Ribbon SBC Edge R9.0 Interop with IP-PBX for Deutsche Telekom CompanyFlex SIP Trunk : Interoperability Guide

Table of Contents

Interoperable Vendors

Deutsche Telekom

Copyright

Document Overview

This document depicts the configuration details for Ribbon SBC Edge interworking & compliance against Deutsche Telekom CompanyFlex SIP Trunking solution.

About Ribbon SBC Edge

The Ribbon Session Border Controller provides best-in class communications security. The Ribbon SBC Edge dramatically simplifies the deployment of robust communications security services for SIP Trunking.

About Deutsche Telekom

Deutsche Telekom is a telecommunications company that offers a range of fixed-network services, such as voice and data communication services based on fixed-network and broadband technology, and sells terminal equipment, other hardware, and services to resellers.

Scope

This document provides configuration best practices for deploying Ribbon's SBC 1000/2000 and SWe Lite series when connecting with Deutsche Telekom CompanyFlex. Note that these are configuration best practices, and each customer may have unique needs and networks. Ribbon recommends that customers work with network design and deployment engineers to establish the network design which best meets their requirements.

Non-Goals

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

Audience

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

Prerequisites

The following aspects are required before proceeding with the interop:

- Ribbon SBC Edge
- SBC License
- IP-PBX SIP Connect 2.0 Compliant
- Deutsche Telekom "CompanyFlex" SIP trunks
    - Contact Deutsche Telekom for Domain, Outbound proxy, Registrar, SIP trunk Registration number, SIP trunk password and block of numbers for the end points.
    - For more information, visit https://hilfe.companyflex.de/de/einrichtung/einrichtung-sip-trunk

> **Note**
> Any IP-PBX which is SIP Connect 2.0 Compliant can be deployed with Ribbon SBC Edge. For this interop testing we have used CUCM 12.5 which is **SIP Connect 2.0 Compliant.**

> **Note**
> During this interop, the SIP Trunk between Deutsche Telekom and Ribbon SBC Edge has been configured with TLS and SRTP.

Product and Device Details

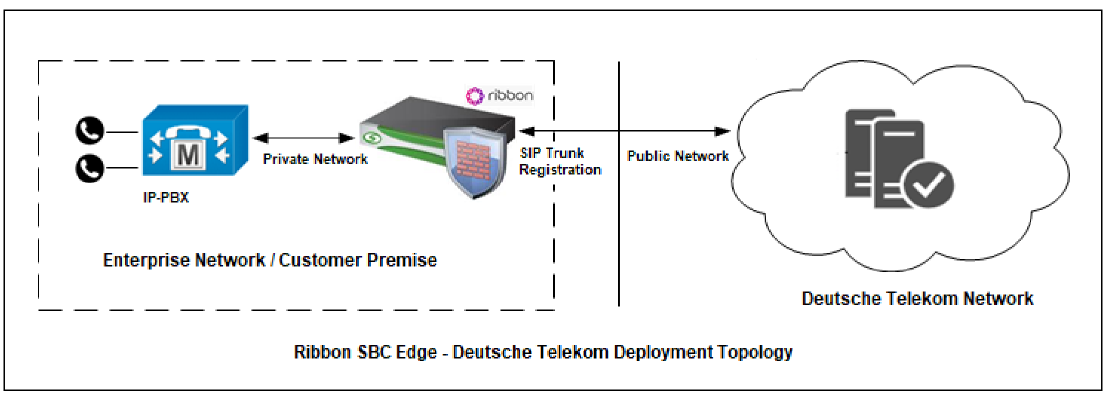
The configuration uses the following equipment and software:

Table 1: Requirements

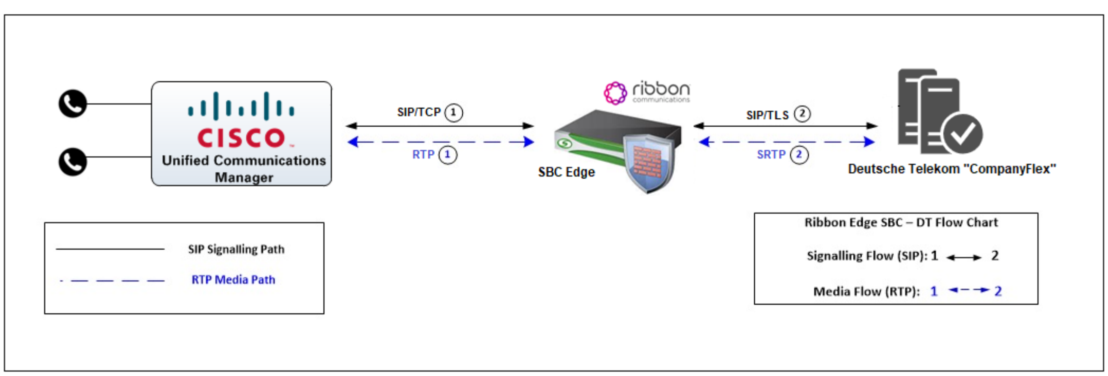
Product	Equipment	Software Version
Ribbon Networks	Ribbon SBC SWe Lite	9.0.3
Third-party Equipment	Cisco Unified Communication Manager	12.5.1.11900-146
Deutsche Telekom	Deutsche Telekom "CompanyFlex"	NA
Administration and Debugging Tools	Wireshark	3.2.7
	LX Tool	2.1.0.6

Network Topology

Deployment Topology



IOT Lab Topology



Section A: Ribbon SBC Edge Configuration

Installing Ribbon SBC Edge

Refer to the following document for installing the Ribbon SBC Edge: Installing SBC 1000/2000.

Accessing Ribbon SBC Edge

Open any browser and enter the SBC IP address.

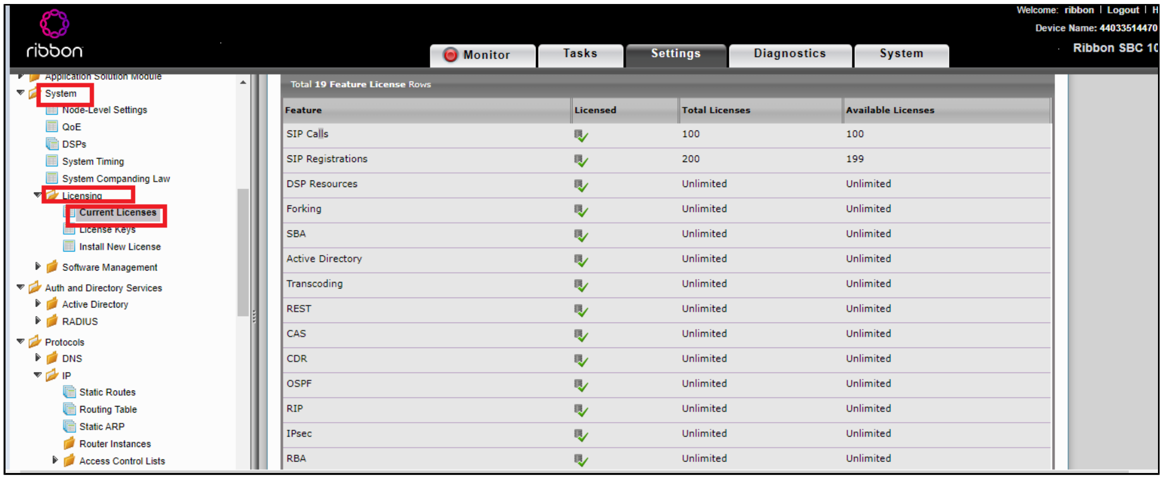
Click **Enter** and log in with a valid User ID and Password.

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.**

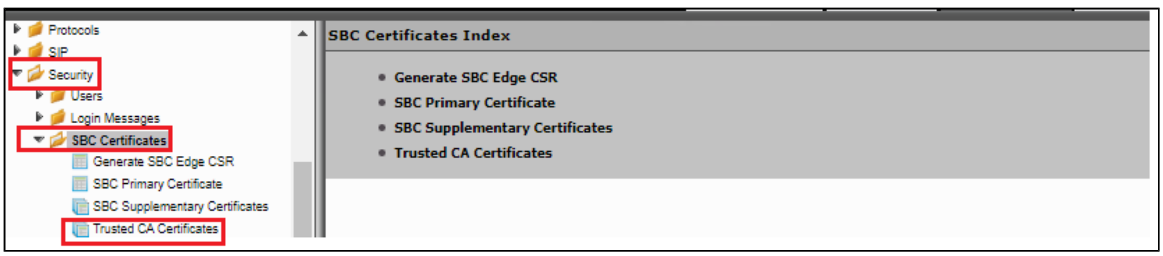


For more details on Licenses, refer to Ribbon SBC Edge Licenses.

Import Trusted Root CA Certificates

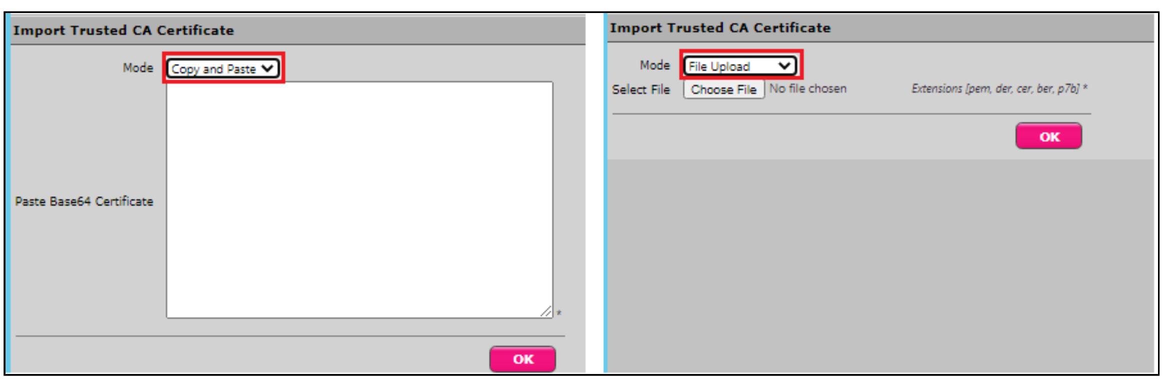
A Trusted CA Certificate is a certificate issued by a trusted certificate authority. Trusted CA Certificates are imported to the SBC SWe Lite to establish its authenticity on the network.

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



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

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



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

> **Note**
> Deutsche Telekom Root certificate: https://corporate-pki.telekom.de/en/GlobalRootClass2.html

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

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

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

View Networking Interfaces

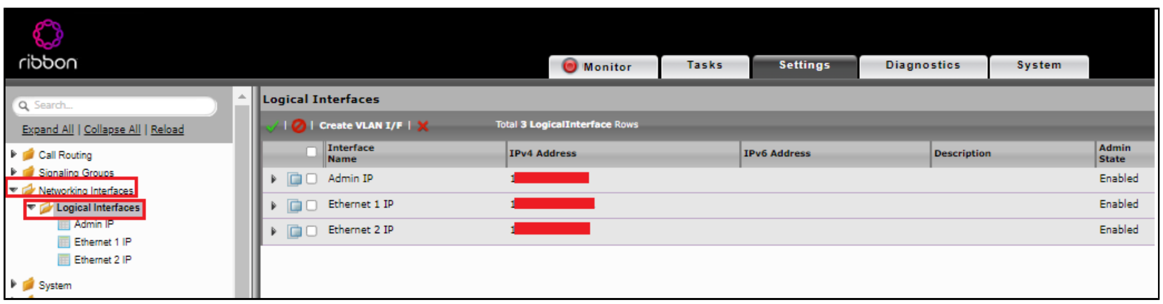
The Ribbon SBC Edge supports five system created logical interfaces (known as **Administrative IP**, **Ethernet 1 IP**, **Ethernet 2 IP**, **Ethernet 3 IP**, and **Ethernet 4 IP**). In addition to the system created logical interfaces, the Ribbon SBC Edge supports user-created VLAN logical sub-interfaces.

Admin IP, Ethernet 2 IP, Ethernet 1 IP are used for this interop.

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

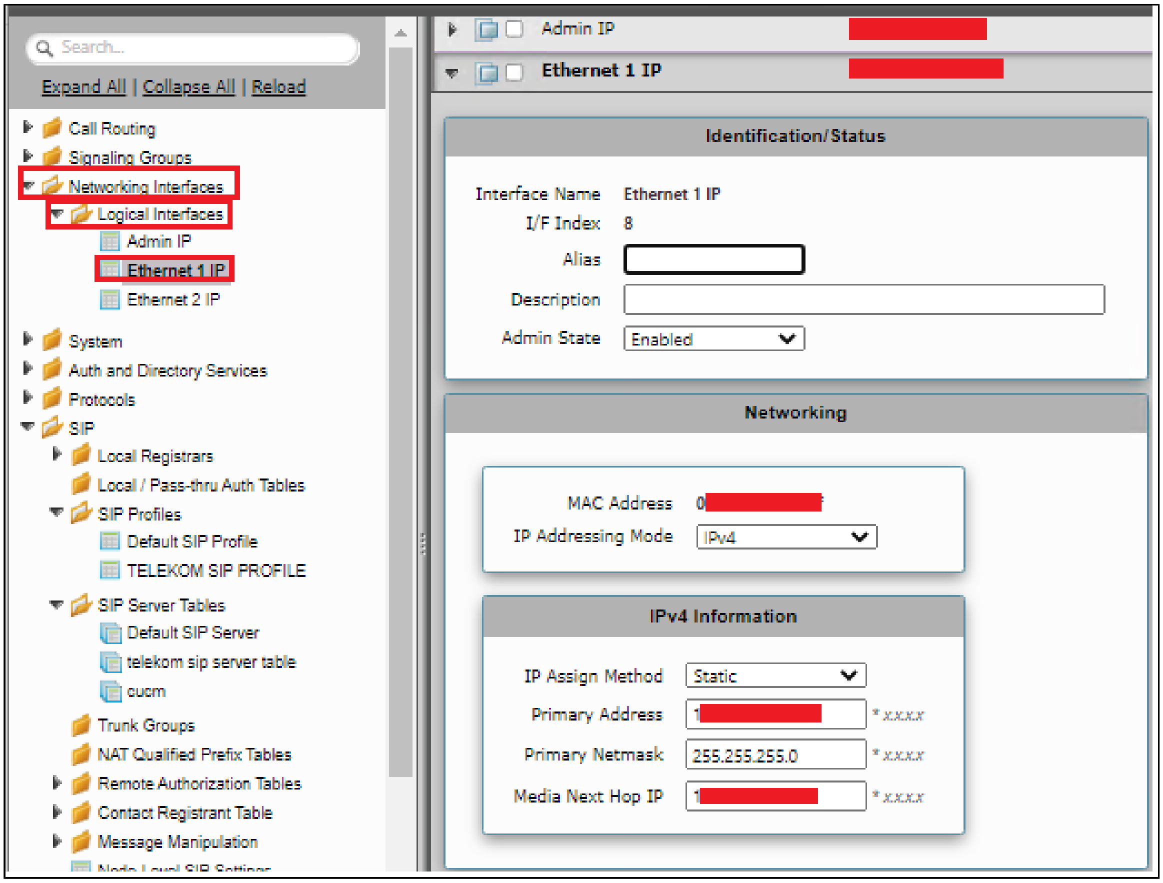
Administrative IP

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



Ethernet 1 IP

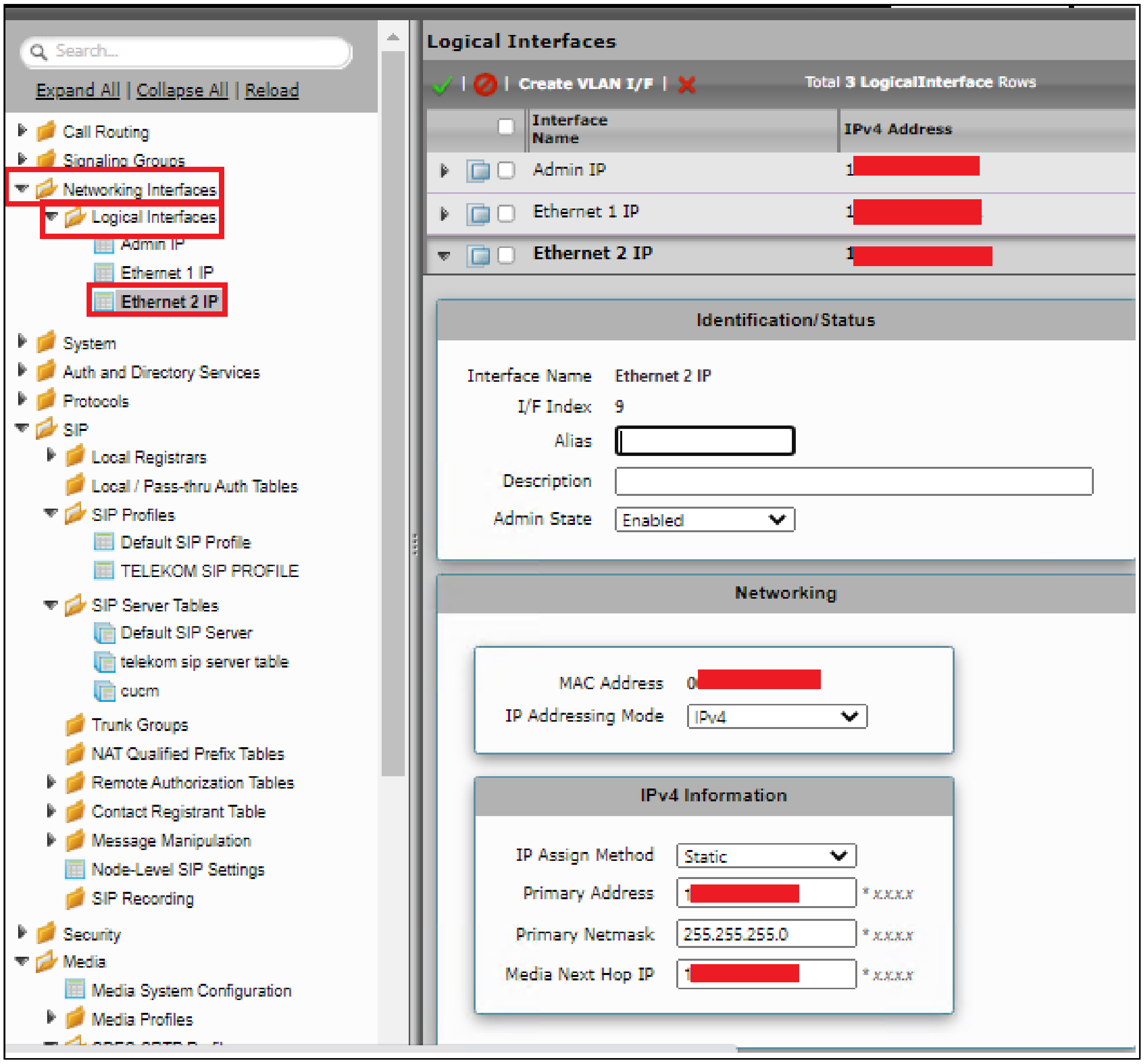
Ethernet 1 IP is assigned an IP address used for transporting all the VOIP media packets (for example, RTP, SRTP) and all protocol packets (for example, SIP, RTCP, TLS). In the default software, **Ethernet 1 IP** is enabled, and an IPv4 address is acquired via a connected DHCP server. You can assign a static IP as well. This interface will face the Deutsche Telekom.



Note
Use Static IP address in the interface towards the Deutsche Telekom.

Ethernet 2 IP

Configure this Ethernet 2 interface as follows according to the requirement. This interface will face the IP-PBX (CUCM).



Attention
If you are migrating from SIP Trunk DeutschlandLAN towards CompanyFlex, ensure that you configure either a second (different) interface IP address on SBC1000 / SBC2000, or in case of SBC SWe Lite, a second interface with a different IP address.

Do not use the same IP for DeutschlandLAN and CompanyFlex on the SBC.

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

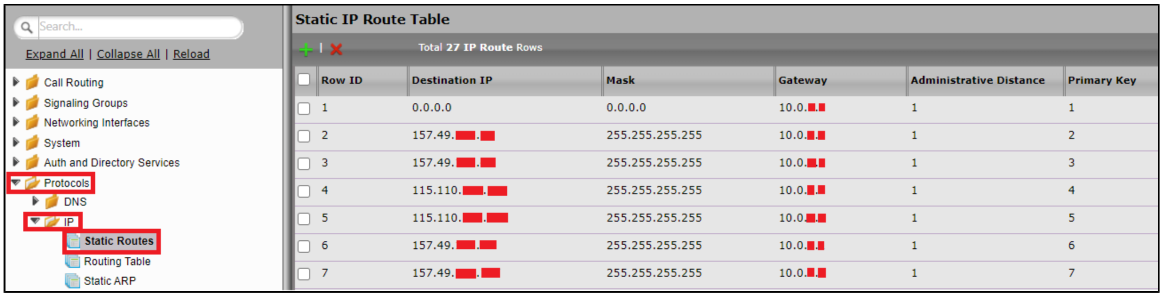
Specifies the network mask of the destination host or subnet. If the 'Destination IP Address' field and 'Mask' field are both 0.0.0.0, the static route is called the 'default static route'.

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.



Ribbon SBC SWe Lite Configuration towards Deutsche Telekom End

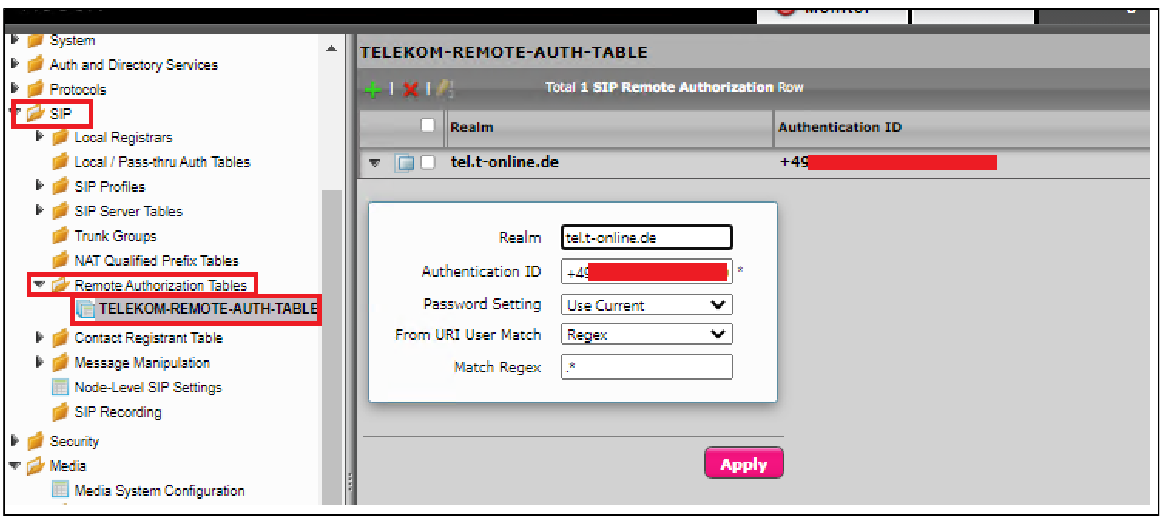
This section describes the steps to configure SBC SWe Lite with TLS/SRTP towards Deutsche Telekom SIP Trunk.

Remote Authorization Table

Select **Settings > SIP > Remote Authorization Tables**.

Remote Authorization Tables entries contain information for responses to request message challenges by an upstream server.

- Create a new entry "SipTrunk2" under "Remote Authorization Table" .
- Add domain name provided by Deutsche Telekom under "Realm".
- Add SIP Trunk number under Authentication ID.
- Add password provided by Deutsche Telekom under "Password" and confirm it.
- Choose regex under "From URI User Match" and add ".* " for "Match regex".

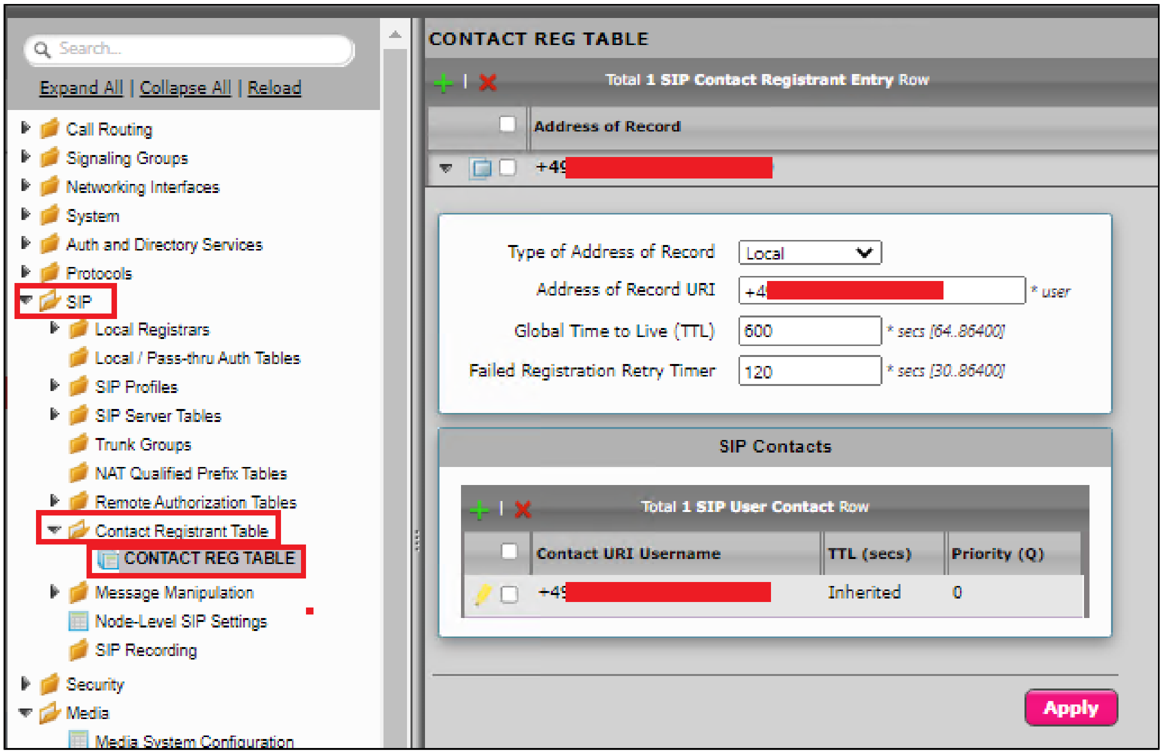


Contact Registration Table

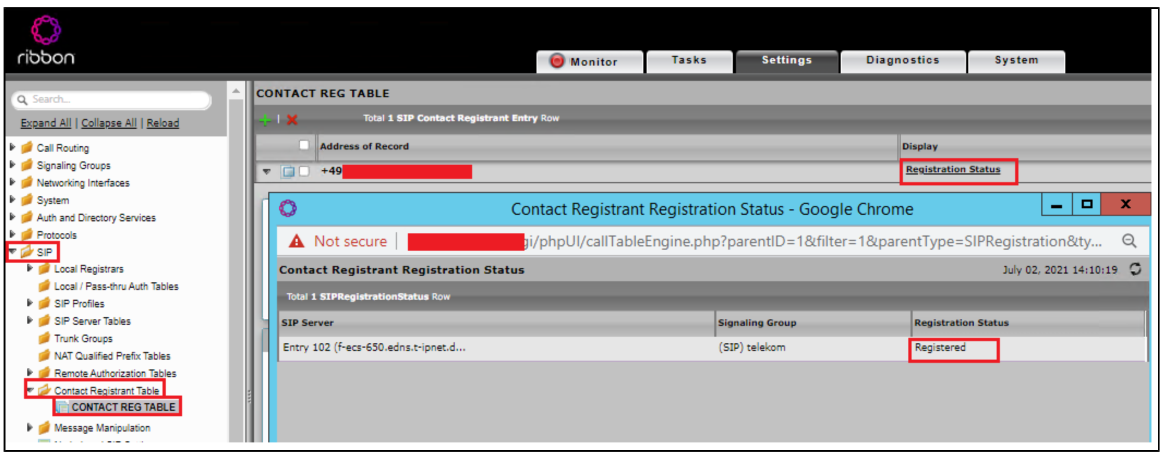
Select **Settings > SIP > Contact Registration Table**.

The Contact Registrant Tables manage contacts that are registered to a SIP server. The SIP Server Configuration can specify a Contact Registrant Table. The username portion of the table is used for outbound calls.

- Create a new entry "Telekom contact reg" under Contact Registrant table.
- Choose local as "Type of address of record".
- Provide the SIP Trunk number provided by Deutsche Telekom under the "Address of record URI".
- Provide 600 seconds for Global Timer to Live and 120 seconds for Failed Registration Retry Timer.
- Create an entry under "SIP Contacts".
- Provide the SIP Trunk number provided by Deutsche Telekom under "Contact URI Username" and set TTL value as "Inherited".



Click on Registration status under the "Contact Registration profile" to see the status of SIP Trunk registration with Deutsche Telekom.

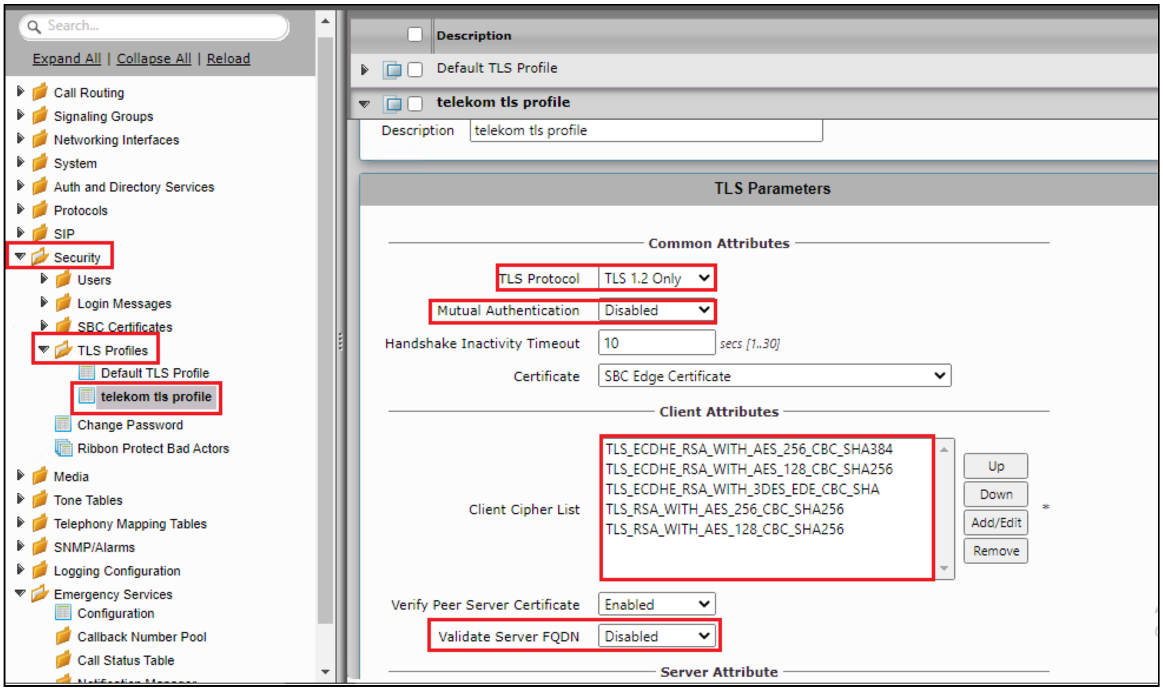


Create TLS Profile

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

Select **Settings** > **Security** > **TLS Profile.** Click the + icon to create a new TLS profile.

- Provide desired description.
- Set TLS protocol as "TLS 1.2 Only".
- Disable "Mutual Authentication".
- Disable "Validate Server FQDN".
- Click "Apply".



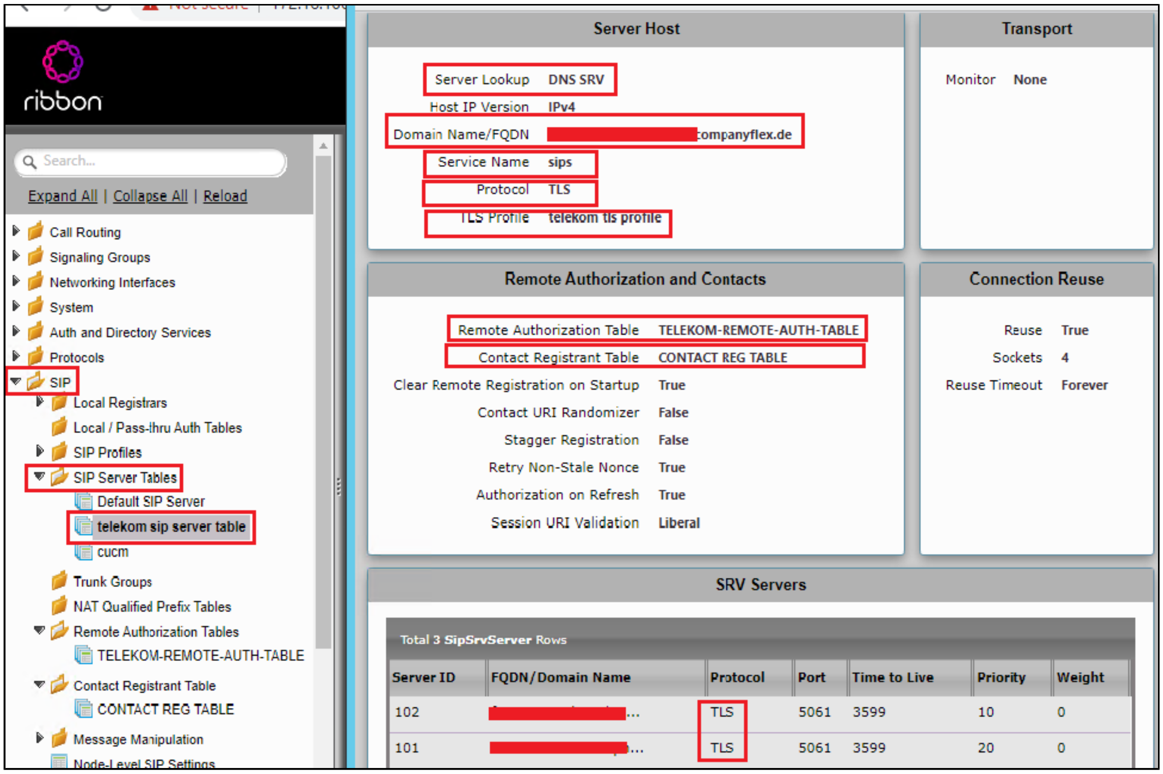
SIP Server Table

Select Settings > SIP > SIP Server Tables

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

When you configure a SIP server table entry with a DNS SRV record, Ribbon recommends that you do not configure another SIP server table entry with the IPs or FQDNs that the DNS SRV record resolves.

- Create a SIP Server Table with a DNS SRV record.
- Add domain name provided by the Deutsche Telekom.
- Update the Service Name as "sips".
- Use TLS protocol.
- For Remote Authorization Table choose "sipTrunk2" that was created earlier.
- For contact Registration table choose "Telekom contact reg" .
- The FQDN provided from Deutsche Telekom will be resolved under SRV servers.
- Attach the TLS profile created in the previous step.
- Verify the FQDN provided from Deutsche Telekom is resolved under SRV servers with protocol as TLS.

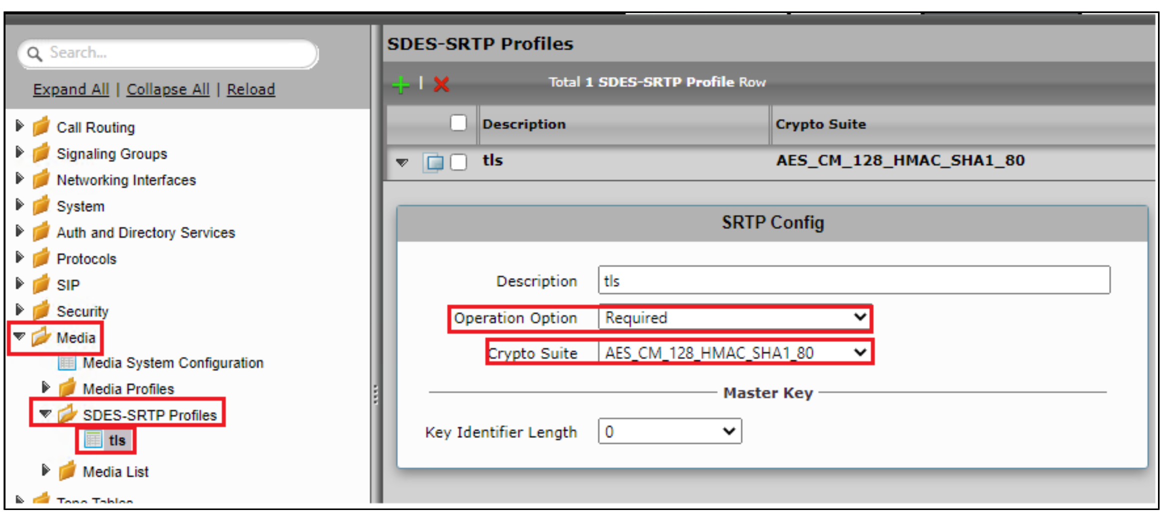


Create SRTP Profile

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

Select **Settings** > **Media** > **SDES-SRTP Profile.** Click the + icon to create a new SRTP profile.

- Provide desired description.
- Set "Operation Option" as Required. This setting permits call connections only if you can use encryption for the call. If the peer device does not support SRTP (Secure Real Time Protocol) for voice encryption over the IP network, the call setup will fail.
- 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.
- Key Identifier Length set to "0" - Set this value to **0** to disable the MKI in SDP.
- Click OK.

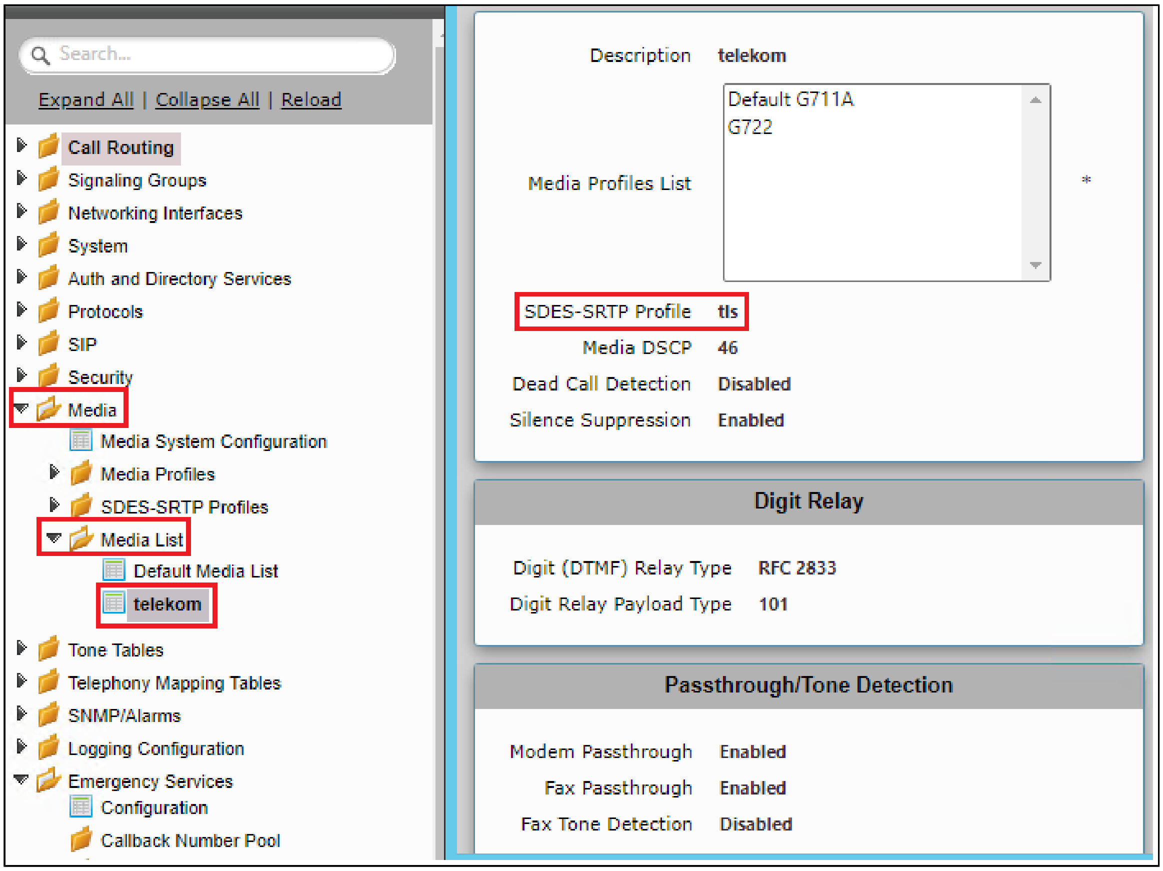


Media Profile

Select **Settings > Media > Media List**.

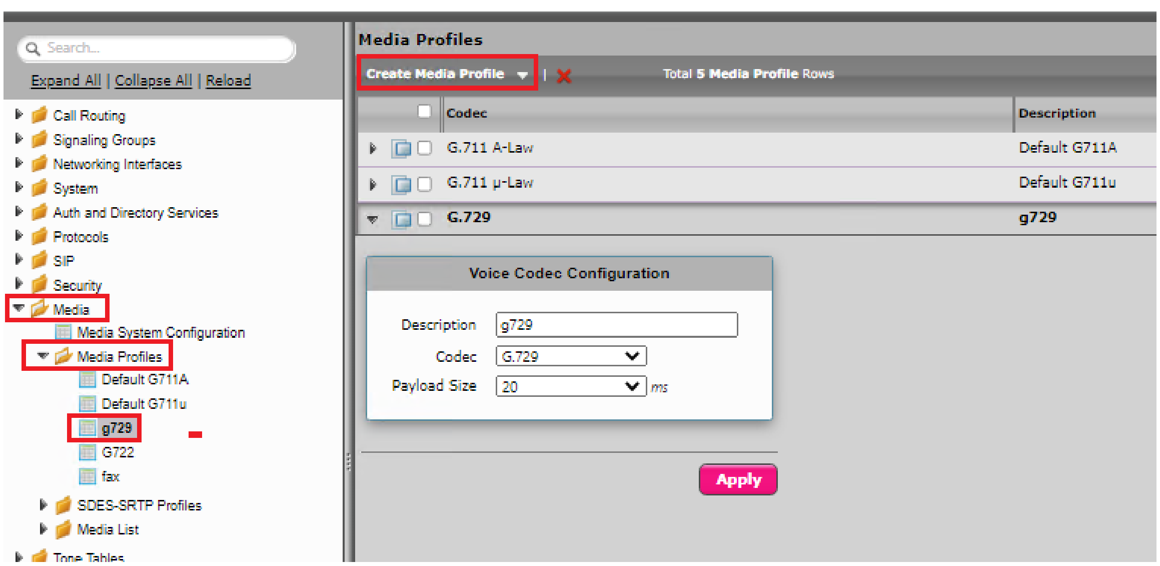
Media Profiles specify the individual voice and fax compression codecs and their associated settings for inclusion into a Media List. Different codecs provide varying levels of compression, allowing the reduction of bandwidth requirements.

- Create new Media list profile.
- G711 media profiles will be there by default under Media profile list, Additional codecs can be added as per the need.
- Attach the SDES-SRTP profile (Specifies the profile for authentication/encryption protocols applied with this Media List) created in the previous step.
- Click Apply.



Select **Settings > Media > Media Profiles**.

Create a Media profile with G729 codec if needed.



Note
As per Deutsche Telekom, T.38 media encryption is not supported. Negotiations within an established connection for T.38 to a UE using encryption are rejected with SIP Error code 488, so that fax transmission will use G.711 with encryption instead.

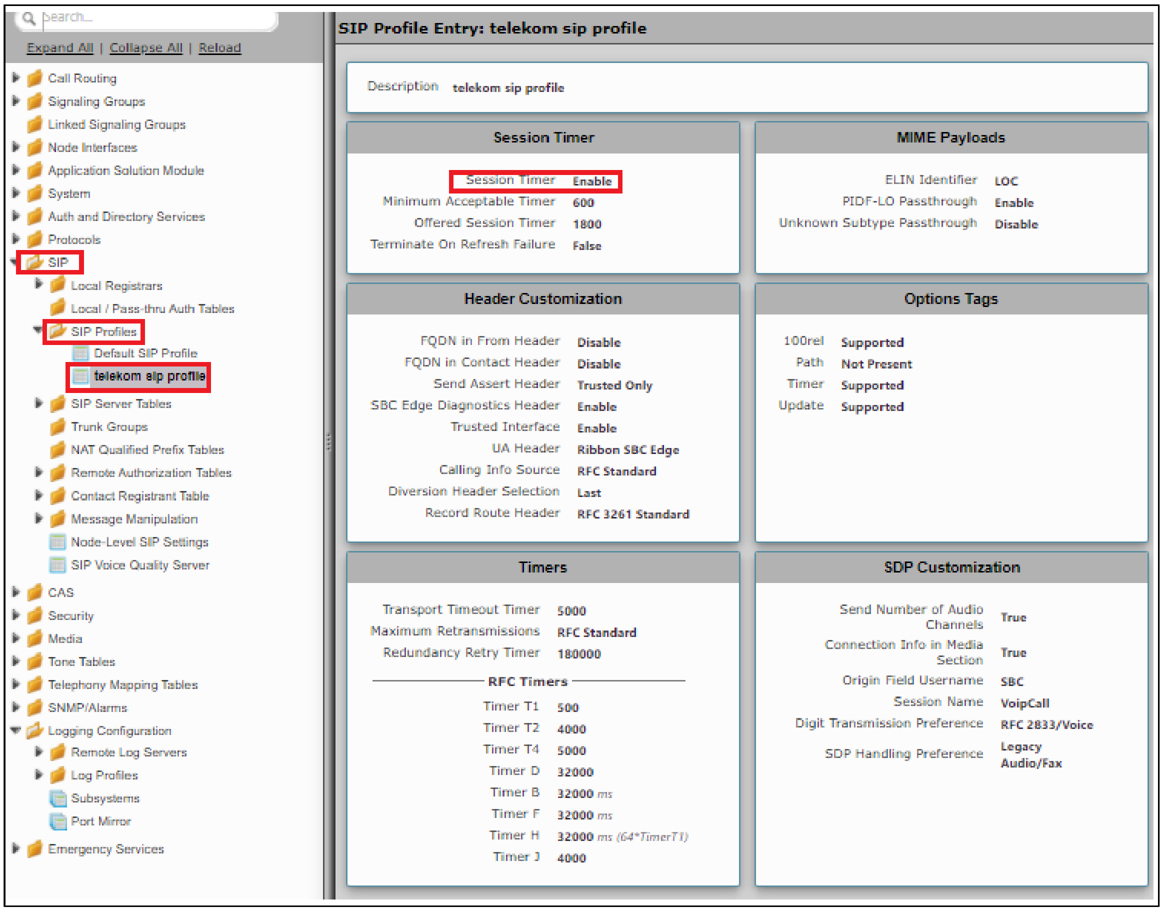
> **Note**
> It is recommended to use a maximum packet time (max pTime) of 20ms for all Voice Codecs.

SIP Profile

Select **Settings > SIP > SIP Profiles**.

SIP Profiles control how the SBC Edge communicates with SIP devices. The SIP Profile controls important characteristics, such as the following: session timers, SIP header customization, SIP timers, MIME payloads, and option tags.

Create a new SIP profile with the name "Telekom sip profile" with the session timer enabled. The Minimum Acceptable Timer is 600, and the Offered Session Timer is 1800.



Signaling Group

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

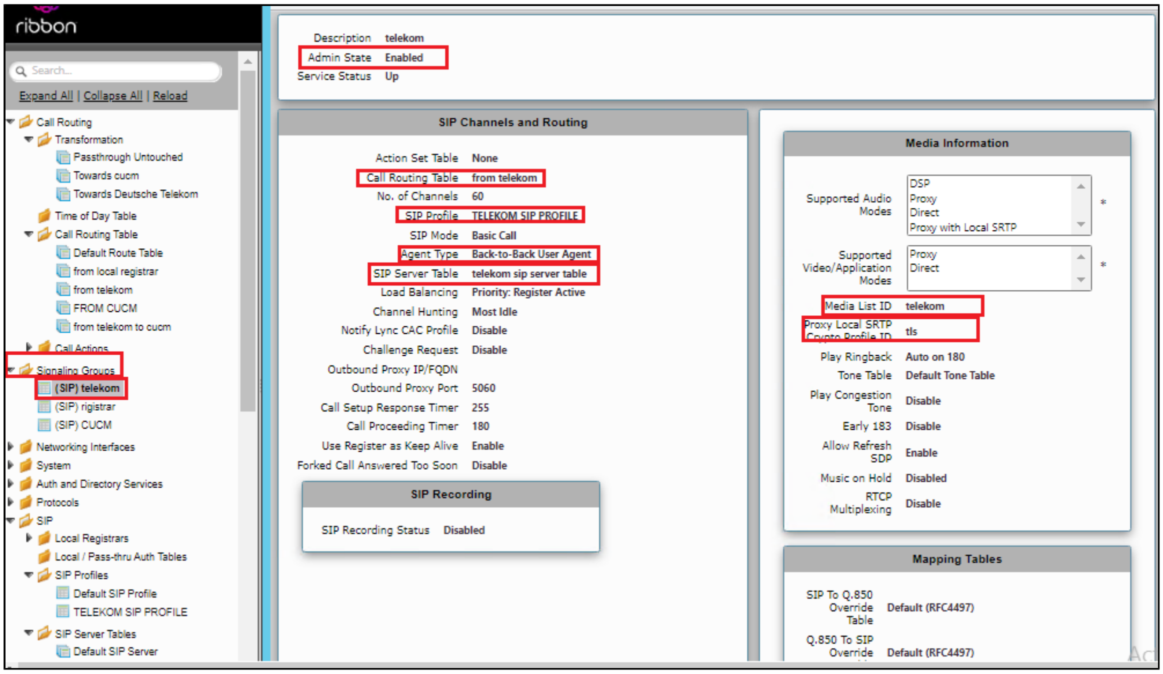
Select Settings > Signaling Groups

- Create an entry in signaling group named "From/To Telekom".
- Choose "Telekom sip profile " under SIP Profile.
- Choose Call Routing as "From Telekom".

> **Note**
> Initially choose Default call Route. Create the Route, as shown in the call Routing section, and then update the call Route to "From Telekom".

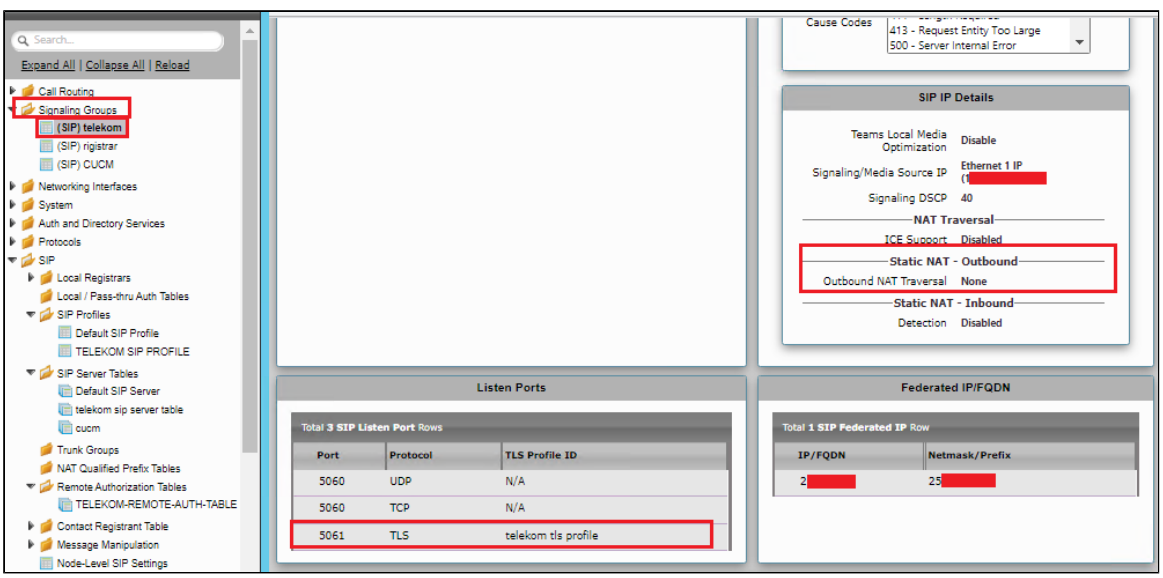
- Choose Agent type as "Back-to-Back user agent" and media list as "telekom media list".

- Choose SIP Server Table as "Telekom SIP Server Table".
- Attach the SRTP profile created in the previous steps under "proxy local SRTP crypto profile ID".



> **Note**
> If NAT is used, then add the external public IP of the NAT box under static NAT outbound of the Signaling Group that is facing towards the Deutsche Telekom server.
>
> Configure NAT so that the external public IP address does not change frequently. If it does, update the new IP address under "Static NAT Outbound".

- Update the Federated IP/FQDN , i.e. the IPs of the Deutsche Telekom servers and gateway, as provided by Deutsche Telekom.
- Add a listening port for TLS (5061).
- Attach the TLS profile created earlier.



Transformation Table

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

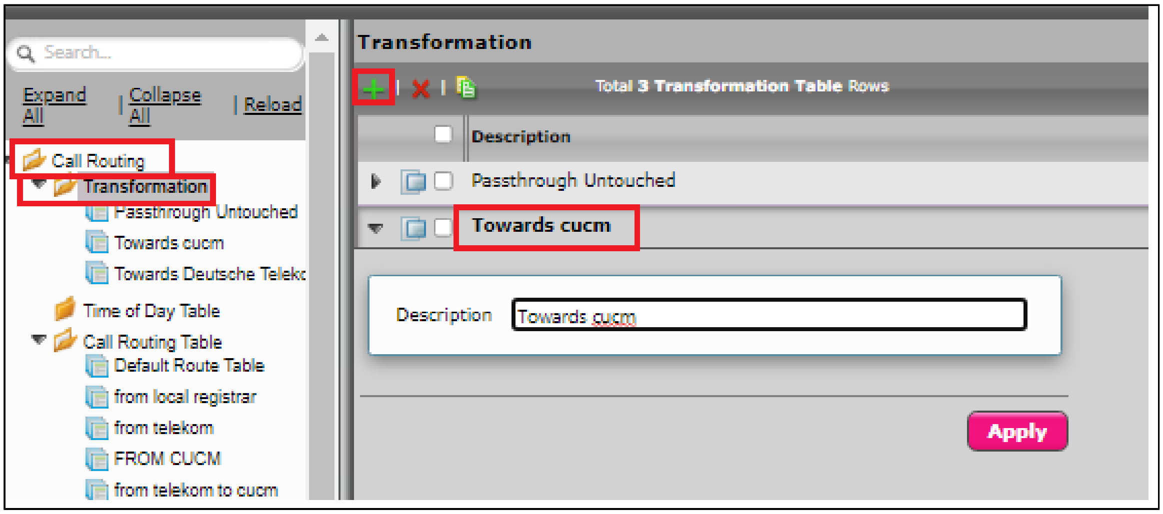
From the **Settings** > **Call Routing** > **Transformation.**

To Create a Transformation Table

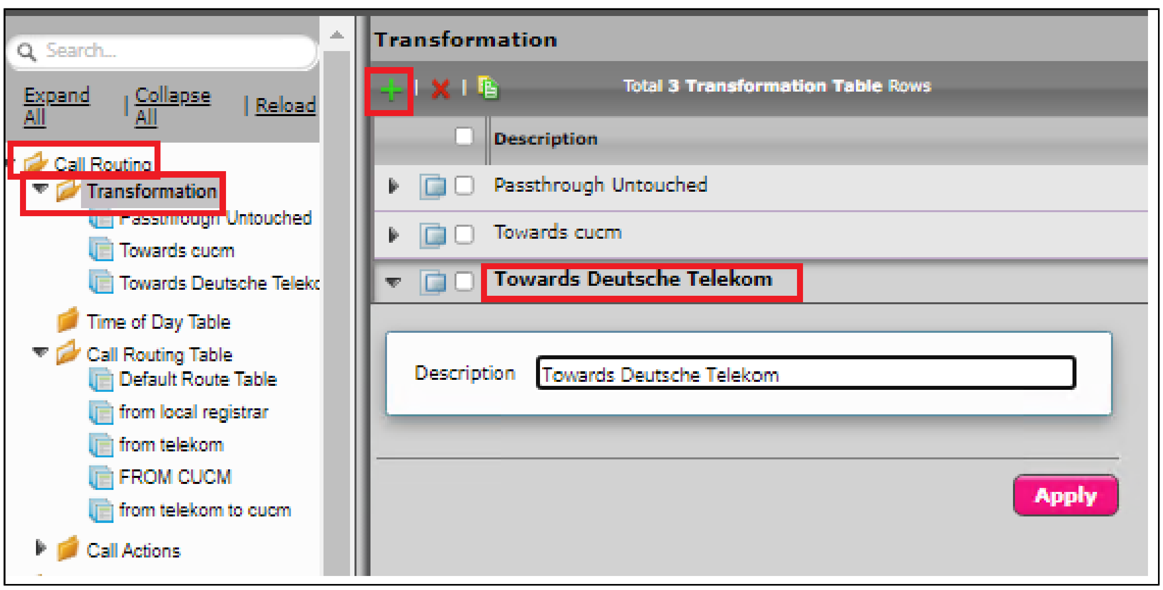
Each Transformation Table contains a list of entries considered as routing rules to execute on. Each rule is executed in order until the end of the table is reached or when a Mandatory entry fails to execute.

Follow the procedure described below to configure Transformation Tables and the Entries.

1. Click the **Create** (+) icon.
2. Enter a descriptive name in the **Description** text field.
3. Click **OK**.



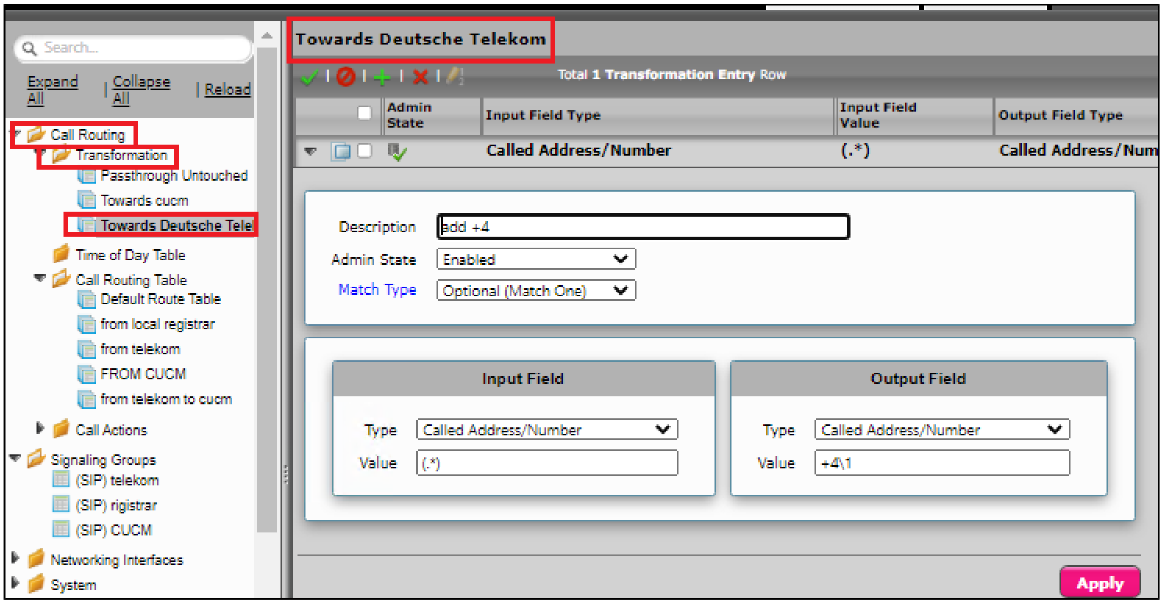
Similarly create transformation table towards Deutsche Telekom.



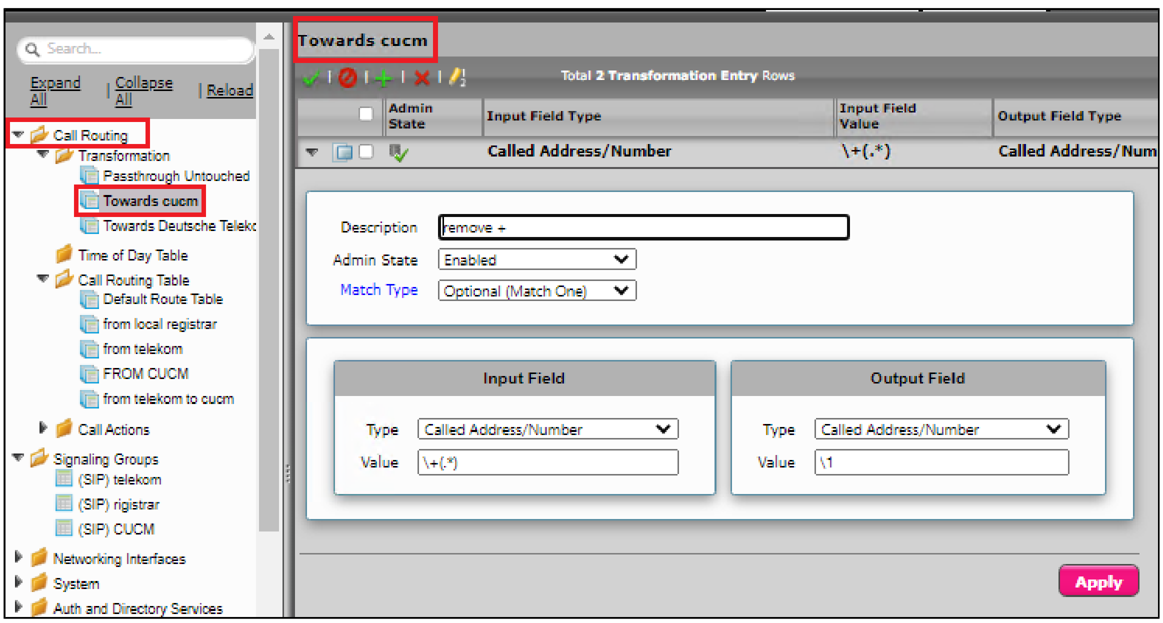
In the lab environment we added +4 to the called number while sending out to Deutsche Telekom. Towards CUCM, we removed + . The followings transformation examples are based on the lab setup. It will differ based on the requirements.

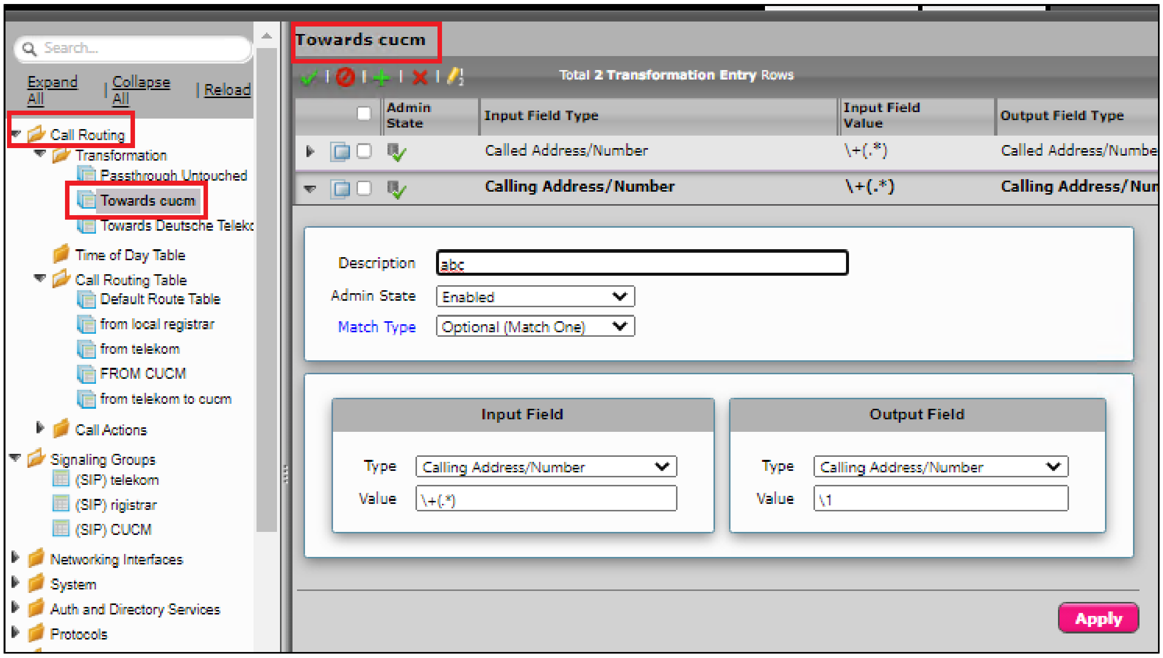
> **Note**
> For details on Transformation Table Entry configuration, refer to Creating and Modifying Entries to Transformation Tables. For call digit matching and manipulation through the use of regular expressions, refer to Creating Call Routing Logic with Regular Expressions.

Towards Deutsche Telekom



Towards CUCM





Call Routing Table

Call Routing allows carrying of calls between Signaling Groups. Routes are defined by Call Routing Tables, which allow for a flexible configuration of which calls to carry, and how to translate them.

Select **Settings** > **Call Routing** > **Call Routing Table.**

Creating an Entry to a Call Routing Table

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

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

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

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

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

To create an entry:

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

   Admin State:

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

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

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

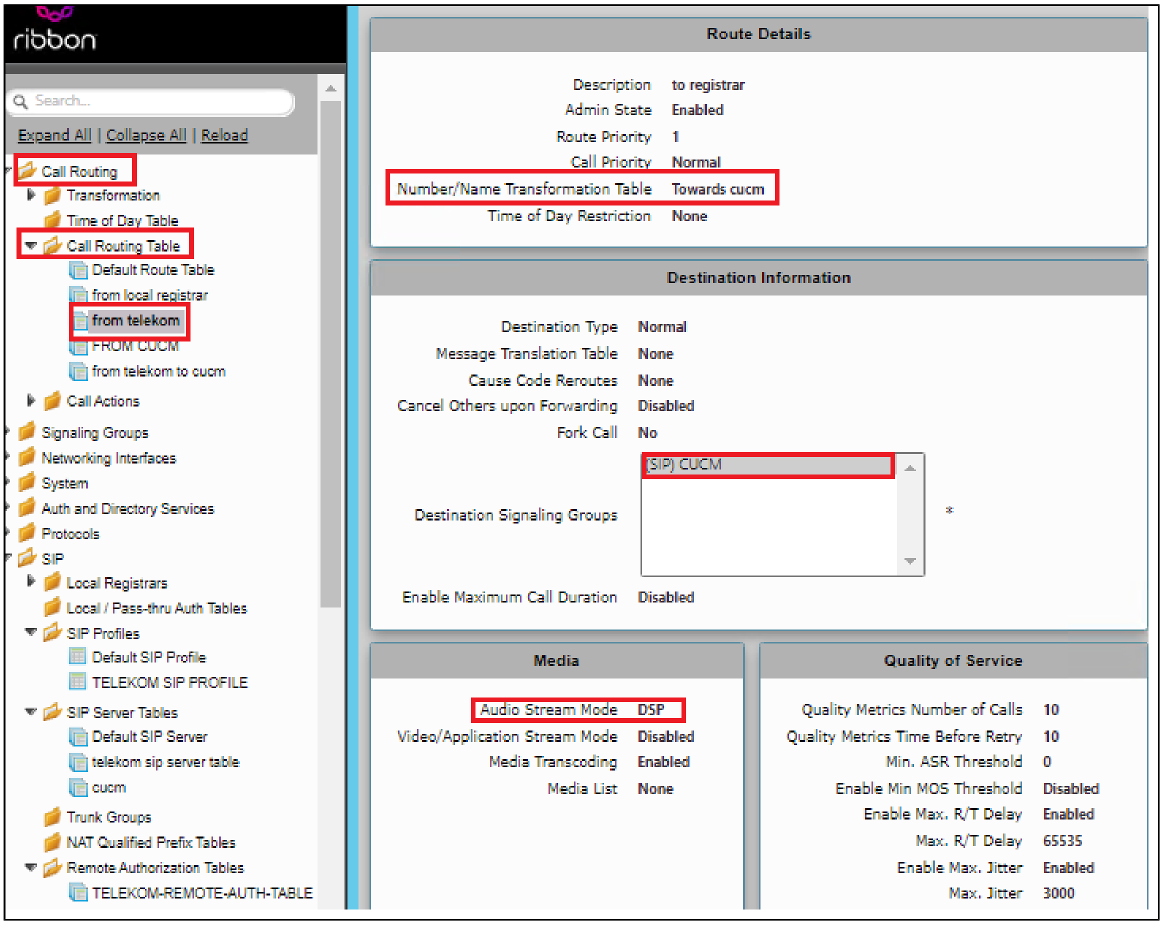
   Destination Signaling Groups:
   Specifies the Signaling Groups used as the destination of calls. The first operational Signaling Group from the list is chosen to place the call. Click the **Add/Edit** button to select the destination signaling group.

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

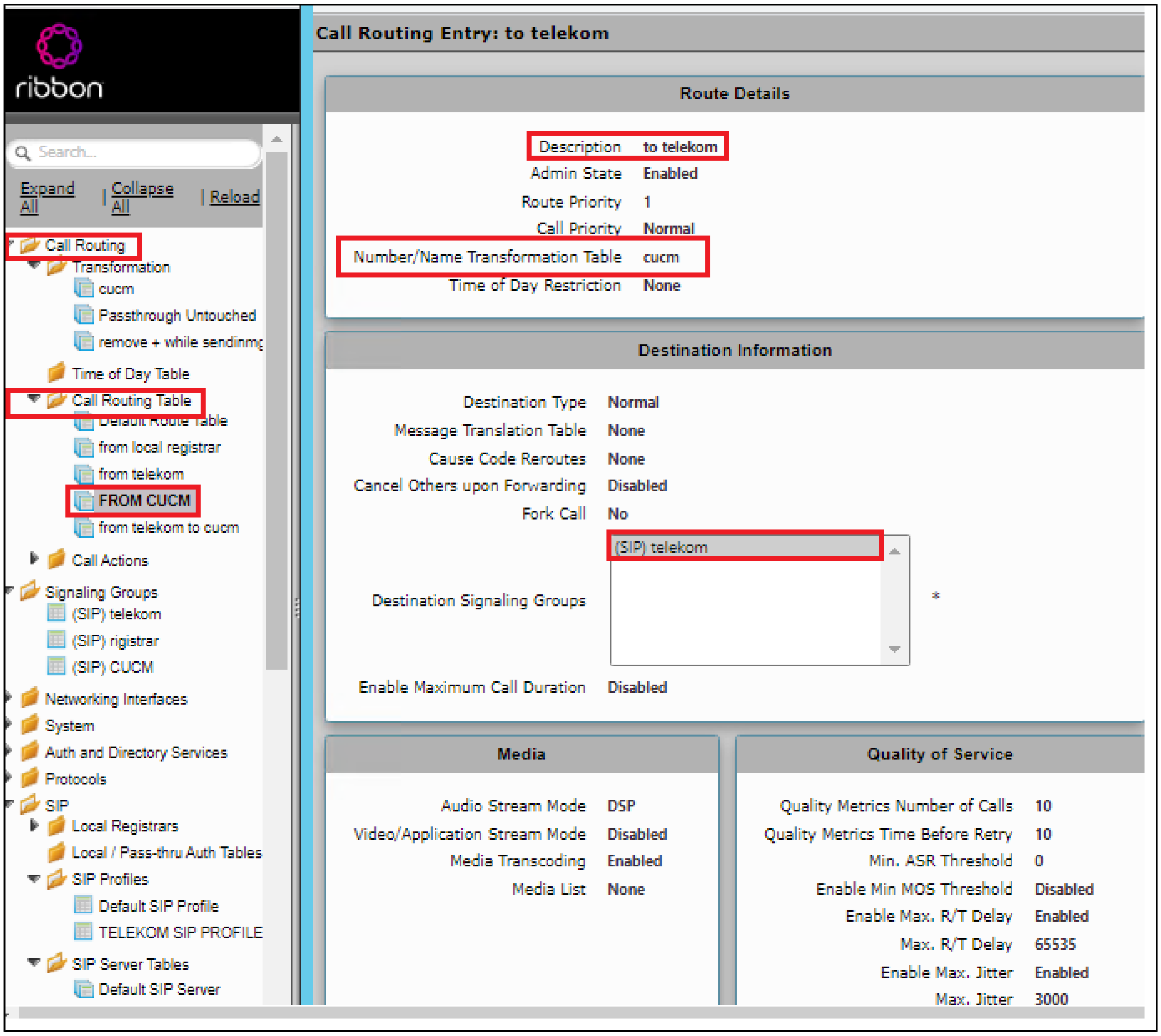
Media Transcoding:
Enabled: Enable Transcoding on SIP-to-SIP calls.

3. Click **Apply**.

Call Routing for Deutsche Telekom signaling group: Any signaling coming from Deutsche Telekom will be routed to CUCM



Call Routing for IP-PBX (CUCM) signaling group : Any signaling coming from CUCM will be routed to Deutsche Telekom



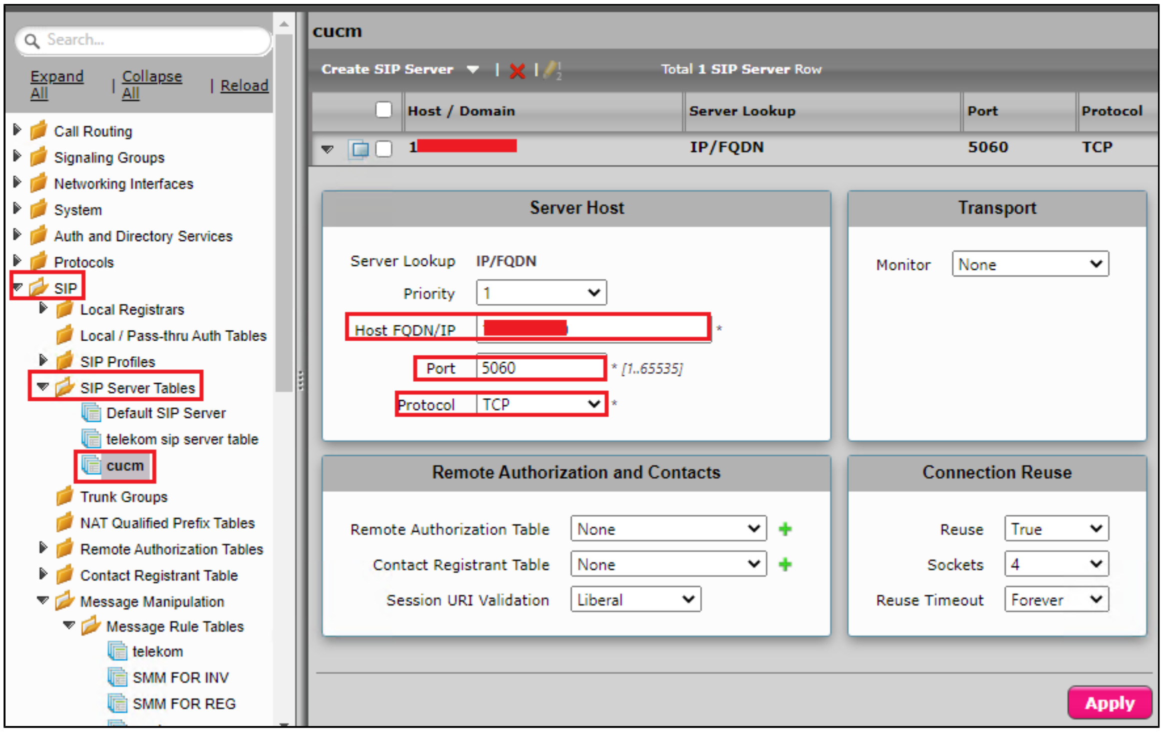
SWe Lite Configuration Towards IP-PBX CUCM

SIP Server Table

SIP Server Tables contain information about the SIP devices connected to the SBC Edge. Create a new SIP Server Table towards IP-PBX (Cisco CUCM)

Select Settings > SIP > SIP Server Tables

- Create a SIP Server Table with IP/FQDN.
- Provide CUCM IP in the Host FQDN/IP.
- Provide Port as 5060.
- Choose Protocol as TCP.
- Click Apply.

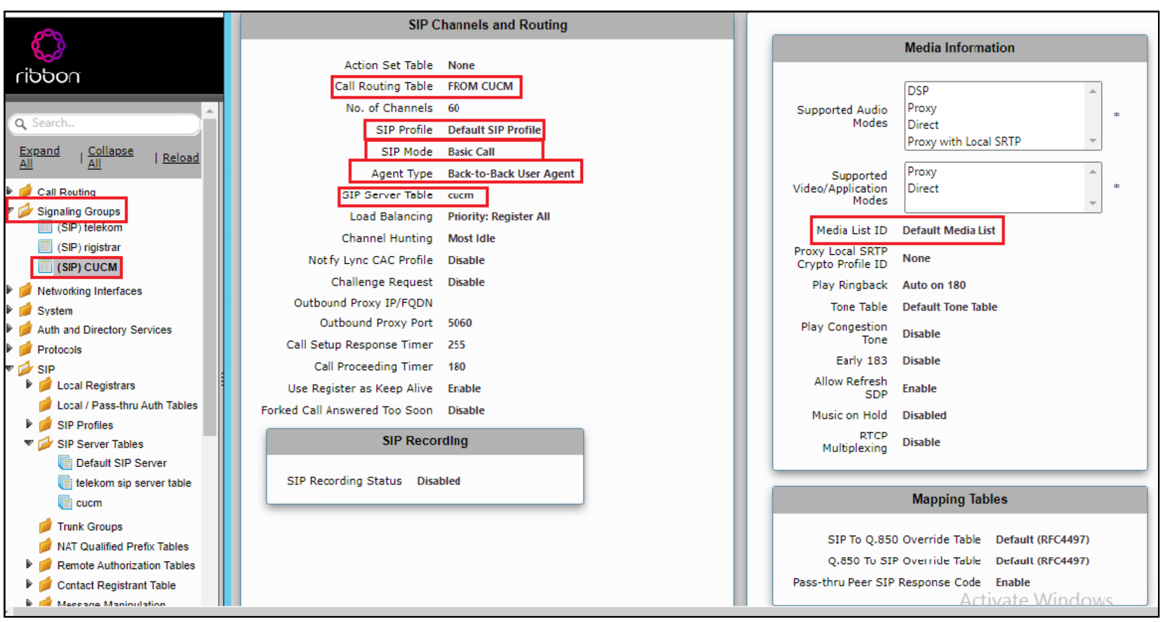


Signaling Group Table

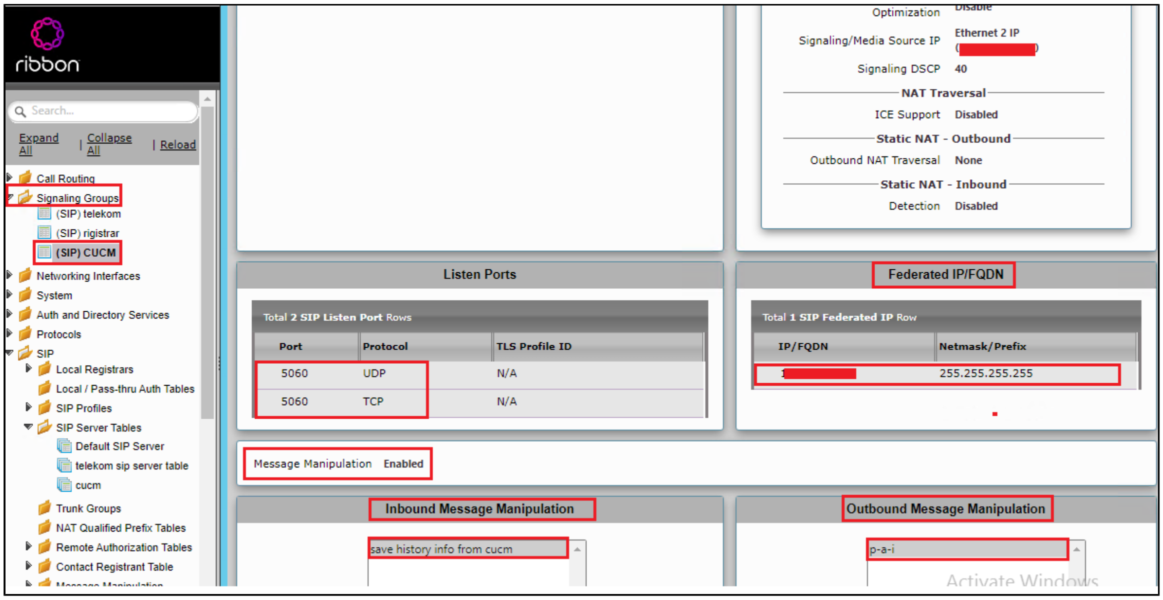
Signaling Groups allow grouping telephony channels together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which Call Routes are selected.

Select Settings > Signaling Groups

- Create an entry in signaling group named "CUCM".
- Choose "Default SIP profile" under SIP Profile.
- Choose Call Routing as "From CUCM".
- Choose Sip Mode as "Basic Call".
- Choose Agent Type "Back to Back user agent".
- Choose Sip Server Table created in the previous step.



- Update the Federated IP/FQDN , i.e. the IP of the CUCM.
- Add a listening port for TCP.



Message Manipulation

The Message Manipulation feature comprises two primary components that work in concert to modify SIP messages. Those components are Condition Rules and Rule Tables. Conditional rule and rule table for the TLS registration and call to work are shown below.

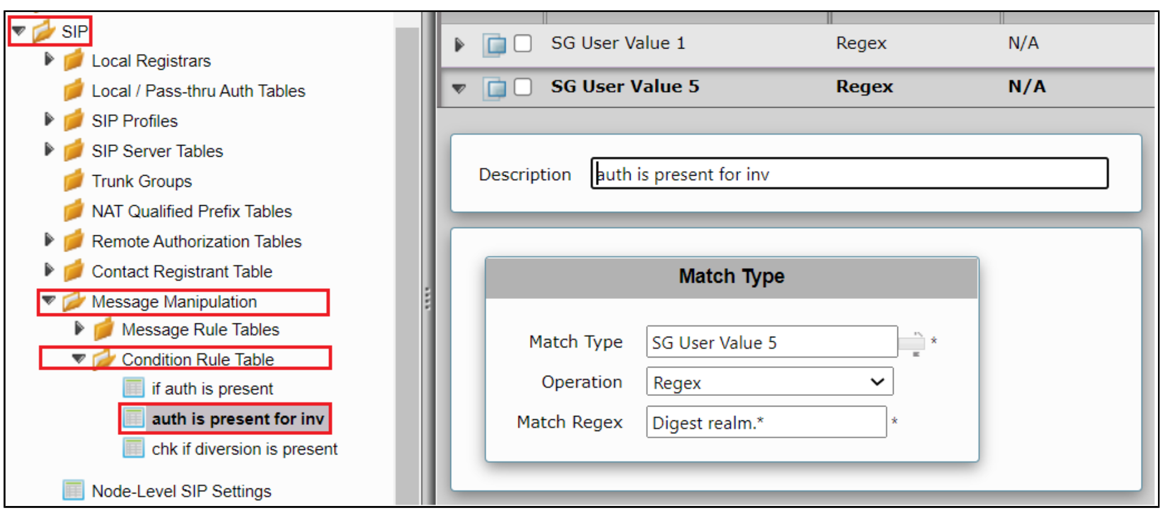
Creating a Condition Rule Table

Condition rules are simple rules that apply to a specific component of a message (e.g., diversion.uri.host, from.uri.host, etc.) The value of the field specified in the Match Type list box can match against a; literal value, token, or REGEX.

Settings > **SIP > Message Manipulation > Condition Rule Table.** Click the Create ( ) icon at the top of the Condition Rule Table page.

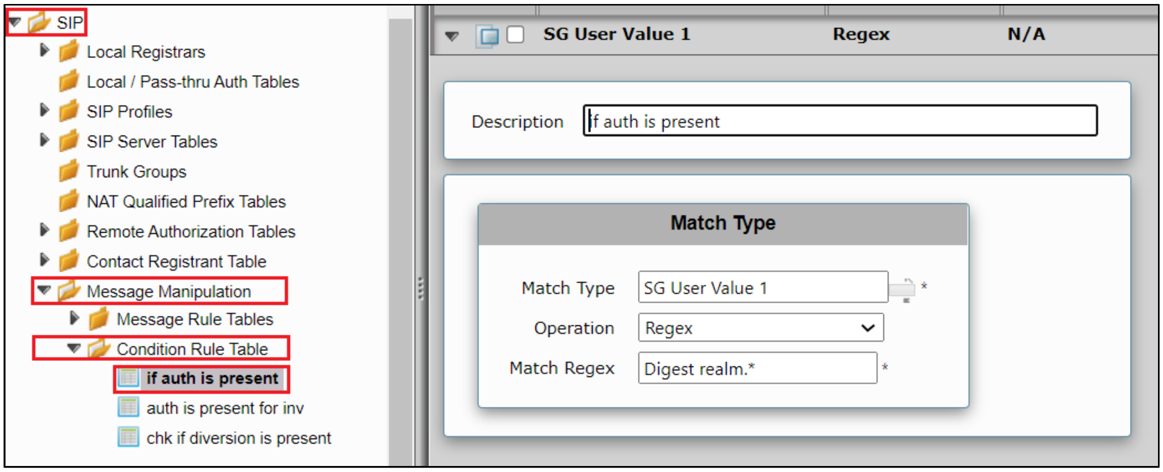
If Authorization is present in INVITE:

- Provide a suitable description for the rule.
- From the Match type drop-down, select "SG USER VALUE 5" as we are checking if the auth is present in the INVITE.
- We have saved the auth header in variable "SG USER VALUE 5" in one of the following Rule tables.



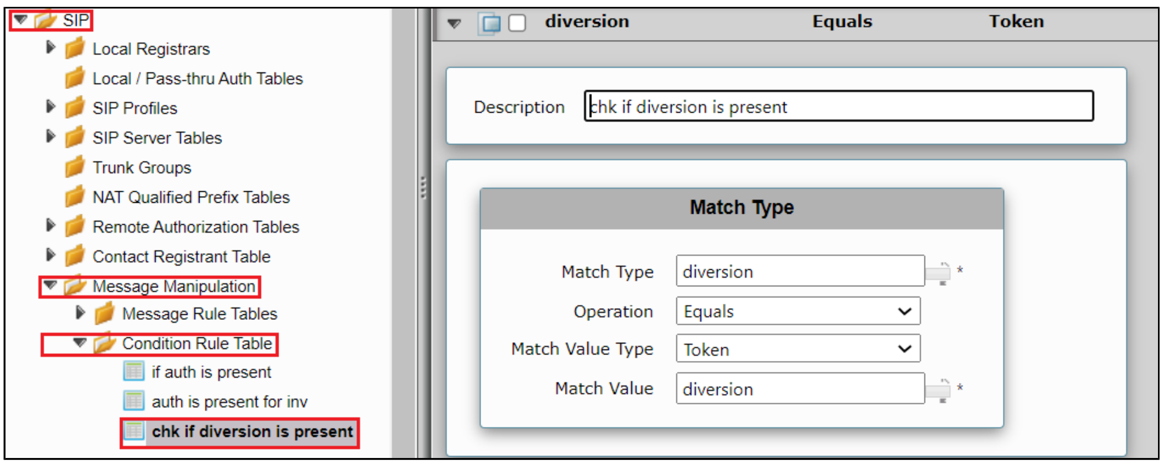
If Authorization is present in REGISTER:

- Provide a suitable description for the rule.
- From the Match type drop-down, select "SG USER VALUE 1" as we are checking if the auth is present in the REGISTER.
- We have saved the auth header in variable "SG USER VALUE 1" in one of the following Rule tables.



If Diversion header is present in INVITE:

- Provide a suitable description for the rule.
- From the Match type drop-down, select "Diversion" .
- Choose Operation as "Equal".
- Choose Match value type as "Token".
- Choose Match Value as Diversion.



Creating a SIP Message Rule Table

Settings > **SIP > Message Manipulation > Message Rule Table.** Click the **Create Message Rule Table(**+)icon.

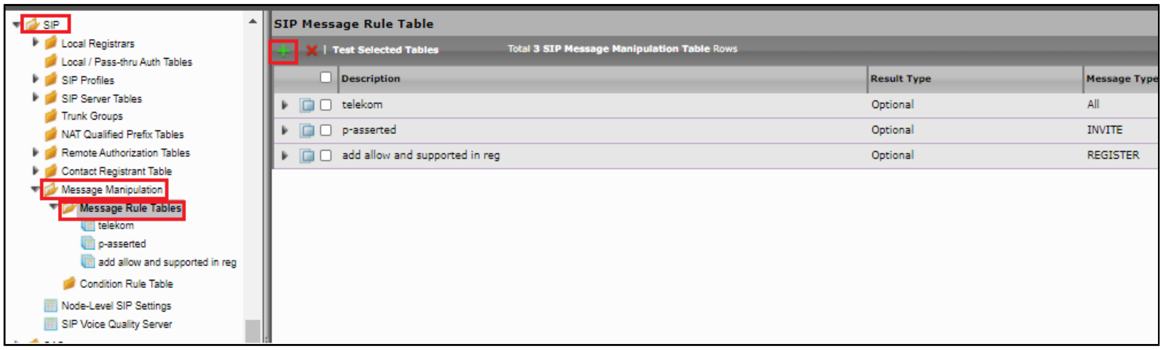
Add FQDN provided by Deutsche Telekom in the URI host of the following headers of the outbound SIP messages.

- To
- From
- Req-URI

Add SIP trunk number in URI user for CONTACT header of all outgoing SIP messages.

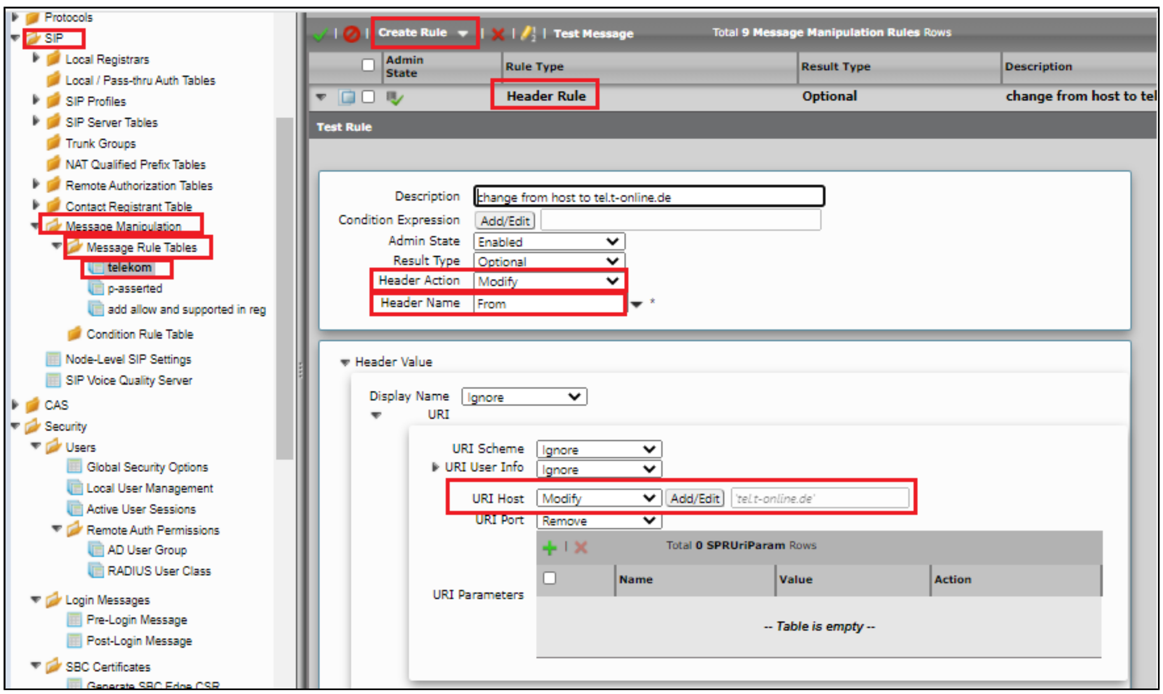
Select Settings > SIP > Message Manipulation > Message Rule Table

Click the Create Message Rule Table(+) icon.

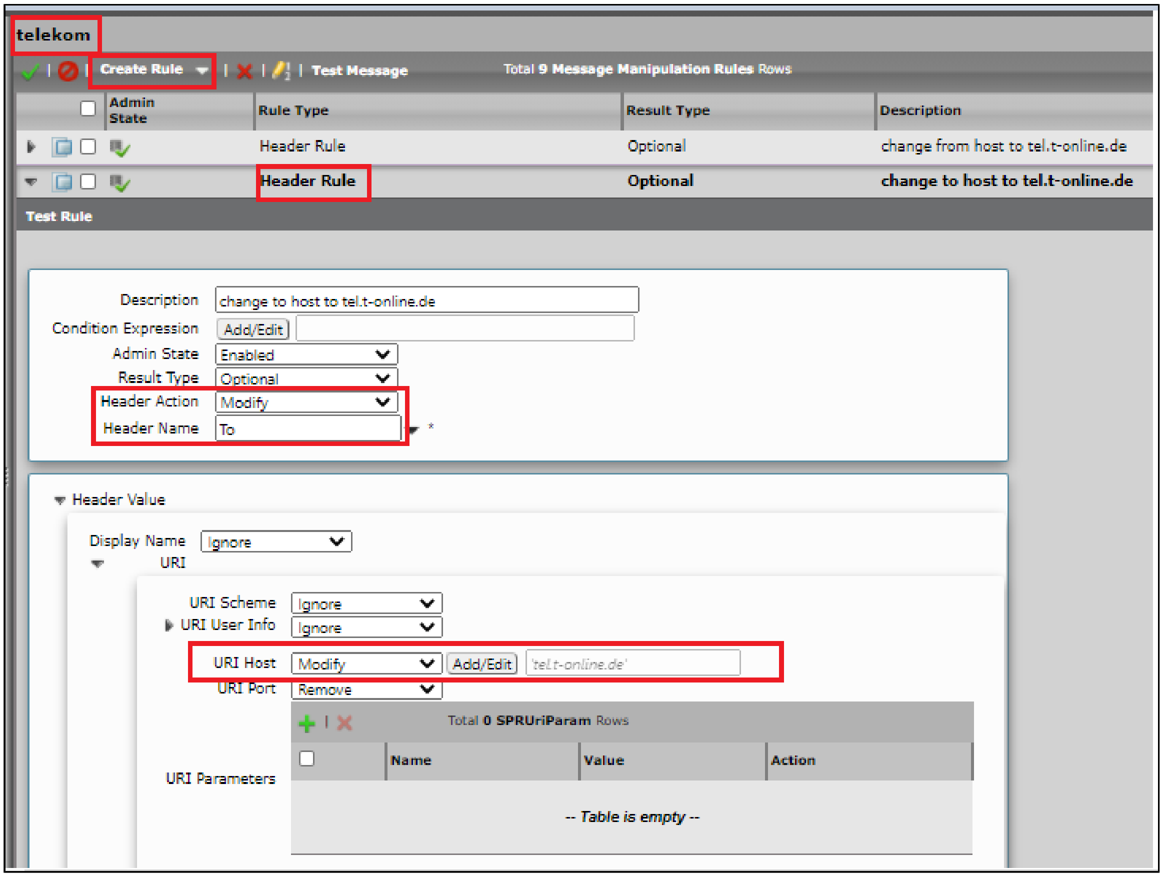


Telekom - From, To, Request URI sends FQDN in URI Host:

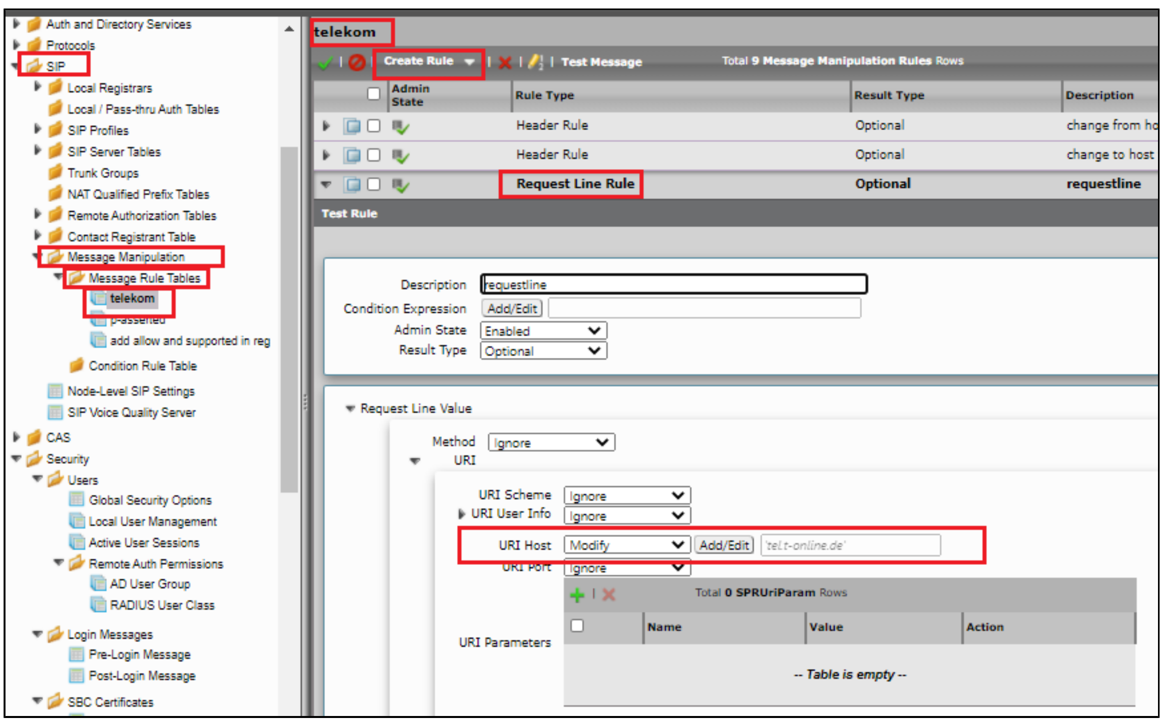
- Provide a description as "Telekom" for the Rule Table.
- Apply the SMM for All messages.
- Click the expand icon next to the Rule Table entry created.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Provide Header action as "Modify" and header name as "From".
- Under URI host give modify and click add/edit. Provide the FDQN that will replace the URI host in from header.



Under "Telekom" Repeat the same for the To header.

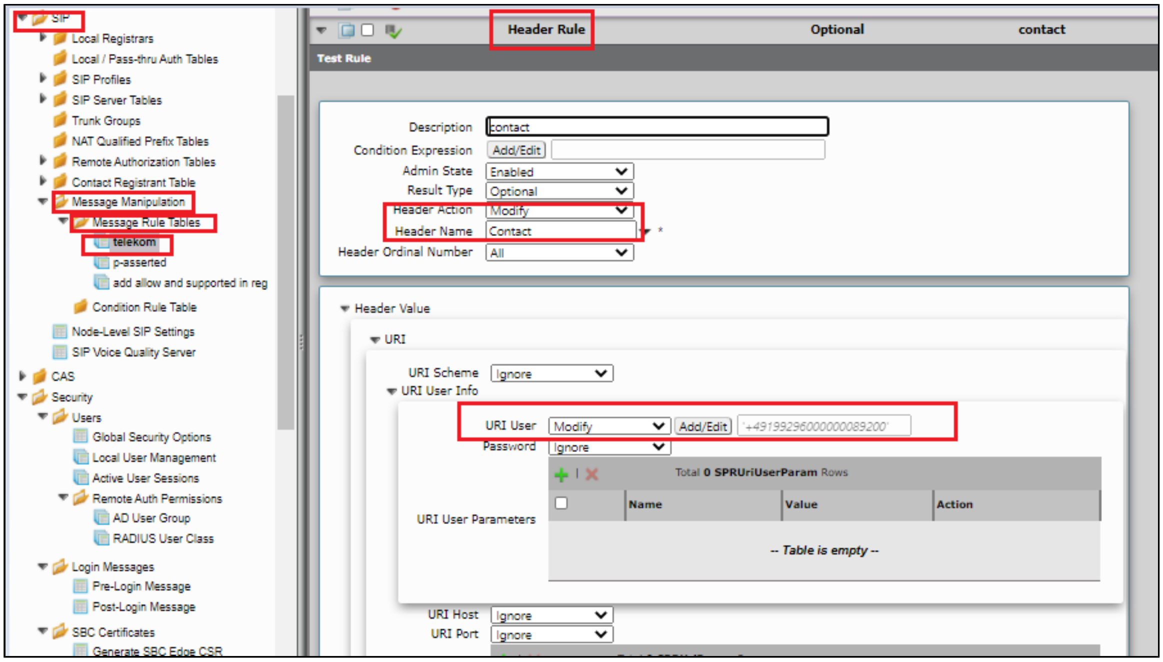


Under "Telekom" repeat the same for request URI.



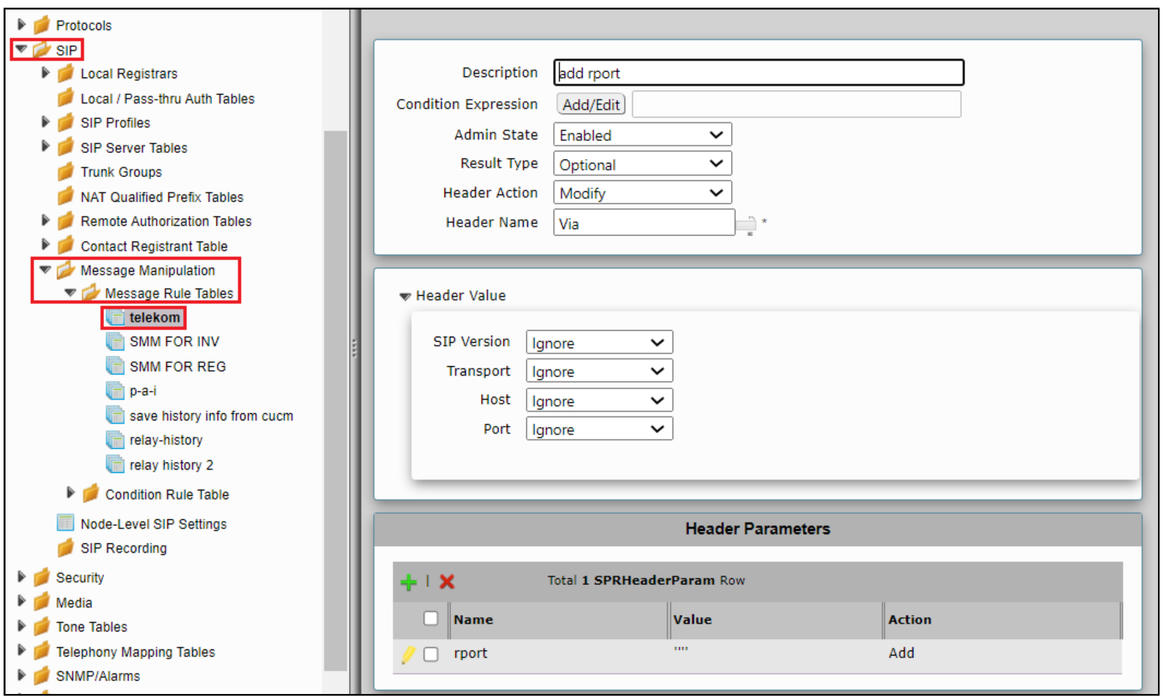
Telekom - add SIP Trunk number in URI user for contact header:

- Click the expand icon next to the Rule Table entry created previously named "Telekom".
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Modify Contact header.
- Add SIP Trunk number under URI User.



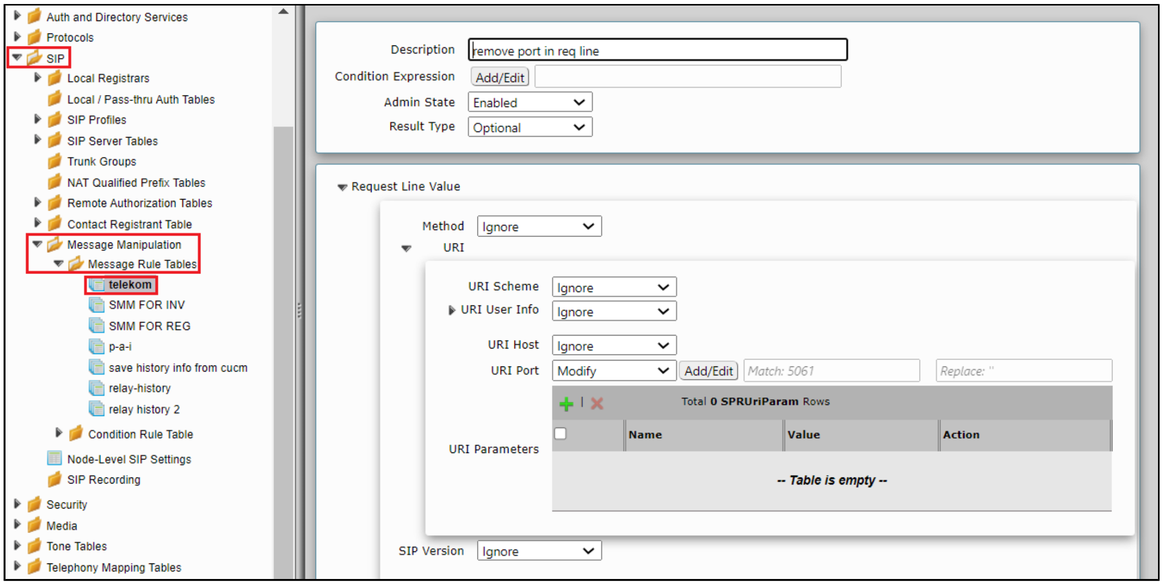
Telekom - add rport in the Via header:

- Click the expand icon next to the Rule Table entry created previously named "Telekom".
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add header parameter "rport" in the Via header.



Telekom - remove port from request line:

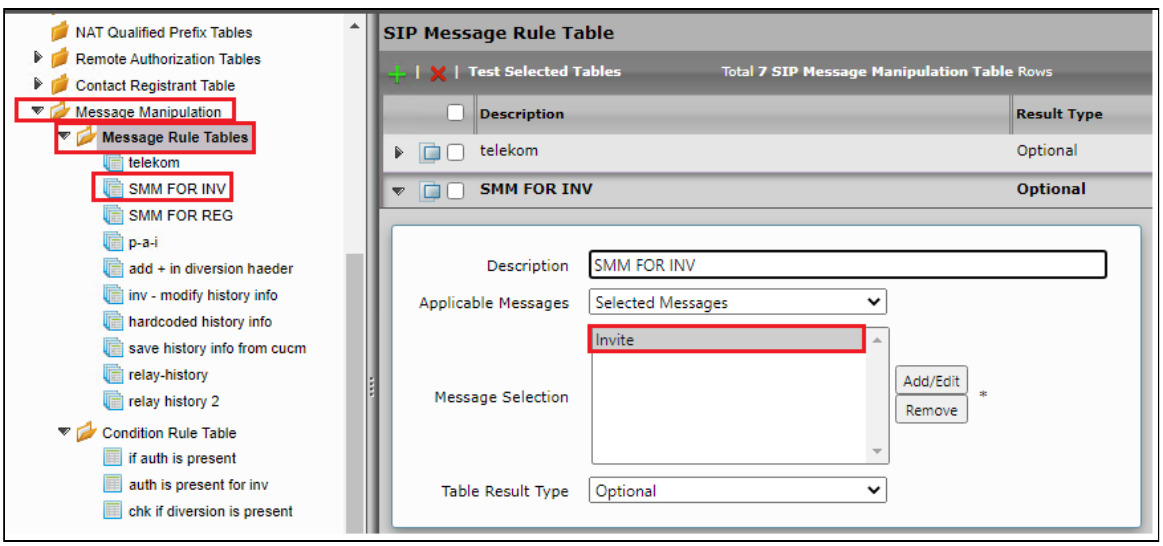
- Click the expand icon next to the Rule Table entry created previously named "Telekom".
- From the Create Rule drop-down box, select Request line Rule.
- Provide the desired description.
- Remove port from request line.



Create a new rule table for INVITE messages.

Settings > **SIP > Message Manipulation > Message Rule Table.** Click the **Create Message Rule Table(**+**)**icon.

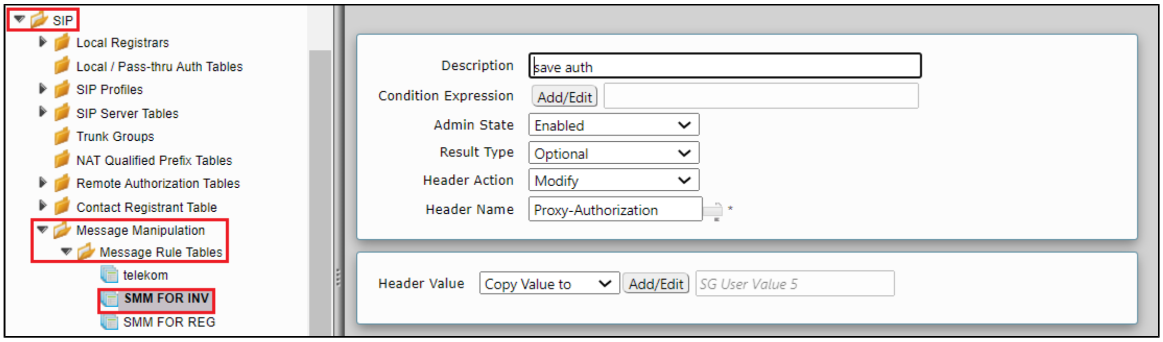
- Provide a description for the Rule Table.
- Apply the SMM only for the Selected messages and choose Invite from the Message Selection list.
- Click **OK.**



SMM for INVITE - save Proxy-Authorization header:

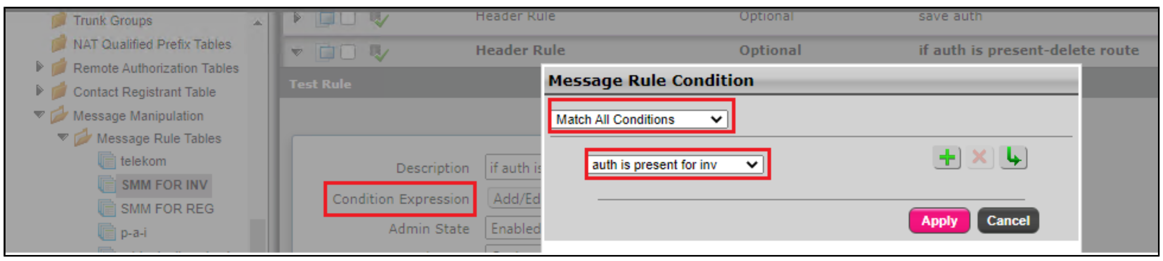
- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Save the Proxy-Authorization header in variable "SG User Value 5".

> **Note**
> This is used in the Condition Rule Table.

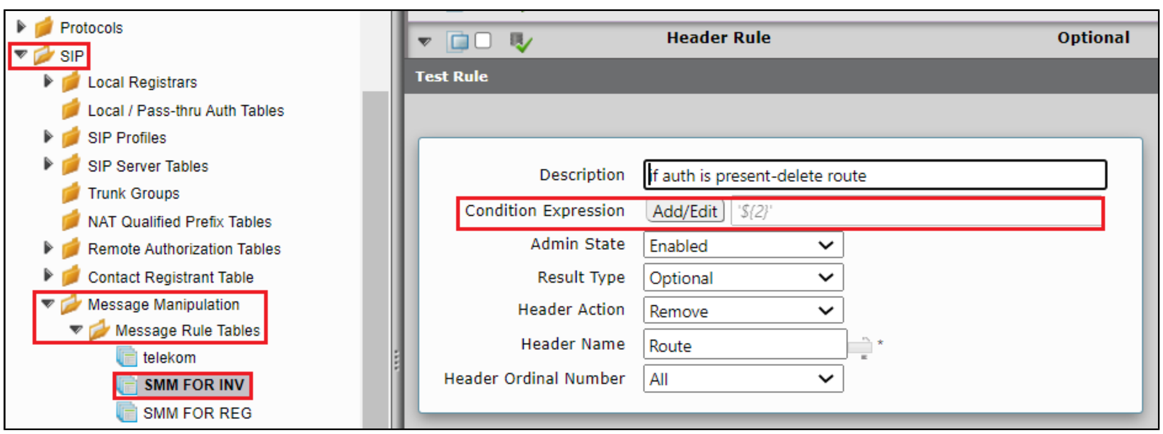


SMM for INVITE - If Authorization is present in INVITE delete route:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Attach Condition Rule "**If Auth is present in INVITE"** in condition Expression.



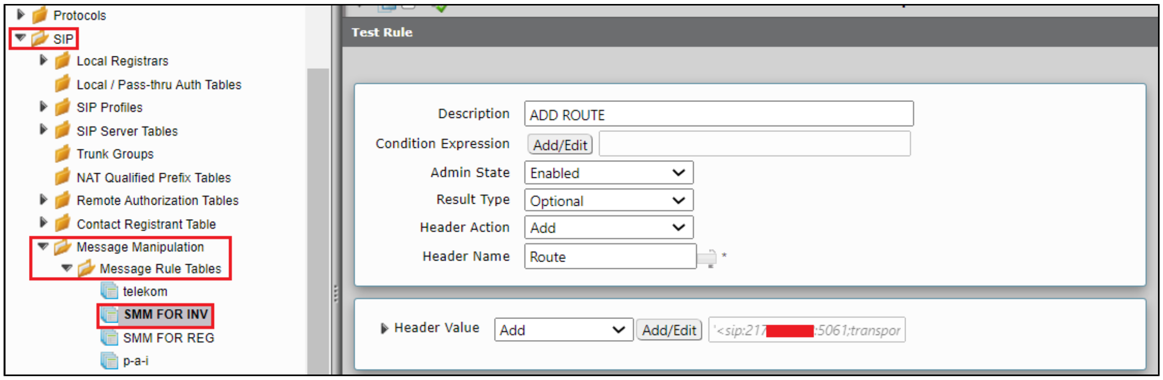
- Remove all Route header from INVITE.



Note
To avoid multiple instances of the same header in INVITE message, All the instances of the header are first removed and then the single instance is added again. Condition Rule is added to achieve it for the following SMM's.

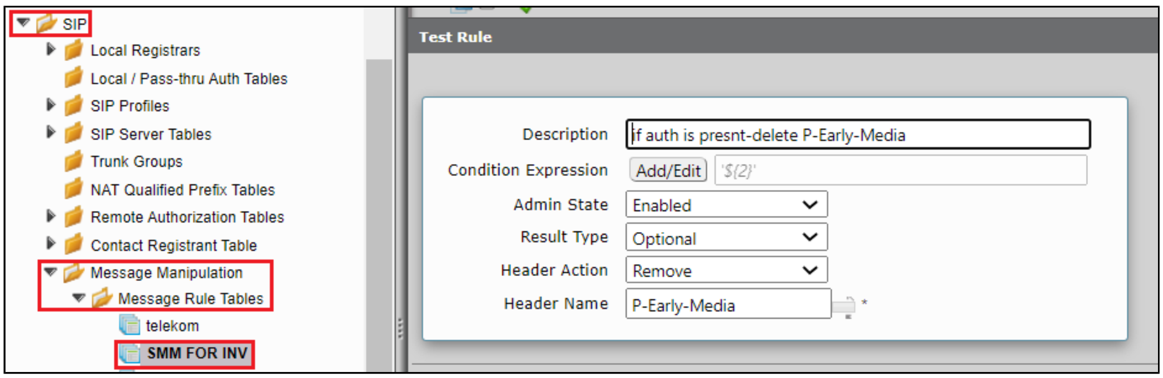
SMM for INVITE - add route:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add Route header with the Deutsche Telekom resolved IP.



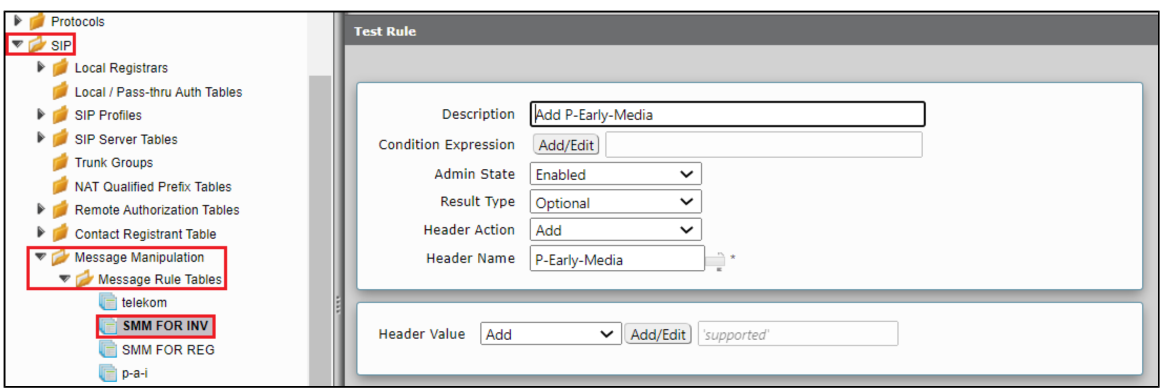
SMM for INVITE - If Authorization is present in INVITE delete P-Early-Media:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Attach Condition Rule "**If Auth is present in INVITE"** in condition Expression.
- Remove all P-Early-Media header from INVITE.



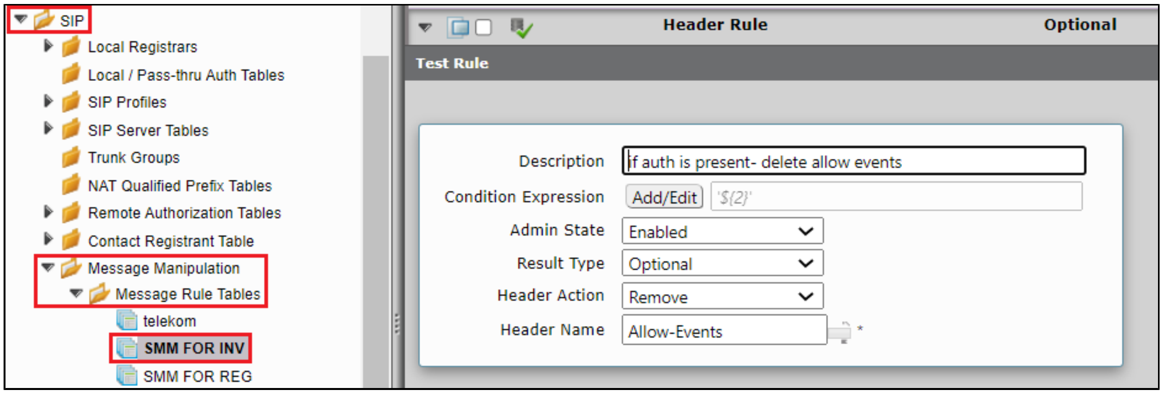
SMM for INVITE - Add P-Early-Media:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add P-Early-Media header.



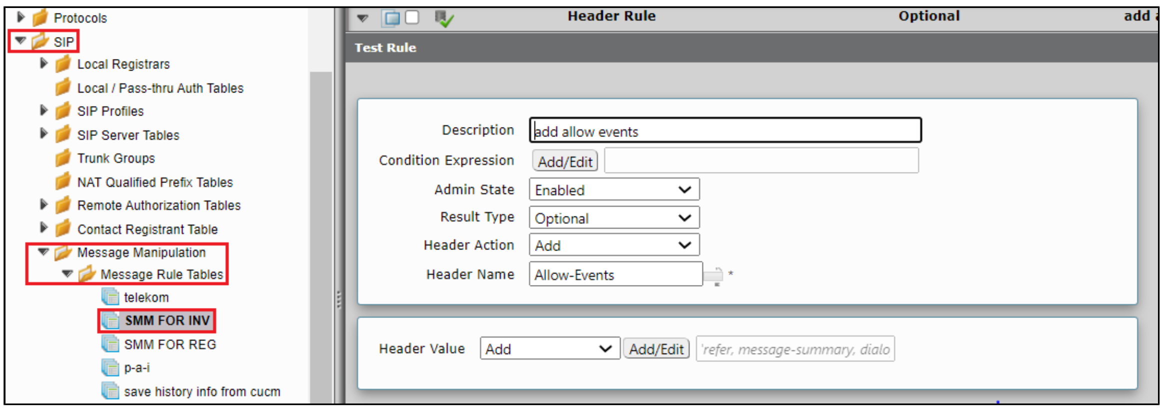
SMM for INVITE - If Authorization is present in INVITE delete Allow-Events:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Attach Condition Rule "**If Auth is present in INVITE"** in condition Expression.
- Remove all Allow-Events header from INVITE.



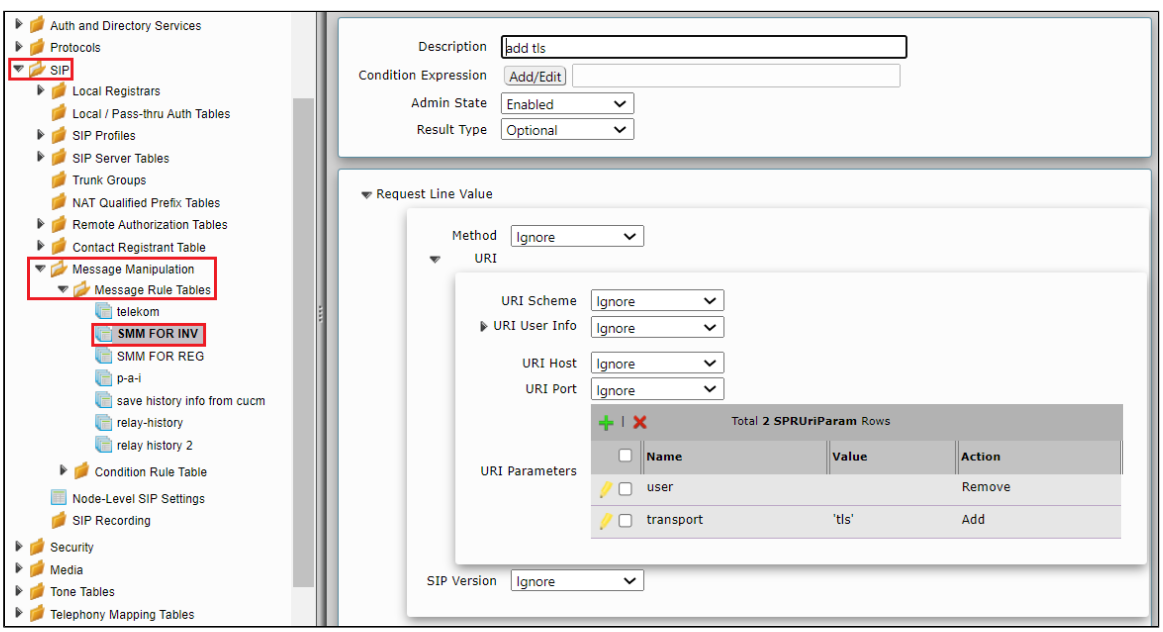
SMM for INVITE - Add Allow-Events

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add Allow-Events header.



SMM for INVITE - Remove user and Add transport parameter in request line URI:

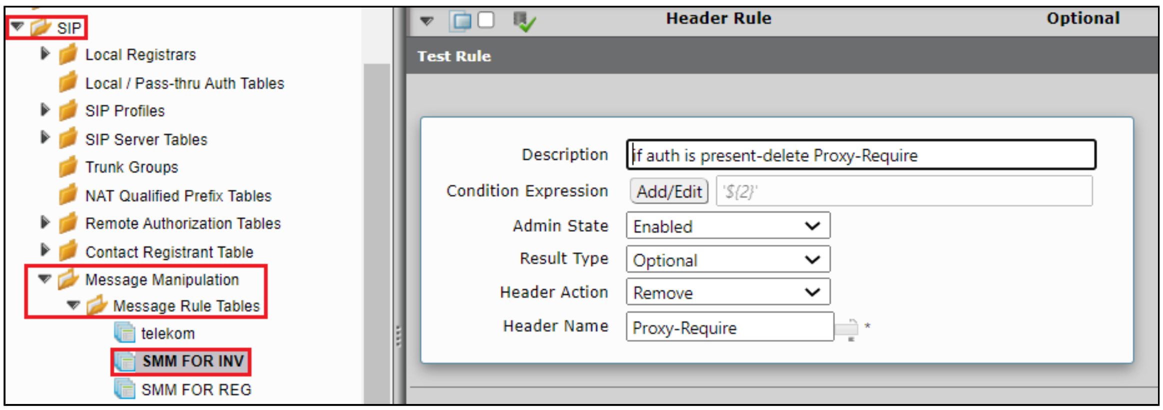
- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Request Line Rule.
- Provide the desired description.
- Remove user and Add transport parameter in request line URI.



> **Note**
> For TLS calls to work INVITE messages sent to Deutsche Telekom should have the following headers.
>
> The initial INVITE includes the SIP header fields:
>
> • Proxy-Require: mediasec
> • Require: mediasec
> • Security-Verify: msrp-tls;mediasec
> • Security-Verify: sdes-srtp;mediasec
> • Security-Verify: dtls-srtp;mediasec
>
> Additionally, the SDP includes the attribute:
>
> • a=3ge2ae:requested

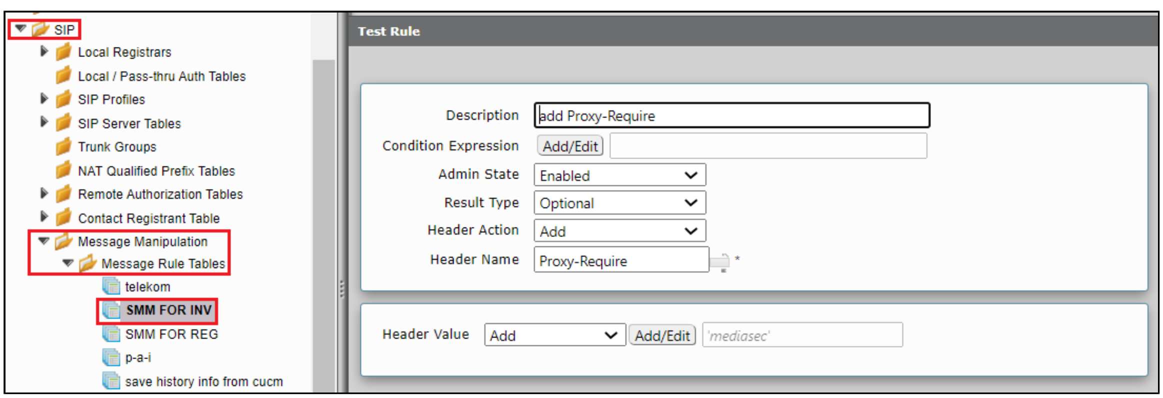
SMM for INVITE - If Authorization is present in INVITE delete Proxy-Require:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Attach Condition Rule "**If Auth is present in INVITE"** in condition Expression.
- Remove all Proxy-Require header from INVITE.



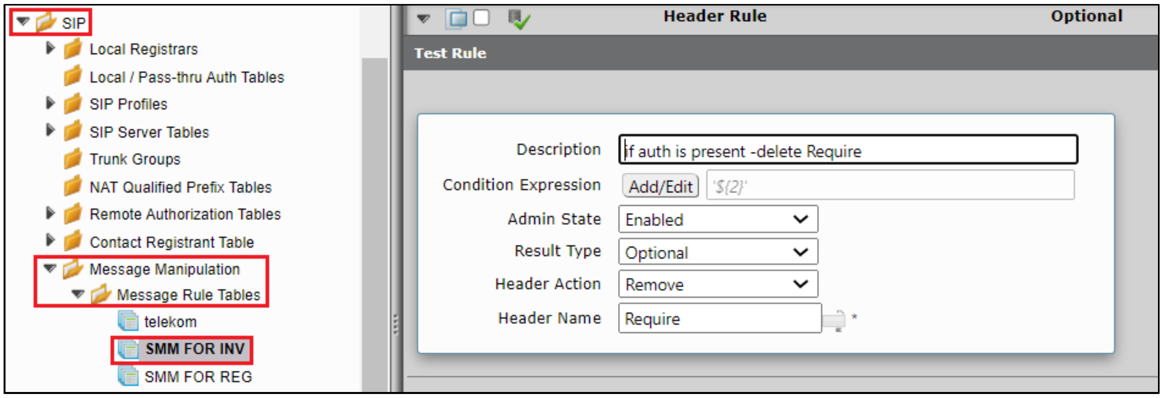
SMM for INVITE - Add Proxy-Require

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add Proxy-Require header with value "mediasec".



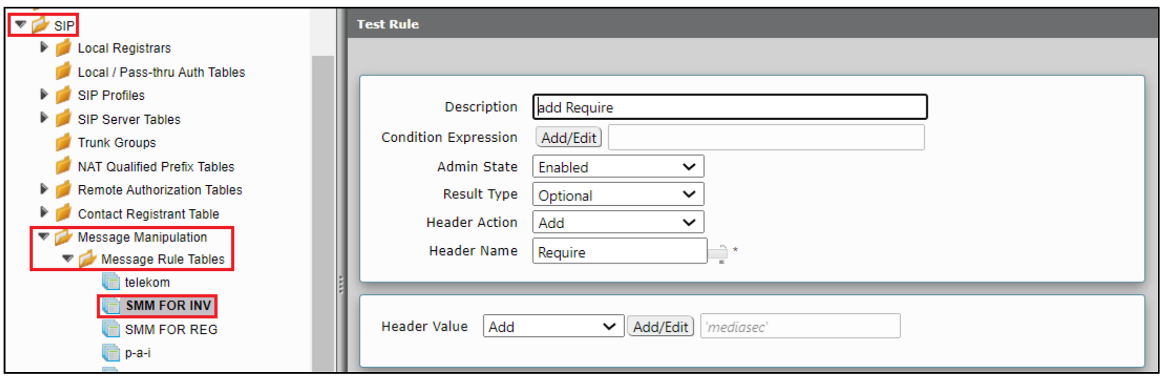
SMM for INVITE - If Authorization is present in INVITE delete Require:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Attach Condition Rule "**If Auth is present in INVITE"** in condition Expression.
- Remove all Require header from INVITE.



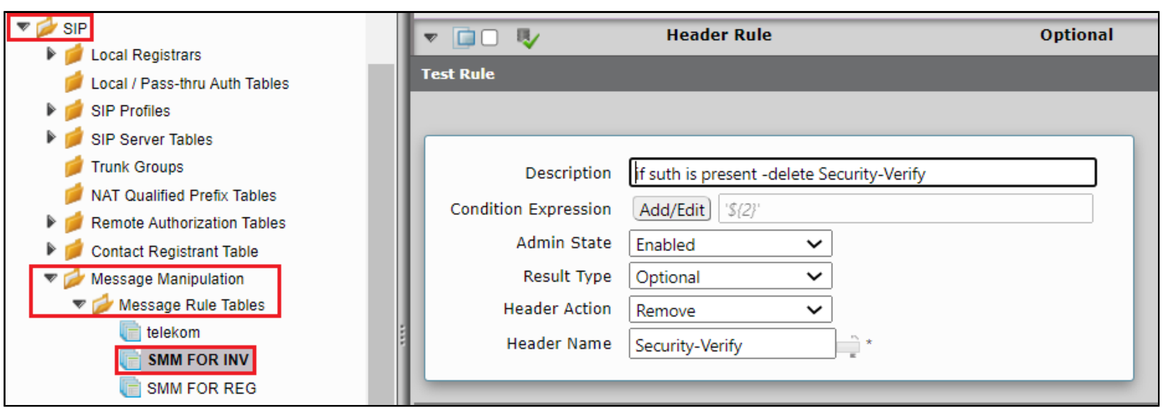
SMM for INVITE - Add Require:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add Require header with value "mediasec".



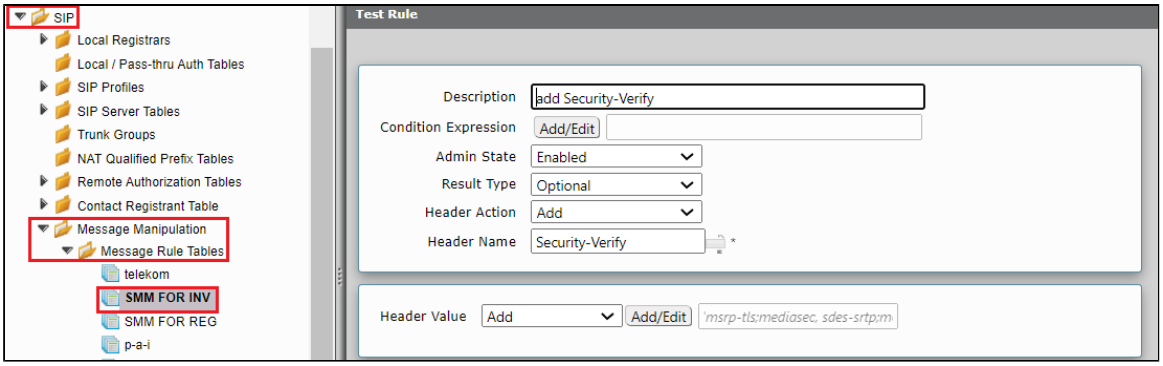
SMM for INVITE - If Authorization is present in INVITE delete Security-Verify:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Attach Condition Rule "**If Auth is present in INVITE"** in condition Expression.
- Remove all Security-Verify header from INVITE.



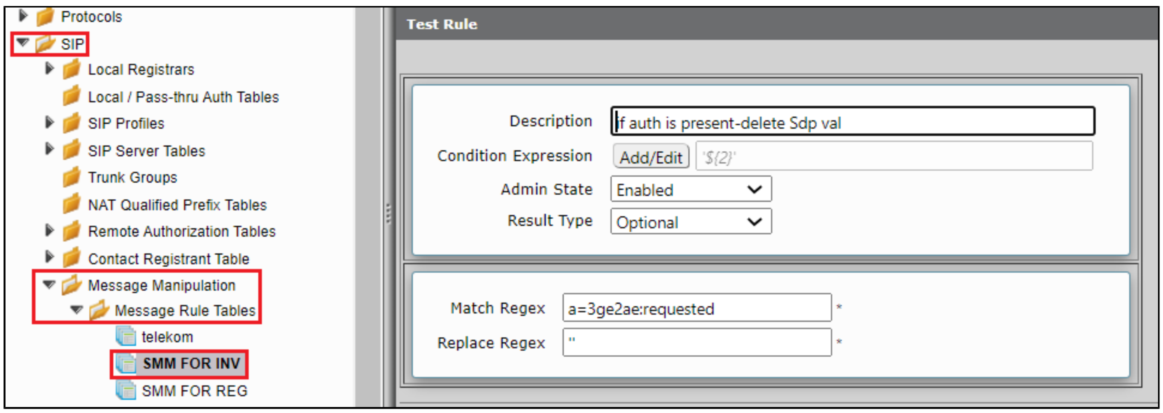
SMM for INVITE - Add Security-Verify:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- AddSecurity-Verify header with value "msrp-tls;mediasec, sdes-srtp;mediasec, dtls-srtp;mediasec".



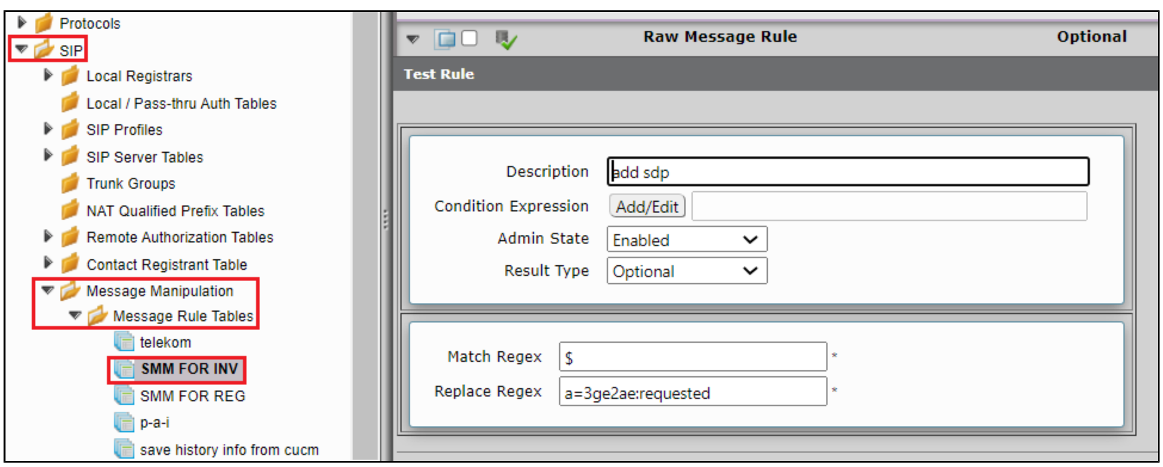
SMM for INVITE - If Authorization is present in INVITE delete SDP info a=3ge2ae:requested:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Raw Message Rule.
- Provide the desired description.
- Attach Condition Rule "**If Auth is present in INVITE"** in condition Expression.
- Remove "a=3ge2ae:requested" from INVITE SDP.



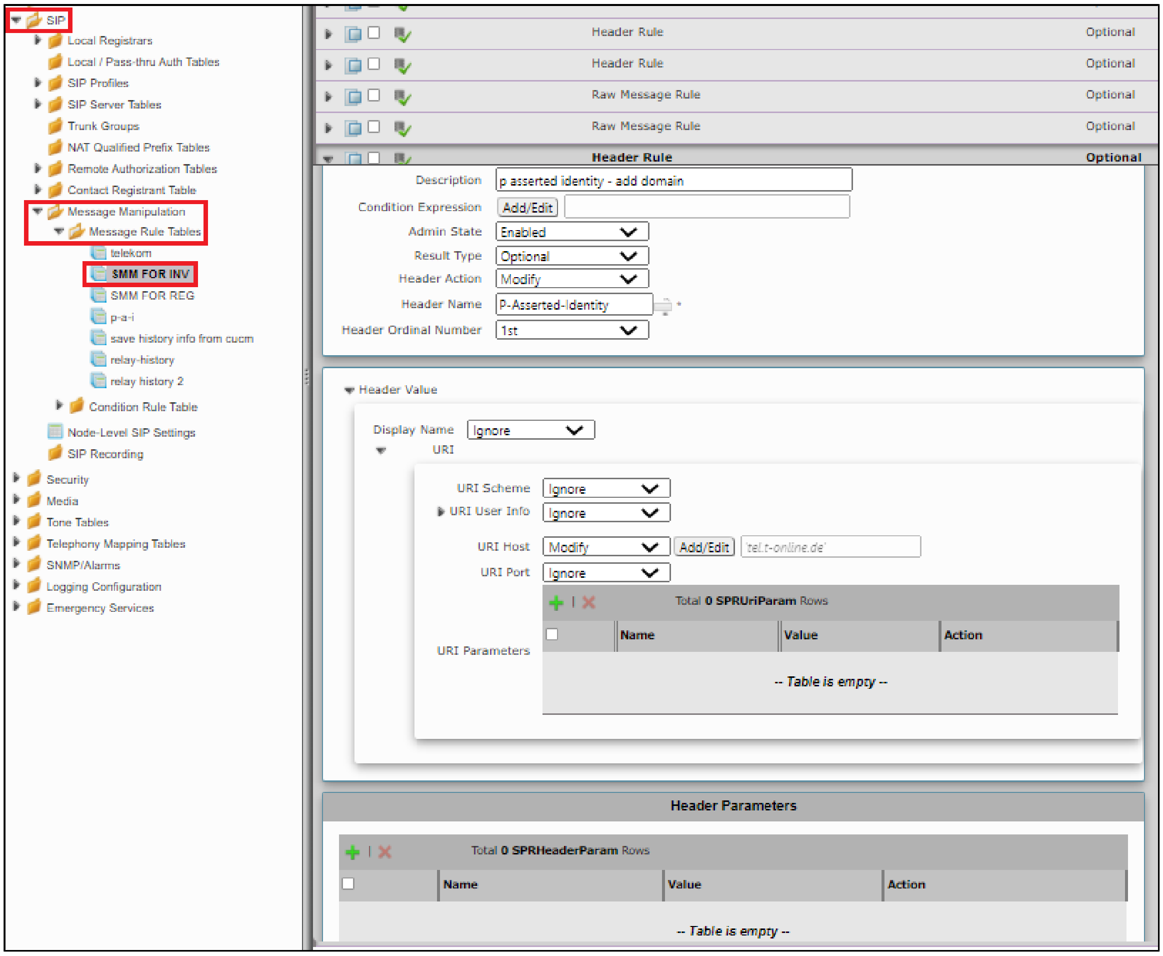
SMM for INVITE - Add a=3ge2ae:requested in INVITE SDP:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Raw Message Rule.
- Provide the desired description.
- Add "a=3ge2ae:requested" from INVITE SDP.



SMM for INVITE - Add P-Asserted-Identity:

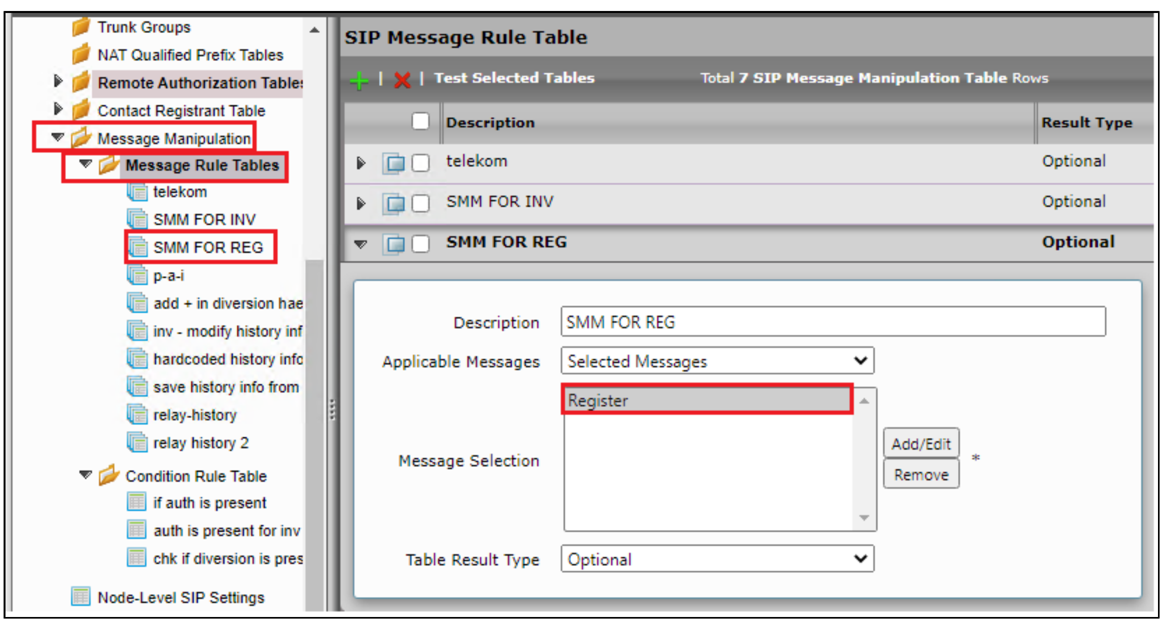
- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Modify P-Asserted-Identity header, the host IP should have Deutsche Telekom domain.



Create a new rule table for REGISTER messages.

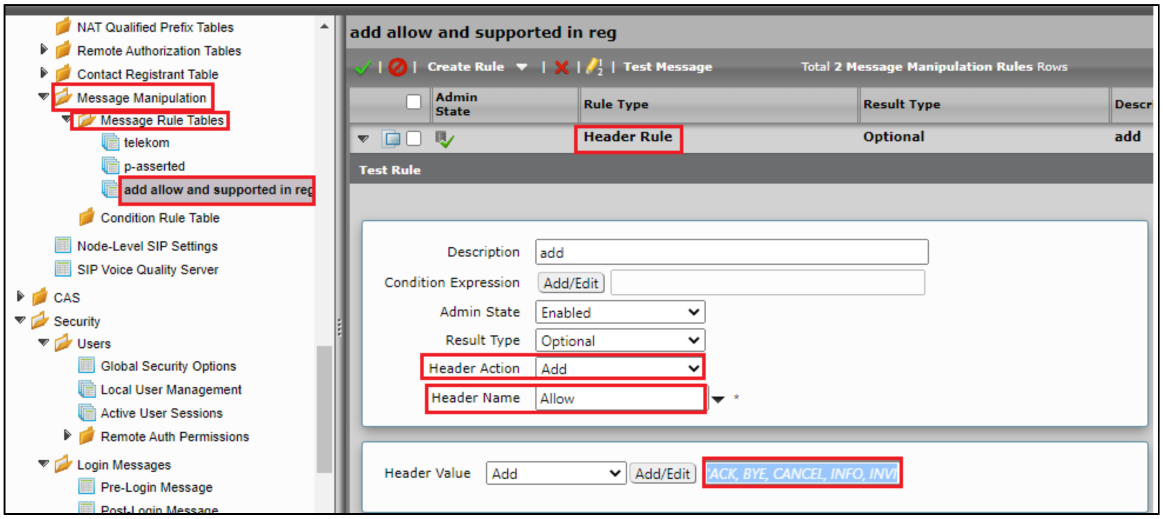
Settings > **SIP > Message Manipulation > Message Rule Table.** Click the **Create Message Rule Table( )** icon.

- Provide a description for the Rule Table.
- Apply the SMM only for the Selected messages and choose Register from the Message Selection list.
- Click **OK**



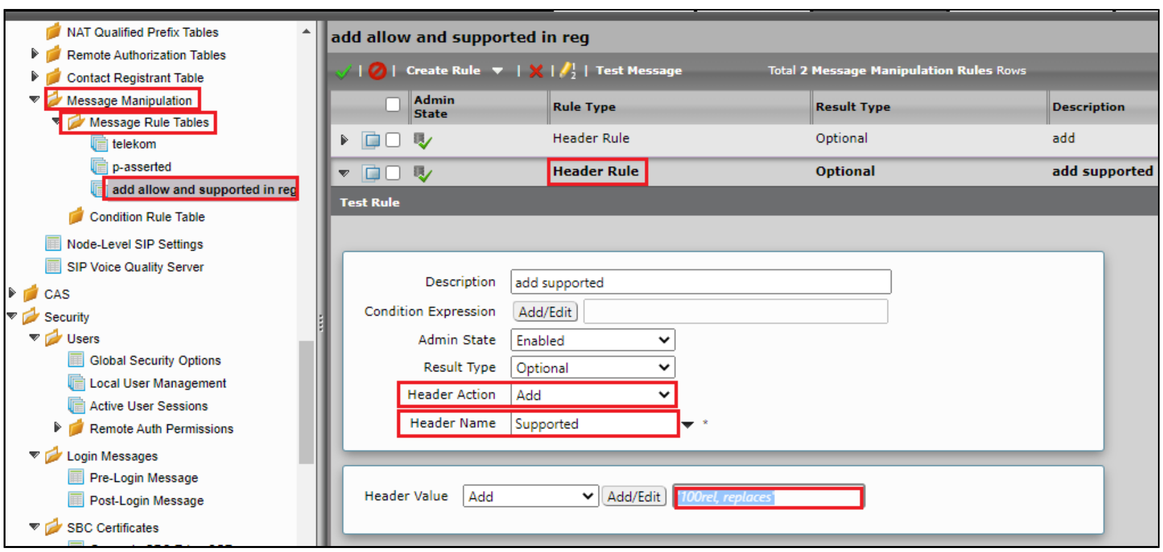
SMM for REG - Add Allow in REGISTER:

- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Provide Header action as "Add" and header name as "Allow".
- Under header value give "Add" and click on add/edit and provide 'ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, MESSAGE, SUBSCRIBE, UPDATE, PRACK, REFER'.
- Click **Apply**.



SMM for REG - Add Supported in REGISTER:

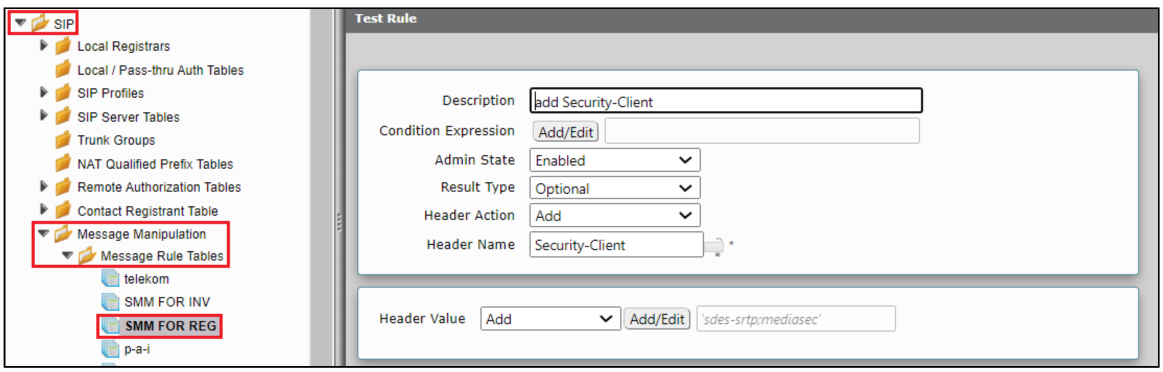
- Under the same Message Rule Table, choose **Create Rule** from the drop-down box, select Header Rule.
- Provide the desired description.
- Provide Header action as "Add" and header name as "Supported".
- Under header value, give "Add" and click on add/edit and provide '100rel, replaces'.
- Click **Apply**.



> **Note**
> For successful registration of trunk to Deutsche Telekom, the following header must be in REGISTER header.
>
> For an initial REGISTER without Authentication Challenge, include the SIP header fields:
>
> • Security-Client: sdes-srtp;mediasec
> • Proxy-Require: mediasec
> • Require: mediasec
>
> For the following REGISTER with Authentication Challenge, in addition to the originally included SIP header fields it should also contain the following headers:
>
> • Security-Verify: msrp-tls;mediasec
> • Security-Verify: sdes-srtp;mediasec
> • Security-Verify: dtls-srtp;mediasec

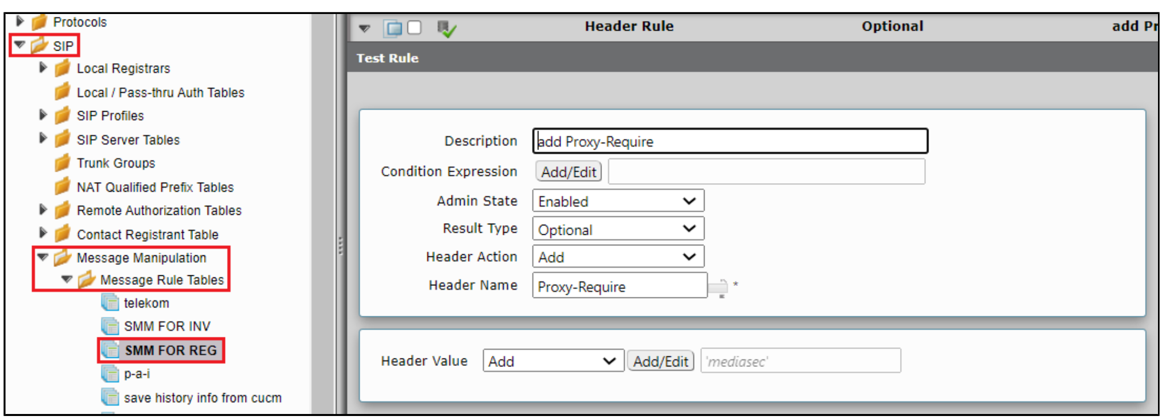
SMM for REG - Add Security-Client:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description
- Add Security-Client with value "sdes-srtp;mediasec".



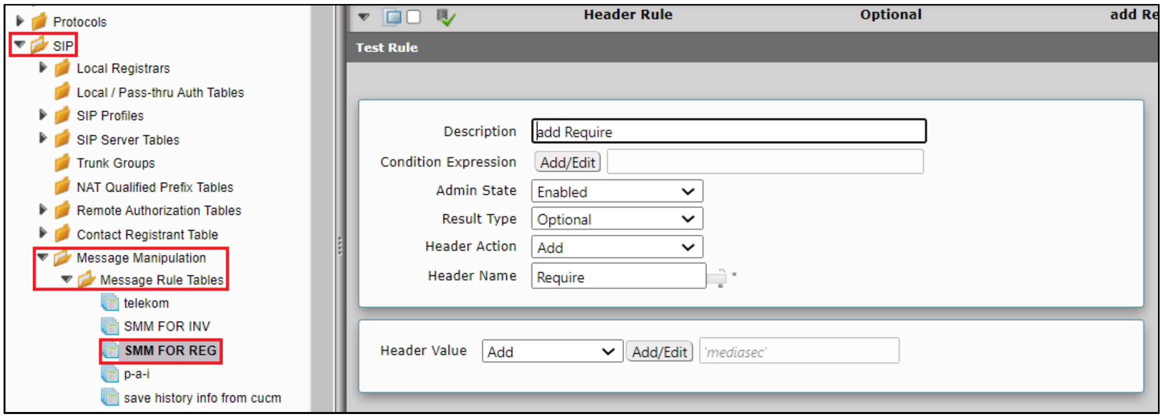
SMM for REG - Add Proxy-Require:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description
- Add Proxy-Require with value "mediasec".



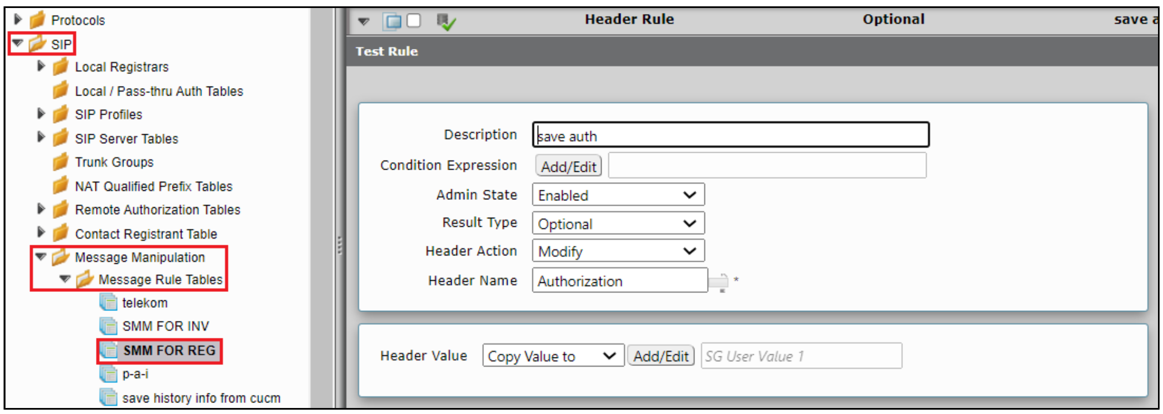
SMM for REG - Add Require:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description
- Add Require with value "mediasec".



SMM for REG - save Authorization:

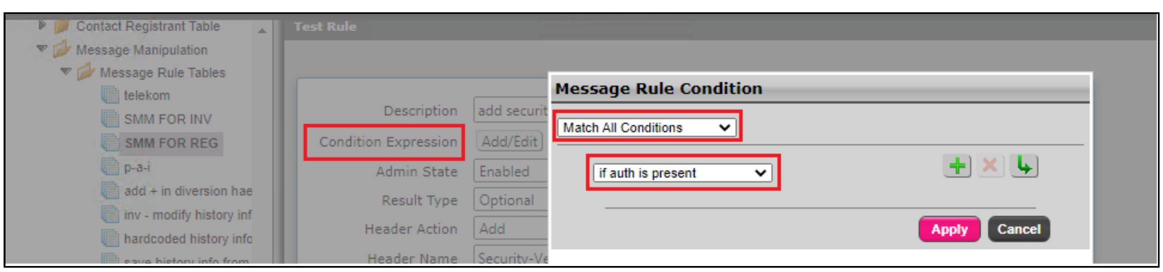
- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description
- Save Authorization under variable "SG User Value 1".



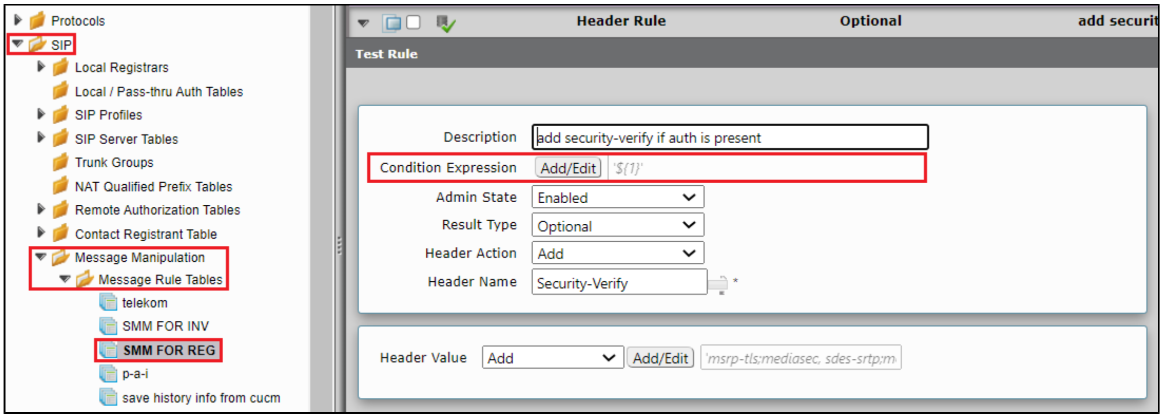
Note
This will be used for condition rule table.

SMM for REG - add Security-Verify:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description
- Add condition and check if Authorization header is present.



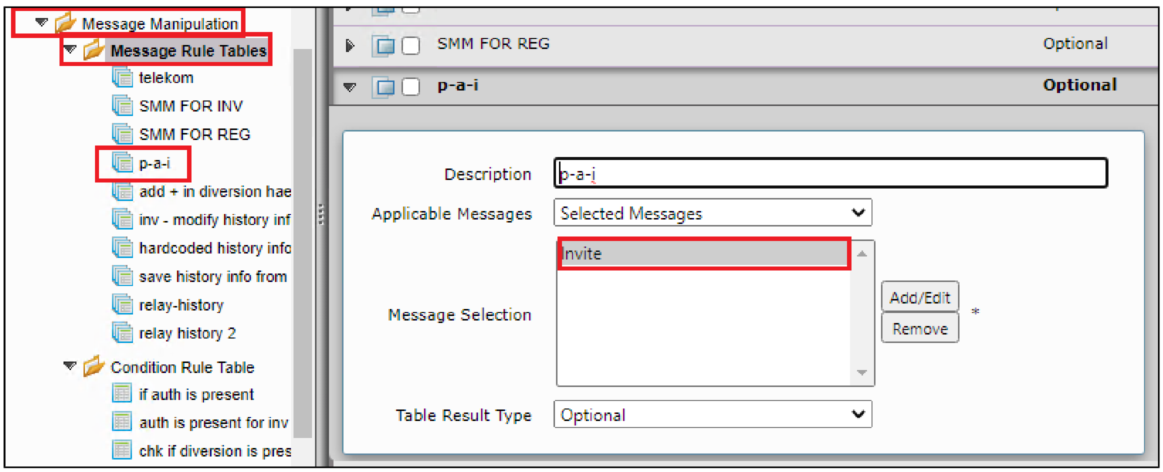
- Add Security-Verify header with value "msrp-tls;mediasec, sdes-srtp;mediasec, dtls-srtp;mediasec".



Create a new rule table for INVITE messages.

Settings > **SIP > Message Manipulation > Message Rule Table.** Click the **Create Message Rule Table(+)** icon.

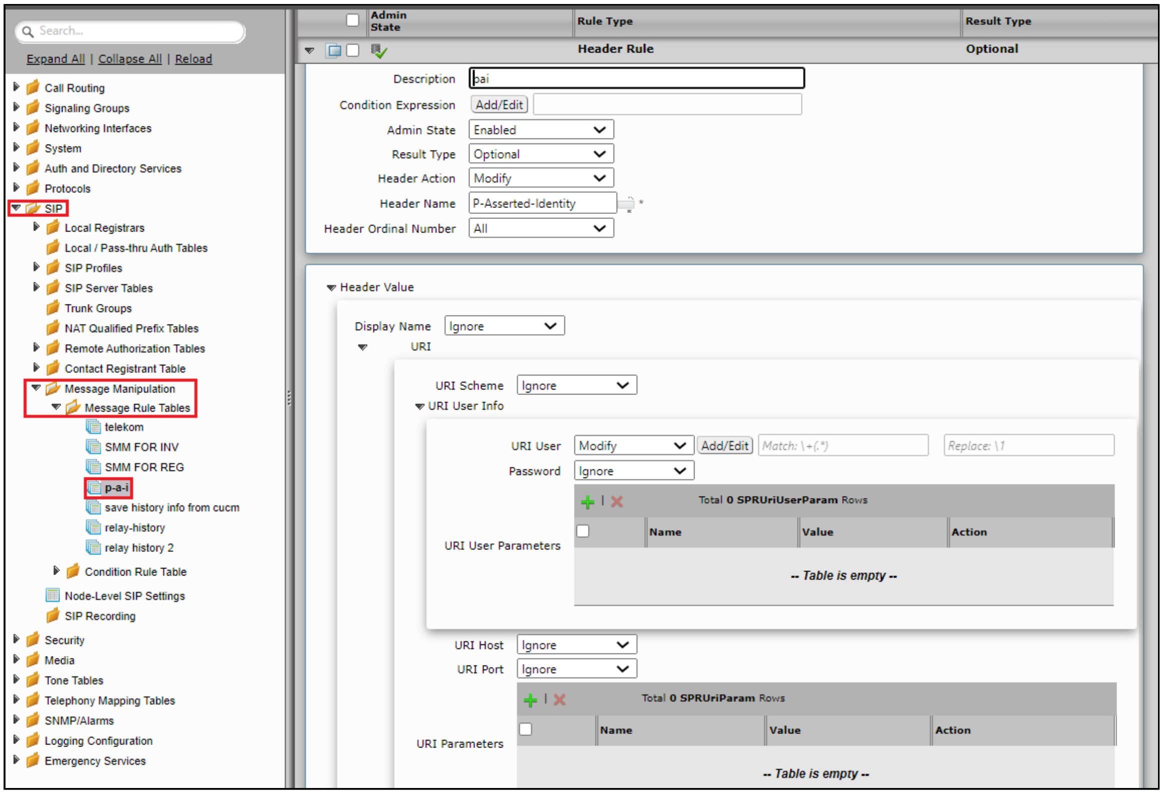
- Provide a description for the Rule Table.
- Apply the SMM only for the Selected messages and choose Invite from the Message Selection list.
- Click **OK**



SMM for PAI - remove + from the number sent out to PBX/PSNT end:

Note
This SMM depends on the number transformation that is chosen in SWe Lite. For example, in our lab setup the phones registered to the PBX has phone number as 4xxxxxxxxxx. Any request from Deutsche Telekom will have number +4xxxxxxxxxx. These changes are handled by transformation tables in SWe Lite. This will update only 'To', 'From' headers, the changes in P-Asserted-Identity header for the number needs to be done using this SMM. Add regex based on the requirements.

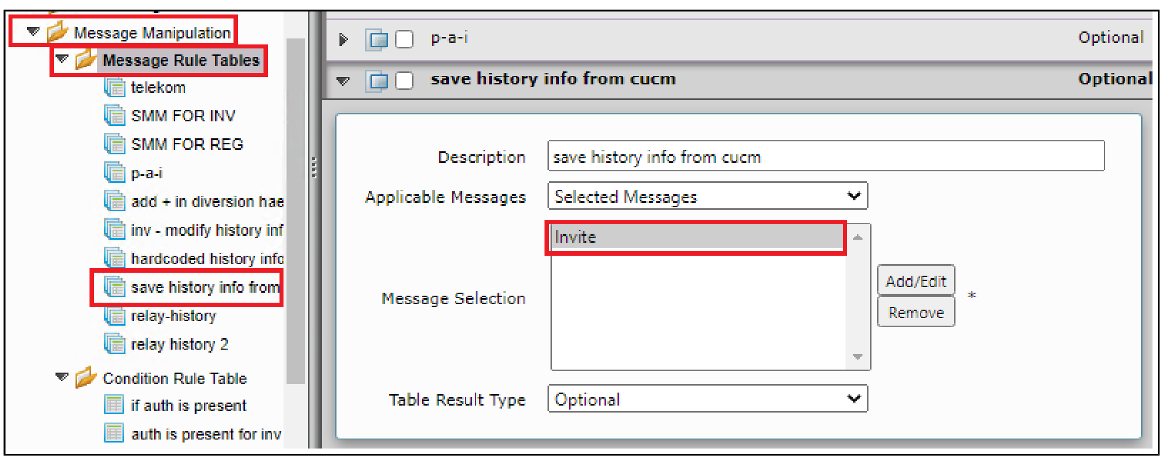
- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Modify P-Asserted-Identity header.
- SMM removes + from the number present in the uri user of P-Asserted-Identity header.



Create a new rule table for INVITE messages.

Settings > **SIP > Message Manipulation > Message Rule Table.** Click the **Create Message Rule Table( )** icon.

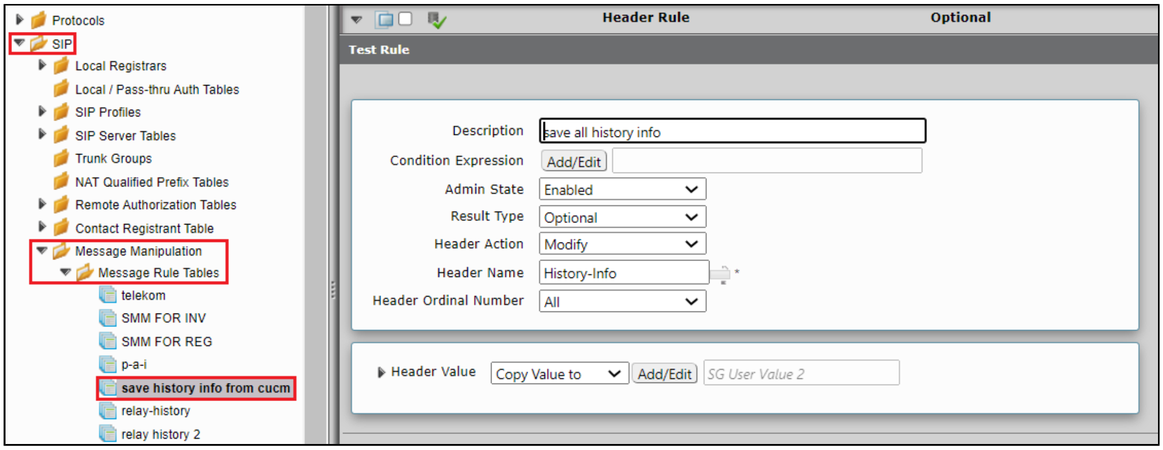
- Provide a description for the Rule Table.
- Apply the SMM only for the Selected messages and choose Invite from the Message Selection list.
- Click **OK**



Note
SWe Lite does not support History Info header. SWe Lite will convert History Info header into Diversion header while relaying it out to Deutsche Telekom. As Deutsche Telekom expects History Info, we are storing the header that we receive from PBX in a local variable. This header will be used later.

Save History info - save History Info in a local variable:

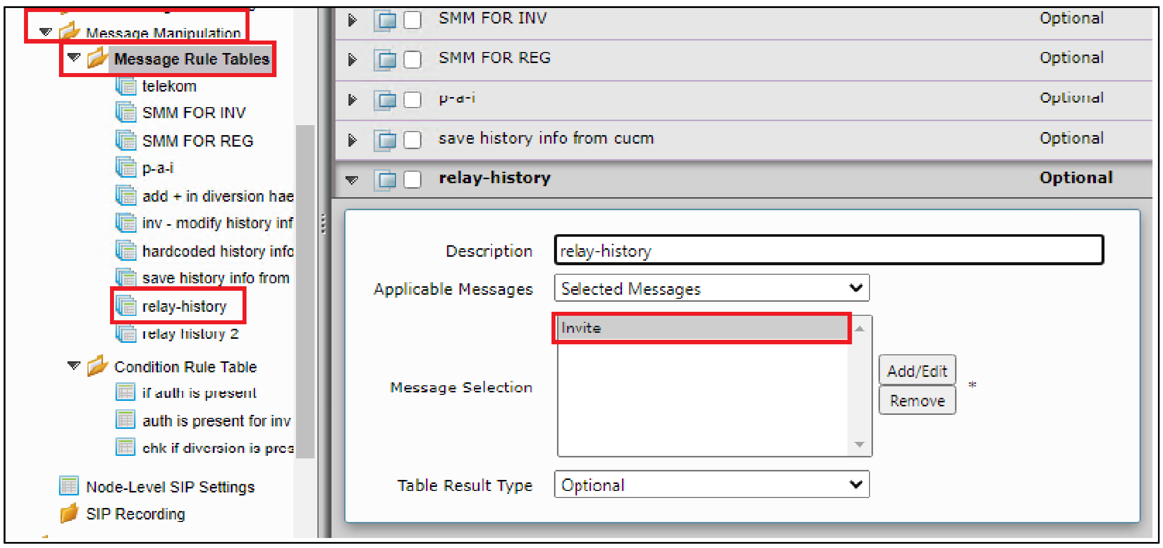
- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description
- Choose header action as 'Modify' and Header name as 'History Info'.
- Choose "Copy Value to" option to store History Info received from PBX in a local variable "SG User Value 2".



Create a new rule table for INVITE messages.

Settings > **SIP > Message Manipulation > Message Rule Table.** Click the **Create Message Rule Table( ) icon.**

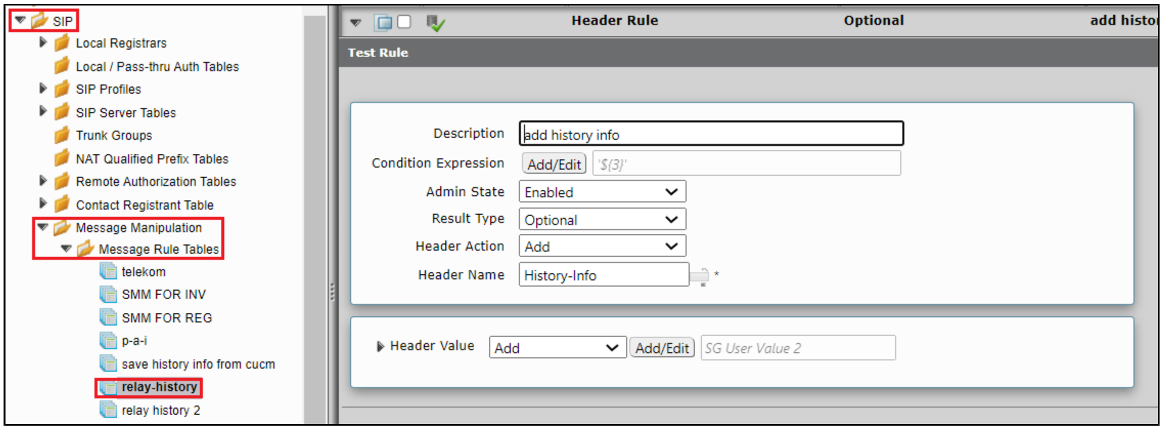
- Provide a description for the Rule Table.
- Apply the SMM only for the Selected messages and choose Invite from the Message Selection list.
- Click **OK**



Note
Add the history-info header that was stored in the previous step to the INVITE sent to Deutsche Telekom.

Save History info - save History Info in a local variable:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Choose header action as 'Add' and header name as 'History-Info'.
- Add value from variable "SG User Value 2".

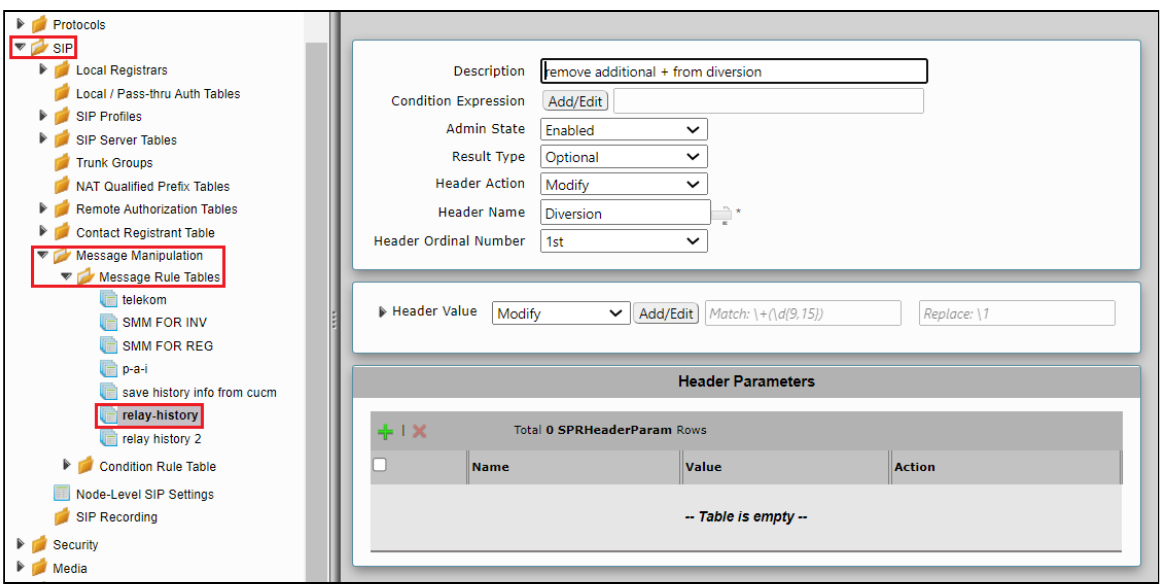


> **Note**
> This SMM depends on the number transformation that is chosen in Swe Lite. For example, in our lab setup the phones registered to the PBX has phone number as 4xxxxxxxxxx. Any request to Deutsche Telekom will have number +4xxxxxxxxxx. To accommodate this in Diversion header we need to add SMM. This SMM will add + before the number.

> **Note**
> To avoid duplicate + on the diversion header during re-Invite we need to remove all the + and then add only one +.

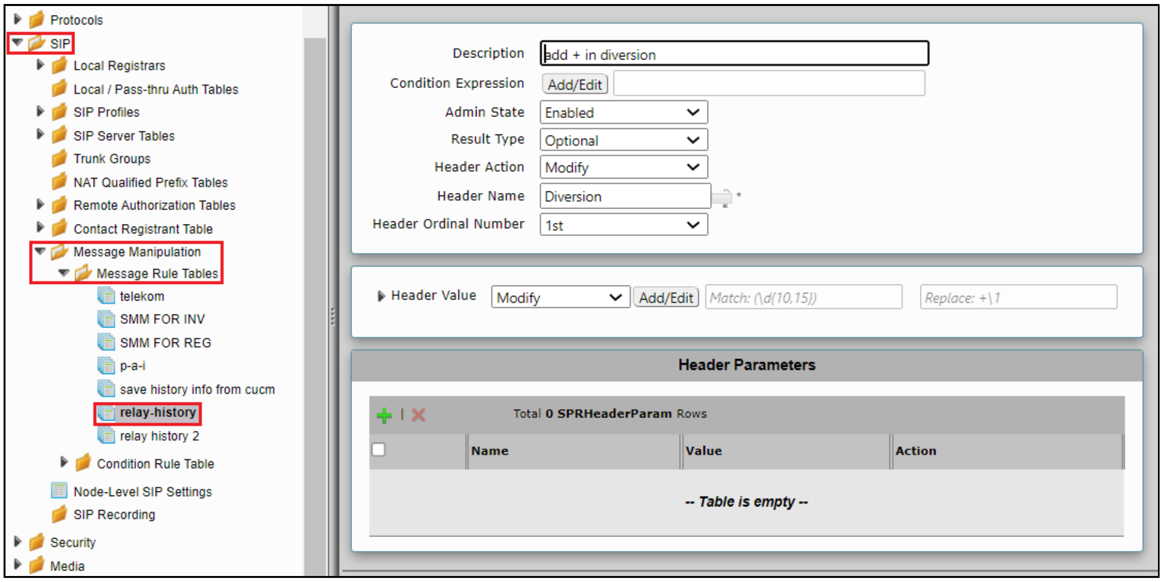
Relay History - remove + from diversion header:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Choose header action as 'Modify' and header name as 'Diversion'.
- Remove + using regex.



Relay History - add + from diversion header:

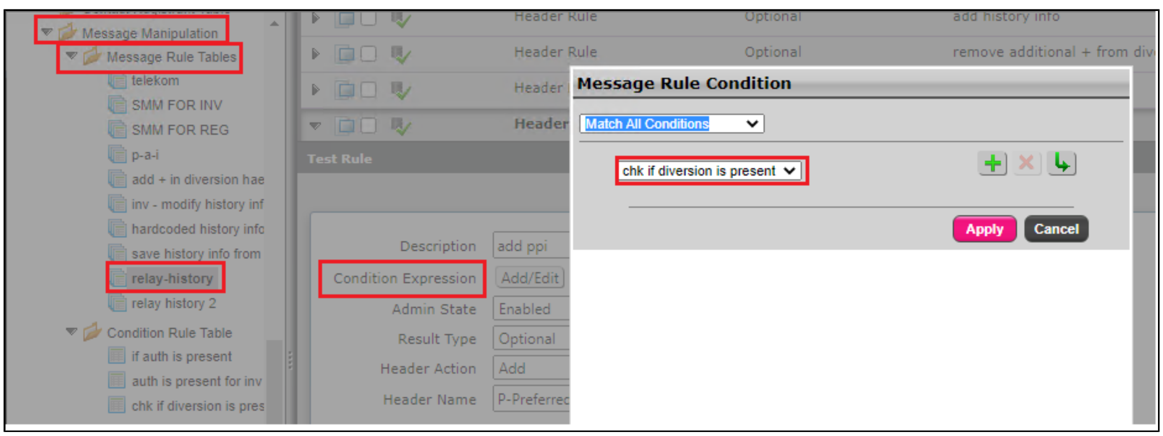
- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Choose header action as 'Modify' and header name as 'Diversion'.
- add + using regex.



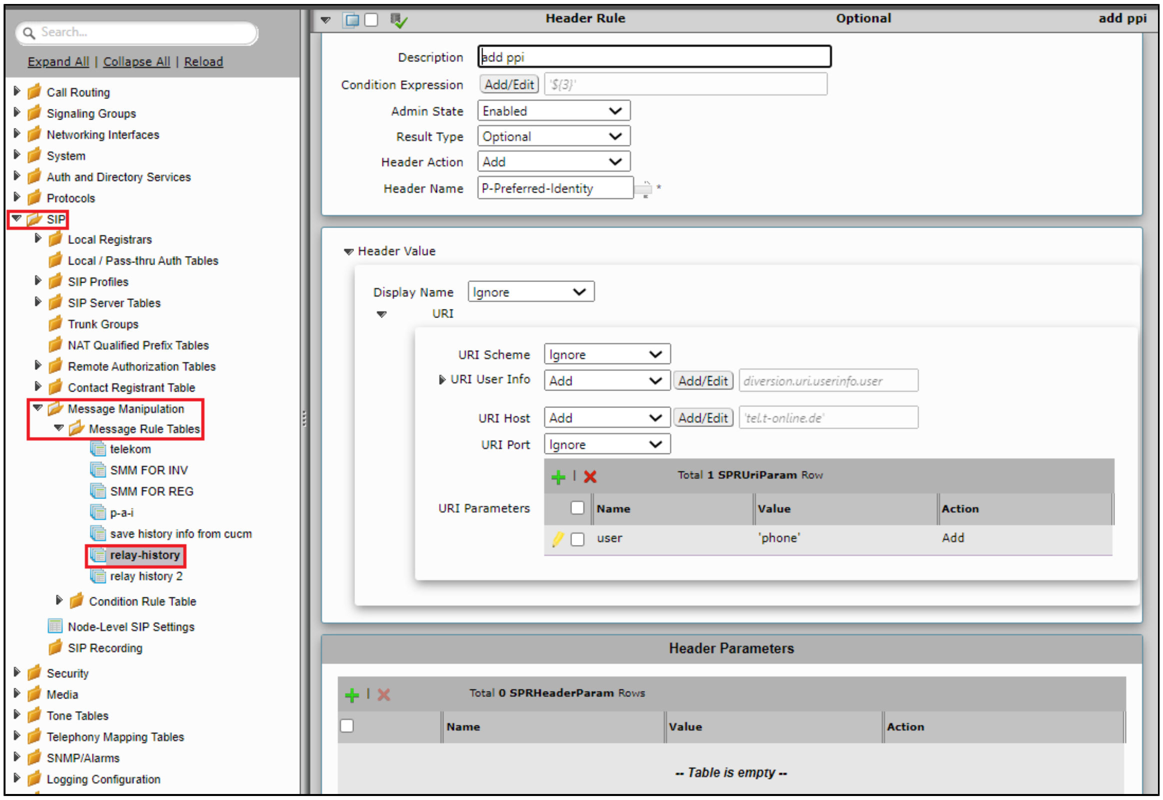
> **Note**
> P-Preferred-Identity header is an important header for Deutsche Telekom during forward cases. The P-Preferred-Identity header should carry the details of the instance that forwarded the call. This is same as that of the diversion header value. Hence P-Preferred-Identity header value will be picked from diversion header.

Relay History - add P-Preferred-Identity:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add condition and check if Diversion header is present (this SMM will be applicable only for forward scenario).



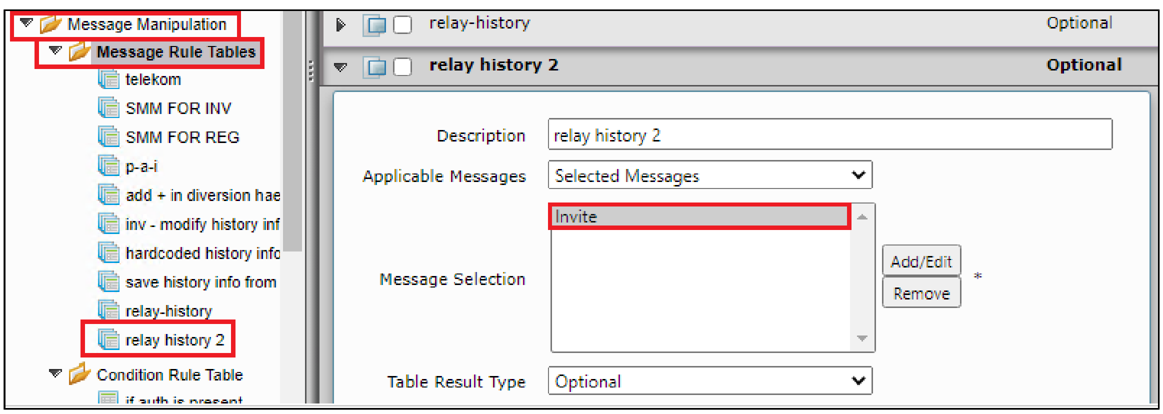
- Choose header action as 'Add' and header name as 'P-Preferred-Identity'.
- Get user info from diversion header, Uri host as Deutsche Telekom domain (tel.t-online.de) and additional parameter 'user'.



Create a new rule table for INVITE messages.

Settings > **SIP > Message Manipulation > Message Rule Table.** Click the **Create Message Rule Table(** **)** icon.

- Provide a description for the Rule Table.
- Apply the SMM only for the Selected messages and choose Invite from the Message Selection list.
- Click **OK**



Note
1st instance of History info relayed to Deutsche Telekom needs to be in the Specific format. Else forwarding wont be successful. The SMM shown below will modify the History info to the following format.

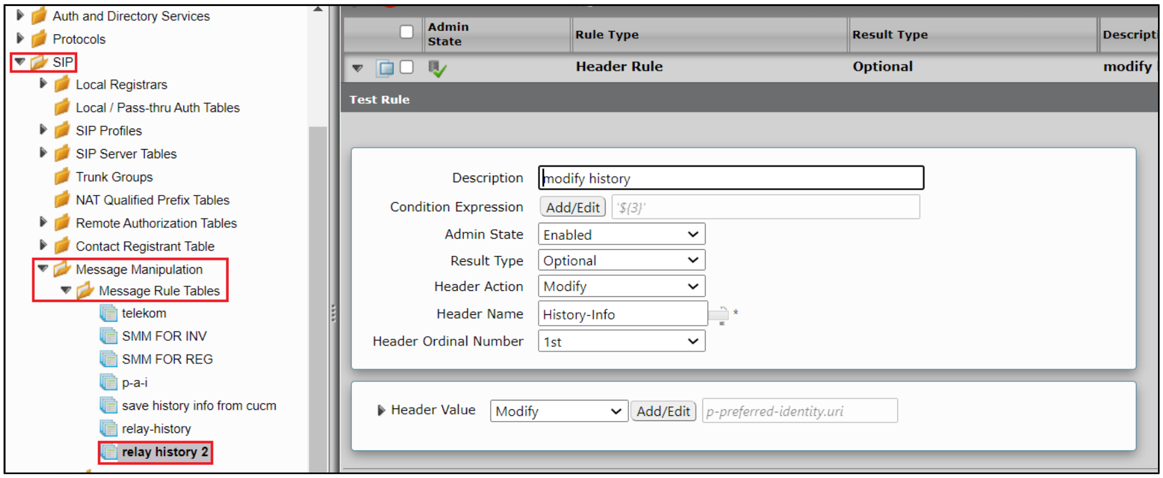
History-Info: <sip:+4XXXXXXXXXX@tel.t-online.de;cause=302>;index=1

Once that is achieved we delete the Diversion header.

Relay History 2 - Modify History-info:

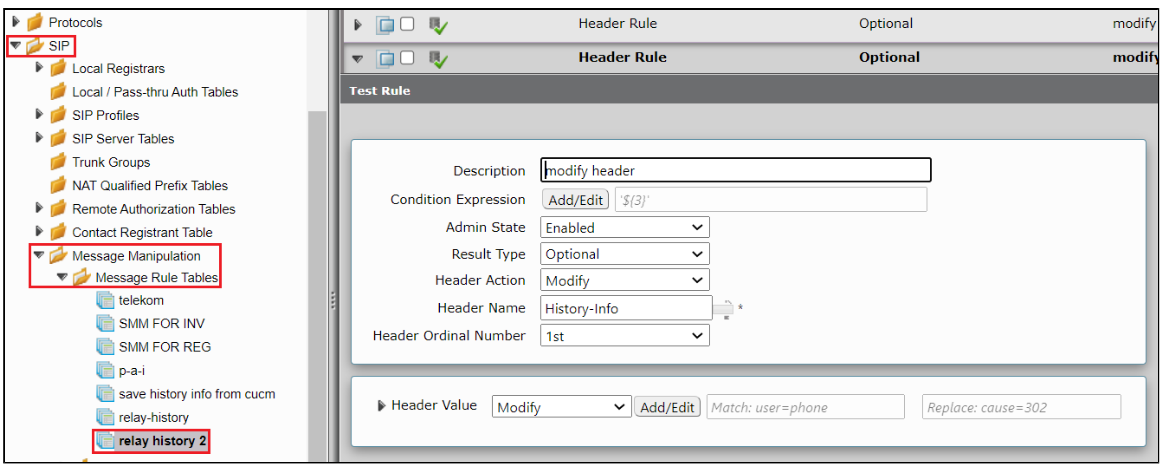
- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add condition and check if Diversion header is present (this SMM will be applicable only for forward scenario).

- Choose header action as 'Modify' ,header name as 'History-Info' and Header Ordinal Number to 1st.
- Get Uri from P-Preferred-Identity.



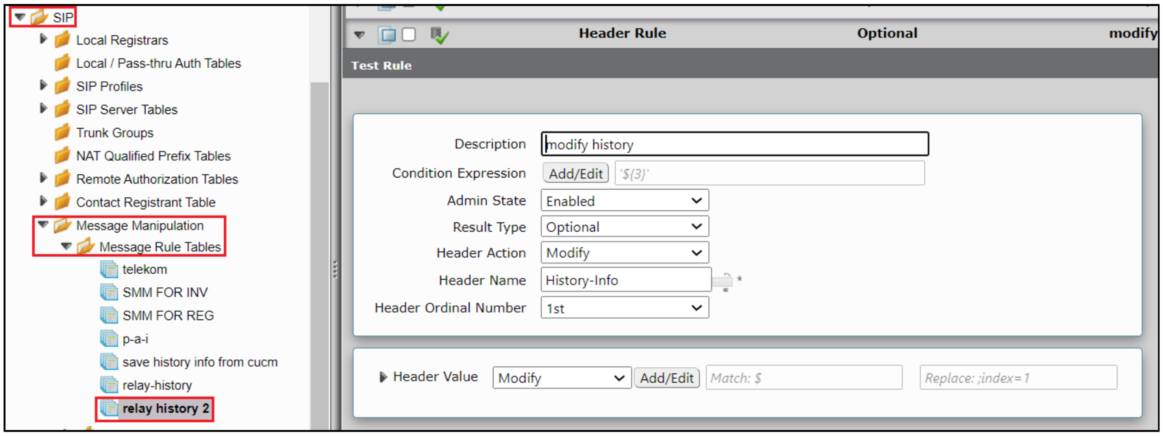
Relay History 2 - Modify History-info:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add condition and check if Diversion header is present (this SMM will be applicable only for forward scenario).
- Choose header action as 'Modify' ,header name as 'History-Info' and Header Ordinal Number to 1st.
- Replace 'user=phone' to 'cause=302'.



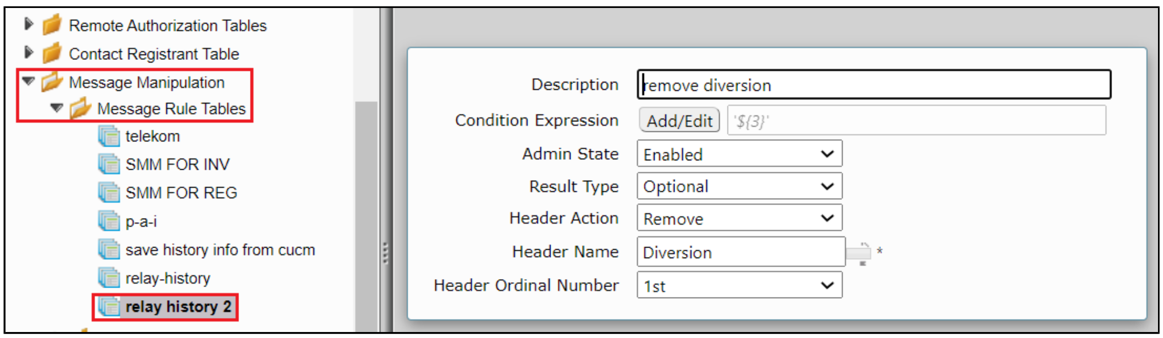
Relay History 2 - Modify History-info:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add condition and check if Diversion header is present (this SMM will be applicable only for forward scenario).
- Choose header action as 'Modify' ,header name as 'History-Info' and Header Ordinal Number to 1st.
- Add 'Index=1' at the end.



Relay History 2 - Modify History-info:

- Click the expand icon next to the Rule Table entry created above.
- From the Create Rule drop-down box, select Header Rule.
- Provide the desired description.
- Add condition and check if Diversion header is present (this SMM will be applicable only for forward scenario).
- Choose header action as 'Remove' ,header name as 'Diversion' and Header Ordinal Number to 1st.



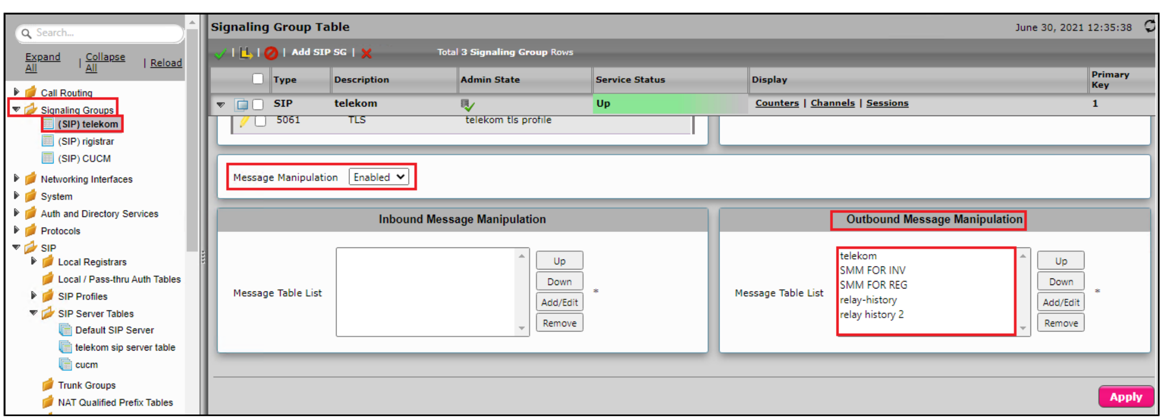
Updating Signaling Group with Message Manipulation

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

Expand the signaling group towards Deutsche Telekom.

Settings > **Signaling Groups.** Click the expand ( ) icon next to the entry.

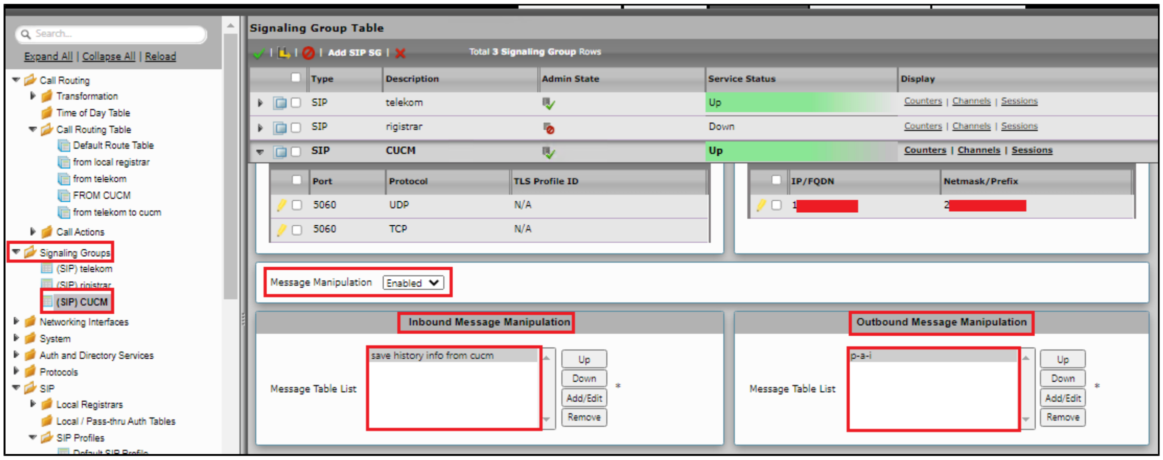
- Enable Message Manipulation.
- Choose "Outbound Message Manipulation".
- Add the following SMM's in the same order.



Expand the signaling group towards IP-PBX Cisco UCM.

Settings > **Signaling Groups.** Click the expand ( ) icon next to the entry.

- Enable Message Manipulation.
- Choose "Outbound Message Manipulation".
- Add the following SMM's in the same order.



Section B: CUCM (IP-PBX) Configuration

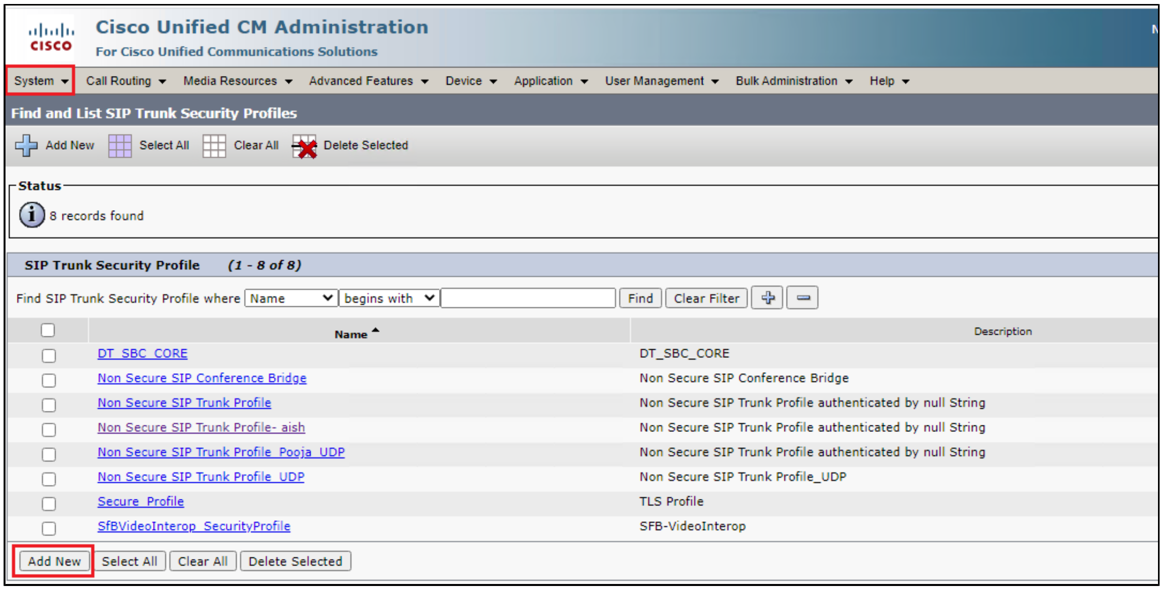
Accessing CUCM (Cisco Unified CM Administration)

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

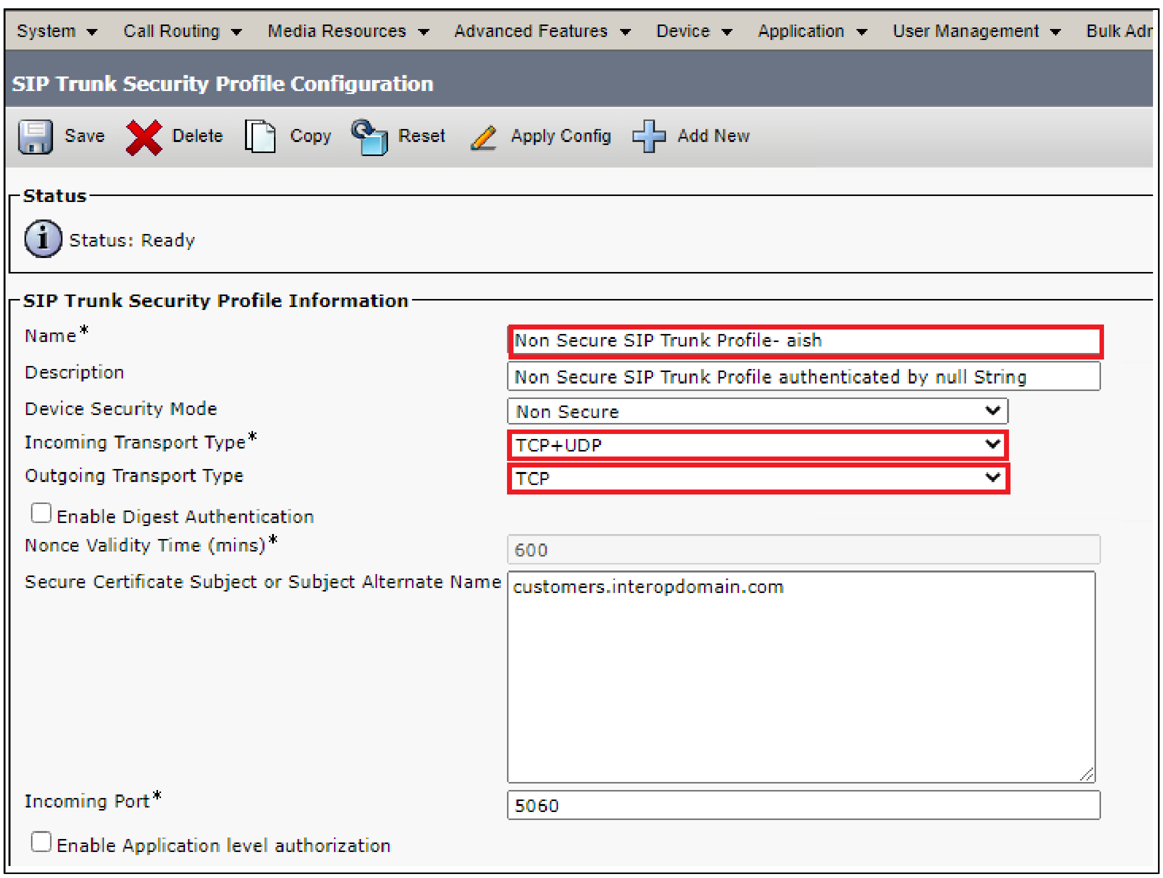
Configure SIP Trunk Security Profile

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

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



- Provide the desired Name and Description.
- Choose **Non Secure** from Device Security Mode.
  - No security features except image authentication apply. A TCP or UDP connection opens to Unified Communications Manager.
- From Incoming Transport Type, select **TCP+UDP**.
  - When Device Security Mode is Non Secure, TCP+UDP specifies the transport type.
- Select Outgoing Transport Type as **TCP**.
- Click **Save**.

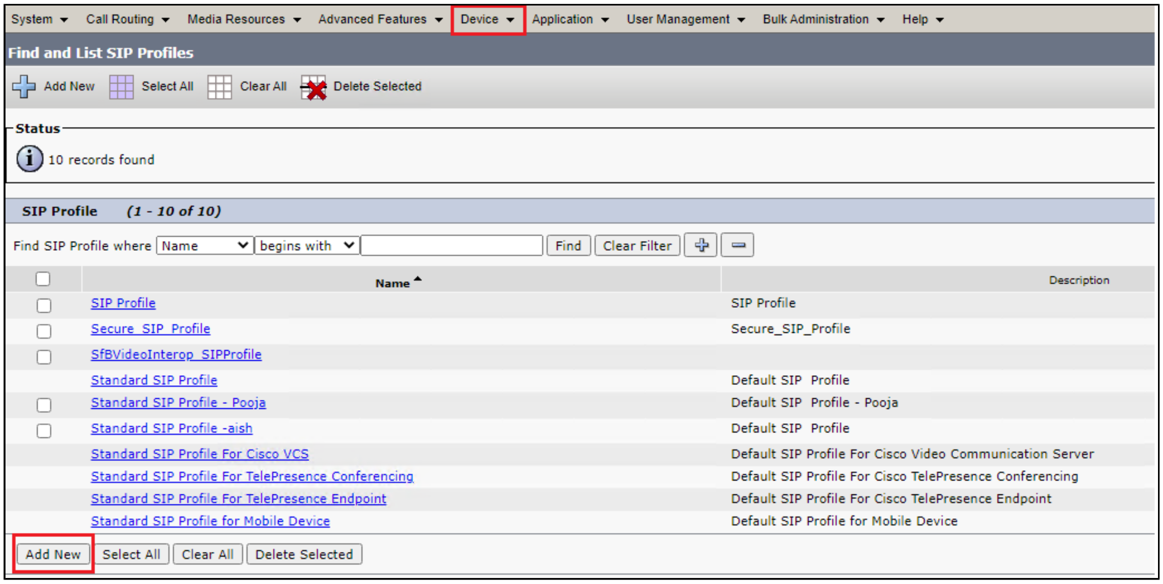


Configure SIP Profiles

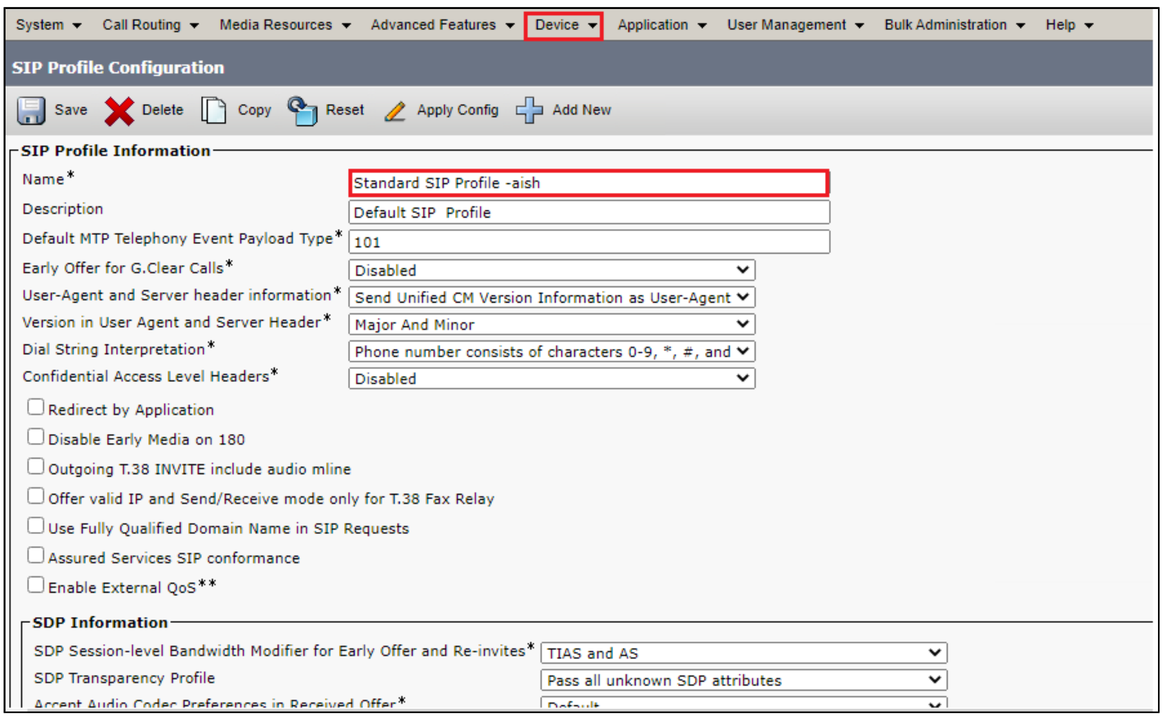
A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that you cannot delete or change.

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

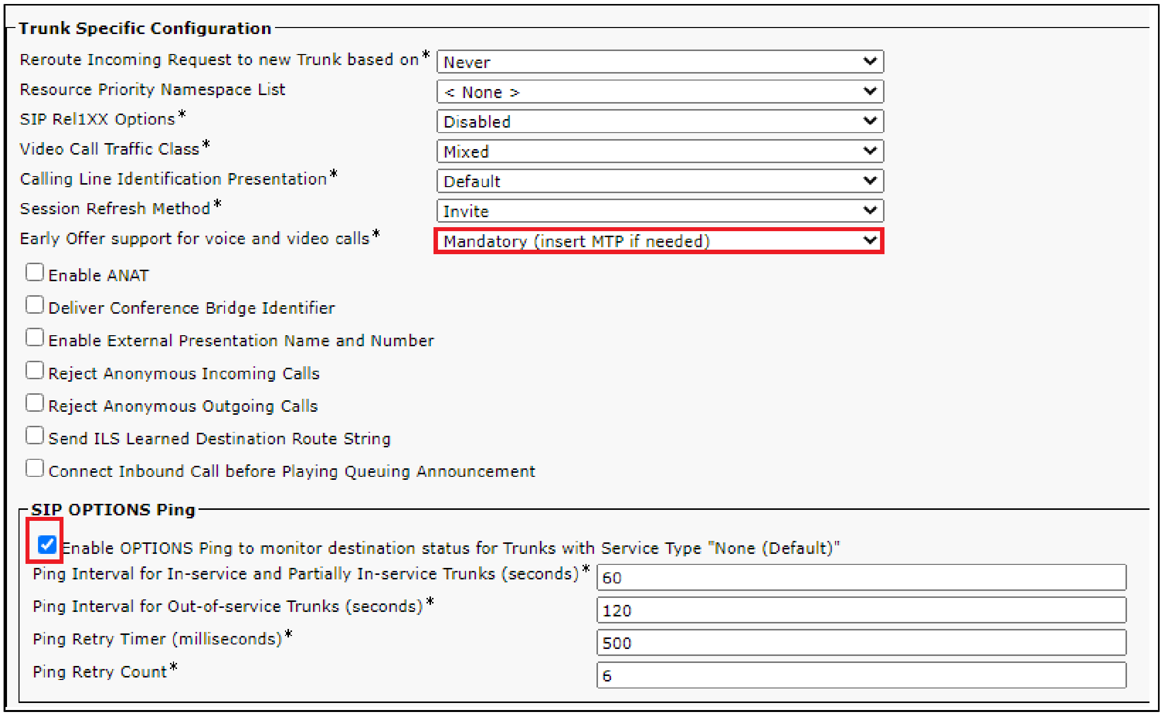
- Click **Add New**.



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



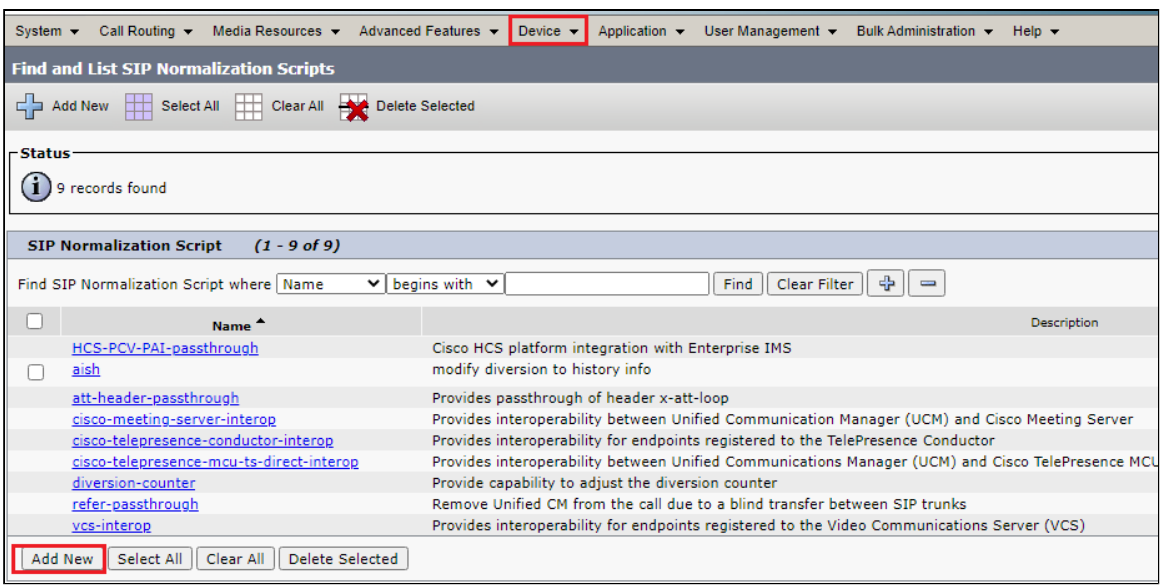
- From Early Offer support for voice and video calls drop-down, choose Mandatory (insert MTP if needed).
- Enable **SIP OPTIONS Ping**.
  - SIP OPTIONS are requests to the configured destination address on the SIP trunk.
- Click **Save**.



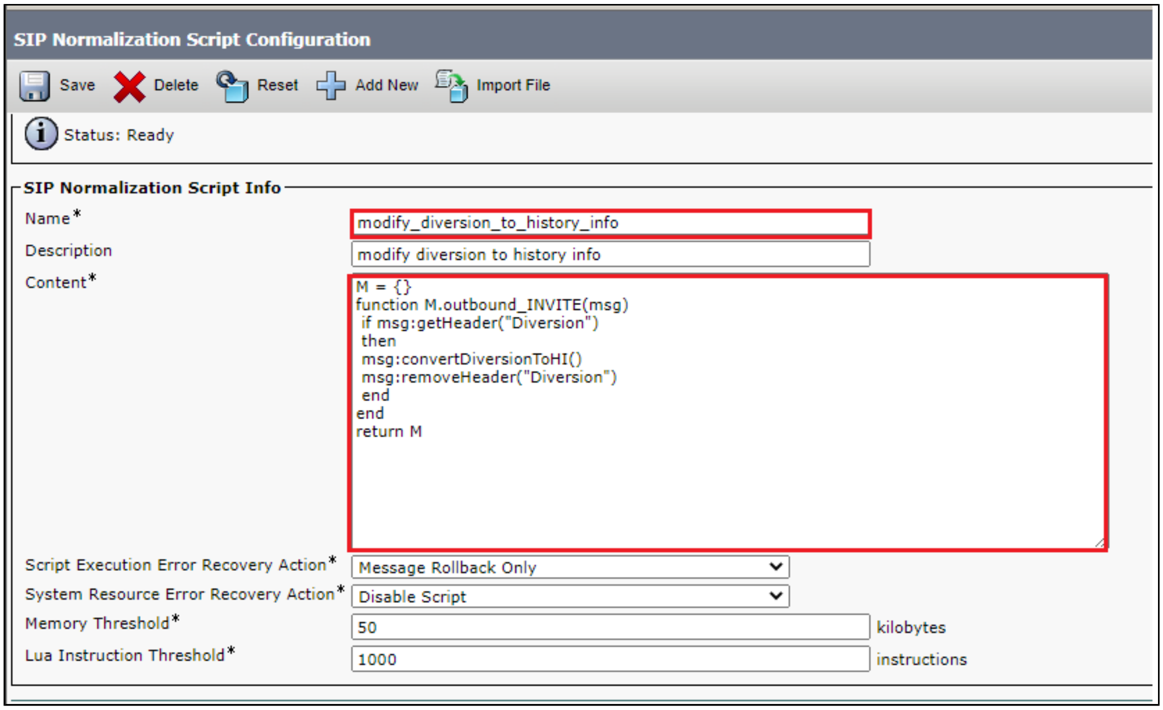
Configure Normalization Script

SIP trunks can connect to a variety of endpoints, including PBXs, gateways, and service providers. Each of these endpoints implements the SIP protocol a bit differently, causing a unique set of interoperability issues. To normalize messages per trunk, Cisco Unified Communications Manager all ows you to add or update scripts to the system and then associate them with one or more SIP trunks.

- From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Normalization Script**
- Click **Add New**.



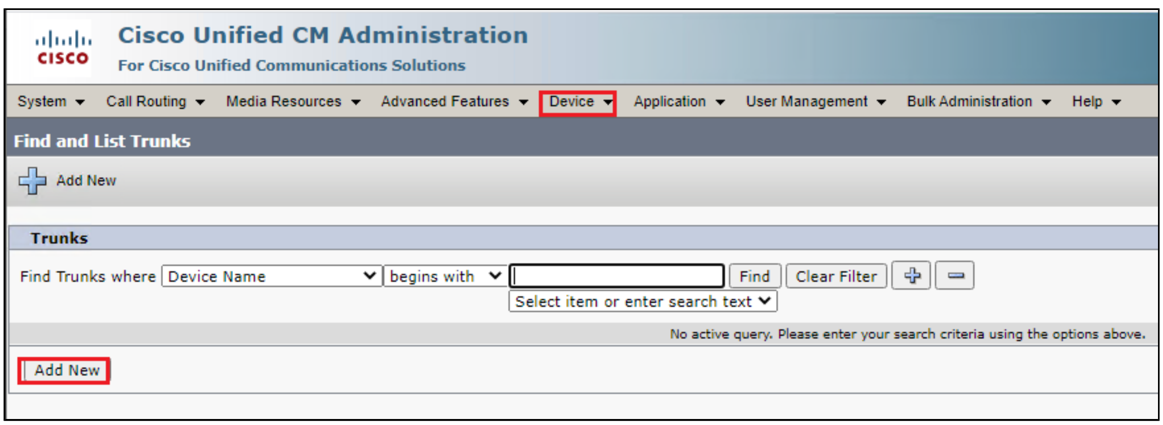
- Provide the desired Name and Description.
- Add the script under content to convert diversion header to history info.



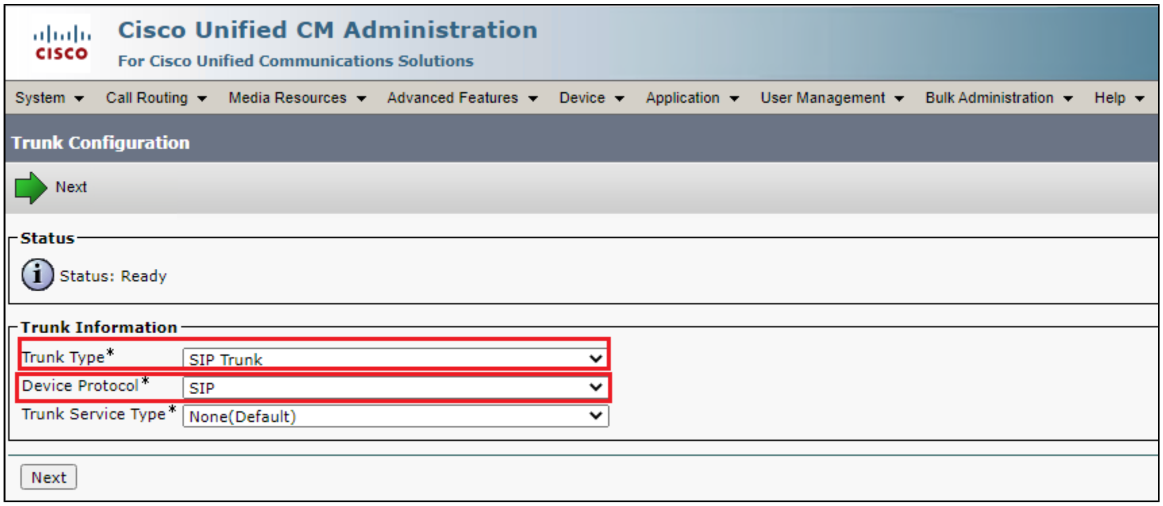
Trunk Configuration

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

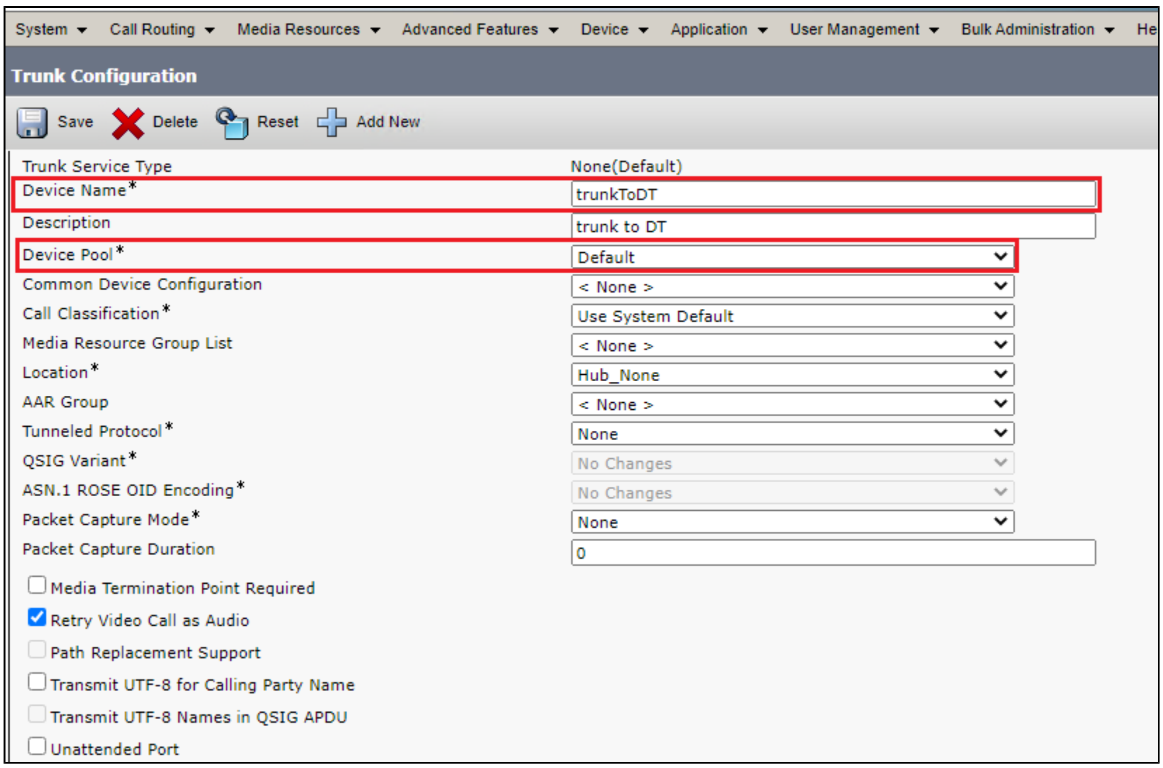
- From Cisco Unified CM Administration, choose **Device > Trunk.**
- Click **Add New**.



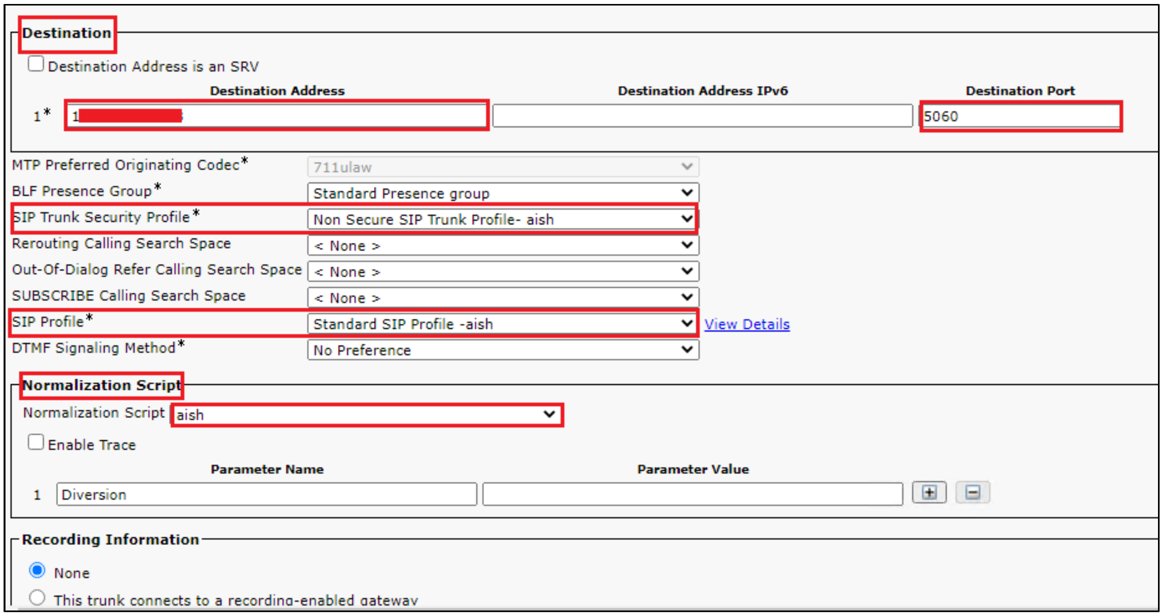
- From the Trunk Type drop-down list, choose **SIP Trunk**.
- Choose **SIP** from Device Protocol drop-down.
- From Trunk Service Type, select the default value (None).
- Click **Next**.



- Enter a unique identifier for the trunk.
- Enter a descriptive name for the trunk.
- Choose the Default Device Pool.



- Provide the destination address.
  - The Destination Address represents the remote SIP peer with which this trunk will communicate.
  - SIP trunks only accept incoming requests from the configured Destination Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk.
- Choose the **SIP Trunk Security Profile** created to apply to the SIP trunk.
- Select the **SIP Profile** created from the list.
- Choose the Normalization Script created previously from the list.
- Click **Save**.



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

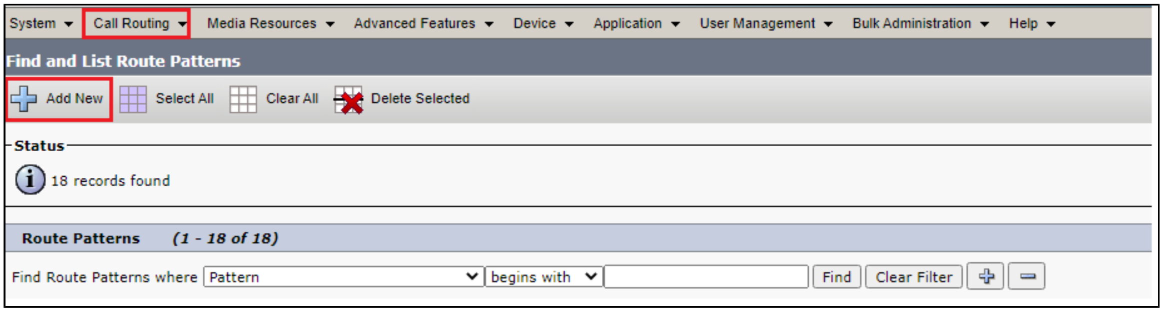
Note
Resetting/restarting a SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager.

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

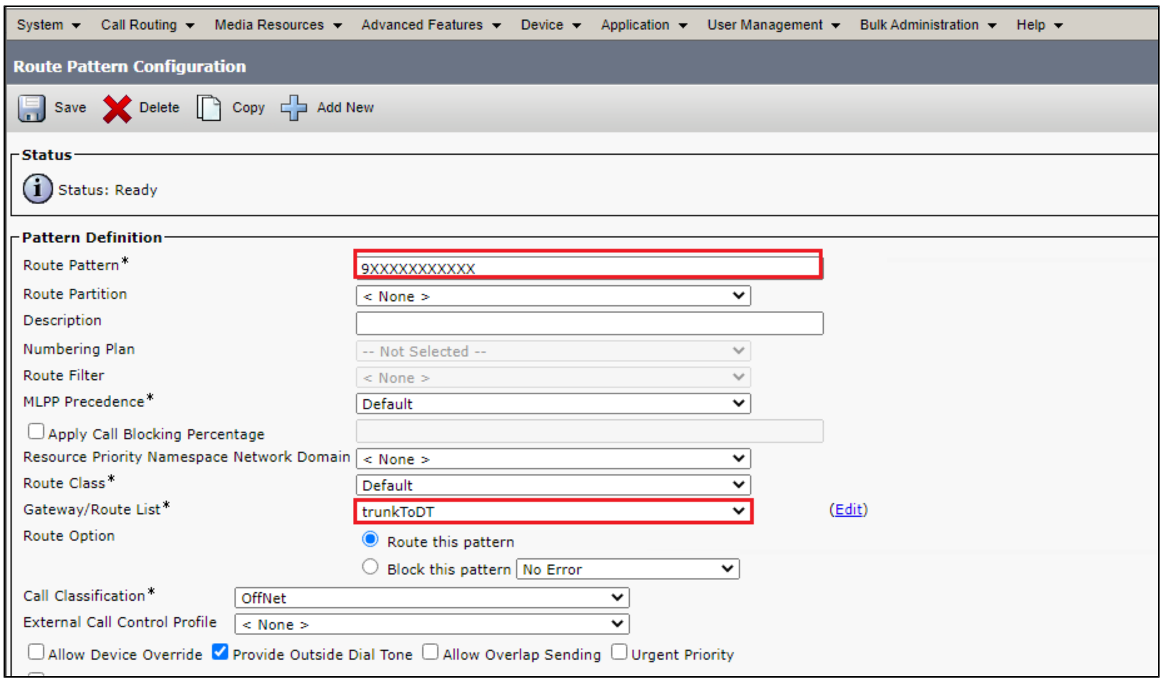
Configure Call Routing

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

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



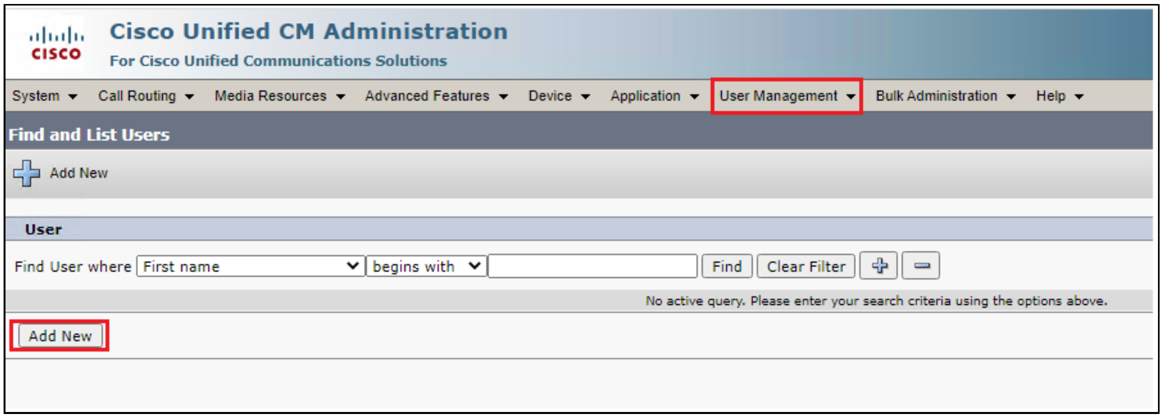
- Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape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



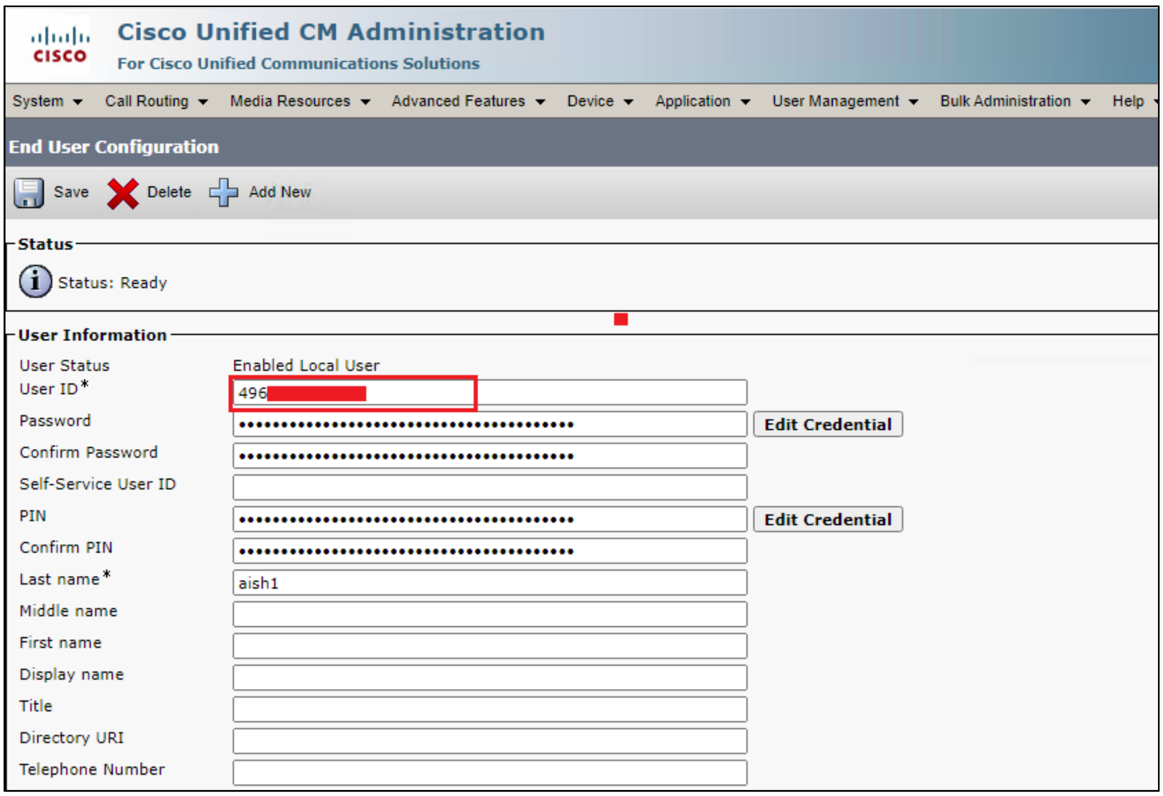
Configure End Users

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

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

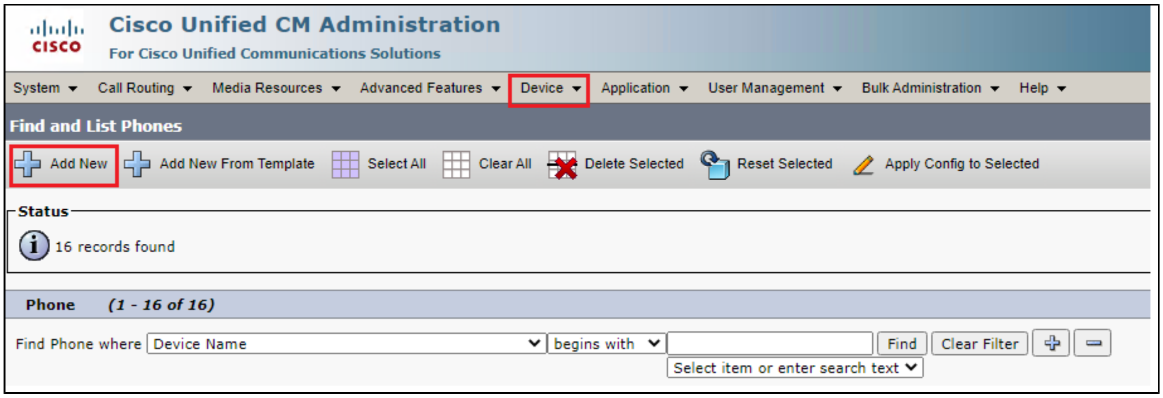


- Enter the unique end user identification name.
- Enter alphanumeric or special characters for the end user password and confirm the same.
- Enter numeric characters for the end user PIN and confirm.
- Enter the end user last name.

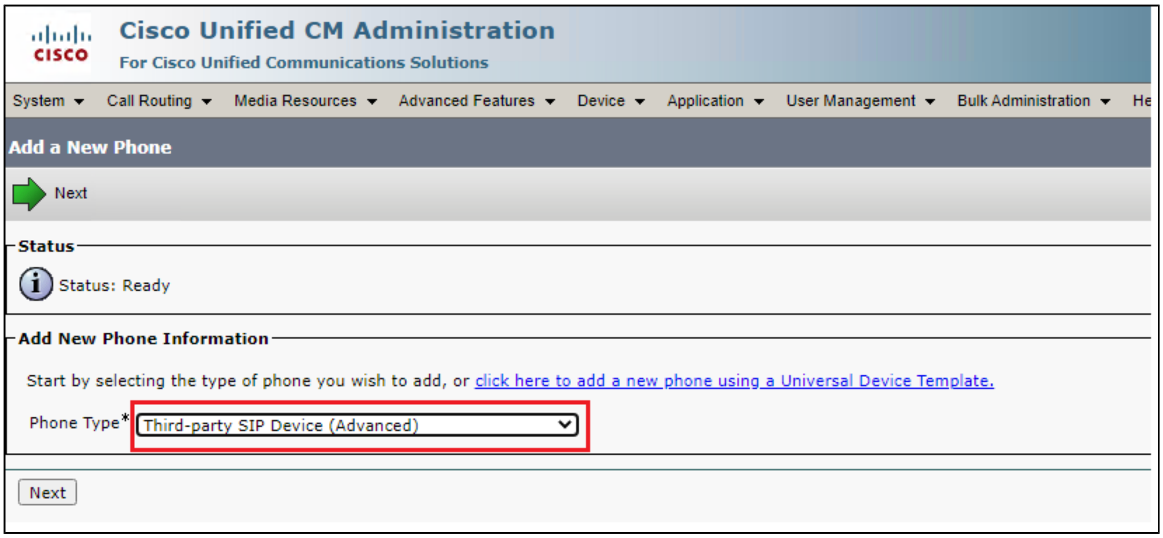


Phone Setup

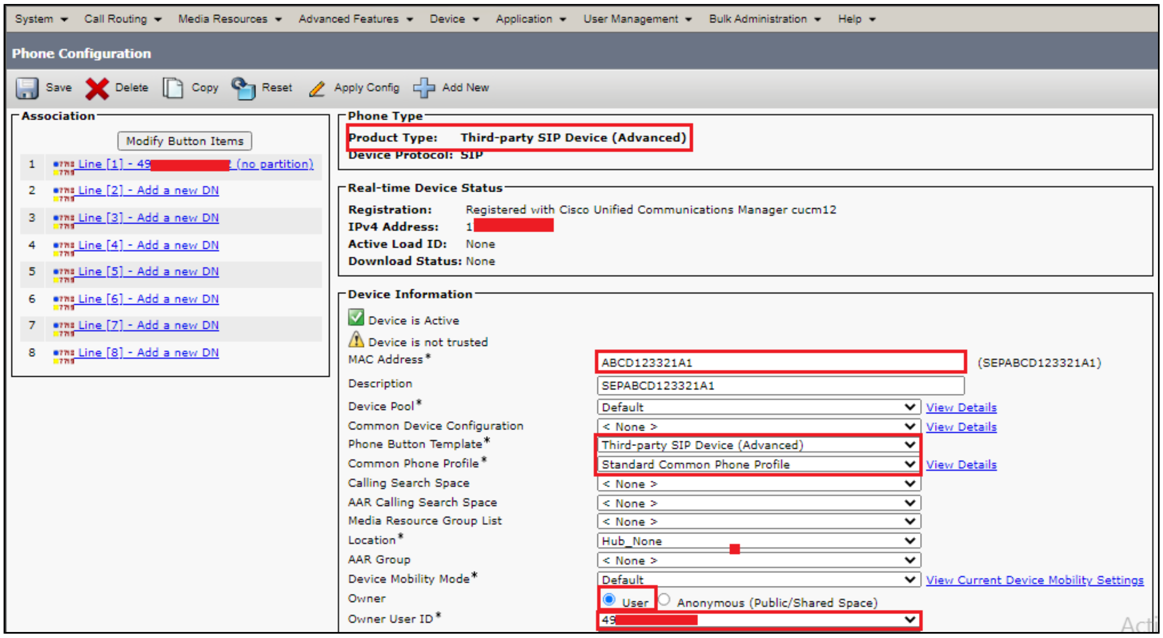
- In Cisco Unified Communications Manager Administration, use the **Device > Phone** menu path to configure phones.
- Click **Add New**.



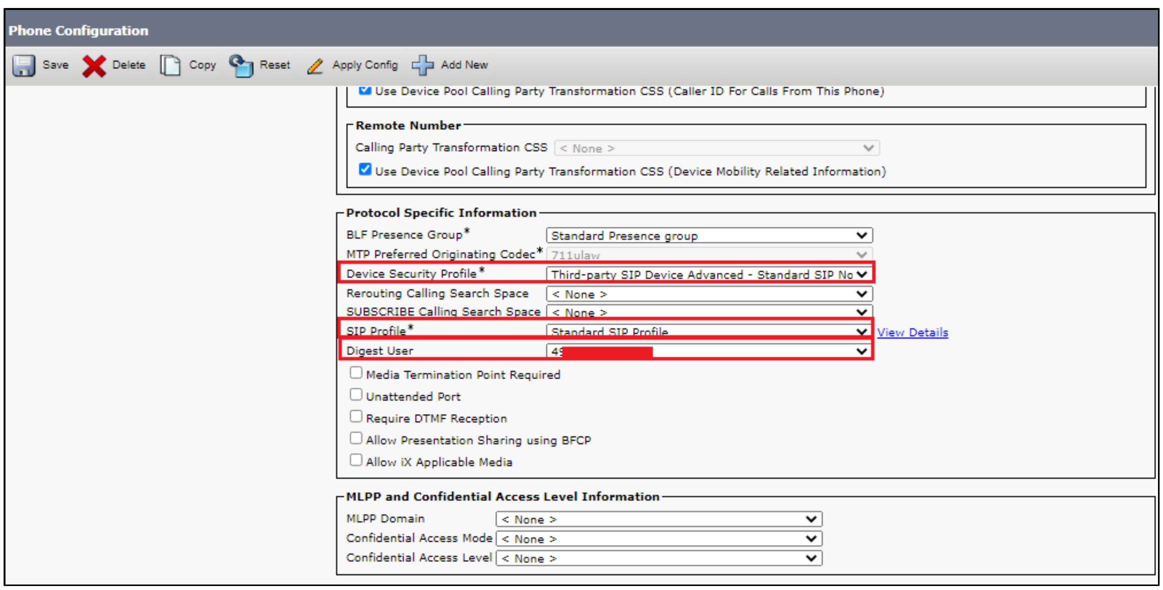
- From the Phone Type drop-down, choose Third-party SIP Device(Advanced) Endpoint.
- Click **Next**.



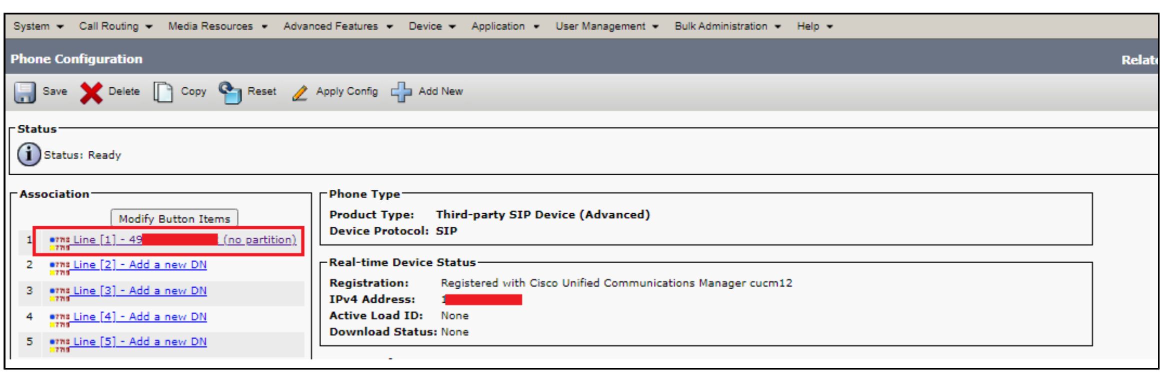
- Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones. Make sure that the value comprises 12 hexadecimal characters.
- Choose **Default** Device pool.
  - A Device pool defines sets of common characteristics for devices, such as region, date/time group, and soft key template.
- Choose **Third-party SIP Device(Advanced)** from the phone button template drop-down.
  - The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
- Choose the user ID of the assigned phone user.



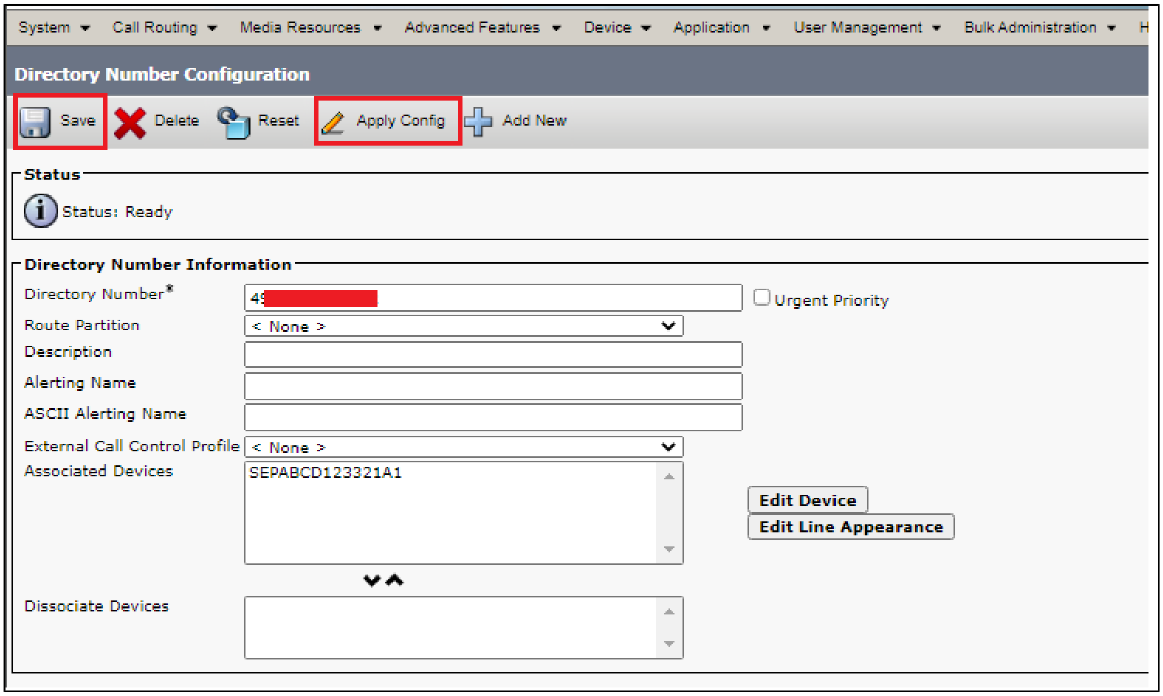
- Choose the security profile Third-party AS-SIP Endpoint - Standard SIP Non-Secure Profile to apply to the device.
- Choose the standard sip profile.
- Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security).
- Click **Save**.



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



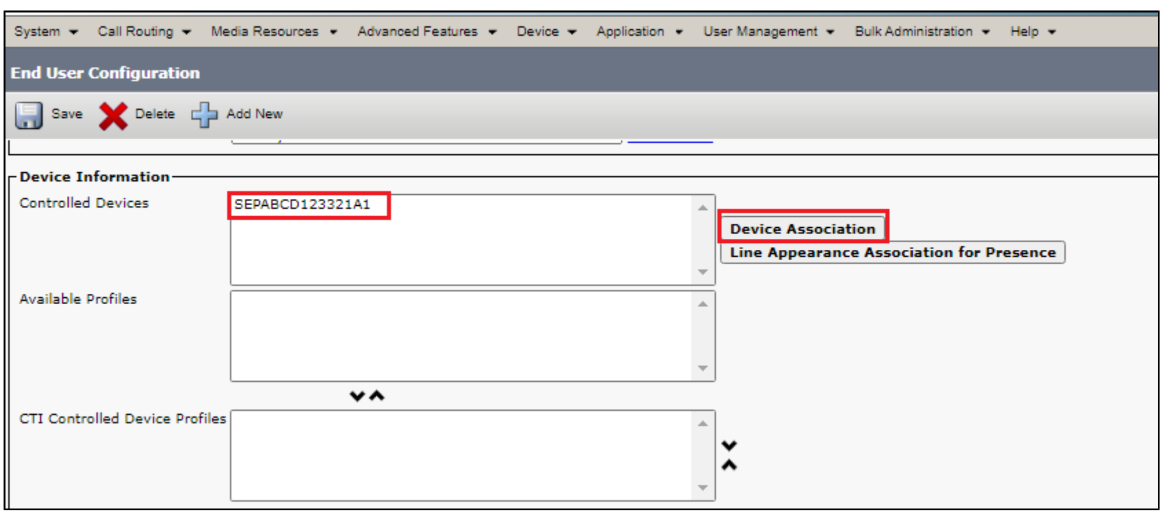
- Add the Directory number.
- Click **Save**.



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

Device Association

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



Supplementary Services and Features Coverage

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

Sr. No.	Supplementary Services/ Features	Coverage
1	SIP Trunk Registration	✓
2	Inbound Call-Mobile PSTN	✓

3	Outbound Call-Mobile PSTN	✓
4	Inbound call-Landline PSTN	✓
5	Outbound call-Landline PSTN	✓
6	Basic Call With Different Codecs	✓
7	Voice Mail	✓
8	Call Forward	✓
9	FAX using G711	✓
10	Call Hold and Resume Outbound	✓
11	Call Hold and Resume Inbound	✓
12	Anonymous Calls Outbound	✓
13	Session Timers	✓
14	FAX - transcoding	✓
15	Call Transfer (Blind)	✓
16	Call Transfer (Attended)	✓
17	Cancel Call	✓
18	Long Duration Calls	✓

Legend

Supported	✓
Not Supported	✗

Note
Observation - Any call to the PSTN mobile display the caller's number with the country code, whereas any call to the PSTN landline excludes the country code.

Caveats

- NA

Support

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

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

References

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

Conclusion

This Interoperability Guide describe the configuration steps required for **Ribbon SBC Edge** to successfully interoperate with **Deutsche Telekom**. All feature and serviceability test cases were completed and passed with the exceptions/observations noted in Test Results

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 is/is not covered.

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