Ribbon SBC Edge Configuration with OBS (TLS)

Table of Contents

Document Overview

This document provides a configuration guide for Ribbon SBC Edge Series (Session Border Controller) when connecting to OBS Business Talk (BTIP) SIP trunk.

This configuration guide supports features given in the BTIP North Profile Compliancy and Compliance tests documents.

Ribbon has configured the BTIP side in a such manner it doesn't matter the 3rd party system connected on the SBC.

The SBC Edge is certified by Orange Business Services as a '**certified Enterprise SBC'**.

- For additional information on OBS, please visit https://www.orange-business.com/en/products/business-talk
- For additional information on Ribbon SBC Edge, please visit https://ribboncommunications.com/

Introduction

The interoperability compliance testing focuses on verifying inbound and outbound call flows between Ribbon SBC Edge and OBS.

Audience

This is a technical document intended for telecommunications engineers for configuring both the Ribbon SBC and the third-party product. Users will perform steps to navigate the third-party products as well as the Ribbon SBC Command Line Interface (CLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP is also essential for completing the configuration and for troubleshooting, if necessary.

> 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.

Requirements

The following equipment and software were used for the sample configuration:

	Equipment	Software Version
Ribbon Communications	Ribbon SBC SWE-Lite	9.0.0
Third-party Equipment	CISCO CUCM	12.5
Other software	VentaFax	7.3.233.582I

Reference Configuration

The following reference configuration shows connectivity between the third-party and Ribbon SBC Edge.

Figure 1: SBC Edge IP Diagram

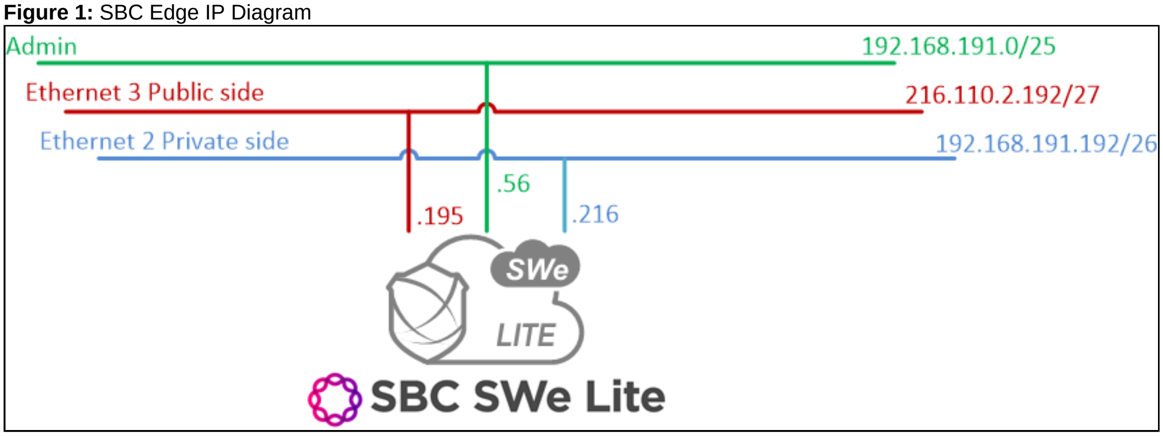
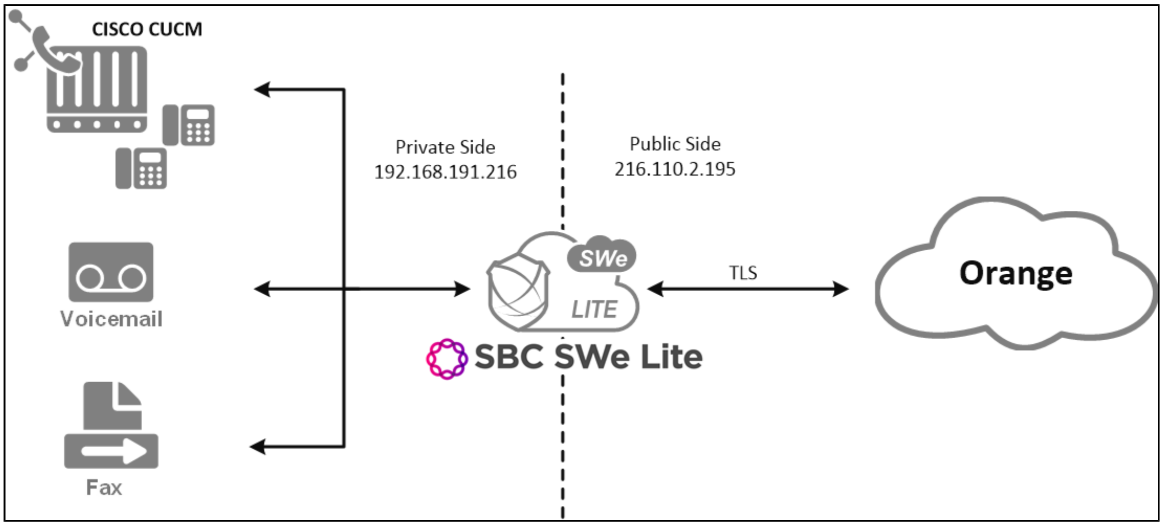


Figure 2: Topology



Support

For any questions regarding this document or its content, please contact your maintenance and support provider.

Third-Party Product Features

Table 1: Product Features

- Basic Call
- Long Duration Call + CLIR
- Call Cancellation
- DTMF + Voicemail
- Transfer
  - Supervised + MOH
  - Blind
- Forward
  - Unconditional
  - Busy
  - No Answer
- Busy Call
- Not Answered Call
- Conference X3
- Prehook
  - With Transfer
  - With Forward
- Call Parking
- Call Pickup
- Hunt Group
- Second Line
- CAC
- Emergency Number
- Fax

Prerequisites

Table 2: Prerequisites

- A Valid SBC Edge License
- VentaFax Software
- Voicemail Software

Verify License

You must have a valid SWE-Lite (key-based) license with the features to run the tests.

Cisco Unified Communications Manager (CUCM)

The following sections describe and provide new procedures for configuring the following:

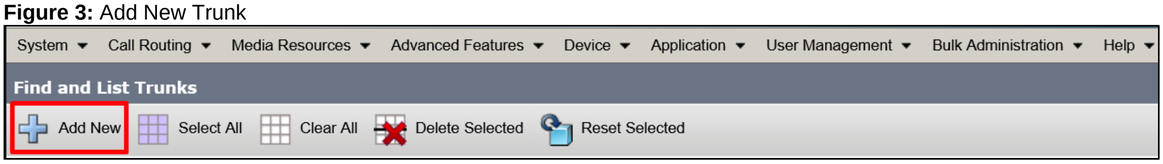
1. SIP Trunk
2. Route Group
3. Route List
4. Route Pattern

SIP Trunk

SIP trunks allow administrators to connect the Cisco Unified Communications Manager to external devices, such as SIP gateways, SIP Proxy Servers, Unified Communications applications, remote clusters, or a Session Management Edition. Ribbon uses the SIP trunk to connect the CUCM to the Ribbon SBC SWE-Lite.

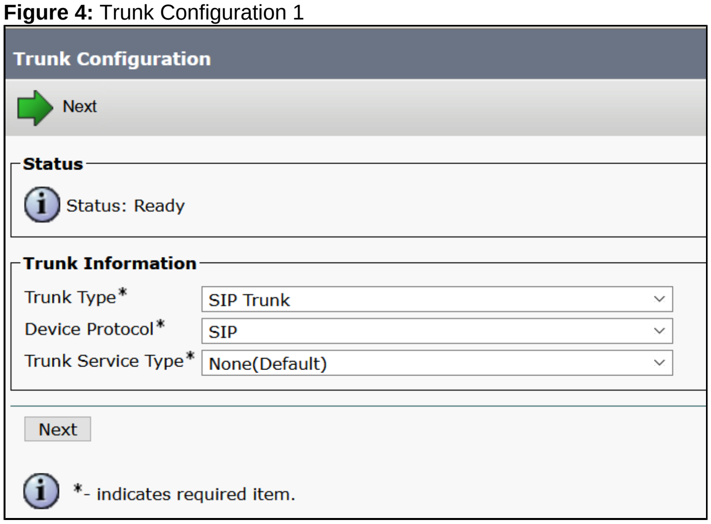
1. Log in to the CUCM as an **admin** user and navigate to **Device > Trunk**.
2. Click **Add New** to add a new Trunk.

Figure 3: Add New Trunk



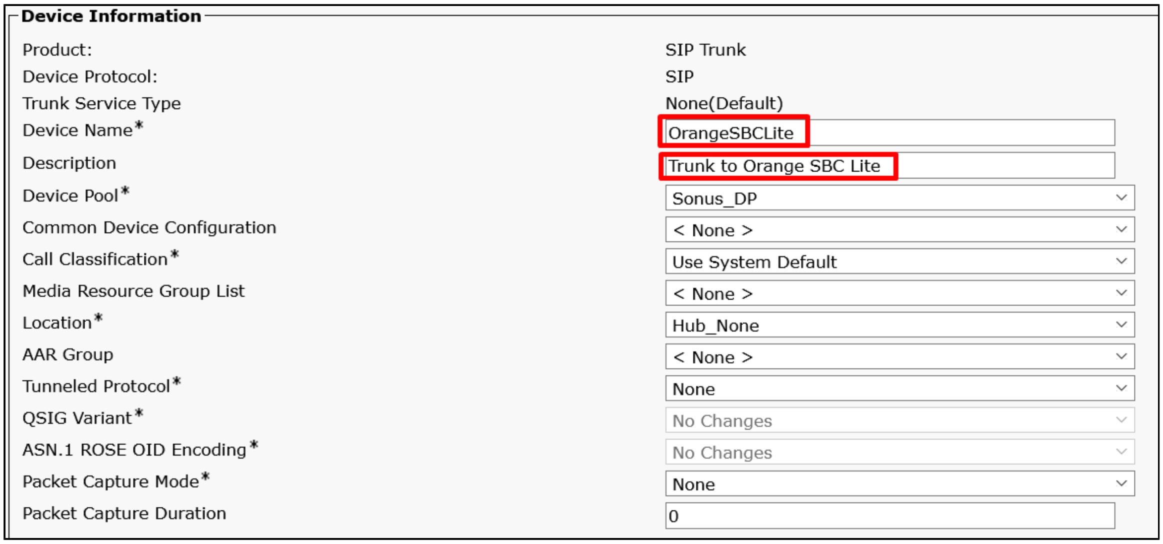
3. Set the trunk configuration.

Figure 4: Trunk Configuration 1



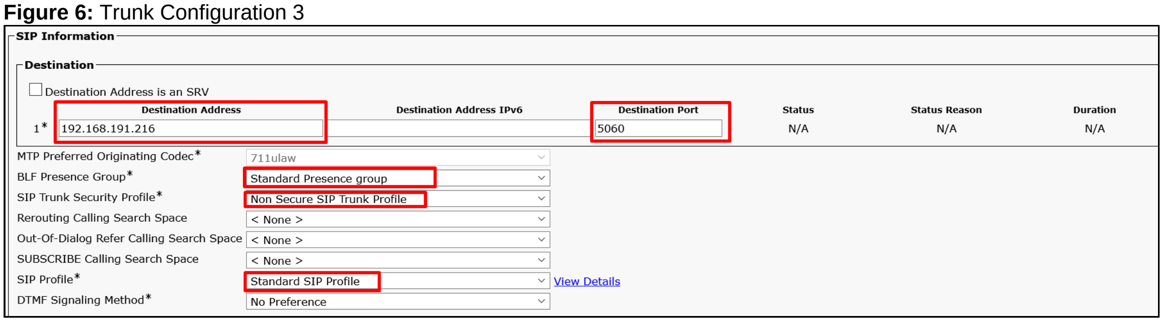
4. Click **Next**.
5. Select the device (trunk) name, the profiles, and the destination IP address that the trunk uses. The following figure shows an example of the Device Information screen.

Figure 5: Trunk Configuration 2



The IP address on the *SWE-Lite* towards the *CUCM* is 192.168.191.216.

Figure 6: Trunk Configuration 3



6. Click **Save**.

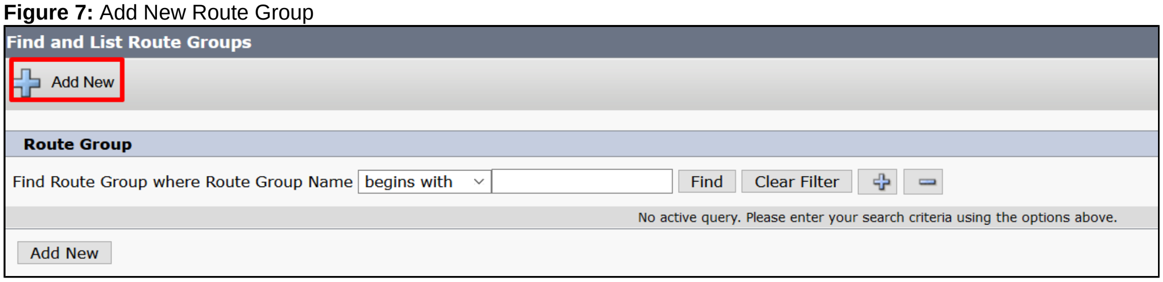
Route Group

A route group allows you to designate the order of selecting gateways and trunks. It allows you to prioritize a list of gateways and ports for outgoing trunk selection.

In the Cisco Unified Communications Manager, use the **Call Routing > Route/Hunt > Route Group** menu path to configure route groups.

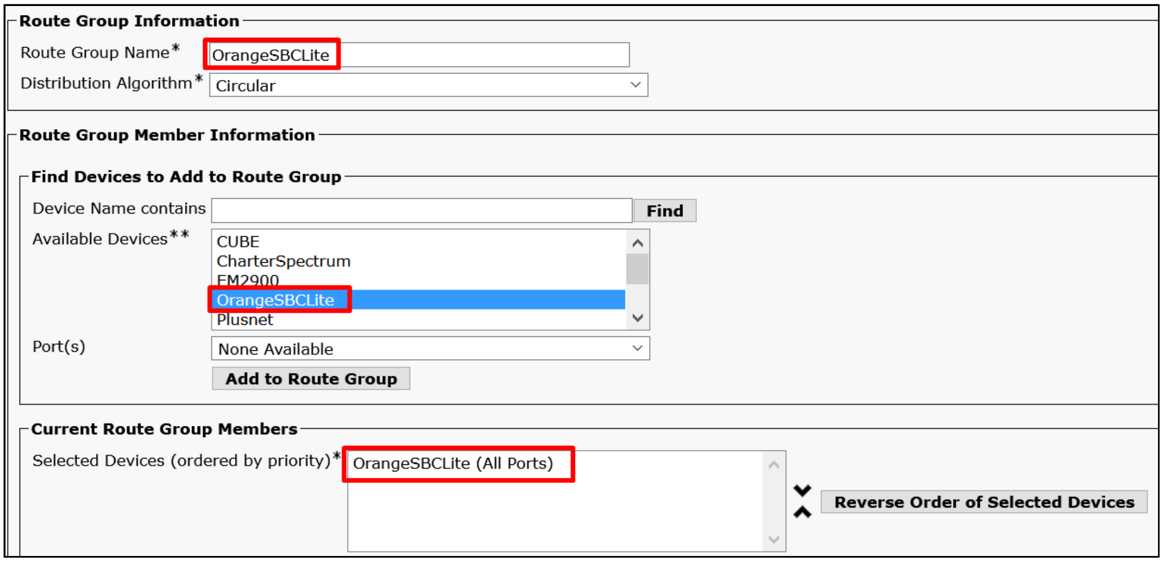
1. Click **Add New** to add a Route Group.

Figure 7: Add New Route Group



2. Specify the **Route Group name**, and select the **devices** that this **Route Group** uses. In the following example, the selected device is OrangeSBCLite that you created in the SIP Trunk section.

Figure 8: Route Group Configuration



3. Click **Save**.

Route List

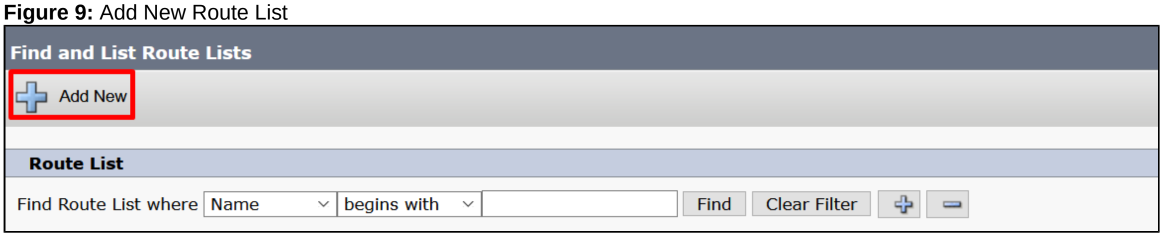
A route list associates a set of route groups in the specified priority order. It associates with one or more route patterns and determines the order of accessing those route groups. The order controls the progress of the search for available devices for outgoing calls.

> **Note**
> A route list can only contain route groups. Each route list must contain at least one route group. Each route group must include at least one device.

In the Cisco Unified Communications Manager Administration, use the **Call Routing > Route/Hunt > Route List** menu path to configure route lists.

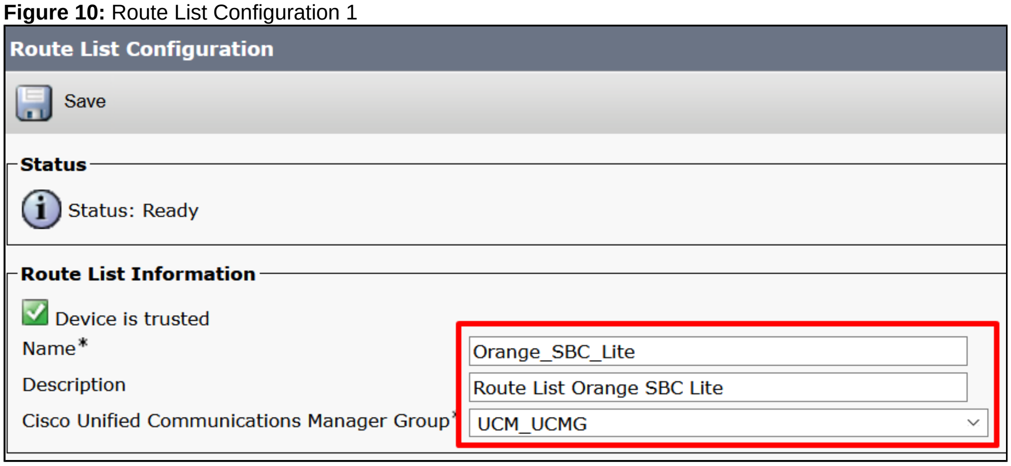
1. Click **Add New** to add a Route List.

Figure 9: Add New Route List



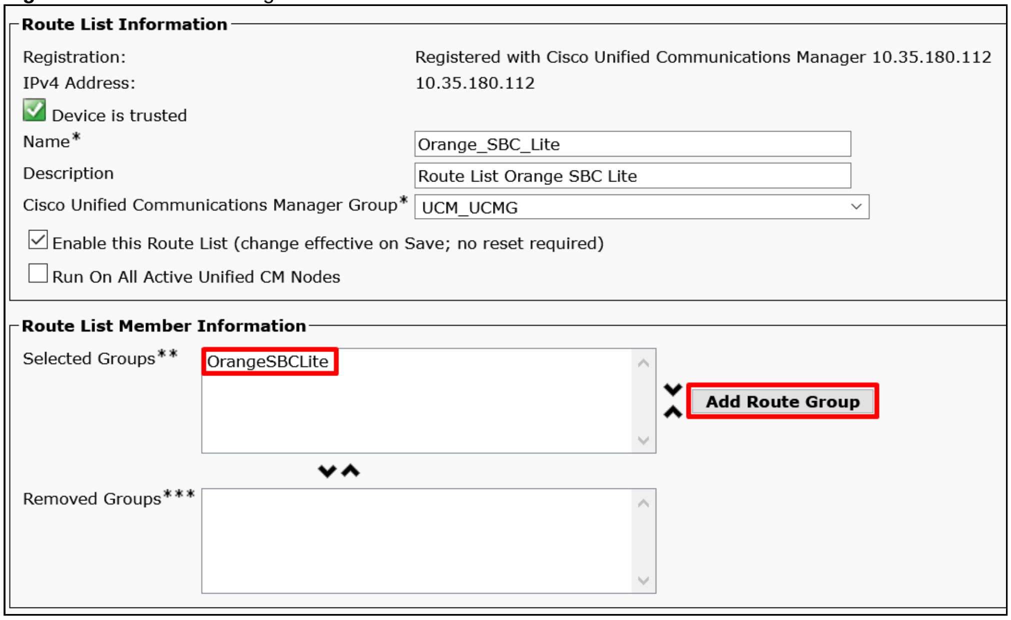
2. Specify the **Route List Name** and **Description** and select the Cisco Unified Communications Manager Group that this Route List uses.

Figure 10: Route List Configuration 1



3. Click **Save**.
4. Click **Add Route Group** to add the Route Group to the Route List.

Figure 11: Route List Configuration 2



5. Click **Save**.

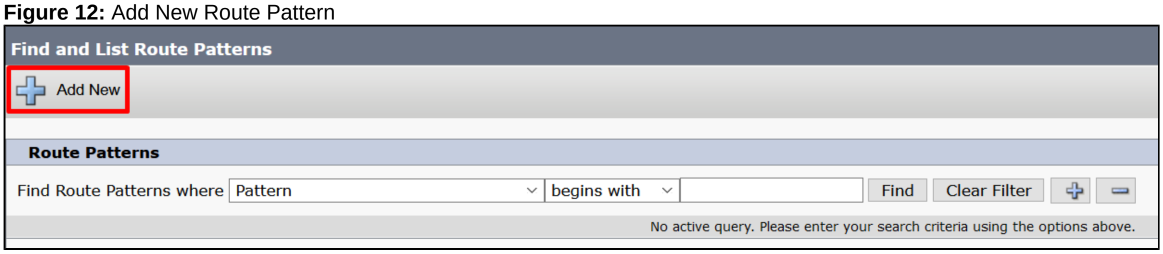
Route Pattern

A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that you can assign to a route list or a gateway. Route patterns provide flexibility in the network design. They work in conjunction with route filters and route lists, directing calls to specific devices and including, excluding, or modifying specific digit patterns.

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

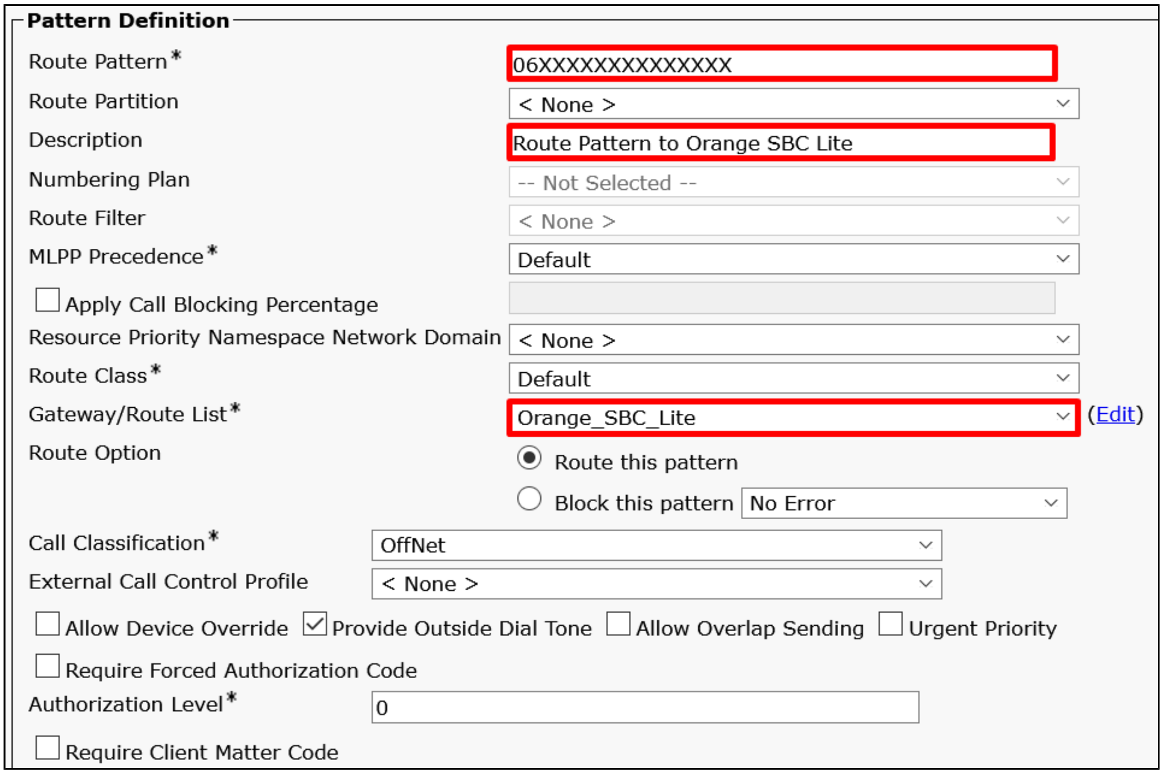
1. Click **Add New** to add a Route Pattern.

Figure 12: Add New Route Pattern



2. Specify the **Route Pattern** and **Description** and select the **Gateway/Route List.**

Figure 13: Route Pattern Configuration



Cisco Wildcard

The X wildcard matches any single digit in the range 0 through 9. For instance, the route pattern 9XXX routes or blocks all numbers in the range 9000 through 9999.

See Appendix A for more information on special characters and settings on the CISCO CUCM.

3. Click **Save**.

Note

All traffic matching the route pattern you just created will now route through the route list *Orange_SBC_Lite.*

SBC SWE-Lite Configuration

This section provides the following information:

1. System Settings
2. Network Interfaces
3. Static Routes
4. SIP Profiles
5. SBC Certificates
6. TLS Profile
7. SIP Server Tables
8. Message Manipulations
9. Media Profiles
10. SDES-SRTP Profiles
11. Media Lists
12. Q.850 to SIP Override Table
13. Signaling Groups
14. Transformations Tables

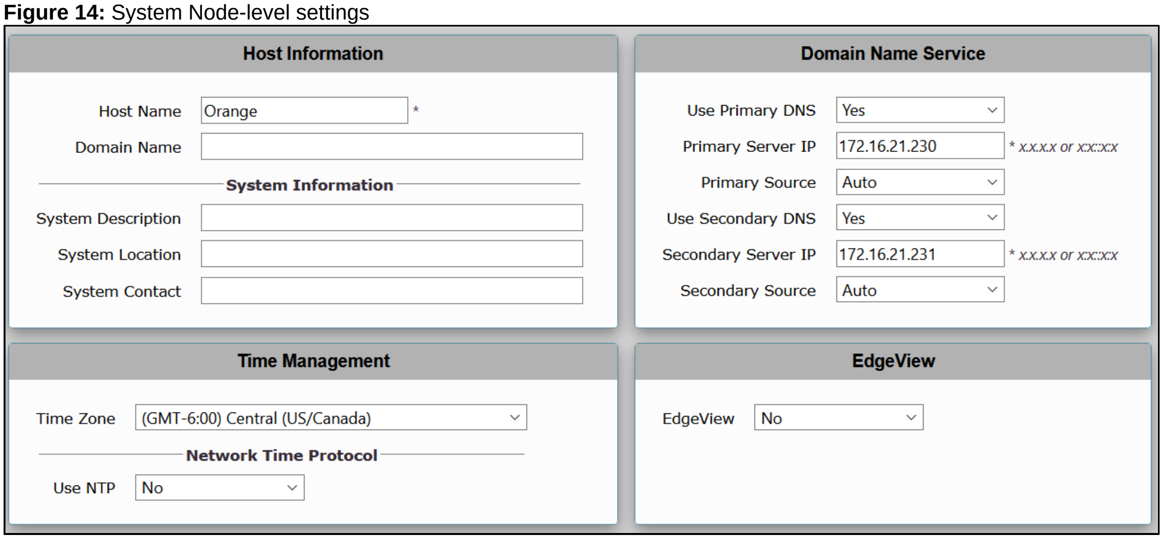
15. Call Routing Tables

System Settings

The **System > Node-Level settings** menu path allows you to set the **Host name**, **Domain name service,** and **Time management**.

The following figure shows an example of the system settings.

Figure 14: System Node-level settings



Network Interfaces

The **Networking Interfaces > Logical Interfaces** menu path allows you to configure the IP addresses (both IPv4 and IPv6) for the Ethernet ports and VLANs.

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

The SBC SWe Lite system supports a logical interface called the Admin IP (Administrative IP), also known as the Management IP. Use the Static IP or DHCP for running the initial setup of the SBC SWe Lite system.

> **Admin IP**
> You must use the Administrative IP interface for Running Initial Setup, as well as all management-related functions from the web browser.

Ethernet IP

The SBC SWe Lite system has four logical interfaces. In most deployments, one of the logical interfaces (typically **Ethernet 1 IP**) is assigned an IP address for transporting all VoIP media packets (for example, RTP, SRTP) and all protocol packets (for example, SIP, RTCP, TLS). Make sure that the DNS servers of the customer's network map the SBC SWe Lite system hostname to this IP address. You can use the hostname or IP addresses for UC-enabling systems, such as SIP-phones, IP-PBX, and Microsoft Lync Servers and for accessing the SBC SWe Lite WebUI.

In the default software, **Ethernet 1 IP** is enabled and an IPv4 IP address is acquired via a connected DHCP server. Use this IP address for performing the initial setup on the SBC SWe Lite. Refer to Running Initial Setup for more information. The default IP address for the logical interface named **Ethernet 2 IP** is 192.168.129.2. After the initial configuration, you can configure the logical interface from the Settings or Tasks tabs in the WebUI.

The following figures show examples of the Admin and Ethernet IP interfaces configuration.

Figure 15: Admin IP Configuration

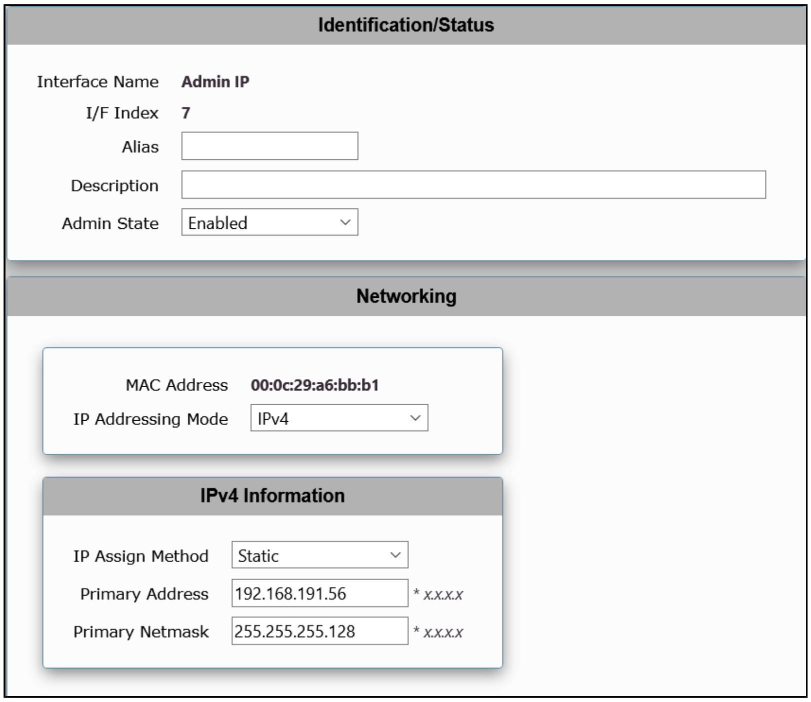
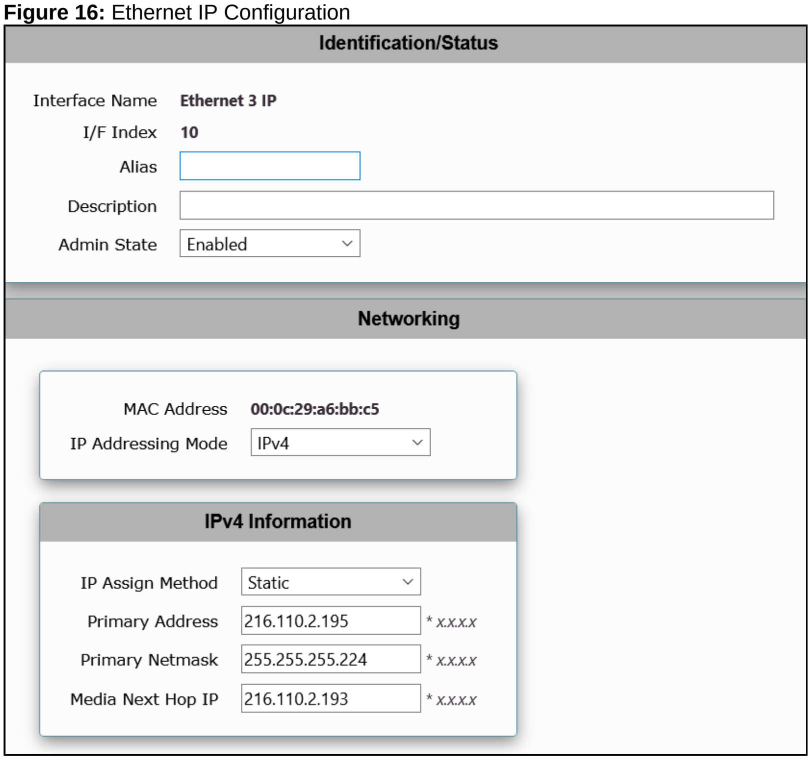


Figure 16: Ethernet IP Configuration



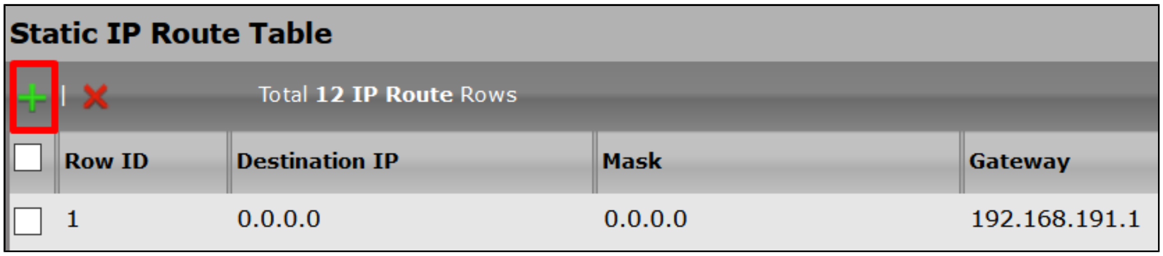
Static Routes

The **Protocols > IP > Static Route Table** menu path allows you to manually specify the next hop routers used for reaching other networks. It also specifies the default routes for the connected IP networks that use `0.0.0.0` as the Destination and Mask.

> **DHCP Configuration**
> When you configure a DHCP on an interface, the default Static Route (0.0.0.0/0) is removed and configured dynamically. To view the dynamically created default route, access the WebUI and navigate to **Protocols > IP > Routing Table**.

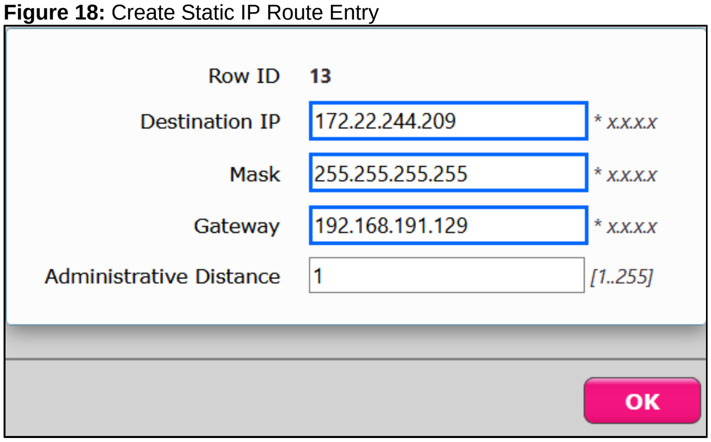
1. To add a new Static Route, click the **plus (+)** icon.

   Figure 17: Add New Static Route



2. Specify the fields in the Create Static IP Route Entry screen.

Figure 18: Create Static IP Route Entry



- **Destination IP**

  Specifies the destination IP Address.

- **Mask**

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

- **Gateway**

  Specifies the IP Address of the next hop router used for this Static Route.

- **Metric**

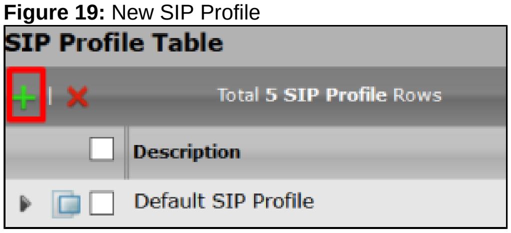
  Specifies the cost of this route, hence indirectly defining the preference of the route. Lower values indicate more preferred routes. The typical value is **1** for most static routes, indicating that users prefer static routes over dynamic routes.

SIP Profiles

The **SIP > SIP Profiles** menu path controls how the SBC Edge communicates with SIP devices. The profiles control important characteristics, such as session timers, SIP header customization, SIP timers, MIME payloads, and option tags.

To add a new SIP Profile, click the **plus (+)** icon.

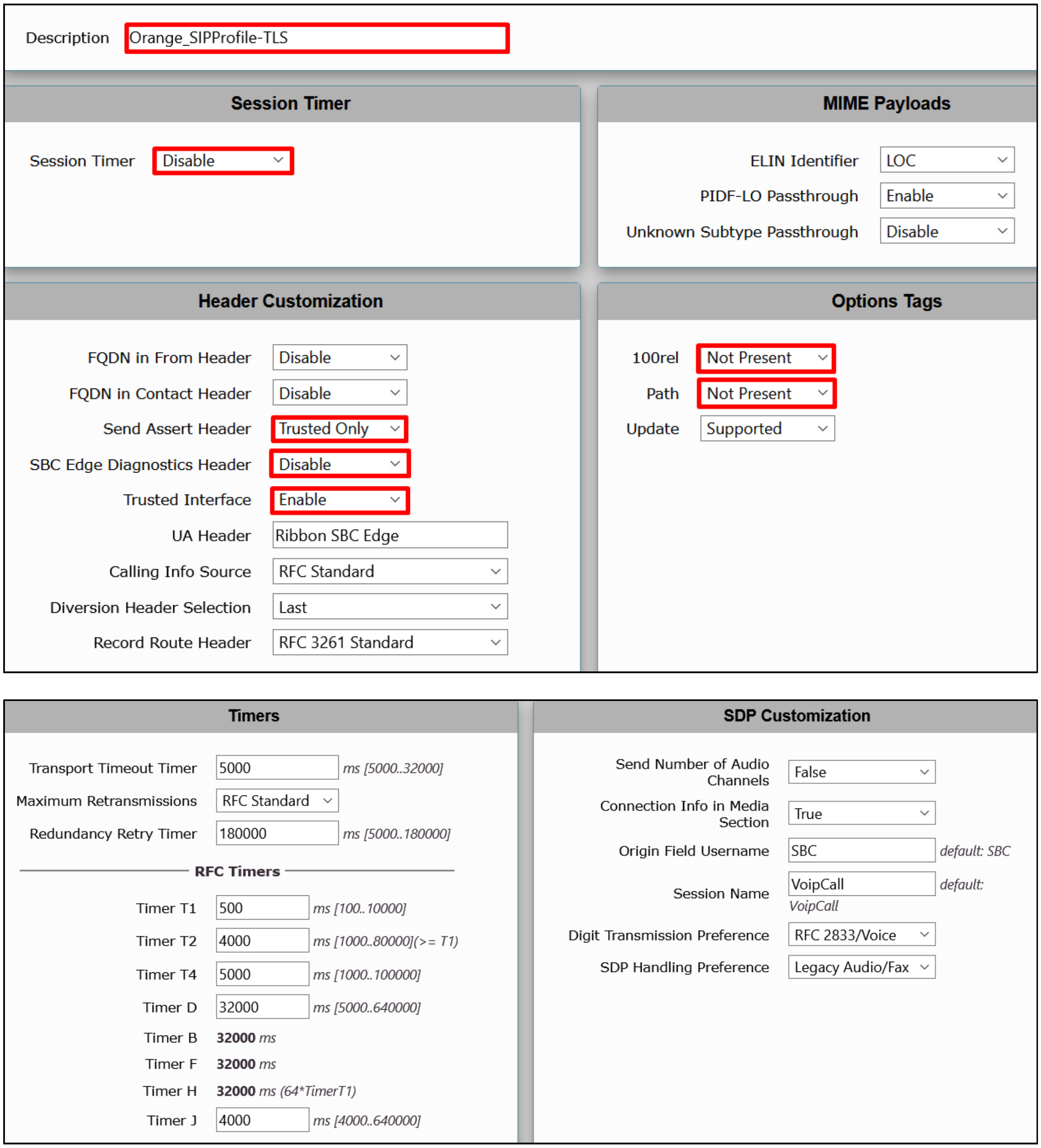
Figure 19: New SIP Profile



OBS SIP Profile Configuration

To configure the OBS SIP Profile, modify the highlighted fields in the following figure to fulfill the OBS requirements. The rest of the features use the default settings.

Figure 20: OBS SIP Profile Configuration



CUCM SIP Profile Configuration

The CUCM SIP Profile uses the default settings.

Figure 21: CUCM SIP Profile Configuration 1

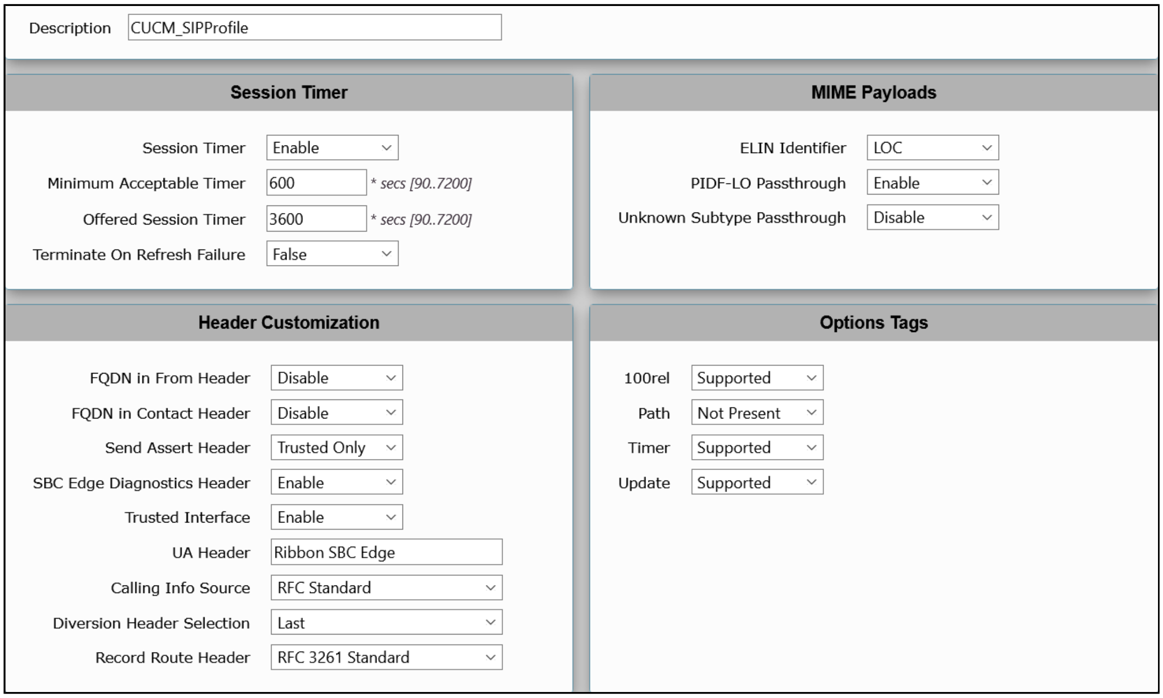
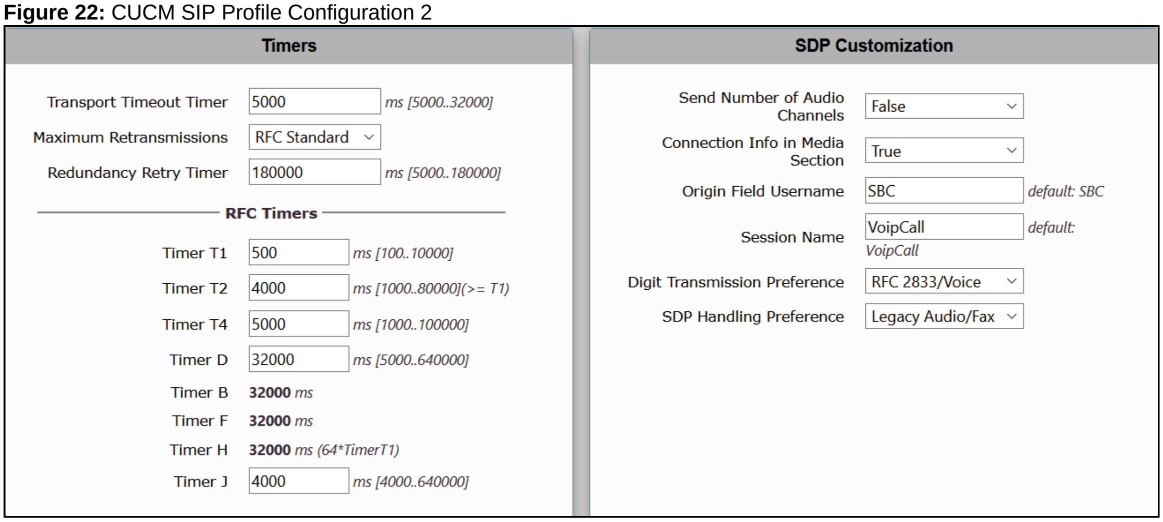


Figure 22: CUCM SIP Profile Configuration 2



Ventafax SIP Profile Configuration

The Ventafax SIP Profile uses the default settings.

Figure 23: Ventafax SIP Profile Configuration 1

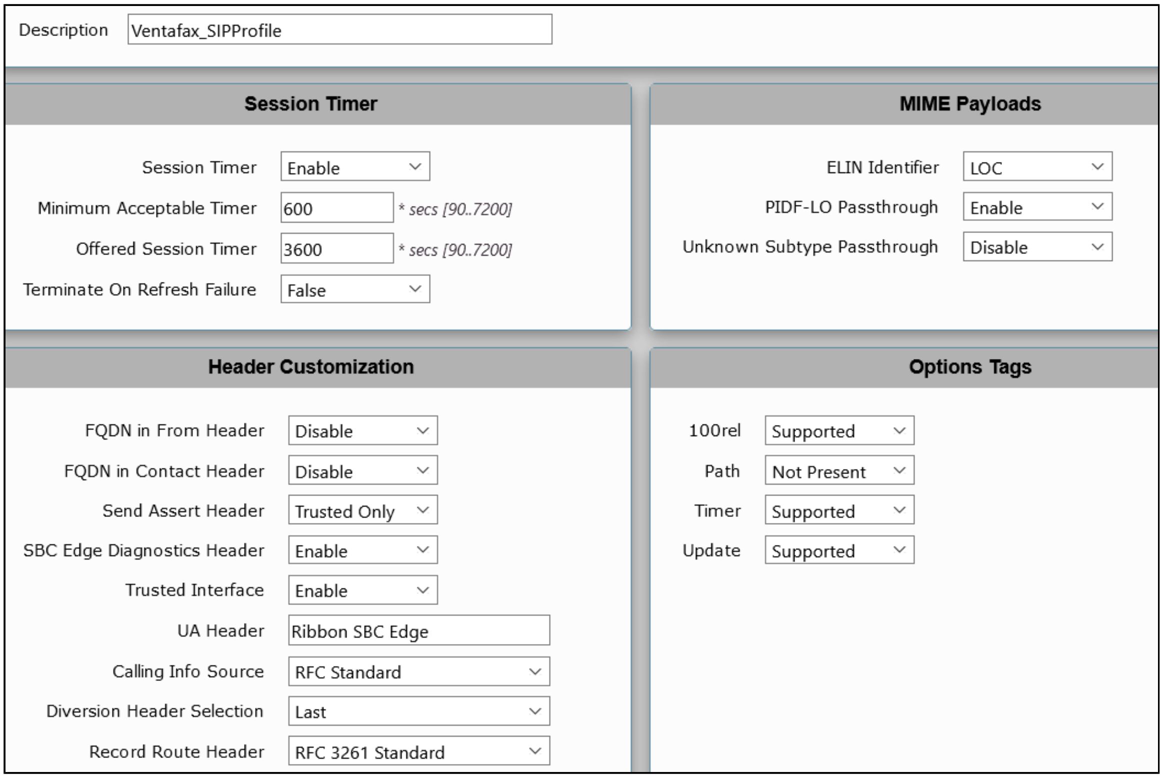
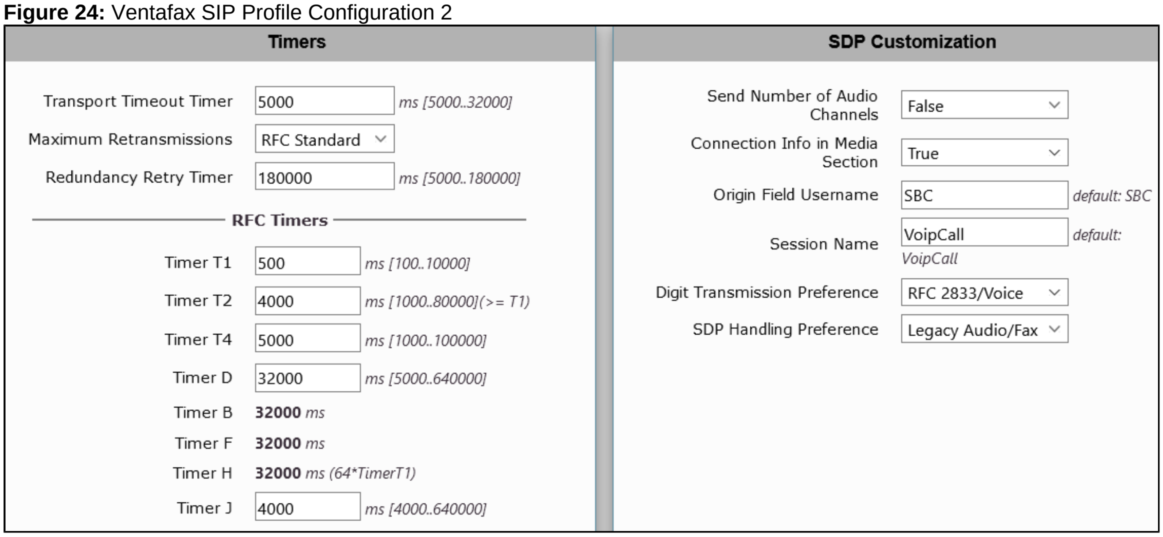


Figure 24: Ventafax SIP Profile Configuration 2



SBC Certificates

You must first generate the CSR (Certificate Signing Request) and then send it to the Certificate Authority (CA) to get the Signed Certificate. Once you receive the Signed Certificate, upload the certificate to the SBC along with the Root and Intermediate certificates you received from the CA.

Generate the CSR

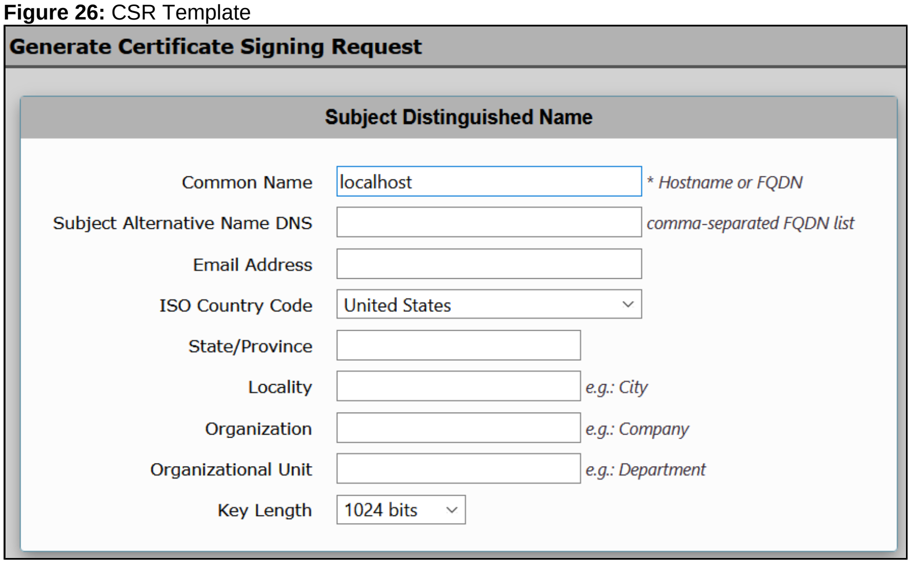
Use the following procedure to generate the CSR.

1. On the left menu, go to **Security > SBC Certificates > Generate SBC Edge CSR.**

   Figure 25: Generate CSR Menu Path

2. Add the information in the CSR template.

Figure 26: CSR Template



CSR Information

The information you add in the template depends on the data that your company provides.

3. Click **OK** to generate the CSR.

Signed Certificate

Once you generate the CSR, be sure to send it to a CA (Certification Authority) to get the signed certificate.

Trusted CA Certificates

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

1. On the left menu, go to **Security > SBC Certificates > Trusted CA Certificates**.

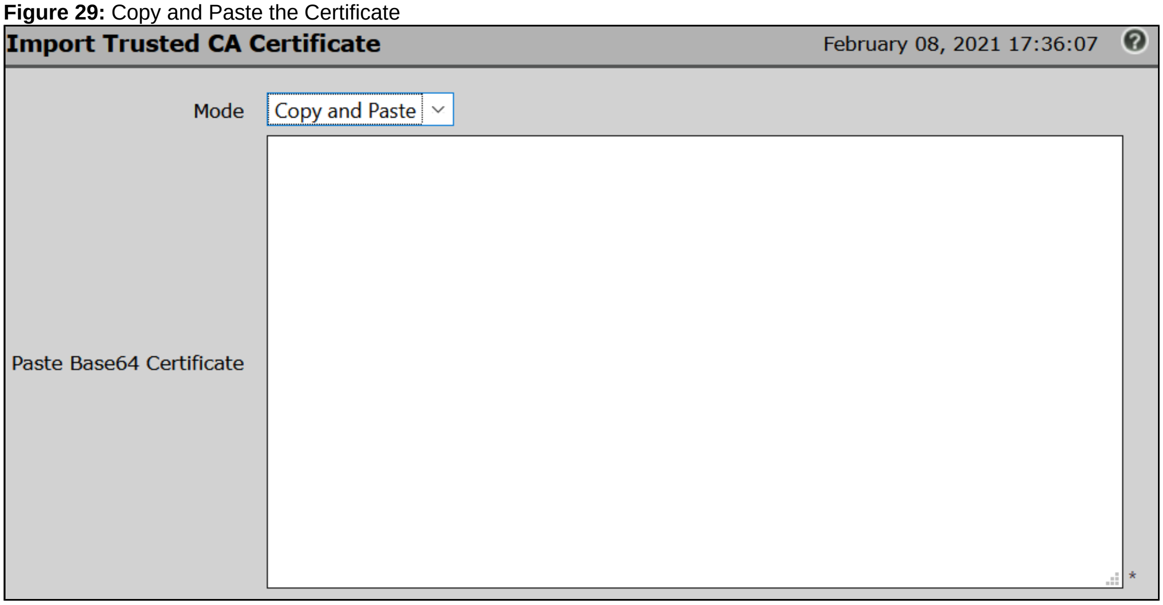
Figure 27: Trusted CA Certificate Table Menu Path

2. Click the **Import Trusted CA Certificate** icon to import the certificates.

Figure 28: Import Trusted CA Certificate

3. The **Import Trusted CA Certificate** pop-uup window prompts you to copy and paste the certificate.

Figure 29: Copy and Paste the Certificate



4. Paste the certificate and click **OK** to save the changes.

> **Additional Certificates**
> Repeat the procedure to import additional certificates.

SBC Primary Certificate

By default, after the Ribbon SBC 1000/2000 system is initialized for the first time, or after a factory reset, the Ribbon SBC 1000/2000 system is pre-configured with a Self-signed Server Certificate.

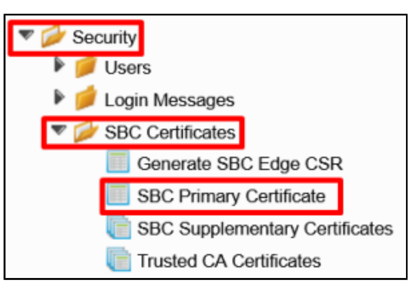
Installing a new Signed Certificate on the Ribbon SBC 1000/2000 comprises the following three procedures that you must perform in the specified order:

1. Generate a Certificate Signing Request (CSR)
2. Obtain and Import a Trusted Root CA Certificate
3. Obtain and Import the Signed Primary Certificate

Use the following steps to generate the SBC Primary Certificate.

1. On the left menu, go to **Security > SBC Certificates > SBC Primary Certificate**.

Figure 30: SBC Primary Certificate MenuPath

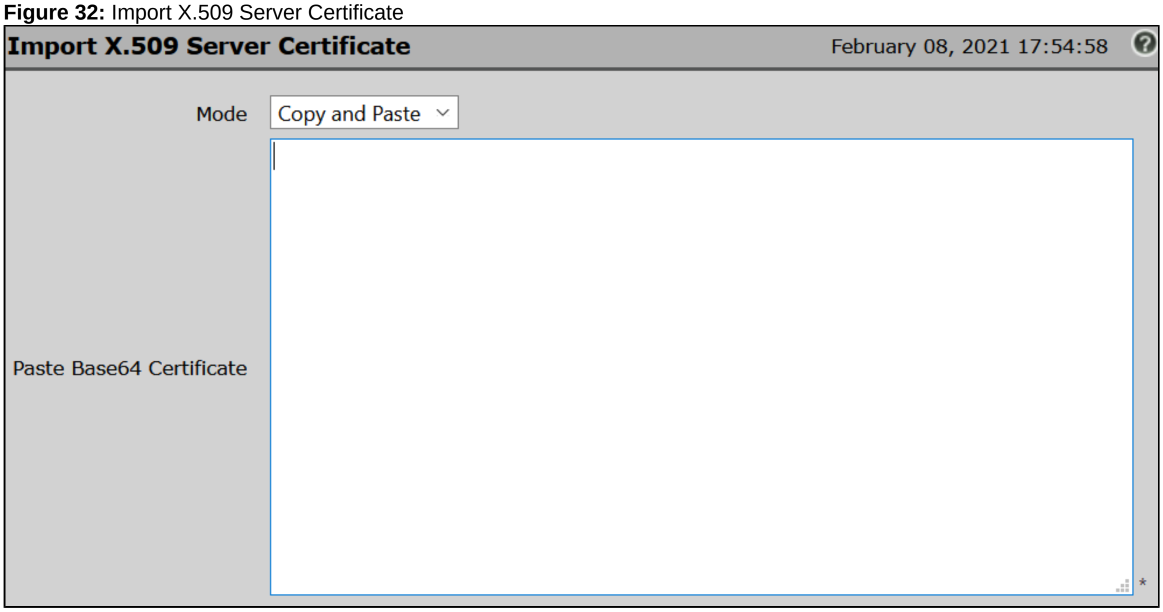


2. Click **Import > X.509 Signed Certificate**.

Figure 31: Import Primary Certificate

3. The **Import > X.509 Signed Certificate** pop-up window prompts you to copy and paste the certificate.

Figure 32: Import X.509 Server Certificate



4. Paste the certificate and click **OK** to save the changes.

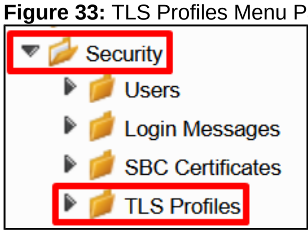
TLS Profile

After the Ribbon SBC 1000/2000 obtains the required certificates, be sure to configure several options and attributes on both the server and client so that the TLS can employ the certificate(s) to establish a secure connection. Configure the attributes in the TLS profiles. Attributes include, but are not limited to items, such as Client Ciphers, and inactivity timeouts.

SIP Signaling Groups use the TLS Profiles when you select the TLS transport type for incoming and outgoing SIP trunks (Listen Ports), and in SIP Server Tables when you select the TLS as the Server Host protocol.

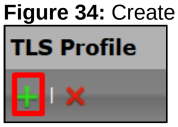
1. On the left menu path, go to **Security > TLS Profiles**.

Figure 33: TLS Profiles Menu Path



2. Click the **plus (+)** icon to add a new entry.

Figure 34: Create TLS Profile



3. Set the TLS Profile as shown in the following figure.

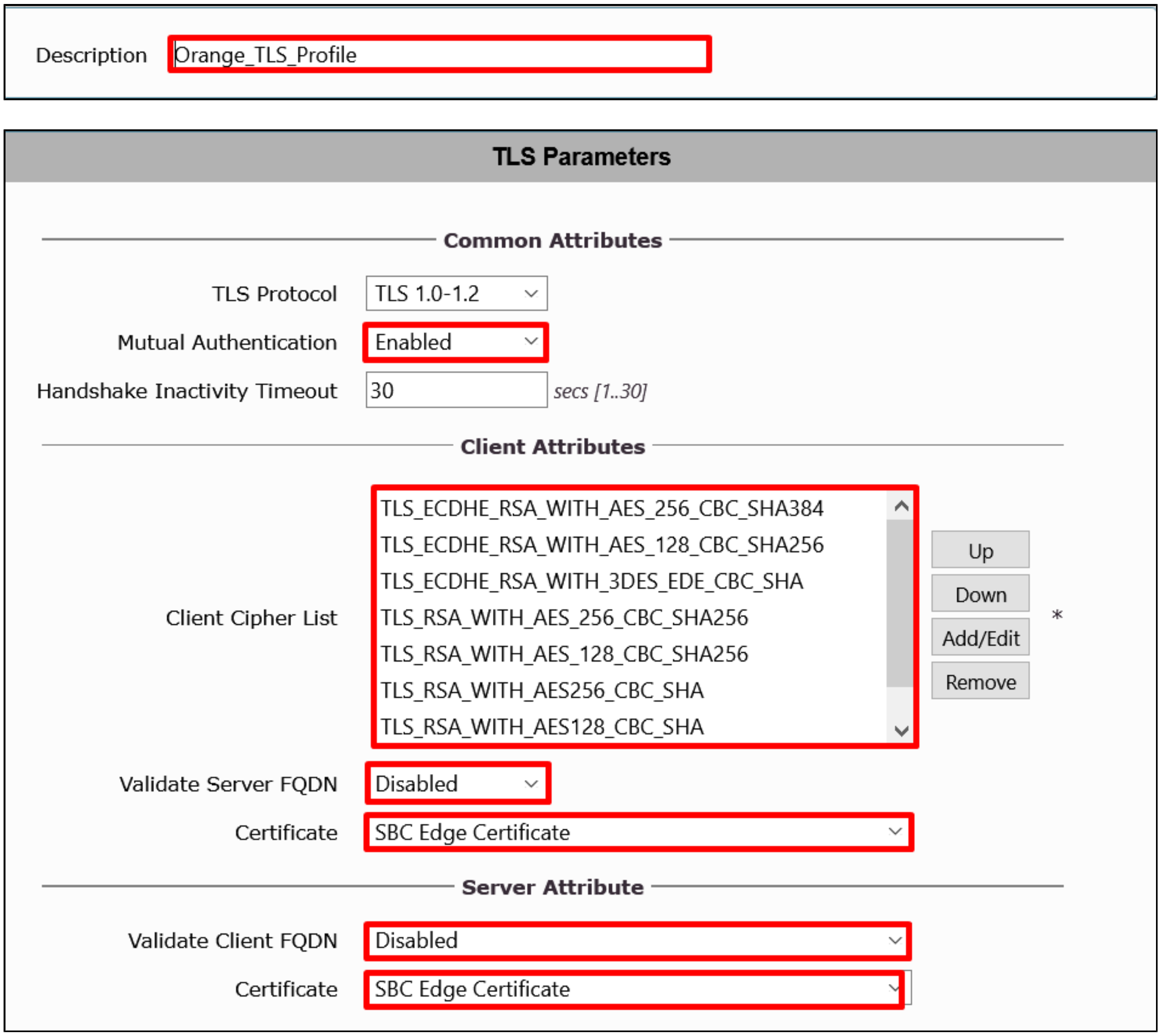


Figure 35: Orange TLS Profile

4. Click **Apply** to save the changes.

SIP Server Tables

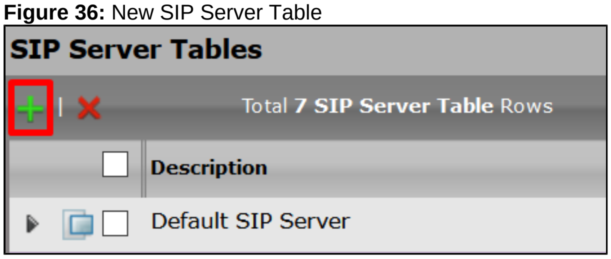
The **SIP > SIP Server Table** menu path contains information about the SIP devices connected to the SBC Edge. The entries in the tables provide information about the IP Addresses, ports, and protocols used to communicate with each server. The table entries also contain links to counters that you use for troubleshooting. The SIP Server supports either an FQDN or IP Address (V4 or V6).

OBS SIP Server Table

sbc1.btoi.one.equant.net

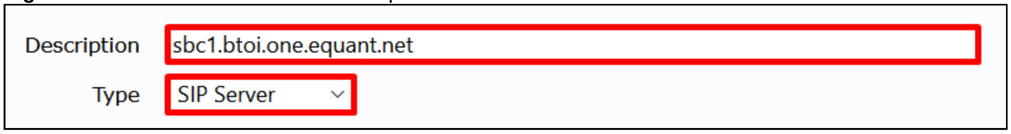
1. To add a new **SIP Server Table,** click the **plus (+)** icon.

Figure 36: New SIP Server Table



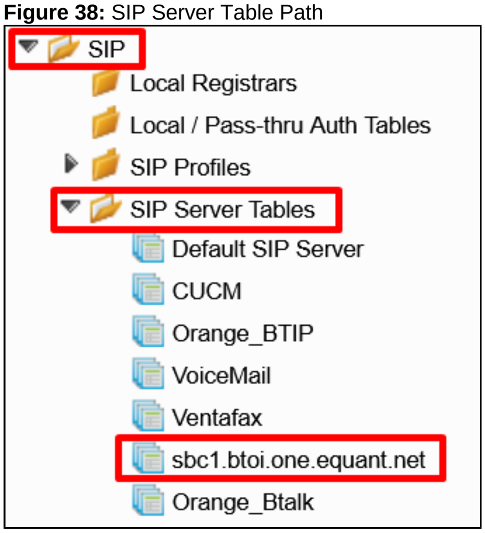
2. Specify the **Description** and select the **SIP Server**.

Figure 37: New SIP Server Table Description



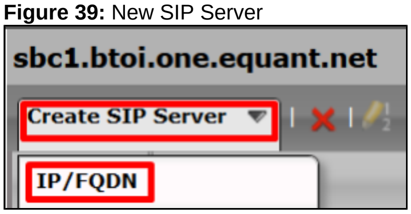
3. Select the **SIP Server Table** that you just created.

Figure 38: SIP Server Table Path



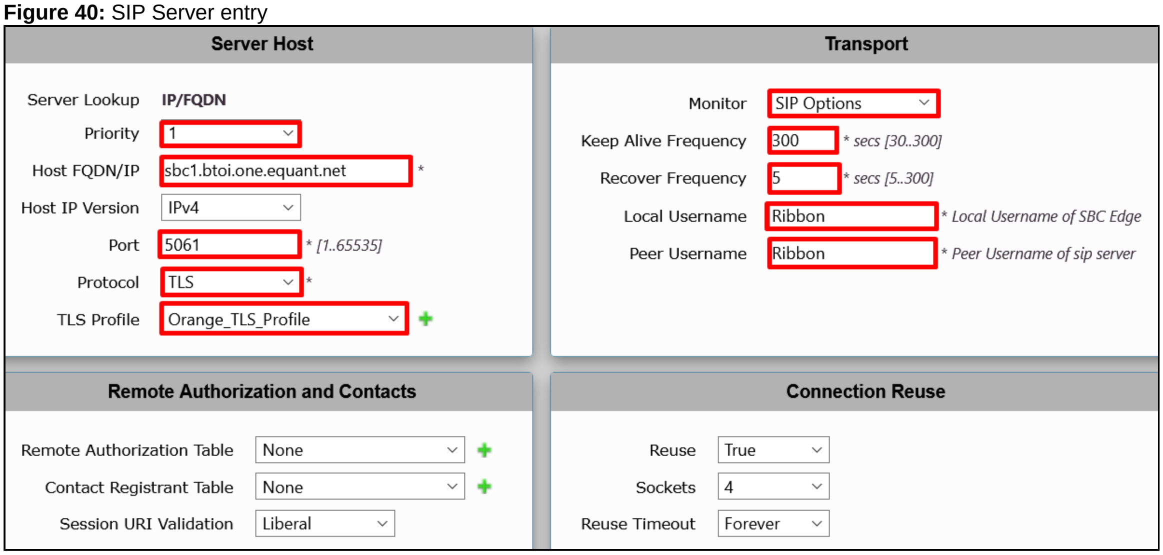
4. Click **Create SIP Server > IP/FQDN** to add a new SIP Server.

Figure 39: New SIP Server



5. Set the new entry as shown in the figure. Modify the highlighted fields to fulfill the OBS requirements. The rest of the features use the default settings.

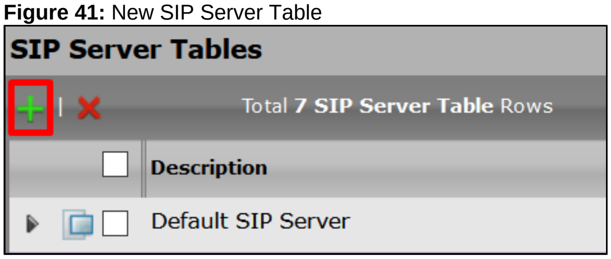
Figure 40: SIP Server entry



CUCM SIP Server Table

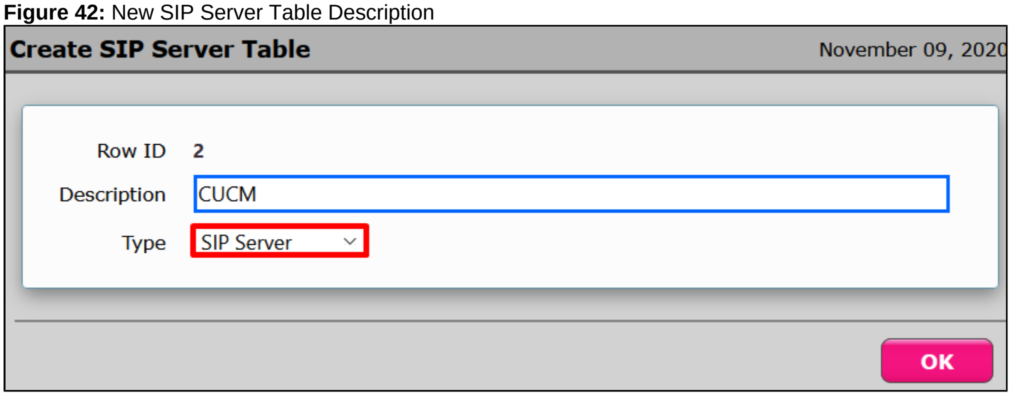
1. To add a new **SIP Server Table,** click the **plus (+)** icon.

Figure 41: New SIP Server Table



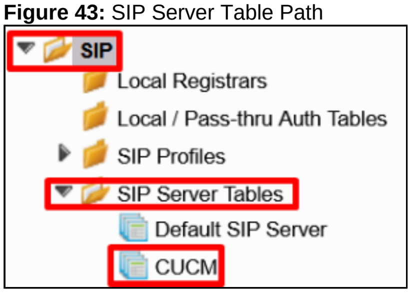
2. Specify the **Description** and select the **SIP Server**.

Figure 42: New SIP Server Table Description



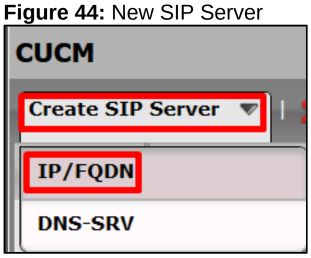
3. Select the **SIP Server Table** that you just created.

Figure 43: SIP Server Table Path



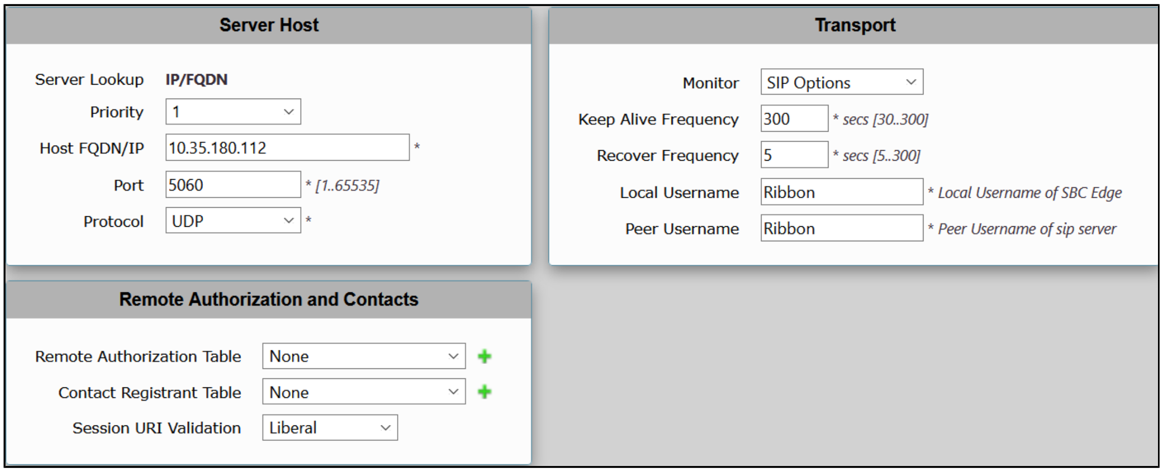
4. Click **Create SIP Server > IP/FQDN** to add a new SIP Server.

Figure 44: New SIP Server



The following figure depicts the CUCM SIP Server Configuration.

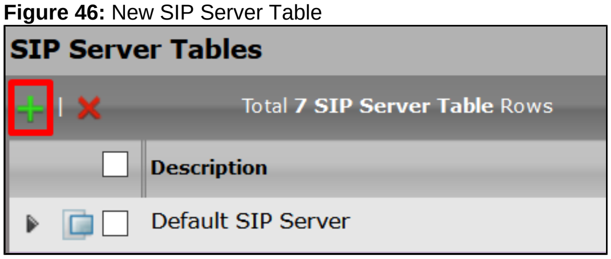
Figure 45: CUCM SIP Server Configuration



Ventafax SIP Server Table

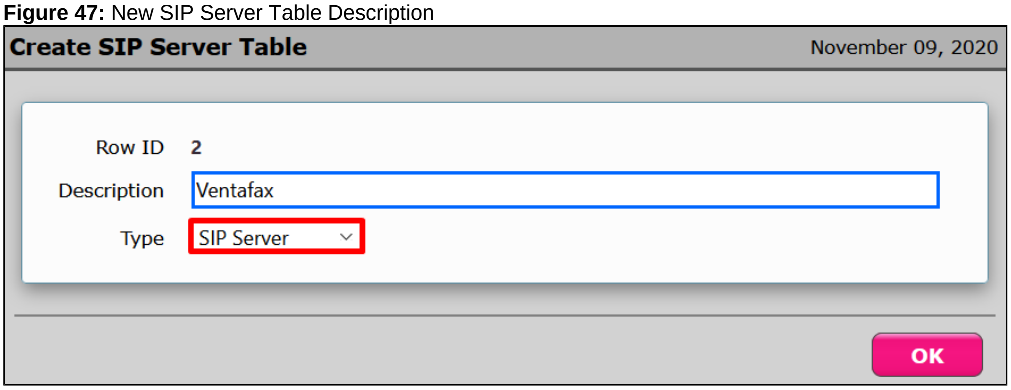
1. To add a new **SIP Server Table,** click the **plus (+)** icon.

Figure 46: New SIP Server Table



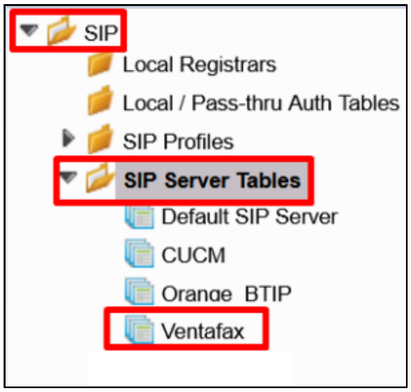
2. Specify the **Description** and select the **SIP Server**.

Figure 47: New SIP Server Table Description



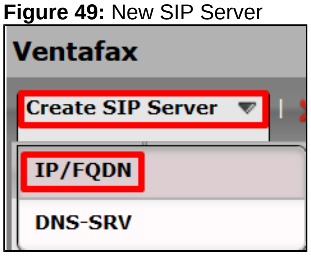
3. Select the **SIP Server Table** that you just created.

Figure 48: SIP Server Table Path



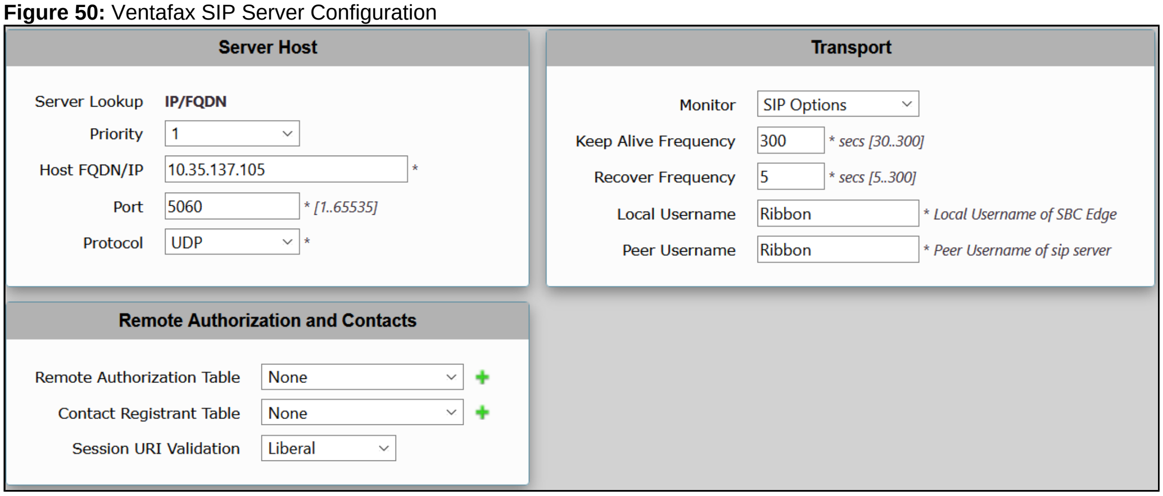
4. Click **Create SIP Server > IP/FQDN** to add a new SIP Server.

Figure 49: New SIP Server



The following figure depicts the Ventafax SIP Server Configuration.

Figure 50: Ventafax SIP Server Configuration



Message Manipulations

The **SIP > Message Manipulation** menu path allows you to manipulate the incoming or outgoing messages. The Message Manipulation feature enhances the interoperability with different vendor equipment and applications. It also corrects any fixable protocol errors in SIP messages spontaneously without requiring any changes to the firmware or software.

Although SIP is considered a mature protocol, devices running old firmware and systems interpret the SIP standard in a non-conforming way. Additionally, in some instances, a compliant message may potentially modify to adapt to an application-specific requirement.

This capability consists of two components: condition rules and message rules.

The Condition rules identify the messages and components required within a message to make any modifications. For example, I want to modify all INVITE messages with a **from uri host** of "ribbon.net".

The Message rules perform the actual modification of a message. Once the conditions of a rule have been met, the message rule(s) are applied. Continuing with the example above, a message rule may change the from uri display name to "Ribbon".

SIP Message Manipulation
See Appendix A for more information about SIP Message Manipulation.

Condition Rule Table

Condition rules are simple rules that apply to a specific component of a message (for example, diversion.uri.host, from.uri.host, and so on). You can match the value of the field specified in the Match Type list box against a literal value, token, or REGEX.

The Condition Rule Table stores a collection of all user-created Condition Rules.

Match_Content-Type

This Condition Rule matches only if **SG User Value 1 = application/sdp**. This condition identifies whether the SDP is present or not in the SIP messages.

SG User Value 1
The **SG User Value 1** is stored using a Message Rule (*Store_Content-Type*). (See Message Rule Tables for more information.)

SG User Value 1 is the predefined name that the SBC uses.

1. To add a new Condition Rule, go to the **SIP > Message Manipulation > Condition Rule Table** menu path, and click the **plus (+)** icon.

Figure 51: Condition Rule Table menu path

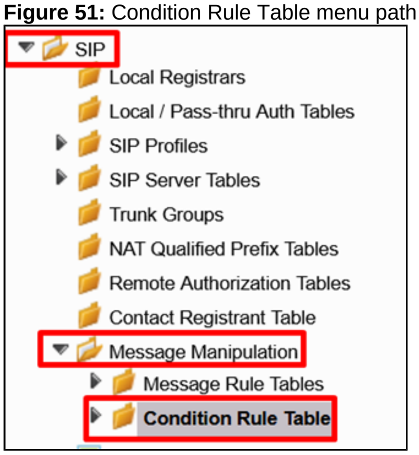
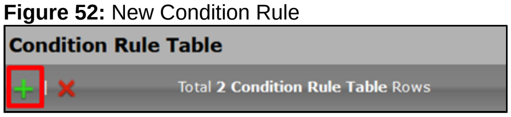
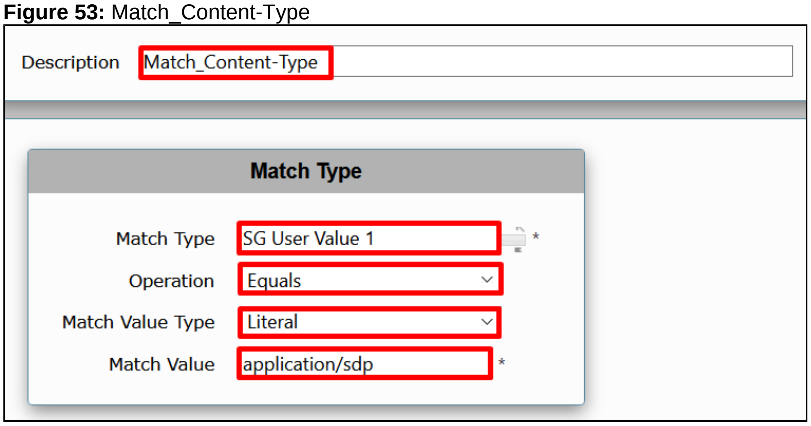


Figure 52: New Condition Rule



2. Set the new entry as shown in the following figure.

Figure 53: Match_Content-Type



Match_Anonymous

This Condition Rule matches only if **from.displayname = Anonymous**.

This rule compares whether the **display name** in the **From** header is equal to **Anonymous**.

> Message Rule **Modify_From_Anonymous** uses this condition rule. (See Message Rule Tables for more information.) This rule sets the format that the OBS requested: ***(sip:anonymous@anonymous.invalid*)**

1. To add a new Condition Rule, go to the **SIP > Message Manipulation > Condition Rule Table** menu path, and click the **plus (+)** icon.

Figure 54: Condition Rule Table menu path

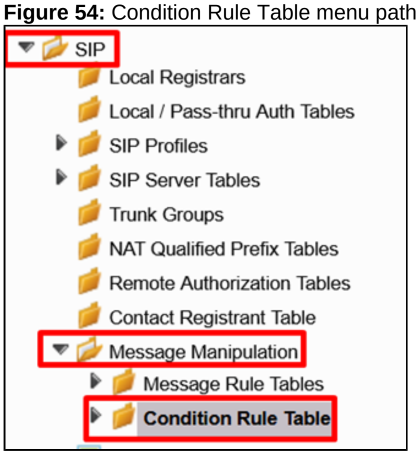
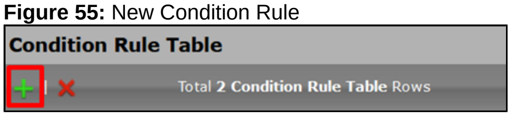
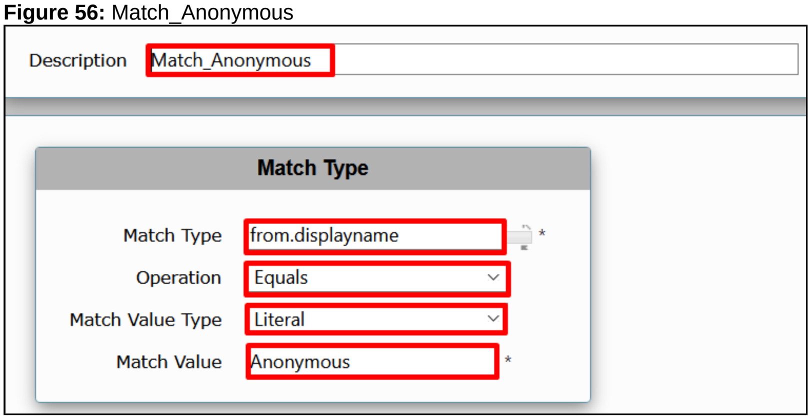


Figure 55: New Condition Rule



2. Set the new entry as shown in the following figure.

Figure 56: Match_Anonymous



Message Rule Tables

Message Rule Tables are simply sets of Condition Rules. Users apply these rules in the SIP Signaling Groups after enabling the Message Manipulation.

The Message Rule Tables collect **SIP Messages Manipulations Rules** and apply them according to the **Message Type** value set in the Message Rule Tables. The following tables define the settings of format that the OBS requested.

Table Description	Rules	Result Type	Message Type	Comments

Add_P-Early-Media	Add P-Early-Media supported Del_P-Early-Media Add_P-Early-Media sendrecv	Optional	180, 183	This table applies only to 180 and 183 response messages. It collects the rules for inserting the P-Early-Media header requested by the OBS.
Store_Content-Type	Store Content-Type	Optional	180, 183	This table applies only to 180 and 183 response messages. It collects the rules for storing the Content-type header value. The value determines whether the SIP message contains an SDP or not.
Store_User-Agent_Value	Store_User-Agent_Value Store_Server_Value	Optional	All	This table applies to all messages. It collects the rules for storing the IPPBX User-Agent and Server headers values.
OBS_SIP_Profile_Adaptation_01	Remove_SGID_From_Header Remove_SGID_To_Header Modify_User-Agent_Header Modify_Server_header Modify_Allow_header	Optional	All	This table applies to all messages. It collects the rules for setting the format that the OBS requested.
OBS_SIP_Profile_Adaptation_02	Modify_PAI Add plus P-Asserted-Identity Modify_From_Anonymous Modify_Diversion	Optional	Requests	This table applies only to request messages. It collects the rules for setting the format that the OBS requested.

Add_P-Early-Media Table

This table collects the rules for adding the **P-Early-Media** header in the SIP 180 and SIP 183 responses.

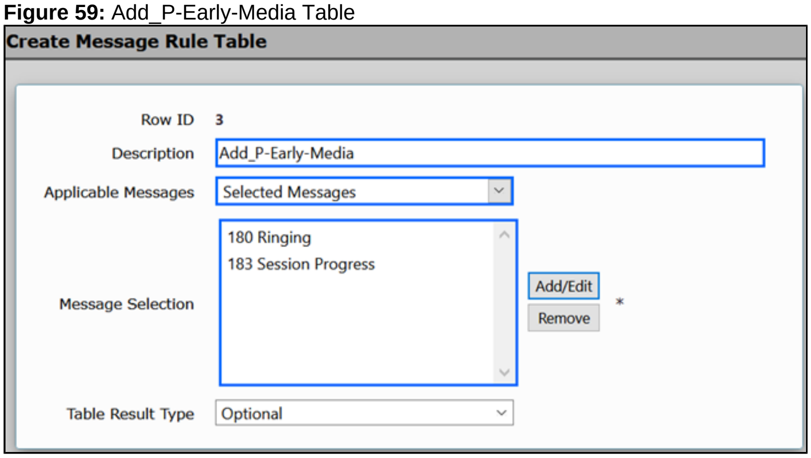
1. To add a new Message Rule Table, go to the **SIP > Message Manipulation > Message Rule Tables** menu path, and click the **plus (+)** icon.

Figure 57: Message Rule Table menu path

Figure 58: New Message Rule Table

2. Set the new entry as shown in the following figure.

Figure 59: Add_P-Early-Media Table



The following table describes the rules for the Add_P-Early-Media table.

Add_P-Early-Media Rules

Description	Rule Type	Result Type	Comments
Add P-Early-Media supported	Header Rule	Optional	Adds the **P-Early-Media header value = supported**
Del_P-Early-Media	Header Rule	Optional	Deletes the P-Early-Media header to avoid duplicate headers.
Add_P-Early-Media sendrecv	Header Rule	Optional	Adds the **P-Early-Media header value = sendrecv**

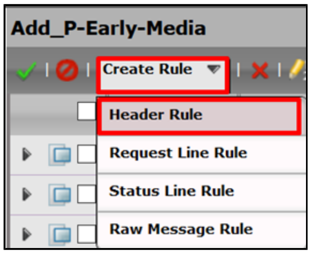
Add P-Early-Media supported

1. To add a new Message Rule, access the left menu path, and click the **Add_P-Early-Media** table you just created.

Figure 60: Add_P-Early-Media menu path

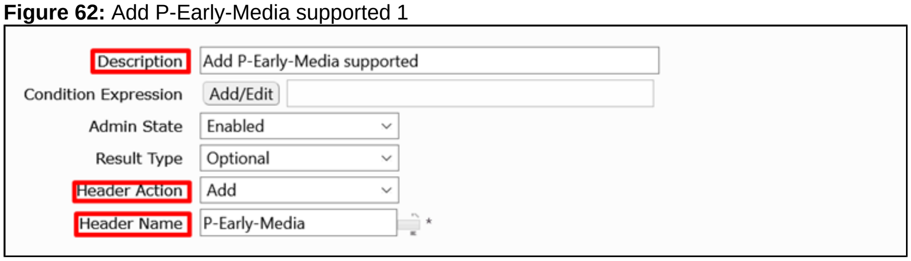
2. Click **Create Rule > Header Rule**.

Figure 61: New Rule



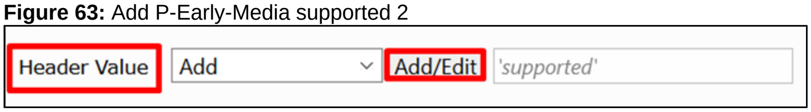
3. Set the new entry as shown in the following figure.

Figure 62: Add P-Early-Media supported 1



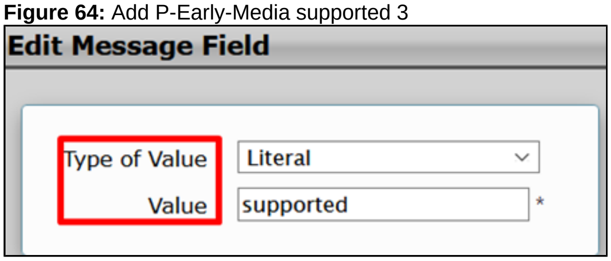
4. Select **Add** in the **Header Action** field.
5. When the **Header Value** field displays, select **Add**.
6. Click **Add/Edit**.

Figure 63: Add P-Early-Media supported 2



7. Set the values as shown in the Edit Message Field window.

Figure 64: Add P-Early-Media supported 3



8. Click **Apply** to save the changes.

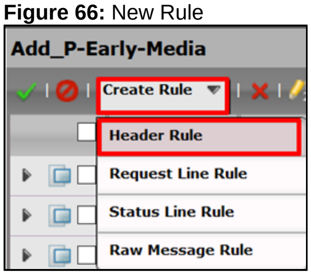
Del_P-Early-Media

1. To add a new Message Rule, click the **Add_P-Early-Media** table on the left menu path.

Figure 65: Add_P-Early-Media menu path

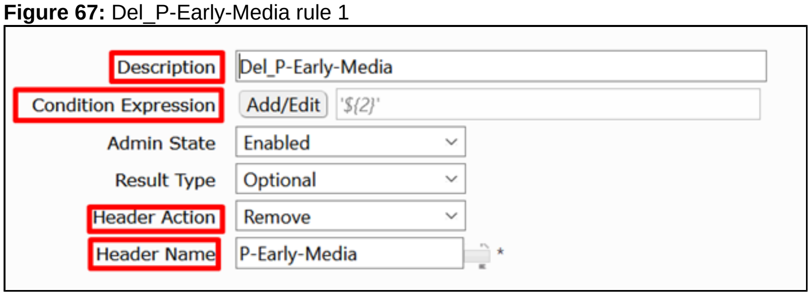
2. Click **Create Rule > Header Rule**.

Figure 66: New Rule



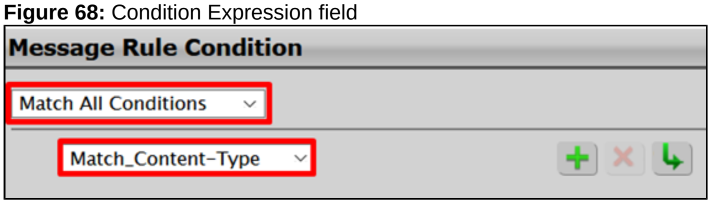
3. Set the new entry as shown in the following figures.
4. Click **Add/Edit** in the **Condition Expression** field.

Figure 67: Del_P-Early-Media rule 1



5. When the Message Rule Condition window displays, set the following fields.

Figure 68: Condition Expression field



6. Click **Apply** to save the changes.

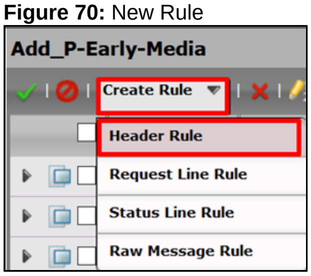
Add_P-Early-Media sendrecv

1. To add a new Message Rule, click the **Add_P-Early-Media** table on the left menu path.

Figure 69: Add_P-Early-Media menu path

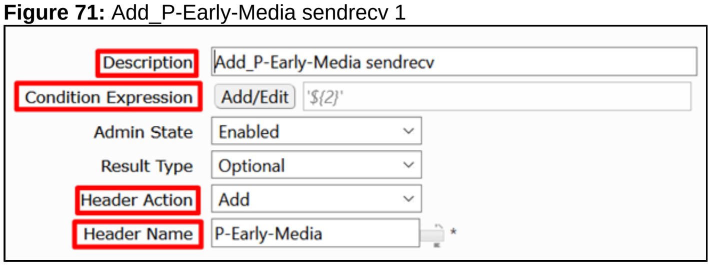
2. Click **Create Rule > Header Rule.**

Figure 70: New Rule



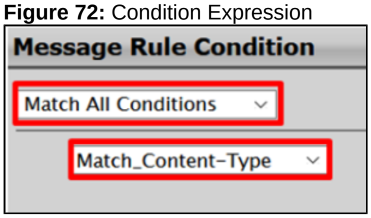
3. Set the new entry as shown in the following figures.
4. Click **Add/Edit** in the **Condition Expression** field.

Figure 71: Add_P-Early-Media sendrecv 1



5. When the Message Rule Condition window displays, set the following fields.

Figure 72: Condition Expression

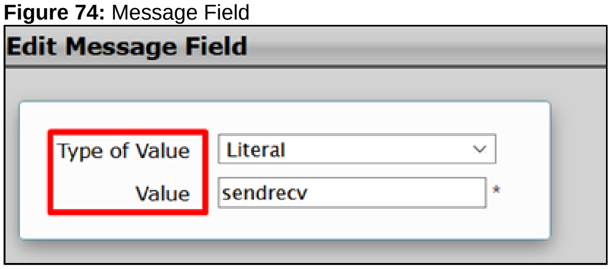


6. Select **Add** in the **Header Action** field.
7. When the **Header Value** field displays, select **Add**.
8. Click **Add/Edit**.

Figure 73: Header Value

9. Set the values as shown in the Edit Message Field window.

Figure 74: Message Field



10. Click **Apply** to save the changes.

Store_Content-Type Table

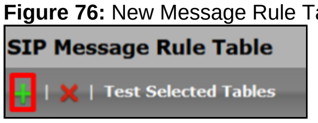
This Store_Content-Type table collects the rule for storing the **Content-Type** value in the **SG User Value 1**. This rule applies only to *180* and *183* response messages.

> ⓘ You must apply this table on the Signaling Group facing the *IPPBX*, and set it as Inbound Message Manipulation.

1. To add a new Message Rule Table, go to the **SIP > Message Manipulation > Message Rule Tables** menu path, and click on the **plus (+)** icon.

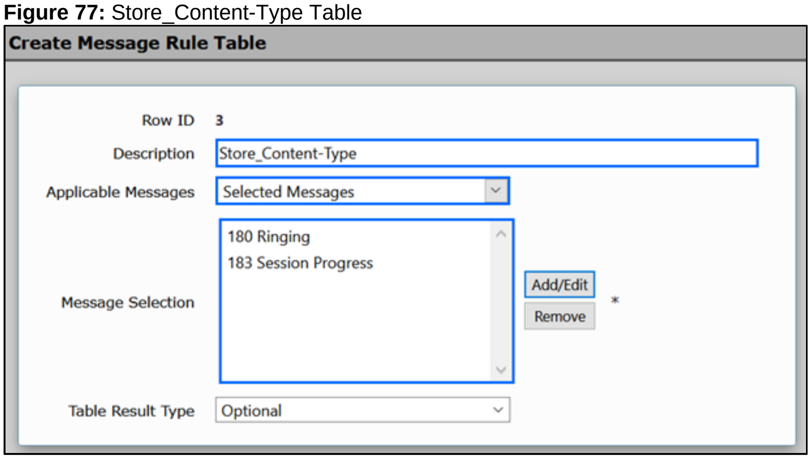
Figure 75: Message Rule Table menu path

Figure 76: New Message Rule Table



2. Set the new entry as shown in the following figure.

Figure 77: Store_Content-Type Table



The following table describes the rules for the Store_Content-Type table.

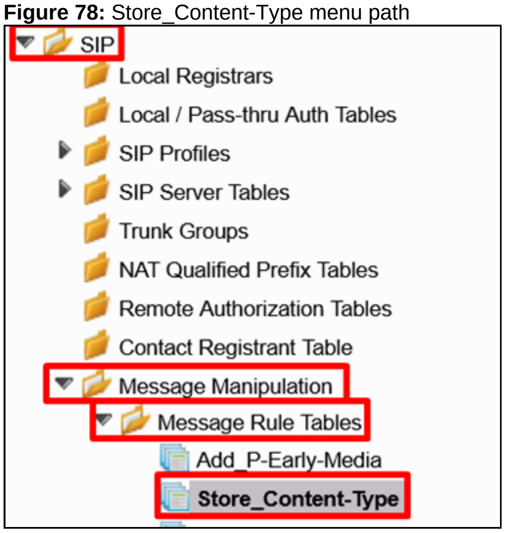
Store_Content-Type Rules

Description	Rule Type	Result Type	Comments
Store Content-Type	Header Rule	Optional	It stores the Content-Type value in the SG User Value 1.

Store Content-Type

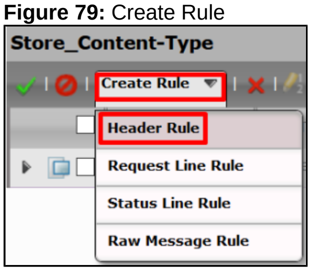
1. To add a new Message Rule, go to the left menu path, and click the **Store_Content-Type** table you just created.

Figure 78: Store_Content-Type menu path



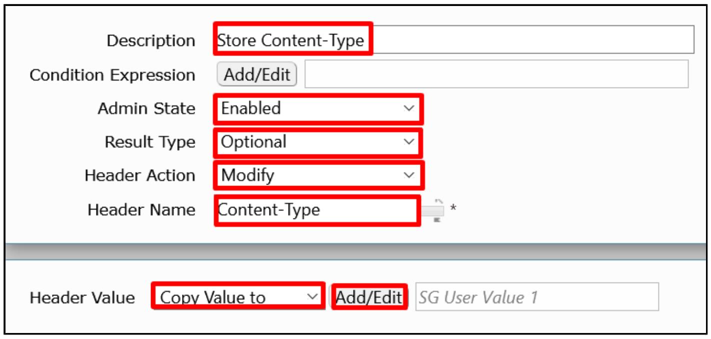
2. Click **Create Rule > Header Rule**.

Figure 79: Create Rule



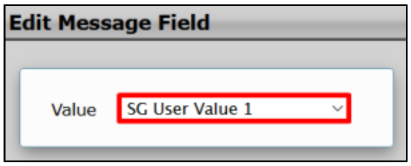
3. Set the new entry as shown in the following figure.
4. Select **Modify** in the **Header Action** field.
5. When the **Header Value** field displays, select **Copy Value to**.
6. Click **Add/Edit**.

Figure 80: Store Content-Type



7. Set the value as shown in the Edit Message Field window.

Figure 81: Edit Message Field



8. Click **Apply** to save the changes.

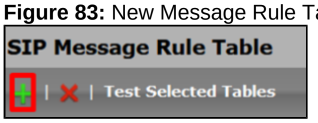
Store_User-Agent Table

The Store_User-Agent table collects the rules for storing the User-Agent and Server headers values received from the IPPBX.

1. To add a new Message Rule Table, go to the **SIP > Message Manipulation > Message Rule Tables** menu path, and click the **plus (+)** icon.

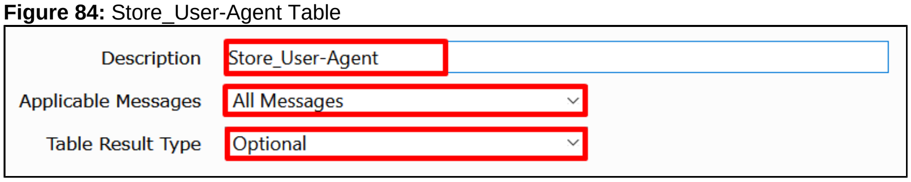
Figure 82: Message Rule Table menu path

Figure 83: New Message Rule Table



2. Set the new entry as shown in the following figure.

Figure 84: Store_User-Agent Table



The following table describes the rules for the Store_User-Agent table.

Store_User-Agent Rules

Description	Rule Type	Result Type	Comments
Store_User-Agent_Value	Header Rule	Optional	Stores the User-Agent value in the SG User Value 2.
Store_Server_Value	Header Rule	Optional	Stores the Server value in the SG User Value 3.

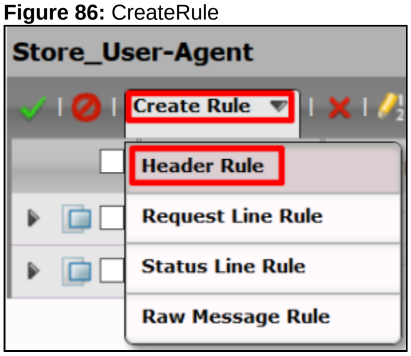
Store_User-Agent_Value

1. To add a new Message Rule, click the **Store_User-Agent** table on the left menu path.

Figure 85: Left Menu Path

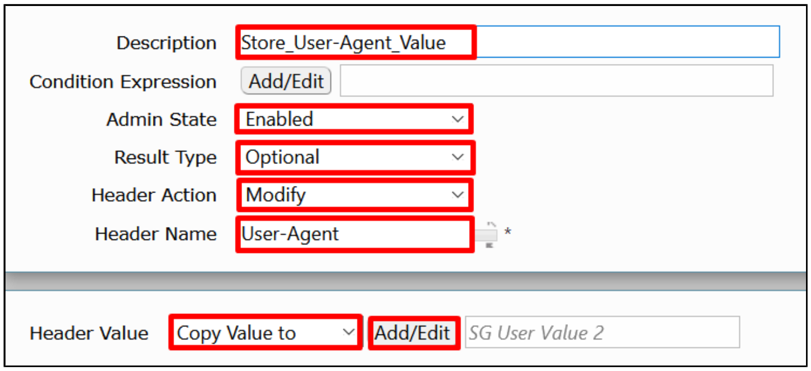
2. Click **Create Rule > Header Rule**.

Figure 86: CreateRule



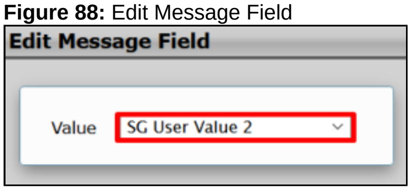
3. Set the new entry as shown in the following figure.
4. Select **Modify** in the **Header Action** field.
5. When the **Header Value** field displays, select **Copy Value to**.
6. Click **Add/Edit**.

Figure 87: Store_User-Agent_Value



7. Set the values as shown in the Edit Message Field window.

Figure 88: Edit Message Field



8. Click **Apply** to save the changes.

Store_Server_Value

1. To add a new Message Rule, click the **Store_User-Agent** table on the left menu path.

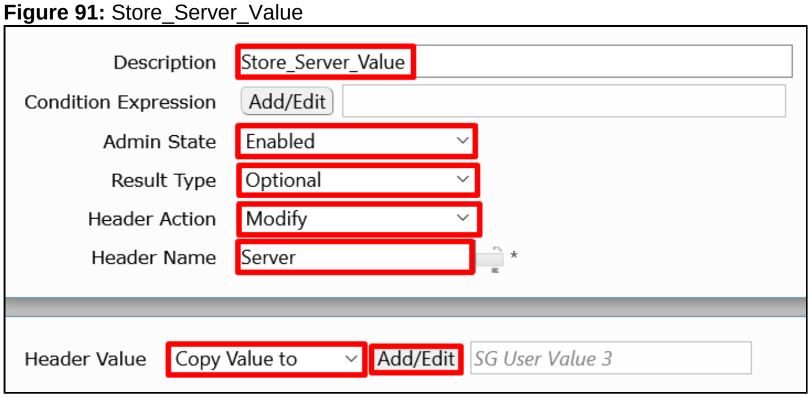
Figure 89: Left Menu Path

2. Click **Create Rule > Header Rule.**

Figure 90: CreateRule

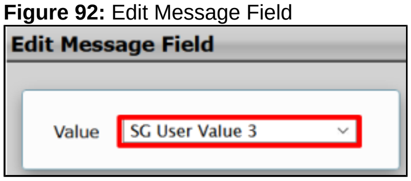
3. Set the new entry as shown in the following figure.
4. Select **Add** in the **Header Action** field.
5. When the **Header Value** field displays, select **Add**.
6. Click **Add/Edit**.

Figure 91: Store_Server_Value



7. Set the values as shown in the Edit Message Field window.

Figure 92: Edit Message Field



8. Click **Apply** to save the changes.

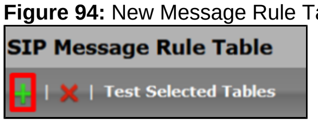
OBS_SIP_Profile_Adaptation_01 Table

The OBS_SIP_Profile_Adaptation_01 table collects rules for setting the format that the OBS requested. It applies to all messages.

1. To add a new Message Rule Table, go to the **SIP > Message Manipulation > Message Rule Tables** menu path, and click the **plus (+)** icon.

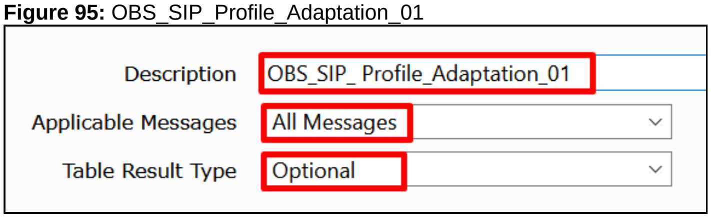
Figure 93: Message Rule Table menu path

Figure 94: New Message Rule Table



2. Set the new entry as shown in the following figure.

Figure 95: OBS_SIP_Profile_Adaptation_01



The following table describes the rules for the OBS_SIP_Profile_Adaptation_01table.

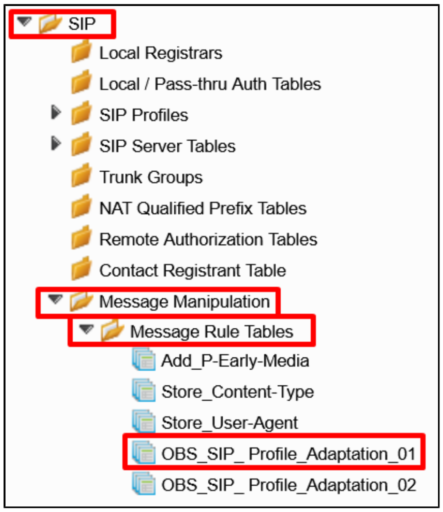
OBS_SIP_Profile_Adaptation_01 Rules

Description	Rule Type	Result Type	Comments
Remove_SGID_From_Header	Header Rule	Optional	Removes the *SGDI* parameter from the *FROM* header.
Remove_SGID_To_Header	Header Rule	Optional	Removes the *SGDI* parameter from the *TO* header.
Modify_User-Agent_Header	Header Rule	Optional	Sets the *User-Agent* value as per OBS requirements.
Modify_Server_header	Header Rule	Optional	Sets the *Server* value as per OBS requirements.
Modify_Allow_header	Header Rule	Optional	Sets the *Allow* value as per OBS requirements.

Remove_SGID_From_Header

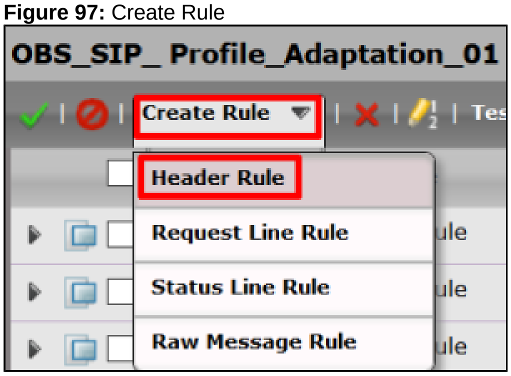
1. To add a new Message Rule, access the left menu path, and click the **OBS_SIP_Profile_Adaptation_01** table you just created.

Figure 96: Left Menu Path



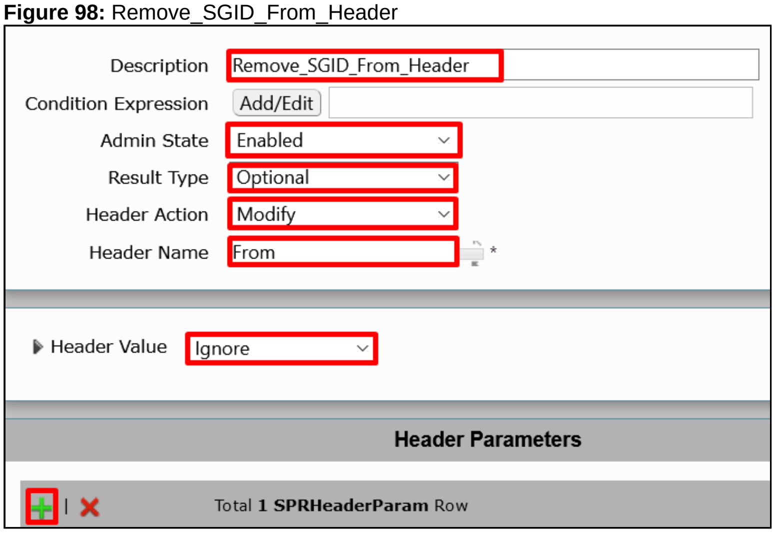
2. Click **Create Rule > Header Rule**.

Figure 97: Create Rule



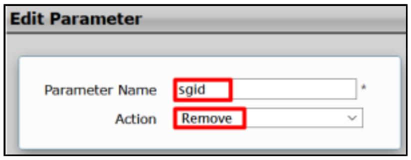
3. Set the new entry as shown in the following figure.
4. Select **Modify** in the **Header Action** field.
5. When the **Header Value** field displays, select **Ignore**.
6. Click the **Add/Edit** icon under the Header Parameters.

Figure 98: Remove_SGID_From_Header



7. Set the field values as shown in the Edit Parameter window.

Figure 99: Edit Parameter

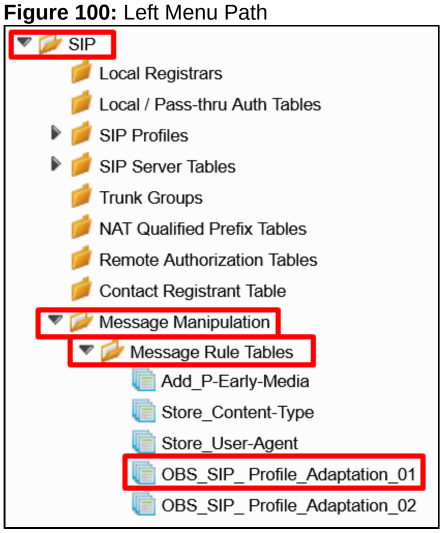


8. Click **Apply** to save the changes.

Remove_SGID_To_Header

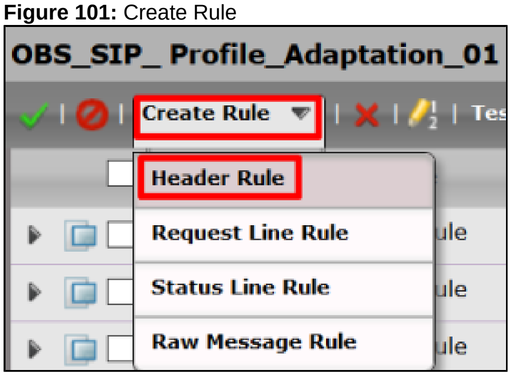
1. To add a new Message Rule, click the **OBS_SIP_Profile_Adaptation_01** table on the left menu path.

Figure 100: Left Menu Path



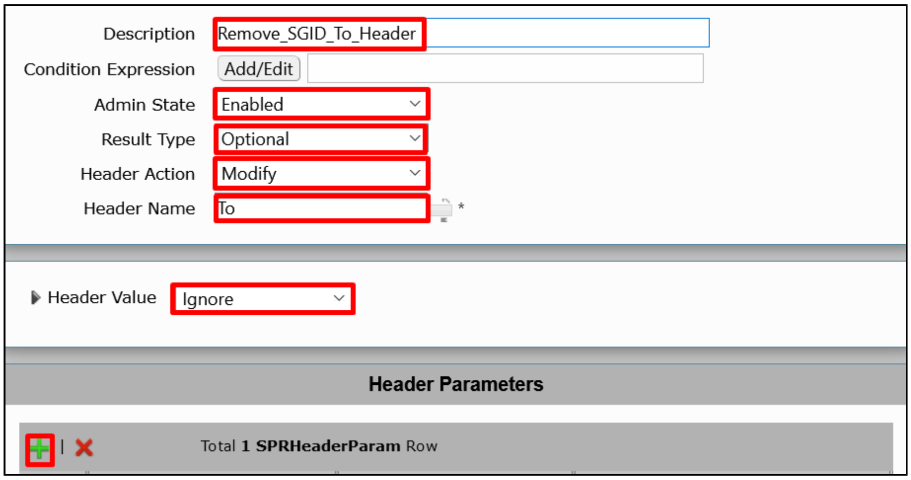
2. Click **Create Rule > Header Rule**.

Figure 101: Create Rule



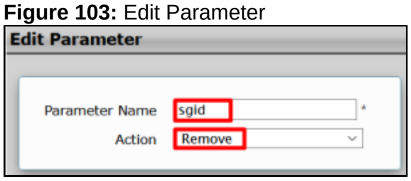
3. Set the new entry as shown in the following figure.
4. Select **Modify** in the **Header Action** field.
5. When the **Header Value** field displays, select **Ignore**.
6. Click the **plus (+)** icon under the Header Parameters.

Figure 102: Remove_SGID_To_Header



7. Set the field values as shown in the Edit Parameter window.

Figure 103: Edit Parameter

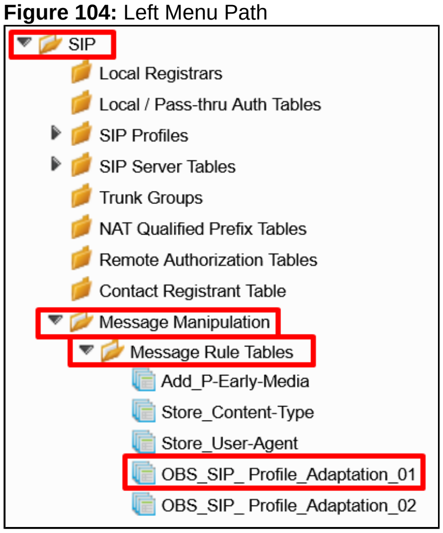


8. Click **Apply** to save the changes.

Modify_User-Agent_Header

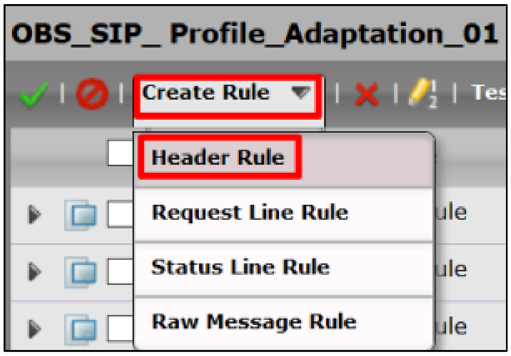
1. To add a new Message Rule, click the **OBS_SIP_Profile_Adaptation_01** table on the left menu path.

Figure 104: Left Menu Path



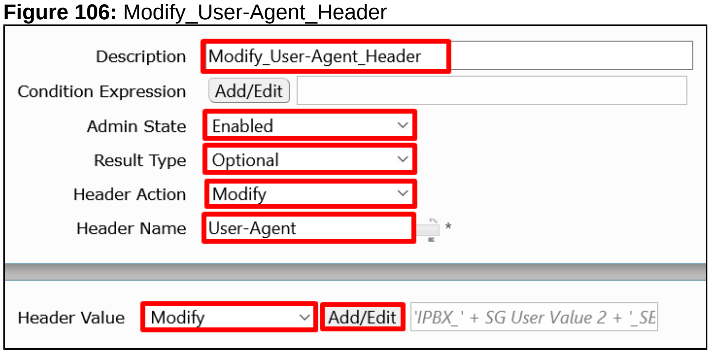
2. Click **Create Rule > Header Rule**.

Figure 105: Create Rule



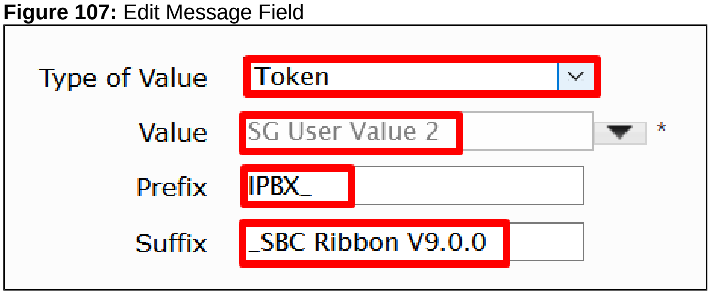
3. Set the new entry as shown in the following figure.
4. Select **Modify** in the **Header Action** field.
5. When the **Header Value** field displays, select **Modify**.
6. Click **Add/Edit**.

Figure 106: Modify_User-Agent_Header



7. Set the field values as shown in the Edit Message Field window.

Figure 107: Edit Message Field

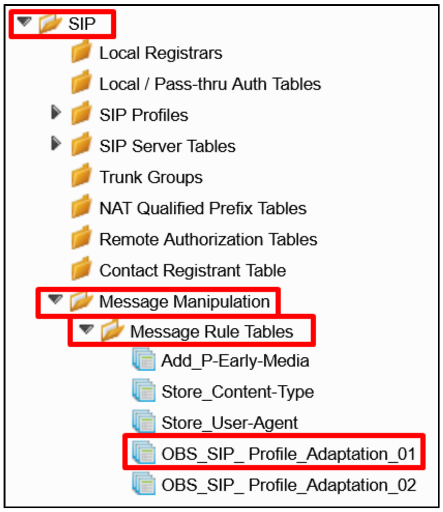


8. Click **Apply** to save the changes.

Modify_Server_Header

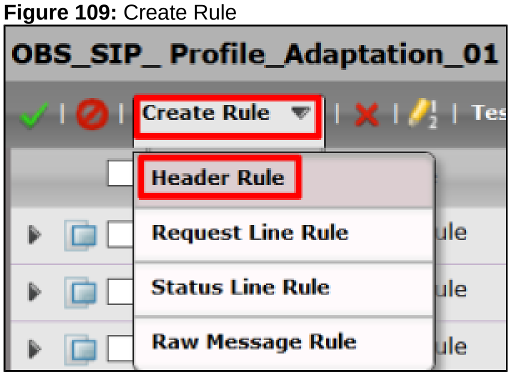
1. To add a new Message Rule, click the **OBS_SIP_Profile_Adaptation_01** table on the left menu path.

Figure 108: Left Menu Path



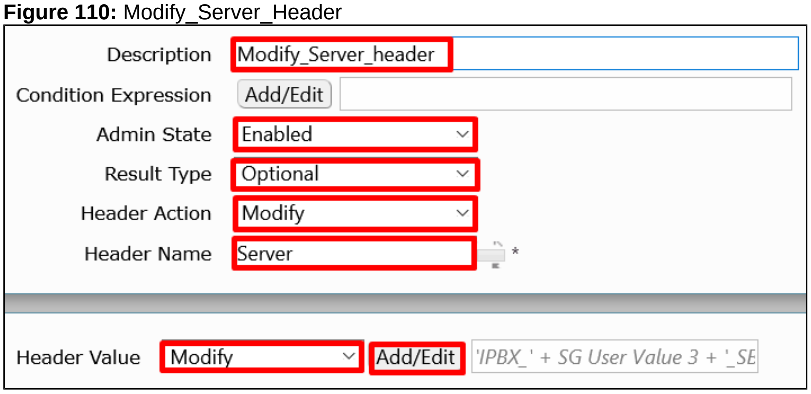
2. Click **Create Rule > Header Rule**.

Figure 109: Create Rule



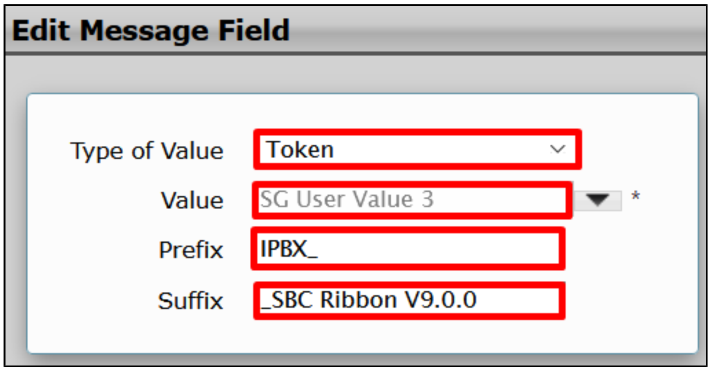
3. Set the new entry as shown in the following figure.
4. Select **Modify** in the **Header Action** field.
5. When the **Header Value** field displays, select **Modify**.
6. Click **Add/Edit**.

Figure 110: Modify_Server_Header



7. Set the field values as shown in the Edit Message Field window.

Figure 111: Edit Message Field

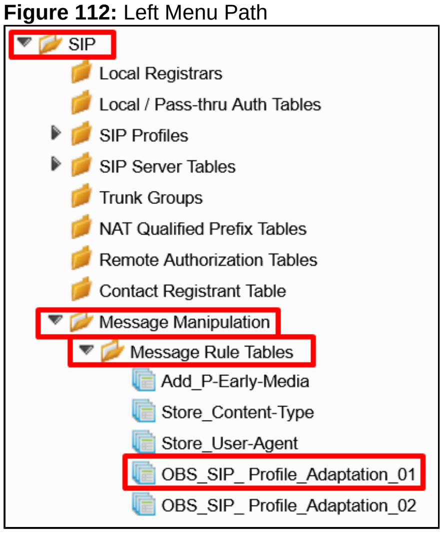


8. Click **Apply** to save the changes.

Modify_Allow_header

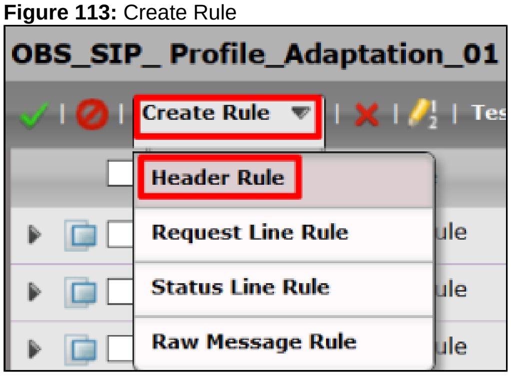
1. To add a new Message Rule, click the **OBS_SIP_Profile_Adaptation_01** table on the left menu path.

Figure 112: Left Menu Path



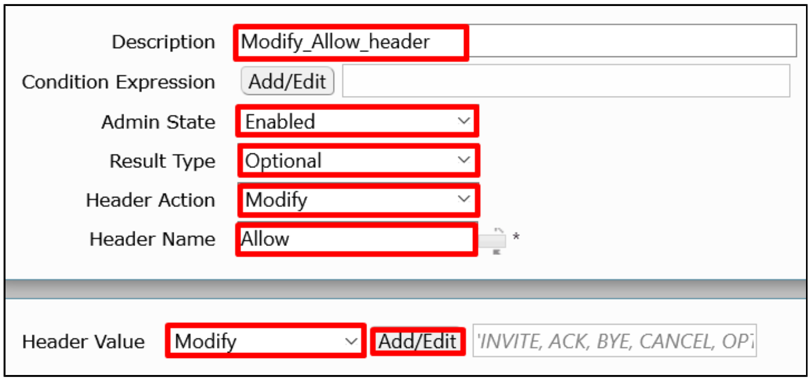
2. Click **Create Rule > Header Rule.**

Figure 113: Create Rule



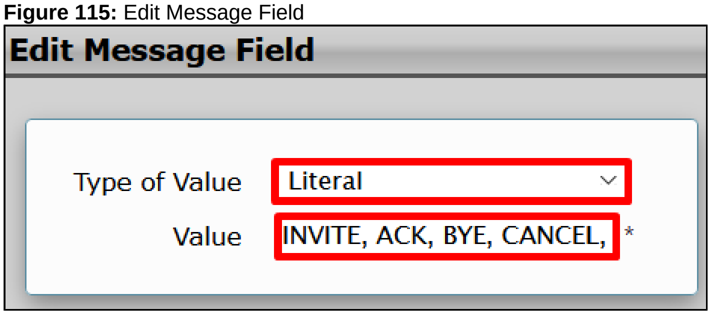
3. Set the new entry as shown in the following figure.
4. Select **Modify** in the **Header Action** field.
5. When the **Header Value** field displays, select **Modify**.
6. Click **Add/Edit**.

Figure 114: Modify_Allow_Header



7. Set the field values as shown in the Edit Message Field window.

Figure 115: Edit Message Field



> **Edit Message Field**
> Make sure the **Value** field contains the following values:
>
> INVITE, ACK, BYE, CANCEL, OPTIONS, UPDATE

8. Click **Apply** to save the changes.

OBS_SIP_Profile_Adaptation_02 Table

The OBS_SIP_Profile_Adaptation_02 table collects rules for setting the format that the OBS requested. It applies to all messages.

1. To add a new Message Rule Table, access the **SIP > Message Manipulation > Message Rule Tables** menu path, and click the **plus (+)** icon.

Figure 116: Message Rule Table menu path

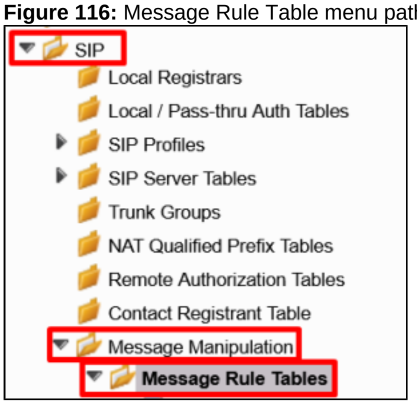
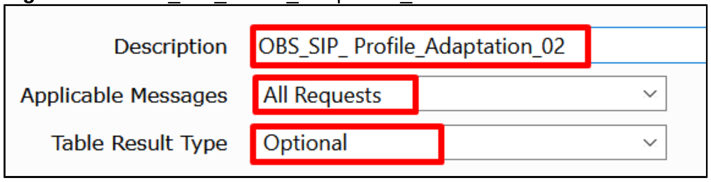


Figure 117: New Message Rule Table

2. Set the new entry as shown in the following figure.

Figure 118: OBS_SIP_Profile_Adaptation_02



The following table describes the rules for the OBS_SIP_Profile_Adaptation_02 table.

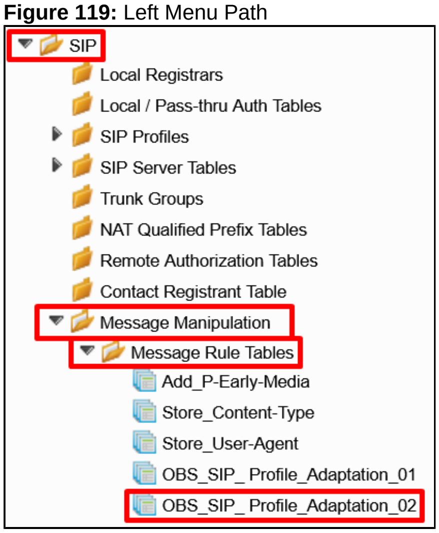
OBS_SIP_Profile_Adaptation_02 Rules

Description	Rule Type	Result Type	Comments
Modify_PAI	Header Rule	Optional	Sets the host part of the URI as the local SWeLite IP address.
Add plus P-Asserted-Identity	Header Rule	Optional	Adds a **plus (+)** icon in the user part of the URI.
Modify_From_Anonymous	Header Rule	Optional	When the SBC receives an **anonymous** call, the **FROM** header is modified according to OBS requirements.
Modify_Diversion	Header Rule	Optional	Adds a **plus (+) icon** in the user part of the URI and adds the **counter** parameter.

Modify_PAI

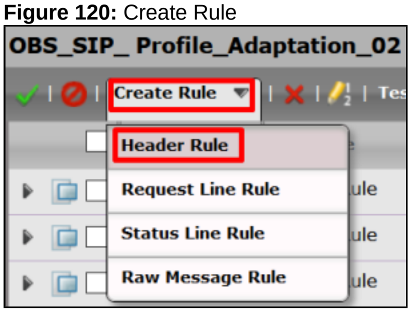
1. To add a new Message Rule, access the left menu path, and click the **OBS_SIP_Profile_Adaptation_02** table you just created.

Figure 119: Left Menu Path



2. Click **Create Rule > Header Rule.**

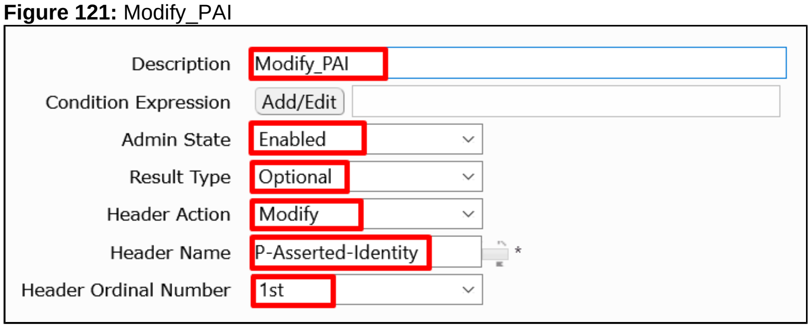
Figure 120: Create Rule



3. Set the new entry as shown in the following figure.

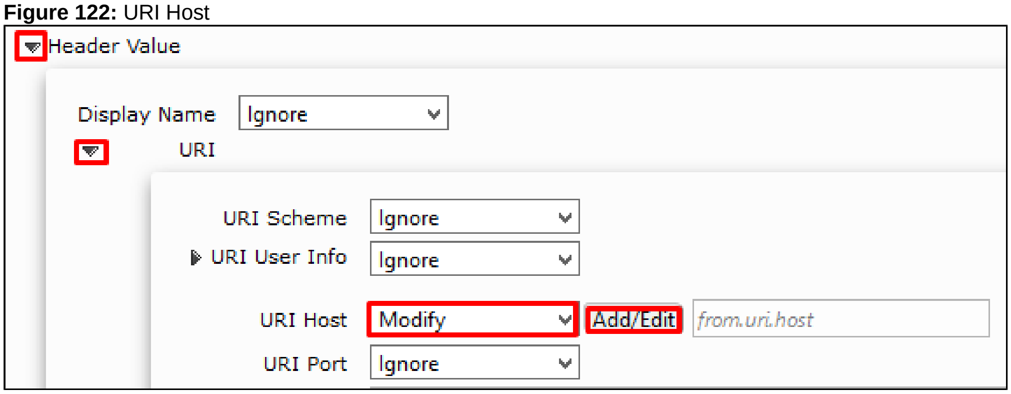
4. Select **Modify** in the **Header Action** field.

Figure 121: Modify_PAI



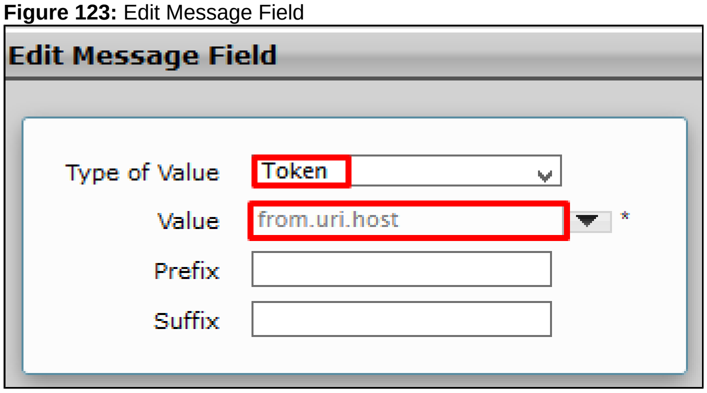
5. When the Header Value window displays, click the arrow beside the **Header Value** and then click the arrow beside the **URI.**
6. Click **Add/Edit**.

Figure 122: URI Host



7. Set the field values as shown in the Edit Message Field window.

Figure 123: Edit Message Field

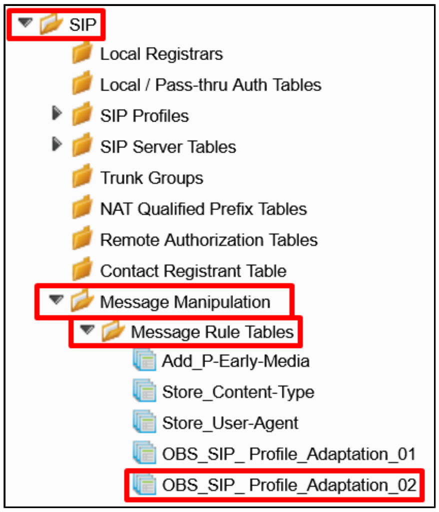


8. Click **Apply** to save the changes.

Add plus P-Asserted-Identity

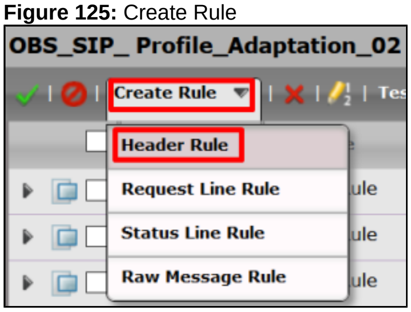
1. To add a new Message Rule, click the **OBS_SIP_Profile_Adaptation_02** table on the left menu path.

Figure 124: Left Menu Path



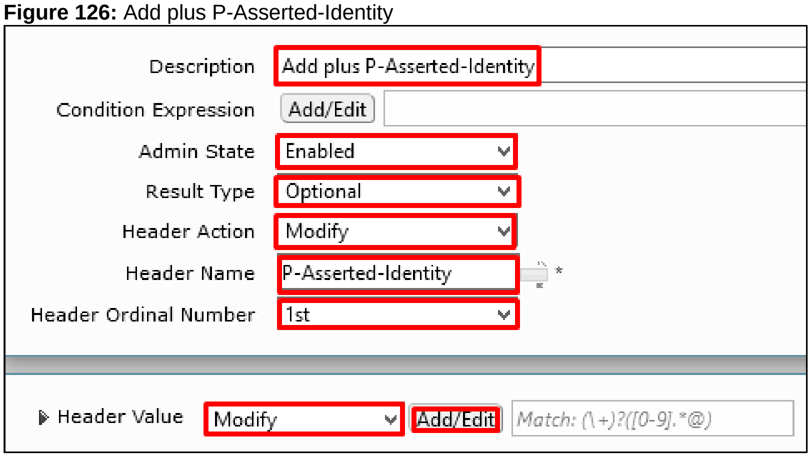
2. Click **Create Rule > Header Rule.**

Figure 125: Create Rule



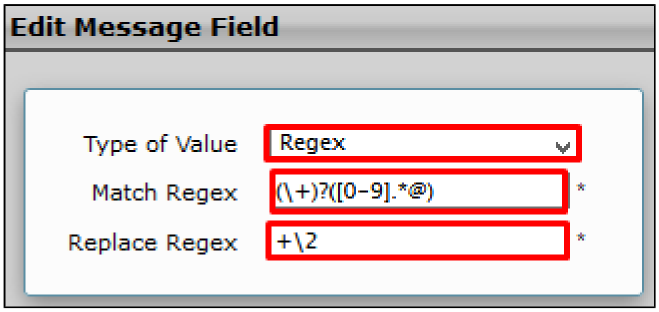
3. Set the new entry as shown in the following figure.
4. Select **Modify** in the **Header Action** field.
5. When the **Header Value** field displays, select **Modify**.
6. Click **Add/Edit**.

Figure 126: Add plus P-Asserted-Identity



7. Set the field values as shown in the Edit Message Field window.

Figure 127: Edit Message Field

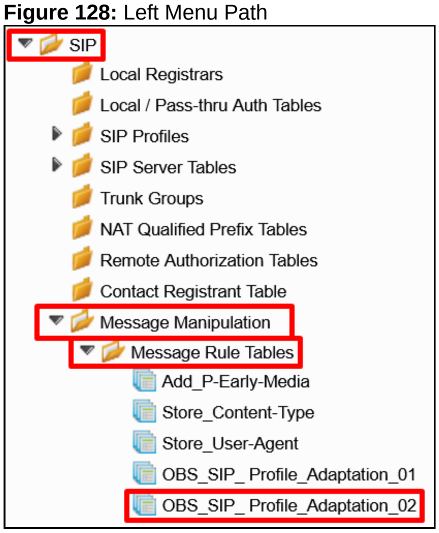


8. Click **Apply** to save the changes.

Modify_From_Anonymous

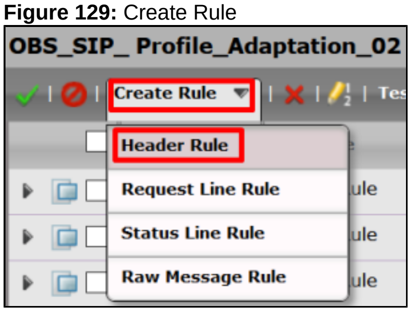
1. To add a new Message Rule, click the **OBS_SIP_Profile_Adaptation_02** table on the left menu path.

Figure 128: Left Menu Path



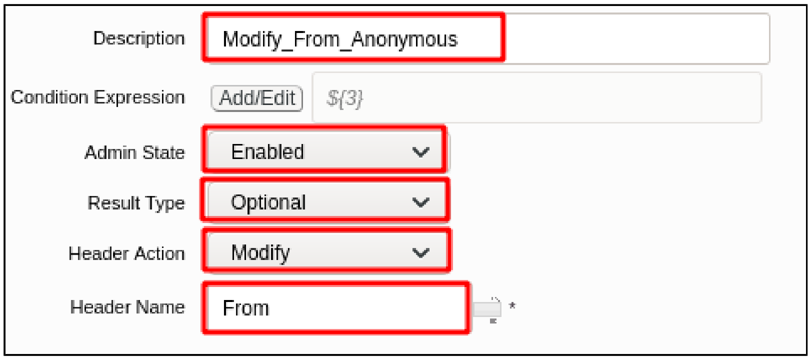
2. Click **Create Rule > Header Rule**.

Figure 129: Create Rule



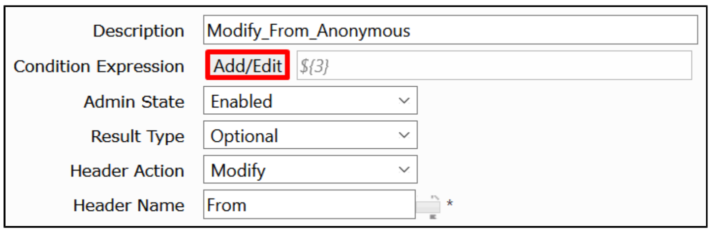
3. Set the new entry as shown in the following figure.

Figure 130: Modify_From_Anonymous



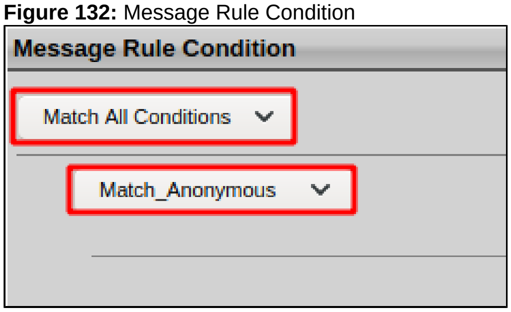
4. Click **Add/Edit** in the **Condition Expression** field to set the Message Rule Condition.

Figure 131: Condition Expression



5. Set the Message Rule Condition as shown in the following figure.

Figure 132: Message Rule Condition

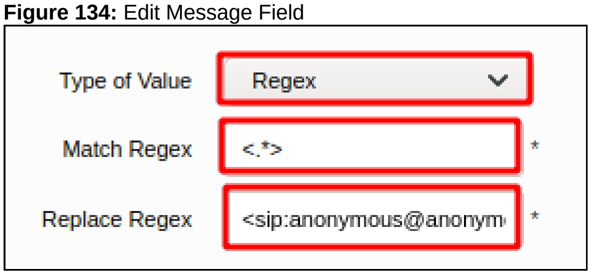


6. Select **Modify** in the **Header Action** field.
7. When the **Header Value** field displays, select **Modify**.
8. Click **Add/Edit**.

Figure 133: Header Value

9. Set the field values as shown in the Edit Message Field window.

Figure 134: Edit Message Field



Edit Message Field

Make sure the **Replace Regex** field contains the following values:

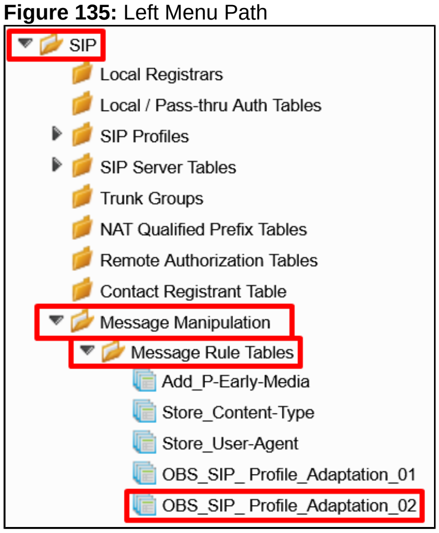
<sip:anonymous@anonymous.invalid>

10. Click **Apply** to save the changes.

Modify_Diversion

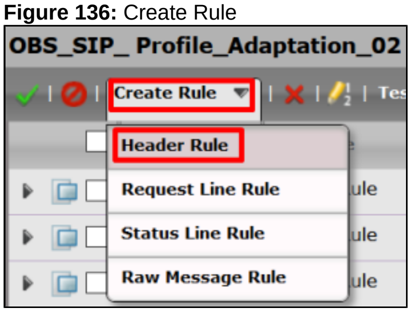
1. To add a new Message Rule, click the **OBS_SIP_Profile_Adaptation_02** table on the left menu path.

Figure 135: Left Menu Path



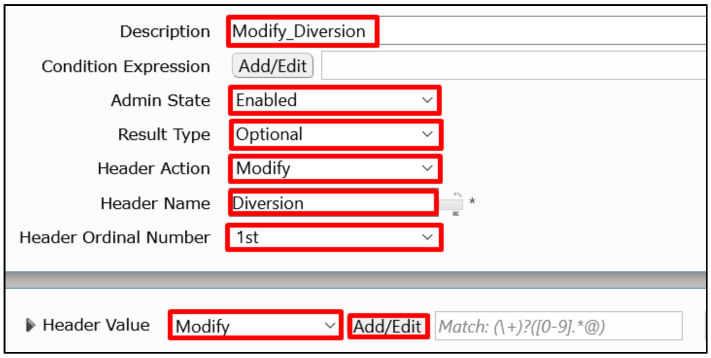
2. Click **Create Rule > Header Rule**.

Figure 136: Create Rule



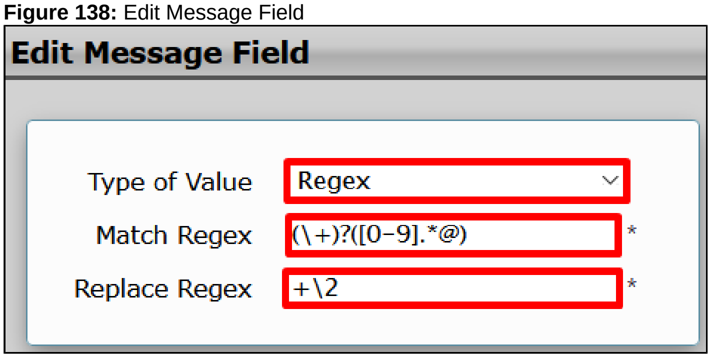
3. Set the new entry as shown in the following figure.
4. Select **Modify** in the **Header Action** field.
5. When the **Header Value** field displays, select **Modify**.
6. Click **Add/Edit**.

Figure 137: Add plus P-Asserted-Identity



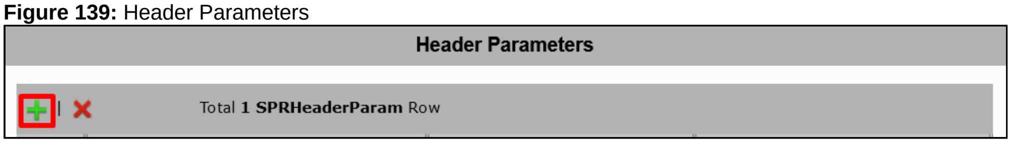
7. Set the field values as shown in the Edit Message Field window.

Figure 138: Edit Message Field



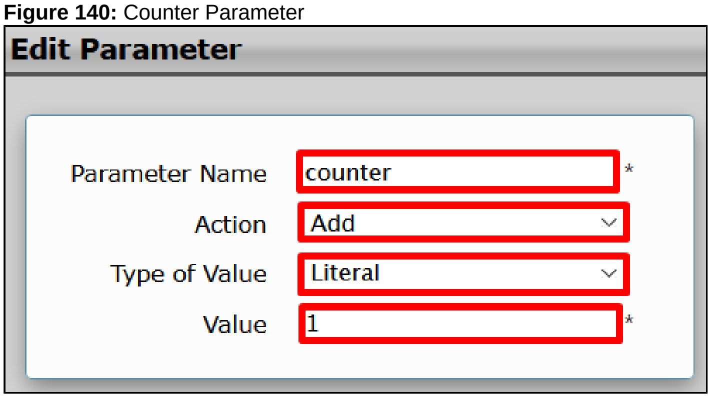
8. Click the **plus (+)** icon under the Header Parameters.

Figure 139: Header Parameters



9. Set the field values as shown in the Edit Message Field window.

Figure 140: Counter Parameter



10. Click **Apply** to save the changes.

Media Profiles

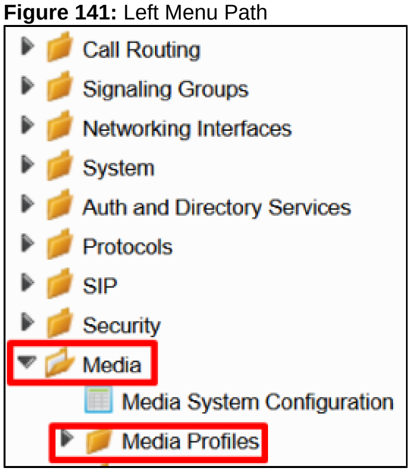
The **Media > Media Profiles** menu path allows you to specify the individual voice and fax compression codecs and their associated settings to include in a Media List. Different codecs provide varying levels of compression, allowing a user to reduce the bandwidth requirements at the expense of voice quality.

Table 3: OBS codecs

Description	Codec	Payload Size
G.722	G.722	20 ms
Default G711A	G.711 A-Law	20 ms
G.729	G.729	20 ms
Default G711U	G.711 U-Law	20 ms
T38	T.38 Fax	

To Create a new Media Profile, go to **Media > Media Profiles** on the left menu path.

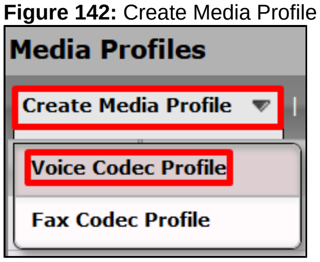
Figure 141: Left Menu Path



G.722 Codec

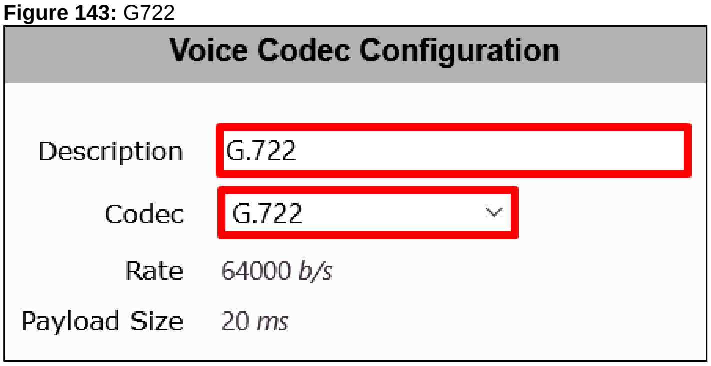
1. To create a profile for the G.722 codec, click **Create Media Profile > Voice Codec Profile.**

Figure 142: Create Media Profile



2. Specify the following values to set the new **G.722** codec.

Figure 143: G722

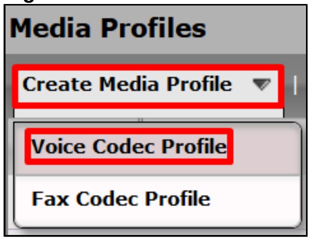


3. Click **Apply** to save the changes.

Default G711A

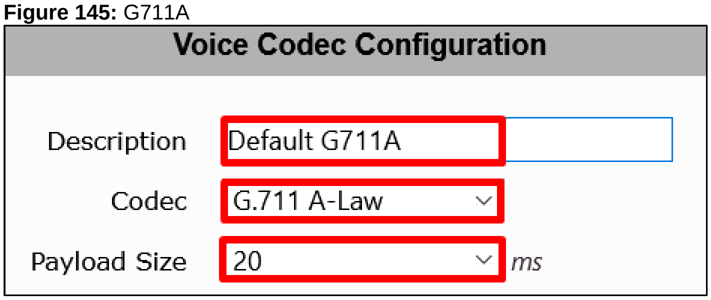
1. To create a profile for the G711A codec, click **Create Media Profile > Voice Codec Profile.**

Figure 144: Create Media Profile



2. Specify the following values to set the **G.711 A-law** codec.

Figure 145: G711A

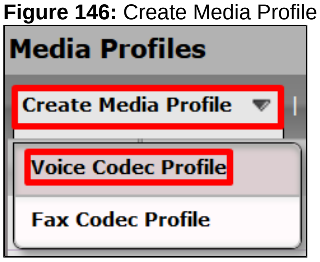


3. Click **Apply** to save the changes.

G.729

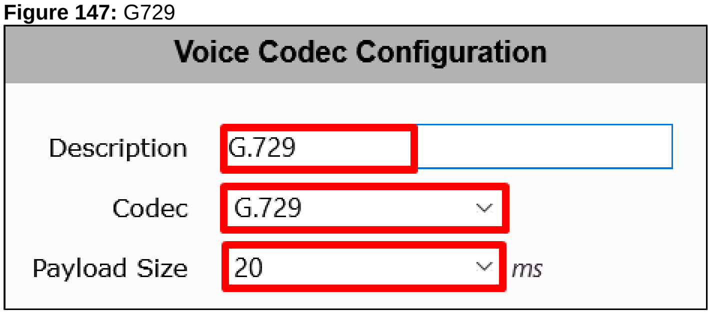
1. To create a profile for the G.729 codec, click **Create Media Profile > Voice Codec Profile.**

Figure 146: Create Media Profile



2. Specify the following values to set the **G.729** codec.

Figure 147: G729

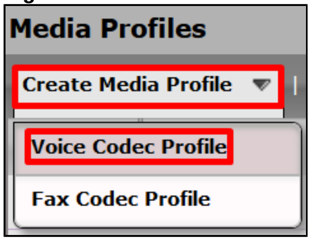


3. Click **Apply** to save the changes.

Default G711U

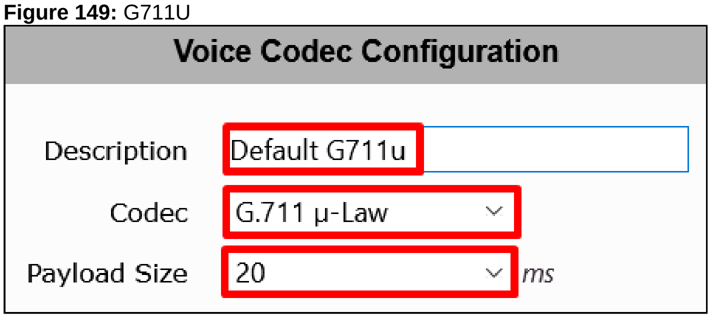
1. To create a profile for the default G711U codec, click **Create Media Profile > Voice Codec Profile.**

Figure 148: Create Media Profile



2. Specify the following values to set the **G.711 U-law** codec.

Figure 149: G711U

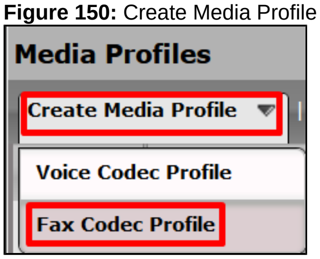


3. Click **Apply** to save the changes.

T38

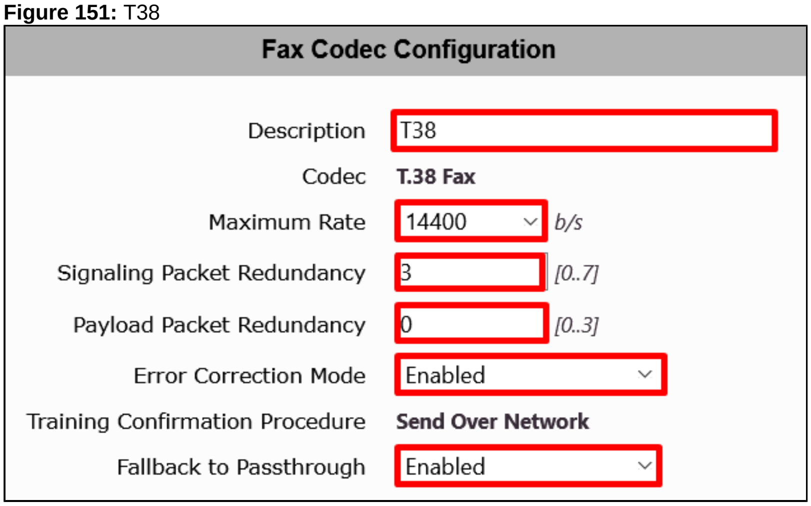
1. To create a profile for the T.38 codec, click **Create Media Profile > Fax Codec Profile.**

Figure 150: Create Media Profile



2. Specify the following values to set the **T.38** codec.

Figure 151: T38



3. Click **Apply** to save the changes.

SDES-SRTP Profiles

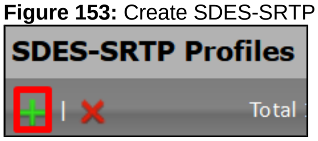
SDES-SRTP Profiles define a cryptographic context and used in SRTP negotiation. SDES-SRTP Profiles are required for enabling encryption, and SRTP are applied to Media Lists.

1. On the left menu path, go to **Media > SDES-SRTP Profiles.**

Figure 152: SDES-SRTP Profiles Menu Path

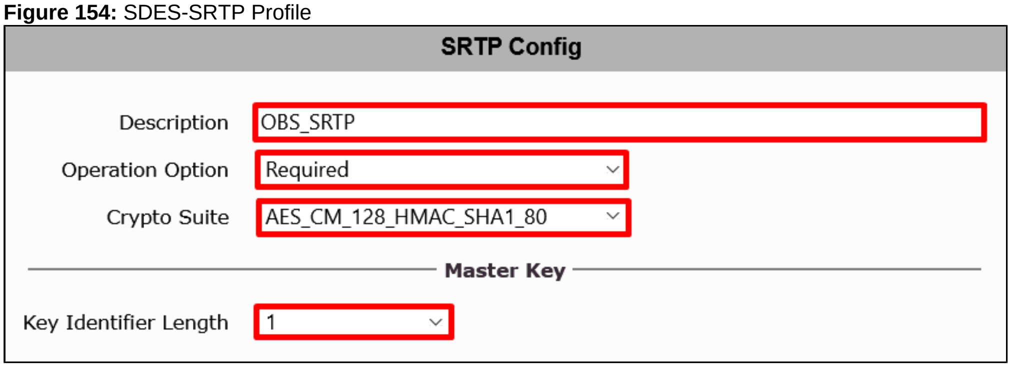
2. Click the **plus (+)** icon to add a new entry.

Figure 153: Create SDES-SRTP Profile



3. Specify the following values to set the new **SDES-SRTP Profile.**

Figure 154: SDES-SRTP Profile



4. Click **Apply** to save the changes.

Media Lists

The **Media > Media List** menu path enables you to specify a set of codecs and fax profiles that are allowed on a given SIP Signaling Group. Media Lists contain one or more Media Profiles that you define in Media Profiles. These lists allow you to accommodate specific transmission requirements and SIP devices that only implement a subset of the available voice codecs.

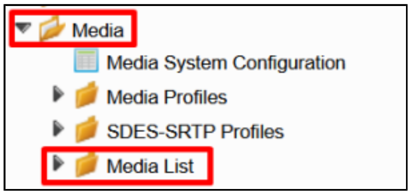
Table 4: Media Lists

Description	Media Profiles List	SDES-SRTP Profile	Media DSCP	Silence Suppression	Modem Passthrough	Fax Passthrough	Fax Tone Detection
CUCM_MediaList	Default G711A G.729	None	46	Disabled	Enabled	Enabled	Enabled
Orange_MediaList-TLS	Default G711A G.729 T38	OBS_SRTP	46	Disabled	Enabled	Enabled	Enabled

CUCM_MediaList

1. To add a Media List, go to **Media > Media List** on the left menu path.

Figure 155: Media List Menu Path

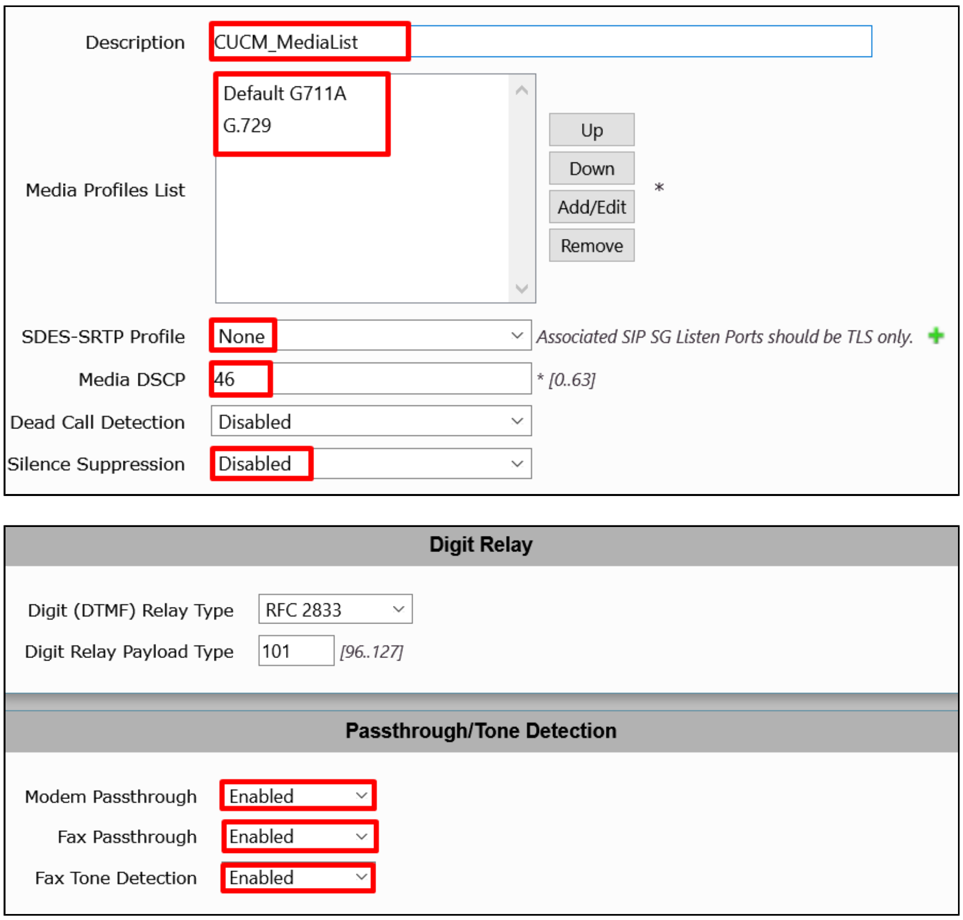


2. Click **the plus (+)** icon to add a new entry.

Figure 156: New Media List

3. Specify the following values to configure the new entry.

Figure 157: CUCM_MediaList

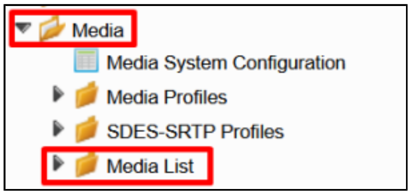


4. Click **Apply** to save the changes.

Orange_MediaList-TLS

1. To add a Media List, go to **Media > Media List** on the left menu path.

Figure 158: Media List Menu Path

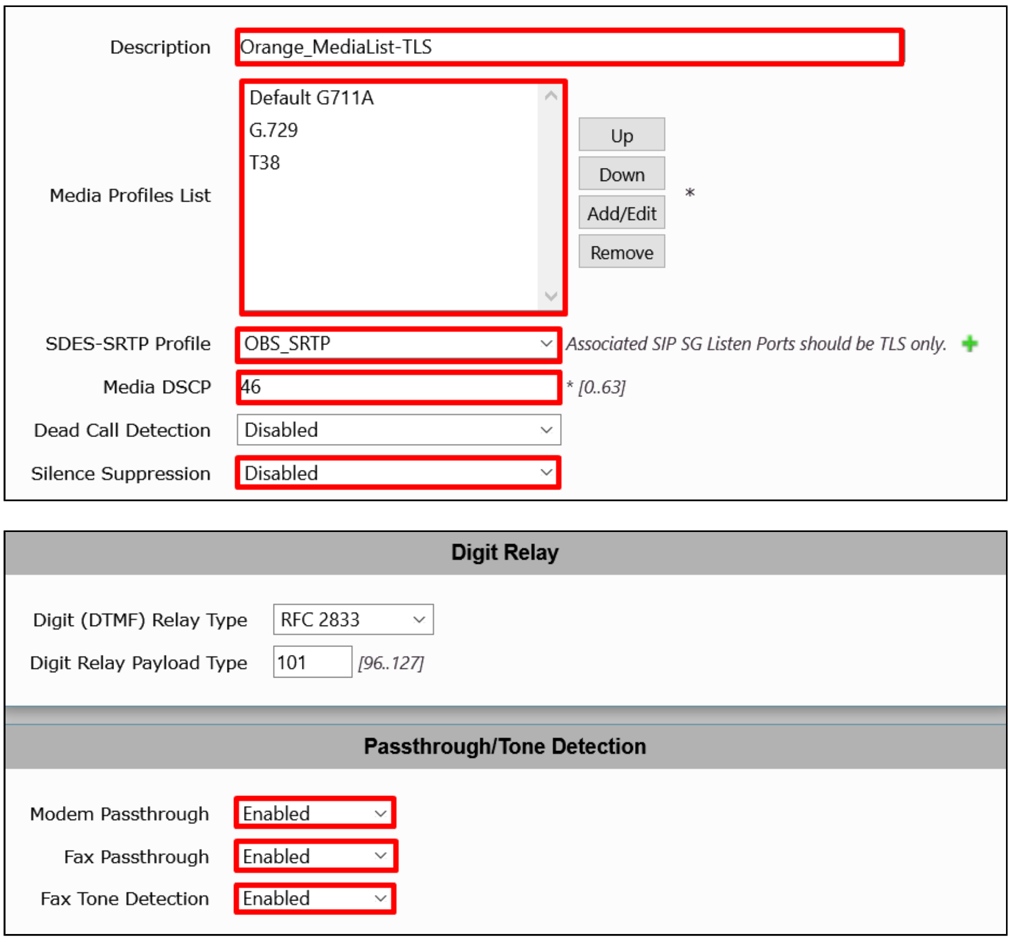


2. Click the **plus (+)** icon to add a new entry.

Figure 159: New Media List

3. Specify the following values to configure the new entry.

Figure 160: Orange_MediaList-TLS



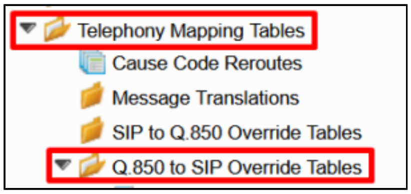
4. Click **Apply** to save the changes.

Q.850 to SIP Override Table

SIP and ISDN use different response messages to communicate why a call failed or could not connect (Q.850 for ISDN and SIP Responses for SIP). By default, the SBC Edge uses RFC 4497 to map these responses to each other. The **Telephony Mapping Tables > Q.850 to SIP Override Tables** menu path allows you to override one or more of these mappings to a different message, an effective method for inter-operating with nonstandard equipment.

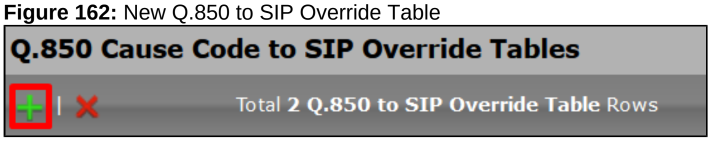
1. To add a new Q.850 to SIP Override Table, go to **Telephony Mapping Tables > Q.850 to SIP Override Tables** on the left menu path.

Figure 161: Q.850 to SIP Override Menu Path



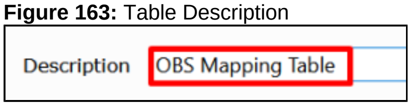
2. To add a new Q.850 to SIP Override Table, click the **plus (+)** icon.

Figure 162: New Q.850 to SIP Override Table



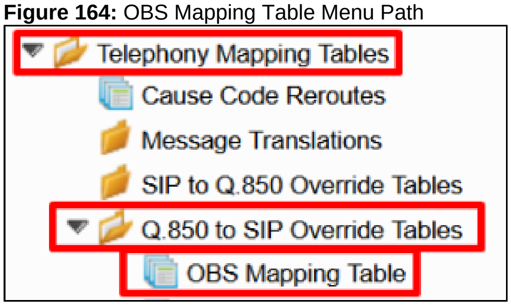
3. Specify the **Description** value.

Figure 163: Table Description



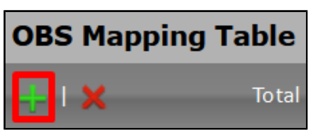
4. On the left menu path, click on the **OBS Mapping Table**.

Figure 164: OBS Mapping Table Menu Path



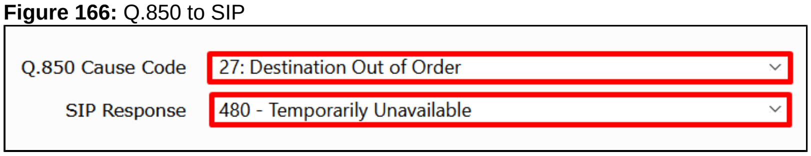
5. Click the **plus (+)** icon to add a new entry.

Figure 165: New Entry



6. Specify the following values to configure the new entry.

Figure 166: Q.850 to SIP



7. Click **Apply** to save the changes.

Signaling Groups

Signaling groups can group telephony channels for routing and shared configuration. You use the Signaling groups to route calls, select call routes, and select Tone Tables and Action Sets.

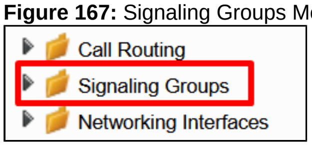
From-To_CUCM

Table 5: CUCM Signaling Group Parameters

Description	Call Routing Table	SIP Profile	SIP Server Table	Media List ID	Federated IP/FQDN	Signaling DSCP	Inbound Message Manipulation	Outbound Message Manipulation
From-To_CUCM	To_Orange	CUCM_SIP Profile	CUCM	CUCM_MediaList	<CUCM IP Address>	40	Store_Content-Type Store_User-Agent	

1. To add a new Signaling Group, go to the **Signaling Groups** menu path.

Figure 167: Signaling Groups Menu Path

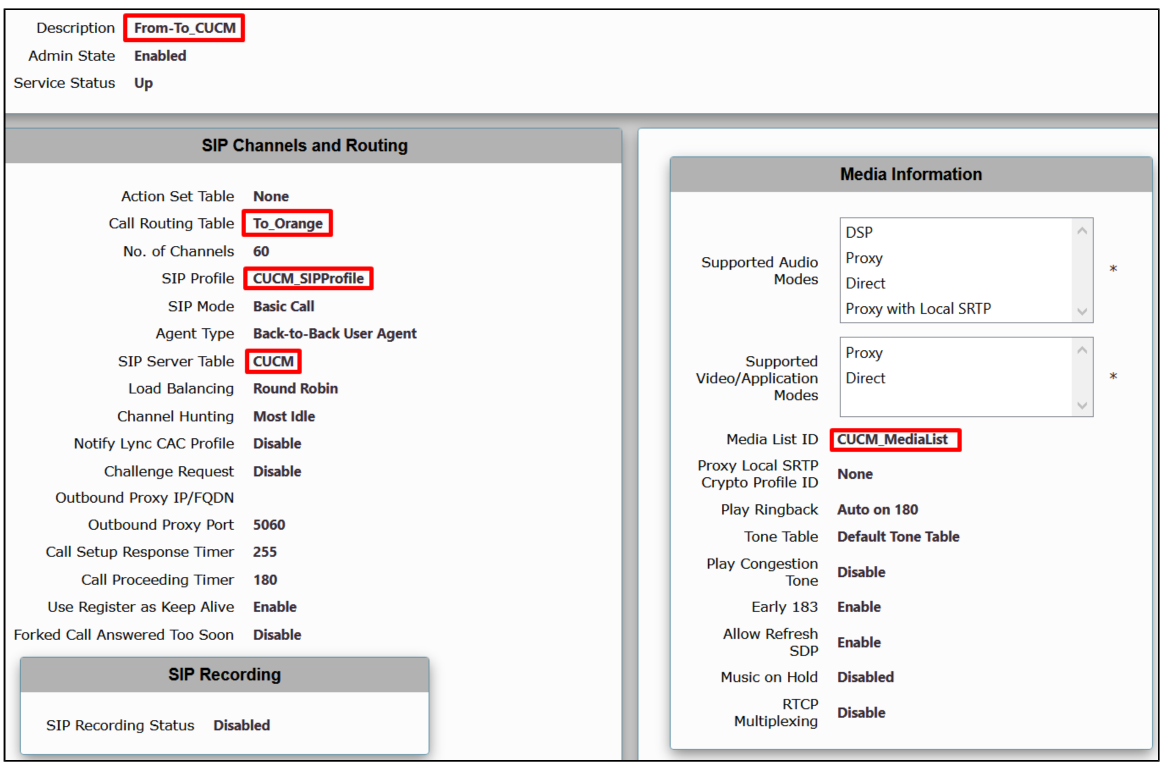


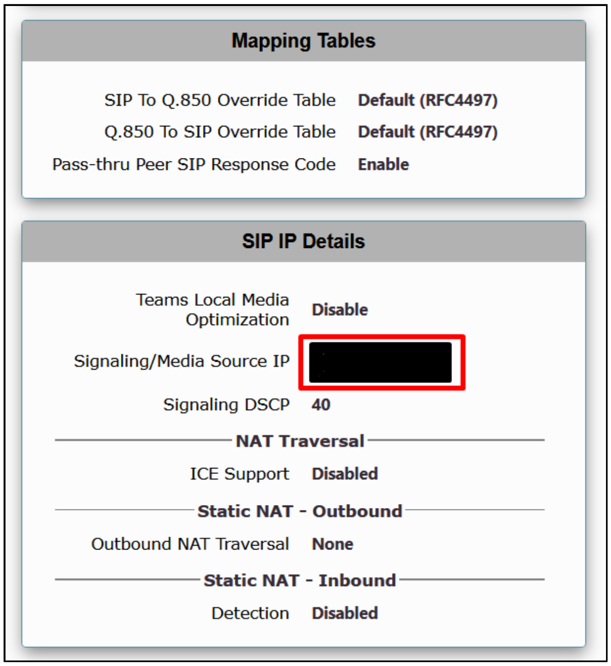
2. Click **Add SIP SG**.

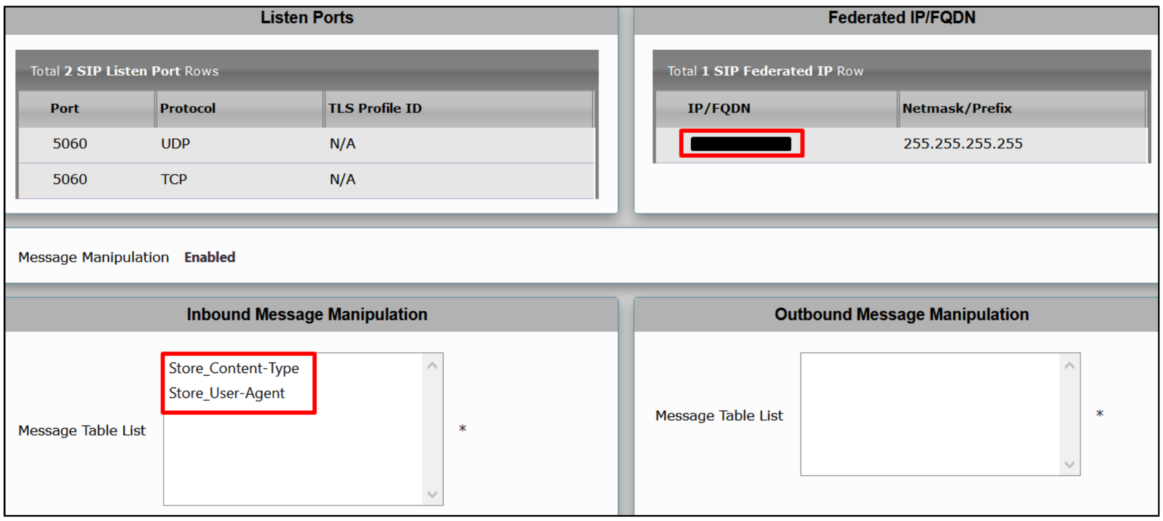
Figure 168: New Signaling Group

3. Set the new entry as shown in the following figures.

Figure 169: From-To_CUCM







4. Click **Apply** to save the changes.

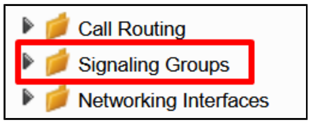
From-To_OBSTLS

Table 6: From-To_OBSTLS Signaling Group Parameters

Description	Call Routing Table	SIP Profile	SIP Server Table	Media List ID	Federated IP/FQDN	Proxy Local SRTP Crypto Profile ID	Signaling DSCP	Q.850 to SIP Override Table	Outbound Message Manipulation
From-To_OBSTLS	To_Private	Orange_SIPProfile-TLS	sbc1.btoi.one.equant.net	Orange_MediaList-TLS	<OBS IP Addresses>	OBS_SRTP	46	OBS Mapping Table	OBS_SIP_Profile_Adaptation_02 OBS_SIP_Profile_Adaptation_01 Add_P-Early-Media

1. To add a new Signaling Group, go to the **Signaling Groups** menu path.

Figure 170: Signaling Groups Menu Path

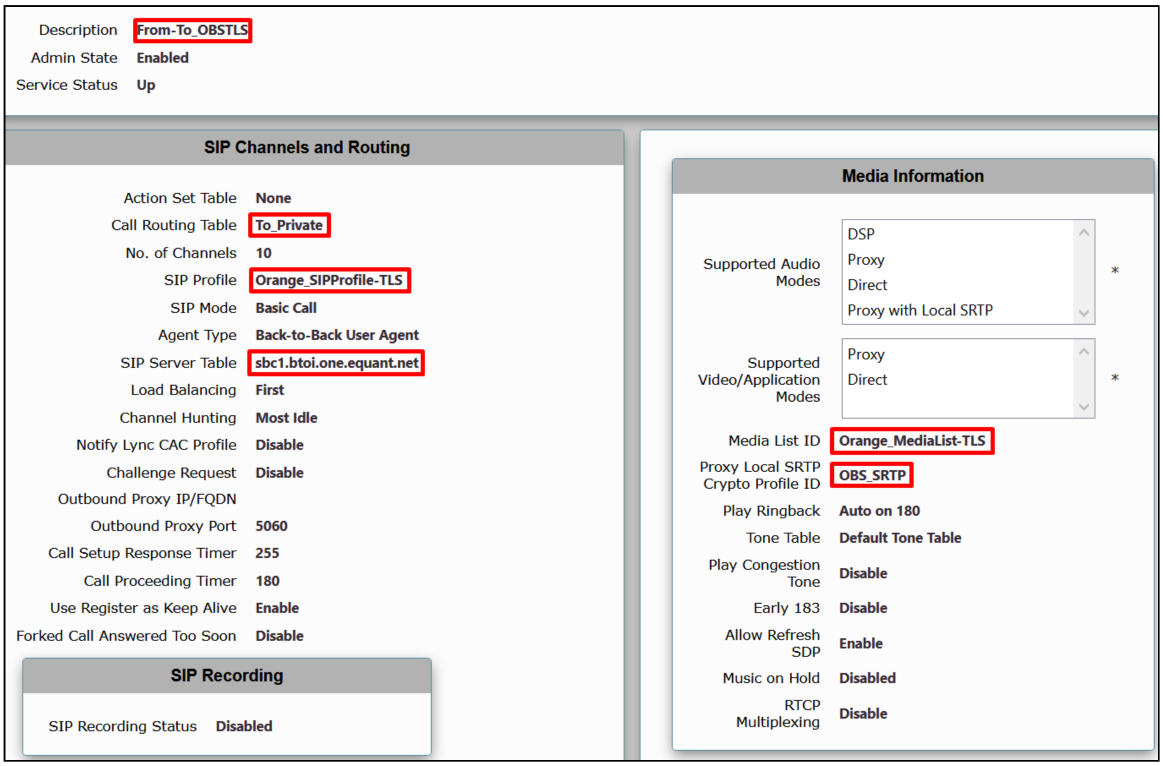


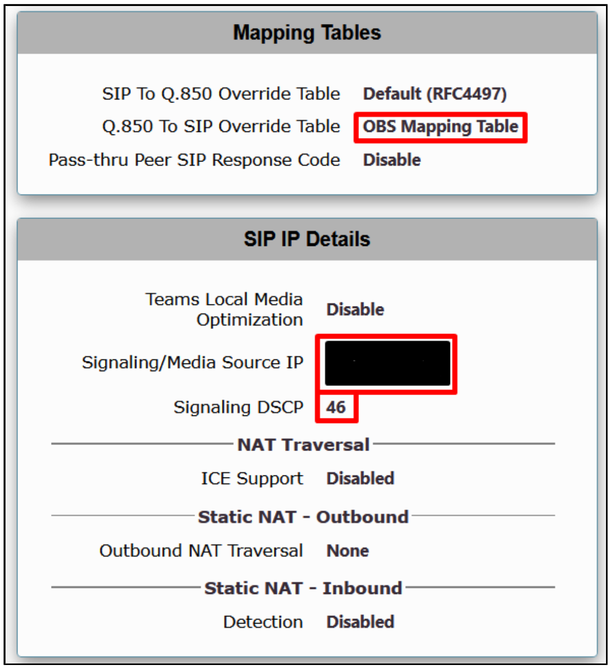
2. Click **Add SIP SG**.

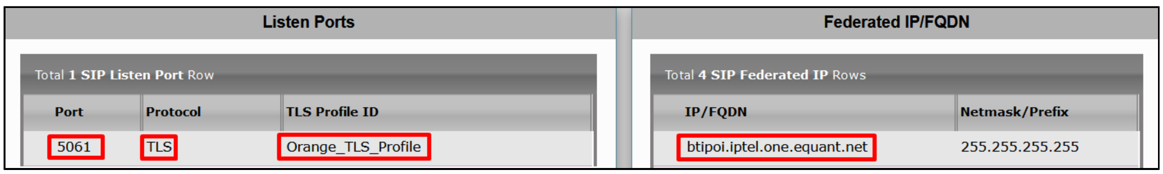
Figure 171: New Signaling Group

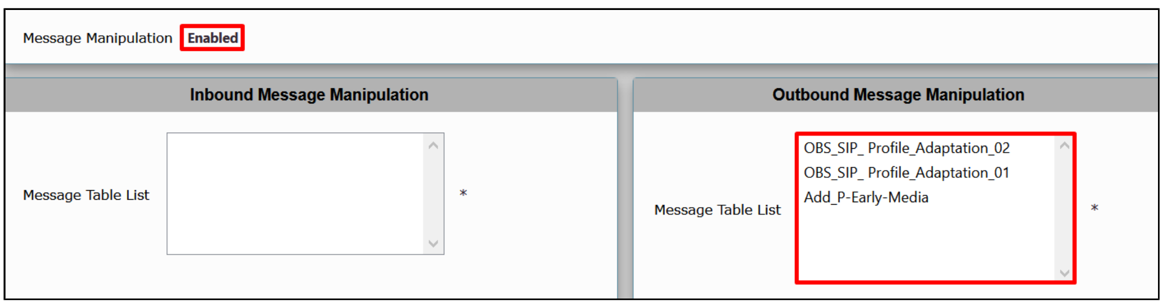
3. Set the new entry as shown in the following figure.

Figure 172: From-To_OBSTLS









4. Click **Apply** to save the changes.

Transformations 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 selected from the Transformation Table.

> **Regular Expressions**
> See Appendix A for more information about Regular Expressions (REGEX) that help to configure Transformation Tables.

Table 7: Transformation Tables

Transformation Table	Transformation Entries
CUCM_Prefixes	To_CUCM
Orange_TLS	Add plus calling number To_OBS-TLS

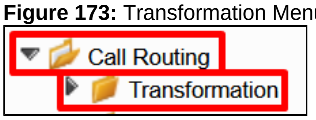
CUCM_Prefixes

Table 8: CUCM_Prefixes entries

Description	Match Type	Input Field		Output Field	
		Type	Value	Type	Value
To_CUCM	Optional	Called Address / Number	(\+?)(33.*)	Called Address / Number	\2

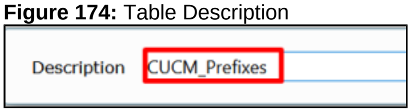
1. To add a new Transformation Table, go to **Call Routing > Transformation** on the left menu path.

   Figure 173: Transformation Menu Path

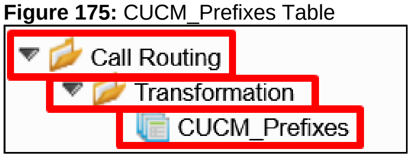
2. Specify the **Description** value.

   Figure 174: Table Description

3. On the left menu path, click the **CUCM_Prefixes** table.

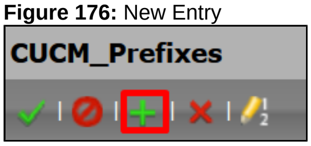
   Figure 175: CUCM_Prefixes Table

To_CUCM

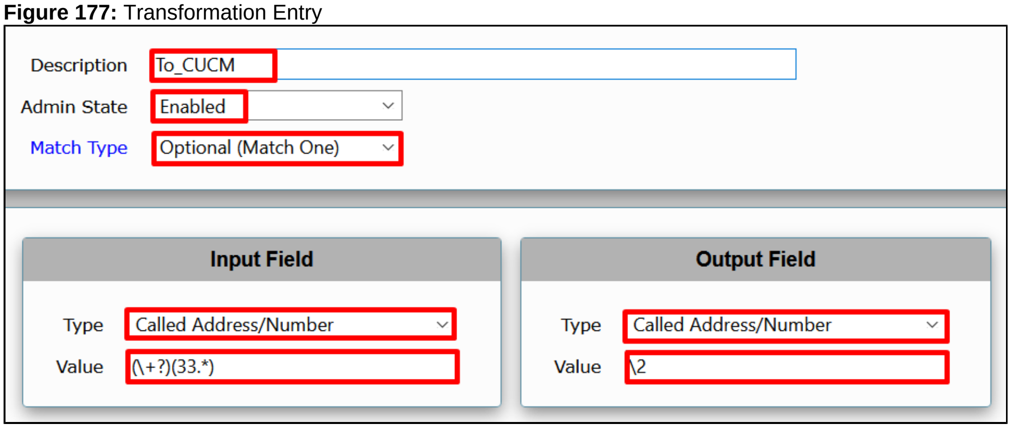
1. To add a new entry, click the **plus (+)** icon.

   Figure 176: New Entry

2. Specify the following values to configure the new entry.

   Figure 177: Transformation Entry

3. Click **Apply** to save the changes.

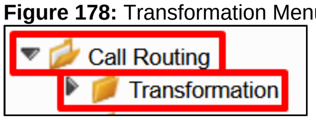
Orange_TLS

Table 9: Orange_TLS entries

Description	Match Type	Input Field		Output Field	
		Type	Value	Type	Value
Add plus calling number	Optional	Calling Address / Number	(\+)?(.*)	Calling Address / Number	+\2
To_OBS-TLS	Optional	Called Address / Number	(\+)?(0)(.*)	Called Address / Number	+\3

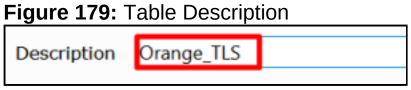
1. To add a new Transformation Table, go to **Call Routing > Transformation** on the left menu path.

Figure 178: Transformation Menu Path



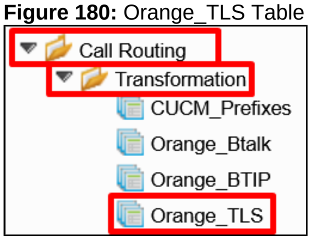
2. Specify the **Description** value.

Figure 179: Table Description



3. On the left menu path, click the **Orange_TLS** table.

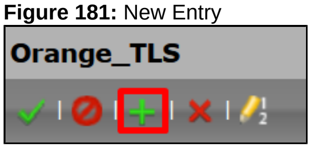
Figure 180: Orange_TLS Table



Add plus calling number

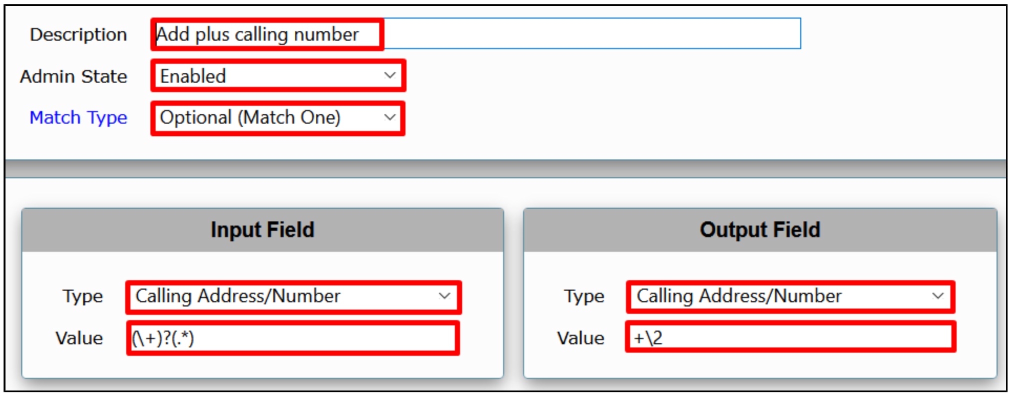
1. To add a new entry, click the **plus (+)** icon.

Figure 181: New Entry



2. Specify the following fields to configure the new entry.

Figure 182: Transformation Entry

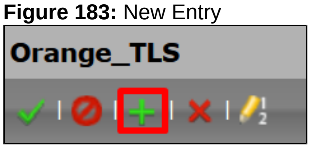


3. Click **Apply** to save the changes.

To_OBS-TLS

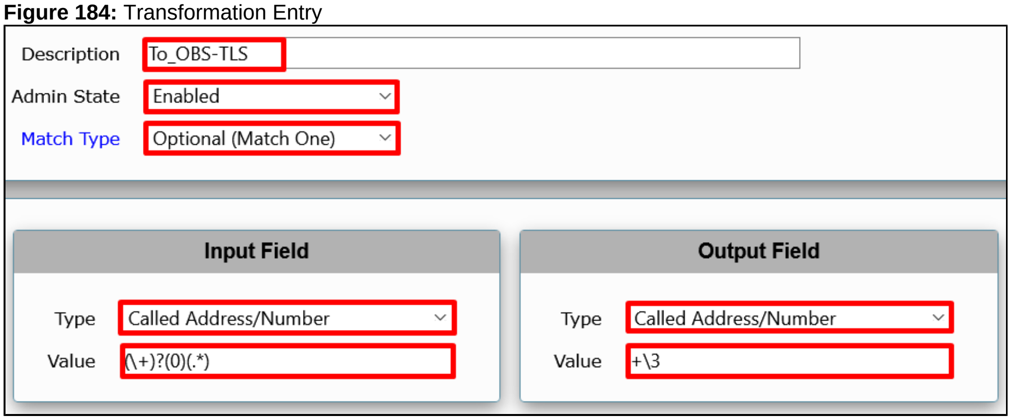
1. To add a new entry, click the **plus (+)** icon.

Figure 183: New Entry



2. Specify the following fields to configure the new entry.

Figure 184: Transformation Entry



3. Click **Apply** to save the changes.

Call Routing Tables

Calling Routing tables carry calls between signaling groups, thereby transferring calls between ports and protocols. They allow users to define routes, specifying which calls to transfer and how to translate the calls. These tables are one of the central connection points of the system, linking Transformation Tables, Message Translations, Cause Code Reroute Tables, Media Lists, and Signaling Group.

Table 10: Call Routing Tables

Call Routing Table	Entry Description	Transformation Table
To_Private	To_CUCM	CUCM_Prefixes
To_Orange	To_OrangeTLS	Orange_TLS

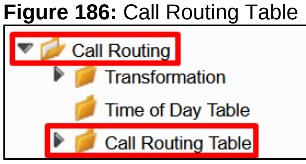
To_Private

Figure 185: Call Route Entry Parameters

Description	Number/Name Transformation Table	Destination Signaling Groups	Audio Stream Mode	Media List
To_CUCM	CUCM_Prefixes	From-To_CUCM	DSP Preferred over Proxy	CUCM_MediaList

1. To add a new Call Routing table, go to **Call Routing > Call Routing Table** on the left menu path.

Figure 186: Call Routing Table Menu Path

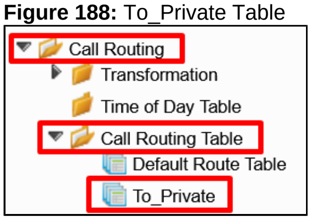


2. Set the **Description** value as shown in the following figure.

Figure 187: Table Description

3. On the left menu path, click the **To_Private** table.

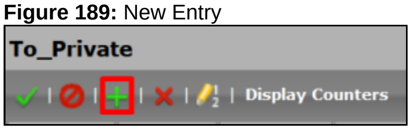
Figure 188: To_Private Table



To_CUCM

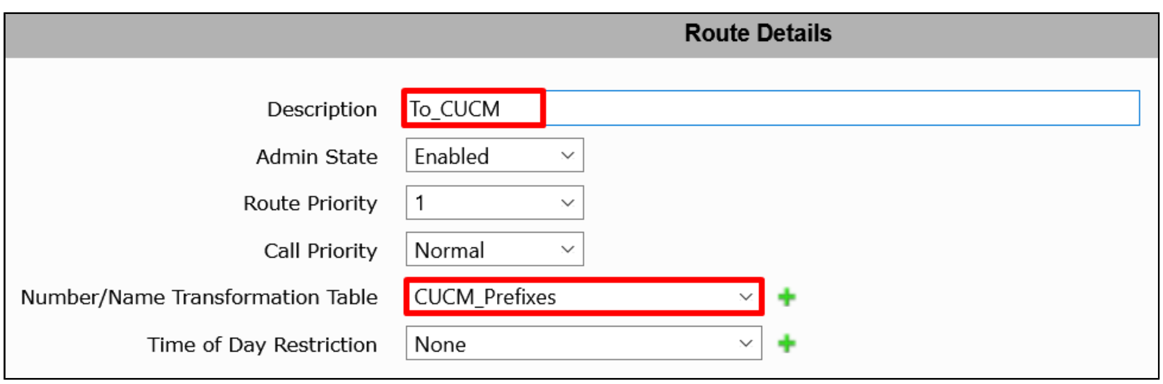
1. To add a new entry, click the **plus (+)** icon.

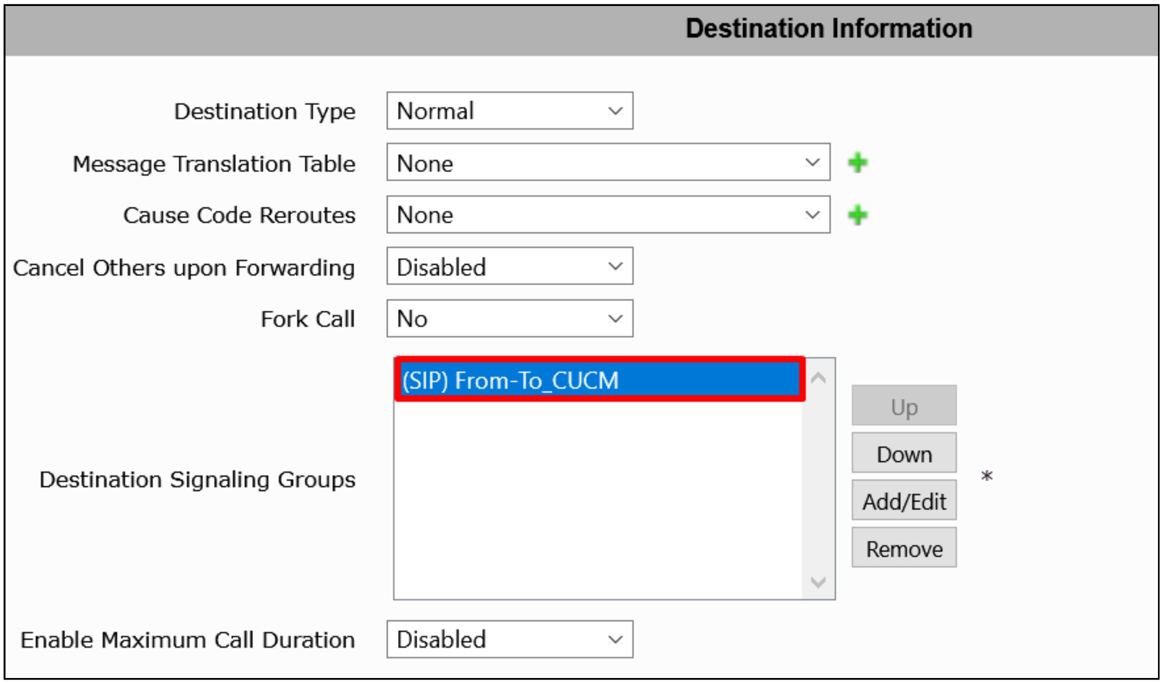
Figure 189: New Entry

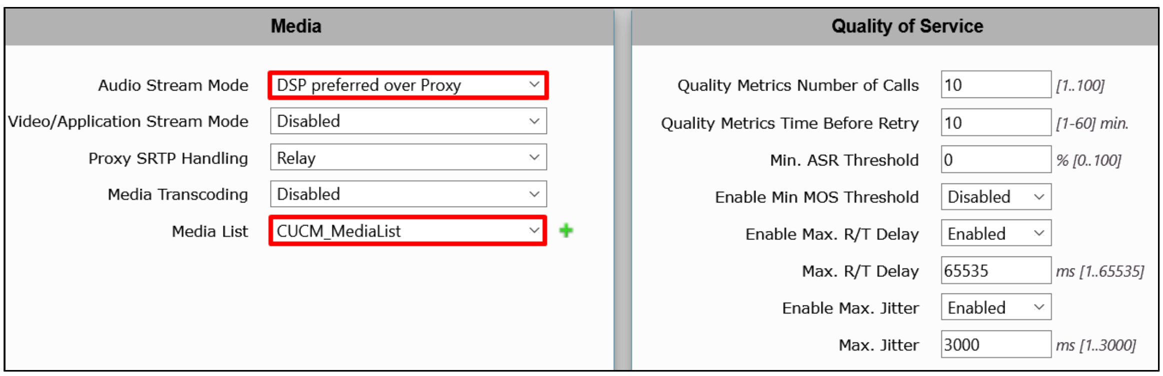


2. Configure the new entry as shown in the figure.

Figure 190: Call Route Entry







3. Click **Apply** to save the changes.

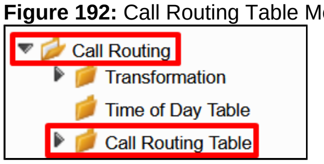
To_Orange

Figure 191: Call Route Entry Parameters

Description	Number/Name Transformation Table	Destination Signaling Groups	Audio Stream Mode	Media Transcoding	Media List
To_OrangeTLS	Orange_TLS	From-To_OBSTLS	DSP Preferred over Proxy	Enabled	Orange_MediaList -TLS

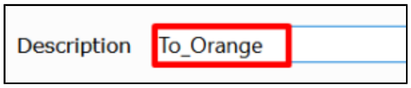
1. To add a new Call Routing table, go to **Call Routing > Call Routing Table** on the left menu path.

Figure 192: Call Routing Table Menu Path



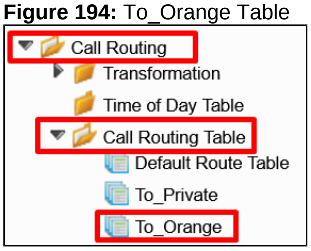
2. Set the **Description** as shown in the following figure.

Figure 193: Table Description



3. On the left menu path, click the **To_Orange** table.

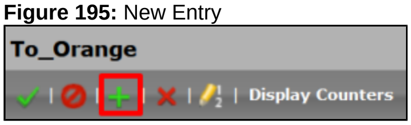
Figure 194: To_Orange Table



To_OrangeTLS

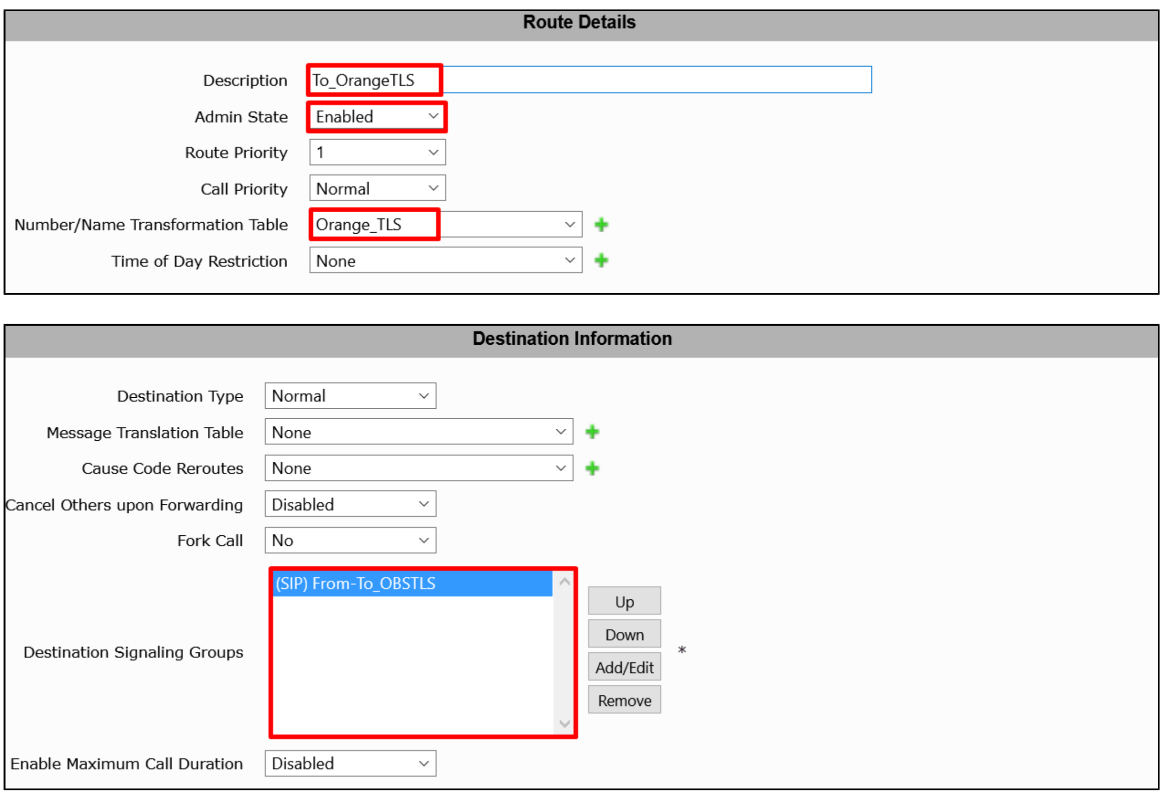
1. To add a new entry, click the **plus (+)** icon.

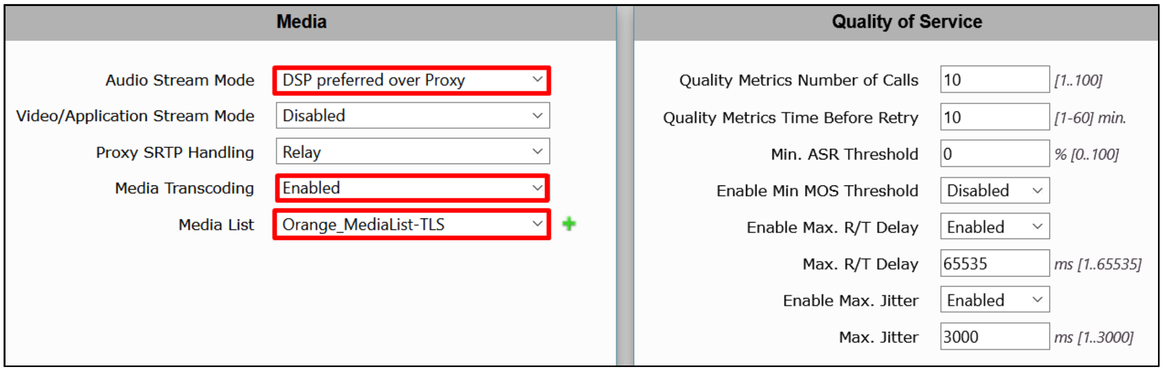
Figure 195: New Entry



2. Configure the new entry as shown in the following figure.

Figure 196: Call Route Entry





3. Click **Apply** to save the changes.

Test Results

Table 11: Test Results

Preliminary Phase					
Use Case		**Test ID**	**Test Case**	**Test Result**	**Comments**
Basic Call		BC01	BC01_[Phone_1]_[OFFNET]	OK	
		BC02	BC02_[OFFNET]_[Phone_1]	OK	
Long Duration Call + CLIR		LCLIR01	LCLIR01_[Phone_1]_[OFFNET]	OK	
		LCLIR02	LCLIR02_[OFFNET]_[Phone_1]	OK	
Call Cancellation		CANC01	CANC01_[Phone_1]_[OFFNET]	OK	
		CANC02	CANC02_[OFFNET]_[Phone_1]	OK	
DTMF + Voicemail		DTMF03	DTMF03_[Phone_1]_[OFFNET-IVR]	OK	
		DTMF04	DTMF04_[OFFNET-voicemail]_[Phone_1]	OK	
Transfer	**Supervised + MOH**	TRMOH 01	TRMOH01_[OFFNET]_[Phone_1]_[OFFNET]	OK	
	Blind	TRAB01	TRAB01_[OFFNET]_[Phone_1]_[OFFNET]	OK	
		TRAB04	TRAB04_[OFFNET]_[Phone_1]_[OFFNET-IVR]	OK	
Forward	**Unconditional**	FWDU01	FWDU01_[OFFNET]_[Phone_1]_[OFFNET]	OK	
		FWDU04	FWDU04_[OFFNET]_[Phone_1]_[OFFNET-IVR]	OK	
	No Answer	FWDNA 01	FWDNA01_[OFFNET]_[Phone_1]_[OFFNET]	OK	
SVAIP		SVAIP02	SVAIP02_[IPBX-ForcedONNET]_[SAN-SVAIP+33296084273]	N/A	Out of scope as currently not possible to perform those tests.
Advanced Phase					
Use Case		**Test ID**	**Test Case**	**Test Result**	**Comments**
Busy Call		BUSY01	BUSY01_[Phone_1]_[OFFNET]	OK	
		BUSY02	BUSY02_[OFFNET]_[Phone_1]	OK	
Not Answered Call		NA01	NA01_[Phone_1]_[OFFNET]	OK	
		NA02	NA02_[OFFNET]_[Phone_1]	OK	
Transfer	**Supervised**	TRAS02	TRAS02_[OFFNET]_[Phone_1]_[Phone_2]	OK	
		TRAS03	TRAS03_[Phone_1]_[Phone_2]_[OFFNET]	OK	
	Blind	TRAB02	TRAB02_[OFFNET]_[Phone_1]_[Phone_2]	OK	

		TRAB03	TRAB03_[Phone_1]_[Phone_2]_[OFFNET]	OK	
Forward	**Unconditional**	FWDU02	FWDU02_[OFFNET]_[Phone_1]_[Phone_2]	OK	
	Busy	FWDB02	FWDB02_[OFFNET]_[Phone_1]_[Phone_2]	OK	
	No Answer	FWDNA02	FWDNA02_[OFFNET]_[Phone_1]_[Phone_2]	OK	
		FWDNA03	FWDNA03_[Phone_1]_[Phone_2]_[OFFNET]	OK	
		FWDNA04	FWDNA04_[OFFNET]_[Phone_1]_[OFFNET-IVR]	OK	
Conference X3		CONF01	CONF01_[OFFNET]_[Phone_1]_[OFFNET]	OK	
Prehook	**(with) Transfer Sup.**	PREHOOK01	PREHOOK01_[OFFNET]_[Phone_1]_[OFFNET]	N/A	
		PREHOOK02	PREHOOK02_[OFFNET]_[Phone_1]_[Phone_2]	N/A	
		PREHOOK03	PREHOOK03_[Phone_1]_[Phone_2]_[OFFNET]	N/A	
	(with) Forward	PREHOOK04	PREHOOK04_[OFFNET]_[Phone_1]_[OFFNET]	N/A	
Call Features	**Call Parking**	CPA01	CPA01_[Phone_1]_[OFFNET]_[Phone_2]	OK	
	Call Pickup	PKU01	PKU01_[OFFNET]_[Phone_1]_[Phone_2]	OK	
	Hunt Group	HUG01	HUG01_[OFFNET]_[Phone_1]	OK	
	Second Line	SL01	SL01_[OFFNET]_[Phone_1]	OK	
DTMF		DTMF03	DTMF03_[Phone_1]_[OFFNET-IVR]	OK	
E2E Overflow		OVF01	OVF01_[NBI-Int+670012144326845]_ [cSBCRibbon+33296031233]_[]	OK	
		OVF02	OVF02_[Offnet-Devil+ +960012144326845]_ [cSBCRibbon+33296086974]_[]	OK	
		OVF03	OVF03_[NBI-Fr+33399106845]_ [cSBCRibbon+33296031233]_[]	OK	
		OVF04	OVF04_[OFFNET]_[select device]_[]	N/A	
		OVF05	OVF05_[OFFNET]_[select device]_[]	N/A	
		OVF06	OVF06_[OFFNET]_[select device]_[]	N/A	
		OVF07	OVF07_[NBI-Int+670012144326845]_ [cSBCRibbon+33296039150]_[]	OK	
		OVF08	OVF08_[cSBCRibbon+33296031233]_[Offnet-NBI-Fr+33399106845]_[]	N/A	
		OVF09	OVF09_[cSBCRibbon+33296031233]_[Offnet-NBI-Fr+33399106845]_[]	N/A	
CAC		CAC01	CAC01_[OFFNET]_[Phone_1]	N/A	
		CAC02	CAC02_[Phone_1]_[OFFNET]	N/A	
		CAC03	CAC03_[Phone_1]_[Phone_2]	N/A	
		CAC04	CAC04_[OFFNET]_[Phone_1]_[Phone_2]	N/A	
		CAC05	CAC05_[OFFNET]_[Phone_1]_[Phone_2]	N/A	
Emergency Number		EMN01	EMN01_[Phone_1]_[OFFNET-EMN]	OK	
		EMN02	EMN02_[Phone_1]_[OFFNET-EMN]	N/A	
		EMN03	EMN03_[Phone_1]_[OFFNET-EMN]	OK	
Attendant Console		AC01	AC01_[OFFNET]_[Phone_1]_[Phone_2]	N/A	
		AC02	AC02_[OFFNET]_[Phone_1]_[Phone_2]	N/A	

Use Case		Test ID	Test Case	Test Result	Comments
		AC03	AC03_[OFFNET]_[Phone_1]_[Phone_2]	N/A	
		AC04	AC04_[OFFNET]_[Phone_1]_[Phone_2]	N/A	
Fax Tests					
Use Case		**Test ID**	**Test Case**	**Test Result**	**Comments**
Fax	**Offnet -> HQ**	Fax_01	Devil+_IPTEL_G3	N/A	
		Fax_02	Devil+_IPTEL_SG3	N/A	
		Fax_03	Neo_IPTEL_G3	N/A	
		Fax_04	Neo_IPTEL_SG3	N/A	
		Fax_05	NBI-France_IPTEL_G3	N/A	
		Fax_06	NBI-France_IPTEL_SG3	N/A	
		Fax_07	NBI-International_IPTEL_G3	N/A	
		Fax_08	NBI-International_IPTEL_SG3	N/A	
	HQ -> Offnet	Fax_09	IPTEL_Devil+_G3	N/A	
		Fax_10	IPTEL_Devil+_SG3	N/A	
		Fax_11	IPTEL_Neo_G3	N/A	
		Fax_12	IPTEL_Neo_SG3	N/A	
		Fax_13	IPTEL_NBI-France_G3	N/A	
		Fax_14	IPTEL_NBI-France_SG3	N/A	
		Fax_15	IPTEL_NBI-International_G3	N/A	
		Fax_16	IPTEL_NBI-International_SG3	N/A	

Conclusion

These Application Notes describe the configuration steps required for Ribbon to successfully interoperate with OBS. All feature and serviceability test cases were completed and passed with the exceptions/observations noted in Test Results.

Appendix A

- **Cisco CUCM - Special Characters and Settings**
- **Ribbon SBC Edge - Understanding Regular Expressions**
- **Ribbon SBC Edge - SIP Message Manipulation**

Appendix B (Known Issues)

CHOR-7729

JIRA NUMBER	Name	Description
CHOR-7729	SWe Lite: T.38 FAX over TLS not working	Orange telecom is trying to send and receive FAX over TLS using T.38. They have requested to use SRTP instead of UDPTL to handle the media stream as UDPTL is not encrypted.