

Microsoft® Teams Direct Routing Enterprise Model and Vodafone IP Anlagen-Anschluss using AudioCodes Mediant™ SBC

Version 7.4



Microsoft Partner
Gold Communications



Table of Contents

Notice	iv
Security Vulnerabilities	iv
WEEE EU Directive	iv
Customer Support	iv
Stay in the Loop with AudioCodes	iv
Abbreviations and Terminology.....	iv
Document Revision Record.....	iv
Documentation Feedback.....	iv
1 Introduction	1
1.1 Intended Audience	1
1.2 About Microsoft Teams Direct Routing	1
1.3 About AudioCodes SBC Product Series	1
2 Component Information	2
2.1 AudioCodes SBC Version	2
2.2 Vodafone IP Anlagen-Anschluss Interface Version	2
2.3 Microsoft Teams Direct Routing Version	2
2.4 Interoperability Test Topology	3
2.4.1 Enterprise Model Implementation	3
2.4.2 Environment Setup.....	4
2.4.3 Infrastructure Prerequisites.....	4
2.4.4 Known Limitations.....	5
3 Configuring Teams Direct Routing.....	6
3.1 Prerequisites.....	6
3.2 SBC Domain Name in the Teams Enterprise Model.....	6
3.3 Example of the Office 365 Tenant Direct Routing Configuration	7
3.3.1 Adding a New SBC to Direct Routing.....	8
3.3.2 Adding a Voice Route and PSTN Usage	9
3.3.3 Adding a Voice Routing Policy	11
3.3.4 Enabling Online User	12
3.3.5 Assigning Online User to the Voice Routing Policy	12
4 Configuring AudioCodes SBC.....	13
4.1 SBC Configuration Concept in Teams Direct Routing Enterprise Model	13
4.2 IP Network Interfaces Configuration	14
4.2.1 Configuring VLANs.....	14
4.2.2 Configuring Network Interfaces.....	15
4.2.3 Configuring NAT Translation (Optional)	15
4.3 SIP TLS Connection Configuration.....	16

4.3.1	Configuring the NTP Server Address	16
4.3.2	Creating a TLS Context for Teams Direct Routing.....	17
4.3.3	Configuring a Certificate.....	17
4.3.4	Method of Generating and Installing the Wildcard Certificate.....	19
4.3.5	Deploying Trusted Root Certificate for MTLS Connection	19
4.4	Configuring Media Realms.....	20
4.5	Configuring SIP Signaling Interfaces	20
4.6	Configuring Proxy Sets and Proxy Address	21
4.6.1	Configuring a Proxy Address	22
4.7	Configuring Coders	23
4.8	Configuring IP Profiles	25
4.9	Configuring IP Groups.....	27
4.10	Configuring SRTP	28
4.11	Configuring Message Condition Rules	28
4.12	Configuring Classification Rules	29
4.13	Configuring IP-to-IP Call Routing Rules	30
4.14	Configuring Firewall Settings (Optional)	31
4.15	Configuring Message Manipulation Rules	32
4.16	Configuring Registration Account (only for Registration Trunk Mode)	41
4.17	Miscellaneous Configuration	42
4.17.1	Configuring Call Forking Mode	42
4.17.2	Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only).....	42

Notice

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

This document is subject to change without notice.

Date Published: March-23-2025

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

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
13123	Initial document release.

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>.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between Vodafone IP Anlagen-Anschluss's interface 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/interoperability-list>.

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and Vodafone partners who are responsible for installing and configuring Vodafone IP Anlagen-Anschluss's interface 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 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.

2 Component Information

2.1 AudioCodes SBC Version

Table 1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none"> ■ Mediant 500/L 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	7.40A.600.221 or later
Protocol	<ul style="list-style-type: none"> ■ SIP/UDP or SIP/TCP or SIP/TLS (to the Vodafone IP Anlagen-Anschluss Interface) ■ SIP/TLS (to the Teams Direct Routing)
Additional Notes	None

2.2 Vodafone IP Anlagen-Anschluss Interface Version

Table 2: Vodafone IP Anlagen-Anschluss Version

Vendor/Service Provider	Vodafone
SSW Model/Service	IP Anlagen-Anschluss Interface
Software Version	R.6
Protocol	SIP
Additional Notes	None

2.3 Microsoft Teams Direct Routing Version

Table 3: Microsoft Teams Direct Routing Version

Vendor	Microsoft
Model	Teams Phone System Direct Routing
Software Version	Release v.2025.2.6.2
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

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

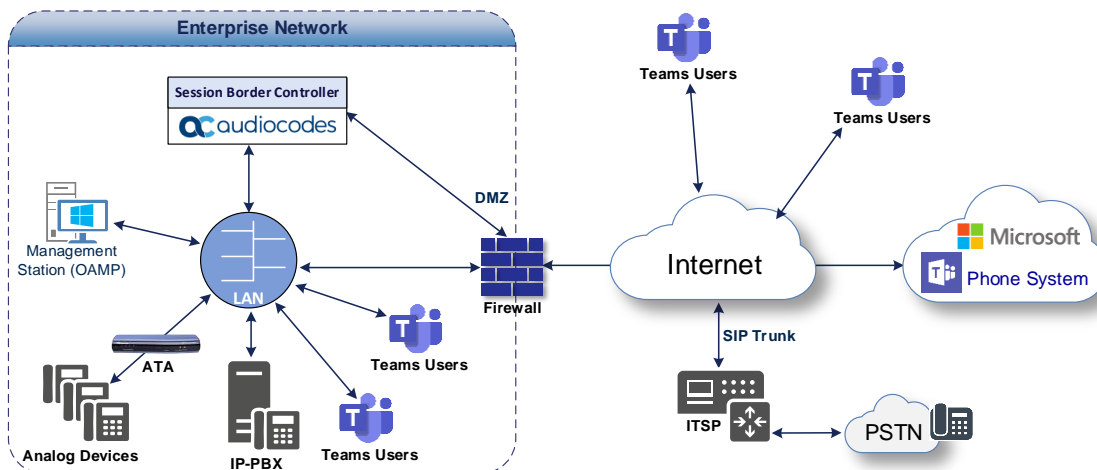
2.4.1 Enterprise Model Implementation

The interoperability testing between AudioCodes SBC and Vodafone IP Anlagen-Anschluss Interface 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 Vodafone IP Anlagen-Anschluss's Interface service
- AudioCodes SBC is implemented to interconnect between the devices in the Enterprise LAN and Microsoft Teams and Vodafone IP Anlagen-Anschluss's Interface on the WAN
 - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
 - **Border:** IP-to-IP network border - the Vodafone IP Anlagen-Anschluss's Interface is located in the Enterprise WAN and the Microsoft Teams Phone Systems is located in the public network.

The figure below illustrates this interoperability test topology:

Figure 1: Interoperability Test Topology between SBC and Microsoft Teams Direct Routing Enterprise Model with Vodafone IP Anlagen-Anschluss Interface



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 4: Environment Setup

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

2.4.3 Infrastructure Prerequisites

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

Table 2-5: Infrastructure Prerequisites

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

2.4.4 Known Limitations

The following limitations were observed during interoperability testing of the AudioCodes SBC interworking between Microsoft Teams Direct Routing and Vodafone IP Anlagen-Anschluss's Interface:

- PRACK Implementation is disabled in Registration Trunk Mode.
- Anonymous calls from Vodafone to Teams were not tested due to fact that the called number was changed by the interconnect carrier and not presented as anonymous.
- For outbound calls (Teams to Vodafone), in the Case of SIP 404 and a few of other Status Codes, Vodafone applies special behavior. This is to avoid side-effects due to CSCF is highly 3GPP based and shared with Consumer Services. Therefore SIP 404 response is replaced with 487.
- Early Media (Fun Tone) didn't pass, probably due to limitation of multiple interconnect carriers.
- Options Ping is implemented only in Static Trunk mode. In Registration Trunk mode, Vodafone responds to the Options request, but does not initiate them.
- Vodafone SIP Trunk supports Session Timers, but does not initiate session expiration negotiation.
- Especially in Registration Trunk Mode, Vodafone network does not recognize the calling number when presented in the SIP **P-Asserted-Identity** header using SIP URI format. This results in the real dialing number not being presented. As a workaround, the **P-Asserted-Identity** header is changed to TEL URI format and then replaced by **P-Preferred-Identity** header.

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

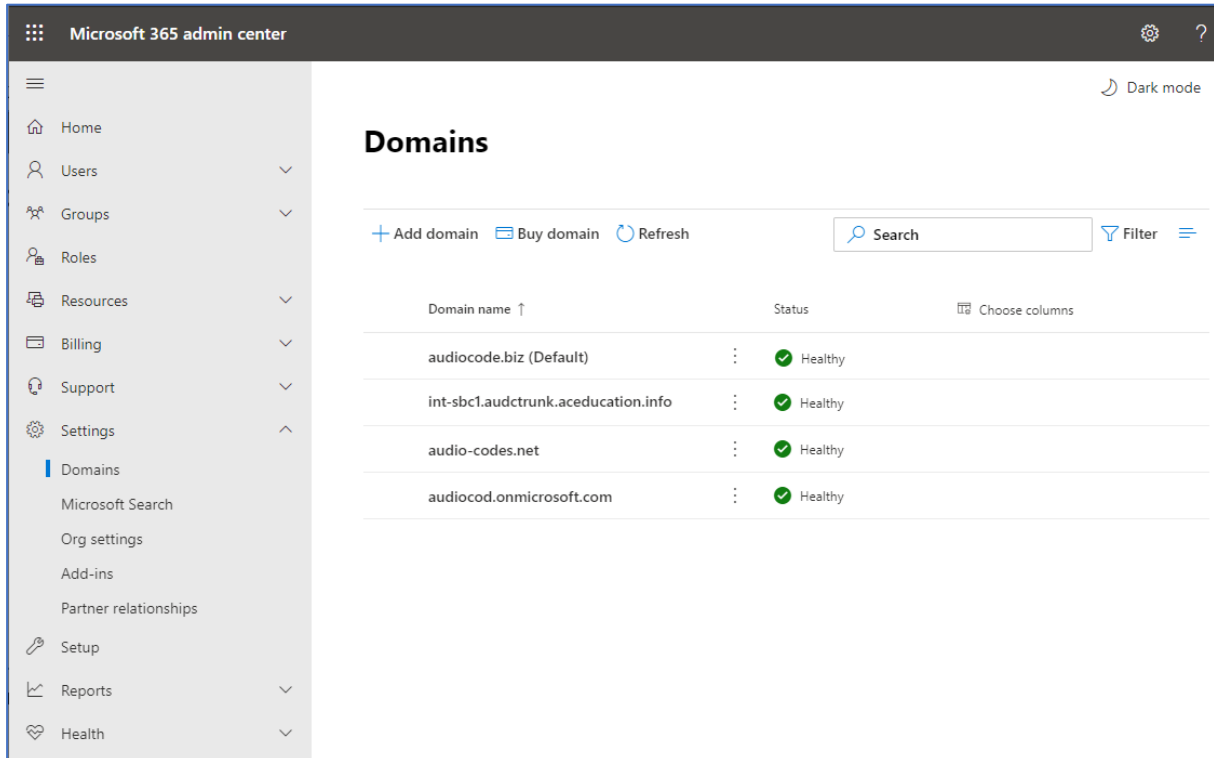
The SBC domain name must be from one of the names registered in 'Domains' of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, the administrator registered the following DNS names for the tenant:

Table 6: 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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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 2: Example of Registered DNS Names

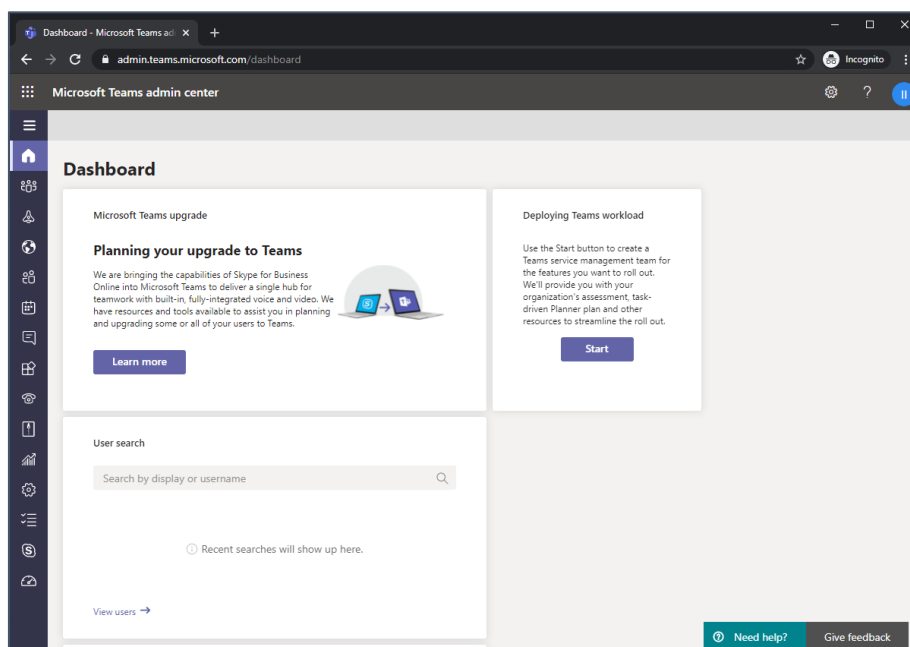


During the creation of the Domain, you will be forced to create public DNS record (**int-sbc1.audctrunk.aceducation.info** in our example.)

3.3 Example of the Office 365 Tenant Direct Routing Configuration

Configuration can be done 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: Teams Admin Center



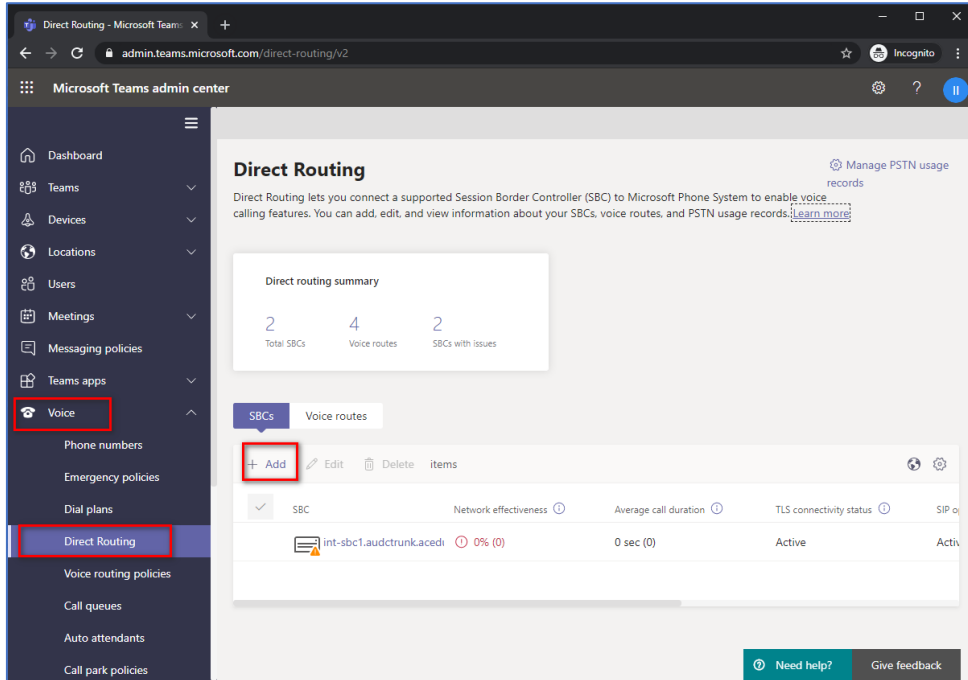
3.3.1 Adding a New SBC to Direct Routing

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

To add New SBC to Direct Routing:

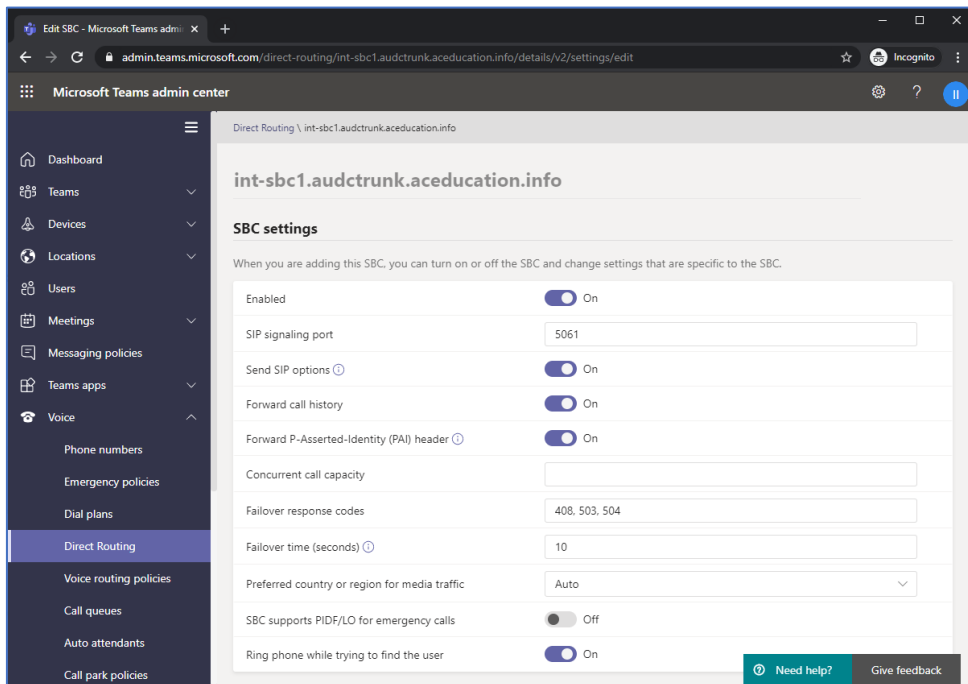
1. In the web interface, select **Voice**, and then click **Direct Routing**.
2. Under SBCs click **Add**.

Figure 4: Add new SBC to Direct Routing



3. Configure SBC.

Figure 5: 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 -SipSignalingPort 5061 -ForwardCallHistory $True -ForwardPai $True -MediaBypass $True -Enabled $True
```

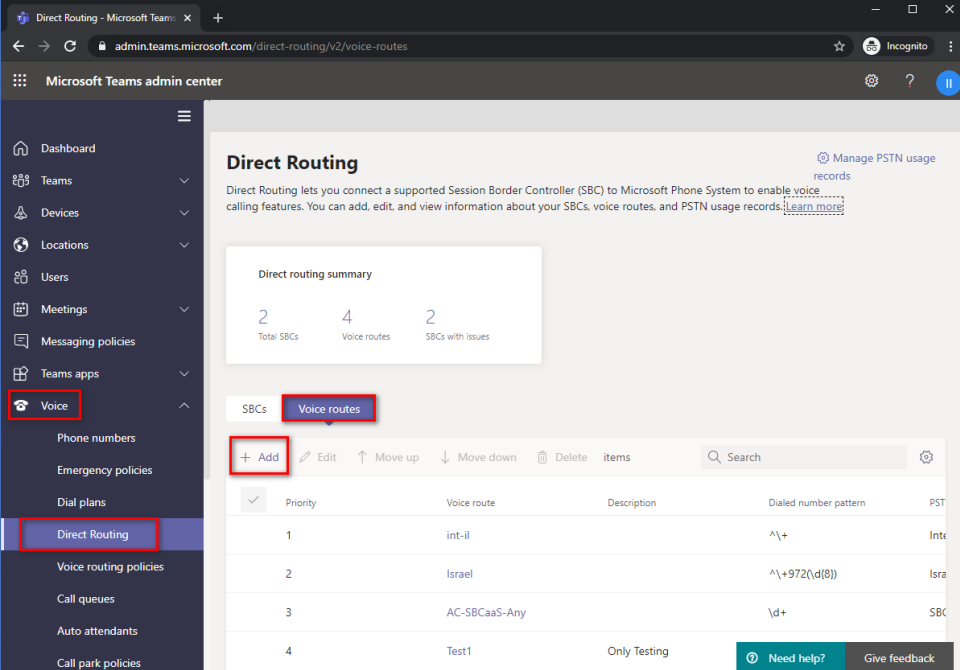
3.3.2 Adding a Voice Route and PSTN Usage

The procedure below describes how to 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 6: Add New Voice Route

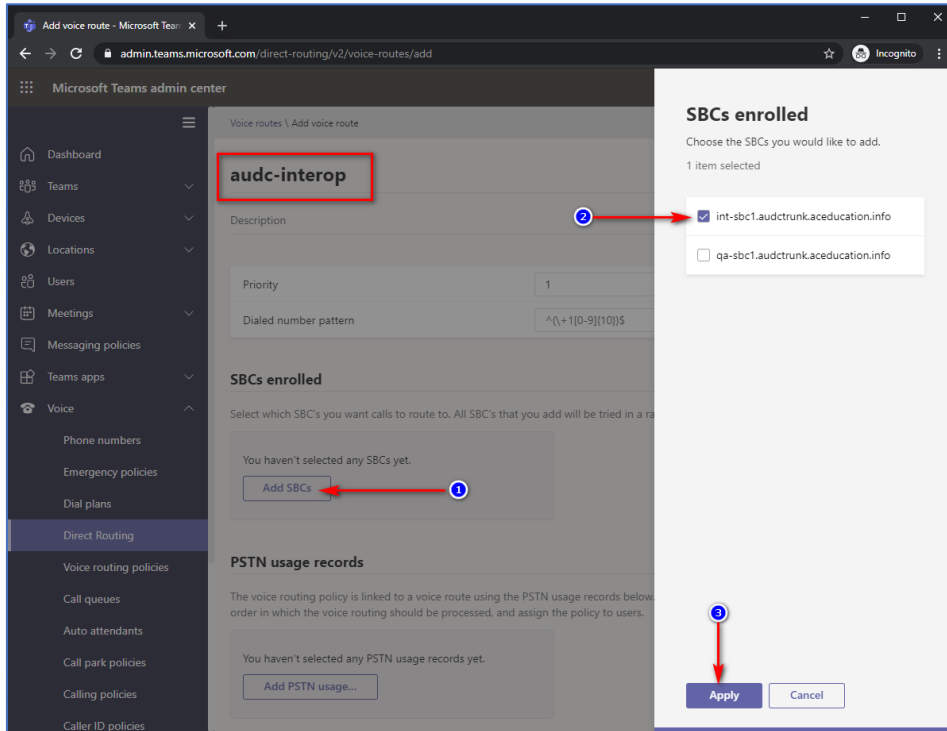


The screenshot displays the Microsoft Teams admin center interface for Direct Routing. The left-hand navigation pane shows the 'Voice' section expanded, with 'Direct Routing' selected. The main content area is titled 'Direct Routing' and includes a 'Direct routing summary' card showing 2 Total SBCs, 4 Voice routes, and 2 SBCs with issues. Below this, the 'Voice routes' tab is active, and the '+ Add' button is highlighted with a red box. A table lists the existing voice routes:

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		

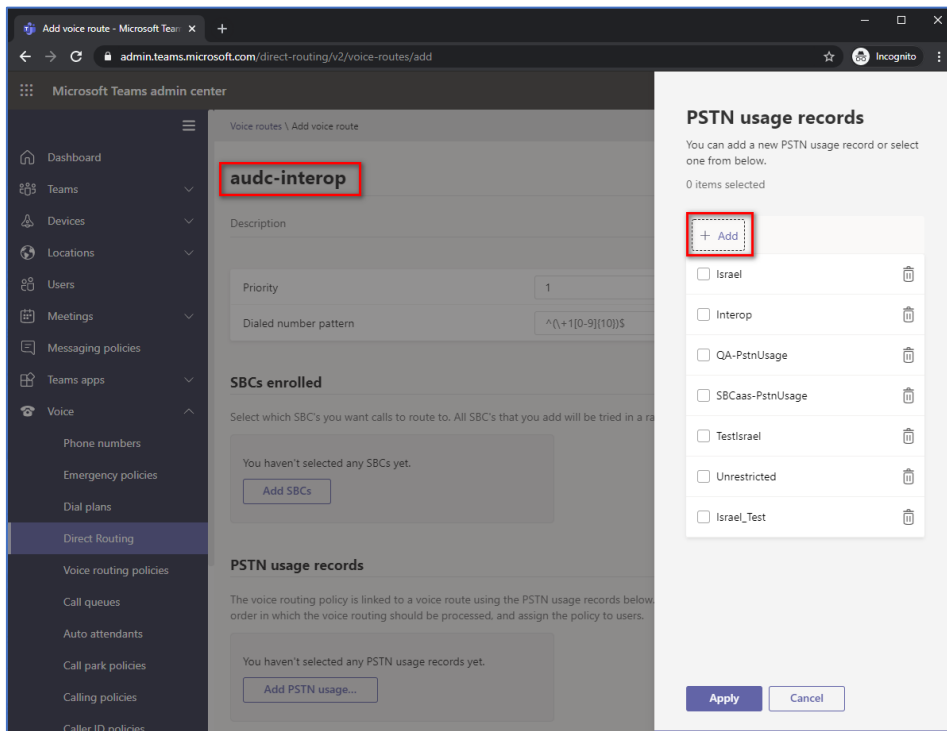
2. Create a new Voice Route and associate it with the SBC, configured in the previous step.

Figure 7: Associate SBC with new Voice Route



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

Figure 8: Associate PSTN Usage with New Voice Route



The same operations can be done using the 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"
```

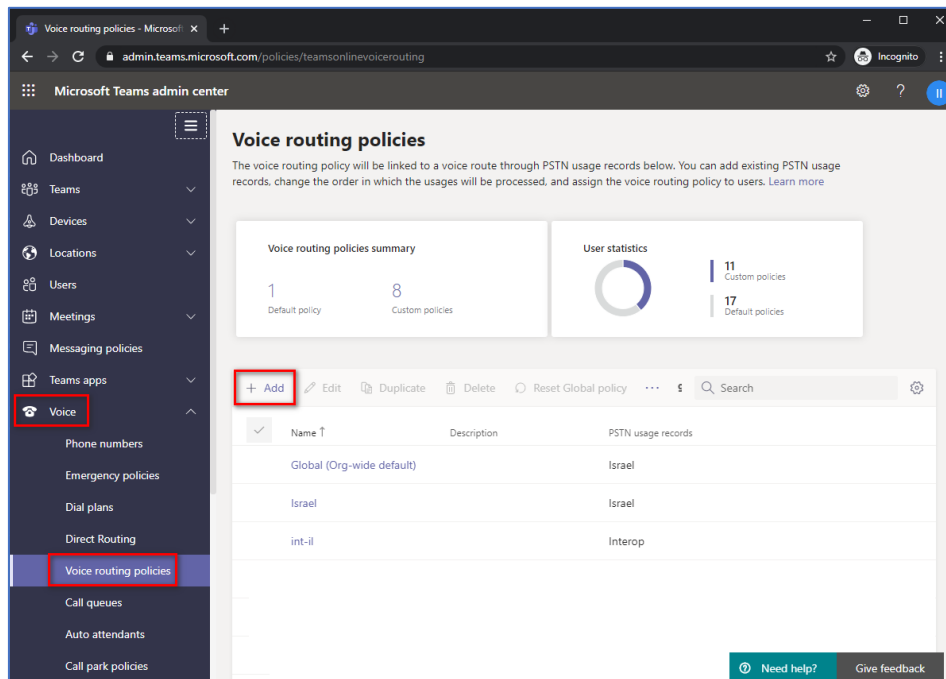
3.3.3 Adding a Voice Routing Policy

The procedure below describes how to add a voice routing policy

To add voice routing policy:

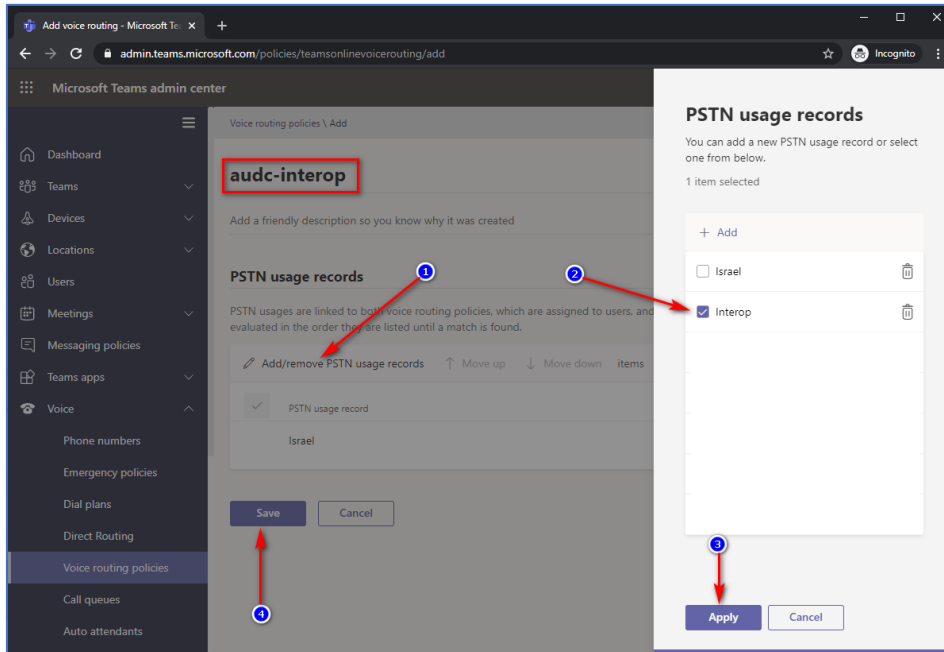
1. In the web interface, under **Voice**, select **Voice routing policies** and click **Add**.

Figure 9: Add New Voice Routing Policy



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

Figure 10: Associate PSTN Usage with New Voice Routing Policy



The same operations can be done using the following PowerShell command:

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



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 Enabling Online User

Use the following PowerShell command for enabling online user:

```
Set-CsPhoneNumberAssignment -Identity user1@company.com -EnterpriseVoiceEnabled $true
Set-CsPhoneNumberAssignment -Identity user1@company.com -PhoneNumber +12345678901 -PhoneNumberType DirectRouting
```

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 Vodafone IP Anlagen-Anschluss Interface. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 3, and includes the following main areas:

- SBC LAN interface – Management Station
- SBC WAN interface – Vodafone IP Anlagen-Anschluss Interface and Teams Direct Routing environment

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



- For implementing Microsoft Teams Direct Routing and Vodafone IP Anlagen-Anschluss Interface 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.
- If your SBC is deployed in a virtual environment and transcoding is required, your virtual machine must have a minimum of two vCPUs. For more information, please refer to the appropriate *Installation Manual*, which can be found on AudioCodes website.
- 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 on 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 11: SBC Configuration Concept

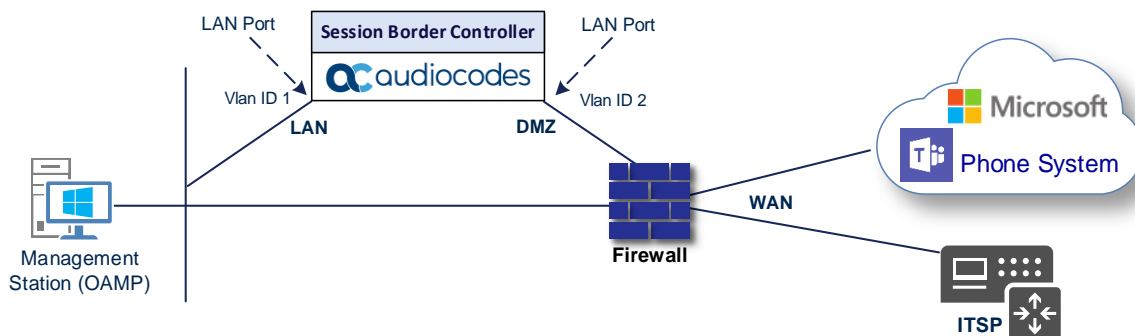


4.2 IP Network Interfaces Configuration

This section describes how to configure 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 Vodafone IP Anlagen-Anschluss Interface, 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 12: Network Interfaces in Interoperability Test Topology



4.2.1 Configuring 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 is one existing row for VLAN ID 1 and underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side

4.2.2 Configuring 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 7: 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	10.15.77.200	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

4.2.3 Configuring NAT Translation (Optional)



This section is relevant only if the SBC is located in the Cloud or just implemented using private IP addresses.

The **NAT Translation table** allows you to configure network address translation (NAT) rules for translating source IP addresses into NAT IP addresses (*global - public*). These addresses are typically used in front of the Cloud or corporate firewall facing the Vodafone IP Anlagen-Anschluss Interface and the Microsoft Teams Network.

A NAT Translation Table is created automatically during the implementation of the Cloud based instance process. But if manual configuration is required, follow the next steps.

To configure the NAT translation rules:

1. Open the NAT Translation table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).
2. Click **+New** (at the top of the interface) to add a new NAT Translation rule.
3. Configure the parameters using the table below as reference.

Table 8: NAT Translation Rule

Index	Source Interface	Source Start Port	Source End Port	Target IP Address	Target Start Port	Target End Port
0	eth0	1	65535	<Public IP Address>	1	65535

4. Click **Apply**.

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 and Vodafone IP Anlagen-Anschluss Interface (if it's required). 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-sbc.audctrunk.aceducation.info
- SAN: int-sbc.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 Configuring the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (any public NTP server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties.

To configure the NTP server address:

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. From the 'NTP Interface' drop-down list, select an appropriated interface (e.g., **WAN_IF**).
3. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **time.google.com**).
4. Click **Apply**.

4.3.2 Creating a TLS Context for Teams Direct Routing

This section describes how to configure TLS Context on the SBC. AudioCodes recommends implementing only TLS to avoid flaws in SSL. The same TLS context can also be used for Vodafone IP Anlagen-Anschluss Interface.

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 9: New TLS Context

Index	Name	TLS Version
1	Teams (arbitrary descriptive name)	TLSv1.2 and TLSv1.3
All other parameters can be left unchanged with their default values.		



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>.

3. Click **Apply**.

4.3.3 Configuring a Certificate

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

The procedure involves the following main steps:

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

To configure a certificate:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
 - a. In the 'Common Name [CN]' field, enter the SBC FQDN name (based on example above, **int-sbc.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 our example, **int-sbc.audctrunk.aceducation.info**).



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 or leave the default value (2048).
 - 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.
4. Copy the CSR from the line "**-----BEGIN CERTIFICATE REQUEST**" to "**END CERTIFICATE REQUEST-----**" to a text file (such as Notepad) and then save it to a folder on your computer with the file name, for example *certreq.txt*.
5. Send *certreq.txt* file to the Certified Authority Administrator for signing.
6. After obtaining an SBC signed and Trusted Root/Intermediate Certificate from the CA, in the SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
 - b. Scroll down to the **Upload certificates files from your computer** group, click the **Choose File** button corresponding to the '**Send Device Certificate...**' field, navigate to the certificate file obtained from the CA, and then click **Load File** to upload the certificate to the SBC.
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.
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.

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 Deploying Trusted Root Certificate for MTLS Connection



Loading Trusted Root Certificates to AudioCodes' SBC is mandatory when implementing an MTLS connection with the Microsoft Teams network



Microsoft 365 is updating services powering messaging, meetings, telephony, voice, and video to use TLS certificates from a different set of Root Certificate Authorities (CAs). For more details of the new Root CAs, refer to Microsoft technical guidance at [Office TLS Certificate Changes](#).

The DNS name of the Teams Direct Routing interface is **sip.pstnhub.microsoft.com**. In this interface, a certificate is presented which is signed by **DigiCert** with Serial Number: 0x033af1e6a711a9a0bb2864b11d09fae5, SHA-1 Thumbprint: DF3C24F9BFD666761B268073FE06D1CC8D4F82A4 and SHA-256 Thumbprint: CB3CCBB76031E5E0138F8DD39A23F9DE47FFC35E43C1144CEA27D46A5AB1CB5F.

To trust this certificate, your SBC must have the certificate in Trusted Certificates storage. Download the **DigiCert Global Root G2** (df3c) certificate in **PEM format** from <https://www.digicert.com/kb/digicert-root-certificates.htm> and follow the steps above to import the certificate to the Trusted Root storage.



Before importing the DigiCert 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 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 Configuring Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the Vodafone IP Anlagen-Anschluss Interface 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 10: 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)

4.5 Configuring SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For the interoperability test topology, towards the Vodafone IP Anlagen-Anschluss Interface and towards the Teams Direct Routing SIP Interfaces must be configured for the SBC.

To configure SIP Interfaces:

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



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 11: 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 Vodafone requirement)	5060 (according to Vodafone requirement)	5065 (according to Vodafone requirement)	Disable (leave default value)	0 (Recommended to prevent DoS attacks)	SIPTrunk	Teams
1	Teams (arbitrary name)	WAN_IF	SBC	0 (Phone System does not use UDP or TCP for SIP signaling)	0	5061 (as configured in Office 365)	Enable	0 (Recommended to prevent DoS attacks)	Teams	Teams

4.6 Configuring 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:

- Vodafone IP Anlagen-Anschluss Interface
- Teams Direct Routing

The Proxy Sets are later 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 12: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	Proxy Load Balancing Method	DNS Resolve Method
1	SIPTrunk (arbitrary name)	SIPTrunk	default	Using OPTIONS / Using OPTIONS on Active Server (For Registration Trunk Mode)	Homing	Enable	Random Weights	SRV
2	Teams (arbitrary name)	Teams	Teams	Using Options		Enable	Random Weights	



On Hybrid SBCs (with Onboard PSTN interfaces), it is recommended to leave Proxy Set 0 unconfigured for possible future use for PSTN Fallback.

4.6.1 Configuring a Proxy Address

This section shows how to configure a Proxy Address.

To configure a Proxy Address for the Vodafone IP Anlagen-Anschluss Interface:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **SIPTrunk**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; and configure the address of the Proxy Set according to the parameters described in the table below:

Table 13: Configuration Proxy Address for the Vodafone IP Anlagen-Anschluss Interface

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	SIPTrunk.com (SIP Trunk FQDN)	UDP or TCP or TLS (according to connection mode)	0	0

3. Click **Apply**.

To configure a Proxy Address for Teams:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **Teams**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; and configure the address of the Proxy Set according to the parameters described in the table below:

Table 14: 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

3. Click **Apply**.

4.7 Configuring 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 Vodafone IP Anlagen-Anschluss Interface may restrict operation with a dedicated coders list, you need to add a Coder Group with the supported coders for each leg, the Microsoft Teams Direct Routing and the Vodafone IP Anlagen-Anschluss Interface.

Note that the Coder Group ID for this entity is 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. Click **New** and configure a name for the Audio Coders Group for Microsoft Teams (e.g., *AudioCodersGroups_Teams*).
3. Click **Apply**.
4. Select the new row that you configured, and then click the **Coders Table** link located below the table; the **Coders Table** opens.
5. Add the required codecs as follows:

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

6. Click **Apply** and confirm the configuration change in the prompt that pops up.

The procedure below describes how to update the default values of the payload types to avoid misconfiguration.

To configure default values of some coder's payload types:

1. Open the RTP/RTCP Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **RTP/RTCP Settings**).
2. Change the default values of the following payload types as follows:

Parameter	Value
RFC 2833 TX Payload Type	101
RFC 2833 RX Payload Type	101
RFC 2198 Payload Type	105
Fax Bypass Payload Type	106
Modem Bypass Payload Type	107

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Vodafone IP Anlagen-Anschluss Interface uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID is assigned to the IP Profile belonging to the Vodafone IP Anlagen-Anschluss Interface in the next step.

To set a preferred coder for the Vodafone IP Anlagen-Anschluss Interface (if required):

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 Vodafone IP Anlagen-Anschluss Interface (e.g., *SIPTrunk-Allowed*).
3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Index	Coder
0	G.711 A-law
1	G.711 U-law
2	G.722
3	G.729

6. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).
7. From the '**Extended Coders Behavior**' drop-down list, select **Include Extensions**.
8. Click **Apply**.

4.8 Configuring 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:

- Vodafone IP Anlagen-Anschluss Interface – to operate in non-secure mode using RTP and SIP over TCP
- Microsoft Teams Direct Routing – to operate in secure mode using SRTP and SIP over TLS

To configure an IP Profile for the Vodafone IP Anlagen-Anschluss Interface:

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	0
Name	SIPTrunk
Media Security	
SBC Media Security Mode	Not Secured or Secured (depending on required mode)
SBC Early Media	
Generate RTP	Until RTP detected
SBC Media	
Allowed Audio Coders	SIPTrunk-Allowed
SBC Signaling	
P-Asserted-Identity Header Mode	Add
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote Replaces Mode	Handle Locally
Play RBT To Transferee	Yes
Remote 3xx Mode	Handle Locally

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	1
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_Teams
RFC 2833 Mode	Extend
RTCP Mode	Generate Always (required, as some ITSPs do not send RTCP packets during while in Hold mode, but Microsoft expected to them)
ICE Mode	Lite (required only when Media Bypass enabled on Microsoft Teams)
SBC Signaling	
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 respond with a=inactive and IP=0.0.0.0 to a Re-Invite with Hold request from Teams. Since the Microsoft Media Stack does not support this format, the SBC replaces 0.0.0.0 with its own IP address)

3. Click **Apply**.

4.9 Configuring IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

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

- Vodafone IP Anlagen-Anschluss Interface located on WAN
- Teams Direct Routing located on WAN

To configure IP Groups:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the Vodafone IP Anlagen-Anschluss Interface:

Parameter	Value
Index	1
Name	SIPTrunk
Type	Server
Proxy Set	SIPTrunk
IP Profile	SIPTrunk
Media Realm	SIPTrunk
SIP Group Name	(according to Vodafone requirement)

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

Parameter	Value
Index	2
Name	Teams
Topology Location	Up
Type	Server
Proxy Set	Teams
IP Profile	Teams
Media Realm	Teams
SIP Group Name	(according to Vodafone requirement)
Classify By Proxy Set	Disable
Local Host Name	<FQDN name of your SBC in the Microsoft Teams tenant> (For example, <i>int-sbc.audctrunk.aceducation.info</i>)
Always Use Src Address	Yes
Teams Direct Routing Mode	Enable
Proxy Keep-Alive using IP Group settings	Enable

4.10 Configuring 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.
3. From the **Offered SRTP Cipher Suites** drop-down list, select **AES-CM-128-HMAC-SHA1-80** (according to Vodafone requirements).
4. Click **Apply**.

4.11 Configuring Message Condition Rules

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

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

To configure a Message Condition rule:

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

Parameter	Value
Index	0
Name	Teams-Contact (arbitrary descriptive name)
Condition	Header.Contact.URL.Host contains 'pstnhub.microsoft.com'

3. Click **Apply**.

4.12 Configuring Classification Rules

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

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

To configure a Classification rule:

1. Open the Classification table (**Setup menu > Signaling & Media tab > SBC folder > Classification Table**).
2. Configure Classification rules as shown in the table below:

Table 15: Classification Rules

Index	Name	Source SIP Interface	Source IP Address	Destination Host	Message Condition	Action Type	Source IP Group
0	Teams_52_112 (arbitrary name)	Teams	52.112.*.*	<FQDN name of your SBC in the Microsoft Teams tenant> (e.g., int-sbc.audctrunk.aceducation.info)	Teams-Contact	Allow	Teams
1	Teams_52_113 (arbitrary name)	Teams	52.113.*.*	<FQDN name of your SBC in the Microsoft Teams tenant> (e.g., int-sbc.audctrunk.aceducation.info)	Teams-Contact	Allow	Teams
2	Teams_52_114 (arbitrary name)	Teams	52.114.*.*	<FQDN name of your SBC in the Microsoft Teams tenant> (e.g., int-sbc.audctrunk.aceducation.info)	Teams-Contact	Allow	Teams
3	Teams_52_115 (arbitrary name)	Teams	52.115.*.*	<FQDN name of your SBC in the Microsoft Teams tenant> (e.g., int-sbc.audctrunk.aceducation.info)	Teams-Contact	Allow	Teams
4	Teams_52_120 (arbitrary name)	Teams	52.120.*.*	<FQDN name of your SBC in the Microsoft Teams tenant> (e.g., int-sbc.audctrunk.aceducation.info)	Teams-Contact	Allow	Teams
5	Teams_52_121 (arbitrary name)	Teams	52.121.*.*	<FQDN name of your SBC in the Microsoft Teams tenant> (e.g., int-sbc.audctrunk.aceducation.info)	Teams-Contact	Allow	Teams
6	Teams_52_122 (arbitrary name)	Teams	52.122.*.*	<FQDN name of your SBC in the Microsoft Teams tenant> (e.g., int-sbc.audctrunk.aceducation.info)	Teams-Contact	Allow	Teams
7	Teams_52_123 (arbitrary name)	Teams	52.123.*.*	<FQDN name of your SBC in the Microsoft Teams tenant> (e.g., int-sbc.audctrunk.aceducation.info)	Teams-Contact	Allow	Teams

3. Click **Apply**.

4.13 Configuring 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 Vodafone IP Anlagen-Anschluss Interface:

- 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 Vodafone IP Anlagen-Anschluss Interface
- Calls from Vodafone IP Anlagen-Anschluss Interface 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 16: Configuration of IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Call Trigger	ReRoute IP Group	Dest Type	Dest IP Group	Internal Action
0	Terminate OPTIONS	Any	OPTIONS			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	SIPTrunk	
3	SIP Trunk to Teams (arbitrary name)	SIPTrunk				IP Group	Teams	



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

4.14 Configuring Firewall Settings (Optional)

As extra security, 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 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 WAN Interface:

Table 17: Firewall Table Rules

Index	Source IP	DNS Query Type	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server> (e.g., time.google.com)	A	32	0	65535	Any	Enable	WAN_IF	Allow
1	52.112.0.0	A	14	0	65535	TCP	Enable	WAN_IF	Allow
2	52.120.0.0	A	14	0	65535	TCP	Enable	WAN_IF	Allow
3	siptrunk.de (SIP Trunk FQDN)	SRV	-	0	65535	Any	Enable	WAN_IF	Allow
49	0.0.0.0	A	0	0	65535	Any	Enable	WAN_IF	Block



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 row of index 3.

4.15 Configuring 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 0**) for the Vodafone IP Anlagen-Anschluss Interface. This rule applies to the SIP OPTIONS messages received from the Vodafone IP Anlagen-Anschluss Interface. Vodafone IP Anlagen-Anschluss Interface send SIP OPTIONS messages with the **Max-Forwards** header value '0', which cause error messages in the syslog. This rule modifies the value of the **Max-Forwards** header with value '10'.

Parameter	Value
Index	0
Name	Change Max-Forwards (arbitrary name)
Manipulation Set ID	0
Message Type	Options.Request
Condition	Header.Max-Forwards=='0'
Action Subject	Header.Max-Forwards
Action Type	Modify
Action Value	'10'

3. Configure a new manipulation rule (**Manipulation Set 1**) for Teams. This rule applies to messages received from the Teams IP Group. This removes the **SIP P-Asserted-Identity** header in all messages, received from the Teams.

Parameter	Value
Index	1
Name	Remove PAI (arbitrary name)
Manipulation Set ID	1
Condition	Header.P-Asserted-Identity exists
Action Subject	Header.P-Asserted-Identity
Action Type	Remove

4. Configure an additional manipulation rule (**Manipulation Set 1**) for Teams. This rule applies to messages received from the Teams IP Group. This removes the **SIP Privacy** Header in all messages, except of call with presentation restriction.

Parameter	Value
Index	2
Name	Remove Privacy Header (arbitrary name)
Manipulation Set ID	1
Condition	Header.Privacy exists And Header.From.URL !contains 'anonymous'
Action Subject	Header.Privacy
Action Type	Remove

5. Configure an additional manipulation rule (**Manipulation Set 3**) for the Vodafone IP Anlagen-Anschluss Interface. This rule applies to messages received from the Vodafone IP Anlagen-Anschluss Interface IP Group. This replaces the user part of the **SIP Request-URI** header with the value from the **SIP P-Called-Party-ID** header.

Parameter	Value
Index	3
Name	Copy P-Called-Party-ID to R-URI (arbitrary name)
Manipulation Set ID	3
Message Type	Invite
Action Subject	Header.Request-URI.URL.User
Action Type	Modify
Action Value	Header.P-Called-Party-ID.URL.User

6. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. This rule applies to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group in a call transfer scenario. This replaces the host part of the **SIP Referred-By** header with the value from the **SIP From** header.

Parameter	Value
Index	4
Name	Call Transfer - change Referred-By host (arbitrary name)
Manipulation Set ID	4
Message Type	Invite
Condition	Header.Referred-By exists
Action Subject	Header.Referred-By.URL.Host
Action Type	Modify
Action Value	Header.From.URL.Host

7. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. This rule applies to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group in a call transfer scenario. This replaces the host part of the **SIP P-Asserted-Identity** header with the value from the **SIP From** header.

Parameter	Value
Index	5
Name	Call Transfer - change Referred-By host (arbitrary name)
Manipulation Set ID	4
Message Type	Invite
Action Subject	Header.P-Asserted-Identity.URL.Host
Action Type	Modify
Action Value	Header.From.URL.Host

8. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. This rule applies to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. This adds the PRACK and UPDATE methods to the **SIP Allow** header to enable implementation of the PRACK in the Vodafone network.

Parameter	Value
Index	6
Name	Add PRACK and UPDATE to Allow Header (arbitrary name)
Manipulation Set ID	4
Condition	Header.Allow regex(.*)
Action Subject	Header.Allow
Action Type	Modify
Action Value	\$1+',PRACK,UPDATE'

9. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. This rule applies to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group, and changes the type of the **SIP P-Asserted-Identity** header from 'sip:' to 'tel:'.

Parameter	Value
Index	7
Name	Change PAI type to tel
Manipulation Set ID	4
Message Type	any.response
Condition	Header.P-Asserted-Identity exists
Action Subject	Header.P-Asserted-Identity.URL.Type
Action Type	Modify
Action Value	'2'

10. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. This rule is applied to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. This replaces the **SIP P-Asserted-Identity** header with the **SIP P-Preferred-Identity** header.

Parameter	Value
Index	8
Name	Replace PAI by PPI
Manipulation Set ID	4
Action Subject	Header.P-Preferred-Identity
Action Type	Add
Action Value	Header.P-Asserted-Identity.URL

11. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. This removes the **SIP P-Asserted-Identity** Header in all messages.

Parameter	Value
Index	9
Name	Remove PAI
Manipulation Set ID	4
Action Subject	Header.P-Preferred-Identity
Action Type	Remove

12. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. **This rule is needed for Static Mode ONLY.** This rule is applied to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. This replaces the user part of the **SIP Contact** header with the value from **SIP From** header.

Parameter	Value
Index	10
Name	Add User to Contact (For Static Mode)
Manipulation Set ID	4
Action Subject	Header.Contact.URL.User
Action Type	Modify
Action Value	Header.From.URL.User



The following set of message manipulation rules is relevant only when implementing encrypted (TLS/SRTP) connections to the Vodafone IP Anlagen-Anschluss Interface.

13. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. **This rule is required ONLY for encrypted connection**, and applies to **Invite, Register**, and **Update** messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. It adds the **SIP Proxy-Require** header with the value **'mediasec'**.

Parameter	Value
Index	20
Name	Add Proxy-Req (RIU)
Manipulation Set ID	4
Condition	Header.Request-URI.MethodType == '5' or Header.Request-URI.MethodType == '11' or Header.Request-URI.MethodType == '18'
Action Subject	Header.Proxy-Require
Action Type	Add
Action Value	'mediasec'

14. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. **This rule is required ONLY for encrypted connection**, and applies to **Invite, Register**, and **Update** messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. It adds the **SIP Require** header with the value **'mediasec'**.

Parameter	Value
Index	21
Name	Add Require (RIU)
Manipulation Set ID	4
Row Role	Use Previous Condition
Action Subject	Header.Require
Action Type	Add
Action Value	'mediasec'

15. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. **This rule is required ONLY for encrypted connection**, and applies to the **Register request** messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. It adds the **SIP Security-Client** header with the value 'sdes-srtp;mediasec'.

Parameter	Value
Index	22
Name	Add Sec-Client (R)
Manipulation Set ID	4
Message Type	Register.Request
Action Subject	Header.Security-Client
Action Type	Add
Action Value	'sdes-srtp;mediasec'

16. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. **This rule is required ONLY for encrypted connection**, and applies to the **Register request** messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. It adds the **SIP Security-Verify** header with the value 'sdes-srtp;mediasec'.

Parameter	Value
Index	23
Name	Add Sec-Verify (R)
Manipulation Set ID	4
Message Type	Register.Request
Action Subject	Header.Security-Verify
Action Type	Add
Action Value	'sdes-srtp;mediasec'

17. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. **This rule is required ONLY for encrypted connection**, and applies to **Invite** and **Update** messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. It adds the **SIP Proxy-Require** header with the value 'sdes-srtp;mediasec'.

Parameter	Value
Index	24
Name	Add Sec-Verify (IU)
Manipulation Set ID	4
Condition	Header.Request-URI.MethodType == '5' or Header.Request-URI.MethodType == '18'
Action Subject	Header.Security-Verify
Action Type	Add
Action Value	'sdes-srtp;mediasec'

18. Configure an additional manipulation rule (**Manipulation Set 4**) for the Vodafone IP Anlagen-Anschluss Interface. **This rule is required ONLY for encrypted connection**, and applies to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. It adds the 'a=3ge2ae:requested' line to the SDP body of the message.

Parameter	Value
Index	25
Name	Add e2ae SDP
Manipulation Set ID	4
Condition	Body.sdp regex (.*)\s{2,}(a\rtpmap.*)
Action Subject	Body.sdp
Action Type	Modify
Action Value	\$1+\$2+'a=3ge2ae:requested'+\$2+\$3

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set IDs (**Manipulation Set IDs 0, 1, 3 and 4**) and which are executed for messages sent to and from the Vodafone IP Anlagen-Anschluss Interface IP Group as well as the Teams Direct Routing IP Group. These rules are specifically required to enable proper interworking between Vodafone IP Anlagen-Anschluss Interface and Teams Direct Routing. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to the SIP OPTIONS messages received from the Vodafone IP Anlagen-Anschluss Interface. This rule modifies the value of the Max-Forwards header with value '10'.	Vodafone IP Anlagen-Anschluss Interface sends SIP OPTIONS messages with the Max-Forwards header value '0', which triggers error messages in the syslog.
1	This rule applies to messages received from the Teams. Removes the SIP P-Asserted-Identity header in all messages, received from the Teams.	If Teams is configured to send a P-Asserted-Identity header: It sends it in a format where the first index is presented as SIP TEL URI (tel:) and the second as SIP URI (sip:), when the DID presented in the TEL URI. Vodafone network reflects calling DID by P-Preferred-Identity header with TEL URI. This is handled in the next rules.
2	This rule applies to messages received from the Teams. Removes the SIP Privacy header in all messages, except for calls with presentation restriction.	
3	This rule applies to messages received from the Vodafone IP Anlagen-Anschluss Interface. Replaces the user part of the SIP Request-URI header with the value from the SIP P-Called-Party-ID header.	Vodafone uses P-Called-Party-ID header to indicate the called number, while Teams looks for it in the Request-URI header.

Rule Index	Rule Description	Reason for Introducing Rule
4	This rule applies to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group during a call transfer scenario. Replaces the host part of the SIP Referred-By header with the value from the SIP From header.	Mainly required for topology hiding.
5	This rule applies to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group in a call transfer scenario. Replaces the host part of the SIP P-Asserted-Identity header with the value from the SIP From header.	Mainly required for topology hiding.
6	This rule applies to messages sent to the Vodafone IP Anlagen-Anschluss Interface. Adds PRACK and UPDATE methods to the SIP Allow Header.	It's required in order to enable implementation of the PRACK in the Vodafone network.
7	This rule is applied to messages sent to the Vodafone IP Anlagen-Anschluss Interface. Changes the type of the SIP P-Asserted-Identity header from 'sip:' to 'tel:'.	Especially in the Registration Trunk Mode Vodafone network does not recognize calling number, presented in the SIP P-Asserted-Identity SIP URI format. As a result, the real dialing number not presented. In order to work around this P-Asserted-Identity header changed to the TEL URI format and after that replaced by P-Preferred-Identity header.
8	This rule is applied to messages sent to the Vodafone IP Anlagen-Anschluss Interface. Replaces the SIP P-Asserted-Identity header with the SIP P-Preferred-Identity header.	
9	This rule is applied to messages sent to the Vodafone IP Anlagen-Anschluss Interface. Removes the SIP P-Asserted-Identity Header in all messages.	
10	This rule is required for Static Mode ONLY. This rule is applied to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. Replaces the user part of the SIP Contact header with the value from SIP From header.	According to Vodafone requirements.
20	This rule is applied to Invite, Register and Update messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. Adds the SIP Proxy-Require header with the value 'mediasec'.	These message manipulation rules is relevant <u>only</u> for implementation encrypted (TLS/SRTP) connection to the Vodafone IP Anlagen-Anschluss Interface.
21	This rule is applied to Invite, Register and Update messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. Adds the SIP Require header with the value 'mediasec'.	
22	This rule is applied to the Register request messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. Adds the SIP Security-Client header with the value 'sdes-srtp;mediasec'.	
23	This rule is applied to the Register request messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. Adds the SIP Security-Verify header with the value 'sdes-srtp;mediasec'.	
24	This rule is applied to Invite and Update messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. Adds the SIP Proxy-Require header with the value 'sdes-srtp;mediasec'.	

Rule Index	Rule Description	Reason for Introducing Rule
25	This rule is applied to messages sent to the Vodafone IP Anlagen-Anschluss Interface IP Group. Adds the 'a=3ge2ae:requested' line to the SDP body of the message.	

19. Assign Manipulation Set ID 0 to the SIPTrunk SIP Interface:
 - a. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
 - b. Select the row of the SIPTrunk SIP Interface, and then click **Edit**.
 - c. Set the 'Pre-classification Manipulation Set ID' field to **0**.
 - d. Click **Apply**.
20. 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**.
 - d. Set the 'Outbound Message Manipulation Set' field to **2**.
 - e. Click **Apply**.
21. Assign Manipulation Set IDs 3 and 4 to the Vodafone IP Anlagen-Anschluss Interface IP Group:
 - a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
 - b. Select the row of the Vodafone IP Anlagen-Anschluss Interface IP Group, and then click **Edit**.
 - c. Set the 'Inbound Message Manipulation Set' field to **3**.
 - d. Set the 'Outbound Message Manipulation Set' field to **4**.
 - e. Click **Apply**.

4.16 Configuring Registration Account (only for Registration Trunk Mode)



This section is relevant for Registration Trunk Mode only. It should be skipped for configuring SBC in the Static Trunk Mode.

This section describes how to configure SIP registration account. This is required so that the SBC can register with the Vodafone IP Anlagen-Anschluss Interface on behalf of Teams Direct Routing. The Vodafone IP Anlagen-Anschluss Interface 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 Vodafone IP Anlagen-Anschluss Interface IP Group.

To configure a registration account:

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

Parameter	Value
Served IP Group	Teams
Application Type	SBC
Serving IP Group	SIPTrunk
Host Name	As provided by the SIP Trunk provider
Register	Regular
Contact User	As provided by the SIP Trunk provider
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

4. Click **Apply**.

According to the Vodafone IP Anlagen-Anschluss Interface requirement, the expiration period of the **Register** should not be less than 900.

To configure a registration expiration period:

1. Open the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).
2. In the 'Registration Time' field, enter **900** (according to Vodafone requirement).
3. Click **Apply**.

4.17 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.17.1 Configuring 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**.
3. Click **Apply**.

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

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

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

To optimize core allocation for a profile:

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

SBC Performance Profile ⚡

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

International Headquarters

Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

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

©2025 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, AudioCodes Meeting Insights, and AudioCodes Room Experience 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-13123

