Ribbon SBC Core R9.2 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 Core interworking and compliance against the Deutsche Telekom CompanyFlex SIP Trunking solution. This is a general reference document that requires user input during the configuration of Ribbon SBC Core.

This guide contains the following configuration sections:

- Section A: Ribbon SBC Core Configuration
  - Captures general SBC Core configurations for deploying with the Deutsche Telekom CompanyFlex SIP Trunking solution.
- Section B: CUCM (IP-PBX) Configuration
  - Captures general CUCM configuration required to make a call with the Deutsche Telekom CompanyFlex SIP Trunking.

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 and other hardware as well as services to resellers.

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.

Scope

This document provides configuration best practices for deploying Ribbon's SBC Core 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.

Audience

This document is intended for telecommunications engineers to use when configuring both the Ribbon SBCs and the third-party product. The steps in this document require navigating the third-party product as well as the Ribbon product using graphical user interface (GUI) or command line interface (CLI). An understanding of the basic concepts of TCP/UDP/TLS, IP/Routing, and SIP/RTP/SRTP is necessary to complete the configuration and any necessary troubleshooting.

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

Prerequisites

The following aspects are required before proceeding with the interop:

- Ribbon SBC Core series
- SBC License
- SIP Connect 2.0 Compliant IP-PBX
- 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 details, refer to 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 Core. For this interop testing we have used CUCM 12.5, which is SIP Connect 2.0 Compliant.

Note
SIP Trunk between Deutsche Telekom and Ribbon SBC Core will be over TLS and SRTP.

Product and Device Details

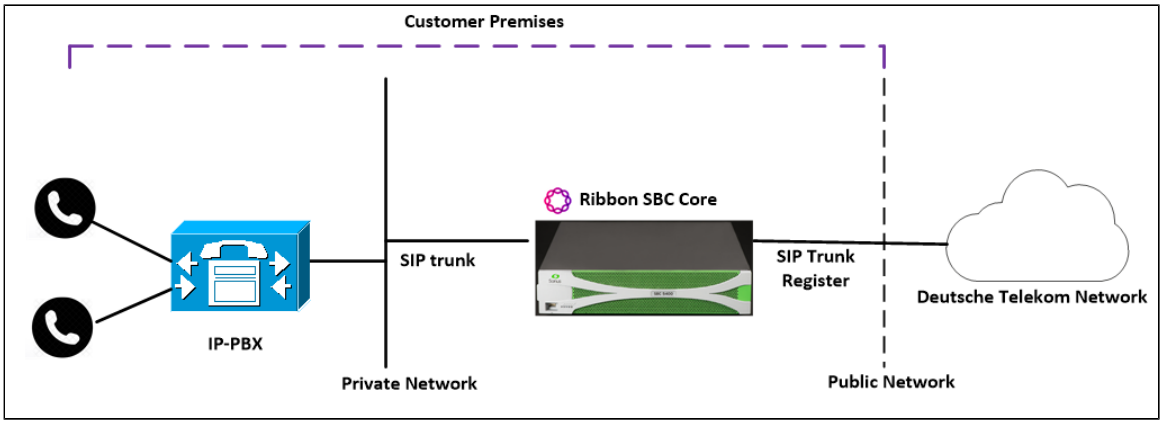
The configuration uses the following equipment and software:

Table 1: Requirements

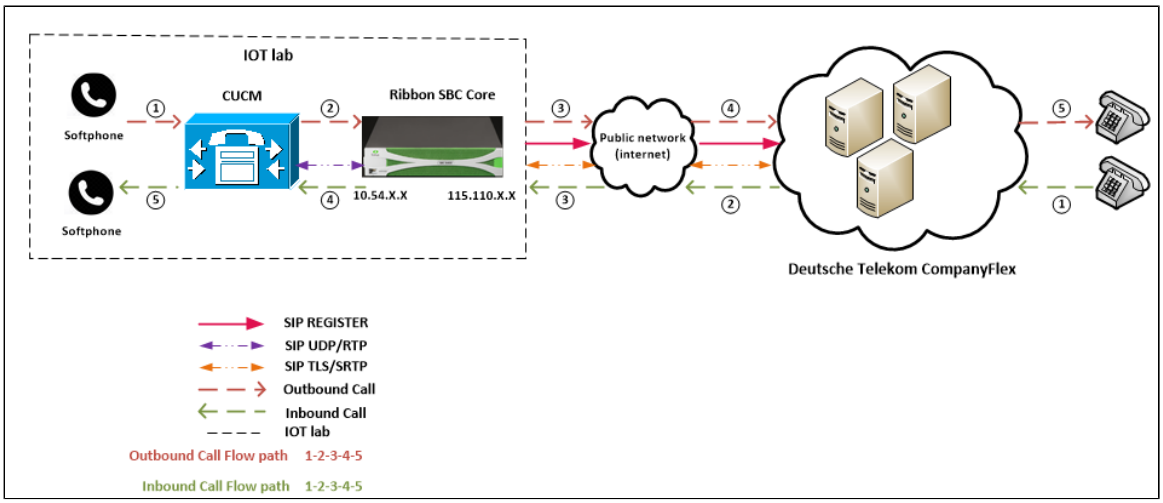
Product	Equipment/Devices	Software/Firmware Version
Ribbon Communications	SBC Core (SWe)	V09.02.00-R002
Cisco	Cisco Unified Communication Manager	12.5
Third Party Phones	Phonerlite	2.93
Deutsche Telekom	Deutsche Telekom "CompanyFlex" SIP trunk	NA

Network Topology

Ribbon SBC Core - Deutsche Telekom CompanyFlex SIP Trunk Deployment Topology



Ribbon SBC Core - Deutsche Telekom CompanyFlex SIP Trunk IOT Lab Topology



Section A: Ribbon SBC Core Configuration

This section provides a sample of the Ribbon SBC Core configuration used during interop testing. The following commands and configurations are only for reference. Other configurations are also possible based on the customer's requirements.

IP-PBX Leg Configuration

Create profiles with a specific set of characteristics corresponding to IP-PBX leg. This includes configuration of the following entities on IP-PBX leg:

1. Codec Entry
2. Packet Service Profile
3. IP Signaling Profile
4. IP Interface Group
5. Zone
6. SIP Signaling Port
7. IP Peer
8. SIP Trunk Group
9. Routing Label
10. Call Routing

1. Codec Entry

Codec entry allows you to specify the codec used for the call. Create the codec entry for G711Alaw codec with packet size 20 and rfc2833 method for dtmf.

```
set profiles media codecEntry G711A codec g711
set profiles media codecEntry G711A law ALaw
set profiles media codecEntry G711A packetSize 20
set profiles media codecEntry G711A dtmf relay rfc2833
set profiles media codecEntry G711A fax toneTreatment faxRelayOrFallbackToG711
commit
```

2. Packet Service Profile (PSP)

Create a Packet Service Profile (PSP) towards the IP-PBX leg. The PSP is attached to sipTrunkGroup created later in this section.

```
set profiles media packetServiceProfile IP_PBX_PSP codec codecEntry1 G711A
set profiles media packetServiceProfile IP_PBX_PSP rtcpOptions rtcp enable
commit
```

3. IP Signaling Profile (IPSP)

Create an IP Signaling Profile with appropriate signaling flags towards IP-PBX.

```
set profiles signaling ipSignalingProfile IP_PBX_IPSP
set profiles signaling ipSignalingProfile IP_PBX_IPSP commonIpAttributes flags usePsxRouteforRegisteredInvite
enable
set profiles signaling ipSignalingProfile IP_PBX_IPSP commonIpAttributes flags noPortNumber5060 enable
set profiles signaling ipSignalingProfile IP_PBX_IPSP egressIpAttributes sipHeadersAndParameters callForwarding
dataMapping none
commit
set profiles signaling ipSignalingProfile IP_PBX_IPSP egressIpAttributes sipHeadersAndParameters callForwarding
diversionHistoryInfoInterworking enable
commit
set profiles signaling ipSignalingProfile IP_PBX_IPSP egressIpAttributes sipHeadersAndParameters callForwarding
historyInformation includeHistoryInformation enable
commit
```

4. IP Interface Group

Create an IP interface group.

> **Note**
> Replace "x.x.x.x" with the SBC's packet interface (pkt) IP address towards INTERNAL (example pkt0 IP), and "Y" with its prefix length. Provide ceName used during an SBC deployment.
>
> Here, the ceName is "SBXUK9".

```
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0_V4 ceName SBXUK9 portName pkt0
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0_V4 ipAddress x.x.x.x prefix Y
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0_V4 mode inService state enabled
commit
```

5. Zone

Create Zone towards IP-PBX and specify the id of the zone.

> **Note**
> This Zone groups the set of objects used for the communication towards IP-PBX.

```
set addressContext default zone INTERNAL id 2
commit
```

6. SIP Signaling Port

Set the SIP Signaling port, which is a logical address used to send and receive SIP call signaling packets and is permanently bound to a specific zone.

> **Note**
> Replace "x.x.x.x" with SIP Signaling Port IP of SBC towards IP-PBX.

```
set addressContext default zone INTERNAL sipSigPort 3 ipInterfaceGroupName LIF1
set addressContext default zone INTERNAL sipSigPort 3 ipAddressV4 x.x.x.x
set addressContext default zone INTERNAL sipSigPort 3 portNumber 5060
set addressContext default zone INTERNAL sipSigPort 3 transportProtocolsAllowed sip-udp,sip-tcp
set addressContext default zone INTERNAL sipSigPort 3 mode inService
set addressContext default zone INTERNAL sipSigPort 3 state enabled
commit
```

7. Surrogate IP Peer

Create a Surrogate IP Peer with the IP address of the IP-PBX and assign it to the INTERNAL Zone.

Create a Surrogate Registration Profile as follows and attach it to the surrogate IP peer.

aorUserName should be the user to be registered to Deutsche Telekom. Provide the Username and Password required to register to the Deutsche Telekom CompanyFlex trunk in surrogateRegistrationProfile aorAuthUserName and aorAuthPassword.

```
set profiles services surrogateRegistrationProfile TEST aorUserName +49199296000000100540 aorAuthUserName
+49199296000000100540
set profiles services surrogateRegistrationProfile TEST aorUserName +49199296000000100540 aorAuthPassword xxxxxxx
set profiles services surrogateRegistrationProfile TEST aorUserName +49199296000000100540 aorState enabled
set profiles services surrogateRegistrationProfile TEST aorUserName +49199296000000100540 aorSendCredentials
challengeForAnyMessageAndInDialogRequests
set profiles services surrogateRegistrationProfile TEST aorUserName +49199296000000100540 userStartRange
4961717040872
set profiles services surrogateRegistrationProfile TEST aorUserName +49199296000000100540 userEndRange
4961717040875
commit
```

Create Surrogate IP Peer as follows:

```
set addressContext default zone INTERNAL ipPeer IP_PBX ipAddress x.x.x.x
set addressContext default zone INTERNAL ipPeer IP_PBX ipPort 5060
set addressContext default zone INTERNAL ipPeer IP_PBX policy description ""
set addressContext default zone INTERNAL ipPeer IP_PBX policy sip fqdn ""
set addressContext default zone INTERNAL ipPeer IP_PBX policy sip fqdnPort 0
set addressContext default zone INTERNAL ipPeer IP_PBX surrogateRegistration state enabled
set addressContext default zone INTERNAL ipPeer IP_PBX surrogateRegistration surrRegProfile TEST
set addressContext default zone INTERNAL ipPeer IP_PBX authentication intChallengeResponse disabled
set addressContext default zone INTERNAL ipPeer IP_PBX authentication incInternalCredentials disabled
commit

set addressContext default zone INTERNAL ipPeer IP_PBX surrogateRegistration state enabled
commit
```

Note
Replace "x.x.x.x" with the IP address of the IP-PBX.

8. IP Signaling Peer Group

Create an IP Signaling Peer Group as follows and attach it to the IP-PBX SIP trunk Group.

Note
Replace "x.x.x.x" with the IP address of IP-PBX.

```
set profiles ipSignalingPeerGroup PEER_GROUP_SURR ipSignalingPeerGroupData 0 serviceStatus inService
set profiles ipSignalingPeerGroup PEER_GROUP_SURR ipSignalingPeerGroupData 0 ipAddress x.x.x.x
set profiles ipSignalingPeerGroup PEER_GROUP_SURR ipSignalingPeerGroupData 0 ipPort 5060
commit
```

9. SIP Trunk Group

Create a SIP Trunk Group towards the INTERNAL and assign corresponding profiles like PSP and IPSP, created in earlier steps.

Warning
You must configure Trunk Group names using capital letters.

```
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG media mediaIpInterfaceGroupName LIF1
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG mode inService state enabled
commit
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG policy digitParameterHandling numberingPlan
GERMANY_NUM_PLAN
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG policy ipSignalingPeerGroup PEER_GROUP_SURR
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG policy media packetServiceProfile IP_PBX_PSP
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG policy signaling ipSignalingProfile IP_PBX_IPSP
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG signaling registration requireRegistration
supported-group
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG signaling registration expires 3600
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG signaling authentication intChallengeResponse
disabled
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG signaling authentication incInternalCredentials
disabled
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG signaling acceptHistoryInfo enabled
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG signaling validateAor disabled
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG services dnsSupportType a-srv-naptr
set addressContext default zone INTERNAL sipTrunkGroup IP_PBX_TG ingressIpPrefix 0.0.0.0 0
commit
```

10. Routing Label

Create a Routing Label with a single Routing Label Route to bind the IP-PBX Trunk Group with the IP Peer.

```
set global callRouting routingLabel IP_PBX_RL routingLabelRoute 1 trunkGroup IP_PBX_TG
set global callRouting routingLabel IP_PBX_RL routingLabelRoute 1 ipPeer IP_PBX
set global callRouting routingLabel IP_PBX_RL routingLabelRoute 1 inService inService
commit
```

11. Call Routing

This entry is used to route all the calls coming from the DT trunk towards the IP-PBX.

> **Note**
> Provide ceName used during an SBC deployment. "SBXUK9" is the ceName.

```
set global callRouting route trunkGroup TELEKOM_TG SBXUK9 standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel INTERNAL_RL
commit
```

DT CompanyFlex Leg Configuration

Create profiles with a specific set of characteristics corresponding to the Deutsche Telekom CompanyFlex trunk. This includes configuration of the following entities on the External(Telekom) leg:

1. Ribbon SBC Configuration for TLS/SRTP
2. Codec Entry
3. Packet Service Profile
4. IP Signaling Profile
5. IP Interface Group
6. Zone
7. SIP Signaling Port
8. IP Peer
9. SIP Message Manipulation
10. SIP Trunk Group
11. Routing Label
12. Call Routing

1. Ribbon SBC Configuration for TLS/SRTP

This section covers the TLS/SRTP configuration between the SBC Core and DT CompanyFlex SIP Trunk.

Prerequisites:

- For TLS to work on the public side of the network, a trusted CA (Certificate Authority) is needed. In this scenario, GoDaddy is used as a Trusted CA.
- Download the Deutsche Telekom Global Root Certificate from https://corporate-pki.telekom.de/en/GlobalRootClass2.html

> **Note**
> The Deutsche Telekom CompanyFlex SIP Trunk prefers to use TLS/SRTP over the internet, so there is a TLS/SRTP connection between the SBC Core and the Deutsche Telekom CompanyFlex SIP Trunk.

Generate a CSR with OpenSSL

```
# To create a Certificate Signing Request (CSR) and key file for a Subject Alternative Name (SAN) certificate with
multiple subject alternate names, complete the following procedure:

Create an OpenSSL configuration file (text file) on the local computer by editing the fields to the company
requirements.

Note 1: In the example used in this article the configuration file is req.conf.

Note 2: req_extensions will put the subject alternative names in a CSR, whereas x509_extensions would be used when
creating an actual certificate file.

[req]
        distinguished_name = req_distinguished_name
        req_extensions = v3_req
        prompt = no
        [req_distinguished_name]
        C = US
        ST = VA
        L = SomeCity
        O = MyCompany
        OU = MyDivision
        CN = www.company.com
        [v3_req]
        keyUsage = keyEncipherment, dataEncipherment
        extendedKeyUsage = serverAuth
        subjectAltName = @alt_names
        [alt_names]
        DNS.1 = www.company.com
        DNS.2 = company.com
        DNS.3 = www.company.net
        DNS.4 = company.net

Make sure there are no whitespaces at the end of the lines.

#Run the following commands to create the Certificate Signing Request (CSR) and a new Key file:
openssl req -new -out company_san.csr -newkey rsa:2048 -nodes -sha256 -keyout company_san.key.temp -config req.conf

#Run the following command to verify the Certificate Signing Request:
openssl req -text -noout -verify -in company_san.csr

# After receiving the CSR with above information, provide it to CA (Certificate Authority). You will then receive
the proper CA signed certificate in .crt format that is convertable into other formats using openssl.

# By default, you should receive two or more certificates from CA (depending upon your CA). One is the SBC
certificate, and other is CA's root and intermediate certificate.

# Upload the certificates to the SBC at /opt/sonus/external and convert them into SBC-readable format, i.e. SBC
certificate is in .pem or .p12 format and root certificate is in .cer or .der.

#Converting .crt to .pem USING OPENSSL for SBC certificate.
openssl x509 -in sbc_cert.crt -out sbc_cert.der -outform DER
openssl x509 -in sbc_cert.der -inform DER -out sbc_cert.pem -outform PEM

#After generating sbc_cert.pem file, convert it to .p12 format using below command and the location of the
certificate key.
openssl pkcs12 -export -out sbc1_cert.p12 -in sbc_cert.pem -inkey /opt/sonus/company_san.key.temp

#CONVERTING CRT to CER USING OPENSSL for CA's root and intermediate certificate.
openssl x509 -in root_cert.crt -out root_cert.cer -outform DER

After converting all these certificates upload them on SBC at /opt/sonus/external location.
```

Generate Required Certificates

```
#Import Public CA Root Certificate into database.
set system security pki certificate CA_ROOT_CERT type remote fileName root_cert.cer state enabled

#Import Public CA Certified SBC Server Certificate into database.
set system security pki certificate SBC_CERT filename sbc1_cert.p12 passPhrase <Password defined during CSR
generation> state enabled type local
```

TLS Profile

A TLS Profile is required for the TLS handshake between the SBC Core and DT CompanyFlex SIP Trunk. This profile defines cipher suites supported by the SBC Core. Create the TLS profile as mentioned below:

```
set profiles security tlsProfile TLS_PROF clientCertName SBC_CERT serverCertName SBC_CERT cipherSuite1
tls_rsa_with_aes_128_gcm_sha256 cipherSuite2 rsa-with-aes-128-cbc-sha-256 cipherSuite3 rsa-with-aes-256-cbc-sha-
256 authClient true allowedRoles clientandserver acceptableCertValidationErrors invalidPurpose
set profiles security tlsProfile TLS_PROF v1_1 disable
set profiles security tlsProfile TLS_PROF v1_0 disable
set profiles security tlsProfile TLS_PROF v1_2 enable
commit
```

Note
Attach the TLS Profile to the SIP Signaling Port of the Telekom Leg later in this section.

Crypto Suite Profile

Crypto Suite Profile contains the payload type for SRTP calls.

```
set profiles security cryptoSuiteProfile CRYPT_PROF entry 1 cryptoSuite AES-CM-128-HMAC-SHA1-80
commit
```

2. Codec Entry

Codec entry allows you to specify the codec used for the call. Create the codec entry for G711 Alaw codec with packet size 20 and rfc2833 method for dtmf.

```
set profiles media codecEntry G711A codec g711
set profiles media codecEntry G711A law ALaw
set profiles media codecEntry G711A packetSize 20
set profiles media codecEntry G711A dtmf relay rfc2833
commit
```

3. Packet Service Profile (PSP)

Create a Packet Service Profile (PSP) for the Telekom leg. The PSP is attached to the sipTrunkGroup that is created later in this section.

```
set profiles media packetServiceProfile TELEKOM codec codecEntry1 G711A
set profiles media packetServiceProfile TELEKOM rtcpOptions rtcp enable
set profiles media packetServiceProfile TELEKOM flags ssrcRandomize enable
set profiles media packetServiceProfile TELEKOM flags ssrcRandomizeForSrtp enable
set profiles media packetServiceProfile TELEKOM secureRtpRtcp cryptoSuiteProfile CRYPT_PROF
set profiles media packetServiceProfile TELEKOM secureRtpRtcp flags enableSrtp enable
commit
```

4. IP Signaling Profile (IPSP)

Create an IP Signaling Profile with appropriate signaling flags towards Telekom.

Note
The SBC Core to Deutsche Telekom CompanyFlex trunk transport type is TLS.

```
set profiles signaling ipSignalingProfile TELEKOM_IPSP commonIpAttributes flags noPortNumber5060 enable
set profiles signaling ipSignalingProfile TELEKOM_IPSP commonIpAttributes flags
includeTransportTypeInContactHeader enable
set profiles signaling ipSignalingProfile TELEKOM_IPSP commonIpAttributes flags insertPeerAddressAsTopRouteHeader
enable
set profiles signaling ipSignalingProfile IP_PBX_IPSP egressIpAttributes sipHeadersAndParameters callForwarding
dataMapping none
commit
set profiles signaling ipSignalingProfile TELEKOM_IPSP egressIpAttributes sipHeadersAndParameters callForwarding
diversionHistoryInfoInterworking enable
set profiles signaling ipSignalingProfile TELEKOM_IPSP egressIpAttributes sipHeadersAndParameters callForwarding
historyInformation includeHistoryInformation enable
set profiles signaling ipSignalingProfile TELEKOM_IPSP egressIpAttributes sipHeadersAndParameters callForwarding
historyInformation causeParameterInRFC4458 enable
set profiles signaling ipSignalingProfile TELEKOM_IPSP egressIpAttributes transport type1 tlsOverTcp
commit
```

5. IP Interface Group

Create an IP interface group.

> **Note**
> Replace "x.x.x.x" with the SBC's packet interface (pkt) IP address towards DT CompanyFlex Trunk (example pkt1 IP), and "Y" with its prefix length. Provide the ceName used during an SBC deployment.
>
> Here, the ceName is "SBXUK9".

```
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 ceName SBXUK9 portName pkt1
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 ipAddress x.x.x.x prefix Y
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 mode inService state enabled
commit
```

6. Zone

Create a Zone towards Telekom and specify the id of the zone.

> **Note**
> This Zone groups the set of objects used for communication towards Telekom.

```
set addressContext default zone TELEKOM id 6
commit
```

7. SIP Signaling Port

Set the SIP Signaling port, which is a logical address used to send and receive SIP call signaling packets and is permanently bound to a specific zone.

> **Note**
> Replace "x.x.x.x" with the SIP Signaling Port IP address of the SBC towards DT trunk.
>
> Attach the TLS profile created earlier.

```
set addressContext default zone TELEKOM sipSigPort 7 ipInterfaceGroupName LIF2
set addressContext default zone TELEKOM sipSigPort 7 ipAddressV4 x.x.x.x
set addressContext default zone TELEKOM sipSigPort 7 portNumber 5060
set addressContext default zone TELEKOM sipSigPort 7 tlsProfileName TLS_PROF
set addressContext default zone TELEKOM sipSigPort 7 transportProtocolsAllowed sip-tls-tcp
set addressContext default zone TELEKOM sipSigPort 7 mode inService
set addressContext default zone TELEKOM sipSigPort 7 state enabled
commit
```

Warning
There are a few areas that result in a TLS negotiation issue. One area involves assigning the incorrect port. Ensure the following are accomplished:

- SBC listens on port number 5061 (default setting).

8. IP Peer

Create an IP Peer with the fqdn towards DT trunk and attach it to TELEKOM Zone.

```
set addressContext default zone EXTERNAL ipPeer TELEKOM policy sip fqdn 551136882893.primary.companyflex.de
set addressContext default zone EXTERNAL ipPeer TELEKOM policy sip fqdnPort 0
commit
```

Warning
There are a few areas that result in a TLS negotiation issue. One area involves assigning the incorrect port. Ensure the following are accomplished:

- Configure the DT Trunk fqdn and fqdnPort as "0" so that SBC performs DNS SRV query for the configured fqdn.

9. SIP Message Manipulation

The Deutsche Telekom SIP trunk expects the following SIP messages to be modified.

- rule 1 - modify the "Request-uri" with the DT CompanyFlex fqdn.
- rule 2 - modify the "To" header with the DT CompanyFlex fqdn.
- rule 3 - modify the "From" header with the DT CompanyFlex fqdn.
- rule 4 - modify the "P-Preferred-Identity" header with the DT CompanyFlex fqdn.
- rule 5 - add "Security-Client: sdes-srtp;mediasec", "Proxy-Require: mediasec" and "Require: mediasec" headers in REGISTER message.
- rule 6 - add "Security-Server: msrp-tls;mediasec", "Security-Server: sdes-srtp;mediasec" and "Security-Server: dtls-srtp;mediasec" in subsequent REGISTER message after SIP 401 Unauthorized.
- rule 7 - add "Proxy-Require: mediasec", "Require: mediasec", "Security-Verify: msrp-tls;mediasec" , "Security-Verify: sdes-srtp;mediasec", "Security-Verify: dtls-srtp;mediasec" in INVITE message.
- rule 8 - add "a=3ge2ae:requested" attribute in SDP of the INVITE message.
- rule 9 - add rport in Via header.
- rule 10 - add "+" in the History-Info User-part.
- rule 11 - replace the host-part of History-Info with the DT CompanyFlex fqdn.
- rule 12 - store History-Info user-part in a variable var1.
- rule 13 - replace the user-part of P-Preferred-Identity with the variable var1.
- rule 14 - store the user-part of From header in a variable var2.
- rule 15 - replace the second History-Info user-part with the variable var2, occurs only in case of call forward scenario.

```
set profiles signaling sipAdaptorProfile REG_TLS state enabled
set profiles signaling sipAdaptorProfile REG_TLS advancedSMM enabled
set profiles signaling sipAdaptorProfile REG_TLS profileType messageManipulation
set profiles signaling sipAdaptorProfile REG_TLS rule 1 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 1 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 1 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 1 criterion 1 message messageTypes requestAll
set profiles signaling sipAdaptorProfile REG_TLS rule 1 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 1 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 1 criterion 2 header name request-line
set profiles signaling sipAdaptorProfile REG_TLS rule 1 criterion 2 header condition exist
```

```
set profiles signaling sipAdaptorProfile REG_TLS rule 1 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 1 action 1 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 1 action 1 operation modify
set profiles signaling sipAdaptorProfile REG_TLS rule 1 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 1 action 1 from type value
set profiles signaling sipAdaptorProfile REG_TLS rule 1 action 1 from value tel.t-online.de
set profiles signaling sipAdaptorProfile REG_TLS rule 1 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 1 action 1 to type token
set profiles signaling sipAdaptorProfile REG_TLS rule 1 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile REG_TLS rule 2 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 2 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 2 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 2 criterion 1 message messageTypes requestAll
set profiles signaling sipAdaptorProfile REG_TLS rule 2 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 2 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 2 criterion 2 header name To
set profiles signaling sipAdaptorProfile REG_TLS rule 2 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 2 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 2 action 1 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 2 action 1 operation modify
set profiles signaling sipAdaptorProfile REG_TLS rule 2 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 2 action 1 from type value
set profiles signaling sipAdaptorProfile REG_TLS rule 2 action 1 from value tel.t-online.de
set profiles signaling sipAdaptorProfile REG_TLS rule 2 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 2 action 1 to type token
set profiles signaling sipAdaptorProfile REG_TLS rule 2 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile REG_TLS rule 3 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 3 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 3 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 3 criterion 1 message messageTypes requestAll
set profiles signaling sipAdaptorProfile REG_TLS rule 3 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 3 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 3 criterion 2 header name From
set profiles signaling sipAdaptorProfile REG_TLS rule 3 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 3 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 3 action 1 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 3 action 1 operation modify
set profiles signaling sipAdaptorProfile REG_TLS rule 3 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 3 action 1 from type value
set profiles signaling sipAdaptorProfile REG_TLS rule 3 action 1 from value tel.t-online.de
set profiles signaling sipAdaptorProfile REG_TLS rule 3 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 3 action 1 to type token
set profiles signaling sipAdaptorProfile REG_TLS rule 3 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile REG_TLS rule 4 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 4 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 4 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 4 criterion 1 message messageTypes requestAll
set profiles signaling sipAdaptorProfile REG_TLS rule 4 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 4 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 4 criterion 2 header name P-Preferred-Identity
set profiles signaling sipAdaptorProfile REG_TLS rule 4 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 4 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 4 action 1 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 4 action 1 operation modify
set profiles signaling sipAdaptorProfile REG_TLS rule 4 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 4 action 1 from type value
set profiles signaling sipAdaptorProfile REG_TLS rule 4 action 1 from value tel.t-online.de
set profiles signaling sipAdaptorProfile REG_TLS rule 4 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 4 action 1 to type token
set profiles signaling sipAdaptorProfile REG_TLS rule 4 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile REG_TLS rule 5 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 5 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 5 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 5 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 5 criterion 1 message methodTypes [ register ]
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 1 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 1 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 1 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 1 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 1 from value "sdes-srtp;mediasec"
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 1 to
```

```
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 1 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 1 to value Security-Client
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 2 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 2 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 2 from
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 2 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 2 from value mediasec
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 2 to
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 2 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 2 to value Proxy-Require
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 3 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 3 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 3 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 3 from
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 3 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 3 from value mediasec
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 3 to
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 3 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 5 action 3 to value Require
set profiles signaling sipAdaptorProfile REG_TLS rule 6 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 6 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 6 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 6 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 6 criterion 1 message methodTypes [ register ]
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 1 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 1 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 1 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 1 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 1 from value "msrp-tls;mediasec"
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 1 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 1 to value Security-Verify
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 2 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 2 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 2 from
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 2 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 2 from value "sdes-srtp;mediasec"
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 2 to
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 2 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 2 to value Security-Verify
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 3 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 3 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 3 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 3 from
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 3 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 3 from value "dtls-srtp;mediasec"
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 3 to
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 3 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 6 action 3 to value Security-Verify
set profiles signaling sipAdaptorProfile REG_TLS rule 7 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 7 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 7 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 7 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 7 criterion 1 message methodTypes [ invite ]
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 1 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 1 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 1 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 1 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 1 from value "mediasec "
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 1 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 1 to value Proxy-Require
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 2 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 2 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 2 from
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 2 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 2 from value "mediasec "
```

```
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 2 to
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 2 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 2 to value Require
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 3 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 3 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 3 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 3 from
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 3 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 3 from value "msrp-tls;mediasec "
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 3 to
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 3 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 3 to value Security-Verify
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 4 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 4 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 4 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 4 from
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 4 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 4 from value "sdes-srtp;mediasec"
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 4 to
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 4 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 4 to value Security-Verify
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 5 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 5 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 5 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 5 from
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 5 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 5 from value "dtls-srtp;mediasec "
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 5 to
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 5 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 5 to value Security-Verify
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 6 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 6 operation add
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 6 headerPosition last
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 6 from
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 6 from type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 6 from value supported
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 6 to
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 6 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 7 action 6 to value P-Early-Media
set profiles signaling sipAdaptorProfile REG_TLS rule 8 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 8 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 8 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 8 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 8 criterion 1 message methodTypes [ invite ]
set profiles signaling sipAdaptorProfile REG_TLS rule 8 criterion 2 type messageBody
set profiles signaling sipAdaptorProfile REG_TLS rule 8 criterion 2 messageBody
set profiles signaling sipAdaptorProfile REG_TLS rule 8 criterion 2 messageBody condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 type messageBody
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 operation regappend
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 from type value
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 from value "\\na=3ge2ae:requested "
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 to type messageBody
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 to messageBodyValue all
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 regexp
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 regexp string "t=0 0"
set profiles signaling sipAdaptorProfile REG_TLS rule 8 action 1 regexp matchInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 9 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 1 message messageTypes all
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 2 header name Via
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 3 type parameter
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 3 parameter
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 3 parameter condition absent
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 3 parameter paramType generic
set profiles signaling sipAdaptorProfile REG_TLS rule 9 criterion 3 parameter name rport
```

```
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 operation regappend
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 from type value
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 from value ";rport"
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 to value Via
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 regexp
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 regexp string .*
set profiles signaling sipAdaptorProfile REG_TLS rule 9 action 1 regexp matchInstance one
set profiles signaling sipAdaptorProfile REG_TLS rule 10 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 10 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 10 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 10 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 10 criterion 1 message methodTypes [ invite ]
set profiles signaling sipAdaptorProfile REG_TLS rule 10 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 10 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 10 criterion 2 header name History-Info
set profiles signaling sipAdaptorProfile REG_TLS rule 10 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 10 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 operation regappend
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 headerInfo fieldValue
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 from type value
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 from value +
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 to value History-Info
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 regexp
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 regexp string <sip:
set profiles signaling sipAdaptorProfile REG_TLS rule 10 action 1 regexp matchInstance one
set profiles signaling sipAdaptorProfile REG_TLS rule 11 applyMatchHeader two
set profiles signaling sipAdaptorProfile REG_TLS rule 11 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 11 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 11 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 11 criterion 1 message methodTypes [ invite ]
set profiles signaling sipAdaptorProfile REG_TLS rule 11 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 11 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 11 criterion 2 header name History-Info
set profiles signaling sipAdaptorProfile REG_TLS rule 11 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 11 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 operation regpostsub
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 headerInfo fieldValue
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 from type value
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 from value tel.t-online.de
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 to type header
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 to value History-Info
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 regexp
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 regexp string @
set profiles signaling sipAdaptorProfile REG_TLS rule 11 action 1 regexp matchInstance one
set profiles signaling sipAdaptorProfile REG_TLS rule 12 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 1 message methodTypes [ invite ]
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 2 header name History-Info
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 3 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 3 token
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 3 token condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 12 criterion 3 token tokenType uriusername
set profiles signaling sipAdaptorProfile REG_TLS rule 12 action 1 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 12 action 1 operation store
set profiles signaling sipAdaptorProfile REG_TLS rule 12 action 1 from
```

```
set profiles signaling sipAdaptorProfile REG_TLS rule 12 action 1 from type token
set profiles signaling sipAdaptorProfile REG_TLS rule 12 action 1 from tokenValue uriusername
set profiles signaling sipAdaptorProfile REG_TLS rule 12 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 12 action 1 to type variable
set profiles signaling sipAdaptorProfile REG_TLS rule 12 action 1 to variableValue var1
set profiles signaling sipAdaptorProfile REG_TLS rule 12 action 1 to variableScopeValue local
set profiles signaling sipAdaptorProfile REG_TLS rule 13 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 1 message methodTypes [ invite ]
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 2 header name P-Preferred-Identity
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 3 type variable
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 3 variable
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 3 variable condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 13 criterion 3 variable variableID var1
set profiles signaling sipAdaptorProfile REG_TLS rule 13 action 1 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 13 action 1 operation modify
set profiles signaling sipAdaptorProfile REG_TLS rule 13 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 13 action 1 from type variable
set profiles signaling sipAdaptorProfile REG_TLS rule 13 action 1 from variableValue var1
set profiles signaling sipAdaptorProfile REG_TLS rule 13 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 13 action 1 to type token
set profiles signaling sipAdaptorProfile REG_TLS rule 13 action 1 to tokenValue uriusername
set profiles signaling sipAdaptorProfile REG_TLS rule 14 applyMatchHeader one
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 1 message methodTypes [ invite ]
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 2 header name From
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 3 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 3 token
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 3 token condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 14 criterion 3 token tokenType uriusername
set profiles signaling sipAdaptorProfile REG_TLS rule 14 action 1 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 14 action 1 operation store
set profiles signaling sipAdaptorProfile REG_TLS rule 14 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 14 action 1 from type token
set profiles signaling sipAdaptorProfile REG_TLS rule 14 action 1 from tokenValue uriusername
set profiles signaling sipAdaptorProfile REG_TLS rule 14 action 1 to
set profiles signaling sipAdaptorProfile REG_TLS rule 14 action 1 to type variable
set profiles signaling sipAdaptorProfile REG_TLS rule 14 action 1 to variableValue var2
set profiles signaling sipAdaptorProfile REG_TLS rule 14 action 1 to variableScopeValue local
set profiles signaling sipAdaptorProfile REG_TLS rule 15 applyMatchHeader two
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 1 type message
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 1 message
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 1 message methodTypes [ invite ]
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 2 type header
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 2 header
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 2 header name History-Info
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 3 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 3 token
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 3 token condition exist
set profiles signaling sipAdaptorProfile REG_TLS rule 15 criterion 3 token tokenType uriusername
set profiles signaling sipAdaptorProfile REG_TLS rule 15 action 1 type token
set profiles signaling sipAdaptorProfile REG_TLS rule 15 action 1 operation modify
set profiles signaling sipAdaptorProfile REG_TLS rule 15 action 1 from
set profiles signaling sipAdaptorProfile REG_TLS rule 15 action 1 from type variable
set profiles signaling sipAdaptorProfile REG_TLS rule 15 action 1 from variableValue var2
set profiles signaling sipAdaptorProfile REG_TLS rule 15 action 1 to
```

```
set profiles signaling sipAdaptorProfile REG_TLS rule 15 action 1 to type token
set profiles signaling sipAdaptorProfile REG_TLS rule 15 action 1 to tokenValue uriusername
```

10. SIP Trunk Group

Create a SIP Trunk Group towards Deutsche Telekom and assign corresponding profiles like PSP and IPSP, that were created in previous steps.

> **Warning**
> You must configure Trunk Group names using capital letters.

```
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG media mediaIpInterfaceGroupName LIF2
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG mode inService state enabled
commit

set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG policy digitParameterHandling numberingPlan
GERMANY_NUM_PLAN
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG policy media packetServiceProfile TELEKOM
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG policy signaling ipSignalingProfile TELEKOM_IPSP
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling messageManipulation
outputAdapterProfile REG_TLS
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling timers sessionMinSE 900
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling registration expires 600
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling registration insideExpiresMinimum 600
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling authentication authUserPart
+491992960000000100540
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling authentication authPassword xxxxxx
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling authentication intChallengeResponse
enabled
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling authentication incInternalCredentials
enabled
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling transportPreference preference1 tls-tcp
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG signaling acceptHistoryInfo enabled
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG services dnsSupportType a-srv-naptr
set addressContext default zone EXTERNAL sipTrunkGroup TELEKOM_TG ingressIpPrefix 0.0.0.0 0
commit
```

11. Routing Label

Create a Routing Label with a single Routing Label Route to bind the DT Trunk Group with the DT IP Peer.

```
set global callRouting routingLabel TELEKOM_RL routingLabelRoute 1 routeType trunkGroup
set global callRouting routingLabel TELEKOM_RL routingLabelRoute 1 trunkGroup TELEKOM_TG
set global callRouting routingLabel TELEKOM_RL routingLabelRoute 1 ipPeer TELEKOM
set global callRouting routingLabel TELEKOM_RL routingLabelRoute 1 inService inService
commit
```

12. Call Routing

This entry is used to route all the calls coming from DT towards endpoint behind SBC.

> **Note**
> Provide the ceName used during an SBC deployment. "SBXUK9" is the ceName.

```
set global callRouting route trunkGroup TELEKOM_TG SBXUK9 standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel IP_PBX_RL
commit
```

Section B: CUCM (IP-PBX) Configuration

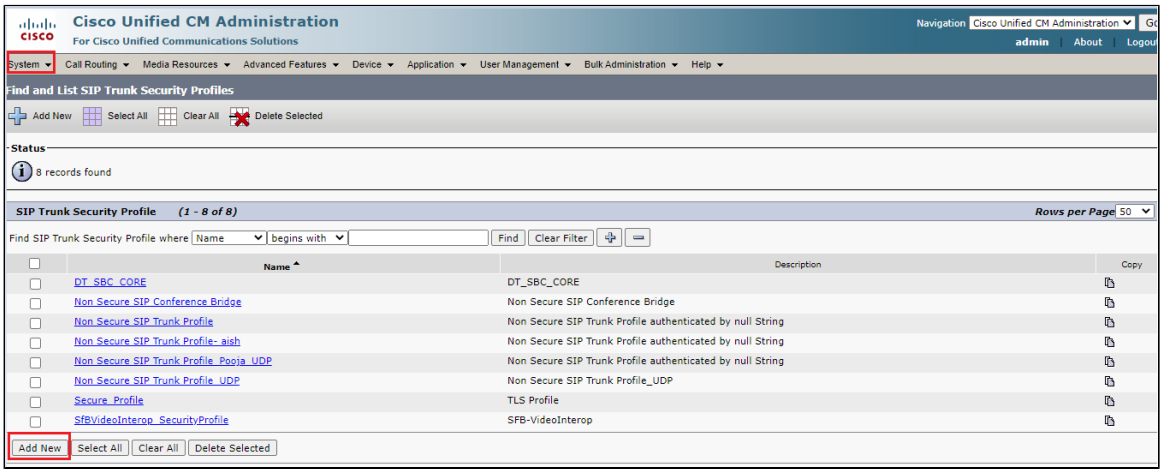
1. Accessing CUCM (Cisco Unified CM Administration)

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**.

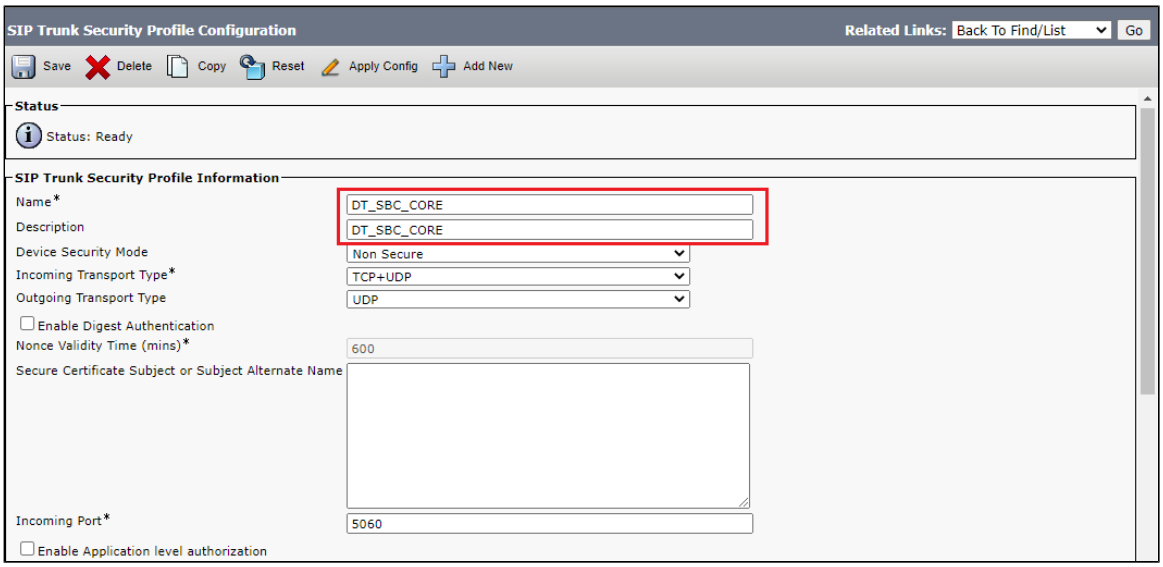
2. SIP Trunk Security Profile

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**.



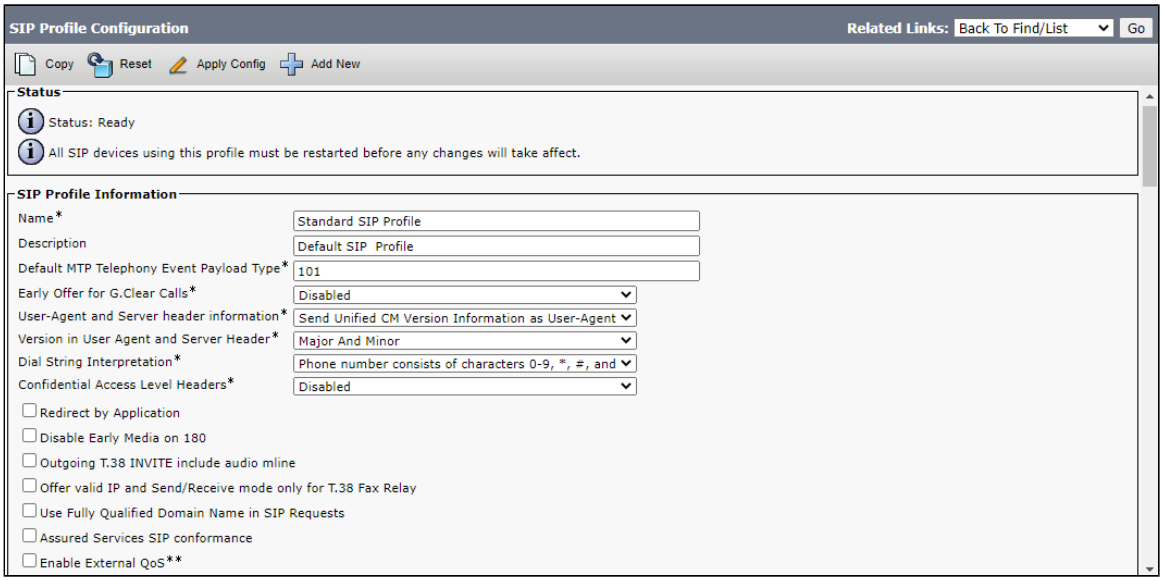
- Provide the desired Name and Description.
- Choose **Non Secure** from Device Security Mode.
  - No security features except image authentication apply. A TCP or UDP connection opens to Unified Communications Manager.
- From Incoming Transport Type, select **TCP+UDP**.
  - When Device Security Mode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

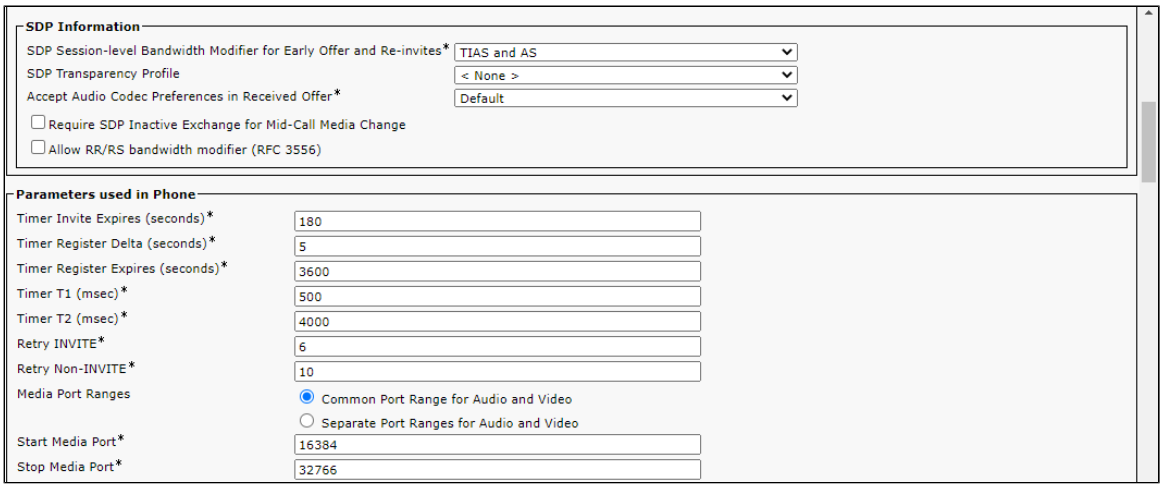


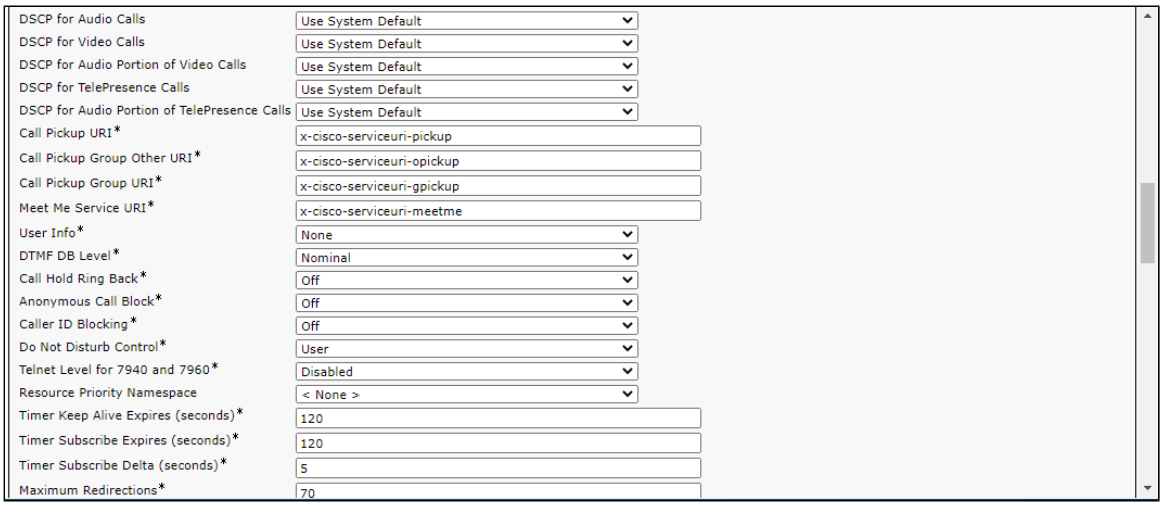
3. SIP Profiles

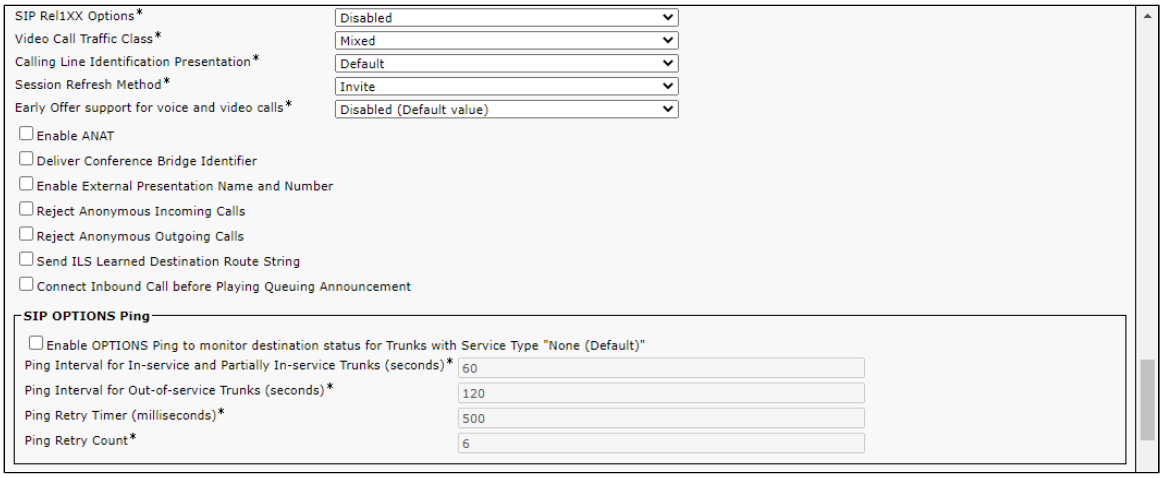
A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that you cannot delete or change.

- From Cisco Unified CM Administration, navigate to **Device > Device Settings > SIP Profile.**
- Use the default **"Standard SIP Profile"**, the configuration is as follows:





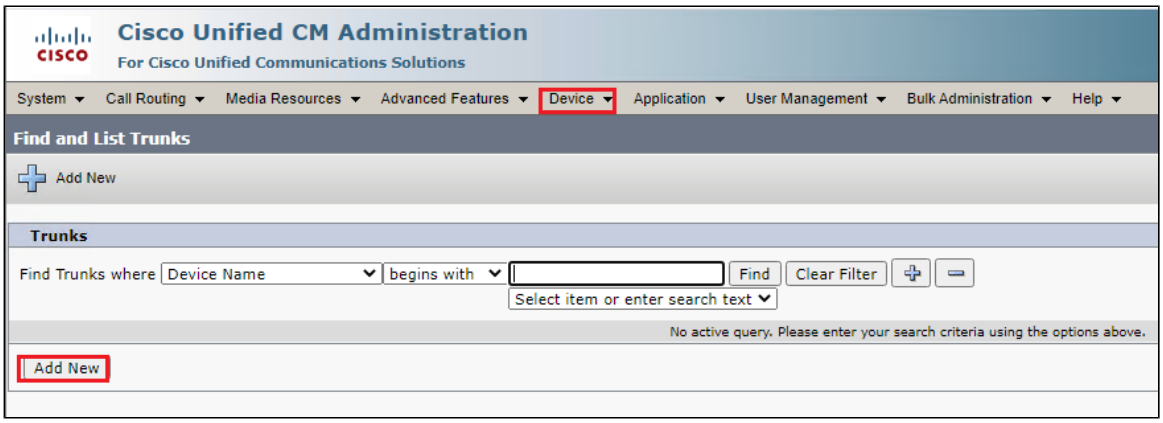




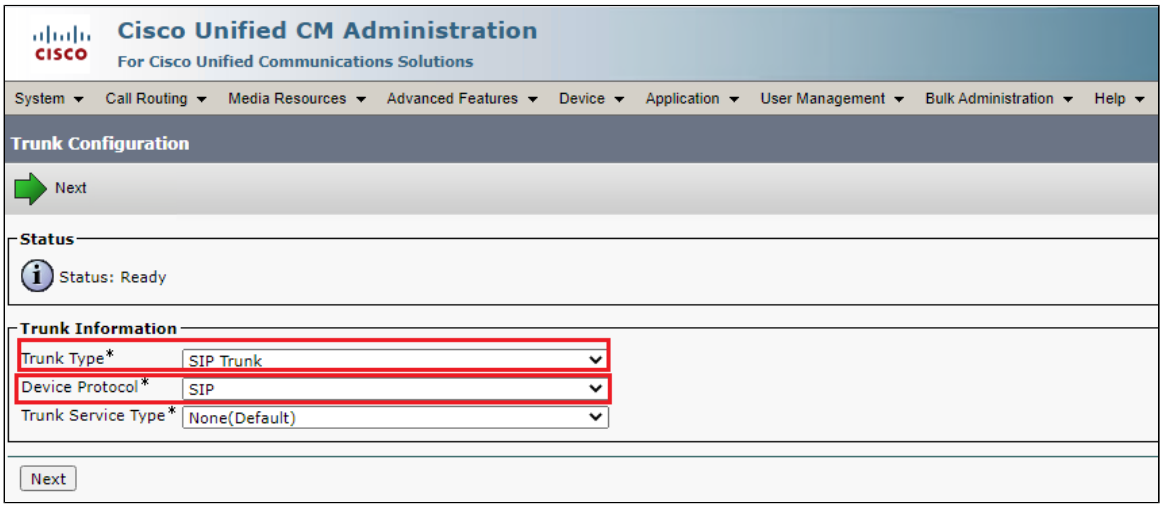
4. Trunk Configuration

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

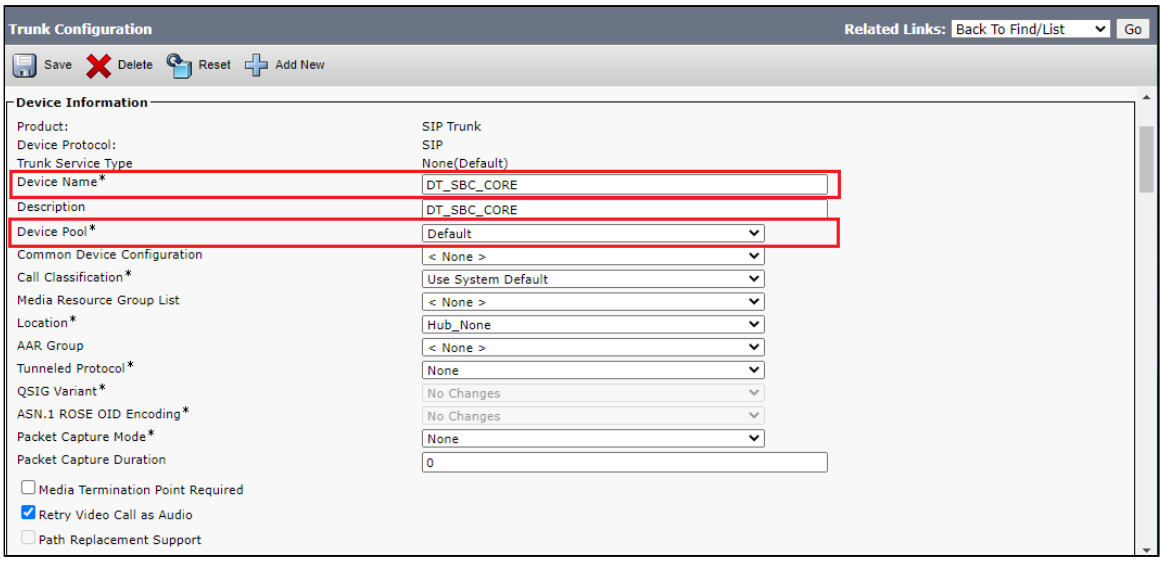
- From Cisco Unified CM Administration, choose **Device > Trunk.**
- Click **Add New**.



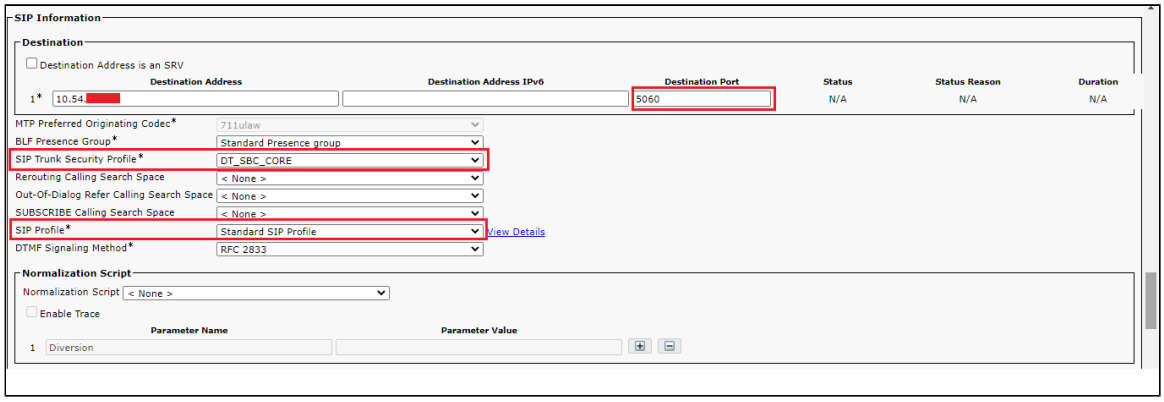
- From the Trunk Type drop-down list, choose **SIP Trunk**.
- Choose **SIP** from Device Protocol drop-down.
- From Trunk Service Type, select the default value (None).
- Click **Next**.



- 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.

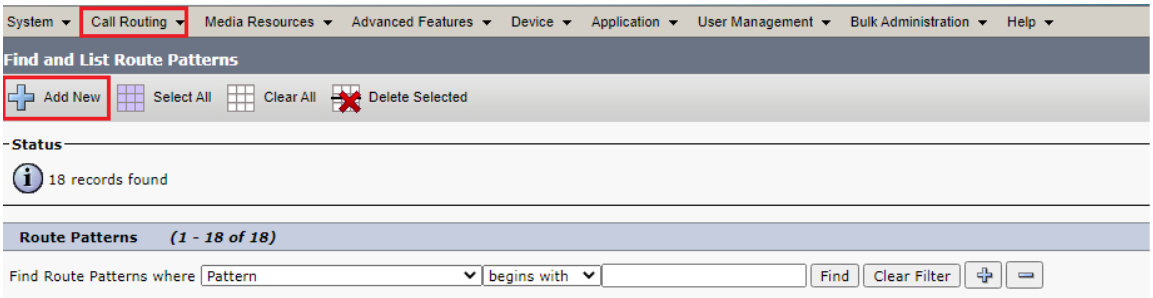
Note
Resetting/restarting a SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager.

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

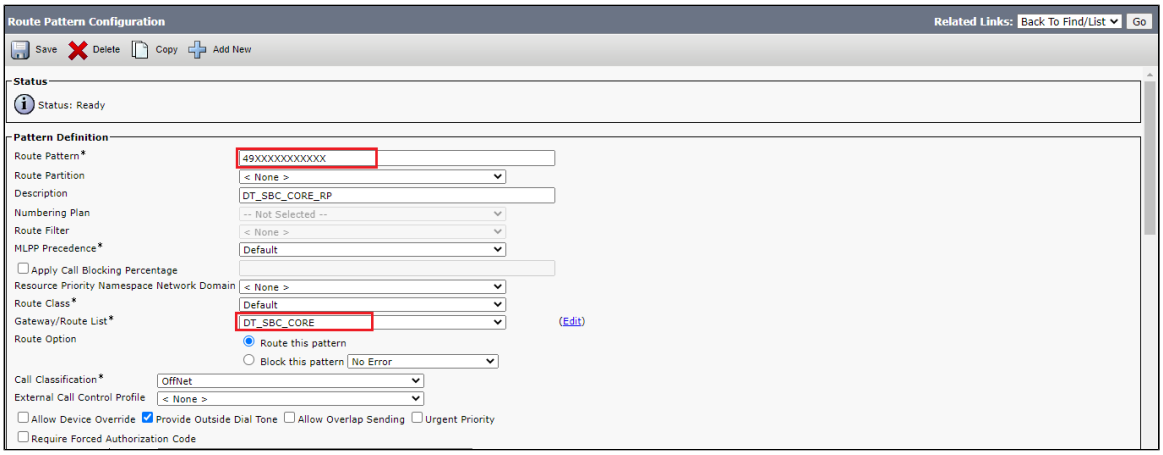
5. Route Pattern

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, 49XXXXXXXXX - 49 followed by 9 digits number would be routed to the Gateway/Route List configured. 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.

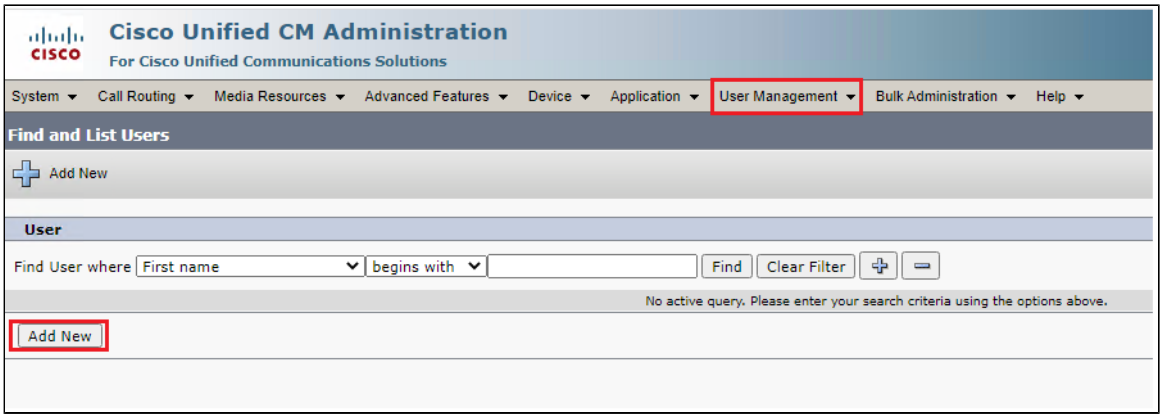


6. Register Third Party SIP Phones to CUCM

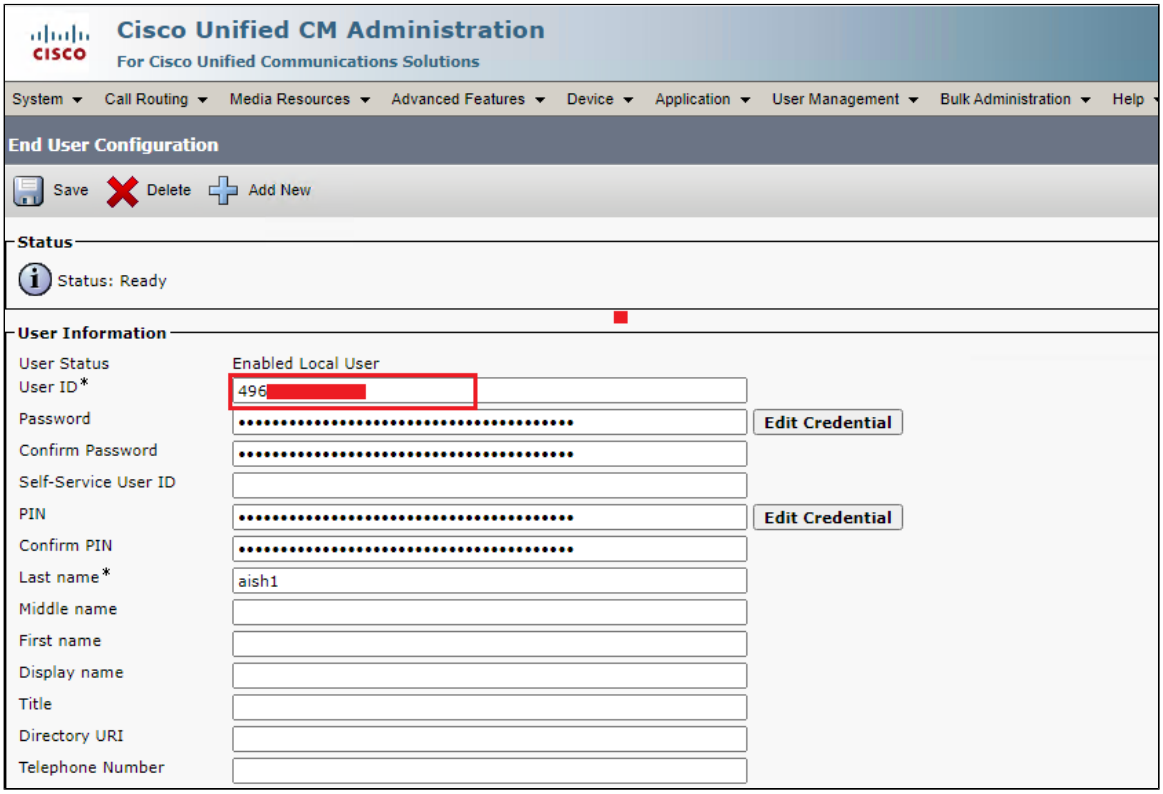
Configure End Users

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**.

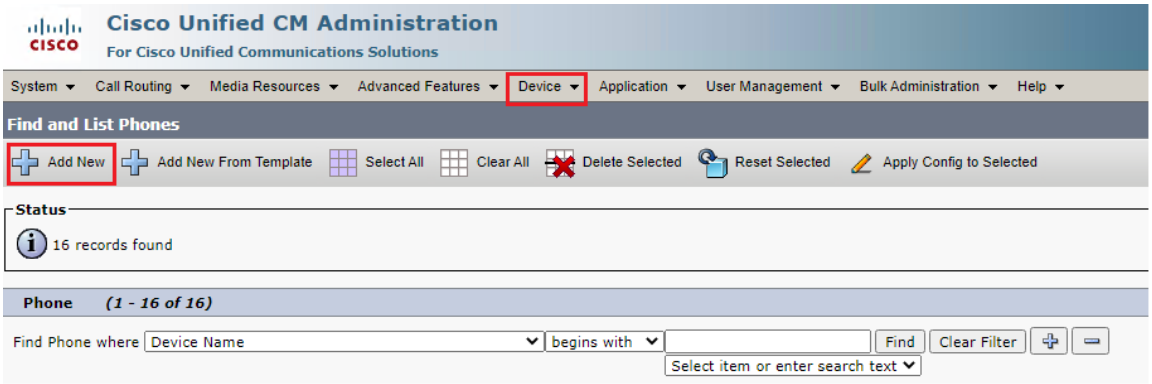


- Enter the unique end user identification name.
- Enter alphanumeric or special characters for the end user password and confirm.
- Enter numeric characters for the end user PIN and confirm.
- Enter the end user last name.

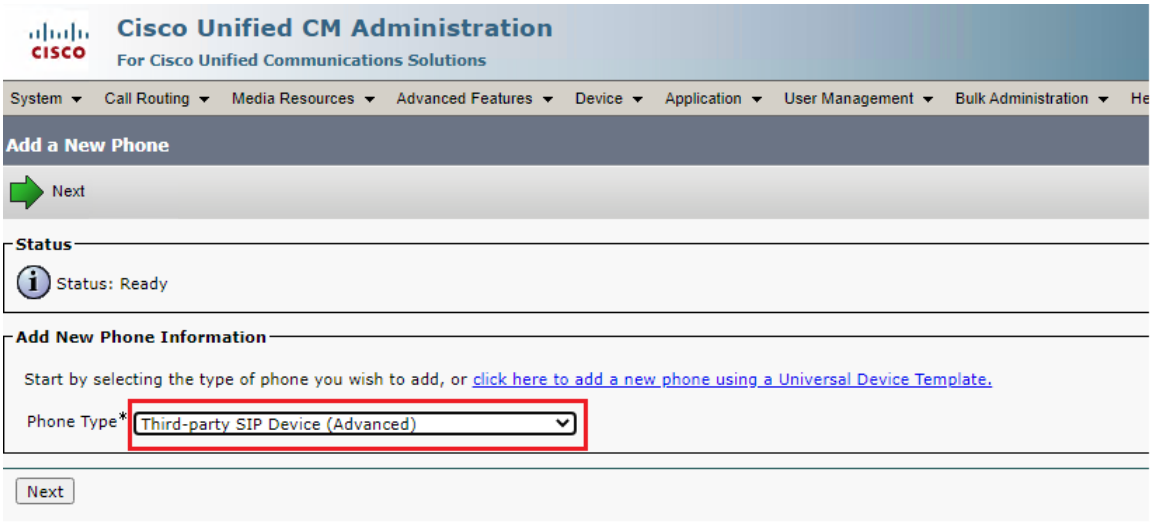


Phone Setup

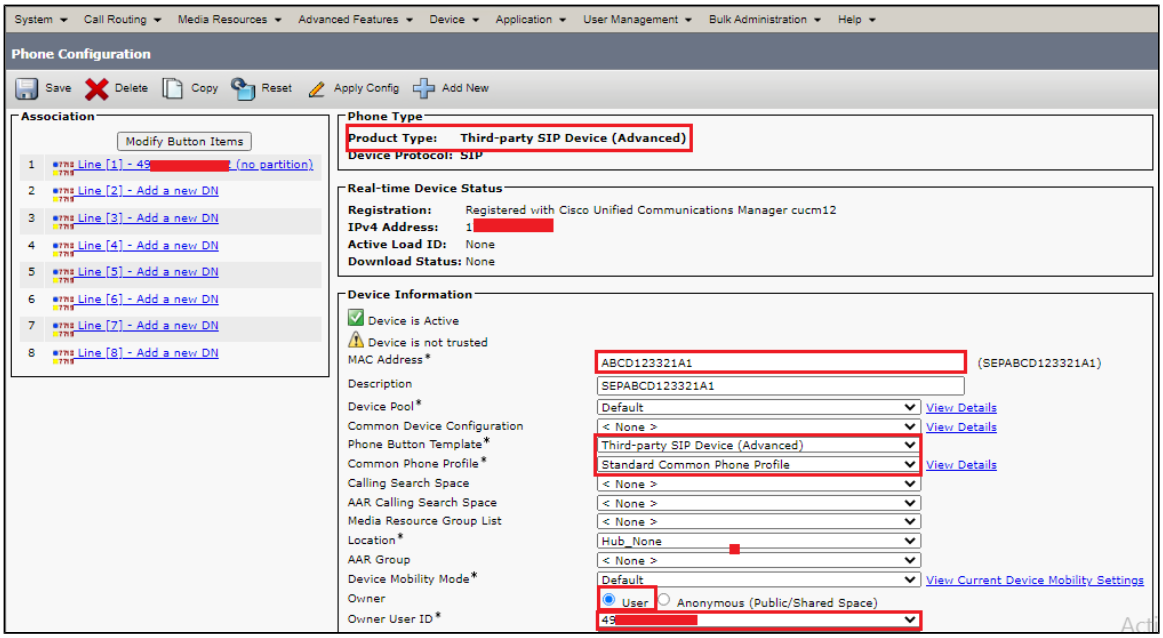
- In Cisco Unified Communications Manager Administration, navigate to **Device > Phone** to configure phones.
- Click **Add New**.



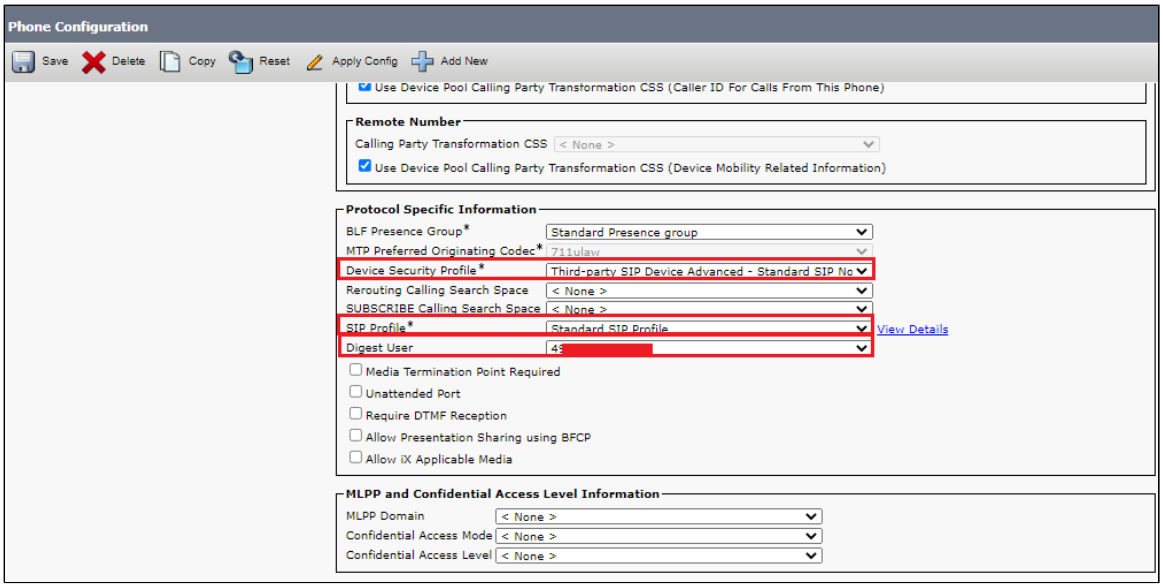
- From the Phone Type drop-down, choose Third-party SIP Device (Advanced) Endpoint.
- Click **Next**.



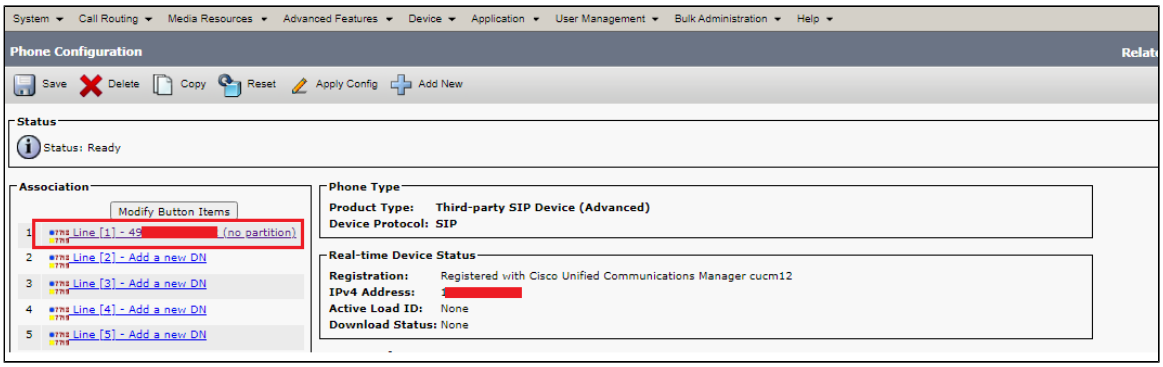
- Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones. Make sure that the value comprises 12 hexadecimal characters.
- Choose **Default** Device pool.
  - A Device pool defines sets of common characteristics for devices, such as region, date/time group, and soft key template.
- 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**.

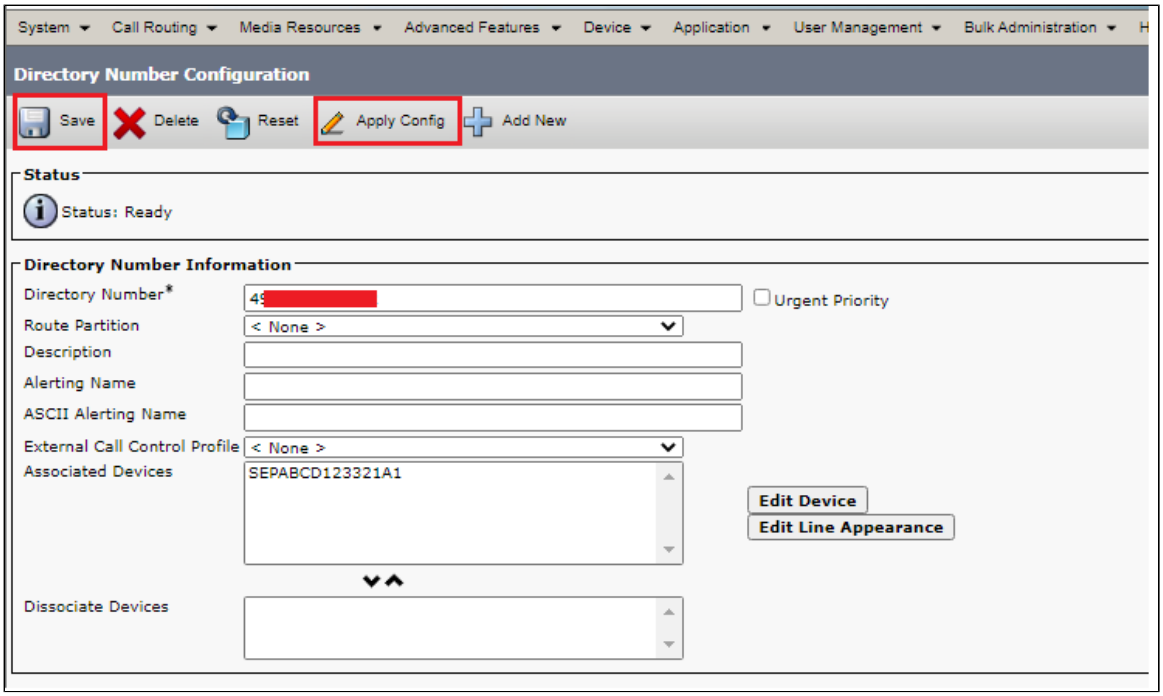


- Click this link to add a remote destination to associate with this device. The Remote Destination Configuration window displays, which allows you to add a new remote destination to associate with this device.



Note
Registration status should be "Registered with Cisco Unified Communication Manager" as shown above.

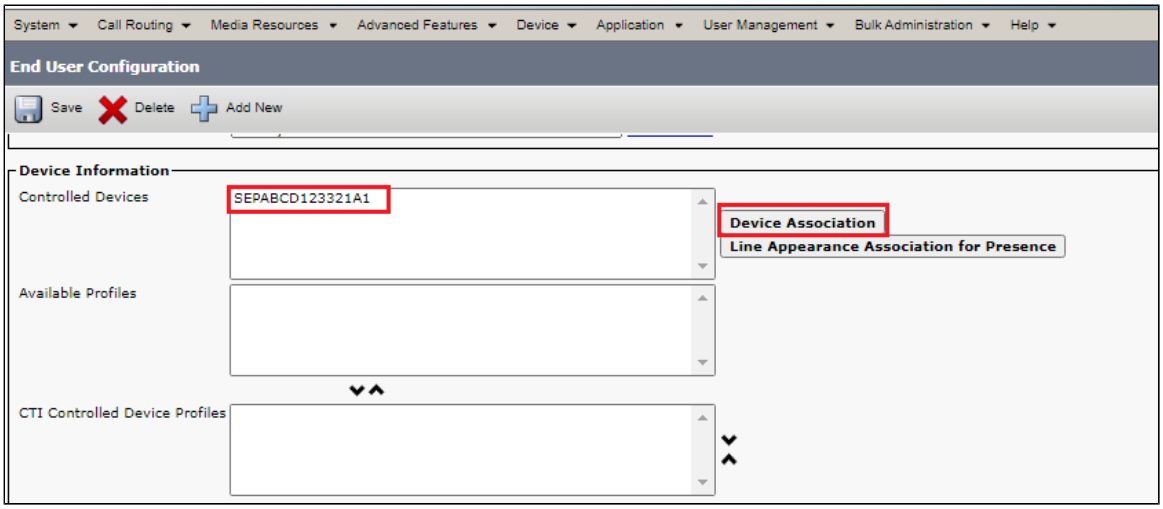
- Add the Directory number.
- Click **Save**.



- 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 displays 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	Call Transfer (Blind)	✓
15	Call Transfer (Attended)	✓
16	Call Busy	✓
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

Download the Deutsche Telekom Global root Certificate from https://corporate-pki.telekom.de/en/GlobalRootClass2.html

The SBC Core will throw the following error when loading the DT Global Root Certificate:

```
[root@SBXUK9 external]# openssl x509 -in GlobalRoot_Class_2.crt -inform PEM -out DTroot_cert.cer -outform DER
unable to load certificate
140620648452160:error:0906D06C:PEM routines:PEM_read_bio:no start line:../crypto/pem/pem_lib.c:686:Expecting:
TRUSTED CERTIFICATE
```

The DT Root Certificate would be as follows:

(BEGIN/END line in same line as encoded cert)

```
-----BEGIN CERTIFICATE-----MIIDwzCCAqugAwIBAEFEWRTHEFEDDFGdsdf6Fuwg==-----END CERTIFICATE-----
```

The SBC Core expects the (BEGIN/END line in a new line as below)

```
-----BEGIN CERTIFICATE-----
MIIDwzCCAqugAwIBAEFEWRTHEFEDDFGdsdf6Fuwg==
-----END CERTIFICATE-----
```

Workaround: Add the new line at the BEGIN/END of the certificate as shown above.

Then convert the DT Global Root certificate from .crt to .der as shown in Ribbon SBC Configuration for TLS/SRTP.

Support

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

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

References

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

For detailed information about Deutsche Telekom products and solutions, visit: https://www.telekom.com/

Conclusion

This Interoperability Guide describes successful configuration covering Deutsche Telekom CompanyFlex SIP Trunk interop involving Ribbon SBC Core. All the necessary features and serviceability aspects stand covered as per the details provided in this interoperability document.