Ribbon SBC Edge SWe Lite R9.0 on Azure Interop with Cisco UCM : Interoperability Guide

Interoperable Vendors

Copyright

Document Overview

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

References

- For additional information on Cisco Unified Communication 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 Lite, refer to Deploying an SBC SWe Lite from the Azure Marketplace

About Ribbon SBC SWe Lite

The Ribbon Session Border Controller Software Edition Lite (SBC SWe Lite) provides best-in class communications security. The SBC SWe Lite dramatically simplifies the deployment of robust communications security services for SIP Trunking, Direct Routing and Cloud UC services. The SBC SWe Lite 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 Communication Manager

Cisco Unified Communication 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.

Scope

This document provides configuration best practices for deploying Ribbon's SBC SWe Lite with Cisco Unified Communication 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 which 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 Lite 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 Lite on Azure
- SBC SWe Lite License
  - This interop requires the acquisition and application of cloud SIP sessions, as documented at Cloud-Based SBC SWe Lite Deployment Licenses
- Public IP Addresses
- Service Provider SIP Trunk
- TLS Certificates for SBC SWe Lite
  - Refer to Working with Certificates

Product and Device Details

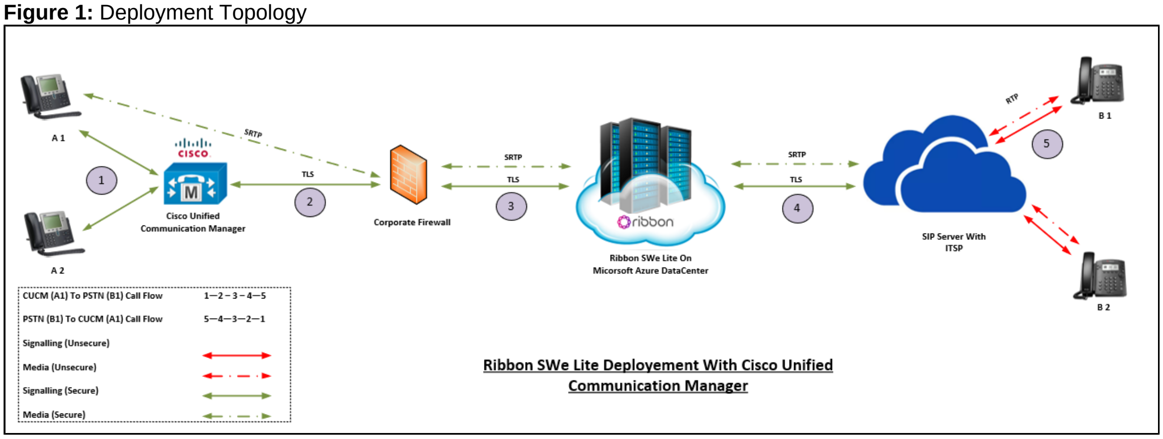
	Equipment/ Product	Software Version
Ribbon Communications	Ribbon SBC SWe Lite	9.0
Third-Party Products	Cisco Unified Communication Manager	11.0

Administration and Debugging Tools	Wireshark	3.2.7
	LX Tool	2.1.0.6

Network Topology Diagram

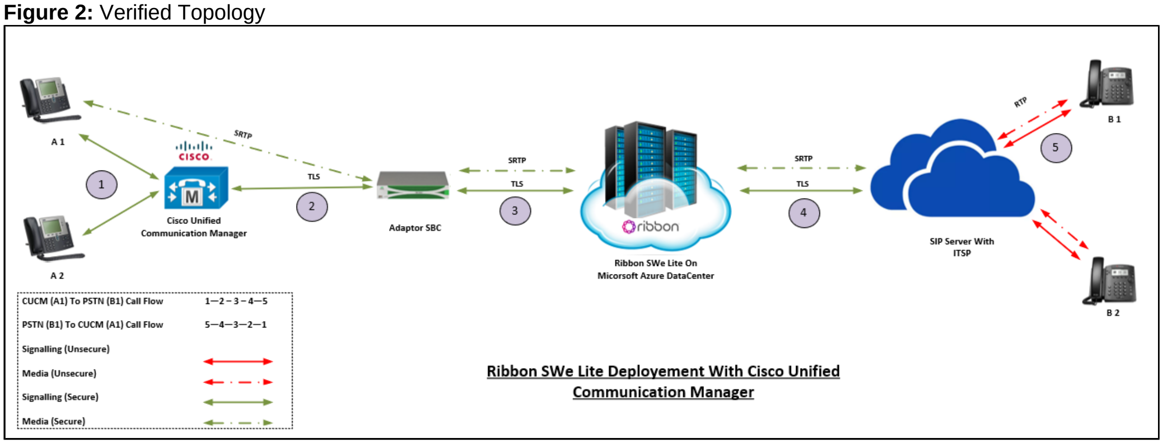
Deployment Topology

Figure 1: Deployment Topology



Interoperability Test Lab Topology (Call Flow Diagram)

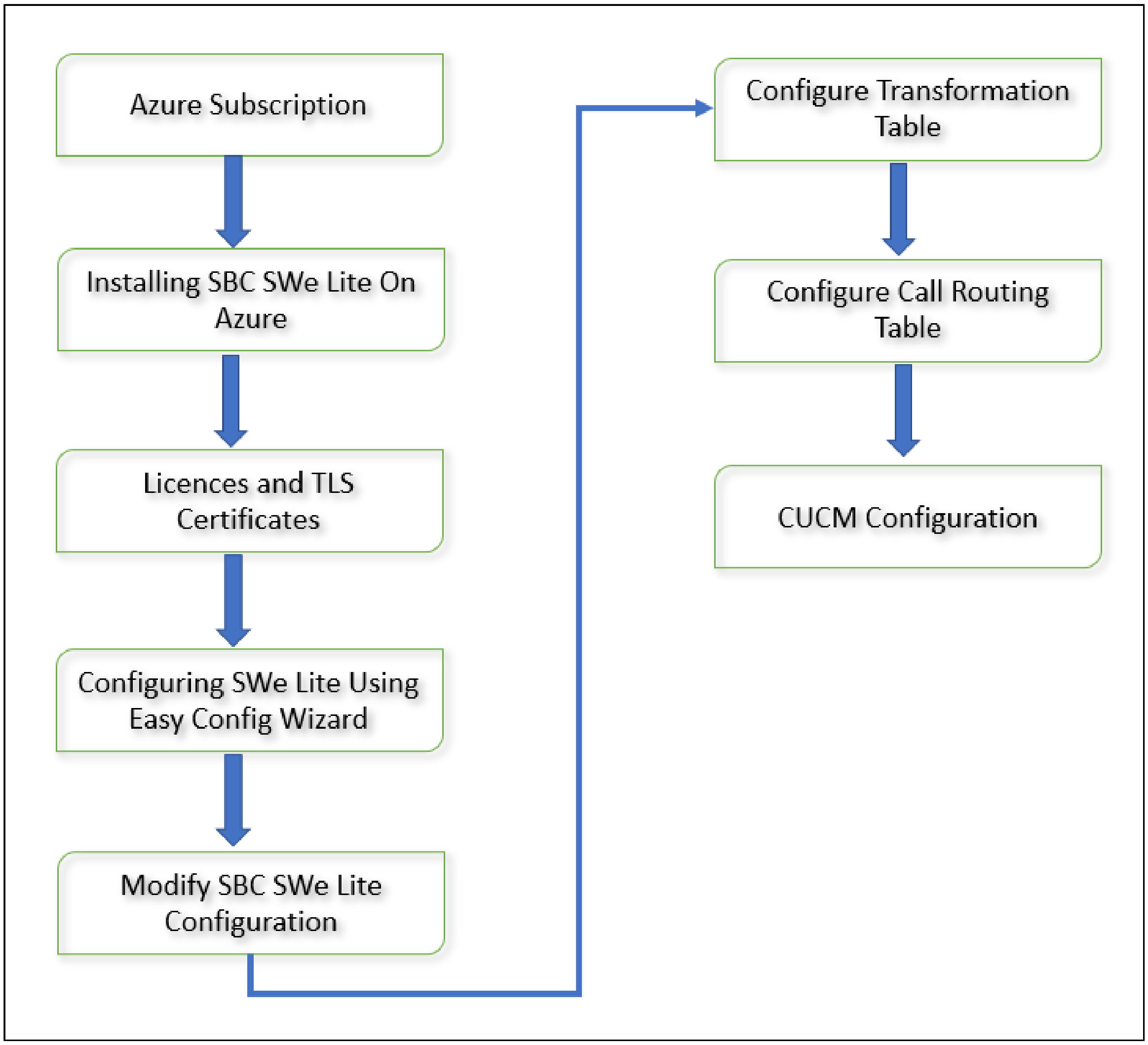
Figure 2: Verified Topology



Document Workflow

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

Figure 3: Document Workflow



Installing SBC SWe Lite On Azure

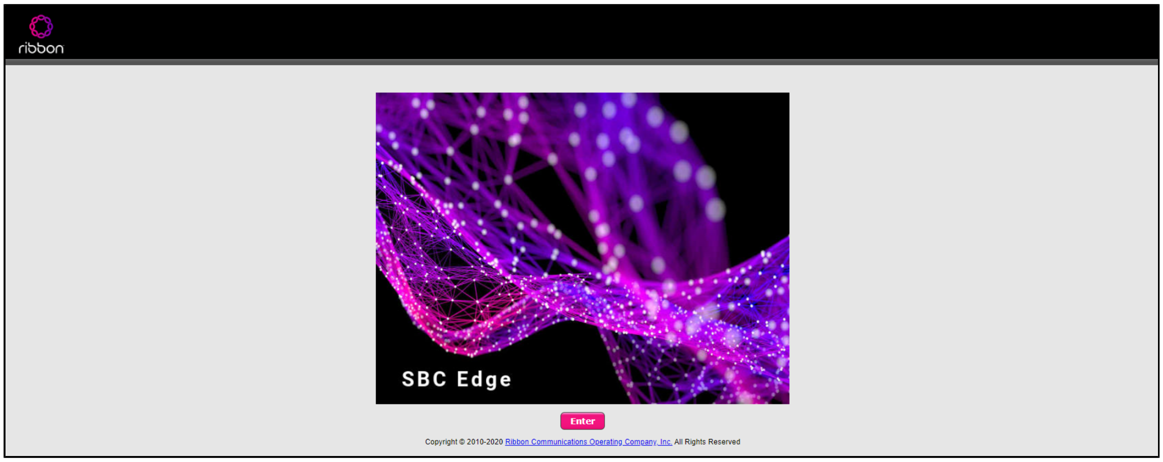
The SBC SWe Lite is available for deployment in Azure. It is created as a virtual machine (VM) hosted in Azure. To deploy an SBC SWe Lite instance, refer to Deploying an SBC SWe Lite from the Azure Marketplace.

SBC SWe Lite Configuration

Accessing SBC SWe Lite

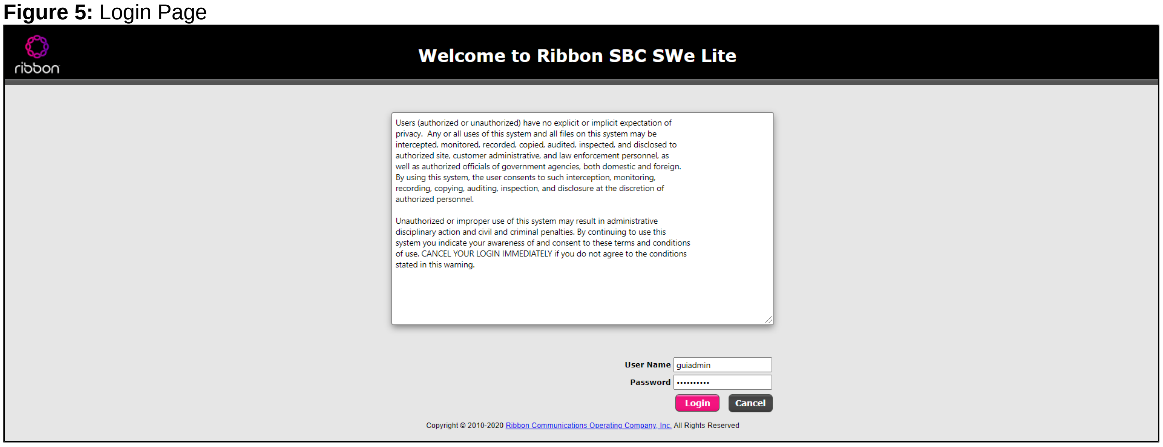
Open any browser and enter the SBC SWe Lite IP address.

Figure 4: Login Page



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

Figure 5: Login Page



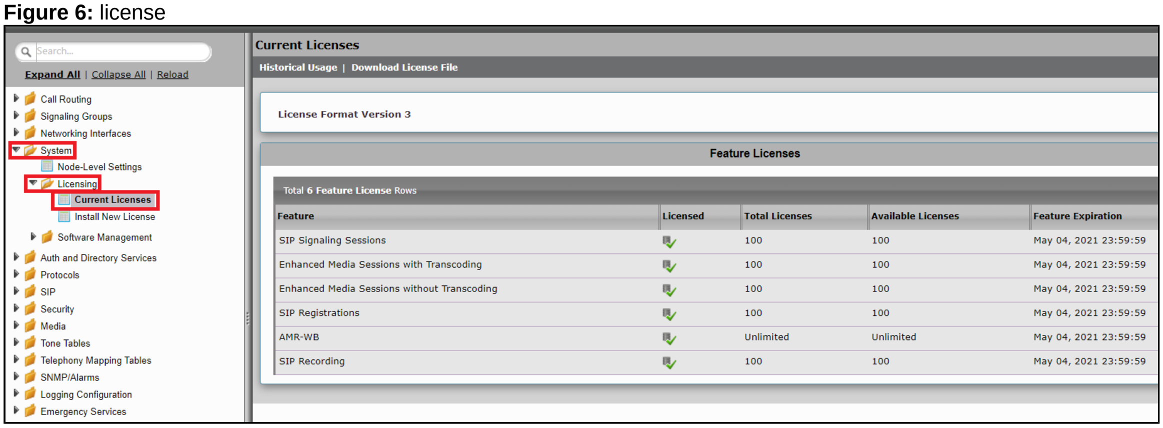
License and TLS Certificates

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.**

Figure 6: license



Feature	Licensed	Total Licenses	Available Licenses	Feature Expiration
SIP Signaling Sessions		100	100	May 04, 2021 23:59:59
Enhanced Media Sessions with Transcoding		100	100	May 04, 2021 23:59:59
Enhanced Media Sessions without Transcoding		100	100	May 04, 2021 23:59:59
SIP Registrations		100	100	May 04, 2021 23:59:59
AMR-WB		Unlimited	Unlimited	May 04, 2021 23:59:59
SIP Recording		100	100	May 04, 2021 23:59:59

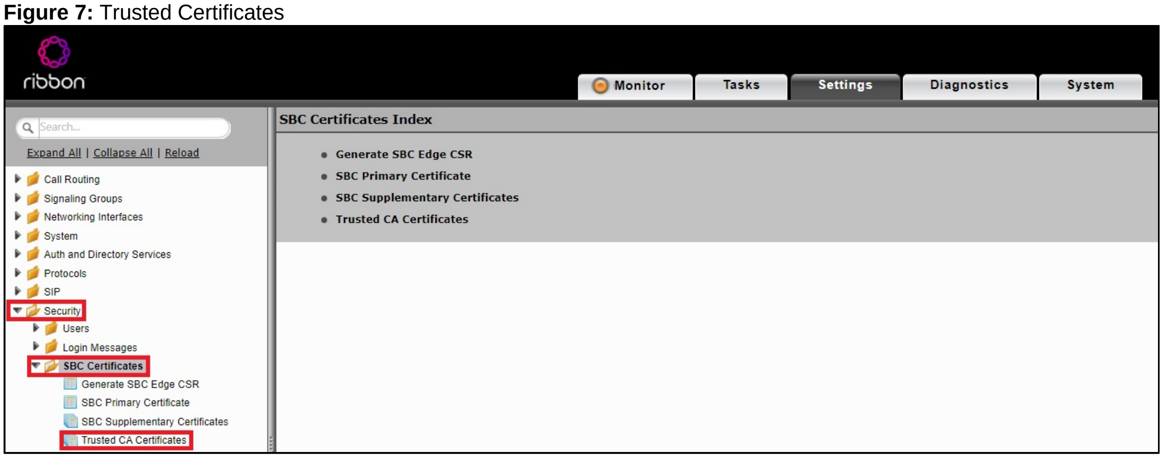
For more details on Licenses, refer to Cloud-Based SBC SWe Lite Deployment Licenses.

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 Lite to establish its authenticity on the network.

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

Figure 7: Trusted Certificates



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

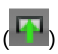
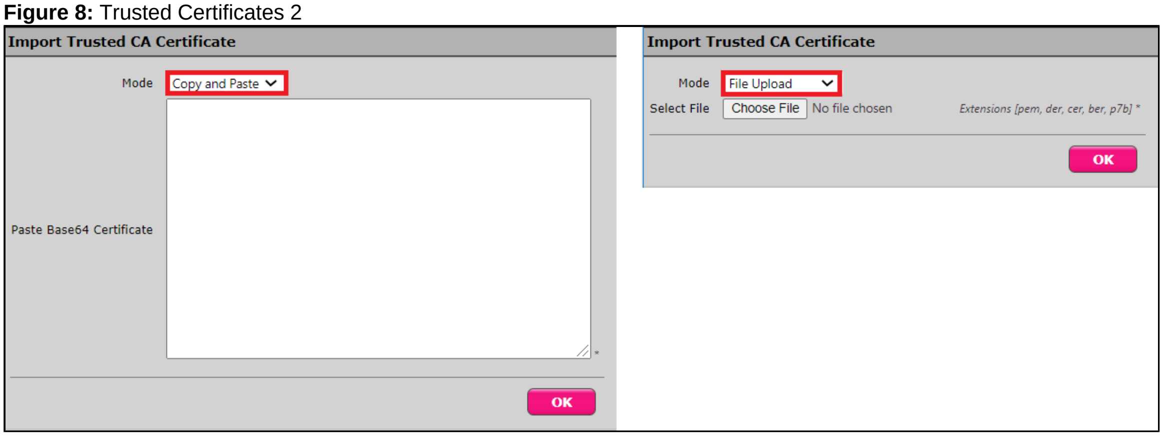
1. To import a Trusted CA Certificate, click the Import Trusted CA Certificate () Icon.
2. Select either Copy and Paste or File Upload from the **Mode** menu.
3. If you choose **File Upload**, use the **Select File** button to find the file.
4. Click **OK**.

Figure 8: Trusted Certificates 2



Follow the above steps 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.

View Networking Interfaces

The SBC SWe Lite 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.

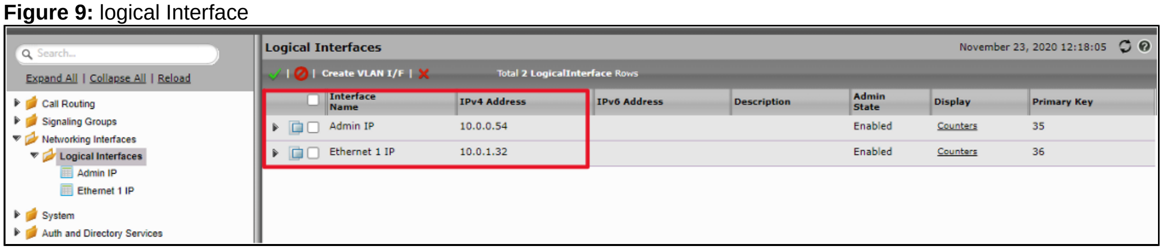
Administrative IP, Ethernet 1 IP and Ethernet 2 IP are used for this interop.

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

Administrative IP

The SBC SWe Lite 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 Lite system.

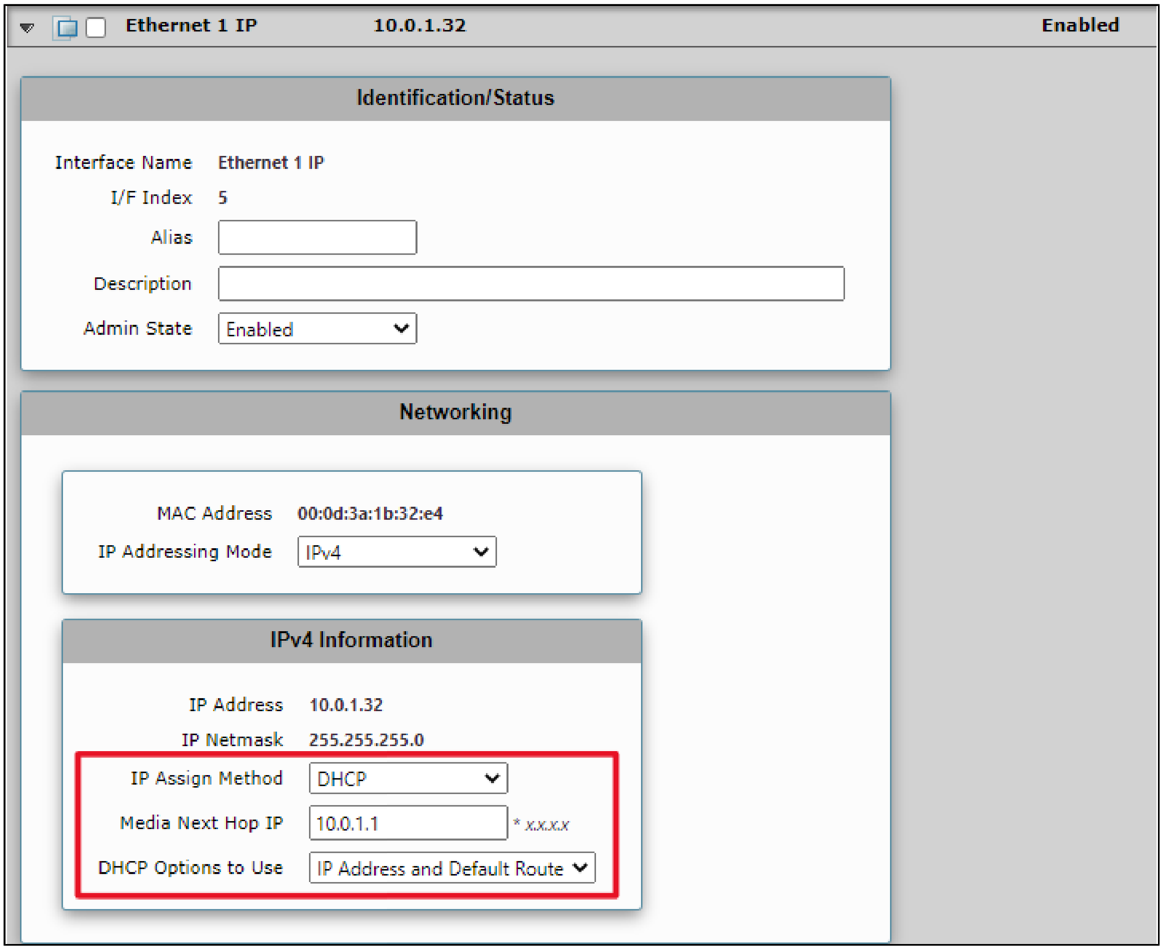
Figure 9: logical Interface



Ethernet 1 IP

Ethernet 1 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 Lite system hostname to this IP address. In the default software, **Ethernet 1 IP** is enabled and an IPv4 address is acquired via a connected DHCP server. This IP address is used for performing Initial Setup on the SBC SWe Lite.

Figure 10: Ethernet 1



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.

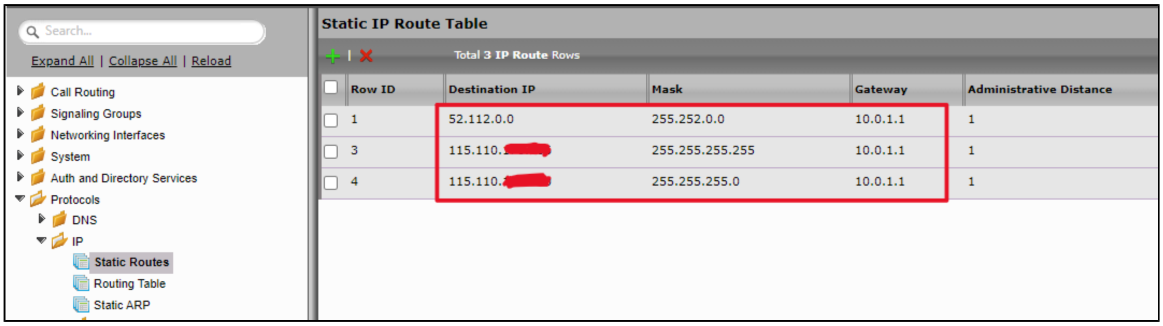
Destination IP
Specifies the destination IP address.

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 this 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.

Figure 11: Static Route



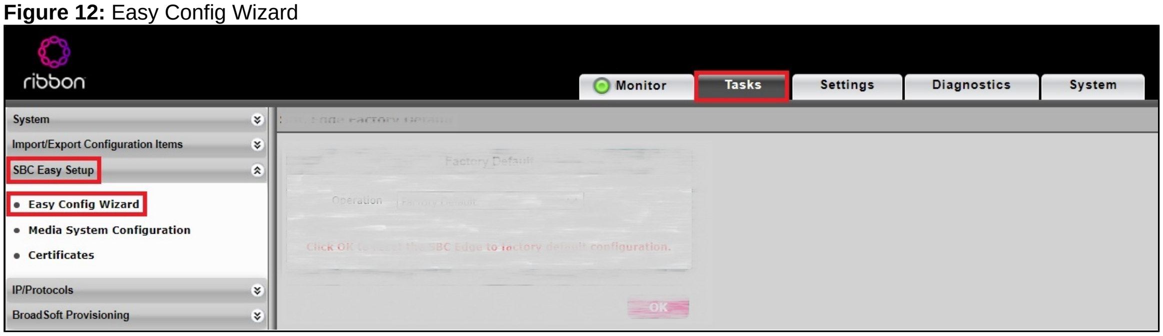
Easy Configuration Wizard

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 lets 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).

Figure 12: Easy Config Wizard



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 SBC SWe Lite for CUCM

Step 1: Use the Single-legged approach to configure IP PBX.

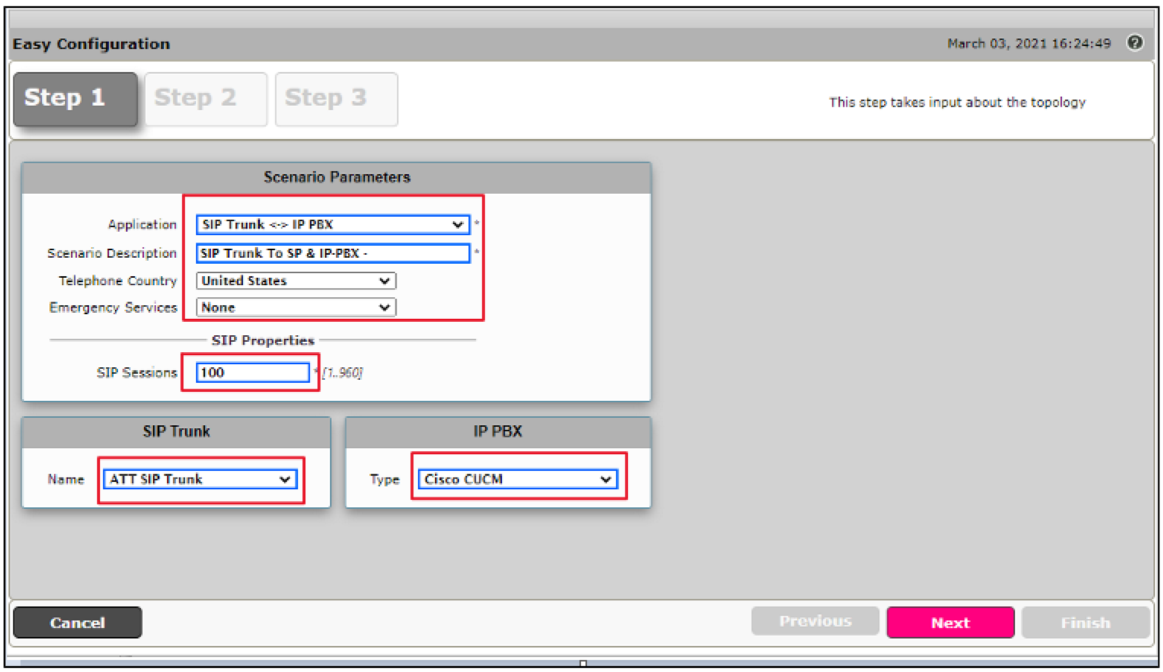
1. Click the drop-down arrow on the **Application** and select IP PBX.
2. Provide the desired description.
3. Select **Telephone Country** as India.
4. Choose from 1 to 1200 to allocate the SIP Sessions.
5. Select Cisco CUCM as **IP PBX Type.**
6. Click **Next**.

During this interop, Multi-legged approach was used to configure Service Provider SIP Trunk and IP-PBX (On-Prem CUCM) (Application: SIP Trunk CUCM)

Configure SBC SWe Lite for Service Provider SIP Trunk and for IP-PBX (On-Prem CUCM)

Step 1: Configure Trunk for Service Provider along with IP-PBX using Multi-legged approach by following the steps below:

1. Choose **SIP Trunk IP-PBX (CUCM)** from the Application dropdown.
2. Provide the Description.
3. Select **United States** in the **Telephone Country** field.
4. Type a number from 1-1200 against **SIP Sessions** field.
5. Select SIP Trunk Name and Cisco CUCM as IP-PBX.
6. Click **Next**.



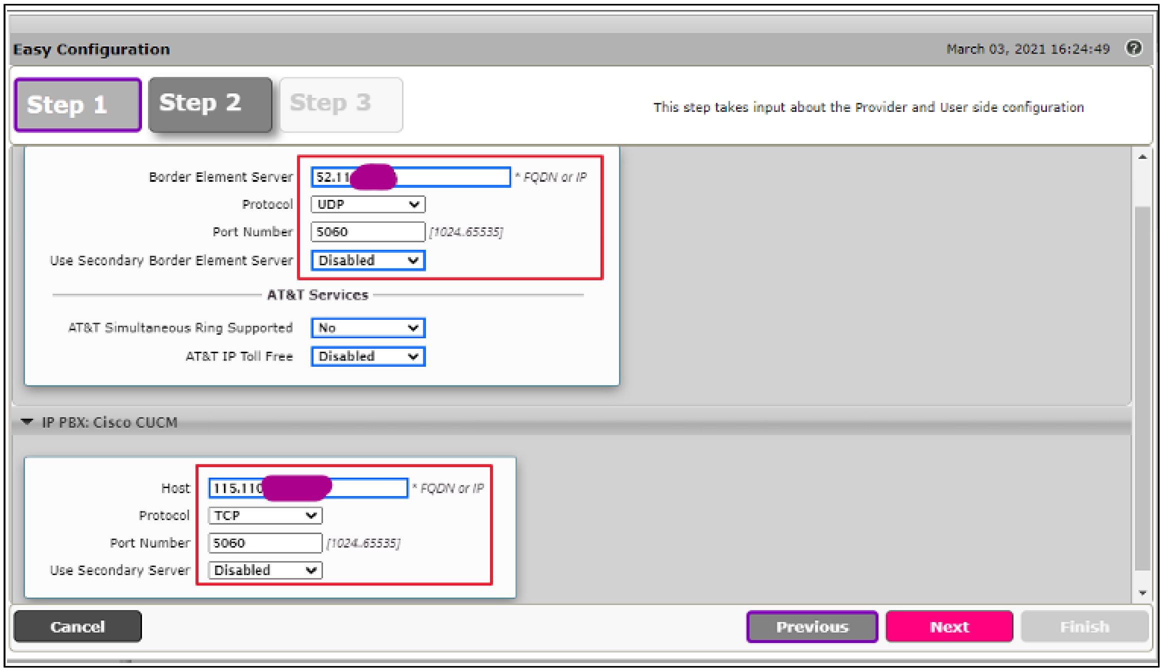
Step 2: After selecting the scenario in Step 1, the following template displays. Complete this step by performing the below actions:

1. Provide the FQDNs r IP address for Primary and Secondary Border Element servers. The traffic is sent to these FQDNs/IP from SBC SWe Lite.
2. Use **UDP/TCP** with port number 5060 for Service Provider SIP trunk configuration.

Step 3: Follow the steps below.

1. Provide the CUCM IP Address.
2. Select **UDP/TCP** as the protocol with port **5060**.

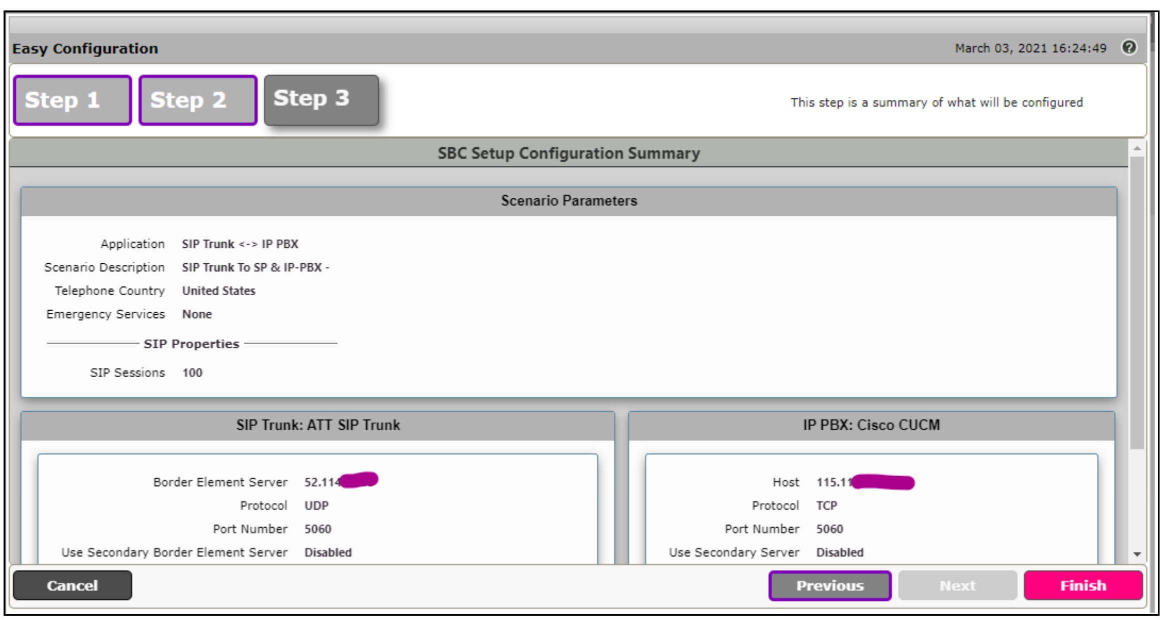
3. Click **Next**.



> **Note**
> While using "Easy Configuration Wizard" **TLS** protocol is not available by default but can be configured later.

Step 4: 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.



- 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 Service Provider and IP-PBX (CUCM) SIP Trunk on SBC SWe Lite.

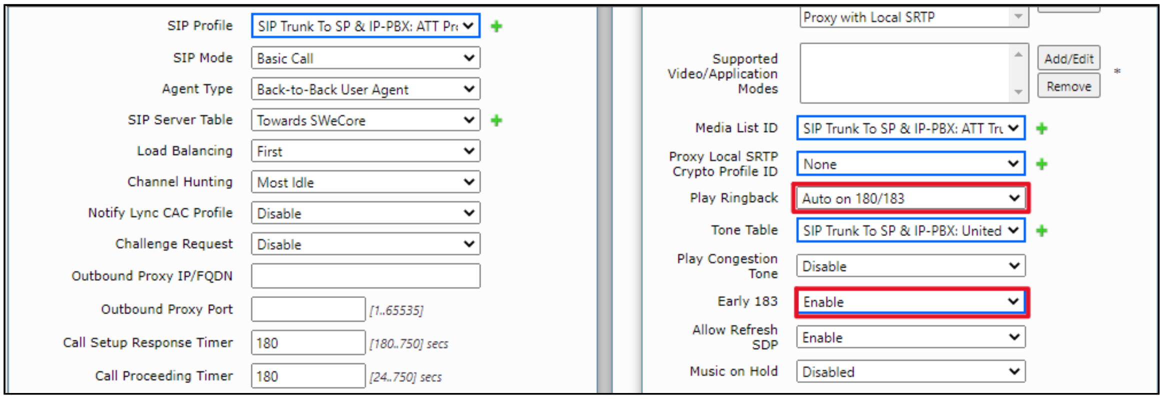
Modify SBC SWe Lite Configuration

The Easy Configuration Wizard does not currently set all applicable variables to the correct settings. This will be addressed in the subsequent SBC SWe Lite releases. Until then, follow the procedures below.

Assign NAT Public IP

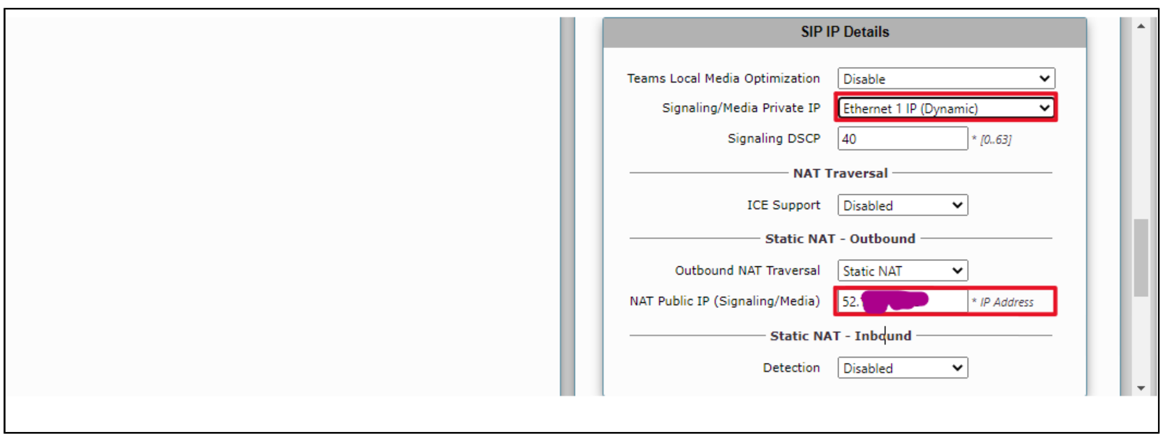
Change the settings on all the SGs as follows:

- 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.

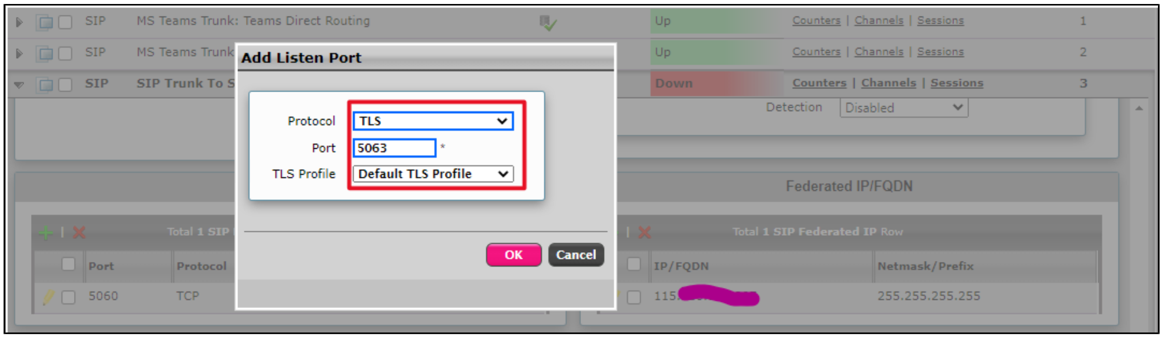


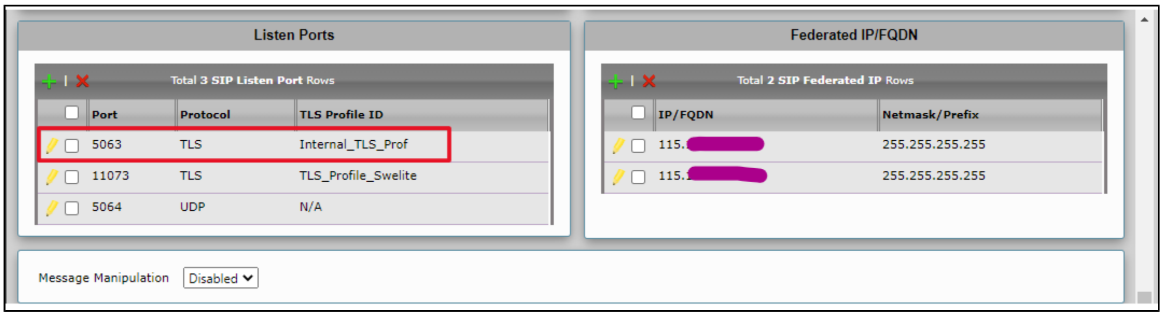
Assign TLS Protocol

> **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.

Steps:

1. Scroll down to the "**Listen Ports**" under the Signaling Group.
2. Click on "**+**" sign.
3. Choose **TLS** as preferred protocol, **Port Number** and **TLS Profile**.





Enable OPTIONS

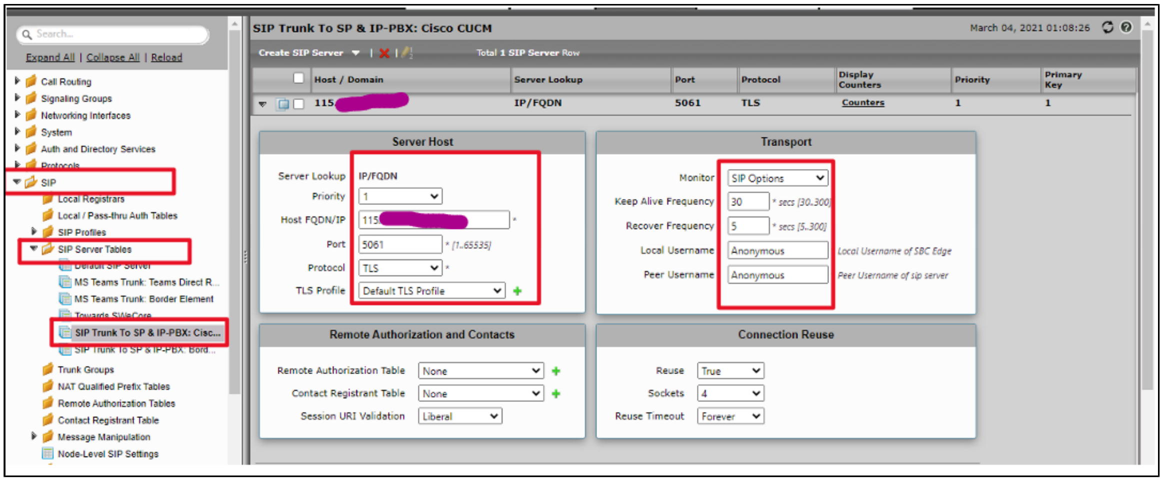
An OPTIONS message is sent to the server. When this option is selected, additional configuration items are displayed:

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.



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

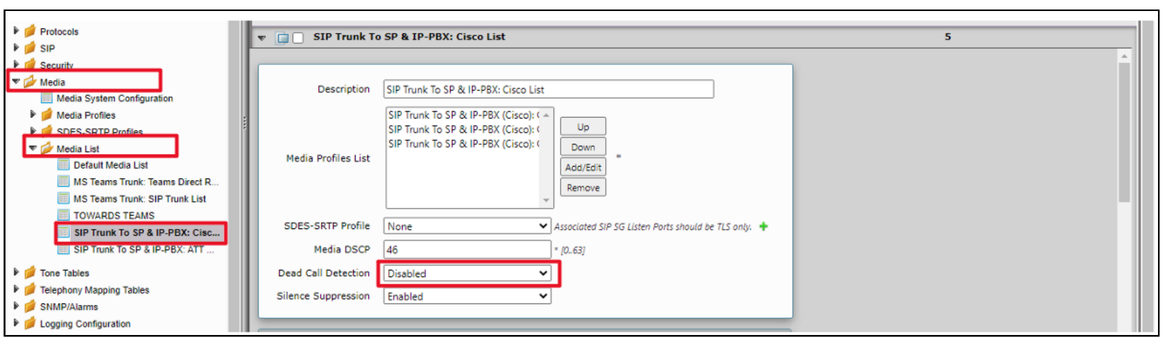
Enable Dead Call Detection

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. Disable DCD for any peer that does not send RTCP packets.

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



SBC SWe Lite Configuration for IP-PBX (CUCM) TLS/SRTP Trunk (Recommended)

This section describes the steps to configure SBC SWe Lite with TLS/SRTP towards IP-PBX (CUCM) SIP Trunk. Ribbon strongly recommends encrypting the connection between IP-PBX SIP Trunk and SBC SWe Lite.

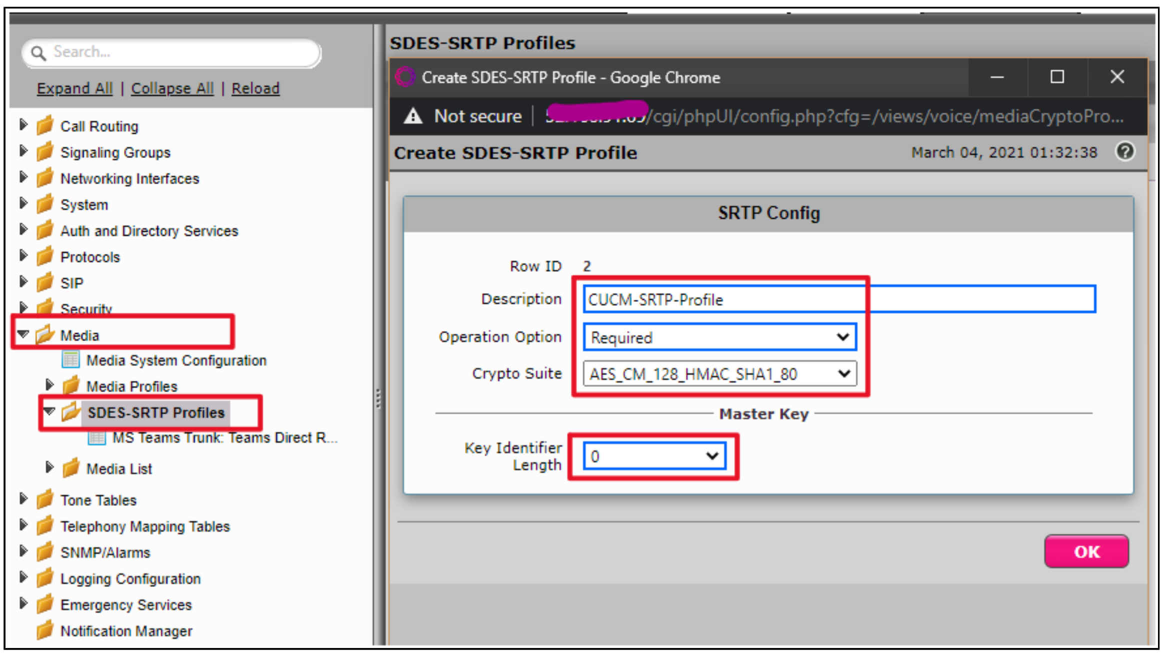
Create SRTP Profile

SDES-SRTP Profiles define a cryptographic context which 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_SHAI_80" - A crypto suite algorithm which 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**.

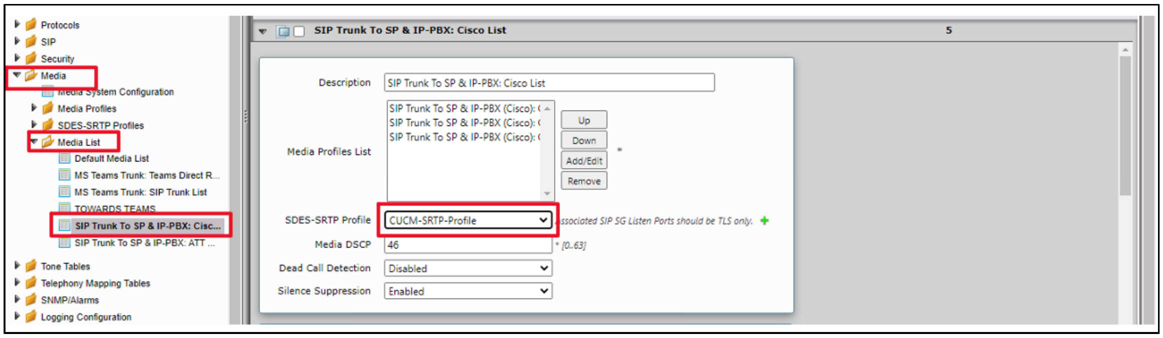


Warning
For SIP Trunk towards CUCM, If the SWe Lite SRTP profile is configured with "**Operation Option**" as "**Required**" and "**Crypto Suit**" as "**AES_CM_128_HMAC_SHA1_80**", call hold initiated from Cisco endpoint will fail. This is a known issue with Cisco CUCM. To overcome it, use "**AES_CM_128_HMAC_SHA1_32"**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

Attach SRTP Profile to the 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. Click Apply.



Update Signaling Group

Signaling Groups allow grouping telephony channels together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which Call Routes are selected.

From the **Settings** tab, navigate to **Signaling Groups.** Click the expand ( ) icon next to the entry.

1. Update the Federated IP/FQDN(Only if the FQDNs for TLS are different)..
2. Click the icon to add Listen Ports for TLS.
3. Use TLS as the Protocol and update the Port Number provided by the Service Provider (Port Number 5061 was used during this interop).
4. Click **Apply**.

Update SIP Server Table

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 > SIP TRUNK TO SP & IP-PBX: Cisco CUCM.** Click the expand ( ) icon next to the entry.

1. Modify the Host FQDN (Only if the FQDNs for TLS are different).
2. Select TLS protocol with Port Number 5061.

Configure Transformation Tables

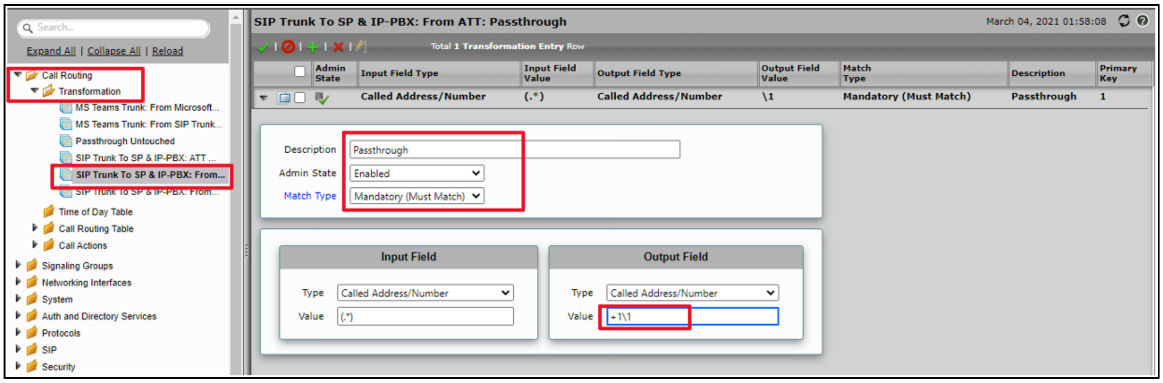
Transformation Tables facilitate the conversion of names, numbers and other fields when routing a call. They can, for example, convert a public PSTN number into a private extension number, or into a SIP address (URI). Every entry in a Call Routing Table requires a Transformation Table, and they are selected 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.

Configure Call Routing Tables

Call Routing allows carrying of calls between Signaling Groups. Routes are defined by Call Routing Tables, which allow for flexible configuration of which 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.

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 which 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 .

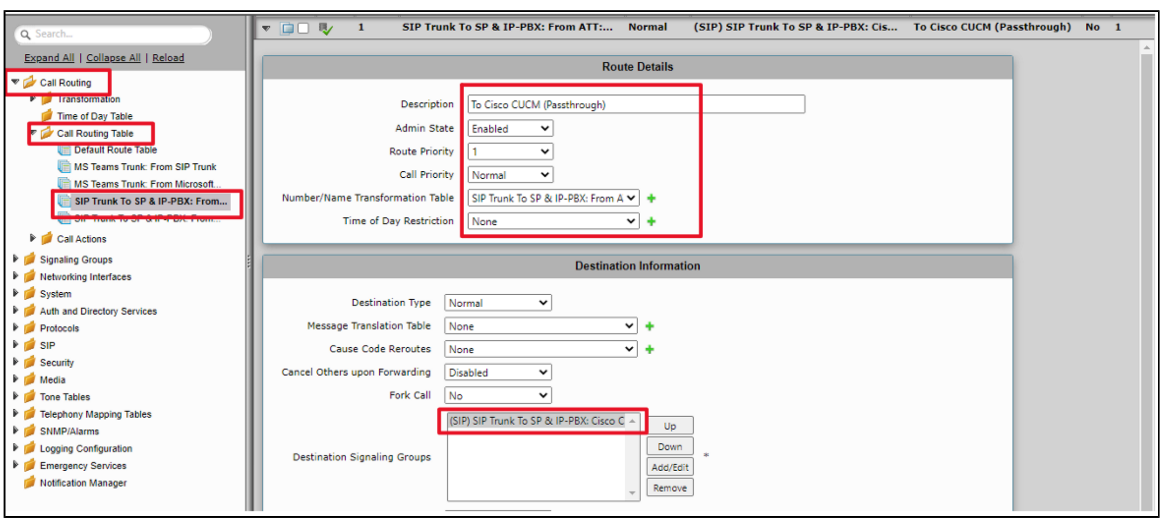
   Route Priority:
   Priority of the route from 1 (highest) to 10 (lowest). Higher priority routes are matched against before lower priority routes regardless of the order of the routes in the table.

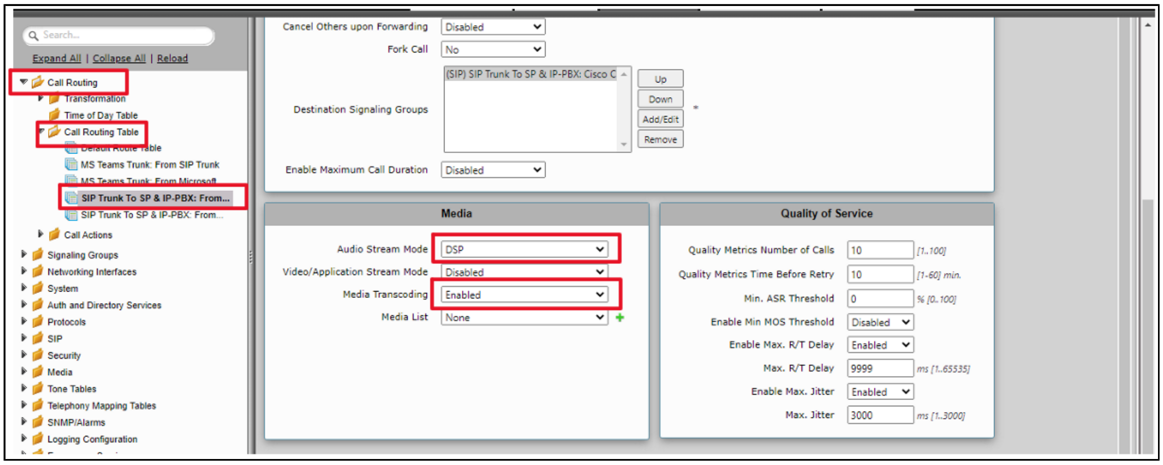
   Number/Name Transformation Table:
   Specifies the Transformation Table to use for this routing entry. This drop down list is populated from the entries in the Transformation Table.

   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**.

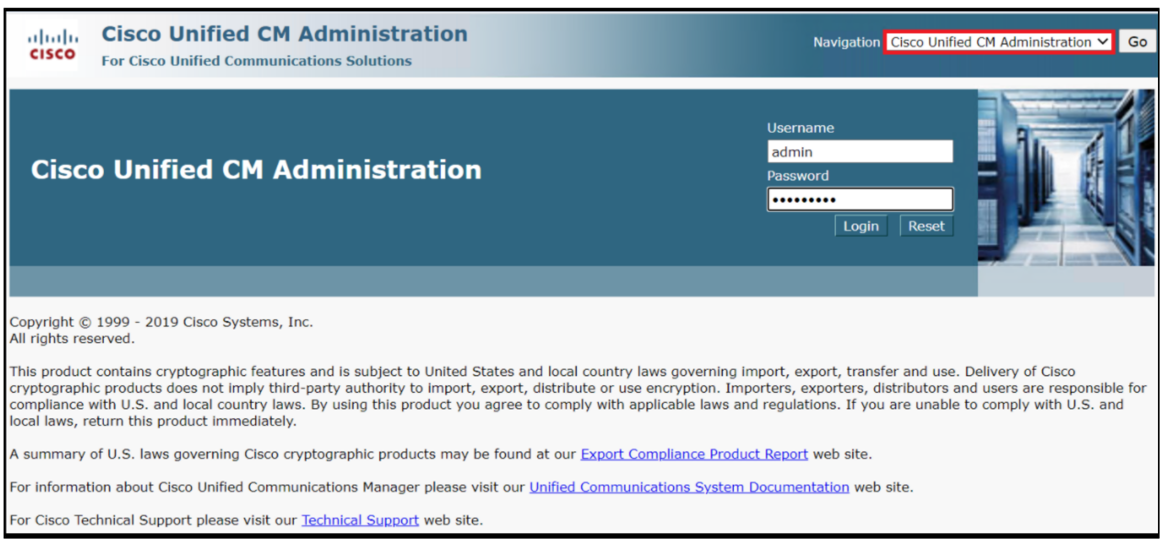




CUCM Configuration

Accessing CUCM (Cisco Unified CM Administration)

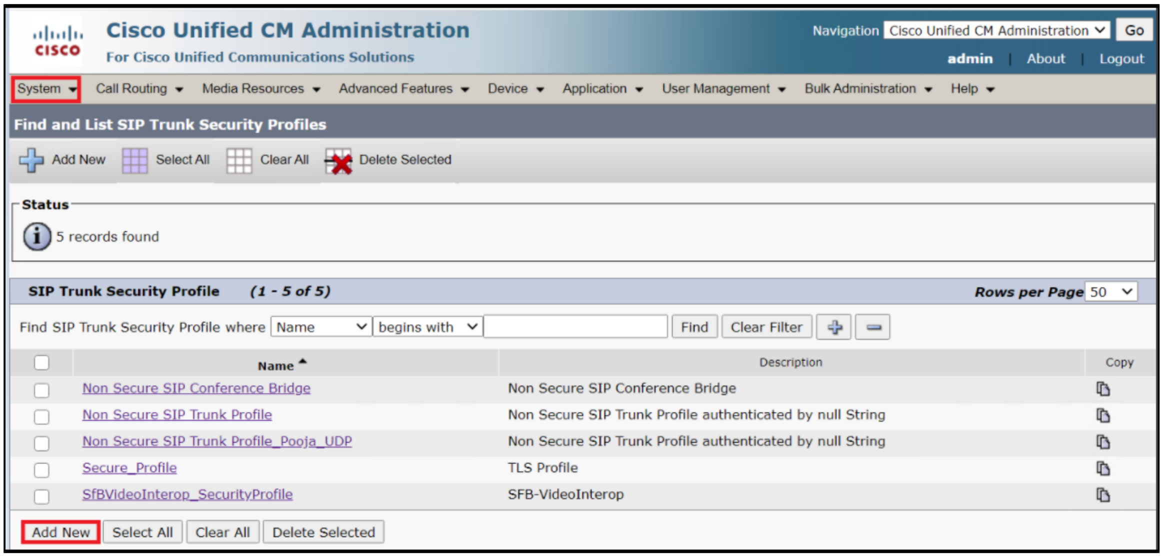
1. Open Browse and enter the CUCM IP Address.
2. Select **Cisco Unified CM Administration** from the Navigation drop-down.
3. Provide the credentials and click **Login**.



Configure SIP Trunk Security Profile

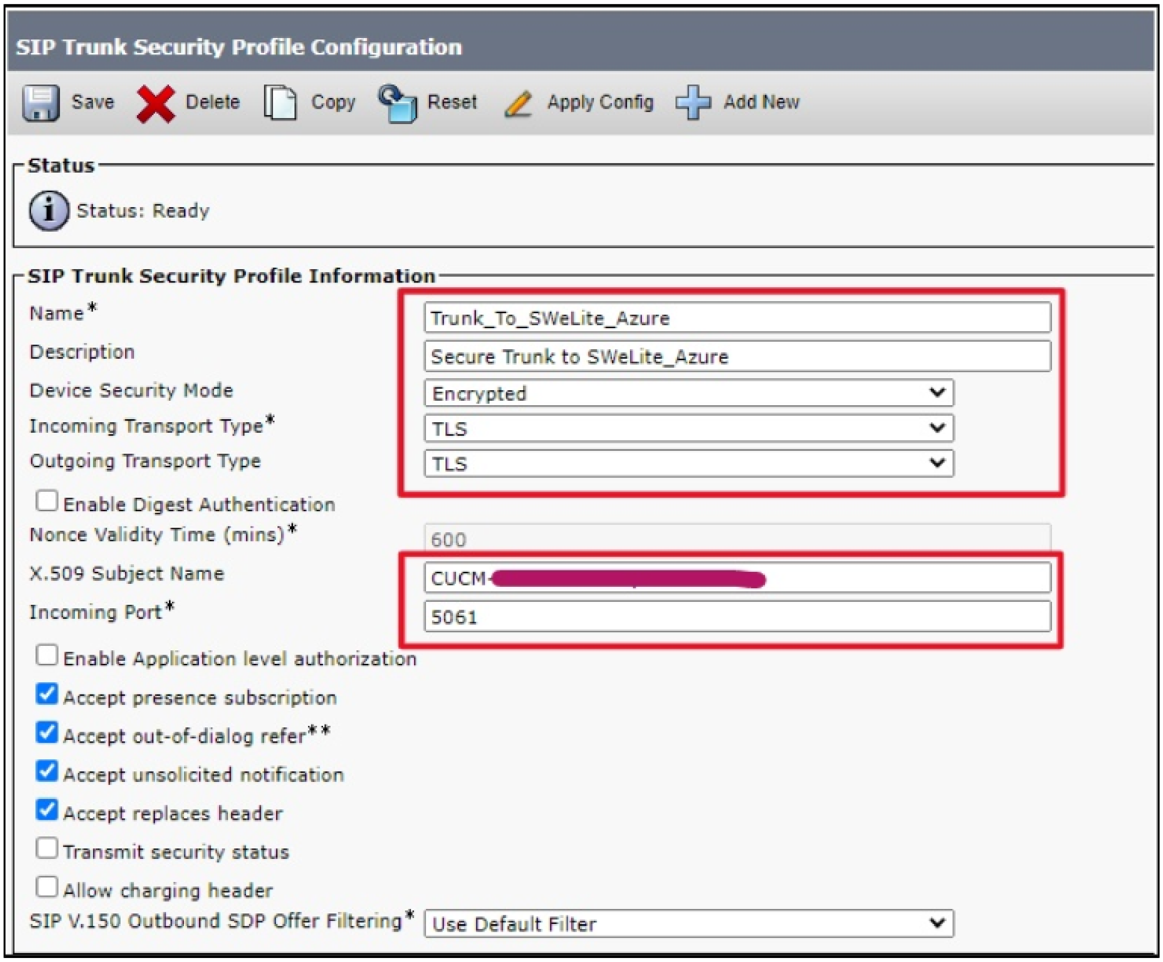
Unified Communications Manager Administration groups security-related settings for the SIP trunk to allow you to assign a single security profile to multiple SIP trunks. Security-related settings include device security mode, digest authentication, and incoming/outgoing transport type settings.

- 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.



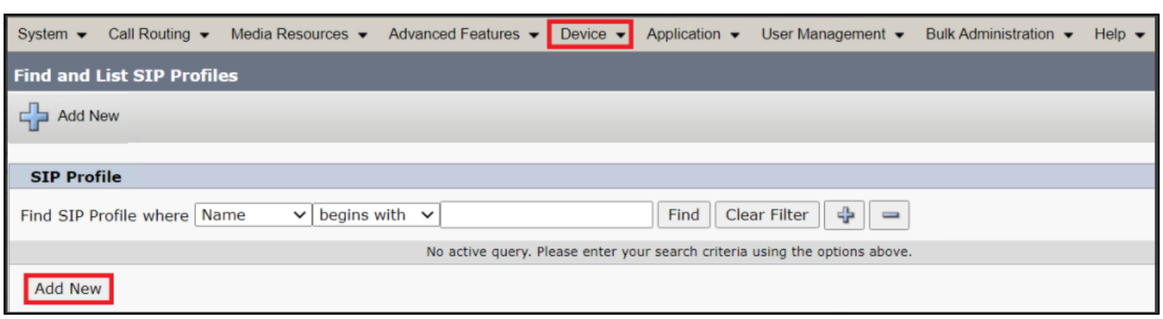
Note

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

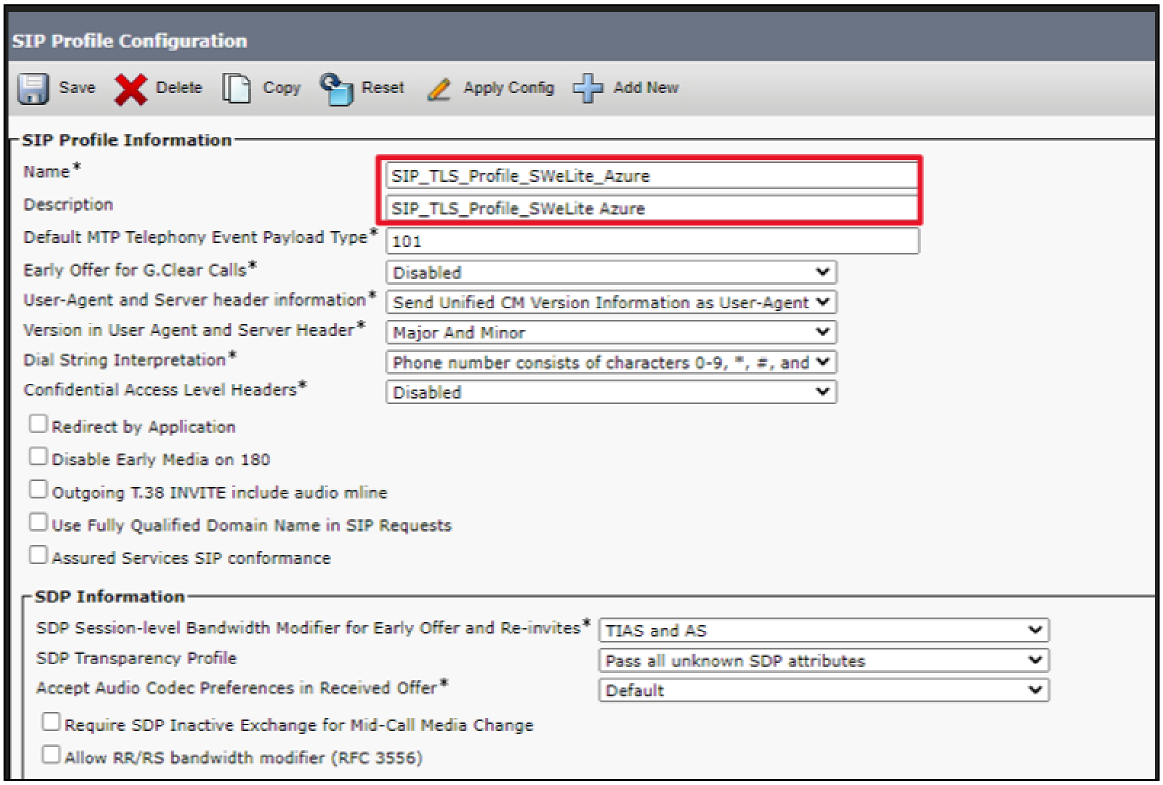
Configure SIP Profiles

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.

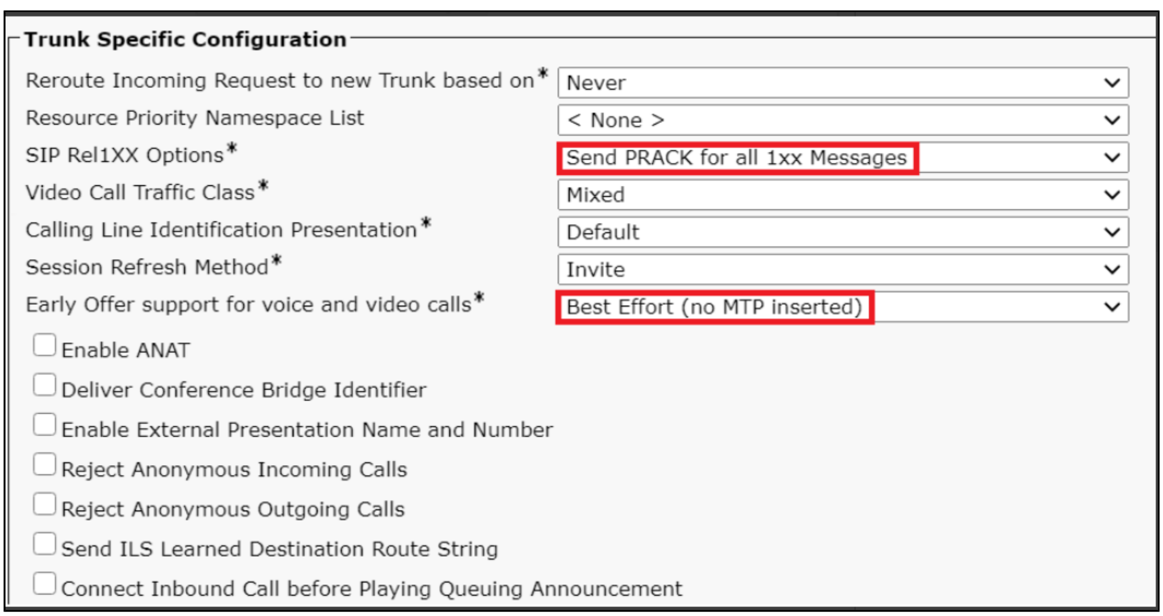
- From Cisco Unified CM Administration, navigate to **Device > Device Settings > SIP Profile.**
- Click **Add New**.



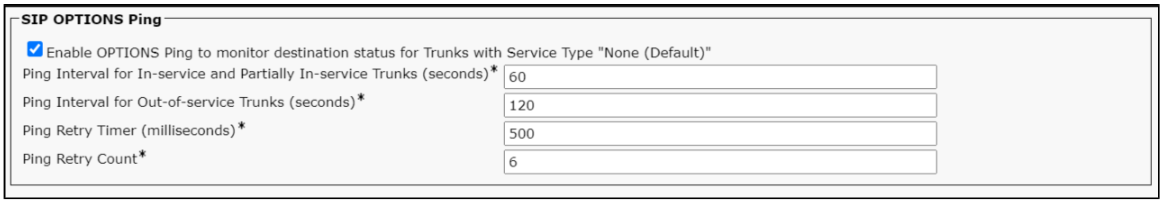
- Enter a name to identify the SIP profile.
- Provide description to identify the purpose of the SIP profile.



- 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.



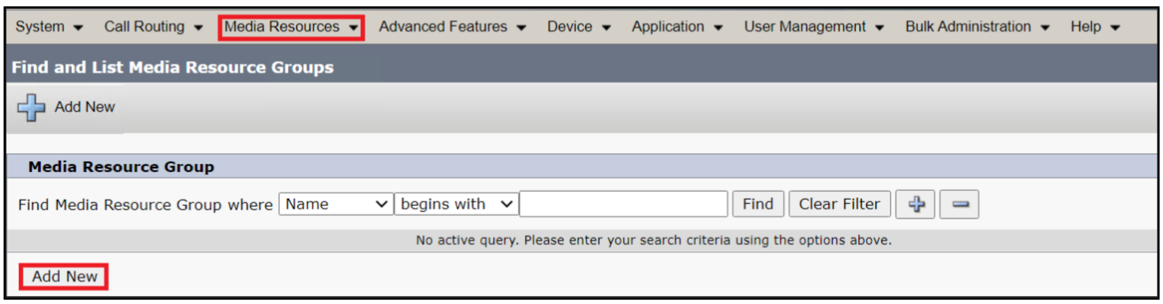
- Enable **SIP OPTIONS Ping**.
  - SIP OPTIONS are requests to the configured destination address on the SIP trunk.
- Click **Save**.



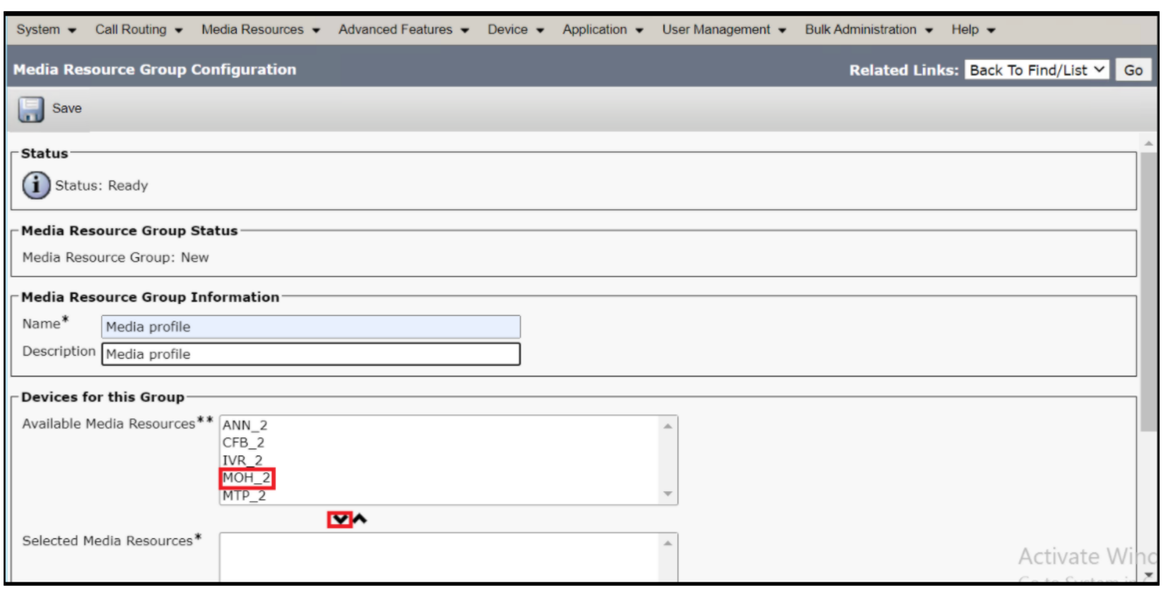
Configure Media Resource Group

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.

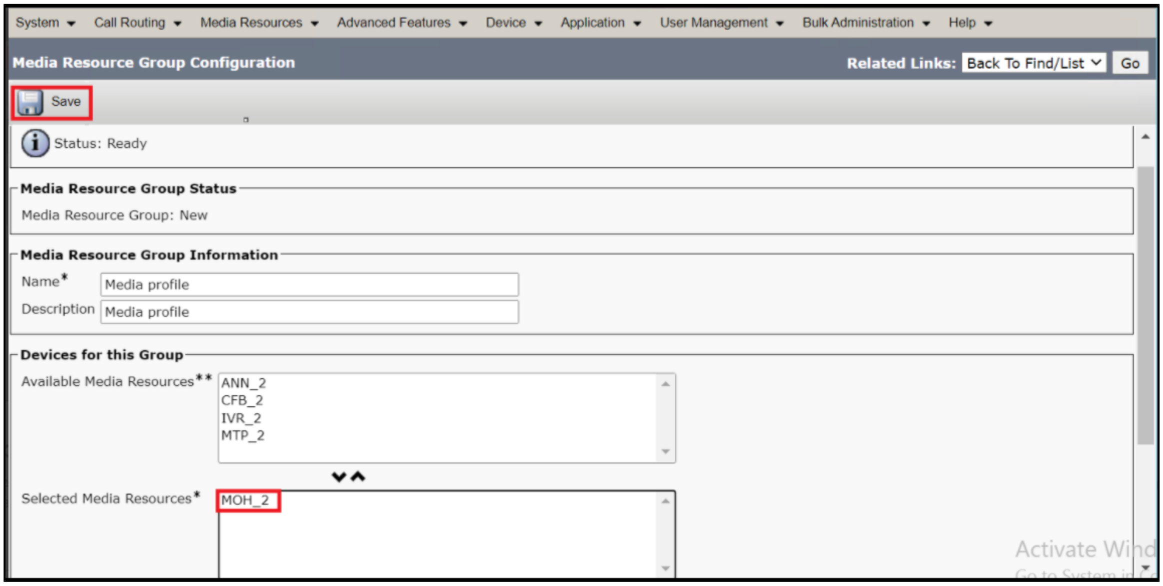
- From Cisco Unified CM Administration, navigate to **Media Resources > Media Resource Group.**
- Click **Add New**.



- 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.



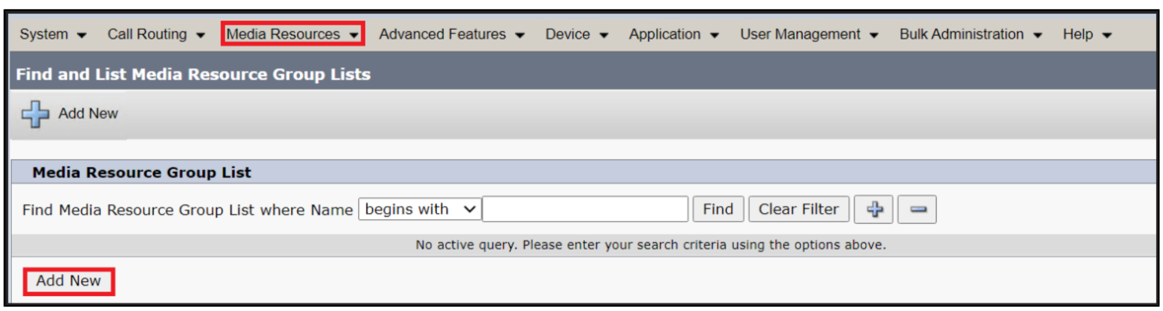
- Click **Save**.



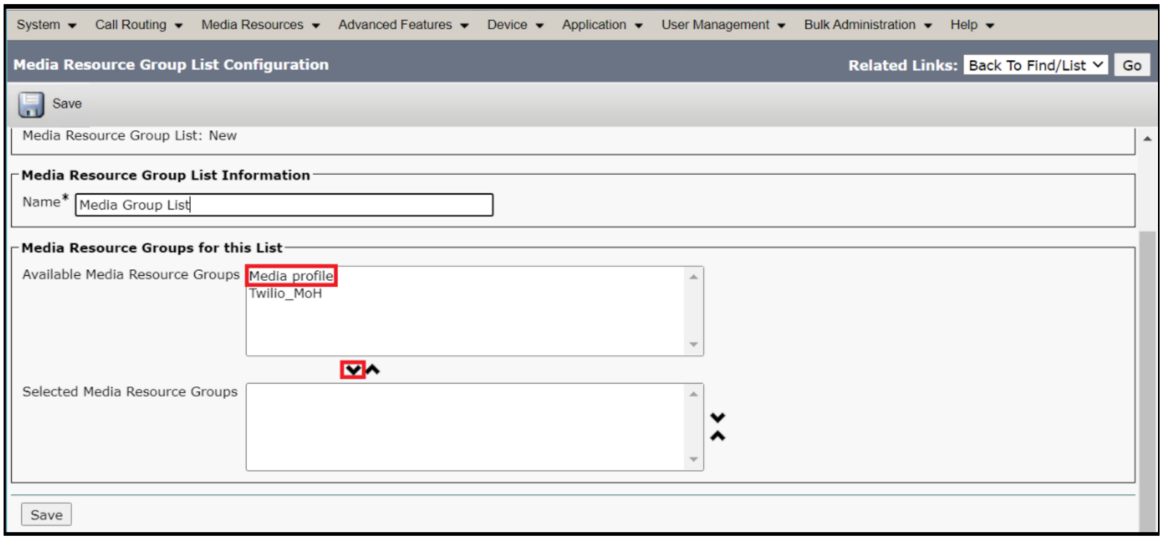
Configure Media Resource Group List

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.

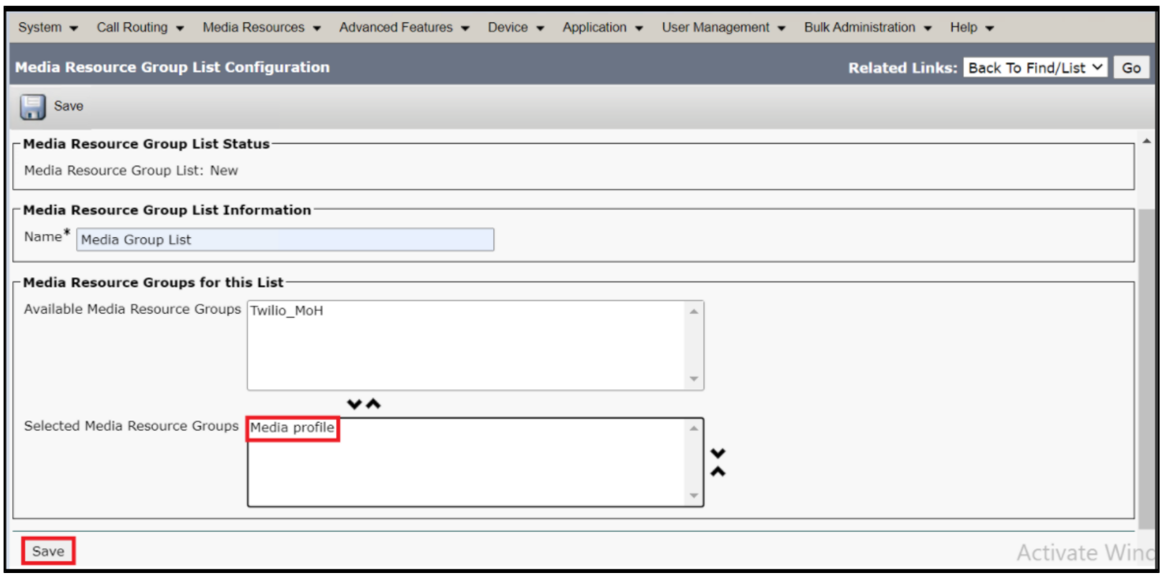
- From Cisco Unified CM Administration, navigate to **Media Resources > Media Resource Group List** menu path to configure media resource group lists.
- Click **Add New**.



- 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.



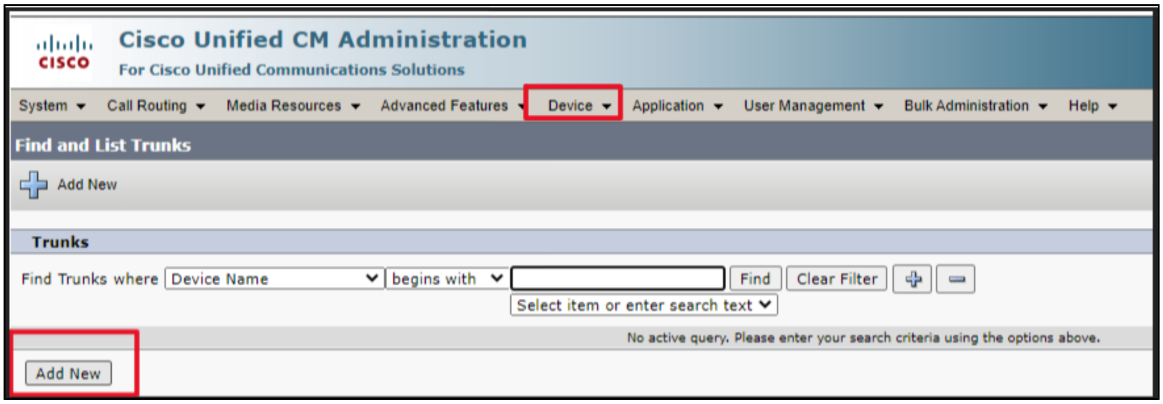
- Click **Save**.



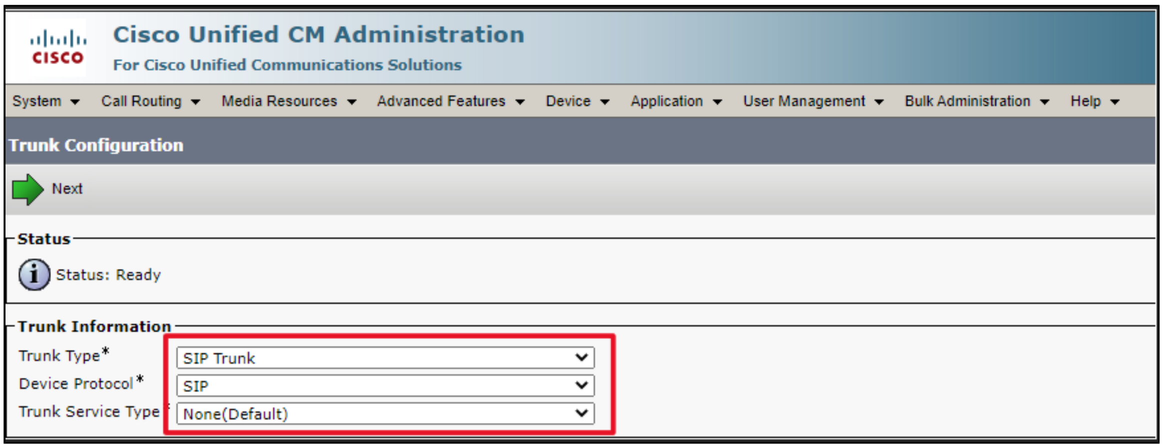
Trunk Configuration

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

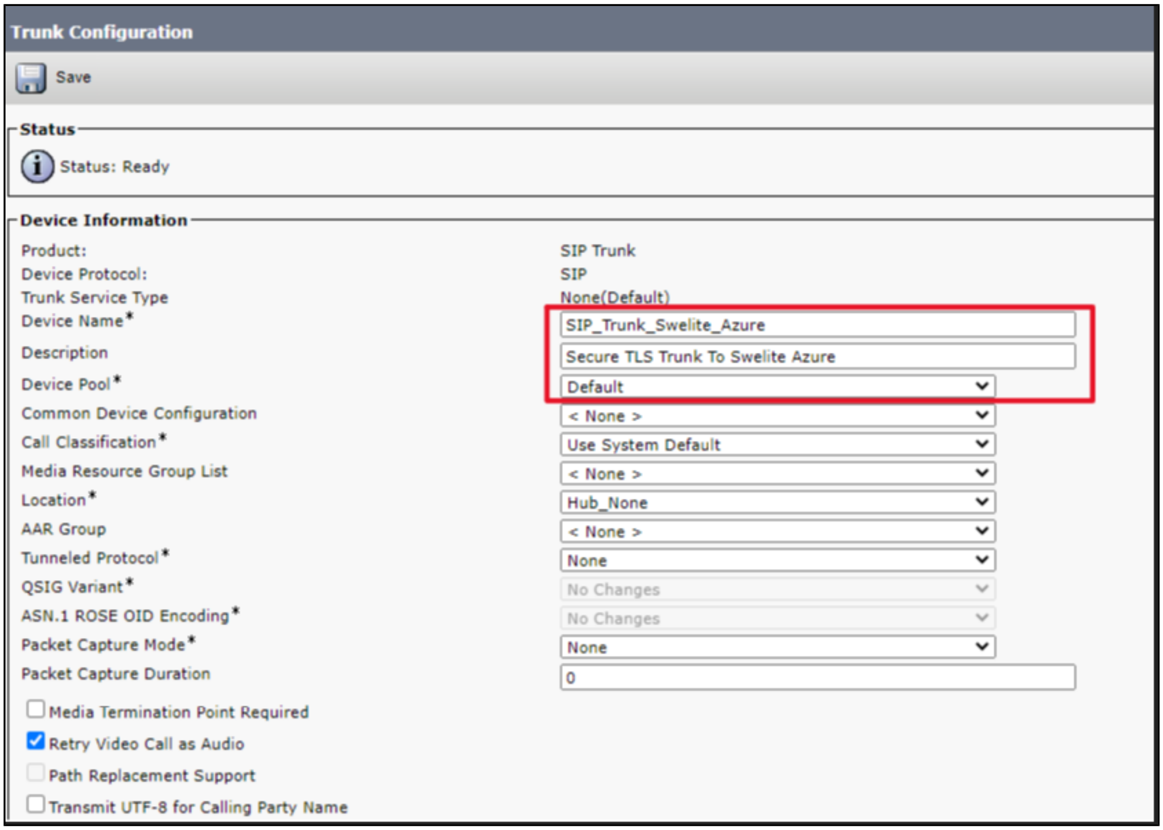
- From Cisco Unified CM Administration, choose **Device > Trunk.**
- Click **Add New**.



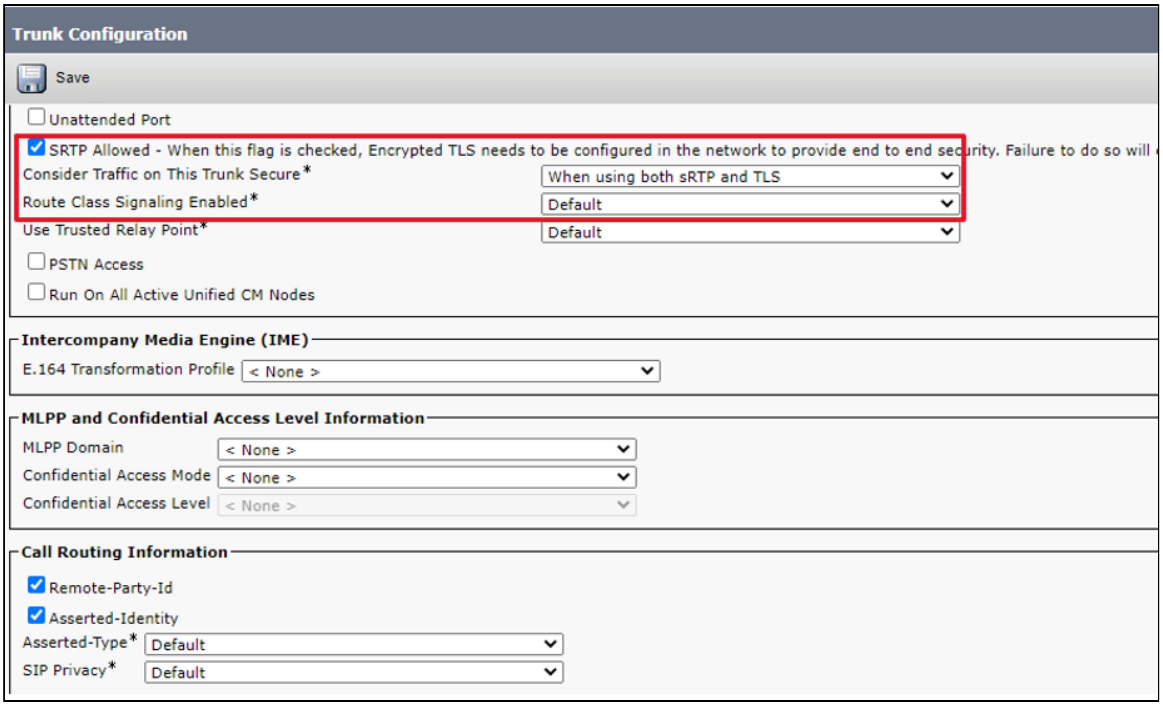
- From the Trunk Type drop-down list, choose **SIP Trunk**.
- Choose **SIP** from Device Protocol drop-down.
- From Trunk Service Type, select the default value (None).
- Click **Next**.

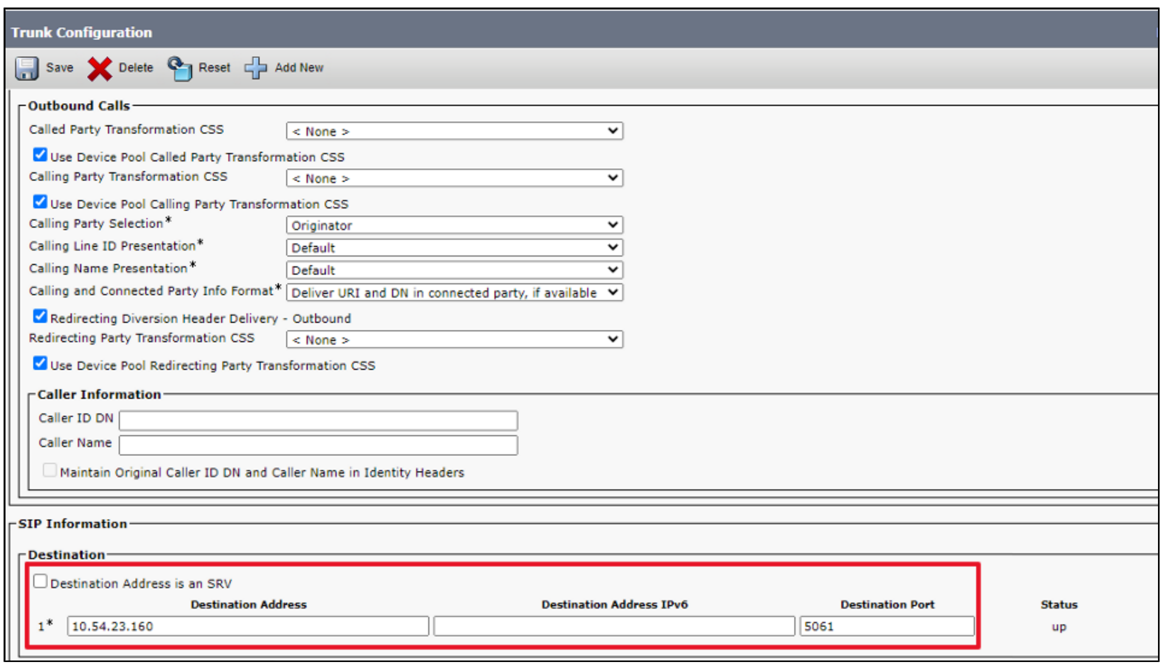


- Enter a unique identifier for the trunk.
- Enter a descriptive name for the trunk.
- Choose the Default Device Pool.
- Choose the Media Resource Group List created in the previous step.



- Provide the destination address.
  - The Destination Address represents the remote SIP peer with which 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 **SRTP 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**.





- 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 Ci sco Unified Communications Manager.

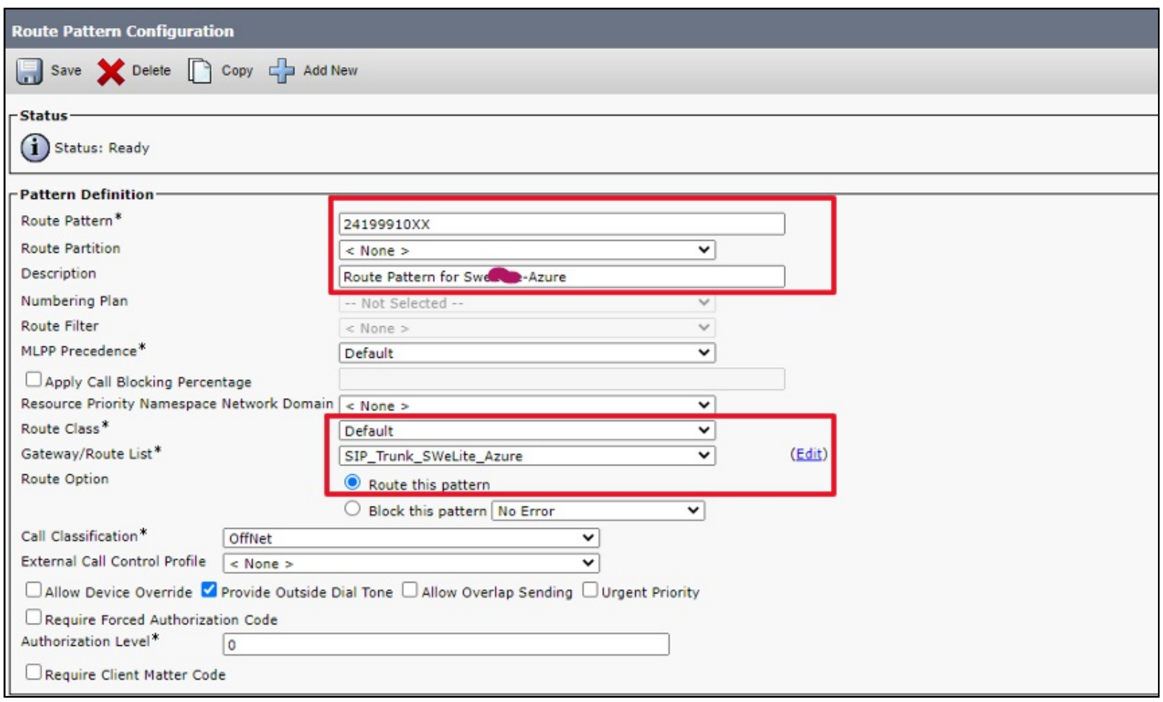
For SIP trunks, Restart and Reset behave the same way, so all active calls will disconnect when either choice is pressed.

Configure Call Routing

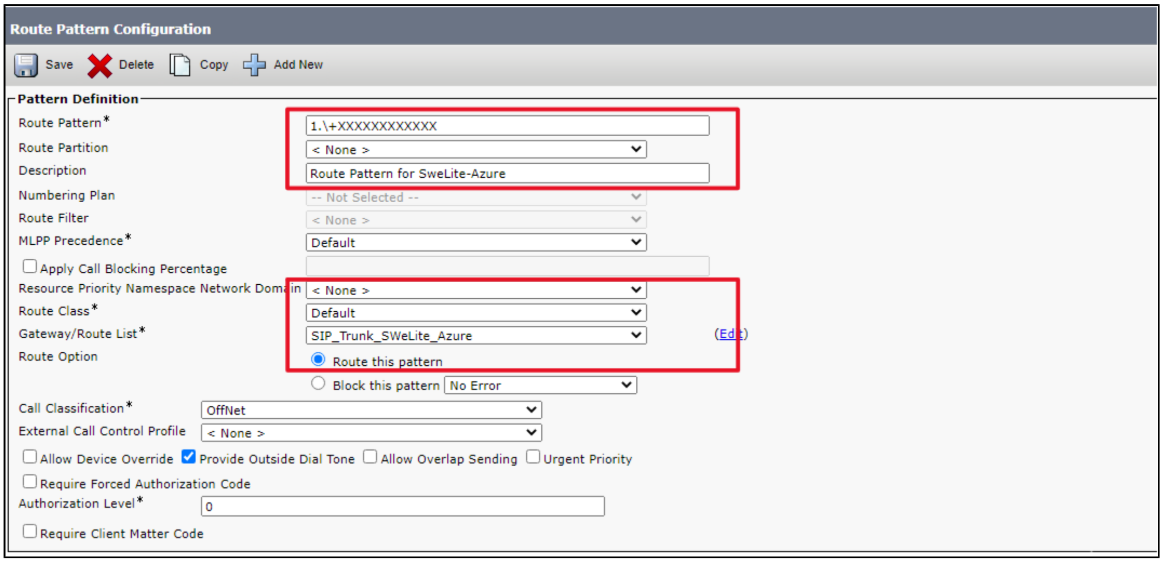
A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns provide flexibility in network design. They work in conjunction with route filters and route lists to direct calls to specific devices and 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. This will allow all the destination numbers dialed with +.
- Choose SIP Trunk created from the gateway or route list drop-down to add the route pattern.



- Or, Configure the pattern as 1.\+XXXXXXXXXXXX. This would require dialing the number as 1.+XXXXXXXXXXXX from the endpoint.
- Choose the **SIP Trunk** created earlier from the gateway or route list drop-down to add the route pattern.

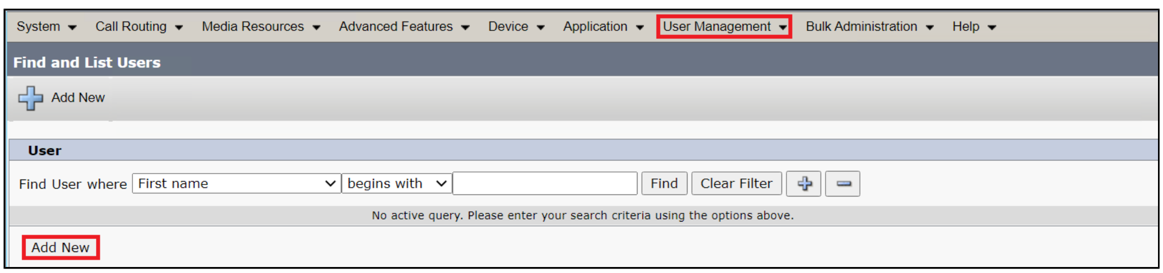


- This way of configuring Route Pattern requires additional settings to remove the digits before the Dot.
- From Discard Digits drop-down, choose **PreDot**.
  - This would remove the digits which are present before the Dot (1 in this case).

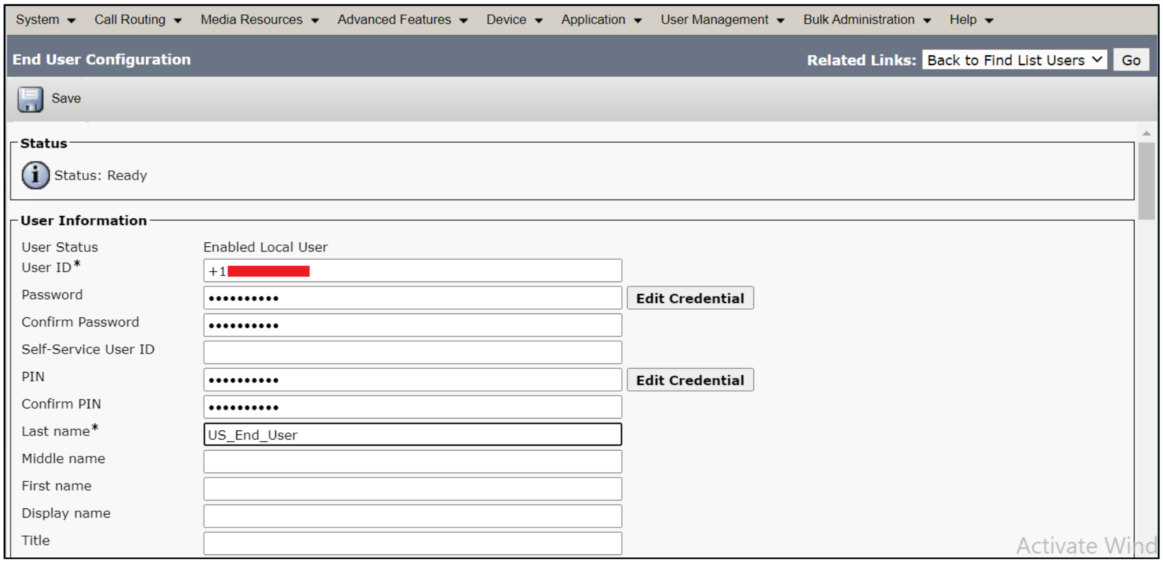
Configure End Users

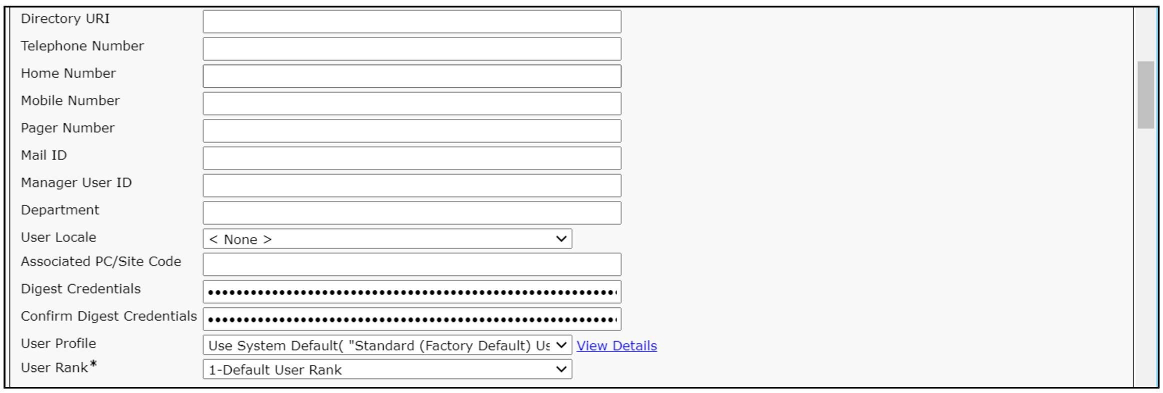
The End User Configuration window allows you to add, search, display, and maintain information about Unified Communications Manager end users. End users can control phones after you associate a phone in the End User Configuration window.

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



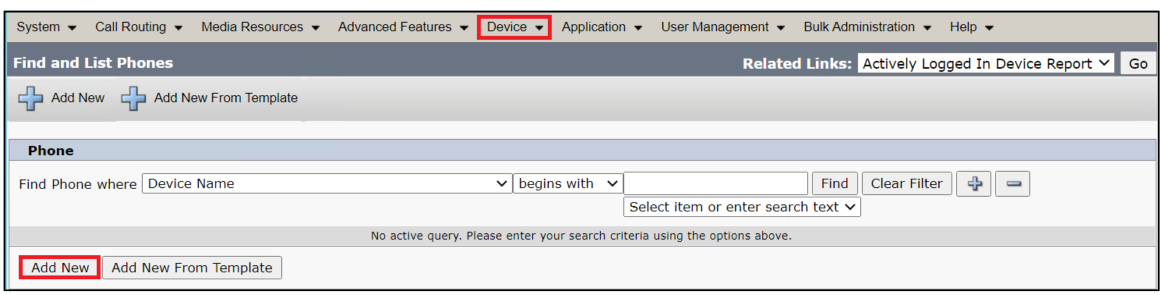
- Enter the unique end user identification name.
- Enter alphanumeric or special characters for the end user password and confirm the same.
- Enter numeric characters for the end user PIN and confirm.
- Enter the end user last name.
- For Digest Credentials, enter a string of alphanumeric characters and confirm.



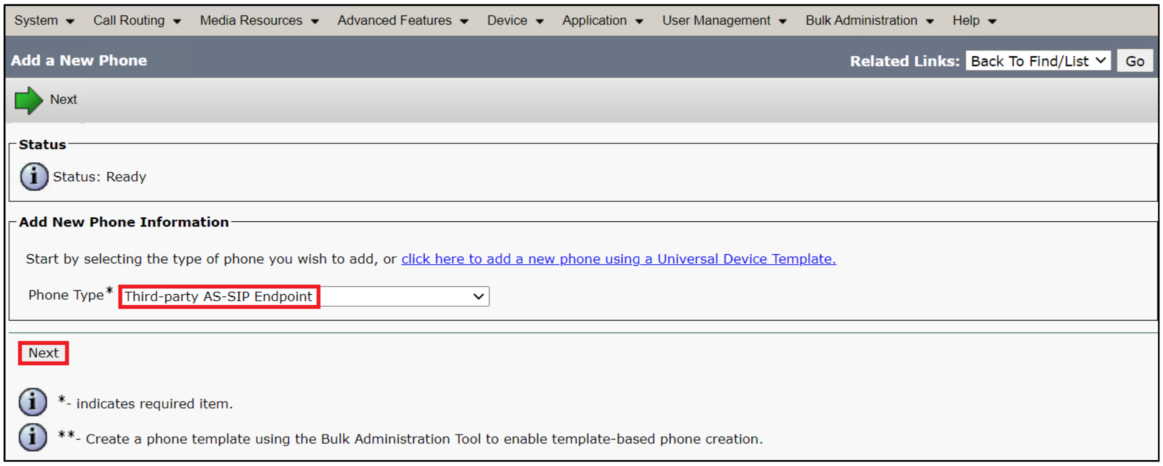


Phone Setup

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



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

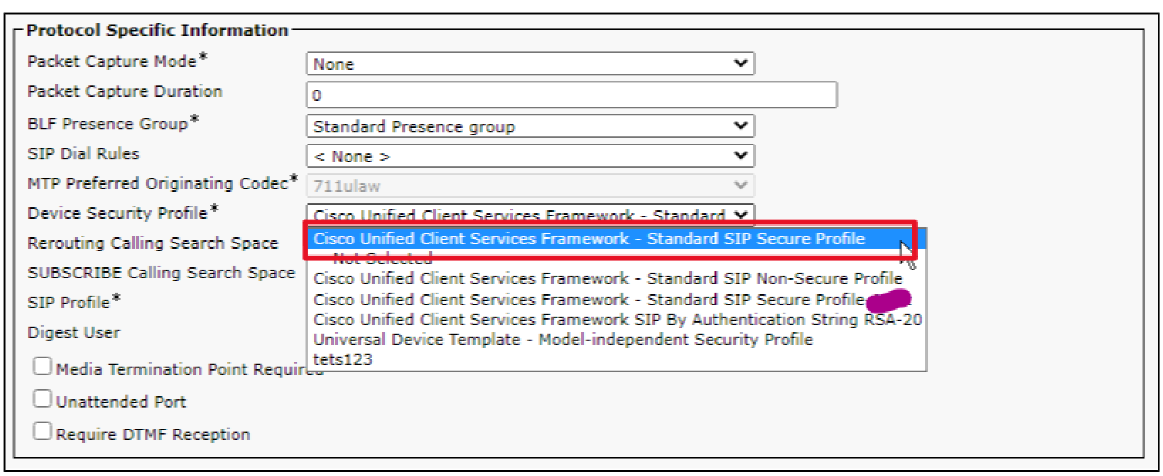


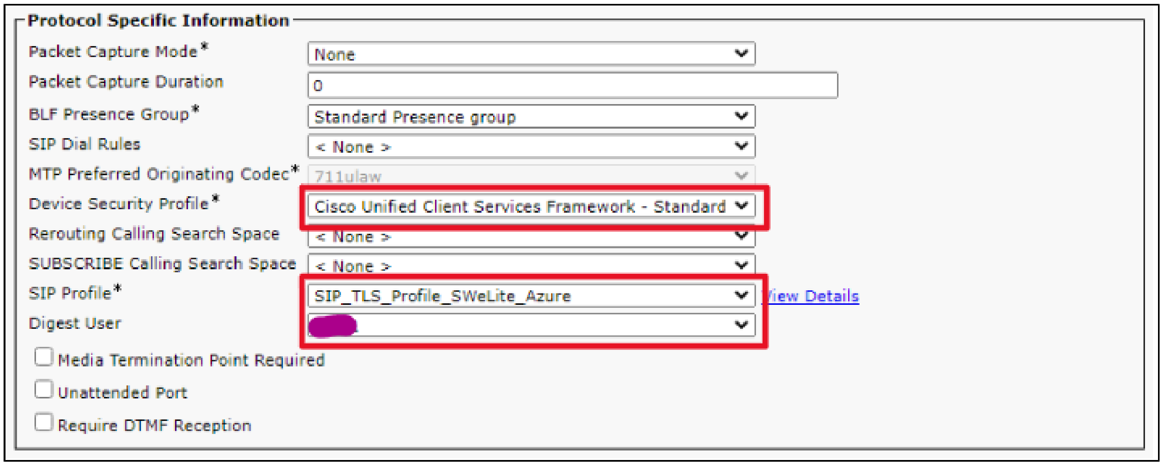
- Choose Device Trust Mode as **Not Trusted**.
- Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones. Make sure that the value comprises 12 hexadecimal characters.
- Choose **Default** Device pool.
  - A Device pool defines sets of common characteristics for devices, such as region, date/time group, and soft key template.
- Choose **Third-party AS-SIP Endpoint** 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/ccmcfg/CUCM_BK_C95ABA82_00_admin-guide-100/CUCM_BK_C95ABA82_00_admin-guide-100_chapter_011010.html

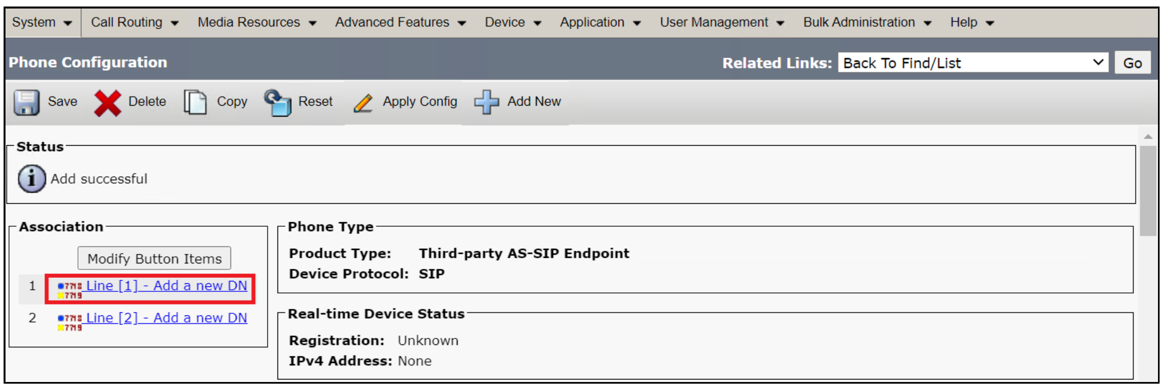
---

- Choose the security profile Third-party AS-SIP Endpoint - Standard SIP Secure 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).
- Click **Save**.



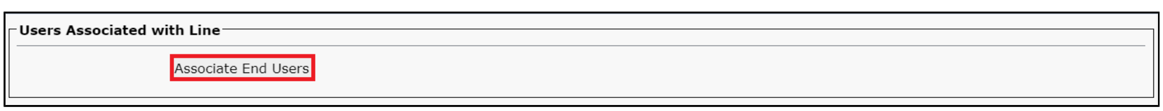


- Click this link to add a remote destination to associate with this device. The Remote Destination Configuration window displays, which allows you to add a new remote destination to associate with this device.

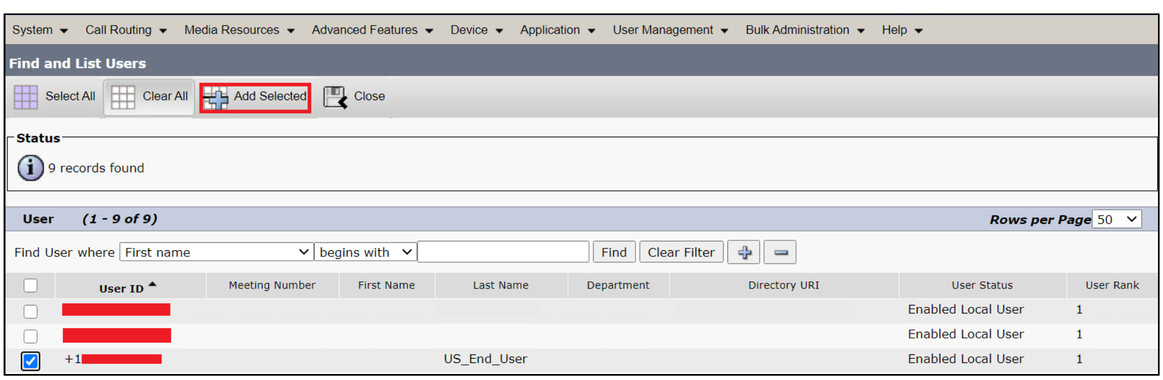


- Add the Directory number.
- Click **Save**.

- Click the **Associate End User** button.

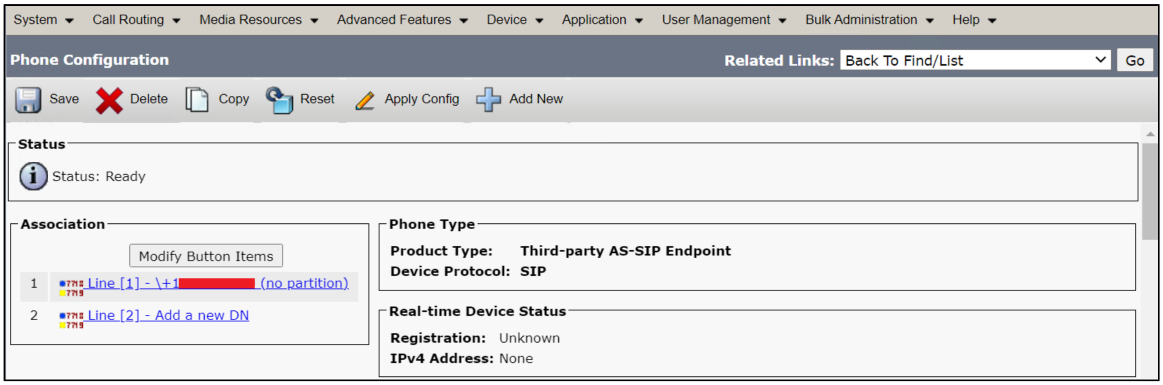


- Select the end user created from the list and click **Add Selected**.



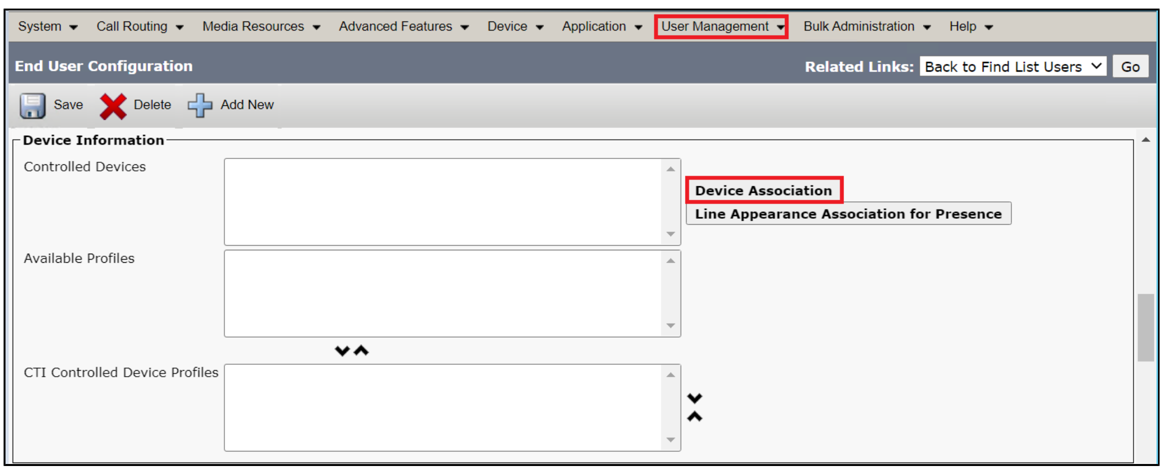
- After the above step, the user association is completed.
- Save the configuration.

- Click **Apply Config** followed by the Reset button.
- Reset, Restart and Close the window.

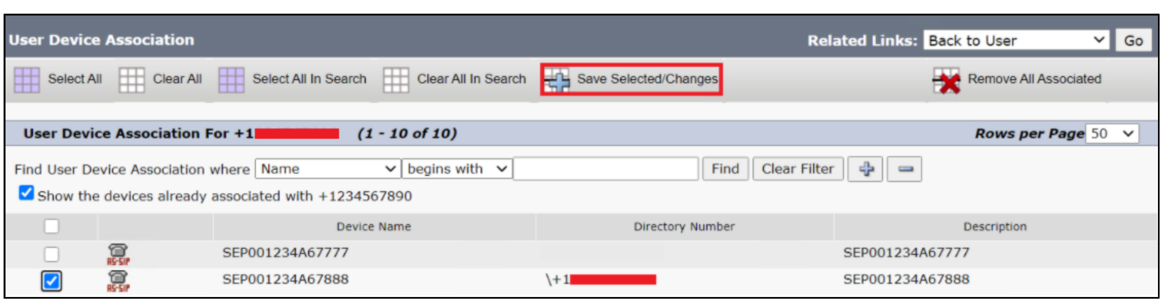


Device Association

- 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.

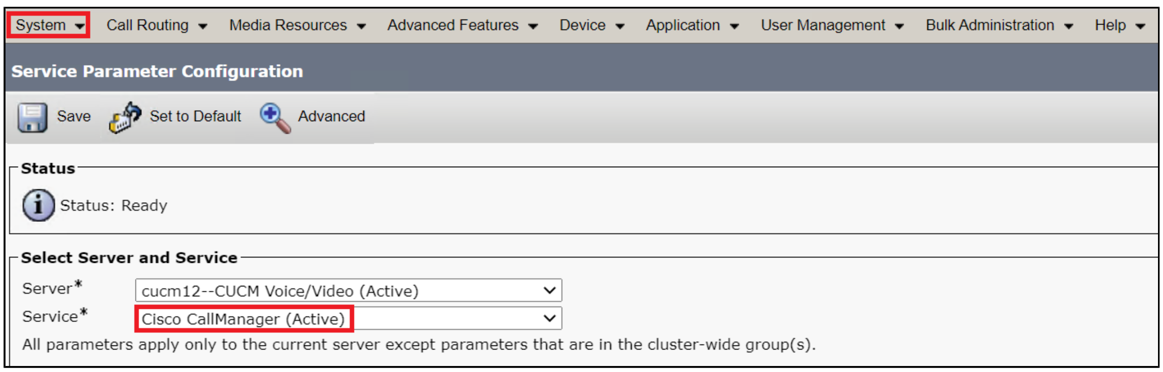


- After selecting the appropriate device, it will appear in the Controlled Devices pane.

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.



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

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 UDP and TLS	✓
03.	Ringing 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 which 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

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 Communication 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 Lite on Azure, please visit: Deploying an SBC SWe Lite from the Azure Marketplace.

Conclusion

This Interoperability Guide describes successful configuration of interop involving Ribbon SBC SWe Lite on Azure, Cisco Unified Communication Manager and SIP Trunk Service Provider.

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.