UNIFY Harmonize your enterprise

OpenScape Business V2

Tutorial

Support of SIP Endpoints connected via the internet

Version 2.1

Definitions

HowTo

An OpenScape Business HowTo describes the configuration of an OpenScape Business feature within the OpenScape Business administration. It addresses primarily trained administrators of OpenScape Business.

Tutorial

Within the OpenScape Business tutorials procedures for installation, administration and operation of specific devices, applications or systems, which are connected to OpenScape Business, are described. The tutorial addresses primarily trained administrators of OpenScape Business.

Table of Contents

Table of History

Date	Version	Changes
2014-11-28	1.0	Initial Creation for V1R3.2
2014-12-08	1.0.1	Minor editorial corrections
2015-02-10	2.0	Add TLS support for V2.0
2015-03-30	2.1	Add technical details

1. Feature description

With OpenScape Business V1R3.2 the new feature "**SIP@Home for STUN enabled SIP endpoints**" is introduced.

This feature will allow you to register SIP endpoints not only in the local office network, in addition they can register over the internet.

This document describes the necessary configuration steps to setup connections between SIP-Endpoints and OpenScape Business over the internet. A typical environment is shown in the following figure:

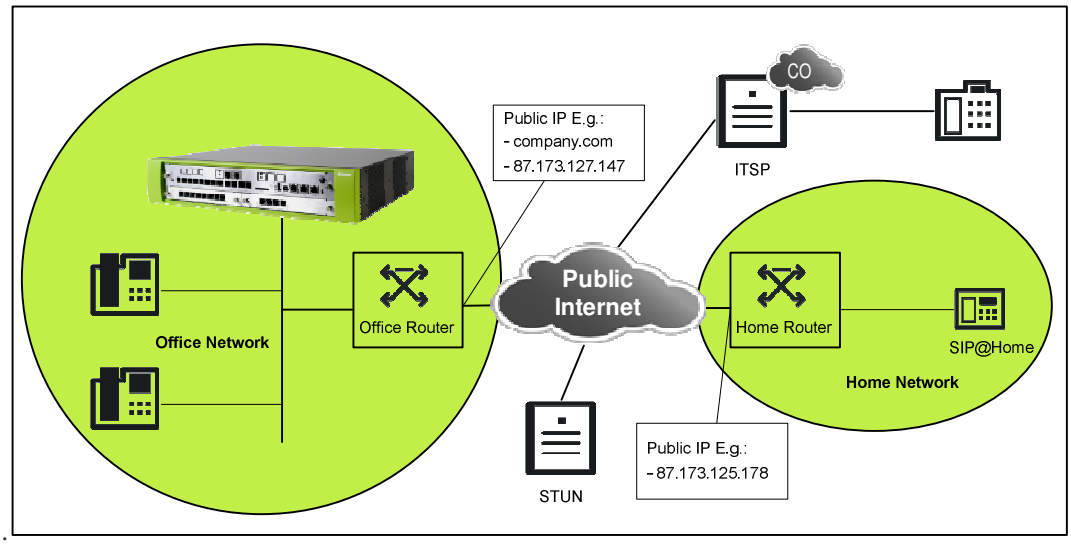


Figure 1 Use case scenario

Connecting SIP endpoints to OpenScape Business requires careful configuration of

- OpenScape Business system
- Office Router
- SIP endpoint

In OpenScape Business you need to allow a SIP endpoint to register over the internet by activating the integrated SBC function for that endpoint (see 2.1). In addition you may activate STUN support if not already used for an ITSP connected to OpenScape Business (see 2.3)

As an endpoint must reach the OpenScape Business system from the Internet you have to configure a port forwarding rule in your office router. (see 3)

Last but not least a SIP endpoint connected over the internet needs appropriate configuration and MUST support STUN (see 4)

In addition to these configuration hints this document provides you with helpful information regarding supported configurations and known limitations.

2. OpenScape Business configuration

2.1. Internet access: supported configurations

There are different possibilities to connect the OpenScape Business system to the internet. The following configurations are supported in a scenario where SIP subscribers shall be able do register via the internet:

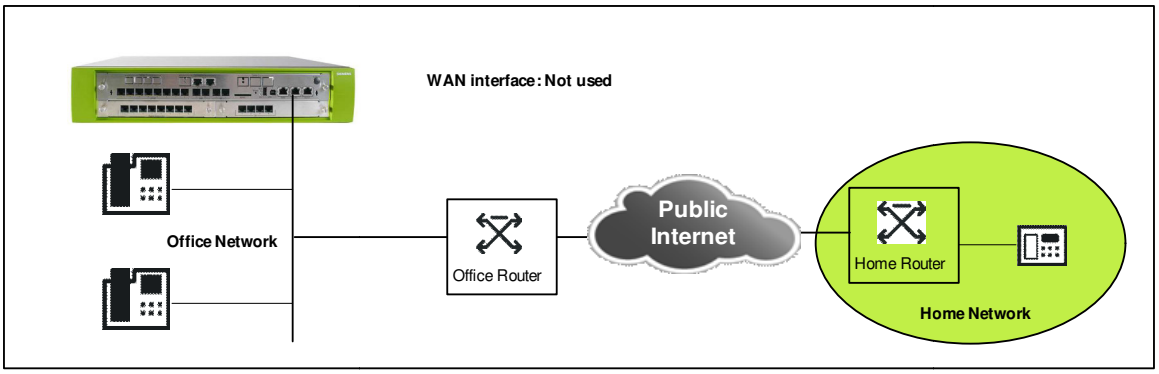


Figure 2 OpenScape Business behind access router connected to LAN2 interface

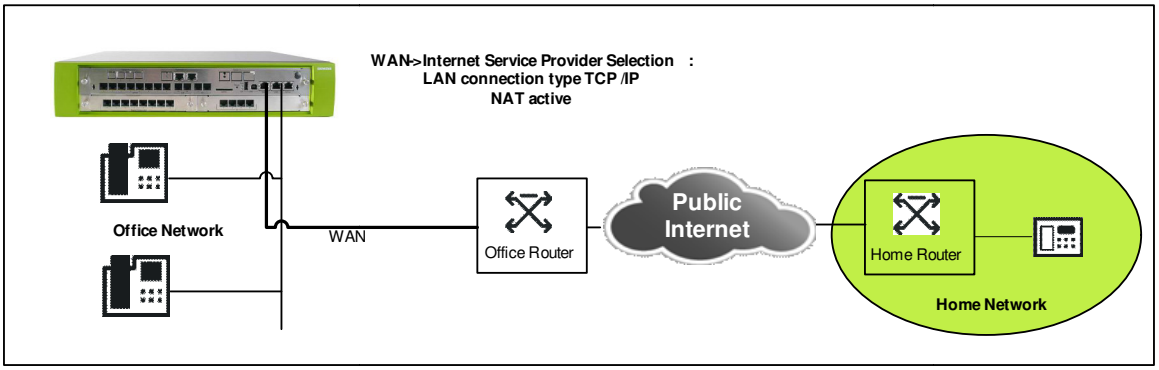


Figure 3 OpenScape Business behind access router connected to LAN1 (WAN) interface

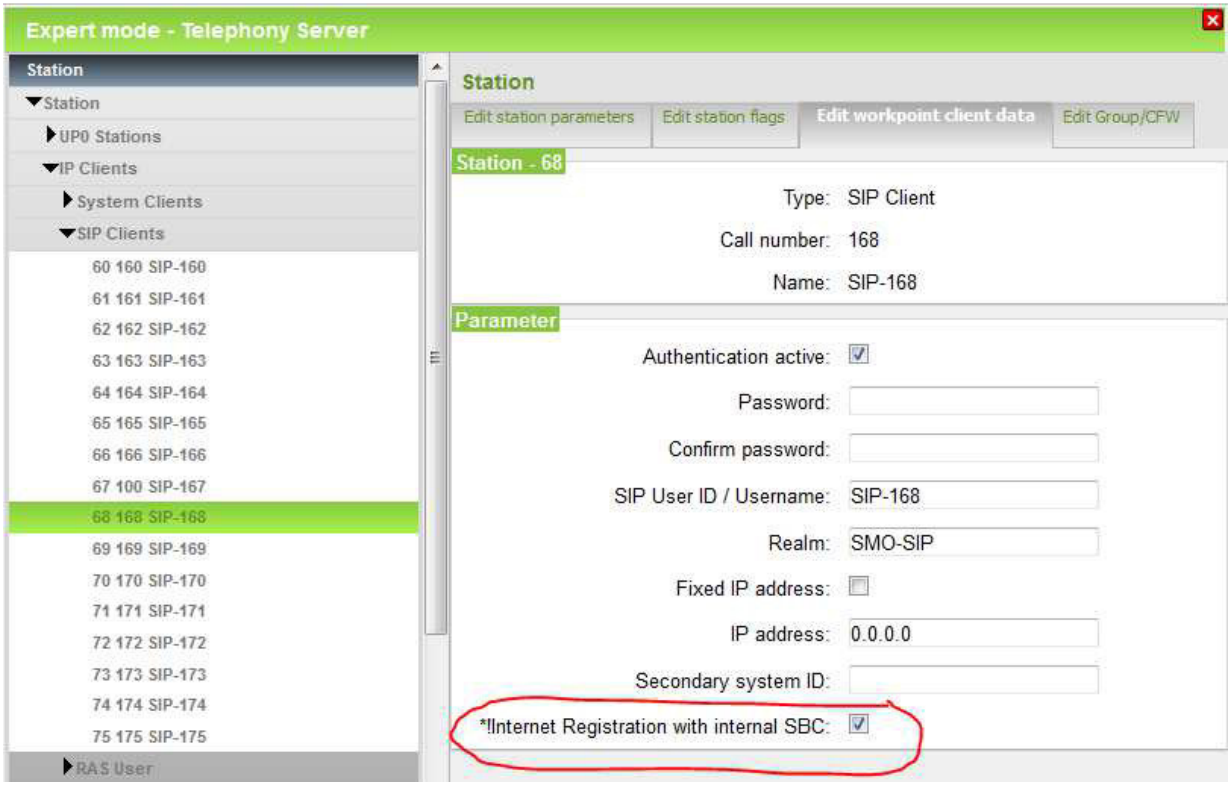
	Internet connections using the OpenScape Business as access router behind a modem connected to the WAN interface are NOT supported.

2.2. Configuring a SIP Endpoint to be used from the internet

Please consult the administration manual for a description how to do the basic setup for SIP endpoints.

In addition to that basic configuration the following setting in "Expert Mode" is necessary.

For an endpoint which should be allowed to register over the internet the flag "**Internet Registration with internal SBC**" MUST be checked.



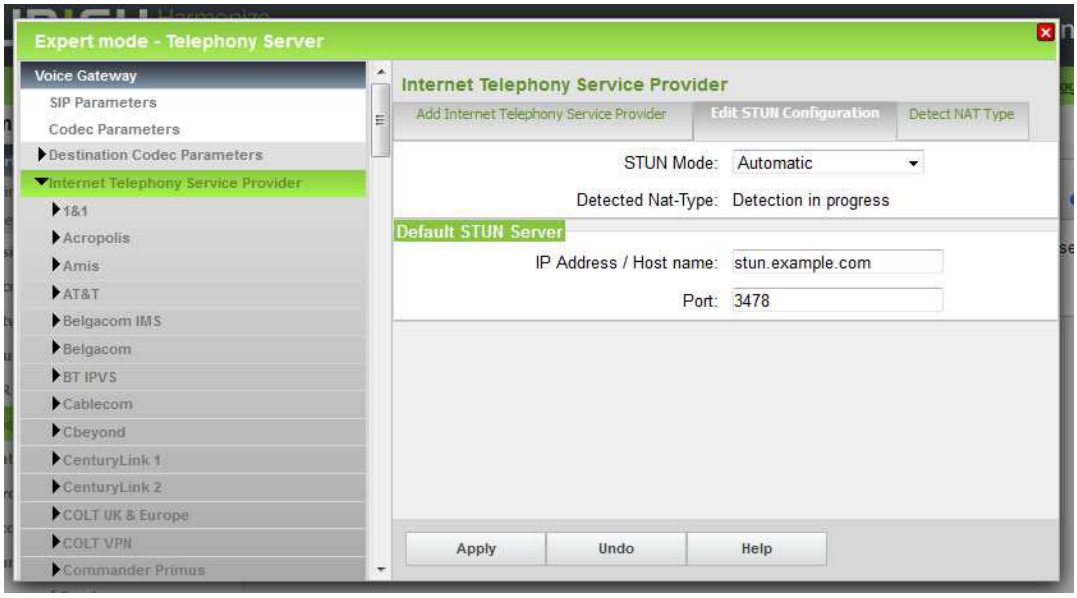
As this station is accessible from the internet make sure that a **STRONG PASSWORD** is used. In addition you may reduce the rights of such a station e.g. to forbid dialing premium or international numbers.

2.3. Configuring STUN

The integrated SBC function of OpenScape Business must be able to detect its public IP-address and SIP port. This is done using the STUN protocol.

- In case the system is already connected to an ITSP with activated STUN server, no additional configuration is necessary. The system is able to detect it's public IP-address and port
- In case the system is connected to an
  - ITSP with STUN switched off or
  - no ITSP is configured in the system,

  additional configuration is necessary enabling the system to detect it's public IP-address and port.
  As shown in the following screenshot, the default STUN server has to be configured in the STUN configuration



The STUN server configured in "Edit STUN Configuration" will be used only if NO STUN server is configured for an ITSP

2.4. Port configuration

No special configuration is needed; the following default ports are used for SIP signalling:

Transport protocol	Default port
UDP / TCP	5060
TLS	5062 (**Attention!** default TLS port 5061 is used for SIPQ trunking)

2.5. General hints

- Internet access

If SIP subscribers registering via internet and ITSP connections are used in parallel all VoIP traffic must use the same interface of OpenScape Business. It is NOT allowed to have a configuration where e.g. the ITSP is connected via WAN (using a static route) and public internet access is realized via LAN interface.

- Holding a remote SIP endpoint:

Due to the fact that RTP streams are necessary to keep firewalls open during a call, the integrated SBC must change sendonly media direction attributes to sendrecv media direction when the HOLD feature is invoked by an office phone. As a consequence the SIP endpoint has no indication to display the hold state.

- Using TLS transport

When TLS transport should be used to connect remote endpoints, the OpenScape Business system must be setup with valid certificates. See appendix for configuration hints.

3. Office Router configuration

3.1. Port forwarding / firewall

In default configuration the firewall in the office router will NOT allow incoming traffic to the OpenScape Business system, thus appropriate port forwarding rules for the SIP port MUST be configured in the router.

Transport protocol	Port in system	External port	
UDP	5060	5070	**SHOULD** be different from default SIP port in system
TCP	5060	5060	**MUST** be same as port in system, **not recommended**!
TLS	5062	5062	MUST be same as port in system!

As SIP attacks are always present in the internet, it is recommended to use a port different from the default SIP port (5060) towards the internet.

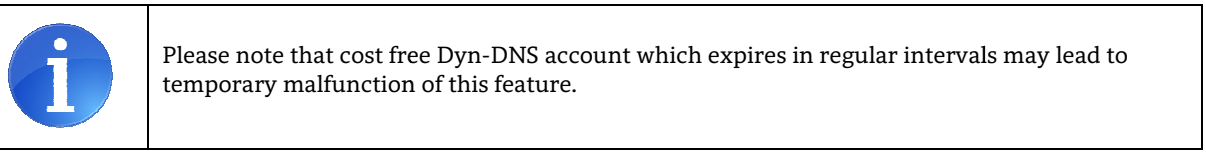
For **UDP** this can be achieved by defining the port forwarding with a different port (e.g. 5070 like shown above). The systems SIP port can stay in default 5060.

For TLS the system already uses a different port (5062). The default SIP-TLS port (5061) is already in use for secure trunking connections in OpenScape Business networks.

TCP transport is not recommended for SIP over the internet, as this needs reconfiguration of the system SIP port (5060) which may result in the need of reconfiguring all local SIP endpoints and networked systems.

3.2. DynDNS / Internet access with dynamic IP Address

If the Office router is connected to the ISP without a fixed IP-Address, appropriate measures are needed to reach OpenScape Business from the client. This can be achieved by using dynamic DNS. The router has to be configured with the DynDNS account and must register the current IP address in regular intervals.



Please note that cost free Dyn-DNS account which expires in regular intervals may lead to temporary malfunction of this feature.

4. SIP Endpoint configuration

The SIP endpoints used for this feature MUST comply with the following requirements:

- Detect own public IP address and port (STUN)
- Use correct public IP:Port in Contact: header field
  (port determined by for UDP, ephemeral (client) port for TCP)
- Use correct public IP in c: line of SDP
- Use correct public RTP port in m: line of SDP
- Keep NAT bindings active
- Start sending RTP payload
- Use sip: URIs (tel:-URIs are not supported for this feature)

The following endpoints have been tested at Unify and fulfill the above requirements

4.1. Yealink T19P

Yealink's SIP-T19P entry-level IP phone:
http://yealink.com/product_info.aspx?ProductsCateID=334

Tested SW Version:

The mentioned SW version (**31.72.0.48**) contains important fixes for the use of this feature, other 31.72.x.x versions (including newer versions available on the Yealink download page) cannot be used!
The V7-Unify software is available in the Wiki on the same page where this document is stored.

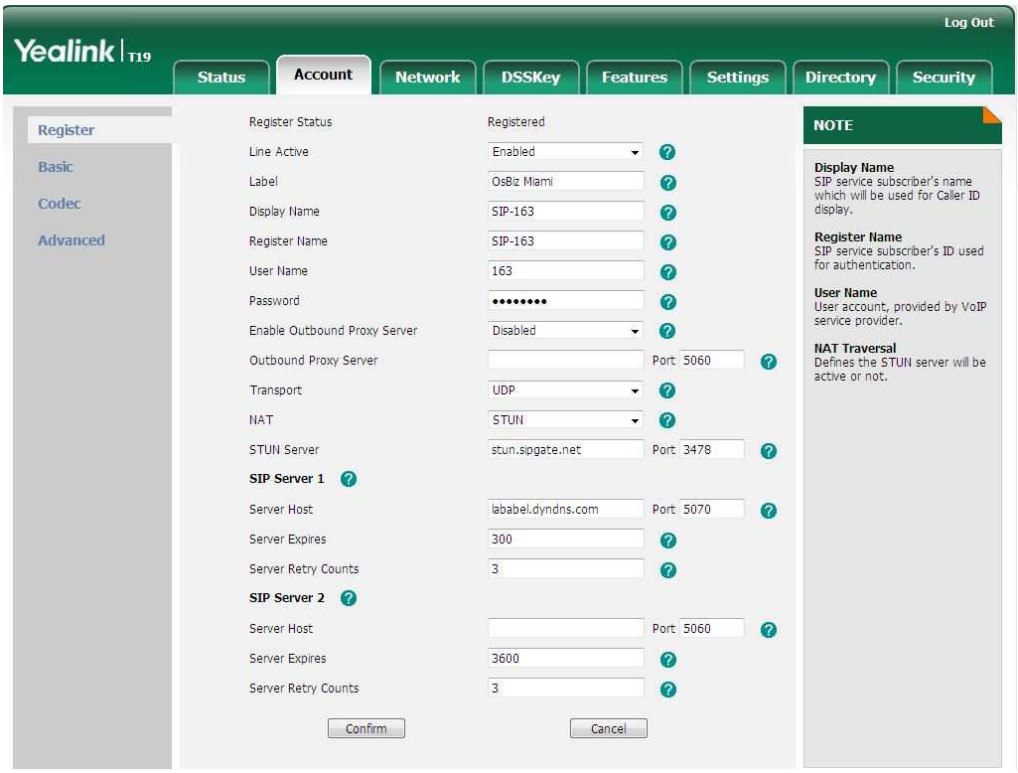
The functionality will be release by Yealink with V8 in the first quarter of 2015.

Account Configuration:
In this tab all data for the used account and SIP server is entered

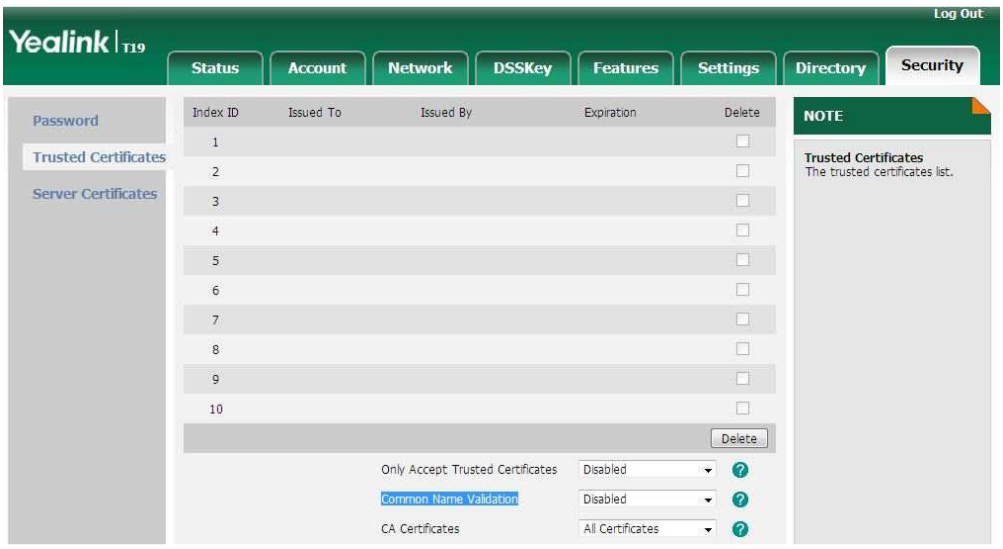
Phone Configuration parameter	**configured in OpenScape Business:** **Telephones / Subscribers-> IP Telephones -> Edit**
Display Name	Optional, Phone name can only be seen in the network traces, OpenScape Business uses the name configured in system
Register name	SIP User ID / Username
User Name	Call number
Password	Password
Transport	Choose the used transport for your deployment: UDP

Phone Configuration parameter	
NAT	MUST be set to STUN
STUN Server	Enter a reachable STUN server (e.g. stun.sipgate.net) and the STUN port (default 3478).

	A list of public available STUN server is available at e.g. http://www.voip-info.org/wiki/view/STUN
Server Host	Public IP-Address or DNS name of OpenScape Business
Port	SIP Port which is configured at the office router (please note the rules defined for port forwarding in Chap. 3.1)



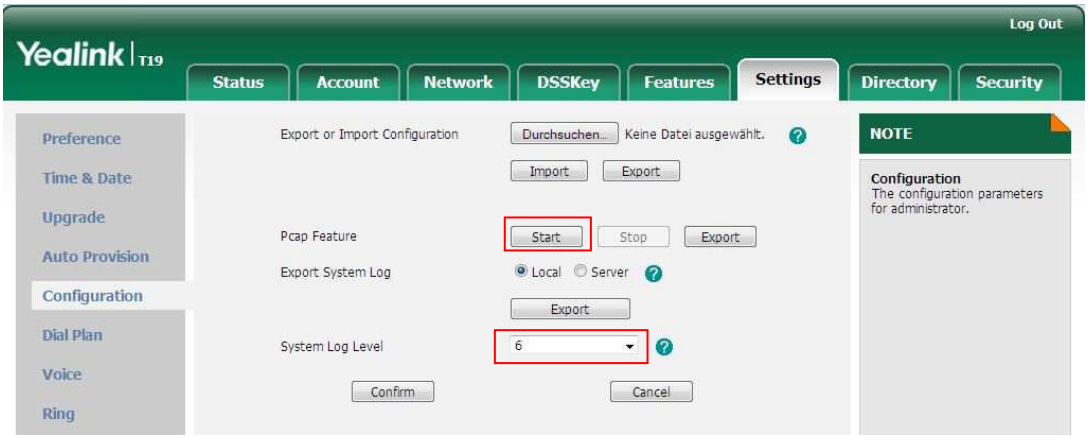
Special hints for configuring TLS transport:



Disable "Common Name validation"

Hints for troubleshooting:

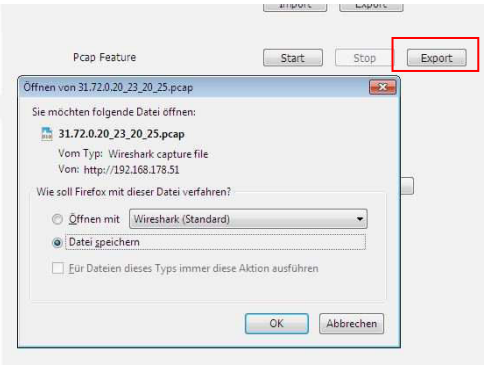
If a Yealink phone is used, the traces at the remote location can be taken directly from the phones WBM. Start the Pcap Feature and set the system Log Level to 6:



Run the scenario where you observed a problem.

At the end “Stop” the Pcap and “Export” it to a file.

In addition “Export” the System log.



4.2. Yealink T41P

Yealink's SIP-T41P feature-rich sip phone for business
http://yealink.com/product_info.aspx?ProductsCateID=313&CateId=147&BaseInfoCateId=313&Cate_Id=313&parentcateid=147

Tested SW Version:

The mentioned SW version (**36.72.0.57**) contains important fixes for the use of this feature, other 36.72.x.x versions (including newer versions available on the Yealink download page) cannot be used!
The V7-Unify software is available in the Wiki on the same page where this document is stored.
The functionality will be release by Yealink with V8 in the first quarter of 2015.

Account Configuration:
For T41 the same data have to be entered as for the T19 model.

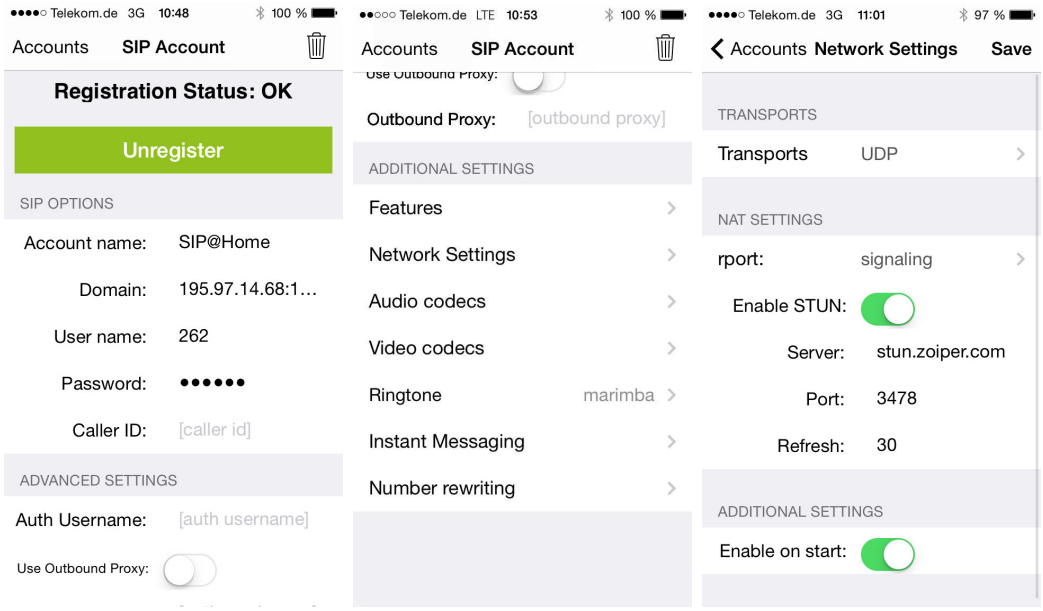
4.3. Zoiper IOS App

Zoiper is a VoIP softphone that lets you make voice calls with your friends, family, colleagues and business partners.:
http://www.zoiper.com/en/voip-softphone/download/zoiper3

Tested SW Version: 2.17

Account Configuration:
Go to Accounts: Create Account -> SIP account
In this tab all data for the used account and SIP server is entered

Phone Configuration parameter	**configured in OpenScape Business:** **Telephones / Subscribers-> IP Telephones -> Edit**
SIP OPTIONS	
Account Name	Optional, Phone name can only be seen in the network traces, OpenScape Business uses the name configured in system
Domain	Public IP-Address or DNS name of OpenScape Business and SIP Port which is configured at the office router (please note the rules defined for port forwarding in Chap. 3.1)
User Name	Call number
Password	Password
Caller ID	
ADVANCED SETTINGS	
Auth Username	SIP User ID / Username
ADDITIONAL SETTINGS -> Network settings	
Transport	UDP is offered in default, keep this setting
Enable STUN	MUST be activated



5. Home-/SOHO-Router

No specific configuration is necessary for this feature in the Home router.

The Home router used for this feature MUST comply with the following requirements:

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

Please make sure that there is sufficient bandwidth available for real time traffic at the remote location. This needs to be taken into account when e.g. using asymmetric DSL connections, which may have reduced upload speed.

6. Known restrictions and limitations

6.1. Use of video is not possible

The implementation of the integrated SBC-light allows for a single media stream per session. It does NOT allow using more than 1 media stream (e.g. voice and video).

6.2. Use of endpoints without STUN support is not possible

The implementation of the integrated SBC-light relies on correct signaling information in terms of SIP signaling and media addresses. It does NOT allow the connection of phones which do not provide correct public IP address information when connected behind a router (e.g. phones without STUN capability).

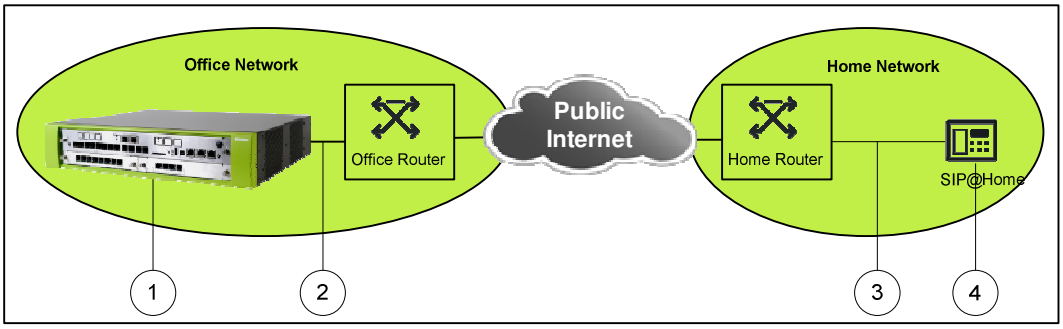
6.3. Use of secured connections

TLS connections for SIP subscribers are supported at the LAN interface of the OpenScape Business system only.

TLS at the WAN interface is NOT supported.

SRTP payload using SDES signalling is NOT supported

7. Troubleshooting



As this feature connects several networks for a connection, in case of connection problems the following traces are needed:

1. Internal trace from OpenScape Business with the following Trace profiles activated:
   - Voice_Fax_connection
   - SIP_Interconnection_Subscriber_ITSP
   - SIP_Registration
2. 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
3. Wireshark trace from the remote location capturing the traffic between the affected SIP phone and the Home-/SOHO-Router. This could be a TCP-dump from the router or a capture taken from the LAN
4. When available diagnostic logs/trace from the device at remote location
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 (phone, routers, OSBiz system)

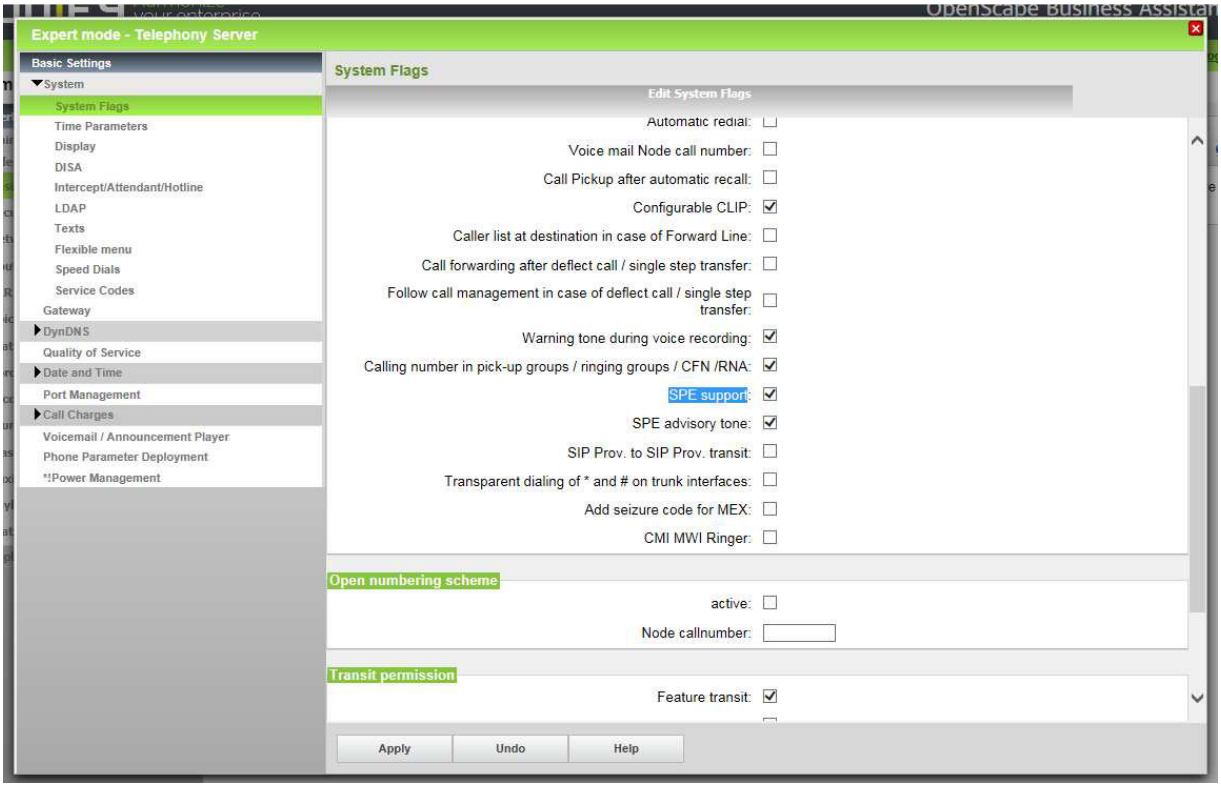
8. Appendix

8.1. Configuration for use of TLS

8.1.1. Security configuration

The system flag "*SPE support*" has to be activated under

Basic settings -> System -> System Flags

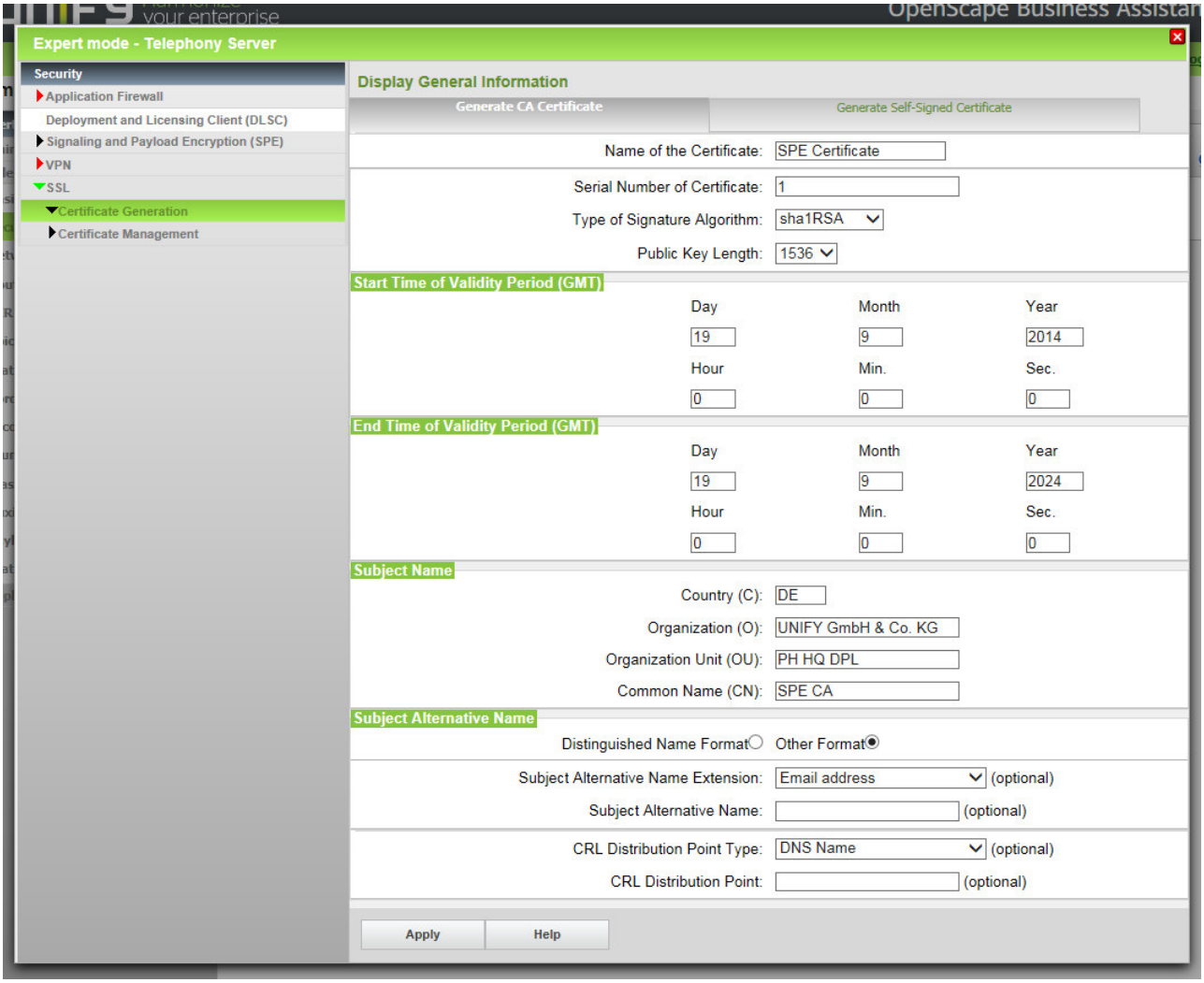


8.1.2. Certificate generation

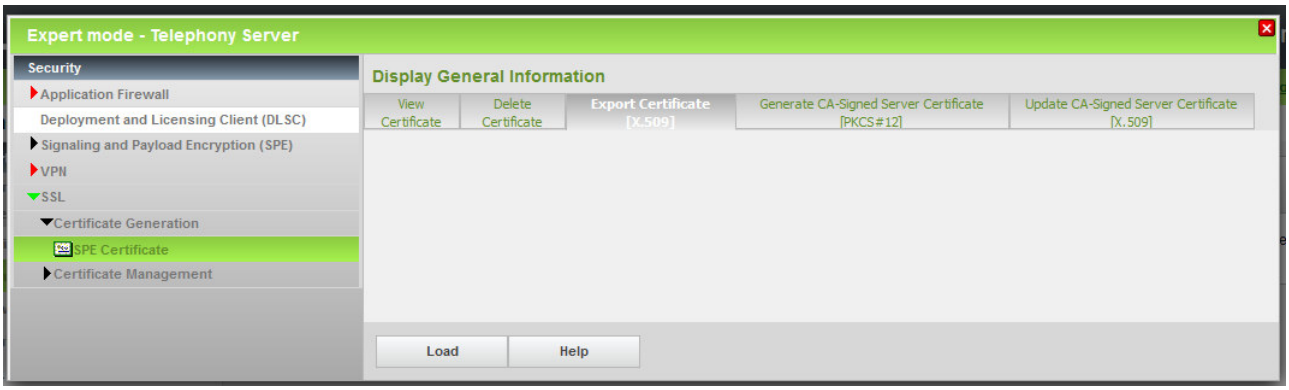
For SIP devices OpenScape Business acts as a TLS server and thus needs to have a TLS server certificate. You may install you own certificate if available (e.g. provided by ITSP) or create a new one. The following steps describe how to create a self signed server certificate.

	With the current implementation only one certificate can be installed for all SIP interfaces (ITSP, SIPQ-interconnection, SIPQ-trunk, SIP subscriber).

First a "CA Certificate" has to be generated. Navigate to Security->SSL-> Certificate Generation and open the "Generate **a CA Certificate" page. Enter the corresponding data and apply the changes. As a result the certificate is stored on the** OpenScape Business system.

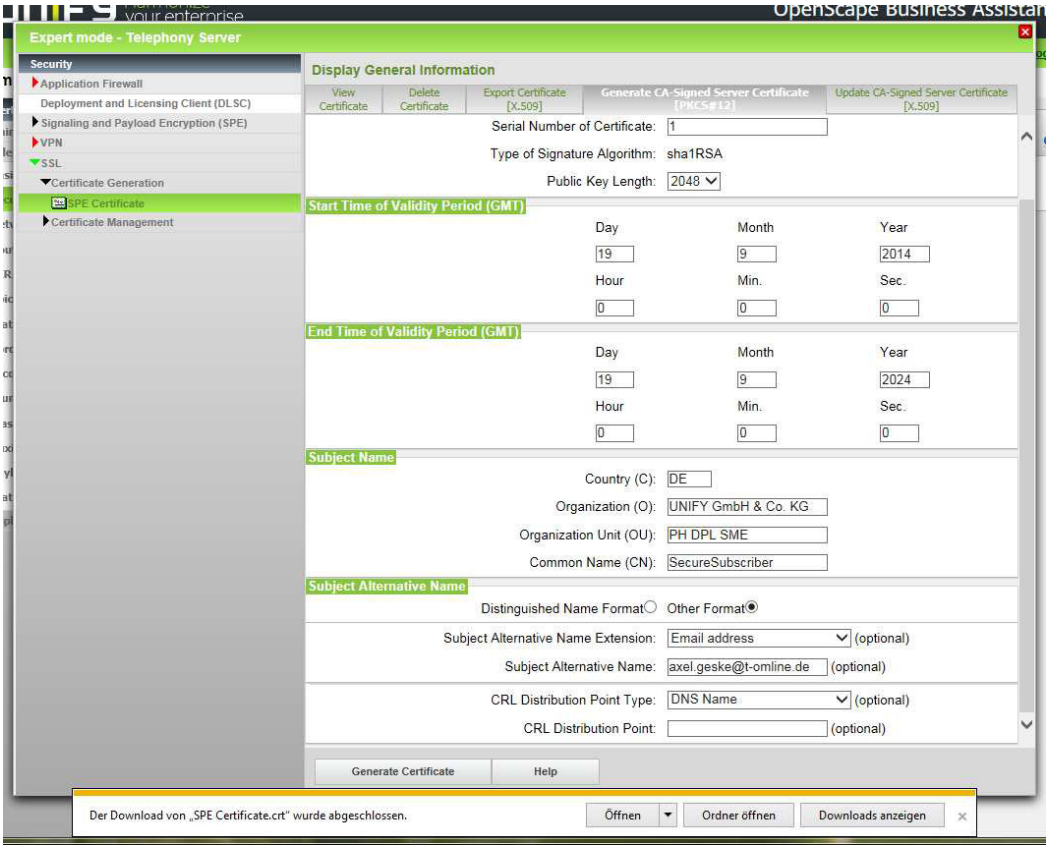


In the next step the “CA Certificate“ has to be exported in X.509 format



Choose and appropriate place on your computer to store the CA certificate (default name: Common Name.crt).

Now the CA signed server certificate can be generated and exported in PKCS#12 format.



The server certificate is stored as BasedOn”Common Name”.p12

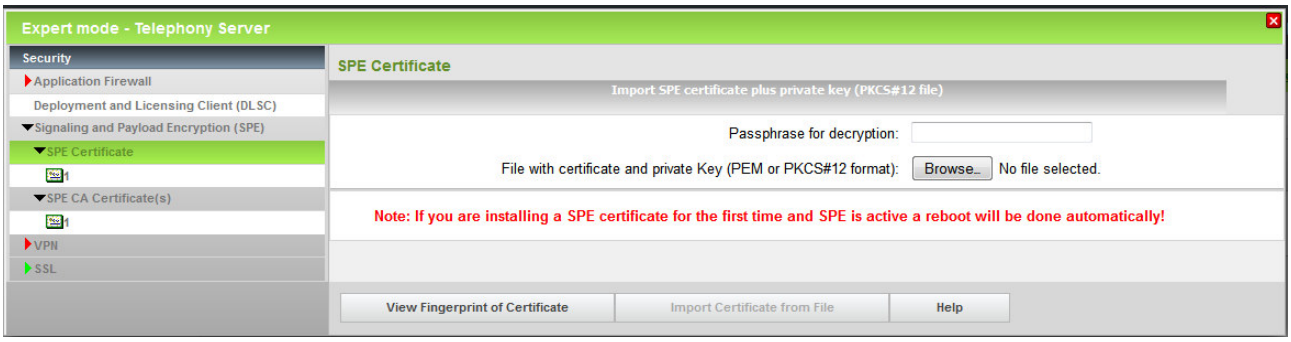
After this step two files are present::

1. CA certificate ”Common Name”.crt
2. PKCS#12 Certificate BasedOn”Common Name”.p12

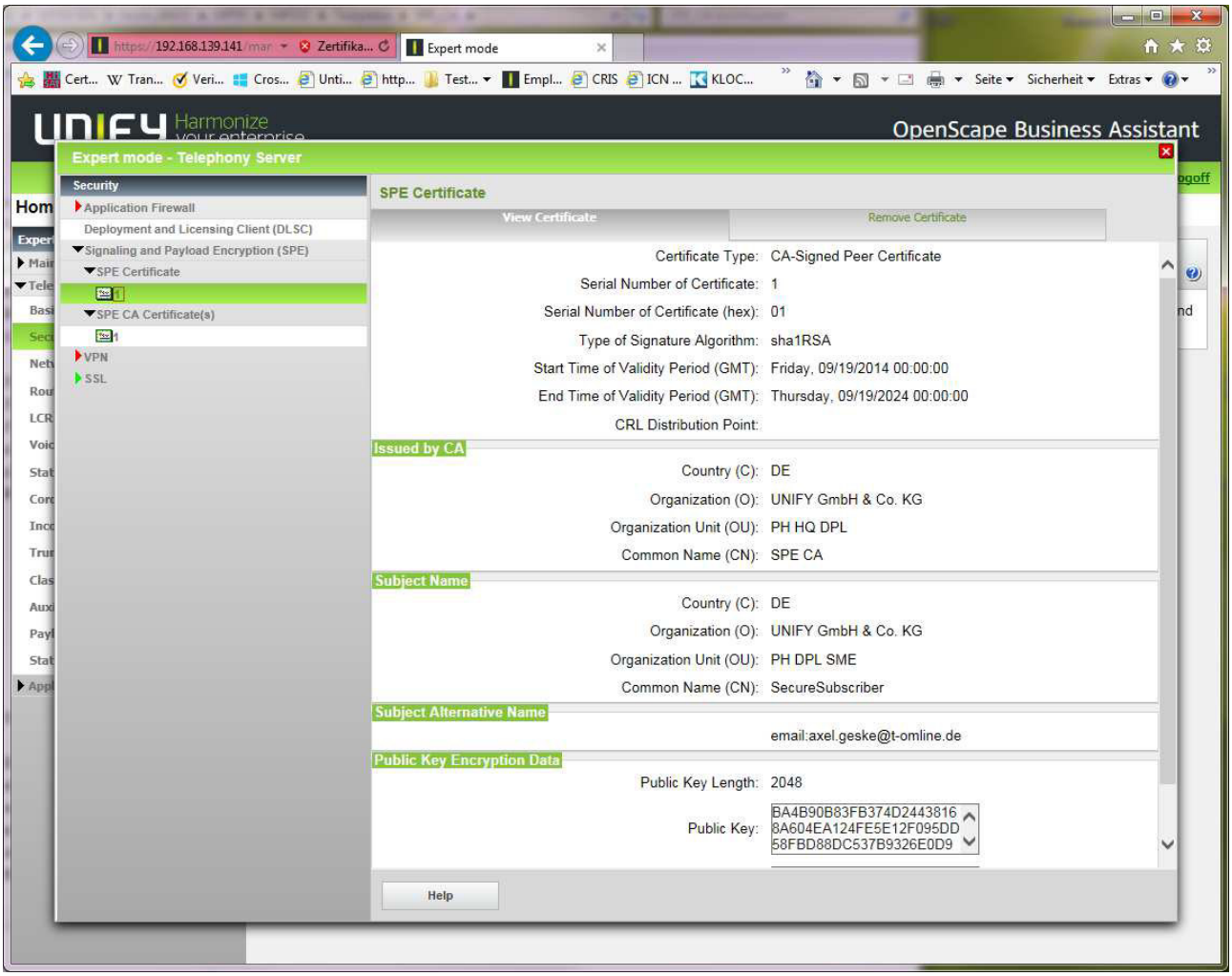
With these certificates the OpenScape Business system can be configured to act as a TLS server.

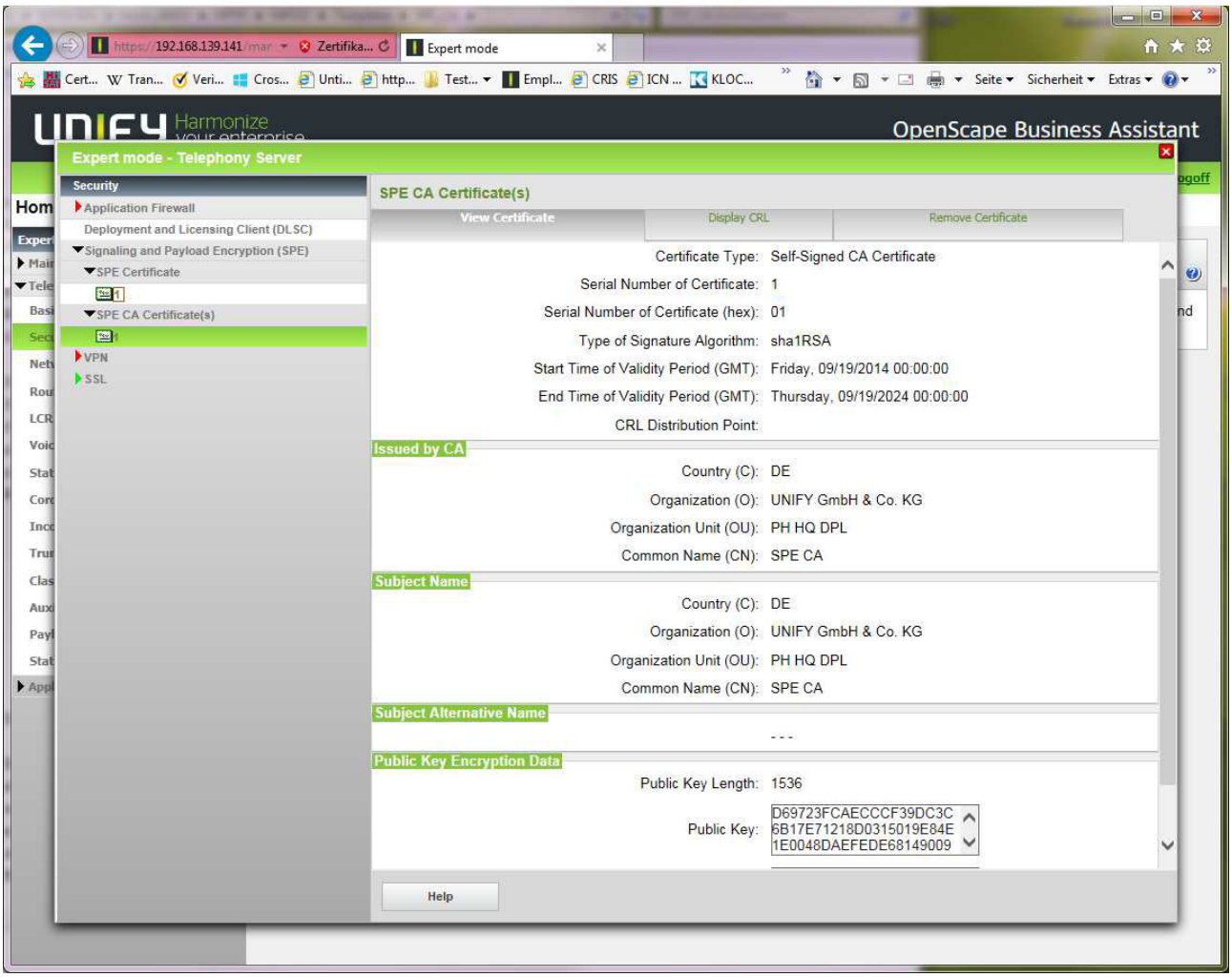
8.1.3. Certificate configuration

The Certificate and CA Certificate generated as described in the previous chapter has to be installed on the OpenScape Business system (in Signalling and Payload encryption (SPE) section).



The installed Certificates can be viewed:




Expert mode
OpenScape Business Assistant
Expert mode - Telephony Server
Security
Application Firewall
Deployment and Licensing Client (DLSC)
Signaling and Payload Encryption (SPE)
SPE Certificate
SPE CA Certificate(s)
VPN
SSL
SPE CA Certificate(s)
View Certificate
Display CRL
Remove Certificate
Certificate Type: Self-Signed CA Certificate
Serial Number of Certificate: 1
Serial Number of Certificate (hex): 01
Type of Signature Algorithm: sha1RSA
Start Time of Validity Period (GMT): Friday, 09/19/2014 00:00:00
End Time of Validity Period (GMT): Thursday, 09/19/2024 00:00:00
CRL Distribution Point:
Issued by CA
Country (C): DE
Organization (O): UNIFY GmbH & Co. KG
Organization Unit (OU): PH HQ DPL
Common Name (CN): SPE CA
Subject Name
Country (C): DE
Organization (O): UNIFY GmbH & Co. KG
Organization Unit (OU): PH HQ DPL
Common Name (CN): SPE CA
Subject Alternative Name
- - -
Public Key Encryption Data
Public Key Length: 1536
Public Key: D69723FCAECCCF39DC3C 6B17E71218D0315019E84E 1E0048DAEFEDE68149009
Help

8.2. Technical Background

The following chapter should give some details about the technical background about this feature. This information might be useful in case you need to do troubleshooting.

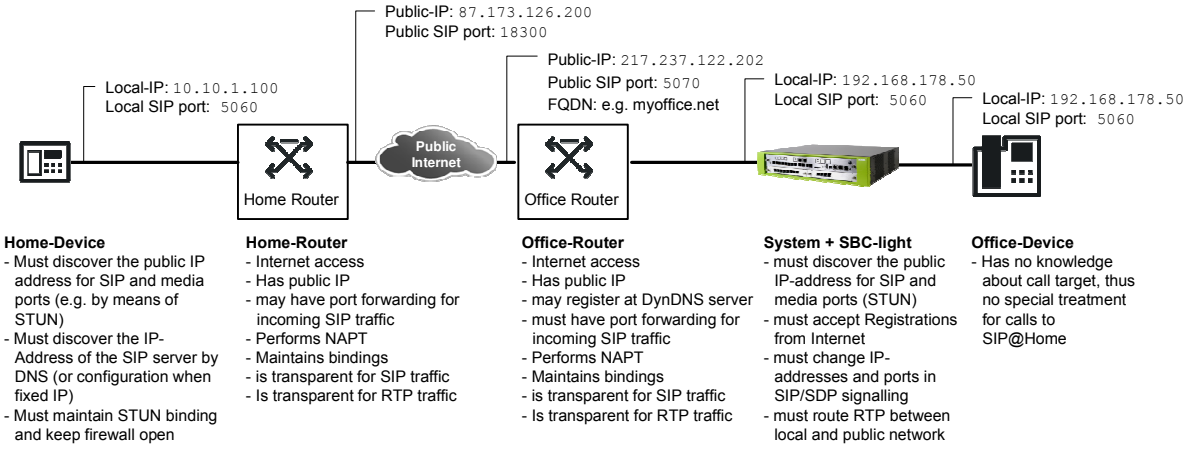


Fig 8.2-1: SIP@Home Scenario overview

For successful registration the SIP@Home phone has to determine its public IP-address and port for SIP.

In addition the phone is configured with the FQDN or public IP address and port of the OpenScape Business Server.

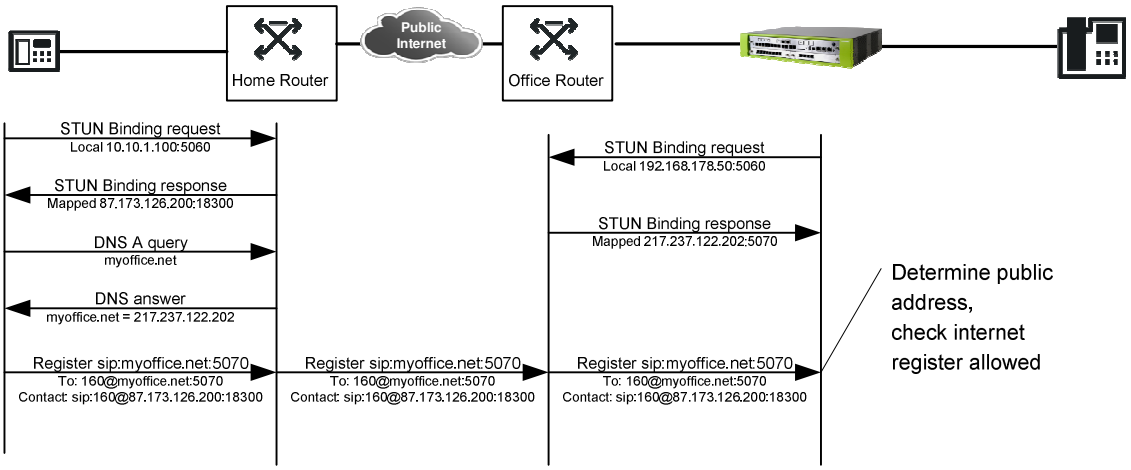


Fig 8.2-2: Detection of public SIP address

The SIP@Home registers with the OpenScape Business system where the information how to reach the phone is retrieved from the received message and stored for later use.
In case of using UDP transport the information is taken from the contact header field.
In case of TLS the information available in the contact header field is not sufficient (as the port cannot be determined by STUN), thus the system will use the transport address from where the packet is received.

The OpenScape Business Server use STUN as well to determine its public IP address and port. The SIP port is checked in regular intervals (STUN monitor function, every 15 seconds). The STUN binding for RTP is done whenever a call is established.

The following figure shows an example for call establishment and the impact of STUN for media transport:

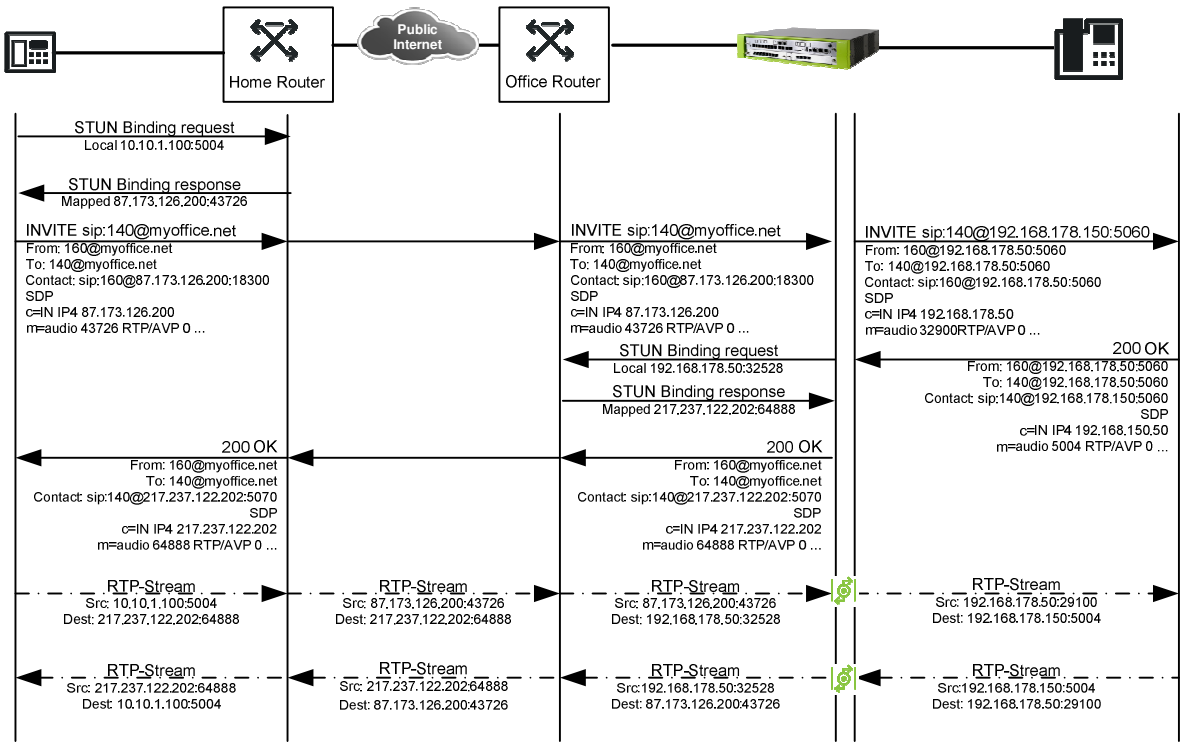


Fig 8.2-3: Call setup and detection of public RTP address

STUN has to be finished before the system can send the SDP information towards the SIP endpoint.

About Unify

Unify is one of the world's leading communications software and services firms, providing integrated communications solutions for approximately 75 percent of the Fortune Global 500. Our solutions unify multiple networks, devices and applications into one easy-to-use platform that allows teams to engage in rich and meaningful conversations. The result is a transformation of how the enterprise communicates and collaborates that amplifies collective effort, energizes the business, and enhances business performance. Unify has a strong heritage of product reliability, innovation, open standards and security.

Unify.com

UNIFY Harmonize your enterprise