AudioCodes Mediant[™] Family of Media Gateways & Session Border Controllers

Connecting AudioCodes' SBC with Analog Device to Microsoft Teams Direct Routing Enterprise Model

Enterprise Model



Table of Contents

Not	ice	•••••		iv			
	Secur	ity Vuln	erabilities	iv			
	WEEE	EU Dire	ective	iv			
	Custo	mer Sup	pport	iv			
	Stay i	n the Lo	op with AudioCodes	iv			
	Abbre	eviations	s and Terminology	iv			
	Relate	mentation	V				
	Docui	ment Re	vision Record	vi			
	Docui	on Feedback	vi				
1	Intro	ductior	٦	1			
	1.1	About	Microsoft Teams Direct Routing	1			
	1.2		AudioCodes SBC Product Series				
	1.3	Validat	ed AudioCodes SBC Version	2			
2	Τορο	logy Ex	ample	3			
-	2.1		rise Model Implementation				
	2.1		nment Setup				
	2.2		ructure Prerequisites				
2							
3	Configuring Teams Direct Routing						
	3.1		uisites				
	3.2		main Name in the Teams Enterprise Model				
	3.3		le of the Office 365 Tenant Direct Routing Configuration				
		3.3.1	Adding New SBC to Direct Routing				
		3.3.2	Adding Voice Route and PSTN Usage				
		3.3.3	Adding Voice Routing Policy				
		3.3.4	Enabling Online User				
		3.3.5	Assigning Online User to the Voice Routing Policy				
		3.3.6	Analog Device Voice Route Configuration				
_		3.3.7	Configuring with User Management Pack 365 (Optional)				
4			AudioCodes SBC				
	4.1		nfiguration Concept in Teams Direct Routing				
	4.2	IP Netv	vork Interfaces Configuration	17			
		4.2.1	Configuring VLANs				
		4.2.2	Configuring Network Interfaces				
	4.3		Connection Configuration				
		4.3.1	Configuring the NTP Server Address				
		4.3.2	Creating a TLS Context for Teams Direct Routing				
		4.3.3	Configuring a Certificate	21			

		4.3.4	Method for Generating and Installing the Wildcard Certificate	
		4.3.5	Deploying Trusted Root Certificate for MTLS connection	25
	4.4	Config	uring Media Realms	26
	4.5	Config	uring SIP Signaling Interfaces	27
	4.6	Config	uring Proxy Sets and Proxy Address	28
		4.6.1	Configuring Proxy Sets	
		4.6.2	Configuring a Proxy Address	
	4.7	Config	uring Coders	
	4.8	0	uring IP Profiles	
	4.9	-	uring IP Groups	
	4.10	Config	uring SRTP	
	4.11	Config	uring Message Manipulation Rules	
	4.12	Config	uring Message Condition Rules	
	4.13	Config	uring Classification Rules	43
	4.14	Config	uring IP-to-IP Call Routing Rules	45
	4.15	Config	uring Firewall Settings	46
	4.16	Config	uring SBC To Play Music On Hold (Optional)	47
5			e Pairing Between the SBC and Direct Routing	
			A Desistant differencies the CDC	
6	Verit	ying Al	A Registered Users in the SBC	
6 A			MP-1xx ATA for Connecting Analog Devices	
		iguring		50
	Conf	iguring Config	MP-1xx ATA for Connecting Analog Devices	50
	Conf	iguring Config Config	MP-1xx ATA for Connecting Analog Devices	50
	Conf A.1 A.2	iguring Config Config Config	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table	50
	Conf A.1 A.2 A.3 A.4	iguring Config Config Config Config	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group	50
Α	Conf A.1 A.2 A.3 A.4	iguring Config Config Config Config iguring	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group uring IP-to-Hunt Group Routing	50
Α	Confi A.1 A.2 A.3 A.4 Confi B.1	iguring Config Config Config Config iguring Config	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group uring IP-to-Hunt Group Routing SIP UDP Transport Type and Fax Signaling Method	50
A B	Confi A.1 A.2 A.3 A.4 Confi B.1	iguring Config Config Config Config iguring Config iguring	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group uring IP-to-Hunt Group Routing SIP UDP Transport Type and Fax Signaling Method uring MP-1xx for LAD	50 50 52 52 53 53 54 55 55
A B	Confi A.1 A.2 A.3 A.4 Confi B.1 Confi	iguring Config Config Config iguring Config iguring Config	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group uring IP-to-Hunt Group Routing SIP UDP Transport Type and Fax Signaling Method uring MP-1xx for LAD MP-20x ATA for Connecting Analog Devices	50 52 52 53 53 54 55 55 56 57
A B	Confi A.1 A.2 A.3 A.4 Confi B.1 Confi C.1	iguring Config Config Config iguring Config iguring Config Config	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group uring IP-to-Hunt Group Routing SIP UDP Transport Type and Fax Signaling Method uring MP-1xx for LAD MP-20x ATA for Connecting Analog Devices uring SIP Interface Settings	50
A B	Confi A.1 A.2 A.3 A.4 Confi B.1 C.1 C.1 C.2 C.3	iguring Config Config Config iguring Config iguring Config Config Config	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group uring IP-to-Hunt Group Routing SIP UDP Transport Type and Fax Signaling Method uring MP-1xx for LAD MP-20x ATA for Connecting Analog Devices uring SIP Interface Settings uring Media Streaming Parameters	50
A B C	Confi A.1 A.2 A.3 A.4 Confi B.1 C.1 C.1 C.2 C.3	iguring Config Config Config iguring Config iguring Config Config Config	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group uring IP-to-Hunt Group Routing SIP UDP Transport Type and Fax Signaling Method uring MP-1xx for LAD MP-20x ATA for Connecting Analog Devices uring SIP Interface Settings uring Media Streaming Parameters	50 52 52 53 53 54 55 55 56 57 58 59 60
A B C	Confi A.1 A.2 A.3 A.4 Confi B.1 Confi C.1 C.2 C.3 Synta	iguring Config Config Config iguring Config iguring Config Config Config Config Config	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group uring IP-to-Hunt Group Routing SIP UDP Transport Type and Fax Signaling Method uring MP-1xx for LAD MP-20x ATA for Connecting Analog Devices uring SIP Interface Settings uring Media Streaming Parameters uring Line Settings uring Line Settings	50 50 52 52 53 53 54 55 55 56 56 57 58 59 60 60
A B C	Confi A.1 A.2 A.3 A.4 Confi B.1 Confi C.1 C.2 C.3 Synta D.1	iguring Config Config Config iguring Config iguring Config Config Config Config Termir Syntax	MP-1xx ATA for Connecting Analog Devices uring Proxy Server and Registration uring the Endpoint Phone Number Table uring the Hunt Group uring IP-to-Hunt Group Routing SIP UDP Transport Type and Fax Signaling Method uring MP-1xx for LAD MP-20x ATA for Connecting Analog Devices uring SIP Interface Settings uring Media Streaming Parameters uring Line Settings uring Line Settings uring Line Settings	50 52 52 53 53 54 55 55 56 57 58 59 60
A B C	Confi A.1 A.2 A.3 A.4 Confi B.1 C.1 C.1 C.2 C.3 Synta D.1 D.2	iguring Config Config Config iguring Config iguring Config	MP-1xx ATA for Connecting Analog Devices	50 52 52 52 53 54 55 56 56 57 58 59 60 60 60 60 60

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: November-20-2024

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.

Related Documentation

Document Name
Mediant 500 Gateway & E-SBC User's Manual
Mediant 500L Gateway & E-SBC User's Manual
Mediant 800 Gateway & E-SBC User's Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 2600 SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
MP-11x and MP-124 SIP User's Manual
MP-20x Telephone Adapter User's Manual
SIP Message Manipulation Reference Guide

Document Revision Record

LTRT	Description
33421	Initial document release for Version 7.2. Teams Enterprise Model.
33422	Modified Section: Deploy Baltimore Trusted Root Certificate (added note for Baltimore Trusted Root Certificate and MTLS implementation).; Configure SIP Signaling Interfaces; Configure IP Groups
33423	Note removed regarding external firewall.
33424	Licenses consolidated into one section.
33425	Update to topology figures and correction for parameter "Remote Update Support" to "SIP UPDATE Support".
33426	Update to the "Related Documentation" table to include the Mediant 1000B Gateway & E-SBC product.
33427	Updates related to the usage of LAD licenses.
33428	Typo fixes, a note regarding external firewall was removed. An additional two IP addresses were added to firewall per Microsoft request.
33429	Update for Message Manipulation rule towards Microsoft Teams.
33430	"SipSignallingPort" replaced by "SipSignalingPort".
33431	Update to the Firewall Table Rules table with two additional IP addresses of the new infrastructure in Japan.
33432	Update to SIP Trunk IP Profile and validated firmware version.
33433	Added section for overcoming problem of not playing music on hold during conversational transfer.
33434	Remote Replaces Mode parameter with value "Handle Locally" was added to the Teams IP Profile due to new Microsoft requirements. The Classification rule was updated.
	Update to the Firewall Table Rules table due to new Microsoft requirements.
33435	TLS Root Certificate Authority updated by Microsoft.
33436	Updated Classification Table with stricter rules to only allow for documented Microsoft SIP Proxies.
33437	Note added detailing deployment in Office 365 GCC DoD and GCC High environments.
33438	TLS Private Key size of 1024 was removed. Microsoft subnets were updated in the Classification and Firewall tables.
33439	Teams IP Profile updated with RFC 2833 Mode parameter.

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 website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This Configuration Note describes an example setup of the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between Company's SIP Trunk, ATA device and Microsoft's Teams Direct Routing environment.

For configuring the Office 365 side, please refer to <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure</u>

This document is intended for IT or telephony professionals.

1.1 About Microsoft Teams Direct Routing

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 thirdparty PBXs, analog devices, and Microsoft Phone System

1.2 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.

i

1.3 Validated AudioCodes SBC Version

Microsoft has successfully conducted validation tests with AudioCodes' Mediant SBC Ver. 7.40A.250. Previous certified firmware versions are 7.20A.258 and 7.40A.100. For updated list refer to <u>List of</u> <u>Session Border Controllers certified for Direct Routing</u>.

For implementing Microsoft Teams Direct Routing based on the configuration described in this document, AudioCodes SBC must be installed with a License Key that includes the following 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)
- LAD (Lync Analog Devices license), which uses AudioCodes' MP-1xx as the ATA to the Microsoft Teams environment through AudioCodes' SBC
- 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.

2 Topology Example

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

2.1 Enterprise Model Implementation

The interoperability example between AudioCodes SBC and Company SIP Trunk with Teams Direct Routing Enterprise Model assume the following topology setup:

- Enterprise deployed with ATA, connected analog devices and the administrator's management station, located on the LAN
- Enterprise deployed with 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 Company's SIP Trunking service
- AudioCodes SBC is implemented to interconnect between the SIP Trunk and Teams Direct Routing located in the WAN

The figure below illustrates this topology example:

Figure 1: Connection Topology with SIP Trunk on the LAN





Figure 2: Connection Topology with SIP Trunk on the WAN

2.2 Environment Setup

The example topology includes the following environment setup:

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

Table 1: Environment Setup

2.3 Infrastructure Prerequisites

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

Table 2-2: Infrastructure Prerequisites						
Infrastructure Prerequisite	Details					
Certified Session Border Controller (SBC)						
SIP Trunks connected to the SBC						
Office 365 Tenant						
Domains						
Public IP address for the SBC						
Fully Qualified Domain Name (FQDN) for the SBC	See Microsoft's desument Dan Direct Bouting					
Public DNS entry for the SBC	See Microsoft's document <i>Plan Direct Routing.</i>					
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						

Table 2-2: Infrastructure Prerequisites

3 Configuring Teams Direct Routing

This section describes <u>an example</u> of Teams Direct Routing configuration 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, the administrator registered the following DNS names for the 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)

Table 2: DNS Names Registered by an Administrator for a Tenant

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.

	Microsoft 365 admin cer	nter						۵	?
=								🕗 Dark r	node
ŵ	Home		Domains						
Я	Users	~							
የአየ	Groups	\sim	+ Add domain 🗔 Buy domain 💍 Refresh			Search		Filter	=
R	Roles					,			
喝	Resources	\sim	Domain name ↑		Status		🗔 Choose columns		
	Billing	~	audiocode.biz (Default)	:	🕑 Heal	thy			
្ច	Support	\sim	int-sbc1.audctrunk.aceducation.info	:	Iteal	thy			
1	Settings	^	audio-codes.net	:	🕑 Heal	thy			
	Domains Microsoft Search		audiocod.onmicrosoft.com	:	Iteal:	thy			
	Org settings								
	Add-ins								
	Partner relationships								
Þ	Setup								
⊵	Reports	\sim							
÷	Health	\sim							

Figure 3: 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 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	4:	Teams	Admin	Center
--------	----	-------	-------	--------

🦸 D	ashboard - Microsoft Teams ad 🗙 🕂		– 🗆 X
÷ -	C admin.teams.microsoft.com/dashboard		🖈 👵 Incognito 🚦
	Microsoft Teams admin center		🕸 ? 🕕
≡			
介 8倍3	Dashboard		
	Microsoft Teams upgrade	Deploying Teams workload	
٢	Planning your upgrade to Teams	Use the Start button to create a Teams service management team for	
දී	We are bringing the capabilities of Skype for Business Online into Microsoft Teams to deliver a single hub for	the features you want to roll out. We'll provide you with your	
Ē	teamwork with built-in fully-integrated voice and video. We have resources and tools available to assist you in planning and upgrading some or all of your users to Teams.	organization's assessment, task- driven Planner plan and other resources to streamline the roll out.	
Ę		Start	
B	Learn more		
6			
۱. ۱	User search		
<i>.</i> 111	Search by display or username Q		
3			
ĩ			
S	 Recent searches will show up here. 		
Ø			
	View users →		
			Need help? Give feedback

3.3.1 Adding 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 5: Add new SBC to Direct Routing

	Direct Routing - Microsoft Team	⊳ × +			- 0	
÷	\rightarrow C \square admin.tean	ns.microso	fl.com/direct-routing/v2	\$	🔒 Incogn	to :
	Microsoft Teams adm	in center			©?	
		≡				
බ	Dashboard		Direct Routing	Ø Mar	iage PSTN u	sage
දිටී	Teams	~	Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable	records voice		
♣	Devices	~	calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records.	earn more		
٢	Locations	~				
සී	Users		Direct routing summary			
Ē	Meetings	~	2 4 2			
Ę	Messaging policies		Total SBCs Voice routes SBCs with issues			
₿	Teams apps	~				
ବ	Voice	^	SBCs Voice routes			
	Phone numbers		+ Add 🖉 Edit 🍈 Delete items		3	ø
	Emergency policies		T Adu // Luit i Delete items		¢	~~
	Dial plans		✓ SBC Network effectiveness ③ Average call duration ③ TLS c	connectivity statu	is 🛈	SIP of
			int-sbc1.audctrunk.acedi () 0% (0) 0 sec (0) Activ	ve		Activ
	Voice routing policies					
	Call queues					-
	Auto attendants					
	Call park policies		⑦ Nee	d help?	Give feedb	ack

3. Configure SBC.

Figure 6: Configure new SBC

ŵ	Edit SBC - Microsoft Teams ad	mir 🗙 🐳	+			-		×
÷	$ ightarrow {f C}$ $ ightarrow$ admin.tea	ms.micros	oft.com/direct-routing/int-sbc1.audctrunk.aceducation.inf	o/details/v2/settings/edit	☆	e	ncognito	
	::: Microsoft Teams admin center							
		≡	Direct Routing \ int-sbc1.audctrunk.aceducation.info					
ଜ	Dashboard		int-sbc1.audctrunk.aceducatio					
දීරී	Teams	\sim	Int-spc1.audctrunk.aceducatio	n.Into				
♣	Devices	\sim	SBC settings					
٢	Locations	~	When you are adding this SBC, you can turn on or off th	e SBC and change settings that are specific to the SBC.				
පී	Users		Enabled	On				
Ē	Meetings	~	SIP signaling port	5061				
Ę	Messaging policies		Send SIP options 🕕	On				
B	Teams apps	~	Forward call history	On				
ି	Voice	^	Forward P-Asserted-Identity (PAI) header 🕕	On				
	Phone numbers Emergency policies		Concurrent call capacity					
	Dial plans		Failover response codes	408, 503, 504				
	Direct Routing		Failover time (seconds) 🕕	10				
	Voice routing policies		Preferred country or region for media traffic	Auto			~	
	Call queues		SBC supports PIDF/LO for emergency calls	Off				
	Auto attendants		Ring phone while trying to find the user	On				
	Call park policies			() Ne	ed help?	Give	feedbac	¢

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
```



Currently, enabling MediaBypass is available only through PowerShell.

3.3.2 Adding 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 7: Add New Voice Route

ŵ	Direct Routing - Microsoft Tear	ns X +		-		×
÷	\rightarrow C $\hat{\mathbf{C}}$ admin.tear	ns.microsoft.com/direct-routing/v2/voice-routes	\$	🔒 Inc	ognito	
	Microsoft Teams adm	nin center		ø		
		=				
ଜ	Dashboard	Direct Routing	Ø Mana	ige PSTN	N usage	
்	Teams	Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable v	records /oice			
\$	Devices	calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records	arn more			
٢	Locations	× .				
දර	Users	Direct routing summary				
Ē	Meetings	× 2 4 2				
Ę	Messaging policies	Total SBCs Volce routes SBCs with issues				
B	Teams apps	× 1				
ବ	Voice	A SBCs Voice routes				
	Phone numbers	+ Add			ø	
	Emergency policies	+ Add			225	
	Dial plans	Vice route Description Dialed	number patter	n	PS	ST
		1 int-il ^\+			In	ite
	Voice routing policies	2 Israel ^\+97	72(\d{8})		Isi	ra
	Call queues	3 AC-SBCaaS-Any \d+			SE	BC
	Auto attendants	4 Test1 Only Testing				
	Call park policies	4 Test Only resting O Need	help?	Give fe	edback	

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

Figure 8: Associate SBC with new Voice Route

👘 Add voice route - Microsoft Tean 🗙			
← → C 🔒 admin.teams.micr	osoft.com/direct-routing/v2/voice-routes/add		🖈 😸 Incognito 🚦
::: Microsoft Teams admin cer			
=	Voice routes \ Add voice route		SBCs enrolled
n Dashboard			Choose the SBCs you would like to add. 1 item selected
දීලී\$ Teams 🗸 🗸	audc-interop		i nem sereceu
👃 Devices 🗸 🗸	Description	2	▶ 🗹 int-sbc1.audctrunk.aceducation.info
O Locations			qa-sbc1.audctrunk.aceducation.info
දි <mark>රි</mark> Users	Priority	1	
🛱 Meetings 🗸 🗸	Dialed number pattern	^(\+1[0-9]{10})\$	
E Messaging policies			
😰 Teams apps 🛛 🗸	SBCs enrolled		
😵 Voice 🔷	Select which SBC's you want calls to route to.	All SBC's that you add will be tried in a ra	
Phone numbers	You haven't selected any SBCs yet.		
Emergency policies		1	
Dial plans			
Direct Routing			
Voice routing policies	PSTN usage records		
Call queues	The voice routing policy is linked to a voice ro order in which the voice routing should be pr		0
Auto attendants			Ĭ
Call park policies	You haven't selected any PSTN usage recor	ds yet.	•
Calling policies	Add PSTN usage		Apply Cancel
Caller ID policies			

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

Figure 9: Associate PSTN Usage with New Voice Route

ŵ	Add voice route - Microsoft Te	arr 🗙	+		-	o x
÷	\rightarrow C $\hat{\bullet}$ admin.tea	ms.micr	osoft.com/direct-routing/v2/voice-routes/add		🖈 🌚 In	ncognito :
	Microsoft Teams adn					
			Voice routes \ Add voice route		PSTN usage records	
					You can add a new PSTN usage record o one from below.	ir select
			audc-interop		0 items selected	
			Description			
					+ Add	
			Priority	1	Srael	Ô
			Dialed number pattern	^(\+1[0-9]{10})\$	Interop	Û
					QA-PstnUsage	Î
			SBCs enrolled		SBCaas-PstnUsage	向
			Select which SBC's you want calls to route to. All SBC's th	nat you add will be tried in a ra	-	
					Testisrael	Û
			You haven't selected any SBCs yet.		Unrestricted	Ô
					Israel_Test	Ô
						_
			PSTN usage records			
			The voice routing policy is linked to a voice route using to order in which the voice routing should be processed, ar			
			You haven't selected any PSTN usage records yet.			
			Add PSTN usage		Apply Cancel	
	Caller ID policies					

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 Adding Voice Routing Policy

The procedure below describes how 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 10: Add New Voice Routing Policy

	Voice routing policies - Microso				
←	\rightarrow C \square admin.tean	s.microsoft.com/policies/teamsonlinevoicerouting	🔒 Inc	ognito	
	Microsoft Teams adm	in center			
ش ئ	Dashboard Teams	Using the order in which the usages will be processed, and assign the voice routing policy to users. Learn more			
- € •	Devices Locations	Voice routing policies summary User statistics 11 Custom policies			
8 1	Users Meetings	1 8 Default policy Custom policies 17 Default policies			
	Messaging policies Teams apps	✓ + Add		Ø	
8	Voice Phone numbers	∧ Name ↑ Description PSTN usage records			
	Emergency policies	Global (Org-wide default) Israel			
	Dial plans	İsrael İsrael			
	Direct Routing	int-il Interop			
	Call queues				
	Auto attendants				
	Call park policies	Need help?	Give fe	edback	

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





The same operations can be done using following PowerShell command:

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



The commands specified in Sections 3.3.4 and 3.3.5, should be run <u>for each</u> Teams user (<u>excluding ATA device users</u>) in the company tenant. They are currently available through PowerShell <u>only</u>.

3.3.4 Enabling Online User

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

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



The command specified in Section 3.3.6 does not need to be run for each ATA device user, if the number pattern already points to the PSTNGateway and has been associated with PSTN Usage (see Section 3.3.2).

3.3.6 Analog Device Voice Route Configuration

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

New-CsOnlineVoiceRoute -Identity "audc-interop" -NumberPattern "^\+12345678901" -OnlinePstnGatewayList int-sbc1.audctrunk.aceducation.info -Priority 1 -OnlinePstnUsages "Interop"

3.3.7 Configuring with User Management Pack 365 (Optional)

As an alternative to PowerShell commands, AudioCodes recommend using User Management Pack 365 (UMP365). UMP365 provides a simple web-portal user interface for configuring and managing the Online Voice Route and associating it with PSTN Usage and PSTN Gateway. See examples below:



Caudiocodes us					
User Management Pac	Add new Voice Route	÷ ٥ د		sync at: August	: 28, 2019 2:02 PM]
SYSTEM Office 340 Settings Letensing Replication History Audi: OVIC Settings Office Value Sould Unasigned Humber Range Reserved Klumbers Bidonies Queuted Changes	Add new Voice Route	w Voice Route Nume: pudcinterop Number Pattern: (+1246678901 brankX som	and a second sec	Interop Israel	Y A Y A Y A Y A

Figure 13: Example of Voice Routes Table

Caudiocodes	USER MANAGEMENT	SYSTEM	A CONFIGURA	ATION						count: UMPAdr	
ser Management	Pack 365								E (Last :	sync at: August	28, 2019
SYSTEM	Dial Plans	Normalizat	tion Rule Ten	nplates	PSTN Gat	eways PSTN	Usage Voic	e Routes	Voice Routing Policies		
Office 365 Settings Licensing	Add N	ew Voice Ro	oute								
Replication History	DataCh	angeType I	Identity	Priority	Pattern	Name	Description	Pattern	PSTN Gateway List	PSTN Usage	
Audit		ŧ	LocalRoute	0	+999	LocalRoute		+999			YA
OVOC Settings				ar .	^\+						YA
Online Voice Routing		l.	US	1	~1+	US		~/+	sbcRTP1.customers.audiocodesaas.com	US	
Unassigned Number Range		ŝ	int-il	2	~\{+	int-il		~1+	int-sbc2.audctrunk.aceducation.info	Interop	YA
Reserved Numbers		1	Israel	3	^\+972	Israel		^\+972	sbc1.AUDCTrunk.aceducation.info	Israel	YA
MsOnline Phone Numbers Queued Changes	14 4	1 2 2								1 - 4 of 4	

4 **Configuring AudioCodes SBC**

This section provides example of step-by-step procedures on how to configure AudioCodes SBC for interworking between Teams Direct Routing and the Company SIP Trunk. These configuration procedures are based on the topology example described in Section 2.1.1 on page 11, and includes the following main areas:

- SBC LAN interface ATA devices environment
- SBC WAN interface Company SIP Trunking and Teams Direct Routing environment

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

- For implementing Teams Direct Routing based on the configuration described in this section, AudioCodes SBC must be installed with a License Key. For more information, see Section 1.3 on page 10.
 - 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

The diagram below represents AudioCodes' device configuration concept.



Figure 14: 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 example employs the following deployment method:

- SBC interfaces with the following IP entities:
 - Teams Direct Routing and Company SIP Trunk, located on the WAN
 - IP-PBX and/or ATA, located on the LAN
- 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 example 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 15: Network Interfaces in the Example Topology



4.2.1 Configuring VLANs

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

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

To configure the VLANs:

- 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 16: Configured VLAN IDs in Ethernet Device

Ethernet Dev	vices (2)				
+ New Edit	Ē	A <	10 🔻 records per page		Q
INDEX 🗢	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING	
0	1	GROUP_1	vlan 1	Untagged	
1	2	GROUP_2	vlan 2	Untagged	

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:

- 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):

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	_	vlan 2

Table 3: Configuration Example of the Network Interface Table

The configured IP network interfaces are shown below:

Figure 17: Configured Network Interfaces in IP Interfaces Table

IP Inter	faces (2)								
+ New	Edit		🛯 🔫 Page	1of1 ► ► 5	Show 10 ▼ recor	rds per page			Q
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 Teams Direct Routing Phone System. This configuration is essential for a secure SIP TLS connection. The configuration instructions example 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 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 (Microsoft NTP server or another global server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that NTP Server will locate on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

To configure the NTP server address:

- 1. Open the Time & Date page (Setup menu > Administration tab > Time & Date).
- 2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.27.1**).



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 Creating 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:

Index	Name	TLS Version							
1	Teams (arbitrary descriptive name)	TLSv1.2							
	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.

Figure 19: Configuring TLS Context for Teams Direct Routing

GENERAL		OCSP	
Index	1	OCSP Server	Disable v
Name •	Teams	Primary OCSP Server	0.0.0.0
TLS Version •	TLSv1.2	Secondary OCSP Server	0.0.0.0
DTLS Version	Any 🔻	OCSP Port	2560
Cipher Server	DEFAULT	OCSP Default Response	Reject v
Cipher Client	DEFAULT		
Strict Certificate Extension Validation	Disable 🔻		
DH key Size •	2048		
TLS Renegotiation	Enable 🔻		
	Canc	el APPLY	

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 Teams Direct Routing.

The procedure involves the following main steps:

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

To configure a certificate:

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

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. Fill in the rest of the request fields according to your security provider's instructions.
- d. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 20: Example of Certificate Signing Request – Creating CSR

TLS Context [#1] > Change Certificates							
ERTIFICATE SIGNING REQUEST							
Common Name [CN]		int-sbc1.	aud	lctrunk.aceducat	ion.info		
Organizational Unit [OU] (optional)							
Company name [O] <i>(optional)</i>							
Locality or city name [L] (optional)							
State [ST] (optional)							
Country code [C] <i>(optional)</i>							
1st Subject Alternative Name [SAN]		DNS	~	int-sbc1.audct	unk.aceducation.inf	ⁱ o	
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					~
Note that the certificate will use the subject name configu- After creating the CSR, copy the text below (including the BEGIN CERTIFICATE REQUEST MIICtOCCAZwCAQMw.jEshCoGAIUEAwwjaWSBLXNiYzEUYXVK Y2F0aH9uLm1uZmBwggE1M406CSqGSID5DQEBAQUA41EBwWw QMKgtq-j3BQLDYIRXVK32U801U9921H313YCMY-kqCYS J/pEA6e0UaHLe2si324VP-lnctA6a00M72uc-1ip09ywlWk P2Hw4hBpx/dXX01VEwv+4UF1St0072b2LppDIYDq2zxDTI zafayjfEdwB0n5NOH6H09u+557s12UQxX-36rTRXUDo+dpdj DIrqmB27DA6RUXhwjipw/sBSQn9F2uZpu3m2rtH/EUCMQ2t 4CrngYsu4HYSSQ6x4gBMAAGqTA7ABkqAtkiS9wBCQAxhj3W I2Ludc12YmWkLm12GI08cnVuay5Nr2VkdWHAG1vbi5pbm2 CwUAA1BQAj-poA2X/FJOSUAGT+2TEu2GMkgaORNV3nzw UKv6E9/2GNhicmR2OoGkFVmRmYL8xerjTdhR3cH14/RP+1eJ skrw8G52jge18rQE5ZUJ07ABPH/xhCV3Te42YekWm3CdAV pA5jwl2B0Hj2FQC+0oxCiVaBH0EJ END CERTIFICATE REQUEST	Generate Self-Signed Certificate Create CSR BEGIN/END lines) and send it to your Certif Y3RydW5rLmfjZWR1 ggEKAoIBAQDBAdaD TIVFInaSESyUL38d 345rZhNK6XKApnF 122R4rPSmqATaTAI 10HPP-dKr4ASJdBY jjm06P/J7mx358Fh Mc4AG1U4Cg0McUcC MA06CSqdSID3DQEB 0aK3pLW8HwK0upk9 pm1173xm01sW/NWX 1hyS5ud7wUyDUYHA P8P3U2ISQ/0gFiyOC	ication Author	ity f	for signing.			
ENERATE NEW PRIVATE KEY							
Private Key Size Press the "Generate Private Key" button to create new pr Important: generation of private key is a lengthy operatio		2048					~
	and an ing million are defined bet free may be a						

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

Figure 21: Uploading the Certificate Obtained from the Certification Authority

UPLOAD CERTIFICATE FILES FROM YOUR COM	IPUTER	
Private key pass-phrase <i>(optional)</i>		•••••
Send Private Key file from your computer to The file must be in either PEM or PFX (PKCS#		
Note: Replacing the private key is not recom	mended but if it's dor	e, it should be over a physically-secure network link.
Send Device Certificate file from your com The file must be in textual PEM format.	puter to the device.	
Choose File No file chosen	Load File	←

- 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 22: Certificate Information Example

• TLS Context [#1] >	Certificate Information	
PRIVATE KEY		
Key size: Status:	2048 bits OK	
CERTIFICATE		
Certificate: Data: Version: 3 (0x2) Serial Number: 45:be:53:11:ad:89:63:80:3b Signature Algorithm: sha256V Issuer: C=IL, O=Domain The N Validity Not Before: May 4 14:24:51 Not After : May 4 14:24:51 Subject: CN= int-sbc1.audct Subject: CN= int-sbc1.audct Subject: Public Key Info: Public Key Algorithm: rsaEr RSA Public-Key: (2048 bit	WithRSAEncryption Net Technologies Ltd, CN=Domain The Net 1 2020 GMT 2022 GMT runk.aceducation.info	Technologies Ltd CA for SSL R2

- 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 23: Example of Configured Trusted Root Certificates

Viev	r -		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 for 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 into AudioCodes' SBC mandatory when implementing MTLS connection with Microsoft.

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 <u>Office TLS</u> <u>Certificate Changes</u>. Services began transitioning to the new Root CAs (e.g., DigiCert) beginning in January 2022 and will continue through October 2022. During this migration period, it's possible to load both the old (Baltimore) and the new (DigiCert) Root certificate to the same TLS Context.

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 <u>https://www.digicert.com/kb/digicert-root-certificates.htm</u> 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 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 Configuring Media Realms

This section describes how to configure Media Realms. Media Realms allow the dividing of UDP port ranges for use on different interfaces. The simplest configuration is to create Media Realms for internal (ATA) and external (Teams and SIP Trunk) traffic.

To configure Media Realms:

- 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):

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	SIPTrunk (arbitrary name)	Up	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)

Table 5: Configuration Example Media Realms in Media Realm Table

The configured Media Realms are shown in the figure below:

Figure 24: Configured Media Realms in Media Realm Table

Media Re	ealms (3)					
+ New E	dit 🟛	14 <4 Page	1 of 1 🄛 🖬	Show 10 v records	per page	Q
INDEX 🗢	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	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 **Configuring SIP Signaling Interfaces**

This section describes how to configure SIP Interfaces. A SIP Interface defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface (configured in the Interface Table above) and Media Realm.

Note that the configuration of a SIP interface for the SIP Trunk and ATA device shows <u>an example</u>, <u>which may be different to</u> your configuration. For specific configuration of interfaces relating to SIP trunks and/or a third-party PSTN environment connected to the SBC, see the trunk / environment vendor documentation.

To configure SIP Interfaces:

- 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 of the 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.

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)	500 (leave default value)	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 (Recommende d to prevent DoS attacks)	Teams	Teams
2	ATA (arbitrary name)	LAN_IF	SBC	5060 (according to Service Provider requirement)	0	0	Disable (leave default value)	500 (leave default value)	MRLan	-

Table 6: Configuration Example of SIP Signaling Interfaces



For implementing an MTLS connection with the Microsoft Teams network, configure 'TLS Mutual Authentication' to "Enable" for Teams SIP Interface.

Loading DigiCert Trusted Root Certificates to AudioCodes' SBC is mandatory for implementing an MTLS connection with the Microsoft Teams network. Refer to Section 4.3.5 on page 34.

The configured SIP Interfaces are shown in the figure below:

Figure 25: Configured SIP Interfaces in SIP Interface Table

SIP Inte	rfaces (3)								
+ New	Edit 🕴 💼		ia <a pa<="" th=""><th>ge 1 of 1</th><th>▶ ► Show</th><th>10 V records</th><th>per page</th><th></th><th>Q</th>	ge 1 of 1	▶ ► Show	10 V records	per page		Q
INDEX 🗢	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULA1 PROTOCOL	MEDIA REALM
0	SIPTrunk	DefaultSF	WAN_IF	SBC	5060	0	0	No encapsula	SIPTrunk
1	Teams	DefaultSF	WAN_IF	SBC	0	0	5061	No encapsula	Teams
2	ATA	DefaultSF	LAN_IF	SBC	5060	0	0	No encapsula	MRLan

4.6 Configuring Proxy Sets and Proxy Address

4.6.1 Configuring Proxy Sets

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 example topology, Proxy Sets need to be configured for the following IP entities:

- Company SIP Trunk
- Teams Direct Routing

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

To configure Proxy Sets:

- 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 7: Configuration Example Proxy Sets in Proxy Sets Table

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

The configured Proxy Sets are shown in the figure below:

Figure 26: Configured Proxy Sets in Proxy Sets Table

Proxy Se	ets (3)						
+ New	Edit 🛛 🗍 面	14 <4	Page 1 of 1	Show 10 ▼	records per page		Q
NDEX 🗢	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP- ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#		SIPTrunk	60		Disable
1	SIPTrunk	DefaultSRD (#		SIPTrunk	60		Disable
2	Teams	DefaultSRD (#		Teams	60		Enable

4.6.2 Configuring a Proxy Address

This section shows how to configure a Proxy Address for the SIP Trunk and Teams entities.

To configure a Proxy Address for SIP Trunk:

- 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; the following dialog box appears:

Figure 27: Configuring Proxy Address for SIP Trunk

Proxy Address			-	x
GENERAL				
Index		0		
Proxy Addre	•	SIPTrunk.com:5060		
Transport T	уре •	UDP T		

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

Table 8: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	SIPTrunk.com:5060 (SIP Trunk IP / FQDN and port)	UDP	0	0

4. Click Apply.

To configure a Proxy Address for Teams:

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

Figure 28: Configuring Proxy Address for Teams Direct Routing Interface

Proxy A	ddress		– x
	GENERAL		
	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:

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

Table 9: Configuration Proxy Address for Teams Direct Routing

4. Click Apply.



If the SBC is deployed in Office 365 GCC DoD or GCC High environments, please contact AudioCodes deployment services, since these environments have different configurations (FQDNs) than the public Office 365 environment.
4.7 Configuring Coders

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

- Open the Coder Groups table (Setup menu > Signaling & Media tab > Coders & Profiles folder > Coder Groups).
- 2. Configure a Coder Group for 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 29: Configuring Coder Group for Teams Direct Routing

Coder Groups									
	Coder	Group Name	1 : A	udioCodersGro	Jp	s_ 1 ▼	Delete	Group	
Coder Name		Packetization	Time	Rate	I	Payload	Туре	Silence Suppression	Coder Specific
SILK-NB	•	20	•	8 🔻	Π	103		N/A 🔻	
SILK-WB	•	20	•	16 🔻	Π	104		N/A 🔻	
G.711A-law	•	20	•	6 4 v	Π	8		Disabled 🔻	
G.711U-law	•	20	•	64 🔻	Ι	0		Disabled 🔹	
G.729	•	20	•	8 🔻		18		Disabled 🔹	
	•		•	•	Π			.	

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 Company 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 Company SIP Trunk in the next step.

To set a preferred coder for the Company SIP Trunk:

- 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 Company SIP Trunk.

	inguite 30. configuring P	mowed coders droup for company sir frank	
Allowe	d Audio Coders Groups [SIPT	runk Allowed Audio Coders]	– x
	GENERAL		
	Index	0	
	Name	SIPTrunk Allowed Audio Coders	

Figure 30: Configuring Allowed Coders Group for Company SIP Trunk

- 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.729

Figure 31: Configuring Allowed Coders for Company SIP Trunk

Allowed Audio Code	ers	– x
		^
GENERAL		
Index	0	
Coder	• G.729	•
User-defin	ned Coder	

- 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 example topology, IP Profiles need to be configured for the following IP entities:

- Company SIP trunk to operate in non-secure mode using RTP and SIP over UDP
- Teams Direct Routing to operate in secure mode using SRTP and SIP over TLS
- ATA device to operate in non-secure mode using RTP and SIP over UDP

To configure an IP Profile for the Company SIP Trunk:

- 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	SIPTrunk
Media Security	
SBC Media Security Mode	Not Secured
SBC Media	
Allowed Audio Coders	SIPTrunk Allowed Coders
Allowed Coders Mode	Preference (lists Allowed Coders first and then original coders in received SDP offer)
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote Replaces Mode	Handle Locally
Play RBT To Transferee	Yes (required, as some SIP Trunks do not play ring-back tone during transfer)
Remote 3xx Mode	Handle Locally

(i

Teams Hold music is not supported by Microsoft in consultative transfer of a PSTN call. The transferee will hear silence during the transfer. To overcome this issue, it is possible to configure SBC to play music during a consultative transfer. To do this, refer to Section 4.16.

IP Profiles [SIPTrunk]					– ×
GENERAL			SBC SIGNALING		
Index	1		PRACK Mode	Transparent	•
Name	SIPTrunk		P-Asserted-Identity Header Mode	Add	•
Created by Routing Server	No		Diversion Header Mode	As Is	•
			History-Info Header Mode	As Is	•
MEDIA SECURITY			Session Expires Mode	Transparent	•
SBC Media Security Mode	Not Secured	•	SIP UPDATE Support	Supported	•
Gateway Media Security Mode	Preferable	•	Remote re-INVITE	Supported	•
Symmetric MKI	Disable	•	Remote Delayed Offer Support	Supported	•
MKI Size	0		MSRP re-INVITE/UPDATE	Supported	•
SBC Enforce MKI Size	Don't enforce	•	MSRP Offer Setup Role	ActPass	•
SBC Media Security Method	SDES	*	MSRP Empty Message Format	Default	•
Reset SRTP Upon Re-key	Disable	•	Remote Representation Mode	According to Operation Mode	•
		Cancel	APPLY		

Figure 32: Configuration example: Company SIP Trunk IP Profile

3. Click Apply.

To configure IP Profile for the Teams Direct Routing:

- 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 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
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 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 doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address)
All other paramet	ers can be left unchanged at their default values.

SBC SIGNALING PRACK Mode P-Asserted-Identity Header Mode Diversion Header Mode History-Info Header Mode Session Expires Mode SIP UPDATE Support	Transparent As Is As Is As Is Transparent Transparent
PRACK Mode P-Asserted-Identity Header Mode Diversion Header Mode History-Info Header Mode Session Expires Mode	As Is
P-Asserted-Identity Header Mode Diversion Header Mode History-Info Header Mode Session Expires Mode	As Is
Diversion Header Mode History-Info Header Mode Session Expires Mode	As Is As Is Transparent
History-Info Header Mode Session Expires Mode	As Is
Session Expires Mode	Transparent 🔻
SIP UPDATE Support	Not Supported
	• 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
	MSRP re-INVITE/UPDATE MSRP Offer Setup Role MSRP Empty Message Format Remote Representation Mode

Figure 33: Configuration example: Teams Direct Routing IP Profile

3. Click Apply.

To configure an IP Profile for the ATA device:

- 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	3
Name	ΑΤΑ
Media Security	
SBC Media Security Mode	Not Secured
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote Replaces Mode	Handle Locally
Remote 3xx Mode	Handle Locally

Figure 34: Configuration example: ATA device IP Profile

IP Prof	IP Profiles [ATA] – x					– x
	GENERAL			SBC SIGNALING		
	Index			PRACK Mode	Transparent	•
	Name •	TA		P-Asserted-Identity Header Mode	As Is	v
	Created by Routing Server	10		Diversion Header Mode	As Is	•
				History-Info Header Mode	As Is	•
	MEDIA SECURITY			Session Expires Mode	Transparent	¥
	SBC Media Security Mode	Not Secured	٣	SIP UPDATE Support	Supported	•
	Gateway Media Security Mode	Preferable	•	Remote re-INVITE	Supported	•
	Symmetric MKI	Disable	T	Remote Delayed Offer Support	Supported	•
	MKI Size	0		MSRP re-INVITE/UPDATE	Supported	v
	SBC Enforce MKI Size	Don't enforce	•	MSRP Offer Setup Role	ActPass	v
	SBC Media Security Method	SDES	Ŧ	MSRP Empty Message Format	Default	•
	Reset SRTP Upon Re-key	Disable	T	Remote Representation Mode	According to Operation Mode	•
			Cancel	APPLY		

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

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

- Company SIP Trunk located on WAN
- Teams Direct Routing located on WAN
- ATA device located on LAN

To configure IP Groups:

 Open the IP Groups table (Setup menu > Signaling & Media tab > Core Entities folder > IP Groups).

Parameter	Value	
Index	1	
Name	SIPTrunk	
Туре	Server	
Proxy Set	SIPTrunk	
IP Profile	SIPTrunk	
Media Realm	SIPTrunk	
SIP Group Name	(according to ITSP requirement)	
All other parameters can remain unchanged with their default values.		

2. Configure an IP Group for the Company SIP Trunk:

Parameter	Value
Index	2
Name	Teams
Topology Location	Up
Туре	Server
Proxy Set	Teams
IP Profile	Teams
Media Realm	Teams
Classify By Proxy Set	Disable
Local Host Name	< FQDN name of the SBC in the enterprise Teams tenant > (For example, <i>sbc.ACeducation.info</i>)
Teams Direct Routing Mode	Enable (Enables the SBC to include Microsoft's proprietary X-MS-SBC header in outgoing SIP INVITE and OPTIONS messages in a Microsoft Teams Direct Routing environment. The header is used by Microsoft Teams to identify vendor equipment. The header's value is in the format 'Audiocodes/ <model>/<firmware>').</firmware></model>
Always Use Src Address	Yes
Outbound Message Manipulation Set	1
Proxy Keep-Alive using IP Group settings	Enable
All other paramete	ers can be left unchanged with their default values.

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

4. Configure an IP Group for the ATA device:

Parameter	Value				
Index	3				
Name	ΑΤΑ				
Topology Location	Up				
Туре	User				
IP Profile	ΑΤΑ				
Media Realm	MRLan				
SIP Group Name	(according to ITSP requirement)				
All other paramete	All other parameters can remain unchanged with their default values.				

4.10 Configuring SRTP

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

To configure media security:

- 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. Click Apply.

4.11 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.

Implementation of the Message Manipulation rule with Microsoft Teams (shown below) is optional according to site deployment requirements.

To configure SIP message manipulation rule for Teams:

- Open the Message Manipulations page (Setup menu > Signaling & Media tab > Message Manipulation folder > Message Manipulations).
- Configure a new manipulation rule (Manipulation Set 2) for Teams IP Group. This rule applies to messages sent towards the Teams IP Group. This rule adds a routing policy rule toward Microsoft for handling different call forwarding scenarios (according to the action values shown below).

Parameter	Value
Index	0
Name	Teams Routing Policy (arbitrary name)
Manipulation Set ID	1
Condition	
Action Subject	header.X-MS-RoutingPolicies
Action Type	Add
Action Value	One of the following values: "none", "no_missed_call", "disable_forwarding", "disable_forwarding_except_phone

4.12 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:

- 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 35: Configuring Condition Table

Messa	ge Conditions [Teams-Con ta	ct]	– x
	GENERAL		
	Index	0	
	Name	Teams-Contact	
	Condition	header.contact.url.host contains 'pstnhub.micro: Editor	

3. Click Apply.

2.

4.13 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:

 Open the Classification table (Setup menu > Signaling & Media tab > SBC folder > Classification Table).

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.*.*	sbc.ACeducation.info (example)	Teams- Contact	Allow	Teams
1	Teams_52_113 (arbitrary name)	Teams	52.113.*.*	sbc.ACeducation.info (example)	Teams- Contact	Allow	Teams
2	Teams_52_114 (arbitrary name)	Teams	52.114.*.*	sbc.ACeducation.info (example)	Teams- Contact	Allow	Teams
3	Teams_52_115 (arbitrary name)	Teams	52.115.*.*	sbc.ACeducation.info (example)	Teams- Contact	Allow	Teams
4	Teams_52_122 (arbitrary name)	Teams	52.122.*.*	sbc.ACeducation.info (example)	Teams- Contact	Allow	Teams
5	Teams_52_123 (arbitrary name)	Teams	52.123.*.*	sbc.ACeducation.info (example)	Teams- Contact	Allow	Teams

Table 10: Classification Rules

Configure Classification rules as shown in the table below:

3. Click Apply.

4. Click **New**, and then configure classification rule for messages from ATA device as follows:

Parameter	Value
Index	10
Name	ATA Users
Source SIP Interface	ΑΤΑ
Source Username Pattern	+12345678901
Action Type	Allow
Source IP Group	ΑΤΑ

lassification [ATA Users]					– ×
	SRD	#0 [Defa	aultSRD]		
MATCH			ACTION		
Index	1		Action Type	Allow	T
Name	ATA Users		Destination Routing Policy		View
Source SIP Interface •	#2 [ATA] • Vie	w	IP Group Selection	Source IP Group	Ŧ
Source IP Address			Source IP Group •	#3 [ATA]	View
Source Transport Type	Any	,	IP Group Tag Name	default	
Source Port	0		IP Profile		View
Source Username Pattern •	+12345678901				
Source Host	*				
Destination Username Pattern	*				
Destination Host	*				
	Car	ncel 🛛	APPLY		

Figure 36: Configuring Classification Rule for ATA users

5. Click Apply.

4.14 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. The routing rules use the configured IP Groups (as configured in Section 4.9 on page 47) to denote the source and destination of the call.

For the example topology, the following IP-to-IP routing rules need to be configured to route calls between Teams Direct Routing and Company SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- REGISTER requests from ATA device
- Re-Route REFER messages to Teams Direct Routing
- Calls from Teams Direct Routing to Company SIP Trunk
- Calls from Company SIP Trunk to ATA device
- Calls from Company SIP Trunk to Teams Direct Routing
- Calls from ATA device to Teams Direct Routing
- Calls from ATA device to Company SIP Trunk

To configure IP-to-IP routing rules:

- 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 11: Configuration Example: IP-to-IP Call Routing Rules

Index	Name	Source IP Group	Request Type	Dest Username Pattern	Call Triger	ReRoute IP Group	Dest Type	Dest IP Group	Internal Action
0	Terminate OPTIONS	Any	OPTIONS				Internal		Reply(Response='200')
1	ATA Registration	ΑΤΑ	REGISTER				All Users		
2	Refer re-routing (arbitrary name)	Any			REFER	Teams	Request URI	Teams	
3	To ATA	Any		+1234567890			IP Group	ΑΤΑ	
4	Teams to SIP Trunk	Teams					IP Group	SIPTrunk	
5	SIP Trunk to Teams	SIPTrunk					IP Group	Teams	
6	ATA to Teams	ΑΤΑ		12345xxxxx#			IP Group	Teams	
7	ATA to SIP Trunk	ATA					IP Group	SIPTrunk	

The configured routing rules are shown in the figure below:

IP-to-IP	Routing (8)										
+ New	Edit Insert 🛉	↓	14	<- Page 1	of 1 🏎 🖬 Show	v 10 ▼ records	per page				Q
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	DESTINATIO ADDRESS
0	Terminate OPTI	Default_SBCRou	Route Row	Any	OPTIONS	*	*	Internal			
1	ATA Registration	Default_SBCRou	Route Row	ATA	REGISTER	*	*	All Users			
2	Refer re-routing	Default_SBCRou	Route Row	Any	All	*	*	Request URI	Teams		
3	To ATA	Default_SBCRou	Route Row	Any	All	*	+1234567890	IP Group	ATA		
4	Teams to BCLD	Default_SBCRou	Route Row	Teams	All	*	*	IP Group	SIPTrunk		
5	BCLD to Teams	Default_SBCRou	Route Row	SIPTrunk	All	*	*	IP Group	Teams		
6	ATA to Teams	Default_SBCRou	Route Row	ATA	All	*	12345xxxxx#	IP Group	Teams		
7	ATA to BCLD	Default SBCRou	Route Row	ATA	All	*	*	IP Group	SIPTrunk		

(i)

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

4.15 Configuring Firewall Settings

As an 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 will apply to all incoming packets, including UDP or TCP responses.

To configure a firewall rule:

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

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<public dns="" ip="" server=""> (e.g., 8.8.8.8)</public>	32	0	65535	Any	Enable	WAN_IF	Allow
1	52.112.0.0	14	0	65535	TCP	Enable	WAN_IF	Allow
2	52.122.0.0	15	0	65535	TCP	Enable	WAN_IF	Allow
3	xxx.xxx.xxx.xxx	32	0	65535	UDP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

Table 12: Firewall Table Rules

(i)

For information about prerequisites and planning your deployment, refer to <u>Plan Direct</u> <u>Routing</u>.

Be aware that if in your configuration, connectivity to the SIP Trunk (or other entities) is performed through the same IP Interface as Teams (WAN_IF in our example), you <u>must</u> add rules to allow traffic from these entities. See an example in the row of index 3.

4.16 Configuring SBC To Play Music On Hold (Optional)

Teams Hold music is not supported by Microsoft in consultative transfer of a PSTN call. The transferee will hear silence during the transfer. To overcome this issue, it is possible to configure SBC to play music during a consultative transfer. To do this, a Prerecorded Tones (PRT) file needs to be prepared and loaded to the SBC. This section shows how to load a PRT file to the SBC. For a detailed procedure how to create a Prerecorded Tones (PRT) file, refer to appropriated AudioCodes' device *User Manual* document.

Update configuration of the SIP Trunk IP Profile:

- Open the Proxy Sets table (Setup menu > Signaling & Media tab > Coders & Profiles folder > IP Profiles).
- 2. Choose SIP Trunk IP Profile, created in the Section 4.8 on the page 43. Configure the parameters using the table below as reference.

Parameter	Value
SBC Hold	
Remote Hold Format	Send Only
Reliable Held Tone Source	No
Play Held Tone	Internal

Table 13: Update Configuration of the SIP Trunk IP Profile

3. Click **Apply**, and then save your settings to flash memory.

To load PRT file to the device using the Web interface:

- 1. Open the Auxiliary Files page:
 - Toolbar: From the Actions drop-down menu, choose Auxiliary Files.
 - Navigation tree: Setup menu > Administration tab > Maintenance folder > Auxiliary Files.
- Click the Browse button corresponding to the Prerecorded Tones file type that you want to load, navigate to the folder in which the file is located, and then click Open; the name and path of the file appear in the field next to the Browse button.
- 3. Click the Load File button corresponding to the file you want to load.
- **4.** Save the loaded auxiliary files to flash memory.

5 Verifying the Pairing Between the SBC and Direct Routing

After you have paired the SBC with Teams Direct Routing using the *New-CsOnlinePSTNGateway* PowerShell command, validate that the SBC can successfully exchange OPTIONS with Direct Routing.

To validate the pairing using SIP OPTIONS:

- 1. Open the Proxy Set Status page (Monitor menu > VoIP Status tab> Proxy Set Status).
- 2. Find the Direct SIP connection and verify that 'Status' is online. If you see a failure, you need to troubleshoot the connection first, before configuring voice routing.

				This page refreshes every 60 seconds					
PROXY SET ID	NAME	MODE	KEEP ALIVE	ADDRESS	PRIORITY	WEIGHT	SUCCESS COUNT	FAILURE COUNT	STATUS
0	ProxySet_0	Parking	Disabled						NOT RESOLVED
1	SIPTrunk	Parking	Enabled						ONLINE
				nn6300southsipconnect.adpt- tech.com(199.19.196.17:8933)(*)	1	50.00	4816	8	ONLINE
2	Teams	Load Balancing	Enabled						ONLINE
				sip.pstnhub.microsoft.com(52.114.75.24:5061)(*)	1	1.00	1	0	ONLINE
				sip2.pstnhub.microsoft.com(52.114.132.46:5061) (*)	2	1.00	1	0	ONLINE
				sip3.pstnhub.microsoft.com(52.114.14.70:5061) (*)	3	1.00	1	0	ONLINE

Figure 38: Proxy Set Status

6 Verifying ATA Registered Users in the SBC

You can view SBC users that are registered with the device. For each user, the Address of Record (AOR) and the corresponding contacts are shown.

To view registered SBC users:

 Open the SBC Registered Users page (Monitor menu > Monitor tab > VoIP Status folder > SBC Registered Users).

Figure 39: SBC Registered Users

C audioc	odes	SETUP	MONITOR	TROUBLESHOOT	Save	Reset	Actions -	<mark>2</mark>	Admin 🗸
M800B MONITOR							₽ Enti	ity, paramete	er, value
SRD All	▼								
☆ MONITOR		SBC Reg	gistered Users	5					
▶ SUMMARY			ADDRE	SS OF RECORD		CON	ITACT		
PERFORMANCE MO	NITORING		+12345678	3901@10.15.77.55	<sip:+12345678901@1< td=""><td>10.15.77.14:50</td><td>60>;expires=180</td><td> IPG:3 SI:</td><td>2 ID:95</td></sip:+12345678901@1<>	10.15.77.14:50	60>;expires=180	IPG:3 SI:	2 ID:95
VOIP STATUS									
IP-to-Tel Calls Count									
Tel-to-IP Calls Count									
SBC Registered User	s								

A Configuring MP-1xx ATA for Connecting Analog Devices

This section describes how to configure AudioCodes MediaPack[™] Series (MP-1xx) VoIP Gateways for connecting analog devices. The ATA device must be configured to send all calls to the AudioCodes SBC.

This section shows partial configuration. For detailed configuration of the MediaPack MP-1xx Series refer to the device's *User's Manual* (https://www.audiocodes.com/library/technical-documents?query=MP-11x).

A.1 Configuring Proxy Server and Registration

This section describes how to configure the proxy server and registration. The configuration below uses the example of an ATA device registered to the SBC device (10.15.77.55).

To configure Proxy Server and Registration:

 Open the Proxy & Registration page (Configuration tab > VoIP menu > SIP Definitions submenu > Proxy & Registration).

Figure 40: Proxy and Registration

& Registration		
Use Default Proxy	Yes	•
Proxy Set Table		
Proxy Name	10.15.77.55	
Redundancy Mode	Parking	٣
Proxy IP List Refresh Time	60	
Enable Fallback to Routing Table	Disable	۲
Prefer Routing Table	No	٣
Use Routing Table for Host Names and Profiles	Disable	•
Always Use Proxy	Disable	•
Redundant Routing Mode	Routing Table	•
SIP ReRoutina Mode	Standard Mode	۲
Enable Registration	Enable	۲
Registrar Name		
Registrar IP Address		
Registrar Transport Type	Not Configured	¥
Registration Time	180	
Re-registration Timing [%]	50	
Registration Retry Time	30	
Registration Time Threshold	0	
Re-register On INVITE Failure	Disable	•
ReRegister On Connection Failure	Disable	•
Gateway Name	10.15.77.55	
Gateway Registration Name		
DNS Query Type	A-Record	•
Proxy DNS Query Type	A-Record	•
Subscription Mode	Per Endpoint	•
Number of RTX Before Hot-Swap	3	
Use Gateway Name for OPTIONS	No	•

2. From the 'Use Default Proxy' drop-down list, select **Yes**.

- 3. In the 'Proxy Name' field, enter the SBC IP address.
- 4. From the 'Enable Registration' drop-down list, select **Enable**.
- 5. In the 'Gateway Name' field, enter the SBC IP address.
- 6. Click the **Proxy Set Table** button, the following page is displayed:

Figure 41: Default Proxy Sets Table

Proxy Set ID 0 ▼ I 10.15.77.55 UDP ▼ 2 Image: Constraint of the second se	Default Proxy Sets Table						
1 10.15.77.55 2 3 4 5 • Enable Proxy Keep Alive Disable • Proxy Keep Alive Time 60 Proxy Load Balancing Method		Proxy Set II	D		0	_	▼
1 10.15.77.55 2 3 4 5 • Enable Proxy Keep Alive Disable • Proxy Keep Alive Time 60 Proxy Load Balancing Method		_					
2 3 4 5 T 5 T Proxy Keep Alive Disable T Proxy Keep Alive Time 60 Proxy Load Balancing Method Disable				Proxy Address			Transport Type
3 4 5 Enable Proxy Keep Alive Proxy Keep Alive Time 60 Proxy Load Balancing Method			1	10.15.77.55			UDP V
4 5 Enable Proxy Keep Alive Disable Proxy Keep Alive Time 60 Proxy Load Balancing Method			2				T
S Image: Solution of the second sec			3				T
▼ Enable Proxy Keep Alive Disable ▼ Proxy Keep Alive Time 60 Proxy Load Balancing Method			4				T
Enable Proxy Keep Alive Disable Proxy Keep Alive Time 60 Proxy Load Balancing Method Disable			5				T
Enable Proxy Keep Alive Disable Proxy Keep Alive Time 60 Proxy Load Balancing Method Disable							
Proxy Keep Alive Time 60 Proxy Load Balancing Method Disable		-	_				
Proxy Load Balancing Method Disable		Enable Prox	у Ке	ep Alive	Disable		T
		Proxy Keep	Aliv	e Time	60		
La Draver Hat Swan		Proxy Load	Bala	ncing Method	Disable		T
15 Proxy Hot Swap		Is Proxy Ho	t Sw	/ap	No		▼

- 7. In the 'Proxy Address' field, enter the SBC IP address.
- 8. Click the **Apply** button.

A.2 Configuring the Endpoint Phone Number Table

The 'Endpoint Phone Number Table' page allows you to activate the MP-1xx ports (endpoints) by defining telephone numbers. The configuration below uses the example of ATA destination phone number '+12345678901' with all routing directed to the SBC device (10.15.77.55).

To configure the Endpoint Phone Number table:

 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 42: Endpoint Phone Number Table Page

	Channel(s)	Phone Number		Hunt Group	ID	Tel Profile ID	
1	1	+12345678901		1		0	
2							
3							
4			= +				

A.3 Configuring the Hunt Group

This section describes how to configure the Hunt Group.

To configure Hunt Group:

 Open the Hunt Group Settings page (Configuration tab > VoIP menu > GW and IP to IP sub-menu > Hunt Group > Hunt Group Settings).

Figure .	42.	11	C	Cattings
riguie	45.	пипс	Group	Settings

Group Settings					
					Bas
-					
Index		1-	12 🔻		
Hunt Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1 1	By Dest Phone Number 🗸	Per Endpoint 🔹	•		
2	▼		•		
3	▼	_	•		
4	▼	-	•		

- 2. From the 'Channel Select Mode' drop-down list, select **By Dest Phone Number**.
- 3. From the 'Registration Mode' drop-down list, select **Per Endpoint**.
- 4. Click the **Apply** button.

A.4 Configuring IP-to-Hunt Group Routing

This section describes how to configure the IP-to-Hunt Group routing rules.

To configure the IP to Hunt Group Routing table:

 Open the Tel to IP Routing page (Configuration tab > VoIP menu > GW and IP to IP submenu > Routing > IP to Hunt Group Routing).

Figure 44: IP to Hunt Group Routing Page

IP To	o Hunt Group Routing Table						-			
										Basic Paramete
		▼					-			
		Routing Index			1-12 🔻					
		IP To Tel Routing) Mode		Route calls after m	anipulation 👻				
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source	e Phone Prefix	Source IP Address	-		IP Profile	Source IP
	Dest, host Prenx	Source Host Prenx	Dest. Phone Prenx	Sourc	e Phone Prenx	Source IP Address	>	Group ID	ID	Group ID
1			*	*		*		1	0	-1
2										
3										
4										

- 2. Configure the entry as shown in the screen above.
- 3. Click the **Apply** button.

B Configuring SIP UDP Transport Type and Fax Signaling Method

In most cases ATA device is used for interconnection fax devices. This step describes how to configure the fax signaling method for the MP-1xx device.

To configure the fax signaling method:

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

SIP General Parameters		
		Basic Parameter List 🔺
▼ SIP General		
🗲 NAT IP Address	0.0.0.0	
PRACK Mode	Supported V]
Channel Select Mode	By Dest Phone Number 🔻]
Enable Early Media	Disable 🔻]
183 Message Behavior	Progress V]
Session-Expires Time	0	
Minimum Session-Expires	90	
Session Expires Method	re-INVITE V	
Asserted Identity Mode	Disabled v	
Fax Signaling Method 2	T.38 Relay]
Detect Fax on Answer Tone	Initiate T.38 on Preamble]
SIP Transport Type 3	UDP 🔻]
SIP UDP Local Port 4	5060	
SIP TCP Local Port	5060	
SIP TLS Local Port	5061	
Enable SIPS	Disable •	
Enable TCP Connection Reuse	Enable v]
TCP Timeout	0	
SIP Destination Port 5	5060	

Figure 45: SIP General Parameters Page

- 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 configuration).
- 5. In the 'SIP Destination Port', enter **5060** (corresponding to the SBC configuration).

B.1 Configuring MP-1xx for LAD

This section describes what need to be configured to enable MP-1xx to work as Analog Device with Microsoft through AudioCodes' SBC.

To configure MP-1xx for LAD:

- Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., <u>http://10.15.77.14/AdminPage</u>).
- 2. In the left pane of the page that opens, click *ini* Parameters.

Figure 46: Configuring MP-1xx for LAD in AdminPage

Image Load to Device	Parameter Name: Enter Value: DECLAREAUDCCLIENT 1
→ ini Parameters	Î
Back to	Output Window
Main	Parameter Name: DECLAREAUDCCLIENT Parameter New Value: 0 Parameter Description:0 (default): Disable 1:Add special header with capabilities for Lync
	Parameter Name: DECLAREAUDCCLIENT Parameter New Value: 1 Parameter Description:0 (default): Disable 1:Add special header with capabilities for Lync

3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
DECLAREAUDCCLIENT	1 (adds a special header with capabilities for Lync)

4. Click the **Apply New Value** button for each field.

l(i

This parameter classifies the MP-1xx's clients as LAD in the SBC.

C Configuring MP-20x ATA for Connecting Analog Devices

This section describes how to configure AudioCodes MediaPack[™] Series (MP-20x) Telephony Adapter for connecting analog devices. The ATA device must be configured to send all calls to the AudioCodes SBC.

This section shows partial configuration. For detailed configuration of the MediaPack MP-20xSeriesrefertothedevice'sUser'sManual(https://www.audiocodes.com/library/technical-documents?query=MP-20x).

C.1 Configuring SIP Interface Settings

This section describes how to configure SIP Signaling Protocol.

To configure SIP Interface Settings:

1. Click the Voice Over IP menu in the side menu bar; the Voice Over IP screen appears.

Figure 47: Signaling Protocol Page

Home Quick Setup	Voice Over IP			
Network Connections Security Voice Over IP	Signaling Protocol Media Dialing Wolce Streaming Volce and Fax Services g	Line Extension Speed Telephone HTTPS Fax Settings Dial Interface Connections		
QoS				
Advanced	Signaling Protocol			
System Monitoring	Signaling Protocol:	SIP		
Logout	SIP Transport Protocol:			
	Local SIP Port:	5060		
	Gateway Name - User Domain:			
	Enable PRACK			
	Include ptime in SDP			
	 Enable rport 			
	Connect media on 180			
	SIP Proxy and Registrar			
	🕑 Use SIP Proxy <			
	Host Name or Address:	10.15.77.55		
	Proxy Port:	5060		
	Maximum Number of Authentication Retr			
	Use SIP Proxy IP and Port for Registre			
	Register Expires:	3600 Seconds		
	Register Failed Expires:	60 Seconds		
	Sip Security:	Allow All SIP traffic 🔹		
	Redundancy Mode:	None v		
	Enable Keep Alive			
	Use SIP Outbound Proxy			
	SIP Timers			
	Retransmission Timer T1:	500 milliseconds		
	Retransmission Timer T2:	4000 milliseconds		
	Retransmission Timer T4:	5000 milliseconds		
	INVITE Timer:	32000 milliseconds		
	Session-Expires:	0 Seconds		
	Min-SE:	0 Seconds		
	√ ок	: Apply X Cancel Basic <<		

- 2. On the **Signaling Protocol** page, the following parameters enable configuration:
 - a. From the 'SIP Transport Type' drop-down list, select UDP.
 - b. In the 'Local SIP Port' field, enter 5060 (corresponding to the SBC configuration)
 - c. In the 'Use SIP Proxy' check the check box.
 - d. In the 'Host Name or Address' field, set the IP address of the SBC.
 - e. In the 'Use SIP Proxy IP and Port for Registration' check the check box.

C.2 Configuring Media Streaming Parameters

The section describes how to configure Media Streaming Parameters.

To configure Media Streaming Parameters:

- 1. Click the **Media Streaming** tab. The Media Streaming screens opens, which enables you to configure the following:
 - Supported Codecs
 - Codecs Priority
 - Packetization Time

Figure 48: Media Streaming Page

 Quick Setup Network Connections Security Voice Over IP QoS 			
Advanced Media Streaming Parameters			
System Monitoring Local RTP Port Range - Contiguous Series of 8 Ports Starting From:			
DTMF Relay RFC2833 Payload Type (default value 101): 101			
G.726/16 Payload Type (default value 98): 98			
Quality of Service Parameters			
Type Of Service (Hex): 0xb8			
Wide-Band Restrictions	I		
SRTP	SRTP		
Enabled			
Method: AES_CM_128_HMAC_SHA1_80 V	Method: AES_CM_128_HMAC_SHA1_80 V		
Codecs			
Codecs Priority Supported Codecs Packetization Time (milliseconds)			
1st Codec G.711, 64kbps, u-Law • 20 •			
2nd Codec G.711, 64kbps, A-Law • 20 •			
3rd Codec G.729, 8kbps • 20 •			
4th Codec G.726, 16kbps • 20 •			
Sth Codec G.726-32, 32kbps 20			
✓ OK T Apply X Cancel Basic <<			
	•		

C.3 Configuring Line Settings

Before you can make phone calls, you need to configure lines. Lines are logical SIP ID numbers (i.e., telephone numbers) which are registered to a SIP proxy server and for which you are charged for calls you make on it. With a MP-20x line setting configuration, you can associate any phone extension to any line.

To configure lines:

1. On the 'Voice Over IP' screen, click the Line Settings tab; the following screen appears.

Figure 49: Line Settings Tab Screen Voice Over IP ♦ Home Quick Setup Network Connections Line **Security** Voice Over IP ♦QoS Lin Actio lser ID Display N Advanced +12345678901 ATA Line 1 1 System Monitoring 2 0000000000 Line 2 ٩. ♦ Logout Phon Phone2 1 X Cancel V OK Apply

2. For each line, click the corresponding **Edit** $\stackrel{>}{\searrow}$ icon to configure the line; the following screen appears:

Figure 50: Line Setting	s Screen for a New Line
-------------------------	-------------------------

		S			
♦Home		Line Settings			
Quick Setup					
Network Connections	Line Number:	1			
♦ Security	User ID:	+12345678901			
♦Voice Over IP	Block Caller ID				
♦ QoS	Display Name:	ATA Line 1			
Advanced	Extensions Registered:	Phone1			
System Monitoring	Extensions Registered.	THORE			
◆ Logout	SIP Proxy				
	Authentication User Name:	admin			
	Authentication Password:	•••••			
	Advanced Line Parameters				
	Enable Supplementary Services	✓ Enable Supplementary Services			
	√ ок	✓ OK X Cancel Basic <<			

- **3.** In the 'User ID' field, enter phone's VoIP user ID used for identification to initiate and accept calls.
- 4. To hide the phone's ID from the remote party, select the 'Block Caller ID' check box.
- 5. In the 'Display Name' field, enter a name to intuitively identify the line. This is also displayed to remote parties as your caller ID.
- 6. Click **OK** to save your settings.

D Syntax Requirements for SIP Messages 'INVITE' and 'OPTIONS'

The syntax of SIP messages must conform with Teams Direct Routing requirements.

This section covers the high-level requirements for the SIP syntax used in 'INVITE' and 'OPTIONS' messages. You can use the information presented here as a first step when troubleshooting unsuccessful calls. AudioCodes has found that most errors are related to incorrect syntax in SIP messages.

D.1 Terminology

Must	Strictly required. The deployment does not function correctly without the correct configuration of these parameters.
------	--

D.2 Syntax Requirements for 'INVITE' Messages

Figure 51: Example of an 'INVITE' Message

```
INVITE sip:+97249888108@10.15.40.55;user=phone SIP/2.0
Via: SIP/2.0/TLS sbc.ACeducation.info:5068;alias;branch=z9hG4bKac496289557
Max-Forwards: 69
From: <sip:+97239762000@10.15.77.12>;tag=lc1642854452
To: <sip:+97249888108@10.15.40.55;user=phone>
Call-ID: 1167963076285201992217@ACeducation.info
CSeq: 1 INVITE
Contact: <sip:+97239762000@sbc.ACeducation.info:5068;transport=tls>
Supported: em,100rel,timer,replaces,path,resource-priority,sdp-anat
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: 10.15.40.55/v.7.20A.250.273
Content-Type: application/sdp
Content-Length: 1114
```

- Contact header
 - **MUST:** When placing calls to the Direct Routing interface, the 'CONTACT' header must have the SBC FQDN in the URI hostname
 - Syntax: Contact: <phone number>@<FQDN of the SBC>:<SBC Port>;<transport type>
 - If the parameter is not configured correctly, calls are rejected with a '403 Forbidden' message.

D.3 Requirements for 'OPTIONS' Messages Syntax

Figure 52: Example of 'OPTIONS' message

```
OPTIONS sip:195.189.192.171 SIP/2.0
Via: SIP/2.0/TLS sbc.ACeducation.info:5068;alias;branch=z9hG4bKac1385438539
Max-Forwards: 70
From: <sip:195.189.192.171>;tag=1c1890841146
To: <sip:195.189.192.171>
Call-ID: 59585523229520193103@ACeducation.info
CSeq: 1 OPTIONS
Contact: <sip sbc.ACeducation.info:5068;transport=tls>
Allow: REGISTER.OPTIONS,INVIE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: 10.15.40.55/v.7.20A.250.273
Accept: application/sdp, application/simple-message-summary, message/sipfrag
Content-Length: 0
```

Contact header

- **MUST:** When placing calls to the Direct Routing interface, the 'CONTACT' header must have the SBC FQDN in the URI hostname
- Syntax: Contact: <phone number>@<FQDN of the SBC>:<SBC Port>;<transport type>
- If the parameter is not configured correctly, the calls are rejected with a '403 Forbidden' message

The table below navigates to the path in the Web interface where the parameters are configured and refers to the relevant location in this document including the configuration instructions.

Parameter	Where Configured	How to Configure
Contact	Setup > Signaling and Media > Core Entities > IP Groups > <group name=""> > Local Host Name</group>	See Section 4.9 Configure IP Groups
	In IP Groups, 'Contact' must be configured. In this field ('Local Host Name'), define the local host name of the SBC as a string, for example, <i>sbc.ACeducation.info</i> . The name changes the host name in the call received from the IP group.	

Table 14: Syntax Requirements for an 'OPTIONS' Message

D.4 Connectivity Interface Characteristics

The table below shows the technical characteristics of the Direct Routing interface.

In most cases, Microsoft uses RFC standards as a guide during development, but does not guarantee interoperability with SBCs - even if they support all the parameters in the table below - due to the specifics of the implementation of the standards by SBC vendors.

Microsoft has a partnership with some SBC vendors and guarantees their devices' interoperability with the interface. All validated devices are listed on Microsoft's website. Microsoft only supports devices *that are validated* in order to connect to the Direct Routing interface.

AudioCodes is one of the vendors who are in partnership with Microsoft.

AudioCodes' SBCs are validated by Microsoft to connect to the Direct Routing interface.

Category	Parameter	Value	Comments
Ports and IP ranges	SIP Interface FQDN Name	See Microsoft's document Deploying Direct Routing Guide.	-
	IP Addresses range for SIP interfaces	See Microsoft's document Deploying Direct Routing Guide.	-
	SIP Port	5061	-
	IP Address range for Media	See Microsoft's document Deploying Direct Routing Guide.	-
	Media port range on Media Processors	See Microsoft's document Deploying Direct Routing Guide.	-
	Media Port range on the client	See Microsoft's document Deploying Direct Routing Guide.	-
Transport	SIP transport	TLS	-
and Security	Media Transport	SRTP	-
Security	SRTP Security Context	DTLS, SIPS Note: Support for DTLS is pending. Currently, SIPS must be configured. When support for DTLS will be announced, it will be the recommended context.	https://tools.ietf.org/html/ rfc5763
	Crypto Suite	AES_CM_128_HMAC_SHA1_80, non-MKI	-
	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP MUX helps reduce the number of required ports
	Supported Certification Authorities	See the Deployment Guide	-
	Transport for Media Bypass (of configured)	 ICE-lite (RFC5245) – recommended Client also has Transport Relays 	-
	Audio codecs	 G711 Silk (Teams clients) Opus (WebRTC clients) - only if Media Bypass is used G729 	-
Codecs	Other codecs	 CN Required narrowband and wideband RED - Not required DTMF - Required Events 0-16 Silence Suppression - Not required 	-

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: <u>https://www.audiocodes.com/corporate/offices-worldwide</u> Website: <u>https://www.audiocodes.com</u>

©2024 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-33439

