
Ribbon SBC Edge SWe Lite R11.0 on Azure Interop with Cisco UCM and Microsoft Teams Direct Routing : Interoperability Guide



- Interoperable Vendors
- Copyright
- Document Overview
 - About Ribbon SBC SWe Edge
 - About Cisco Unified Communications Manager
 - About Microsoft Teams Direct Routing
- Scope
- Non-Goals
- Audience
- Pre-Requisites
- Product and Device Details
- Network Topology Diagram
 - Deployment Topology
 - Interoperability Test Lab Topology (Call Flow Diagram)
- Document Workflow
- Section A: Ribbon SBC SWe Edge Configuration
 - Installing Ribbon SBC SWe Edge On Azure
 - Accessing Ribbon SBC SWe Edge
 - View Networking Interfaces
 - Configure Static Routes
 - License and TLS Certificates
 - View License
 - Import Trusted Root CA Certificates
 - Ribbon SWe Edge Configuration towards CUCM and Microsoft Teams Cloud
 - Access the Easy Configuration Wizard
 - Configure Ribbon SBC SWe Edge for CUCM and Microsoft Teams
 - Create and Modify Ribbon SBC SWe Edge Configuration
 - Create SRTP Profile
 - Update Media List
 - Enable Dead Call Detection
 - TLS Profile
 - Update Signaling group
 - Update SIP Server Tables
 - Transformation Table
 - To Modify a Transformation Table
 - Creating an Entry to a Message Transformation Table
 - Call Routing Table
 - Modifying an Entry to a Call Routing Table
 - Creating an Entry to a Call Routing Table
- Section B: CUCM Configuration
 - Accessing CUCM (Cisco Unified CM Administration)
 - Configure SIP Trunk Security Profile
 - Configure SIP Profiles
 - Configure Phone Security Profiles
 - Configure Media Resource Group
 - Configure Call Routing
 - Configure End Users
 - Phone Setup
 - Enable MoH
- Section C: Microsoft Teams Direct Routing
- Supplementary Services & Features Coverage
- Caveats
- Support
- References
- Conclusion

Interoperable Vendors



Copyright

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved. The compilation (meaning the collection, arrangement and assembly) of all content on this site is protected by U.S. and international copyright laws and treaty provisions and may not be used, copied, reproduced, modified, published, uploaded, posted, transmitted or distributed in any way, without prior written consent of Ribbon Communications Inc.

The trademarks, logos, service marks, trade names, and trade dress ("look and feel") on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

Document Overview

This document provides the configuration snapshot of the interoperability performed between Ribbon's SWe Edge on Azure with on-premise Cisco Unified Communications Manager (CUCM).

References

- For additional information on Cisco Unified Communications Manager, refer to <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>
- For additional information on Ribbon's SWe Edge, refer to [Deploying an SBC SWe Edge from the Azure Marketplace](#)

Alert

From Release 11.0.0 onwards, Ribbon "**SBC SWe Lite**" has been rebranded as "**SBC SWe Edge**".

About Ribbon SBC SWe Edge

The Ribbon Session Border Controller Software Edition Edge (SBC SWe Edge) provides best-in class communications security. The SBC SWe Edge dramatically simplifies the deployment of robust communications security services for SIP Trunking, Direct Routing and Cloud UC services. The SBC SWe Edge operates natively in the Azure and AWS Cloud as well as on virtual machine platforms including Microsoft Hyper-V, VMware and Linux KVM.

About Cisco Unified Communications Manager

Cisco Unified Communications Manager is a core call-control application of Cisco UCM. It provides enterprise-class call control, session management, voice, video, messaging, mobility and conferencing services in a way that is efficient, highly secure, scalable and reliable.

About Microsoft Teams Direct Routing

Microsoft Phone System Direct Routing allows the connection of a supported customer-provided Session Border Controller (SBC) to a Microsoft Phone System. Direct Routing enables using virtually any PSTN trunk with the Microsoft Phone System and configuring interoperability between customer-owned telephony equipment, such as a third-party private branch exchange (PBX), analog devices, and Microsoft Phone System.

Scope

This document provides configuration best practices for deploying Ribbon's SBC SWe Edge with Cisco Unified Communications Manager (CUCM). Note that these are configuration best practices and each customer may have unique needs and networks. Ribbon recommends that customers work with network design and deployment engineers to establish the network design that best meets their requirements.

Non-Goals

It is not the goal of this guide to provide detailed configurations that will meet the requirements of every customer. Use this guide as a starting point and build the SBC configurations in consultation with network design and deployment engineers.

Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring both the Ribbon SBC and the third-party product. Navigating the third-party product as well as the Ribbon SBC SWe Edge GUI is required. Understanding the basic concepts of TLS/TCP/UDP, IP/Routing, and SIP/SRTP is also necessary to complete the configuration and any required troubleshooting.

Pre-Requisites

The following aspects are required before proceeding with the interop:

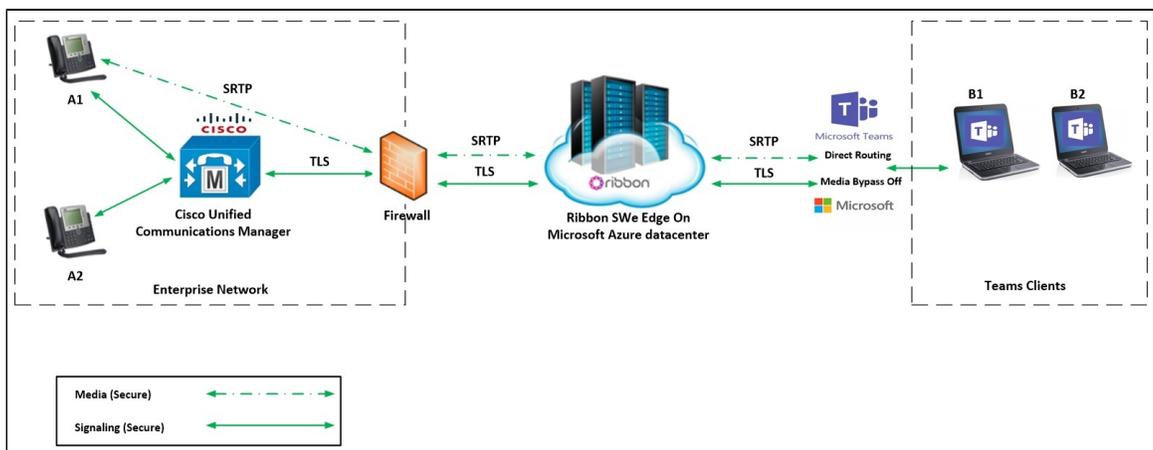
- Microsoft Azure subscription
- Ribbon SBC SWe Edge on Azure
- SBC SWe Edge License
 - This interop requires the acquisition and application of cloud SIP sessions, as documented at [Cloud-Based SBC SWe Edge Deployment Licenses](#)
- Public IP Addresses
- Service Provider SIP Trunk
- TLS Certificates for SBC SWe Edge
 - Refer to [Working with Certificates](#)

Product and Device Details

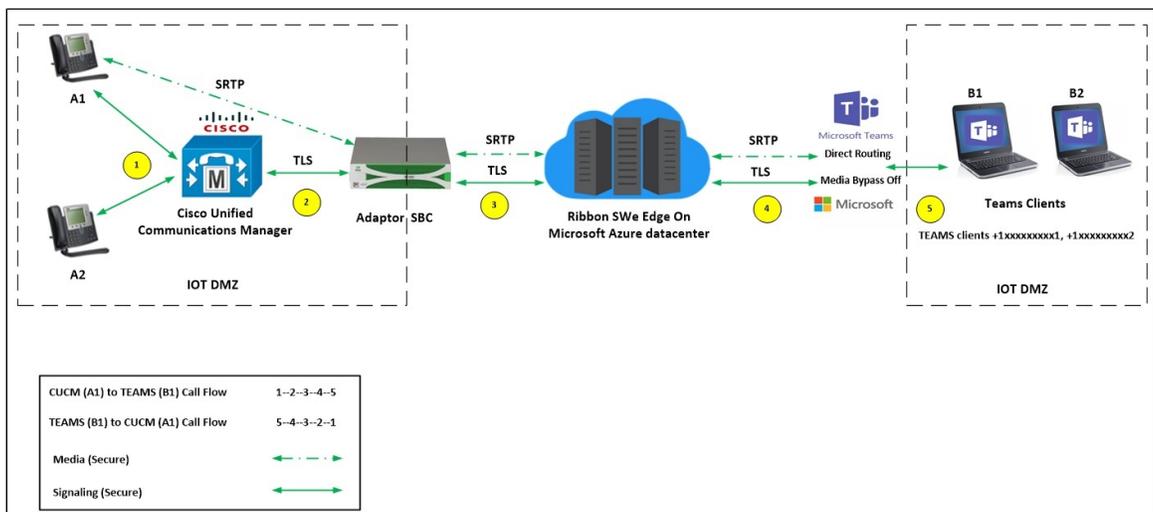
	Equipment/ Product	Software Version
Ribbon Communications	Ribbon SBC SWe Edge	11.0
Third-Party Products	Cisco Unified Communications Manager	12.5
Third-Party Phones	Cisco Jabber client	12.6.1.34405
Microsoft Corporation	Microsoft Teams Client Desktop app	1.4.00.19572
	Microsoft Teams Client Mobile app	1416
Administration and Debugging Tools	Wireshark	3.2.7
	LX Tool	2.1.0.6

Network Topology Diagram

Deployment Topology

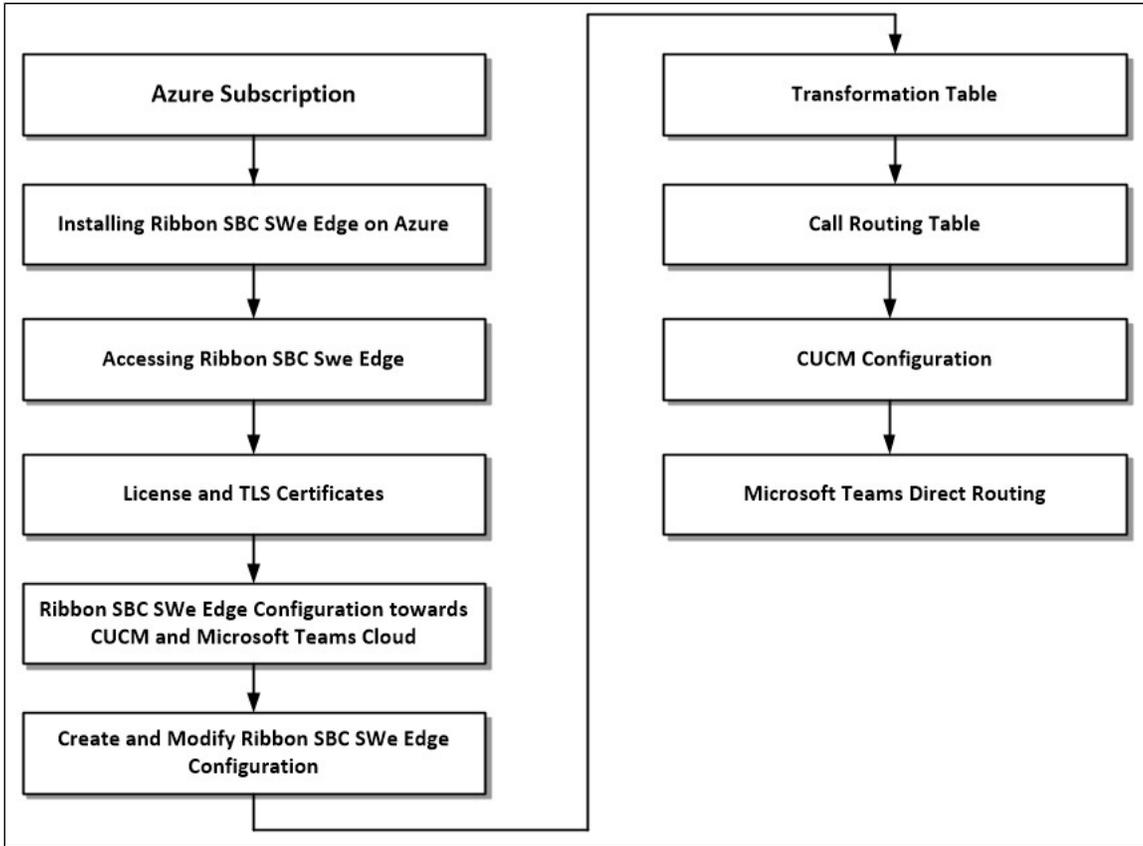


Interoperability Test Lab Topology (Call Flow Diagram)



Document Workflow

The sections in this document follow the sequence below. The reader is advised to complete each section for successful configuration.



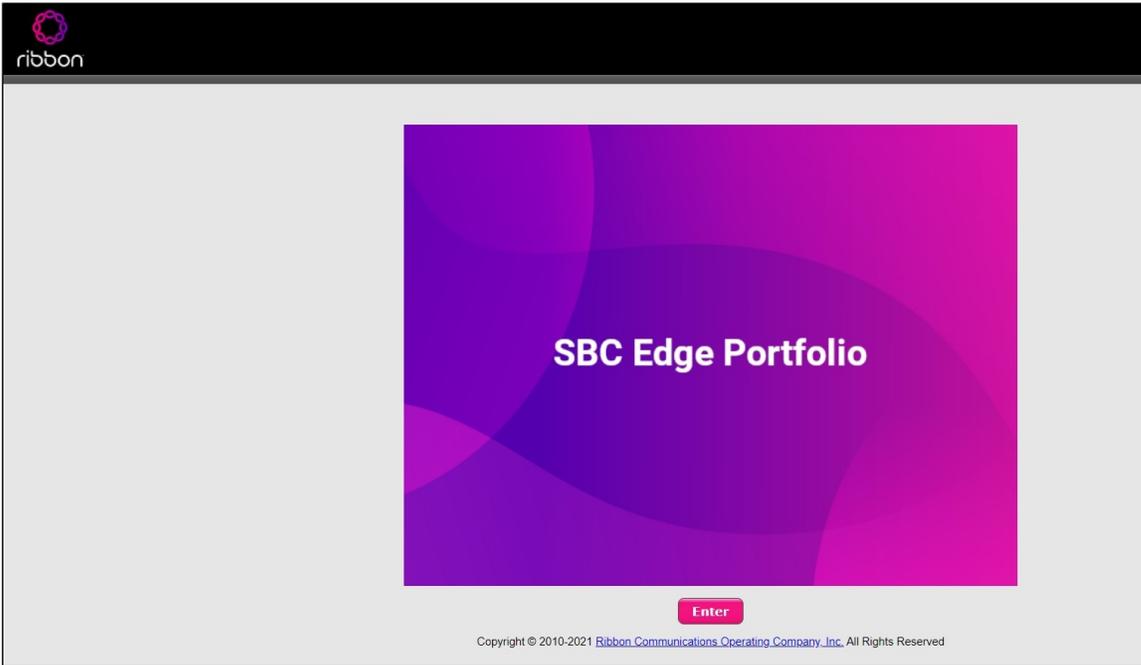
Section A: Ribbon SBC SWe Edge Configuration

Installing Ribbon SBC SWe Edge On Azure

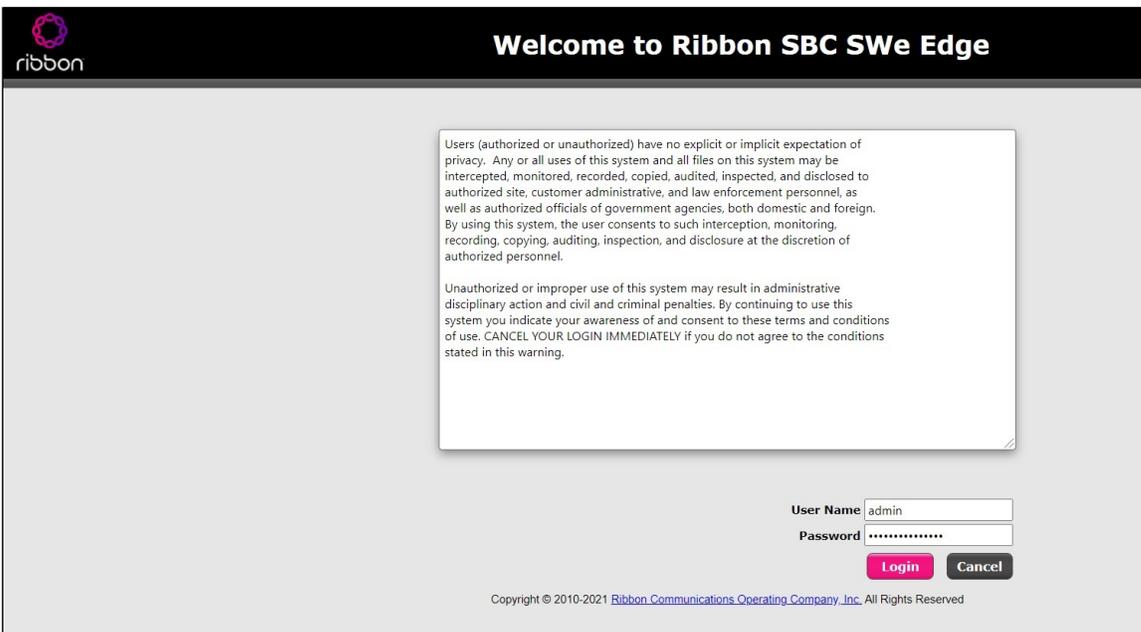
The SBC SWe Edge is available for deployment in Azure. It is created as a virtual machine (VM) hosted in Azure. To deploy an SBC SWe Edge instance, refer to [Deploying an SBC SWe Edge from the Azure Marketplace](#).

Accessing Ribbon SBC SWe Edge

Open any browser and enter the SBC SWe Edge IP address.



Click **Enter** and log in with a valid User ID and Password.



View Networking Interfaces

The SBC SWe Edge supports five system created logical interfaces (known as **Administrative IP**, **Ethernet 1 IP**, **Ethernet 2 IP**, **Ethernet 3 IP**, and **Ethernet 4 IP**). In addition to the system created logical interfaces, the Ribbon SBC SWe supports user-created VLAN logical sub-interfaces.

Administrative IP, Ethernet 1 IP and Ethernet 2 IP are used for this interop.

From the **Settings** tab, navigate to **Networking Interfaces > Logical Interfaces**.

The SBC SWe Edge system supports a logical interface called the Admin IP (Administrative IP, also known as the Management IP). A Static IP or DHCP is used for running Initial Setup of the SBC SWe Edge system.

Administrative IP

Logical Interfaces		Total 3 LogicalInterface Rows					
Interface Name	IPv4 Address	IPv6 Address	Description	Admin State	Display	Primary Key	
Admin IP	10.4.1.4			Enabled	Counters	35	
Ethernet 1 IP	10.4.2.4			Enabled	Counters	36	
Ethernet 2 IP	10.4.3.4			Enabled	Counters	37	

Ethernet 1 IP and Ethernet 2

Ethernet 1 and 2 IP is assigned an IP address used for transporting all the VOIP media packets (for example, RTP, SRTP) and all protocol packets (for example, SIP, RTCP, TLS). DNS servers of the customer's network should map the SBC SWe Edge system hostname to this IP address. In the default software, **Ethernet 1 and 2 IP** is enabled and an IPv4 address is acquired through a connected DHCP server. This IP address is used for performing Initial Set up on the SBC SWe Edge.

▼ Ethernet 1 IP
10.4.2.4
Enabled

Identification/Status

Interface Name **Ethernet 1 IP**

I/F Index **5**

Alias

Description

Admin State **Enabled** ▼

Networking

MAC Address **00:0d:3a:57:77:2d**

IP Addressing Mode **IPv4** ▼

IPv4 Information

IP Address **10.4.2.4**

IP Netmask **255.255.255.0**

IP Assign Method **DHCP** ▼

Media Next Hop IP * x.x.x.x

DHCP Options to Use **IP Address and Default Route** ▼

Ethernet 2 IP 10.4.3.4 Enabled

Identification/Status

Interface Name **Ethernet 2 IP**
 I/F Index **6**
 Alias
 Description
 Admin State **Enabled** ▼

Networking

MAC Address **00:0d:3a:57:7a:2d**
 IP Addressing Mode **IPv4** ▼

IPv4 Information

IP Address **10.4.3.4**
 IP Netmask **255.255.255.0**

IP Assign Method **DHCP** ▼
 Media Next Hop IP * x.x.x.x
 DHCP Options to Use **IP Address and Default Route** ▼

Configure Static Routes

Static routes are used to create communication to remote networks. In a production environment, static routes are mainly configured for routing from a specific network to another network that you can only access through one point or one interface (single path access or default route).

Derive the Private IP address and Gateway for each interface on Azure.

Destination IP

Specifies the destination IP address.

Mask

Specifies the network mask of the destination host or subnet. If the 'Destination IP Address' field and 'Mask' field are both 0.0.0.0, the static route is called the 'default static route'.

Gateway

Specifies the IP address of the next-hop router to use for a specific static route.

Metric

Specifies the cost of this route and therefore indirectly specifies the preference of the route. Lower values indicate more preferred routes. The typical value is 1 for most static routes, indicating that static routes are preferred to dynamic routes.

Search...

Expand All | Collapse All | Reload

- Call Routing
- Signaling Groups
- Networking Interfaces
- Virtual DR SBA
- System
- Auth and Directory Services
- Protocols
 - DNS
 - IP
 - Static Routes**
 - Routing Table
 - Static ARP
 - Access Control Lists
 - NAT

Static IP Route Table

Total 3 IP Route Rows

Row ID	Destination IP	Mask	Gateway	Metric	Primary Key
1	52.115.115.1	255.252.0.0	10.4.3.1	1	1
2	115.115.115.1	255.255.255.255	10.4.2.1	1	2
3	115.115.115.1	255.255.255.0	10.4.2.1	1	3

License and TLS Certificates

View License

This section describes how to view the status of each license along with a copy of the license keys installed on your SBC. The **Feature Licenses** panel enables you to verify whether a feature is licensed, along with the number of remaining licenses available for a given feature at run-time.

From the **Settings** tab, navigate to **System > Licensing > Current Licenses**.

Feature	Licensed	Total Licenses	Available Licenses	Feature Expiration
SIP Signaling Sessions	100	100	100	March 22, 2022 23:59:59
Enhanced Media Sessions with Transcoding	100	100	100	March 22, 2022 23:59:59
Enhanced Media Sessions without Transcoding	100	100	100	March 22, 2022 23:59:59
SIP Registrations	100	100	100	March 22, 2022 23:59:59

For more details on Licenses, refer to [Cloud-Based SBC SWe Edge Deployment Licenses](#).

Import Trusted Root CA Certificates

A Trusted CA Certificate is a certificate issued by a trusted certificate authority. Trusted CA Certificates are imported to the SBC SWe Edge to establish its authenticity on the network.

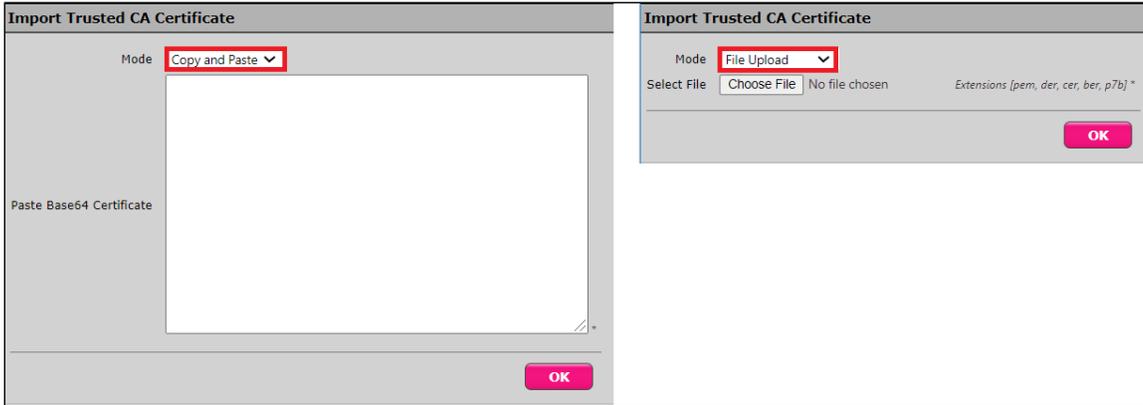
From the **Settings** tab, navigate to **Security > SBC Certificates > Trusted CA Certificates**.

- Generate SBC Edge CSR
- SBC Primary Certificate
- SBC Supplementary Certificates
- Trusted CA Certificates

This section describes the process of importing Trusted Root CA Certificates, using either the File Upload or Copy and Paste methods.

1. To import a Trusted CA Certificate, click the Import Trusted CA Certificate (📁) Icon.
2. Select either Copy and Paste or File Upload from the **Mode** menu.
3. If you choose **File Upload**, use the **Select File** button to find the file.
4. Click **OK**.

Figure 1: Trusted Certificates 2



Follow the steps above to import the Service Provider's Root and Intermediate certificates of their Public CA.

For more details on Certificates, refer to [Working with Certificates](#).



Note

When the **Verify Status** field in the Certificate panel indicates Expired or Expiring Soon, replace the Trusted CA Certificate. You must delete the old certificate before importing a new certificate successfully.



Warning

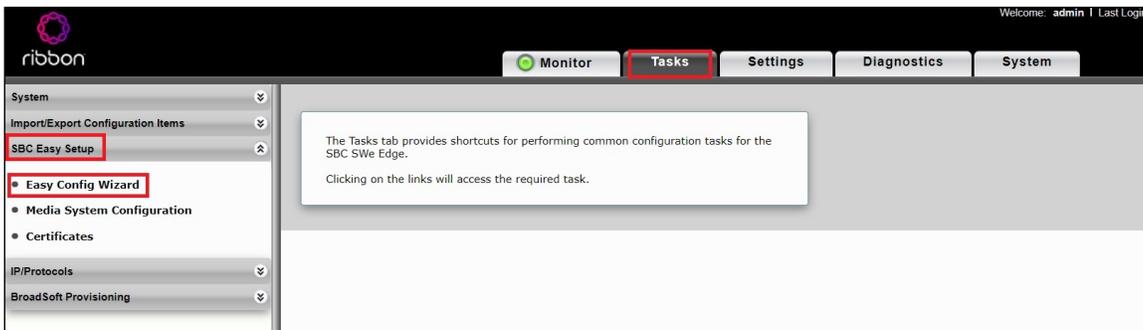
Most Certificate Vendors sign the SBC Edge certificate with an intermediate certificate authority. There is at least one, but there could be several intermediate CAs in the certificate chain. When importing the Trusted Root CA Certificates, import the root CA certificate and all Intermediate CA certificates. Failure to import all certificates in the chain causes the import of the SBC Edge certificate to fail. Refer to [Unable To Get Local Issuer Certificate](#) for more information.

Ribbon SWe Edge Configuration towards CUCM and Microsoft Teams Cloud

Access the Easy Configuration Wizard

1. In the WebUI, click the **Tasks** tab.
2. In the left navigation pane, navigate to **SBC Easy Setup > Easy Config Wizard**. The Easy Configuration screen opens.

The SBC Edge WebUI provides a built-in Easy Configuration wizard that allows you quickly and easily deploy the SBC for operation with provider endpoints (SIP trunk, ISDN PSTN trunk, or IP PBX trunk) and user endpoints (Microsoft Teams, Microsoft On Premises - Skype for Business /Lync, IP Phones, or ISDN PBX or IP PBX).



Navigating the Wizard

As the wizard runs, it directs you through three configuration steps:

Step 1: Set the following parameters to describe the topology for the telephony service provider and user ends of the scenario.

- **Application:** Click the drop-down arrow, then select the Service Provider and user endpoint types that the SBC is to connect to.
- **Scenario Description:** Type up to 32 characters to describe the connectivity scenario.
- **Telephone Country:** Click the drop-down arrow, then select the country in which the telephone services operate.
- **Emergency Services:** Choose **ELIN Identifier**, **E911/E112**, or **None** as the emergency services type.
- **SIP Sessions:** Type a number from 1-1200 to indicate the SIP sessions to allocate for the scenario.

Step 2: Configure the items required for the endpoints selected, fields display based on the endpoint selection in Step 1.

Step 3: The Easy Config validates the final parameters and displays a read-only summary of the configuration that the wizard will apply when you click **Finish** at Step 3. Before you click **Finish**, you can return to previous steps to make adjustments to the data summarized.

The wizard displays the following buttons for navigation:

- **Previous:** Moves back to the previous step.
- **Next:** Advances to the next step when the current step is validated and complete.
- **Finish:** Submits the data to the SBC.
- **Cancel:** Cancels the Easy Configuration data entered and redirects to the main WebUI.

Configure Ribbon SBC SWe Edge for CUCM and Microsoft Teams

Step 1: Use the Multi-legged approach to configure IP PBX and Microsoft Teams.

1. Click the drop-down arrow on the **Application** and select IP PBX Microsoft Teams.
2. Provide the desired description.
3. Select **Telephone Country** as Unites States.
4. Choose from 1 to 1200 to allocate the SIP Sessions.
5. Select Cisco CUCM as **IP PBX Type**.
6. Select Teams Direct Routing as **Teams Connection**.
7. Click **Next**.

The screenshot shows the 'Easy Configuration' wizard interface. At the top, it displays 'Step 1', 'Step 2', and 'Step 3' buttons. A message states 'This step takes input about the topology'. The main configuration area is divided into 'Scenario Parameters' and 'SIP Properties' sections. In 'Scenario Parameters', the 'Application' dropdown is set to 'IP PBX <-> Microsoft Teams', 'Scenario Description' is 'CUCM', 'Telephone Country' is 'United States', and 'Emergency Services' is 'None'. In 'SIP Properties', 'SIP Sessions' is set to '100'. Below these are two sub-sections: 'IP PBX' with 'Type' set to 'Cisco CUCM', and 'Microsoft Teams' with 'Teams Connection' set to 'Teams Direct Routing'. At the bottom, there are 'Cancel', 'Previous', 'Next', and 'Finish' buttons.

Step 2: After selecting the scenario in Step 1, the following template displays. Complete this step by performing the actions listed below:

1. Provide the Host IP address or FQDN for Cisco CUCM. The traffic is sent to these FQDNs/IP from the SBC SWe Edge.
2. Use **UDP/TCP** with port number 5060 for Service Provider SIP trunk configuration.
3. Select the **Signaling/Media Source IP** from drop down.
4. Provide the NAT Public IP (Signaling/Media).
5. Click **Next**.

Easy Configuration December 17, 2021 13:31:50

Step 1 **Step 2** **Step 3** This step takes input about the Provider and User side configuration

▼ IP PBX: Cisco CUCM

Host * FQDN or IP
 Protocol
 Port Number [1024..65535]
 Use Secondary Server

▼ Microsoft Teams: Teams Direct Routing

Teams Connection Type
 Signaling/Media Source IP External I/F *
 Apply ACL
 NAT Public IP (Signaling/Media) * IP Address
 Protocol
 Server Port Number
 Listening Port Number * Port Number

Cancel **Previous** **Next** **Finish**



Note

While using "Easy Configuration Wizard" TLS protocol is not available by default for Cisco CUCM but can be configured later.

For more information about Microsoft Teams Direct Routing configuration , refer to the following: [Connect SBC Edge to Microsoft Teams Direct Routing](#)

Step 3: This step displays a read-only summary of the configuration.

1. Check if the information entered in the previous steps is correct. If the entered information is wrong, return to the previous step by clicking **Previous** and modify the required field.
2. Click **Finish** to complete the configuration.

Easy Configuration December 17, 2021 13:31:50

Step 1 **Step 2** **Step 3** This step is a summary of what will be configured

Application **IP PBX <-> Microsoft Teams**
 Scenario Description **CUCM**
 Telephone Country **United States**
 Emergency Services **None**

———— SIP Properties ————
 SIP Sessions **100**

IP PBX: Cisco CUCM

Host
 Protocol
 Port Number
 Use Secondary Server

Microsoft Teams: Teams Direct Routing

Teams Connection Type
 Signaling/Media Source IP
 Apply ACL
 NAT Public IP (Signaling/Media)
 Protocol
 Server Port Number
 Listening Port Number

Cancel **Previous** **Next** **Finish**

- A pop up window appears once all the 3 steps are completed. Click **OK** to continue.
- Wait for the configuration to complete and click **OK** on the next window. This completes the configuration of Microsoft Teams and IP-PBX (CUCM) SIP Trunk on the SBC SWe Edge.

Create and Modify Ribbon SBC SWe Edge Configuration

The Easy Configuration Wizard does not currently set all applicable variables to the correct settings. This will be addressed in the subsequent SBC SWe Edge releases. Until then, follow the procedures below. This section describes the steps to configure the SBC SWe Edge with TLS /SRTP towards IP-PBX (CUCM) SIP Trunk. Ribbon strongly recommends encrypting the connection between the IP-PBX SIP Trunk and the SBC SWe Edge.

Create SRTP Profile

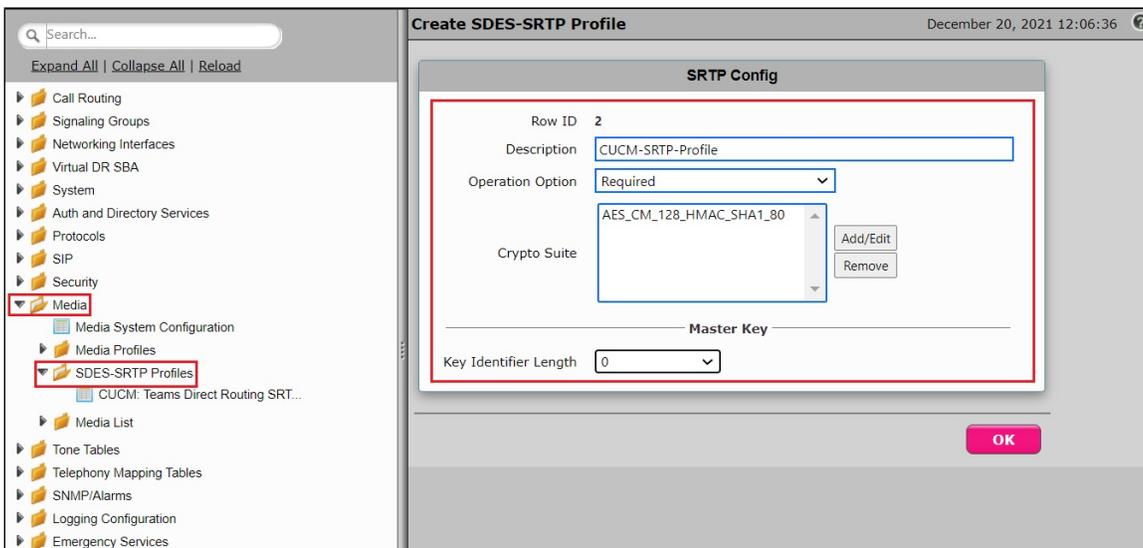
SDES-SRTP Profiles define a cryptographic context that is used in SRTP negotiation. SDES-SRTP Profiles required for enabling encryption and SRTP are applied to Media Lists. SDES-SRTP Profiles was previously named Media Crypto Profiles.

From the **Settings** tab, navigate to **Media > SDES-SRTP Profiles**. Click the **+** icon to create a new SRTP profile.



Follow the steps below to complete the configuration:

1. Provide the desired description for the profile.
2. Set Operation Option as "Required". This setting permits call connections only if you can use encryption for the call. If the peer device does not support SRTP (Secure Real Time Protocol) for voice encryption over the IP network, the call setup will fail.
3. Attach the Crypto suite "AES_CM_128_HMAC_SHA1_80" - A crypto suite algorithm that uses the 128 bit AES-CM encryption key and a 80 bit HMAC_SHA1 message authentication tag length.
4. Key Identifier Length set to "0" - Set this value to **0** to disable the MKI in SDP.
5. Click **OK**.





Warning

For SIP Trunk towards CUCM, If the SWe Edge SRTP profile is configured with "Operation Option" as "Required" and "Crypto Suit" as "AES_CM_128_HMAC_SHA1_80", call hold initiated from Cisco endpoint will fail. This is a known issue with Cisco CUCM. To overcome it, use "AES_CM_128_HMAC_SHA1_32" between CUCM and SWe Edge.

Update Media List

From the **Settings** tab, navigate to **Media > Media List**, Click the expand () icon next to the entry.

1. Attach the SDES-SRTP profile (Specifies the profile for authentication/encryption protocols applied with this Media List) created in the previous step.
2. Select the required Media Profiles list.
3. Update the Media Profiles List as required for both Media List configurations.
4. Click **Apply**.

The screenshot shows the 'Media List View' configuration page. On the left is a navigation tree with 'Media List' selected. The main area shows a table with 3 rows: 'Default Media List' (Primary Key 1), 'CUCM: Teams Direct Routing List' (Primary Key 2), and 'CUCM: Cisco List' (Primary Key 3). The 'CUCM: Cisco List' entry is expanded, showing a configuration form with the following fields:

- Description: CUCM: Cisco List
- Media Profiles List: A list containing 'CUCM (Cisco): G.711 Mu-Law' and 'CUCM (Cisco): G.711 A-Law'.
- SDES-SRTP Profile: CUCM-SRTP-Profile (with a note: 'Associated SIP SG Listen Ports should be TLS only.')
- Media DSCP: 46 (with a note: '* [0..63]')
- Dead Call Detection: Disabled
- Silence Suppression: Enabled

The screenshot shows the 'Media List View' configuration page. On the left is a navigation tree with 'Media List' selected. The main area shows a table with 3 rows: 'Default Media List' (Primary Key 1), 'CUCM: Teams Direct Routing List' (Primary Key 2), and 'CUCM: Cisco List' (Primary Key 3). The 'CUCM: Teams Direct Routing List' entry is expanded, showing a configuration form with the following fields:

- Description: CUCM: Teams Direct Routing List
- Media Profiles List: A list containing 'CUCM (Teams): G.711 Mu-Law' and 'CUCM (Teams): G.711 A-Law'.
- SDES-SRTP Profile: CUCM: Teams Direct Routing SRT (with a note: 'Associated SIP SG Listen Ports should be TLS only.')
- Media DSCP: 46 (with a note: '* [0..63]')
- Dead Call Detection: Disabled
- Silence Suppression: Enabled

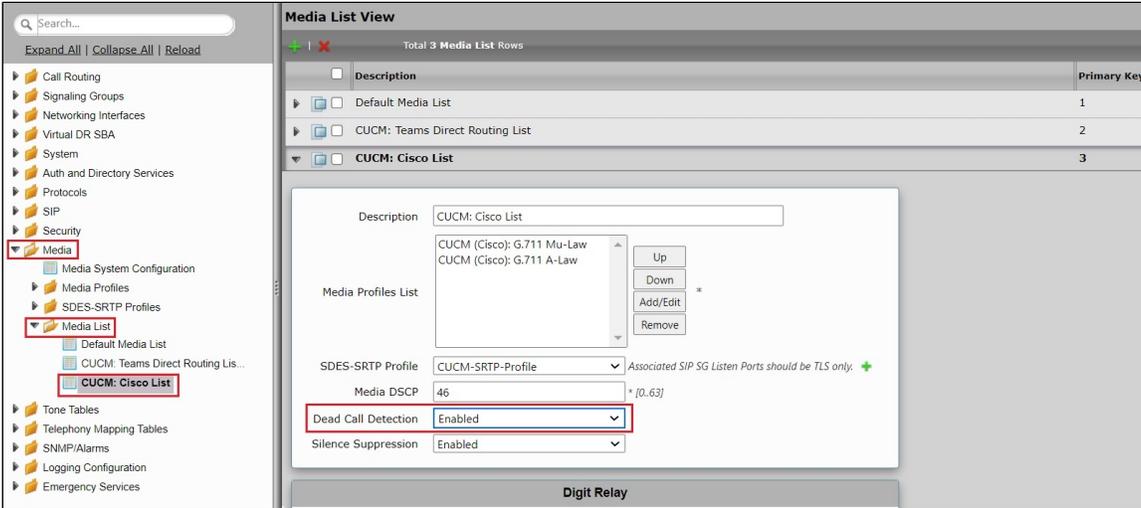
Enable Dead Call Detection

Specifies whether or not to use RTCP-based Dead Call Detection (DCD).

Dead Call Detection is accomplished by monitoring incoming RTCP packets. If this feature is enabled and no RTCP packets are received from the peer for 30 seconds, the call is considered "dead" and is disconnected.

From the **Settings** tab, navigate to **Media > Media List**. Click the **expand** () Icon next to the entry you wish to enable the feature.

- Enable DCD from the options provided in the drop-down.



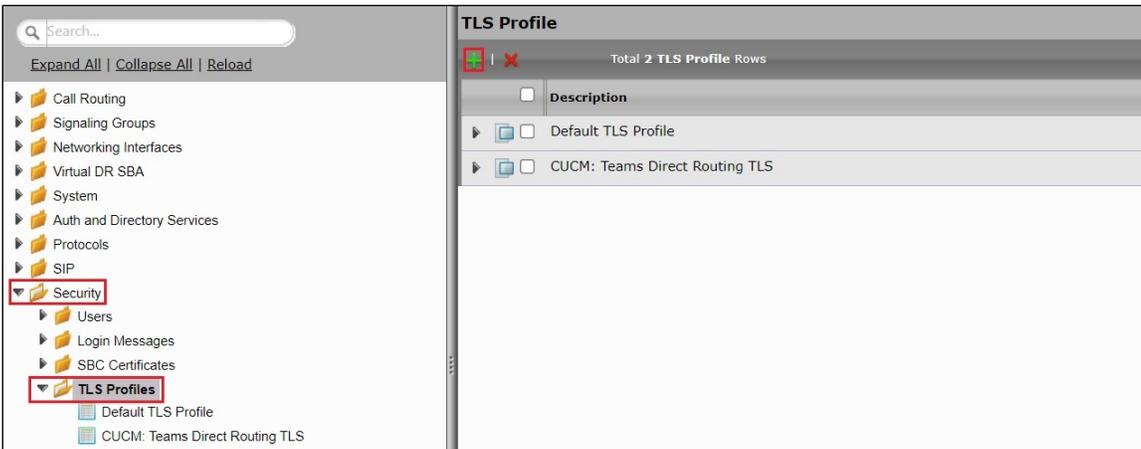
Description	Primary Key
Default Media List	1
CUCM: Teams Direct Routing List	2
CUCM: Cisco List	3

Configuration details for CUCM: Cisco List:

- Description: CUCM: Cisco List
- Media Profiles List: CUCM (Cisco): G.711 Mu-Law, CUCM (Cisco): G.711 A-Law
- SDES-SRTP Profile: CUCM-SRTP-Profile
- Media DSCP: 46
- Dead Call Detection: Enabled
- Silence Suppression: Enabled

TLS Profile

From the **Security** tab, navigate to **TLS Profiles**. Click the  icon to create a new TLS profile.



Description
Default TLS Profile
CUCM: Teams Direct Routing TLS

1. Provide the table's **Description** as desired.
2. Modify the Values as required.
3. Click **OK**.

Create TLS Profile

Row ID 3
Description **CUCM: Cisco CUCM**

TLS Parameters

Common Attributes

TLS Protocol: TLS 1.0-1.2
Mutual Authentication: Enabled
Handshake Inactivity Timeout: 10 secs [1..30]
Certificate: SBC Edge Certificate

Client Attributes

Client Cipher List:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES256_CBC_SHA
- TLS_RSA_WITH_AES128_CBC_SHA

 (Up, Down, Add/Edit, Remove buttons)

Validate Server FQDN: Enabled

Server Attribute

Validate Client FQDN: Enabled

OK

Update Signaling group

Change the settings on all the SGs as follows:

- Update the signaling group "**CUCM: Cisco CUCM**".
- Play Ringback - **Auto on 180/183** - Ringback is determined when processing 180 or 183.
- Early 183 - **Enable** - Specifies whether to send a SIP 183 response immediately after receiving an Invite message.
- Assign the interfaces for Signaling/Media Private IP to all the Signaling Groups accordingly.
- Enable Static NAT and map the respective IP addresses for both Signaling Groups.
- Add the listen port for TLS.

SIP Channels and Routing

Action Set Table: None
Call Routing Table: CUCM: From Cisco CUCM
No. of Channels: 100 * [1..1200]
SIP Profile: CUCM: Cisco Profile
SIP Mode: Basic Call
Agent Type: Back-to-Back User Agent
SIP Server Table: CUCM: Cisco CUCM
Load Balancing: Round Robin
Notify Lync CAC Profile: Disable
Challenge Request: Disable
Outbound Proxy IP/FQDN: [1..65535]
Outbound Proxy Port: [1..65535]

Media Information

Supported Audio Modes: DSP, Proxy, Direct, Proxy with Local SRTP (Add/Edit, Remove buttons)
Supported Video/Application Modes: (Add/Edit, Remove buttons)
Media List ID: CUCM: Cisco List
Proxy Local SRTP Crypto Profile ID: CUCM-SRTP-Profile
Play Ringback: Auto on 180/183
Tone Table: CUCM: United States
Play Congestion Tone: Disable

Outbound Proxy IP/FQDN

Outbound Proxy Port [1..65535]

Call Setup Response Timer 180 [180..750] secs

Call Proceeding Timer 180 [24..750] secs

Use Register as Keep Alive

Forked Call Answered Too Soon

SIP Recording

SIP Recording Status

Tone Table

Play Congestion Tone

Early 183

Allow Refresh SDP

Music on Hold

RTCP Multiplexing

Mapping Tables

SIP To Q.850 Override Table

Q.850 To SIP Override Table

SIP IP Details

Teams Local Media Optimization

Signaling/Media Private IP

Signaling DSCP 40 * [0..63]

NAT Traversal

ICE Support

Static NAT - Outbound

Outbound NAT Traversal

NAT Public IP (Signaling/Media) 13.90.116.85 * IP Address

Static NAT - Inbound

Detection

Detection

Listen Ports

Listen Port

Federated IP/FQDN

Total 1 SIP Federated IP Row

IP/FQDN	Netmask/Prefix
115.110.170.208	255.255.255.255

Message Manipulation



Note

You can configure SIP Trunk between Service provider and IP-PBX over UDP or TCP or TLS. Ribbon recommends use of TLS protocol to ensure security. Customers who do not wish to use TLS as preferred protocol can skip this section.

Update SIP Server Tables

SIP Server Tables contain information about the SIP devices connected to the SBC Edge. The entries in the tables provide information about the IP Addresses, ports, and protocols used to communicate with each server. The Table Entries also contain links to counters that are useful for troubleshooting.

From the **Settings** tab, navigate to **SIP > SIP Server Tables > CUCM: Cisco CUCM**. Click the expand () icon next to the entry.

Keep Alive Frequency

Specifies how often, in seconds, the SBC Edge queries the server with an OPTIONS message to determine the server's availability. Visible only when SIP Options is selected from the Monitor field. If the server does not respond, the SBC Edge marks the Signaling Group as down. When the server begins to respond to the OPTIONS messages again, it is marked as up. In this case, Keep Alive Frequency is set to 30 seconds.

Recover Frequency

Specifies frequency in seconds to check server to determine whether it has become available. Recovery Frequency is set to 5 seconds for this interop.

Local Username

Local user name of the SBC Edge system. Default entry: **Anonymous**. Visible only when **SIP Options** is selected from the **Monitor** field.

Peer Username

User name of the SIP Server. Visible only when **SIP Options** is selected from the **Monitor** field. The user can change Local and Peer Usernames according to their wishes.

1. Select Protocol **TLS** and Port 5061.
2. Attach the TLS Profile.

Host / Domain	Server Lookup	Port	Protocol	Display Counters	Priority	Primary Key
115.110.170.208	IP/FQDN	5060	TCP	Counters	1	1

Server Host

Server Lookup: IP/FQDN
Priority: 1
Host FQDN/IP: 115.110.170.208
Port: 5061
Protocol: TLS
TLS Profile: CUCM: Cisco CUCM

Transport

Monitor: SIP Options
Keep Alive Frequency: 30
Recover Frequency: 5
Local Username: Anonymous
Peer Username: Anonymous

Remote Authorization and Contacts

Remote Authorization Table: None
Contact Registrant Table: None
Session URI Validation: Liberal

Connection Reuse

Reuse: True
Sockets: 4
Reuse Timeout: Forever

Apply



Note

Repeat the steps above to enable OPTIONS on other SIP Server Tables.



Note

During this interop the signaling group "CUCM: Cisco CUCM" Listen Port section is updated to TLS only. Update the signaling group accordingly.



Note

From the **System > Node-Level Settings** update the node level settings as required.

Transformation Table

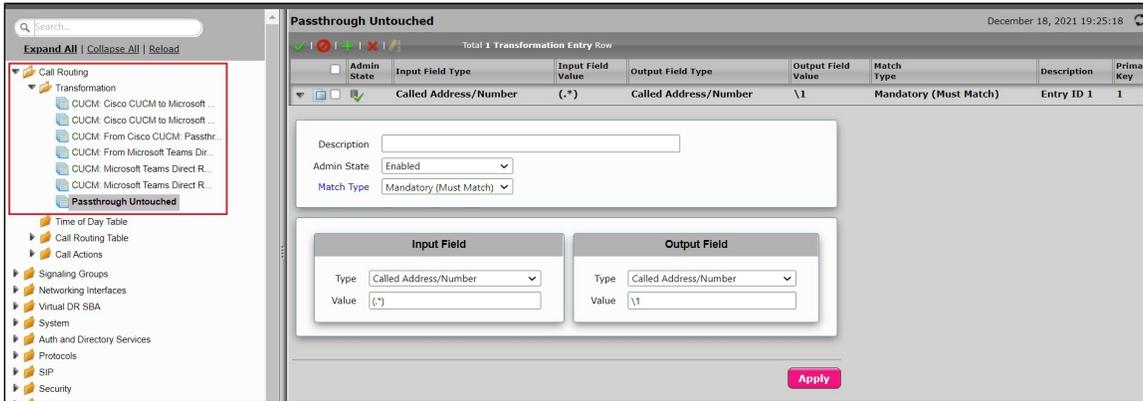
Transformation Tables facilitate the conversion of names, numbers and other fields when routing a call. They can, for example, convert a public PSTN number into a private extension number, or into a SIP address (URI). Every entry in a Call Routing Table requires a Transformation Table, and they are selected from there. In addition, Transformation tables are configurable as a reusable pool that Action sets can reference.

From the **Settings** tab, navigate to **Transformation**.

To Modify a Transformation Table

The Transformation Tables are created for Service Provider SIP Trunk through Easy Config Wizard. These are modified to allow specific patterns to reach the destination Signaling Group.

1. Click the **expand** () icon next to the entry you wish to modify.
2. Modify the table's **Description** as desired.
3. Modify the Values from **Input field** and **Output field** as required.
4. Set the Match Type as **Optional (Match one)**.
5. Click **OK**.



Creating an Entry to a Message Transformation Table

For this interop, the entries are created based on the numbers associated with each endpoint. Users are free to select their own variables or Regular expressions.

1. Click the **Create** (+) icon next to the table created in the previous step.
2. Provide the below details:

Admin State:

Enabled - The default state is Enabled.

Match Type:

Optional: Optional entries must match at least one of that Input Field type.

When a call arrives at a Transformation Table, the incoming message contains a number of Informational Elements (IEs). These IEs include important call information such as: Called Address/Number, Called Extension, Calling Name, Redirecting Number and others. Each Informational Element is processed row by row in the Transformation Table.

Value (Input/Output):

Specifies the value to match against for the selected type. Depending on the type selected, values are free-form or selected from a menu.

3. Click **Apply**.



Note

For details on Transformation Table Entry configuration, refer to [Creating and Modifying Entries to Transformation Tables](#). For call digit matching and manipulation through the use of regular expressions, refer to [Creating Call Routing Logic with Regular Expressions](#).



Note

During this interop "Passthrough" transformation table only is used on both the sides.

Call Routing Table

Call Routing allows carrying of calls between Signaling Groups. Routes are defined by Call Routing Tables, which allow for flexible configuration where calls are carried, and how they are translated.

From the **Settings** tab, navigate to **Call Routing > Call Routing Table**.

The Call Routing Tables are created to route the calls between IP-PBX (CUCM) -Service Provider through Easy Config Wizard. The user is allowed to modify these tables as per the requirement.

Modifying an Entry to a Call Routing Table

1. Click the **expand** (▸) icon next to the entry you wish to modify.
2. Edit the entry properties as required.

Search...

Expand All | Collapse All | Reload

- Call Routing
 - Transformation
 - Time of Day Table
 - Call Routing Table
 - Default Route Table
 - CUCM: From Cisco CUCM
 - CUCM: From Microsoft Teams Dir...
- Call Actions
- Signaling Groups
- Networking Interfaces
- Virtual DR SBA
- System
- Auth and Directory Services
- Protocols
- SIP
- Security
- Media
- Tone Tables
- Telephony Mapping Tables
- SNMP/Alarms
- Logging Configuration
- Emergency Services

1 CUCM: From Cisco CUCM: Passthrough Normal (SIP) CUCM: Teams Direct Routing To Microsoft Teams Direct Routing (Passthrough) No

Route Details

Description: To Microsoft Teams Direct Routing (Passthrough)

Admin State: Enabled

Route Priority: 1

Call Priority: Normal

Number/Name Transformation Table: CUCM: From Cisco CUCM: Passth

Time of Day Restriction: None

Destination Information

Destination Type: Normal

Message Translation Table: None

Cause Code Reroutes: None

Cancel Others upon Forwarding: Disabled

Fork Call: No

Destination Signaling Groups: (SIP) CUCM: Teams Direct Routing

Enable Maximum Call Duration: Disabled

Search...

Expand All | Collapse All | Reload

- Call Routing
 - Transformation
 - Time of Day Table
 - Call Routing Table
 - Default Route Table
 - CUCM: From Cisco CUCM
 - CUCM: From Microsoft Teams Dir...
- Call Actions
- Signaling Groups
- Networking Interfaces
- Virtual DR SBA
- System
- Auth and Directory Services
- Protocols
- SIP
- Security
- Media
- Tone Tables
- Telephony Mapping Tables
- SNMP/Alarms
- Logging Configuration
- Emergency Services

Message Translation Table: None

Cause Code Reroutes: None

Cancel Others upon Forwarding: Disabled

Fork Call: No

Destination Signaling Groups: (SIP) CUCM: Teams Direct Routing

Enable Maximum Call Duration: Disabled

Media

Audio Stream Mode: DSP

Video/Application Stream Mode: Disabled

Media Transcoding: Enabled

Media List: None

Quality of Service

Quality Metrics Number of Calls: 10 [1..100]

Quality Metrics Time Before Retry: 10 [1..60] min.

Min. ASR Threshold: 0 % [0..100]

Enable Min MOS Threshold: Disabled

Enable Max. R/T Delay: Enabled

Max. R/T Delay: 9999 ms [1..65535]

Enable Max. Jitter: Enabled

Max. Jitter: 3000 ms [1..3000]

Apply

Search...

Expand All | Collapse All | Reload

- Call Routing
 - Transformation
 - Time of Day Table
 - Call Routing Table
 - Default Route Table
 - CUCM: From Cisco CUCM
 - CUCM: From Microsoft Teams Dir...
- Call Actions
- Signaling Groups
- Networking Interfaces
- Virtual DR SBA
- System
- Auth and Directory Services
- Protocols
- SIP
- Security
- Media
- Tone Tables
- Telephony Mapping Tables
- SNMP/Alarms
- Logging Configuration
- Emergency Services

1 CUCM: From Microsoft Teams Direct R... Normal (SIP) CUCM: Cisco CUCM To Outside (Passthrough) No 3

Route Details

Description: To Outside (Passthrough)

Admin State: Enabled

Route Priority: 1

Call Priority: Normal

Number/Name Transformation Table: CUCM: From Microsoft Teams Dir

Time of Day Restriction: None

Destination Information

Destination Type: Normal

Message Translation Table: None

Cause Code Reroutes: None

Cancel Others upon Forwarding: Disabled

Fork Call: No

Destination Signaling Groups: (SIP) CUCM: Cisco CUCM

Enable Maximum Call Duration: Disabled

The screenshot shows the configuration page for a Call Routing Table. The left sidebar contains a navigation tree with categories like Call Routing, Transformation, Signaling Groups, and Media. The main area is divided into three sections:

- Message Translation Table:** Includes fields for Message Translation Table (None), Cause Code Reroutes (None), Cancel Others upon Forwarding (Disabled), Fork Call (No), Destination Signaling Groups (a list with a search bar and 'Up/Down' buttons), and Enable Maximum Call Duration (Disabled).
- Media:** Includes Audio Stream Mode (DSP), Video/Application Stream Mode (Disabled), Media Transcoding (Enabled), and Media List (None).
- Quality of Service:** Includes Quality Metrics Number of Calls (10), Quality Metrics Time Before Retry (10), Min. ASR Threshold (0), Enable Min MOS Threshold (Disabled), Enable Max. R/T Delay (Enabled), Max. R/T Delay (9999), Enable Max. Jitter (Enabled), and Max. Jitter (3000).

An 'Apply' button is located at the bottom right of the configuration area.

Creating an Entry to a Call Routing Table

Call Routing Tables are one of the central connection points of the system, linking Transformation Tables, Message Translations, Cause Code Reroute Tables, Media Lists and the three types of Signaling Groups (ISDN, SIP and CAS).

In the SBC Edge, call routing occurs between **Signaling Groups**.

In order to route any call to or from a call system connected to the SBC, you must first configure a Signaling Group to represent that device or system. The following list illustrates the hierarchical relationships of the various Telephony routing components of a SBC call system:

- Signaling Group describes the source call and points to a routing definition known as a Call Route Table
- Call Route Table contains one or more Call Route Entries
- Call Route Entries points to the destination Signaling Group(s)

Each call routing entry describes how to route the call and also points to a Transformation Table that defines the conversion of names, numbers and other fields when routing a call.

To create an entry:

1. Click the **Create Routing Entry** () icon.
2. Set the following fields:

Admin State:

Enabled - Enables the call route entry for routing the call, displays in configuration header as .

Route Priority:

Priority of the route from 1 (highest) to 10 (lowest). Higher priority routes are matched against before lower priority routes regardless of the order of the routes in the table.

Number/Name Transformation Table:

Specifies the Transformation Table to use for this routing entry. This drop down list is populated from the entries in the Transformation Table.

Destination Signaling Groups:

Specifies the Signaling Groups used as the destination of calls. The first operational Signaling Group from the list is chosen to place the call. Click the Add/Edit button to select the destination signaling group.

Audio Stream Mode:

DSP (default entry): The SBC uses DSP resources for media handling (transcoding) but it does not facilitate the capabilities/features between endpoints that are not supported within the SBC (codec/capability mismatch). When DSP is configured, the Signaling Groups enabled to support DSP are attempted in order.

Media Transcoding:

Enabled: Enable Transcoding on SIP-to-SIP calls.

3. Click **Apply**.

**Note**

During this interop only "Passthrough" transformation table is used for call routing and removed other transformation entries.

**Warning**

In Call routing table "Audio Stream Mode" by default is DSP mode. It is recommended to use the default DSP mode configuration.

Section B: CUCM Configuration

Accessing CUCM (Cisco Unified CM Administration)

1. Open Browse and enter the CUCM IP Address.
2. Select **Cisco Unified CM Administration** from the Navigation drop-down.
3. Provide the credentials and click **Login**.

Configure SIP Trunk Security Profile

Unified Communications Manager Administration groups security-related settings for the SIP trunk to allow you to assign a single security profile to multiple SIP trunks. Security-related settings include device security mode, digest authentication, and incoming/outgoing transport type settings.

- From Cisco Unified CM Administration, navigate to **System > Security > SIP Trunk Security Profile**.
- Click **Add New**.

- Provide the desired Name and Description.
- Choose **Secure** from Device Security Mode.
- From Incoming Transport Type, select **TLS**.
 - When Device Security Mode is Non Secure, TCP+UDP specifies the transport type.
- Select Outgoing Transport Type as **TLS**.
- Click **Save**.

**Note**

Customers are free to choose any transport medium depends on their requirements. Ribbon strongly recommends use of secure TLS protocol.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status
Status: Ready

SIP Trunk Security Profile Information

Name*

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)*

Secure Certificate Subject or Subject Alternate Name

Incoming Port*

Enable Application level authorization

Incoming Port*

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

SIP V.150 Outbound SDP Offer Filtering*

Save Delete Copy Reset Apply Config Add New

i *- indicates required item.

i **If this profile is associated with an EMCC SIP trunk, Accept Out-of-Dialog REFER is enabled regardless of the setting on this page

**Note**

For more information on regarding CSR and Certificate generation for CUCM, refer to <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-border-element/215412-configure-sip-tls-between-cucm-cube-cube.html>

Configure SIP Profiles

A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that you cannot delete or change.

- From Cisco Unified CM Administration, navigate to **Device > Device Settings > SIP Profile**.
- Click **Add New**.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ **Device ▾** Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List SIP Profiles

+ Add New

SIP Profile

Find SIP Profile where Name ▾ begins with ▾ Find Clear Filter

No active query. Please enter your search criteria using the options above.

Add New

- Enter a name to identify the SIP profile.
- Provide description to identify the purpose of the SIP profile.

SIP Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

i Status: Ready

i All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name*

Description

Default MTP Telephony Event Payload Type*

Early Offer for G.Clear Calls*

User-Agent and Server header information

Version in User Agent and Server Header*

Dial String Interpretation*

Confidential Access Level Headers*

Redirect by Application

Disable Early Media on 180

Outgoing T.38 INVITE include audio mline

Offer valid IP and Send/Receive mode only for T.38 Fax Relay

Use Fully Qualified Domain Name in SIP Requests

Assured Services SIP conformance

Enable External QoS**

SDP Information

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*

SDP Transparency Profile

Accept Audio Codec Preferences in Received Offer*

Require SDP Inactive Exchange for Mid-Call Media Change

Allow RR/RS bandwidth modifier (RFC 3556)

- From SIP Rel1XX Options drop-down, choose **Send PRACK for all 1xx Messages**.
- From Early Offer support for voice and video calls drop-down, choose Best Effort (no MTP inserted).
 - Provide Early Offer for the outbound call only when caller side's media port, IP and codec information is available.
 - Provide Delayed Offer for the outbound call when caller side's media port, IP and codec information is not available. No MTP is inserted to provide Early Offer in this case.

SIP Profile Configuration

Save Delete Copy Reset Apply Config Add New

Conference Join Enabled
 RFC 2543 Hold
 Semi Attended Transfer
 Enable VAD
 Stutter Message Waiting
 MLPP User Authorization

Normalization Script

Normalization Script < None >

Enable Trace

	Parameter Name	Parameter Value
1		

External Presentation Information

Anonymous External Presentation

External Presentation Number

External Presentation Name

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on* Never

Resource Priority Namespace List < None >

SIP Rel1XX Options* Send PRACK for all 1xx Messages

Video Call Traffic Class* Mixed

Calling Line Identification Presentation* Default

Session Refresh Method* Invite

Early Offer support for voice and video calls* Best Effort (no MTP inserted)

Enable ANAT

Deliver Conference Bridge Identifier

- Enable **SIP OPTIONS Ping**.
- SIP OPTIONS are requests to the configured destination address on the SIP trunk.
- Click **Save**.

SIP OPTIONS Ping

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)* 60

Ping Interval for Out-of-service Trunks (seconds)* 120

Ping Retry Timer (milliseconds)* 500

Ping Retry Count* 6

SDP Information

Send send-receive SDP in mid-call INVITE

Allow Presentation Sharing using BFCP

Allow IX Application Media

Allow multiple codecs in answer SDP

Save Delete Copy Reset Apply Config Add New

ⓘ *- indicates required item.
 ⓘ ** - setting only takes effect if the External QoS Enabled Service Parameter is set to true.

Configure Phone Security Profiles

- From Cisco Unified CM Administration, navigate to **System > Security > Phone Security Profile**.
- Click **Add New**.
- Provide the required details.
- Click **Save**.

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Phone Security Profile Configuration

Save | Delete | Copy | Reset | Apply Config | Add New

Status
 Status: Ready

Phone Security Profile Information
 Product Type: Cisco Unified Client Services Framework
 Device Protocol: SIP
 Name*: secure_jabber
 Description: secure_jabber
 Device Security Mode: Encrypted
 Transport Type*: TLS
 TFTP Encrypted Config
 Enable OAuth Authentication

Phone Security Profile CAPF Information
 Authentication Mode*: By Null String
 Key Order*: RSA Only
 RSA Key Size (Bits)*: 2048
 EC Key Size (Bits): < None >
 Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone
 SIP Phone Port*: 5061

Save | Delete | Copy | Reset | Apply Config | Add New

Configure Media Resource Group

Media resource management comprises working with media resource groups and media resource group lists. Media resource management provides a mechanism for managing media resources, so all Cisco Unified Communications Managers within a cluster can share them. Media resources provide conferencing, transcoding, media termination, annunciator, and music on hold services.

- From Cisco Unified CM Administration, navigate to **Media Resources > Media Resource Group**.
- Click **Add New**.

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Find and List Media Resource Groups

+ Add New

Media Resource Group

Find Media Resource Group where Name | begins with | Find | Clear Filter | + | -

No active query. Please enter your search criteria using the options above.

Add New

- Enter a unique name in this required field to identify the media resource group.
- Enter a description for the media resource group.
- To add a media resource for this media resource group, choose one (MoH_2 in this case) from the available Media Resources list and click the down arrow. After a media resource is added, its name moves to the Selected Media Resources pane.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Media Resource Group Configuration

 Save
  Delete
  Copy
  Add New

Status

 Status: Ready

Media Resource Group Status

Media Resource Group: san_media_profile (used by 6 devices)

Media Resource Group Information

Name*

Description

Devices for this Group

Available Media Resources**

- ANN_2
- CFB_2
- IVR_2
- MTP_2

Selected Media Resources*

- MOH_2 (MOH)

Use Multi-cast for MOH Audio (If at least one multi-cast MOH resource is available)

- Click **Save**.

Configure Media Resource Group List

A Media Resource Group List provides a prioritized grouping of media resource groups. An application selects the required media resource, such as a music on hold server, from among the available media resources according to the priority order that is defined in a Media Resource Group List.

- From Cisco Unified CM Administration, navigate to **Media Resources > Media Resource Group List** menu path to configure media resource group lists.
- Click **Add New**.

System ▾ Call Routing ▾ **Media Resources** ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List Media Resource Group Lists

 Add New

Media Resource Group List

Find Media Resource Group List where Name  

No active query. Please enter your search criteria using the options above.

- Enter a unique name in this required field to identify the Media Resource Group List.
- Choose the Media Resource Group created in the previous step from the Available Media Resource Groups list and click the down arrow that is located between the two panes. After a media resource group is added, its name moves to the Selected Media Resource Groups pane.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Media Resource Group List Configuration

Save Delete Copy Add New

Status
 Status: Ready

Media Resource Group List Status
 Media Resource Group List: san_media_grplist (used by 6 devices)

Media Resource Group List Information
 Name*

Media Resource Groups for this List

Available Media Resource Groups

Selected Media Resource Groups

- Click **Save**.

Trunk Configuration

Use a trunk device to configure a logical route to a SIP network.

- From Cisco Unified CM Administration, choose **Device > Trunk**.
- Click **Add New**.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ **Device** ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List Trunks

Add New

Trunks

Find Trunks where ▾ begins with

No active query. Please enter your search criteria using the options above.

- From the Trunk Type drop-down list, choose **SIP Trunk**.
- Choose **SIP** from Device Protocol drop-down.
- From Trunk Service Type, select the default value (None).
- Click **Next**.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ **Device** ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Trunk Configuration

Next

Status

Status: Ready

Trunk Information

Trunk Type*

Device Protocol*

Trunk Service Type*

*- indicates required item.

- Enter a unique identifier for the trunk.
- Enter a descriptive name for the trunk.
- Choose the Default Device Pool.
- Choose the Media Resource Group List created in the previous step.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ **Device** ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Trunk Configuration

Save Delete Reset Add New

Status

Status: Ready

SIP Trunk Status

Service Status: Full Service
Duration: Time In Full Service: 4 days 23 hours 46 minutes

Device Information

Product:
Device Protocol:
Trunk Service Type
Device Name*
Description
Device Pool*
Common Device Configuration
Call Classification*
Media Resource Group List
Location*
AAR Group
Tunneled Protocol*
QSIG Variant*
ASN.1 ROSE OID Encoding*
Packet Capture Mode*
Packet Capture Duration
 Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name

- Provide the destination address.
 - The Destination Address represents the remote SIP peer with that this trunk will communicate.
 - SIP trunks only accept incoming requests from the configured Destination Address and the incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk.
- Choose the **S RTP Allowed** (only when SIP Trunk profile is created as TLS)
- Choose the **SIP Trunk Security Profile** created to apply to the SIP trunk.
- Select the **SIP Profile** created from the list.
- Choose **RFC 2833** as DTMF Signaling Method.
- Click **Save**.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Trunk Configuration

Save Delete Reset Add New

Transmit UTF-8 Names in QSIG APDU

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Consider Traffic on This Trunk Secure* When using both sRTP and TLS

Route Class Signaling Enabled* Default

Use Trusted Relay Point* Default

PSTN Access

Run On All Active Unified CM Nodes

Intercompany Media Engine (IME)

E.164 Transformation Profile < None >

MLPP and Confidential Access Level Information

MLPP Domain < None >

Confidential Access Mode < None >

Confidential Access Level < None >

Call Routing Information

Remote-Party-Id

Asserted-Identity

Asserted-Type* Default

SIP Privacy* Default

Trust Received Identity* Trust All (Default)

Inbound Calls

Significant Digits* All

Connected Line ID Presentation* Default

Connected Name Presentation* Default

Calling Search Space < None >

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Trunk Configuration

Save Delete Reset Add New Related Links: Back To Find

Destination

Destination Address is an SRV

ID	Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
1*	10.54.22.31		5061	up		Time Up: 4 days 23 hours 46 minutes

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Adaptor_san_swecore

Retouring Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* SAN_SIP_PROFILE [View Details](#)

DTMF Signaling Method* KHL_Z833

Normalization Script

Normalization Script < None >

Enable Trace

ID	Parameter Name	Parameter Value
1		

Recording Information

None

This trunk connects to a recording-enabled gateway

This trunk connects to other clusters with recording-enabled gateways

Geolocation Configuration

Geolocation < None >

Geolocation Filter < None >

Send Geolocation Information

- Click **Save**
- Click the **Reset** button.

-
- Reset, Restart and Close the window. Refresh the SIP trunk page and wait until the Server status changes from Unknown to Full Service.
-



Note

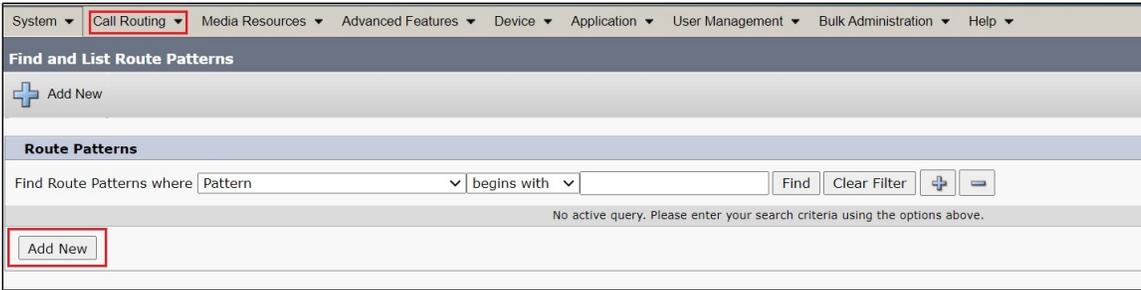
Resetting/restarting a SIP device does not physically reset/restart the hardware, it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager.

For SIP trunks, Restart and Reset behave the same way, so all active calls will disconnect when either choice is pressed.

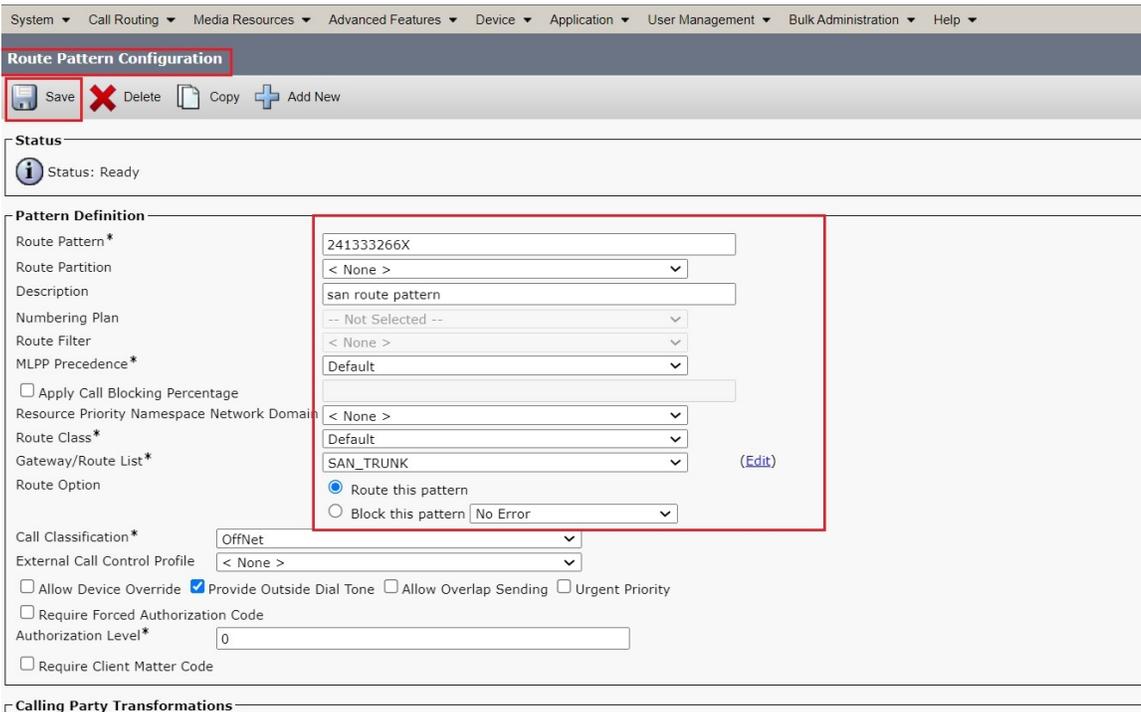
Configure Call Routing

A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns provide flexibility in network design. They work in conjunction with route filters and route lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

- In Cisco Unified Communications Manager Administration, use the **Call Routing > Route/Hunt > Route Pattern** menu path to configure route patterns.
- Click **Add New**.



- Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape character +.
- Configure the Route Pattern as below.
- Choose SIP Trunk created from the gateway or route list drop-down to add the route pattern.



- Click **Save**.

Configure End Users

The End User Configuration window allows you to add, search, display, and maintain information about Unified Communications Manager end users. End users can control phones after you associate a phone in the End User Configuration window.

- In Cisco Unified CM Administration, use the **User Management > End User** menu path to configure end users.
- Click **Add New**.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ **User Management** ▾ Bulk Administration ▾ Help ▾

Find and List Users

Add New

User

Find User where: ▾ ▾ Find Clear Filter

No active query. Please enter your search criteria using the options above.

Add New

- We have two examples taken to configure End Users (Cisco Jabber and Cisco DX650).
- Enter the unique end user identification name.
- Enter alphanumeric or special characters for the end user password and confirm the same.
- Enter numeric characters for the end user PIN and confirm.
- Enter the end user last name.
- For Digest Credentials, enter a string of alphanumeric characters and confirm.
- For Cisco Jabber as below.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

End User Configuration

Save Delete Add New

Status

Status: Ready

User Information

Active Enabled LDAP Synchronized User

User Status
 User ID* iotuser1
 Self-Service User ID
 PIN **Edit Credential**
 Confirm PIN
 Last name* iot
 Middle name
 First name iotuser1
 Display name iotuser1 iot
 Title
 Directory URI
 Telephone Number
 Home Number
 Mobile Number
 Pager Number
 Mail ID
 Manager User ID
 Department
 User Locale
 Associated PC/Site Code
 Digest Credentials
 Confirm Digest Credentials
 User Profile [View Details](#)
 User Rank*

Convert User Account

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

End User Configuration

Save Delete Add New

Device Information

Controlled Devices

Available Profiles

CTI Controlled Device Profiles

Device Association
Line Appearance Association for Presence

Extension Mobility

Available Profiles

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

End User Configuration

Save Delete Add New

[View Details](#)

Permissions Information

Groups
 Application Client Users
 Standard Audit Users
 Standard CAR Admin Users
 Standard CCM Admin Users [View Details](#)

Roles
 Standard Admin Rep Tool Admin
 Standard Audit Log Administration
 Standard CCM Admin Users
 Standard CCM End Users [View Details](#)

Add to Access Control Group
Remove from Access Control Group

Conference Now Information

Enable End User to Host Conference Now

Meeting Number

Attendees Access Code

Save Delete Add New

*- indicates required item.

- For Cisco DX650 as below.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

End User Configuration

Save Delete Add New

Status
 Status: Ready

User Information

User Status: Enabled Local User

User ID*: 9993332004

Password:

Confirm Password:

Self-Service User ID:

PIN:

Confirm PIN:

Last name*: US_END_USER4

Middle name:

First name:

Display name:

Title:

Directory URI:

Telephone Number:

Home Number:

Mobile Number:

Pager Number:

Mail ID:

Manager User ID:

Department:

User Locale: < None >

Associated PC/Site Code:

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

End User Configuration

Save Delete Add New

Device Information

Controlled Devices: SEP2C3ECF76A6AF

Available Profiles:

CTI Controlled Device Profiles:

Extension Mobility

Available Profiles:

Controlled Profiles:

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

End User Configuration

Save Delete Add New

MLPP User Identification Number

MLPP Password

Confirm MLPP Password

MLPP Precedence Authorization Level

CAPF Information

Associated CAPF Profiles

[View Details](#)

Permissions Information

Groups

- Admin-3rd Party API
- Application Client Users
- Standard Audit Users
- Standard CAR Admin Users
- Standard CCM Admin Users

[View Details](#)

Roles

- Standard AXL API Access
- Standard Admin Rep Tool Admin
- Standard Audit Log Administration
- Standard CCM Admin Users
- Standard CCM End Users

[View Details](#)

Add to Access Control Group

Remove from Access Control Group

Conference Now Information

Enable End User to Host Conference Now

Meeting Number

Attendees Access Code

Save Delete Add New

Phone Setup

- In Cisco Unified Communications Manager Administration, use the **Device > Phone** menu path to configure phones.
- Click **Add New**.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Find and List Phones

Related Links: [Actively Logged In Device Report](#) Go

Add New Add New From Template

Phone

Find Phone where begins with Find Clear Filter

Select item or enter search text

No active query. Please enter your search criteria using the options above.

Add New Add New From Template

- From the Phone Type drop-down, choose Third-party AS-SIP Endpoint.
- Click **Next**.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Add a New Phone

Next

Status

Status: Ready

Add New Phone Information

Start by selecting the type of phone you wish to add, or [click here to add a new phone using a Universal Device Template](#).

Phone Type*

Next

*- indicates required item.

** - Create a phone template using the Bulk Administration Tool to enable template-based phone creation.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Phone Configuration Related Links: [Back To Find/List](#)

Save Delete Copy Reset Apply Config Add New

Status
Status: Ready

Association

Modify Button Items

- Line [1] - 9993332009 (no partition)
- Line [2] - Add a new DN
- Line [3] - Add a new DN
- Line [4] - Add a new DN
- Line [5] - Add a new DN
- Line [6] - Add a new DN
- Line [7] - Add a new DN
- Line [8] - Add a new DN

Phone Type

Product Type: Cisco Unified Client Services Framework
Device Protocol: SIP

Real-time Device Status

Registration: Unknown
IPv4 Address: None

Device Information

Device is Active
 Device is trusted

Device Name* iotuser1
Description iotuser1 SANTOSH
Device Pool* Default [View Details](#)
Common Device Configuration < None > [View Details](#)
Phone Button Template* Standard Client Services Framework
Common Phone Profile* Standard Common Phone Profile [View Details](#)
Calling Search Space < None >
AAR Calling Search Space < None >
Media Resource Group List san_media_grplist

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Phone Configuration Related Links: [Back To Find/List](#)

Save Delete Copy Reset Apply Config Add New

Packet Capture Mode* None
Packet Capture Duration 0
BLF Presence Group* Standard Presence group
SIP Dial Rules < None >
MTP Preferred Originating Codec* 711ulaw
Device Security Profile* secure_jabber
Rerouting Calling Search Space < None >
SUBSCRIBE Calling Search Space < None >
SIP Profile* SAN_SIP_PROFILE [View Details](#)
Digest User iotuser1

Media Termination Point Required
 Unattended Port
 Require DTMF Reception

Certification Authority Proxy Function (CAPF) Information

Certificate Operation* No Pending Operation
Authentication Mode* By Null String
Authentication String

Key Order* RSA Only
RSA Key Size (Bits)* 2048
EC Key Size (Bits)
Operation Completes By 2021 12 30 12 (YYYY-MM-DD:HH)
Certificate Operation Status: None
Note: Security Profile Contains Addition CAPF Settings.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Directory Number Configuration

Save Delete Reset Apply Config Add New

Status
Status: Ready

Directory Number Information

Directory Number* 9993332009 Urgent Priority
Route Partition < None >
Description
Alerting Name
ASCII Alerting Name
External Call Control Profile < None >
 Allow Control of Device from CTI
Associated Devices iotuser1 [Edit Device](#)
[Edit Line Appearance](#)
Dissociate Devices

Directory Number Settings

Voice Mail Profile < None > (Choose <None> to use system default)
Calling Search Space < None >
BLF Presence Group* Standard Presence group

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List Users

Select All Clear All Add Selected Close

Status
2 records found

User (1 - 2 of 2) Rows per Page 250 ▾

Find User where First name begins with iot Find Clear Filter + -

<input type="checkbox"/>	User ID ^	Meeting Number	First Name	Last Name	Department	Directory URI	User Status	User Rank
<input checked="" type="checkbox"/>	iotuser1		iotuser1	iot			Active Enabled LDAP Synchronized User	1
<input type="checkbox"/>	iotuser2		iotuser2	iot			Active Enabled LDAP Synchronized User	1

Select All Clear All Add Selected Close

- Choose Device Trust Mode as **Not Trusted**, if third part end point is selected for phone button template.
- Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones. Ensure that the value comprises 12 hexadecimal characters.
- Choose **Default** Device pool.
 - A Device pool defines sets of common characteristics for devices, such as region, date/time group, and soft key template.
- Choose **Cisco Unified Client Services Framework** for Jabber clients or **Cisco DX650** for DX650 phones from the phone button template drop-down.
 - The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
- Associate the Media Resource Group List created.
- Choose the user ID of the assigned phone user.



Note

CUCM supports auto registration of Cisco endpoints, refer to the following link for more details:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/10_0_1/ccmctg/CUCM_BK_C95ABA82_00_admin-guide-100/CUCM_BK_C95ABA82_00_admin-guide-100_chapter_011010.html

- Choose the security profile to apply to the device. Customer can choose to have a Non-Secure SIP Profile if they are using a Non-Secure SIP Trunk.
- Associate the SIP Profile created before.
 - SIP profiles provide specific SIP information for the phone such as registration and keep-alive timers, media ports, and do not disturb control.
- Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security).
- Update the CAPF information.
- Click **Save**.
- For DX650 select as below.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Add a New Phone

Next

Status
Status: Ready

Add New Phone Information

Start by selecting the type of phone you wish to add, or [click here to add a new phone using a Universal Device Template](#).

Phone Type* Cisco DX650 ▾

Next

i *- indicates required item.
i **- Create a phone template using the Bulk Administration Tool to enable template-based phone creation.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Phone Configuration Related Links: [Back To](#)

Save
 Delete
 Copy
 Reset
 Apply Config
 Add New

Protocol Specific Information

Packet Capture Mode*
 Packet Capture Duration
 BLF Presence Group*
 SIP Dial Rules
 MTP Preferred Originating Codec*
 Device Security Profile*
 Rerouting Calling Search Space
 SUBSCRIBE Calling Search Space
 SIP Profile* [View Details](#)
 Digest User
 Media Termination Point Required
 Unattended Port
 Require DTMF Reception

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*
 Authentication Mode*
 Authentication String

 Key Order*
 RSA Key Size (Bits)*
 EC Key Size (Bits)
 Operation Completes By (YYYY:MM:DD:HH)
 Certificate Operation Status: None
 Note: Security Profile Contains Addition CAPF Settings.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Phone Configuration Related Links: [Back To](#)

Save
 Delete
 Copy
 Reset
 Apply Config
 Add New

Protocol Specific Information

Packet Capture Mode*
 Packet Capture Duration
 BLF Presence Group*
 SIP Dial Rules
 MTP Preferred Originating Codec*
 Device Security Profile*
 Rerouting Calling Search Space
 SUBSCRIBE Calling Search Space
 SIP Profile* [View Details](#)
 Digest User
 Media Termination Point Required
 Unattended Port
 Require DTMF Reception

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*
 Authentication Mode*
 Authentication String

 Key Order*
 RSA Key Size (Bits)*
 EC Key Size (Bits)
 Operation Completes By (YYYY:MM:DD:HH)
 Certificate Operation Status: None
 Note: Security Profile Contains Addition CAPF Settings.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Phone Configuration Related Links: [Back To Find/List](#)

Save Delete Copy Reset Apply Config Add New

22	Group Call Pickup	Privacy*	Off	▾
23	Intercom [1] - Add a new Intercom	Device Mobility Mode*	Default	▾ View Current Device Mobility Settings
24	Malicious Call Identification	Wireless LAN Profile Group	< None >	▾ View Details
25	Meet Me Conference	Owner	<input checked="" type="radio"/> User <input type="radio"/> Anonymous (Public/Shared Space)	
26	Mobility	Owner User ID*	9993332004	▾
27	Other Pickup	Mobility User ID	< None >	▾
28	Quality Reporting Tool	Phone Personalization*	Default	▾
29	Record	Services Provisioning*	Default	▾
30	Add a new SURL	Phone Load Name	<input type="text"/>	
31	Services	Use Trusted Relay Point*	Default	▾
32	Add a new BLF SD	BLF Audible Alert Setting (Phone Idle)*	Default	▾
33	Hunt Group Logout	BLF Audible Alert Setting (Phone Busy)*	Default	▾
34	Queue Status	Always Use Prime Line*	Default	▾
35	Privacy	Always Use Prime Line for Voice Message*	Default	▾
36	None	Geolocation	< None >	▾
		Feature Control Policy	< None >	▾

Ignore Presentation Indicators (internal calls only)
 Allow Control of Device from CTI
 Logged Into Hunt Group
 Remote Device
 Protected Device****

Number Presentation Transformation

- Click this link to add a remote destination to associate with this device. The Remote Destination Configuration window displays, which allows you to add a new remote destination to associate with this device.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Directory Number Configuration

Save Delete Reset Apply Config Add New

Directory Number Information

Directory Number* Urgent Priority

Route Partition ▾

Description

Alerting Name

ASCII Alerting Name

External Call Control Profile ▾

Allow Control of Device from CTI

Associated Devices

Dissociate Devices

Directory Number Settings

Voice Mail Profile ▾ (Choose <None> to use system default)

Calling Search Space ▾

BLF Presence Group* ▾

User Hold MOH Audio Source ▾

Network Hold MOH Audio Source ▾

Auto Answer* ▾

Reject Anonymous Calls

- Add the Directory number.
- Click **Save**.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Directory Number Configuration Related Links: [Configure Device \(SEP2C3ECF76A6AF\)](#) Go

Save Delete Reset Apply Config Add New

Monitoring Calling Search Space: < None >

Log Missed Calls

Multiple Call/Call Waiting Settings on Device SEP2C3ECF76A6AF

Note: The range to select the Max Number of calls is: 1-200

Maximum Number of Calls*:

Busy Trigger*: (Less than or equal to Max. Calls)

Forwarded Call Information Display on Device SEP2C3ECF76A6AF

Caller Name
 Caller Number
 Redirected Number
 Dialed Number

Users Associated with Line

	Full Name	User ID	Permission
<input checked="" type="checkbox"/>	US_END_USER4	9993332004	

Associate End Users | Select All | Clear All | Delete Selected

Save Delete Reset Apply Config Add New

* - indicates required item.
 ** - Changes to Line or Directory Number settings require restart.

- Click the **Associate End User** button.
- Select the end user created from the list and click **Add Selected**.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Find and List Users

Select All Clear All Add Selected Close

Status

1 records found

User (1 - 1 of 1) Rows per Page: 250

Find User where User ID begins with 9993332004 Find Clear Filter

User ID	Meeting Number	First Name	Last Name	Department	Directory URI	User Status	User Rank
<input checked="" type="checkbox"/>	9993332004		US_END_USER4			Enabled Local User	1

Select All Clear All Add Selected Close

- After the above step, the user association is completed.
- Save the configuration.
- Click **Apply Config** followed by the Reset button.
- Reset, Restart and Close the window.

Device Association

- Navigate back to **User Management > End User**.
- In the Device Information field, click **Device Association**. This will display all the available devices.
- Select the device created in the previous step and save.
- After selecting the appropriate device, it will appear in the Controlled Devices pane.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

User Device Association Related Links: [Back to User](#)

Select All Clear All Select All In Search Clear All In Search Save Selected/Changes Remove All Associated

User Device Association For iotuser1 (1 - 25 of 25) Rows per Page: 50

Find User Device Association where Name begins with Find Clear Filter

Show the devices already associated with iotuser1

	Device Name	Directory Number	Description
<input checked="" type="checkbox"/>	iotuser1	9993332009	iotuser1 SANTOSH
<input type="checkbox"/>	BAT401190095433		
<input type="checkbox"/>	SEP0004F24FD1F5	9993332029	SEP0004F24FD1F5

Device Information

Controlled Devices:

Available Profiles:

CTI Controlled Device Profiles:

Device Association:

- For DX650 as below.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

End User Configuration

Save Delete Add New

Device Information

Controlled Devices:

Available Profiles:

CTI Controlled Device Profiles:

Device Association:

Extension Mobility

Available Profiles:

Controlled Profiles:

Enable MoH

In Cisco Unified Communications Manager Administration, use the **System > Service Parameters** menu path to configure service parameters.

- In the Server drop-down list box in the Service Parameter Configuration window, choose the CUCM server being used. In this case, active means that you provisioned the server in Cisco Unified Communications Manager Administration.
- From Service drop-down select Cisco CallManager. The service displays as active in the Service Parameters Configuration window.

System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help

Service Parameter Configuration

Save Set to Default Advanced

Related Links: Parameters for All Servers Go

Status: Ready

Select Server and Service

Server*:

Service*:

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

Cisco CallManager (Active) Parameters on server 10.54.22.250--CUCM Voice/Video (Active)

Parameter Name	Parameter Value	Suggested Value
Call Throttling		
Code Yellow Entry Latency *	<input type="text" value="20"/>	20
Code Yellow Exit Latency Calculation *	<input type="text" value="40"/>	40
Code Yellow Duration *	<input type="text" value="5"/>	5
Max Events Allowed *	<input type="text" value="2000"/>	2000
System Throttle Sample Size *	<input type="text" value="10"/>	10

- Set the Duplex Streaming Enabled flag to True. This parameter determines whether Music On Hold (MOH) and Annunciator use duplex streaming.
- Click **Save**.

Service Parameter Configuration		
Clusterwide Parameters (Service)		
Default Network Hold MOH Audio Source ID *	1	1
Default User Hold MOH Audio Source ID *	1	1
Duplex Streaming Enabled *	True	False
Media Exchange Interface Capability Timer *	8	8
Send Multicast MOH in H.245 OLC Message *	True	True
Media Exchange Timer *	12	12
Media Exchange Stop Streaming Timer *	8	8
Open Video Channel Response Timer for SIP Interop *	500	500
Port Received Timer After Call Connection *	500	500
Media Resource Allocation Timer *	12	12
MTP and Transcoder Resource Throttling Percentage *	95	95
Intercluster Capabilities Mismatch Timer *	1000	1000
Silence Suppression *	False	False
Silence Suppression for Gateways *	False	False
Strip G.729 Annex B (Silence Suppression) from Capabilities *	False	False
Enable Source IP Address Verification for Software Media Devices *	True	True
Clusterwide Parameters (System - General)		
Always Use Dial Tone Setting *	Default	Default
Restart Cisco CallManager on Initialization Exception *	True	True
Doit Analysis Timer *	6	6
Statistics Enabled *	True	True

- From Service drop-down select Cisco IP Voice Streaming App. The service displays as active in the Service Parameters Configuration window.
- Set the Supported MOH Codecs.
- Click **Save**.

Service Parameter Configuration

Status: Update successful

Select Server and Service

Server*: 10.54.22.250--CUCM Voice/Video (Active)

Service*: Cisco IP Voice Media Streaming App (Active)

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

Clusterwide Parameters (Parameters that apply to all servers)

Supported MOH Codecs *

711 mulaw
711 alaw
729 Annex A

Section C: Microsoft Teams Direct Routing

For Microsoft Teams related configurations and queries, please contact the Microsoft technical support team, for details visit: <https://support.microsoft.com/contactus>

For detailed information about Microsoft Teams direct routing products and solutions, please visit:

- <https://docs.microsoft.com/en-us/microsoftteams/cloud-voice-landing-page>
- <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure>



Note

This interop was performed with Media-Bypass OFF configuration on Microsoft Teams Direct Routing.

Supplementary Services & Features Coverage

The following checklist depicts the set of services/features covered through the configuration defined in this Interop Guide.

Sr. No.	Supplementary Services/ Features	Coverage
01.	OPTIONS validation	✓
02.	Call Setup and Termination over TLS	✓
03.	Ringling and Local Ringback Tone	✓

04.	Remote Ringback Tone Handling	✓
05.	Cancel Call, No Answer, Busy and Call Rejection	✓
06.	Basic Call with different codecs	✓
07.	DTMF	✓
08.	Anonymous Calls	✓
09.	Call Hold and Resume	✓
10.	Call Forward - Unconditional, Busy and No Answer	✓
11.	Call Transfer (Blind/Unattended)	✓
12.	Call Transfer (Attended)	✓
13.	Call Conference	✗
14.	Meet Me Conference	✗
15.	4xx/5xx Response Handling	✓
16.	Long Duration Calls	✓
17.	Early and Late Media	✓
18.	Simultaneous Ringing	✓
19.	Transcode Calls	✓

Legend

Supported	✓
Not Supported	✗

Caveats

- Meet Me and Adhoc conference could not be tested due to unavailability of hardware transcoder within the lab environment. Lab has CUCM software conference bridge that does not support sRTP. Customers using non-secure trunk and media will not face this issue. For more details visit https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/11_0_1/secugd/CUCM_BK_C1A78C1D_00_cucm-security-guide-1101/secure_conference_resources_setup.pdf
- Media packet Loss issue is observed between the end points for basic call scenarios that is a known issue to Ribbon. This issue has been addressed and will be fixed in the upcoming SBC release.
- Media packet Loss issue is observed between the TEAMS end points for call forward and call transfer scenarios that is a known issue to Ribbon. This issue has been addressed and will be fixed in the upcoming SBC release.
- Proxy with sRTP relay mode for comfort noise and RTCP passthrough scenarios issue is observed that is a known issue to Ribbon. This issue has been addressed and will be fixed in the upcoming SBC release.

Support

For any support related queries about this guide, please contact your local Ribbon representative, or use the details below:

- Sales and Support: 1-833-742-2661
- Other Queries: 1-877-412-8867
- Website: <https://ribboncommunications.com/about-us>

References

For detailed information about Ribbon products and solutions, please visit: <https://ribboncommunications.com/products>

For additional information on Cisco Unified Communications Manager, please visit: <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>

For additional information on Ribbon SBC SWe Edge on Azure, please visit: [Deploying an SBC SWe Edge from the Azure Marketplace](#).

Conclusion

This Interoperability Guide describes successful configuration of interop involving Ribbon SBC SWe Edge on Azure, Cisco Unified Communications Manager and Microsoft Teams.

All features and capabilities tested are detailed within this document - any limitations, notes or observations are also recorded in order to provide the reader with an accurate understanding of what has been covered and what has not.

Configuration guidance is provided to enable the reader to replicate the same base setup - additional configuration changes are possibly required to suit the exact deployment environment.

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved.