



# OpenScape Business V2

Tutorial

System Device@Home - Configuration

Version 1.1

## Table of Contents

1. Configuration Overview	4
1.1. Network Scenario Description:	4
1.2. Configuration Steps	5
1.2.1. Overview OpenScape Business Configuration	5
1.2.2. Overview Company Internet Router Configuration	5
1.2.3. Overview System Device@Home Configuration	5
1.3. Technical boundaries and limitations	5
1.3.1. Internet access of OpenScape Business	5
1.3.2. NAT configuration within Company and Home Router	5
1.3.3. myPortal to go VoIP client:	6
1.3.4. Firmware Update of System Devices	6
1.3.5. Capacities	6
2. OpenScape Business configuration	7
2.1. Supported Internet Access Scenarios for System Device@Home	7
2.1.1. OpenScape Business behind access router connected to LAN2 interface	7
2.2. Configuring a System Client to be used from the Internet	7
2.3. Configuring the number of simultaneous internet calls	8
2.4. Configuring STUN	8
2.5. Port configuration within OpenScape Business	9
2.5.1. Signalling Ports	9
2.5.2. Voice Payload Ports	9
3. Company Internet Router Configuration	10
3.1. Port forwarding / firewall	10
3.2. Internet access with dynamic IP Address (DynDNS)	10
3.3. NAT type	10
4. System Device configuration	11
4.1. System Device Configuration	11
4.2. myPortal to go VoIP Client configuration	11
5. Home Internet Router	12
6. Security considerations	12
7. Troubleshooting	12
8. Abbreviations	14

## 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

# 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.

## Note:

Within the following the term “**System Device**” is used in general for all system clients, which support the **HFA** protocol such as OpenStage and Deskphone IP phones and also the VoIP client within the myPortal to go apps.

## 1. Configuration Overview

The feature “**Device@Home**” has been released for System Devices and for myPortal to go apps with Voice over IP (VoIP) support from OpenScape Business V2R1 on. The feature 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.

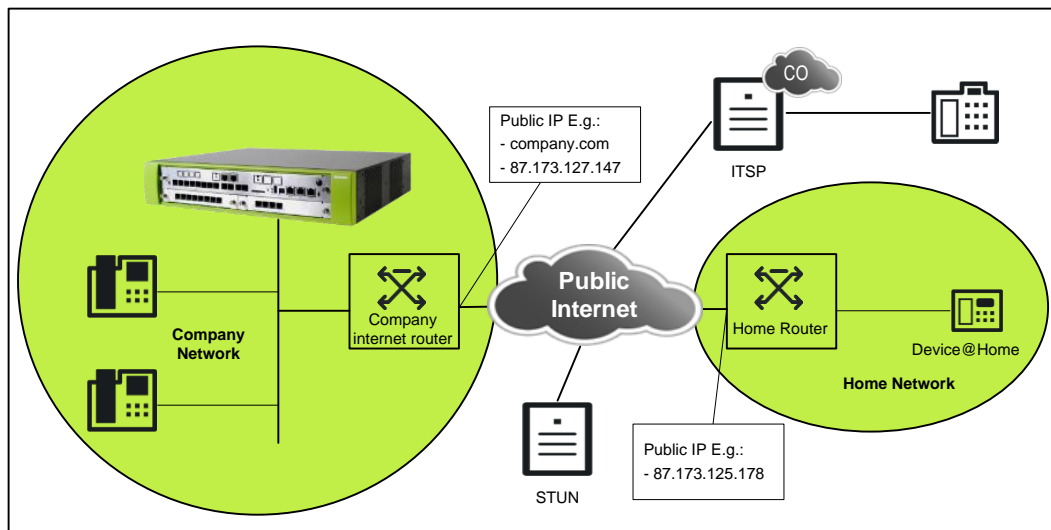


Figure 1 Typical network environment

### 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 one System Client as externally connected client and assign an IP user license. This is also required if the myPortal to go VoIP option is used.
- 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 t (see 2.3).
- Enable Authentication and configure **STRONG, individual** passwords for **ALL** System Clients regardless of their location (internal or external) .

### 1.2.2. Overview Company Internet Router Configuration

As the System (HFA) 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 HTTPS (only when using myPortal to go VoIP @Home).
- If the company router restricts outbound IP traffic, it may be necessary to explicitly open the ports also for outgoing IP traffic.

### 1.2.3. Overview System Device@Home Configuration

Within the System (HFA) 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
- Leave the DLS IP address field empty - DLS/DLI are currently not supported for System Device@Home.)

## 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.

### 1.3.3. myPortal to go VoIP client:

- The VoIP client within the myPortal to go APP required direct HTTPS access to TCP/8802 port within OpenScape Business.
- myPortal to go VoIP supports only G.711 codec.
- myPortal to go VoIP client is not released in combination with Deskshare users.

### 1.3.4. Firmware Update of System Devices

- For security reasons automatic firmware updates are not supported from remote. Before using a system device as Device@Home, it has to be connected once internally to the OpenScape Business in the company in order to perform a firmware update to the latest version, which is delivered with OpenScape Business V2R1 or later.

### 1.3.5. 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 a 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

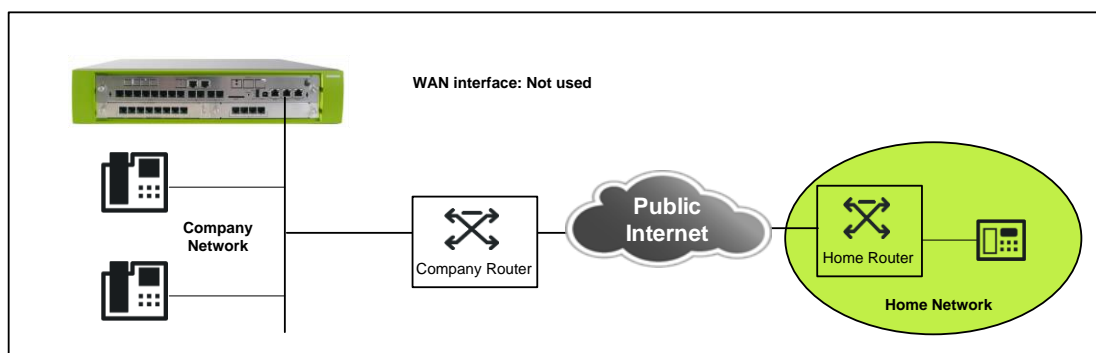


Figure 2 OpenScape Business behind access router connected to LAN2 interface

### 2.2. Configuring a System Client to be used from the Internet

System Devices with HFA protocol are configured as System Clients within OpenScape Business Administration Portal (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

In case that at least one System Client is configured for connection via Internet, the flag "Authentication" and strong, individual passwords have to be configured for ALL System Clients within OpenScape Business.

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.

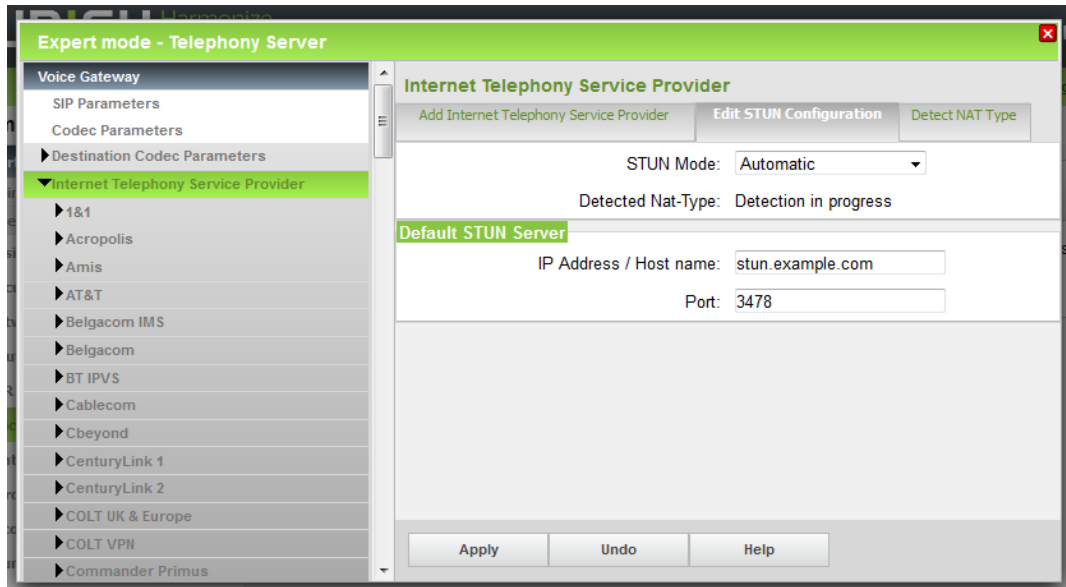
In case that the system is already connected to an ITSP with activated STUN server, no additional configuration is required. The system is able to detect its public IP-address and port

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, should not be changed within the system configuration

### 2.5.1. Signalling Ports

Protocol	Default port
HFA	TCP/4060 (for HFA phones)
HTTPS	TCP/8802 (for myPortal to go)

### 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)

# 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)
HFA	TCP/4060	TCP/4070 <b>SHOULD</b> be different from internal port in system
HTTPS	TCP/8802	TCP/8802 <b>MAY</b> be same as port in system
RTP	UDP/30274-30529 UDP/30528-30887	UDP/30274-30529 for OSBiz X; <b>MUST</b> be same range as in system! UDP/30528-30887 in OSBiz S; <b>MUST</b> be same range as in system!

### Note:

The gateway port configuration of the System Device@Home has to be adapted according to the TCP external port of port forwarding setting of the Company Internet 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.



## 4. System Device configuration

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

Device / Client	Minimum software version
OpenStage HFA	V3R0.33.1
Desk Phone IP HFA	V3R0.33.1
myPortal to go (Android) VoIP	V2R1.61.14
myPortal to go (iOS) VoIP	(coming soon...)

### 4.1. System Device Configuration

Please configure:

- 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
  - = as usual
- HFA password
  - = Password as configured within OpenScape Business
- Update Service / DLS:
  - = None

### 4.2. myPortal to go VoIP Client configuration

Please configure:

- User Account - WAN server IP address
  - = Public IP or DNS name of the OpenScape Business
- User Account - 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
- User Account - LAN server IP port
  - = 8802
- More - VoIP settings:
  - = Enable "VoIP" flag
- More - VoIP settings:
  - = 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.

The System Device @Home connection provides following security measures

Client type	Security level
Desk Phone @Home	- Authentication via HFA password - Signalling and payload encryption currently not supported
myPortal to go @Home	- Authentication via encrypted UC password - Signalling encryption via SSL (HTTPS) - Payload encryption currently not supported.

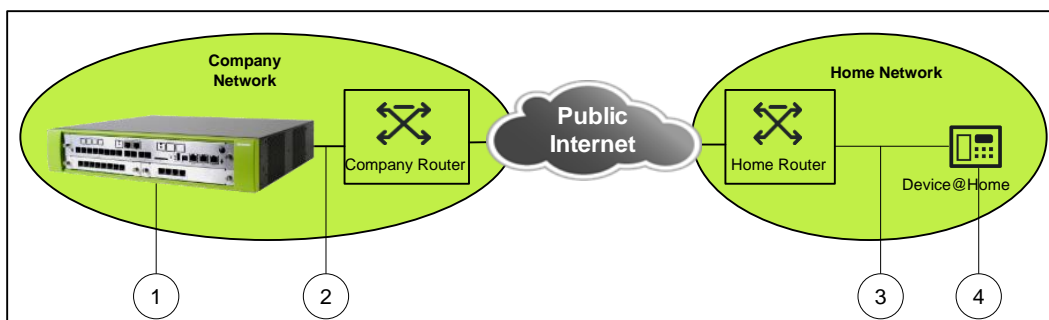
It is recommended to use myPortal to go VoIP only in trusted WiFi environments (company, home office, ...).

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

- Customers with security critical business / information in general
- Environments with strict router/firewall policies where port forwarding from the internet are not allowed or symmetric NAT is in place
- Customers with strict requirements regarding signaling and payload encryption

In these cases, a VPN infrastructure between the central office and the home / mobile worker has to be considered.

## 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
STUN	Session Traversal Utilities for NAT
VoIP	Voice over IP
WAN	Wide Area Network

Copyright © Unify Software and Solutions GmbH & Co. KG 2016  
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 GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.