Security Checklist

OpenScape Business V1

Version: 1.0
Date: 2013-04-03

SEN VA SME PSM / Baseline Security Office
Siemens Enterprise Communications

Siemens Enterprise Communications
www.siemens-enterprise.com

SIEMENS

Table of Content

1 Introduction

1.1 General Remarks

Information and communication - and their seamless integration in "Unified Communications and Collaboration" (UCC) - are important and valuable assets for an enterprise and are the core parts of their business processes. Therefore, they have to be adequately protected. Every enterprise may require a specific level of protection, which depends on individual requirements to availability, confidentiality, integrity and compliance of the used IT and communication systems.

Siemens Enterprise Communications attempts to provide a common standard of features and settings of security parameters within the delivered products. Beyond this, we generally recommend

- to adapt these default settings to the needs of the individual customer and the specific characteristic of the solution to be deployed
- to outweigh the costs (of implementing security measures) against the risks (of omitting a security measure) and to "harden" the systems appropriately.

As a basis for that, the Security Checklists are published. They support the customer and the service in both direct and indirect channel, as well as self-maintainers, to agree on the settings and to document the decisions that are taken.
The Security Checklists can be used for two purposes:

- **In the planning and design phase** of a particular customer project:
  Use the Security Checklists of every relevant product to evaluate, if all products that make part of the solution can be aligned with the customer's security requirements – and document in the Checklist, how they can be aligned.
  This ensures that security measures are appropriately considered and included in the Statement of Work to build the basis for the agreement between SEN and the customer: who will be responsible for the individual security measures:
  - During installation/setup of the solution
  - During operation
- **During installation and during major enhancements or software upgrade activities:**
  The Security Checklists (ideally documented as described in step 1.) are used to apply and/or control the security settings of every individual product.

Update and Feedback

By their nature, security-relevant topics are prone to continuous changes and updates. New findings, corrections and enhancements of this checklist are being included as soon as possible.

Therefore, we recommend using always the latest version of the Security Checklists of the products that are part of your solution.

They can be retrieved from the partner portal Siemens Enterprise Business Area (SEBA) at the relevant product information site.

We encourage you to provide feedback in any cases of unclarity, or problems with the application of this checklist.

Please contact the Baseline Security Office (obso@siemens-enterprise.com).

1.2 History of Change

Date	Version	What
2013-04-03	1.0	

1.3 Customer Deployment - Overview

This Security Checklist covers the product **OpenScape Business V1** with its related optional applications **OpenScape Business UC Suite** and **Xpressions Compact Card.** It lists the security relevant topics and settings to be considered for the specific customer installation.

	Customer	**Supplier**
Company Name Address Telephone E-Mail		
Covered Systems (e.g. System, SW version, devices, MAC/IP-addresses)		
General Remarks		
Open Issues to be solved until		
Date		

2 OpenScape Business Hardening Measures in General

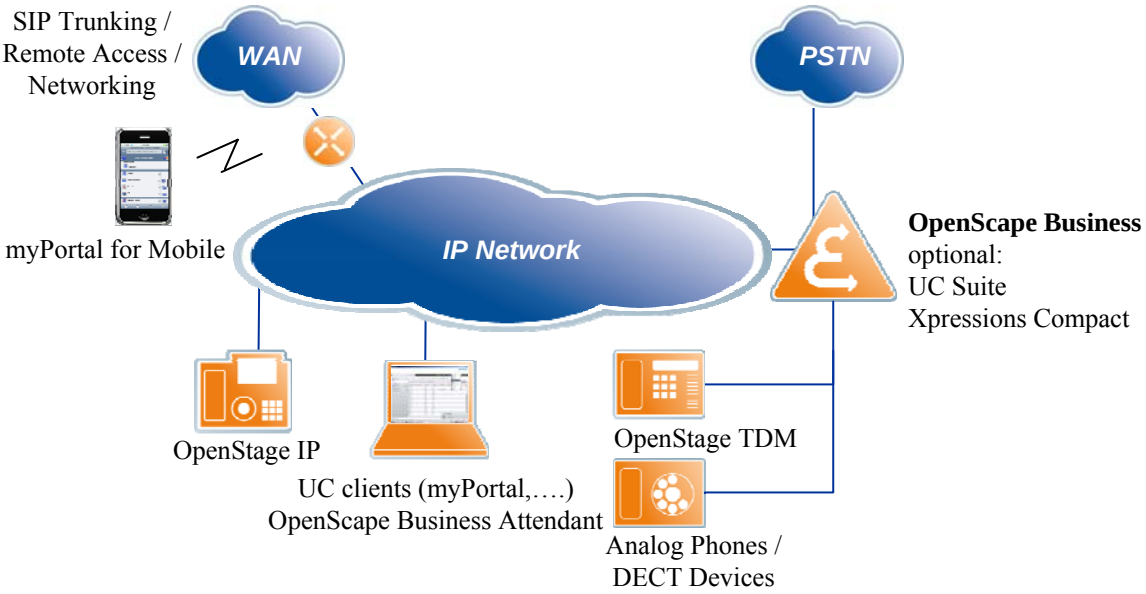
This checklist covers the following models and the related integrated or external applications:

OpenScape Business X3 **OpenScape Business X5** **OpenScape Business X8**

OpenScape Business S

server-based solution

Configuration overview



The availability of many features depends on activated licenses.

For safeguarding a OpenScape Business based communications solution all components have to be considered:

OpenScape Business is providing basic voice services for TDM and IP devices and trunks as well as Unified Communication (UC). Administration access and features like class of service have to be configured carefully. Physical and logical protection of system and infrastructure against manipulation of features as well as sabotage is necessary. OpenScape Business X3 / X5 / X8 are embedded solutions. OpenScape Business S and OpenScape Business UC Booster Server use a dedicated Linux server which has its own administration. Protection from unauthorized access and breach of confidentiality has to be enforced through protection of all interfaces.

Xpressions Compact Card is an option for an integrated voicemail, mobility and conferencing server with its own administration. Special care has to be taken to protect the customer from toll fraud through call forwarding within mailboxes.

Desktop and Server PCs are used for communication clients and central components. Admission control has to be implemented by suitable password, provisioning with actual security updates and virus protection for all involved PCs.

Subscriber Devices (e.g. OpenStage phones, Software Clients) provide the user interface to the phone including unified communications services. On the user and terminal side, security considerations have to be made for desktop and mobile phones as well as for soft clients and the devices they are running on. Access protection in case of absence as well as restriction of reachable call numbers for protection against misuse and resulting toll fraud has to be considered.

Precondition
We recommend strongly always using the latest released software in all components.

CL-1 All components	**Up-to-date SW**		
Measures	Up-to-date SW installed for		
OpenScape Business	Yes: ☐	No: ☐	
OpenScape Business Booster Card (OCAB)	Yes: ☐	No: ☐	Not installed: ☐
Xpressions Compact Card	Yes: ☐	No: ☐	Not installed: ☐
HiPath Manager	Yes: ☐	No: ☐	Not installed: ☐
PCs / Servers			
OpenScape Business S / OpenScape Business UC Booster Server	Yes: ☐	No: ☐	Not installed: ☐
Server for TAPI	Yes: ☐	No: ☐	Not installed: ☐
Other	Yes: ☐	No: ☐	Not installed: ☐
Devices			
OpenStage phones	Yes: ☐	No: ☐	
Other	Yes: ☐	No: ☐	Not installed: ☐

Clients			
OpenScape Business myPortal, myAttendant, myAgent, …	Yes: ☐	No: ☐	Not installed: ☐
OpenScape Business Attendant	Yes: ☐	No: ☐	Not installed: ☐
OpenScape Personal Edition	Yes: ☐	No: ☐	Not installed: ☐
other	Yes: ☐	No: ☐	Not installed: ☐
Customer Comments and Reasons			

The following chapters list the recommended measures for the **OpenScape Business V1** solution.

2.1 System Access Protection

The administration of the system and the involved components has to be protected from unauthorized access. This includes the following aspects:

- Authentication of every user (user name, password, digital certificates)
- Authorization (roles and privileges)
- Audit (activity log)

Fixed or easy to guess passwords are a serious security risk. In any case, individual and complex passwords must be used for all users. Every user shall only get those rights or roles, which are necessary for him.

Access to central components like OpenScape Business appliance / server or LAN switches and routers shall only be possible for technicians and administrators. This protects the system against direct access via administration port or USB interfaces.
Personal data, communication data and communication content like voicemails are stored in the communication solution. Confidentiality has to be assured through protection of the administration access. The backup data at external drives or servers has to be safeguarded as well e.g. by passwords.

2.2 Administration

Secure communication for local and remote administration access is especially important.

2.2.1 OpenScape Business Assistant

The access to the OpenScape Business Assistant occurs web-based and is always encrypted via HTTPS. A self-signed server certificate for HTTPS encryption is delivered by default. This has to be accepted as trusted by the user in the browser.

For server authentication and against man-in-the-middle attacks, an individual certificate is necessary, which relies on a root certificate authority. This enables the browser, used for administration, to set up a secure end-to-end connection with OpenScape Business.

CL-2 **OpenScape Business**	**Customer specific SSL/TLS certificate**
Measures	Import a customer certificate, which is issued for the OpenScape Business (server name or IP address) and activate it for the administration access.
References	Manual [1] Information about Customer certificate find also in Addendum 10.3
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

A new password for OpenScape Business Assistant has to be entered after first start. Please observe the password recommendations for all users.

CL-3 **OpenScape Business**	**Add OpenScape Business Assistant Accounts**
Measures	Implement necessary user accounts for the roles • Basic • Advanced • Expert with strong individual passwords and list all needed user accounts in addendum 10.2.1
References	Manual [1] for passwords see chapter 10.1
Needed Access Rights	Advanced / Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

A strong PIN code shall be defined for activating system shut down. This PIN is used when activating the system shut down from a system phone.

CL-4 **OpenScape Business**	**PIN for shutdown from phone**
Measures	Configure a strong PIN via OpenScape Business Assistant 'Expert Mode' Maintenance' 'Restart/Reload' 'Enable/disable shut down'
Reference	Strong PIN see 10.1 How to change PIN see manual [1]
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

2.2.2 HiPath Manager E

For special administration tasks a PC SW tool is provided, which has its own access control. Use only variable password concept for HiPath Manager E. The fixed password concept must not be used. For details see [2]. Password has to be numerical, if administration via telephone is needed.

CL-5 **HiPath Manager E**	**Change initial passwords**
Measures	Select strong passwords for all users in all roles
Reference	Strong PIN see 10.1 List of default PINs see 10.2.2 How to change users, roles and PIN see Manual [2]
Needed Access Rights	Service
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

2.2.3 Assistant T/TC

Administration by phone is always possible from the first two system phones. The same passwords as for HiPath Manager E are applicable.

Assign the first two system phones (HFA) to administrators or trusted users. Do not deploy those phones in places with visitor access.

2.2.4 Smart Service Delivery Platform (SSDP)

The Smart Services Delivery Platform connects SEN systems via a secured internet connection to the SEN Remote Service Infrastructure. This can be used by authorized sales and service partners.

OpenScape Business establishes a secure authenticated connection. SSDP is the most secure way for remote administration and should be used wherever possible.

In addition SSDP can be activated by the customer for every single service task e.g. via phone.

CL-6 **OpenScape Business**	**Secure remote Administration through SSDP**
Measures	• Activate remote access via SSDP • Define strong PIN for activation / deactivation by phone
References	[1] activation and PIN code at Service Center > Remote Access
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐ not applicable: ☐
Customer Comments and Reasons	

2.2.5 Remote Access over VPN

Direct unprotected access from Internet must not be used, as this brings high risks from Internet attacks. A secure tunnel shall be used for remote administration via IP, when SSDP is not available. This can be implemented via OpenScape Business X3/X5/X8 or via an external VPN router (see also 3.3.). The integrated

access can be activated by the customer for every single service task e.g. via phone. This shall be protected with a strong PIN (same as for SSDP).

2.2.6 Remote Access over ISDN / BRI

Remote Access over ISDN / BRI via incoming connection should be used only with call back. See also 3.2.3. It can be activated by the customer for every single service task e.g. via phone.

2.3 Communication Access and Toll Fraud Protection

Toll fraud can lead to considerable phone charges. The following measures have to be observed to protect against unauthorized calls through OpenScape Business.

2.3.1 Class of Service

OpenScape Business provides calls to external destinations either directly from the phone or through call forwarding or via 3rd party call control. This includes foreign and special call numbers with high charges. The reachable call destinations shall be restricted to the necessary numbers for toll fraud protection. This has to be considered also for Modem and Fax ports. For calls which are controlled via UC Suite e.g. with Call Me or Conference a restriction can be defined for the route VSL in all COS groups.

CL-7 **OpenScape Business**	**Toll restriction for devices**
Measures	Suitable Class of Service (COS) is assigned for every device via OpenScape Business Assistant • Internal or outward-restricted trunk access for devices, where no external calls are needed (emergency calls still possible). • Allowed Lists configured for well-defined necessary business connections, other destinations are blocked. • Denied Lists configured to block special numbers or countries (as an alternative least cost routing (LCR) may be used). For UC Suite the route VSL is restricted to the necessary numbers in all COS groups e.g. with allowed or denied list in the same way as for trunk groups. Further possibilities: • Setup COS for trunk group connections (which trunk group is allowed to connect with which trunk group) in “CON Group assignment” and then “CON Matrix” • Delete the “call forwarding external” flag for all devices, which do not need it, especially for devices within reach of external persons. • Disable the three “Transit permission” flags in system parameters, if no transit traffic is needed.
References	Manual [1]
Needed Access Rights	Advanced / Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

Notes:

- All conducted calls are logged in the system and can be checked with an accounting tool. For logging incoming calls, the flag “Log incoming calls” in Call Charges > Output format must be activated. Internal node calls and transit calls are not logged.

- Alarms can be configured for an attendant console in case of trunk resources occupied from external – external connections. It is possible to release such calls (toll fraud feature).

2.3.2 OpenScape Business UC Smart

OpenScape Business UC Smart is offered for use by the web-based applications

- myPortal Smart (for desktop PC)
- myPortal for Mobile / Tablet
- myPortal for OpenStage
- OpenScape Business Application Launcher
- Customer specific applications

By default the HTTPS protocol is activated. For mobile devices with low performance, it may be necessary to use less secure HTTP instead. This is also true for OpenStage V2 devices.

The individual UC Smart user password has to be changed before the Client can be used. It is valid for the client as well as for the web-based administration of the personal contacts and password. It is recommended to keep the default password policy 'Force user to choose secure password' in OpenScape Business Assistant and to set up a secure system-wide initial password.

Note: Port-forwarding for port 8802 (HTTPS) or 8801 (HTTP) has to be activated to be able to use the Web Services via WAN (see 3.2.1). UC Smart user administration communicates via port 8803. It is recommended not to open the port for external access. To increase security for the internal LAN, an external web proxy can be used.

2.3.3 OpenScape Business Smart Voicemail

Change the initial PIN to an individual, safe value to secure mailboxes against unauthorized access and forwarding of external calls via mailbox. Users have to change the 6-digit PIN at first use to an individual strong password from an internal phone. Mailbox access is denied after 6 attempts with wrong PIN.

CL-8 **Smart Voice Mail**	**Restrict calls out of voice mail**
Measures	• Set Class of Service (COS) for the Smart VM ports to 'outward-restricted' for day and night service. • If call forwarding out of mailboxes is needed, e.g. for myPortal for Mobile, auto attendant or notification call, COS shall be extended carefully only to those destinations, which are allowed to be reached. • If Least Cost Routing is active, 'Class of Service' at Routing > LCR > Dial Plan must be activated (default).
References	for change of default PIN see 10.2 Manual [1] 'Expert Mode' Classes of Service'
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

2.3.4 Associated Dialling and Services

Associated Dialling / Services allow e.g. call setup or activation of call forwarding for other stations. Assign rights only to subscribers who need them to avoid misuse.

CL-9 OpenScape Business	**Restrict Associated Features**
Measures	• Enable the station flag only for users who need the function. • Inform concerned users about handling and security risks.
References	Manual [1]
Needed Access Rights	Advanced / Expert End user instruction
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	The following users are enabled for associated dialling:

2.3.5 Direct Inward System Access (DISA)

The DISA feature allows call setup to external destinations and feature programming from external e.g. for call forwarding. Unrestricted access to DISA could be used by unauthorized parties for toll fraud. Access to DISA should be restricted.

If DISA is not used, no DISA number must be configured. The feature shall be enabled only for users who need the function and DISA users shall be informed to keep the PIN confidential.

CL-10 OpenScape Business	**Change default PIN for DISA**
Measures	• The PIN used for DISA is the same as that for individual code lock (see 2.3.8.) It has to be set to an individual value by every DISA user. A 5-digit sequence, which cannot be guessed easily, has to be selected
References	Change of default PIN see10.2.3; strong PIN see10.1 Default Service Code *93
Needed Access Rights	End user instruction
Executed	Yes: ☐ No: ☐ DISA not used ☐
Customer Comments and Reasons	

2.3.6 Mobility

The feature mobility allows calls and feature activation via OpenScape Business for authorized users from mobile phones. The subscriber is identified through his transmitted phone number. The devices, which are registered for this service, shall be protected from unauthorized access. A small risk for toll fraud lies in pretending a registered calling number by fraudulent callers (CLIP no screening, possible via some VoIP providers).

Make sure to protect registered devices from unauthorized access (e.g. PIN for mobile phones).

CL-11 Mobile Devices	**Protect the devices registered for mobile access**
Measures	• Use call back for enhanced security. • Inform Mobility users to protect registered devices from unauthorized access.
References	[1]
Needed Access Rights	Advanced / Expert End user instruction
Executed	Yes: ☐ No: ☐ Mobility not used: ☐
Customer Comments and Reasons	Callback Yes ☐ No ☐

2.3.7 Desk Sharing

An office phone can be shared between several users. Desk sharing is activated by the system wide flag 'relocate allowed'. The feature can be blocked at dedicated phones, if needed (type 'non mobile and blocked').

CL-12 OpenScape Business	**Protect the access of desk sharing users**
Measures	• A strong password has to be set up (same as code lock see 2.3.8)
References	See 10.1, 10.2
Needed Access Rights	End user instruction
Executed	Yes: ☐ No: ☐ Desk sharing not used: ☐
Customer Comments and Reasons	

2.3.8 Access to Phones

Especially for places with visitor access or with special functions, it is recommended to protect the phone access by a 'code lock'. Special functions are for instance system phone lock (COS changeover), switch night mode, associated dialling and silent monitoring / call supervision as well as phone lock reset for other phones. Code lock is handled via phone menu or key.

Flex Call (call from any device with own authorization) is protected by the code lock PIN as well.

CL-13 System phones	**Use code lock**
Measures	• For HFA and TDM devices with danger of misuse, code lock is used with an individual 5-digit PIN.
References	Default service code *93 Rules for PIN see 10.1
Needed Access Rights	End user instruction
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

2.3.9 Door Opener

OpenScape Business X3 / X5 / X8 provides activation of door openers via phone. Remote access to door stations, which are controlled via DTMF, might be a security risk.

CL-14 OpenScape Business	**Restrict authorization for door opener**
Measures	• Authorization is assigned only to those stations, where it is necessary.
References	Door Release DTMF flag, see manual [2]
Needed Access Rights	Manager E: Service
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	List of stations:

2.4 Confidentiality of Communications

2.4.1 Transmission via internal IP networks (LAN)

For the internal IP network, the requirements according to the administrator documentation have to be met. Access to central components like switches and routers shall be restricted to technicians and administrators. A logical or physical decoupling of voice and data network should be considered depending on the existing infrastructure. The IT service provider of the customer may have to be involved.

In networking scenarios, some information like system database, CTI and UC networking information is transmitted unencrypted. Data may be disclosed, if unauthorized persons get LAN access. For security critical environments this may be not appropriate and separate TLS connections may be necessary.

2.4.2 Signalling and Payload Encryption

For confidentiality and integrity of VoIP communication, the activation of signalling and payload encryption (SPE) shall be considered.

Calls with HFA phones and conferences can be secured. This includes SIP-Q network calls with other OpenScape Business, HiPath 4000 and OpenScape Voice systems. Other connections, where the OpenScape Business UC application is involved in payload (e.g. for call recording) can currently not be secured. This is also true for SIP client and ITSP calls.

CL-15 OpenScape Business	**Signalling and Payload Encryption**
Measures	• System wide flag ‘SPE support’ activated • Payload Security activated for all relevant subscribers • SPE CA Certificate and SPE Certificate imported to OpenScape Business. (If no customer certificates are available, self-signed certificates can be generated.) • TLS has been selected for transport on the IP end-points (HFA-WBM or device configuration interface DLS/DLI) • Make setting, if gateway calls e.g. with ISDN/PRI trunk are considered as secure. This influences the display at the phones. • Enable certificate handling alarms (In WBM, Check that an e-mail is sent to the administrator when events involving SPE certificates occur (Maintenance → Events → Reaction Table → MSG_SPE_CERT_xxx)

References	Provision of certificate see also 10.3 Manual [1]
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

2.4.3 IP Transmission with Public Networks

VoIP access to public networks (ITSP) is based usually on a user account and password delivered by the provider. This data is entered at the OpenScape Business administration and has to be kept confidential.
For extended security, a provider with a dedicated line or secure VPN access is recommended.

2.4.4 External Subscribers

External subscribers like tele-workers or mobile workers shall be connected via VPN to protect confidentiality and to avoid misuse of the subscriber access by unauthorized persons. With VPN, an encrypted tunnel is set up for the communication. This can be done by OpenScape Business X3 / X5 / X8 or by an external VPN Router. For VPN details see chapter 3.3.

2.4.5 Networking for OpenScape Business

Protection of the IP connections for networking between different sites by VPN is strongly recommended to ensure confidentiality and to avoid misuse by unauthorized persons. This can be done by OpenScape Business X3 / X5 / X8 or by an external VPN Router. Voice communication, UC communication, DSS server signalling and administration take place via IP networking. For VPN details see chapter 3.3.

2.4.6 Privacy

Some common features allow listening into a room via telephone or monitoring of phone calls. Among those are room monitoring, speaker calls with direct answering, override and call recording, They should be activated only for subscribers who need them. Keep predefined alerting tones and use them in accordance with country and company regulations. Please be aware that also with conference and open listening other persons may hear a phone conversation unnoticed.

CL-16 OpenScape Business	**Change Service Code for Room Monitor**
Measures	• If room monitoring is configured in the system, define a service code with maximum length, which cannot be guessed easily (5 digit)
References	Manual [1] For activating / deactivating the feature system-wide see [2]
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐ Not configured: ☐
Customer Comments and Reasons	

2.5 Availability

OpenScape Business was developed for high reliability. This can be enhanced by measures in the infrastructure.

CL-17 Infrastructure / OpenScape Business	**Enhanced Availability**
Measures	• A possible weakness is electrical power supply. Redundant power supplies can be used. For countries with higher probability of power outages, the optional PSU boards and battery packs or a separate uninterruptible power supply (UPS) for OpenScape Business and related components may be sensible. • Two or more independent public network trunks extend availability in case of carrier failures. • For the server-based OpenScape Business components, a server with redundancy can be used (please see current release documentation). • Higher availability for OpenScape Business Servers is achieved by using a suitable virtual server environment. • Please note that excessive security scans may lead to reduced availability.
References	For UPS boards see Service Manual [3]
Needed Access Rights	Information regarding system design
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	Please describe measures taken:

3 IP Interfaces OpenScape Business X3 / X5 / X8

3.1 IP Interfaces and Ports

Interfaces, which are not used, are deactivated by default and shall not be activated without explicit need. The ports used with OpenScape Business can be found in 10.4. This information may be used for external firewall configuration e.g. for network separation to increase security.

The OpenScape Business main board provides three 1 Gbit Ethernet interfaces (Administration, LAN, WAN). Special measures should be considered for some IP services.

3.1.1 Administration Access with HiPath Manager E

Limit access to the OpenScape Business administration port to the administrator's PC. HiPath Manager E should only be able to communicate with the system from the administrator's machine. It is usually protected by a numerical password only (PIN).

CL-18 **OpenScape Business**	**Restrict access with HiPath Manager E**
Measures	• Access to the Manager-E port (TCP port 7000 by default) should be limited to the administrator's PC (IP address). This can be done through OpenScape Business Assistant application firewall configuration.
References	[1]
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

3.1.2 SMTP Interface

The Simple Mail Transfer Protocol (SMTP) is used to send mails to users and administrators. Encryption is recommended. SMTP can only be used with encryption when the used mail server supports that.

CL-19 **OpenScape Business**	**SMTP Interface secure**
Measures	• Secure communication is selected at WBM > Service Center > Email Forwarding (TLS/SSL)
References	[1]
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐ Deactivated: ☐
Customer Comments and Reasons	

3.1.3 SNMP Interface

The Simple Network Management Protocol (SNMP) can be used for sending error messages from the OpenScape Business to the SNMP server by trap. Form the standard security point of view this is

unproblematic. If the SNMP server sends get or set advices to OpenScape Business there may be a risk. Thus in this case the SNMP interface should be configured more secure.

A community string is available in SNMP V1/V2. It is comparable with a user ID that allows access to data of a device. The common community string names „public" and "private" should be changed into individual names. As the community string is transmitted in clear text it can be eavesdropped easily. Thus also IP addresses of systems that may contact OpenScape Business via SNMP shall be limited.

The SNMP V1 interface is not activated by default (i.e. IP address is 127.0.0.1). Enable SNMP only if necessary.

CL-20 **OpenScape Business**	**SNMP Interfaces secured**
Measures	• Restrict access for Read, Write and Trap communities to defined IP addresses and define individual community names.
References	[1] chapter SNMP
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐ Deactivated: ☐
Customer Comments and Reasons	

3.1.4 LDAP Interface

The Lightweight Directory Access Protocol (LDAP) is used for access to external databases. Unauthorized access may disclose company directory data. The interface is disabled by default.

CL-21 LDAP Server	**Protect LDAP access**
Measures	• Set up strong LDAP password at LDAP Server and OpenScape Business.
References	Administration manual LDAP Server [1]
Needed Access Rights	End user instructions
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

3.2 Firewalls

Firewalls are available within OpenScape Business X3 / X5 / X8 for routing via WAN and ISDN ports as well as for general IP access to OpenScape Business.

3.2.1 Port Opening

For some applications to be used via Internet, specific services/ports have to be enabled for the WAN interface to be forwarded to OpenScape Business and the internal LAN.

- Port forwarding is not active by default. All incoming IP traffic at the WAN interface without initial request from internal is blocked.

- Please use ‘opening ports’ with care. The firewall is no longer in place for those IP services/ports. The enabled communicating applications shall meet extended security standards e.g. by encryption and efficient access control and robustness against denial-of-service attacks and message floods.
- A web proxy in a DMZ may enhance security, but can lead to dependencies with some devices and browsers.

Notes:

- Port Forwarding must not be used for external VoIP subscribers and trunks as this bears the risk of attacks and toll fraud by unauthorized access. Please use only VPN for remote IP subscribers.
- Port Forwarding must not be used for application access from external e.g. by OpenScape Business desktop clients or CSTA applications. These interfaces are not completely secured and may be intercepted and misused.

If an external router/firewall is used instead of the integrated firewall, the rules below apply as well.

CL-22 **OpenScape Business / external router**	**Port Opening inactive or restricted**
Measures	• Necessity and risk for opening ports is checked. • Not essential port openings are deleted.
References	[1]
Needed Access Rights	Advanced
Executed	Yes: ☐ No: ☐ none active: ☐
Customer Comments and Reasons	Please document forwarded ports and usage

3.2.2 Application Firewall

IP address filtering protects OpenScape Business against unauthorized access from the internal or external network. Access via LAN is possible for all needed ports by default. Access to defined ports/services can be restricted to specific IP addresses or ranges of IP addresses or can be blocked totally by entering 127.0.0.1.

Use application firewall restrictions for the predefined ports with care since you can lose all access to OpenScape Business. Please check the rules diligently before activating them.

CL-23 **OpenScape Business**	**Application Firewall / IP address filtering**
Measures	• Enable rules for application firewall, if it is seen necessary and does not hinder administration access
References	Administration manual [1]
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐ not active: ☐
Customer Comments and Reasons	Please document IP address filtering

3.2.3 PSTN Peers Communication

PSTN peers communication can be used for remote devices or administration via ISDN or analogue modems. CHAP is preconfigured in OpenScape Business within “Routing PSTN” and shall be used, if it is supported by the communication partner.

CL-24 OpenScape Business / external router	**PSTN Peers communication secured**
Measures	• Keep CHAP setting and use strong password • Activate call back and / or call number verification and use only outgoing direction if possible
References	[1]
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

3.3 Secure Tunnel (VPN)

Secure tunnels are strongly recommended for networking as well as for remote access. For every VPN remote subscriber a dedicated authentication shall be selected. This allows easy blocking of a remote access e.g. when an employee leaves the company.

Recommended operation mode:
IKE "Main Mode" with Perfect Forward Secrecy and DH Group 2 / 5 / 14 (Default)
Encryption with AES (check consistent setting in the VPN Client)

A) **Pre-shared Key** (Recommended only for a limited number of devices)

- Chose key word according to password recommendation with minimum length of 20 bytes (see 10.1).
- A secure transmission and storage of the key word has to be guaranteed.

B) **Certificates** shall be used for increased security requirements or with an existing PKI Infrastructure. Configuration is more complex (expert mode).

- Recommended operation mode: RSA 2048 bit and hash function with SHA-2
- Documentation of certificates and serial numbers and safe storage has to be guaranteed.

CL-25 OpenScape Business / external router	**Networking and remote access allowed via VPN only**
Measures	• Check with end user that all remote user, remote administrator or networking connections are secured with VPN. If necessary implement VPN.
References	[1]
Needed Access Rights	End user instructions
Executed	Yes: ☐ No: ☐ No networking/remote access: ☐

Customer Comments and Reasons	Pre-shared key ☐ Certificates ☐

4 OpenScape Business UC Suite (Option)

If OpenScape Business UC Suite is not part of the solution, please continue with chapter 5.

The OpenScape Business UC Suite offers extended functionality and can be used instead of UC Smart. The OpenScape Business UC Suite and the CSTA interface are provided by the optional OpenScape Business UC Booster Card or by OpenScape Business UC Booster Server. The administration of OpenScape Business UC Booster Card is integrated with the base system.

For differences, when using the OpenScape Business UC Booster Server see chapter 5. For general PC and server security requirements see chapter 8.

4.1 OpenScape Business UC Clients

The OpenScape Business UC Suite delivers unified communication with personal, attendant and Contact Center clients. Passwords according to the password rules have to be used. For the PC based communication clients an alphanumerical password would be possible. In most cases, access to voice mail from normal phones is also needed. To cover that use case, a numerical Password (PIN) has to be selected. The minimum recommended and default length is 6 digits.

The following OpenScape Business client applications are available:

- myPortal for Desktop, myPortal for Outlook, myPortal for Mobile / Tablet
- myPortal for OpenStage, OpenScape Business Fax Printer
- myAgent, myReports
- myAttendant

Client applications provide amongst others rule-based call forwarding and automated attendant or conferences. This could be misused for toll fraud, if unauthorized persons get access to the applications. To protect from unauthorized access, the general password rules have to be followed for the client software and the devices on which they are running.

Notes:

- Unauthorized access to the call journal and log files at the client PC may disclose the individual communication history of the user.
- The clients provide call recording for calls and conferences. This can be disabled system-wide within OpenScape Business Assistant.
- Callback out of voicemail is possible by default only from specific call numbers configured for the user. Please be aware that changing this setting brings a residual risk of misuse by fraudulent callers.

CL-26 OpenScape Business Clients	**Change password for myPortal, myAgent, myAttendant and protect the devices, where they are running**
Measures	• The login password (also used as mailbox PIN, numerical) has to be set to an individual value, by every user • Unattended PCs and mobile devices must be locked
References	PIN recommendations see 10.1
Needed Access Rights	End user instructions
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

4.2 IP Interfaces UC Booster Card

The optional UC Booster card provides two 1 Gbit Ethernet interfaces. Only one is currently used for communication via customer infrastructure. It provides all those IP services, which are necessary for the OpenScape Business functionality. Some IP services can be restricted, if needed.

4.2.1 SAMBA Share (File Service)

A SAMBA share provides help files to the OpenScape Business clients. It is also needed for first distribution of OpenScape Business client software, and for system backup.
The directories are read-only by default where possible. The file service can be switched off, if customer security policy requires that. In this case, the automated functions mentioned above are not available. Distribution of client SW and help files has to be done manually by the administrator. The necessary files are available via OpenScape Business Assistant at Service Center.

CL-27 **OpenScape Business**	**SAMBA is deactivated (option)**
Measure	Deactivate SAMBA share
References	[1] at Telephony > Security > SAMBA Share
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

4.2.2 XMPP Interface

The Extensible Messaging and Presence Protocol (XMPP) is used for presence federation and chat (e.g. with Google Talk). The OpenScape Business XMPP server offers encrypted and unencrypted communication. Selection depends on the communication partner. Communicate only with XMPP servers which support encrypted communication, if instant messages and presence status has to be confidential. In this case the default self-signed certificates have to be accepted by the external XMPP Server.

Note: Port-forwarding for TCP port 5269 has to be activated to be able to use XMPP via WAN (see 3.2.1)

CL-28 **OpenScape Business**	**Secure XMPP communication**
Measures	Use an external XMPP Server, which supports secure communication. Remark: servers who do not accept self-signed certificates cannot be used.
References	---
Needed Access Rights	End user instructions
Executed	Yes: ☐ No: ☐ XMPP not active: ☐
Customer Comments and Reasons	Used external XMPP Server :

4.2.3 SMTP Interface

Simple Mail Transfer Protocol (SMTP) is used within UC Suite to receive mails for Contact Center agents. Encryption is recommended. SMTP can only be used with encryption when the used mail server supports that. This is an additional interface independent from the base system.

CL-29 **OpenScape Business**	**SMTP Interface secured**
Measures	• Select 'Use SSL' for inbound e-mail services at UC Suite > OpenScape Business > Contact Center
References	[1]
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐ Deactivated: ☐
Customer Comments and Reasons	

4.2.4 LDAP Interface

The Lightweight Directory Access Protocol (LDAP) is used in OpenScape Business UC Suite for access to external databases / LDAP servers as a client. This is an additional interface independent from the base system.

Unauthorized access may disclose company directory data.

CL-30 **OpenScape Business**	**Protect access to external LDAP Server**
Measures	Please make sure to use strong passwords for external LDAP servers. Set up strong LDAP password at OpenScape Business Assistant 'Expert mode' 'UC Suite' for the LDAP connector
References	[1]
Needed Access Rights	End User Information, Configuration: Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

4.2.5 Open Directory Service

The Open Directory Service (ODS) is providing subscriber information from OpenScape Business to other applications and clients via LDAP. The information is collected from internal and external databases. Unauthorized access may disclose company directory data.

Notes:

- Port 389 has to be open for access to the integrated LDAP server within OpenScape Business / Linux.
- For access to external SQL servers, strong passwords shall be defined as well..

CL-31 **OpenScape Business**	**Protect internal LDAP server access**
Measures	Set up strong LDAP password at OpenScape Business Assistant 'Open Directory Service' for the integrated LDAP server.
References	[1], Password policy see 10.1
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

4.2.6 CSTA Interface

The Computer-supported telecommunications applications (CSTA) interface allows monitoring and control of devices, which are connected, to OpenScape Business. This functionality is used by OpenScape Business UC application as well as via CSTA interface or via TAPI 120/170 middleware by external 3rd party CTI applications. External applications are served via UC Booster Card or Server only.

Attackers with LAN access and CSTA knowledge might exploit this interface to initiate calls.

CL-32 **OpenScape Business**	**Disable or limit CSTA access**
Measures	• Limit access to specific servers using application firewall or block access if not needed (see 3.2.2)
References	[1]
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

5 OpenScape Business S / UC Booster Server (Option)

If OpenScape Business S or UC Booster Card Server is not part of the solution, please continue with chapter 6.

OpenScape Business S is the UC soft switch, which runs on a standard server with Suse Linux Enterprise Server (SLES) operating system. It has basically the same features and IP interfaces as OpenScape Business X3 /X5 / X8, but no WAN interface, router and VPN is supported within OpenScape Business.

OpenScape Business Booster server is used instead of the integrated OpenScape Business UC Booster Card for higher subscriber or traffic ranges. It has its own web-based administration. Relevant differences regarding administration and interfaces are described in this paragraph.

5.1 Server Administration

OpenScape Business S / Booster Server is running on SLES 11 operating system, which is administrated independently. The administrator of the server has root rights, which are have to be protected.

The same rules as for OpenScape Business X3 / X5 / X8 apply for the web-based local and remote administration of the OpenScape Business itself, see 2.2 . The server PC for OpenScape Business shall be kept protected as much as possible, see also 2.1.

Notes:

- Security threat through viruses is considered to be low in a protected environment for the Linux-based OpenScape Business S or Booster Server. There is a risk of degradation of real-time performance by Anti-Virus software. For customers whose policy requires Anti-Virus software in any case, the Trend Micro software 'ServerProtect for Linux' can be used.
- A SLES Appliance solution is under evaluation to be used instead of the standard SLES operating system. This may affect the SLES SW update.

CL-33 OpenScape Business Server PC	**Protect OpenScape Business Server Operating System Suse Linux Enterprise Server (SLES)**
Measures	• Automatic SLES update is activated at installation • Secure and confidential root password implemented • No user accounts in addition to the original settings • The root account should have no additional rights in the customer network and the server should not be used for other applications.
References	[8]
Needed Access Rights	Linux administrator
Executed	Yes: ☐ No: ☐ Not part of solution ☐
Customer Comments and Reasons	

5.2 IP Interfaces Server

Only the IP services, which are needed for OpenScape Business operation, are activated in the Linux Firewall during installation. It is strongly recommended not to open additional ports. If it is required to close some ports, which are not essential and not used in the specific customer installation, this can be done within Linux.
After an OpenScape Business restart the integrated rules are activated again, additional rules are not changed.

6 Xpressions Compact Card (Option)

If Xpressions Compact Card is not part of the solution, please continue with chapter 7.

Inadequate handling of mailbox passwords by customers increases the risk of toll fraud. This can happen via the use of substitute auto attendant or call back feature. In order to avoid such issues, the measures described below must be taken.

6.1 Administration Xpressions Compact Card

Outgoing traffic should be blocked from Xpressions Compact for day and night service, by setting all IVM ports to system class of service (COS) 'outward restricted' from HiPath Manager E.

CL-34 **Xpressions Compact**	**Limit IVM Ports Class of Service to 'Outward-restricted'**
Measures	• In HiPath Manager E under 'Classes of Service → station' check that the default COS group is 'Outward restricted'. • In Day and Night service the class of service is set to 'Outward restricted'. • If Least Cost Routing is active Class of Service at LCR > Dial Plan has to be activated (default):
References	[2]
Needed Access Rights	Service
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

Also the default Class of Service for IVM mailboxes should be set to COS3 instead of the default COS, if the feature 'call forwarding to substitute' is not needed.

CL-35 **Xpressions Compact**	**Limit IVM mailbox Class of Service to COS3**
Measures	• In HiPath Manager E under 'Auxiliary equipment →Integrated voicemail (IVM)' change the setting from COS4 to COS3 for configured IVM ports.
References	[2]
Needed Access Rights	Service
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

By using the IVM WBM, it is possible for the Administrator to view and modify all user accounts by logging in as Super user. The Super user PIN should be set according to the recommendations in section 10.1. The maximum length of the Super user PIN is 8 (configurable from Manager E or Xpressions Compact WBM).
For the administration role 'service' the same credentials as for HiPath Manager are used.

CL-36 **Xpressions Compact**	**Implement a strong PIN for Super user**
Measures	Choose a strong PIN for the Super user account in the HiPath Xpressions Compact WBM. This is configured via the 'Mailbox Administration → SU Super user → General Settings' menu options.
References	[4]
Needed Access Rights	Service
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

The DLI login page is also accessible from the HiPath Xpressions Compact WBM, and this introduces the security risk of an unauthorized party altering phone configurations or accessing other privileged information. To avoid the risk it is necessary to change the default password of the DLI user from "DLI" to a more secure combination.

CL-37 **Xpressions Compact**	**Implement a strong PIN for the DLI user**
Measures	Choose a strong PIN for the DLI account. This setting is accessible from within the HiPath Xpressions Compact WBM via the 'Basic Settings → Change Password' menu options.
References	[4] for password policy see 10.1
Needed Access Rights	Service
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

6.2 Mailbox Protection

Along with these features, it is important to explain the importance of safe mailbox code numbers to the customer, that they should be kept confidential and that they protect by this voice messages and features out of the mailbox. It is recommended to keep the default code number length of at least 6 digits. All users have to change their mailbox PIN immediately. This is enforced during the first mailbox access. The mailbox PIN is also used for the WBM 'user role'.

CL-38 **Xpressions Compact**	**Protect all mailboxes by individual PINs**
Measures	• Each user is instructed to choose a strong PIN • All group mailboxes and auto-attendant mailboxes get a strong PIN
References	For password policy see 10.1 Note: The setting is also accessible from within the Xpressions Compact WBM.
Needed Access Rights	End user instructions

Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

Maximum login attempts should be set to 3 to block brute force attacks. (Default)

CL-39 Xpressions Compact	**Set maximum login attempts to 3**
Measures	Check / configure number In Manager E, under Auxiliary equipment →Integrated Voice Mail (IVM) → IVM → Additional Settings → Additional
References	[2]
Needed Access Rights	Service
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

The measures described above block toll fraud but they also limit access to the following features:

- Call back external party from voice mailbox
- Message notification call to external destination
- Call forwarding to substitute number
- Auto-attendant for external destinations
- Xpressions Mobility
- Xpressions Conference

If those features are needed, the OpenScape Business COS for the IVM ports has to be extended with care e.g. to allow only local or national calls.

6.3 IP Interfaces Xpressions Compact Card

The LAN interface of Xpressions Compact Card is used for

- Voice-mail to E-Mail
- Web-based Management (customer, super user and service)
- Service tasks like fast SW-update

Several IP ports and services are used for HiPath Xpressions Compact, which cannot be administrated. Please make sure, that access to the LAN interface of Xpressions Compact Card is not possible from unauthorized devices and especially from the Internet.

Note:
The application firewall in Manager E to protect specific IVM interfaces is currently not available.

7 Further Components

All released applications and components are documented in the OpenScape Business V1 sales information or current release note. Please take into account the product-specific security checklists for all components, which are included in the solution.

7.1 OpenScape Business Cordless / HiPath Cordless IP (DECT)

For unsecured and inappropriate configurations, eavesdropping attacks at DECT devices have been reported. The following has to be observed to impede such attacks:

Encryption is active for HiPath Cordless DECT devices by default. This setting must be changed only temporarily e.g. for diagnostics.
Only the officially released components out of the Gigaset / OpenStage professional family shall be used. DECT-Headsets, DECT TAE plugs or other DECT devices can jeopardize confidentiality.

7.2 Wireless LAN (WLAN)

WLAN phones can also be used with OpenScape Business. Please make sure that a secure transmission like WPA2 is chosen (compare product related security checklist and / or administration manual).

7.3 TAPI 120 / TAPI 170 / CallBridge IP

These applications provide CTI interfaces for phone call control and monitoring. They run on Windows client PCs or servers and are protected by Windows' own security mechanisms e.g. access control and user accounts. The TAPI middleware makes use of the CSTA interface, see 4.2.6.

Access to the hosting PCs has to be protected. For server security measures see chapter 8.

7.4 OpenScape Business Attendant

OpenScape Business Attendant is a Windows application which allows call monitoring and call transfer as well as feature control (e.g. call forwarding) for a single system or a network of OpenScape Business systems. It is connected via USB or LAN at a suitable OpenScape Business phone.
OpenScape Business BLF (Busy Lamp Field) uses the same interface.

For the hosting PCs the rules from chapter 8 apply.

Notes:

- Network-wide subscriber busy state information is exchanged via IP with a central BLF Server. This Windows application is part of the product. It uses by default TCP, default port 3001. This port has to be accessible in all nodes (see also 3.2.1).
- The number of simultaneously operated OpenScape Business Attendant applications is restricted by the installed number of licenses.
- SW update is possible via Internet from a fixed IP address.

7.5 OpenStage Gate View

OpenStage Gate View is an integrated video surveillance application, which displays pictures from up to eight cameras at OpenStage phones. Display is also possible for mobile phones via app or web browsers using HTTPS. Video recordings can be stored at the system or a network drive.

The administration of the Gate View application is done within OpenScape Business Assistant. This includes user set-up and monitoring of live pictures and recordings. Appropriate measures should be taken to protect video streams and recordings against unauthorized access.

Note: For picture display at mobile phones or external web browsers, the port 443 has to be accessible from the Internet. For risks of port forwarding, see 3.2.1.

CL-40 OpenStage Gate View	**Secure Access to Videos and Recordings**
Measures	• Change the user names and passwords for all used cameras – never use the well-known default • Set up strong user names and passwords for user web-access. Instruct users to use strong individual passwords. • Change the passwords for every camera web-access • Define strong user name and password for the network drives, if video recordings are stored there and have to be protected.
References	[1], 10.1
Needed Access Rights	Expert and End user instructions
Executed	Yes: ☐ No: ☐ Not Part of Solution: ☐
Customer Comments and Reasons	

8 Desktop and Server PCs

General requirements for all PCs, which run communication clients and applications:

- The operating system version is released for the communication software (see sales information)
- Current security updates for the Operating System and Java are installed (see also [5]).
- A suitable virus protection SW shall be installed and active (see also [6]). This is especially true for mail servers and Windows PCs.
- Access is protected by passwords according to the password rules (see 10.1)
- Virtual environments have to be secured accordingly

Depending on the responsibility for the devices which host the OpenScape Business solution components this is a service or an end user instruction.

CL-41 Desktop and Server PCs	**Security updates, virus protection and access control**
Measures	Security updates, virus protection and access control are implemented
Desktop PCs for OpenScape Business Clients	Yes: ☐ No: ☐ Not part of solution ☐
Server for OpenScape Business	Yes: ☐ No: ☐ Not part of solution ☐
Server for TAPI	Yes: ☐ No: ☐ Not part of solution ☐
PC for OpenScape Business Attendant	Yes: ☐ No: ☐ Not part of solution ☐
Other	…….. Yes: ☐ No: ☐ Not part of solution ☐
Customer Comments and Reasons	PC Operating System / Update Antivirus

9 Phones and Voice Clients

OpenScape Business supports several system and system independent phones and clients e.g.

- OpenStage T (TDM)
- OpenStage HFA (IP, full system feature set)
- OpenStage SIP (IP, standard SIP protocol)
- OpenScape Client Personal Edition (IP soft client)

Please observe the product-related security checklists and / or administration manuals. For OpenStage HFA devices, compare checklist [7]. Use released devices according to the current sales information only.

It is recommended that the **administration** access to the devices is protected by individual passwords. Do not keep the initial value.

CL-42 All Phones and Voice Clients	**Administration access protected by strong password (PIN)**
Measures	Change password at phone or via phone WBM
References	Phone Administration Guides and 10.1
Needed Access Rights	admin
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	System-specific PIN ☐ device-specific PIN ☐

Note for IP Phones:
The web-based HPT tool allows for displaying and operating the phone interface from a remote PC for service purposes. Precondition is the download of a “dongle key” to the phone by the administrator and for observation sessions the agreement by the phone user. Access is protected by the password above. The “dongle key” can be disabled, if not needed.

In addition, the **registration** of an IP device with OpenScape Business shall be protected by an individual password. This secures from bringing a new device with a known call number to the network which will take over the part of the original device. For HFA devices activation of authentication is recommended.

CL-43 OpenScape Business and HFA Devices	**HFA device authentication activated (option)**
Measures	Activate authentication at OpenScape Business Assistant and set up related passwords in the phones.
References	[1], Phone Administration Guide, 10.1
Needed Access Rights	Expert, admin
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	System-specific PIN ☐ device-specific PIN ☐

For SIP devices, **authentication** must be used in OpenScape Business to protect against registration of unauthorized devices. This applies also to HiPath Cordless IP devices and SIP terminal adapters. Increasing SIP attacks may lead to toll fraud or service degradation. As SIP is a widely-used standard, threat is higher than for HFA phones.

CL-44 **OpenScape Business and SIP devices**	**SIP device authentication activated**
Measures	• Authentication activated for all SIP subscribers with strong passwords • An individual password is used for every device (so that not the whole system is corrupted if one phone is lost) • SIP User ID is different from call number (e.g. by using a system specific prefix)
References	[1], 10.1
Needed Access Rights	Expert
Executed	Yes: ☐ No: ☐
Customer Comments and Reasons	

10 Addendum

10.1 Recommended Password Policy

These are the recommended criteria for selection of passwords or PINs (numerical passwords). Please implement them unless other company specific rules are defined at customer site.

	Password	**PIN**
Minimal Length	8	6
Minimal number of upper case letters	1	-
Minimal number of numerals	1	all
Minimal number of special characters	1	-
Minimal number of lower case letters	1	-
Maximal number of consecutive identical characters (e.g. bbb, 333)	3	2
Maximal number of sequential characters in increasing or decreasing order (e.g. abc, 123, 987)	3	3
Account name (reversed too) may not be part of password	true	true
Change interval (maximum password age)	90 days	90 days
Password history (latest used passwords must not be used again)	5	5
Minimum character count for changed password characters	2	2

Do not use trivial or easy to guess passwords. Take care that password entry cannot be observed.

Currently there is no enforcement of these rules within OpenScape Business. All users have to be instructed to comply with password policies and are responsible for their observation.

For UC Smart clients unsafe passwords are rejected by default.

10.2 Accounts

Here the accounts for OpenScape Business inclusively user accounts of systems that can access OpenScape Business are listed.

Since the default passwords are publicly available, it is absolutely necessary to change them into customer specific passwords immediately after installation process.

Be aware that most successful attacks to SEN systems base on unchanged default passwords.

10.2.1 OpenScape Business Assistant

#	User Name	User Role	SEN Default PW (to be changed immediately)	Description
1	administrator	Advanced	administrator	Administration of OpenScape Business (Change is requested at first logon.)
2	---	Expert	---	Will be set up by administrator
3	---	Basic	---	optional

10.2.2 HiPath Manager E

#	User Name	User Role	SEN Default PW (to be changed immediately)	Description
1	31994	Service	31994	Administration of OpenScape Business for special tasks
2	office or 633423	Customer	633423	Administration of selected items by customer (usually done with OpenScape Business Assistant)
3				

10.2.3 Clients

#	User Name	SEN Default PW (to be changed immediately)	Description
1	<phone number>	1234	OpenScape Business UC Suite Clients and access to voicemail from phone Change is requested at first logon (6 digits)
2	<phone number>	00000	Individual Phone Lock Code, DISA PIN, Desktop sharing PIN, Flex call PIN
3	<phone number>	System-specific initial PIN	Mailbox Access for Smart Voicemail
4	<phone number>	-----	Client access for Smart UC (User or system specific password defined by administrator)

10.2.4 Xpressions Compact Card

#	User Name	SEN Default PW (to be changed immediately)	Description
1	administrator	31994	Same as for Manager E
2	super user	12345678	Change is requested at first logon
3	user	1234	Change is requested at first logon

10.2.5 OpenStage Gate View

#	User Name	SEN Default PW (to be changed immediately)	Description
1	admin	----	Access via OpenScape Business Assistant as Expert
2	user	-----	Optional, initial value defined by admin
3			

10.3 Certificates

Please define here, which certificates are used.

Interface	Customer requirement	Default	Usage
HTTPS		SEN default certificate	Server authentication for web-based administration (OpenScape Business Assistant and web services / myPortal)
TLS / SRTP		Generated via lightweight CA	Signalling and payload encryption for secure voice calls with HFA Phones
IPSEC		Pre-shared key	Virtual private network for IP networking and remote access

Please make sure that pre-shared keys and certificates are stored and transmitted confidentially.

10.4 Port List

A current list of the ports which are used with OpenScape Business can be found at in the appendix of the Administration Manual [1] or via the SEN Partner portal SEBA, at the menu item 'Support' > 'Interface Management (IFMDB)'.

10.5 References

Link to OpenScape Business V1 Product Information:
https://enterprise-businessarea.siemens-enterprise.com/productinfo/producthomepageservice.jsp;?mainTab=external_productversion&view=spp&phase=home&pvid=515258&portalViewLeftNavigation=productinformation

[1] **OpenScape Business V1 Administrator Documentation**
available via e-Doku or SEBA Portal / product information

[2] **HiPath Manager E Administrator Documentation**
available via e-Doku or SEBA Portal / product information

[3] **OpenScape Business V1 Service Manual**
available via e-Doku or SEBA Portal / product information

[4] **Xpressions Compact Installation and Administration Manual**
available via e-Doku or SEBA Portal / product information

[5] **Support of Operating System Updates for Server Applications**
http://wiki.siemens-enterprise.com/images/c/c0/Security_Policy_-_Support_of_Operating_System_Updates_for_Server_Applications.pdf

[6] **Support of Virus Protection Software for Server Applications**
http://wiki.siemens-enterprise.com/images/2/21/Security_Policy_-_Support_of_Virus_Protection_Software_for_Server_Applications.pdf

[7] **Security Checklist OpenStage V2 Phones**
https://enterprise-businessarea.siemens-enterprise.com/productinfo/document/Fz!Eyz-tRHM_/OpenStage%20SIP%20V2%20Installation%20Guide%20-%20Security%20Checklist.pdf

[8] **OpenScape Business V1 Installation Linux**
available e-Doku or SEBA Portal / product information

About Siemens Enterprise Communications:

Siemens Enterprise Communications is a leading global provider of unified communications (UC) solutions and network infrastructure for enterprises of all sizes. Leveraging 160 years of experience, we deliver innovation and quality to the world's most successful companies, backed by a world-class services portfolio which includes international multi-vendor managed and outsourcing capabilities. Our OpenScape communications solutions provide a seamless and efficient collaboration experience – on any device – which amplifies collective effort and dramatically improves business performance. Together, our global team of UC experts and service professionals set the standards for a rich communications experience that empowers teams to deliver better results. Siemens Enterprise Communications is a joint venture of The Gores Group and Siemens AG, and includes Enterasys Networks, a provider of network infrastructure and security solutions, creating a complementary and complete enterprise communications solutions portfolio.

For more information, please visit:
www.siemens-enterprise.com or www.enterasys.com

Siemens Enterprise Communications
www.siemens-enterprise.com

Siemens Enterprise Communications GmbH & Co. KG is a Trademark Licensee of Siemens AG

Hofmannstr. 51
81359 Munich, Germany

Status 10/2012