



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

2

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

1. Feature description	4
2. OpenScape Business configuration	5
2.1. Internet access: supported configurations	5
2.2. Configuring a SIP Endpoint to be used from the internet	6
2.3. Configuring STUN	7
2.4. Port configuration	7
2.5. General hints	8
3. Office Router configuration	8
3.1. Port forwarding / firewall	8
3.2. DynDNS / Internet access with dynamic IP Address	8
4. SIP Endpoint configuration	9
4.1. Yealink T19P	9
4.2. Yealink T41P	12
4.3. Zoiper IOS App	13
5. Home-/SOHO-Router	14
6. Known restrictions and limitations	14
6.1. Use of video is not possible	14
6.2. Use of endpoints without STUN support is not possible	14
6.3. Use of secured connections	14
7. Troubleshooting	15
8. Appendix	16
8.1. Configuration for use of TLS	16
8.1.1. Security configuration	16
8.1.2. Certificate generation	17
8.1.3. Certificate configuration	19
8.2. Technical Background	21

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

4

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.

Edit station parameters Edit station flags Edit workpoint client data Edit Group (CE)					
one point calcine do to	are or oup your v				
P Client					
8					
D 469					
P-100					
	_				
P-168					
-+0978	_				
MO-SIP					
[
	-				
0.0.0					
~					
	-				

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

oice Gateway		Internet Telephony Service Provi	ider		
SIP Parameters Codec Parameters	E	Add Internet Telephony Service Provider	Ed	it STUN Configuration	Detect NAT Type
Destination Codec Parameters	- 49	STUN Mo	de	Automatic	-
Internet Telephony Service Provider				Harrison and Anna and	
▶18.1		Detected Nat-Ty	pe:	Detection in progress	
Acropolis		Default STUN Server			
Amis		IP Address / Host nar	me:	stun.example.com	
▶AT&T		P	ort:	3478	1
Belgacom IMS				and the second s	
▶ 8elgacom					
▶ BT IPVS					
▶ Cablecom					
Cbeyond					
CenturyLink 1					
CenturyLink 2					
COLT UK & Europe					
COLT VPN		Apply Undo		Help	
Commander Primus	-				

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	Externa	al 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).

9

OpenScape Business V2 – Tutorial: Support of SIP Endpoints connected over the internet

	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)

	Status	Account	Network	DSSKey	Featu	res	Settings	Directory	Security
Register	Reg	lister Status		Registered				NOTE	
	Line	e Active		Enabled		0			
5d5lC	Lab	el 🚽		OsBiz Miami		0		SIP service su	e Ibscriber's name
Codec	Disp	olay Name		SIP-163		0		display.	used for Caller IL
Advanced	Reg	lister Name		SIP-163		0		Register Nar	ne Ihscriher's ID use
	Use	r Name		163		0		for authentica	ation.
	Pas	sword		•••••		0		User Name User account	, provided by Vo
	Ena	ble Outbound Prox	ty Server	Disabled	÷	0		service provid	er.
	Out	bound Proxy Serve	er			Port 5	060 🕜	NAT Travers Defines the S	al TUN server will t
	Tra	nsport		UDP		0		active or not.	
	NA	r		STUN		0			
	STU	JN Server		stun.sipgate.net		Port 3	478 🕜		
	SIP	Server 1 🕜							
	Ser	ver Host		lababel.dyndns.d	iom	Port 5	070 🕜		
	Ser	ver Expires		300		0			
	Ser	ver Retry Counts		3		0			
	SIF	Server 2 🕜							
	Ser	ver Host		1	(Port 5	060 🕜		
	Ser	ver Expires		3600		0			
	Ser	ver Retry Counts		3		0			

Special hints for configuring TLS transport:

alink							Log
	Status	Account	Network DSSKey	Features	Settings	Directory	Security
Password	Index ID	Issued To	Issued By	Expiration	Delete	NOTE	
Functed Cartificates	1					Trusted Contri	
rusted Ceruncates	2					The trusted certil	rtificates list.
Server Certificates	3						
	4						
	5						
	6						
	7						
	8						
	9						
	10						
					Delete		
			Only Accept Trusted Certificates	Disabled	• 0		
			Common Name Validation	Disabled	- 0		
			CA Certificates	All Certificates	- 0		

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:

Vealink			Log Out
	Status Account Network	DSSKey Features Settings	Directory Security
Preference	Export or Import Configuration	Durchsuchen Keine Datei ausgewählt. 🕜	NOTE
Time & Date		Import Export	Configuration The configuration parameters
Upgrade	Pran Feature	Start Stop Evport	for administrator.
Auto Provision	Export: System Log	Local Server	
Configuration		Export	
Dial Plan	System Log Level	6 🗸 🌒	
Voice	Confirm	Cancel	
Ring			

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:

12

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.: <u>http://www.zoiper.com/en/voip-softphone/download/zoiper3</u>

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

●●●●○ Telekom.de 3G 1	10:48 🕴 100 % 페 🕨	•• ooo Telekom.de LTE 10:53	* 100 % 💼	•••• Telekom.de 3G	11:01 🕴 97 % 페
Accounts SIP A	Account	Accounts SIP Account	Ŵ	Accounts Network	vork Settings Save
Registratio	on Status: OK	Outbound Proxy: Outbound Proxy:	und proxy]	TRANSPORTS	
Unre	egister	ADDITIONAL SETTINGS		Transports	UDP >
SIP OPTIONS		Features	>	NAT SETTINGS	
Account name:	SIP@Home	Network Settings	>	rport:	signaling >
Domain:	195.97.14.68:1	Audio codecs	>	Enable STUN:	
User name:	262	Video codecs	>	Server:	stun.zoiper.com
Password:	•••••	Ringtone	marimba >	Port:	3478
Caller ID:	[caller id]	Instant Messaging	>	Refresh:	30
ADVANCED SETTING	GS	Number rewriting	>		
Auth Username:	[auth username]			ADDITIONAL SETT	NGS
Use Outbound Proxy:	\bigcirc			Enable on start:	

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
- 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
-------------------	-----------	--------	-------

System System System Fiags Time Parameters Display DISA Intercept/Attendant/Hotline LDAP Texts Flexible menu Speed Dials Service Codes Gateway	Edit System Flags Automatic redial: Voice mail Node call number: Call Pickup after automatic recall: Configurable CLIP: Caller list at destination in case of Forward Line: Call forwarding after deflect call / single step transfer: Follow call management in case of deflect call / single step	
System Flags Time Parameters Display DISA Intercept/Attendant/Hotline LDAP Texts Flexible menu Speed Dials Service Codes Gateway	Coll System Fags Automatic redial: Voice mail Node call number: Call Pickup after automatic recall: Configurable CLIP: Caller list at destination in case of Forward Line: Call forwarding after deflect call / single step transfer: Follow call management in case of deflect call / single step	
Time Parameters Display DISA Intercept/Attendant/Hotline LDAP Texts Flexible menu Speed Dials Service Codes Gateway	Automatic redial: Voice mail Node call number: Call Pickup after automatic recall: Configurable CLIP: Caller list at destination in case of Forward Line: Call forwarding after deflect call / single step transfer: Follow call management in case of deflect call / single step	
Display DISA Intercept/Attendant/Hotline LDAP Texts Flexible menu Speed Dials Service Codes Gateway	Voice mail Node call number: Call Pickup after automatic recall: Configurable CLIP: Caller list at destination in case of Forward Line: Call forwarding after deflect call / single step transfer: Follow call management in case of deflect call / single step	
DISA Intercept/Attendant/Hotline LDAP Texts Flexible menu Speed Dials Service Codes Gateway	Call Pickup after automatic recall: Configurable CLIP: Caller list at destination in case of Forward Line: Call forwarding after deflect call / single step transfer: Follow call management in case of deflect call / single step	
Intercept/Attendant/Hotline LDAP Texts Flexible menu Speed Dials Service Codes Gateway	Caller list at destination in case of Forward Line: Caller list at destination in case of Forward Line: Call forwarding after deflect call / single step transfer: Follow call management in case of deflect call / single step	
LDAP Texts Flexible menu Speed Dials Service Codes Gateway	Configurable CLIP: Caller list at destination in case of Forward Line: Call forwarding after deflect call / single step transfer: Follow call management in case of deflect call / single step	
Texts Flexible menu Speed Dials Service Codes Gateway	Caller list at destination in case of Forward Line: Call forwarding after deflect call / single step transfer: Follow call management in case of deflect call / single step	
Flexible menu Speed Dials Service Codes Gateway	Call forwarding after deflect call / single step transfer: Follow call management in case of deflect call / single step	
Service Codes Gateway	Follow call management in case of deflect call / single step	
Gateway	Follow call management in case of deflect call / single step	
catoriaj	transfer	
DvnDNS		
Quality of Service	warning tone during voice recording.	
Date and Time	Calling number in pick-up groups / ringing groups / CFN /RNA:	
Port Management	SPE support	
Call Charges	SPE advisory tope	7
Voicemail / Announcement Player		
Phone Parameter Deployment	SIP Prov. to SIP Prov. transit:	
*!Power Management	Transparent dialing of * and # on trunk interfaces:	
	Add seizure code for MEX	
	CMI MWI Ringer:	
	Open numbering scheme	_
	active:	
	Node callnumber:	
	Transit population	
	Feature transit:	

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.

JUT S vour enterprise		OpenScape Business Assista
Expert mode - Telephony Server		
Security Application Firewall Deployment and Licensing Client (DLSC)	Display General Information Generate CA Certificate	Generate Self-Signed Certificate
Signaling and Payload Encryption (SPE) VPN	Name of the Certificate:	SPE Certificate
▼SSL	Serial Number of Certificate:	1
Certificate Generation	Type of Signature Algorithm:	sha1RSA 🗸
b	Public Key Length:	1536 🗸
	Start Time of Validity Period (GMT)	
	Day	Month Year
c	19	9 2014
	Hour	Min. Sec.
-	0	0
x	End Time of Validity Period (GMT)	
	Day	Month Year
s	19	9 2024
x	Hour	Min. Sec.
4	0	0
4	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	
	Distinguished Name Format〇	Other Format®
	Subject Alternative Name Extension:	Email address V (optional)
	Subject Alternative Name:	(optional)
	CRL Distribution Point Type:	DNS Name V (optional)
	CRL Distribution Point:	(optional)
	Apply Help	

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

Expert mode - Telephony Server						×
Security	Display Ge	neral Inform	ation			
Application Firewall	View	Delete	Export Certificate	Generate CA-Signed Server Certificate	Undate CA-Signed Server Certificate	
Deployment and Licensing Client (DLSC)	Certificate	Certificate		[PKCS#12]	[X.509]	
Signaling and Payload Encryption (SPE)						
VPN						
▼SSL						
Certificate Generation						
SPE Certificate						
Certificate Management						
	Load		Help			

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.

ecurity	Display Ge	neral Inform	ation				
Application Firewall	View	Delete	Export Certificate	Generate (A-Signed Server Certificate	Lindate CA-Signed Server Certificat	e.
Deployment and Licensing Client (DLSC)	Certificate	Certificate	[X.509]		[PKC5#12]	[X.509]	
Signaling and Payload Encryption (SPE)			Serial Number	of Certificate:	1		
VPN			Type of Signatu	re Algorithm:	sha1RSA		
SSL			Public	Key Longth:	2048		
Certificate Generation	Const Change			. Key Lengui.	2040 +		_
Certificate Management	Start Time of	r validity Per		Dev	84	V	
-				Day	wonth	rear	
				19	9	2014	
				Hour	Min.	Sec.	
				0	0	0	
	End Time of	Validity Perio	od (GMT)		, 1 .		
				Day	Month	Year	
				19	9	2024	
				13	<u> </u>	2024	
				Hour	Min.	Sec.	
				0	0	0	
	Subject Nam	e					
				Country (C):	DE		
			Org	anization (O):	UNIFY GmbH & Co. KG		
			Organizati	on Unit (OU):	PH DPL SME	-	
			organizad	on one (00).			
			Commor	n Name (CN):	SecureSubscriber		_
	Subject Alte	mative Name	1				
	-		Distinguished Na	me Format	Other Format®		
		Sub	oject Alternative Nar	ne Extension:	Email address	✓ (optional)	
			Subject Alter	native Name:	axel.geske@t-omline.de	(optional)	
			CRL Distributio	n Point Type:	DNS Name	V (optional)	
			CRI Dist	ibution Point:		(ontional)	
			ONE DIST	ioddon r oine.	L		
	Genera	ate Certificate	Help				

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

After this step two files are present::

18

- 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).

Expert mode - Telephony Server	
Security	SPF Certificate
Application Firewall	Impart SPE certificate plus private key (PKCS#12 file)
Deployment and Licensing Client (DLSC)	aniport are consider provincing the function of Consider and
Signaling and Payload Encryption (SPE)	Passphrase for decryption:
▼SPE Certificate	
	File with certificate and private Key (PEM or PKCS#12 format): Browse_ No file selected.
▼SPE CA Certificate(s)	
1	Note: If you are installing a SPE certificate for the first time and SPE is active a reboot will be done automatically!
VPN	
▶ SSL	
	View Fingerprint of Certificate Import Certificate from File Help

The installed Certificates can be viewed:



0			_		
510	Image: Apple 192.168.139.141 / mar + Source Zerti	fikaC Expert mode ×			11 🛠
≥ <u> </u>	Cert W Tran 🧭 Veri 📒 Cros 🛃 Unti.	🗿 http 🔰 Test 👻 🚺 Empl 🗿 CRIS 🗿 ICN 🔣 KLOC		🚡 🕶 🔝 👻 🚍 🖶 👻 Seite 🕶 Sicherheit 🕇	🔹 Extras 👻 🔞 👻
ΠÎ	n CU Harmonize			OponScopo Businos	e Accietan
ч				Openscape Busines	
	Expert mode - relepitony server				00
om	Application Firewall	SPE CA Certificate(s)			
	Deployment and Licensing Client (DLSC)	View Certificate Display	CRL	Remove Certificate	
Mair	 Signaling and Payload Encryption (SPE) 	Certificate Typ	e: Self-S	igned CA Certificate	
Tele	SPE Certificate	Serial Number of Certifica	e: 1		
Basi	▼SPE CA Certificate(s)	Serial Number of Certificate (he	<): 01		nd
Sect		Type of Signature Algorith	n: sha1R	RSA	
Net	VPN	Start Time of Validity Period (GM): Friday	, 09/19/2014 00:00:00	
Rou	SSL	End Time of Validity Period (GM): Thurso	day. 09/19/2024 00:00:00	
LCR		CRL Distribution Po	nt:		
Voic		Issued by CA			
Stat		Country (): DE		
Conc		Organization (): UNIFY	/ GmbH & Co. KG	
Incc		Organization Unit (O	J): PH HO	2 DPL	
True		Common Name (C	I): SPE C	A	
Clas		Subject Name			
Auxi		Country (;): DE		
Payl		Organization (): UNIFY	/ Gm <mark>bH &</mark> Co. KG	
Stat		Organization Unit (O	J): PH HO	2 DPL	
Appl		Common Name (C	I): SPE C	A	
		Subject Alternative Name			
			200		
		Public Key Encryption Data	N. 4500		
		Public Key Leng	n: 1536		
I		Public K	big 106972 99: 6B17E 1E004	23FCAECCCF39DC3C E71218D0315019E84E 18DAEFEDE68149009	~
		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

UNFY Harmonize your enterprise

Copyright © Unify Software and Solutions GmbH & Co. KG 2015 Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany 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.