

OpenScape 4000
OpenScape SBC



How to Configure
htp Business FleX SIP-Trunk smart
of htp GmbH

Table of Contents

Trunk Configuration Data provided by htp	4
OpenScape 4000 Configuration.....	5
WBM Configuration for htp Native SIP Trunk - Gateway Properties.....	8
WBM Configuration for htp Native SIP Trunk - SIP Parameters	9
WBM Configuration for htp Native SIP Trunk - Codec Parameters.....	11
SIP trunk Profile:	12
OpenScape SBC Configuration	13
Core Realm Interface	13
SIP Server	14
Certificates	14
Media Profile	17
Codec Manipulation Options	17
Remote Endpoints	21
SIP Provider Profile	23
Restrictions and Remarks	29
Remarks.....	29
Restrictions.....	30
Known Issues.....	31

Table of History

Date	Version	Changes
17.11.2022	1.0	Initial version

Trunk Configuration Data provided by htp

The SIP trunk configuration data (IP addresses etc.) needed to setup the SIP trunk can be found in the htp interconnection document provided by htp.

(<https://www.htp.net>)

OpenScope 4000 Configuration

In this section the typical AMO (Administration and Maintenance Order) commands to create a native SIP trunk between htp SSP and OS4000 vHG board will be described as an example.

See also OpenScope 4000 Service Documentation – IP Solutions

The AMO commands are executed through ComWin application that interfaces to OS4000's database.

Add function block for vHG board:

```
ADD-BFDAT:FCTBLK=6,FUNCTION=HG3550,BRDBCHL=BCHL120,ATTR=SOCO;
CHANGE-BFDAT:CONFIG=CONT,FCTBLK=6,FUNCTION=HG3550,LINECNT=4,UNITS=3;
CHANGE-BFDAT:CONFIG=OK,FCTBLK=6,ANSW=YES;
```

Add vHG board in the SWU:

```
ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=99,SLOT=1,PARTNO="Q2330-
X",FCTID=1,LWVAR="0",FCTBLK=6,BCHL3550=30,ALARMNO=0,IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO;
```

Configure vHG board data (device specific parameters e.g., board IP, default gateway, assign number of SIP channels etc.):

```
ADD-CGWB:LTU=99,SLOT=1,SMODE=NORMAL,IPADR=10.8.242.115,NETMASK=255.255.255.0;
CHANGE-
CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=GLOBIF,PATTERN=213,VLAN=NO,VLANID=0,DEFRT=10.8.242.1,TRPRSIP
=120,
TRPRSIPQ=0,TRPRH323=0,TPRH323A=0,TLSP=4061,DNSIPADR=10.8.251.103,DNSIPAD2=0.0.0.0,USEWANIF=NO,
WPUBIP=0.0.0.0,SIPTCPP=5060,SIPTLSP=5061;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=SERVIF,LOGINTRM="TRM",PASSW="HICOM";
CHANGE-
CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=ASC,UDPPRTLO=29100,UDPPRTHI=30099,TOSPL=184,TOSSIGNL=104,T38
FAX=NO,RFCFMOIP=NO,RFCDTMF=YES,REDRFTN=NO,PRIO=PRIO1,CODEC=G711A,VAD=NO,RTP=30;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=ASC,PRIO=PRIO2,CODEC=G729A,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=ASC,PRIO=PRIO3,CODEC=NONE,VAD=NO,RTP=30;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=ASC,PRIO=PRIO4,CODEC=NONE,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=ASC,PRIO=PRIO5,CODEC=NONE,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=ASC,PRIO=PRIO6,CODEC=NONE,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=ASC,PRIO=PRIO7,CODEC=G729AB,VAD=YES,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=ASC,PRIO=PRIO8,CODEC=G722,VAD=NO,RTP=20;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=ASC,PRIO=PRIO9,CODEC=OPUS,VAD=NO,RTP=20;
CHANGE-
CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=MGNTDATA,MGNTIP=10.8.242.100,MGNTPN=8000,BUSIP=10.8.242.100,
BUSPN=443,UIMODE=CLASSIC;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=DMCDATA,DMCCONN=0,SMP=YES,SMP4OSV=NO;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=WBMDATA,LOGINWBM="HP4K-DEVEL",ROLE=ENGR;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=WBMDATA,LOGINWBM="HP4K-SU",ROLE=SU;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=WBMDATA,LOGINWBM="HP4K-ADMIN",ROLE=ADMIN;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=WBMDATA,LOGINWBM="HP4K-READER",ROLE=READONLY;
CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=GWDATA,GWID1="PRIMARYRASMANAGERID";
```

CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=SIPTRERH,GWAUTREQ=NO;

CHANGE-

CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=SIPTRSSA,SIPREG=NO,REGIP1=0.0.0.0,PORTTCP1=5060,PORTTLS1=5061,REGTIME=300,REGIP2=0.0.0.0,PORTTCP2=5060,PORTTLS2=5061;

CHANGE-

CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=DLSDATA,DLSIPADR=10.6.25.5,DLS
PORT=18443,DLSACPAS=YES;

CHANGE-

CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=JB,AVGDLYV=40,MAXDLYV=120,MINDLYV=20,PACKLOSS=4,AVGDLYD=60,MAXDLYD=200,JBMODE=2;

CHANGE-CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=IPCONF,IPMODE=IPV4,DHCPV4=NO,DHCPV6=NO;

CHANGE-

CGWB:MTYPE=CGW,LTU=99,SLOT=1,TYPE=MANLANIF,MIPADR=0.0.0.0,MNETMASK=0.0.0.0,MVLAN=NO,MVLANID=0,MDEFRT=0.0.0.0;

Add Class Of Parameter (used to specify the line parameters for signaling control of the device handler):

ADD-COP:COPNO=1,PAR=ANS&L3AR&IMEX,TRK=TA,TOLL=TA;

CHANGE-COP:COPNO=1,COPTYPE=COPADD,DEV=INDEP,INFO="IP TR";

Add Class Of Trunk (used to specify the switching technology parameters):

ADD-

COT:COTNO=1,PAR=RCL&IIDL&IVAC&INAU&ANS&CHRT&AEOD&CEBC&COTN&IEVT&IDIS&BSHT&BLOC&PROV&LWNC&INDG&NLRC&TSCS&ICZL&ABNA&ABPD&WAAN&DFNN&IONS&NLRD&NOFT&AMFC&NPIS&NTON;

Add Class Of Service (used to specify the authorizations and features assigned to stations and trunks):

ADD-COSSU:NEWCOS=1,INFO="";

CHANGE-COSSU:TYPE=COS,COS=1,AVCE=TA&TNOTCR&CDRINT&COSXCD&MB&DATA&CFNR&VCE;

CHANGE-COSSU:TYPE=COS,COS=1,AVCE=RSVLN&DICT&SPKR&FWDNWK&TTT&MSN&CFB&MULTRA;

CHANGE-COSSU:TYPE=COS,COS=1,AVCE=FWDEXT&CCBS&CW&GRPCAL;

CHANGE-COSSU:TYPE=COS,COS=1,AFAX=TA&TNOTCR;

CHANGE-COSSU:TYPE=COS,COS=1,ADTE=TA&TNOTCR&CDRINT&BASIC&MSN&MULTRA;

Add Bundle (used to specify trunk group number identifier):

ADD-BUEND:TGRP=2,NAME="http

SSP",NO=30,TRACENO=0,ACDTHRH=*,PRIONO=2,TDDRFLAG=OFF,GDTRRULE=0,ACDPMGRP=0,CHARCON=NEUTRAL;

Add digital trunk circuits in the SWU (used for the external gateway for IP trunking configuration):

ADD-TDCSU:OPT=NEW,PEN=1-99-001-0,COTNO=1,COPNO=1,DPLN=0,ITR=0,COS=1,LCOSV=1,LCOSD=1,CCT="http
SSP",

DESTNO=0,PROTVAR=ECMAV2,SEGMENT=8,DEDSVC=NONE,TRTBL=GDTR,SIDANI=N,ATNTYP=CO,CBMATTR=NONE,TCHAR
G=N,SUPPRESS=0,ISDNIP=0,ISDNNP=0,TRACOUNT=30,SATCOUNT=MANY,ALARMNO=0,FIDX=1,CARRIER=1,ZONE=EM
PTY,COTX=1,FWDX=5,CHIMAP=N,

UUSCCX=16,UUSCCY=8,FNIDX=0,NWMUXTIM=10,SRCGRP=5,CLASSMRK=EC&G711&G729AOPT,TCCID="",TGRP=2,SRCH
MODE=DSC,INS=Y,SECLEVEL=TRADITIO,HMUSIC=0,CALLTIM=60,WARNTIM=60,DEV=HG3550CO,BCHAN=1&&15,BCNEG
=N,BCGR=1,LWPP=0,LWLT=0,LWPS=0,LWR1=0,LWR2=0,DMCALLWD=N,GWPROT=NONE;

Add digit analysis (point access code to a suitable route):

ADD-WABE:CD=17,DAR=NETRTE;

Add SIP trunk destination (used for allocating SIP trunk access codes):

```
ADD-RICT:MODE=LRTENEW,LRTE=2,LSVC=ALL,NAME="htp SSP",TGRP=2,DNNO=1-1-122,ROUTOPT=NO,DTMFCONV=FIX,DTMFTEXT="",DTMFPULS=PP80,ROUTATT=NO,EMCYRTT=NO,INFO="",PDNNO=0,CHARCON=NEUTRAL,CONFTONE=NO,RERINGRP=NO,NOPRCFWD=NO,NITO=NO,CLNAMEDL=NO,FWDSWTCH=NO,LINFEMER=NO,NOINTRTE=NO;
```

For MWI:

```
ADD-RICT:MODE=PM,IDX=1,SAN=49511920946309,NAME="XPR",STYPE=XPRESION;
```

Add LCR outdial rule (used to specify outdial rule number identifier):

```
ADD-LODR:ODR=2,CMD=NPI,NPI=ISDN,TON=INTERNAT;
```

```
ADD-LODR:ODR=2,CMD=ECHO,FIELD=2;
```

```
ADD-LODR:ODR=2,CMD=END;
```

```
ADD-LODR:ODR=2,INFO="htp SSP";
```

Add Administration of LCR (used to specify the accumulation of the trunk groups):

```
ADD-
```

```
LDAT:LROUTE=2,LSVC=ALL,LVAL=1,TGRP=2,ODR=2,LAUTH=1,CARRIER=1,ZONE=EMPTY,LATTR=WCHREG,VCCYC=4;
```

Add digits to dial plan (refers to the digit analysis results of a dialed digit sequence or dialed code):

```
ADD-WABE:CD=9,DAR=CO,CHECK=N;
```

Add Administration LCR – Dialplan (used to specify the LCR digit patterns - LDP):

```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="9"- "Z",DPLN=0&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15,LROUTE=2,LAUTH=1,PINDP=N;
```

WBM Configuration for http Native SIP Trunk - Gateway Properties

Navigate to HG WBM >> Configuration >> Basic Settings >> Gateway.

The screenshot displays the Unify OpenScape 4000 WBM configuration interface. The top navigation bar includes 'Configuration', 'Maintenance', 'Help', and 'Logoff'. The left sidebar shows the 'Configuration' menu with options for 'Basic Settings', 'Security', 'Network & Routing', and 'Voice Gateway'. The main content area is titled 'Gateway Properties' and is divided into two sections: 'General' and 'Additional Features'.

General

- Board Name:
- Physical Node Number (4K): 1-30-300
- PBC Number in Shelf: 1
- Gateway Location: SG99
- Contact Address:
- System Country Code: 49 (Germany)
- Global Gateway of Type G.711: A-law
- Supported IP Version: IPV4 only
- Gateway IP Address: 10.8.242.115
- Gateway Subnet Mask: 255.255.255.0
- Public WAN IP Address:

Additional Features

- Conference Improvement:
- Support Dispatch Application: only for Native SIP Trunking GW
- Allow SIP Register for Trunking: only for Native SIP Trunking with profile
- Enable SMP: value from AMO CGWB
- Maximum number of DMC connections: 0
- Use Early Media for Disconnect to SIP: only for Native SIP Trunking GW
- Enable SMP for OSV SIPQ trunk: value from AMO CGWB
- Signaling Protocol for IP Networking: SIP
- SIP Protocol Variant for IP Networking: Native SIP
- DisplayName Character Code Set:

Buttons: **Apply** **Undo**

Footer information:

V10 R0 1-99-1	HP4K-DEVEL pksgw50.A9.115	SoftGate-SIP SG99	06.09.2022 09:39:43 28d 16h 22m
------------------	------------------------------	----------------------	------------------------------------

Make sure that:

- **Signaling Protocol for IP Networking:** SIP
- **SIP Protocol Variant for IP Networking:** Native SIP

WBM Configuration for http Native SIP Trunk - SIP Parameters

The vHG "SIP Parameters" used for the certification activities are shown under **HG WBM >> Configuration >> Voice Gateway >> SIP Parameters**.

The screenshot displays the configuration page for SIP Parameters in the Unify OpenScape 4000 vHG 3500 interface. The left sidebar shows the navigation tree with 'Voice Gateway' expanded to 'SIP Parameters'. The main content area is titled 'SIP Parameters' and contains the following settings:

- SIP User Agent:** "SIP User Agent" settings ignored due to usage of SIP trunk profiles.
 - Use SIP Registrar: No
 - SIP Registrar IP Address: 0.0.0.0
 - SIP Registrar TLS Port Number: 5061
 - SIP Registrar TCP/UDP Port Number: 5060
 - Alternative SIP Registrar IP Address: 0.0.0.0
 - Alternative SIP Registrar TLS Port Number: 5061
 - Alternative SIP Registrar TCP/UDP Port Number: 5060
 - Period of Registration (sec): 300
- SIP Server (Registrar / Redirect):**
 - SIP Server IP Address: 10.8.242.115
 - SIP Server TCP/UDP Port Number: 5060
 - SIP Server TLS Port Number: 5061
 - Default Registration Period (sec): (used when no 'Expires' value received)
 - Range used for Randomized Registration (%): 0 means: don't use Randomization
- RFC 3261 Timer Values:**
 - Transaction Timeout (msec): (Should only be changed for DNS failover scenarios)
- SIP Transport Protocol:**
 - SIP via TCP: Yes
 - SIP via UDP:
 - SIP via TLS: Yes

At the bottom of the interface, there is a status bar with the following information:

V10 R0	HP4K-DEVEL	SoftGate-SIP	06.09.2022 10:05:02
1-99-1	pzksgw50.A9.115	SG99	28d 16h 47m

Unify OpenScope 4000
vHG 3500

Configuration Maintenance Help Logoff

Configuration

- Basic Settings
- Security
- Network & Routing
- Voice Gateway

- Voice Gateway
 - H.323 Parameters
 - SIP Parameters
 - Codec Parameters
 - IP Networking Mode
 - SIP Trunk Profile Parameter
 - SIP Trunk Profiles
 - Hunt Group
 - Destination Codec Parameters
 - DARs for MLPP
 - Clients
 - CICA
 - ISDN Classmarks
 - Payload
 - Payload Parameters
 - Fax/Modem Tone Handling

SIP Session Timer

RFC 4028 Support:

Session Expires (sec):

Minimal SE (sec):

DNS-SRV Records / SIP Flooding Defense

Blocking time for unreachable destination/flood defense (sec):

Trunking Parameters

SIP OPTIONS ping interval (sec, 0=deactivate):

Keep Alive Timers

SIP OPTIONS ping interval (Subscriber, sec, 0=deactivate):

SIP OPTIONS retry attempts (Subscriber):

SIP loop call

SIP loop call From number:

SIP loop call To number:

SIP loop call frequency (sec, 0=deactivate):

SIP loop call Out of service threshold:

Call Supervision

MakeCallReq Timeout (sec):

SIP Connect Timeout (sec):

Apply **Undo**

V10 R0	HP4K-DEVEL	SoftGate-SIP	06.09.2022 10:08:53
1-99-1	pzksgw50.A9.115	SG99	28d 16h 51m

WBM Configuration for http Native SIP Trunk - Codec Parameters

Go to **HG WBM >> Configuration >> Voice Gateway >> Codec Parameters** to view the vHG "Codec Parameters" utilized for the current testing environment. As an example:

The screenshot shows the 'Codec Parameters' configuration page in the Unify OpenScope 4000 vHG 3500 interface. The left sidebar shows the navigation tree with 'Voice Gateway' expanded. The main content area displays a table of codecs and their parameters, followed by sections for 'Opus-Parameter' and 'T.38 Fax'.

Codec	Priority	Voice Activity Detection	Frame Size
G.711 A-law	Priority 1	VAD: <input type="checkbox"/>	30 msec
G.711 μ-law	not used	VAD: <input type="checkbox"/>	30 msec
G.729	not used	VAD: <input type="checkbox"/>	20 msec
G.729A	Priority 2	VAD: <input type="checkbox"/>	20 msec
G.729B	not used	VAD: <input checked="" type="checkbox"/>	20 msec
G.729AB	Priority 7	VAD: <input checked="" type="checkbox"/>	20 msec
G.722	Priority 8	VAD: <input type="checkbox"/>	20 msec
Opus	Priority 9	VAD: <input type="checkbox"/>	20 msec

Opus-Parameter

- Use Inband Forward Error Correction (FEC):
- Use Constant Bitrate:
- Low Delay:
- Payload Type for Opus: 124
- Max. Playback Sample Rate (Hz): 16000
- Complexity: 1

T.38 Fax

- T.38 Fax:
- Max. UDP Datagram Size for T.38 Fax (bytes): 375
- Error Correction Used for T.38 Fax (UDP): t38UDPRedundancy
- Time Range for Immediate Switch to T.38 Fax (s): 0 (0 means: No Immediate Switching)

The screenshot shows the 'Misc.' configuration page in the Unify OpenScope 4000 vHG 3500 interface. The left sidebar shows the navigation tree with 'Voice Gateway' expanded. The main content area displays various configuration options for 'Misc.' and 'RFC2833'.

Misc.

- ClearMode (ClearChannelData): Frame Size: 20 msec

RFC2833

- Transmission of Fax/Modem Tones according to RFC2833:
- Transmission of DTMF Tones according to RFC2833:
- Payload Type for ClearChannel: 96
- Payload Type for RFC2833: 98
- Payload Type for RFC2198: 99 (= 'Payload Type for RFC2833' + 1)
- Redundant Transmission of RFC2833 Tones according to RFC2198:
- Payload Type for RFC4733 WideBand: 100 (= 'Payload Type for RFC2833' + 2)

Apply **Undo**

Note 1: The greyed out options can be changed via AMO CGWB.

Note 2: In real-life production environments http requires "Frame Size" value to be set to "20".

SIP trunk Profile:

SIP Trunk Profile

Profile Name: **HTP GmbH**

User Notes:

Activate Trunk Profile:

Account/Authentication Required:

Remote Domain Name:

IP Transport Protocol: **TCP** (used for O/G call establishment)

Default PAI: (for outgoing "Anonymous" and CLIP "default PAI" profiles)

Security

Released Security Level: Signaling and Payload Security

TLS used: profile not active

RTP Security Mode: **secure Payload (SDES) with fallback to insecure**

Payload Encr. used: profile not active

Additional Mediasec Parameters Supported: **Not supported**

Registrar

Use Registrar:

IP Address / Host name:

Specify Port:

Port:

Reregistration Interval (sec)

Proxy

IP Address / Host name:

Specify Port:

TCP/UDP Port:

TLS Port:

Outbound Proxy

Use Outbound Proxy:

IP Address / Host name:

Specify Port:

Port:

OpenScape SBC Configuration

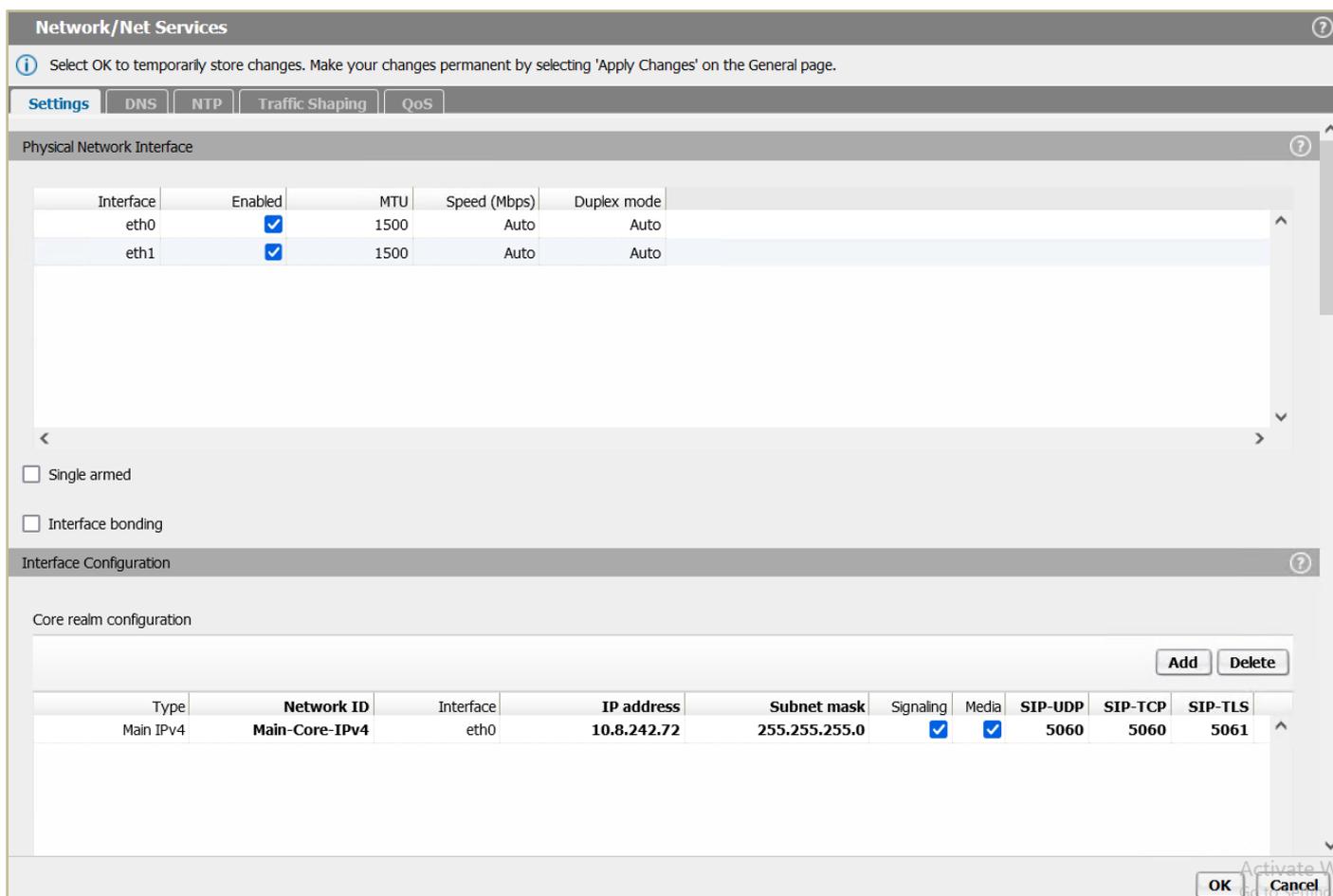
This chapter outlines the configuration of OpenScape SBC for interworking with htp Enterprise Voice network.

The OpenScape SBC will be configured with the connection to OS4000 and SSP (htp) endpoints. Routine or non-project specific OS SBC configuration will be omitted.

Core Realm Interface

Use the TCP ("Proxy") port number configured as outbound proxy in the OS4K WBM for the connection of OS SBC's eth0 (core) interface to OS4000.

Go to **OS SBC Management Portal >> Network/Net Services**.



The screenshot displays the 'Network/Net Services' configuration page. It includes a 'Physical Network Interface' table and a 'Core realm configuration' table.

Interface	Enabled	MTU	Speed (Mbps)	Duplex mode
eth0	<input checked="" type="checkbox"/>	1500	Auto	Auto
eth1	<input checked="" type="checkbox"/>	1500	Auto	Auto

Type	Network ID	Interface	IP address	Subnet mask	Signaling	Media	SIP-UDP	SIP-TCP	SIP-TLS
Main IPv4	Main-Core-IPv4	eth0	10.8.242.72	255.255.255.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5060	5060	5061

On **"Settings"** tab and in **"Core realm configuration"** area, make sure that for **"eth0"** interface, **"SIP-TCP"** has the value **"5060"**.

Click on **[OK]**.

Click on **[Apply Changes]** on OS SBC main page.

SIP Server

The SIP connectivity to OS4000 is configured in **OS SBC Management Portal >> VOIP** window.

VOIP

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

Sip Server Settings | Port and Signaling Settings | Media | QoS Monitoring

General

Comm System Type: Simplex

Allow Register from SERVER

Other trusted servers

Node 1

Target type: Binding

Primary server: 10.8.242.115 | Transport: TCP | Port: 5060

Backup server: | Transport: TCP | Port:

SRV record: | Transport: TCP

Node 2

Target type: Binding

Primary server: | Transport: TCP | Port:

Backup server: | Transport: TCP | Port:

SRV record: | Transport: TCP

Timers and Thresholds

Failure threshold (pings): 2 | OPTIONS interval (sec): 60

Success threshold (pings): 1 | OPTIONS timeout (sec): 4

OK Cancel

On "**Sip Server Settings**" tab, enter the following:

- **Comm System Type:** Simplex
- **Allow Register from SERVER:** Enabled
- **Target Type:** Binding
- **Primary Server:** (OS4000 HG card IP address of the trunk)
- **Transport:** TCP
- **Port:** 5060 (listening port)

Click on **[OK]**.

Click on **[Apply Changes]** on OS SBC main page.

Certificates

In case TLS interconnection is required between OpenScape SBC and htp systems, 1 file in pem format is required in OS SBC:

CA certificate (e.g., **serverCA.pem**)

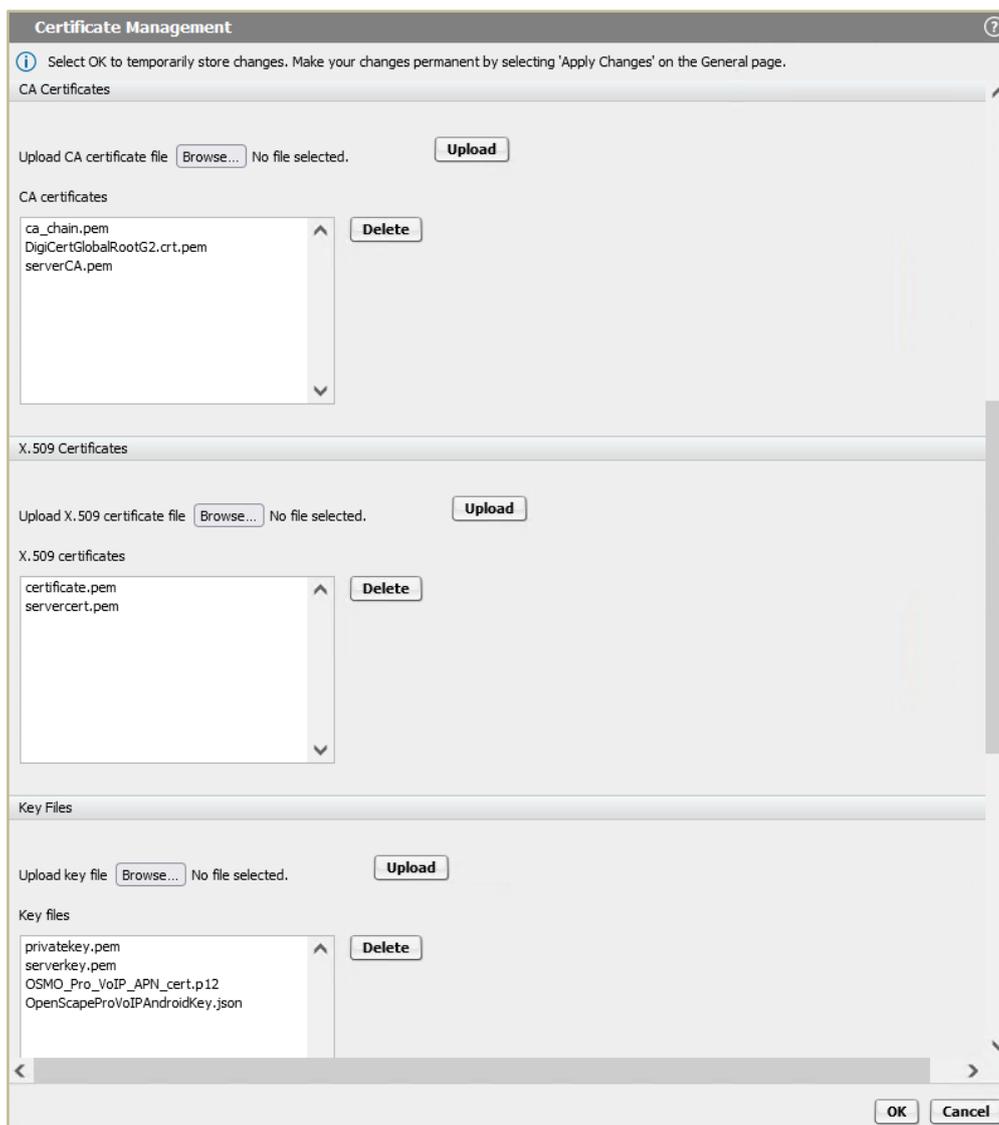
Server certificate for OS SBC (e.g., **servercert.pem**)

OS SBC server certificate private key used for the CSR to CA (e.g., **serverkey.pem**)

In current certification activities the default certificates and private key were used. Custom certificate and private key files may be used after uploading these files to SBC. For the TLS negotiation the SBC operates as a client and http as a server, therefore the certificate provided by http should be included in OS SBC.

Navigate to **OS SBC Management Portal >> Security >> General** and click on **"Certificate Management"** button.

In case custom OS SBC certificates are required, the corresponding files may be uploaded from **"CA Certificates"**, **"X.509 Certificates"** and **"Key Files"** areas correspondingly, as shown in figure below:



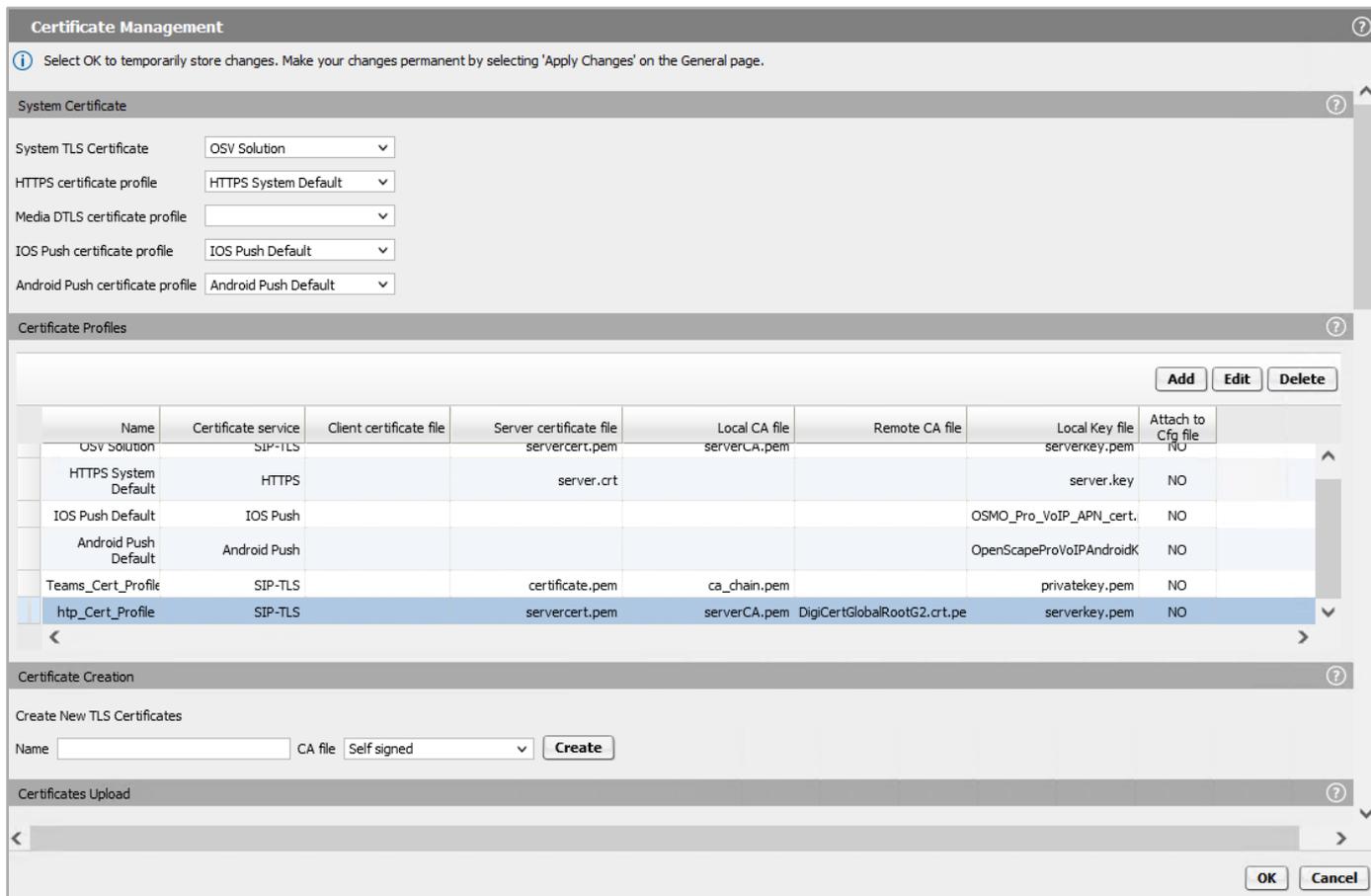
The certificate provided by http, **"DigiCertGlobalRootG2.crt.pem"**, is also uploaded.

On the same window, click on **[Add]** to create the certificate profile.

Enter the following:

- **Certificate profile name:** htp_Cert_Profile (friendly name)
- **Certificate service:** SIP-TLS
- **Local server certificate file:** servercert.pem
- **Local CA file:** serverCA.pem
- **Local key file:** serverkey.pem
- **Remote CA file:** DigiCertGlobalRootG2.crt.pem
- **Minimum TLS version:** TLS V1.2

Click on **[OK]**.



Click on **[OK]** on **Certificate Management** window and then click on **[OK]** on **Security** window.
Click on **[Apply Changes]** on OS SBC main page.

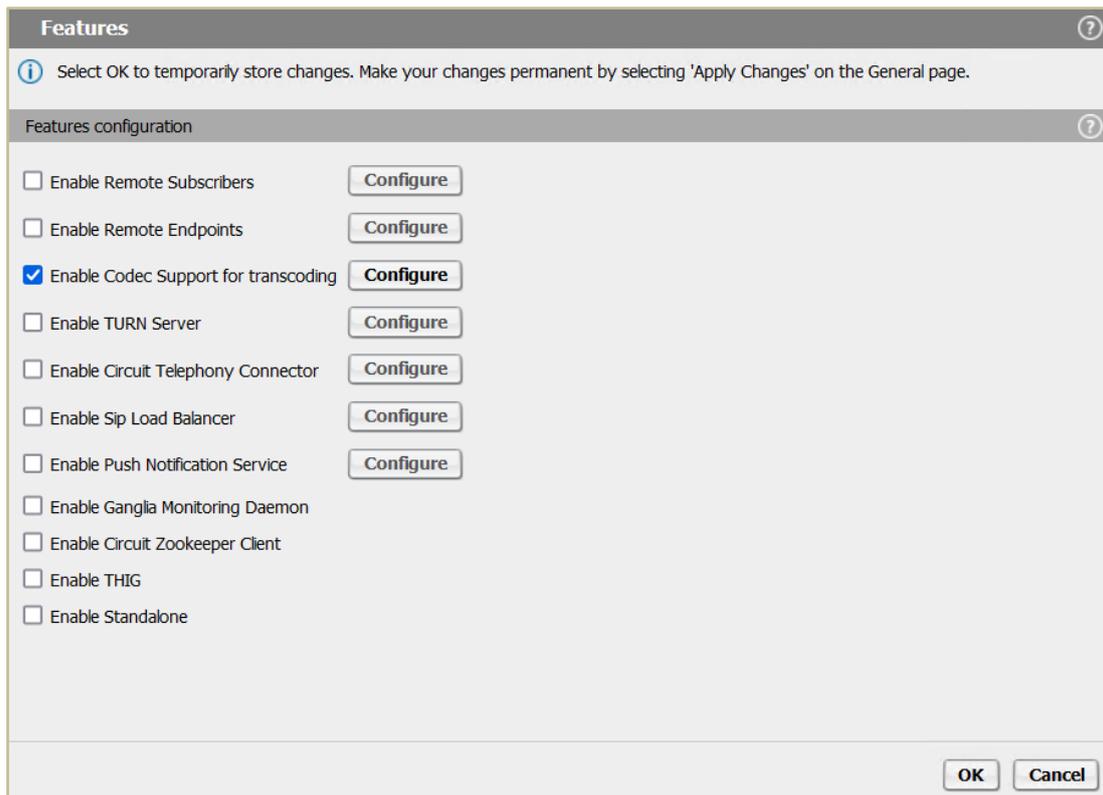
Media Profile

With **Media Profiles** settings, various parameters regarding the SDP messages and audio (RTP) traffic may be configured for the OS SBC SIP endpoints to SSP (htp) and OS4000.

Codec Manipulation Options

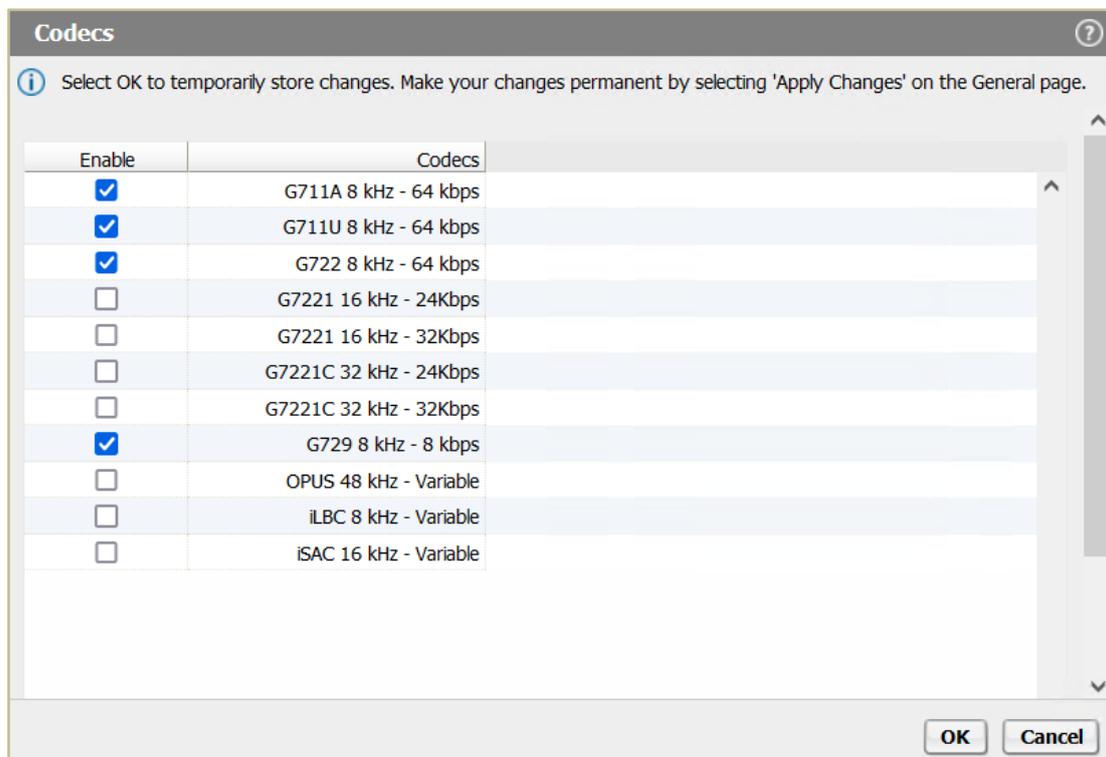
In case transcoding or certain codec prioritization for audio is required for the OS SBC – OS SBC – SSP media profile for the corresponding SIP trunk, it is required to enable the codec configuration options first for the media profile setup.

To do so, access **OS SBC Management Portal >> Features** window and select **"Enable Codec Support for transcoding"**.



Click on **[Configure]**.

On **"Codecs"** window, select the codecs to be available for the media profiles (for e.g. transcoding, prioritization). As an example:



Click on **[OK]** and on the rest open windows.

Click on **[Apply Changes]** on OS SBC main page.

Media Profile

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

General

Name

Media protocol Direct Media Support

Support ICE

Enable TURN Client

RTP/RTCP Multiplex in offer

SDP Compatibility Mode

Support Mid Attribute

Do not set port to zero on session timer answer SDP

SRTP configuration

SRTP crypto context negotiation MIKEY SDES DTLS

Mark SRTP Call-leg as Secure

RTCP configuration

RTCP Mode

RTCP generation timeout

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

Priority	Codec	Packetization interval

In **"Media Profiles"** area click on **[Add]** to create the media profile for OS SBC - SSP trunk by entering the following:

- **Name:** htp (friendly name)
- **Media protocol:** Best Effort SRTP
- **SRTP crypt context negotiation:** SDES (when secure media is required)
- **RTP/RTCP Multiplex in offer:** Enabled
- **Allow unconfigured codecs:** Enabled

Click on **[OK]** to return to **Media** window.

Click on **[OK]** on **"VOIP"** window.

Click on **[Apply Changes]** on OS SBC main page.

In "**Media Profiles**" area click on **[Add]** to create the media profile for OS SBC – OS4000 connection with the default settings:

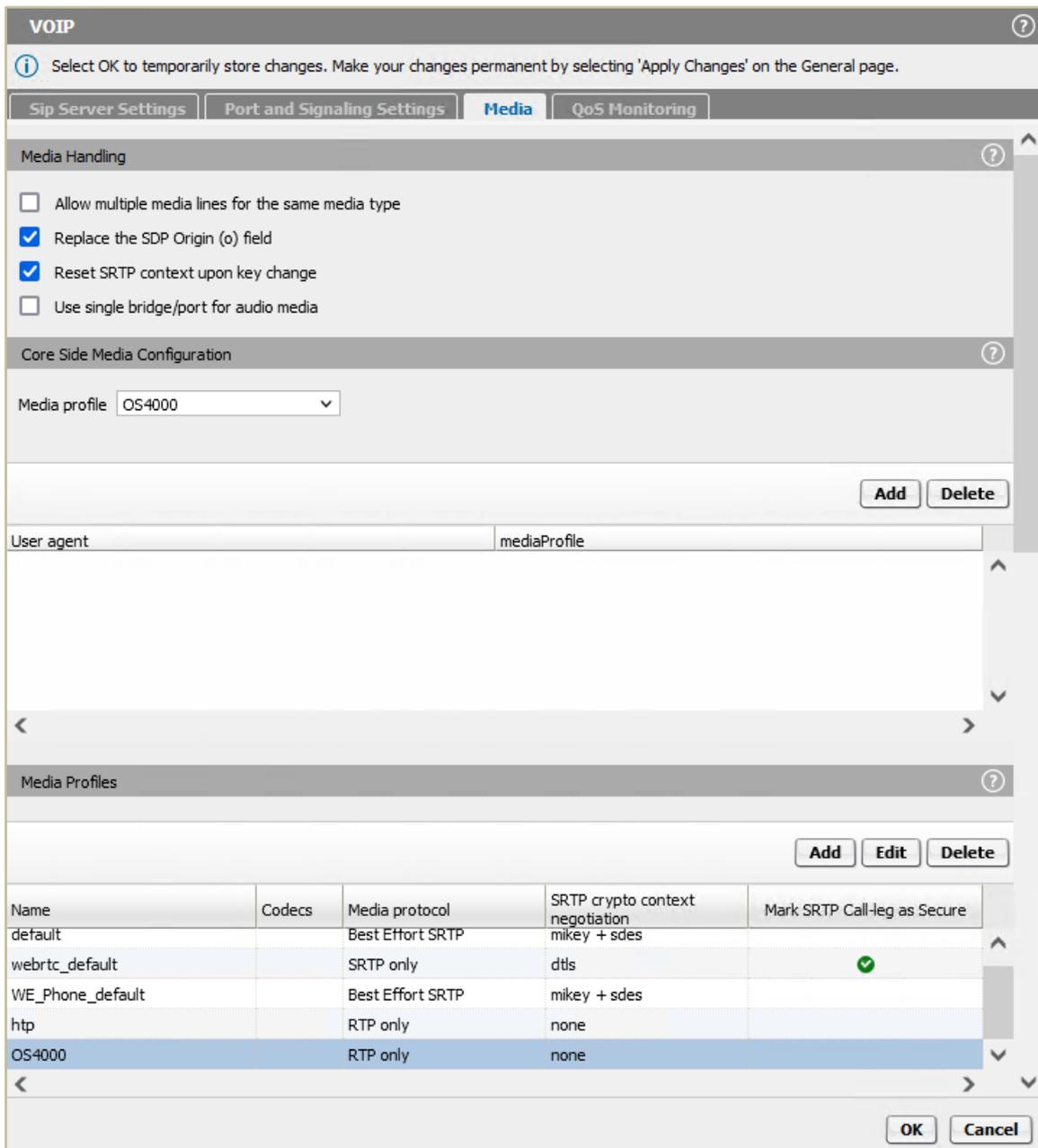
- **Name:** OS4000 (friendly name)
- **Media protocol:** RTP only
- **RTP/RTCP Multiplex in offer:** Enabled
- **Allow unconfigured codecs:** Enabled

Click on **[OK]** to return to "**Media**" window.

Click on **[OK]** on "**VOIP**" window.

Click on **[Apply Changes]** on OS SBC main page.

After creating the media profiles, configure the general media setting on **OS SBC Management Portal >> VOIP >> Media** window.



In **"Core Side Media Configuration"** area set **"OS4000"** from the **"Media profile"** dropdown list for the media profile used for the OS SBC – OS4000 SIP trunk.

In **"Media Handling"** enable the following:

- **Replace the SDP Origin (o) field:** Enabled
- **Reset SRTP context upon key change:** Enabled

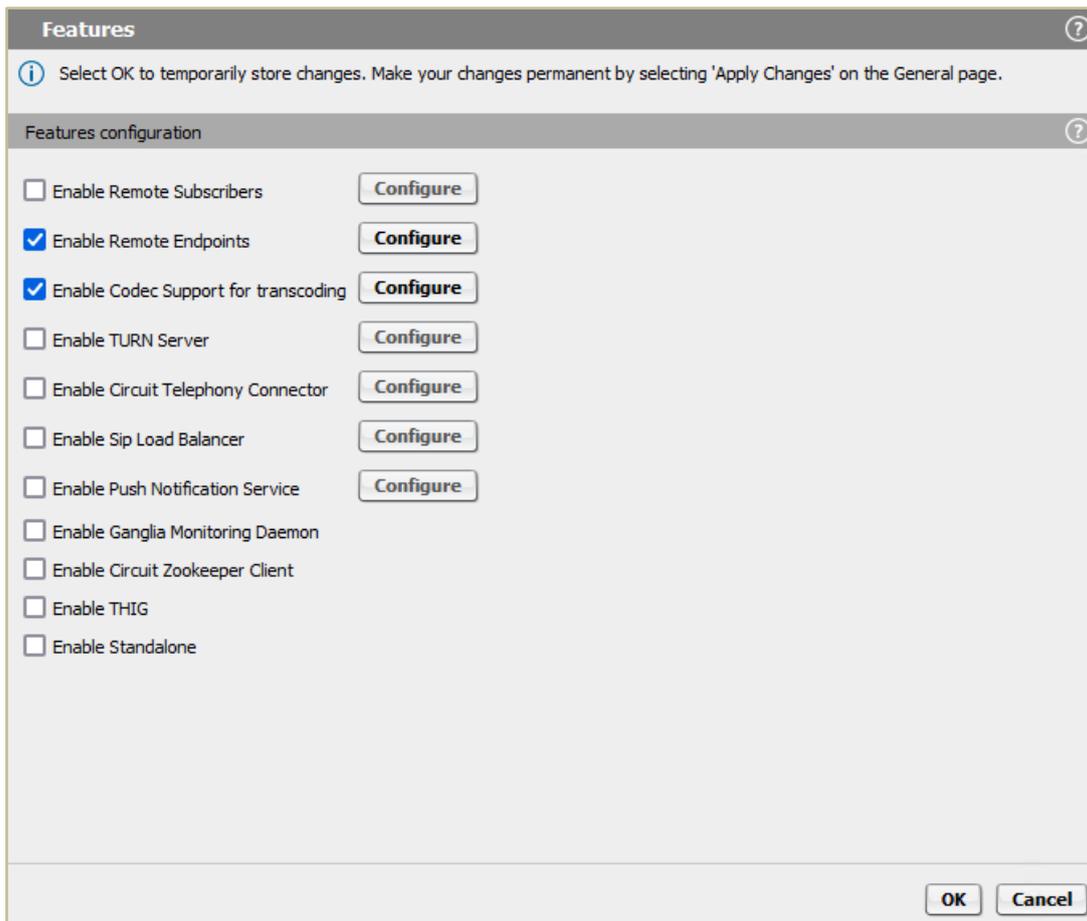
Click on **[OK]**.

Click on **[Apply Changes]** on OS SBC main page.

Remote Endpoints

In **Remote Endpoint** configuration the OS SBC with the SSP (htp) is setup.

Navigate to **OS SBC Management Portal >> Features** window and set **"Enable Remote Endpoints"** to **"Enabled"**.



On **OS SBC Management Portal >> Features >> Enable Remote Endpoints** window, click on **[Configure]**.

SIP Provider Profile

On **Remote Endpoints** window click on **[Add]** in **"SIP Service Provider Profile"** area to add the endpoint profile for the OS SBC – http SIP trunking.

SIP Service Provider Profile

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

General

Name Default SSP profile

Use SIP Service Address for identity headers

SIP service address

Use SIP Service Address in Request-URI header

Use SIP Service Address in From header

Use SIP Service Address in To header

Use SIP Service Address in P-Asserted-Identity header

Use SIP Service Address in Diversion header

Use SIP Service Address in Contact header

Use SIP Service Address in Via header

Use SIP Service Address in P-Preferred-Identity header

SIP User Agent

SIP User Agent towards SSP SIP User Agent

Registration

Registration required

Registration interval (sec)

Business Identity

Business identity required

Business identity DN

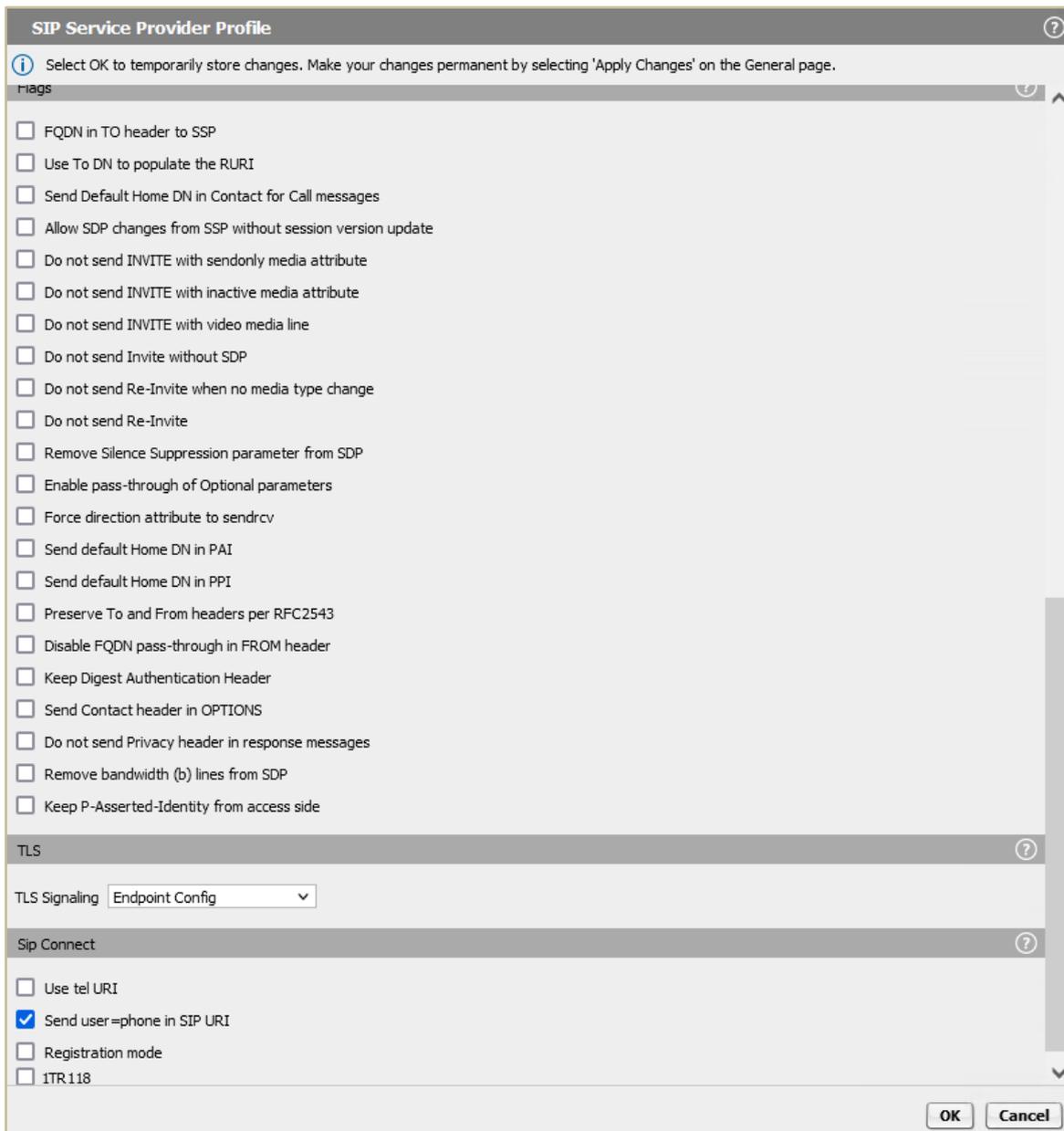
Outgoing SIP manipulation

Insert anonymous caller ID for blocked Caller-ID

Manipulation

Incoming SIP manipulation

Calling Party Number



On "**SIP Service Provider**" window, enter the following:

- **Name:** http (friendly name)
- **Default SSP Profile:** Blank (in case the
provider doesn't exist in the dropdown
selection list, the field should
remain blank and the user must
manually configure the required flags for
the SSP in use)
- **Use SIP Service Address for identity headers:** Enabled
- **SIP service address:** siptrunk.htp.net
- **Use SIP Service Address in Request-URI header:** Enabled
- **Use SIP Service Address in From header:** Enabled
- **Use SIP Service Address in To header:** Enabled
- **Use SIP Service Address in P-Asserted-Identity header:** Enabled
- **Use SIP Service Address in Diversion header:** Enabled

- **Registration required:** Enabled
- **Send user=phone in SIP URI:** Enabled

Click on **[OK]** to return to **"Remote Endpoints"** window.

Note: An http **"Default SSP Profile"** will be available for user selection in future OS SBC versions.

In **"Remote endpoint configuration"** area, click on **[Add]**.

On **"Remote endpoint configuration"** window, enter the following in the **"Remote Endpoint Settings"** area:

- **Name:** htp (friendly name)
- **Type:** SSP
- **Profile:** htp

Continue to **"Remote Location Information"** area:

- **Signaling address type:** DNS SRV

Click on **[Add]** in **"Remote Location domain list"** area.

Remote Location Domain ⓘ

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

General ⓘ ^

Remote URL Shared domain

Remote port

Remote transport ▾

Signaling ⓘ

INVITE No Answer timeout (msec)

INVITE No Reply timeout (msec)

TLS ⓘ

TLS mode ▾

Certificate profile ▾

TLS keep-alive

Keep-alive interval (seconds)

Keep-Alive timeout (sec)

Media Configuration ⓘ

Media profile ▾

Media realm subnet IP address

Outbound Proxy Configuration ⓘ

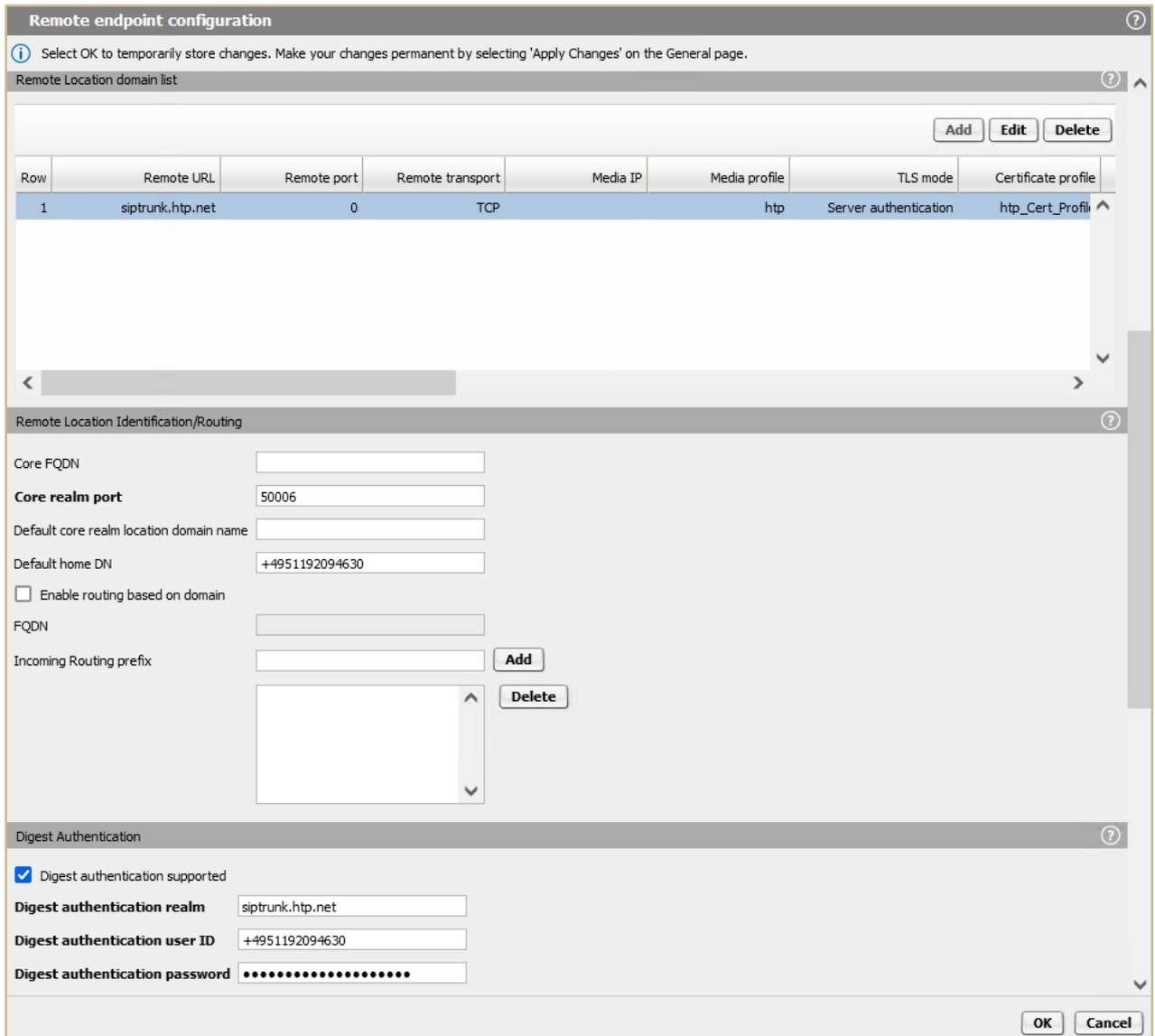
Outbound Proxy

Outbound Proxy Port

On "**Remote Location Domain**" window, enter the following:

- **Remote URL:** siptrunk.htp.net (see section 4.1)
- **Remote port:** 0
- **Remote transport:** TCP (UDP or TLS are also possible)
- **TLS mode:** Server authentication (when TLS is used)
- **Certificate profile:** htp_Cert_Profile (when TLS is used- refer to sub-section 4.3.2)
- **Media profile:** htp (refer to sub-section 4.3.3)

Click on **[OK]** to return to "**Remote endpoint configuration**" window.



In **"Remote Location Identification/Routing"** area, enter the following:

- **Core realm port:** **50006** (as configured in the OS\$K WBM 4.2.5)
- **Default home DN:** **+49XXX**

In **"Digest Authentication"** area, enable **"Digest authentication supported"** and fill in with the values below:

- **Digest authentication realm:** **siptrunk.htp.net**
- **Digest authentication user ID:** **+49XXX**
- **Digest authentication password:** **passphrase** (provided by htp)

Click on **[OK]** to return to **"Remote Endpoints"** window.

The **"Remote Endpoints"** window should look like the picture below:

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	htp	<input checked="" type="checkbox"/>	3600

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
1	htp	Main-Access-Realm - ipv4	SSP	htp	siptrunk.htp.net	0	TCP	

Click **[OK]** on all open windows.

Click on **[Apply Changes]** on OS SBC main page.

Restrictions and Remarks

Remarks

- **General Information**

In certification test environment there aren't any SPEP PSTN subscribers for testing, so SPPN (mostly) or SPGSM are used instead.

The test scenarios were performed twice with both HFA and SIP OS4K internal stations. All call scenarios were executed with TCP transport protocol.

- **Voicemail**

No voicemail service is provided by htp.

- **Conference**

When OS4000 subscriber exits the conference, the PSTN subscribers continue to display the OS4000 subscriber (conference initiator), instead of each other.

Conference display on various devices isn't propagated over the SIP trunk from OS4000.

- **Codecs**

G.722, G.729 codecs aren't supported by htp's voice network.

- **DTMF**

The htp network supports both RFC2833 and inband for DTMF transport methods.

However, the inband isn't tested in current certification activities because htp is using only RFC2833 in production system and a change would affect all users.

Atos Unify phone devices are using RFC2833 by default, but inband is also supported.

There is no configuration option to disable RFC2833 on the phones. CP phones switch to inband only if remote side doesn't support RFC2833.

Restrictions

- **Basic Call**

In a basic call scenario, where an OS4000 subscriber makes a call to a PSTN subscriber, the OS4000 subscriber displays only the number and not the name of the PSTN called party. Additionally, the PSTN subscriber displays only the number of the OS4000 calling party. On the other hand, when the PSTN subscriber is the calling party and the OS4000 subscriber is the called party, the PSTN subscriber will display the OS4000 subscriber's number and not the name. OS4000 sends PAI in "200OK" to htp, but this is not taken into consideration for IP phone display update.

The htp service doesn't use PAI for display update purposes, but only for call validation, and display info is extracted by FROM header.

- **COLR**

When a PSTN subscriber calls an OS4000 subscriber and the latter has COLR feature activated, OS4000 sends "Privacy: id" header in "200OK" to htp, but PSTN subscriber continues to display OS4000 subscriber's number. When htp receives "Privacy: id" header, the PAI header is removed from "200OK" by htp system, but this manipulation seems not to be enough for PSTN subscriber to have "Anonymous" call display. When the same scenario is tested with a networked OS Voice PBX node to OS4000, the caller has "Anonymous" call display.

On the other hand, when the OS4000 subscriber is the caller and the PSTN subscriber on htp network has the COLR feature activated, there is no "Anonymous" call display on OS4000 subscriber. htp adaptation for COLR is not to send PAI, however OS4000 expects "Privacy: id" header in order OS4000 station to display an "Anonymous" call.

- **Call Hold**

In a basic call between an OS4000 subscriber and a PSTN subscriber, when the OS4000 subscriber holds the call, the PSTN SIP subscriber doesn't display "held remotely" indication and hears MOH from OpenScape 4000. OS4000 sends re-INVITE (or ACK) for the hold with "sendonly" attribute in SDP.

If the PSTN subscriber puts a call with an OS4000 subscriber on hold, the OS4000 subscriber won't display "held remotely" indication and hears MOH coming from PSTN. PSTN replies with an SDP attribute "inactive" in 200 OK. PSTN doesn't send SDP attribute "sendonly" or "inactive" in a hold re-INVITE.

- **Call Transfer**

In call transfer scenarios (A->B->C), when subscriber "B" ("transferring" party) belongs to a different system than "A" ("transferred" party) and "C" ("transferred to" party) i.e., PSTN carrier vs OS4000, then after transfer is completed from "B", "A" and "C" will continue to display "B", instead of the connected party, when "A" and "C" are PSTN subscribers and "B" is an OS4000 internal station.

After transfer completion, the display of the connected party information on the "transferred" and on the "transferred to" call participants, varies according to the relation with the "transferring" party (system-wise), if the "transferring" party is "A", "B" or "C" (in the indicative transfer scenario A->B->C mentioned above) and from the transfer flavor (attended, semi-attended, blind).

The root cause for the display behavior in transfers is described in "**Restrictions – Basic Call**" bullet point. For more details refer to the corresponding test results in chapter 3.

- **Call Forwarding**

In the indicative call forwarding scenario (A->B->C), when subscriber "B" ("forwarding" party) belongs to a different system than "A" ("forwarded" party) and regardless of where "C" ("forwarded to" party) belongs i.e., PSTN carrier vs OS4000, then after call forwarding completion from "B", "A" will continue to display "B", instead of the connected party and will not display forwarded call information. The same goes for various call forwarding

combinations in terms where the subscriber is registered and what flavor of call forwarding is used (Call Forward Unconditional, Call Forward Busy, Call Forward No Reply). Subscriber "A" will display the connected party only if "A" and "B" belong in the same system. Refer to test results in chapter 3 for the details.

- **Fax**

The http network doesn't support fax exchange with T.38, but only with G.711.

Known Issues

- **Call Transfer**

When an OS4000 SIP subscriber performs an attended transfer of a PSTN call to an OS4000 HFA subscriber, on HFA phone the connected party name isn't updated while the number display is correctly updated. The issue isn't reproducible when the OS4000 HFA subscriber performs the transfer.