Deutsche Telekom DeutschlandLAN

Configuration of the Unify OpenScape Enterprise Express Servers / OpenScape Voice with OpenScape SBC

Customer Solution Lab Munich

Version 1.4 – 14th September 2020

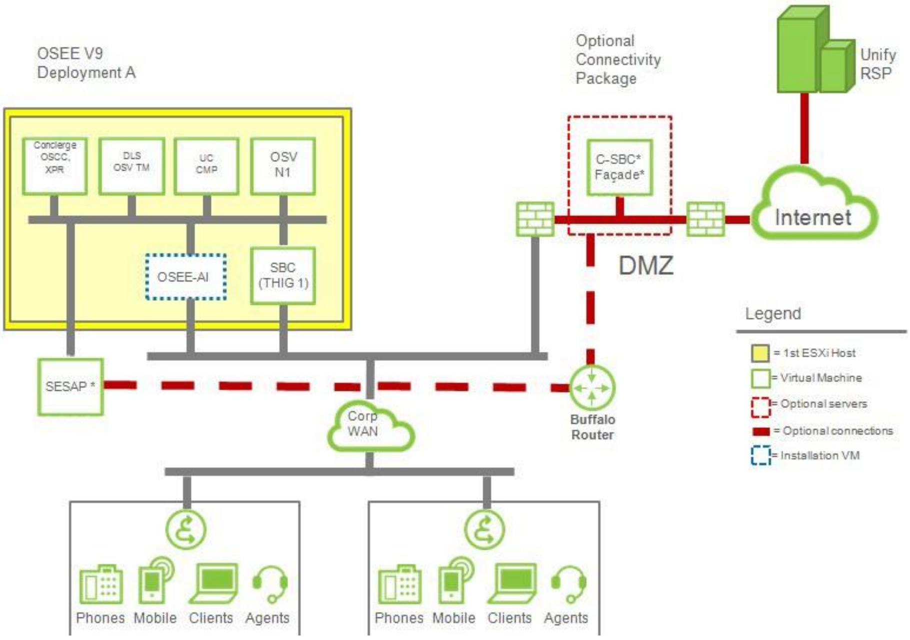
CSL Customer Solution Lab

Table of Contents

1. Document Overview

1.1. Executive Summary

This document describes the configuration of the OpenScape Enterprise Express V9R2 servers to connect to Deutsche Telekom DeutschlandLAN via SIP trunk as they were configured during a certification test in the Deutsche Telekom certification lab. This document and the described configuration is valid also for OpenScape Voice with OpenScape SBC deployments. Deutsche Telekom is hereinafter referred to as Telekom.



1.2. Document Control

1.2.1. Authors of the Document

Name	Company - Department
Rolf Lang	Unify Communications and Collaboration GmbH & Co. KG – IDM CCS PS SP
Dino Culvan	Unify Communications and Collaboration GmbH & Co. KG – PH LE PM

Only the individuals listed above are authorized to make changes to the document.

1.2.2. Version / Changes

Date	Version	Author	Remarks
12th of March 2018	0.1	Rolf Lang	Initial structure
15th of May 2018	1.0	Rolf Lang	Released

18th of May 2018	1.1	Rolf Lang	Change of Digest Authentication data
06th of February 2020	1.2	Dino Culvan	Updates on certificate CA description chapter 2.7
19th of August 2020	1.3	Dino Culvan	Updates on certificate CA links after Telekom changes in chapter 2.7
14th of September 2020	1.4	Dino Culvan	Updates on certificate CA links after Telekom changes in chapter 2.7

2. OpenScape SBC Configuration

For the certification test was used SBC version 09.03.25.01-1 on the Central SBC and THIG SBC.

The configuration data has be taken out from the letter from Telekom:

ERLEBEN, WAS VERBINDET.

TELEKOM DEUTSCHLAND GMBH

Telekom Deutschland GmbH

ZUGANGSDATEN

Vertraulich, bitte aufbewahren!

Datum	01. März 2016
Ortsvorwahl	0228
Durchwahlnr.	12345
Abfragestelle	0

Registrierungsrufnummer

Rufnummernblock

von 000 bis 299

Sehr geehrte Damen und Herren,

2 Internet-Zugang einrichten

Anschlusskennung:	002529108945
Zugangsnummer:	551129501234 5
Mitbenutzernummer:	0001
Persönliches Kennwort:	25170493

3 Telefonie einrichten

Telefonie-Benutzername:	551129601234 5
Telefonie-Passwort:	Yni2Fi84
Outbound-Proxy:	reg.sip-trunk.telekom.de
Registrar:	sip-trunk.telekom.de

Ein Wort in Sachen Sicherheit.

Wenn Sie Fragen haben, ... **kostenfrei unter 0800 33 02524.**

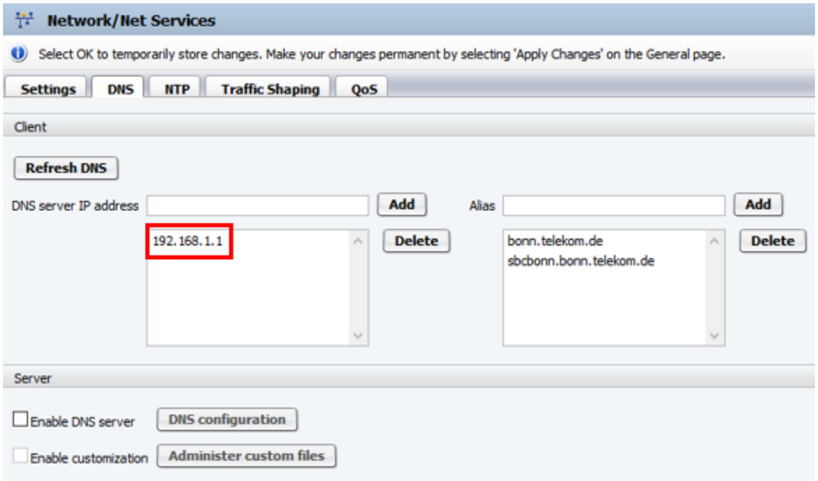
Freundliche Grüße

Ihre Telekom

TELEKOM DEUTSCHLAND GMBH, GESCHÄFTSKUNDENSERVICE

2.1. DNS

It must be configured a DNS server which can resolve the Telekom DNS records configured in the Remote Endpoints:



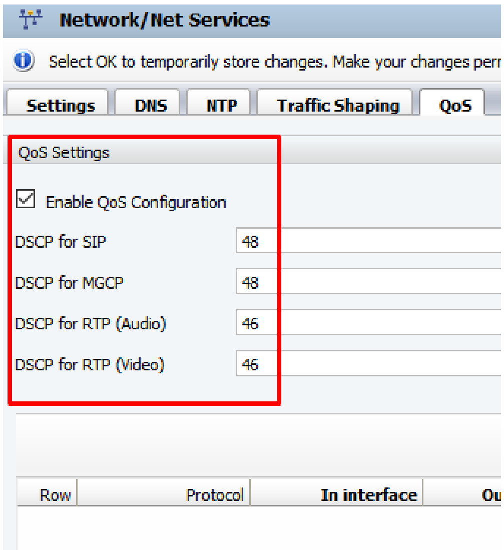
2.2. Quality of Service (QoS)

Telekom has specified in their 1TR114 document QoS requirements which must be applied on the SBC:

8.4.2 Traffic Classes in Layer 3

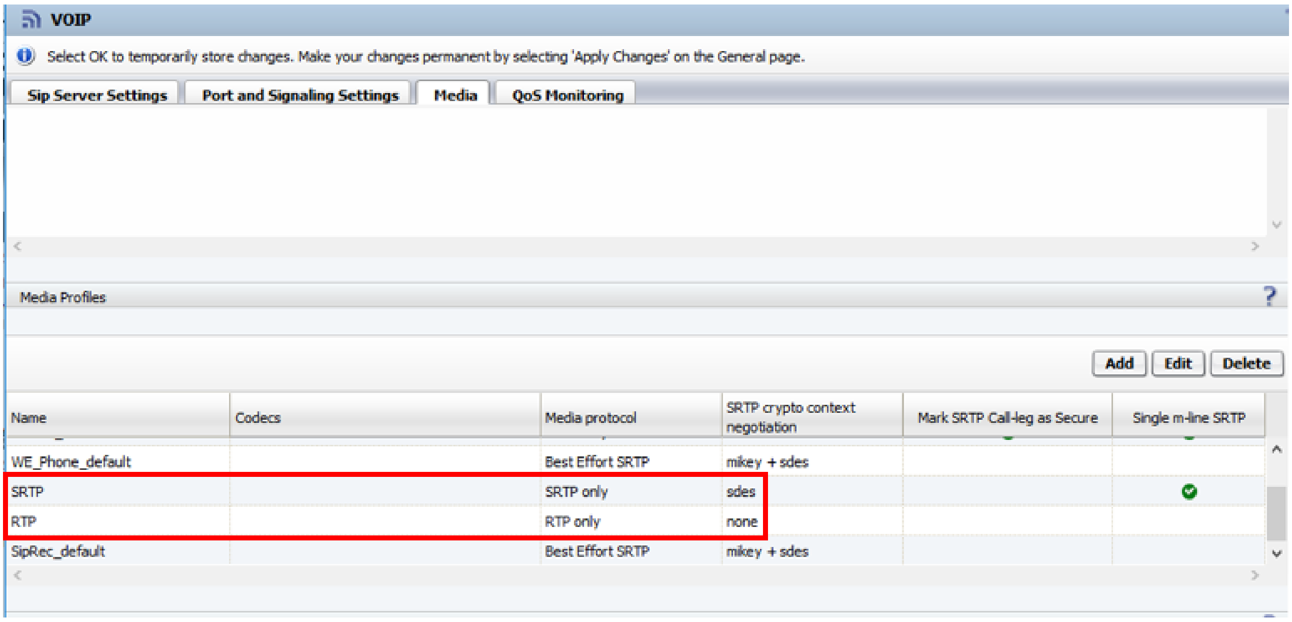
The UE uses the following traffic classes at Layer 3 (according to the Architecture of T-Home)

- Voice Control Class 6 (DSCP 110 000)
- Voice Bearer Class 5 (DSCP 101 110)

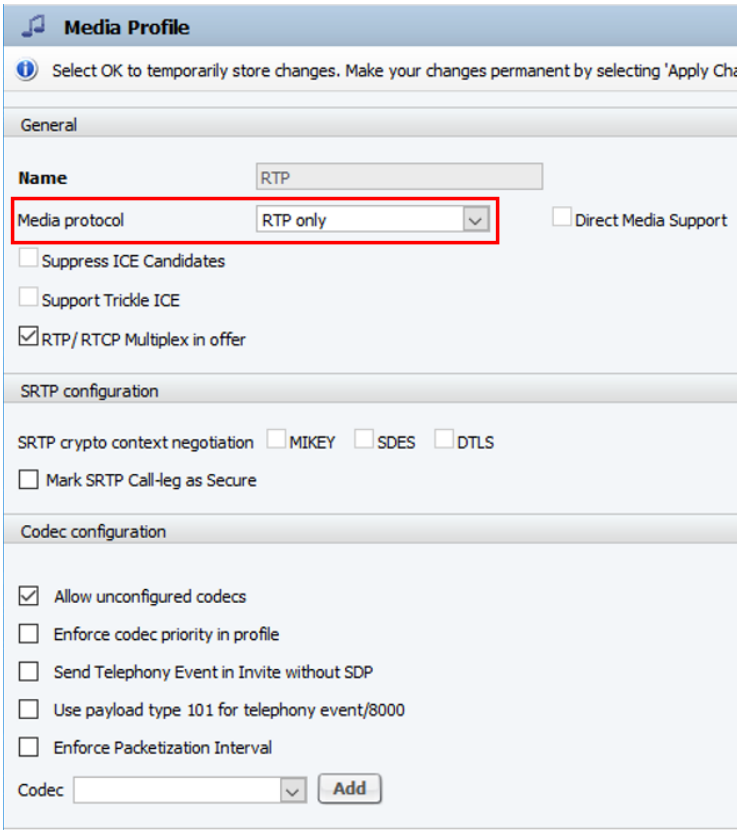


2.3. Media Profile

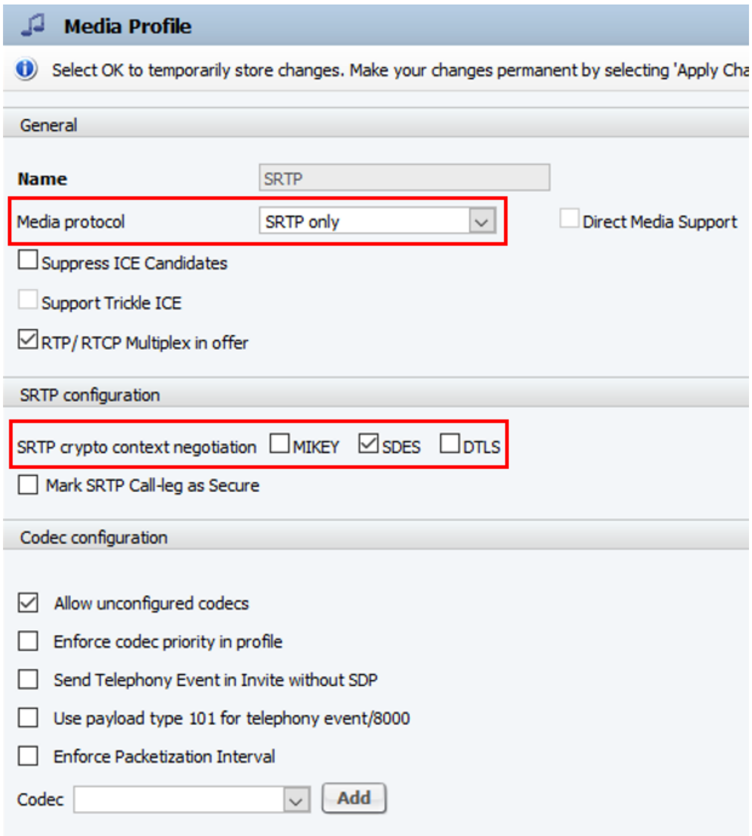
Depending on whether the SIP trunk is encrypted via TLS or not it were prepared two Media Profiles:



For an unencrypted SIP trunk the Media Protocol **RTP** was used:



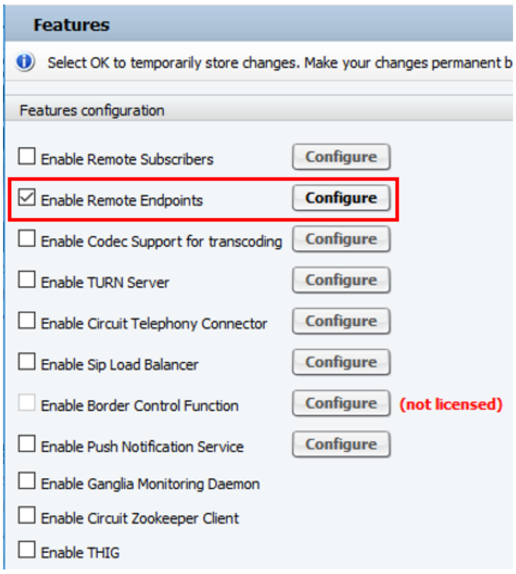
For an encrypted SIP trunk the Media Protocol **SRTP** and **SDES** to negotiate the cryptographic parameters was used. MIKEY may not be enabled because it’s not supported by Telekom.



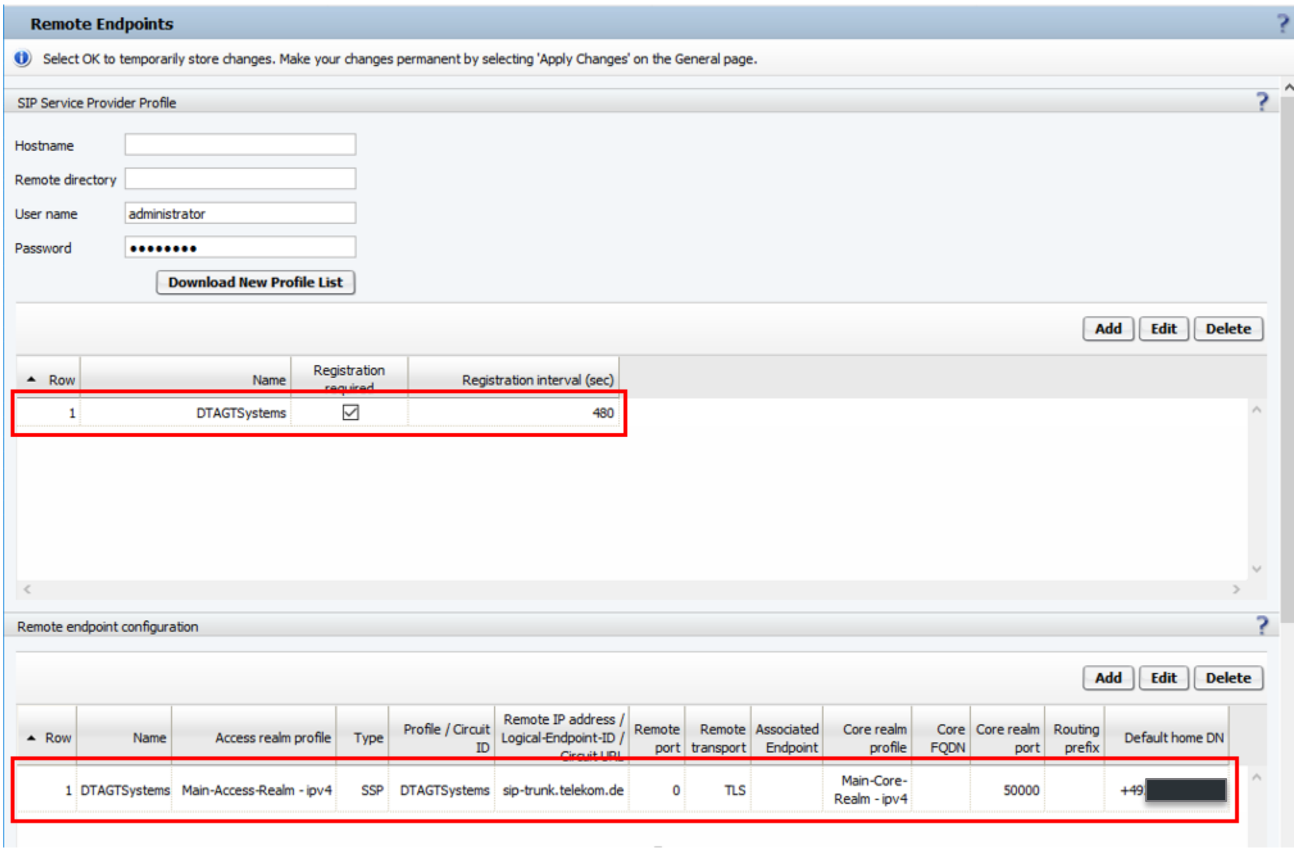
The application of the Media Profile used for the SIP trunk is described in the section *Remote Endpoint* below.

2.4. Remote Endpoint

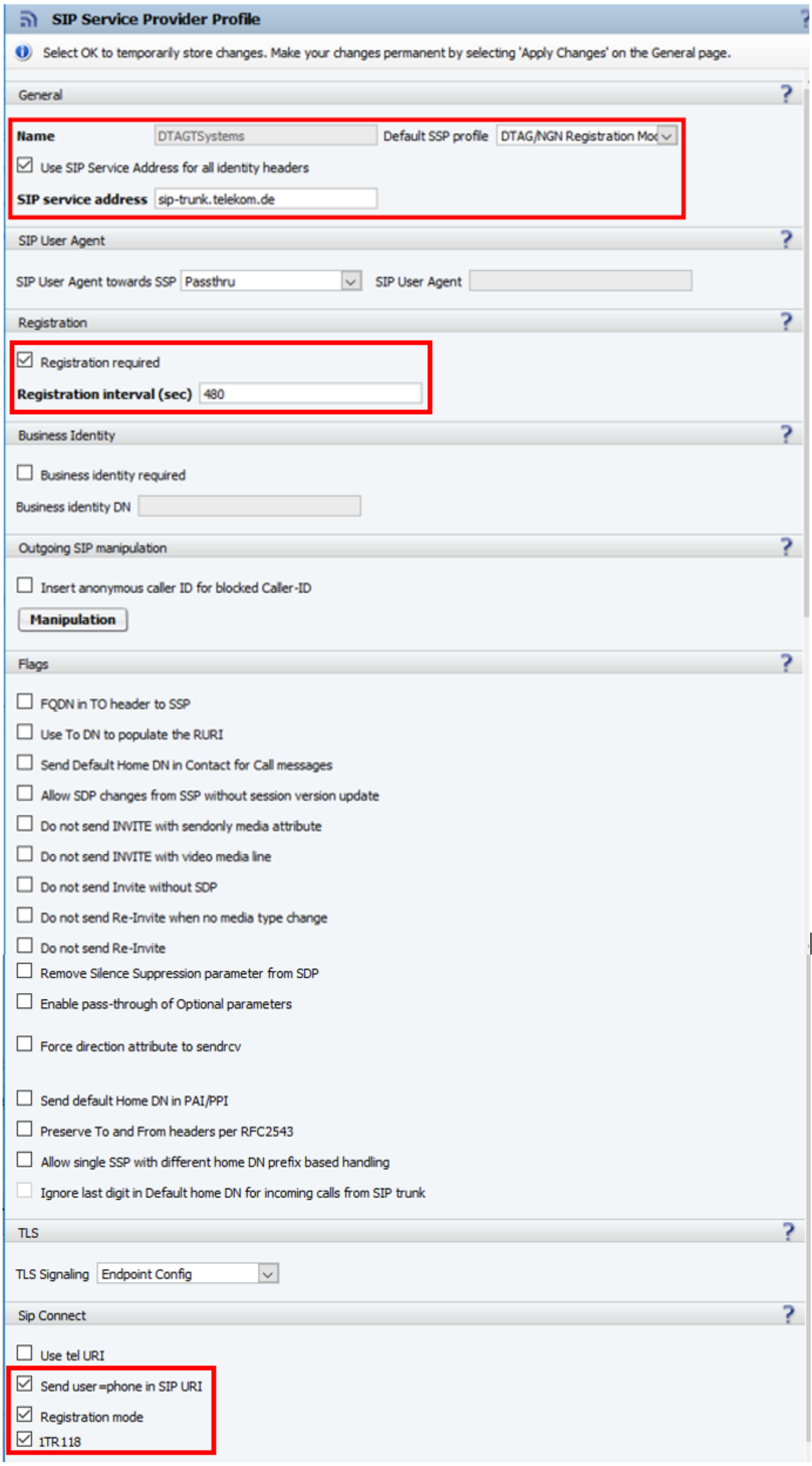
On the Central SBC must be activated *Enable Remote Endpoints*:



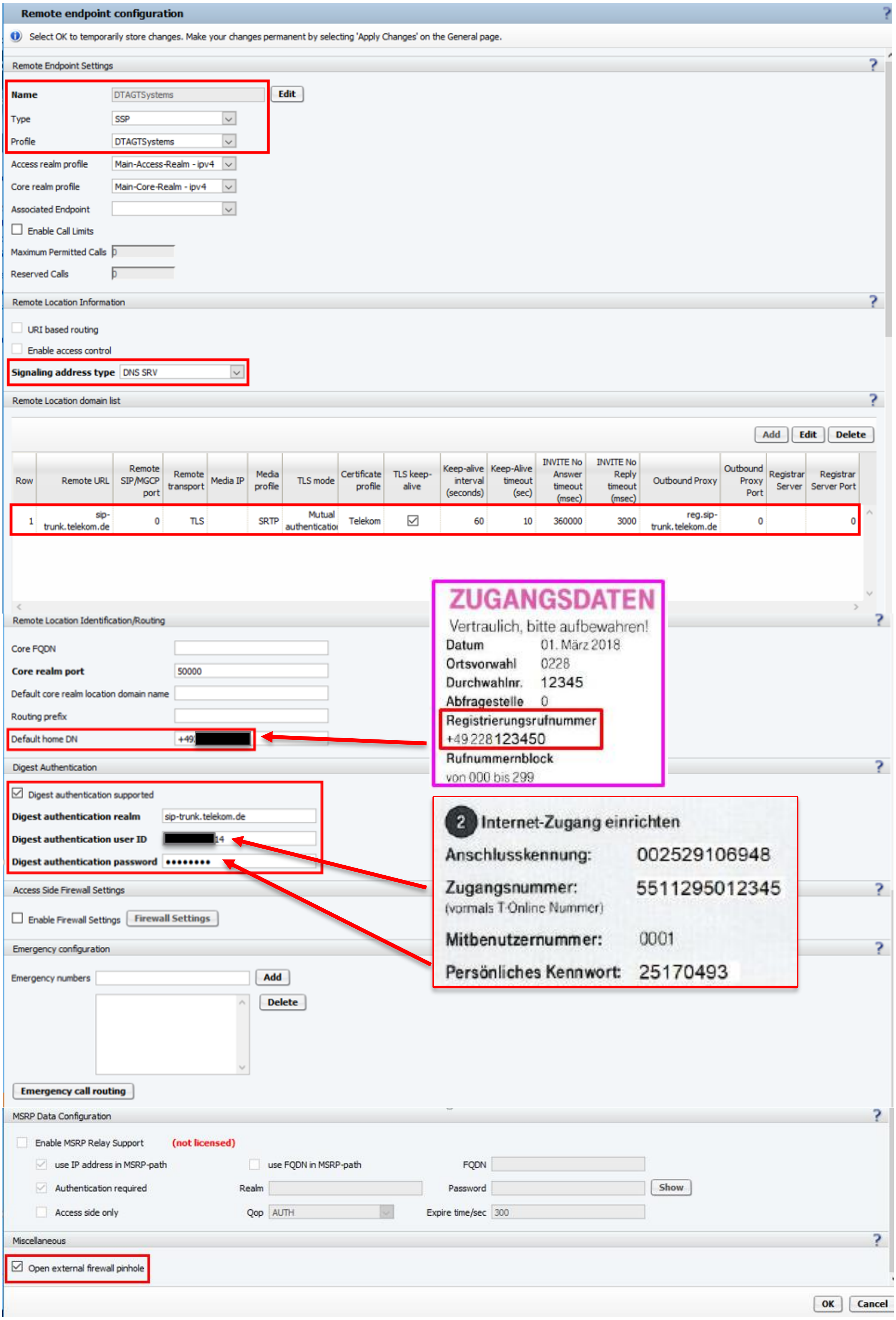
When opening the *Remote Endpoints* window the *SIP Service Provider Profile* and the *Remote Endpoint* has to be configured:



In the *SIP Service Provider Profile* window must be selected as default SSP profile *DTAG/NGN Registration Mode*. The registration interval has to be set to 480 seconds:

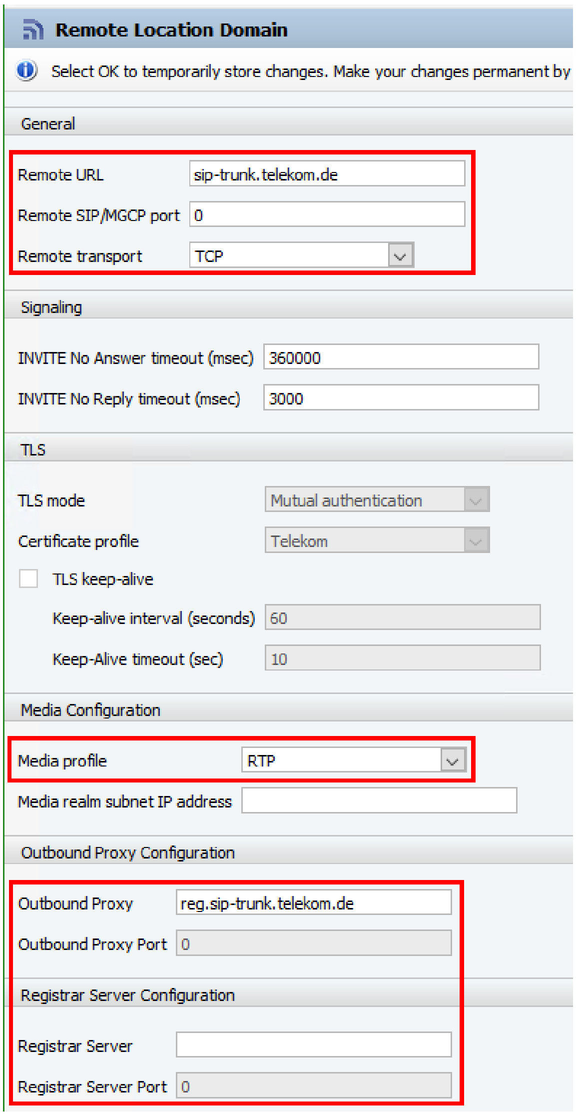


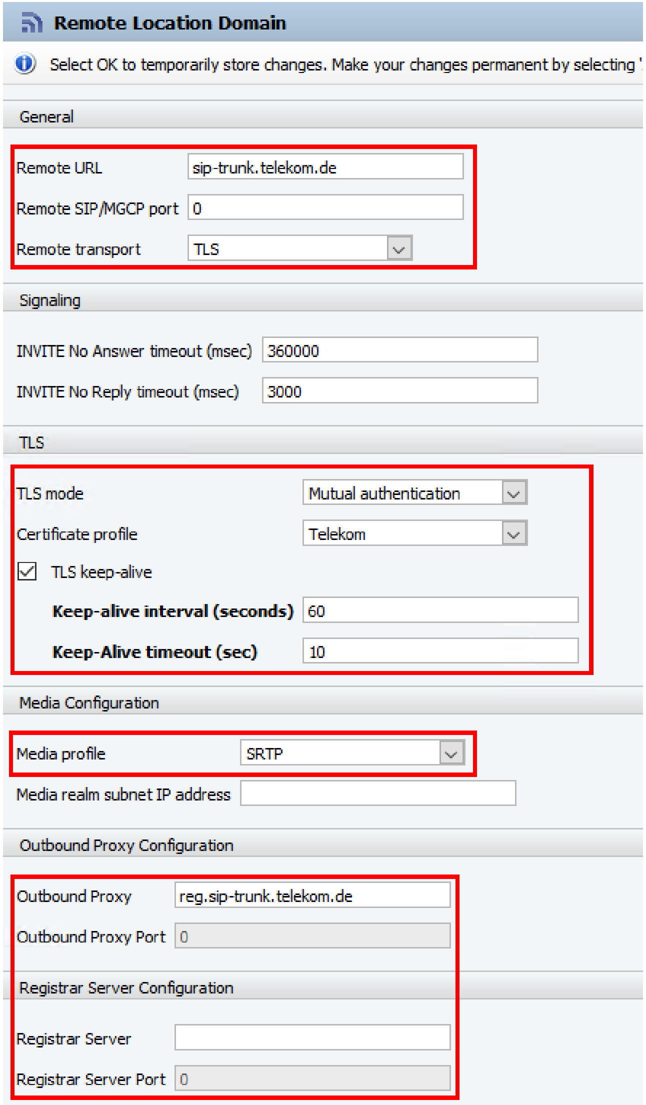
In the *Remote Endpoint Configuration* window the *SIP Service Provider Profile* shown above has to be selected:



If a NAT router is in between SBC and SIP Trunk *Open external firewall pinhole* must be enabled so the SBC will open the RTP port on the NAT router by sending UDP packets to let the NAT router pass RTP packets from a PSTN phone.

The figures below show the *Remote Location Domain* window for an unencrypted SIP trunk using TCP and RTP on the left and for an encrypted SIP trunk using TLS and SRTP on the right:





2.7. Preparing and Installing TLS Certificates

For using TLS and SRTP over the SIP trunk, uploading and configuration of the Deutsche Telekom CA certificates on the SBC is required. The actual Telekom CA certificates can be downloaded here:

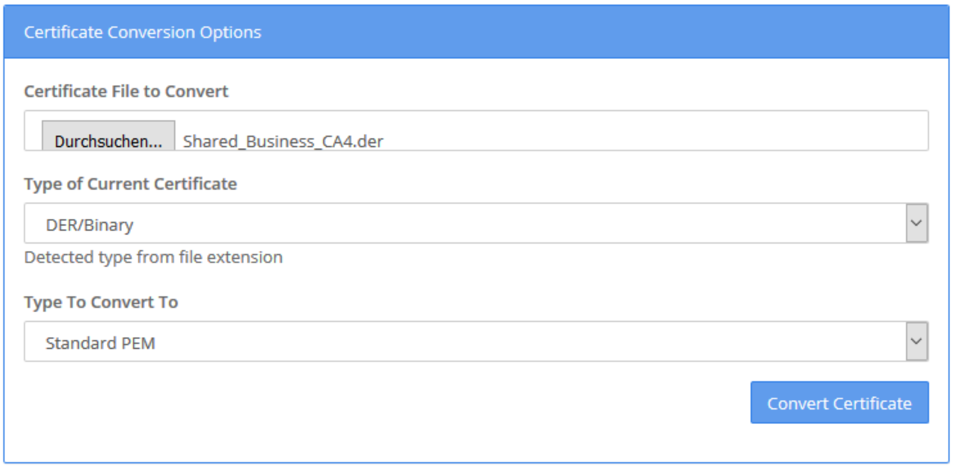
- Download the Telekom *Root-CA-Certificate* **T-TeleSec GlobalRoot Class 2** from URL https://www.telesec.de/assets/downloads/PKI-Repository/T-TeleSec_GlobalRoot_Class_2.cer

Important note:
Please make sure that the certificates are still valid. In case they are expired or not available anymore, please contact Telekom Deutschland GmbH or use the ones from the public websites, e. g.

https://www.telesec.de/de/root-programm/informationen-zu-ca-zertifikaten/root-ca-zertifikate/

Because the OpenScape SBC supports only certificates in pem format the Telekom ‚ *Root-CA-Certificate*‘ certificate T-TeleSec_GlobalRoot_Class_2.cer has to be converted

- via Linux shell e.g. on the OpenScape SBC via command
  openssl x509 -inform der -in T-TeleSec_GlobalRoot_Class_2.cer -out T-TeleSec_GlobalRoot_Class_2.pem
- or via e.g. online converter https://www.sslshopper.com/ssl-converter.html



Click on *Convert Certificate* and save the converted certificate with file extension .pem.

Create in the next step a chained certificate based on the certificates *Root-CA-Certificate* named e.g. dt-chain-ca.pem and copy the content of this certificate files into it in the following order:

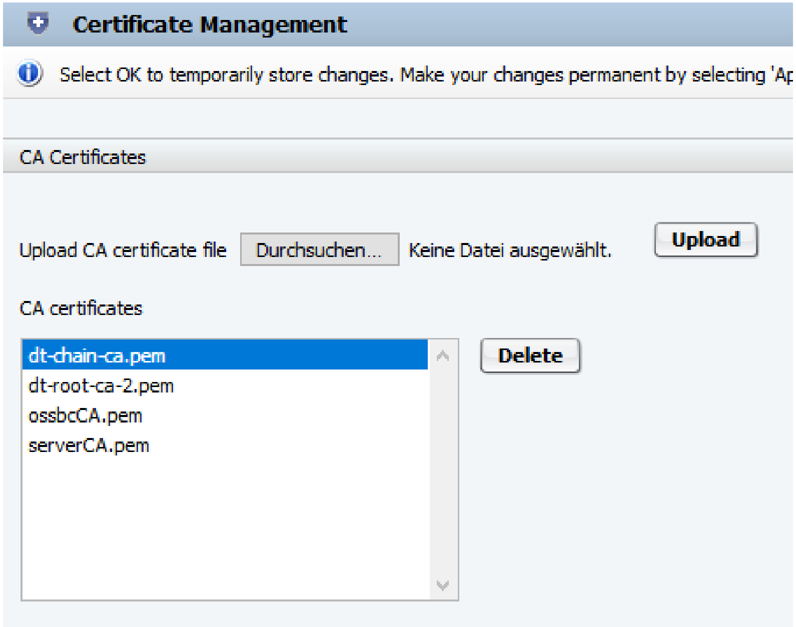
-----BEGIN CERTIFICATE-----
<dt-root-ca-2.cer>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
< T-TeleSec_GlobalRoot_Class_2.cer>
-----END CERTIFICATE-----

Then the chained certificate should look like as below:

```
-----BEGIN CERTIFICATE-----
MIIGiTCCBXGgAwIBAgIIMBWLWM1WMfUwDQYJKoZIhvcNAQELBQAwcTELMAkGA1UE
...
nfKouiXc6eG1ojopwckO/uEu0JVEnyMOzGoIPU2/PhFvG6aAPsB4tvv/AHzR
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

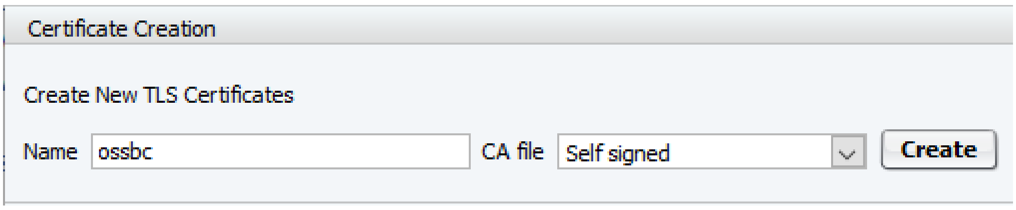
```
MIIDnzCCAoegAwIBAgIBJjANBgkqhkiG9w0BAQUFADBxMQswCQYDVQQGEwJERTEc
...
Cm26OWMohpLzGITY+9HPBVZkVw==
-----END CERTIFICATE-----
```


Then upload this certificate via GUI at Security -> General -> Certificate Management into OpenScape SBC in the in section *CA Certificates* by selecting this certificate and clicking on *Upload*. Then the certificate appears in the CA certificates list:

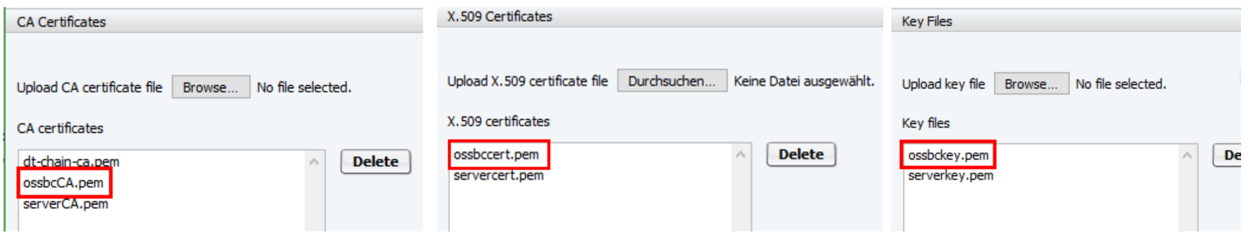


To replace the OpenScape SBC default certificates provided by installation execute the following steps:

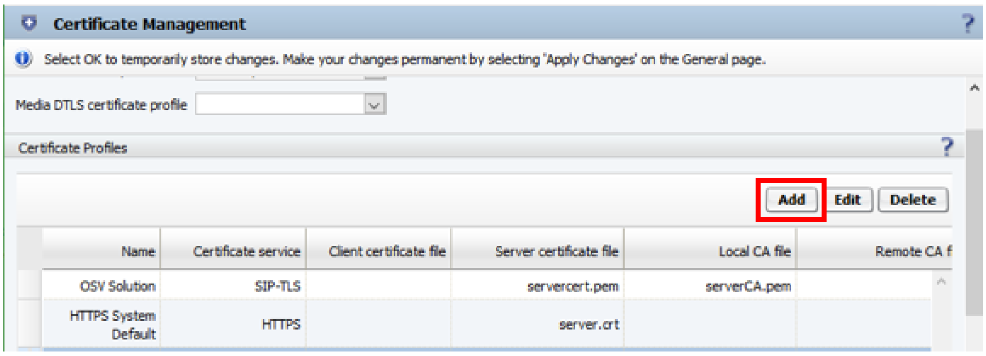
The in *Certificate Creation* section enter e.g. ossbc in the *Name field* an click on Create leaving *Self signed* as *CA file* unchanged:



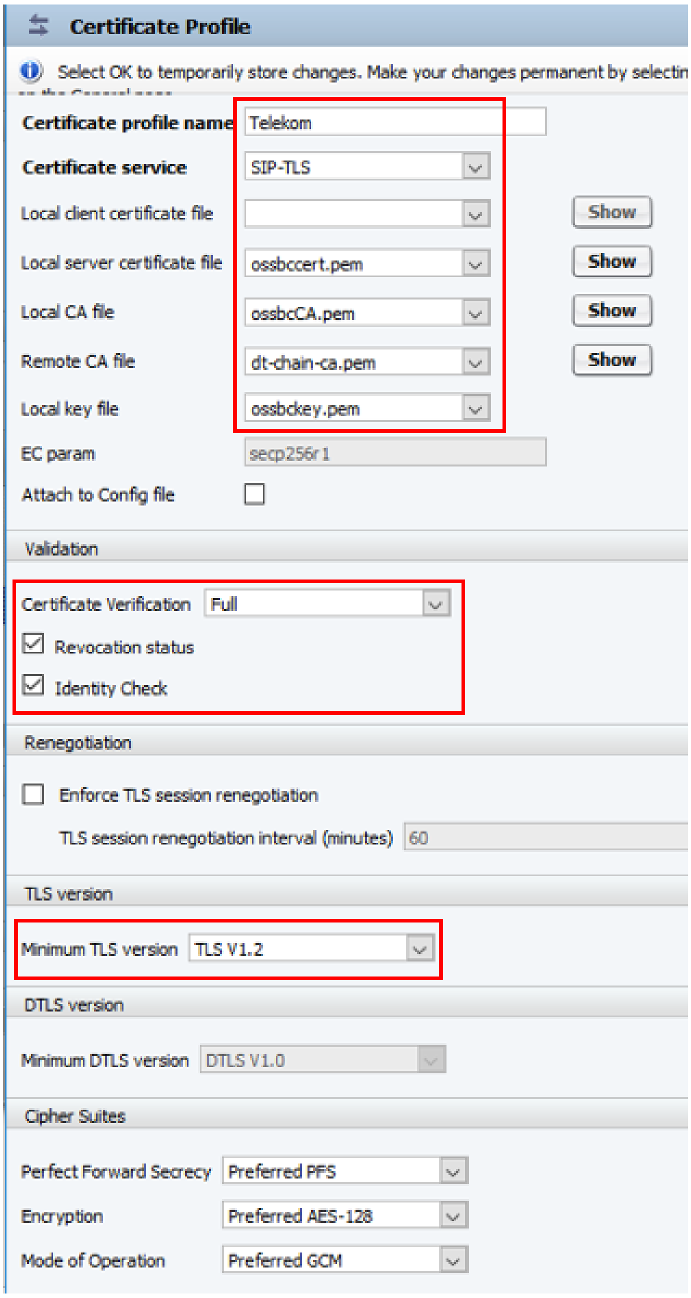
In the *CA certificates*, *X.509 Certificates* and *Key files* windows appears now the new certificates:



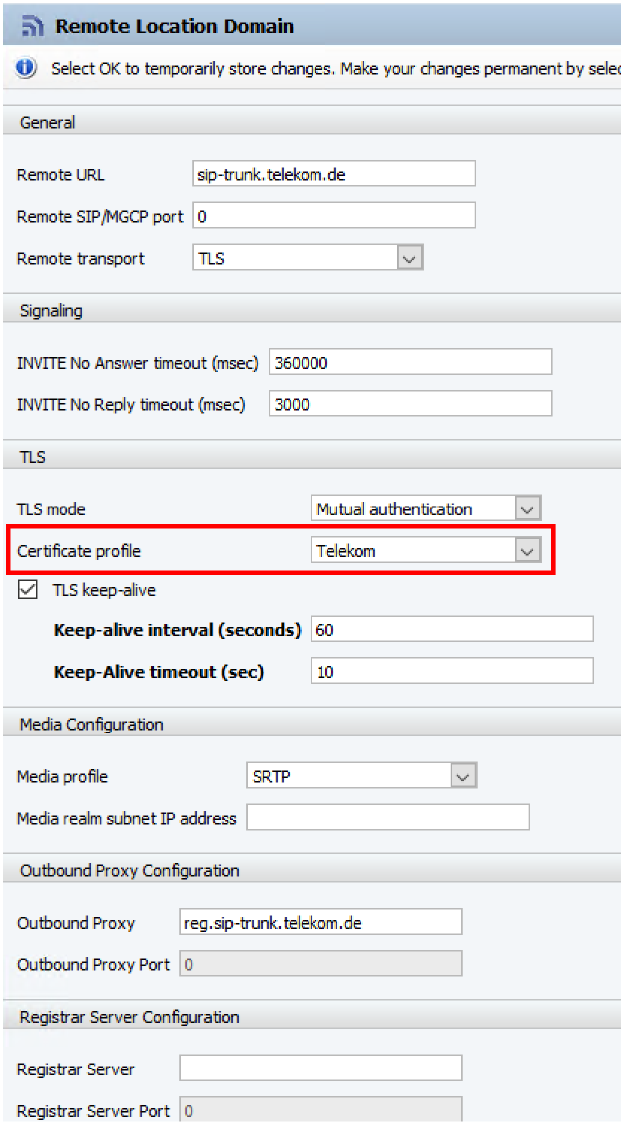
In the *Certificate Profiles* section click on *Add*:


Certificate Management
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.
Media DTLS certificate profile
Certificate Profiles
Add
Edit
Delete
Name
Certificate service
Client certificate file
Server certificate file
Local CA file
OSV Solution
SIP-TLS
servercert.pem
serverCA.pem
HTTPS System Default
HTTPS
server.crt

Create a new Certificate Profile selecting the certificates created before:



Finally the created Certificate Profile has to be configured in the *Remote Location Domain* window:

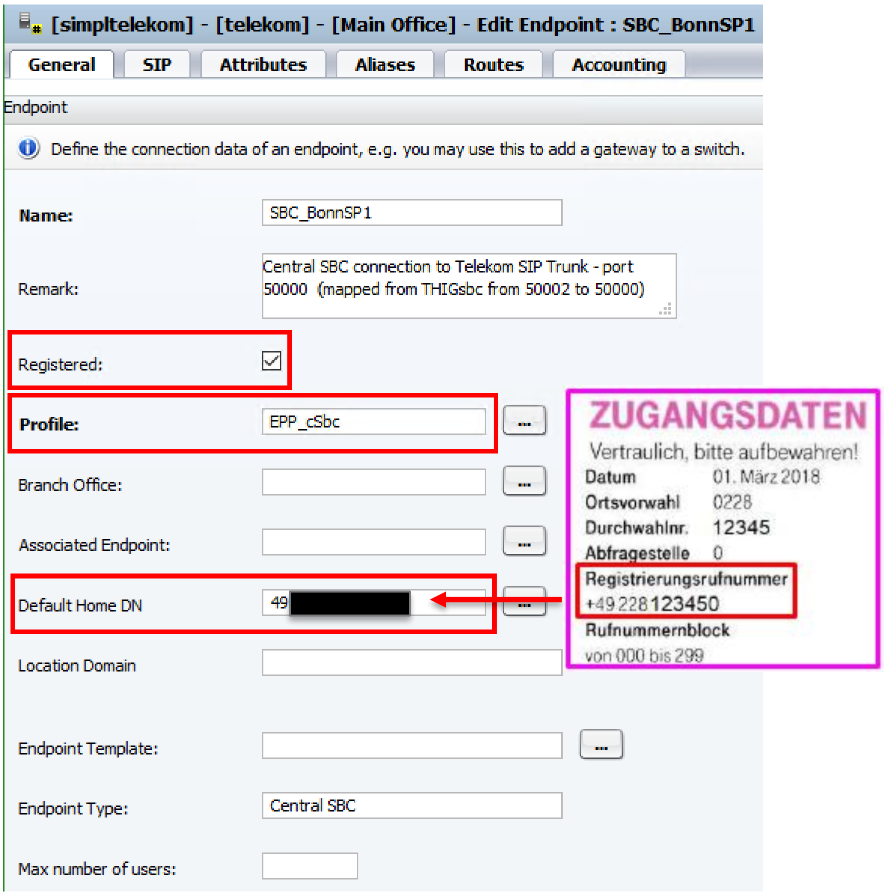


4. OpenScape Voice Configuration

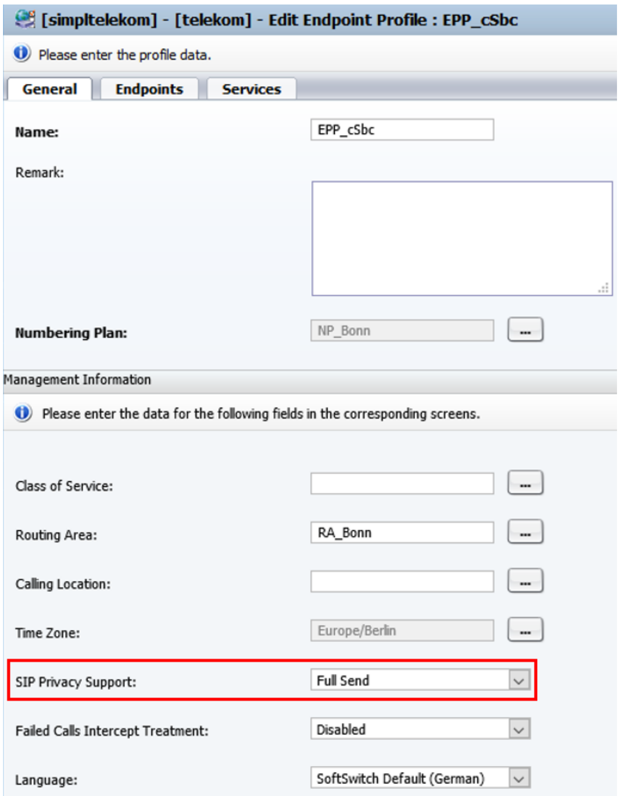
The following configurations are done via Voice Assistant.

4.1. Central SBC Endpoint

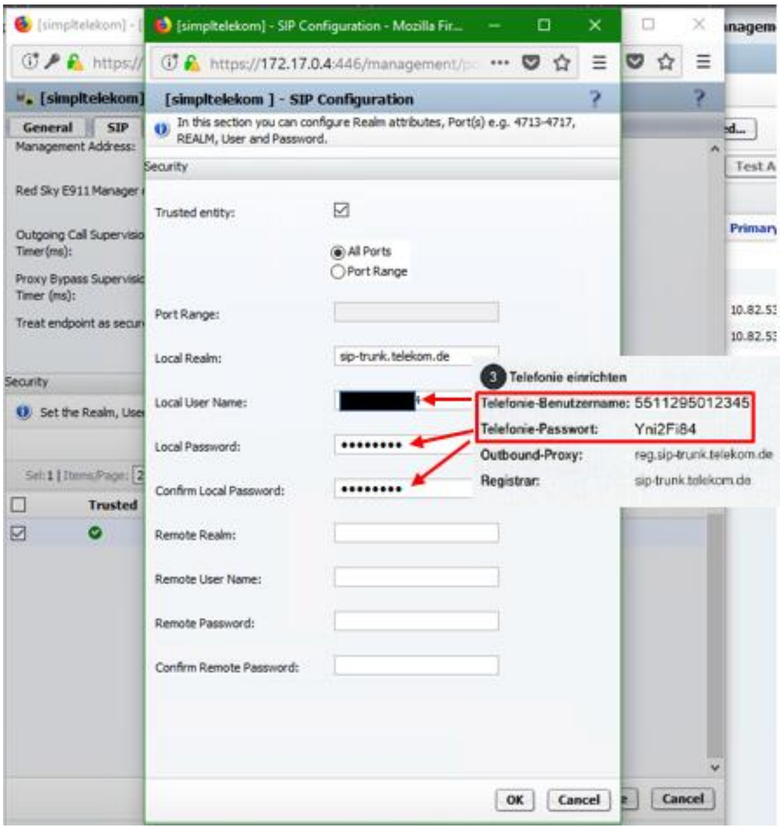
The following figure shows the general settings:



Telekom specifies in INVITEs received over the SIP trunk in the P-Asserted-Identity SIP header the SIP trunk ID which has not to be displayed on the called phone. Therefore *SIP Privacy Support* has to be set to **Full Send** in the SBC Endpoint Profile. This causes the P-Asserted-Identity header to be ignored for incoming calls but supported for outgoing calls.



In the SBC endpoint on tab *SIP* in section *Security* has be configured the telephony authentication credentials to enable Voice to reply to Digest Authentication challenges from Telekom:



The following figures show the SBC endpoint attributes used:

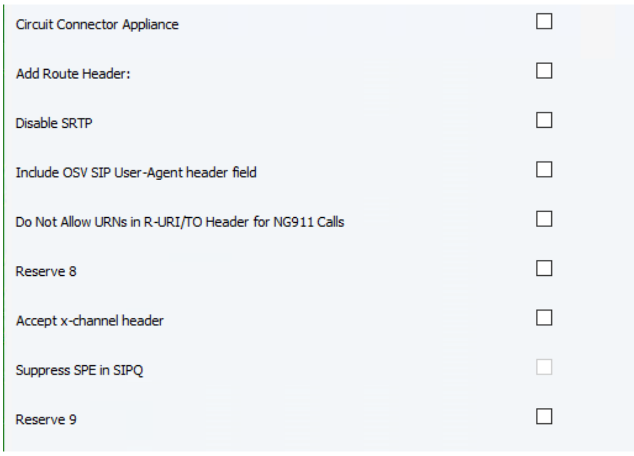
[simpltelekom] - [telekom] - [Main Office] - Edit Endpoint : SBC_BonnSP1

General | SIP | Attributes | Aliases | Routes | Accounting

Attributes

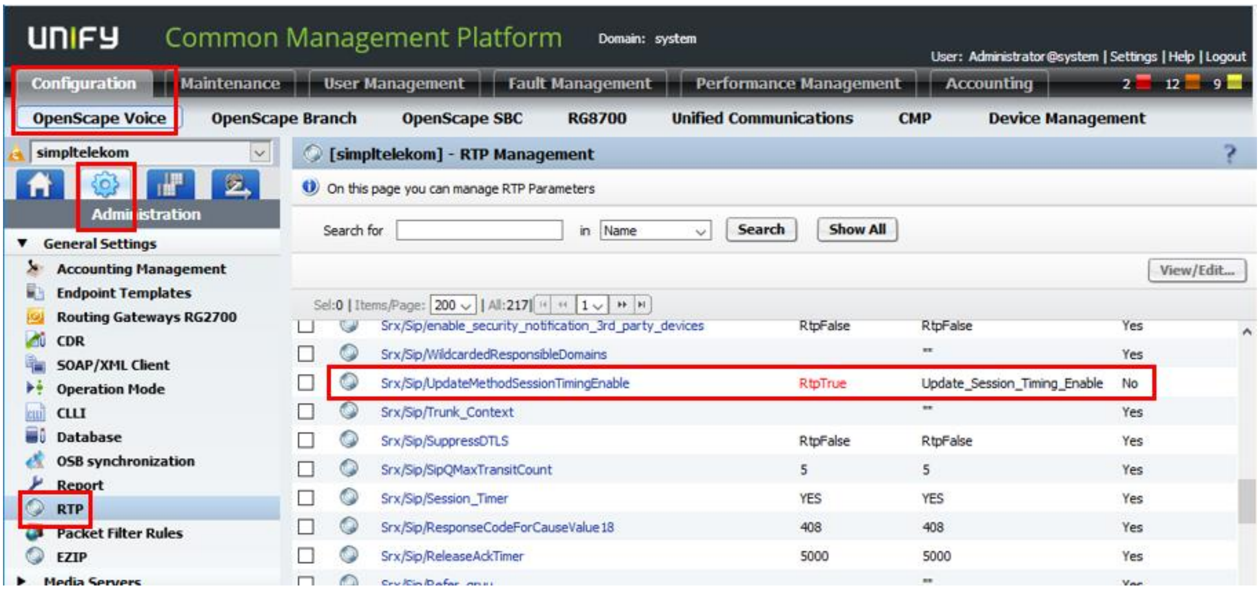
Attributes available for this SIP endpoint

Supports SIP UPDATE Method for Display Updates	☐
UPDATE for Confirmed Dialogs Supported	☐
Survivable Endpoint	☐
SIP Proxy	☐
Central SBC	☐
Route via Proxy	☐
Allow Proxy Bypass	☐
Public/Offnet Traffic	☑
Accept Billing Number	☐
Use Billing Number for Display Purposes	☐
Allow Sending of Insecure Referred-By Header	☐
Override IRM Codec Restriction	☐
Transfer HandOff	☐
Send P-Preferred-Identity rather than P-Asserted-Identity	☐
Send domain name in From and P-Preferred-Identity headers	☐
Send Redirect Number instead of calling number for redirected calls	☐
Do not send Diversion header	☑
Do not Send Invite without SDP	☐
Send International Numbers in Global Number Format (GNF)	☑
Rerouting Direct Incoming Calls	☐
Rerouting Forwarded Calls	☐
Enhanced Subscriber Rerouting	☐
Automatic Collect Call Blocking supported	☐
Send Authentication Number in P-Asserted-Identity header	☑
Send Authentication Number in Diversion Header	☐
Send Authentication Number in From Header	☐
Use SIP Endpoint Default Home DN as Authentication Number	☐
Use Subscriber Home DN as Authentication Number	☐
Set NPI/TON to Unknown	☐
Include Restricted Numbers in From Header	☐
SIPQ Truncated MIME	☐
Enable Session Timer	☑
Ignore Answer for Announcement	☐
Enable TLS RFC5626 Ping	☐
Enable TLS Dual Path Method	☐
Ignore Receipt of 181 Call is Being Forwarded	☐
Use extended max. count for loop prevention	☐
Do Not Audit Endpoint	☐
Use Proxy/SBC ANAT settings for calls to subscribers	☐
Support for Callback Path Reservation	☐
Send Progress to Stop Call Proceeding Supervision Timer	☐
Limited PRACK Support	☐
Support Media Redirection	☐
Voice Mail Server	☐
Disable Long Call Audit	☐
Send/Receive Impact Level	☐
Do not send alphanumeric SIP URI	☐
Send alphanumeric SIP URI when available	☐
Support Peer Domains	☐
Reserve 6	☐
Allow endpoint to Unregister Stale Registrations	☐
Enable Media Termination Point (MTP) Flow	☐
Video call allowed	☐
Trusted Subscriber	☐
Enable Fast Connect	☐



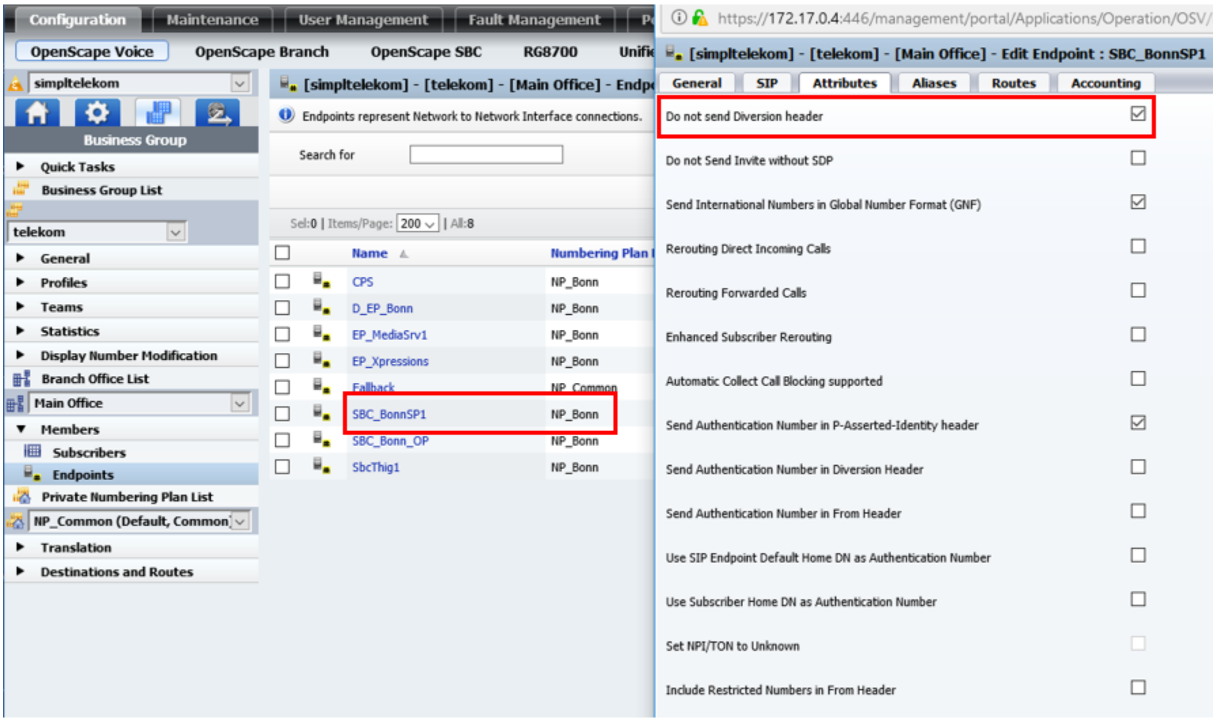
4.2. Avoiding Re-Invite during Session Refresh

When in a long duration call Voice usually send regularly INVITEs to refresh the session. If the SDP o-line version info is different between INVITE and the related 200 OK then Voice detects a change for the session so Voice needs to inform the peer by sending a re-INVITE. To avoid this Voice will send SIP UDPATE messages instead of re-INVITEs by setting the parameter Srx/Sip/UpdateMethodSessionTimingEnable to RtpTrue, as shown below:



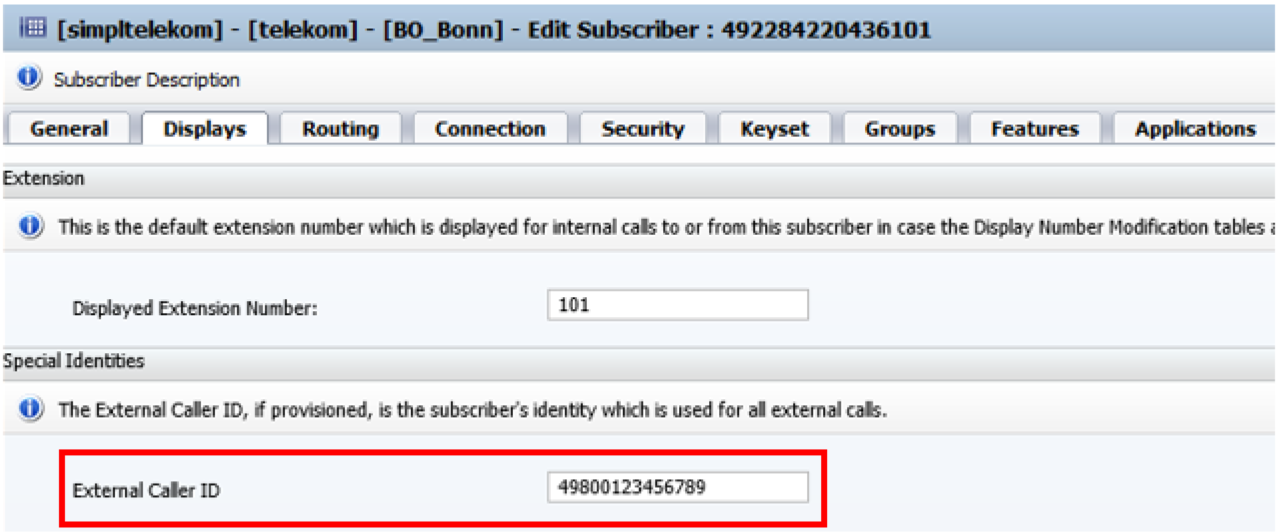
4.3. Disabling to send Diversion SIP Header

Because Telekom doesn't support the Diversion header in SIP messages, sending this header should be prevented in the SIP attributes of the SBC endpoint by enabling *Do not send Diversion header*:



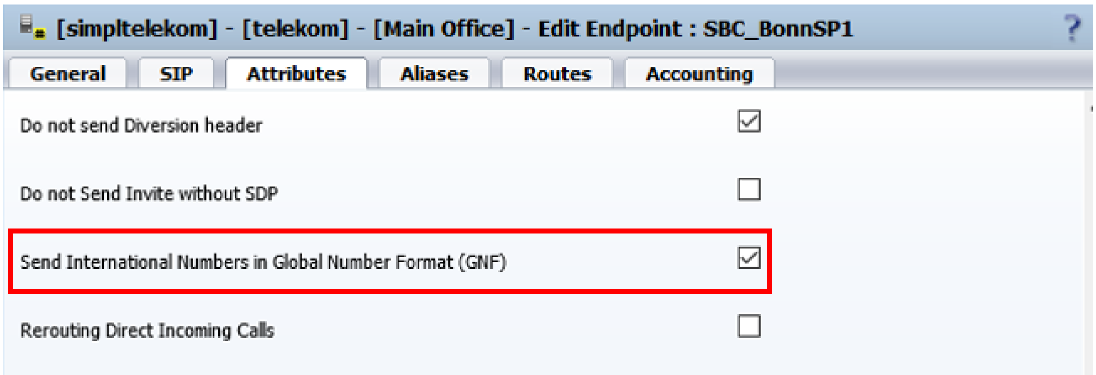
4.4. Sending External Numbers with leading +

In Voice Assistant can be configured any phone number for a subscriber in the *External Caller ID* field to be displayed on a called phone using feature CLIP*:*



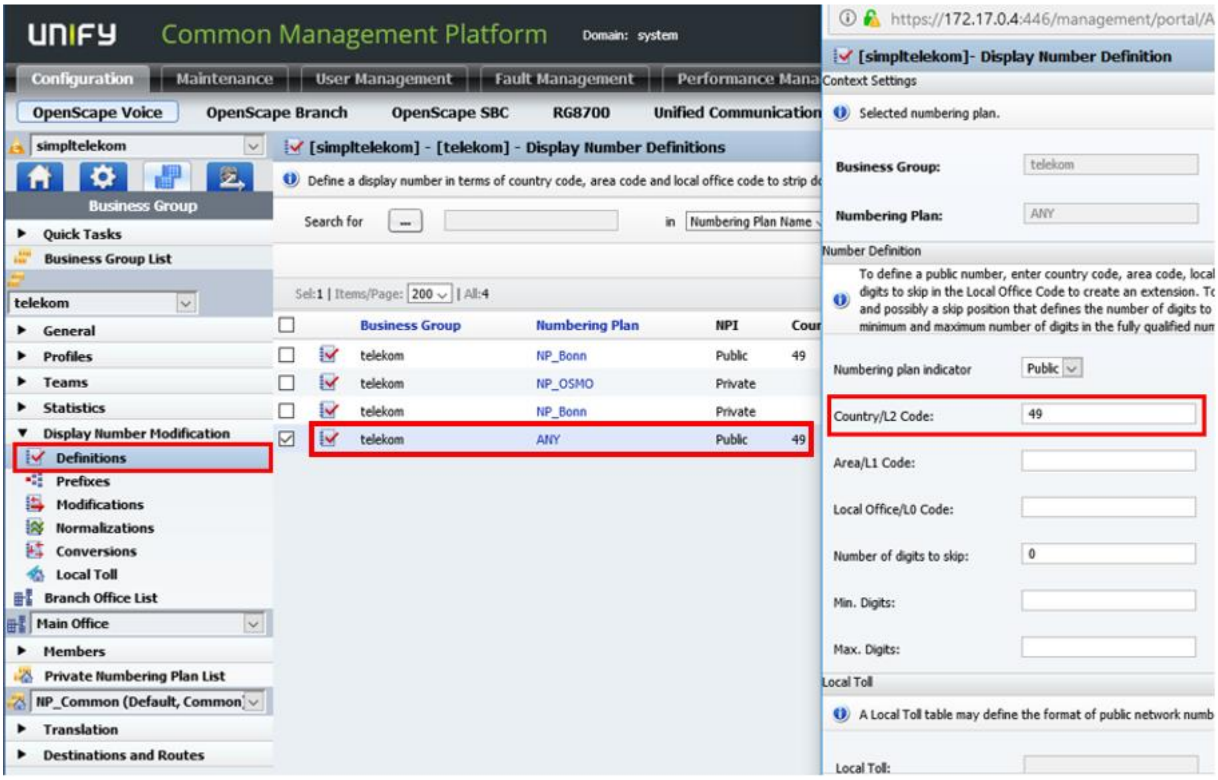
To enable Voice to send this number with a leading + via Central SBC to Telekom two preconditions must be met:

1. In the SBC endpoint must be enabled the attribute *Send International Numbers in Global Number Format (GNF)*:



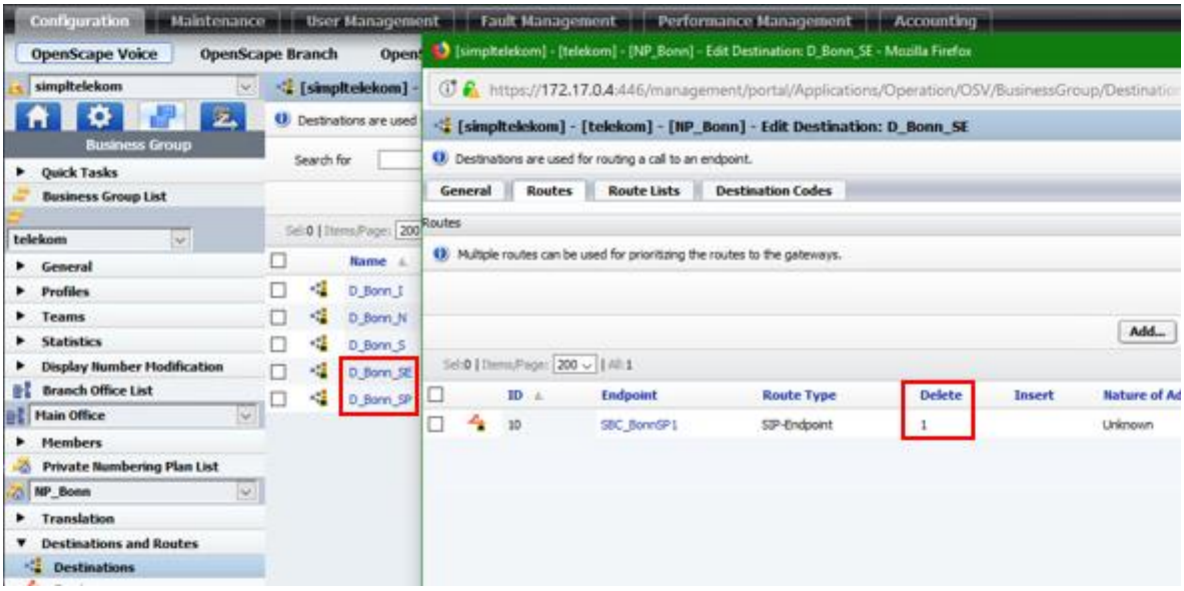
   This cause Voice to send a number in international number format with a leading + sign.

2. To recognize an *External Caller ID* as a number in international format the country code used must be configured as a *Display Number Modification Definition*, as shown for the German country code below:



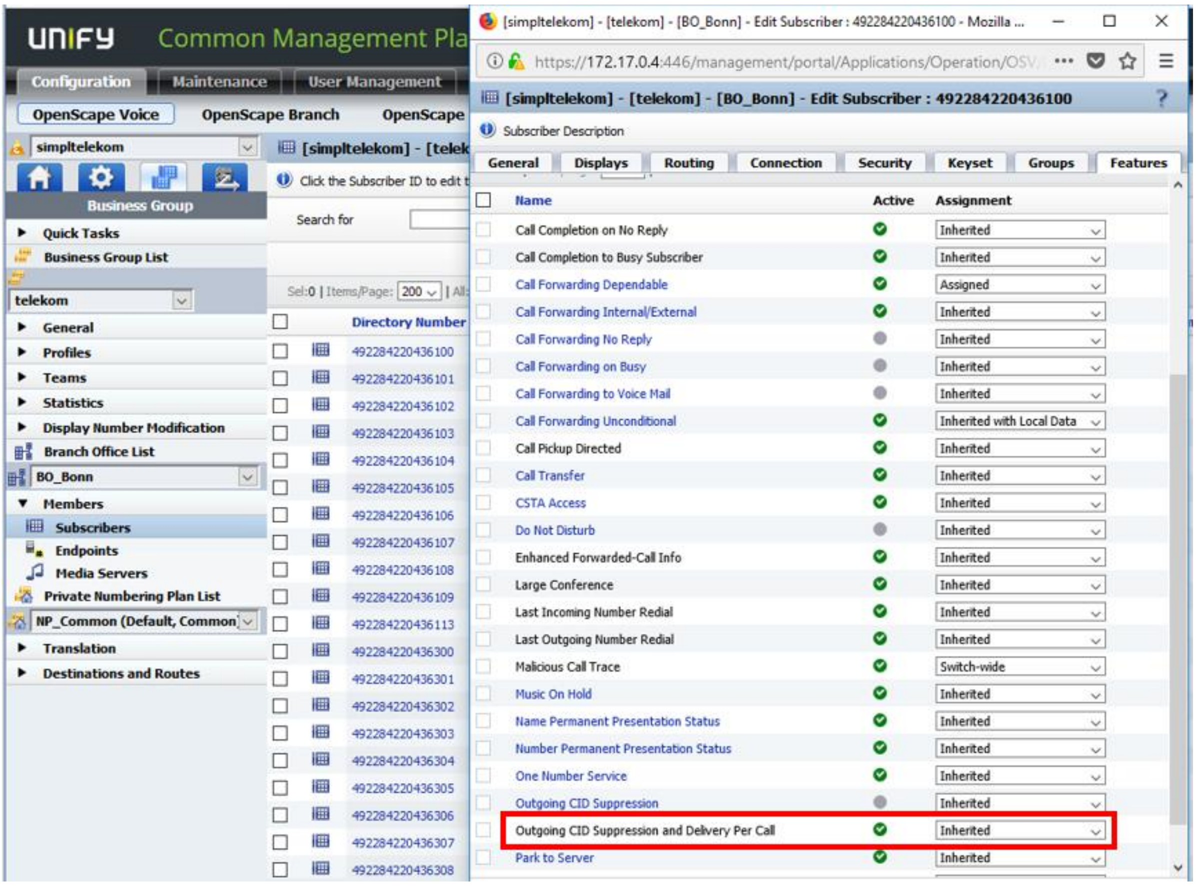
4.5. Sending Special Numbers without leading 0

Unless not already fixed in WebCDC in the Destinations D_xxx_SP for traffic type *Premium Rate* and D_xxx_SE for traffic type *Emergency* in the phone numbering plan in each route must be deleted the leading 0:



4.6. Caller ID Suppression

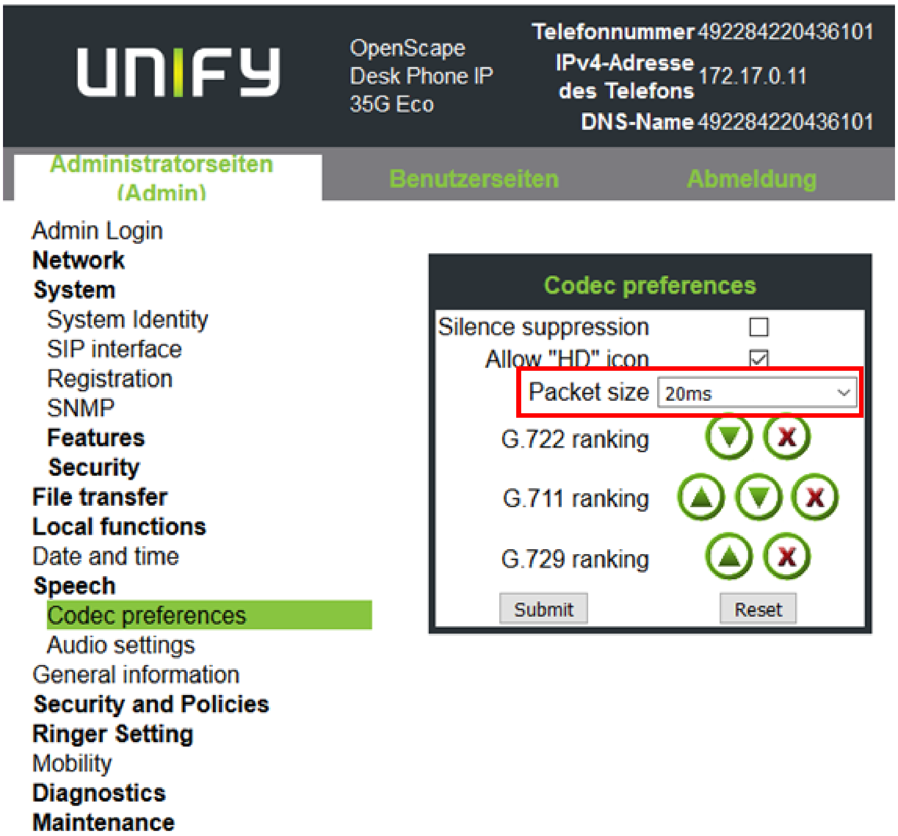
To allow subscribers to use the feature *Caller ID Suppression* the subscribers must be assigned the feature *Outgoing CID suppression and Delivery per Call* by, which is activated by using the prefix *51 by default. This assignment can be done on subscriber level or via Feature Profile.



5. SIP Phones

5.1. Packet Size

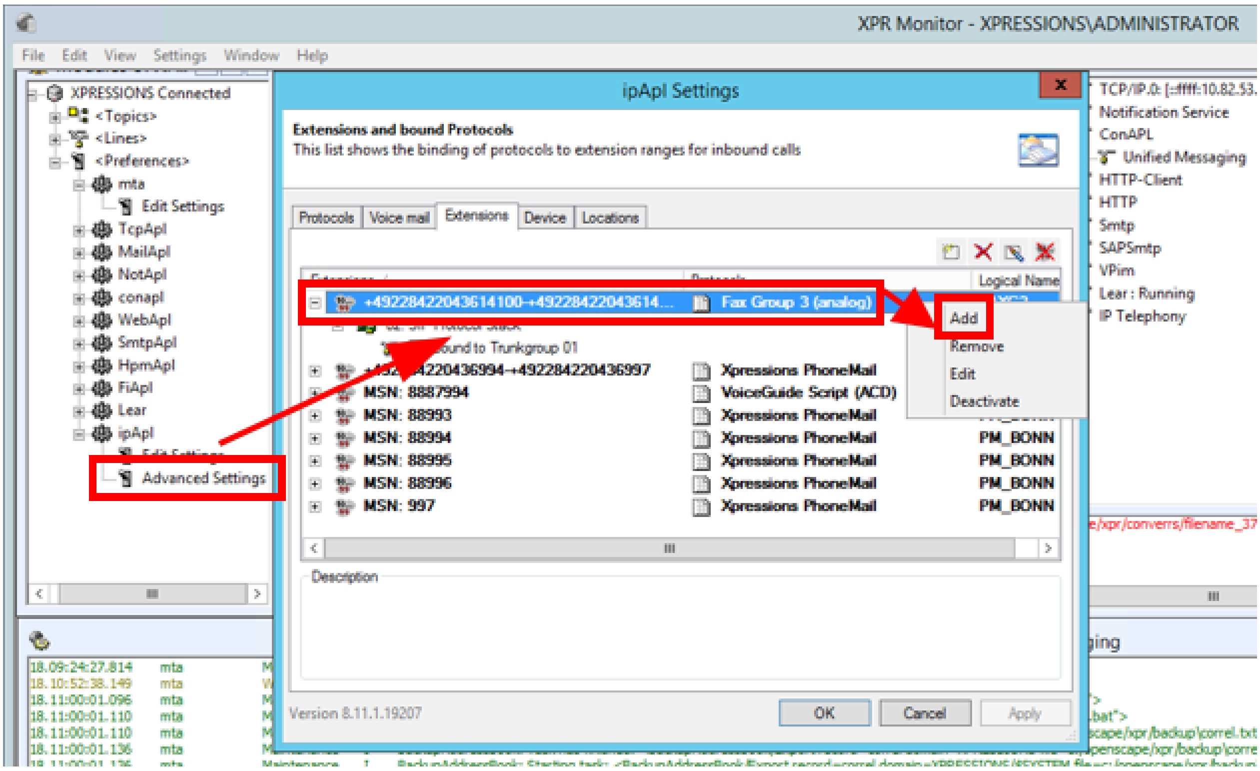
It has to make sure that the Packet Size has to be set to 20 ms on the SIP phones:



6. OpenScape Xpressions

6.1. Adding Extension Range

The Xpressions Extension Range to be added manually:



About Unify

Unify is the Atos brand for communication and collaboration solutions. At the core of the Atos Digital Workplace portfolio, Unify technology enables organizations of all sizes to transform the way they collaborate, creating a more connected and productive workforce which can dramatically improve team performance, individual engagement and business efficiency.

Unify products represent a strong heritage of technology innovation, reliability and flexibility. Their award-winning intuitive user experience can be delivered through almost any device and in any combination of cloud or on-premise deployment. Augmented by Atos' secure digital platforms, vertical solutions and transformation services, they set the global standard for a rich and reliable collaboration experience that empowers teams to deliver extraordinary results.

unify.com

unify
atos collaboration solutions