OpenScape Business V2

Tutorial

System Device@Home – Configuration

Version 1.4

Table of Contents

Table of History

Date	Version	Changes
2016-02-25	1.0	Initial Creation for OpenScape Business V2R1
2016-03-24	1.1	Minor enhancements and functional boundary regarding WAN interface added
2016-06-16	1.2	Enhancements for V2R2
2017-06-29	1.3	Enhancements for V2R3
2019-03-06	1.4	Enhancements for V2R6 Chapter added for Signalling and Payload Encryption (SPE)

Preface

This document describes the required configuration steps for the configuration of the feature **Device@Home** for **System Devices**. It also provides useful information regarding supported scenarios, known limitations and security considerations.

This description refers to OpenScape Business V2R6.

Within the following the term **"System Device"** is used in general for the following system clients, which support the **HFA** protocol: OpenStage, OpenScape DeskPhone IP and OpenScape DeskPhone CP phones as well as the integrated **VoIP client** within the myPortal to go apps.

1. Configuration Overview

The feature **"Device@Home"** offers registration and operation of System Devices, which are connected over the Internet as internal devices of OpenScape Business.

For all examples within the document, the following basic network scenario is used.

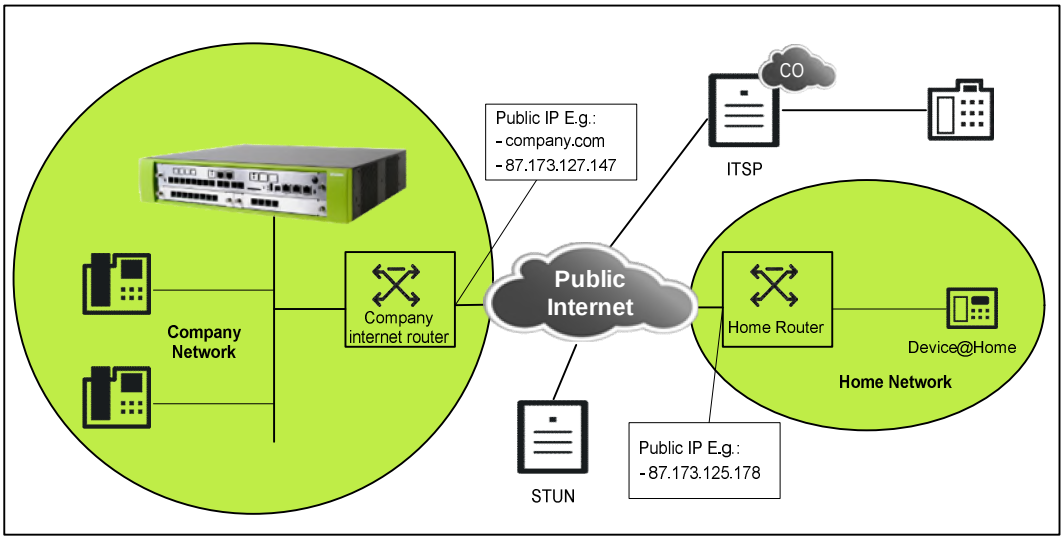


Figure 1 Typical network environment

1.1. Network Scenario Description:

OpenScape Business is located within a company LAN, which is connected to the Internet via the Company Internet Router. This router is accessible from the Internet either via public IP Address **87.173.127.147** or via DNS name **company.com**.

The System Device@Home is connected to the LAN within a Home Network, which is connected to the Internet via a Home Internet Router. The Home Router is accessible from the Internet with the public Internet Address **87.173.125.178**.

Within the Internet a STUN (Session Traversal Utilities for NAT) Server for public IP address discovery and an ITSP for Internet Telephone in general are available.

1.2. Configuration Steps

To connect the System Device@Home to OpenScape Business the following components need to be configured accordingly:

- OpenScape Business system within the company
- Company Internet Router
- System Devices @Home

- myPortal to go client (optional).

1.2.1. Overview OpenScape Business Configuration

In OpenScape Business the following configuration steps are required:

- Activate STUN support, if not already done for an ITSP, which is connected to OpenScape Business.
- Configure the number of “simultaneous Internet calls”. This value is implicitly set when the parameter “upstream up to (Kbps)” is set to a useful value in the basic installation wizard.
- Configure System Client as externally connected client
    - Assign an IP user license. (This is also required if the myPortal to go VoIP option is used).
    - Enable Authentication and configure **STRONG** passwords for the System Device@Home, which is connected via Internet.
    - Allow System Client registration from external (i.e. over the Internet) individually for each System Client by activating the integrated SBC function for that System Client.
- Enable SW Deployment for @home devices
- Optional: Enable signalling (and payload) encryption (SPE) for the System Device@home (only if required).

1.2.2. Overview Company Internet Router Configuration

As the System Device@Home must reach the OpenScape Business system from the Internet and vice versa. The following configuration steps have to be done for the Company Internet Router:

- Configuration of a UDP port forwarding (see 3) for the RTP protocol port range.
- Configuration of a TCP port forwarding for the HFA protocol (when using System Devices).
- Configuration of a TCP port forwarding rule for the DLI service
- Optional: Configuration of a TCP port forwarding rule for HTTPS (only when using myPortal to go VoIP @Home or DeskPhone CP 400/600 @Home).

Note:

If the company Internet router restricts outbound IP traffic, it may be necessary to explicitly open the ports also for outgoing IP traffic.

The normal SW-Update procedure of the DLI for an internally connected device cannot be used for System Device (HFA)@Home as the DLI cannot determine the IP address of device which resides in a LAN environments using NAT in the Internet Router. Therefore the DLI SW-Update procedure uses an additional HTTPS connection via port 8804 (default setting) in combination with the DLI port 18443 (default setting) to determine SW version of the Device@Home and to perform the SW-Update.

1.2.3. Overview System Device@Home Configuration

Within the System Device@Home, following configuration steps have to be fulfilled:

- Configuration of the gateway IP address: Enter the public IP address (if fix) or public domain name of the OpenScape Business
- Configuration of the HFA password
- Configuration of DLS:

1.3. Technical boundaries and limitations

1.3.1. Internet access of OpenScape Business

- Device@Home is tested and released for connection to the LAN2 interface of OpenScape Business. The WAN (LAN1) interface is not supported
- ITSP trunks and System Device@Home have to be connected to the same LAN interface of OpenScape Business. Using different LAN interfaces, e.g. ITSP connected to the LAN 1 (WAN) and Device@Home connected via Internet to LAN 2, is not supported.

1.3.2. NAT configuration within Company and Home Router

Routers with NAT type ”Symmetric NAT” are not compatible to the Device@Home solution. If the NAT behaviour is configurable in the router, it needs to be changed accordingly if possible.

Note:

The NAT type detection of the OpenScape Business (see Assistant) may falsely detect the NAT type of the Company router as “Symmetric NAT”, if outbound IP traffic is restricted in the Company Internet router.

1.3.3. myPortal to go VoIP client:

- The VoIP client within the myPortal to go App requires direct HTTPS access to TCP/8802 port within OpenScape Business.
- myPortal to go VoIP supports only G.711 codec.

1.3.4. OpenScape DeskPhone CP 400/600:

- The OpenScape DeskPhone CP 400/600 requires direct HTTPS access to TCP/8802 port within OpenScape Business, if UC server access is configured.

1.3.5. Secured Connections to System Device @Home

- Signaling:
  For secured connections the TLS protocol is used for encryption of the signaling information.
  TLS version 1.2 is used per default. A fallback to TLS 1.0 is possible in V2R6, if the device does not support TLS 1.2.
  TLS is not supported at WAN interface.
- Payload:
  Payload encryption using SRTP and SDES is not supported for System Device @Home.

1.3.6. Desksharing Support

The feature System Device@Home, incl. myPortal to go VoIP client, is not released in combination with Deskshare mobility (relocate).

1.3.7. Capacities

Open Scape Business uses a so called “RTP proxy” for all VoIP connection via Internet. The RTP Proxy offers **a shared pool** with a **limited amount of channels** which are assigned to the Internet connections as follows:

- 1 RTP proxy channel per ITSP call
- 1 RTP proxy channel per Circuit call
- 1 RTP proxy channel per System Device @Home in a call
- 1 RTP proxy channel per SIP Device @Home in a call
- 1 RTP proxy channel per myPortal to go VoIP @Home in a call

Within the different OpenScape Business models following resources are available:

System variant	**RTP proxy channels**
OpenScape Business X1/X3/X5/X8 with or without Booster card/server	60
OpenScape Business S	180

2. OpenScape Business configuration

In general there are different scenarios to connect OpenScape Business system to the internet.

1. Behind an Internet Router connected to LAN2 interface
2. Behind an Internet Router connected to LAN 1 (WAN) interface
3. Behind an Broadband Modem connected to LAN1 (WAN) interface

Only scenario 1 is supported for device @home.

Scenario 2 and 3 cannot be used for connection of System Device@Home.

2.1. Supported Internet Access Scenarios for System Device@Home

The following scenarios are supported for connection of a System Device@Home via the Internet to OpenScape Business.

2.1.1. OpenScape Business behind access router connected to LAN2 interface

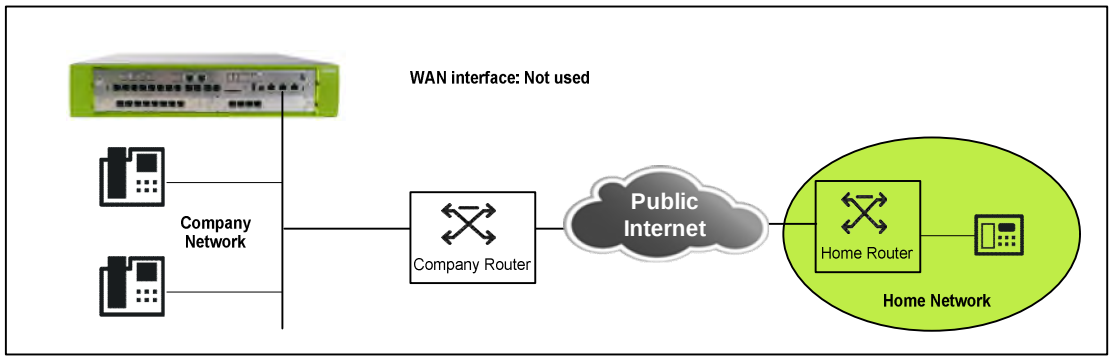


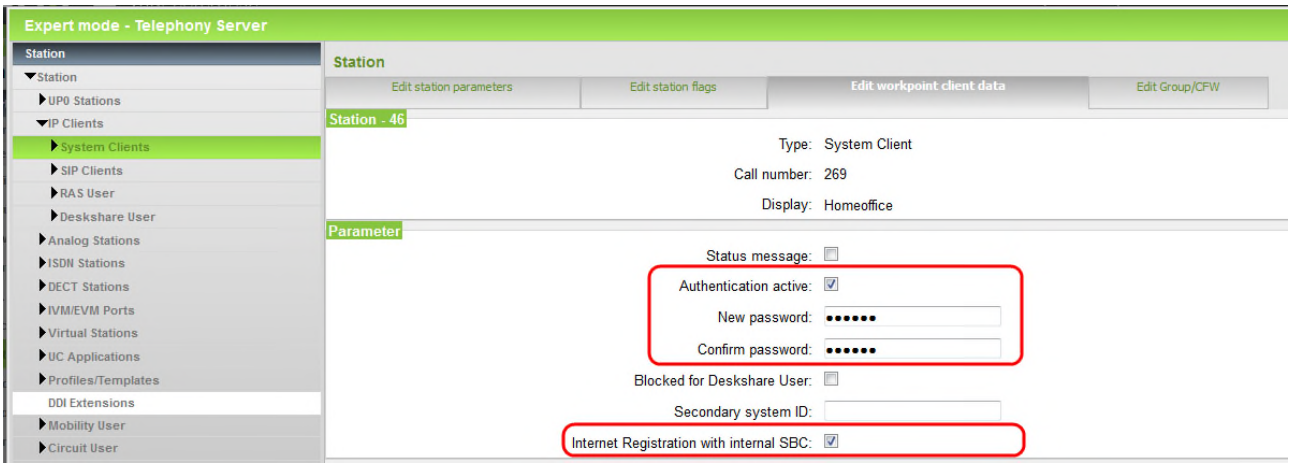
Figure 2 OpenScape Business behind access router connected to LAN2 interface

2.2. Configuring a System Client to be used from Internet

System Devices with HFA protocol are configured as System Clients within OpenScape Business Assistant (WBM). The general configuration of a System Client is described within the administration manual of OpenScape Business. In addition to the basic configuration the following settings in “Expert Mode” are necessary for System Device@Home.

The flag “**Internet Registration with internal SBC**” MUST be set for each System Client, which is connected via Internet.

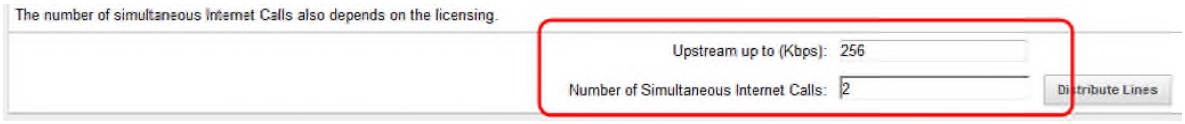
The authentication has to be enabled for the external device and a strong authentication password has to be chosen before the SBC flag can be set. The password has to comply with the password policy of the Administration Portal, otherwise it is not accepted and guidelines are displayed.



In addition the Class of Service (COS) and System Flags should be reduced to the required needs for the System Clients in order to prevent toll fraud by dialing expensive premium or international numbers or by programming call forwarding to such numbers.

2.3. Configuring the number of simultaneous internet calls

Set the “Number of simultaneous internet calls” to a value bigger than zero. The value is implicitly set when the parameter “Upstream up to (Kbps)” is set to a useful value in the basic installation wizard.



2.4. Configuring STUN

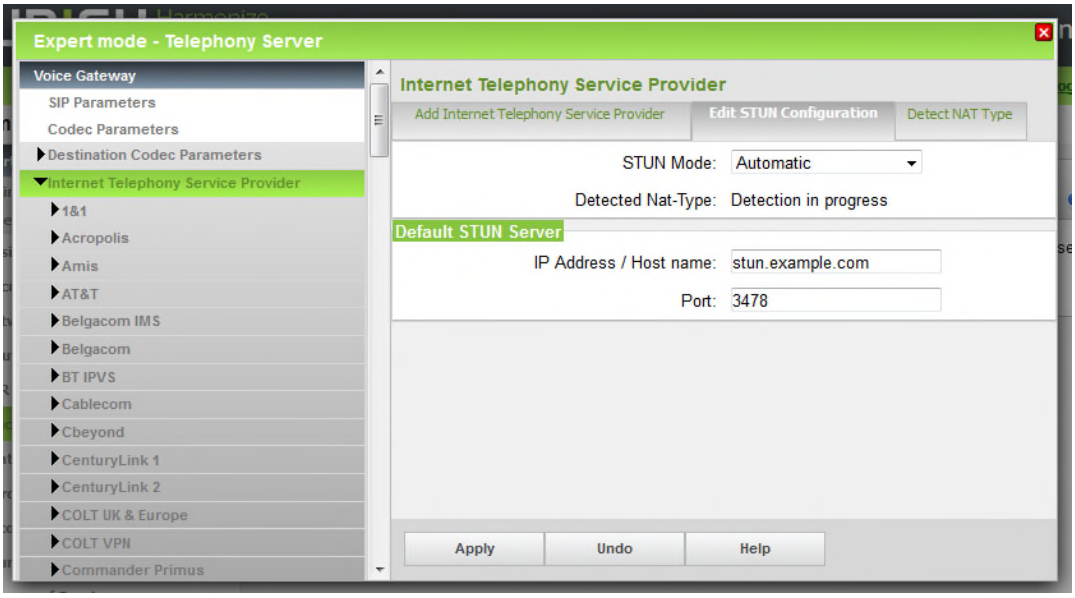
The integrated Session Boarder Controller (SBC) function of OpenScape Business must be able to detect its public IP-address and -ports. This is done by using the STUN protocol.

In case that the system is already connected to an ITSP with activated STUN server, no additional configuration is required. The system is able to detect its public IP-address and port

In case that:

- OpenScape Business is connected to an ITSP with disabled STUN
- No ITSP is configured in the system

a STUN configuration is necessary within the system in order to determine its public IP address and port.



This STUN server configured in “Edit STUN Configuration” will be used only if no STUN server is configured for an ITSP.

2.5. Port configuration within OpenScape Business

The subsequent ports, which are used by OpenScape Business for signalling and voice payload transmission to externally connected System Devices, must not be changed within the system configuration

2.5.1. Signalling Ports

Protocol	**Default port**
HFA (not encrypted)	TCP 4062 (for HFA phones)

HFA (encrypted)	TLS 4063	(for HFA phones)
HTTPS	TCP/8802	(for myPortal to go and for OpenScape DeskPhone CP 400/600)

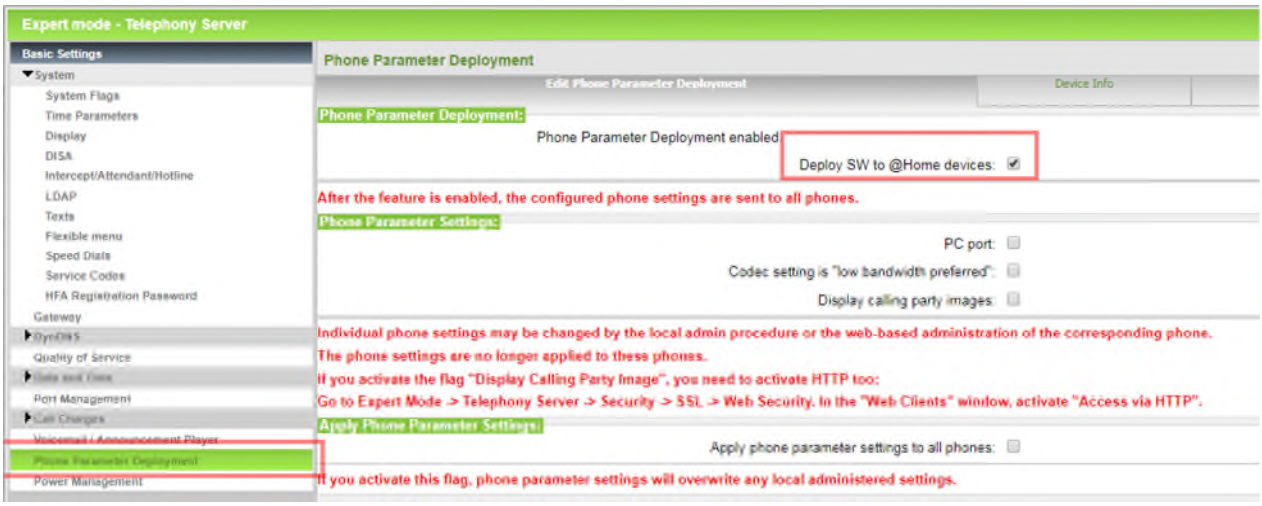
2.5.2. Voice Payload Ports

For voice payload, the following port range is used:

Protocol	**Default port**
RTP	UDP/30274-30529 (for OpenScape Business X1/X3/X5/X8) UDP/30528-30887 (for OpenScape Business S)

2.6. Configuring SW Deployment

From V2R6 on automatic firmware update via DLI is also supported for System Device@Home. The software update of a Device@Home by the DLI has to be configured in OpenScape Business. It is disabled per default and needs to be enabled explicitly.



2.7. Configuring SPE (optional)

From V2R6 on OpenScape Business supports Signalling and Payload Encryption (SPE) also for System Device @Home. The SPE configuration of a system device @home is done in general in the same way as for locally connected system devices.

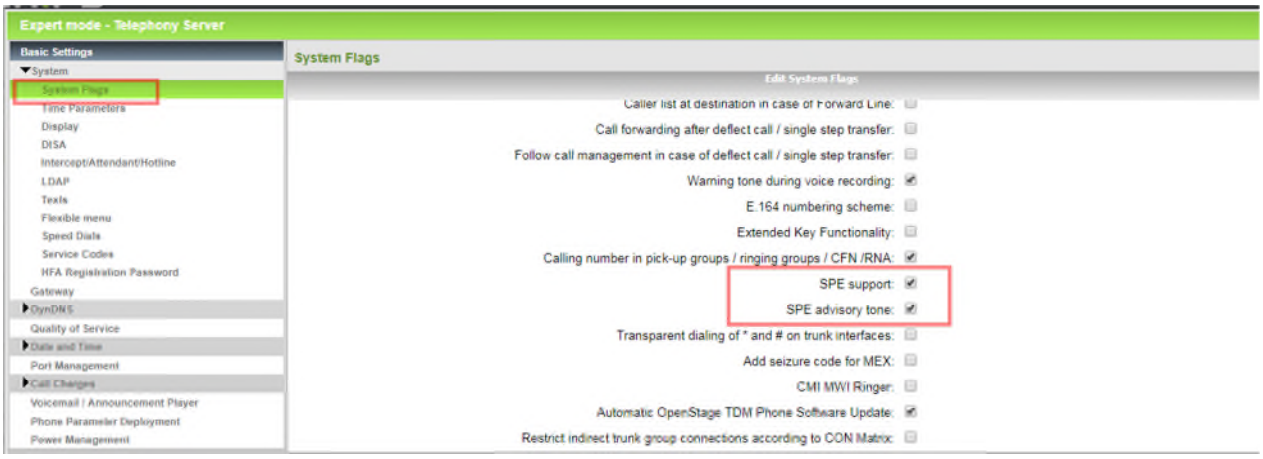
Certificates are required for encryption and authentication. Certificates used for device authentication needs to be deployed via DLS to the devices. At least one Root CA certificate and one Server / Peer certificate are required for SPE encryption.
OpenScape Business supports creation of self-signed Root CA certificates and the import of Trusted Center signed Root CA certificates.

The SPE feature needs to be enabled on system and on device level within the system configuration.

In the following the main steps for SPE configuration and the handling of the “encryption certificate” is described, as a DLS for certificate deployment is not available in most installations.

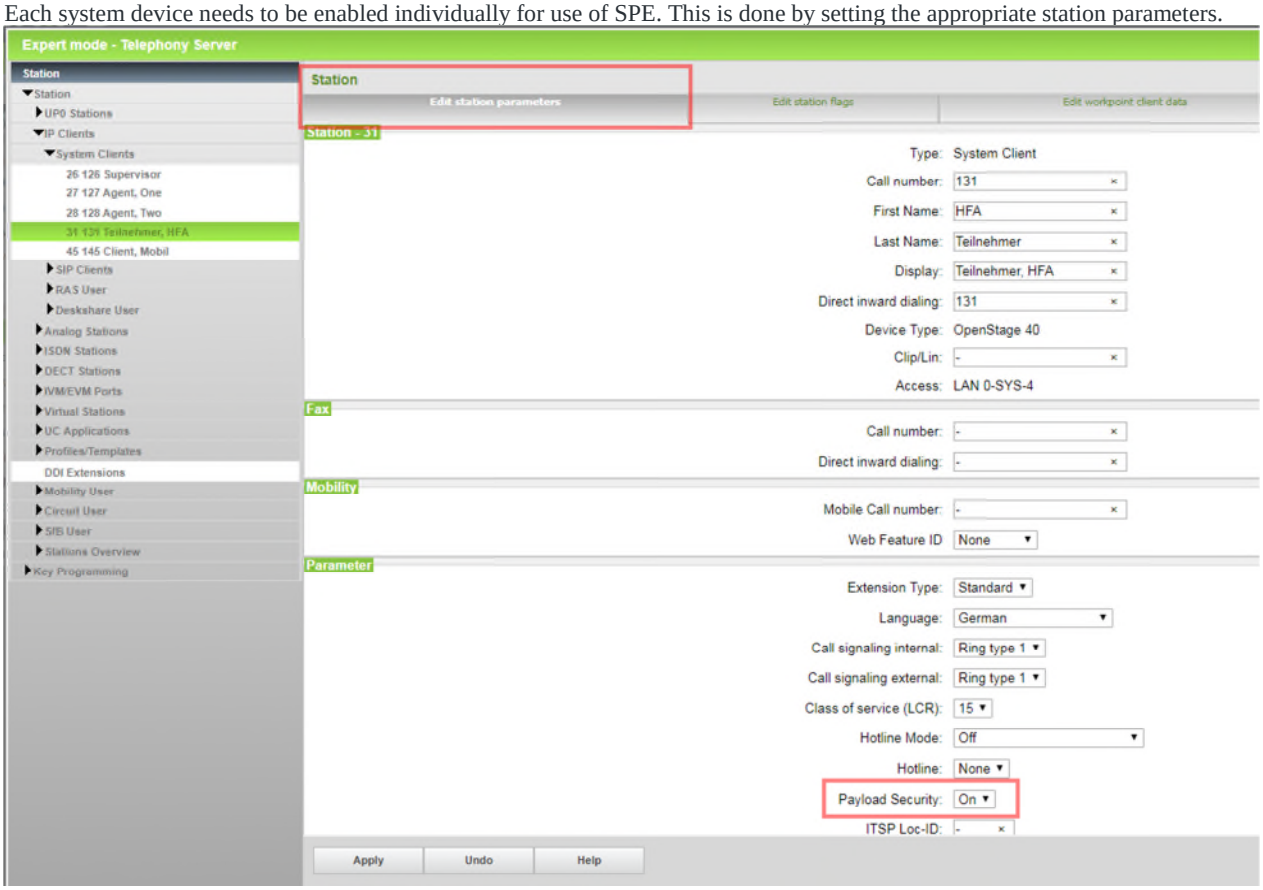
2.7.1. SPE Enabling for the system

The system flags enable the feature in general. A system restart is required to activate the settings.



2.7.2. SPE enabling for Stations

Each system device needs to be enabled individually for use of SPE. This is done by setting the appropriate station parameters.



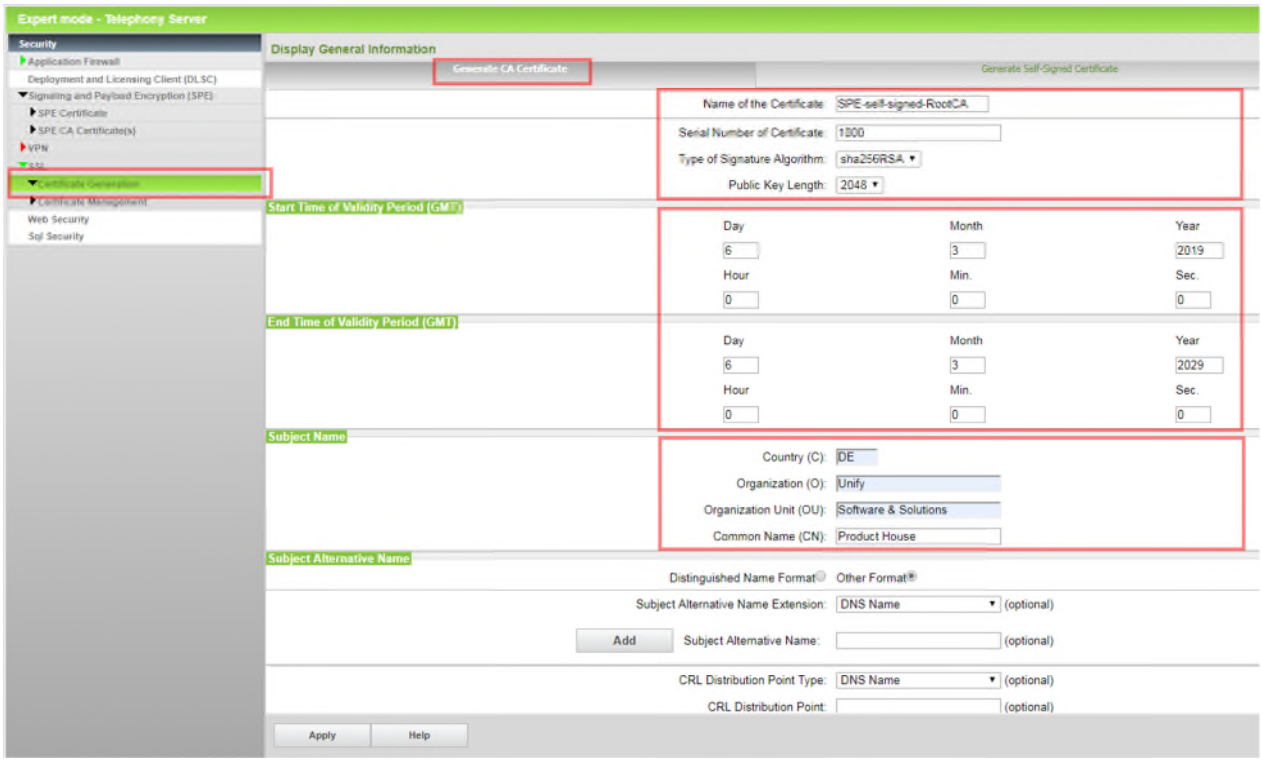
2.7.3. SPE Certificates

In a first step the minimal length of encryption keys used for SPE has to be defined and the certificate validation function has to be disabled.

2.7.3.1. Root CA Certificate Creation

In no Trust Center generated Root CA Certificate is available a self signed Root CA Certificate has to be created and imported into the SPE certificate store. This is done in Expert Mode: Telephony → Security → SSL → Certificate Generation → Generate CA Certifikate.

- Enter a name for the requested certificate under **Certificate Name** (Do not use blanks in the name).
- Enter a serial number of your choice under Serial Number of the Certificate
- A serial number that has already been assigned cannot be used again for another certificate, since the serial numbers for all certificates that were ever created must be unique.
- Under Type of Signature Algorithm, enter the desired algorithm for the certificate sha256RSA or sha512RSA.
- Under Public Key Length, enter the length of the public key e.g., 2048. This value must comply with the minimum key length for SPE that has been configured before)
- In the next step, enter the date and time for the start of the validity period under Start Time of Validity Period (GMT). The date specified is interpreted as Greenwich Mean Time (GMT).
- Enter the date and time for the end of the validity period under End Time of Validity Period (GMT).
- Under Subject Name, enter the Country (C), the Organization (O), the Organization Unit (OU) and Common Name (CN).
- Leaves the optional field at default values
    - You can optionally also enter an alternative subject name under the Subject Alternative Name field. If you have done this, you will also need to select a format (e.g., IP address or DNS name). The input window depends on the selected format.
    - Enter the distribution point for the CRL lists (listed in a drop-down menu) in the CRL Distribution Point field.

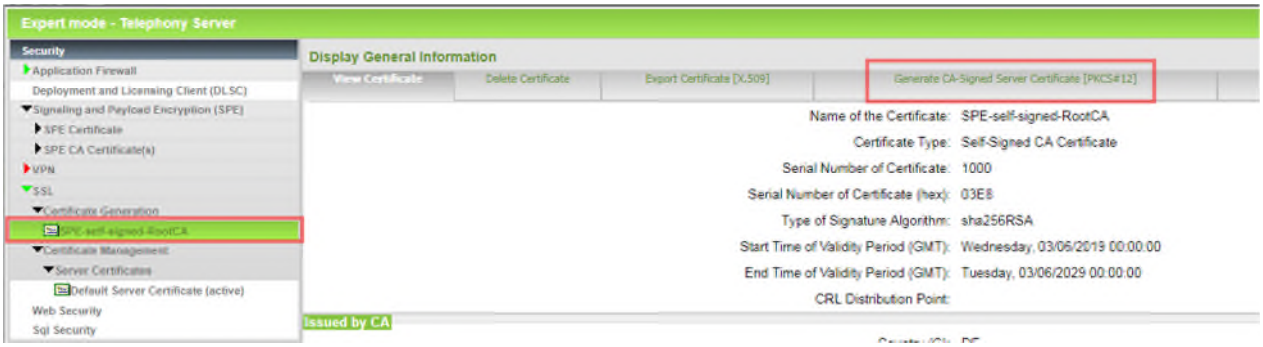


Click on Apply.

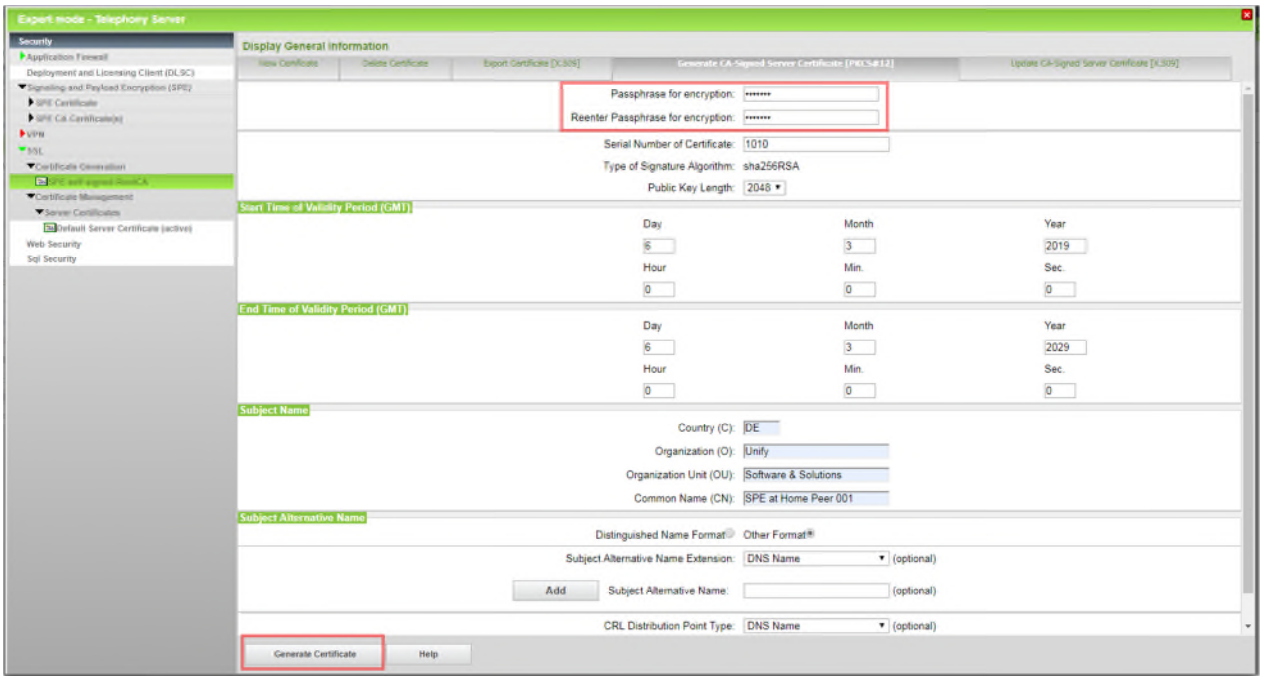
The self-signed Root CA Certificate is now available in the SSL certificate store.

2.7.3.2. Server (Peer) Certificate Creation

A double click to the Root CA Certificate name opens the certificate content and offers the option to create a Server (Peer) Certificate signed by the Root CA Certificate. Click to the Tab Generate CA-Signed Server Certifiate (PKCS#12).

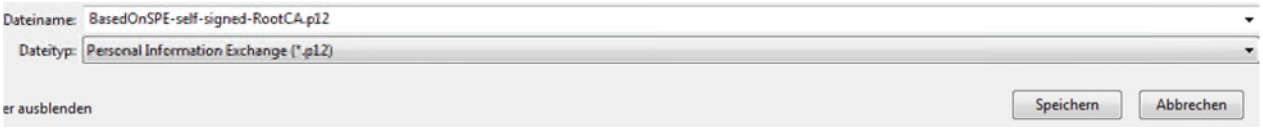


Fill in the data for the Server (Peer) Certificate. The requested passphrase is used to encrypt and to decrypt the file containing the certificate.



Click to **Generate Certificate**

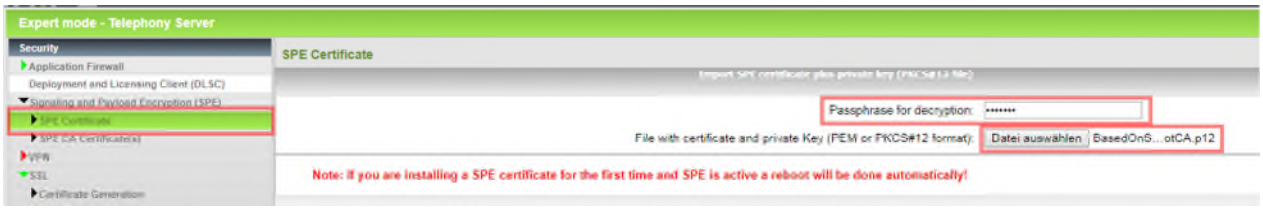
An encrypted .p12 file is created that contains the server certificate. The file can be stored on the admin PC for further use e.g. import or transport.



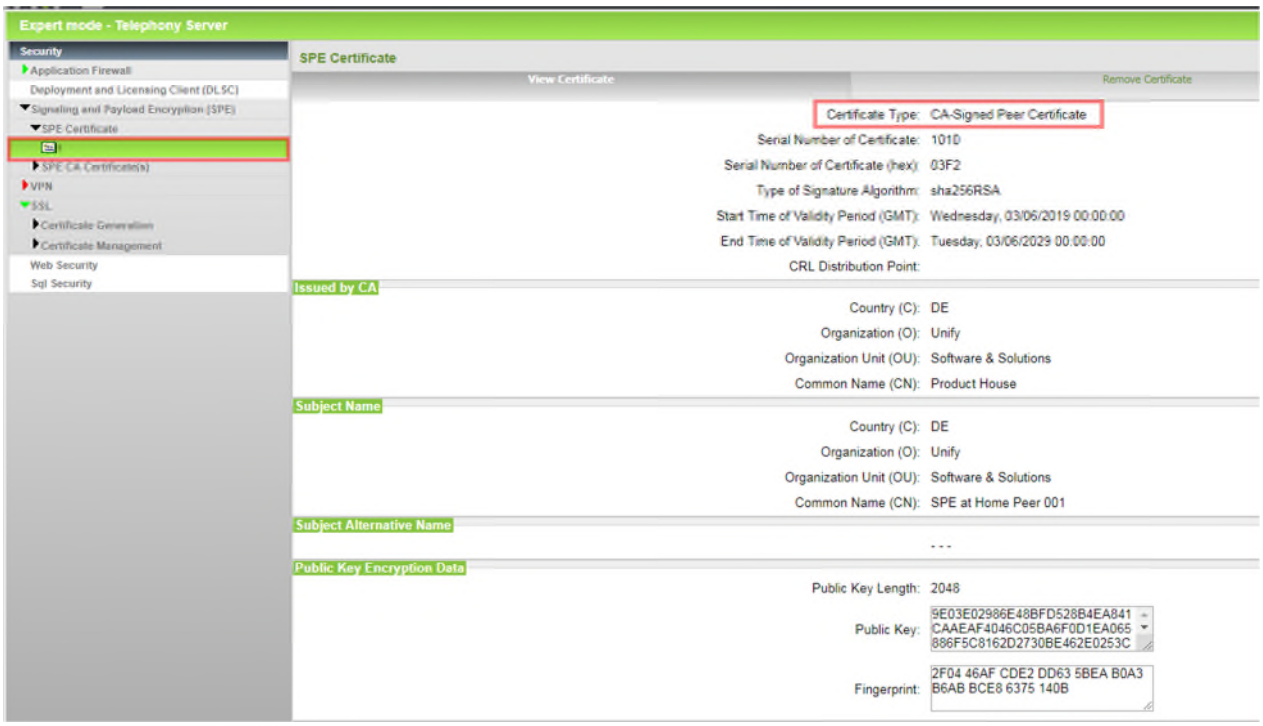
2.7.3.3. Server (Peer) Certificate Import

The generated server certificate has to be imported into the SPE certificate store.

This is in Expert Mode Telephony Server → Security → Signaling and Payload Encryption (SPE) → SPE Certificate.
Type in passphrase for decryption of the file and choose the previously stored .p12 file for import.



Click to **View Fingerprint** and to **Import Certificate from file** afterwards. The certificate is now imported in the SPE Server Certificate store. A click to the number of the imported certificated displays its content.



The certificate is used by the SPE function for encryption.

3. Company Internet Router Configuration

3.1. Port forwarding / firewall

The default configuration of the firewall within the Company Internet Router does not allow incoming VoIP traffic to the OpenScape Business system. Therefore the following port forwarding rules have to be defined within the router.

Protocol	Internal Port in system	External port (Internet)	Comment
HFA not encrypted	TCP/UDP 4062	TCP/UDP 4060	
HFA encrypted	TCP/UDP 4063	TCP/UDP 4061	
HTTPS	TCP/UDP 8802	TCP/UDP 8802	Port forwarding only if myPortal to go is used

DLI DLI HTTPS	TCP/UDP 18443 TCP 8804	TCP/UDP 18443 TCP 8804	Only if SW update is required for device @home
RTP	UDP/30274-30529 UDP/30528-30887	UDP/30274-30529 UDP/30528-30887	Port range for OSBiz X Port range for OSBiz S

Note:

No gateway port adaptation is required within the System Device@Home. All related settings are done within the company router.

3.2. Internet access with dynamic IP Address (DynDNS)

In case that the Internet Service Provider provides only a dynamic IP address (DynDNS) instead of a static IP address for the Internet connection of the company, appropriate means have to be taken into account to publish the current IP address of the company.

This can be achieved by using a dynamic DNS service like DynDNS. The Company Internet Router has to be configured with the dynamic DNS account data, which are supplied by the service provider.

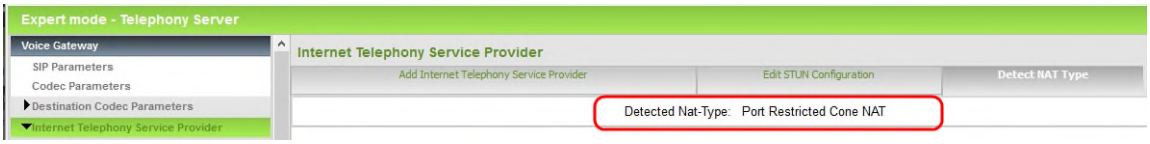
Note:

Usually dynamic DNS accounts which are free of charge expire in regular intervals without manual reconfirmation. This will cause an outage of the Device@Home feature.

3.3. NAT type

The System Device@Home feature does not work in combination with company internet routers or home routers with NAT type ”Symmetric NAT”.

The NAT type detection option within OpenScape Business can be used to determine the configured NAT type of the company internet router. If possible please change the NAT behavior of the router, in case that “Symmetric NAT” is detected by OpenScape Business.



Note: The NAT type detection of the OpenScape Business (may falsely detect the NAT type of the Company router as “Symmetric NAT” if outbound IP traffic is restricted in the Company router. Please make sure that the ports listed above are open in outbound direction as well.

4. System Device configuration

The feature System Device@Home is supported by the following devices and clients:

Device / Client	Minimum software version
OpenStage HFA	V3 R0.40.4
Desk Phone IP HFA	V3 R0.40.4
DeskPhone CP HFA	V1 R2.8.0
myPortal to go (Android) VoIP	V2R2.26.19
myPortal to go (iOS) VoIP	V2R5.11.01

4.1. System Device Configuration

Network

IP configuration

- IP address of the device in the home network
  = either fixed IP address manually entered or DHCP

System

Gateway

- IP address either
  = Public IPv4 address of the OpenScape Business (if available via a fix IP address) or
  Public DNS name of the OpenScape Business.
- Subscriber number / Identity
  = Internal phone number
- Password
  = Password as configured for device authentication within OpenScape Business

Security (optional if SPE is used)

- System
  - Signalling transport main = TLS
  - TLS renegotiation = Secure (RFC5746)

Date and Time

Source = System

Network

Update Service DLS

Update Service / DLS: = public IP address of OSBiz [fix IP address]

4.2. myPortal to go VoIP Client configuration

User Account

WAN server IP address = Public IP or DNS name of the OpenScape Business

WAN server IP port = 8802 or other port according to the port forwarding in the Company Internet Router.

Optionally: User Account

LAN server IP address = Internal IP address of OpenScape Business in your company WiFi

LAN server IP port = 8802

More VoIP settings

Enable “VoIP” flag

Enable “Use VoIP in remote WiFi networks” flag

Note:

myPortal to go VoIP is only available in WiFi environments, but not via mobile data connections (3G/4G/...). A successful VoIP registration is shown in the status field of the VoIP settings menu.

5. Home Internet Router

Usually no specific configuration is necessary for the System Device@Home feature in the Home Internet Router. The router MUST comply with the following requirements:

- The Home router must provide VoIP enabled NAT (no symmetric NAT) ,
- The ALG function in the router must be deactivated, if available.

Note:

It has to be ensured that the Home Internet connection provides sufficient bandwidth for real time traffic. This applies especially for asymmetric DSL connections, which may have reduced upload bandwidth.

6. Security considerations

The System Device@Home feature is designed to be a cost effective option to connect home- and mobile worker etc. to OpenScape Business. It provides following security measures

Client type	Security level
System Device@Home	- Access control by device / user authentication secured by enforced password - Signalling and payload encryption by SPE feature - Use of different IP ports for internally and externally connected system devices
myPortal to go @Home	- Authentication via encrypted UC password - Signalling encryption via SSL (HTTPS) - Payload encryption currently not supported.

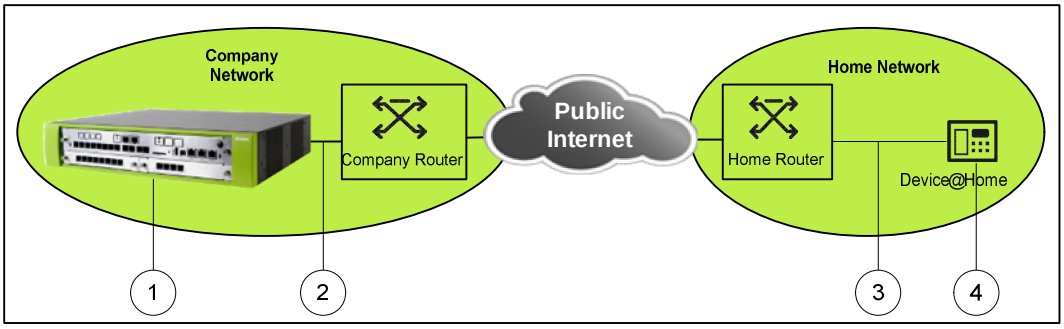
The System Device@Home feature is **not** applicable for:

Environments with strict router/firewall policies where port forwarding from the internet are not allowed or symmetric NAT is in place. In this case, a VPN infrastructure between the central office and the home / mobile worker has to be considered.

Note:

It is recommended to use myPortal to go VoIP only in trusted WiFi environments (company, home office, ...).

7. Troubleshooting



In case of connection problems the following traces are needed. The numbers within the figure demonstrate which the physical location of the data which are traced.

1. Internal trace from OpenScape Business with the following Trace profiles activated:
   - Voice_Fax_connection
   - SIP_Interconnection_Subscriber_ITSP
   - Calls_with_System_Device_HFA
   - CSTA_applications (when using myPortal to go)
2. If myPortal to go is used please provide additionally:
   - Application trace from OpenScape Business
   - myPortal to go client trace via the feedback option in the app (currently only available with Android)
3. Wireshark trace capturing the traffic between the office router and the OpenScape Business system. This could be a TCP-dump from the router or a capture taken from the LAN
4. Wireshark trace from the remote location capturing the traffic between the affected HFA phone and the Home-/SOHO-Router. This could be a TCP-dump from the router (if supported) or a capture taken from the LAN
5. Information about Setup, e.g.
   Used device (type and software release) at remote location
   Used router at remote location
   Used router at office location
   List of IP addresses of all involved entities (HFA phone, smart phone, routers, OpenScape Business system)

8. Abbreviations

ALG	Application Layer Gateway
CO	Central Office
HFA	HiPath Feature Access (protocol)
HTTPS	Hypertext Transport Protocol Secure
IP	Internet Protocol
ITSP	Internet Telephone Service Provider
LAN	Local Area Network
NAT	Network Address Translation
SBC	Session Boarder Controller
SIP	Session Initiation Protocol
OSBiz X	OpenScape Business X model
OSBiz S	OpenScape Business Server model
SPE	Signaling and Payload Encryption
STUN	Session Traversal Utilities for NAT
VoIP	Voice over IP
WAN	Wide Area Network

unify
atos collaboration solutions