Configuration Note

AudioCodes Professional Services – Interoperability Lab

Connecting Talkdesk Cloud Contact Center to Generic SIP Trunk using AudioCodes Mediant™ SBC

Table of Contents

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: December-14-2022

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
39365	Initial document release.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Session Border Controller (hereafter, referred to as *SBC*) for interworking between Talkdesk's Cloud Contact Center and Generic SIP Trunk.

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

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and Talkdesk partners who are responsible for configuring Talkdesk's Cloud Contact Center and Generic SIP Trunk for enabling interconnection between them using AudioCodes SBC.

1.2 About Talkdesk's Cloud Contact Center

Talkdesk's Cloud Contact Center offers a full set of enterprise-level, integrated Contact Center applications for customer self-service, omnichannel engagement, workforce engagement, employee collaboration, and customer experience analytics to align and drive Contact Center winning behaviors across the organization — all native on Talkdesk's Cloud platform. This full set of enterprise-level, integrated Contact Center applications includes tools.

1.3 About AudioCodes SBC Product Series

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

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

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

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

2 Component Information

2.1 AudioCodes SBC Version

Table 1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500/L Gateway & E-SBC ▪ Mediant 800B/C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000/B SBC ▪ Mediant 9000/9030/9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.40A.250.609 or later
Protocol	SIP/TLS (to both, Talkdesk and SIP Trunk)
Additional Notes	None

2.2 Talkdesk Cloud Call Center

Table 2: Talkdesk Cloud Call Center

Vendor/Service Provider	Talkdesk
SSW Model/Service	Cloud Call Center
Software Version	
Protocol	SIP
Additional Notes	None

2.3 SIP Trunking Version (Optional)

Table 3: SIP Trunking Version

Vendor	
Model	
Software Version	
Protocol	SIP
Additional Notes	None

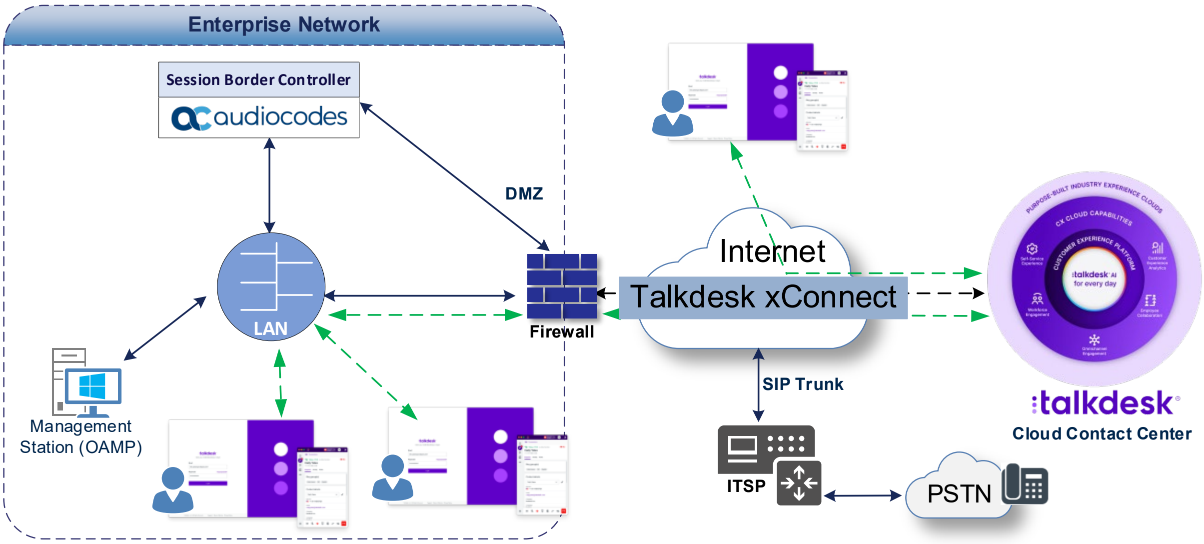
2.4 Interoperability Test Topology

The interoperability testing between Talkdesk Cloud Call Center and Generic SIP Trunk using AudioCodes SBC was done using the following topology setup:

- Enterprise deployed with the administrator's management station, located on the LAN
- Talkdesk platform deployed in the public Cloud
- Enterprise wishes to offer its employees an end-to-end contact center solution with enterprise-voice capabilities and to connect the Talkdesk Cloud Call Center to the PSTN network using the Generic SIP Trunking service
- AudioCodes SBC is implemented to interconnect between the Talkdesk platform and the Generic SIP Trunk using the following:
    - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
    - **Border:** IP-to-IP network border – both, Talkdesk's platform and Generic SIP Trunk are located in the public network.

The figure below illustrates this interoperability test topology:

Figure 1: Layout of an Interoperability Test Environment



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 4: Environment Setup

Area	Setup
Network	Both, Talkdesk's platform and Generic SIP Trunk are located in the public network
Signaling Transcoding	Both, Talkdesk's platform and Generic SIP Trunk operates with SIP-over-TLS transport type
Codecs Transcoding	Generic SIP Trunk supports G.711A-law, G.711U-law and G.729 coders Talkdesk platform supports G.711A-law and G.711U-law coders
Media Transcoding	Both, Talkdesk's platform and Generic SIP Trunk operates with SRTP media type

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes SBC interworking between Talkdesk's platform and Generic SIP Trunk.

3 Talkdesk BYOC Onboarding

Customers interested in the interconnection between Generic SIP Trunk and Talkdesk xConnect BYOC platform, should contact Talkdesk's representative for the onboarding process.

4 Configuring AudioCodes SBC

This section provides step-by-step procedures on how to configure AudioCodes SBC for interworking between the Talkdesk platform and the Generic SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 3, and includes the following main areas:

- SBC LAN interface – Management Station
- SBC WAN interface – Talkdesk platform and Generic SIP Trunk

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

- For implementing Generic SIP Trunk and the Talkdesk platform based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
- **Number of SBC sessions** (based on requirements)
- **Transcoding sessions** (only if media transcoding is needed)
- **Coders** (based on requirements)

  For more information about the License Key, contact your AudioCodes sales representative.
- If your SBC is deployed in a virtual environment and transcoding is required, your virtual machine must have a minimum of two vCPUs. For more information, please refer to the appropriate *Installation Manual,* which can be found on AudioCodes website.
- The scope of this document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at AudioCodes web site

4.1 SBC Configuration Concept

The diagram below represents AudioCodes' device configuration concept.

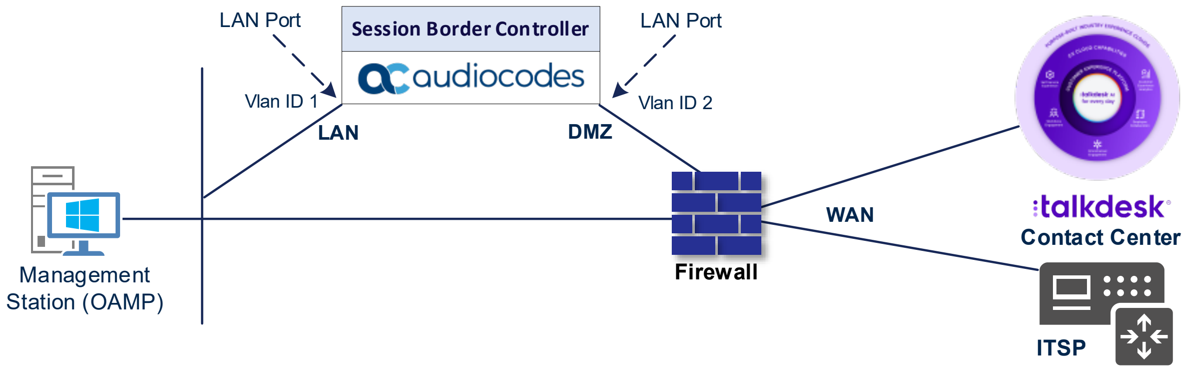
Figure 2: SBC Configuration Concept

4.2 IP Network Interfaces Configuration

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

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

Figure 3: Network Interfaces in Interoperability Test Topology



4.2.1 Configure VLANs

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

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

To configure the VLANs:

1. Open the Ethernet Device table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).
2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side

4.2.2 Configure Network Interfaces

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

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

To configure the IP network interfaces:

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

Table 5: Configuration Example of the Network Interface Table

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

4.3 SIP TLS Connection Configuration

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

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

This certificate module is based on the customer’s own TLS Certificate.

The Talkdesk platform allows ***only*** TLS connections from SBCs for SIP traffic with a certificate signed by one of the Trusted Certification Authorities.

Public Certificates used by Talkdesk are:

- GeoTrust_TLS_RSA_CA_G1
- DigiCert_Global_Root_G2

4.3.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (any local or global NTP 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**).
3. Click **Apply**.

4.3.2 Create a TLS Context for Talkdesk platform

This section describes how to configure TLS Context in the SBC. The Talkdesk platform supports TLS Version 1.2 and SSL v3. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

To configure the TLS version:

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

Table 6: New TLS Context

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

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

3. Click **Apply**.

4.3.3 Configure a Certificate

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

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 our example, **int-sbc1.audctrunk.aceducation.info**).
   c. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024.

   d. To change the key size on TLS Context, go to: **Generate New Private Key**, change the 'Private Key Size' to the value required by your CA and then click **Generate Private-Key**. To use **2048** as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
   e. Fill in the rest of the request fields according to your security provider's instructions.
   f. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button.
4. Copy the CSR from the line **"----BEGIN CERTIFICATE REQUEST" to "END CERTIFICATE REQUEST----**" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, for example *certreq.txt*.
5. Send *certreq.txt* file to the Certified Authority Administrator for signing.
6. After obtaining an SBC signed and Trusted Root/Intermediate Certificate from the CA, in the SBC's Web interface, return to the **TLS Contexts** page and do the following:
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
   b. Scroll down to the **Upload certificates files from your computer** group, click the **Choose File** button corresponding to the '**Send Device Certificate**...' field, navigate to the certificate file obtained from the CA, and then click **Load File** to upload the certificate to the SBC.
7. Confirm that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.
8. In the SBC's Web interface, return to the **TLS Contexts** page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name.
9. In the SBC's Web interface, return to the **TLS Contexts** page.
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   b. Click the **Import** button, and then select all Root/Intermediate Certificates obtained from your Certification Authority to load.
10. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

4.3.4 Method of Generating and Installing the Wildcard Certificate

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

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

To install the certificate:

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

4.4 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the SIP Trunk traffic and one for the Talkdesk platform traffic.

To configure Media Realms:

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

Table 7: Configuration Example Media Realms in Media Realm Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	MR-SIPTrunk (arbitrary name)		WAN_IF	7000	100 (media sessions assigned with port range)
1	MR-Talkdesk (arbitrary name)	Up	WAN_IF	6000	100 (media sessions assigned with port range)

4.5 Configure SIP Signaling Interfaces

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

Configuration of a SIP Interface for the Generic SIP Trunk is a configuration example and your configuration might be different. For specific configurations of interfaces pointing to SIP trunks and/or a third-party PSTN environments connected to the SBC, refer to the trunk / environment vendor documentation.

To configure SIP Interfaces:

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

The Talkdesk platform can only use TLS for a SIP port. It does not support using TCP due to security reasons.

Table 8: Configured SIP Interfaces in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name
0	**SI-SIPTrunk** (arbitrary name)	**WAN_IF**	**SBC**	**0**	**0**	**5062** (according to Service Provider requirement)	**Enable**	**0** (Recommended to prevent DoS attacks)	**MR-SIPTrunk**	**default**
1	**SI-Talkdesk** (arbitrary name)	**WAN_IF**	**SBC**	**0** (Talkdesk does not use UDP or TCP for SIP signaling)	**0**	**5061** (as configured in the Talkdesk)	**Enable**	**0** (Recommended to prevent DoS attacks)	**MR-Talkdesk**	**Talkdesk**

4.6 Configure Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- Talkdesk platform
- Generic SIP Trunk

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

To configure Proxy Sets:

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

Table 9: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap
1	SIPTrunk (arbitrary name)	SI-SIPTrunk	default	Using Options	-	-
2	Talkdesk (arbitrary name)	SI-Talkdesk	Talkdesk	Using Options	Homing	Enable

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

4.6.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

To configure a Proxy Address for SIP Trunk:

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

Table 10: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	SIPTrunk.com:5061 (SIP Trunk IP / FQDN and port)	TLS	0	0

3. Click **Apply**.

To configure a Proxy Address for Talkdesk platform:

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

Table 11: Configuration Proxy Address for Talkdesk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	sbc2.eu-west-3.cpaas.talkdeskapp.com:5061	TLS	1	1
1	sbc2.eu-south-1.cpaas.talkdeskapp.com:5061	TLS	2	1

3. Click **Apply**.

This example is based on configuration Talkdesk's Europe Servers. In your implementation, the FQDN may be different according to your region. Contact your Talkdesk representative for other Talkdesk Regional Servers.

4.7 Configure Coders

This section describes how to configure coders (termed *Coder Group*). As Talkdesk xConnect BYOC platform supports the G.711 A-law and G.711 U-law coders while the network connection to the Generic 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 Talkdesk platform and the Generic SIP Trunk.

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

To configure coders:

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

Parameter	Value
Coder Group Name	**AudioCodersGroups_1**
Coder Name	▪ G.711 A-law ▪ G.711 U-law

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 Talkdesk environment uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the Talkdesk in the next step.

To set a preferred coder for the Talkdesk:

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New,** and then configure a name for the Allowed Audio Coders Group for Talkdesk (e.g., *Talkdesk Allowed Coders*).
3. Click **Apply.**
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

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

6. Click **Apply.**

> Repeat the same procedure for Generic SIP Trunk if it's required.

4.8 Configure IP Profiles

This section describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

- Generic SIP trunk – to operate in secure mode using SRTP and SIP over TLS
- Talkdesk platform – to operate in secure mode using SRTP and SIP over TLS

To configure an IP Profile for the Generic SIP Trunk:

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

Parameter	Value
General	
Index	**1**
Name	**SIPTrunk** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_0**
Allowed Audio Coders	**SIPTrunk Allowed Coders**

3. Click **Apply**.

The configuration may change according to the SIP Trunk specific requirements.

To configure IP Profile for the Talkdesk platform:

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

Parameter	Value
General	
Index	**2**
Name	**Talkdesk** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Remove Unknown Crypto	**Yes**
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
Allowed Audio Coders	**Talkdesk-allowed**
RFC 2833 Mode	**Extend**
SBC Signaling	
Remote re-INVITE Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**

3. Click **Apply**.

4.9 Configure IP Groups

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

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

- Generic SIP Trunk
- Talkdesk platform

To configure IP Groups:

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

Parameter	Value
Index	**1**
Name	**SIPTrunk** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**SIPTrunk**
IP Profile	**SIPTrunk**
Media Realm	**MR-SIPTrunk**
SIP Group Name	(according to ITSP requirement)

3. Configure an IP Group for the Talkdesk platform:

Parameter	Value
Index	**2**
Name	**Talkdesk** (arbitrary descriptive name)
Topology Location	**Up**
Type	**Server**
Proxy Set	**Talkdesk**
IP Profile	**Talkdesk**
Media Realm	**MR-Talkdesk**
Proxy Keep-Alive using IP Group settings	**Enable**

4.10 Configure SRTP

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

To configure media security:

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

4.11 Configure IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Talkdesk platform and Generic SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Calls from Talkdesk to Generic SIP Trunk
- Calls from Generic SIP Trunk to Talkdesk

To configure IP-to-IP routing rules:

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

Table 12: Configuration IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Call Triger	ReRoute IP Group	Dest Type	Dest IP Group	Internal Action
0	Terminate OPTIONS	Any	OPTIONS			Internal		Reply (Response=' 200')
1	Talkdesk to SIP Trunk (arbitrary name)	Talkdesk				IP Group	SIPTrunk	
2	SIP Trunk to Talkdesk (arbitrary name)	SIPTrunk				IP Group	Talkdesk	

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

4.12 Configure Number Manipulation Rules

This section describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups as configured in Section 4.9 on page 17 to denote the source and destination of the call.

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

For example, for this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number (if it not exists) for calls from the Generic SIP Trunk IP Group to the Talkdesk IP Group for any destination username pattern.

To configure a number manipulation rule:

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

The table below shows an example of configured IP-to-IP outbound manipulation rules for calls between Generic SIP Trunk IP Group and Talkdesk IP Group:

Rule Index	Description
0	Calls from ITSP IP Group to Talkdesk IP Group with the prefix destination number "+", do nothing.
1	Calls from ITSP IP Group to Talkdesk IP Group with any destination number (*), add "+" to the prefix of the destination number.

4.13 Configure Message Manipulation Rules (Optional)

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.

> This document describes a configuration example for the Generic SIP Trunk and your configuration might be different. For specific configurations of the message manipulation rules related to SIP trunks and/or a third-party PSTN environment connected to the SBC, refer to the trunk / environment vendor documentation.

4.14 Configure Registration Accounts (Optional)

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the Generic SIP Trunk on behalf of Talkdesk, if the Generic SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group was Talkdesk IP Group and the Serving IP Group was Generic SIP Trunk IP Group.

To configure a registration account:

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

Parameter	Value
Served IP Group	**Talkdesk**
Application Type	**SBC**
Serving IP Group	**SIPTrunk**
Host Name	As provided by the SIP Trunk provider
Register	**Regular**
Contact User	**xxxxxxxxxxxx** (trunk main line DID)
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

4. Click **Apply**.

4.15 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.15.1 Configure Call Forking Mode

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

To configure call forking:

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

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

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

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

To optimize core allocation for a profile:

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

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

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

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

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

Document #: LTRT-39365