

Deutsche Telekom

DeutschlandLAN

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

© Unify Communications and Collaboration GmbH & Co. KG

Customer Solution Lab Munich

Version 1.4 – 14th September 2020

The information contained in this document is provided to customers of Unify Communications and Collaboration GmbH & Co. KG for their internal review and distribution only. This information is provided with the understanding that it shall not be copied, reproduced, or otherwise distributed outside of the receiving company without the prior written permission of Unify Communications and Collaboration GmbH & Co. KG.

This document is subject to change by Unify Communications and Collaboration GmbH & Co. KG without notice.

This is a controlled document. Printed copies must have issue number verified prior to each use.



Customer Solution Lab

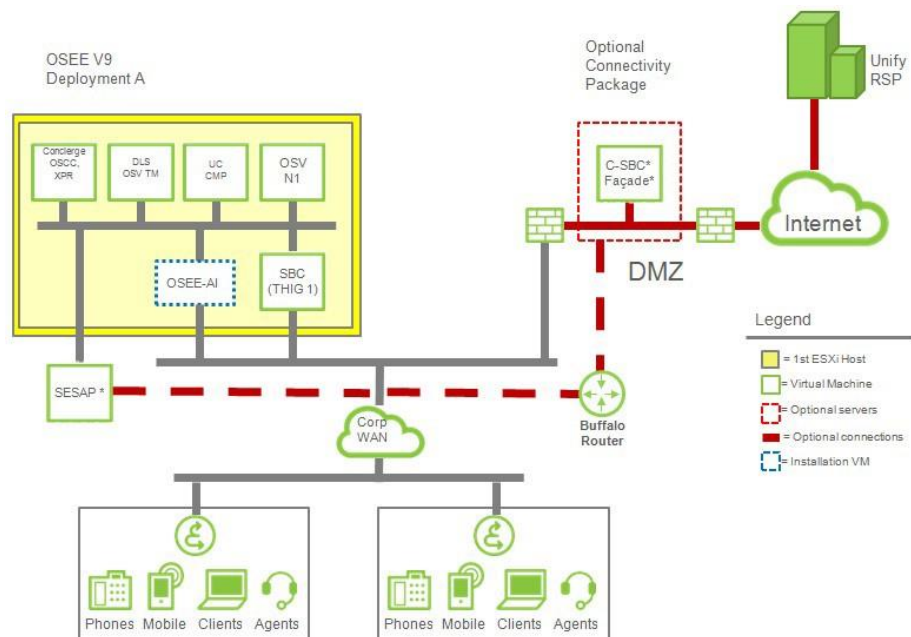
Table of Contents

1. Document Overview	3
1.1. Executive Summary	3
1.2. Document Control	3
1.2.1. Authors of the Document	3
1.2.2. Version / Changes	3
2. OpenScape SBC Configuration	5
2.1. DNS	6
2.2. Quality of Service (QoS)	6
2.3. Media Profile	7
2.4. Remote Endpoint	8
2.7. Preparing and Installing TLS Certificates	13
4. OpenScape Voice Configuration	18
4.1. Central SBC Endpoint	18
4.2. Avoiding Re-Invite during Session Refresh	21
4.3. Disabling to send Diversion SIP Header	22
4.4. Sending External Numbers with leading +	22
4.5. Sending Special Numbers without leading 0	24
4.6. Caller ID Suppression	24
5. SIP Phones	25
5.1. Packet Size	25
6. OpenScape Xpressions	26
6.1. Adding Extension Range	26

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
12 th of March 2018	0.1	Rolf Lang	Initial structure
15 th of May 2018	1.0	Rolf Lang	Released

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



2.1. DNS

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

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP Traffic Shaping QoS

Client

Refresh DNS

DNS server IP address: Add

192.168.1.1

Alias: Add

bonn.telekom.de
sbcbonn.bonn.telekom.de

Server

☐ Enable DNS server

☐ Enable customization

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)

Network/Net Services

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Settings DNS NTP Traffic Shaping QoS

QoS Settings

☒ Enable QoS Configuration

DSCP for SIP: 48

DSCP for MGCP: 48

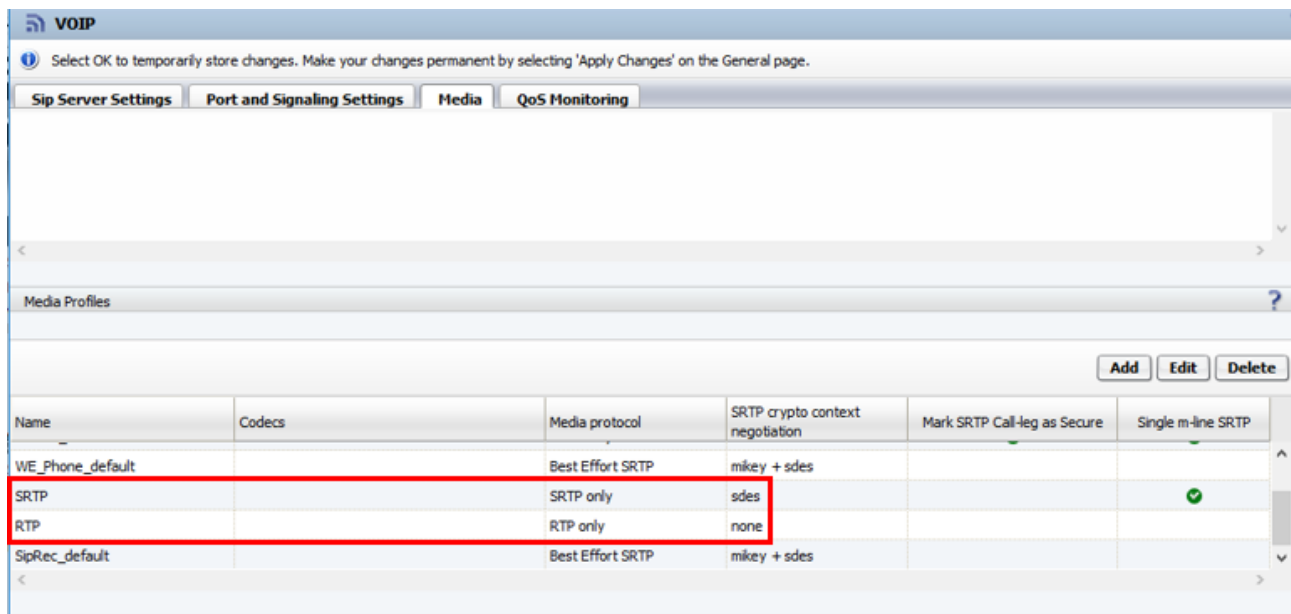
DSCP for RTP (Audio): 46

DSCP for RTP (Video): 46

Row	Protocol	In interface	Out interface
-----	----------	--------------	---------------

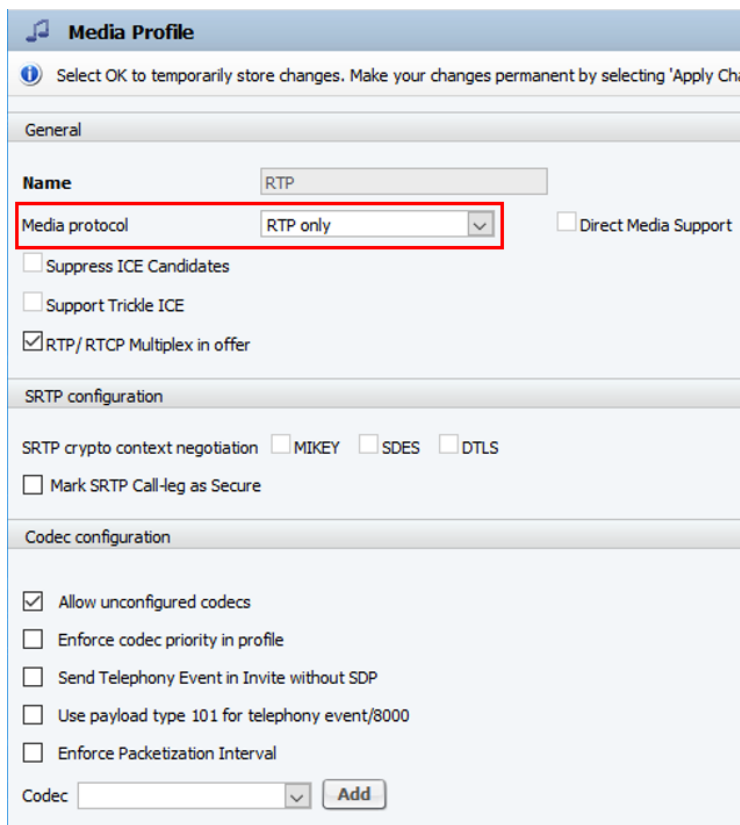
2.3. Media Profile

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



Name	Codecs	Media protocol	SRTP crypto context negotiation	Mark SRTP Call-leg as Secure	Single m-line SRTP
WE_Phone_default		Best Effort SRTP	mikey + sdes		
SRTP		SRTP only	sdes		✓
RTP		RTP only	none		
SipRec_default		Best Effort SRTP	mikey + sdes		

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



Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name: RTP

Media protocol: RTP only

☐ Direct Media Support

☐ Suppress ICE Candidates

☐ Support Trickle ICE

☒ RTP/RTCP Multiplex in offer

SRTP configuration

SRTP crypto context negotiation: ☐ MIKEY ☐ SDES ☐ DTLS

☐ Mark SRTP Call-leg as Secure

Codec configuration

☒ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

☐ Use payload type 101 for telephony event/8000

☐ Enforce Packetization Interval

Codec: Add

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.

Media Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes'.

General

Name: SRTP

Media protocol: SRTP only (highlighted with red box)

☐ Direct Media Support

☐ Suppress ICE Candidates

☐ Support Trickle ICE

☒ RTP/RTCP Multiplex in offer

SRTP configuration

SRTP crypto context negotiation: ☐ MIKEY ☒ SDES ☐ DTLS (highlighted with red box)

☐ Mark SRTP Call-leg as Secure

Codec configuration

☒ Allow unconfigured codecs

☐ Enforce codec priority in profile

☐ Send Telephony Event in Invite without SDP

☐ Use payload type 101 for telephony event/8000

☐ Enforce Packetization Interval

Codec: [] Add

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*:

Features

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes'.

Features configuration

☐ Enable Remote Subscribers Configure

☒ Enable Remote Endpoints Configure (highlighted with red box)

☐ Enable Codec Support for transcoding Configure

☐ Enable TURN Server Configure

☐ Enable Circuit Telephony Connector Configure

☐ Enable Sip Load Balancer Configure

☐ Enable Border Control Function Configure (not licensed)

☐ Enable Push Notification Service Configure

☐ Enable Ganglia Monitoring Daemon

☐ Enable Circuit Zookeeper Client

☐ Enable THIG

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

Remote Endpoints

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

SIP Service Provider Profile

Hostname:
 Remote directory:
 User name:
 Password:

Row	Name	Registration required	Registration interval (sec)
1	DTAGTSystems	<input checked="" type="checkbox"/>	480

Remote endpoint configuration

Row	Name	Access realm profile	Type	Profile / Circuit ID	Remote IP address / Logical-Endpoint-ID / Circuit-URL	Remote port	Remote transport	Associated Endpoint	Core realm profile	Core FQDN	Core realm port	Routing prefix	Default home DN
1	DTAGTSystems	Main-Access-Realm - ipv4	SSP	DTAGTSystems	sip-trunk.telekom.de	0	TLS		Main-Core-Realm - ipv4		50000	+49	

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:

SIP Service Provider Profile

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

General

Name: DTAGSystems Default SSP profile: DTAG/NGN Registration Mode

☒ Use SIP Service Address for all identity headers

SIP service address: sip-trunk.telekom.de

SIP User Agent

SIP User Agent towards SSP: Passthru SIP User Agent:

Registration

☒ Registration required

Registration interval (sec): 480

Business Identity

☐ Business identity required

Business identity DN:

Outgoing SIP manipulation

☐ Insert anonymous caller ID for blocked Caller-ID

Manipulation

Flags

☐ FQDN in TO header to SSP

☐ Use To DN to populate the RURI

☐ Send Default Home DN in Contact for Call messages

☐ Allow SDP changes from SSP without session version update

☐ Do not send INVITE with sendonly media attribute

☐ Do not send INVITE with video media line

☐ Do not send Invite without SDP

☐ Do not send Re-Invite when no media type change

☐ Do not send Re-Invite

☐ Remove Silence Suppression parameter from SDP

☐ Enable pass-through of Optional parameters

☐ Force direction attribute to sendrcv

☐ Send default Home DN in PAI/PPI

☐ Preserve To and From headers per RFC2543

☐ Allow single SSP with different home DN prefix based handling

☐ Ignore last digit in Default home DN for incoming calls from SIP trunk

TLS

TLS Signaling: Endpoint Config

Sip Connect

☐ Use tel URI

☒ Send user=phone in SIP URI

☒ Registration mode

☒ 1TR118

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

Remote endpoint configuration

Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.

Remote Endpoint Settings

Name: DTAGSystems Edit

Type: SSP

Profile: DTAGSystems

Access realm profile: Main-Access-Realm - ipv4

Core realm profile: Main-Core-Realm - ipv4

Associated Endpoint:

☐ Enable Call Limits

Maximum Permitted Calls: 0

Reserved Calls: 0

Remote Location Information

☐ URI based routing

☐ Enable access control

Signaling address type: DNS SRV

Remote Location domain list

Row	Remote URL	Remote SIP/MGCP port	Remote transport	Media IP	Media profile	TLS mode	Certificate profile	TLS keep-alive	Keep-alive interval (seconds)	Keep-alive timeout (sec)	INVITE No Answer timeout (msec)	INVITE No Reply timeout (msec)	Outbound Proxy	Outbound Proxy Port	Registrar Server	Registrar Server Port
1	sip-trunk.telekom.de	0	TLS		SRTP	Mutual authentication	Telekom	<input checked="" type="checkbox"/>	60	10	360000	3000	reg.sip-trunk.telekom.de	0		0

Remote Location Identification/Routing

Core FQDN:

Core realm port: 50000

Default core realm location domain name:

Routing prefix:

Default home DN: +49 [redacted]

Digest Authentication

☒ Digest authentication supported

Digest authentication realm: sip-trunk.telekom.de

Digest authentication user ID: [redacted]

Digest authentication password: [redacted]

Access Side Firewall Settings

☐ Enable Firewall Settings Firewall Settings

Emergency configuration

Emergency numbers: Add

Delete

Emergency call routing

MSRP Data Configuration

☐ Enable MSRP Relay Support (not licensed)

☒ use IP address in MSRP-path

☐ use FQDN in MSRP-path

FQDN:

☒ Authentication required

Realm:

Password: Show

☐ Access side only

Qop: AUTH

Expire time/sec: 300

Miscellaneous

☒ Open external firewall pinhole

OK Cancel

ZUGANGSDATEN

Vertraulich, bitte aufbewahren!

Datum 01. März 2018

Ortsvorwahl 0228

Durchwahlnr. 12345

Abfragestelle 0

Registrierungsrufnummer +49 228 123450

Rufnummernblock von 000 bis 299

2 Internet-Zugang einrichten

Anschlusskennung: 002529106948

Zugangsnummer: 5511295012345
(vormals T-Online Nummer)

Mitbenutzernummer: 0001

Persönliches Kennwort: 25170493

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:

Remote Location Domain

Select OK to temporarily store changes. Make your changes permanent by selecting 'OK'.

General

Remote URL: sip-trunk.telekom.de

Remote SIP/MGCP port: 0

Remote transport: TCP

Signaling

INVITE No Answer timeout (msec): 360000

INVITE No Reply timeout (msec): 3000

TLS

TLS mode: Mutual authentication

Certificate profile: Telekom

☐ TLS keep-alive

Keep-alive interval (seconds): 60

Keep-Alive timeout (sec): 10

Media Configuration

Media profile: RTP

Media realm subnet IP address:

Outbound Proxy Configuration

Outbound Proxy: reg.sip-trunk.telekom.de

Outbound Proxy Port: 0

Registrar Server Configuration

Registrar Server:

Registrar Server Port: 0

Remote Location Domain

Select OK to temporarily store changes. Make your changes permanent by selecting 'OK'.

General

Remote URL: sip-trunk.telekom.de

Remote SIP/MGCP port: 0

Remote transport: TLS

Signaling

INVITE No Answer timeout (msec): 360000

INVITE No Reply timeout (msec): 3000

TLS

TLS mode: Mutual authentication

Certificate profile: Telekom

☒ TLS keep-alive

Keep-alive interval (seconds): 60

Keep-Alive timeout (sec): 10

Media Configuration

Media profile: SRTP

Media realm subnet IP address:

Outbound Proxy Configuration

Outbound Proxy: reg.sip-trunk.telekom.de

Outbound Proxy Port: 0

Registrar Server Configuration

Registrar Server:

Registrar Server Port: 0

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:

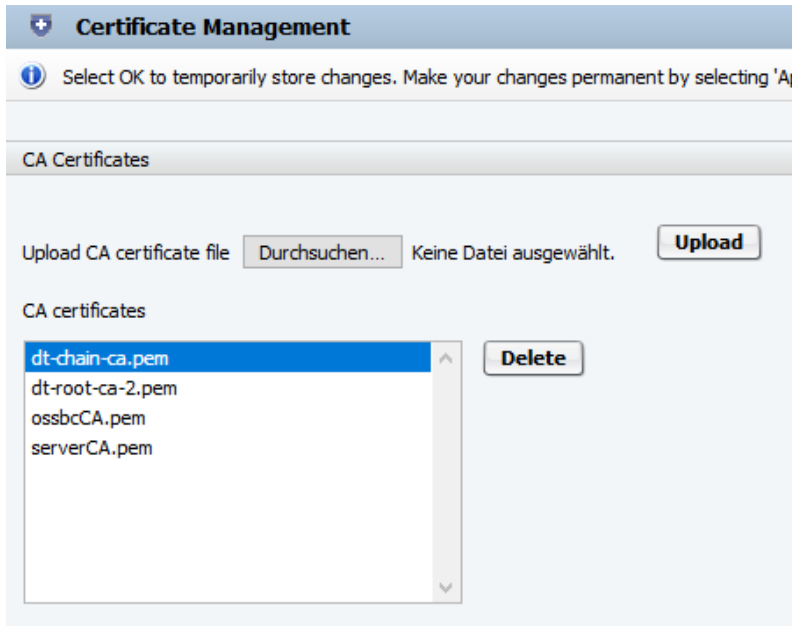
```
-----BEGIN CERTIFICATE-----
<dt-root-ca-2.cer>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
< T-TeleSec_GlobalRoot_Class_2.cer>
-----END CERTIFICATE-----
```

Then the chained certificate should look like as below:

```
-----BEGIN CERTIFICATE-----
MIIGiTCCBXGgAwIBAgIIMBWLWM1WMfUwDQYJKoZIhvcNAQELBQAwTELMAkGA1UE
...
nfKouiXc6eG1ojopwck0/uEu0JVEHyM0zGoIPU2/PhFvG6aAPsB4tvv/AHzR
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

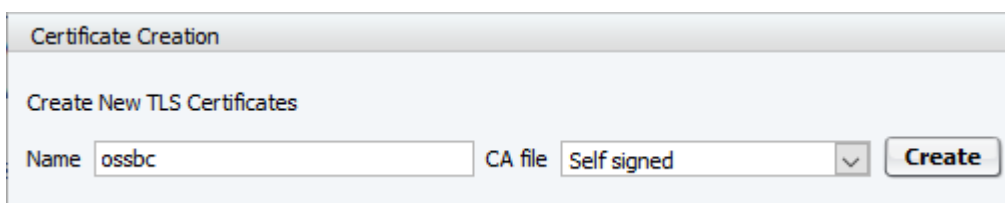
```
MIIDnzCCAoegAwIBAgIBJjANBgkqhkiG9w0BAQUFADBxMQswCQYDVQQGEWJERTec
...
Cm26OWMohpLzGITY+9HPBVZkVw==
-----END CERTIFICATE-----
```

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:

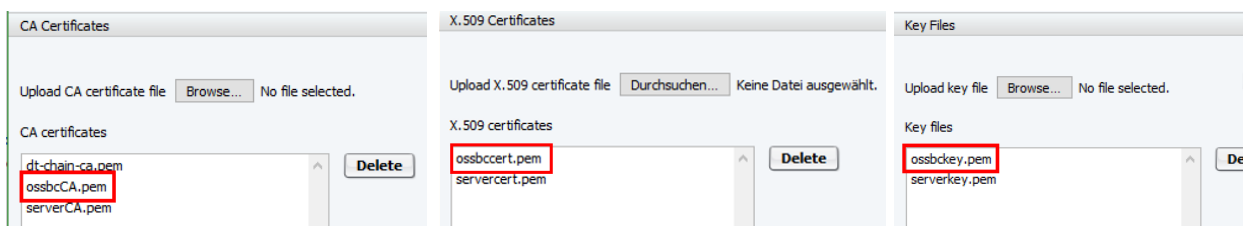


To replace the OpenScape SBC default certificates provided by installation execute the following steps:

The in *Certificate Creation* section enter e.g. ossbc in the *Name* field and 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	Remote 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:

Certificate Profile

Select OK to temporarily store changes. Make your changes permanent by selecting the OK button.

Certificate profile name

Certificate service

Local client certificate file

Local server certificate file

Local CA file

Remote CA file

Local key file

EC param

Attach to Config file ☐

Validation

Certificate Verification

☒ Revocation status

☒ Identity Check

Renegotiation

☐ Enforce TLS session renegotiation

TLS session renegotiation interval (minutes)

TLS version

Minimum TLS version

DTLS version

Minimum DTLS version

Cipher Suites

Perfect Forward Secrecy

Encryption

Mode of Operation

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

Remote Location Domain

Select OK to temporarily store changes. Make your changes permanent by selecting OK and Save.

General

Remote URL: sip-trunk.telekom.de

Remote SIP/MGCP port: 0

Remote transport: TLS

Signaling

INVITE No Answer timeout (msec): 360000

INVITE No Reply timeout (msec): 3000

TLS

TLS mode: Mutual authentication

Certificate profile: Telekom

☒ TLS keep-alive

Keep-alive interval (seconds): 60

Keep-Alive timeout (sec): 10

Media Configuration

Media profile: SRTP

Media realm subnet IP address:

Outbound Proxy Configuration

Outbound Proxy: reg.sip-trunk.telekom.de

Outbound Proxy Port: 0

Registrar Server Configuration

Registrar Server:

Registrar Server Port: 0

4. OpenScape Voice Configuration

The following configurations are done via Voice Assistant.

4.1. Central SBC Endpoint

The following figure shows the general settings:

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

General SIP Attributes Aliases Routes Accounting

Endpoint

Define the connection data of an endpoint, e.g. you may use this to add a gateway to a switch.

Name: SBC_BonnSP1

Remark: Central SBC connection to Telekom SIP Trunk - port 50000 (mapped from THIGsbc from 50002 to 50000)

Registered: ☒

Profile: EPP_cSbc

Branch Office:

Associated Endpoint:

Default Home DN: 49 [redacted]

Location Domain:

Endpoint Template:

Endpoint Type: Central SBC

Max number of users:

ZUGANGSDATEN

Vertraulich, bitte aufbewahren!

Datum 01. März 2018

Ortsvorwahl 0228

Durchwahlr. 12345

Abfragestelle 0

Registrierungsrufnummer
+49 228 123450

Rufnummernblock
von 000 bis 299

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.

[simptelekom] - [telekom] - Edit Endpoint Profile : EPP_cSbc

Please enter the profile data.

General | Endpoints | Services

Name: EPP_cSbc

Remark:

Numbering Plan: NP_Bonn

Management Information

Please enter the data for the following fields in the corresponding screens.

Class of Service:

Routing Area: RA_Bonn

Calling Location:

Time Zone: Europe/Berlin

SIP Privacy Support: Full Send

Failed Calls Intercept Treatment: Disabled

Language: SoftSwitch Default (German)

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:

[simptelekom] - SIP Configuration

In this section you can configure Realm attributes, Port(s) e.g. 4713-4717, REALM, User and Password.

Security

Trusted entity: ☒

☒ All Ports
☐ Port Range

Port Range:

Local Realm: sip-trunk.telekom.de

Local User Name: [masked]

Local Password: [masked]

Confirm Local Password: [masked]

Remote Realm:

Remote User Name:

Remote Password:

Confirm Remote Password:

Outbound-Proxy: reg.sip-trunk.telekom.de

Registrar: sip-trunk.telekom.de

3 Telefonie einrichten

Telefonie-Benutzername: 5511295012345

Telefonie-Passwort: Yni2Fi84

OK Cancel

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

Circuit Connector Appliance	<input type="checkbox"/>
Add Route Header:	<input type="checkbox"/>
Disable SRTP	<input type="checkbox"/>
Include OSV SIP User-Agent header field	<input type="checkbox"/>
Do Not Allow URNs in R-URI/TO Header for NG911 Calls	<input type="checkbox"/>
Reserve 8	<input type="checkbox"/>
Accept x-channel header	<input type="checkbox"/>
Suppress SPE in SIPQ	<input type="checkbox"/>
Reserve 9	<input type="checkbox"/>

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 UPDATE messages instead of re-INVITEs by setting the parameter Srx/Sip/UpdateMethodSessionTimingEnable to RtpTrue, as shown below:

The screenshot shows the Unify Common Management Platform interface. The 'Configuration' tab is selected, and the 'OpenScope Voice' section is active. The 'RTP Management' page is displayed, showing a list of parameters. The parameter 'Srx/Sip/UpdateMethodSessionTimingEnable' is highlighted with a red box, and its value is set to 'RtpTrue'.

Parameter	RtpFalse	RtpTrue	Update_Session_Timing_Enable	Yes
Srx/Sip/enable_security_notification_3rd_party_devices	RtpFalse	RtpFalse	Yes	Yes
Srx/Sip/WildcardedResponsibleDomains		**	Yes	Yes
Srx/Sip/UpdateMethodSessionTimingEnable	RtpTrue	Update_Session_Timing_Enable	No	
Srx/Sip/Trunk_Context		**	Yes	Yes
Srx/Sip/SuppressDTLS	RtpFalse	RtpFalse	Yes	Yes
Srx/Sip/SipQMaxTransitCount	5	5	Yes	Yes
Srx/Sip/Session_Timer	YES	YES	Yes	Yes
Srx/Sip/ResponseCodeForCauseValue18	408	408	Yes	Yes
Srx/Sip/ReleaseAckTimer	5000	5000	Yes	Yes

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*.

The screenshot shows the OpenScope management portal interface. The left sidebar contains navigation menus for 'Business Group', 'Main Office', 'Members', 'Subscribers', 'Endpoints', and 'Private Numbering Plan List'. The main content area displays a list of endpoints under the heading 'Endpoints represent Network to Network Interface connections.' The endpoint 'SBC_BonnSP1' is highlighted with a red box. To the right, the 'SIP' tab is selected, showing various SIP attributes. The attribute 'Do not send Diversion header' is checked, indicated by a red box. Other attributes like 'Do not Send Invite without SDP', 'Send International Numbers in Global Number Format (GNF)', and 'Send Authentication Number in P-Asserted-Identity header' are also visible.

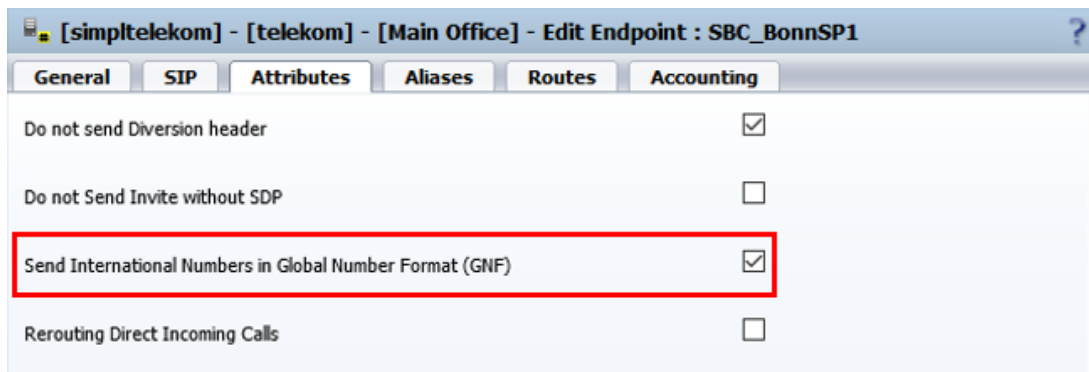
4.4. Sending External Numbers with leading +

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:

The screenshot shows the 'Edit Subscriber' configuration page for subscriber 492284220436101. The 'Routing' tab is selected. The 'Extension' section shows the 'Displayed Extension Number' as 101. The 'Special Identities' section shows the 'External Caller ID' field, which is highlighted with a red box and contains the value 49800123456789. The page includes tabs for 'General', 'Displays', 'Routing', 'Connection', 'Security', 'Keyset', 'Groups', 'Features', and 'Applications'.

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)*:



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

General SIP Attributes Aliases Routes Accounting

Do not send Diversion header ☒

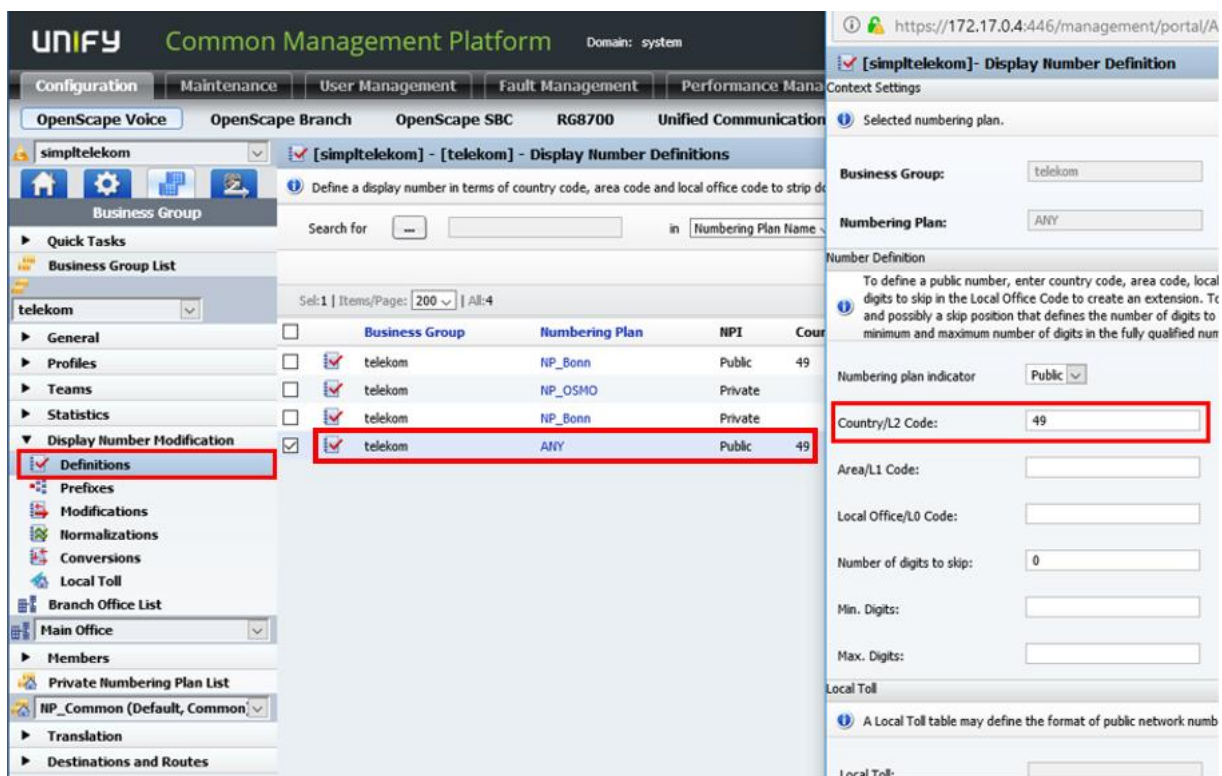
Do not Send Invite without SDP ☐

Send International Numbers in Global Number Format (GNF) ☒

Rerouting Direct Incoming Calls ☐

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:



UNIFY Common Management Platform Domain: system

Configuration Maintenance User Management Fault Management Performance Management

OpenScape Voice OpenScape Branch OpenScape SBC RG8700 Unified Communication

[simpltelekom] - [telekom] - Display Number Definitions

Define a display number in terms of country code, area code and local office code to strip digits

Business Group: telekom

Search for: in: Numbering Plan Name

Set: 1 | Items/Page: 200 | All: 4

Business Group	Numbering Plan	NPI	Country Code
telekom	NP_Bonn	Public	49
telekom	NP_OSMO	Private	
telekom	NP_Bonn	Private	
telekom	ANY	Public	49

Number Definition

To define a public number, enter country code, area code, local digits to skip in the Local Office Code to create an extension. To and possibly a skip position that defines the number of digits to minimum and maximum number of digits in the fully qualified number

Numbering plan indicator: Public

Country/L2 Code: 49

Area/L1 Code:

Local Office/L0 Code:

Number of digits to skip: 0

Min. Digits:

Max. Digits:

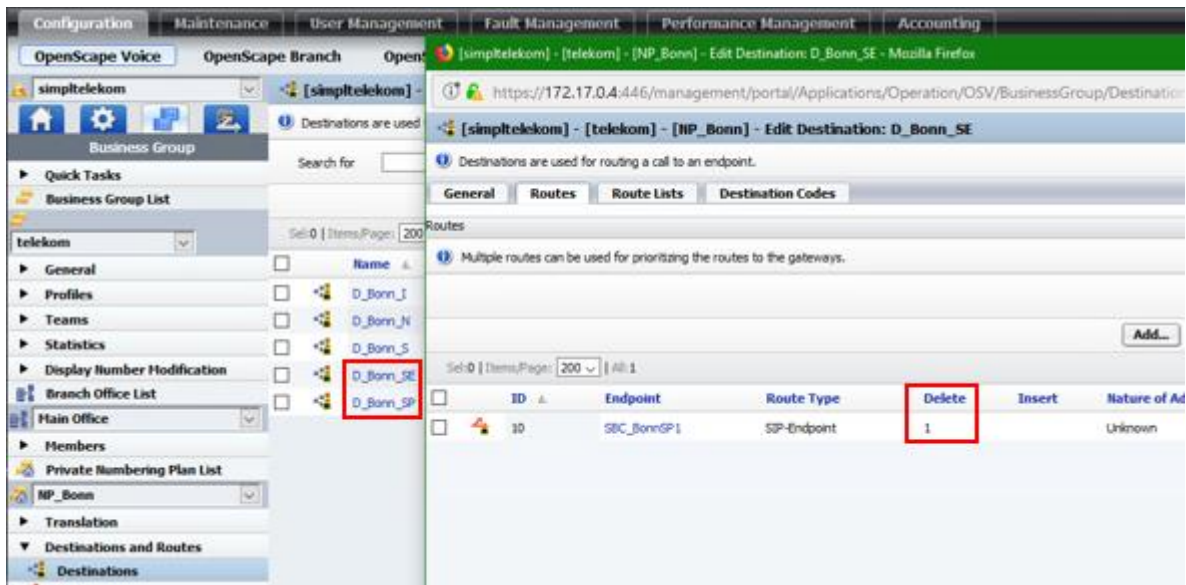
Local Toll

A Local Toll table may define the format of public network number

Local Toll:

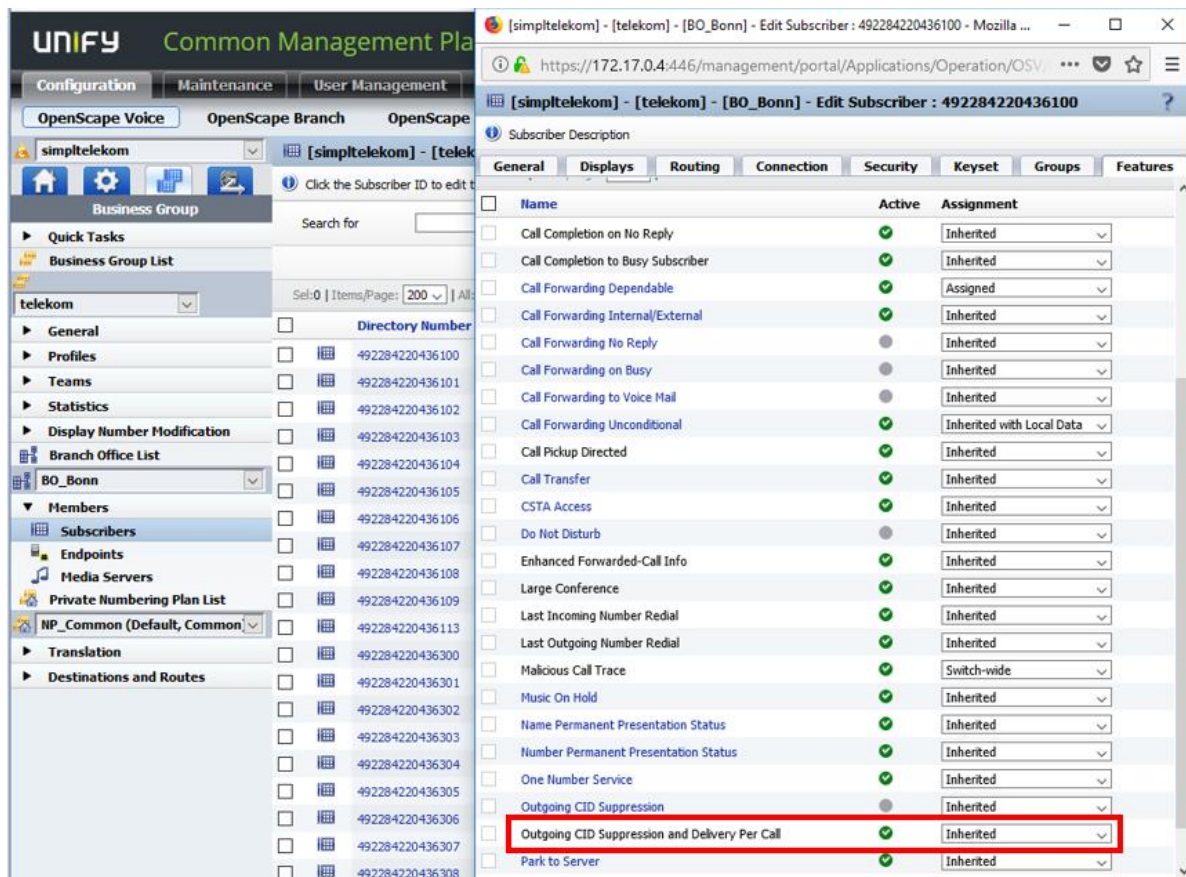
4.5. Sending Special Numbers without leading 0

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*, 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

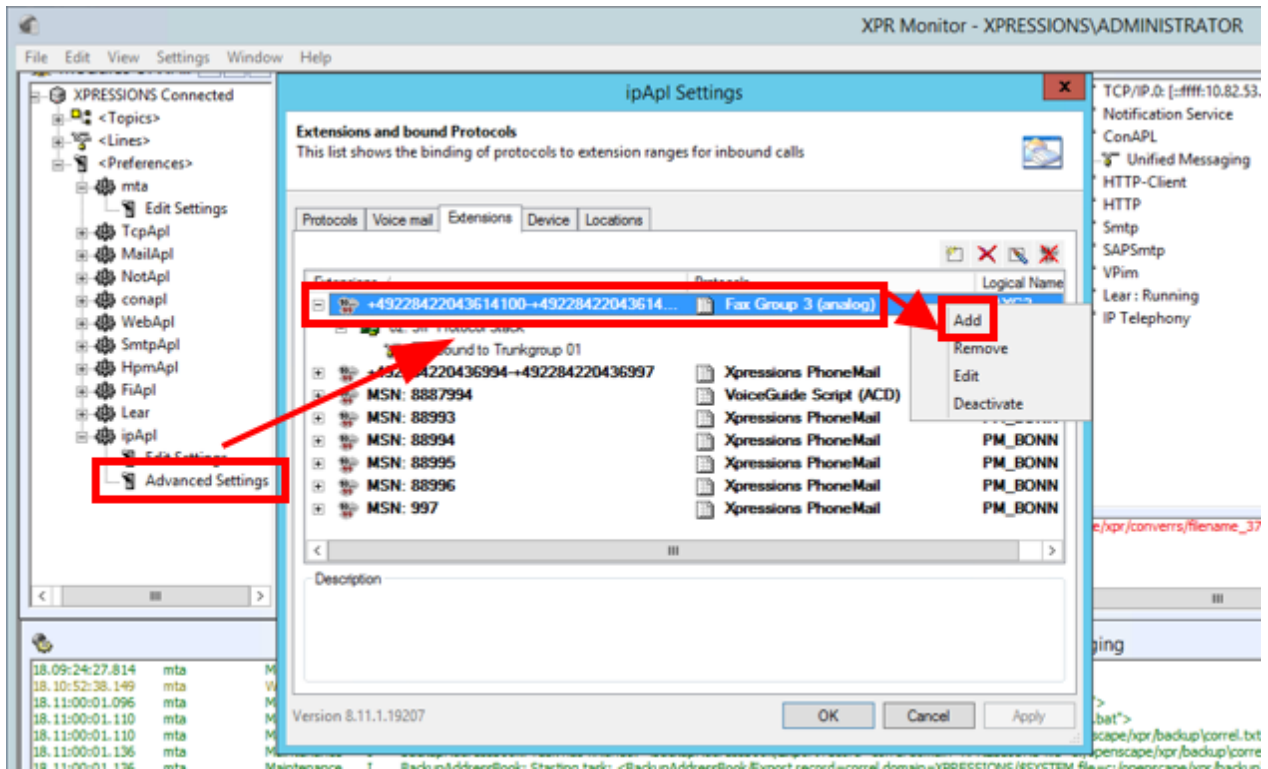
It has to make sure that the Packet Size has to be set to 20 ms on the SIP phones:

The screenshot displays the Unify OpenScape administration interface. At the top, the 'UNIFY' logo is on the left, and system information is on the right: 'OpenScape Desk Phone IP 35G Eco', 'Telefonnummer 492284220436101', 'IPv4-Adresse des Telefons 172.17.0.11', and 'DNS-Name 492284220436101'. Below this is a navigation bar with 'Administratorseiten (Admin)' (highlighted), 'Benutzerseiten', and 'Abmeldung'. The left sidebar lists various configuration categories: Admin Login, Network, System, Features, Security, File transfer, Local functions, Date and time, Speech (highlighted), and Maintenance. Under 'Speech', 'Codec preferences' is selected and highlighted in green. The main content area shows the 'Codec preferences' window. It includes a 'Silence suppression' checkbox (unchecked), an 'Allow "HD" icon' checkbox (checked), and a 'Packet size' dropdown menu set to '20ms' (highlighted with a red rectangle). Below these are three ranking sections: 'G.722 ranking' with a down arrow and a red X; 'G.711 ranking' with up, down, and red X arrows; and 'G.729 ranking' with an up arrow and a red X. At the bottom of the window are 'Submit' and 'Reset' buttons.

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



Copyright © Unify Software and Solutions GmbH & Co. KG, 2020
All rights reserved.

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.