Detect Fax on Answer Tone	Initiate T.38 on Preamble ▼
SIP Transport Type	UDP ▼
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPs	Disable ▼
Enable TCP Connection Reuse	Enable ▼
TCP Timeout	0
SIP Destination Port	5060

2. From the 'Fax Signaling Method' drop-down list, select **G.711 Transport** for G.711 fax support and select **T.38 Relay** for T.38 fax support.
3. From the 'SIP Transport Type' drop-down list, select **UDP**.
4. In the 'SIP UDP Local Port' field, enter **5060** (corresponding to the SBC UDP transmitting port configuration).
5. In the 'SIP Destination Port', enter **5060** (corresponding to the SBC UDP listening port configuration).

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>

©2021 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-39344

