SBC Edge 1K_2K_SWe Edge R11.0 Interop with Cisco WebEx Calling : Interoperability Guide

Table of Contents

- Interoperable Vendors
- Copyright
- Document Overview
    - About Ribbon SBC Edge
    - About Cisco Webex
- Scope/Non-Goals
- Audience
- Prerequisites
- Product and Device Details
- Network Topology and E2E Flow Diagrams
    - Deployment Topology
    - Interoperability Test Lab Topology
    - Call Flow Diagram
- Document Workflow
- Installing Ribbon SBC Edge
- Ribbon SBC Edge Configuration
    - Accessing SBC Edge
    - License and TLS Certificates
        - Installing License on SWe Edge
        - Installing license on SBC 1K/2K
        - SBC Certificate
        - Trusted CA Certificates
    - Networking Interfaces
    - Configure Static Routes
    - SBC Edge Configuration for PSTN side and Enterprise Solutions
        - Media List - PSTN
        - SIP Profile - PSTN
        - SIP Server Table - PSTN
        - Call Routing Table - PSTN
        - SIP Signaling Group - PSTN
        - SIP Server Table - PBX
        - Call Routing Table - PBX
        - SIP Signaling Group - PBX
    - SBC Edge Configuration for Cisco Webex Calling side
        - Node-Level Settings
        - TLS Profile
        - DNS Host
        - SDES-SRTP Profile - Webex
        - Media Profiles - Webex
        - Media List - Webex
        - Message Manipulation
        - SIP Profile - Webex
        - SIP Server - Webex
        - Call Routing Table - Webex
        - SIP Signaling Group - Webex
        - Call Routing Table Entry
    - Multi-Tenant with Single IP / Multiple Port on SBC
        - TLS Certificates
        - TLS Profile
        - SIP Server Table Tenant2
        - Message Manipulation
        - Call Routing Table Tenant2 to PSTN
        - SIP Signaling Group - Webex Tenant2
        - Call Routing
    - Multi-Tenant with Single IP and Port on SBC
        - TLS Certificates
        - TLS Profile
        - SIP Profile
        - Message Manipulation
        - Message Rule Table Entry for Tenant1
        - Signaling Group
    - Multi-Tenant with Multiple IP and Port on SBC
- Cisco Webex Calling Configuration
- Supplementary Services and Features Coverage
- Caveats
- Support
- References
- Conclusion

Interoperable Vendors

Copyright

Document Overview

This document outlines the configuration best practices for the Ribbon SBC Edge when deployed with Cisco Webex Calling.

About Ribbon SBC Edge

The SBC Edge (SBC 1K, 2K, SWe Edge) provides best-in-class communications security with the convenience of deployment from popular virtual machine platforms as well as hosting in cloud environment. The SBC Edge dramatically simplifies the deployment of robust communications security services for SIP Trunking, Direct Routing, and Cloud UC services. SBC 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 Webex

Webex Calling Cloud service (Webex Calling) supports "Bring Your Own PSTN" and Enterprise dialing using what is termed as a Local Gateway that is located at the edge of the customer's VoIP network. A local gateway is a SIP Session Border Controller that interworks with Webex Calling cloud service in specific ways. This Local gateway must operate using specified conditions with Webex Calling and this document suggests to OEM vendors the requirements to interoperate with Webex Calling Cloud services.

Scope/Non-Goals

This document provides configuration best practices for deploying Ribbon's SBC Edge for Cisco Webex Calling interop. 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.

It is not the goal of this guide to provide detailed configurations that meet the requirements of every customer. Use this guide as a starting point, 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 the Ribbon SBC.

To perform this interop, you need to:

- use the graphical user interface (GUI) or command line interface (CLI) of the Ribbon product.
- understand the basic concepts of TCP/UDP/TLS and IP/Routing.
- have SIP/RTP/SRTP to complete the configuration and for troubleshooting.

> **Note**
> This configuration guide is offered as a convenience to Ribbon customers. The specifications and information regarding the product in this guide are subject to change without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided "AS IS". Users must take full responsibility for the application of the specifications and information in this guide.

Prerequisites

The following aspects are required before proceeding with the interop:

- Ribbon SBC Edge
- Ribbon SBC Edge license
    - This interop requires the acquisition and application of SIP sessions, as documented at Working with License.
- Public IP addresses
- TLS certificates for SBC Edge
    - For more details, please visit Working with Certificates.
- Cisco Control Hub and Domain
    - Cisco Control Hub Premier license for the users.
    - For more details, contact Cisco Webex Support.

Product and Device Details

The configuration uses the following equipment and software:

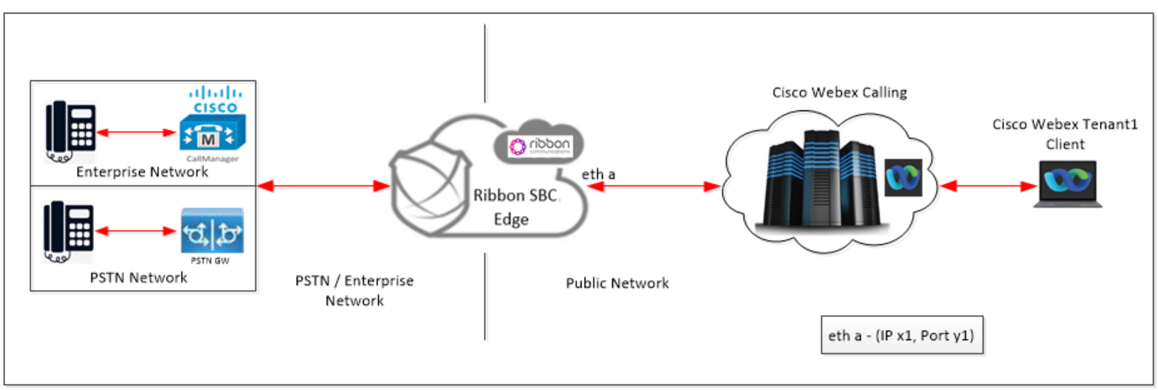
Product	Appliance/ Application/ Tool	Software Version
Ribbon SBC	SBC SWe Edge	11.0.2 build 99
	SBC 1K/2K	11.0.1 build 634
Cisco Webex	Cisco Control Hub	Build: 20230607-38bdcbf (mfe)
	Cisco Webex Client	43.5.0.26155
Third-party Equipment	Cisco Unified Communications Manager	12.5.1.11900-146
	Poly VVX 601	5.8.2.4732
Administration and Debugging Tools	Wireshark	3.4.9

Network Topology and E2E Flow Diagrams

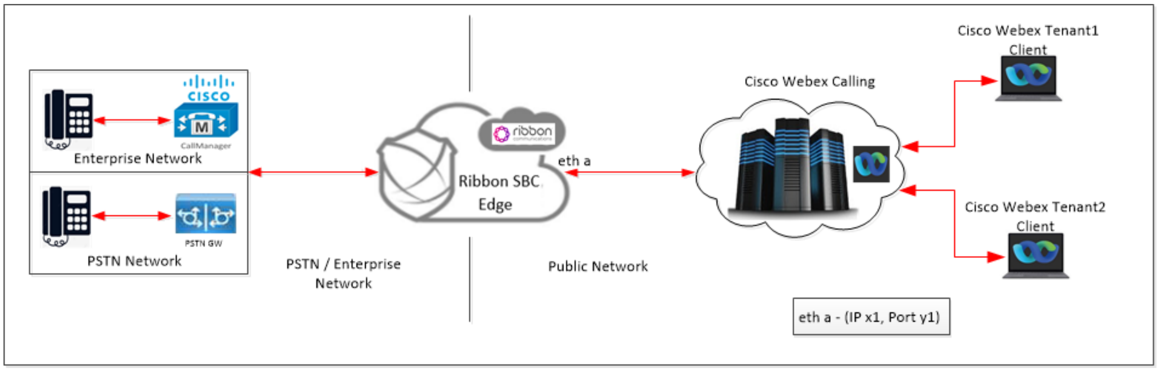
Deployment Topology

> **Note**
> There can be more number of deployment topologies beyond those depicted below.

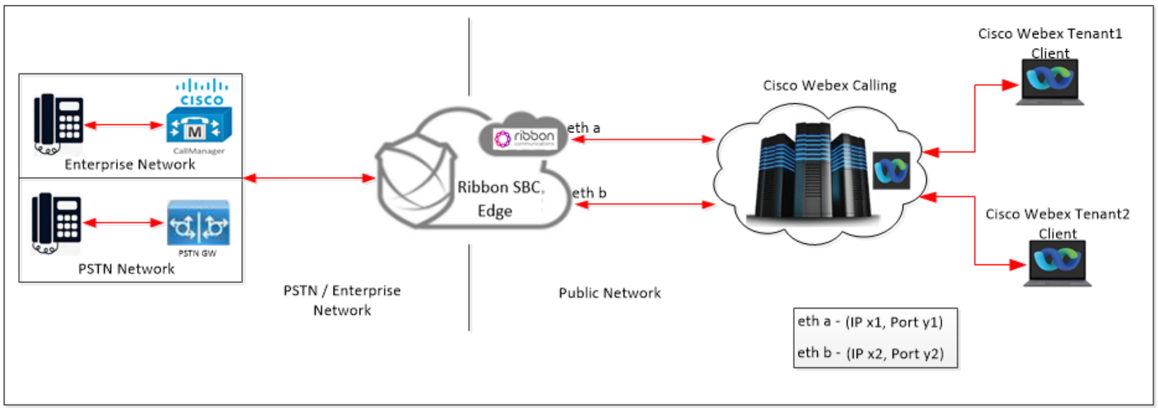
Single Webex Tenant and Single IP & Single Port on SBC



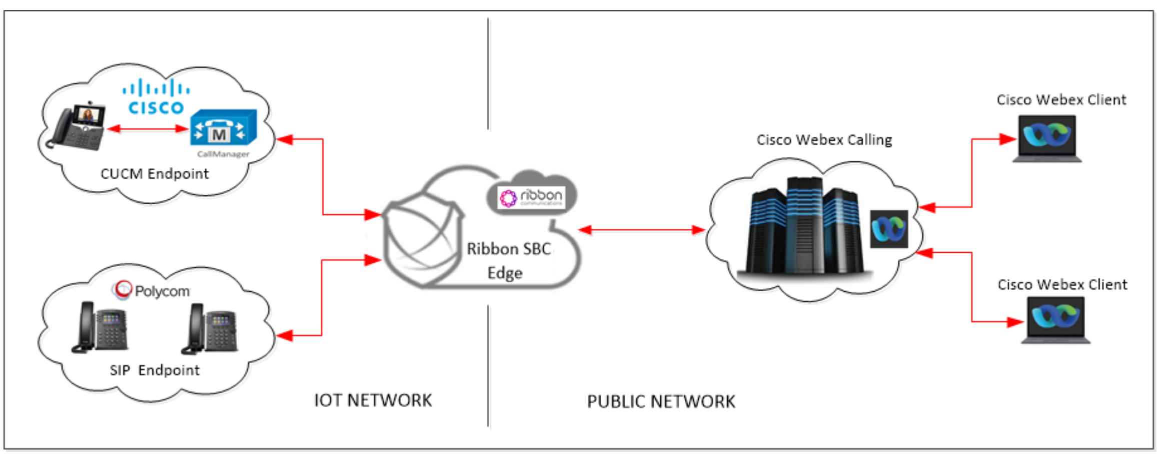
Multiple Webex Tenant and Single IP & Single Port on SBC



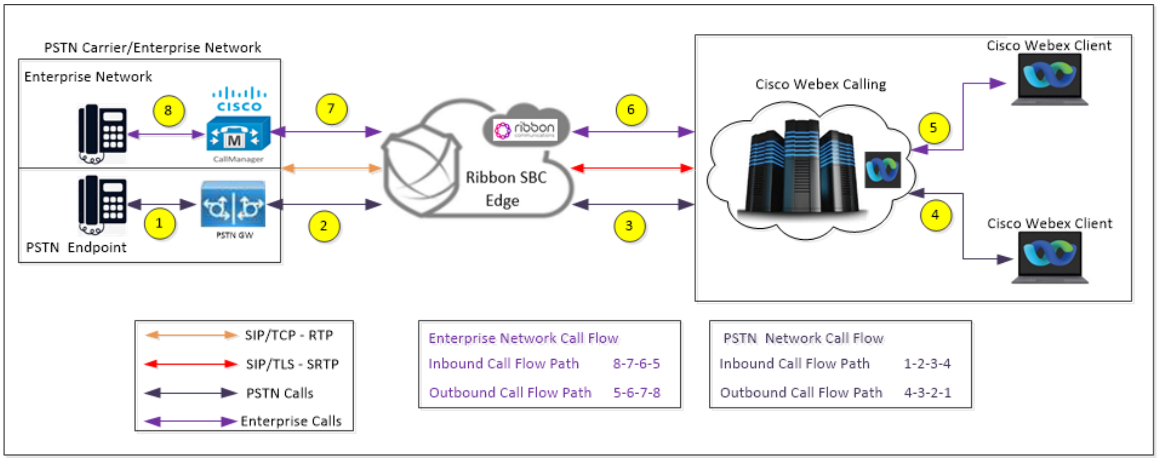
Multiple Webex Tenant and Multiple IPs / Ports on SBC



Interoperability Test Lab Topology

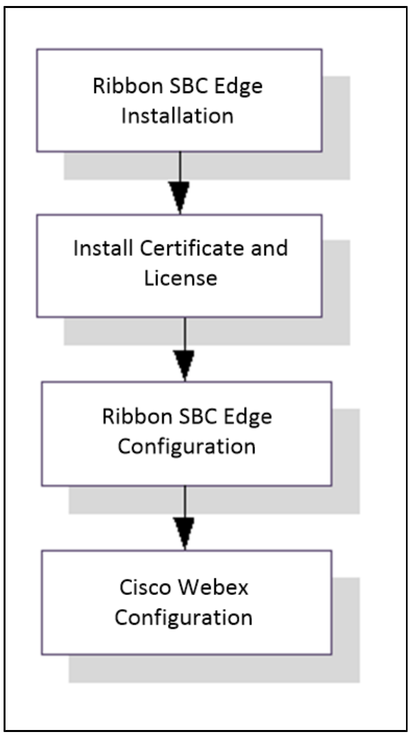


Call Flow Diagram



Document Workflow

The sections in this document follow the sequence below. Complete each section for the configuration to be successful.



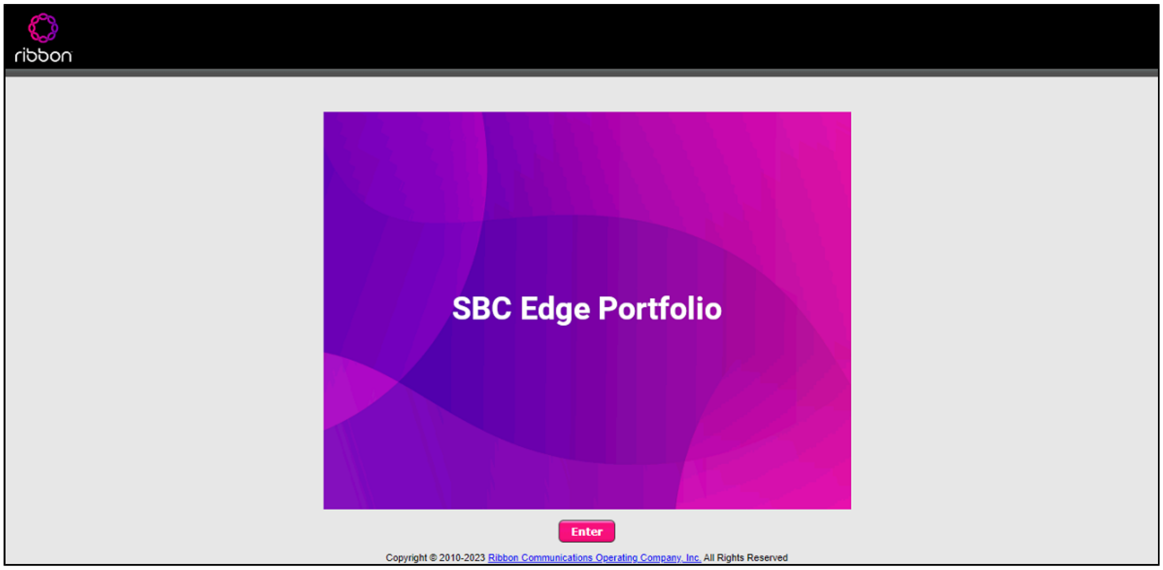
Installing Ribbon SBC Edge

To deploy Ribbon SBC Edge instance, refer to Installing SBC Edge.

Ribbon SBC Edge Configuration

Accessing SBC Edge

Open any browser and enter the SBC Edge IP address.



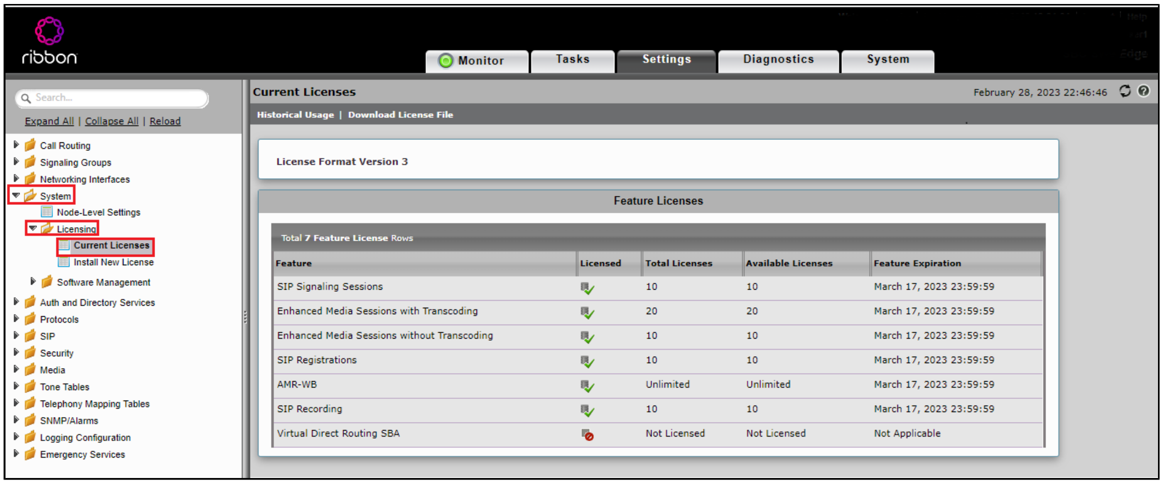
Click Enter and log in with a valid User ID and Password.

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** pan el 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.**

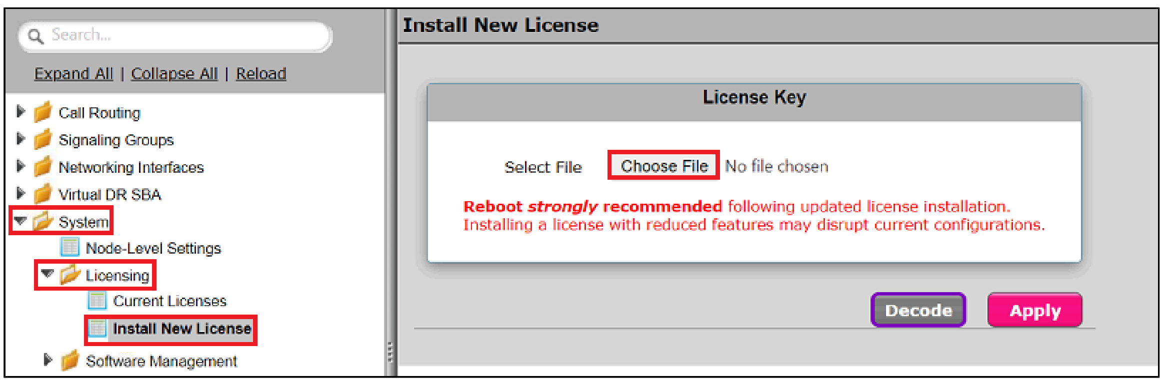


For more details on Licenses, refer to Working with Licenses.

Installing License on SWe Edge

After receiving the license file, follow the below steps to apply license on SWe Edge.

1. From the **Settings** tab, navigate to **System > Licensing > Install New License.**
2. Upload the License file by selecting Choose File and click Apply.

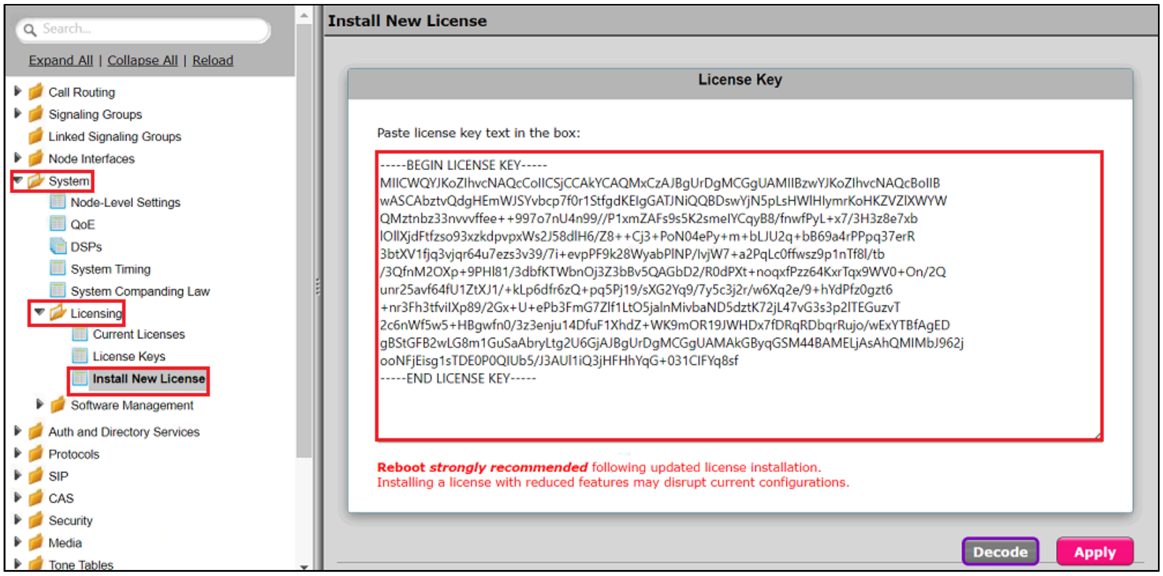


Installing license on SBC 1K/2K

Please ignore this step for SBC SWe Edge.

After receiving the license file, follow the below steps to apply license on SBC 1K/2K.

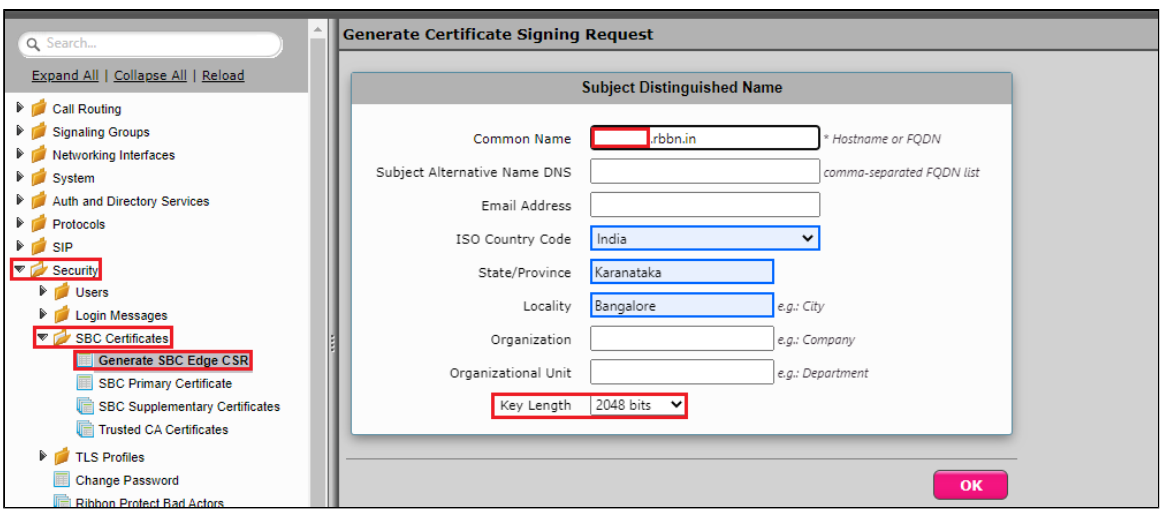
1. From the **Settings** tab, navigate to **System > Licensing > Install New License.**
2. Open the license file to get the license key and paste in the tab as shown in the snapshot.
3. Click Apply.



SBC Certificate

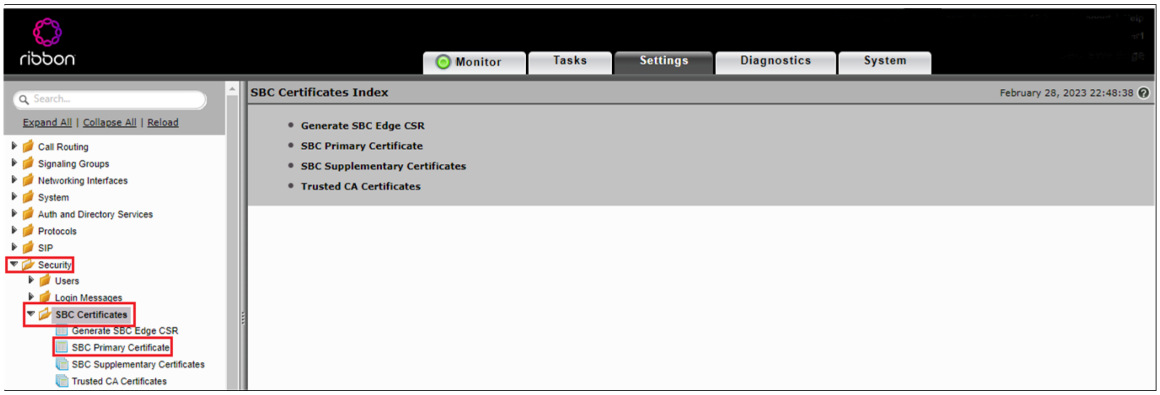
From the **Settings** tab, navigate to **Security > SBC Certificates > Generate SBC Edge Certificates.**

1. Provide the Common Name of the SBC that includes Host and Domain.
2. Set the Key Length to 2048 bits.
3. Provide the location information.
4. Click OK.
5. The CSR will be generated and displayed in the result text box.



After generating the CSR on Ribbon SBC, provide it to the Certificate Authority. CA would generally provide the following certificates:

- SBC Certificate
- CA's Root Certificate
- Intermediate Certificate



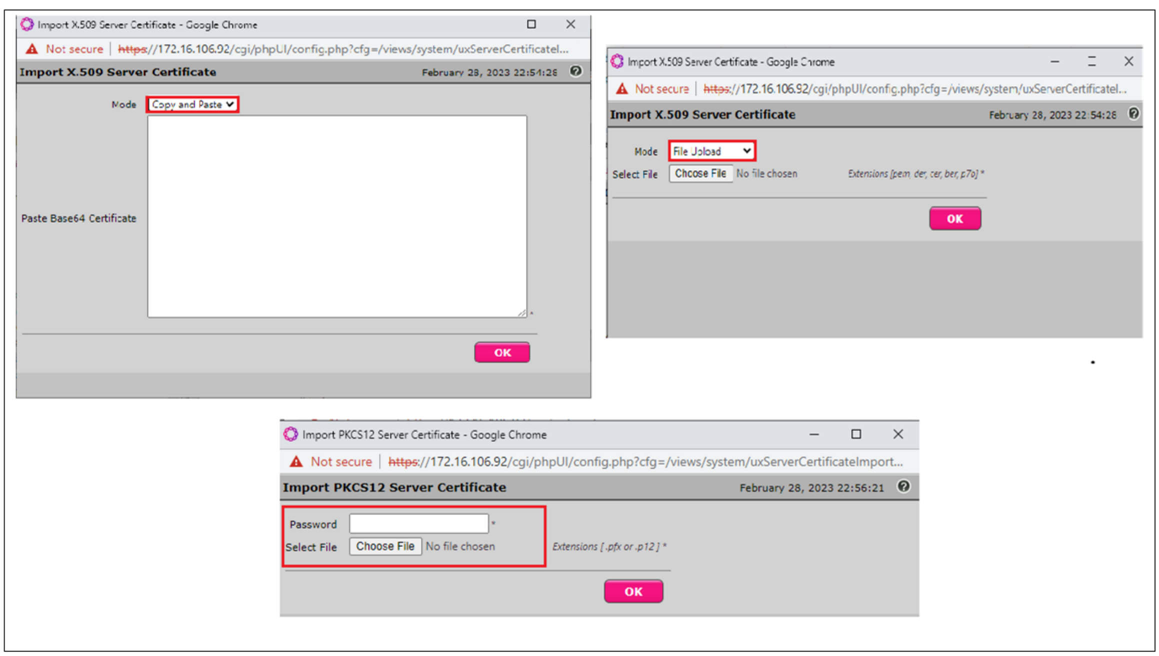
There are two ways to import SBC Primary Certificate as described below:

To import an X.509 signed certificate:

1. Select X.509 Signed Certificate from the Import menu at the top of the page.
2. Choose the import mode (Copy and Paste or File Upload) from the Mode pull-down menu.
3. If you choose File Upload, use the Browse button to find the file and click OK.
4. If you choose Copy and Paste, open the file in a text editor, paste the contents into the Paste Base64 Certificate text field and click OK.

To import a PKCS12 Certificate and Key:

1. Select PKCS12 Certificate and Key from the Import menu at the top of the page.
2. Enter the password used to export the certificate in the Password field.
3. Browse for the PKCS certificate and key file and click OK.



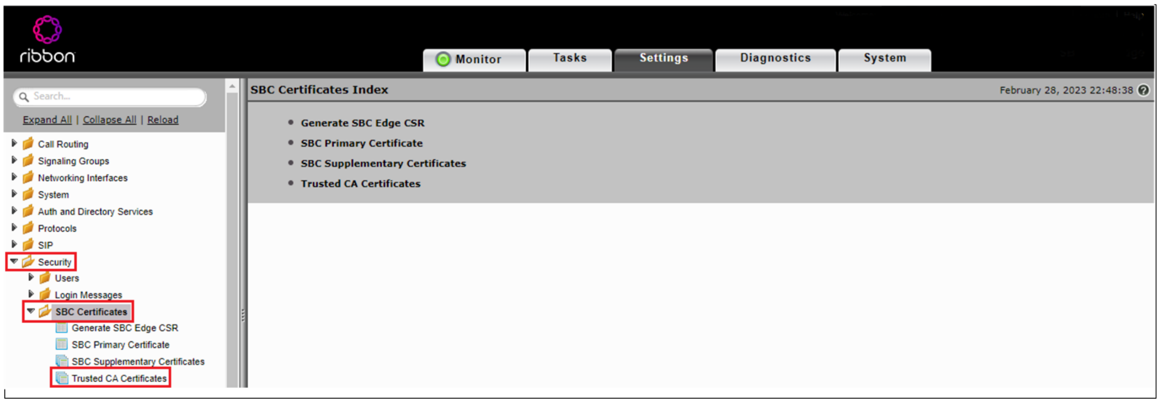
Trusted CA Certificates

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

- For TLS to work, a Trusted CA (Certificate Authority) is required. For this interop, GoDaddy is used as Trusted CA.
- Add an entry in the Public DNS to resolve Ribbon SBC Edge FQDN to Public IP Address.
- Obtain Trusted Root certificate from your certification authority.
- In the trust store of the SBC, ensure you have the following certificates as part of the root certificate trust:
    - Cisco Control HUB Root R1
    - GlobalSign Root CA (if required)

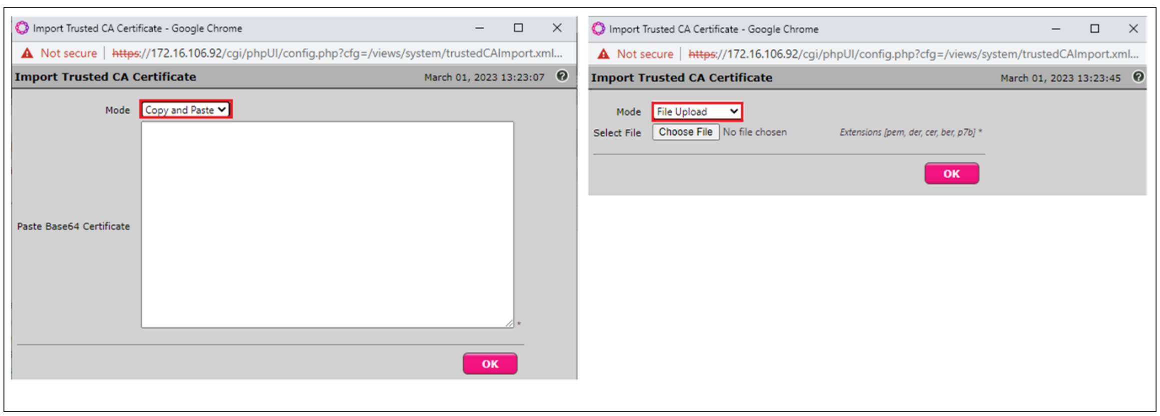
> **Note**
> Refer to Root Certificate - Cisco Webex.

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



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

1. To import a Trusted CA Certificate, click the Import Trusted CA Certificate () Icon.
2. Select File upload or copy paste for the menu listed.
3. If you choose File upload, browse the certificate and Click OK.



> **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.

Networking Interfaces

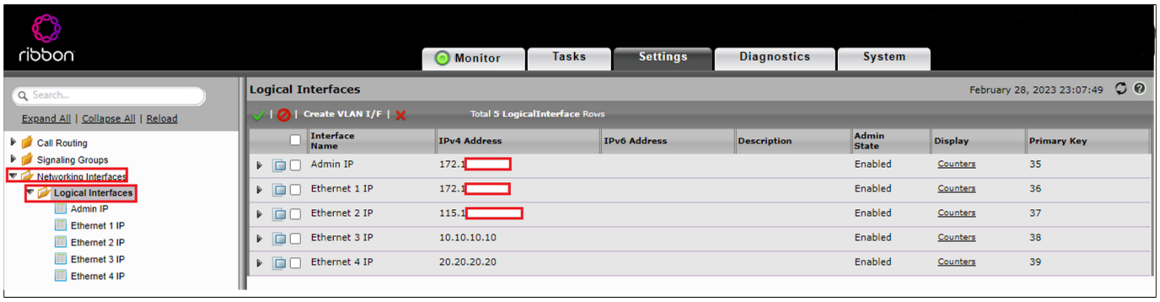
The SBC Edge supports five system created logical interfaces known as Administrative IP, Ethernet 1 IP, Ethernet 2 IP, Ethernet 3 IP, and Ethernet 4 IP. In addition to the system-created logical interfaces, the Ribbon SBC Edge supports user-created VLAN logical sub-interfaces.

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

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

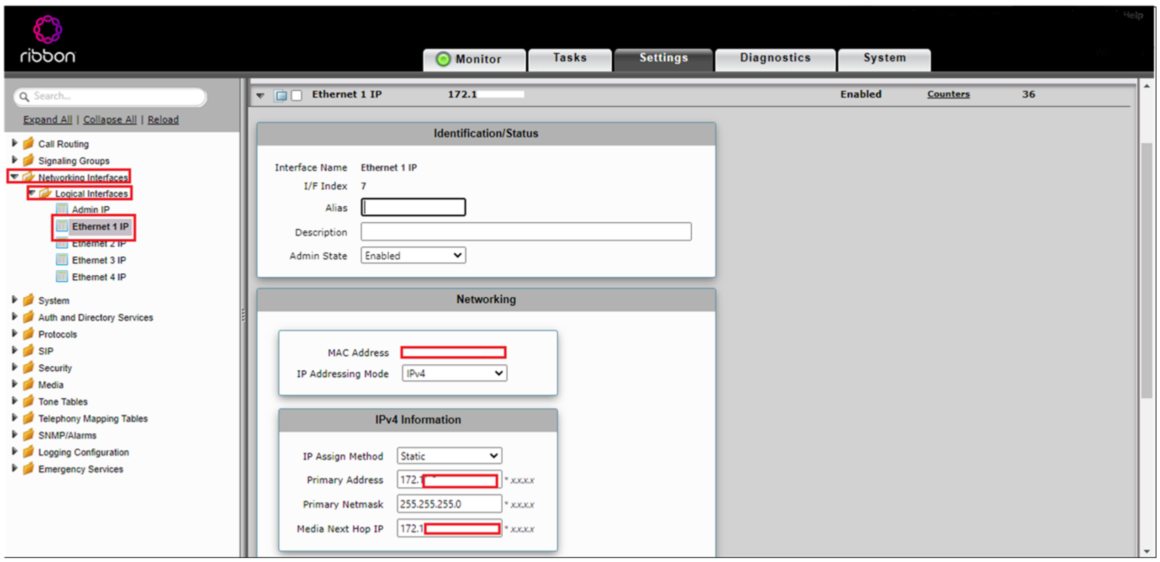
Administrative IP

The SBC 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 Edge system.



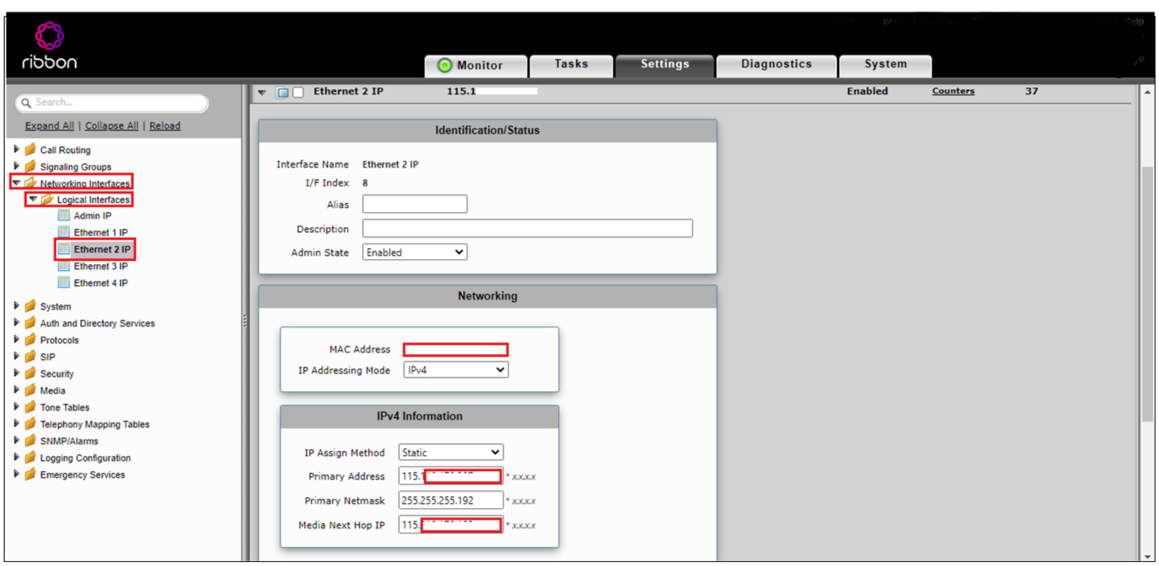
Ethernet 1 IP

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). In the default software, **Ethernet 1 IP** is enabled, and an IPv4 address is acquired through a connected DHCP server or you can assign a static IP as well.



Ethernet 2 IP

After initial configuration, you may configure this logical interface using the Settings or Tasks tabs in the WebUI or you can use the IP address configured during Initial Setup. This interface will face towards Cisco Webex.



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).

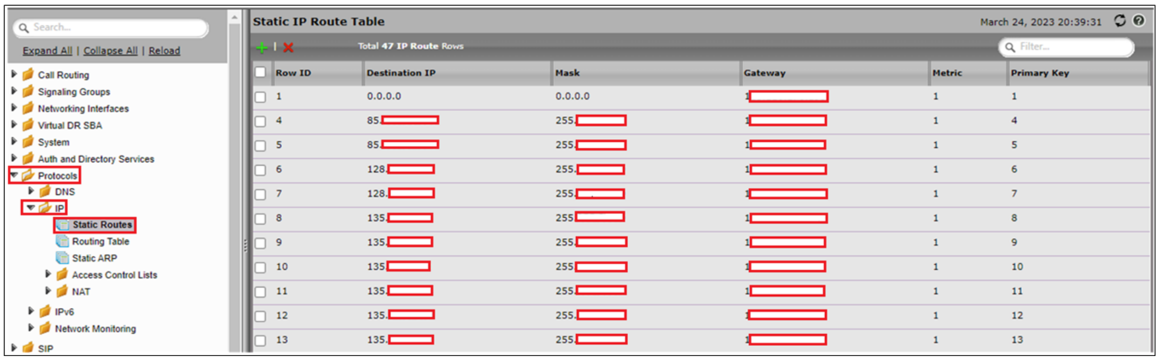
Destination IP
Specifies the destination IP address.

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.

From the **Settings** tab, navigate to **Protocols > IP > Static Routes.** Click the icon to add the entries.

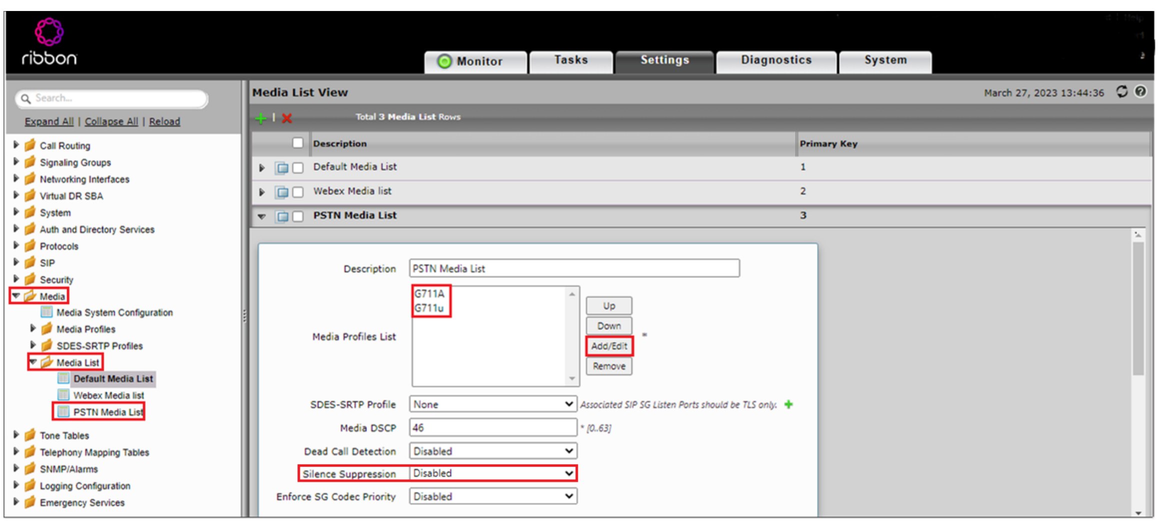


SBC Edge Configuration for PSTN side and Enterprise Solutions

Media List - PSTN

From the **Settings** tab, navigate to **Media > Media List**. Click the icon at the top of the Media List View page.

1. Provide a name for the profile.
2. Attach the Media Profiles by clicking Add/Edit.
3. The SBC by default has G711A and G711U media profiles.
4. Click OK.

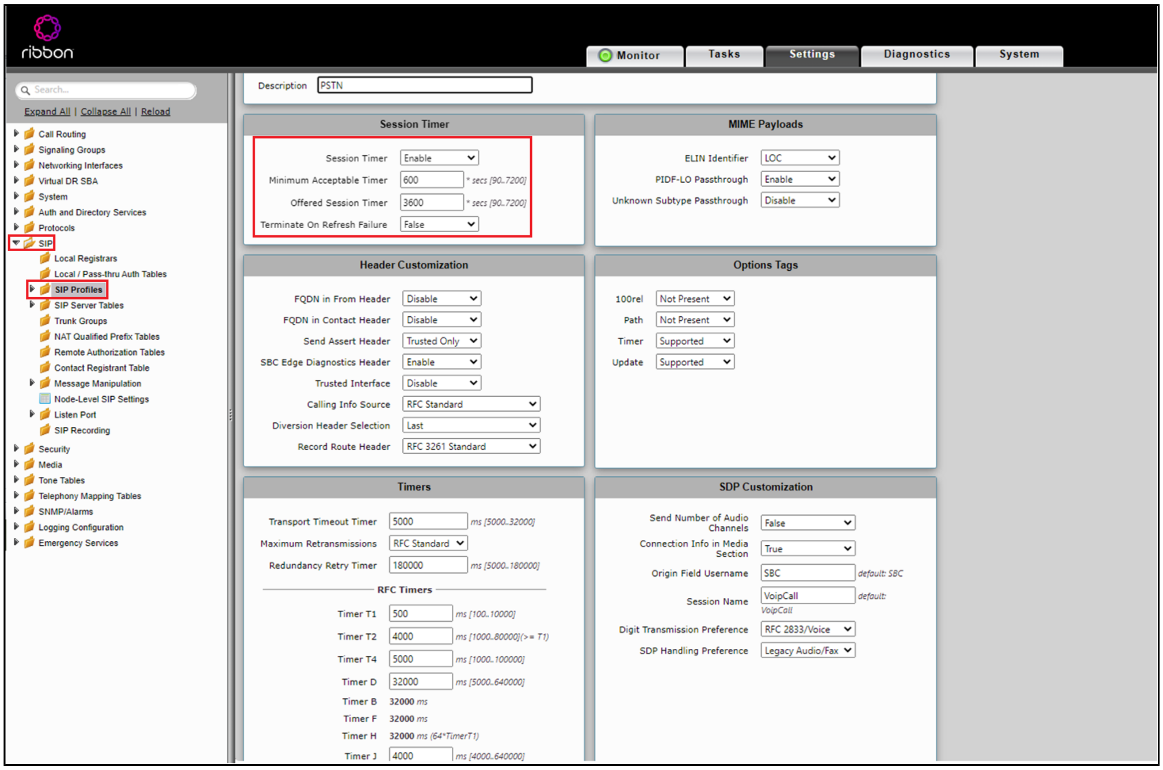


SIP Profile - PSTN

SIP Profiles control how SBC Edge communicates with SIP devices. They control important characteristics, such as Session Timers, SIP Header Customization, SIP Timers, MIME Payloads, and Option Tags.

From the **Settings** tab, navigate to **SIP > SIP Profiles.** Click the icon to create a new SIP Profile.

1. Provide a name for the profile in the Description field.
2. Enable Session Timer. This field specifies whether or not to use Session Timer to verify the SIP session.
3. Set Minimum Acceptable Timer to 600 and Offered Session Timer to 3600.
4. Click OK.

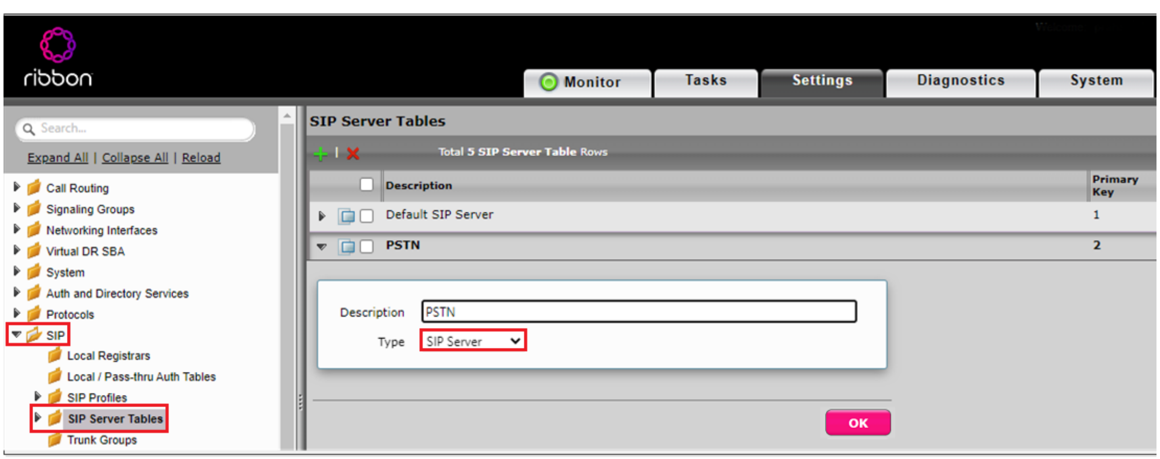


SIP Server Table - PSTN

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.

From the **Settings** tab, navigate to **SIP > SIP Server Tables.** Click the + icon to create a new SIP Server Table.

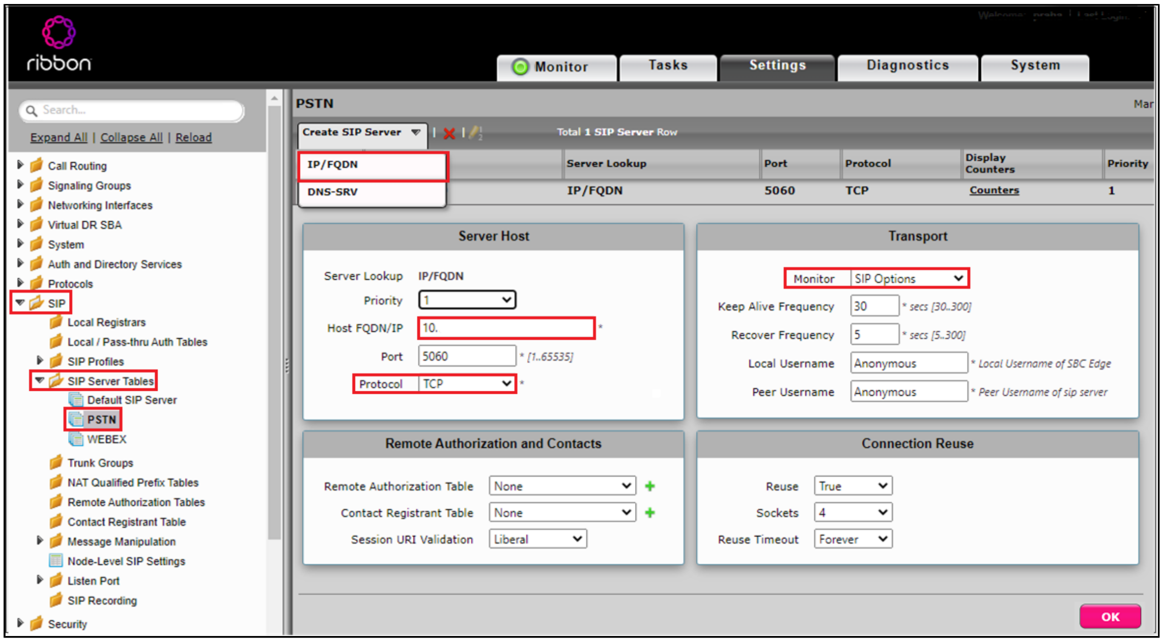
1. Provide a name for the SIP Server.
2. From the Type drop-down menu, choose SIP Server.
3. Click OK.



SIP Server Table Entry

1. Click on the SIP Server Table created in the previous step.

2. From the Create SIP Server drop-down menu, select IP/FQDN.
3. Provide IP Address and Port Number of the PSTN endpoint
4. Enable SIP OPTIONS by selecting SIP OPTIONS under transport section and click OK

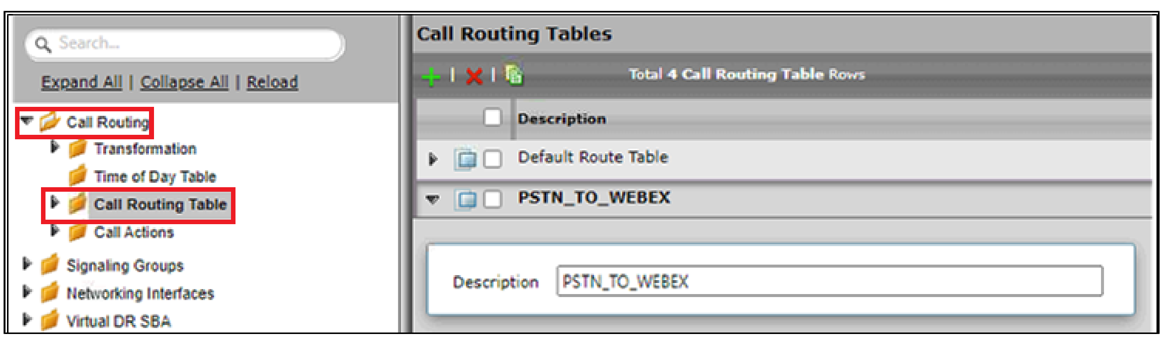


Call Routing Table - PSTN

Call Routing allows calls to be carried between Signaling Groups and 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).

From the **Settings** tab, navigate to **Call Routing** > **Call Routing Table.** Click the + icon to create a Call Routing Table.

1. Provide a name for the Routing Table and Click OK.



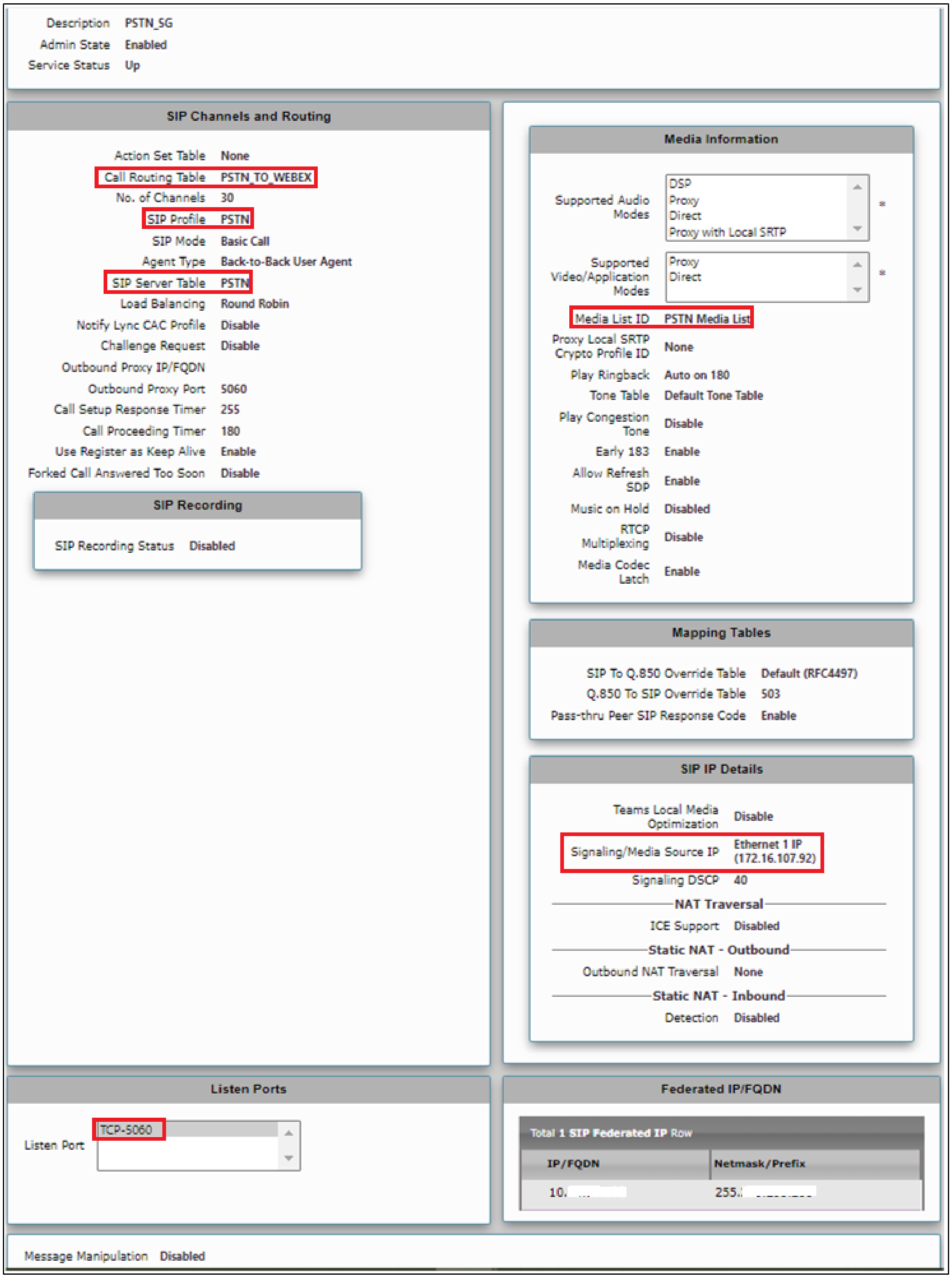
SIP Signaling Group - PSTN

Signaling groups allow telephony channels to be grouped 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 Routing Tables are selected.

From the **Settings** tab, navigate to Signaling Groups. Click Add SIP SG.

1. Attach the Call Routing Table CallRoutingTable-PSTN.
2. Attach the SIP Profile SIPProfile-PSTN.
3. Attach the SIP Server Table SIPServerTable-PSTN.
4. Attach the Media List ID MediaList-PSTN.
5. Configure Protocol and Listen Ports in the "Listen Ports" panel.

6. Associate the appropriate IP address in the "Signaling/Media Source IP" field. This address is used as the source IP for all SIP messages leaving the SBC Edge.
    a. This specifies the Logical IP address at which SIP messages are received.
7. Federated IP addresses and FQDNs specified in a SIP Signaling Group are only allowed and configure the PSTN's address. The IP/FQDN specify which IP/FQDN can access the Signaling Group.

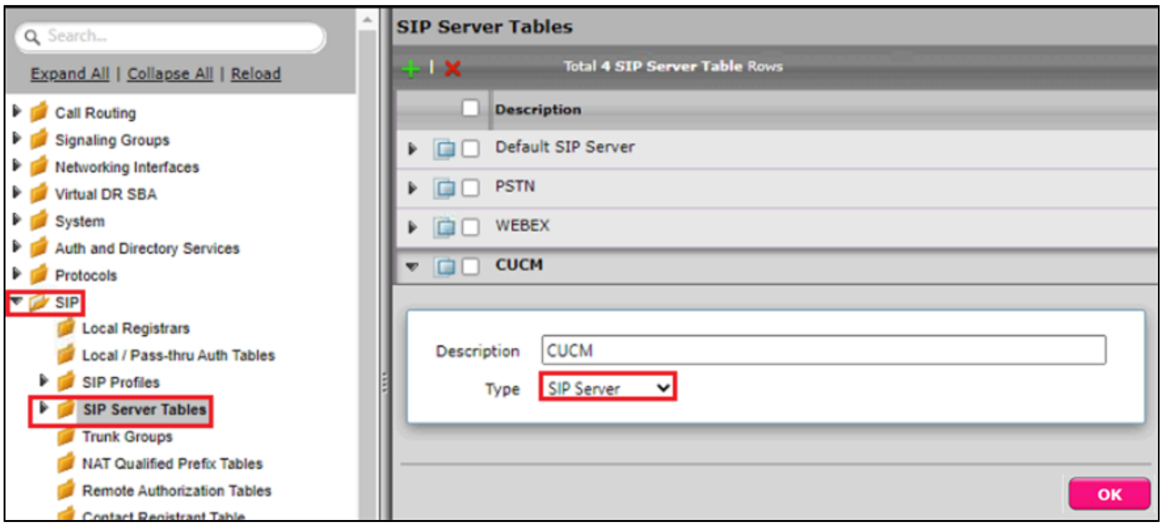


Note
'Proxy with local SRTP' is supported only in SBC SWe Edge, 'Proxy with Local SRTP' is used to switch the media stream between endpoints using SRTP media encryption on a call leg basis.

SIP Server Table - PBX

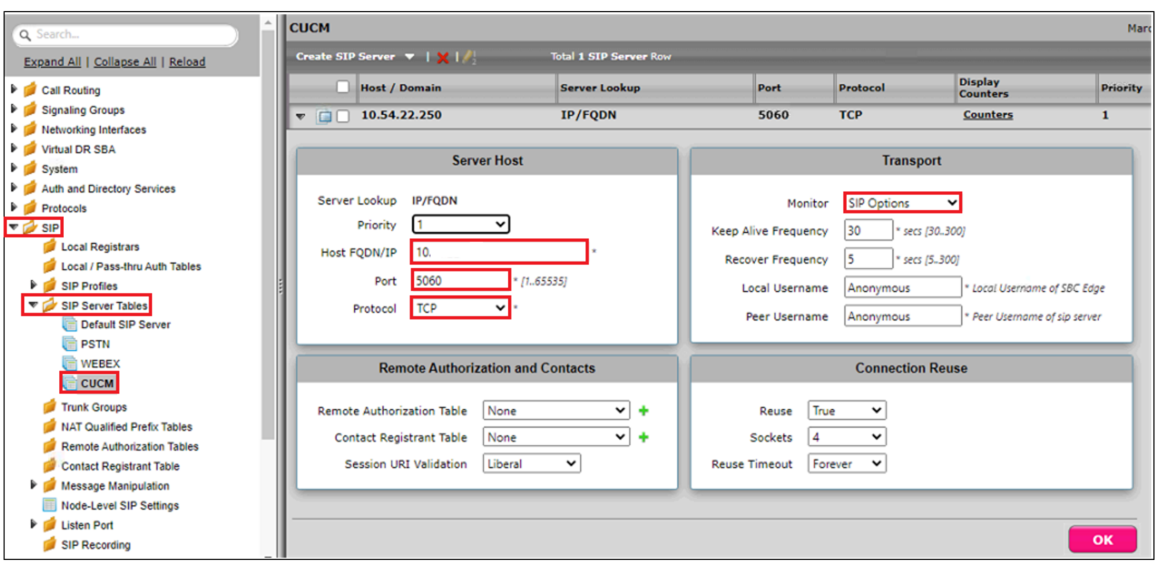
From the **Settings** tab, navigate to **SIP > SIP Server Tables.** Click the icon to create a new SIP Server Table.

1. Provide a name for the SIP Server.
2. From the Type drop-down menu, choose SIP Server.
3. Click OK.



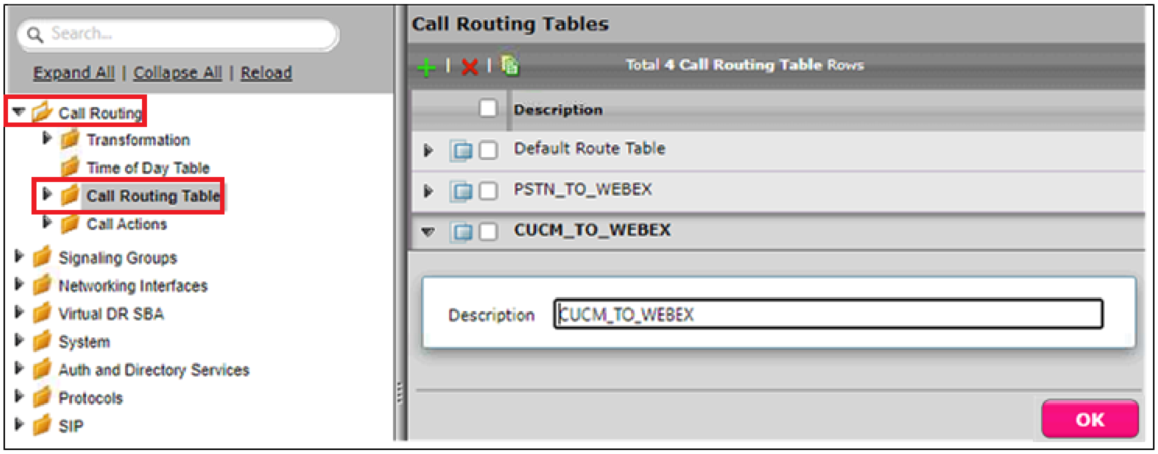
SIP Server Table Entry

1. From the Create SIP Server drop-down menu, select IP/FQDN.
2. Provide IP Address and Port Number of the PBX endpoint.



Call Routing Table - PBX

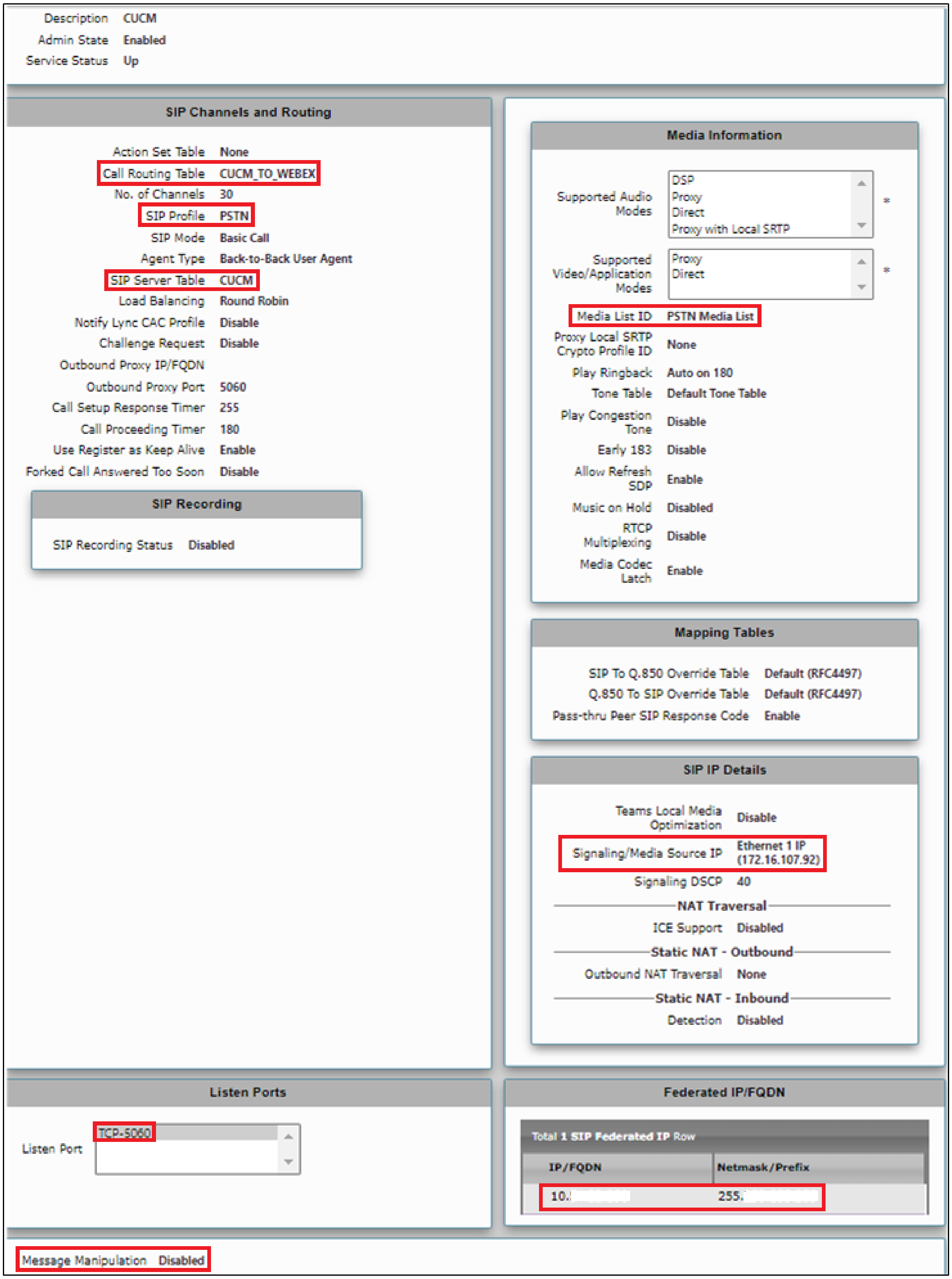
Create a Call Routing Table to route the call from PBX to Webex.



SIP Signaling Group - PBX

SIP Profile and Media List which created for PSTN can be attached in the PBX Signaling group as well.

1. Attach the SIP Server Table SIPServerTable-PBX.
2. Attach the Call Routing Table CallRoutingTable-PBX.
3. Federated IP/FQDN should be configured with PBX's address.



> **Note**
> 'Proxy with local SRTP' is supported only in SBC SWe Edge, Proxy with Local SRTP is used to switch the media stream between endpoints using SRTP media encryption on a call leg basis.

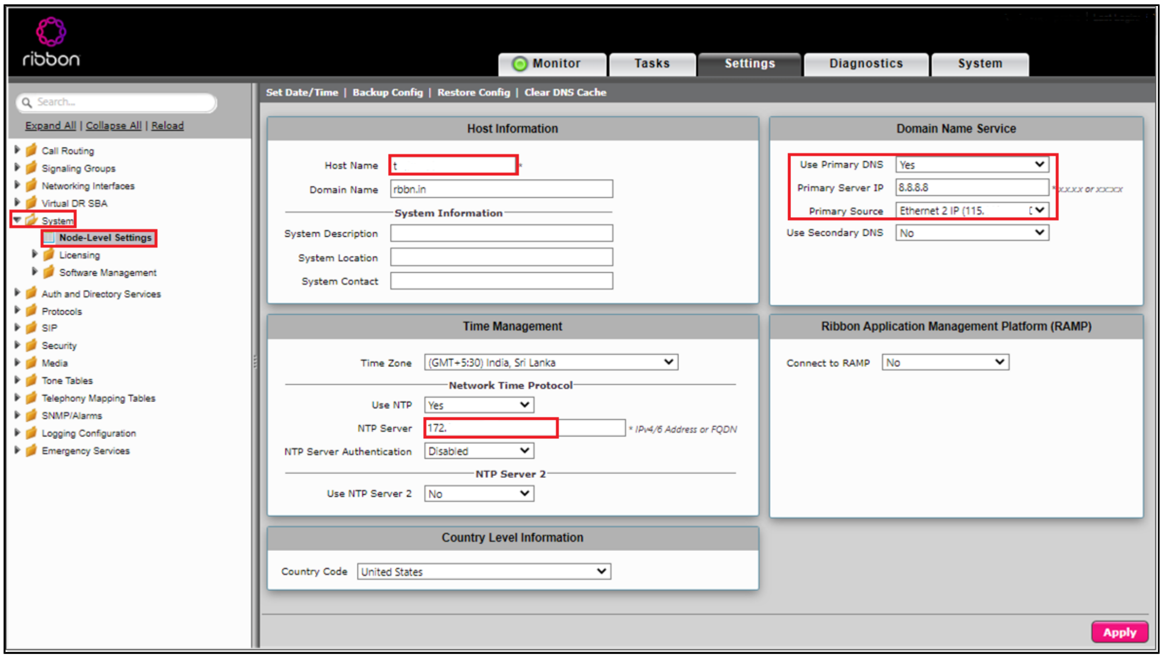
SBC Edge Configuration for Cisco Webex Calling side

Node-Level Settings

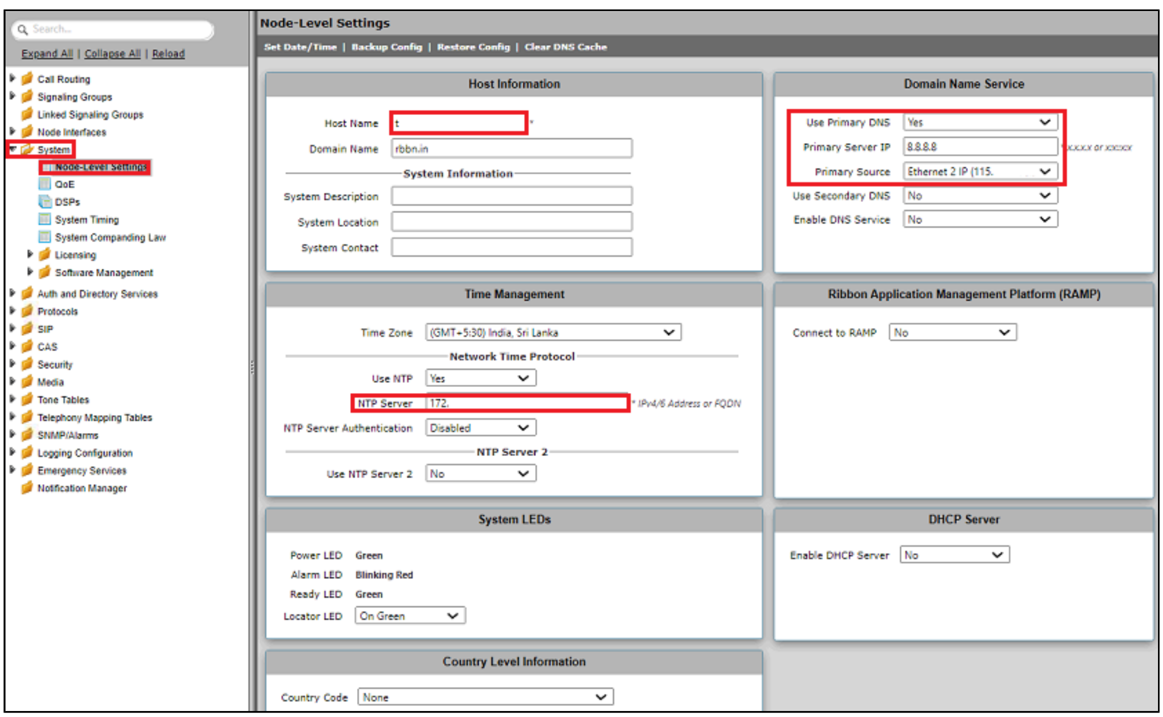
From the **Settings tab**, navigate to **System > Node-Level Settings**.

1. From the Use Primary DNS drop-down menu, select Yes.
2. Provide the Primary DNS IP address and select the Ethernet pointing towards the Cisco Webex.
3. Configure the Host name and Domain name based on the name of the tenant1's FQDN.
4. Provide the desire NTP (Network Time Protocol) server, used for clock synchronization.

For **SBC SWe Edge,** refer to the snapshot below.



For **SBC 1K/2K**, refer to the snapshot below.



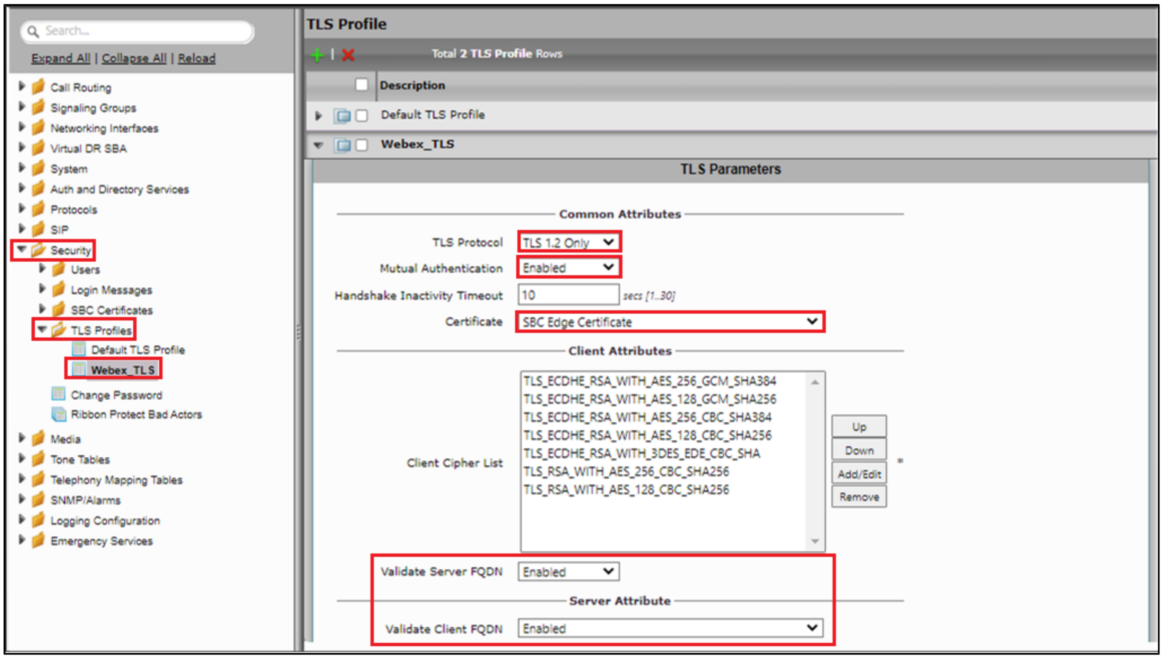
TLS Profile

The TLS profile defines the crypto parameters for the SIP protocol.

TLS Profiles are used by SIP Signaling Groups when the TLS transport type is selected for incoming and outgoing SIP trunks (Listen Ports), and in SIP Server Tables when TLS is selected as the Server Host protocol.

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

1. From the TLS Protocol drop-down menu, select TLS 1.0-1.2.
2. Attach the certificate which is uploaded in the SBC Certificate.
3. Add the cipher suites that are supported on Cisco Webex.
4. Enable the Validate Server and Client FQDN fields to validate the CN and SAN name in the certificate send by Server and Client.
5. Click OK.

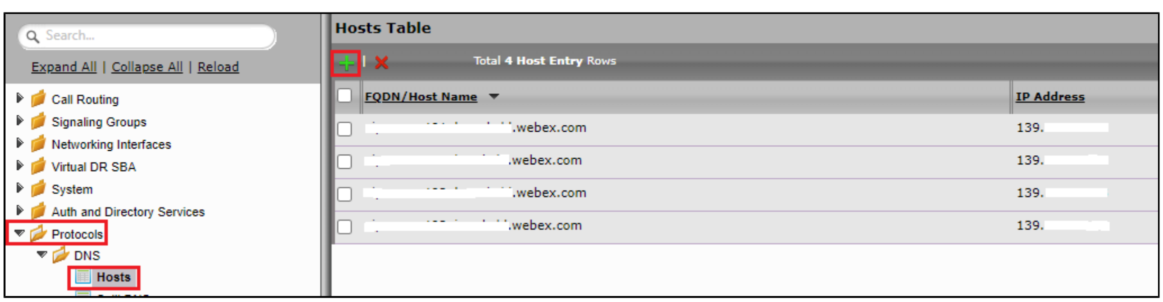


Note
The SBC doesn't support tracking active/closed TLS connections.

DNS Host

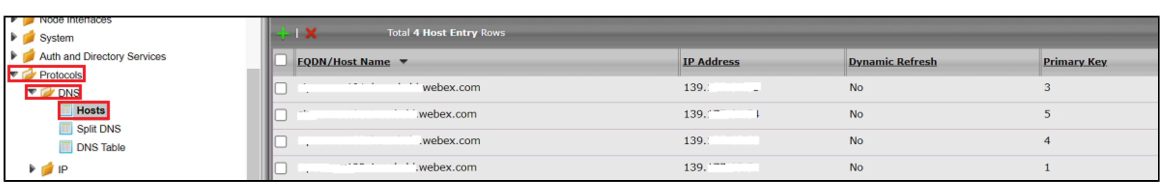
To **Validate the Client FQDN**, add the FQDN entries and corresponding IPs that are resolved from the Cisco Webex SRV under the Host section on the SBC.

DNS host on SBC SWe Edge:



DNS host on SBC 1K/2K:

Please ignore this step for SBC SWe Edge. In SBC 1K/2K, the Dynamic Refresh should be configured as No.



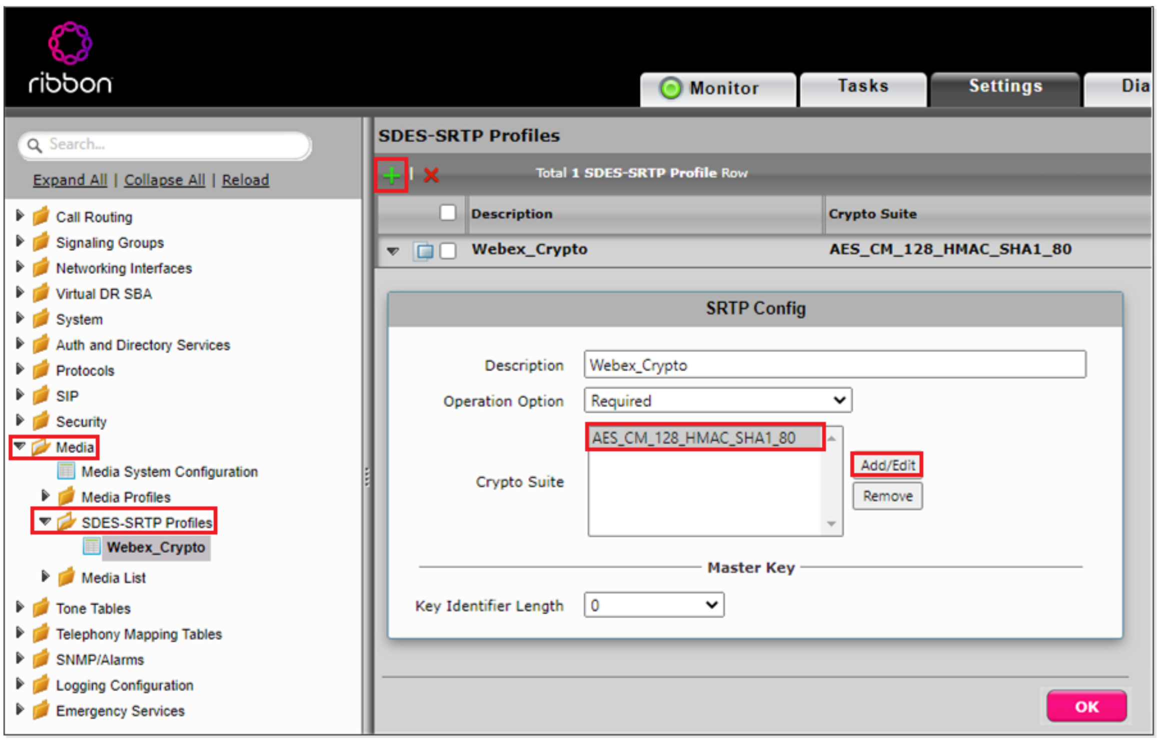
SDES-SRTP Profile - Webex

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

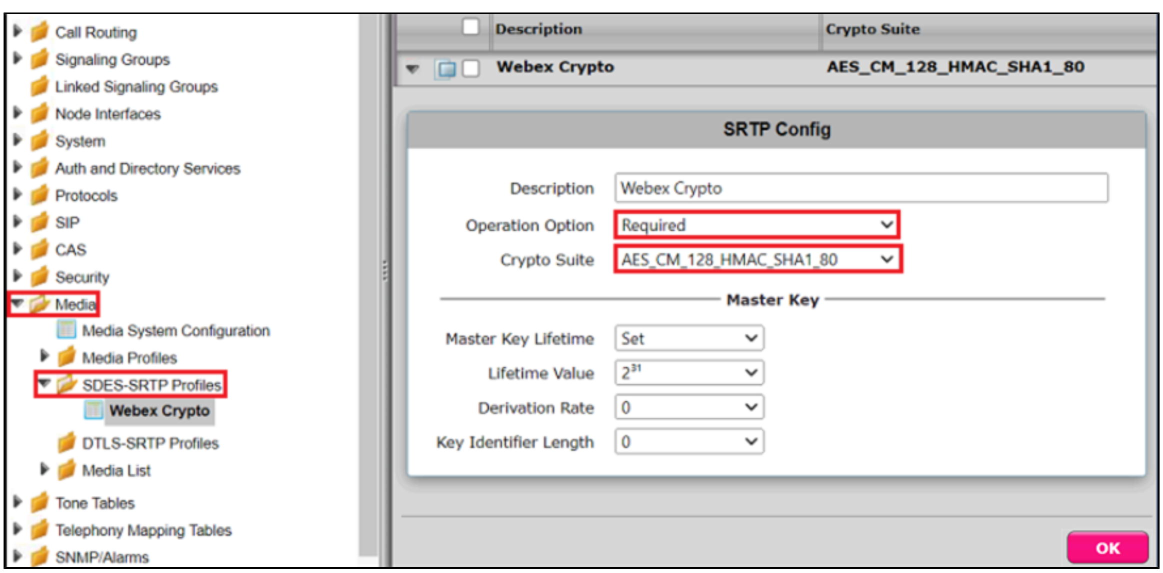
From the **Settings** tab, navigate to **Media > SDES-SRTP Profiles.** Click the + icon to create a new SDES-SRTP profile.

1. Provide a name for the profile in the Description field.
2. 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.
3. Operation Option should be **Required**.
4. Set the Key Identifier Length to 0 to disable the MKI in SDP.
5. Click OK.

For **SBC SWe Edge,** refer to the snapshot below.



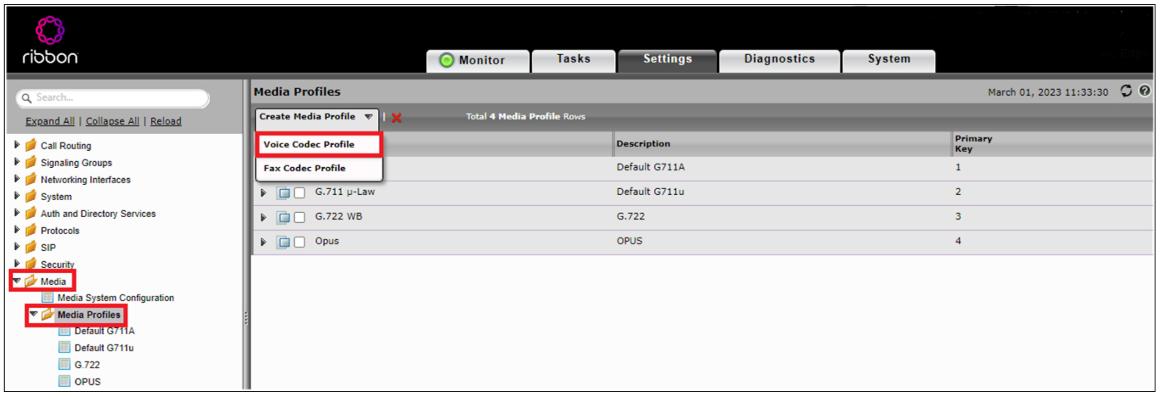
For **SBC 1K/2K,** refer to the snapshot below.



Media Profiles - Webex

Media Profiles allow you to specify the individual voice and fax compression codecs and their associated settings, for inclusion in a Media List.

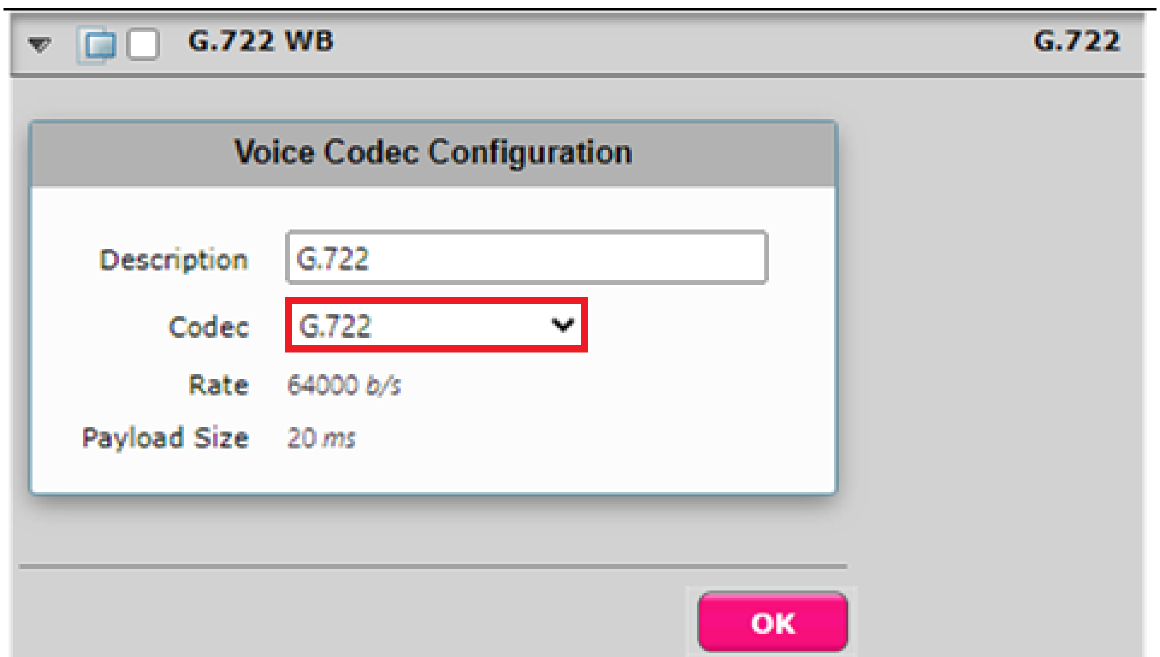
From the **Settings** tab, navigate to **Media > Media Profiles.** From the **Create Media Profile** drop-down, select **Voice Codec Profile.**



For G.711U-Law and G.711A-Law, the SBC Edge has default profiles.

For G722:

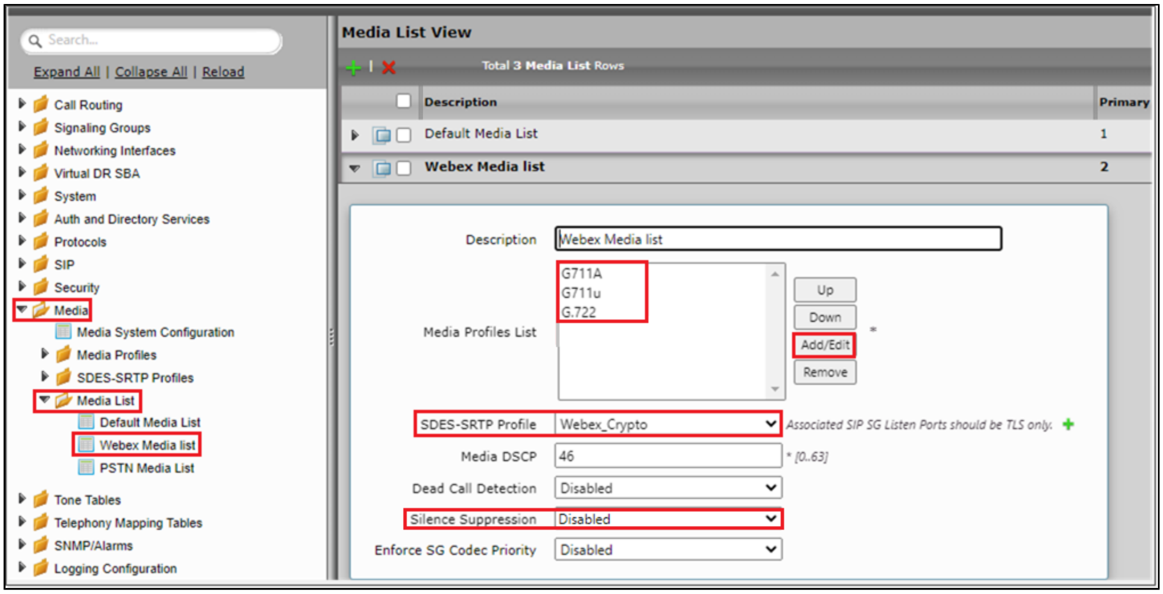
1. Provide the profile's description.
2. Select G.722 from the Codec drop-down menu.
3. Click OK.



Media List - Webex

Media Profiles specify the individual voice and fax compression codecs and their associated settings for inclusion into a Media List. Different codecs provide varying levels of compression, allowing the reduction of bandwidth requirements.

- Select **Settings > Media > Media List**.
- Create a media list with desired descriptions "**Webex Media List**", add the media profile List, and attach the SDES-SRTP Profile **"Webex_Crypto".**



Message Manipulation

a) IP to FQDN Conversion in P-Asserted-Identity

The Message Manipulation is used convert IP to tenant1's FQDN in the P-Asserted-Identity.

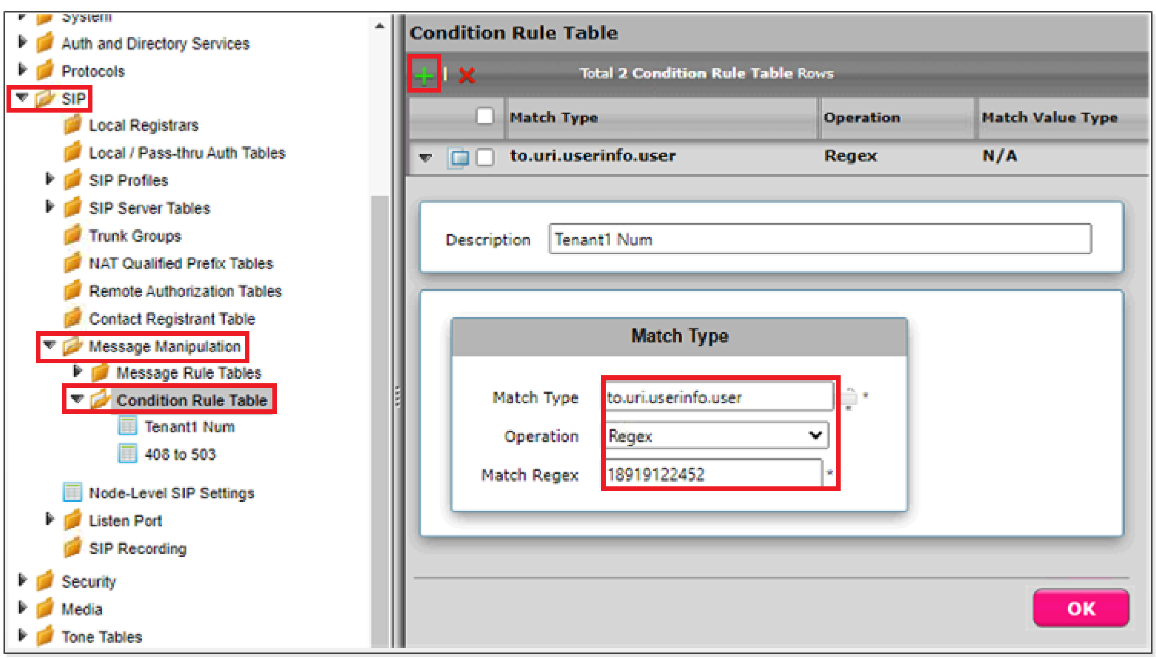
Condition Rule Table

Condition Rule Tables are used to apply the Message Manipulation only if the provided conditions are matched.

Here, the Condition Rule Table is used to match Tenant1 Cisco Webex's number.

From the **Settings** tab, navigate to **SIP > Message Manipulation > Condition Rule Table.** Click the icon to create a new Condition Rule Table.

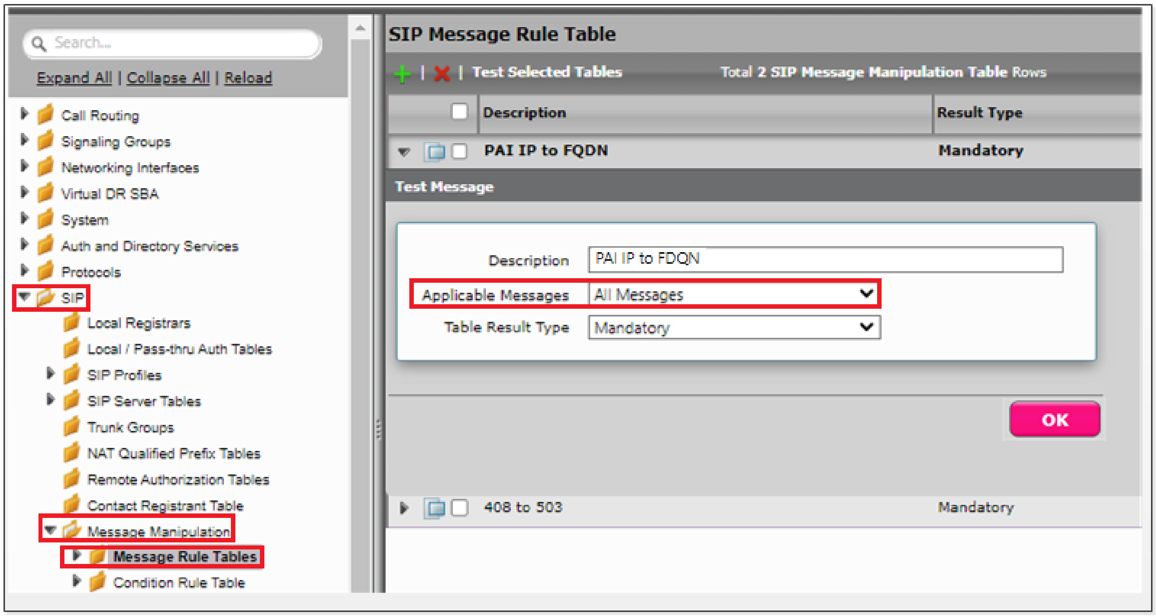
1. Provide a name for the Rule table.
2. From the Match Type drop-down menu, select to.uri.userinfo.user.
3. Under Operation, select Regex.
4. Under Match Regex, enter Tenant1's number.
5. Click OK.



Message Rule Table

From the **Settings** tab, navigate to **SIP > Message Manipulation > Message Rule Table**. Click the + icon to create a Message Rule Table.

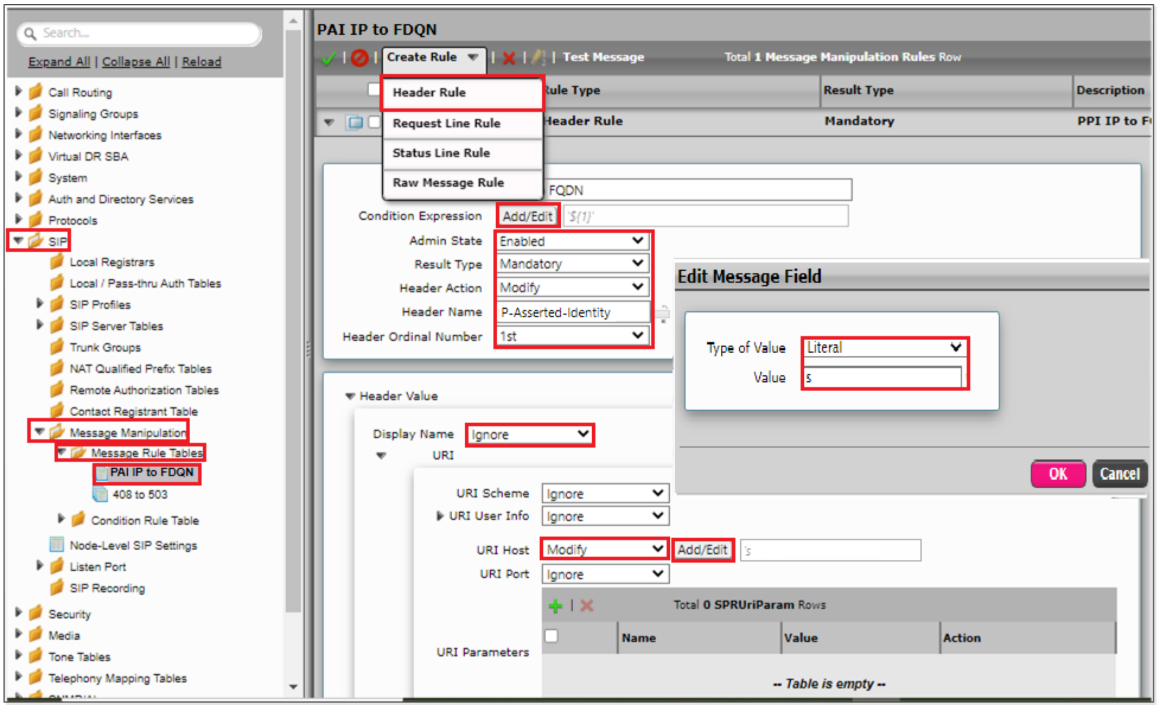
1. Provide a description for the Rule Table.
2. Apply the message rule to All Messages, since the P-Asserted-Identity has to be changed on all the messages.
3. Click OK.



Message Rule Table Entry

Header Rule:

1. Select **Message Rule Tables > PAI IP to FQDN**.
2. From the Create Rule drop-down menu, select **Header Rule**.
3. Under Condition Expression> **Add/Edit** and select Message Rule Condition > **Match all Condition** and from the drop-down menu, select the condition rule as **Tenant1 Num**.
4. Select Header Action as Modify and Header Name as **P-Preferrred-Identity**.
5. Under Header Value > URI Host, select **Modify**.
6. Click on Add/Edit. Under the Edit Message Field, set Type of Value as **Literal** and Value as **Tenant1's FQDN**.
7. Click OK and Apply.



b) 408 Request Time-Out to 503 Service Unavailable

Note

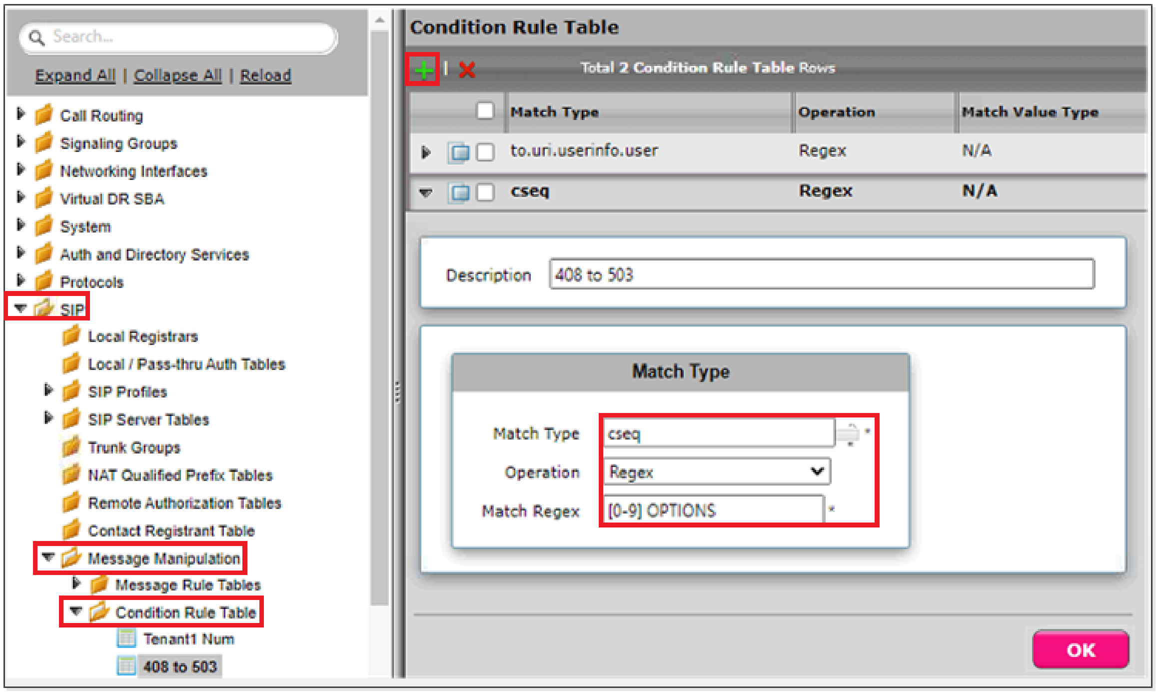
- The SBC doesn't generate an alarm and the inactive node is not removed from call routing when a 408 response is received from the Webex node for SIP OPTIONS.
- It is recommended to use the SMM given below to convert **408 Request Time-out** to **503 Service Unavailable**.

Condition Rule Table

The Condition Rule Table is here to match the 408 response that is coming only for SIP OPTIONS.

From the **Settings** tab, navigate to **SIP > Message Manipulation > Condition Rule Table.** Click the + icon to create a new Condition Rule Table.

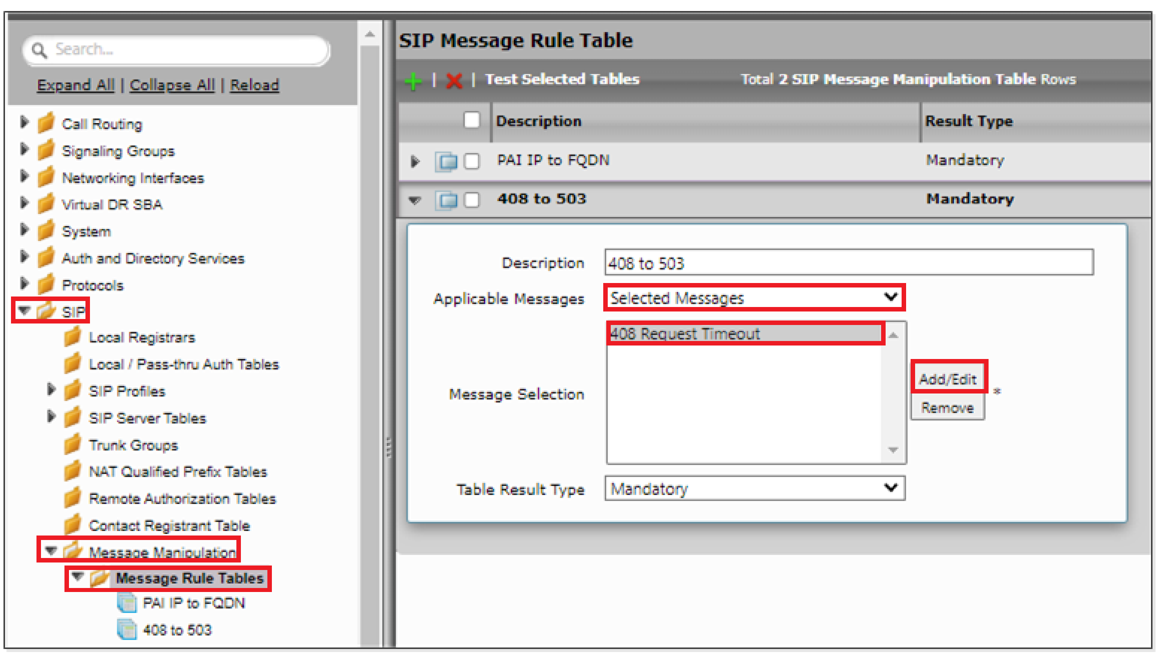
1. Provide a name to Rule table.
2. From the Match Type drop-down menu, select CSeq.
3. Under Operation, select Regex.
4. Under Match Regex, give the regular expression as [0-9] OPTIONS.
5. Click OK.



Message Rule Table

From the **Settings** tab, navigate to **SIP** > **Message Manipulation > Message Rule Table**. Click the + icon to create a Message Rule Table.

1. Provide a description for the Rule Table.
2. Apply the message rule to Selected Messages.
3. Under Message Selection, click on Add/Edit and select 408 Request Timeout.
4. Click OK.

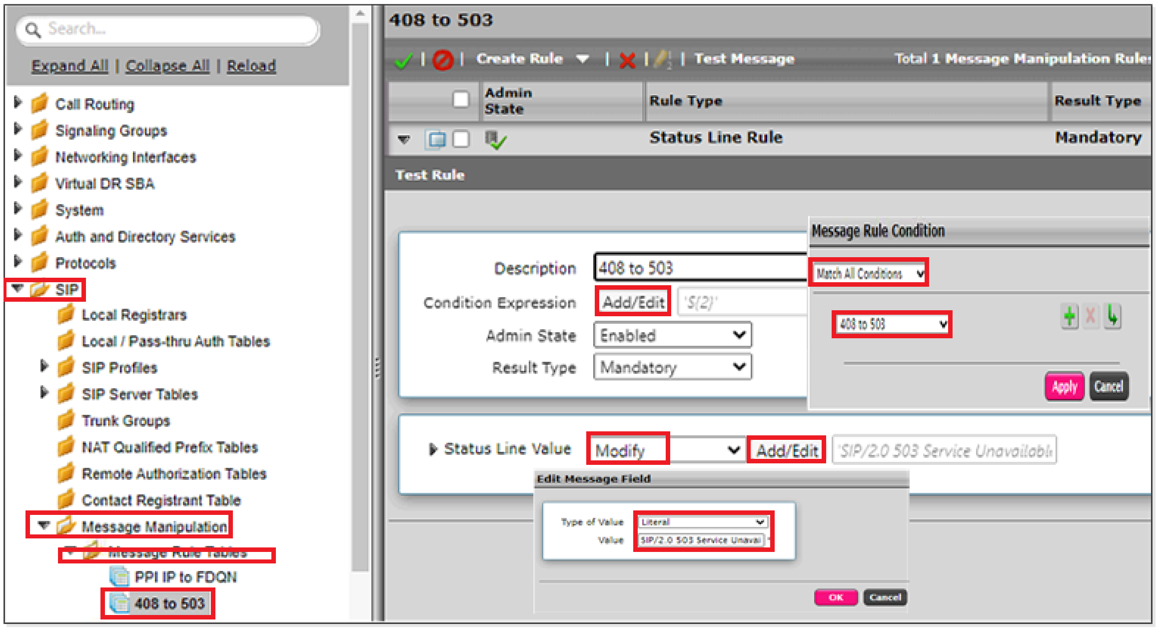


Message Rule Table Entry

Status Line Rule:

1. Click on the Message Rule Table 408 to 503.
2. From the Create Rule drop-down menu, select Status Line Rule.

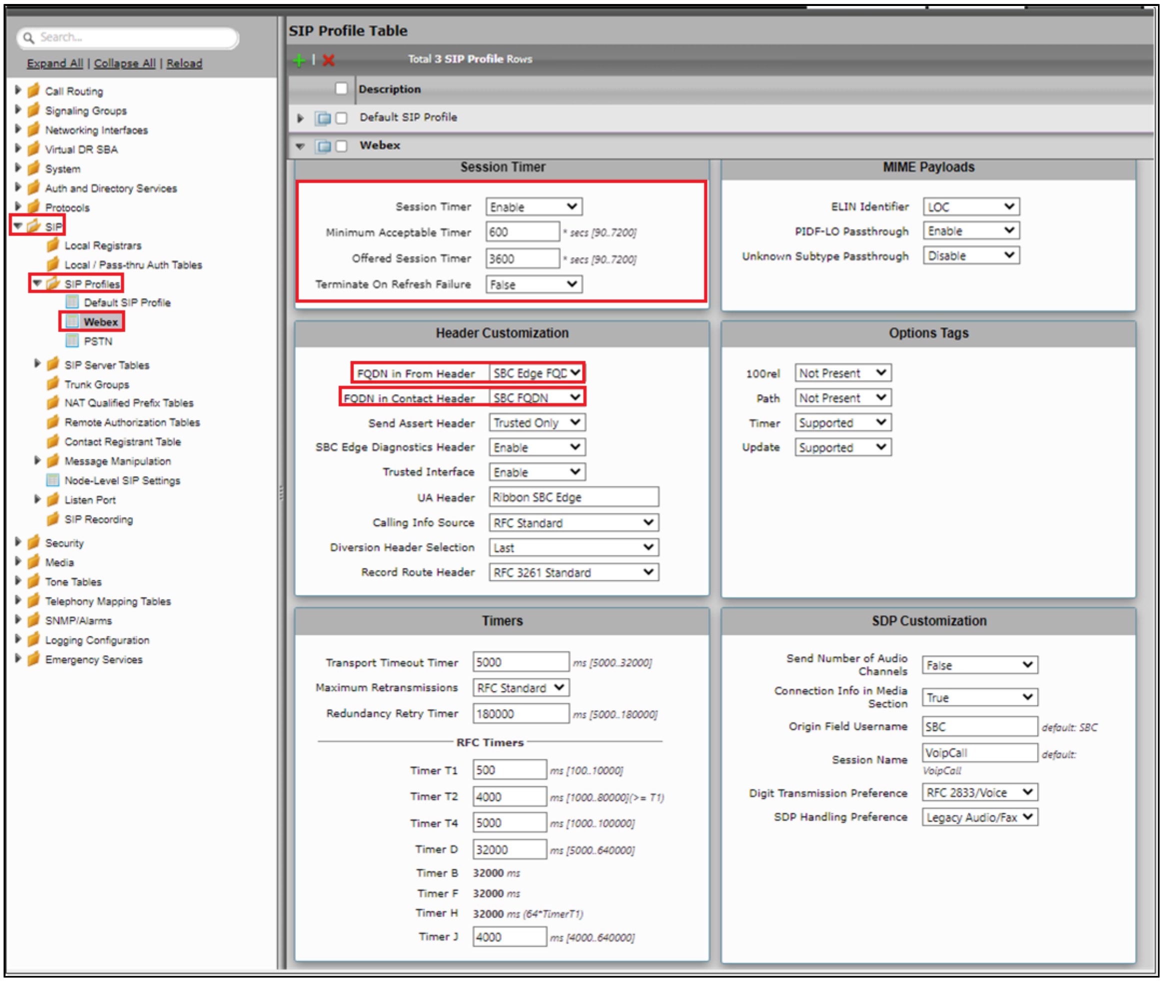
3. Under Condition Expression> Add/Edit, select Message Rule Condition > Match all Condition, and from the drop-down menu, select the condition rule as 408 to 503.
4. Under Status Line Value > Modify > Add/Edit, set Type of Value as Literal and Value as 503 Service Unavailable.
5. Click OK.



SIP Profile - Webex

From the **Settings** tab, navigate to **SIP > SIP Profiles.** Click the + icon to create a new SIP Profile.

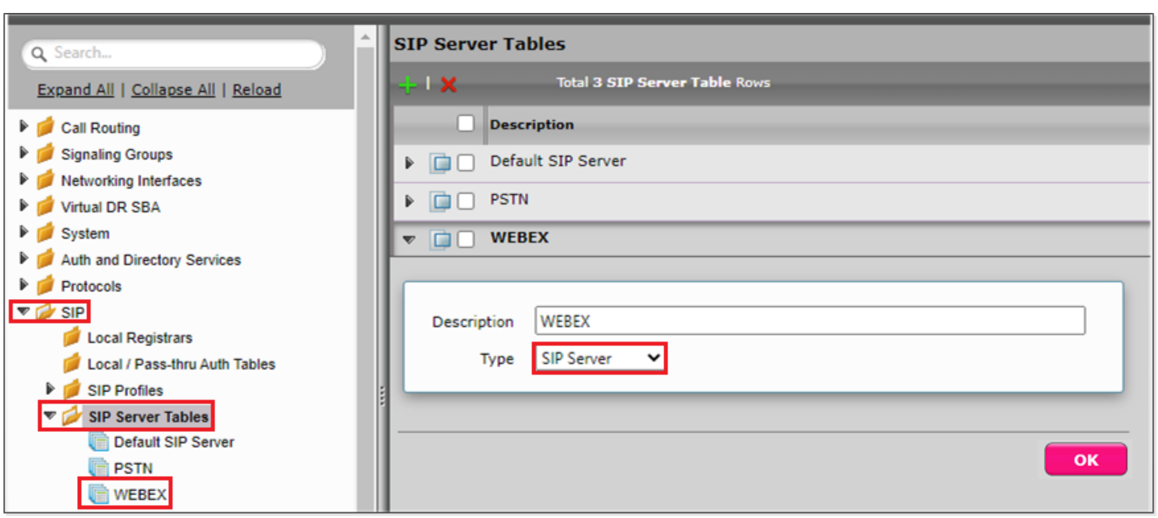
1. Provide a name for the profile in the Description field.
2. Enable Session Timer. This field specifies whether or not to use Session Timer to verify the SIP session.
3. Set Minimum Acceptable Timer to 600 and Offered Session Timer to 3600.
4. From the FQDN in From Header drop-down menu, select SBC Edge FQDN, so that sip Messages from SBC Edge to Webex will have SBC FQDN in From header
5. From the FQDN in Contact Header drop-down menu, select SBC FQDN, so that sip Messages from SBC Edge to Webex will have SBC FQDN in Contact header.
6. Click OK.



SIP Server - Webex

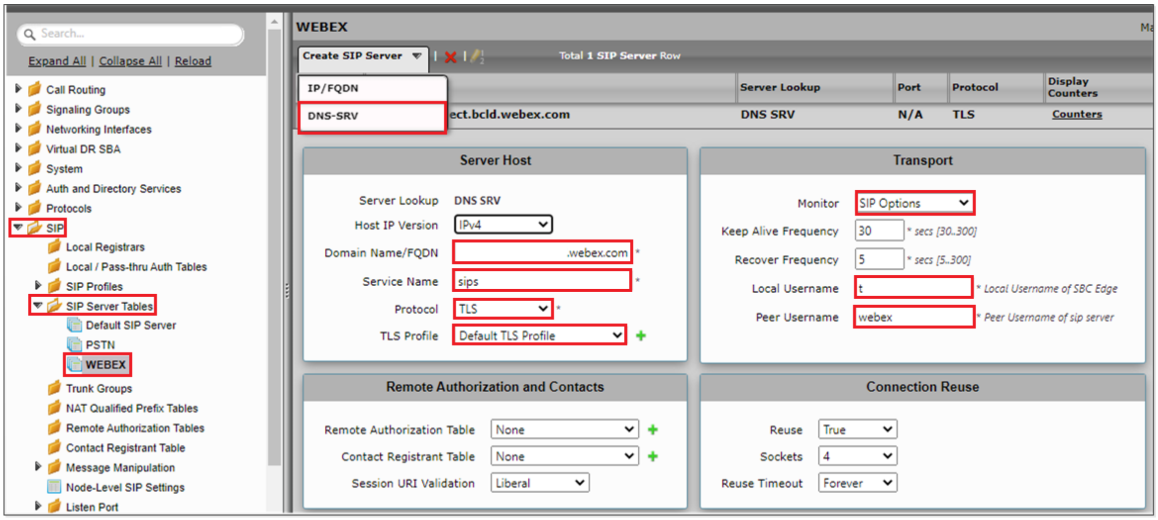
From the **Settings** tab, navigate to **SIP > SIP Server Tables.** Click the + icon to create a new SIP Server Table.

1. Provide a name for the SIP Server.
2. From the Type drop-down menu, select SIP Server.
3. Click OK.



SIP Server Table Entry

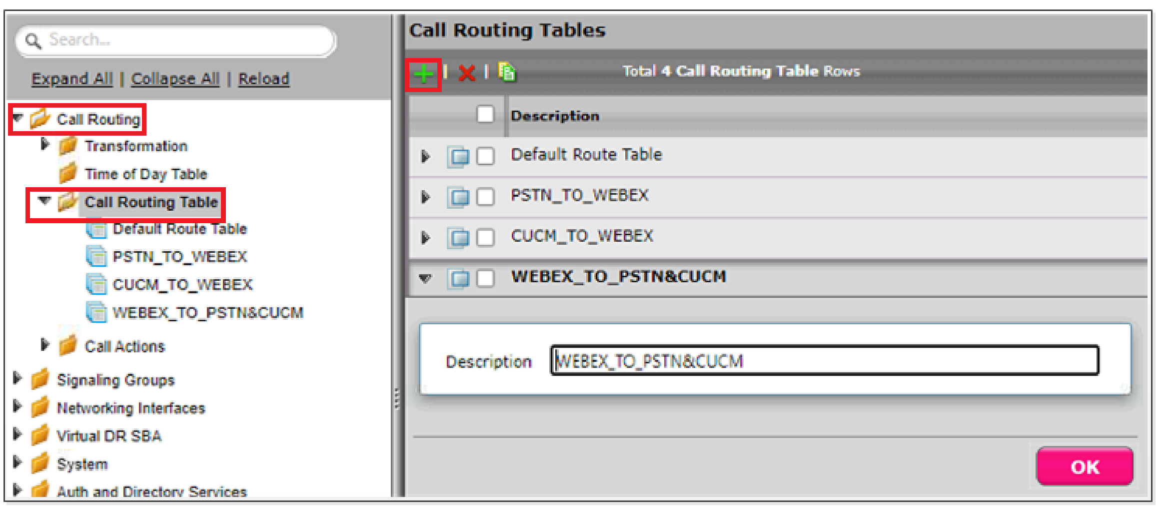
1. Click on the SIP Server Table created in the previous step.
2. From the Create SIP Server drop-down menu, select DNS-SRV.
3. Provide the SRV of the Cisco Webex and service of the SRV as sips.
4. Select the Protocol as TLS and attach the TLS profile which was created previously.
5. Under the Transport section, enable sip OPTIONS by selecting SIP OPTIONS from the Monitor drop-down menu, and set the Local username as SBC host name and the Peer Username as Webex.
6. Click OK.



Call Routing Table - Webex

From the **Settings** tab, navigate to **Call Routing** > **Call Routing Table.** Click the + icon to create a Call Routing Table.

1. Provide a name for the Routing Table.
2. Click OK.

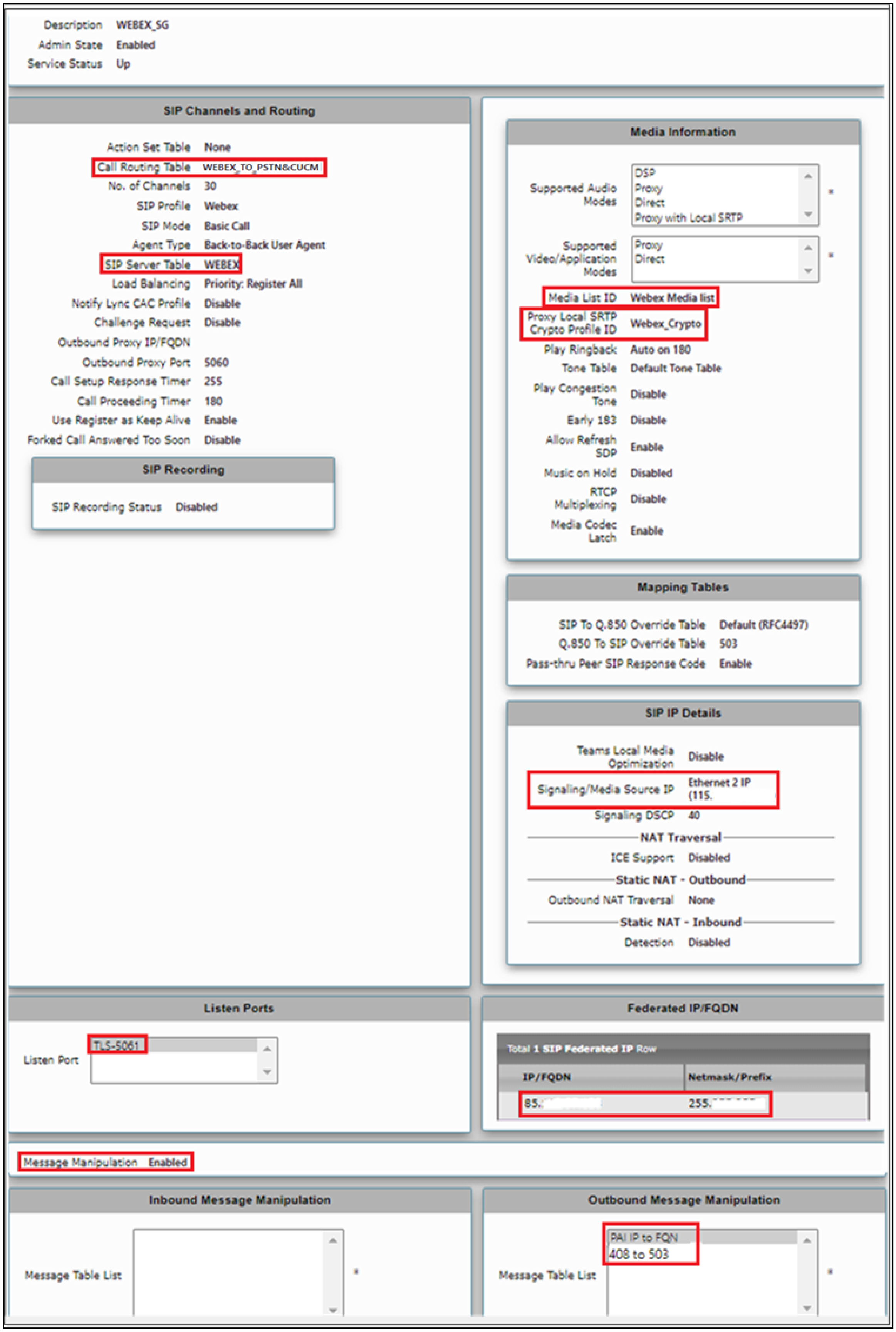


SIP Signaling Group - Webex

From the **Settings** tab, navigate to **Signaling Groups**. Click **Add SIP SG**.

1. Attach the Call Routing Table (CallRoutingTable-Webex).
2. Attach the Sip Profile (SipProfile-Webex).
3. Attach the SIP Server Table (SIPServerTable-PSTN).
4. Attach the SDES-SRTP Profile (SDES-SRTPProfile-Webex).

5. Attach the Media List (MediaList-Webex).
6. Associate the appropriate IP address in the "Signaling/Media Source IP" field.
7. Configure Protocol and Listen Ports in the "Listen Ports" panel.
8. Create an entry in the Federated IP/FQDN panel.
9. Enable Message Manipulation and attach the profile **"PAI IP to FQDN"** and **"408 to 503"** in the outbound Message Manipulation Table List.
10. Click OK.



Note

'Proxy Local SRTP Crypto Profile ID' is available for SBC SWe Edge only. This field is available only when 'Proxy with Local SRTP' (Supported only in SWe Edge) is included in the 'Supported Audio modes'.

Call Routing Table Entry

Call Routing entries must to be created after creating SIP Signaling Groups as Destination SGs need to be attached to these entries.

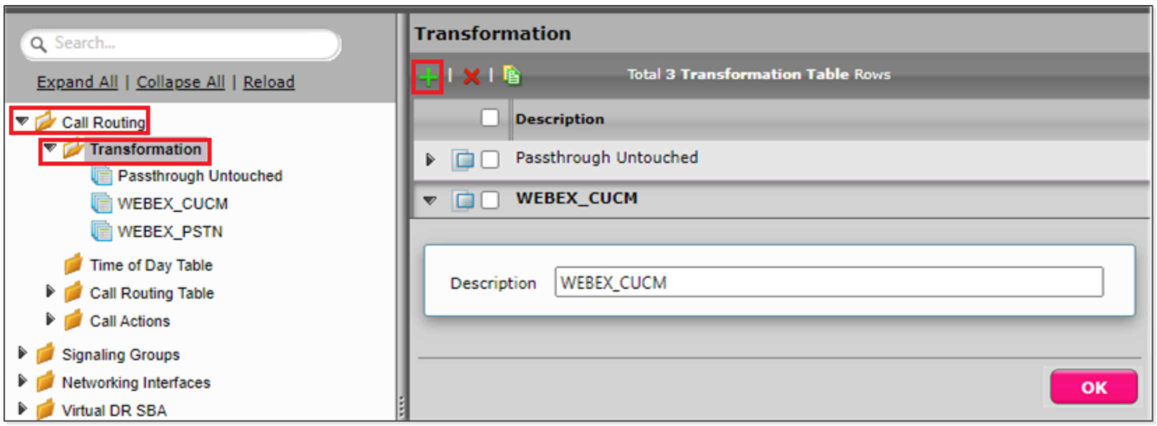
Transformation Table

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. In addition, Transformation tables are configurable as a reusable pool that Action Sets can reference.

Transformation Table Webex to PBX

From the **Settings** tab, navigate to **Call Routing > Transformation**. Click the + icon to create a Transformation Table.

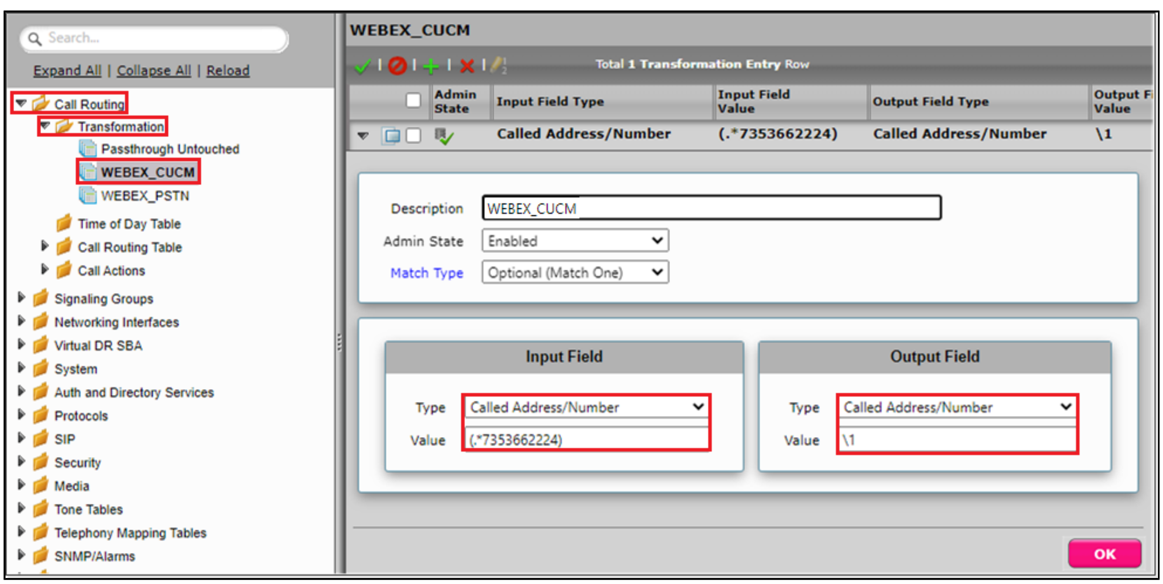
1. Provide a desired name for the transformation table.
2. Click OK.



Transformation Table Entry PBX

From the **Settings** tab, navigate to **Call Routing > Transformation > Webex_CUCM**. Click the + icon to create a Transformation Table Entry.

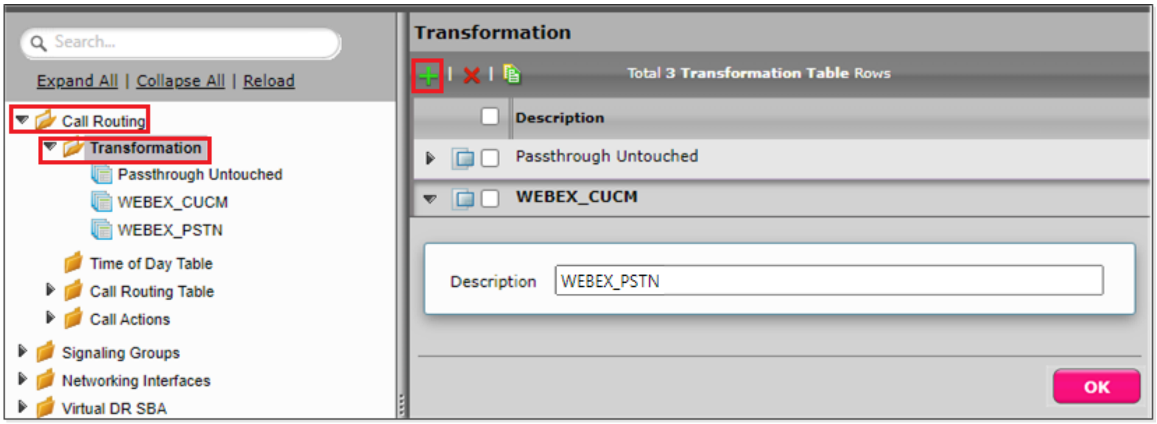
1. Under Input Field, enter the PBX number that is dialed from the Webex.
2. Click OK.



Transformation Table Webex to PSTN

From the **Settings** tab, navigate to **Call Routing > Transformation**. Click the + icon to create a Transformation Table.

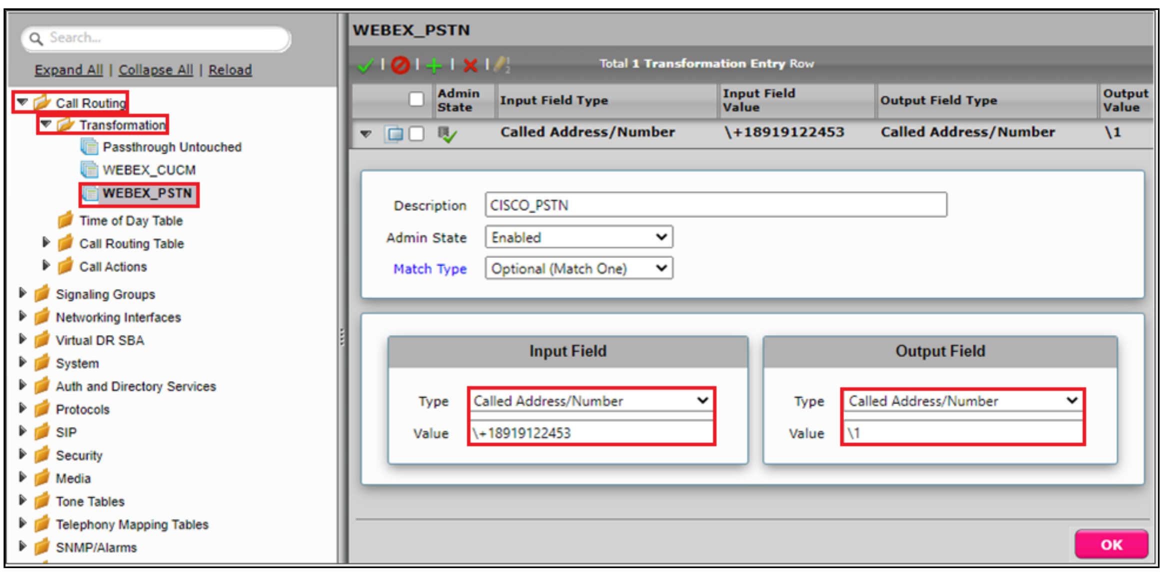
1. Provide a desired name for the transformation table.
2. Click OK.



Transformation Table Entry PSTN

From the **Settings** tab, navigate to **Call Routing > Transformation > Webex_PSTN**. Click the + icon to create a Transformation Table Entry.

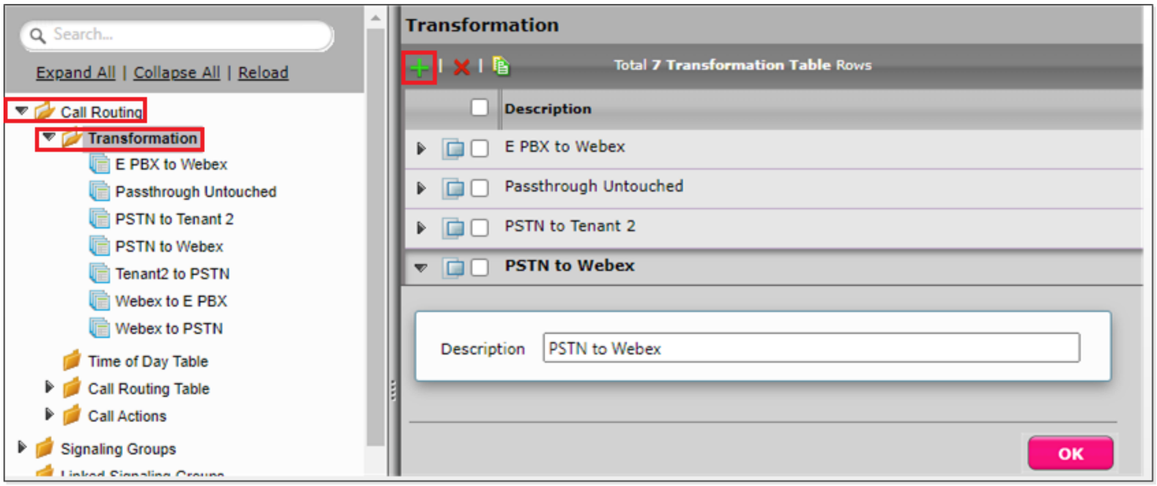
1. Under Input Field, enter the PSTN number that is dialed from the Webex.
2. Click OK.



Transformation Table PSTN to Webex Tenant1

From the **Settings** tab, navigate to **Call Routing > Transformation**. Click the + icon to create a Transformation Table.

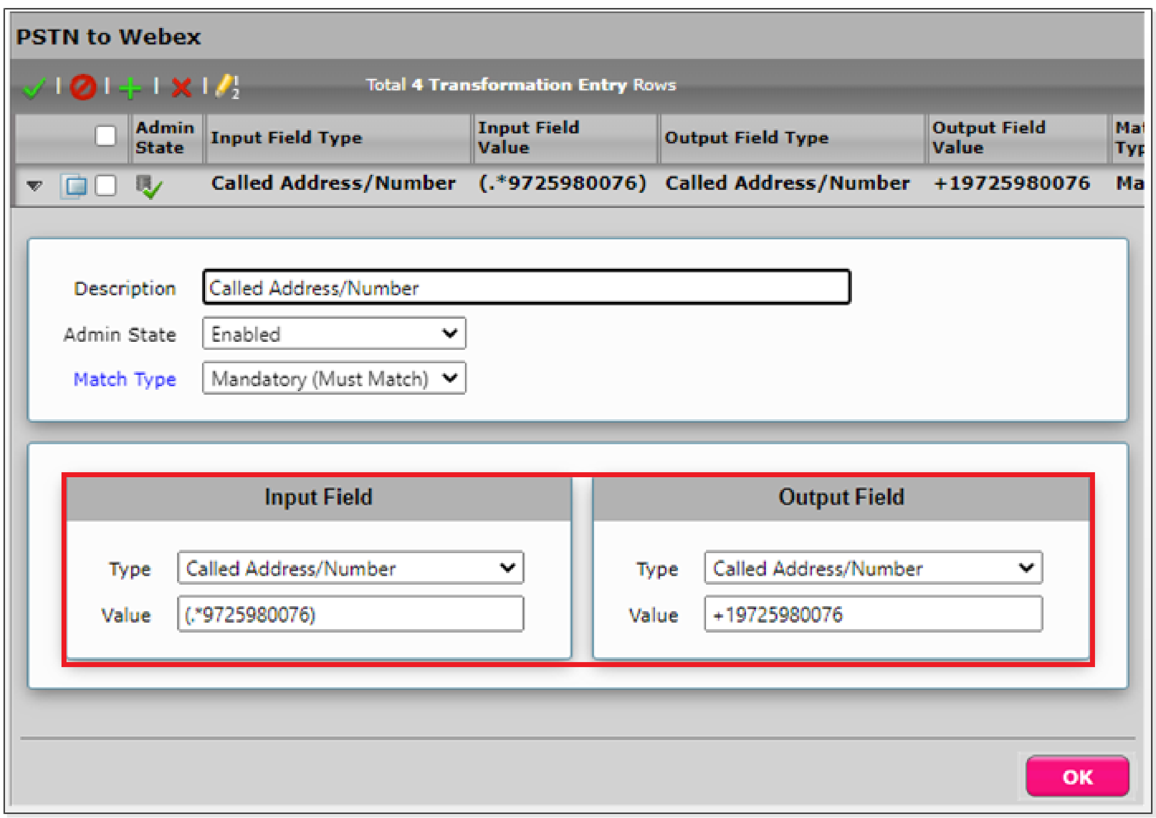
1. Provide a desired name for the transformation table.
2. Click OK.



Transformation Table Entry

From the **Settings** tab, navigate to **Call Routing > Transformation > PSTN to Webex**. Click the icon to create a Transformation Table Entry.

1. Under Input Field, enter the Webex Tenant1 number that is dialed from the PSTN.
2. Click OK.



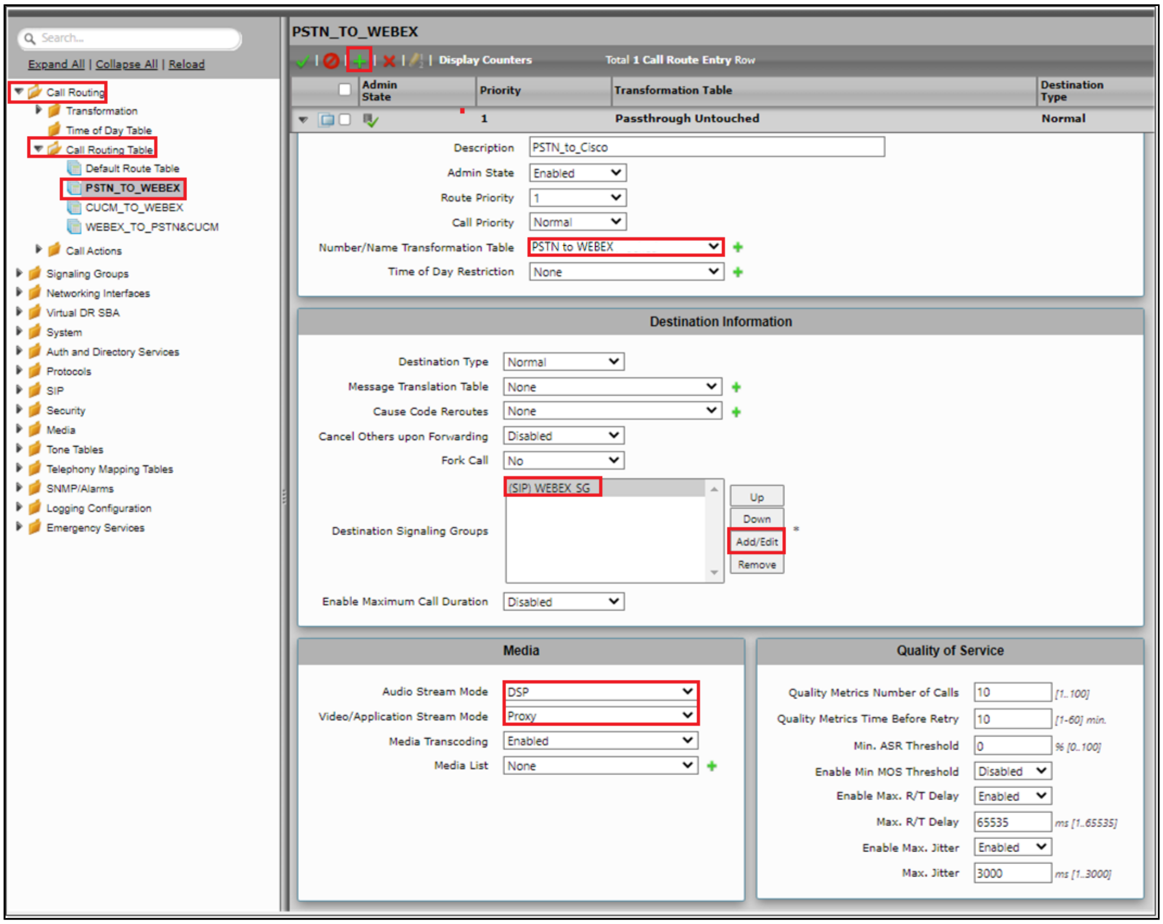
Note
The same Transformation Table can be used for PBX Call Routing also because here, we only check the Webex Tenant1 number.

Call Routing Table Entry

PSTN to Webex

From the **Settings** tab, navigate to **Call Routing > Call Routing Table > PSTN_TO_Webex.** Click the icon to create a Call Routing Table.

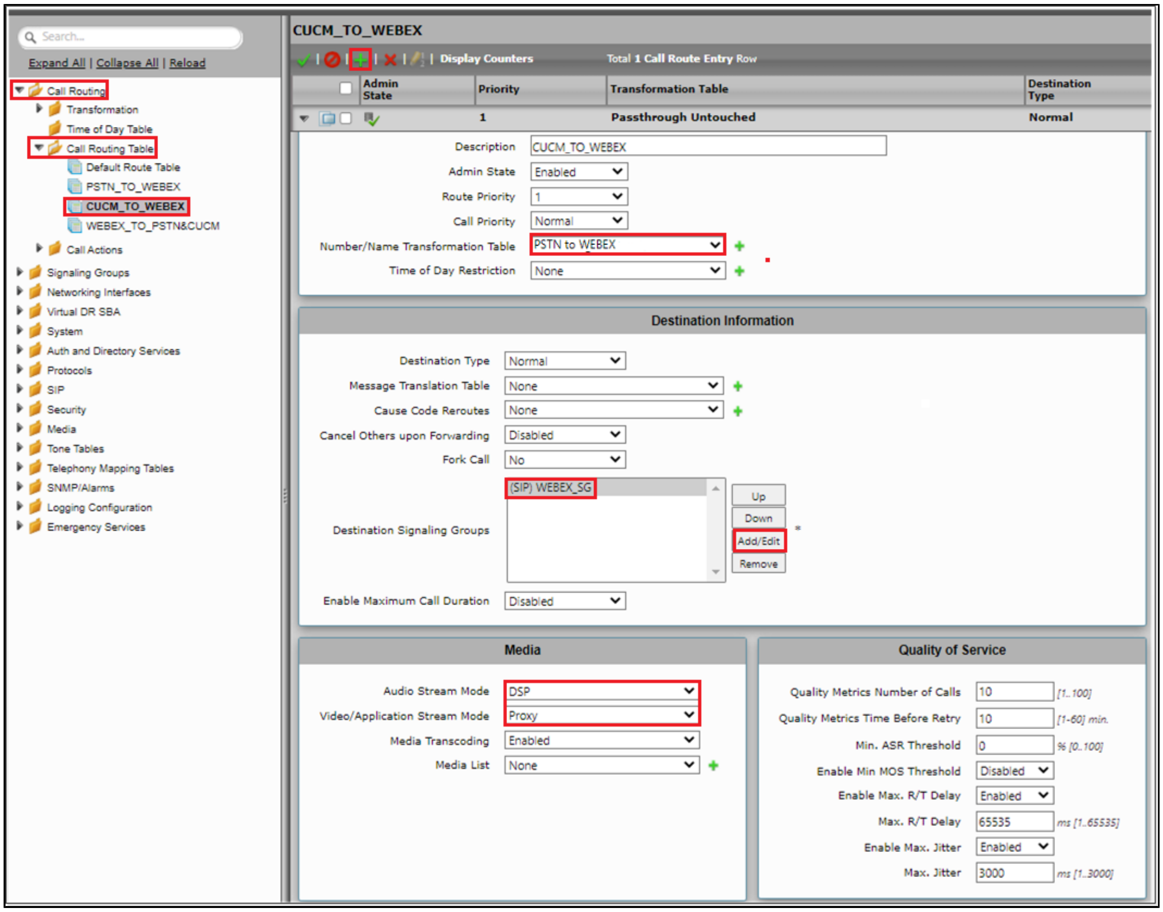
1. Attach the **PSTN to Webex** Transformation Table, which is present in the SBC Edge by default.
2. Click on **Add/Edit** under Destination Signaling Groups, and select Webex_SG.
3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
4. Click OK.



PBX to Webex

From the **Settings** tab, navigate to **Call Routing > Call Routing Table > CUCM_TO_Webex.** Click the + icon to create a Call Routing Table.

1. Attach the **PSTN to Webex** Transformation Table, which is present in the SBC Edge by default.
2. Click on **Add/Edit** under Destination Signaling Group and select Webex_SG.
3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
4. Click OK.

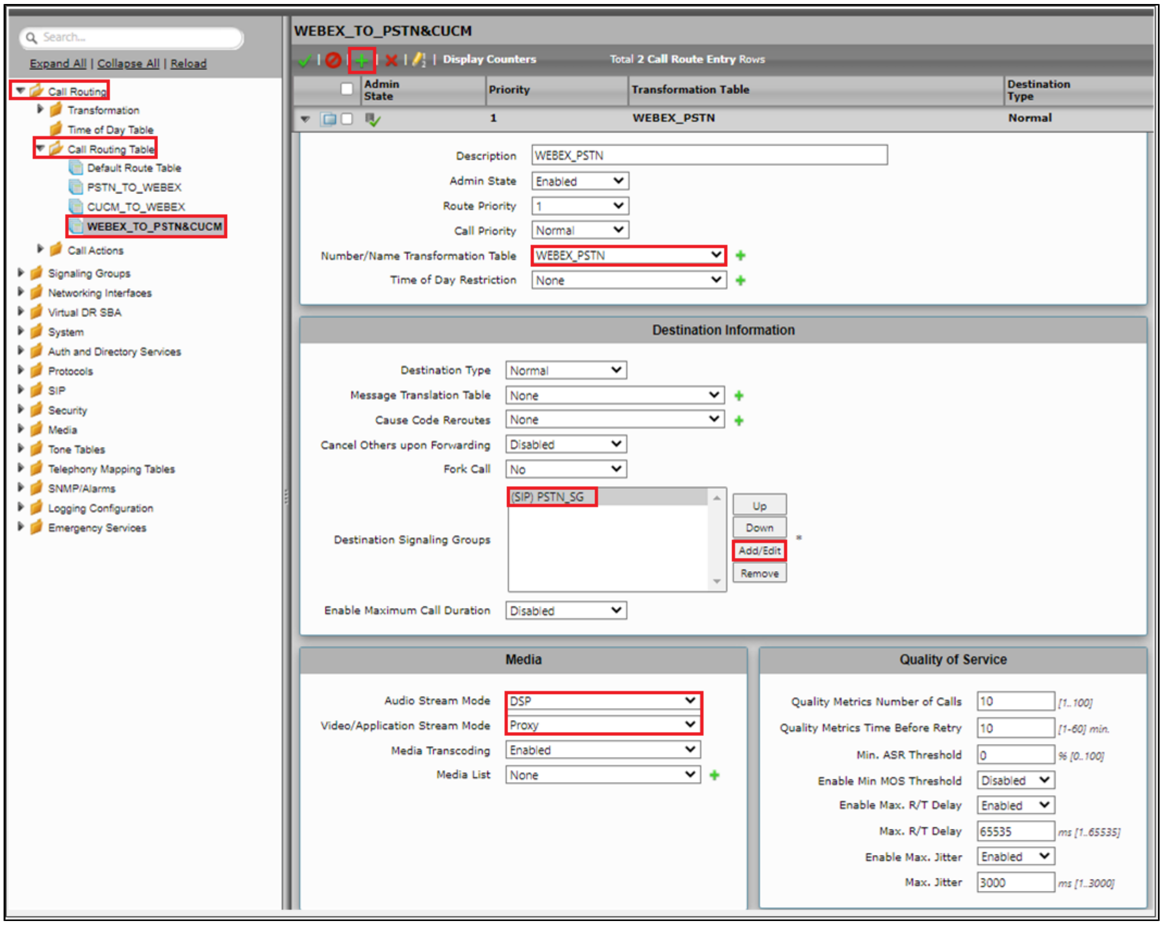


> **Note**
> For Passthrough calls, 'Audio Stream Mode' can be set to 'Proxy preferred over DSP' and enable SRTP on PBX leg.

Webex to PSTN

From the **Settings** tab, navigate to **Call Routing > Call Routing Table > Webex_TO_PSTN&CUCM.** Click the  icon to create a Call Routing Table.

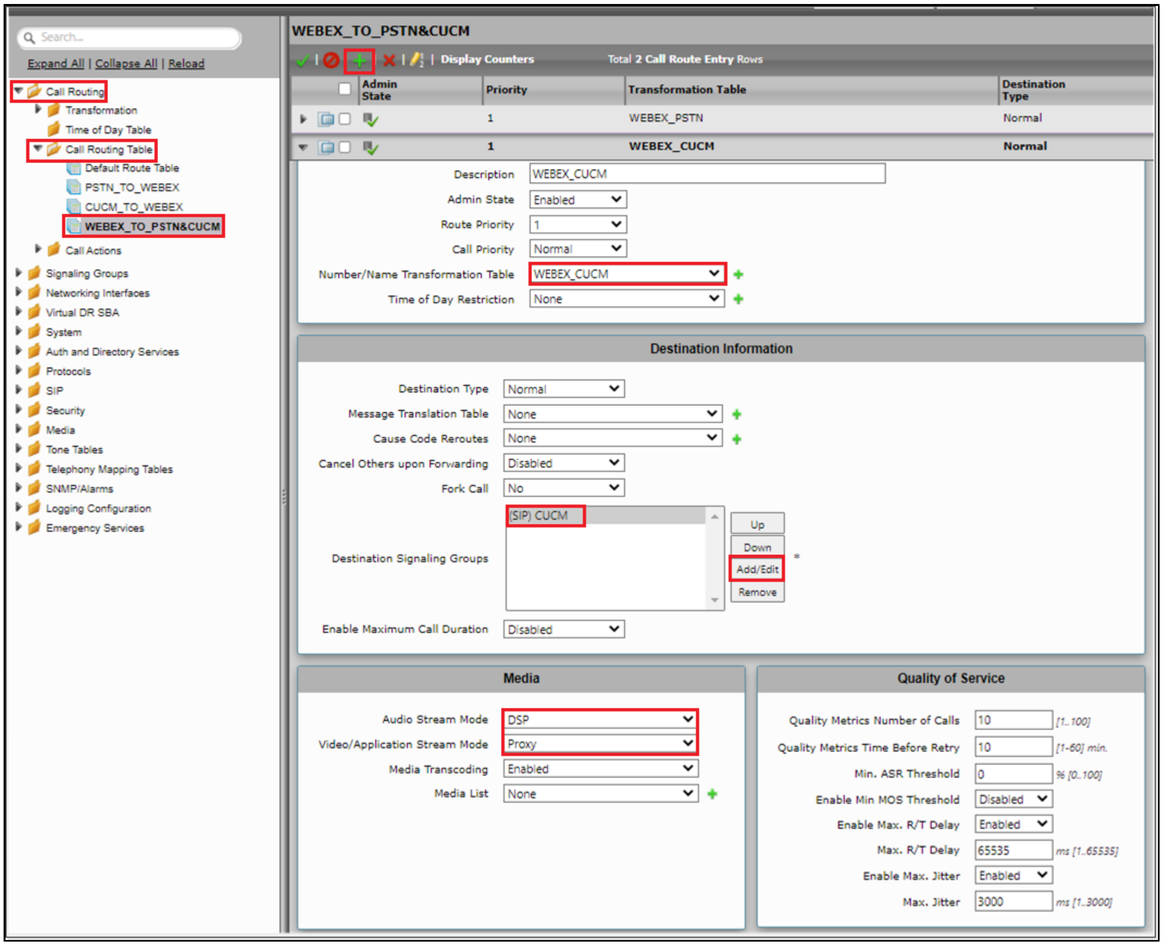
1. Attach the Webex_PSTN Transformation Table to the match the PSTN's number.
2. Click on **Add/Edit** under Destination Signaling Groups, and select PSTN_SG.
3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
4. Click OK.



Webex to PBX

From the **Settings** tab, navigate to **Call Routing > Call Routing Table > Webex_TO_PSTN&CUCM.** Click the + icon to create a Call Routing Table.

1. Attach the Webex_CUCM Transformation Table to the match the PBX's number.
2. Click on **Add/Edit** under Destination Signaling Groups, and select CUCM_SG.
3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
4. Click OK.



Multi-Tenant with Single IP / Multiple Port on SBC

For Multi-Tenant deployment, refer to SBCEdgeConfigurationforCiscoWebexCallingside for Tenant1. Refer to the following configuration for Tenant 2.

TLS Certificates

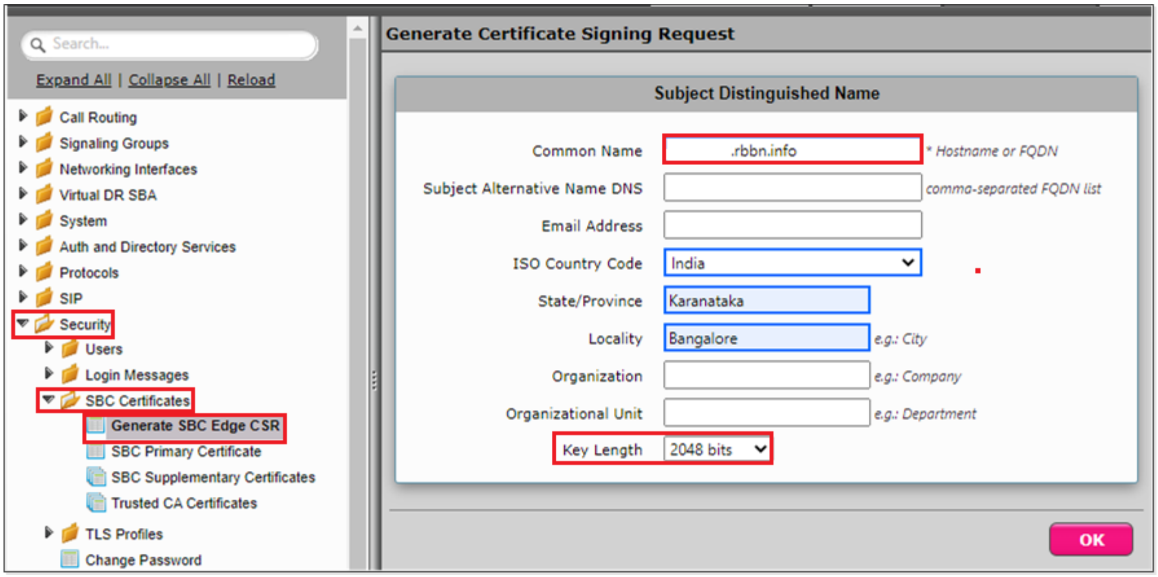
CN-based TLS Certificate for Multiple Tenants

Create the certificate for Ribbon SBC with the CN containing the SBC's FQDN for Tenant 2.

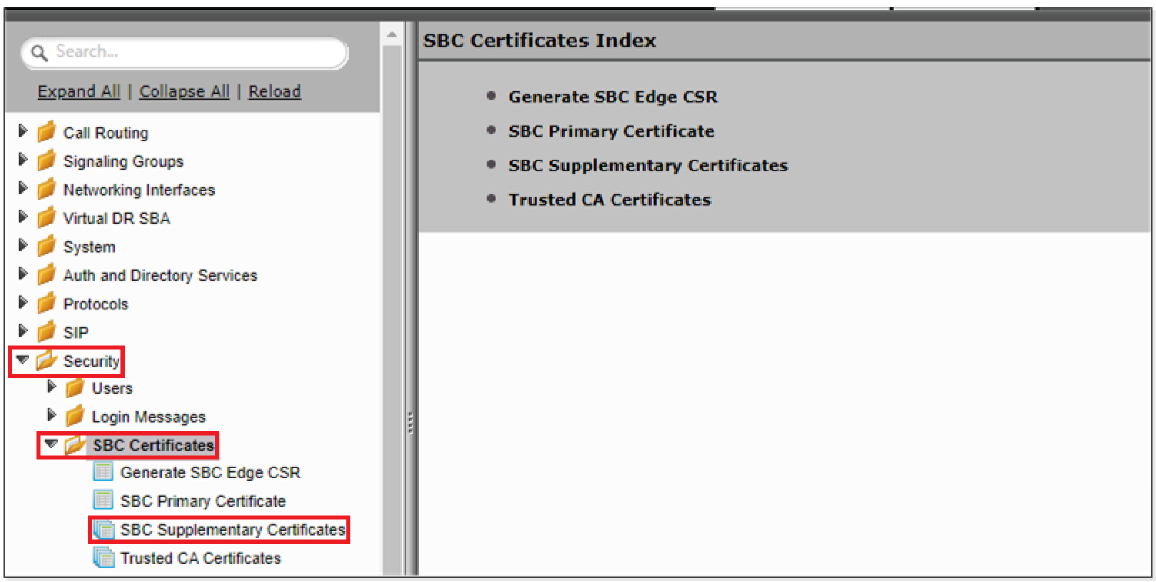
Generating CSR Key for Tenant2 Certificate

From the **Settings** tab, navigate to **Security > SBC Certificates > Generate SBC Edge Certificates.**

1. Provide the Common Name of the Tenant2 that includes Host and Domain.
2. Set the Key Length to 2048 bits.
3. Provide the location information.
4. Click OK.
5. The CSR will be generated and displayed in the result text box.



After generating the certificate, import the Tenant2 certificate under **Settings** tab, navigate to **Security > SBC Certificates > SBC Supplementary Certificate.**



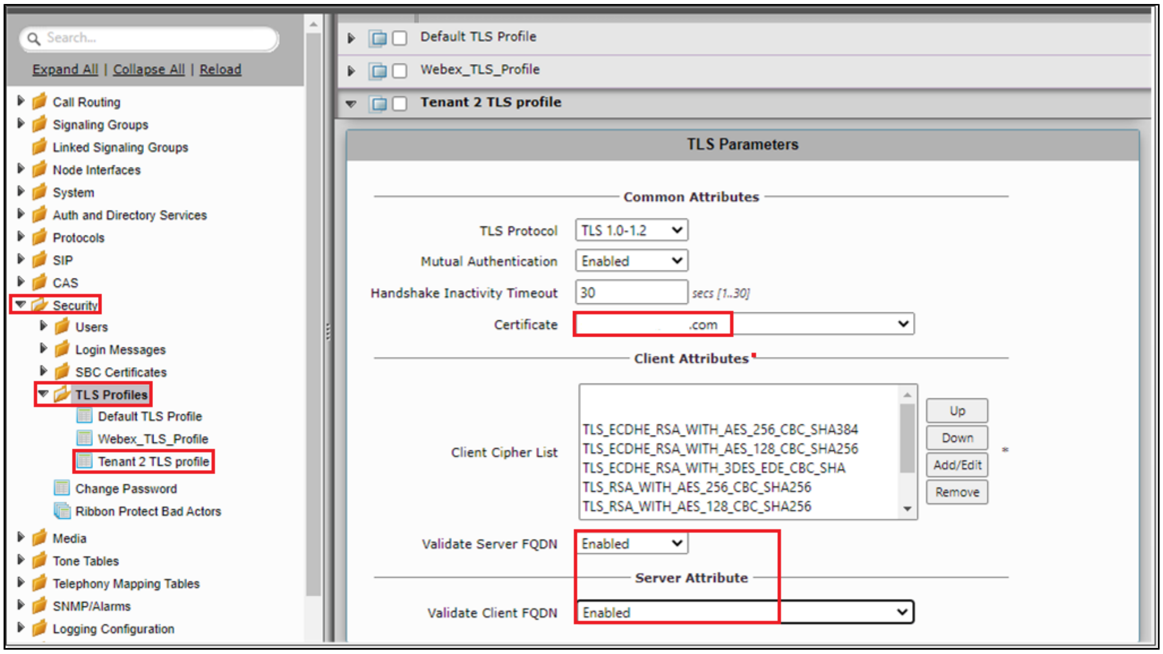
Upload the certificate in the SBC certificate (Refer to SBC Certificate).

Info
The SAN/CN name for the TLS establishment with Webex is CASE SENSITIVE on the Cisco Webex side.

TLS Profile

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

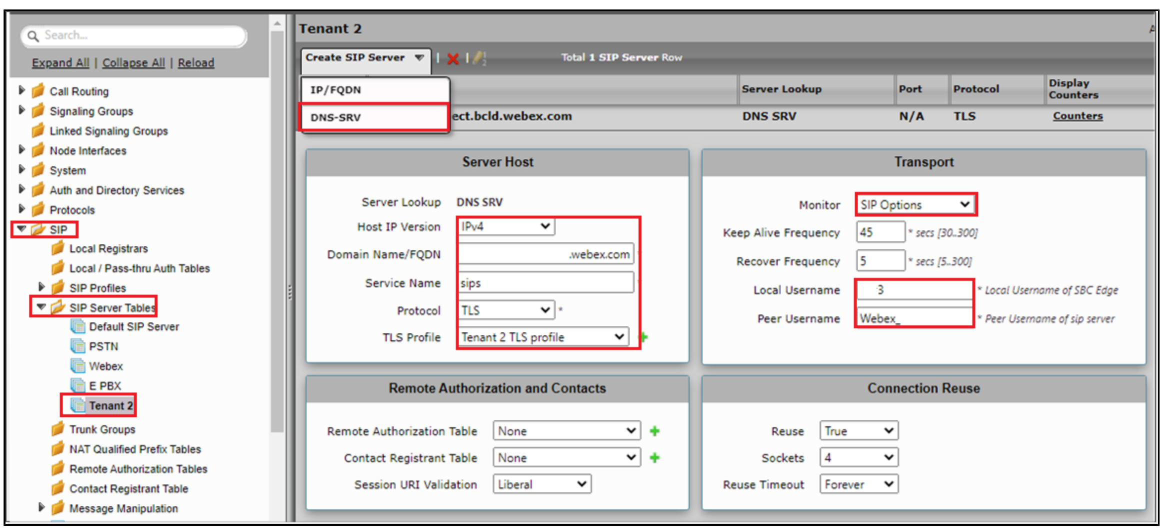
1. From the TLS Protocol drop-down menu, select TLS 1.0-1.2.
2. Attach the certificate which is uploaded in the supplementary certificate.
3. Add the cipher suites that are supported on Cisco Webex.
4. Enable the Validate Server and Client FQDN fields to validate the CN and SAN name in the certificate send by Server and Client.
5. Click OK.



SIP Server Table Tenant2

Create a sip server table similar to the one created before.

1. From the Create SIP Server drop-down menu, select DNS-SRV.
2. Provide the SRV of the Cisco Webex and set the service of the SRV as sips.
3. Select the Protocol as TLS and attach the TLS profile which was created using the Tenant2 certificate.
4. Under the Transport section, enable sip OPTIONS by selecting SIP OPTIONS from the Monitor drop-down menu, and set the Local username as the SBC host name and the Peer Username as Webex.
5. Click OK.



Message Manipulation

IP to FQDN Conversion in P-Asserted-Identity

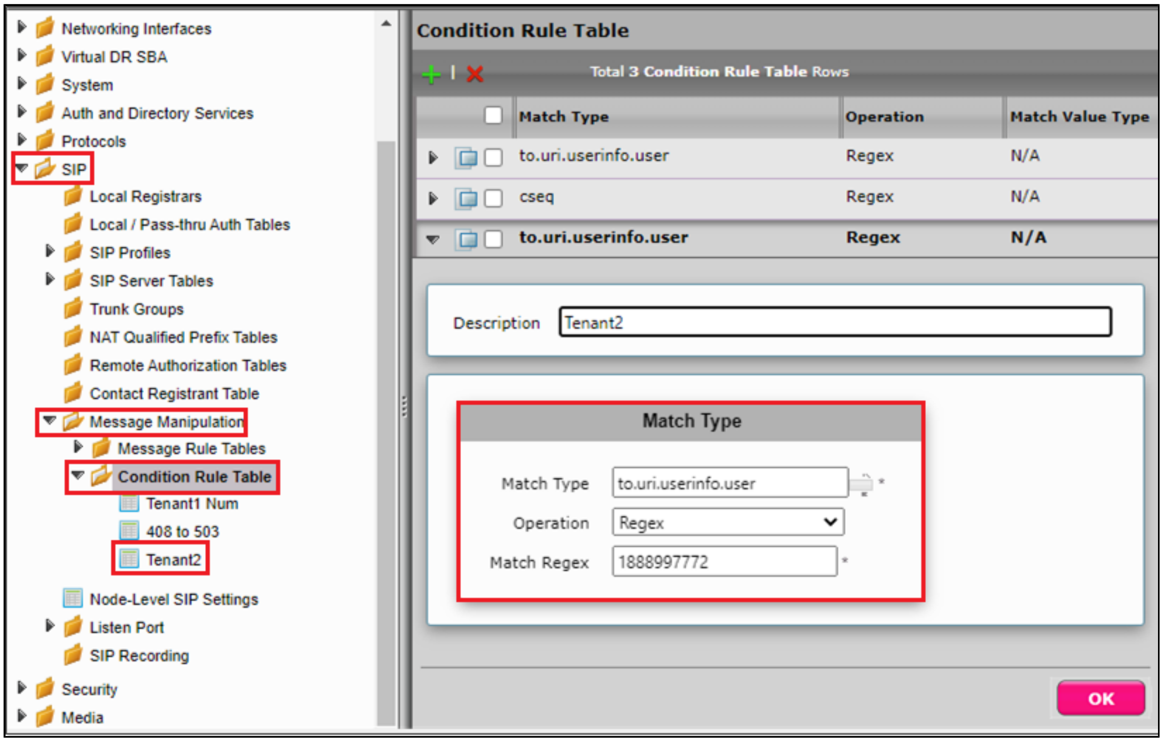
The Message Manipulation is used to convert IP to tenant2's FQDN in the P-Asserted-Identity.

Condition Rule Table for Tenant2

The Condition Rule Table mentioned below is used to match Tenant2 Cisco Webex's number.

From the **Settings** tab, navigate to **SIP > Message Manipulation > Condition Rule Table.** Click the + icon to create a new Condition Rule Table.

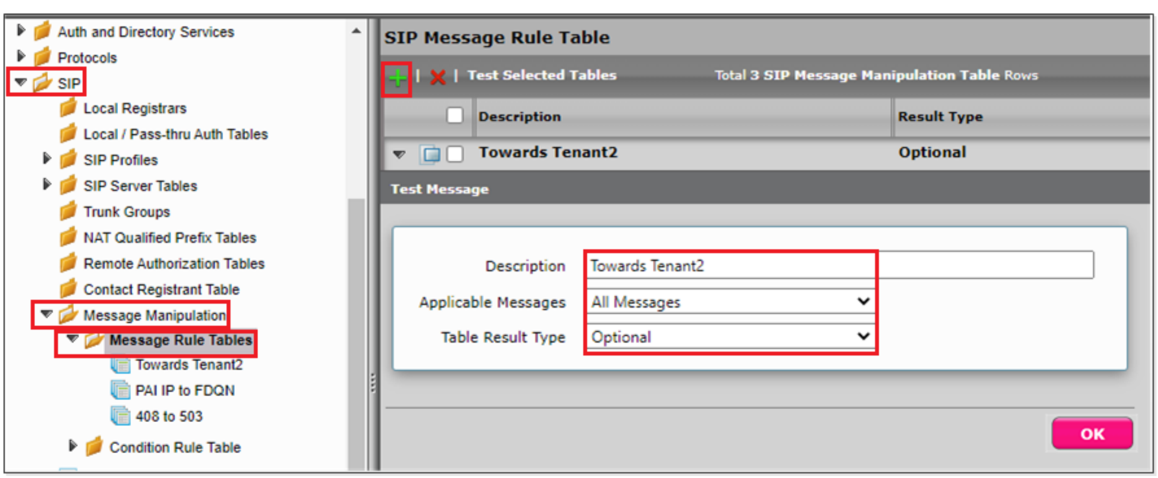
1. Provide a name to Rule table.
2. From the Match Type drop-down menu, select to.uri.userinfo.user.
3. Under Operation, select Regex.
4. Under Match Regex, enter Tenant2's number.
5. Click OK.



Message Rule Table for Tenant2

From the **Settings** tab, navigate to **SIP > Message Manipulation > Message Rule Table**. Click the + icon to create a Message Rule Table.

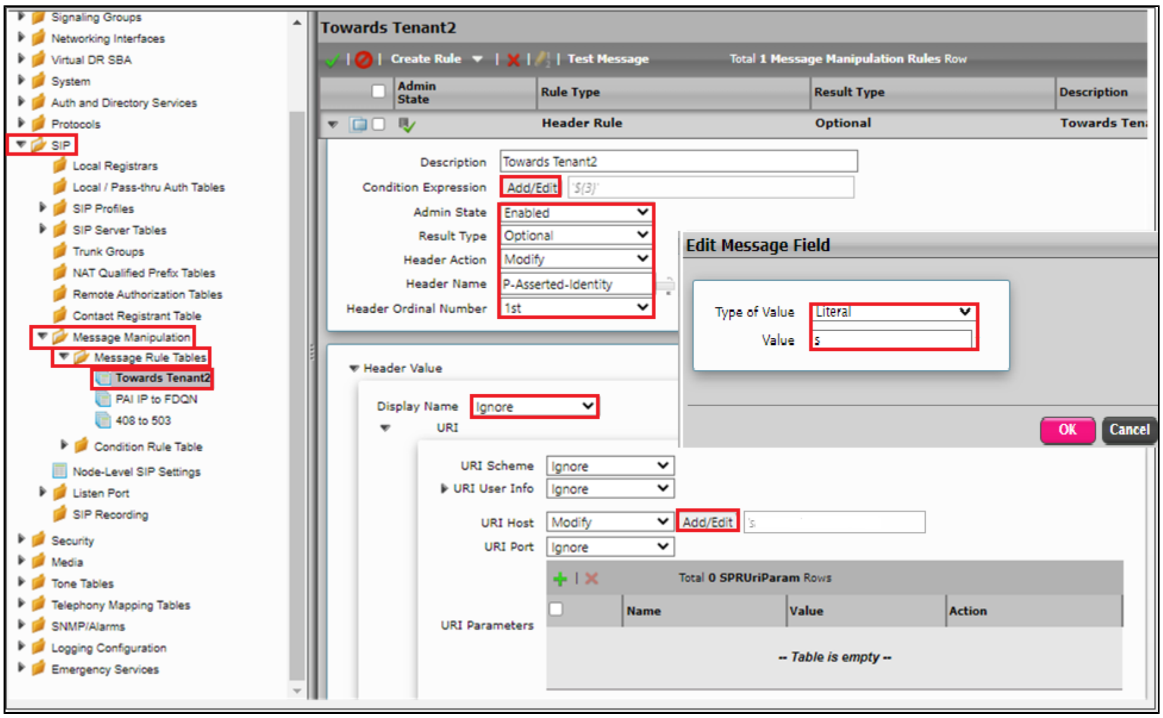
1. Provide a description for the Rule Table.
2. Apply the message rule to All Messages, since the P-Asserted-Identity has to be changed on all the messages.
3. Click Ok.



Message Rule Table Entry for Tenant2

Header Rule:

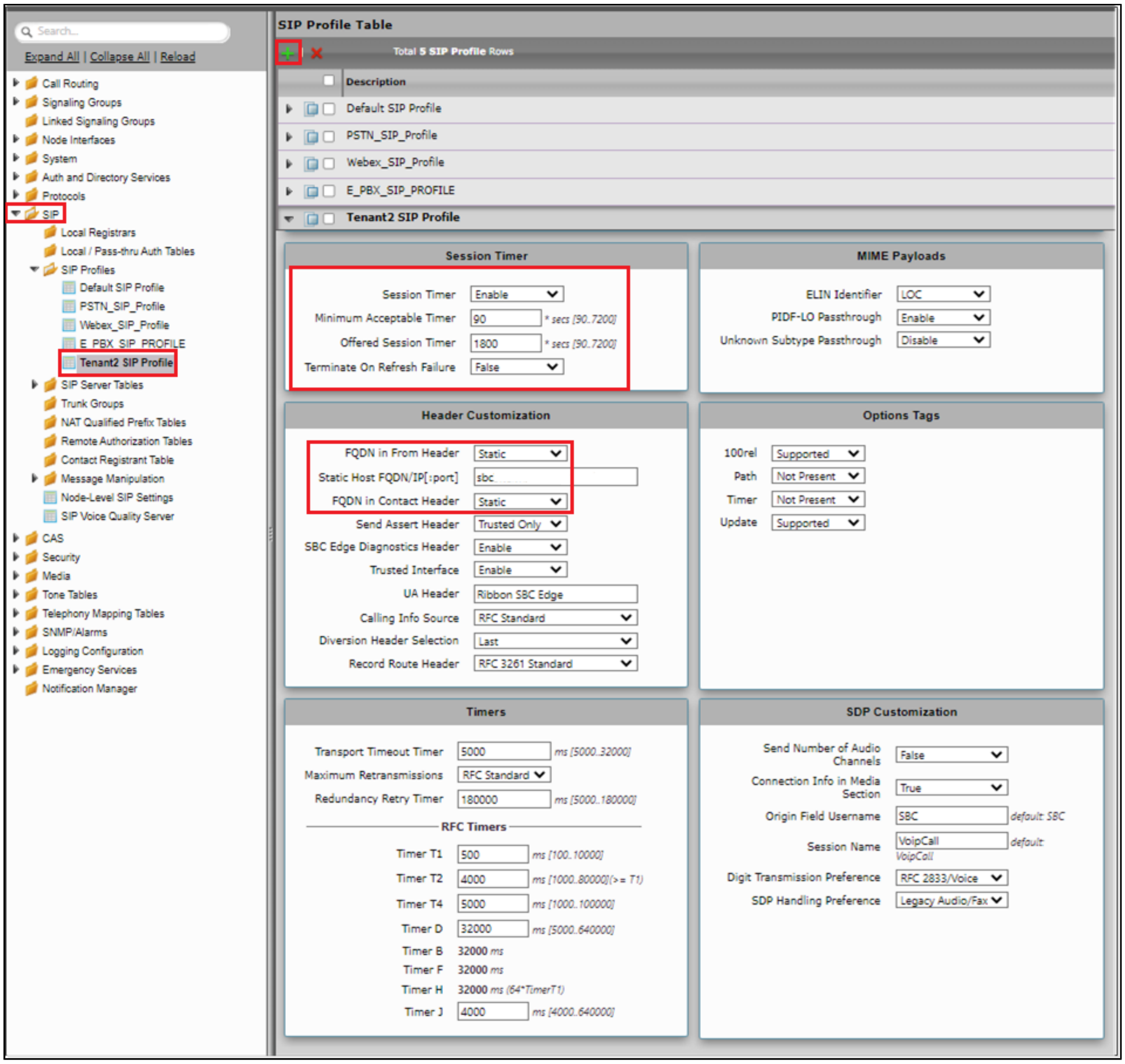
1. Select **Message Rule Tables > Towards Tenant2**.
2. From the Create Rule drop-down menu, select Header Rule.
3. Under Condition Expression> **Add/Edit** and select Message Rule Condition > **Match all Condition** and from the drop-down menu, select the condition rule as **Tenant2**.
4. Select Header Action as Modify and Header Name as **P-Preferrred-Identity**.
5. Under Header Value > URI Host select **Modify**.
6. Click on Add/Edit. Under the Edit Message Field, set Type of Value as **Literal** and Value as **Tenant2's FQDN**.
7. Click OK and Apply.



SIP Profile Webex Tenant2

From the **Settings** tab, navigate to **SIP > SIP Profiles.** Click the  icon to create a new SIP Profile.

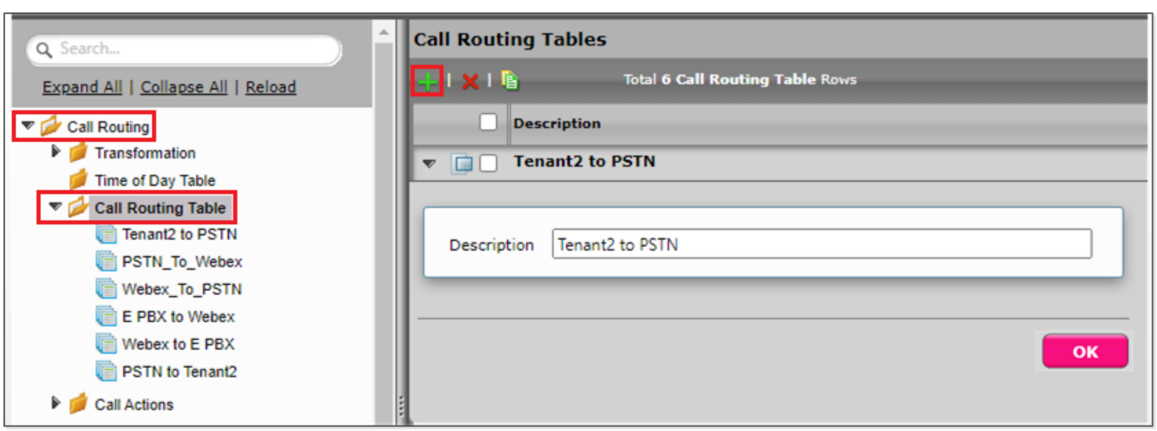
1. Provide a name for the profile in the Description field.
2. Enable Session Timer. This field specifies whether or not to use Session Timer to verify the SIP session.
3. Set Minimum Acceptable Timer to 600 and Offered Session Timer to 3600.
4. From the drop-down menus of both FQDN in From Header and FQDN in Contact Header, select **Static** and enter the Tenant2 FQDN in the Static Host FQDN/IP.
5. Webex is **case-sensitive** for FQDN in the contact header.
6. Click OK.



Call Routing Table Tenant2 to PSTN

From the **Settings** tab, navigate to **Call Routing** > **Call Routing Table.** Click the + icon to create a Call Routing Table.

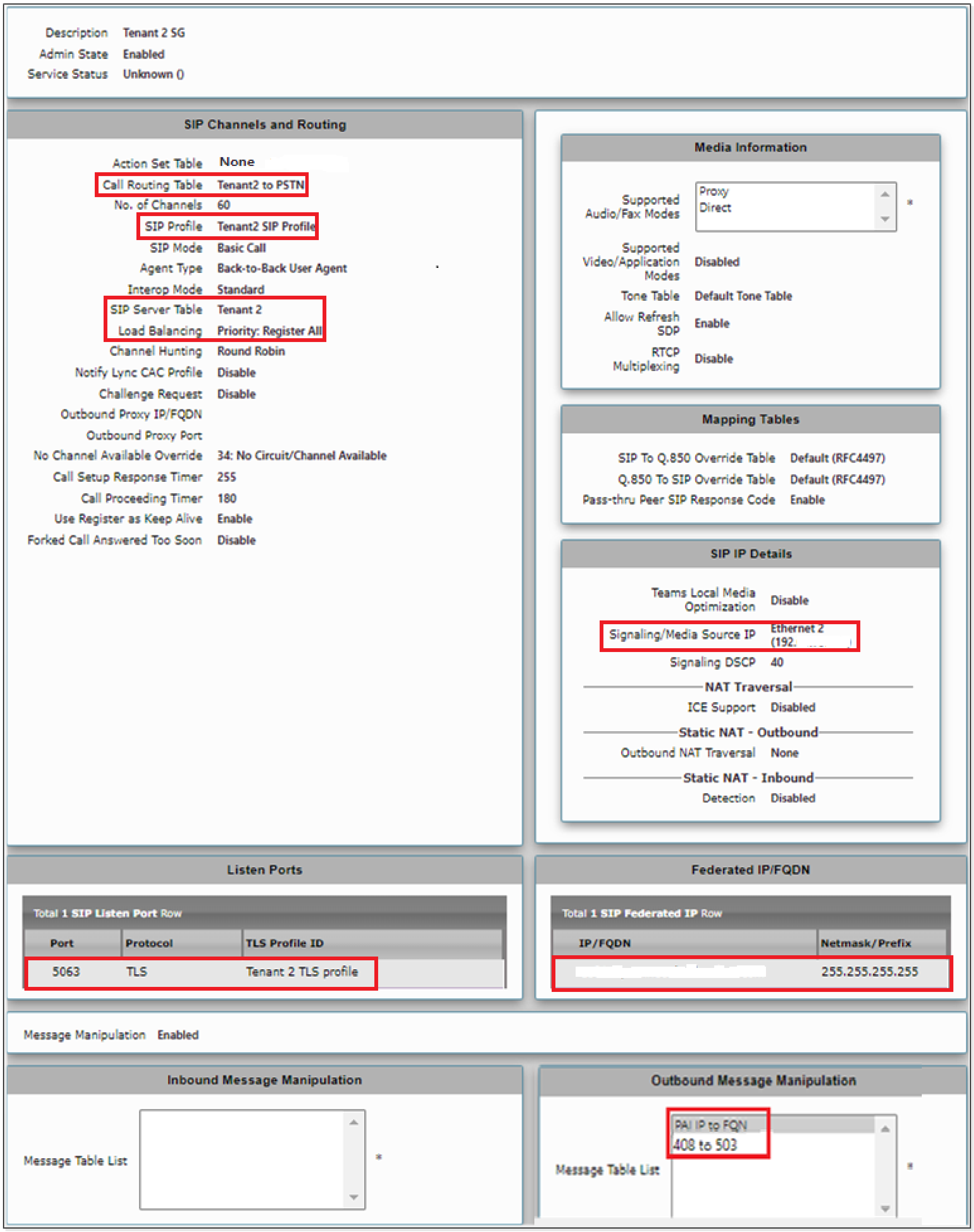
1. Provide a name for the Routing Table.
2. Click OK.



SIP Signaling Group - Webex Tenant2

From the Settings tab, navigate to Signaling Groups. Click Add SIP SG.

1. Attach the Call Routing Table (CallRoutingTableTenant2toPSTN).
2. Attach the Sip Profile (SipProfile).
3. Attach the SIP Server Table (SipServerTableTenant2).
4. Attach the SDES-SRTP Profile which is used for Tenant1 (SDES-SRTPProfile-Webex).
5. Attach the Media List which is used for Tenant1 (MediaList-Webex).
6. Associate the appropriate IP address in the "Signaling/Media Source IP" field which is used for Tenant1.
7. Configure Protocol and Listen Ports in the "Listen Ports" panel.
8. Create an entry in the Federated IP/FQDN panel.
9. Enable Message Manipulation and attach the profile **"Towards Tenant2"** and **"408 to 503"** in the outbound Message Manipulation Table List.
10. Click OK.



> **Note**
> Proxy Local SRTP Crypto Profile ID is available for SBC SWe Edge only. This field is available only when **Proxy with Local SRTP** (Supported only in SWe Edge) is included in the Supported Audio mode list.

Call Routing

Create Transformation Table from Tenant2 to PSTN and PSTN to Tenant2.

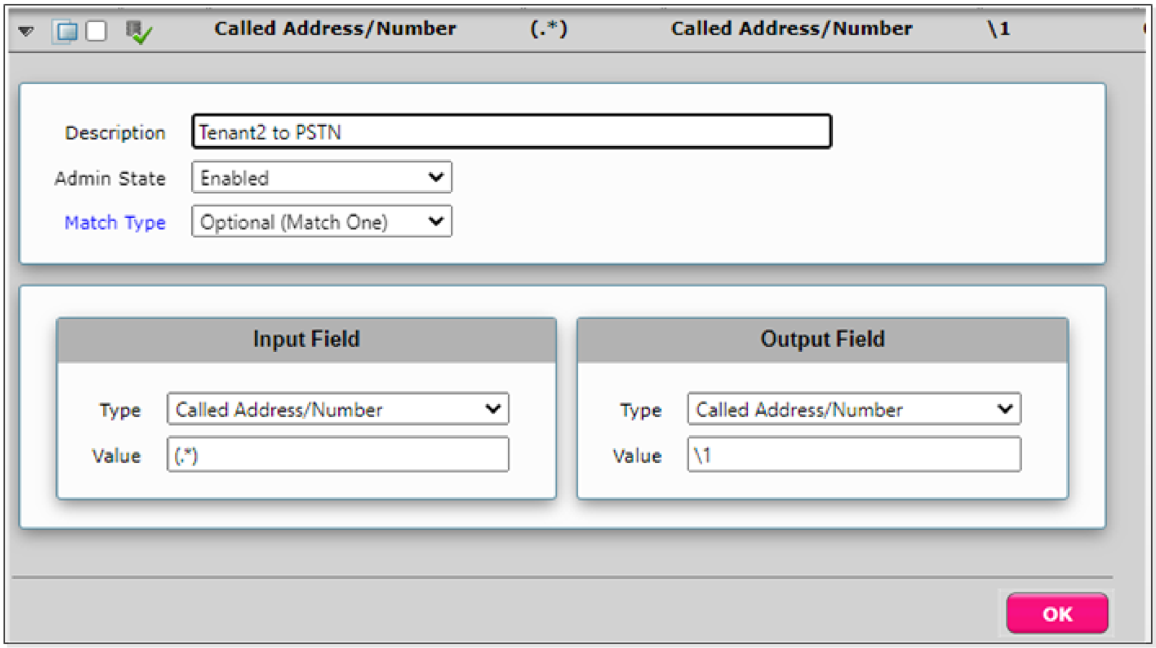
Transformation Table

Tenant2 to PSTN

Create a Transformation Table similar to the one for Tenant1.

From the Settings tab, navigate to **Call Routing > Transformation >** click on the new table created. Click the icon to create a Transformation Table Entry.

1. Under Input Field give the PSTN number that is dialed from the Webex or Passthrough can be used since we are creating a separate Call Routing for Tenant2 to Webex.
2. Click Ok.

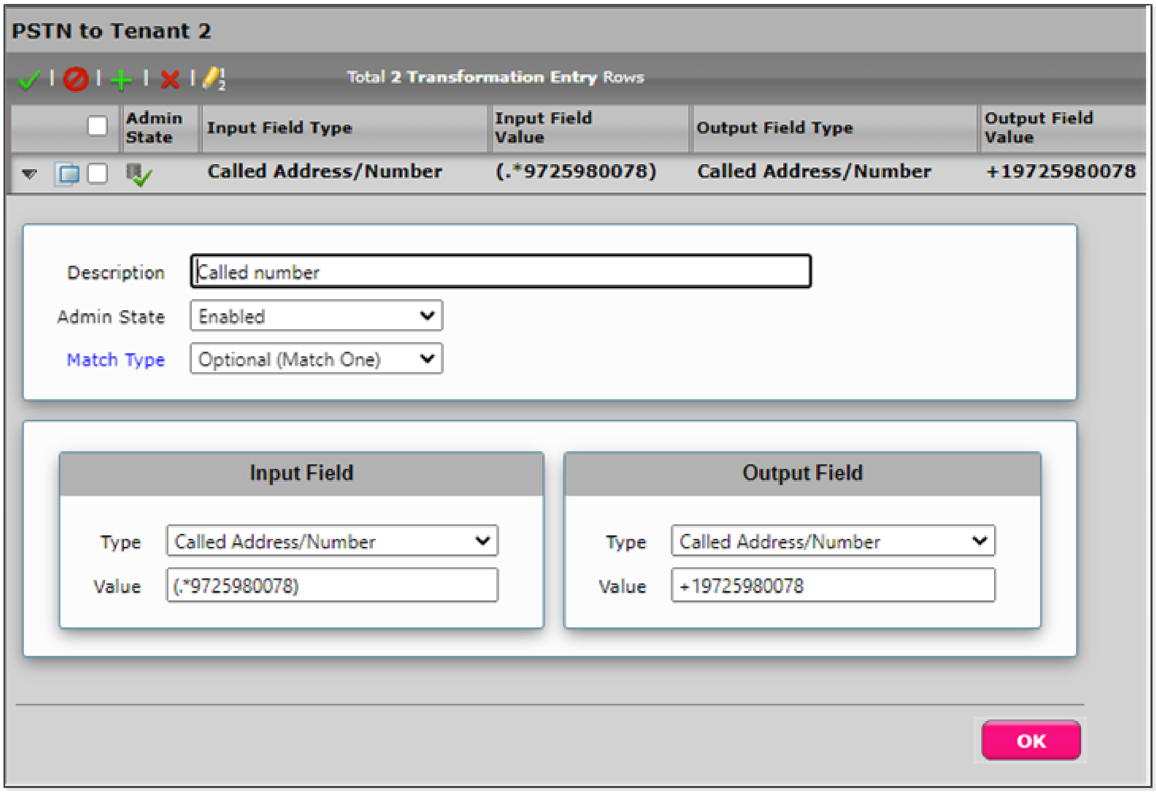


PSTN to Tenant2

Create a Transformation Table.

From the Settings tab, navigate to **Call Routing > Transformation >** click on the new table created. Click the icon to create a Transformation Table Entry.

1. Under Input Field, enter the Tenant2 number of Webex that is dialed from the PSTN.
2. Click OK.

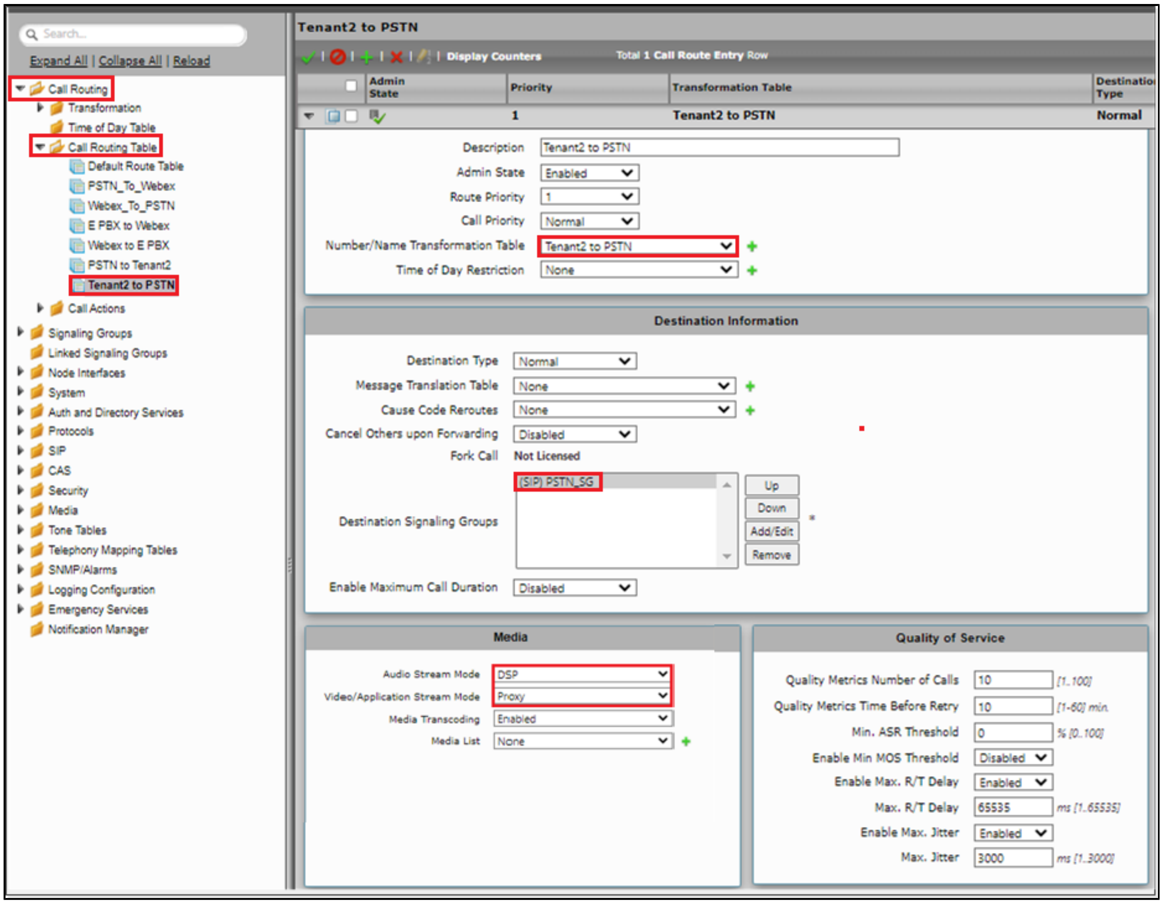


Call Routing Table

Webex Tenant2 to PSTN

From the Settings tab, navigate to **Call Routing > Call Routing Table > Tenant2 to PSTN**. Click the  icon to create a Call Routing Table.

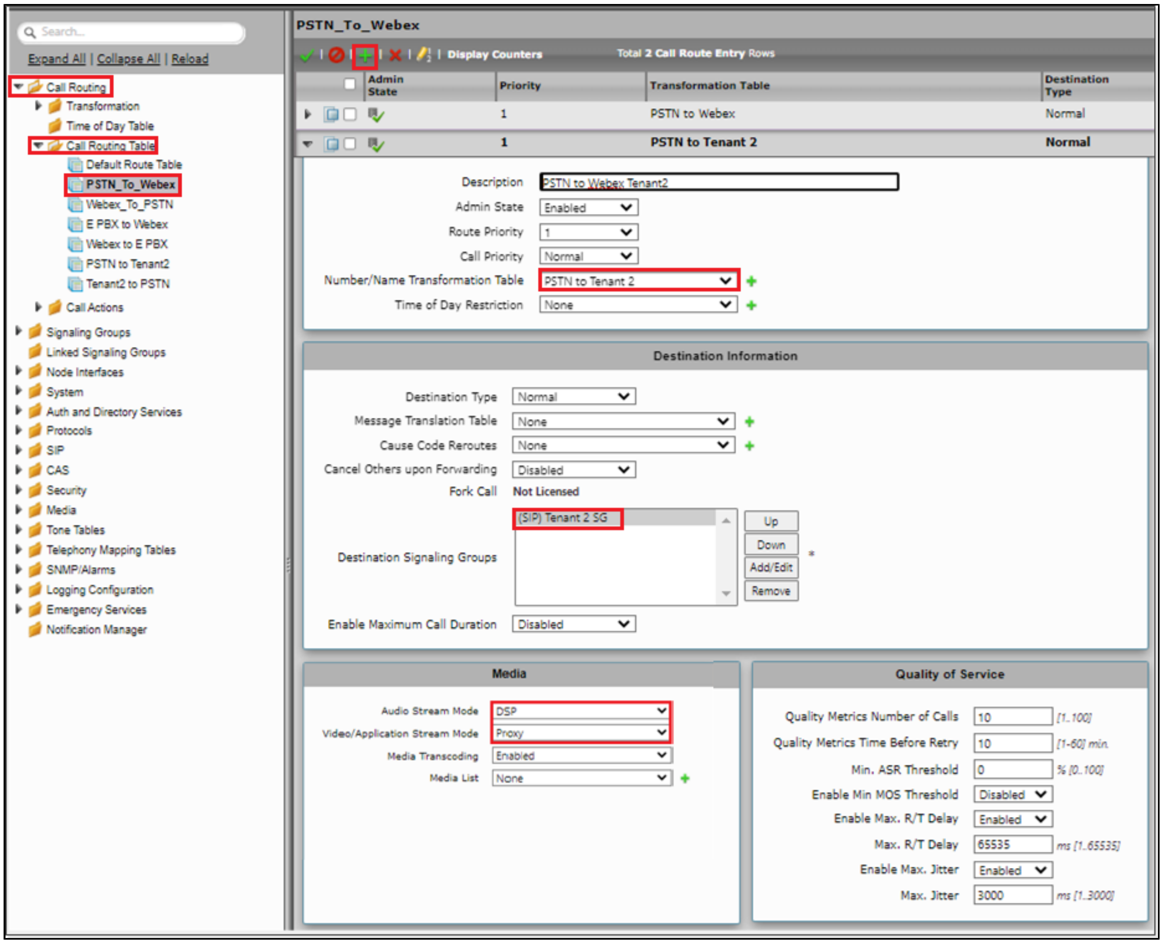
1. Attach the Tenant2 to PSTN Table.
2. Click on **Add/Edit** under Destination Signaling Group and select PSTN_SG.
3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
4. Click OK.



PSTN to Tenant2

In the existing Call Routing table which is created for Tenant1, add another Call Routing Table by clicking on + .

1. Attach the PSTN to Tenant2 Table.
2. Click on **Add/Edit** under Destination Signaling Group and select Tenant 2 SG.
3. Select DSP for Audio Stream Mode and Proxy for Video Stream Mode.
4. Click OK.



Multi-Tenant with Single IP and Port on SBC

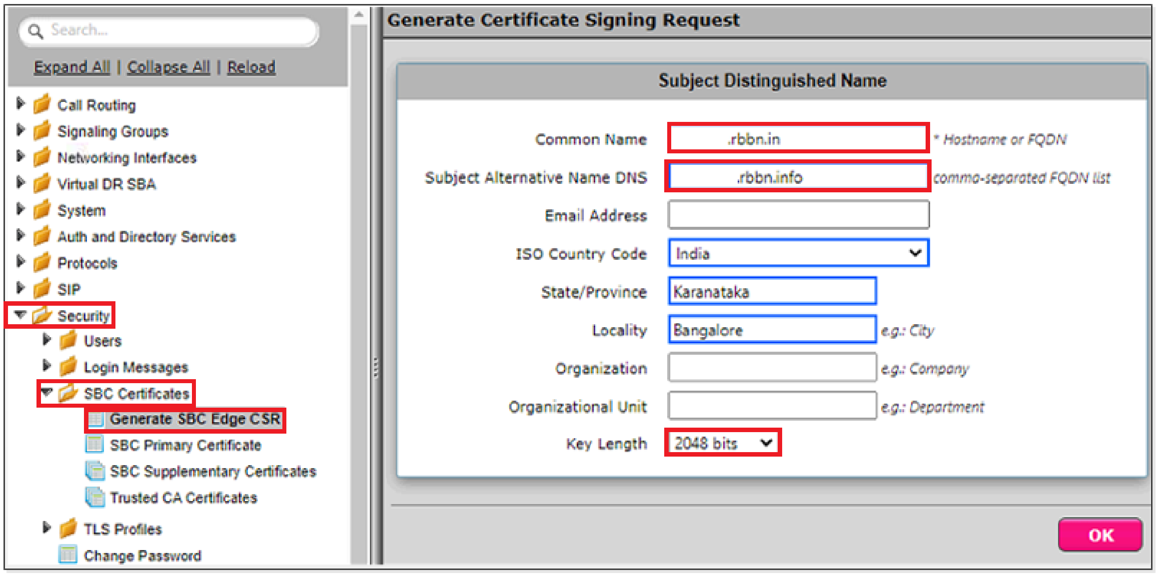
For Multi-Tenant deployment with a single IP/Port, refer to SBCEdgeConfigurationforCiscoWebexCallingside with some changes in the following profiles.

TLS Certificates

SAN-based TLS Certificate for Multiple Tenants

From the **Settings** tab, navigate to **Security > SBC Certificates > Generate SBC Edge Certificates.**

1. Provide the Tenant1's FQDN in the Common Name and Tenant2's FQDN in the Subject Name Alternative.
2. Set the Key Length to 2048 bits.
3. Provide the location information.
4. Click OK.
5. The CSR will be generated and displayed in the result text box.



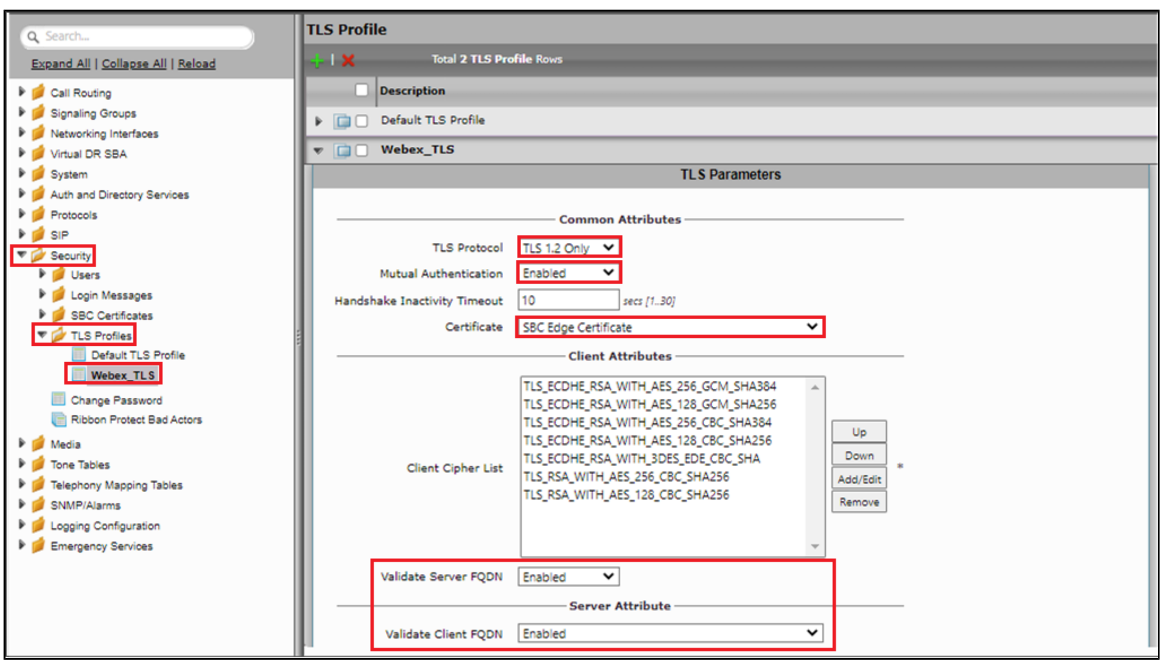
After generating the CSR on Ribbon SBC, provide it to the Certificate Authority and get the SBC certificate.

Upload the certificate in the SBC certificate (Refer SBC Certificate).

TLS Profile

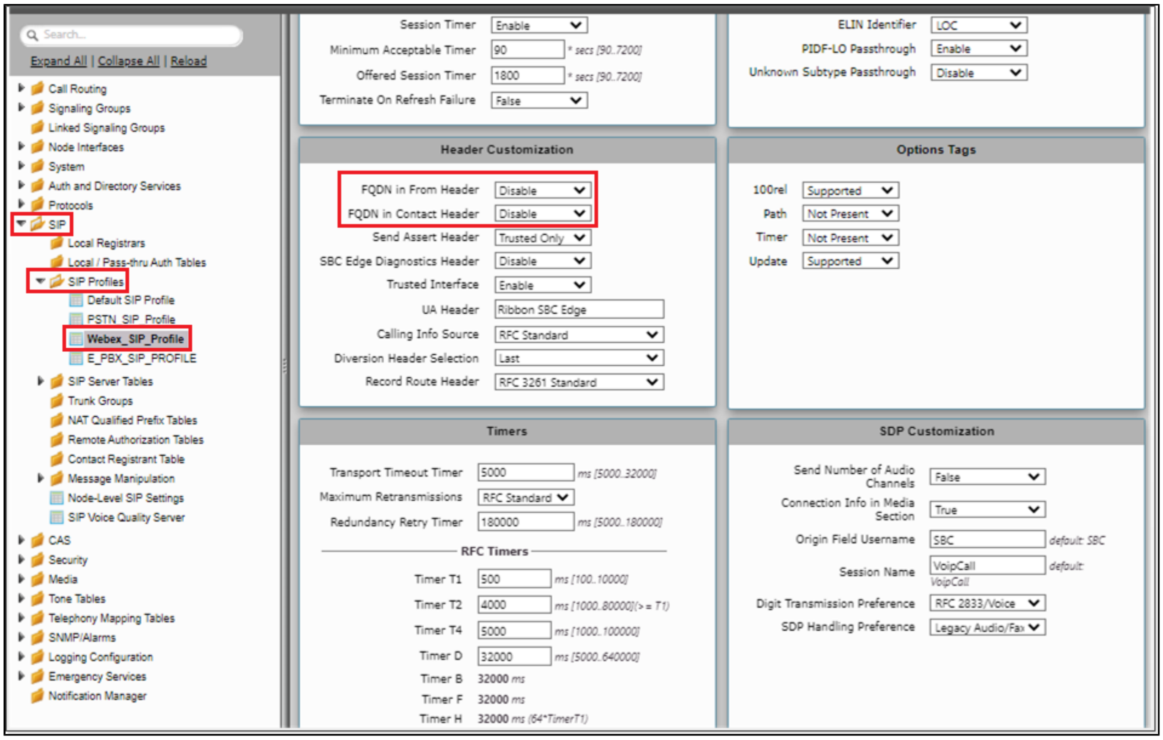
From the **Settings** tab, navigate to **Security > TLS Profiles.** Click the icon to create a new TLS profile.

1. From the TLS Protocol drop-down menu, select TLS 1.0-1.2.
2. Attach the certificate which is uploaded in the SBC certificate.
3. Add the cipher suites that are supported on Cisco Webex.
4. Enable the Validate Server and Client FQDN fields to the validate the CN and SAN name in the certificate sent by Server and Client.
5. Click OK.



SIP Profile

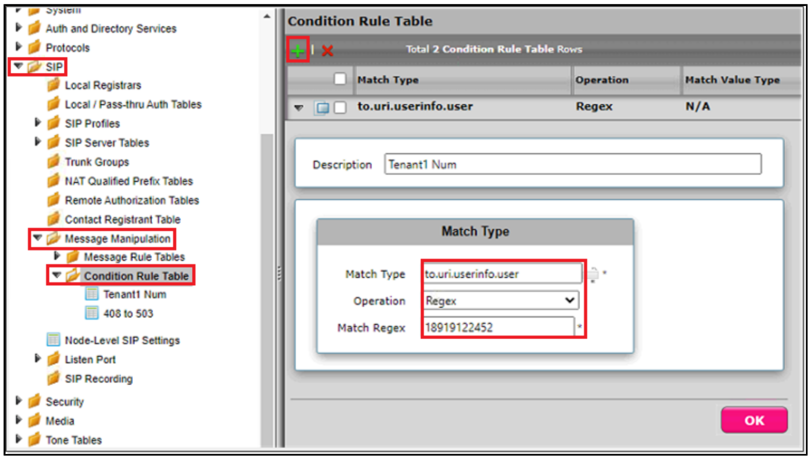
In the existing sip profile which is created in the single tenant, **Disable** the FQDN in **From Header and Contact header**.

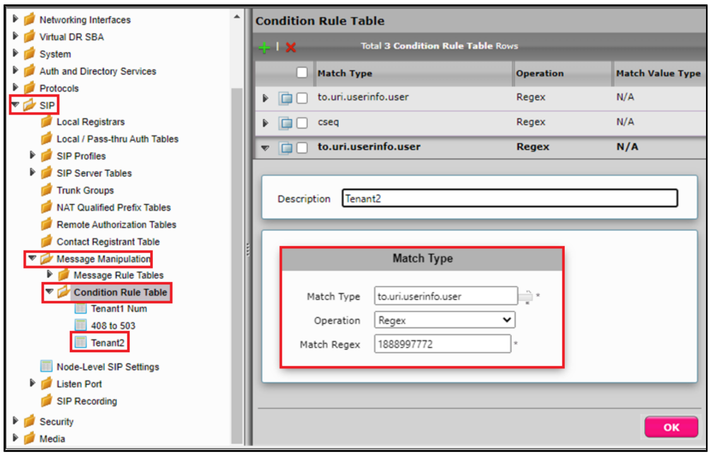


Message Manipulation

Condition Rule Table

Create 2 condition Rule Tables for matching the Tenant1 and Tenant2 Number each as shown in the snapshot below.

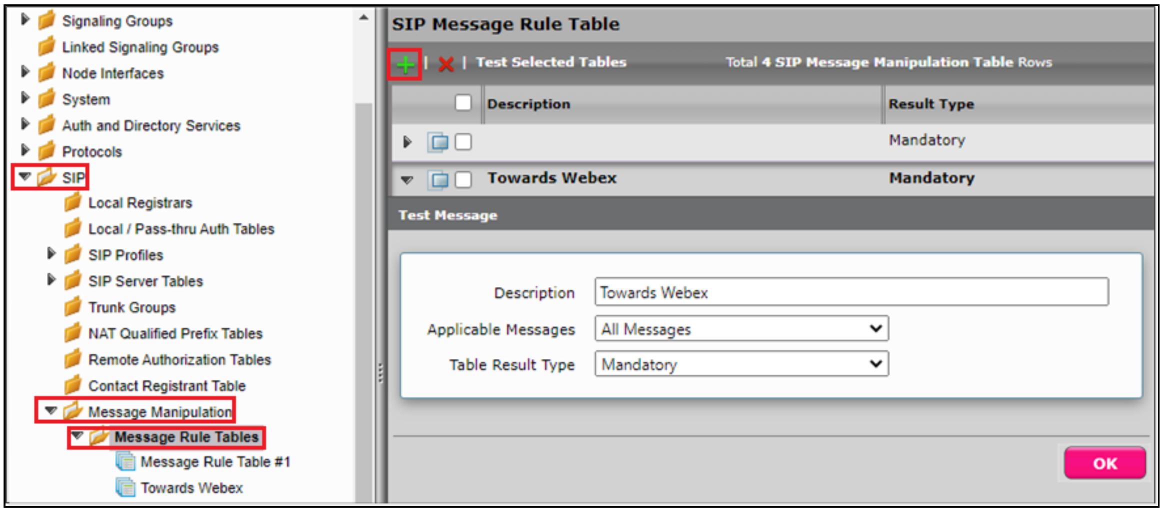




Message Table

From the Settings tab, navigate to SIP > Message Manipulation > Message Rule Table. Click the icon to create a Message Rule Table.

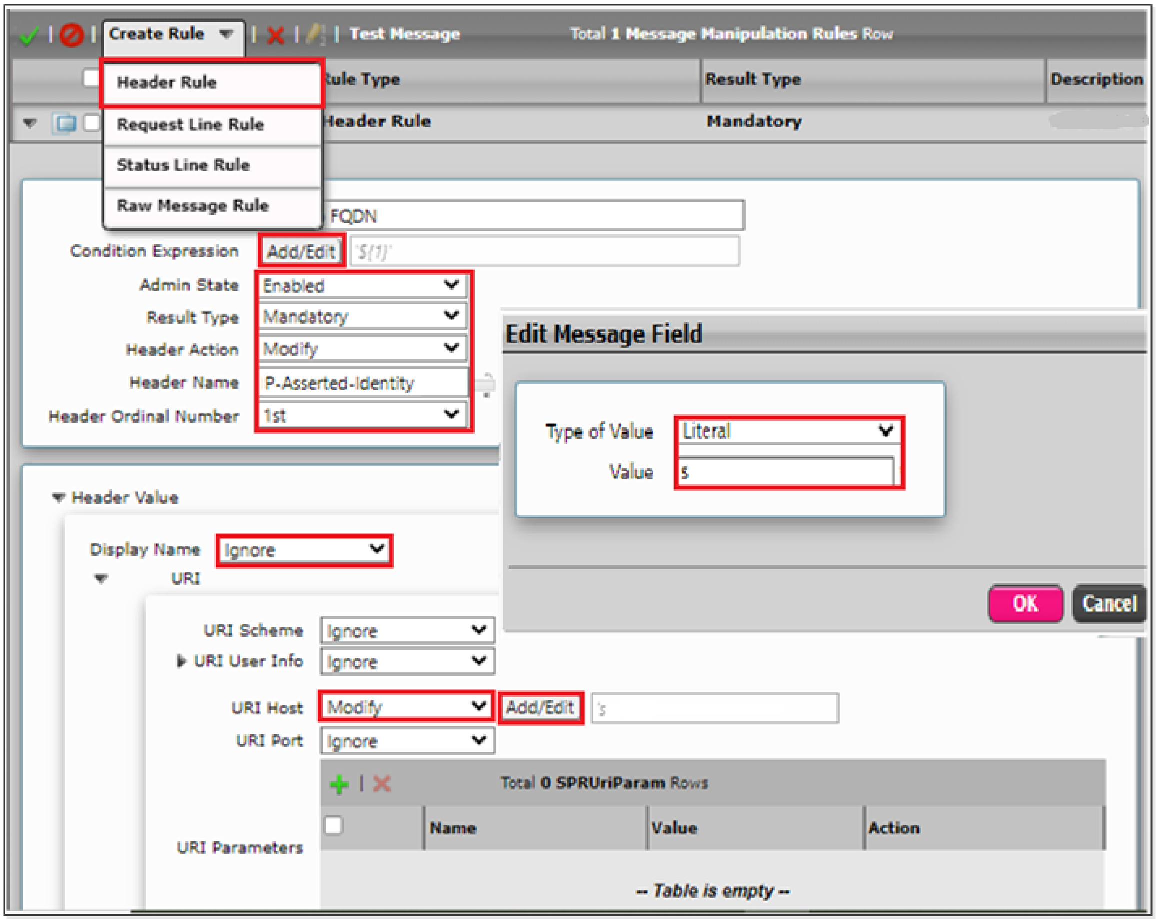
1. Provide a description for the Rule Table.
2. Apply the message rule to All Messages, since the P-Asserted-Identity has to be changed on all the messages.
3. Click OK.



Message Rule Table Entry for Tenant1

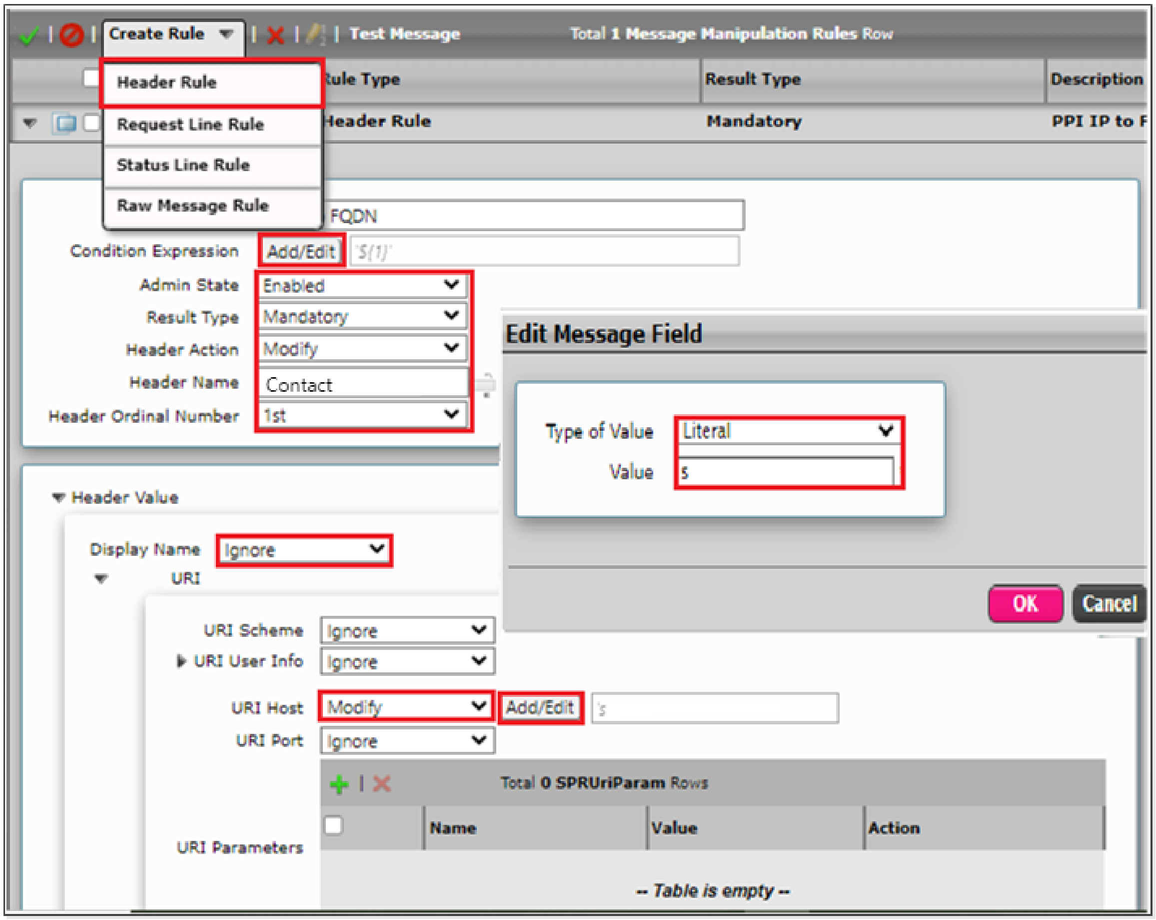
P-Preferrred-Identity Header IP to FQDN

1. Click on the Message Rule Table Towards Webex.
2. From the Create Rule drop-down menu, select Header Rule.
3. Under Condition Expression> **Add/Edit** and select Message Rule Condition > **Match all Condition** and from the drop-down menu, select the condition rule as **Tenant1**.
4. Select Header Action as Modify and Header Name as **P-Preferrred-Identity**.
5. Under Header Value > URI Host select **Modify**.
6. Click on Add/Edit. Under Edit Message Field, set Type of Value as **Literal** and Value as **Tenant1's FQDN**.
7. Click OK and Apply.



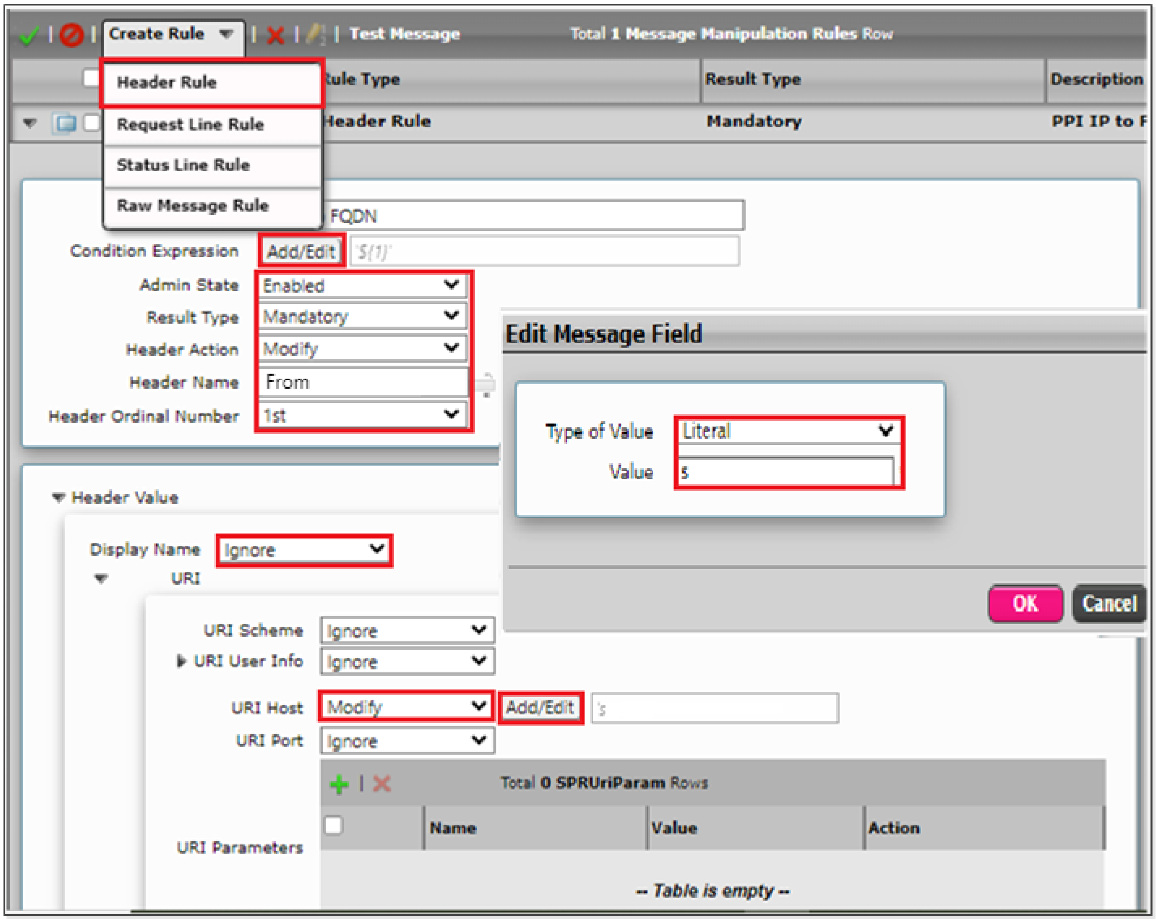
Contact Header IP to FQDN

1. Click on the Message Rule Table Towards Webex.
2. From the Create Rule drop-down menu, select Header Rule.
3. Under Condition Expression> **Add/Edit** and select Message Rule Condition > **Match all Condition** and from the drop-down menu, select the condition rule as **Tenant1**.
4. Select Header Action as Modify and Header Name as **Contact**.
5. Under Header Value > URI Host, select **Modify**.
6. Click on Add/Edit. Under Edit Message Field, set Type of Value as **Literal** and Value as **Tenant1's FQDN**.
7. Click OK and Apply.



From Header IP to FQDN

1. Click on the Message Rule Table Towards Webex.
2. From the Create Rule drop-down menu, select Header Rule.
3. Under Condition Expression> **Add/Edit** and select Message Rule Condition > **Match all Condition** and from the drop-down menu, select the condition rule as **Tenant1**.
4. Select Header Action as Modify and Header Name as **From**.
5. Under Header Value > URI Host, select **Modify**.
6. Click on Add/Edit. Under Edit Message Field, set Type of Value as **Literal** and Value as **Tenant1's FQDN**.
7. Click OK and Apply.

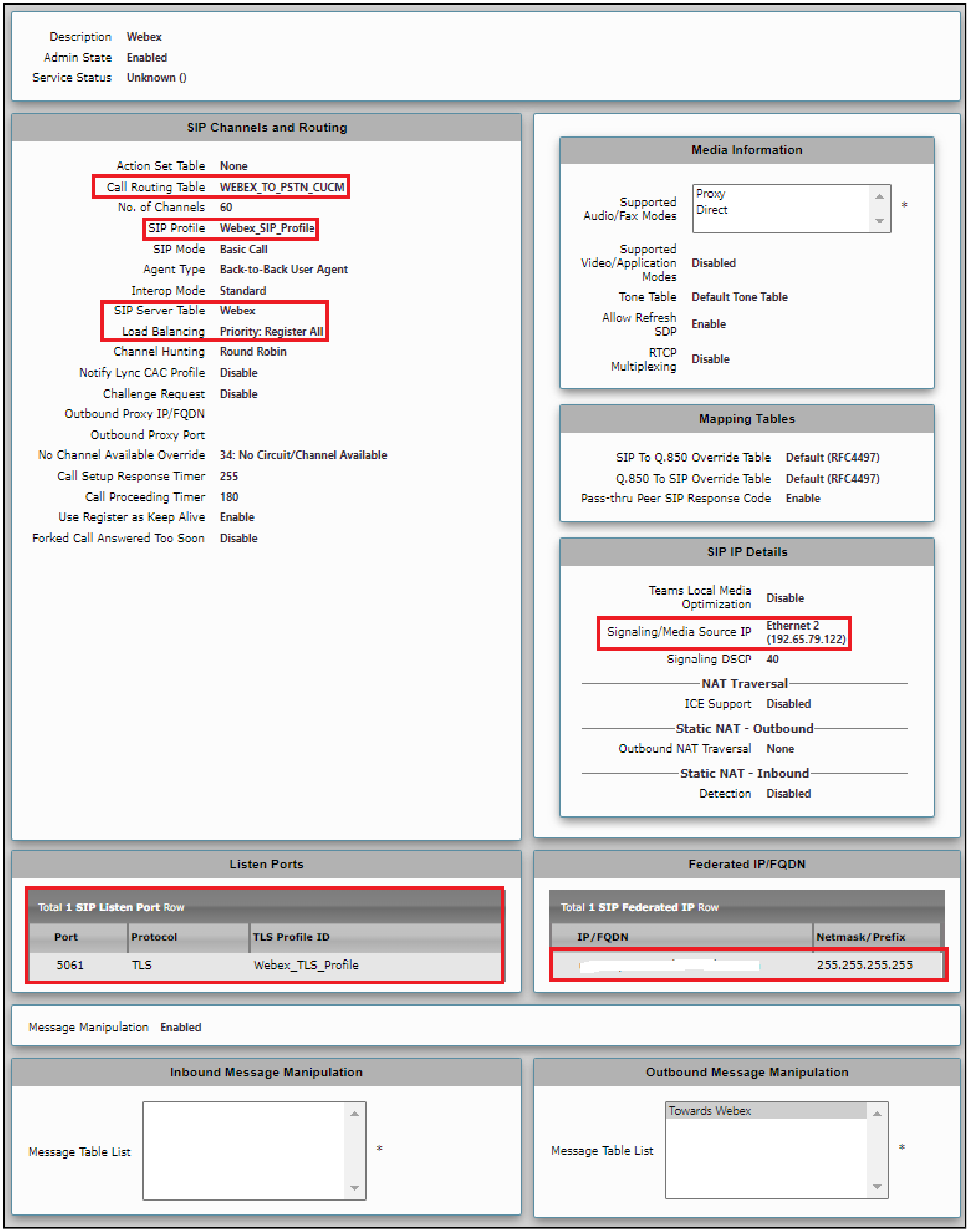


Note
Message Rule Table Entry for Tenant2:

1. Attach the Tenant2 Condition Rule Table.
2. Edit Message Field, set Type of Value as Literal and Value as Tenant2's FQDN.

Signaling Group

- The same Signaling Group can be used by attaching the newly created **SIP Profile** and **Message manipulation.**
- Attach the newly created **TLS profile** in the existing **sip server table** which is used for single tenant configuration.
- The same Call Routing Table can be used which is used for single tenant configuration.
- Both Tenant FQDN will be using the same listen port.



Note

The same Call Routing can be used which is used in the Single Tenant Configuration by adding an Transformation table entry in PSTN and PBX towards Webex to match the Tenant2 number.

Multi-Tenant with Multiple IP and Port on SBC

- For Multi-Tenant deployment with Multiple IP and Port, you can refer to SBCEdgeConfigurationforCiscoWebexCallingside for Tenant1. For Tenant 2, refer to Multi-TenantwithSingleIP/MultiplePortonSBC.
- For Multi-Tenant with Multiple IP and Port, the same configuration above can be used by changing the signaling/media Source IP on 'SIP Signaling Group - Webex Tenant2'.
- If multiple Webex tenants are in same 'Webex control hub location' and when the SBC's source ethernet IPs are in different networks, it is recommended to configure the static route using 'different netmasks' for the same destination (Location).

Cisco Webex Calling Configuration

For configuration on Cisco Webex, visit https://help.Webex.com/.

Supplementary Services and Features Coverage

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

Sr. No.	Supplementary Services/ Features	Coverage
1	Basic Call Setup & Termination	✓
2	Call Transfer (Attended/ Consultative)	✓
3	Call Transfer (Unattended/ Blind)	✓
4	TLS trunk connections	✓
5	Load Balancing (SRV based)	✓
6	Trunk Monitoring	✓
7	Media encryption	✓
8	Voice Transcoding	✓
9	Multi-tenancy	✓
10	Call Park/Retrieve	✓
11	Video Calls	✓
12	Fax	✓
13	Calling Line ID	✓
14	DTMF	✓
15	Session Audit	✓
16	Call Diversion	✓

Legend

Supported	✓
Not Supported	✗

Caveats

Note the following items in relation to this Interop - these are either limitations, untested elements or useful information pertaining to the interoperability.

STUN packets (ICE) not received from Webex during the Ringback stage

- For Webex to PSTN calls with the ICE mode enabled, the SBC doesn't receive any STUN packets from Webex. Due to this, the SBC rejects the call with 5XX response.
- As a workaround solution, it is recommended to enable 'static NAT' on the Webex signaling group.

Not blocklisting the Webex node when the SBC receives 503 for the INVITE

- When PSTN calls Webex client and the Webex node sends a 503 response, the INVITE goes to the next available Webex node but the SBC does not blocklist the Webex node. But this status will be for a short period only till OPTIONS is sent.
- This issue does not have any impact on calls.

Displaying the status/history of the nodes

- When the SBC receives 503/408/no response for SIP Options from Webex, the SBC generates an alarm in the Monitor tab but there is no status (up/down) displayed for that particular node.
- Functionality is working fine but from a serviceability perspective, the SBC is unable to display the node status/history.

TTL issue

- The SBC is not adhering to the Time To Live (TTL) for sending the SRV query.
- This issue is observed only in SBC 1K/2K and not observed in SWe Edge.

SBC response to OPTIONS during drain mode

- When the SIP signaling group is in drain mode, the SBC is not responding with 503 Service Unavailable for incoming SIP OPTIONS.
- This issue is observed only in SBC 1K/2K and not observed in SWe Edge.

SBC supports only Proxy mode for Video calls

- The SBC supports only Proxy mode for Video calls, so the SBC relays Crypto lines without decrypting or encrypting.
- As a workaround, it is suggested to use SRTP on the Enterprise network.

These issues will be addressed by Ribbon in their upcoming releases.

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/services/ribbon-support-portal

References

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

For detailed information about Cisco Webex, visit: https://www.Webex.com/.

Conclusion

This Interoperability Guide describes successful configuration for Ribbon SBC Edge interop involving Cisco Webex Calling for customer deployments.

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 - there may be additional configuration changes required to suit the exact deployment environment.