

# V3 Security Checklist

## Planning Guide

A31003-P3030-P100-06-76A9

# Contents

- History of Changes .....3
- 1 Introduction .....4
- 2 OpenScape Business V3 Hardening Procedures in General.....7
- 3 Server Hardening .....17
- 4 Virtualization.....26
- 5 Cloud Installation.....27
- 6 OpenScape Business V3 .....28
- 7 3<sup>rd</sup> Party Components.....70
- 8 Administration .....73
- 9 Protection of LAN based Communications .....85
- 10 LAN Interfaces and Protocols .....93
- 11 Phones and Voice Clients .....123
- 12 Addendum .....131
- 13 Abbreviations .....147
- 14 References .....149

# History of Changes

Date	Version	What
2020-05-29	3.0.0	Initial Creation for OpenScape Business V3
2021-01-15	3.1.0	Creation for OpenScape Business V3R1
2021-08-01	3.1.2	Enhancements for OpenScape Business V3R1.2
2022-04-04	3.2	Creation for OpenScape Business V3R2
2022-11-08	3.2.1	Enhancements for OpenScape Business V3R2.1
2023-05-12	3.3	Creation for OpenScape Business V3R3 <ul style="list-style-type: none"> <li>editorial changes</li> <li>remove: Gate View, XMPP (Openfire), OpenSSL</li> <li>add: OpenScape Desk Phone CP700 family, Media Sever V3 mainboard family</li> <li>update: 6.2.13 Unify Phone</li> </ul>
2023-06-14	3.3.0.1	Update for GA OpenScape Business V3R3 <ul style="list-style-type: none"> <li>editorial changes</li> <li>remove: 10.4.3 fallback to TLS 1.0</li> <li>update: 6.2.14.1 MS Teams Direct Routing (link to How To)</li> <li>update: 12.2.3.1 Root access</li> </ul>
2023-07-21	3.3.0.2	2 <sup>nd</sup> Update for GA OpenScape Business V3R3 <ul style="list-style-type: none"> <li>update: 10.5.6.1 SSH interface</li> </ul>

# 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.

Unify 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 channels, 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:

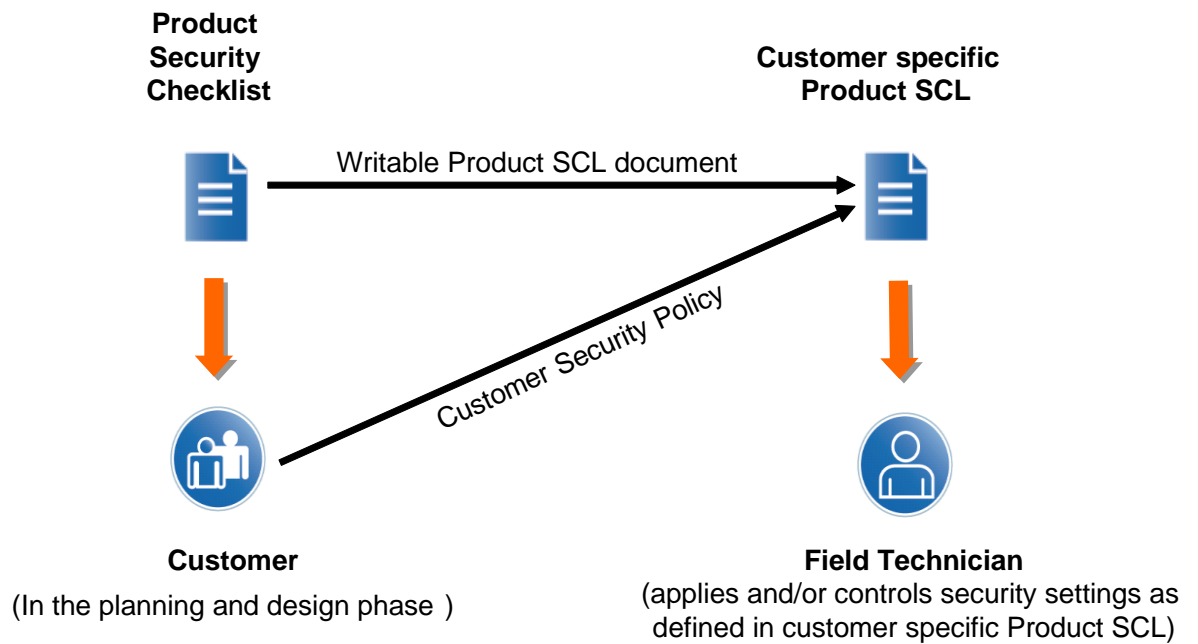
Use the Product Security Checklists of every relevant product to evaluate, if all products that make part of the solution can be aligned with the customer's security requirements – and document in the Checklist, how they can be aligned. The Product Security Checklist containing customer alignments can be identified as Customer specific Product Security Checklist.

This ensures that security measures are appropriately considered and included in the Statement of Work to build the basis for the agreement between Unify and the customer: who will be responsible for the individual security measures:

- a. During installation/setup of the solution
- b. During operation

- **During installation and during major enhancements or software upgrade activities:**

The Customer specific Product Security Checklists are used by a technician to apply and/or control the security settings of every individual product.



**Figure 1: Usage of Security Checklists (SCL)**

### 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 always using the latest version of the Security Checklists of the products that are part of your solution.

They can be retrieved from the Unify partner portal  
<https://unify.com/en/partners/partner-portal>

## 1.2 Customer Deployment - Overview

This Security Checklist covers the product OpenScape BusinessV3 (referred as OpenScape Business V3 in the following) and lists their security relevant topics and settings in a comprehensive form.

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



# 2 OpenScape Business V3 Hardening

## Procedures in General

The information in this document is intended to support the service technicians, re-sellers, customers and consultants in the examination and setting of the required security measures in the software and at the hardware for OpenScape Business V3 and the affiliated products listed below. The current security settings are to be confirmed by the customer by means of signature in the delivery of OpenScape Business V2 and the affiliated products. Deviations of the security settings on customer request have to be documented.

### 2.1 Scope

Software version V3 supports two kinds of mainboard families within the OpenScape Business X models. On one hand the so called "V3 Mainboards" that have been newly introduced together with SW version V3. On the other hand, the so called "V2 Mainboards" that have been introduced with the first introduction of OpenScape Business X models itself.










"V3 Mainboards" offer significantly higher performance than "V2 Mainboards" and do not require any additional UC Booster hardware.

All information within this security checklist referring to UC Booster Card (OCAB) or UC Booster Server apply only to OpenScape Business X models with "V2 Mainboards" and are not valid for systems with "V3 Mainboards".

If a chapter within this document is only valid for specific mainboard family a note is added in the heading of the chapter.

- "V3 MB only" refers to OpenScape Business X systems with "V3 Mainboards"
- "V2 MB only" refers to OpenScape Business X systems with "V2 Mainboards" and optional UC Booster HW.

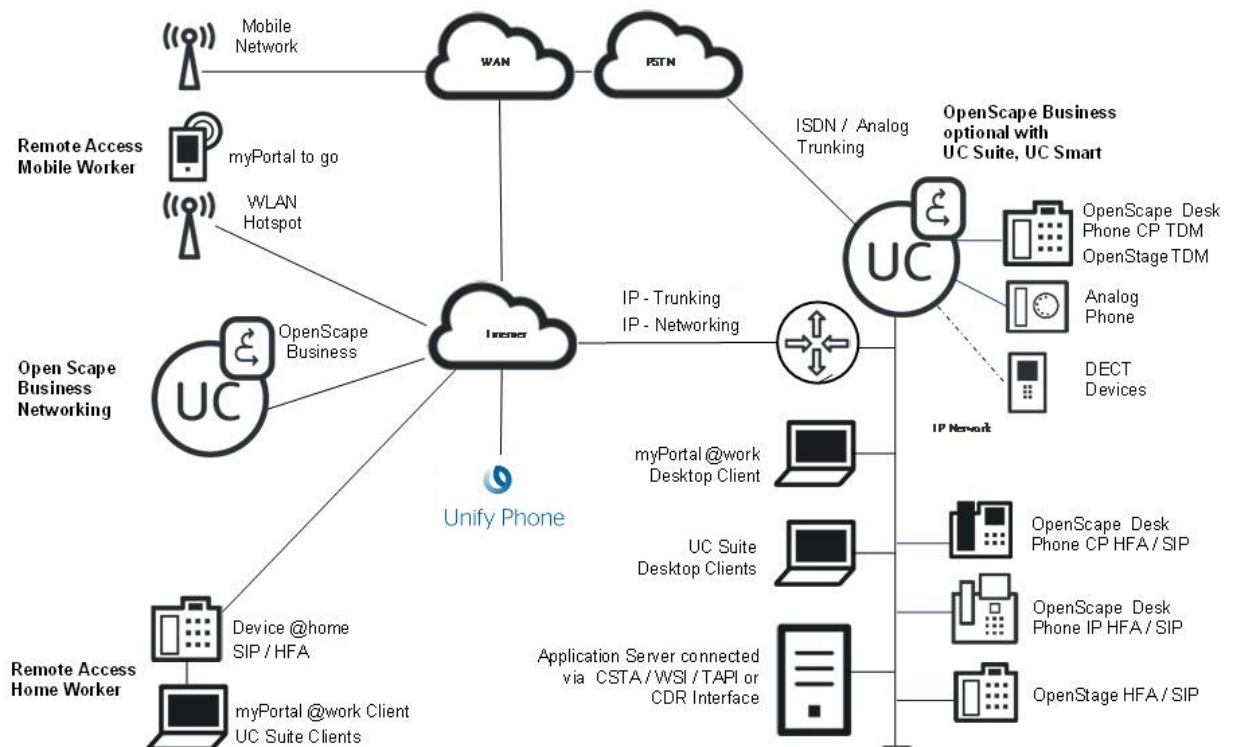
## 2.2 OpenScape Business Models

OpenScape Business X1	OpenScape Business X3	OpenScape Business X5	OpenScape Business X8	UC Booster Server (V2 MB only)	OpenScape Business S
Rack Version	Rack Version	Rack Version	Rack Version	Rack Version	Rack Version
				n/a	n/a
Wall Version	Wall Version	Wall Version	Wall Version	Wall Version	Wall Version
				n/a	n/a
Server-based solution	Server-based solution	Server-based solution	Server-based solution	Server-based solution	Server-based solution
n/a	n/a	n/a	n/a		

**Table 1: OpenScape Business models**



## 2.3 OpenScape Business Configuration Overview



**Figure 2: OpenScape Business Configuration Overview**

Beneath the pure call processing OpenScape Business offers various applications/services either embedded as an "All in One" solutions or located at an external computer.

Unified Communications solutions with: Auto Attendant, Voicemail, E-Mail-, Fax-routing and presentation of user and/or device status is as well supported as pure voice call routing between various kinds of trunks and subscribers with different devices.

In addition, OpenScape Business supports mobile workers or home workers by:

- the integration of their mobile devices like Smartphones, Tablet PCs, or their desk phones at home into the call processing and into the UC solution
- the interaction with Unify Phone, Unify's cloud based collaboration solution.

Several services like Directory- or LDAP-service, standard APIs like TAPI and the support of standard protocols like CSTA broadens up the data exchange with external 3rd party applications and data sources.

The availability of many features depends on the activated licenses.

OpenScape Business administration can be done either by embedded web-based Administration Portal, external PC application or via telephone.

On premise administration access is supported as well as remote access via Internet connection or via ISDN.

## 2.4 OpenScape Business safeguarding

For safeguarding of an OpenScape Business based communications solution all components have to be considered. The recommended measures are listed in the following chapters.

First point is to install only up-to-date software. The latest software version of software that is delivered by Unify is available on the Unify Software Supply Server. We recommend to also the installation of up-to-date software versions and patches of additionally needed 3rd party software. Please also consider manufacturer advisories as well as Unify security advisories (see chapter 14 [7]).

### 2.4.1 Infrastructure (LAN, WAN)

For the internal / external IP network, the requirements according to the administrator documentation [1] have to be met.

Unauthorized access to LAN infrastructure components may open the LAN and its components for attackers. Eavesdropping, Toll Fraud and malfunctions in general are possible if unauthorized persons can access the LAN.

Access to central components like switches and routers has to be restricted to technicians and administrators.

### 2.4.2 OpenScape Business Communication Platform

provides 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 offers two different deployment options in general:

- **OpenScape Business X1, X3, X5 or X8**

are "All-In-One" solutions with on board IP access and support for up to 500 subscribers with IP, digital (UP0E), ISDN (BRI), analogue (a/b), cordless (DECT) devices. UC Smart / Suite application is fully embedded. Connection to public WAN is done via SIP (LAN), ISDN (BRI and PRI) or analogue trunks.

OpenScape Business X models use proprietary computer HW (no standard PC HW) with proprietary Boot Loader and an embedded Linux OS.

- **OpenScape Business S**

is the server-based "All-In-One" telephony and UC platform, which supports up to 1500 IP subscribers and IP (SIP) connection to the public network (WAN). It is designed for Linux (Novell SLES) operating system and can be operated either on a physical or on virtual machines with VMware vSphere or Microsoft Hyper V.

OpenScape Business S can be networked with OpenScape Business X1, X3, X5 or X8 as gateway for ISDN or analogue trunks or TDM / analogue devices.

Open Scape Business S model uses standard PC server HW with BIOS etc.

### 2.4.3 UC Booster Server (V2 MB only)

UC Booster server provides the following applications, services and functions in general:

- UC Suite Application (optional)
- UC Smart Application (optional)
- Open Directory Service (optional)
- CSTA interface for connecting external applications

Location of SW components is controlled dynamically by the OpenScape Business base system during system initialization depending on the system configuration:

UC Booster server bases on computer HW with LAN interfaces. It is available in two HW flavors:

- **UC Booster Card**

as an HW option for OpenScape Business X3/X5 or X8.

It is inserted into OpenScape Business X3, X5 and X8 models

UC Booster card uses proprietary computer HW (no standard PC HW) with proprietary

Boot Loader and an embedded Linux OS.

- **UC Booster Server**

is based on a standard PC server HW and is an option for OpenScape Business X3/X5 or X8. UC Booster Server is derived from OpenScape Business S in order to enhance the number of UC participants. From technical point of view, it is the same HW / SW and functionality as OpenScape Business S, except the telephony application. 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.

## **2.4.4 Standard Desktop PCs and Tablet PC**

Standard Desktop PCs and Tablet PC are used for communication clients and central components.

General requirements for all PC are:

- The operating system version is released for the communication software (see sales information)
- Current security updates for the Operating System and Java are installed.
- A suitable virus protection SW shall be installed and active. This applies especially true for mail servers and Windows PCs.
- Access is protected by passwords according to the password rules (see chapter 12.1)

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

## **2.4.5 Desk Phones and Mobile Phone Devices**

Subscriber devices like OpenScape CP phones and 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.

General requirements for all desk phones and mobile phones are:

- The operating system version is released for the communication software (see sales information)
- Current security updates for the Operating System are installed.
- Access is protected by passwords according to the password rules (see chapter 12.1)

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

## **2.4.6 Application Server**

External Telephony-, Unified Communication- or Contact Center Server etc. use the CSTA, WSI, CDR etc. interfaces of OpenScape Business in order to offer their services. OpenScape Business offers admission control to these interfaces and optionally data

encryption depending on the interface. In general interfaces should only be enabled within OpenScape Business if server applications are connected. In case interfaces are enabled strong passwords have to be used for access control. If possible, data encryption has to be enabled to protect OpenScape Business data from breach of confidentiality.

<b>Client Application SW</b>		
<b>UC Suite Clients</b>		
myPortal for Desktop	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
myAttendant	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
myPortal for Outlook	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
myAgent	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
myReports	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
myPortal @work	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
myPortal for Teams	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
<b>UC Smart Client</b>		
myPortal @work	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
myPortal for Teams	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
<b>Mobility Clients</b>		
myPortal to go App	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
<b>Miscellaneous Clients</b>		
Application Launcher	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
ODBC-ODBC Bridge Server component	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
OpenStage Personal Edition	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
Manager E	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:

<p><b>Further SW components</b></p> <p><b>Unify SW</b></p> <p>OpenScape Business TAPI 170</p> <p>OpenScape Business TAPI 120</p> <p>CallBridge Collection</p> <p><b>3rd party SW</b></p> <p>Internet Browser</p> <p>Java (JRE)</p>	<p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/> Version:</p> <p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/> Version:</p> <p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/> Version:</p> <p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/> Version:</p> <p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/> Version:</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>PCs / Servers / Devices Operating Systems / Firmware</b>		
<b>Servers</b>		
OpenScape Business S	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
UC Booster (V2 MB only)	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
OpenScape Business TAPI 170	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
<b>Client PCs</b>		
UC Suite Client PC	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
UC Smart Client PC	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
OpenScape Business TAPI 120 PC	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
CallBridge Collection PC	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
Other PC	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
<b>Mobile Devices:</b>		
Smartphones OS	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
Tablet PCs OS	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
<b>Desk phones / Devices Firmware</b>		
OpenScape DeskPhone CP (HFA/SIP)	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version
OpenScape DeskPhone CP T	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
OpenScape DeskPhone IP (HFA/SIP)	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
OpenStage HFA	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
OpenStage SIP	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
OpenStage T	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
Other Devices	Yes: <input type="checkbox"/>	No: <input type="checkbox"/> Version:
<b>Customer Comments / Reasons</b>		

**Note:** Based on the SW installed, the necessary patch management for the customer shall be defined. Patch management is out of scope of the Product Security Checklist.

## 2.5 Availability

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

CL-Avalab LAN Infrastructure	Enhanced Availability
Measures	<p>A possible weakness is electrical power supply. For countries with higher probability of power outages, a separate uninterruptible power supply (UPS) for telephony and related components may be sensible.</p> <p>Two or more independent public network trunks extend availability in case of carrier failures.</p> <p>For the server based OpenScape Business, a server with redundant power supply and/or hard disk (SW RAID) can be used.</p> <p>Higher availability is achieved by using a suitable virtual server environment (please see current release documentation).</p>
References	
Needed Access Rights	
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

## 2.6 Redundancy

OpenScape Business single node does not provide any redundancy.

Redundancy can be achieved either by means of virtual machines (OpenScape Business S only) or within an OpenScape Business network by survivability scenarios. Details about survivability scenarios are described within the administration manual [1].

## 2.7 Backup and Restore

Backup and Restore of the OpenScape Business database is supported via the administration portal. From security aspect it is recommended to backup and archive data periodically.

Backup files are secured by system specific content encryption against unauthorized access.

**Note:**

Encryption applies for the complete Backup option only. The Diagnostic Backup option is stored unencrypted and has to be secured against unauthorized access.



## 2.8 Storage Media

OpenScape Business uses mass storage media (SDHC card, M.2 SATA SSD or M.2 M.2 NVMe SSD) for the operating system, system configuration and dynamic data collected during operation.

Dynamic data can contain depending on system configuration: Personal data, personal and company directories, call data records, voicemails, e-mails, faxes, instant messages.

### **Risk:**

Data content of the mass storage media of OpenScape Business is not encrypted. Data can be retrieved by an attacker from the storage media in case of physical access to the media.

### **Measures:**

Data media that have once been used in OpenScape Business may not be made available to unauthorized persons and have to be treated confidentially in general.

Customer has to be informed about the content of the data media.

In case of data media exchange (for example, for service purpose), data on storage media have to be erased by appropriate tools, (formatting only or repartitioning is not sufficient in this case). Data media used in OpenScape Business may not be refurbished and sold without individual check and proof that data are deleted and cannot be restored.

Measures above apply for:

- The operating system version is released for the communication software (see sales information)
- Current security updates for the Operating System are installed.
- Access is protected by passwords according to the password rules (see chapter 12.1)

<b>CL-Storage Media Handling OSBiz V3</b>	<b>Storage media handling</b>
Measures	Inform customer about data content of OpenScape Business storage media.  Destroy data content of storage media irreversibly using appropriate tools in case that storage media is changed.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

## 3 Server Hardening

Each standard server HW that runs OpenScape Business V3 must be hardened. A distributed deployment of OpenScape Business V3 may need more than one server.

General requirements for all standard server PCs, which run communication servers and applications:

- The operating system version is released for the communication software (see sales information)
- Current security updates are installed (see chapter 2)
- A suitable virus protection should be installed and should be activated (see 3.7). This applies especially for mail servers and Windows PCs.
- The access to the system must be protected by passwords according to the password rules in chapter 12.1.1.
- After installation all SW components which were required for the installation process (diagnostic tools like Wireshark, putty) and old SW versions have to be removed from the server.

### Note:

OpenScape Business X systems use proprietary HW with a proprietary Boot Loader and embedded Linux OS.

### 3.1 Hardware Security Settings

Communication systems are important parts of every company. Physical access to the communication system HW, to its power supply and the main network infrastructure components have to be restricted to authorized persons only.

Appropriate means and access controls have to be implemented to prevent physical access of unauthorized persons to the communication system.

CL-SRV-Access	Restrict physical access to server HW
Measures	Physical access has to be limited to authorized persons only e.g. by locking the room or the cabinet / rack.
References	N/A
Needed Access Rights	Authorized Persons equipped with key
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>  By means of: .....
Customer Comments / Reasons	

### 3.2 Bios Settings

The PC server BIOS access and its settings have to be configured in a way that unauthorized persons cannot get access to the server system, to its storage media, to the operating system or to the application, e.g. by booting the server from an USB-Stick.

### 3.2.1 BIOS password protection

Access to the BIOS allows changing the boot order of the server. Once changed an intruder may use tools that are bootable from CD-ROM or USB device that allow a user to change the administrator password, install files or retrieve sensitive information. To prevent this, BIOS needs to be password protected.

CL-SRV-BIOS-PW	BIOS password protection
Measures	A BIOS password needs to be set to avoid changing essential settings (i.e. boot order) in the BIOS setup.
References	N/A
Needed Access Rights	Server Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 3.2.2 BIOS Boot order

If boot order in BIOS setup is set wrong, any intruder may use tools that are bootable from CD-ROM or USB device which allow him to change the administrator password, install files or retrieve sensitive information. The boot order must be set properly to prevent misuse.

CL-SRV-BIOS-BO	BIOS Boot order
Measures	Set boot order in BIOS setup to <b>NOT</b> boot from removable media.
References	N/A
Needed Access Rights	Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 3.2.3 BIOS Remote-Hardware-Monitoring

The OpenScape Business software does not rely on the iRMC (Integrated Remote Management Controller) interface or on any kind of these remote monitor/control functions, which are available by default in some Server HW. These remote management interfaces should be disabled per default within the BIOS.

<b>CL-SRV-BIOS-RMC</b>	<b>Remote hardware monitoring usage</b>
Measures	From the OpenScape Business perspective, usage of iRMC for remote hardware monitoring is disabled. The service technician should disable therefore the iRMC feature in BIOS, if available.
References	N/A
Needed Access Rights	Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 3.2.4 BIOS Remote Console

The OpenScape Business software does not rely on the remote console interface which is available by default on some server. These remote interfaces should be disabled per default within the BIOS.

<b>CL-SRV-BIOS-RCon</b>	<b>Remote console on some server HW</b>
Measures	From the OpenScape Business software perspective, usage of remote console is not needed. The service technician should disable therefore this feature in BIOS.
References	N/A
Needed Access Rights	Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

## 3.3 Operating System (OS) Hardening

OpenScape Business model X and UC Booster card (V2 MB only) are so called "SW Appliances", which include HW, Operating System and the application SW, while OpenScape Business S and UC Booster Server include only the applications SW. OpenScape Business S and UC Booster application SW are installed on standard Server HW platform with standard Linux OS (SLES).

Therefore, different OS hardening procedures have to be considered for OpenScape Business model X and model S.

### 3.3.1 OS Hardening for OpenScape Business X models

The operating system of the OpenScape Business X systems is delivered and installed as an integral part of the OpenScape Business X SW image.

All relevant OS updates are part of Fix- or Minor Releases (FR/MR), which are released regularly. In special cases a Hotfix can be provided for OS security relevant update. In both these SW packages the OS dependencies are already resolved, thus no manual or separate OS maintenance is necessary, possible or allowed. The transfer and activation of software updates takes place either on premise via Service Center within the Administration Portal or remotely.

**Note:**

In order to update OpenScape Business X systems a valid OpenScape Business SW support is required. Otherwise, the system will refuse SW updates. New ordered OpenScape Business systems are equipped with an initial SW support license for 3 or for 5 years. The SW support can be extended for 1 or 2 years by ordering additional licenses.

CL-OS Hardening OSBiz X V3	OS Hardening for OpenScape Business X-Models
Measures	<ul style="list-style-type: none"><li>• Check that SW support is valid within the system</li><li>• Setup system settings for manual or automatic SW update</li><li>• Setup Internet access to SW update Server</li><li>• Communicate SW Support expiring date to customer</li><li>• Advise customer to renew SW support before expiring date</li></ul>
References	<ul style="list-style-type: none"><li>• Security advisories</li><li>• Technical Release Notes</li><li>• Administration Manual</li></ul>
Needed Access Rights	Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 3.3.2 OS Hardening for OpenScape Business S and OpenScape Business UC Booster Server (V2 MB only)

OpenScape Business S and UC Booster Server run on Novell SLES 12. The SLES 12 OS software is delivered with default setting and default configuration by Unify on a separate DVD in a bundle with the OpenScape Business S / Booster Server DVD.

A so called "SLES Subscription registration key" can be ordered separately. This key grants a 3 year SW updates for SLES by Novell beginning with the day of subscription.

**Note:**

OpenScape Business customers have to purchase the SLES Subscription and to register it at Novell. In addition, internet access for the server has to be setup and SW update has to be activated within the SLES administration.

In case of SLES subscription the SW update settings within YAST have to be configured in a way that security relevant patches for SLES OS are downloaded and installed automatically.

CL-OS Hardening OSBiz S V3 UC Booster Server V3	OS Hardening for S Modell and UC Booster Server (V2 MB only)
Measures	<ul style="list-style-type: none"> <li>• <b>For SLES 12 OS</b> Ensure that customer has ordered SLES Subscription registration key and ensure that customer registers it at Novell.  Setup Internet access for the sever PC</li> <li>• <b>For OpenScape Business S / UC Booster SW</b> Check if SW support licenses are activated within the System  Setup system settings for manual or automatic SW update  Setup access to SW update Server of Novell within SLES</li> <li>• <b>Inform customers about expiring dates and renewal procedure</b> Communicate SW Support expiring dates to the customer  Advise customer to renew SW support before expiring dates  <b>Configure SLES (Yast) in a way that security patches are downloaded and installed automatically</b></li> </ul>
References	<ul style="list-style-type: none"> <li>• Sales Information</li> <li>• Administration Manual [1]</li> </ul>
Needed Access Rights	SLES Administrator

Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 3.4 OpenScape Business Application SW Hardening

All relevant OpenScape Business SW updates are part of Fix- or Minor-releases (FR/MR), which are released regularly. In specific cases a hotfix can be provided for an OpenScape Business SW security relevant update.

The transfer and activation of software updates takes place either on premise via Service Center within the Administration Portal or remotely.

In order to update OpenScape Business X and S Application SW, a valid OpenScape Business SW support is required. Otherwise, the system will refuse SW updates. New ordered OpenScape Business systems are equipped with an initial SW support licence for 3 or 5 years. The SW support can be extended for 1 or 2 years by purchasing additional licenses.

<b>CL-SW Hardening OSBiz V3 Application SW.</b>	<b>Application SW Hardening for OpenScape Business</b>
Measures	Check that SW support licenses are activated within the system Setup system settings for manual or automatic SW update Setup Internet access to SW update Server Communicate SW Support expiring date to customer Advise customer to renew SW support before expiring date
References	<ul style="list-style-type: none"> <li>• Security advisories</li> <li>• Technical release note</li> <li>• Administration Manual [1]</li> </ul>
Needed Access Rights	Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	



### 3.5 Clean Customer Deployment

<b>CL-CleanDeployment OSBiz S V3 UC Booster Server V3 (V2 MB only)</b>	<b>Remove all SW coming from Unify that is not necessary for the customer deployment.</b>
Measures	After Installation all SW that were necessary as installation help (Diagnostic tools like Wireshark, putty, old SW Versions ...) has to be removed from Server.
References	
Needed Access Rights	Administrator
Executed Server 1: Server 1: Etc.	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 3.6 OpenScape Business S / UC Booster Server Protection on Server Level

Depending on the customer deployment the user accounts on the Operating System level may be part of the OpenScape Security Checklist. Many customers take care of the OS user accounts by themselves. Nevertheless, the customer must be aware, that the security of server access on OS level is not independent of the security of OpenScape Business S or UC Booster Server.

- Access right settings for user accounts (read/write access to file system)
- OS Password policies (details see 12.1.4)
- Default PW replacement (details see also 12.2.3)

#### Single Sign On password

A user cannot access the OpenScape Business S or UC Booster server by Single Sign on, which is based on the Operating System accounts that are stored on the server. Specific login data (user / password) are required for OpenScape Business administration access etc.

#### OpenScape Business V3 Data Protection on Server:

For the protection of the data stored locally (e.g. in file systems) the user accounts for the OS should have only limited access rights.

Description, which user roles are possible (user/administrator/others)

Which default OS accounts are necessary is depicted in the appendix in Chapter 12.2.3.

<b>CL-SrvPwd OSBiz V3 Server PCs</b>	<b>Access to the server / PCs are protected by passwords.</b>
------------------------------------------	---------------------------------------------------------------

Measures	Customer specific PW policy is defined as depicted in addendum chapter 12.1.1. Default accounts are depicted in chapter 12.2. The default passwords are replaced by individual passwords.
References	Valid PW policies see chapter 12.1.1. Default Accounts see chapter 12.2.
Needed Access Rights	Administrator
Executed Server 1: Server 1: Etc.	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 3.7 Virus Protection

Trend Micro Virus Protection SW is released for use within OpenScape Business S or UC Booster Server.

Virus Protection SW of other manufacturers can also be used, if customer security policies do not allow the Trend Micro SW. In this case customer bears the responsibility for the functionality. If malfunctions are caused by this SW component, the Trend Micro SW has to be used instead.

<b>CL-VirusProtect OSBiz V3 Server PCs</b>	<b>Virus protection software is installed and active.</b>
Measures	Virus scanner to be used (e.g. Trend Micro)
References	
Needed Access Rights	
Executed Server 1: Server 1: Etc.	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Yes: <input type="checkbox"/> No: <input type="checkbox"/> Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 3.8 SAMBA File and Print services

SAMBA is a free software suite to make the Server Message Block protocol (SMB) of windows available for UNIX Systems. SMB also is known as Common Internet File

System (CIFS), LAN Manager or NetBIOS protocol. SAMBA provides file and print services for various Microsoft Windows clients and can be integrated with a Windows Server domain, either as a Primary Domain Controller (PDC) or as a domain member. It can also be part of an Active Directory domain. SAMBA is standard on nearly all distributions of Linux and is commonly included as a basic system service on other Unix-based operating systems as well.

In the SMB/CIFS networking world, there are only two types of security: user-level and share-level. In fact, SAMBA implements share-level security only one way, but have four ways of implementing user-level security. They are known as share, user, domain, ADS, and server modes.

Details find here:

<http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html>

## 4 Virtualization

OpenScape Business S and UC Booster Server can be operated on following virtualized Server environments.

- vSphere by VMware
- HyperV by Microsoft

OpenScape Business S specific settings for virtual machines are described within the OpenScape Business S Installation Guide [15].

The virtualization SW is not part of the software delivery of OpenScape Business S and it is out of scope of this document. The customer is responsible for the implementation of hardening measures.

We recommend hardening according to CIS Benchmarks. Please follow the Benchmarks dependent on your virtualization SW of the Center of Internet Security CIS.

<https://benchmarks.cisecurity.org/en-us/?route=downloads>.

# 5 Cloud Installation

The advantage of cloud-based services is that they can be accessed via the Internet at any time and from any location. However, this advantage is accompanied by the risk that the connections on the Internet are vulnerable to attack.

For this reason, cloud providers provide special access and authorization mechanisms to ensure the security of their cloud services and protect them from unauthorized access and misuse.

To protect customer-specific applications from unauthorized access and misuse, the Cloud Providers offer their customers various tools and applications. These must be installed and set up by the customer itself or by a company commissioned by the customer in accordance with the requirements of its application.

## 5.1 OpenScape Business S on the Google Cloud Platform

Unify provides a specially prepared SW image for the installation of OpenScape Business S SW in the Google Cloud Platform (GCP). This contains a pre-installed Novell SLES operating system and a pre-installed OpenScape Business S system, which are installed and operated in the GCP as a server.

After the OpenScape Business S system has been installed and booted up, it is initially not possible to access the OpenScape Business Assistant (WBM) via HTTPS from the Internet. All ports are blocked by Google Cloud. HTTPS access and access to all other ports of the SLES operating system is not possible without corresponding configuration of the cloud environment.

All connections required to operate ITSP trunks, telephone devices, VoIP or UC clients on the OpenScape Business S system must be configured accordingly in the GCP firewall.

### **Risk:**

Each connection from or to the OpenScape Business S server in the cloud is routed directly via the Internet. In case of misconfiguration of the Google Cloud environment and / or OpenScape Business, these connections are open to attackers. Depending on a potential misconfiguration, all thinkable misuse scenarios are possible, from toll fraud, eavesdropping, spying on call data records via changing the configuration up to destroying the system.

### **Measures:**

After installation, the OpenScape Business S system and all connections to the system must be protected in the same way as would be required for an installation on a physical computer and as described in the corresponding chapters of this security checklist.

In the event that connections need to be protected by specific Internet router and firewall settings, the appropriate Google Cloud Platform tools or applications must be used. In addition, all connections to the OpenScape Business S system in the Google Cloud must be encrypted on GCP. This applies to both the signaling and the payload connection.

In the event that OpenScape Business S cannot encrypt a requested connection using its own means, the GCP VPN service must be used for this purpose.

All installed services and interfaces of OpenScape Business S and the means to protect them must be documented and communicated to the customer.

The configuration of OpenScape Business S and GCP must be performed by system specialists. Access to the cloud and OpenScape Business S administration must be restricted to these specialists.

## 6 OpenScape Business V3

OpenScape Business provides powerful Call Processing features for various devices and trunks via various interfaces and protocols. Among many other features the internal and external call routing is as well supported as call forwarding to internal and external destinations. Destination numbers can be dialed directly by the phone device, by the system using call forwarding or by applications using the call control interfaces.

In addition to the native call processing OpenScape Business offers embedded applications that are part of the OpenScape Business SW, and which are either located on the Mainboard or UC Booster HW (V2 Mainboard only) in case of OpenScape Business X models or on the OpenScape Business S server HW.

OpenScape Business provides several measures to allow or restrict dialing of outbound phone numbers. It also offers powerful mechanisms to allow or restricts feature and interface access for users and applications.

### 6.1 Call Processing

The call processing of OpenScape Business allows the user or an application to initiate calls to internal or external destinations using various interfaces, protocols and service providers.

General Risks:

Outbound calls dialed by user or application via public or private service providers are usually charged. Depending on the dialed number, duration of the connection or data volume the charges for outbound calls differ.

Unauthorized dialing of call numbers with high charges either directly or per call forwarding can be abused for toll fraud. This can lead to considerable costs.

Numbers with high charges can be dialed in general by:

- Local and networked subscribers
- Mobile subscribers using the DISA Port
- Embedded applications
- Externally connected applications

Call Forwarding can be programmed and / or used by:

- Local and networked subscribers
- UC Application with status depending on call forwarding
- Voicemail
- Auto Attendant, Personal Attendant application
- Contact Center application
- All Applications that use the call control interfaces

General Measures:

- Restrict allowed area codes for outbound dialling according to the user specific needs by setting appropriate Class of Service (COS) for day and night operation.
- Allow executable features like programming of call forwarding only according to the user specific needs e.g. by setting the user flags. Disable all features that are not necessary or not allowed for the user.
- Disable feature Associated Services, if not needed.
- Restrict DISA port access and feature execution by setting user flags.
- Disable call forwarding or call forwarding based features within external or embedded application if these features are not needed.
- Disable all embedded applications that are not needed.

- Disable all interfaces for connection of external application or clients that are not required.
- Protect phone devices and Client PC from unauthorized access

### 6.1.1 Access to Public Network - Class of Service (COS)

In general, the reachable call destinations have to be restricted per user or user group to the necessary numbers. The same applies for internal users that are controlled by embedded applications like Voicemail, Auto Attendant and all users that are controlled by embedded or 3rd Party applications. This has to be considered also for day / night service and also for modem and fax ports.

The restriction is done by definition of appropriate class of service (COS) and the assignment to users / trunks.

A restriction can be defined for calls that are controlled by the UC Suite e.g. with Call Me or Conference by proper setting of the route VSL feature in all COS groups.

CL-Set COS OSBiz V3	Restrict access to public networks for users / devices by appropriate COS
Measures	<p>Suitable Class of Service (COS) is assigned for every device via OpenScape Business Assistant</p> <ol style="list-style-type: none"> <li>1. Internal or outward-restricted trunk access for devices, where no external calls are needed (emergency calls still possible).</li> <li>2. Allowed Lists configured for well-defined necessary business connections, other destinations are blocked.</li> <li>3. Denied Lists configured to block special numbers or countries (as an alternative least cost routing (LCR) may be used).</li> </ol> <p>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.</p> <p>Further possibilities:</p> <ol style="list-style-type: none"> <li>1. 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"</li> <li>2. Delete the "call forwarding external" flag for all devices, which do not need it, especially for devices within reach of external persons.</li> <li>3. Disable the three "Transit permission" flags in system parameters if no transit traffic is needed.</li> </ol>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>



Customer Comments / Reasons	
-----------------------------	--

**Notes:**

- All outbound calls are logged in the system and can be checked with an accounting tool. For logging inbound 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).

## 6.1.2 Public Network Access – Transit Trunk

OpenScape Business provides the feature "Transit Trunk", which allows incoming outbound calls to seize another trunk directly by trunk access code and to dial outbound numbers. No authorization checks are done for this transit and no Least Cost Routing (LCR) rules are applied to these calls.

**Risk:**

Unauthorized dialling of call numbers with high charges via Transit Trunk can be easily abused for toll fraud. This can lead to considerable costs.

**Measures:**

The feature is disabled by factory delivery and controlled by a system flag, which. Due to the importance of the feature, it has to be checked, that the flag has not been enabled by hazard.

<b>CL-Check Transit Trunk OSBiz V3</b>	<b>Check Transit Trunk setting</b>
Measures	Check the system flag "Transit Trunk and ensure that it is disable if the feature it not used. In case that the feature is required then the customer has to be informed about the risk of toll fraud.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 6.1.3 Feature access - User Flags

CL-Set User Rights OSBiz V3	CL-Set User Rights
Measures	Restrict feature execution by setting the user flags for feature programming by the user according to the needs of the user.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 6.1.4 Associated Dialing and Associated Services

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

**Risk:**

Associated Dialing / Services can be executed by user at the phone as well as by applications via call control interfaces.

**Measures:**

Associated Dialing / -Services Flags may only be activated for users who need these features.

CL- Restrict Associate Services OpenScape Business V3	Restrict Associated Dialing / Services
Measures	<ol style="list-style-type: none"> <li>1. Enable the station flag only for users who need the function.</li> <li>2. Inform concerned users about handling and security risks.</li> </ol>
References	Administrator Manual User guide: Lock PIN - Service code *93 per default
Needed Access Rights	OSBiz: Expert of Administration Portal End user instruction
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>

Customer Comments and Reasons	The following users are enabled for associated dialing
-------------------------------	--------------------------------------------------------

## 6.1.5 Direct Inward System Access (DISA)

The Direct Inward System Access (DISA) port can be used by internal or external callers to dial call numbers via OpenScape Business and to execute features of OpenScape Business by dialing the feature codes.

Use of the DISA port is secured by a user individual lock code consisted of the internal call number and the PIN for the lock code. Access to external destination from DISA Port can be restricted by an appropriate class of Service (COS)

### Risk:

Unauthorized access to the DISA port can be used for calling external numbers with high charges and for programming of call forwarding for specific devices. Both can be used to commit toll fraud.

### Measures:

In general, the DISA port has to be disabled (no number assigned), if not used.

The DISA port is disabled within the factory settings of OpenScape Business. It has to be checked that the port is still disabled in case there are no mobile users to be supported by the system.

In case, that the DISA port is used the class of service, which is assigned to the DISA port, has to be checked for the correct settings.

The DISA login credentials have to be kept confidential by the users.

CL-DISA Port Check access OSBiz V3	Restrict DISA port access and features
Measures	Check that DISA port is disabled, if not used. Check COS for DISA port for correct settings if DISA is used Set individual PIN for each DISA user individually. A 5-digit sequence, which cannot be guessed easily, has to be selected
References	Administration Manual [1] User guide: Lock PIN - Service code *93 per default
Needed Access Rights	OSBiz: Expert of Administration Portal (DISA configuration) User: for lock PIN
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 6.1.6 Mobility feature

The feature "Mobility" integrates mobile phones and tablet PC into OpenScape Business. Beneath other features these devices are allowed to initiate calls via

OpenScape Business and to activate feature like call forwarding within OpenScape Business. The Mobility features can be accessed either by DISA port and DTMF control or via the myPortal to go application.

In both cases the mobile subscriber is identified through his transmitted phone number and in case of myPortal to go also by his login credential for the UC application.

**Risk:**

A small risk for toll fraud lies in pretending a registered calling number by fraudulent callers (CLIP no screening, possible via some VoIP providers).

**Measures:**

The devices that are registered for this service, have to be protected from unauthorized access.

For mobile devices the Callback dial method should be used for initiating outbound calls via OpenScape Business.

The instructions regarding the DISA port itself (6.1.5) have also to be considered

<b>CL-Protect Mobility Device OSBiz V3</b>	<b>Protect the devices registered for DISA / use callback</b>																								
Measures	Registered devices are protected from unauthorized access (e.g. PIN for mobile phones). Callback is used for enhanced security. Mobility users are informed and briefed.																								
References	Administrator Manual																								
Needed Access Rights	OSBiz: Expert of Administration Portal End user instruction																								
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Mobility not used: <input type="checkbox"/>																								
Customer Comments / Reasons	<p>The following users are registered for Mobility:</p> <table> <thead> <tr> <th>Mobile number</th><th>Callback activated</th></tr> </thead> <tbody> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> <tr><td>_____</td><td>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></td></tr> </tbody> </table>	Mobile number	Callback activated	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>	_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Mobile number	Callback activated																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								
_____	Yes: <input type="checkbox"/> No: <input type="checkbox"/>																								

## 6.1.7 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').

<b>CL-DeskSharing PIN OpenScape Business V3</b>	<b>Strong PIN for desk sharing users</b>
Measures	A strong system "Device Authentication Password" has to be set up within the system configuration for each desk sharing user.  (see chapter 12.1.1).  End user has to be informed about his password.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Desk sharing not used <input type="checkbox"/>
Customer Comments and Reasons	

## 6.1.8 Phones open to public access

### Risk:

Unauthorized access to "public phones" can be used to dial numbers with high charges or to program call forwarding which can be used for toll fraud. In case that such a phone is one of the first two system phones, system configuration can be modified by accessing Assistant T. In this case system integrity is breached.

### Measures:

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 dialing 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.

Do not place any of the first system phones for public access.

<b>CL-Protect "public accessible" devices OSBiz V3</b>	<b>Use code lock for phone device and set COS. Do not use one of the first two system phones.</b>
Measures	Use phone lock with an individual PIN to protect device.  Set COS for phone lock in order to restrict devices to the required functions.  Do not expose any of the first two system phones for public access.
References	Service code *93 (default) for PIN programming  Rule for PIN see chapter 12.1.1

Needed Access Rights	End user instruction
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> No phone for public access <input type="checkbox"/>
Customer Comments and Reasons	

### 6.1.9 Door Opener

OpenScape Business X1/X3/X5/X8 provides activation of door openers via phone.

**Risk:**

Remote access to door stations, which are controlled via DTMF, might be a security risk.

**Measures:**

Restrict access and authorization for door opener

<b>CL-Restrict Door Opener OSBiz V3</b>	<b>Restrict authorization for door opener</b>
Measures	Authorization is assigned only to those stations, where it is necessary
References	Manager E - Door release DTMF flag
Needed Access Rights	Service
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Door Opener not used <input type="checkbox"/>
Customer Comments and Reasons	List of stations

### 6.1.10 Call Supervision (Silent Monitoring)

The feature "Call Supervision" is disabled in OpenScape Business default configuration. The use of the features is forbidden in some countries or is only allowed within country specific regulations. Please observe the legal regulations in your country. In case of doubt the feature may not be enabled.

**Risk:**

Unauthorized access to the feature can be used for eavesdropping.

**Measures:**

It has to be ensured by protection of administration access and of authorized devices that this function is not misused.

<b>CL-Restrict Call Supervision OSBiz V3</b>	<b>Restrict Call Supervision (Silent Monitoring)</b>
--------------------------------------------------	------------------------------------------------------

Measures	Subscriber authorization and possible targets are restricted to the minimum needed.
References	
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Not used <input type="checkbox"/>
Customer Comments / Reasons	

### 6.1.11 Room Monitoring

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.

#### Risks:

Features mentioned above can be used by unauthorized persons for eavesdropping conversions within a room.

#### Measures:

The features listed above should be activated only for subscribers who need them. Keep predefined alerting tones and use them in accordance with country and company regulations.

#### Note:

Be aware that also with conference and open listening other persons may hear a phone conversation unnoticed.

<b>CL-Restrict Room Monitor OSBiz V3</b>	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	Administration Manual [1] Password Policy see chapter 12.1
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Not configured: <input type="checkbox"/>
Customer Comments and Reasons	

### 6.1.12 Online User

The Online User is a virtual subscriber within the system that is used for service purposes.

It is automatically set up after the first initialization of OpenScape Business SW with an internal call number and a DID number as the last subscriber in the system.

The call number depends on the OpenScape Business standard call number plan.



The Online User can be remotely controlled via the Manager E administration tool and supports the Assistant T system programming functions in this operating mode.

The Online User is not active after first SW initialization in this case "idle" is entered in the "access" column in the station configuration. It becomes active after the first access via the Manager E service tool. In this case the remark "ONLINE CARD xx-x" is entered within the "access" column.

From SW Version V3R2.1 onwards the Online User is initiated with enhanced security settings:

- One individual Call Distribution List (CDL) for day, night and intern
- Quality of Service (COS) is set to "local"
- No individual Call Forwarding (CFU, CFNR, etc.) is possible
- Session time out: after 15 minutes inactive or 30 minutes active time

Within previous SW versions Online User was initiated with the following defaults.

- Same Call Distribution List (CDL) for day, night and intern as all internal subscribers
- Quality of Service (COS) is set to "international"
- Individual Call Forwarding (CFU, CFNR, etc.) is possible
- No Session Timeout. Once the online user was activated, it can no longer be blocked via the OpenScape Business Assistant or Manager E administration tools.

**Note:**

In case of a SW upgrade or migration from V2 or V3R.x to V3R2.1 or higher, the existing Online User settings are kept and not reinitialized.

**Risks:**

The online user can be misused for toll fraud by forwarding incoming internal or external calls to external destination numbers with high charges.

Unauthorized access to the Online User via the Manager E service tool, either internally or externally, can be abused to program call forwarding, to commit toll fraud, or to change the system configuration. In this case, the system is compromised by the attacker.

**Measures:**

1. Restrict Online User features

In case that the "Online User" function is required for service tasks, the following measures must be done depending on the required service tasks.

- Delete DID number  
Deleting DID number prevent that external calls can reach the Online User.
- Delete internal number  
Deleting the internal station number prevents that internal calls can reach the Online User.  
This measure does not affect the Manager E online function to make calls via the online user and use Assistant T functionality for system administration.
- Delete station flag "FWD external permitted"  
This measure restricts call forwarding to internal destinations only.
- Change Call Destination List (CDL)  
The default CDL of the Online User is also used for other stations. It must be changed to **one** individual CDL for day, night and internal (\*,-,-,-) for the Online

User. This ensures that incoming calls to the Online User are not accidentally forwarded to unwanted external or internal destinations.

- Change Class of Service (COS) and restrict outgoing calls to local  
Set the COS of the Online User to "local". This ensures that calls to internal destinations can be initiated only.

2. Disable Manager E access via LAN connection within application firewall

In case that the Manager E tool and "Online User" function is not required the Manager E protocol can be disabled within the "Application Firewall" of the system. This can be done either in general or for specific IP addresses or IP address ranges.

Note:

The application firewall of the system affects only the LAN connection but not the ISDN connection of the Manager E.

The customer needs to be informed that the system provides a service access that he cannot control. He needs also to be informed about the features that can be performed using this kind of service access.

<b>CL-Online User Feature Restriction OSBiz V3</b>	Restrict Online User features
Measures	Check current settings of the Online User Restrict features to the minimum. Customer must be informed about remote access and available features.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	<div>DID number deleted Yes: <input type="checkbox"/> No: <input type="checkbox"/></div> <div>Internal number deleted Yes: <input type="checkbox"/> No: <input type="checkbox"/></div> <div>Fwd to external destination flag deleted Yes: <input type="checkbox"/> No: <input type="checkbox"/></div> <div>Individual CDL assigned Yes: <input type="checkbox"/> No: <input type="checkbox"/></div> <div>COS changed to local Yes: <input type="checkbox"/> No: <input type="checkbox"/></div> <div>Customer was informed Yes: <input type="checkbox"/> No: <input type="checkbox"/></div>
Customer Comments and Reasons	

<b>CL-Online User Disabled OSBiz V3</b>	Disable Manager E protocol
Measures	Block Manager E protocol for all or selected IP addresses within the application firewall.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Application firewall is set Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 6.2 Connection to an “other application”

Connections to subsequently mentioned applications are optionally. None of the applications are mandatory for the basic operation of OpenScape Business. In case that an application is not used by the customer the appropriate chapter can be marked as not relevant and need not to be considered.

In case that an external application was manufactured / delivered by Unify the application specific security checklist has to be considered in addition to this checklist.

### Risks:

Some Risks and measures are independent from a specific application such as unauthorized access to an unprotected Client PC and monitoring / recording of the LAN traffic. This gives attackers the chance to spy out data and to compromise the application and OpenScape Business, by

- Using call control features
- Spying out company and private directories and call journal:
- Spying out and modifying user account data.
- Spying out and modifying client / system configuration.

Eavesdropping of data transmission within the LAN

Connections between Client and Server can be eavesdropped easily within the LAN and especially within the Internet. This can be used to spy out the complete conversation and system login data

### Measures:

- Protect PC client from unauthorized access by
  - strong login credentials
  - automatic client locking
  - etc.
- Protect application by choosing strong individual password for application access.
- Use encrypted connection for data transmission within the LAN whenever feasible. Encryption is mandatory in case of Internet connections.

### 6.2.1 UC Suite

The OpenScape Business UC Suite is a powerful Unified Communication Application for voice calls, fax, instant messaging and e-mail. It offers user individual presence status with status dependent forwarding, individual journals for voice calls, fax and e-mail, user individual voicemail boxes, company attendant, personal attendant, virtual conference rooms and contact center functionalities beneath some other features.

The UC Suite application is located either on the UC Booster Card / Server (X-models) or on the server PC (S-model).

UC Suite provides the following client applications on base of Microsoft Windows OS:

- Native UC Suite clients
  - myPortal for Desktop (native UC Suite Client, also running on MAC OS)
  - myPortal for Outlook (native UC Suite Client)
  - myAttendant (native UC Suite Client)
  - myAgent (native UC Suite Client)
  - myReports (native UC Suite Client)
- Clients providing UC Suite functions
  - myPortal to go (client for UC Smart / UC Suite)
  - myPortal @work (client for UC Smart / UC Suite)
  - OpenScape Desk Phone CP 400/600/700 embedded UC application

In addition, a telephony user interface (TUI) on base of a DTMF tone control is available for voicemail handling via phone.

The login credentials of a UC Suite account consist of the username and a password. These login credentials are also used by the following clients (via the Web Services API):

- OpenScape Business Attendant
- OpenScape Business Busy Lamp Field
- Application Launcher
- 3rd Party applications connected to the WebService Interface (WSI)
- OpenScape Desk Phone CP 400/600/700 embedded UC application

UC Suite administration is done via the Administration Portal (WBM) of OpenScape Business. Specific administration pages within the Administration Portal can also be evoked by a Contact Center supervisor using the myAgent client.

UC Suite communicates via LAN interface with TCP/IP / UDP with its clients and services. Depending on the client, requested service and function several protocols are used.

The data transmission between the native UC Suite clients and the UC Suite server can be encrypted by using TLS. The encryption option is enabled within in the factory settings.

Protocol	Purpose	Checklist Reference
CSTA	Communication with OpenScape Business for call control and device monitoring	Chapter 10.5.11
TCP TCP / TLS	Communication with native UC Suite Client (except myReports) on base of proprietary protocol. For encryption either self-signed or trusted certificates can be used	Chapter 10.4.1; 10.4.3
SMTP	Communication with external E-Mail Server POP3 or IMAP secured or unsecured depending on e-mail server	Chapter 10.5.5
LDAP LDAPS	Communication with LDAP capable Directory Server.	Chapter 10.5.7
SQL SQLS	Native Client communication with UC Suite database server. Secured via TLS protocol	Chapter 10.5.10
HTTPS	Communication via HTTPS with OpenScape Business Web Server for UC Suite web based administration  Communication via HTTPS to MS-Exchange Server	Chapter 10.5.1
WSI	Web Services Interface for client login of non UC Suite clients using UC Suite credentials	Chapter 10.5.13.4
SMB	Import of a Contacts into the external directory from a CSV file.	Chapter 10.5.12

	Export of Contcat Center reports as file to a location in the network. (NFS, NAS etc).	
SFTP	Export of Contact Center reports as file to a location in the network. (NFS, NAS etc).	Chapter 10.5.3

### Risks:

UC Suite and its client applications allow for instance rule-based call forwarding and automated attendant or conferences. Callback out of voicemail is possible by default only from specific call numbers configured for the user. These mechanisms can be misused for toll fraud if unauthorized persons get access to the application.

Unauthorized access to the call journal, voicemail box and log files at the client PC may disclose the individual communication history of the user.

### Measures:

The UC user has to change the internal subscriber number as default login name to an individual not easy to guess name.

In addition, a strong password has to be used for login into a UC client.

For the PC based communication clients an alphanumerical password is possible.

Access to voice mail from normal phones can be protected by a numerical password (PIN) only.

The general password rules have to be followed for the client software and the devices on which they are running. Possible password and PIN policies including the default settings are depicted in the addendum 12.1.1.

Please add a chapter in the addendum with the policy the customer wants to be applied in his system.

Bypass of VM PIN must not be possible.

It has to be ensured by a system policy, that UC Suite user are not allowed to set the flag "Bypass of VM PIN" within their UC Suite client settings. This system policy is active per default from V3 on. Systems which are upgraded from previous SW versions have to be checked accordingly.

Enable TLS Encryption: In order to prevent eavesdropping of the data transmission in the LAN between UC Suite client and OpenScape Business TLS encryption has to be enabled within the OpenScape Business UC Suite configuration.

<b>CL-UC Suite ClientPwd OSBiz V3</b>	<b>Change login name and password for myPortal, myAgent, myAttendant and protect the devices, on which they are operated</b>
Measures	<p>Customer specific PW policy is defined as depicted in the appendix</p> <p>Default accounts are depicted in the appendix</p> <p>The login password (also used as mailbox PIN, numerical) has to be set to an individual value, by every user.</p> <p>Unattended PCs and mobile devices must be locked (see details in Customer Comments)</p>
References	Valid PW policies see chapter 12.1 "Password Policies"

	Default Accounts see chapter 12.2 Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal User
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-UC Bypass VM PIN OSBiz V3</b>	<b>Set UC Suite Policy in order to prevent "Bypass of VM PIN"</b>
Measures	Check that the UC-Suite system policy is active which prevents "Bypass of VM PIN" in the user settings.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-UC Suite Encryption OSBiz V3</b>	<b>Enable UC Suite TLS data encryption for myPortal, myAttendant, myAgent and myReports</b>
Measures	Data encryption is enabled within the OpenScape Business UC Suite server configuration
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

### 6.2.1.1 Remote connection of UC Suite clients

A VPN connection has to be used primarily for the connection of UC Suite clients via the Internet or other unsecure connections to OpenScape Business to ensure confidentiality.

**Note:** The connection of MS Outlook to a MS Exchange Server is out of scope of this Security Checklist in case of myPortal for Outlook.

In case that a VPN cannot be used the flag "TLS" is set within the UC Suite server configuration section. This enforces the tunnelling of all client connections within one encrypted connection to OpenScape Business.

The "DB" flag for "Direct Database" access of the clients must not be set in the server configuration.

Port 5432 for access to OpenScape Business UC Suite Database Server may not be opened in the Internet router of the company LAN.

<b>CL-UC Suite Remote Client - VPN OSBiz V3</b>	<b>Setup VPN for remote connection of UC Suite</b>
Measures	VPN connection from remote UC Suite client to OpenScape Customer has been established.  In case of myPortal for Outlook: Customer has been informed about the risk of an unencrypted Exchange Server connection.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-UC Suite Remote Client – TLS Encryption OSBiz V3</b>	<b>Setup TLS connection for remote connection of UC Suite</b>
Measures	"TLS" flag is set within the OpenScape Business UC Suite server configuration. "DB" flag is not set in the OpenScape Business UC Suite server configuration. Port 5432 is closed in the company Internet router.  In case of myPortal for Outlook: Customer has been informed about the risk of an unencrypted Exchange Server connection.



References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 6.2.2 UC Smart

OpenScape Business UC Smart is a Unified Communication application for voice calls. It offers user individual presence status with status dependent forwarding, individual journals for voice calls, directories and conference control beneath some other features.

UC Smart supports control of Smart Voice Mail via its graphical interface but Smart VM itself is an independent application within OpenScape Business (see Chapter 6.2.3 for details)

Within OpenScape Business X-models the UC Smart application is primarily operated on the main board. It is operated on the UC Booster card / server (V2 MB only) if a certain number of UC Smart users is exceeded.

Within OpenScape Business S UC Smart is always operated on the same machine as the OpenScape Business SW.

UC Smart provides the following UC client applications:

- Native UC Suite clients
  - myPortal Smart (native UC Smart client)
- Clients providing UC Smart functions
  - myPortal to go client (client for UC Smart / UC Suite)
  - myPortal @work (client for UC Smart / UC Suite)
  - OpenScape Desk Phone CP 400/600/700 embedded UC application

The login credentials of an UC Smart account consist of the username and a password. These login credentials are also used by the following clients (via the Web Services API):

- OpenScape Business Attendant
- OpenScape Business Busy Lamp Field
- Application Launcher
- 3rd Party applications connected to the WebService Interface (WSI)
- OpenScape Desk Phone CP 400/600 embedded UC application

UC Smart administration in general is done via the Administration Portal (WBM) of OpenScape Business.

The UC Smart Assistant within the Administration Portal allows a user to manage his profile settings by himself.

UC Smart communicates with its clients via LAN interface with TCP/IP using the Web Services API (WSI) and HTTPS. Depending on the client, requested service and function several other protocols are used.

Protocol	Purpose	Checklist Reference
----------	---------	---------------------

HTTPS	Communication via HTTP(S) with OpenScape Business Web Server.	Chapter 10.5.1
WSI	Web Services Interface for all UC features and call control	Chapter 10.5.13.4

### **Risks**

UC Smart client applications allow for instance rule-based call forwarding. This mechanism can be misused for toll fraud if unauthorized persons get access to the applications.

Unauthorized access to the call journal and log files at the client PC may disclose the individual communication history of the user.

### **Measures**

To protect UC Smart from unauthorized access, the individual UC Smart user password has to be changed before the client can be used. The password is valid for the UC smart client as well as for the UC Smart Assistant and also for those clients providing UC functionalities that are listed above.

It has to be ensured further on that the communication between UC Smart client and OpenScape Business is encrypted by using HTTPS.

#### **6.2.2.1 UC Smart User Password**

No default password exists for UC Smart users.

While setting up a UC Smart user the system administrator has to assign a password according to the UC Smart password policy either individually for each user or for all users. The UC Smart client cannot be used without an assigned password. With first login a UC Smart user is forced to change the password. The UC Smart user password is saved with encryption in the UC Smart database.

<b>CL-UC Smart ClientPwd OSBiz V3</b>	<b>Set user password for UC Smart account and protect the devices, on which they are operated</b>
Measures	<p>Customer specific PW policy is defined as depicted in the appendix</p> <p>Default accounts are depicted in the appendix</p> <p>The login password has to be set to an individual value, by every user.</p> <p>Unattended PCs and mobile devices must be locked</p>
References	<p>Administration Manual [1]</p> <p>Valid PW policies see chapter 12.1</p> <p>UC Smart Account see chapter 12.2</p>
Needed Access Rights	OSBiz: Expert of Administration Portal User
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

#### 6.2.2.2 UC Smart client protocol

The UC Smart Clients use the Web Services API with HTTPS or HTTP. The UC Smart Assistant uses HTTPS. Use of HTTP instead of HTTPS is only allowed for connection of:

- CP400/600 phones with embedded UC application using the OpenScape Business directories only.

These exceptions have to be documented.

For accessing myPortal to go via WAN it is necessary to configure a port-forwarding for port 8802 (HTTPS) or 8801 (HTTP) within the Internet Router. It is not recommended to also open port 8803 for external access.

To increase security for the internal LAN, an external web proxy can be used.

<b>CL-UC Smart Client Protocol OSBiz V3</b>	<b>Set clients protocol to HTTPS within system administration</b>
Measures	<p>Enable HTTPS for Web Services API within system administration.</p> <p>Disable HTTP protocol if it is not used by other clients.</p> <p>Document clients which use HTTP</p> <p>Set communication protocol to HTTPS within UC Smart Clients.</p>
References	<p>Administration Manual [1]</p> <p>myPortal Smart User manual</p>
Needed Access Rights	OSBiz: Expert of Administration Portal

Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	Clients using HTTP:

### 6.2.3 Smart Voicemail (VM)

The Smart Voicemail application is independent from UC Smart within OpenScape Business. It offers voicemail and auto attendant functionalities. The voicemail function plays a greeting to callers and offers them the option of recording a message or being routed to another number. Recorded voice message can be send as attachment to an e-mail recipient.

The AutoAttendant function can either be used as a personal Auto Attendant for subscribers / groups or as a central AutoAttendant in combination with a central attendant console.

Within OpenScape Business X-models the Smart VM application is primarily operated on the main board. It is operated on the UC Booster card / server if a certain number of Smart VM users are exceeded.

Within OpenScape Business S Smart VM is always operated on the same machine as the OpenScape Business SW.

Smart VM does not offer own clients. Voicemail and attendant functions are controlled and configured via the telephony user interface (TUI) by using DTMF. Received voice messages are indicated by Message Waiting Indicator (LED) of the phone and/or optionally via telephone display.

MyPortal Smart, myPortal @work, myPortal to go and myPortal for OpenStage clients allow the control of the Smart VM voicemail via their graphical user interfaces.

Smart VM is disabled by default. The initial setup is performed via the Administration Portal of OpenScape Business.

Smart VM communicates via several interfaces and protocols with the phone device or UC Smart clients.

Protocol	Purpose	Checklist Reference
SMTP	Default SMTP Port is 25 Encryption via TLS possible	Chapter 10.5.4
Analog DTMF	Voicemail control via tones generate by phone	n/a
Analog a/b	VM indication at analog phone, proprietary protocol	n/a
Digital Up <sub>0e</sub>	VM indication at digital Up <sub>0e</sub> phone, proprietary protocol	n/a
IP / HFA	VM indication at OpenStage /OpenScape Phones with proprietary HFA protocol	Chapter 10.5.13.1
IP / SIP	VM indication at SIP capable phones using SIP	Chapter 10.5.8

WSI	Web Services Interface (WSI) of OpenScape Business for: Communication with myPortal Smart clients	Chapter 10.5.13.4
-----	---------------------------------------------------------------------------------------------------	-------------------

#### **Risks:**

Callback out of voicemail is possible by default only from specific call numbers configured for the user. These mechanisms can be misused for toll fraud if unauthorized persons get access to the application.

#### **Measures**

In order to protect Smart VM from unauthorized access individual PINs for each user have to be used for login into Smart VM. Change the initial PIN to an individual, safe value to secure mailboxes against unauthorized access and the forwarding of external calls via mailbox.

Restrict Class of Service for the Smart VM port to "outward restricted". This is the default setting for Smart VM ports.

#### **Note:**

The following features require trunk access:

- Call sender of a voice message
- Mobility users can listen to voice messages via callback
- Messages are transferred to an external destination using the AutoAttendant

In case that trunk access is required the external numbers have to be entered within the so called "allowed lists".

<b>CL-Smart VM PIN OSBiz V3</b>	<b>Set user individual PIN for Smart VM.</b>
Measures	Customer specific PW policy is defined as depicted in the appendix Default PIN is depicted in the appendix The initial PIN has to be set to an individual value, by every user. Unattended phones, UC clients must be locked
References	Administration Manual [1] Valid PW policies see chapter 12.1 Smart VM Account see chapter 12.2
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-Smart VM COS OSBiz V3</b>	<b>Restrict calls out of voice mail</b>
Measures	Set Class of Service (COS) for the Smart VM ports to 'outward-restricted' for day and night service.

	<p>If call forwarding out of mailboxes is needed, COS shall be extended carefully only to those destinations, which are allowed to be reached.</p> <p>If Least Cost Routing is active, 'Class of Service' at Routing &gt; LCR &gt; Dial Plan must be activated (default).</p>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	<p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></p>
Customer Comments and Reasons	

## 6.2.4 Open Directory Service

Open Directory Service is an embedded Meta directory service that can be accessed via LDAP by clients, applications and communication devices. The Open Directory Service provides data from internal data sources like: Internal Subscribers, Speed Dials and optionally UC Suite internal and external directory. In addition, Open Directory Service can provide data from external data sources via optionally available data connectors for SQL or ODBC based databases.

Open Directory Service is located either on the UC Booster card / server (X-models) or the server PC (S-model). It does not provide native clients.

Administration is done via the OpenScape Business Administration Portal (WBM). The Open Directory server is disabled by default.

Open Directory Service communicates via LAN interface with TCP/IP with LDAP clients and external databases. Following protocols are used.

Protocol	Purpose	Checklist Reference
LDAP	<p>Communication with LDAP capable clients or applications.</p> <p>Note: Secure transmission via LDAPS is not supported</p>	Chapter 10.5.7
TCP / SQL	TCP / IP connection to / external SQL database server	Chapter 10.4.1

### Risks:

Open Directory Service allows access to all user contact data, internal Speed dials number and data which are stored in external directories, via LDAP. Unauthorized access to the directory service may disclose individual and company directory data.

### Measures

To protect from unauthorized access user name and password have to be used for login from an LDAP client into the Directory Service. Depending on the user account different data are provided.

Possible password and PIN policies including the default settings are depicted in the addendum 12.1.1.

LDAP transmission is not encrypted within the network. If customer security policy requires encrypted transmission, external means must be used.

For LDAP transmission port 389 is used as default. The port has to be changed according to the customer security policies if required. LDAP port has to be enabled within OpenScape Business or external firewall depending on customer's security policy. In addition, the ports used by the optional database connectors of Open Directory Service have to be enabled within the firewall.

<b>CL-ODS LDAP Pwd OSBiz V3</b>	<b>Choose strong individual passwords for every user to protect LDAP server of ODS</b>
Measures	Choose appropriate user account Set up strong Password for LDAP access of Directory Server
References	Administration Manual [1] Password policy
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

#### 6.2.4.1 SQL Connector

Open Directory Service provides SQL connectors, which allow TCP/IP connection to external relational data base servers like Microsoft SQL Server, PostgreSQL and Sybase SQL etc.

##### **Risk:**

The connection from OpenScape Business Directory Service to an SQL server is not encrypted and can be eavesdropped. Attackers with full access to the SQL server may get access to company directory data or in a worst case can corrupt / compromise the database.

##### **Measures:**

Open Directory Service access to the external data base server must be limited to "read only".

Therefore, the data source administrator has to create a "read only" user account for Open Directory Service. This user account has to be protected by a strong password according to the password policies for the SQL server.

The port for accessing the external SQL server has also to be opened within the firewall.

<b>CL-ODS SQL Pwd OSBiz V3</b>	<b>Secure ODS SQL connector for data source access</b>
Measures	Create own user account with read only permission within SQL data base server Choose strong password within database Server for this user account.
References	Administration Manual [1] Password policy for SQL server

Needed Access Rights	OSBiz: Expert of Administration Portal Database Server Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

#### 6.2.4.2 SQL Connector

Open Directory Service provides SQL connectors, which allow TCP/IP connection to external relational data base servers like Microsoft SQL Server, PostgreSQL and Sybase SQL etc.

##### Risk:

The connection from OpenScape Business Directory Service to an SQL server is not encrypted and can be eavesdropped. Attackers with full access to the SQL server may get access to company directory data or in a worst case can corrupt / compromise the database.

##### Measures:

Open Directory Service access to the external data base server must be limited to "read only".

Therefore, the data source administrator has to create a "read only" user account for Open Directory Service. This user account has to be protected by a strong password according to the password policies for the SQL server.

The port for accessing the external SQL server has also to be opened within the firewall.

<b>CL-ODS SQL Pwd OSBiz V3</b>	<b>Secure ODS SQL connector for data source access</b>
Measures	Create own user account with read only permission within SQL data base server Choose strong password within database Server for this user account.
References	Administration Manual [1] Password policy for SQL server
Needed Access Rights	OSBiz: Expert of Administration Portal Database Server Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

#### 6.2.4.3 ODBC Connector

Open Directory Service provides optionally an ODBC connector, which allows access to relational or non-relational data sources which are running on Microsoft Windows operating systems.



Realization is done in a way that the OpenScape Business ODBC to ODBC Bridge SW is installed on the computer which operates the data source. Open Directory Service can access the ODBC Bridge by its embedded ODBC connector via a LAN (TCP/IP) connection.

**Risk:**

The LAN connection from OpenScape Business ODBC Bridge server to the ODBC Bridge client can be eavesdropped.

Attackers with full access to the ODBC Bridge on the external computer may get access to company directory data or in the worst case can corrupt / compromise the database.

**Measures:**

The communication between the ODBC connector of Open Directory Service and ODBC Bridge on the external computer has to be encrypted.

Access to the ODBC Bridge by Open Directory Service has to be protected by a strong password within the ODBC Bridge server part.

An own user account with strong password protection has to be created within the data source for access by the ODBC Bridge, if data source provides such protection mechanisms.

The port for accessing the ODBC Bridge server part has to be opened within the firewall.

<b>CL-ODS ODBC Pwd OSBiz V3</b>	<b>Secure ODBC connector and data source access</b>
Measures	Set encryption flag within the ODBC Bridge Choose strong password for login of Open Directory Service into ODBC Bridge Create own user account with read only permission for the ODBC Bridge within the data source or data base server Choose strong password within database Server for this user account.
References	Administration Manual [1] Password policy for database server
Needed Access Rights	OSBiz: Expert of Administration Portal Database Server Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 6.2.5 TAPI Service Provider

Many CTI and CRM applications in the marketplace use the Microsoft TAPI interface for connection to the telephone system. TAPI Service Providers, which are optimized for the system architecture and network topology of OpenScape Business, allow the connection of those applications to OpenScape Business.

Three TAPI Service Providers are available for OpenScape Business, which have in common, that they run on Microsoft Windows client PCs or servers and which are protected by native security mechanisms of Microsoft Windows OS. E.g. access control and user accounts.

### Risk:

TAPI Service Providers allow call control in general and programming of features e.g. call forwarding in particular. These mechanisms can be misused for toll fraud if unauthorized persons get access to the TAPI application. In addition, unauthorized access to the TAPI line may also disclose the individual communication of the user.

### Measures:

User rights for those devices, which are controlled by TAPI, have to be set in a way that only features, which are required by the user are enabled. Classes of Service (COS) and user flags have to be adapted to these needs within OpenScape Business

Connection and access to OpenScape Business have also to be protected. This is depending on the kind of connection and described within the following subsections.

### Note:

PC Server and PC Client access has to be protected by Microsoft Windows mechanisms. This is out of scope of this security checklist.

CL-TAPI Rights OSBiz V3	Restrict rights of a TAPI user
Measures	Restrict outbound calls by setting appropriate COS for day/night according to the need of the TAPI user.  Restrict feature execution by setting the user flags for feature programming by a TAPI user according to the needs of the TAPI user.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

### 6.2.5.1 OpenScape Business TAPI 170

OpenScape Business TAPI 170 is a "third-party" TAPI Service Provider that is installed on a Microsoft Server and is connected centrally via LAN to the OpenScape Business System.

TAPI 170 does not provide native clients, when using the so-called "Remote TAPI" function, it is not necessary to install the TAPI Service Provider on the client PCs. TAPI 170 administration is done within the "Telephony and Modem" section of the Windows Control Panel.

TAPI 170 users have to be licensed within OpenScape Business. TAPI 170 checks available licenses and allows access to TAPI functions only for licensed users.

TAPI 170 uses CSTA protocol for communication with OpenScape Business

Protocol	Purpose	Checklist Reference
CSTA	Communication with OpenScape Business CSP component for call control and device monitoring	Chapter 10.5.11

#### **Risk:**

TAPI 170 allows call control in general and programming of features e.g. calls forwarding in particular for **all licensed TAPI users**. These mechanisms can be misused for toll fraud if unauthorized persons get access to the TAPI application.

In addition, unauthorized access to the TAPI line may also disclose the individual communication of the user.

#### **Measures**

Beneath the Measures shown in chapter 6.2.5, measures for securing of the CSTA interface have to be applied. (see chapter 10.5.11)

### **6.2.5.2 OpenScape Business TAPI 120**

OpenScape Business TAPI 120 is a centrally connected "first -party" TAPI Service Provider.

TAPI 120 is installed on each Microsoft Windows PC client that is running a TAPI application and is connected via LAN to the OpenScape Business System.

TAPI 120 does not provide a native client. Administration is done within the "Telephony and Modem" section of the Windows control panel.

TAPI 120 users have to be licensed within OpenScape Business. TAPI 120 checks available licenses and allows access to TAPI functions only for licensed uses.

TAPI 120 uses either CSTA protocol or Web Services API (WSI) (V2 MB only) for communication with OpenScape Business

Protocol	Purpose	Checklist Reference
CSTA	Communication with OpenScape Business CMD component for call control and device monitoring	Chapter 10.5.11
WSI	Communication with OpenScape Business Web Services for call control and device monitoring	Chapter 10.5.13.4

#### **Risk:**

TAPI 120 allows call control in general and programming of features e.g. calls forwarding in particular. These mechanisms can be misused for toll fraud, if unauthorized persons get access to the TAPI application.

In addition, unauthorized access to the TAPI line may also disclose the individual communication of the user.

#### **Measures**

In case that the CSTA interface is used, access to the CSTA interface can be restricted to authorized call numbers by appropriate configuration of the CTI firewall within the CSTA Message Dispatcher (CMD) component.

<b>CL – TAPI CTI Firewall OSBiz V3</b>	<b>Fill in “Allowed List” within CTI Firewall of CMD</b>
Measure	Use CTI Firewall within CMD configuration to grant access for TAPI 120 users.
References	Administration Manual [1] OpenScape Business TAPI 120/170 Installation Guide
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

The CTI firewall of the CMD does not work if the Web Services API (WSI) is used (V2 MB only). Authorization is done in this case by the UC Smart user login credentials. Therefore, a strong individual UC user password has to be chosen for the TAPI 120 user.

<b>CL – TAPI WSI Pwd OSBiz V3</b>	<b>Choose strong UC Smart user password for WSI access. (V2 MB only)</b>
Measure	Set strong individual UC user password for the TAPI 120 users.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

### 6.2.5.3 CallBridge Collection

CallBridge Collection is a first-party TAPI Service Provider which is directly connected to system phones of OpenScape Business. It is installed on each Microsoft Windows client OS which is running the TAPI application, and which is connected to a system phone either via LAN or USB cable.

CallBridge Collection does not provide a native client. Administration is done within the “Telephony and Modem” section of the Windows control panel.

TAPI connections via the CallBridge Collection are not licensed in general.

CallBridge Collection uses proprietary Cornet TS protocol for communication with the system phone.

Protocol	Purpose	Checklist Reference
----------	---------	---------------------

Cornet TS	Communication with system phones of OpenScape Business	
-----------	--------------------------------------------------------	--

**Risk:**

CallBridge Collection allows call control in general and programming of features e.g. calls forwarding in particular. These mechanisms can be misused for toll fraud if unauthorized persons get access to the TAPI application.

In addition, unauthorized access to the TAPI line may also disclose the individual communication of the user.

**Measures:**

User rights for the user device which is controlled by TAPI have to be set in a way that only features which are required by the user are enabled. Classes of Service (COS) and user flags have to be adapted to these needs within OpenScape Business

In case of a LAN connection to the system phone a strong user password has to be set within the device configuration and within the CallBridge Collection (CallBridge IP).

CL – TAPI UserPwd OSBiz V3	Set strong user Password with system device and CallBridge IP
Measure	In case that CallBridge IP is used a strong user individual password has to be set within the system phone.
References	System phone operation manual
Needed Access Rights	Phone: Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 6.2.6 OpenScape Business Attendant

The OpenScape Business Attendant is an external client application, which allows call control, call monitoring and feature programming as well as the presentation of current device and user status. The feature set is completed by integration of several directories.

The SW is located on a Microsoft Windows client PC.

OpenScape Business Attendant administration is mainly done within the application itself. It provides different user accounts with user individual settings. The user accounts are bound to the Microsoft Windows client login. Administration of required interfaces and licenses has to be done within the OpenScape Business Administration Portal (WBM) and within the administration of the phone device.

OpenScape Business Attendant communicates via LAN interface to the associated phone device and to OpenScape Business using several protocols. Depending on the phone device the connection can also be done via USB interface.

Protocol	Purpose	Checklist Reference
Cornet TS	Proprietary protocol for communication with OpenScape Business system phones via LAN or USB for call control and device monitoring.	n/a

WSI	Communication with the Web Services API (WSI) in order to read write user presence status. HTTPS is the default protocol, which cannot be modified	Chapter 10.5.13.4
LDAP	Communication with LDAP capable directory server. Secure transmission via LDAPS is not supported	Chapter 10.5.7
BLF server protocol	Proprietary protocol for communication with optional BLF Server in order to get network wide user and device presence status.	n/a

#### **Risk:**

OpenScape Business Attendant client application allows call control in general and programming of user individual features. It uses "Associated Services" e.g. for programming call forwarding for other users. In addition, Business attendant can activate user status dependent call forwarding for other users.

These mechanisms can be misused for toll fraud, if unauthorized persons get access to the Business Attendant application. Unauthorized access may also disclose the user individual presence status and status dependent forwarding.

LDAP connection of the OpenScape Business Attendant is not encrypted. Eavesdropping of server login within the LAN and disclosure of directory data is possible.

#### **Measures:**

Access to OpenScape Business Attendant applications has to be protected. As the user accounts are bound to the MS Windows client login, a strong login password has to be assigned for every PC user incl. PC administrator.

In case of a LAN connection to the associated device a strong user password has to be chosen within the device configuration and within OpenScape Business Assistant.

HTTPS has to be used for the LAN connection to the WSI of OpenScape Business.

LDAP connection has to be secured if necessary, by external means within the LAN.

<b>CL –Business Attendant Pwd OSBiz V3</b>	<b>Set strong Windows client user password</b>
Measure	Strong individual passwords have to be chosen for every user account of the MS Windows Client according to password policy within chapter 12.1.
References	MS Windows OS operation manual
Needed Access Rights	MS Windows client administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL –Business Attendant Device Pwd OSBiz V3</b>	<b>Set strong user Password with system device configuration</b>
Measure	In case that OpenScape Business Attendant is connected via LAN a strong user individual password has to be set within the system phone.
References	System Phone operation manual
Needed Access Rights	Phone administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 6.2.7 Application Launcher

Application Launcher is a Microsoft Windows client application that is triggered by incoming calls. It retrieves caller data for caller identification from different sources within OpenScape Business, controls other applications, which are located at the client PC via batch files or URL requests and passed over the retrieved caller data. Application Launcher is able to initiate and control calls by means of the optional Desktop Dialer SW component.

Application Launcher is installed on a PC with Microsoft Windows client operating system.

Application Launcher communicates via LAN with TCP / IP using several interfaces and protocols of OpenScape Business. Communication with 3<sup>rd</sup> Party application is either done via client PC SW components or via HTTP requests.

Protocol	Purpose	Checklist Reference
WSI	Web Services Interface (WSI) of OpenScape Business for device monitoring and call control	Chapter 10.5.13.4
HTTP/HTTPS	Communication with: <ul style="list-style-type: none"> <li>- OpenScape Business Web Server</li> <li>- 3<sup>rd</sup> party Application (optional).</li> </ul>	Chapter 10.5.1
LDAP	Communication with Open Directory Server. (Secure transmission via LDAPS is not supported)	Chapter 10.5.7

### Risks

Application Launcher allows call control and for instance programming call forwarding. This mechanism can be misused for toll fraud, if unauthorized persons get access to the applications.

Unauthorized access to the Application Launcher may disclose data stored within the external application

### Measures

To protect Application Launcher, an individual user password has to be used for login. The Application Launcher uses either the UC smart or UC Suite user account data

depending on the UC solution. Password modification has to be done within the appropriate UC client of the user.

Enable only call control features which are required for the Application Launcher.

Ensure that the communication between Application Launcher client and OpenScape Business is encrypted by HTTPS.

In case that the directory service of OpenScape Business is connected via LDAP, strong password for LDAP access has to be chosen with the Open Directory Service. The LDAP connection to the Open Directory Service is not encrypted. This has to be done by external means in case this connection is done via Internet or if the customer security policy requires encryption.

<b>CL-AppLauncher Rights OSBiz V3</b>	<b>Restrict rights of an Application Launcher user</b>
Measures	Restrict outbound calls by setting appropriate COS for day/night according to the need of the Application Launcher user.  Restrict feature execution by setting the user flags for feature programming by an Application Launcher user according to the needs of the user.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

### 6.2.8 OpenScape Business 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 OpenScape Cordless DECT devices by default. This setting may be changed only temporarily e.g. for diagnostics.
- Only the officially released components out of the Gigaset Professional family shall be used. DECT-Headsets, DECT TAE plugs or other DECT devices can jeopardize confidentiality.

### 6.2.9 Wireless LAN (WLAN)

For OpenScape Business V3 the following WLAN components are released:

- optiPoint WL3 professional

Please make sure that a secure transmission like WPA2 is chosen (compare product related security checklist and / or administration manuals).

### 6.2.10 Deployment Service Integrated (DLI)

DLI can be used to centrally configure all IP system phones connected to the communication system and to equip them with the latest phone software. The embedded DLI uses the integrated FTP server on which the latest phone software is stored.



If the IP address of the DLI is known to the DHCP server, the DHCP server sends this data to the IP system telephone (HFA, SIP) as soon as the phone logs into the internal network. This enables the telephone to retrieve the current software from the FTP server of the communication system. The DLI is configured by default in the internal DHCP server.

#### SW update of System Device(HFA)@Home

The normal SW-Update procedure of the DLI for an internally connected device cannot be used for System Device (HFA)@Home as the DLI cannot determine the IP address of device which resides in a LAN environment using NAT in the Internet Router.

Therefore, the DLI SW-Update procedure uses an additional HTTPS connection via port 8804 (default setting) in combination with the DLI port 18443 (default setting) to determine SW version of the Device@Home and to perform the SW-Update.

The software update of a Device@Home by the DLI has to be configured in OpenScape Business. It is disabled per default and needs to be enabled explicitly.

Protocol	Purpose	Checklist Reference
FTP	SW update of locally connected devices	Chapter 10.5.2
HTTPS	SW update for System Device@Home	Chapter 10.5.1

## 6.2.11 Circuit

Circuit, Unify's cloud based collaboration solution, can be connected via a native SIP trunk to OpenScape Business. The connection allows Circuit to use OpenScape Business as a Gateway for voice calls and allows the Circuit client user to control his associated telephony device (CTI). In addition to the device control the CTI connection exchanges the device / client status between Circuit and Open Scape Business.

Incoming calls from central office (CO) lines or internal subscribers are signaled in parallel on the circuit client and on the OpenScape Business device. Calls can be answered either on the circuit client or the device.

Outgoing calls to external numbers via CO line or to internal OpenScape Business subscribers use the OpenScape Business extension number as CLIP information.

Active calls can be pulled / pushed seamlessly between the circuit clients and the OpenScape Business device

The CTI connection enhances the telephony functions of the Circuit client by typical CTI features like consultation, transfer, hold conference etc. In addition, the client / device status information is exchanged.

OpenScape Business offers admission control by the tenant specific "API-Key" that is provided by Circuit. Data encryption with TLS is enabled by default within OpenScape Business for the signaling protocols but not for the payload protocols.

Use of the OpenScape Business Telephony Connector for voice calls is license controlled by Circuit. The use of CTI features is controlled by OpenScape Business.

Within the default configuration of OpenScape Business the Circuit and the CTI connection is disabled.

Following IP protocols are used in order to offer the circuit services.

Protocol	Purpose	Checklist Reference
HTTPS	Web based tenant administration	Chapter 10.5.1

TCP / TLS	Secured Transport	Chapter 10.4.1; 10.4.3
SIP	Signaling	Chapter 10.5.8
RTP	Payload Transport	Chapter 10.5.9

### **Risk:**

The OpenScape Business Telephony Connector allows outgoing connections to any destination in the PSTN via OpenScape Business. The connection can be used for unauthorized dialing of call numbers with high charges. This can lead to considerable costs.

The Circuit CTI connection allows call control via the associated device in general and programming of features e.g. call forwarding in particular. These mechanisms can be misused for toll fraud.

In addition, unauthorized access to the Circuit client may also disclose the individual communication of the user.

### **Measures:**

Classes of Service (COS) and user flags for the associated virtual subscriber in OpenScape Business has to be set according to the needs of the user.

The user flags of the associated virtual subscriber have to be set according to the user needs within OpenScape Business.

### **Note:**

Access to the Circuit Client device has to be protected. This is depending on the kind of used device and out of scope of this security checklist.

<b>CL-Circuit Rights OSBiz V3</b>	<b>Restriction of right of a Circuit user in OpenScape Business</b>
Measures	<p>Restriction of outbound calls is in place. An appropriate COS for day/night of the virtual user in OpenScape Business that is associated to the Circuit user according to the needs of the Circuit user is set.</p> <p>Restriction of feature execution is in place. User flags for the virtual user that is associated to the Circuit user are set accordingly.</p>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 6.2.12 Unify Office

Unify Office is the successor to Circuit as a cloud-based collaboration solution. It is connected to OpenScape Business via SIP trunk, like an ITSP. Encryption of the connection is supported by OpenScape Business.

The same risks and measures exist for the Unify Office connection as for the ITSP connection via SIP trunk, see chapter "9.2.4 IP Transmission with VoIP Service Provider (ITSP)".

## 6.2.13 Unify Phone

Unify Phone is available in two different flavors:

- Unify Phone for OpenScape  
Unify Phone is used as a stand-alone OpenScape communication system telephony client.
- Unify Phone for Unify Video  
Unify Phone is used in conjunction with Unify Video allowing Unify Video users to communicate with others via phone calls.

In addition to its own softphone for mobile devices and desktop PCs, Unify Phone also offers connection to OpenScape Business systems.

OpenScape Business provides the local telephony functions as well as access to the public telephone network via the connection to Unify Phone which is connected to OpenScape Business via SIP trunk. SIP signaling is encrypted by TLS. The RTP protocol used for payload transmission is not encrypted. Access to the Unify Phone administration is done via HTTPS. OpenScape Business offers admission control by the tenant specific "API-Key" that is provided by Unify Phone. Data encryption with TLS is enabled by default within OpenScape Business for the signaling protocols but not for the payload protocols.

Incoming calls from central office (CO) lines or internal subscribers can be signaled in parallel on the Unify Phone client and on the OpenScape Business device. Calls can be answered either on the Unify Phone client or the device.

Outgoing calls to external numbers via CO line or to internal OpenScape Business subscribers use the OpenScape Business extension number as CLIP information.

Active calls can be pulled / pushed seamlessly between the Unify Phone clients and the OpenScape Business device

The CTI connection enhances the telephony functions of the Unify Phone client by typical CTI features like consultation, transfer, hold conference etc. In addition, the client / device status information is exchanged.

Use of the OpenScape Business Telephony Connector for voice calls is license controlled. The use of CTI features is controlled by OpenScape Business.

Within the default configuration of OpenScape Business the Unify Phone connection is disabled.

Following IP protocols are used in order to offer the Unify Phone services.

Protocol	Purpose	Checklist Reference
HTTPS	Web based tenant administration	Chapter 10.5.1
TCP / TLS	Secured Transport	Chapter 10.4.1; 10.4.3
SIPS	Signaling	Chapter 10.5.8

RTP	Payload Transport	Chapter 10.5.9
-----	-------------------	----------------

#### **Risk:**

The OpenScape Business Telephony Connector allows outgoing connections to any destination in the PSTN via OpenScape Business. The connection can be used for unauthorized dialing of call numbers with high charges. This can lead to considerable costs.

The Unify Phone CTI connection allows call control via the associated device in general and programming of features e.g. call forwarding in particular. These mechanisms can be misused for toll fraud.

In addition, unauthorized access to the Unify Phone client may also disclose the individual communication of the user.

#### **Measures:**

Classes of Service (COS) and user flags for the associated virtual subscriber in OpenScape Business has to be set according to the needs of the user.

#### **Note:**

Access to the Unify Phone Client device has to be protected. This is depending on the kind of used device and out of scope of this security checklist.

<b>CL- Unify Phone Rights OSBiz V3</b>	<b>Restriction of right of an Unify Phone user in OpenScape Business</b>
Measures	<p>Restriction of outbound calls is in place. An appropriate COS for day/night of the virtual user in OpenScape Business that is associated to the Unify Phone user according to the needs of the Unify Phone user is set.</p> <p>Restriction of feature execution is in place. User flags for the virtual user that is associated to the Unify Phone user are set accordingly.</p>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## **6.2.14 Microsoft Teams**

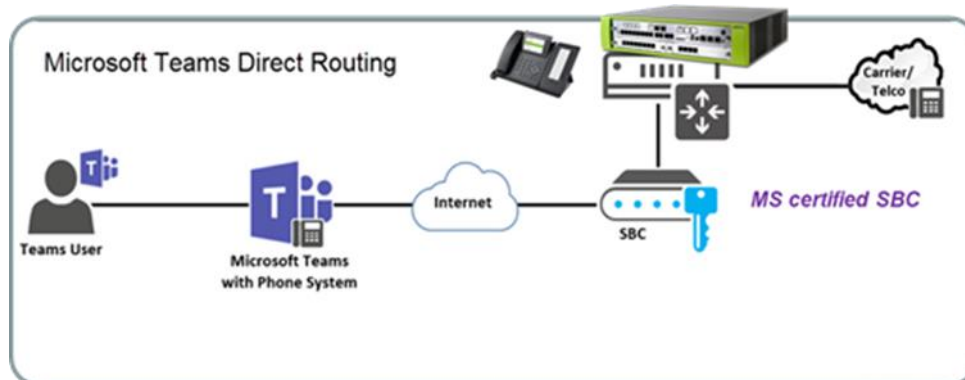
OpenScape Business supports different connection variants to Microsoft Teams:

- Direct Routing
- myPortal for Teams plug-in

The different types of connection also require a different consideration of the potential risk.

#### 6.2.14.1 Microsoft Teams via Direct Routing

With Direct Routing, the OpenScape Business is connected to the telephony client integrated in MS Teams via a Microsoft-certified Session Border Controller (SBC).



The connection from OpenScape Business to the Session Border Controller is done via a native SIP trunk connection. The configured connection to the SCB is not encrypted. No login credentials are used in this case within the SBC for the trunk line to OpenScape Business.

This type of connection allows phone calls from public network to MS-Teams clients and vice versa and also calls between OpenScape Business users and MS-Teams clients.

Following IP protocols are used in order to connect OpenScape Business to MS Teams via a SBC.

Protocol	Purpose	Checklist Reference
SIP	Signaling	Chapter 10.5.8
RTP	Payload Transport	Chapter 10.5.9

#### Risk:

A potential attacker can eavesdrop the connection between OpenScape Business and SBC easily.

In a scenario that integrates MS Teams via a 3<sup>rd</sup>-pty SBC particular care needs to be taken to avoid misconfiguration that facilitates toll fraud. The reason is that there is no authentication of the MS Teams subscriber when connecting to the SBC. The security mainly relies on a trust relationship that is established between MS Teams and the SBC during the TLS connection.

As Microsoft teams does not check any class of service for the telephony clients, toll fraud is possible by dialing premium service numbers from MS Teams Clients using OpenScape Business as a gateway to the public telephone network.

#### Measures:

SBC must be installed in the customer LAN and note security hint for 3<sup>rd</sup>-pty SBC in the specific How To:

[https://wiki.unify.com/images/4/4f/How\\_To\\_Configure\\_OSBiz\\_MS\\_Teams\\_Interworking.pdf](https://wiki.unify.com/images/4/4f/How_To_Configure_OSBiz_MS_Teams_Interworking.pdf).

The trunk connection between SBC and OpenScape Business within the customer LAN should be encrypted by external means if sensitive data is transferred.

The customer must be informed of the potential risk if an unencrypted connection is used.

If the SBC cannot be installed in the customer LAN a VPN between OpenScape Business and SBC must be used.

To prevent calls to premium services or toll fraud, the numbers that are not allowed to be dialed from the MS Teams client via the SBC trunk line must be entered the Denied List 1 within the OpenScape Business configuration.

As an additional measure, the MS-Teams Client can be configured as a "Trusted mobile User" within OpenScape Business. In this case, the OpenScape Business Class of Service (COS) lists can be applied to the associated user within OpenScape Business.

<b>CL-MS Teams Direct Routing OSBiz V3</b>	<b>Prevent Eavesdropping</b>
Measures	<p>Install the Session Border Controller within the customer LAN</p> <p>Use encryption by external means to secure the LAN Connection between OpenScape Business and the SBC.</p> <p>Inform the customer about the risk of eavesdropping if encryption is not available.</p>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Advanced or Expert of Administration Portal
Executed	<p>SBC installed within LAN:    Yes: <input type="checkbox"/>                  No: <input type="checkbox"/></p> <p>Encryption in place:                  Yes: <input type="checkbox"/>                  No: <input type="checkbox"/></p> <p>Customer informed:                  Yes: <input type="checkbox"/>                  No: <input type="checkbox"/> about risk of eavesdropping</p>
Customer Comments and Reasons	

<b>CL-MS Teams Direct Routing OSBiz V3</b>	<b>Restrict Calls to Public Network and Feature execution for MS Teams Clients</b>
Measures	<p>Create "Denied List 1" and enter the numbers that are not allowed to be dialed into the public network</p> <p>If "Trusted Mobile User" is configured for MS-Teams connection set:</p> <ul style="list-style-type: none"> <li>- "Class of Service"</li> <li>- Station Flags</li> </ul> <p>in order to prevent misuse of OpenScape Business features and toll fraud.</p>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Advanced or Expert of Administration Portal

Executed	Denied list:                      Yes: <input type="checkbox"/> No: <input type="checkbox"/>  Class of Service:              Yes: <input type="checkbox"/> No: <input type="checkbox"/>  Stations Flags:                                      Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

#### 6.2.14.2 Microsoft Teams plug-in

The OpenScape Business myPortal for Teams Plug-In is an extension of the Microsoft Teams client. It enables the user to execute OpenScape Business telephony functions directly from the MS Teams client. It interacts exclusively with OpenScape Business. Therefore, no Microsoft Enterprise or Phone System license is required to use the Plug-In features.

The connection from the MS-Teams client to OpenScape Business is done via LAN using a WebSocket connection to the Common API secured by HTTPS.

The user has to enter his UC login credentials for the first login. An automatically generated token secures all following logins using the same Web session.

Following IP protocols are used in order to connect OpenScape Business to the MS Teams Plugin.

Protocol	Purpose	Checklist Reference
HTTPS WebSocket	Bidirectional Communication between MS Teams Client and OpenScape Business Common API	Chapter 10.5.1

#### Risk:

Unauthorized access to the MS-Teams Plugin can be used for unauthorized phone call or access to call journal and directory data of the user.

#### Measures:

To protect MS-Teams Plugin, an individual user password has to be used for login. The MS-Teams Plugin uses either the UC smart or UC Suite user account data depending on the UC solution. Password modification has to be done within the appropriate UC client of the user.

Enable only call control features within the OpenScape Business system which are required for the MS-Teams Plugin.

<b>CL-UC MS Teams Plug In ClientPwd OSBiz V3</b>	<b>Set user password for the Plug In</b> <b>Protect access to the client PC in general</b>
Measures	Customer specific PW policy is defined as depicted in the appendix.  Default accounts are depicted in the appendix.  The login password has to be set to an individual value, by every user.  Unattended PCs must be locked.

	Use customer individual certificate for authentication and encryption.
References	Administration Manual [1] Valid PW policies see chapter 12.1 UC Account see chapter 12.2
Needed Access Rights	OSBiz: Expert of Administration Portal User
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 6.2.15 XML Data Import

OpenScape Business provides import / export service for an appropriate XML configuration data file. Import / export is done either manually via the OpenScape Business Assistant (WBM) or automated by an appropriate application via a WebSocket interface.

Within the default settings the WebSocket interface is enabled after first system setup and accessible via port 443 (default).

The manual file import can only be done via the OpenScape Business Assistant. It requires successful login as expert, advanced, enhanced or basic user.

The automatic file import can be done via TCP/IP connection to the WebSocket interface using HTTPS. A user authentication is required in the same way as for manual access to OpenScape Business Assistant.

The imported XML data are checked validated by OpenScape Business before executed in order to avoid import of corrupted data or malicious code.

Following IP protocols are used by the WebSocket Interface.

Protocol	Purpose	Checklist Reference
HTTPS	Communication with: <ul style="list-style-type: none"> <li>• OpenScape Business Web Server</li> <li>• OpenScape Business WebSocket interface</li> </ul> 3 <sup>rd</sup> party Application (optional).	Chapter 10.5.1

### Risk:

Access to the WebSocket Interface cannot be enabled / disabled by a service task as it is also used by the OpenScape Business Assistant (WBM). SW vulnerabilities of the web server within OpenScape Business can be exploited by attackers if web server / WebSocket interface is directly accessible from the Internet.

### Measures:

Access to the customer LAN and to OpenScape Business within the LAN has to be controlled either by setting appropriate port forwarding within the Internet router or by use of a firewall.



Do not open Port 443 for direct access from the Internet use port forwarding within the Internet router or a firewall.

<b>CL-Remote XML file import via Internet OSBiz V3</b>	<b>Secure WebSocket Interface Administration Portal</b>
Measures	Do not open port 443 for direct access from Internet. Configure port forwarding within the internet router.  Use customer individual certificate for authentication and encryption
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> not applicable <input type="checkbox"/>
Customer Comments and Reasons	

# 7 3<sup>rd</sup> Party Components

The following 3<sup>rd</sup> party SW components are used within OpenScape Business V3.

- Apache Web Server
- Tomcat
- PostgreSQL
- Open LDAP Server
- Open SSL
- SAMBA File Service

General responsibility for the hardening of the 3<sup>rd</sup> party components depends on the kind of SW deployment.

- **Deployment as SW Appliance (OpenScape Business X and UC Booster Card)**

Unify is responsible for hardening of the 3<sup>rd</sup> party component in case of OpenScape Business Model X and UC Booster Card.

Security relevant modifications of the 3<sup>rd</sup> party component configuration is done by Unify within the SW support.

SW updates of 3<sup>rd</sup> party components due to security reasons are done by Unify within the SW support.

- **Deployment as SW Application (OpenScape Business S or UC Booster Server)**

Customer and/or the company which delivered the Linux Operating system, including the 3<sup>rd</sup> party components, are responsible for hardening of the 3<sup>rd</sup> party components in case of OpenScape Business S and UC Booster Server.

Security relevant modifications of the 3<sup>rd</sup> party component configuration have to be done by the system administrator.

SW updates of 3<sup>rd</sup> party components due to security reasons have to be done by the system administrator

See also chapter 3.3 for further information about OS hardening and OpenScape Business SW hardening.

An administrator of an OpenScape Business X system cannot modify the general configuration of these 3<sup>rd</sup> party components. An administrator of OpenScape Business S system must not modify the configuration.

Even if the system is pre-hardened the measures which are described in the following subchapters have to be considered for specific 3<sup>rd</sup> party applications in order to minimize security risks.

## 7.1 PostgreSQL

OpenScape Business stores all data such as system configuration, call data records or user account data etc. into a PostgreSQL database management system. For database access several accounts with different rights are defined.

### **Risk:**

An attacker, who gets access to the LAN interface of OpenScape Business can use the password for the PostgreSQL server administrator account to read, modify or delete the configuration data and user accounts etc.

### **Measures:**

The PostgreSQL administrator account password is machine generated and unique for each OpenScape Business system. The passwords are disclosed to the administrator in general. In case of a system upgrade the existing password is kept. It has to be checked if the "default" password is still active. If so, the password has to be changed manually to a machine generated PW via the Administration Portal.

For diagnostic purpose and for compatibility in networks with old SW versions the PostgreSQL administrator account password can be changed back to the "old" factory default.

The status of the PostgreSQL password is shown at the landing page of the Administration Portal. In case of a warning the password has to be changed to a machine generated PW.

An access to the PostgreSQL LAN port from connections via Internet may not be granted. The appropriate port needs to be blocked within the Internet router or firewall.

<b>CL-PostgresSQL PW OSBiz V3</b>	<b>Secure PostgreSQL by password change</b>
Measures	PostgresSQL root password is set to machine generated. Check password status at the Administration Portal homepage. If the "old" password is used change the password to a machine generated one.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-PostgresSQL Port OSBiz V3</b>	<b>Disable PostgreSQL port</b>
Measures	Disable access to the internal PostgreSQL LAN port within the Internet router.
References	
Needed Access Rights	LAN administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 7.2 SAMBA Share-Mode (File Service)

A SAMBA share could provide e.g. help files, first distribution SW of clients, and system backups.

The service can be switched off if customer security policy requires that. The functions mentioned above are not available in this case. If not possible to switch off SAMBA Share-Mode:

OpenScape Business V3 does not use SAMBA shares therefore SAMBA services have to be deactivated within the OS.

**Note:**

SAMBA share mode and SAMBA protocol (SMB-protocol) are different services and have to be handled separately from security point of view. For information about the SAMBA protocol see chapter 10.5.12.

<b>CL-SAMBA1</b> <b>OSBiz S V3</b> <b>UC Booster Server</b>	<b>Switch off SAMBA services</b>
Measure	Switch off SAMBA services within the SLES operating system
References	SLES administration manual
Needed Access Rights	Administrator
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	N/A

# 8 Administration

The administration of the system has to be protected from unauthorized access.

The system offers protection mechanisms from unauthorized access. This includes the following aspects:

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

Due to the history of the system, different administration tools with different mechanisms for protection against unauthorized access are implemented.

The specific concepts of these administration tools are addressed in the following subsequent chapter.

OpenScape Business provides following administration tools, which can be used either in combination or alternatively:

- **OpenScape Business Administration Portal (WBM)**  
an embedded, web-based application within OpenScape Business
- **OpenScape Business Manager E**  
a Microsoft Windows based application installed and operated on an external computer.
- **Online User**  
As part of Manager E
- **Assistant T**  
Administration of specific OpenScape Business features via system phone user interface.

## 8.1 System Access Protection – Authorization

### 8.1.1 User Authorization

OpenScape Business provides a user role-based administration concept, where access privileges are assigned to user roles. The roles are predefined in the administration tool and are described in detail in the appropriate administration manual. Depending on the used administration tool, different user roles are provided.

#### 8.1.1.1 Administration Portal (WBM)

The Administration Portal supports 4 predefined user roles. Customer specific user roles are not supported. Details are described within Administration Manual [1]

#### 8.1.1.2 Manager E

The Manager E tool supports 6 predefined user roles. Customer specific user roles are not supported. Details are described within the Manager E Administration documentation [2]

#### 8.1.1.3 Assistant T

The Assistant T supports in general the same user roles as Manager E. Details are described within the Manager E Administration documentation [2] and within the HiPath 3000 V9 Service Manual.

## 8.2 System Access Protection – Authentication

### 8.2.1 Password based Authentication

OpenScape Business Administration tools support password / PIN based authentication. Within factory delivery default passwords are available for first system access.

OpenScape Business request a password change according to the password policies described within chapter 12.1.

Password policies are specific for Administration Portal, for Manager E and Assistant T administration tool.

Fixed passwords are a serious security risk. In any case, individual and safe passwords must be used for all users. Every user must only get those rights or roles, which are necessary for her / him.

<b>CL Admin PWD Concept OSBiz V3</b>	<b>Overall customer specific password concept</b>
Measures	Rules for customer specific password handling are defined see 12.1
References	Administration Manual [1] Manager E Administration Manual [2]
Needed Access Rights	OSBiz: Expert of Administration Portal Manager E: Service
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

A new password has to be entered after the first start according to Password Policy (see chapter 12.1).

**Note:**

Default passwords of Manager E and Administration Portal have to be changed by using the appropriate administration tool. Password settings of both tools are independent from each other. The Administration Portal cannot change the Manager E passwords and vice versa.

<b>CL-Admin PWD Default OSBiz V3</b>	<b>Change ALL default PW into customer individual passwords</b>
Measures	Implement individual passwords for Predefined roles within Administration Portal Predefined roles within Manager E Use both administration tools for modification
References	Administration Manual [1] Manager E Administration Manual [2]
Needed Access Rights	OSBiz: Expert of Administration Portal Manager E: Service

Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

### 8.2.1.1 Administration Portal (WBM)

OpenScape Business Administration provides only one user within the Expert account as factory default. When accessing the Administration Portal for the first time a change of the default password is enforced. Wrong entry of login credentials for three times disables the login dialog for a specific time. Additional users and administration roles can be defined afterwards according to the requirements. Strong individual passwords have to be assigned to each user according to the password policies in chapter 12.1.1.

<b>CL-Admin WBM Account PWD OSBiz V3</b>	<b>Assign appropriate accounts to users and choose strong individual passwords.</b>
Measures	<p>Implement necessary user accounts for the roles</p> <ul style="list-style-type: none"> <li>• Basic</li> <li>• Enhanced</li> <li>• Advanced</li> <li>• Expert</li> </ul> <p>with strong individual passwords List all needed user accounts in addendum</p>
References	<p>Administration Manual [1] Password policy see chapter 12.1.1</p>
Needed Access Rights	OSBiz: Advanced or Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

### 8.2.1.2 Manager E

Due to compatibility reasons with old HiPath systems Manager E provides a fixed and a variable password concept. In combination with OpenScape Business only the variable password concept has to be used. The fixed password concept must not be used. For details see [2].

Password has to be numerical, if administration via telephone is also needed.

After first access of Manager E tool to OpenScape Business a new individual password for the Manager E administration access has to be entered. Please observe the password recommendations with chapter 12.1 for all Manager E users.

Manager E login credentials for service and development roles are disabled in general and have to be configured within the Administration Portal (WBM) prior to first system access via Manager E.

<b>CL-Admin Manager E Account PWD OSBiz V3</b>	<b>Variable Password concept, assign appropriate accounts to users and choose strong individual passwords.</b>
Measures	Choose variable password concept Implement necessary user accounts for the required roles and assign strong individual passwords. List all needed user accounts in addendum
Reference	Manager E Administration Manual [2] Password policy see chapter 12.1.1
Needed Access Rights	Manager E: Service
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

### 8.2.1.3 Assistant T

Administration by phone is always possible from the first two system phones. The same passwords as for Manager E are applicable. Use only variable password concept. The fixed password concept must not be used.

Assistant T login credentials for service and development roles are disabled in general and have to be configured within the Administration Portal (WBM) prior to first system access via Assistant T.

<b>CL-Admin Assistant T Account PWD OSBiz V3</b>	<b>Variable Password concept, assign appropriate accounts to users and choose strong individual passwords.</b>
Measures	Choose variable password concept Implement necessary user accounts for the required roles and assign strong individual passwords. List all needed user accounts in addendum
Reference	Manager E Administration Manual [2] HiPath 3000 V9 Service manual Password policy see chapter 12.1.1
Needed Access Rights	Assistant T: Service
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 8.2.2 Certificate Based Authentication

### 8.2.2.1 Administration Portal (WBM)

OpenScape Business Administration Portal is a service running on the Web server within OpenScape Business, which can be accessed by an Internet Browser.



The access to the Administration Portal is always secured via HTTPS. A self-signed server certificate, which is delivered by default or a customer specific certificate, which relies on a root certificate authority or by a customer individual certificate can be used for encryption and authentication (see also chapter 12.3).

<b>CL-Admin WBM Certificate</b> <b>OSBiz V3</b>	<b>Use customer specific certificate</b>
Measures	Import customer certificates for every protocol and mechanism where necessary, that is issued for the OpenScape Business V3 (server name or IP address) and activate it (for the administration access).
References	OpenScape Business Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

#### 8.2.2.2 Manager E

Manager E authentication cannot be secured by a certificate

#### 8.2.2.3 Assistant T

Assistant T authentication cannot be secured by a certificate

### 8.2.3 System Administration Access Protection – Miscellaneous

OpenScape Business system can be shut down from a phone device by entering a feature code followed by a PIN. Unauthorized / Unwanted shutdown of the system interrupts inbound / outbound communication.

<b>CL-Admin PIN for System Shutdown</b> <b>OSBiz V3</b>	Change default PIN for system shutdown from device
Measures	Change default PIN to a strong PIN for system shutdown from device
Reference	Administration Manual [1] Manager E Administration Manual [2] PIN policy see chapter 12.1.1
Needed Access Rights	OSBiz: Expert of Administration Portal Manager E: Service
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

It has to be ensured that the first two system phones are assigned to trusted users, who know about the extended functionality of these phones and that they are not accessible from visitor etc.

<b>CL-Admin Assistant T Devices OSBiz V3</b>	<b>Protect physical access to first two system phones</b>
Measures	Assign first two system phones to trusted used Do not deploy those phones in places with visitor access
Reference	n/a
Needed Access Rights	n/a
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 8.3 Remote Administration

Remote Administration of OpenScape Business is possible by:

- Administration Portal of OpenScape Business (access from Internet Browser)
- Manager E incl. Online User tool

via LAN (Internet) or ISDN connections.

Regardless of the kind of remote access and used tool it must always be ensured, that:

- Remote access is only enabled for the maintenance timeslot and is disabled for the rest of time.
- Authentication and authorization of the remote user / machine is done.
- Encryption of the data transmission is done wherever possible, either by internal or external means.

### **Risk:**

Depending on the used remote administration tool and kind of access the remote connection can be eavesdropped and login credentials for OpenScape Business administration access can be spied out.

High risks exist in case of a direct, unencrypted system access via ISDN / Internet connection.

### **Measures:**

A direct unprotected remote access to OpenScape Business via WAN (Internet / ISDN) must not be used.

It is highly recommended to use the Remote Service Platform (Rsp.servicelink) of Unify for remote access to OpenScape Business systems. The Remote Service Platform of Unify ensures correct authentication of the remote user and secure data transmission between the customer system and the remote workstation / PC.

### **8.3.1 Remote access using Rsp.servicelink Platform**

The Rsp.servicelink platform connects Unify systems via secured connections to the Unify Remote Service Infrastructure. This platform can be used by authorized sales and service partners. Rsp.servicelink is the most secure way for remote administration and should be used wherever possible. In addition, Rsp.servicelink can be activated by the customer for every single service task e.g. via phone.

<b>CL-Remote Admin Platform OSBiz V3</b>	<b>Configure Rsp.servicelink as Remote Service Platform</b>
Measures	Activate remote access via Rsp.servicelink Define strong PIN for activation / deactivation by phone
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> not applicable <input type="checkbox"/>
Customer Comments and Reasons	

## 8.3.2 Secure Direct Remote Access over Internet (IP) connection

### Risk:

Direct unprotected access from Internet must not be used, as the connection can be eavesdropped. If passwords can be spied out there is a high risk from Internet attacks.

### 8.3.2.1 Remote access to the Administration Portal with Internet Browser

Remote Access to the Administration Portal of OpenScape Business with an Internet Browser is protected by secured transmission using HTTPS. For higher security it is recommended to use a customer individual certificate instead of the OpenScape Business default certificate (see chapter 12.3).

### Risk:

Remote Access to the Administration Portal (WBM) cannot be enabled / disabled by a service task. SW vulnerabilities of the web server within OpenScape Business can be exploited by attackers if web server is directly accessible from the Internet.

### Measures:

Access to the customer LAN and to OpenScape Business within the LAN has to be controlled either by setting appropriate port forwarding within the Internet router or by use of a firewall.

Do not open Port 443 for direct access from the Internet use port forwarding within the Internet router or a firewall.

<b>CL-Remote Admin WBM via Internet OSBiz V3</b>	<b>Secure Administration Portal</b>
Measures	Do not open port 443 for direct access from Internet. Configure port forwarding within the internet router.  Use customer individual certificate for authentication and encryption
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal

Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> not applicable <input type="checkbox"/>
Customer Comments and Reasons	

### 8.3.2.2 Remote access to the system using Manager E LAN access

Remote Access using the Manager E tool over Internet establishes a direct TCP/IP connection to the administration port of OpenScape Business. This connection is not encrypted.

#### Risk:

The direct connection of Manager E via Internet / LAN can be eavesdropped easily. If passwords and login credentials can be spied out there is a high risk from Internet attacks.

Once established, the remote access to the Manager E administration port of OpenScape Business cannot be deactivated by the customer.

#### Measures:

It is recommended to use VPN for remote administration using Manager E tool via Internet. The VPN tunnel can be implemented either via OpenScape Business X1/X3/X5/X8 or via an external VPN router.

Application firewall within OpenScape Business can be used to grant access for defined IP addresses or to block the Manager E port within OpenScape Business in general.

<b>CL-Remote Admin Manager E via Internet OSBiz V3</b>	<b>Secure Manager E port and data transmission</b>
Measures	Use VPN for secure data transmission between Manager E and OpenScape Business.  Use Application firewall to restrict access to specific IP addresses or to block Manager E port.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> not applicable <input type="checkbox"/>
Customer Comments and Reasons	

### 8.3.3 Secure Direct Remote Access over ISDN BRI /PRI

Remote Access over ISDN using either X.75 or Point to Point (PPP) protocol is an easy target for attacks from the public networks.

The remote access port via ISDN is disabled within factory delivery of OpenScape Business. It has to be configured and enabled by the system administrator. Remote

Access via ISDN must not be enabled permanently. It has to be enabled by customer only temporarily upon request.

Following measures have to be considered in general to secure the remote access via ISDN.

<b>CL-Remote Admin via ISDN OSBiz V3</b>	<b>Secure direct Remote Access over ISDN</b>
Measures	Use of call back procedure for authentication of the caller / connection (strongly recommended)  Configure 5-digit access code for the remote ISDN connection within OpenScape Business  Instruct Customer about the handling of enabling / disabling of the remote access
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> not applicable <input type="checkbox"/>
Customer Comments / Reasons	

### **8.3.3.1 Remote Access over ISDN using PPP**

An ISDN PPP connection is used between a remote computer and OpenScape Business for:

- Access to the Administration Portal (WBM)

The PPP connection is not encrypted in general. The login credentials for setting up the transmission channel are encrypted if using PAP/CHAP for authentication.

Within OpenScape Business a PPP connection is configured automatically ("remote ISDN Peer" and the "RAS user") at the moment when the system administrator enables the Remote Access via ISDN. Within this automatic configured PPP connection PAP/CHAP with default login credentials for authentication are used.

An unknown password is set for the user authentication of the PSTN Peer (remote ISDN) in case that "Remote Access via ISDN" is enabled the first time.

After a system upgrade system behavior has to be differentiated between:

1. Systems with enabled PSTN peer with default password
2. Systems with enabled PSTN peer and customized password

In the first case the default password is replaced by a new unknown password and system administrator has to overwrite the password. In the second case the customer individual password stays untouched. No further action is required in this case. If a PPP connection and a RAS user is established within the OpenScape Business system a remote computer can have full access to the LAN segment in which OpenScape Business is located.

#### **Risk:**

In general, there is a high risk as not only the OpenScape Business and its services but also all other computers within the same LAN segment, in which OpenScape Business is located, can be accessed via the PPP connection.

Data transmission of the PPP connection is not encrypted by default and can be eavesdropped. Transmitted data can be spied out. In case of accessing the Administration Portal (WBM) the risk of eavesdropping is low as the data between remote computer and OpenScape Business are transmitted via HTTPS. In case of other server / services within the LAN segment it depends on the used protocols.

#### Measures:

It has to ensure by external means (like router, firewall, switches, VLAN etc.), that a remote connection via RAS user cannot access other components within the customer LAN. The customer network has to be designed in a way that OpenScape Business and its clients / devices are logically separated from other security critical LAN components.

Default user and password for PAP/CHAP within the "remote ISDN Peer" have to be changed. A strong password must be used according to the password policy within chapter 12.1. From V2R2 on well-known passwords of previous versions or trivial password are not accepted as new password.

#### Note:

Remote Access via ISDN using PPP is enabled / disabled within the Administration Portal (WBM) under the Tab "Remote Access". This setting does not affect the Manager E remote access via digital modem to the Manager E port of the system (ISDN with X.75 protocol).

<b>CL-Remote Access via ISDN and PPP OSBiz V3</b>	<b>Secure PPP connection and customer LAN</b>
Measures	<p>OpenScape Business and its devices have to be decoupled logically from other components within customer LAN.</p> <p>Check that PPP with PAP/CHAP is activated for the "remote ISDN Peer" connection.</p> <p>Change the username and especially the password to a strong individual password according to chapter 12.1</p>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> not applicable <input type="checkbox"/>
Customer Comments and Reasons	

### 8.3.3.2 Remote Access over ISDN using X.75 protocol

The Manager E tool with an underlying ISDN CAPI can establish a direct ISDN connection with X.75 protocol to OpenScape Business. In this case the Digital Modem subscriber number is used for dial in into OpenScape Business.

Remote Access via ISDN using Manager E is disabled within factory delivery of OpenScape Business. It has to be enabled by system Administrator via Manager E or using one of the first two system phones with Assistant T.

Manager E login credentials for service and development role are disabled in general and have to be configured within the Administration Portal (WBM) prior to first system access.

#### Risk:

Remote Access via ISDN using X.75 is enabled from the moment on when the default password has been changed. It cannot be disabled by service task at the system phone.

As default a dial in number is used and system does not prevent the re-entry of the default password a risk exists that unauthorized persons can access the system remotely using the defaults.

**Measures:**

The callback mechanism to define numbers has to be configured for remote ISDN connections. Within initial system configuration the variable password has to be enabled. A strong individual password, according to chapter 12.1, has to be chosen for remote access.

**Note:**

Remote Access via ISDN using Manager E is enabled via Manager E or Assistant T. This setting does not affect access of Administration Portal via ISDN PPP connection

<b>CL-Remote Access via ISDN and X.75 OSBiz V3</b>	<b>Secure remote access via X.75 to Manager E port</b>
Measures	<p>Enable and configure callback for remote access.</p> <p>Change the default username and especially the password to a strong individual password according to chapter 12.1.</p> <p>For Manager E access is blocked until password for Manager E service and development role are changed via Administrator Portal (WBM)</p>
References	<p>Administration Manual [1]</p> <p>Manager E Administrator documentation [2]</p>
Needed Access Rights	<p>OSBiz: Expert of Administration Portal</p> <p>Manager E: Service</p>
Executed	<p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/>      not applicable <input type="checkbox"/></p>
Customer Comments and Reasons	

## 8.4 Secure Phone Administration

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

- OpenStage T (TDM)
- OpenStage (SIP /HFA)
- OpenScape Client Personal Edition (IP soft client)
- OpenScape Deskphone IP (SIP/HFA)
- OpenScape Deskphone CP (SIP/HFA)
- OpenScape Deskphone CP (TDM)

Please observe the product-related security checklists and / or administration manuals. For OpenStage HFA devices, compare checklist [9] [10]. 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.

<b>CL-PhoneAdmin PWD System Phone OSBiz V3</b>	<b>Administration access protected by strong password (PIN)</b>
Measures	Change password at phone or via phone WBM
References	Phone Administration Guides
Needed Access Rights	Phone: admin
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	System-specific PIN <input type="checkbox"/> device-specific PIN <input type="checkbox"/>

**Note for IP Phones:**

The web-based HPT tool allows the display and operation of 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.



# 9 Protection of LAN based Communications

## 9.1 General Protection Measures

The LAN interfaces of the OpenScape Business have to be protected in general against unauthorized access from the internal LAN and from the Internet. The LAN segment in which OpenScape Business is operated has to be separated from the rest of the LAN by using a LAN Switch with appropriate forwarding for the OpenScape Business Clients and Devices.

<b>CL-LAN Switch LAN infrastructure</b>	<b>Secure LAN interface access in general</b>
Measures	Use an LAN switch with appropriate forwarding to restrict access to the LAN Interfaces of the system.
References	
Needed Access Rights	
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

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.

<b>CL-VLAN LAN infrastructure</b>	<b>Decoupling of voice and data network</b>
Measures	Use separate VLAN for voice communication (optional)
References	
Needed Access Rights	
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

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.

<b>CL-TLS LAN infrastructure</b>	<b>Secure specific LAN connection by encryption</b>
Measures	Use external encryption measures (e.g. TLS) to secure sensitive protocols and data within the LAN infrastructure in case no internal means are available.
References	
Needed Access Rights	
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

Information about the LAN communication of OpenScape Business embedded services and related clients are depicted in chapter 5.

Information about the specific protocols and interfaces of OpenScape Business are described in chapter 10.

## 9.2 Secure VoIP Transmission

### 9.2.1 General Signaling and Payload Encryption

For confidentiality and integrity of VoIP communication, the activation of signaling and payload encryption (SPE) has to be considered.

End to end payload encryption for connections with HFA devices is supported by OpenScape Business. 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.

End to end payload encryption for connections with SIP devices is **not** supported by OpenScape Business.

Connections with the OpenScape applications and conferences including external parties are partly secured by encryption.

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.

<b>CL-VoIP Encryption OSBiz V3</b>	<b>Signaling and Payload Encryption</b>
Measures	System wide flag 'SPE support' activated Payload Security activated for all relevant subscribers SPE CA Certificate and SPE Certificate imported to OpenScape Business.

	<p>(If no customer certificates are available, self-signed certificates can be generated.)</p> <p>TLS has been selected for transport on the IP endpoints (HFA-WBM or device configuration interface DLS/DLI)</p> <p>Make setting, if gateway calls e.g. with ISDN/PRI trunk are considered as secure. This influences the display at the phones.</p> <p>Enable certificate handling alarms (Navigate in WBM and check that an e-mail is sent to the administrator when events involving SPE certificates occur (Maintenance → Events → Reaction Table → MSG_SPE_CERT_xxx)</p>
References	Provision of certificate see also 12.3 Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 9.2.2 IP Transmission to internal VoIP Subscribers

### 9.2.2.1 Internal SIP Devices

The connection of system devices with SIP protocol is unsecure as OpenScape Business SPE does include SIP devices. Voice payload and signaling communication is not encrypted.

#### Risk:

Voice and signaling data can be eavesdropped. Voice call content can be disclosed and unsecured signaling can be used for toll fraud.

#### Measures:

SIP device registration with authentication must be enabled within OpenScape. Strong individual password has to be chosen for authentication according to chapter 12.1

VPN has to be used for security sensitive devices.

<b>CL-VoIP Transmission internal SIP Device OSBiz V3</b>	<b>Internal SIP device data encryption</b>
Measures	<p>Check together with customer if SIP phones have to be used in security sensitive areas.</p> <p>If so choose appropriate (encryption) measures to keep payload and signaling data confidential.</p>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>

Customer Comments and Reasons	SIP phone in security sensitive environment Yes: <input type="checkbox"/> No: <input type="checkbox"/> Measures to keep data confidential:
-------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------

### 9.2.2.2 Internal HFA Devices

The connection of system devices (OpenStage, OpenScape DeskPhone IP, OpenScape DeskPhone CP) with HFA protocol is not encrypted by default.

#### Risk:

The connection can be eavesdropped and recorded easily if access to the internal LAN is given.

#### Measures:

In case of security sensitive call the connection between internal HFA devices can be encrypted using the Signaling and Payload Encryption (SPE) feature. In case that internal SPE feature is not sufficient then external encryption means have to be used within the LAN.

<b>CL-VoIP Transmission internal HFA Device OSBiz V3</b>	<b>Internal HFA device data encryption</b>
Measures	Activate Signaling a Payload Encryption (SPE) within OpenScape Business Check if SPE covers all security sensitive connections. If necessary, choose external means for encryption.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	SPE is sufficient Yes: <input type="checkbox"/> No: <input type="checkbox"/>

### 9.2.3 IP Transmission to external VoIP Subscribers (Tele- and Mobile Worker)

OpenScape Business supports Tele- and mobile working. It allows SIP devices and System (HFA) devices to connect via the Internet and treats those devices as internal phones. For the operation of such IP phones appropriate communication ports have to be opened and the correct authentication of those devices has to be ensured.

#### Risk:

Signaling data of SIP/HFA devices connected via Internet is not encrypted. Voice payload and device login information can be retrieved, easily. Confidentiality of voice data is not given. Attackers can also exploit insufficient secured IP devices for toll fraud or for compromising OpenScape Business in general.

**Measures:**

Despite the encryption issue, device authentication has to be enabled within OpenScape Business in general for ALL IP devices and clients. ALL internal and external IP devices have to be considered. It is not sufficient to authenticate only the external devices. Strong individual passwords have to be chosen for authentication according to chapter 12.1.

External IP subscribers / clients should be connected via a virtual private network (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 has to be done by an external VPN Router. For VPN details see chapter 10.7.

<b>CL-VoIP Transmission External IP Devices OSBiz V3</b>	<b>Secure external IP devices</b>
Measures	Provide teleworkers encrypted tunnel by configuration of external VPN router.  Use authentication and strong individual password for device registration.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	Shall the teleworker VPN be configured via VPN router or via OpenScape Business?

**9.2.3.1 External SIP Device (Device@Home)**

OpenScape Business SPE does not affect the encryption via public network for SIP devices. The connection of external connected SIP devices is unsecure

**Risk:**

See 9.2.3

**Measures:**

Regardless of data encryption and VPN, device registration with authentication must be enabled within OpenScape Business for the SIP Device@Home and in addition for **all** SIP devices within OpenScape Business. A strong individual password has to be chosen for authentication according to chapter 12.1.

This ensures that a new device with a known call number doesn't register in the network by taking the place of the original device.

See also 9.2.3

<b>CL-VoIP Transmission SIP Pwd OSBiz V3</b>	<b>SIP device registration password</b>
Measures	Activate authentication at OpenScape Business Assistant and set up related passwords in the phones  Default password has to be replaced by a strong individual password according to the PW policy within chapter 12.1.1

References	Administration Manual [1] Valid PW policies see in chapter 12.1 "Password Policies" Default Accounts see chapter 12.2
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	System-specific PIN <input type="checkbox"/> Device-specific PIN <input type="checkbox"/>

### 9.2.3.2 External HFA Devices (Device@Home)

OpenScape Business SPE does not affect the encryption via public network. The connection of external connected system devices with HFA protocol is unsecure.

#### Risk:

See 9.2.3

Voice and signaling communication is not protected within the Internet and can be eavesdropped and disclosed.

#### Measures:

Regardless of data encryption and VPN, device registration with authentication must be enabled within OpenScape Business for the HFA Device@Home and in addition for **all** HFA devices within OpenScape Business. A strong individual password has to be chosen for authentication according to chapter 12.1.

This ensures that a new device with a known call number doesn't register in the network by taking the place of the original device.

<b>CL-VoIP Transmission</b> <b>HFA Pwd</b> <b>OSBiz V3</b>	<b>Enable authentication of IP system device (HFA)</b>
Measures	Activate authentication at OpenScape Business Assistant and set up strong passwords in the system and in the phones  Default password has to be replaced by a strong individual password according to the PW policy within chapter 12.1
References	Administration Manual [1] Valid PW policies see in chapter 12.1 "Password Policies" Default Accounts see chapter 12.2
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	System-specific PIN <input type="checkbox"/> Device-specific PIN <input type="checkbox"/>

## 9.2.4 IP Transmission with VoIP Service Provider (ITSP)

The user account and password are delivered by the VoIP service provider. This data is entered at the OpenScape Business administration and has to be kept confidential.

VoIP access to public networks (ITSP) is based in general on SIP for signaling and RTP for payload transmission.

Secured variants of SIP and RTP protocol are supported by OpenScape Business only for those ITSP who support encryption. Unsecured connections to ITSP can be eavesdropped easily.

For extended security, a provider with encryption support or secure VPN access is recommended.

## 9.2.5 Networking of OpenScape Business

Voice communication, UC communication, DSS server signaling, and administration take place via IP networking.

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 an external VPN Router. For VPN details see chapter 10.7.

<b>CL-VoIP Transmission VPN for Networking OSBiz V3</b>	<b>IP Networking only via VPN</b>
Measures	Provide VPN tunnel for the IP connection between the OpenScape Business nodes.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> No networking: <input type="checkbox"/>
Customer Comments / Reasons	

## 9.3 Secure signaling and authentication of UC and mobile clients

### 9.3.1 UC Smart Client @ Home

Signaling data between UC Smart Client and OpenScape Business is secured by encryption via SSL.

Authentication is done via UC Smart login credentials.

In order to secure the connection

- A strong individual UC Smart password has to be set according to password policy within chapter 12.1.1
- HTTPS protocol has to be chosen for the communication to the mobile device within OpenScape Business
- Customer individual certificated should be used instead of OpenScape Business default certificate (see chapter 12.3)

### 9.3.2 UC Suite myPortal Client

Signaling data between UC Suite myPortal Client and OpenScape Business is secured by encryption via SSL.

Authentication is done via UC Suite login credentials.

In order to secure the connection

- A strong individual UC Suite password has to be set according to password policy within chapter 12.1.1.
- Encryption has to be enabled (default) within the UC Suite administration protocol has to be chosen for the communication to the mobile device within OpenScape Business.
- Customer individual certificated should be used instead of OpenScape Business default certificate (see chapter 12.3)

### 9.3.3 UC Client myPortal @work

Signaling data between myPortal @work and OpenScape Business is secured by encryption via SSL. Authentication is done via UC Suite / UC Smart login credentials.

The data of the built in VoIP client is encrypted with DTLS and SRTP using

- the Media Server (V3 Mainboards) and OpenScape Business S
- the RTPproxy (V2 Mainboards)

of OpenScape Business.

In order to secure the connection

- HTTPS protocol has to be chosen for the communication to the mobile device within OpenScape Business
- A strong individual UC Suite/ UC Smart password has to be set according to password policy within chapter 12.1.2

### 9.3.4 Mobile Devices with myPortal to go

Signaling data between myPortal to go and OpenScape Business is secured by encryption via SSL. Authentication is done via UC Suite / UC Smart login credentials and by registered mobile number.

The voice data of the built in VoIP client is not encrypted.

In order to secure the connection

- HTTPS protocol has to be chosen for the communication to the mobile device within OpenScape Business
- A strong individual UC Suite/ UC Smart password has to be set according to password policy within chapter 12.1.2



# 10 LAN Interfaces and Protocols

In the following chapter information about the LAN interfaces and the signaling and transmission protocols and their purpose within OpenScape Business are given. The OSI communication layer model is used to sort the protocols.

Most protocols are disabled by default and are only be enabled by OpenScape Business depending on specific configuration scenarios. Protocols should not be activated manually in general without explicit needs.

In case that specific risks in OpenScape Business environment exist using a protocol, the risk and appropriate countermeasures are pointed out.

The default communication ports of the specific protocols used by OpenScape Business can be found in chapter 12.4.. This information has to be used for configuration of routers and firewalls.

## 10.1 Layer 1 - Physical Layer

OpenScape Business provides Ethernet LAN interfaces in general. Depending on the OpenScape Business model only one LAN interface or multiple LAN interfaces are used. In case of multiple LAN interfaces, the communication streams are routed via different IP addresses, depending on the HW/SW configuration of the system. The interface assignment of OpenScape Business is displayed within the administration portal. This has to be considered in case, that switches, router and firewalls are used within the LAN in order to secure the communication.

### 10.1.1 OpenScape Business X1/X3/X5/X8

The OpenScape Business main board provides three (two for OpenScape Business X1) physically independent 1 Gigabit Ethernet interfaces labeled as:

- Admin (not OpenScape Business X1)
- LAN
- WAN

The optional UC Booster card provides two physically independent 1 Gigabit 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.

For communication with external devices different LAN interface with different transmission protocols are used. Depending on the HW / SW constellation and system administration the LAN protocols are assigned to different LAN interfaces. Details are described within the administration manual [1]

### 10.1.2 OpenScape Business S

OpenScape Business S uses only one LAN interface for all communication to devices / clients and computers.

### 10.1.3 UC Booster Server (V2 MB only)

UC Booster Server uses only one LAN interface for all communication to clients and computers.

## 10.2 Layer 2 – Data Link Layer

### 10.2.1 Point to Point Protocol (PPP)

In computer networking, Point-to-Point Protocol (PPP) is a data link protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption (using ECP, RFC 1968), and compression.

Within OpenScape Business PPP is used for "PSTN peers communication" via ISDN.

For connection authentication Challenge Handshake Authentication Protocol (CHAP) can be used. Encryption is not supported by OpenScape Business.

Two preconfigured PPP connections are available within the factory delivery.

- Access to the administration Portal (Remote ISDN)
- Access to the Central License Server (CLS)

The following applies for these PPP connections:

- Connections are disabled per default.
- Default user and password are used for CHAP authentication.

#### **Risk:**

Use of default user and password is a risk therefore the defaults have to be changed.

A strong password according to password policy with chapter 12.1 has to be chosen.

#### **Measures:**

If remote administration with PPP via ISDN is used, Callback option to the remote partner has to be configured and activated within the Administration Portal of OpenScape Business

<b>CL-PPP OSBiz V3</b>	<b>PSTN Peers communication secured</b>
Measures	Keep CHAP setting and change default password to a strong individual password  Activate call back mechanism and / or call number verification and use only outgoing direction if possible
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 10.3 Layer 3 – Network Layer

### 10.3.1 IP Protocol

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

OpenScape Business supports version 4 (IPv4) of the Internet protocol for IP based LAN connections.

## 10.4 Layer 4 – Transport Layer

### 10.4.1 TCP

The Transmission Control Protocol (TCP) is a core protocol of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network.

OpenScape Business uses TCP/IP indirectly via the application layer of a specific protocol implementation (protocol stack). But in few cases OpenScape Business services address TCP/IP transport mechanisms directly for data transmission to external communication partners.

Following applications / services of OpenScape Business use the direct TCP / IP connection.

<b>Application / Services</b>	<b>Description / Remarks</b>	<b>Protocol</b>	<b>Encrypted by:</b>	<b>Factory setting</b>
CDR transmission	Call Data Record transmission (record by record) to a specific port of a TCP/IP client.	TCP/IP	no	Disabled
Manager E	Manager E access over LAN connection is done via direct TCP/IP connection to a specific port within OpenScape Business.	TCP/IP	no	Disabled
Open Directory Service	Transmission of SQL instructions, queries and results to a database server	TCP/IP	No	Disabled

#### **Risk:**

The direct data transmissions can be eavesdropped and manipulated easily by attackers. This applies also for higher layer protocols if the content is not encrypted.

## Measures:

In case that data transmission is done via TCP/IP it has to be secured by external means from unauthorized access within the LAN.

### 10.4.2 UDP

The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network. Prior communications are not required in order to set up communication channels or data paths.

UDP uses a simple connectionless communication model with a minimum of protocol mechanism. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network; There is no guarantee of delivery, ordering, or duplicate protection.

If error-correction facilities are needed at the network interface level, an application may use Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP) which are designed for this purpose.

Open Scape Business uses UDP as payload transport protocol via the Realtime Communication Protocol (RTP) to / from:

- SIP endpoints
- SIP Server
- Internet Telephony Service Provider (ITSP):

### 10.4.3 TLS / SSL / DTSL

Transport Layer Security (TLS) frequently referred to as 'SSL' is a cryptographic protocol designed to provide communications security over a computer network. Several versions of the protocols are in widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP).

In applications design, TLS is usually implemented on top of Transport Layer protocols, encrypting all of the protocol-related data of protocols such as HTTP, FTP, SMTP and NNTP.

Historically, TLS has been used primarily with reliable transport protocols such as the Transmission Control Protocol (TCP). However, it has also been implemented as DTLS protocol with datagram-oriented transport protocols, such as the User Datagram Protocol (UDP).

OpenScape Business accepts only TLS /DTLS 1.2 connections and uses TLS to secure TCP/IP communication and DTLS to secure UDP communication to internal and external services and application.

If TLS / DTLS is supported for a protocol it should be used in any case to protect OpenScape Business from eavesdropping and internet attackers.

Certificates are required for encryption with TLS or DTLS. Either the OpenScape Business default certificate or an imported customer certificate can be used.

<b>CL-TSL hardening OSBiz V3</b>	<b>Ensure TLS 1.2 support in all connected clients</b>
Measures	<ul style="list-style-type: none"><li>• Check all connected clients for TLS 1.2 support.</li><li>• Perform client SW upgrades/updates to support TLS 1.2</li><li>• Document clients with and without TLS 1.2 support</li></ul>

References	Administration Manual [1] Client descriptions and manuals
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

## 10.5 Layer 5 to 7 - Session, Presentation and Application Layers

### 10.5.1 HTTP and HTTPS

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. Within OpenScape Business it is used for following communication between OpenScape Business and following client applications, computer services or devices.

HTTP is not encrypted and is transmitted in plain ASCII. Therefore HTTP can be eavesdropped easily.

Within public networks or unsecure networks, the encrypted protocol variant HTTPS has to be used.

The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data

For encryption Transport Layer Security (TLS, see chapter 10.4.3) is used. The encryption strength of HTTPS depends on the TLS cipher suite, the kind of established authentication (none, server only, client and server) and the strength of the used certificate.

OpenScape Business supports HTTP and /or HTTPS for specific applications / services.

Application / Services	Description / Remarks	Protocol	Encrypted by:	Factory setting:
Administration Portal (WBM)	Communication with an Internet Browser. Used for administration of OpenScape Business via Webserver application.	HTTPS	TLS	Enabled
CDR file transmission	External billing applications can pull a file which contains the CDR from OpenScape Business	HTTPS	TLS	Optional / Disabled
XML configuration	External applications can import a file into OpenScape Business, which	HTTPS	TLS	Enabled

data file transmission	contains configuration data in XML format using the WebSocket interface of the WebServer			
Web Services Interface (API)	Data transmission of the Web Services Application Interface (WSI) bases on HTTP / HTTPS. Connections to following clients: <ul style="list-style-type: none"> <li>• myPortal Smart</li> <li>• myPortal to go</li> <li>• myPortal@ work</li> <li>• CP400/600</li> <li>• Application Launcher</li> <li>• OpenStage Business Attendant</li> <li>• OpenStage Business BLF</li> <li>• TAPI 120 WSI</li> </ul>	HTTP / HTTPS	TLS (optional)	Disabled
System Backup file transmission	System can download the Backup file via HTTP to an external compute e.g. Service PC,	HTTPS	TLS	Disabled
DLI	SW update by DLI for System (HFA)@home	HTTPS	TLS	Disabled
Circuit	Connection to the web based administration interface of Circuit,	HTTPS	TLS	Disabled
Unify Phone	Connection to the web based administration interface of Unify Phone	HTTPS	TLS	Disabled

## 10.5.2 FTP and FTPS

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network.

FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

**FTPS** is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols. FTPS should not be confused with the SSH File Transfer Protocol (SFTP).

OpenScape Business supports FTP / FTPS for following applications / services.

### Note:

For Backup Restore secure FTP (FTPS) supports certificates with a maximum key length of 2048 bit.

Application / Services	Description / Remarks	Protocol	Encrypted by:	Factory setting:
------------------------	-----------------------	----------	---------------	------------------

OpenScape Business Assistant (WBM)	Used by the Backup/Restore function to store /read backup files on /from a computer in the LAN.	FTP FTPS	No TLS	Optional / Disabled
DLI	File upload to devices used by DLI used for SIP and System (HFA) devices	FTP	No	Enabled
System (HFA) Devices	Used for file upload to device via FTP server.	FTP	No	Enabled
FTP client	Used for file upload / download to / from / to Xpressions Compact.	FTP	No	Enabled

### 10.5.3 SFTP

The SSH File Transfer Protocol (also Secure File Transfer Protocol, or SFTP) is a network protocol that provides file access, file transfer, and file management over any reliable data stream. It was designed as an extension of the Secure Shell protocol (SSH) version 2.0 to provide secure file transfer capabilities.

OpenScape Business supports FTP / FTPS for following applications / services.

<b>Application / Services</b>	<b>Description / Remarks</b>	<b>Protocol</b>	<b>Encrypted by:</b>	<b>Factory setting:</b>
UC Suite Server	Used for report file export to an NFS (NAS).	FTPS	SSH	Optional

### 10.5.4 SMTP and SMTPS

Simple Mail Transfer Protocol (SMTP) is an Internet standard for e-mail transmission across IP networks. SMTP is a connection-oriented, text-based protocol in which an e-mail sender communicates with an e-mail receiver by issuing command strings and supplying necessary data over a reliable ordered data stream channel, typically a TCP connection.

SMTP connections can be secured by TLS / SSL, known as SMTPS but only if the mail server supports that. Even if secure transfer is configured the connection falls back automatically to unsecured transmission if the used e-mail server does not support secure transfer.

Within OpenScape Business SMTP is used by following components.

<b>Application / Services</b>	<b>Description / Remarks</b>	<b>Protocol</b>	<b>Encrypted by:</b>	<b>Factory setting</b>
-------------------------------	------------------------------	-----------------	----------------------	------------------------

OpenScape Business Base SW	The e-mail SW component of OpenScape Business is used by the system services and system clients to send and receive e-mail via an external e-mail server.  UC Suite and UC Suite clients use only partially this SW component	SMTP / SMTPS	TLS (if supported by e-mail server)	Not configured
UC Suite Servers	The UC Suite server uses an own e-mail SW component to send and receive e-mail to / from an e-mail server.	SMTP / SMTPS	TLS (if supported by e-mail server)	Not configured
myReports client	The UC Suite myReports client uses the e-mail SW component of the UC Suite SW to send out reports to predefined e-mail recipients via an e-mail server.	SMTP / SMTPS	TLS (if supported by e-mail server)	Not configured

#### **Risk:**

As SMTP is not encrypted there is a risk of eavesdropping.

#### **Measures:**

Use encrypted SMTPS. Ensure that e-mail server supports SMTPS and does not fallback to unencrypted protocol.

Each of the application / client mentioned above has to be setup individually for secured transmission.

<b>CL-SMTP1</b> <b>OSBiz V3</b>	<b>SMTP Interface secured</b>
Measures	Secure communication is selected at Administration Portal Secure communication within myReports EMAIL Setup dialog box
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Deactivated: <input type="checkbox"/>
Customer Comments and Reasons	

## **10.5.5 SNMP**

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.



SNMP is used by OpenScape Business for sending error messages to the SNMP server by trap. From the standard security point of view this is unproblematic.

OpenScape Business supports also SNMP server GET or SET advice.

**Risk:**

As SNMP is not encrypted there may be a risk. In this case the SNMP interface should be configured more secure within OpenScape Business.

Application / Services	Description / Remarks	Protocol	Encrypted by:	Factory setting
OpenScape Business Base SW	The OpenScape Business Base SW used SNMP for monitoring and system configuration.	SNMP	Not encrypted	Disabled

Community String:

A community string is available in SNMP v1 and SNMP v2. It is comparable with a password that allows access to statistical data of a device. The standard community string names "public" (read only; get) and "private" (read and write access; get, set) should be changed into individual names. The individual names should conform to the customer's password policy. Be aware that the change of the community String has to be done on SNMP Agent and Manager side if Traps shall contain community strings, please make sure that the management applications (SNMP Managers) process the community string. Normally trap managers also make use of the community string.

Access rights (r/w or r/o) shall be set as restrictive as possible. Only if set operation is necessary on the SNMP agent, a r/w access is necessary.

Allowed Host IP Addresses:

As the community string is transmitted in clear text it can be eavesdropped easily. Thus, also IP addresses of the management applications that may contact the monitored system via SNMP shall be defined. This is only possible with static IP addresses for the hosts.

The SNMP interface is disabled by default within OpenScape Business. Enable SNMP only if necessary.

<b>CL-SNMPv1/v2</b> <b>OSBiz V3</b>	SNMP (v1, v2) security settings
Measures	Set individual Community String name; delete change the default community string names (public) into an individual value and set access rights as restrictive as possible  If Traps shall contain community strings, please make sure that the management applications (SNMP Managers) process the community string.  Restrict SNMP Managers (hosts) that may contact the monitored system by giving the hosts IP addresses
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> Deactivated: <input type="checkbox"/>
Customer Comments / Reasons	

## 10.5.6 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.

OpenScape Business supports SSH-2 protocol.

The Secure Shell interface (SSH) is reserved for system diagnosis by developers. It is not necessary for normal administration and maintenance task.

SSH is provided by:

- OpenScape Business X / UC Booster Card
- OpenScape Business S / UC Booster Server

Application / Services	Description / Remarks	Protocol	Encrypted by:	Factory setting
External SSH client	<p>SSH access is not necessary for system operation, administration and maintenance tasks. It is used by development for deep dive system diagnosis.</p> <p><b>Measures:</b></p> <ul style="list-style-type: none"><li>• disable forwarding of Port 22 in Internet Router</li><li>• keep SSH closed if not needed</li></ul> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>• closing the firewall does not interrupt an active ssh connection</li></ul>	SSH	encrypted	Disabled (OSBiz X)

### 10.5.6.1 SSH interface of OpenScape Business X / UC Booster Card

The SSH interface is provided by the Linux OS of the OpenScape Business X mainboard and in addition by the Linux OS of the UC Booster card. The SSH interface port is disabled within factory delivery.

The SSH interface port can only be enabled by the firewall setting within the Administration Portal of OpenScape Business. The firewall settings affect the mainboard and the UC Booster card equally.

The SSH config file is not accessible by normal administration. No settings can be made within the file.

Enabled SSH ports are not closed automatically in OpenScape Business X systems when upgrading the system SW.

<b>CL-SSH hardening OSBiz Model X OSBiz V3</b>	<b>OpenScape Business X - De-activate SSH interface</b>
--------------------------------------------------------	---------------------------------------------------------

Measures	Check if SSH has been opened by hazard. If so close SSH ports within OSBiz firewall settings.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	If SSH cannot be deactivated, describe measures taken:

### 10.5.6.2 SSH interface of OpenScape Business S and UC Booster Server.

The SSH protocol is provided by the SUSE Linux Enterprise Server (SLES). During installation of OpenScape Business S or UC Booster the SSH interface port is disabled within the firewall settings, as it is not used by OpenScape Business.

The SSH port can be enabled by the Linux administrator. He can also access and edit the SSH\_config file directly.

If SSH interface is enabled (not recommended) on the Linux server following measures have to be taken into account for SSH hardening.

- Only use SSH v2 (default)
- Do not allow Host-based Authentication (default)
- Do not allow empty passwords (default)
- Use PAM (Pluggable authentication modules) for authentication. (default)
- Use privilege Separation (default)
- Disable X11 forwarding (default)
- Enable strict mode (default)
- Disable root logins or allow forced commands only
- Use public Key authentication (default is keyboard based password login)
- Disable Challenge response Authentication (default: enabled)
- Only allow specific groups access (Allow Group)
- Only allow specific hosts access
- Only listen on proper interfaces
- Disable unused settings
- Disable TCP forwarding
- MaxStartups 10:30:60
- LoginGraceTime 60
- MaxAuthTries 10

<b>CL-SSH hardening OSBiz Model S OSBiz V3</b>	<b>SSH settings are hardened</b>
Measures	Check and correct the /etc/ssh/sshd_config if needed according to the above recommendations  Restart the ssh server if needed: /etc/init.d/ssh restart
References	SLES firewall documentation

Needed Access Rights	Root privileges
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	

## 10.5.7 LDAP and LDAPS

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network.

OpenScape Business uses LDAP clients and server to access external directories.

LDAP connections can be secured by TLS / SSL, known as LDAPS.

With OpenScape Business LDAP / LDAPS is used by the components listed in the following table.

The LDAP interface of the Open Directory Server within OpenScape Business is disabled per default.

Application / Services / Clients	Description / Remarks	Protocol	Encrypted by:	Factory setting
OpenScape Business Base Call Processing SW	OpenScape Business Call Processing uses an LDAP client for search in external phone books from system devices	LDAP	Not encrypted	Not configured
System Software Component LAN Device Handler (LDH)	The system SW component LDH uses LDAPS to establish the connection to a Microsoft Active Directory Server in order to retrieve the user information for system configuration.	LDAPS	Encrypted	Optional / Not configured
Open Directory Server	The embedded OpenDirectory Server is an LDAP Server and is used to access external directories of any kind.	LDAP	Not encrypted	Optional / Disabled
UC Suite	UC Suite uses an own LDAP client to retrieve caller information and for the UC client directory search function	LDAP or LDAPS	Encrypted	Optional / Not configured
Application Launcher	Application Launcher uses LDAP to retrieve caller identification information from the OpenDirectory Server	LDAP	Not encrypted	Optional / Not configured

Business Attendant	Business Attendant used LDAP to retrieve caller information from any LDAP server	LDAP	Not encrypted	Optional / Not configured
OpenStage / OpenScape devices	These devices use an own (embedded) LDAP client to retrieve caller information from any LDAP server	LDAP or LDAPS	Encrypted	Optional / Not configured
DECT IP system	The DECT IP system uses an own LDAP client to retrieve caller information from any LDAP server for caller identification and name search function of the DECT Devices	LDAP		Optional / Not configured

### Risk:

Unauthorized access to LDAP servers and clients may disclose company directory data.

### Measures

In case that LDAP interfaces are required they have to be enabled. If supported LDAPS must be used. In general, a strong password according to chapter 12.1 must be used within LDAP server in order to protect the information against unauthorized access.

<b>CL- LDAP access</b> <b>OSBiz V3</b>	<b>Protect LDAP access</b>
Measures	Set up strong LDAP password at LDAP Server
References	Administration manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 10.5.8 SIP / SIPS

The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging, over Internet Protocol (IP) networks.

The increasing concerns about security of calls that run over the public Internet has made SIP encryption more popular. Because VPN is not an option for most service providers, most service providers that offer secure SIP (SIPS) connections use TLS for securing signaling.

OpenScape Business supports SIP and SIPS for connections of SIP endpoints and SIP trunks.

Application / Services / Clients	Description / Remarks	Protocol	Encrypted by:	Factory setting
----------------------------------	-----------------------	----------	---------------	-----------------

SIP Devices	OpenStage family (SIP) OpenScape DeskPhone IP family (SIP). OpenScape DeskPhone CP family (SIP) Personal Edition (SIP)	SIP SIPS	No TLS	Optional / Not configured
SIP ITSP	ITSP connection to public network	SIP SIPS	No TLS	Optional / Not configured
SIP Trunk	Native SIP Trunk connection to Circuit  Native SIP Trunk to other OSBiz systems  Native SIP Trunk to any other SIP Client	SIP SIPS	No TLS	Optional / Not configured
SIP TieLine	Connection between networked OpenScape Business Systems	SIPQ SIPQS	No TLS	Optional / Not configured

#### **Risk:**

SIP is a widely known and used standard signaling protocol. Malicious SIP based SW is available for download on the Internet that can be used by anybody for Toll Fraud attacks and for disguising of the caller number of fraudulent calls etc.

#### **Measures:**

SIP connections have to be secured by strong authentication and if even possible by encryption.

### **10.5.9 RTP / SRTP**

The Real-time Transport Protocol (RTP) is a network protocol for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications, television services and web-based push-to-talk features.

The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications

OpenScape Business supports RTP and SRTP for connections to endpoints and trunks.

<b>Application / Services / Clients</b>	<b>Description / Remarks</b>	<b>Protocol</b>	<b>Encrypted by:</b>	<b>Factory setting</b>
System Phones (HFA)	OpenStage family (HFA) OpenScape DeskPhone IP family (HFA).	RTP SRTP	No TLS	Optional / Not configured

	OpenScape DeskPhone CP family (HFA) Personal Edition (HFA)			
myPortal to go	Mobile Client with optional Voice over IP feature	RTP SRTP	No TLS	Optional / Not configured
SIP Phones / Clients	OpenStage family (SIP) OpenScape DeskPhone IP family (SIP). OpenScape DeskPhone CP family (SIP) Personal Edition (SIP) 3 <sup>rd</sup> party SIP phones	RTP SRTP	No TLS	Optional / Not configured
SIP Trunk	Native SIP Trunk connection to Circuit  Native SIP Trunk to other OSbiz systems  Native SIP Trunk to any other SIP Server	RTP SRTP	No TLS	Optional / Not configured
SIP ITSP Trunk	ITSP connection to public network	RTP SRTP	No TLS	Optional / Not configured
SIP TieLine	Connection between networked OpenScape Business Systems	RTP SRTP	No TLS	Optional / Not configured

**Risk:**

RTP transmission can be eavesdropped easily in the LAN or on the Internet.

**Measures:**

TLS encrypted protocol variant (SRTP) has to be used whenever supported by the device, client, server or ITSP.

## 10.5.10 PostgreSQL Server Protocol

PostgreSQL Server uses a message-based protocol for communication between frontends and backends (clients and servers). The protocol is supported over TCP/IP and over Unix-domain sockets. Port number 5432 has been registered as the TCP port number for servers supporting this protocol, but in practice any non-privileged port number can be used. PostgreSQL Server is able to encrypt the protocol by using TLS. The encrypted protocol version is referred in the following as SQLS.

OpenScape Business Postgres Server supports SQL and SQLS depending on the application.

<b>Application / Services / Clients</b>	<b>Description / Remarks</b>	<b>Protocol</b>	<b>Encrypted by:</b>	<b>Factory setting</b>
Networked OpenScape Business	A slave node in the network need to read the database of the master node in the network	SQL	No	Enabled / Optional
UC Booster	UC Booster resident SW component like CMD, CSP, DSS need to access the OpenScape Business Database to read / write configuration and status data.	SQL	No	Enabled / Optional
UC Suite Clients	All UC suite client need to access the UC Suite database server to read Journal data voicemails recordings etc.	SQL SQLS	No TLS	Enabled / Optional

#### **Risk:**

SQL protocol is an open and plain text protocol. It can be easily eavesdropped and decoded.

In case of UC Suite user authentication and journal data can be spied out.

Postgres server administration tools, that are available in the Internet, can be used by an attacker to get access to the database server via the standard port 5432

#### **Measures:**

Restrict access of internal clients to the Postgres Server port by separate the LAN segment of OpenScape Business and restrict access to the UC Suite clients only within the switch settings.

Disable port 5432 in general in the Internet Router

Use always the dynamic generated database password within OpenScape Business for access to Postgres SQL database

Enable TLS encryption for the UC Suite server to client connection

### **10.5.11 CSTA**

Computer-Supported Telecommunications Applications (CSTA) is an abstraction layer for telecommunications applications. It is independent of underlying protocols. It has a telephone device model that enables CTI applications to work with a wide range of telephone devices.

OpenScape Business supports CSTA Phase III protocol either on base of ROSE/ASN.1 or XML coding.

It is available for connection of:

- OpenScape Business internal CSTA based applications like:
  - UC-Suite
  - CSTA Message Dispatcher (CMD)
  - Direct Station Server (DSS)
- External CSTA based application like:
  - OpenScape Business TAPI 170
  - OpenScape Business TAPI 120



- OpenScape Contact Center

CSTA protocol is provided on the LAN Interface by the embedded CSTA Service Provider (CSP), which supports multiple CSTA links. The specific CSTA links mentioned above can be disabled selectively by the system administrator within the administration portal.

After initial setup of OpenScape Business (factory delivery) only the CSTA links of embedded CSTA applications are enabled automatically, which are configured within OpenScape Business. CSTA links for external CSTA application are disabled in general.

The embedded CSTA Message Dispatcher (CMD) is able to multiplex multiple external CSTA links into one internal CSTA link. The CMD can only be used for connection of OpenScape Business TAPI 120 TAPI service provider. All other external CSTA applications are blocked in general by the CMD. CMD controls CSTA access of TAPI 120 users by its internal CTI firewall.

CSTA protocol links of the CSP are protected by login credentials (user and password) in general.

<b>Application / Services / Clients</b>	<b>Description / Remarks</b>	<b>Protocol</b>	<b>Encrypted by:</b>	<b>Factory setting</b>
UC-Suite	UC-Suite is an (embedded) CSTA based application which connects to one of the CSTA link of the CSTA Service Provider (CSP) within OpenScape Business.	CSTA III ASN.1 coded	Not encrypted	Optional / Enabled
CMD	CSTA Message Dispatcher (CMD) is an (embedded) CSTA based application, which connects to one of the CSTA link of the CSTA Service Provider (CSP) within OpenScape Business.	CSTA III ASN.1 coded	Not encrypted	Optional / Enabled
DSS	Directs Station Server (DSS) is an (embedded) CSTA based application, which connects to one of the CSTA link of the CSTA Service Provider (CSP) within OpenScape Business.	CSTA III ASN.1 coded	Not encrypted	Optional / Enabled
OpenScape Business TAPI 170	OpenScape Business TAPI 170 is an external CSTA application. Is connects to one of the CSTA links of the CSTA Service Provider (CSP) within OpenScape Business.	CSTA III ASN.1 coded	Not encrypted	Optional / Disabled
OpenScape Business Contact Center	OpenScape Contact Center is an external CSTA application. Is connects to one of the CSTA links of the CSTA Service Provider (CSP) within OpenScape Business	CSTA III ASN.1 coded	Not encrypted	Optional / Disabled
External CSTA applications	Other external applications connect to one of the CSTA links of the CSTA	CSTA III ASN.1 coded	Not encrypted	Optional / Disabled

	Service Provider (CSP) within OpenScape Business			
OpenScape Business TAPI 120	OpenScape Business TAPI 120 is an external CSTA application. Is connects to the CSTA link of the CSTA Message Dispatcher (CMD).	CSTA III ASN.1 coded	Not encrypted	Optional / Disabled

### Risk:

The CSTA interface allows monitoring and control of all devices, which are connected to OpenScape Business. It is a "plain text" protocol and is not encrypted. Attackers with LAN access to OpenScape Business and CSTA know-how might exploit this to monitor calls, initiate calls and to commit Toll Fraud.

### Measures:

The CSTA protocol has to be enabled only if required. A strong password according to chapter 12.1 has to be chosen for connection authentication.

As CSTA is not encrypted, the OpenScape Business must be in the same internal IP network as the CSTA communication partner. Protection of this internal network through an external firewall is required.

Access to this network is restricted to authorized network administrators. In addition to firewall configuration, usage of IP Sec (VPN) between OpenScape Business V3 and CSTA communication partner should be considered.

In case that CSTA connection is routed via public networks (Internet) VPN is mandatory.

<b>CL-CSTA1 OSBiz V3</b>	<b>Protect CSTA via CSP with strong password</b>
Measures	<p>Choose a strong password according to chapter 12.1, if enabling the CSTA interface via CSP.</p> <p>Do not use the "default" password known from previous versions of OpenScape Business or HiPath 3000 systems</p> <p>Document use of "Default" password to the customer in case that the application cannot be adapted to the new password.</p>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	<p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></p>
Customer Comments and Reasons	<p>The "Default" CSTA password has been modified"</p> <p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></p>

<b>CL-CSTA2</b> <b>OSBiz V3</b>	<b>Protect CSTA via CMD interface by CTI firewall</b>
Measures	Enter only allowed TAPI 120 users into the CTI firewall of the CMD.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	Following users are entered within the CTI firewall

<b>CL-CSTA3</b> <b>OSBiz V3</b>	<b>Protect infrastructure for CSTA</b>
Measures	<p>Keep OpenScape Business V3 in the same internal network as the CSTA application server / client and protect it with a firewall.</p> <p>Access to the internal network only for authorized persons and trusted devices (reference necessary)</p> <p>Usage of VPN (IPSec) for CSTA Protocol (details see chapter 10.7 )</p>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

### 10.5.12 SMB Protocol

In computer networking, Server Message Block (SMB), also known as Common Internet File System (CIFS), operates as an application-layer network protocol mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network. It also provides an authenticated inter-process communication mechanism. Most usage of SMB involves computers running Microsoft Windows, where it was known as "Microsoft Windows Network".

SMB protocol is used within OpenScape Business by following client / functions:

<b>Application / Services / Clients</b>	<b>Description / Remarks</b>	<b>Protocol</b>	<b>Encrypted by:</b>	<b>Factory setting</b>
OpenScape Business – Assistant Backup / Restore	The OpenScape Business Assistant (WBM) uses the SMB protocol to store or read a backup file to/ from a computer in a network.	SMBv2	Not encrypted	Optional
OpenScape Business – Assistant SDHC Backup	The OpenScape Business Assistant (WBM) uses the SMB protocol to store an SDHC backup file to/ from a computer in a network n.	SMBv2	Not encrypted	Optional
UC-Suite CSV import	UC-Suite uses the SMB protocol to import data into the external directory from a CSV file located on a computer /NAS within the customer LAN	SMBv2	Not encrypted	Optional
UC-Suite myReports	UC-Suite uses the SMB protocol to store report files that are created by myReports on a computer /NAS within the customer LAN.	SMBv2	Not encrypted	Optional

#### **Risk:**

The SMBv1 protocol is regarded as unsecure due to several vulnerabilities. It is a “plain text” protocol and is not encrypted. Attackers with LAN access to OpenScape Business might exploit the protocol to get access to the system.

#### **Measures:**

Open Scape Business supports SMBv2 only. A fallback to SMBv1 is not implemented.

SMBv2 does not support encryption. In case that the connection between OpenScape Business and the client / server / NAS is routed via the Internet or other unsecure connections, encryption by setting up a VPN is recommended.

As an alternative to VPN, encrypted protocols can be used instead of SMBv2, if supported by OpenScape Business.

#### OpenScape Business Assistant - System Backup / Restore:

For System Backup / Restore to/from a computer in the customer LAN: SMBv2 is used. Alternatively, the encrypted HTTPS or FTPS protocols are available.

#### OpenScape Business Assistant - SDHC Backup:

For SDHC card backup to NFS, SMBv2 has to be used no secured alternative protocol is supported. Encryption has to be done by external means (e.g. VPN).

#### UC-Suite -External Directory CSV Import:

SMBv2 is used. No alternative protocol is supported. Encryption has to be done by VPN.

### UC-Suite - Report Export

SMBv2 is used. Alternatively, the encrypted SFTP protocols is available.

<b>CL-SMB2-1</b> <b>OSBiz V3</b>	<b>OpenScape Business Assistant</b> <b>Use HTTPS or for Backup / Restore</b>
Measures	Choose HTTPS or FTPS to transfer the backup file to a computer in the network if possible. Do not use the unsecured SMB option  Inform customer about a potential risk if SMBv2 protocol is used instead of HTTPS/FTPS.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-SMB2-2</b> <b>OSBiz V3</b>	<b>OpenScape Business Assistant</b> <b>Use VPN to transfer SDHC Card Backup</b>
Measures	Setup a VPN between Open Scape Business and the computer/ NAS, that stores the SDHC card backup file in the LAN/WAN.  Inform customer about a potential risk if SMBv2 protocol is used unencrypted in the LAN instead via VPN.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-SMB2-3</b> <b>OSBiz V3</b>	<b>UC-Suite CSV file import</b> <b>Use VPN for permanent CSV file import from computer / NAS or via the Internet</b>
Measures	Setup a VPN between OpenScape Business and the computer/NAS, that stores the CSV file in the LAN.  Inform customer about a potential risk if SMBv2 protocol is used unencrypted in the LAN instead via VPN.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal

Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-SMB2-4 OSBiz V3</b>	<b>UC Suite: myReports file export Use SFTP or VPN for report transmission</b>
Measures	Transfer reports via SFTP for export or via secured e-mail between OpenScape Business and the computer/ NAS, that stores the report files in the LAN.  Inform customer about a potential risk if SMBv2 protocol is used unencrypted in the LAN instead of SFTP or using encrypted e-mails.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 10.5.13 Proprietary Protocols, not standardized

### 10.5.13.1 HiPath Feature Access protocol (HFA)

HiPath Feature Access protocol is an IP based protocol, which tunnels the proprietary "CorNet TS" protocol.

### 10.5.13.2 Call Data Record (CDR) transmission protocol

OpenScape Business collects billing information which is then transmitted via the CDR interface to Billing applications. This can be either the billing tool, which is deployed with OpenScape Business SW, or the Unify OpenScape Accounting Server or a 3rd party application.

The CDR interface is disabled within the factory settings. It should be enabled only if needed.

Billing data (CDR) data either be pulled by the billing application from OpenScape Business using the Administration Portal access or can be pushed actively via TCP/IP from OpenScape Business to the billing application.

#### Risks:

Attackers with LAN access might exploit the CDR interface to get information about incoming and outgoing calls of OpenScape Business users.

#### Measures:

Use File Transfer using HTTPS via Administration Portal of OpenScape Business.

For privacy reasons last 4 digits of caller- or called numbers can be suppressed by OpenScape Business system. Suppression has to be enabled by OpenScape Business administrator if requested by customer.

<b>CL-CDR 1</b> <b>OSBiz V3</b>	<b>Protect Call Data Records</b>
Measures	Enable CDR interface only if needed  Use secure data transmission via HTTPS instead of unsecured TCP/IP connection if possible
References	Administration manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	Please describe measures taken:

<b>CL-CDR 2</b> <b>OSBiz V3</b>	<b>Ensure privacy</b>
Measures	Ensure privacy in general by digit suppression
References	Administration manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

### **CDR data pulled by application**

Billing data (CDR) are transmitted by OpenScape Business on request as HTTPS file download to the billing application. Therefore, HTTPS requests are sent from the billing application to OpenScape Business.

This is the recommended method for CDR transmission.

A specific user account with limited rights has to be created within OpenScape Business administration portal for access to the Billing Server.

<b>CL-CDR 3</b> <b>OSBiz V3</b>	<b>Create specific user account for CDR transmissions</b>
Measures	Use secure data transmission via HTTPS a specific user account with the role "Basic" has to be created.  For authentication a strong password according to administration portal password policy (chapter 12.1) has to be chosen
References	Administration manual [1]

Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	Please describe measures taken:

### CDR data pushed by OpenScape Business

In this case OpenScape Business pushes record by record in plain ASCII coding via a native TCP/IP connection to the billing server. The IP address of the computer to which CDR is sent has to be configured within OpenScape Business.

#### Risk:

The transmission of CDR in this way is risky as privacy cannot be ensured, because the CDR data can easily be eavesdropped.

#### Measures:

External measures within the LAN have to be taken into account in order to protect the billing data from unauthorized access.

<b>CL-CDR 4</b> <b>OSBiz V3</b>	<b>Restrict access to CDR data transmission</b>
Measures	Note the IP address of the computer which receives the CDR data.  Protect access to CDR by external means within the LAN
References	n/a
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	Please note the IP address of the computer which receives CDR    Describe the means for securing the transmission from unauthorized access:  :

### 10.5.13.3 Manager E Transmission Protocol

Manager E administration tool uses a proprietary protocol for communication with OpenScape Business. Depending on the underlying network protocol is either transmitted via LAN or ISDN infrastructure.

In case of LAN infrastructure, a direct TCP/IP connection is setup from Manager E to the appropriate communication port of OpenScape Business.



In case of ISDN infrastructure an ISDN connection is setup to the digital modem within OpenScape Business, which converts data stream and connects internally also to the appropriate TCP port.

The Manager E port is disabled per factory default. It has to be enabled for system administration locally via Manager E or Assistant T.

**Risk:**

Data transmission between Manager E is not encrypted. It can be eavesdropped easily and used by attackers to get access to the administration port of OpenScape Business.

**Measures:**

Limit access to the OpenScape Business administration port to the administrator's PC using the OpenScape Business Application Firewall. 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).

Data Encryption (VPN) has to be used in case of remote administration via Internet.

<b>CL-Manager E Protocol OSBiz V3</b>	<b>Restrict access with Manager E</b>
Measures	Access to the Manager-E port (TCP port 7000 by default) should be limited to the administrator's PC (IP address) within Application Firewall.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

#### 10.5.13.4 Web Services API (WSI) Protocol

OpenScape Business provides an API called "Web Services Interface" (WSI) which enables external applications to monitor and control devices of the UC users as well as to get information about their presence status, journal and phone book entries.

It is used by various OpenScape Business clients, but it can also be use by any 3rd party application, which has been developed on base of the WSI API description.

The WSI is disabled within factory delivery. It uses HTTPS or HTTP protocol for communication between application and OpenScape Business.

<b>Application / Services / Clients</b>	<b>Description / Remarks</b>	<b>Protocol</b>	<b>Encrypted by:</b>	<b>Factory setting</b>
myPortal Smart myPortal @work	See chapter 6.2.1	HTTPS / HTTP	only with HTTPS	Optional / Disabled

myPortal to go		HTTPS /	yes	Optional / Disabled
myPortal for OpenStage		HTTP	no	Optional / Disabled
Application Launcher	See chapter 6.2.7	HTTPS / HTTP	only with HTTPS	Optional / Disabled
OpenScape Business TAPI 120	Only within UC Smart mode. See chapter 6.2.5.2	HTTPS / HTTP	only with HTTPS	Optional / Disabled
OpenScape Business Attendant	See chapter 6.2.6	HTTPS / HTTP	only with HTTPS	Optional / Disabled
OpenScape Business Busy Lamp Field (BLF)	See chapter 6.2.1	HTTPS / HTTP	only with HTTPS	Optional / Disabled
CP400 / CP600 Phones: Directory application	See chapter 11.4	HTTPS / HTTP	only with HTTPS	Optional / Disabled

### **Risk:**

HTTP is a clear text protocol and therefore target of all known attacks on such protocols.

### **Measures:**

It is strongly recommended to use WSI only in combination with HTTPS instead of HTTP. Especially for devices / applications, which are connected via public network to OpenScape Business.

### **Note:**

HTTP has been used for the OpenStage V2 devices because HTTPS is not supported by such devices.

If HTTP is used by mobile devices, the cookie (which is saving the password) should be disabled. This has the disadvantage for the user, that manual password entry is necessary every time.

Port-forwarding for port 8802 (HTTPS) or 8801 (HTTP) has to be activated to be able to use the Web Services via WAN Interface. To increase security for the internal LAN, an external web proxy can be used.

<b>CL-WSI OSBiz V3</b>	<b>Secure Access to Web Services</b>
Measures	'HTTPS only' is activated Cookies are disabled (recommended if HTTP is used) Disable Interface if not needed
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments / Reasons	Describe measures taken:

### 10.5.13.5 Common API

OpenScape Business provides a proprietary API called "Common API" (CAPI) which enables external applications to monitor and control devices of the UC users as well as to get information about their presence status, journal and phone book entries.

It uses HTTPS protocol for communication between application and OpenScape Business.

<b>Application / Services / Clients</b>	<b>Description / Remarks</b>	<b>Protocol</b>	<b>Encrypted by:</b>	<b>Factory setting</b>
myPortal for Teams Plugin	See chapter 6.2.14.2	HTTPS	TLS	Enabled

## 10.6 Firewalls within OpenScape Business

### 10.6.1 Firewalls within OpenScape Business X systems

Within OpenScape Business X systems several Firewalls are available depending on the model:

- OpenScape Business X1/X3/X5/X8
  - Firewall for routing via WAN interface
  - Firewall for routing via the LAN interfaces of the mainboard and UC Booster Card

OpenScape Business X specific settings within the Linux firewall are done automatically during installation process, depending on the chosen SW package and operation mode.

The ports used with OpenScape Business V3 can be found in the addendum 12.4. This information may be used for external firewall configuration e.g. for network separation to increase security.

Interfaces and ports, which are not used, are deactivated by default and shall not be activated without explicit need.

## 10.6.2 Firewalls within OpenScape Business S / UC Booster Server

Within OpenScape Business S / UC Booster Server the firewall of the operating system is used to protect the LAN interface. The OpenScape Business S / UC Booster Server specific settings within the Linux firewall are done automatically during installation process, depending on the chosen SW package and operation mode.

### 10.6.2.1 External firewall for the OpenScape Business S WAN Interface

In case that a second Ethernet card is used in the OpenScape Business S server, it is automatically detected by OpenScape Business S SW and can be used as WAN interface. OpenScape Business automatically assigns the internal firewall setting of the LAN interface also to the WAN interface. **But no Network address translation (NAT) is used.**

In case that the WAN interface is connected directly to an DSL / Cable modem it has to be ensured that the ITSP only provides telephony data and does not grant internet access via the connection. In addition, it has to be ensured that no public IP address is used by ITSP for the WAN interface.

If a public address and Internet access is granted the ITSP the WAN interface of the system is visible within the Internet and can be attacked.

In this case the WAN interface needs to be connected via TCP/IP to an external router with NAT and firewall to protect the interface from attacks.

The ports used with OpenScape Business V3 for ITSP connection can be found in the addendum 11.4. This information may be used for external firewall configuration e.g. for network separation to increase security.

## 10.6.3 NAT Port Opening / Port Forwarding

Specific ports have to be enabled and forwarded to the internal LAN by Network Address translation (NAT) for some Internet applications.

In case that the WAN interface of an OpenScape Business X model is used for Internet access the port forwarding can also be set within OpenScape Business WAN interface configuration. In all other cases the port forwarding has to be configured within an external Internet router.

- 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 ports. The communicating applications shall meet extended security standards e.g. by encryption and efficient access control.
- Port Forwarding should not be used for external VoIP subscribers (Device@Home) as this bears the risk of toll fraud by unauthorized access. If the Device@Home feature is requested by customer, device authentication has to be enabled and strong individual passwords for authorization have to be used.  
In case of security sensitive customers / devices VPN has to be used for encryption and authentication.

- Port Forwarding must not be used for application access from external e.g. by OpenScape Business desktop clients or CSTA applications which do not support encryption. These interfaces are not completely secured and may be intercepted and misused.
- Following ports must not be opened or forwarded 1:1 to the internal IP-address of the system:
  - Port 5432 to the SQL Server
  - Port 443 to the Web Server
  - Port 22 to Linux SSH
- A web proxy in a DMZ may enhance security but can lead to dependencies with some devices and browsers.

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

<b>CL-PortForwd</b> <b>OSBiz V3</b> <b>or external Router</b>	<b>Port Forwarding restricted</b>
Measures	Necessity and risk checked. Not essential port forwarding is deleted.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> not active: <input type="checkbox"/>
Customer Comments / Reasons	Please document forwarded ports and usage

## 10.6.4 IP address filtering / 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.

<b>CL-Application Firewall</b> <b>OSBiz V3</b>	<b>Application Firewall / IP address filtering</b>
Measures	Enable rules for application firewall, if it is seen necessary and does not hinder administration access

References	Administration manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/> not active: <input type="checkbox"/>
Customer Comments and Reasons	Please document IP address filtering

## 10.7 Secure Tunnel (VPN)

Virtual Private Network (VPN) also known as secure tunnel offers:

- Secure connection via an unprotected medium (Internet)
- Protection of confidential data against manipulation
- Secure business processes
- Reliable integration of external partners in the corporate network
- Access to corporate information for field service

Secure tunnels are 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.

VPN can be realized in different ways. The most used mechanism is to realize a VPN with IPSec.

IPSec supports the automatic key management system, Internet Key Exchange (IKE). This is a standard that is integrated in IPSec.

OpenScape Business provides embedded VPN functionality for the WAN interface (V2 MB only).

For connection of

- Connecting Home- and Mobile workers via a VPN
- Networking Communication Systems via a VPN

Via LAN interface an external Router with VPN functionality has to be used.

<b>CL-VPN1</b> <b>OSBiz V3</b>	Networking and Home- / Mobile Worker access allowed via VPN only
Measures	<p>Setup VPN with recommended operation mode:</p> <ul style="list-style-type: none"> <li>○ IKE(Internet-Key-Exchange-Protocol) "Main Mode" with Perfect Forward Secrecy and DH Group 2 / 5 (provides automatic key exchange management) (Default)</li> <li>○ Encryption with AES (check setting in the VPN Client)</li> </ul> <p>A) Pre-shared Key (Recommended only for a limited number of devices)</p> <ul style="list-style-type: none"> <li>○ Chose key word according to password recommendation (chapter 12.1)</li> </ul>

	<ul style="list-style-type: none"> <li>○ A secure transmission and storage of the key word has to be guaranteed</li> </ul> <p>B) Certificates may be used for increased security requirements or with an existing PKI Infrastructure</p> <ul style="list-style-type: none"> <li>○ Recommended operation mode: RSA and hash function with SHA-1</li> <li>○ Configuration is more complex (expert mode). Documentation of certificates, serial numbers and safe storage has to be guaranteed.</li> </ul>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	<p>Yes: <input type="checkbox"/>      No: <input type="checkbox"/></p> <p>No networking/remote access: <input type="checkbox"/></p>
Customer Comments / Reasons	<p>Pre-shared key <input type="checkbox"/>      Certificates <input type="checkbox"/></p>

## 11 Phones and Voice Clients

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

- System Devices with full system feature set:
  - OpenStage T (TDM)
  - OpenStage HFA (IP)
  - OpenScape Desk Phone IP HFA
  - OpenScape DekPhone CP HFA
  - OpenScape Client Personal Edition HFA (soft client)
- SIP devices with standard SIP protocol
  - OpenStage SIP
  - OpenScape Desk Phone IP
  - OpenScape DekPhone CP

Please observe the product-related security checklists and / or administration manuals. For OpenStage / OpenScape devices, compare checklist [9] [10]. Use released devices according to the current sales information only.

Within the following only OpenScape Business specific security issues are described.

### 11.1 Secure Communication using Phone Device

#### 11.1.1 Code Lock

For places with visitor access or with special functions, it is recommended to protect the phone access by code lock. Special functions are for instance system phone lock (COS changeover), switch night mode, associated dialing and silent monitoring / call supervision as well as phone lock reset for other phones. Code lock is handled via phone menu or key. Flexcall (call from any device with own authorization) is protected by the code lock PIN as well. For desk share users (logon at any device) the authentication password for the mobile user has to be activated.

The code for the lock is stored in the OpenScape Business system.

Information and briefing of the users are recommended, but not subject of the Security Checklist.

<b>CL-PhoneLock System phones</b>	<b>Code lock activated</b>
Measures	<ul style="list-style-type: none"> <li>• If Password policy can be set individually, refer to customer specific PW policy in Appendix 12.1</li> <li>• For devices with danger of misuse, code lock is used with an individual 5-digit PIN which is not easy to guess.</li> <li>• For mobile users 'Authentication at the communication system' is activated at WBM expert settings.</li> </ul>
References	<ul style="list-style-type: none"> <li>• Reference to manual would be useful!</li> <li>• PW Policy see appendix 12.1</li> <li>• Default accounts see appendix 12.2</li> </ul>
Needed Access Rights	
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

### 11.1.2 Phone Device Authentication Password, Registration credentials

The phone device authentication information and the registration information is stored within the device in general.

#### Risk:

A device can be easily removed from one location and connected to another location either within the customer network or in the public network in case of Device@Home.

If an attacker gets access to a telephone device with valid authentication and registration information, he can use the device in the same way as the authorized user. He is able to establish connections to value-add number and setup forwarding in order to commit toll fraud.

#### Measures:

In case of a legitimated change of a device e.g. for an internal shift, repair etc. the device has to be resetted to factory defaults before it is removed in order to delete passwords.

In case of device theft, the system administrator has to be informed in order to disable the device or the change the device authentication password and the registration information within the OpenScape Business system. The users have to be instructed to report device thefts or losses immediately.

## 11.2 Secure SIP Phone and SIP Device@Home

SIP based devices can be connected to OpenScape Business either internally via LAN or externally via the Internet. A SIP device is identified in general by the configured



(internal) phone number and in case of external connection by the used communication port. SIP Phones offer authentication for registration to OpenScape Business.

#### **Risk:**

As SIP is a widely used standard the attacker can try to register a SIP device which is controlled by him as an OpenScape Business device. Once registered within OpenScape Business the attacker can establish connections to value-add number and setup forwarding in order to commit toll fraud.

SIP attacks are running fully automated. Known OpenScape Business phone numbers are called, and SIP registrations are tried out either with or without registration authentication. In case of authentication well known and default password are used systematically by the attacker.

#### **Measures:**

1.) It has to be ensured by OpenScape Business, that SIP devices can be identified clearly as a internally or externally connected.

For this reason, OpenScape Business provides separate ports for internally (default Port 5060) and externally (default Port 5070) connected SIP devices

2.) All SIP devices regardless of if connected internally or via Internet as SIP Device@Home, must use **authentication** with strong password in order to protect OpenScape Business against registration of unauthorized devices. This applies also to OpenScape Cordless IP devices and SIP terminal adapters. The system forces the administrator to use authentication. SIP phones without authentication are deactivated in case of a SW upgrade.

3.) The embedded session border controller (SBC) of Open Scape Business has to be activated for externally connected SIP devices. This can be done within the station configuration dialog by setting the tic to the appropriate checkbox.

4.) It is recommended to use a SIP server port (on the external side of router) different from the SIP default 5060. This setting has also to be configured within the SIP Device@Home. This measure does not prevent attack but makes it more difficult for the attacker.

<b>CL-SIP SIP-Port OSBiz V3</b>	<b>Different ports for internal and external SIP Devices assigned</b>
Measures	<ol style="list-style-type: none"><li>1. Different SIP ports are assigned for external and internal devices. In case of same ports, ports must be changed to different values.</li><li>2. Appropriate port forwarding for externally connected SIP Device@Home is set within the Internet router (external SIP port 5060, 5062 to internal port 5070, 5071 (defaults).</li></ol>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-SIP Device Pwd OSBiz V3</b>	<b>SIP Device authentication activated</b>
Measures	<ol style="list-style-type: none"> <li>1. Authentication activated for all SIP subscribers with strong passwords</li> <li>2. An individual password is used for every device (so that not the whole system is corrupted if one phone is lost)</li> <li>3. SIP User ID is different from call number (e.g. by using a system specific prefix)</li> </ol>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-SIP Device SBC OSBiz V3</b>	<b>External SIP Device - SBC enabled</b>
Measures	Enable embedded SBC for the external SIP device by setting the appropriate checkbox in the station configuration dialog.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 11.3 Secure System (HFA) Phone and System Device@Home

System (HFA) Phones can be connected either internally or externally via the Internet (System Device@Home). A system device is identified in general by the configured (internal) phone number and in case of externally connected by the used communication port. System Phones offer an authentication for registration to OpenScape Business.

### **Risk:**

If no authentication is used it is possible to connect a new system device into the system. This can be used to execute unauthorized connections, feature like call forwarding etc. and the end for toll fraud.

### **Measures:**

The registration of an external system (HFA) device must be protected by authentication with a strong individual password. This ensures that a new device with a known call number doesn't register in the network by taking the place of the original device.

In case of externally connected system devices the embedded session border controller (SBC) has to be activated within the station configuration dialog in order to be able to distinguish between different communication ports for internal and external traffic.

Defaults are:

4060 for internal and 4062 for external System devices with no encryption  
4061 for internal and 4063 for external System devices with encryption

<b>CL-HFA HFA-Port OSBiz V3</b>	<b>Different ports for internal and external System Devices assigned</b>
Measures	<ol style="list-style-type: none"> <li>1. Different ports are assigned for external and internal system devices. In case of same ports, ports must be changed to different values</li> <li>2. Appropriate port forwarding for externally connected System Device@Home is set within the Internet router (external port 4060, 4061 to internal port 4062, 4063 (defaults)).</li> </ol>
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

<b>CL-HFA Device Pwd OSBiz V3</b>	<b>System (HFA) device registration password</b>
Measures	<p>Activate authentication at OpenScape Business Administration Portal and set up related passwords in the phones</p> <p>Customer specific PW policy is defined as depicted in the appendix.</p> <p>Default accounts are depicted in the appendix</p> <p>The default passwords are replaced by individual passwords.</p>
References	<p>Administration Manual [1]</p> <p>Valid PW policies see in chapter 12.1</p>
Needed Access Rights	OSBiz: Expert of Administration Portal

Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	System-specific PIN <input type="checkbox"/> Device-specific PIN <input type="checkbox"/>

<b>CL-HFA Device SBC OSBiz V3</b>	<b>External System (HFA) Device - SBC enabled</b>
Measures	Embedded SBC within station dialog is enabled for external system devices
References	Administration Manual [1] Valid PW policies see in chapter 12.1
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 11.4 Secure CP400, CP600 and CP700 System (HFA) Device

OpenScape DeskPhone CP400, CP600 and CP700 system (HFA) devices can also be used as System Device@Home. In addition to the risks and measures which are described in chapter 11.3 it has to be considered the CP 400/600/700 devices establish an additional connection to the Web Service Interface of OpenScape Business.

Two operating modes have to be considered for this WSI connection. Depending on the operation mode, different protocols and authentication mechanisms are used.

### Non-UC mode.

In this mode only the phonebook application of the CP 400/600/700 device can be used. The connection the Webservices Interface is done using either HTTP or HTTPS protocol.

The "Non-UC mode" requires the system device registration password for WSI user authentication. The password is transmitted encrypted to the WSI. HTTP connection must not be used for Device@Home connections.

### UC mode

The "UC mode" allows the use of the phonebook and UC functionality of the CP 400/600/700 device. The connection to the Webservices Interface (WSI) is done by HTTPS. HTTP is not supported in this case. UC login credentials are required for the WSI user authentication.

The login credentials for the WSI are entered in the device by the device administrator / user and are stored in the device.

### Risk:

HTTP is a plain text protocol and can be easily eavesdropped within the Internet or LAN

In case that a CP400/600/700 device is changed for repair or has been stolen it is possible to use the device from other locations to connect to WSI and to execute functions.

If an attacker knows the login credentials for the WSI, that are stored in the device he can use the WSI from other applications and to execute all function of the WSI incl. features like call forwarding etc.

#### Measures:

The system / device administrator has to choose a "strong" password for device registration in case of the Non-UC mode. In case of UC mode, the UC user has to choose a "strong" UC user password and login name. (See also chapter 12.1)

HTTPS has to be used for WSI connection of System Device@Home

In case that CP400/600/700 devices are changed or shifted the login credentials have to be deleted within the device.

The device password or the UC user login has to be deleted or changed immediately within OpenScape Business by the system administrator if devices were removed for repair or were stolen.

CL-CP400/600/700 HFA HTTPS protocol OSBiz V3	Enable HTTPS for CP400/600/700 Device@Home
Measures	Use HTTPS protocol for connection of CP400/600/700 to WSI in Non-UC mode.
References	Administration Manual [1]
Needed Access Rights	OSBiz: Expert of Administration Portal
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	

## 11.5 Secure Data Transmission -Signaling and Payload Encryption

For confidentiality and integrity of VoIP communication, the activation of signaling and payload encryption (SPE) shall be considered. For further information SPE see chapter 9.2.1

## 11.6 Secure Administration of Phone Devices

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

CL-Device Admin Pwd OSBiz V3	Administration access protected by strong password (PIN)
Measures	Change password at phone or via phone WBM
References	Device Administration Guides

Needed Access Rights	Device: Admin
Executed	Yes: <input type="checkbox"/> No: <input type="checkbox"/>
Customer Comments and Reasons	System-specific PIN <input type="checkbox"/> device-specific PIN <input type="checkbox"/>

# 12 Addendum

## 12.1 Password Policies

### 12.1.1 Recommended Password Policy

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. The product password policies are mandated by technical means.

Within the following table the recommended criteria for selection of passwords or PINs (numerical passwords) for OpenScape Business are described.

	<b>Recommended Password Policy of OpenScape Business V3</b>	<b>Password</b>	<b>PIN</b>
1	Minimal PW Length	10	6
2	Maximal PW Length	Depending on component	
3	Minimal number of upper-case letters	1	n/a
4	Minimal number of lower-case letters	1	n/a
5	Minimal number of numerals	1	all
6	Minimal number of special characters	1	n/a
7	Maximal number of repeated characters (e.g. bbb, 333)	3	2
8	Maximal number of sequential characters (e.g. abc, 123, 987)	3	3
9	Account name (reversed too) may not be part of password	true	true
10	Use blacklist of strings which may not be contained in password	n/a	n/a
11	Minimum character count for changed password characters	2	2
12	Password history (latest used passwords must not be used again)	5	5
13	Maximum password age standard in days	90	90
14	Minimum password age in days	Depending on component	
15	Notification before password expiration in days	n/a	n/a
16	Password change requires knowledge of old password	Depending on component	
17	Force change default passwords/PINs after the first use	Depending on component	
18	Maximum number of erroneous login attempts	Depending on component	
19	Account lockout duration in minutes	n/a	n/a
20	Next logon attempt after Lockout	n/a	n/a
21	Automatic logoff after a predefined time	Depending on component	

**Note:**

Currently there is no enforcement of these rules within all OpenScape Business clients and devices. All users have to be instructed to comply with password policies and are responsible for their observation. Do not use trivial or easy to guess passwords.

Please implement the rules above unless other company specific rules are defined at customer site. In that case the deviation required by customer should be documented within the table in chapter 12.1.3.

### **12.1.2 Specific Password Policies**

OpenScape Business technically supports the password policies depicted in the subsequent chapters. Due to historical reasons, there is no common PW policy for all OpenScape Business administration tools, features, clients and devices. In case that no values are shown in the tables below, the appropriate values of the "Recommended Password Policy" in chapter 12.1.1 have to be applied, if technically supported.



	Specific Password / PIN Policy for:	Admin Portal (WBM)	Manager E	Assistant T	UC-Suite Client	UC-Smart Client	Device Authentication	Samrt Voicemail	Xpressions Compact Superuser	Xpressions Compact Mailbox
#	Type	Pwd	Pwd	Pwd	Pwd	Pwd	Pwd	PIN	PIN	PIN
1	Minimal PW Length	8	6	6	6	8	8	6	8	6
2	Maximal PW Length	128	15	15	10		20		8	8
3	Minimal number of upper-case letters				n/a	1		n/a		
4	Minimal number of lower-case letters	1			n/a	1		n/a		
5	Minimal number of numerals	1			6	1		6		
6	Minimal number of special characters	1			n/a	1		n/a		
7	Maximal number of repeated characters (e.g. bbb, 333)				2			6		
8	Maximal number of sequential characters (e.g. abc, 123, 987)				3			6		
9	Account name (reversed too) may not be part of password				true					
10	Use blacklist of strings which may not be contained in password				n/a			n/a		
11	Minimum character count for changed password characters									
12	Password history (latest used passwords must not be used again)				n/a					
13	Maximum password age standard in days				n/a					
14	Minimum password age in days				n/a					
15	Notification before password expiration in days				n/a					
16	Password change requires knowledge of old password				true	true				
17	Force change default passwords/PINs after the first use	true	true	true	true	true		true		true
18	Maximum number of erroneous login attempts	3			5	5		6 (2)		3
19	Account lockout duration in minutes	5 - 160			n/a	15				
20	Next logon attempt after Lockout				n/a					
21	Automatic logoff after a predefined time				n/a					

### **12.1.2.1 System Administration in general**

Within the system configuration not all password entries are enforced according to the recommended PW- policy. In addition, sometimes only PINs can be entered instead of passwords, depending on the feature. In those cases, the system administrator has to choose strong passwords / PINs according to the "Recommended PW-Policy" (chapter 12.1.1) and is responsible for their observation.

### **12.1.2.2 Administration Portal (WBM)**

The Administration Portal (WBM) account of a user is blocked for a certain time after 3 erroneous login attempts. After the 3<sup>rd</sup> attempts blocking time increases by each erroneous attempt from 5 minutes to max. 160 minutes. After the 8<sup>th</sup> attempt the time does not increase further. Account blocking refers always to a specific user account but not to the login procedure in general.

Blocking of the WBM user account is done always within the node that has been accessed. Within networked systems each system blocks its WBM account individually. Blocked accounts of a specific node in a network cannot be accessed from other nodes via the WBM.

### **12.1.2.3 Manager E Administration Tool**

The password policy applies on one hand for the Login into the Manager E tool and indirectly also for the authentication of the manager E user within OpenScape Business. The password policy can only be applied if the "Variable Password Concept" has been enabled within OpenScape Business.

Within the system configuration using Manager E not all password entries are enforced according to the recommended PW- policy. In addition, sometimes only PINs can be entered instead of passwords, depending on the feature. In those cases, the system administrator has to choose strong passwords / PINs according to the "Recommended PW-Policy" (chapter 12.1.1 ) and is responsible for their observation.

Alphanumeric characters can be used for password. In this case it can happen the login from Assistant T is not possible, if character set is not supported by the system phone used for the Assistant T.

### **12.1.2.4 Assistant T Administration Tool**

The password policy above can only be applied if the "Variable Password Concept" has been enabled within OpenScape Business.

Within the system configuration using Assistant T not all password entries are enforced according to the recommended PW- policy. In addition, sometimes only PINs can be entered instead of passwords, depending on the feature. In those cases, the system administrator has to choose strong passwords / PINs according to the "Recommended PW-Policy" (chapter 12.1.1) and is responsible for their observation.

Alphanumeric characters can be used for the password if the used system phone supports it. Otherwise only the characters 0-9,\*,# can be used for password entry.

### **12.1.2.5 UC Suite Client**

The password policy applies for the login into OpenScape Business UC Suite clients. The password is valid for login into:

- myPortal for Desktop / myAttendant
- myPortal for Outlook
- myAgent
- myReports
- UC Suite Voicemail access via phone
- UC Suite Fax Printer access
- myPortal to go (in combination with UC Suite)
- myPortal @work
- OpenStage Desk Phone CP 400/600 (in combination with UC Suite)
- Application Launcher (in combination with UC Suite)

User is responsible to choose strong password according to the PW-policy and is responsible for their observation.

#### 12.1.2.6 UC Smart client

The password policy applies for the login into OpenScape Business UC Smart clients. The password is valid for login into:

- myPortal Smart
- myPortal to go (in combination with UC Smart)
- myPortal @work (in combination with UC Smart)
- OpenStage Desk Phone CP 400/600 (in combination with UC Smart)
- Application Launcher (in combination with UC Smart)
- WebServices Interface (WSI, login)

User is responsible to choose strong password according to the PW-policy and is responsible for their observation.

#### 12.1.2.7 Device Authentication

The password policy applies for authentication of system (HFA) or SIP devices within the registration procedure. In addition, the password is used for the login of the embedded CP400/600 phonebook application if no UC account exists for the user.

The system administrator is responsible for setting the device authentication per user device and for choosing the strong password for authentication.

#### 12.1.2.8 Smart VM

The password policy applies for the login into OpenScape Business UC Smart Voicemail.

User is responsible to choose strong password according to the PW-policy and is responsible for their observation.

#### 12.1.2.9 Miscellaneous PIN protected features

The following policy applies for the protection of miscellaneous features within of OpenScape Business. Note most features are protected by a PIN with fixed number of digits.

	<b>PIN Policy of OpenScape Business Feature</b>	<b>PIN length</b>	<b>fixed</b>	<b>Assigned by:</b>
	Phone Lock Code	5	yes	User
	Direct Inward Access (DISA)	5	yes	Administrator
	Deskshare user PIN	5	yes	Administrator
	Flex Call	5	yes	
	Protection of ISDN remote access connection to Digital Modem	5	yes	Administrator

PINs can be assigned either by user or administrator, depending on the specific feature.

OpenScape Business does not enforce all PINs according to the PW-Policy. The system administrator / user has to choose strong PINs according to the "Recommended PW-Policy" (chapter 12.1.1 ) and is responsible for their observation.

### 12.1.3 OpenScape Business PW Policy agreed for customers deployment

These are the customer PW/PIN rules for the PW Policy on OpenScape Business V3

Please implement them as default values. Filling the below table with customer specific values is only necessary if the customer PW Policy is different from the default values depicted in chapter 12.1.1.

	<b>Customer Policy</b>	<b>Password</b>	<b>PIN</b>
--	------------------------	-----------------	------------

1	Minimal PW Length		
2	Maximal PW Length		
3	Minimal number of upper-case letters		
4	Minimal number of lower-case letters		
5	Minimal number of numerals		
6	Minimal number of special characters		
7	Maximal number of repeated characters (e.g. bbb, 333)		
8	Maximal number of sequential characters (e.g. abc, 123, 987)		
9	Account name (reversed too) may not be part of password		
10	Use blacklist of strings which may not be contained in password		
11	Minimum character count for changed password characters		
12	Password history (latest used passwords must not be used again)		
13	Maximum password age standard in days		
14	Minimum password age in days		
15	Notification before password expiration in days		
16	Password change requires knowledge of old password		
17	Force change default passwords/PINs after the first use		
18	Maximum number of erroneous login attempts		
19	Account lockout duration in minutes		
20	Next logon attempt after Lockout		
21	Automatic logoff after a predefined time		

### 12.1.4 PW-Policy for Operating System

Even if the Operating System (OS) is not delivered by Unify and the security of the OS is up to the customer, be aware that the security of the product is dependent on the security of the whole system and especially of the OS. Thus take the advantage and harden the OS PW policy as well.

As an example, the Windows 2008 PW policy according to CIS Benchmark for Enterprise Profile is depicted here.

#	Windows 2008 PW Policy according to CIS Benchmark	Password
1	Minimal PW Length	Enterprise Profile: 8 or more
2	Maximal PW Length	
3- 6, 9, 10	Complexity requirements	Longer than 6, not compromised or principals username or real name, contains at least three distinct character classes (uppercase, lowercase, integer, non-alphanumeric)
12	Password History	24 (24 or more)

13	Maximum password age standard in days	42 days (90 or less)
14	Minimum password age in days	0 (1 or more)
18	Maximum number of erroneous login attempts	0 (Enterprise profile: 10) (SSLF: 15)
19	Account lockout duration in minutes	Not defined (15 or more)
20	Next logon attempt after Lockout	0 (15 or more)

## 12.1.5 Operating System PW-Policy agreed for customers deployment

These are the customer rules for the PW/PIN policy on Operating System level. Please implement them.

	Customer Policy	Password	PIN
1	Minimal PW Length		
2	Maximal PW Length		
3	Minimal number of upper-case letters		
4	Minimal number of lower-case letters		
5	Minimal number of numerals		
6	Minimal number of special characters		
7	Maximal number of repeated characters (e.g. bbb, 333)		
8	Maximal number of sequential characters (e.g. abc, 123, 987)		
9	Account name (reversed too) may not be part of password		
10	Use blacklist of strings which may not be contained in password		
11	Minimum character count for changed password characters		
12	Password history (latest used passwords must not be used again)		
13	Maximum password age standard in days		
14	Minimum password age in days		
15	Notification before password expiration in days		
16	Password change requires knowledge of old password		
17	Force change default passwords/PINs after the first use		
18	Maximum number of erroneous login attempts		
19	Account lockout duration in minutes		
20	Next logon attempt after Lockout		

21	Automatic logoff after a predefined time		
----	------------------------------------------	--	--

## 12.2 Default Accounts

Here are described the Default Accounts for OpenScape Business V3 including the user accounts of systems that can access OpenScape Business V3. User Accounts are listed here as well as machine accounts that are used for authentication between SW applications.

After the installation of OpenScape Business a default password is assigned to each account.

**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 Unify systems are based on unchanged default passwords.**

Following is described for every account:

- Component, that provides this account (e.g. Database...)
- Purpose (e.g. administration, diagnostics, ...)
- PW Policy that is valid for the account
- Privileges (read/write access to the following components...)
- Change instruction for PW (refer to manual where it is described how the PW can be changed).

### 12.2.1 OpenScape Business Administration

#### 12.2.1.1 Administration Portal (WBM)

User Name	Necessary privileges	PW Policy configured	Unify Default PW	Description
---	Expert	see chapter 12.1.2.1	No default	OSBiz Admin Manual [1]
administrator@system	Advanced	see chapter 12.1.2.1	administrat or	OSBiz Admin Manual [1]
---	Enhanced	see, chapter 12.1.2.1	No default	OSBiz Admin Manual [1]
---	Basic	see, chapter 12.1.2.1	No default	OSBiz Admin Manual [1]

#### 12.2.1.2 Manager E

Manager E can be used either with a variable (recommended) or a fixed (not recommended) password concept.

Within the **variable password** concept up to 16 users can be assigned their own user ID with individual name, password, and a user group consisting of six pre-determined user groups. Only the data authorized for the relevant user group can be read and administrated.

Within the **fixed password** concept only fixed user groups with unchangeable default user names and default passwords are used. Also, new users cannot be configured in the user administration.

#### Manager E with variable password concept

This is the recommended PW-concept for Manager E

User Name	Necessary privileges	PW Policy	Unify Default PW	Description
-----------	----------------------	-----------	------------------	-------------

		<b>configured</b>	<b>(to be changed immediately)</b>	
18140815	Developer	see chapter 12.1.2.3	18140815	Development user group has the possibility of administering additional data in the communication system.
31994	Service	see chapter 12.1.2.3	31994	this user group has the access rights to all administrable system data and the execute rights for all actions available in the system.
633423	Administration Customer	see chapter 12.1.2.3	633423	This user group can access data that is intended for administration by the customer.
----	Call charges	see chapter 12.1.2.3	No default	This user group has the access rights to the data from call detail recording, call charge data records and the call detail counter.
----	Revision (Audit)	see chapter 12.1.2.3	No default	This user group has the access rights to the Security protocol dialog.
---	User admin	see chapter 12.1.2.3	No default	This user group has the access rights to the User administration dialog, where the user and the linked user groups are set up.

### Manager E with fixed password concept

**This operating mode must not be used**, as the default users and passwords cannot be changed

User Name	Necessary privileges	PW Policy configured	Unify Default PW (to be changed immediately)	Description
18140815	Developer	No, because not possible	18140815	Development user group has the possibility of administering additional data in the communication system.
31994	Service	No, because not possible	31994	this user group has the access rights to all administrable system data and the execute rights for all actions available in the system.
633423	Administration Customer	No, because not possible	632423	This user group can access data that is intended for administration by the customer.

### 12.2.1.3 Assistant T

Assistant T can only be used via authorized stations via access code. (\*95 default).

User data is protected via telephone lock feature. Assistant T can be used either with a variable (recommended) or a fixed (not recommended) password concept.

Within the variable password concept up to 16 users can be assigned their own user ID with individual name, password, and a user group consisting of six pre-determined user groups. Only the data authorized for the relevant user group can be read and administrated.

Within the fixed password concept only fixed user groups with unchangeable default user names and default passwords are used. Also, new users cannot be configured in the user administration.

### Assistant T with variable password concept

This is the recommended PW-concept for Assistant T

User Name	Necessary privileges	PW Policy configured	Unify Default PW (to be changed immediately)	Description
18140815	Developer	see chapter 12.1.2.4	18140815	Development user group has the possibility of administering additional data in the communication system.
31994	Service	see chapter 12.1.2.4	31994	this user group has the access rights to all administrable system data and the execute



				rights for all actions available in the system.
*95	Administration Customer	see chapter 12.1.2.4	No password	it is possible to administer customer-relevant data using the telephone with this user group.

### Assistant T with fixed password concept

**This operating mode must not be used**, as the default users and passwords cannot be changed

User Name	Necessary privileges	PW Policy configured	Unify Default PW (to be changed immediately)	Description
18140815	Developer	No, because not possible	18140815	Development user group has the possibility of administering additional data in the communication system.
31994	Service	No, because not possible	31994	it is possible to administer customer-relevant data using the telephone with this user group.
*95	Administration Customer	No, because not possible	No password	it is possible to administer customer-relevant data using the telephone with this user group.

## 12.2.2 OpenScape Business embedded Applications and Services

### 12.2.2.1 UC Suite Client Accounts

Client	Necessary privileges	User Name	PW Policy configured	Unify Default PW (to be changed immediately)	Description
myPortal for Desktop	UC Suite user	<phone number>	see chapter 12.1.2.5	1234	Client access to UC Suite server.
myPortal for Outlook	UC Suite user	<phone number>	see chapter 12.1.2.5	1234	Client access to UC Suite server.
myAttendant myAgent	UC Suite user	<phone number>	see chapter 12.1.2.5	1234	Client access to UC Suite server.
myAgent	UC Suite user	<phone number>	see chapter 12.1.2.5	1234	Client access to UC Suite server.
myReports	UC Suite user	<phone number>	see chapter 12.1.2.5	1234	Client access to UC Suite server.

myReports	MyReports Administrator	Administrator	No, because of client specific enhancement	reports	myReports access to UC Suite plus additional client internal functions. Password Change is not requested. Has to be modified by myReports administrator
UC Suite user individual Voicemailbox	UC Suite user	<phone number>	see chapter 12.1.2.5	1234	UC Suite voicemail access from phone
myPortal @work	User	<phone number>	see chapter 12.1.2.5	1234	Client access to UC suite server
myPortal to go	User	<phone number>	see chapter 12.1.2.5	No default	Mobile Client for UC Suite functions

### 12.2.2.2 UC Smart Client Account

User account is only enabled if system administrator has assigned an initial password to the UC Smart user. The UC Smart Account is used for authentication by several OpenScape Business clients and services.

Client	Necessary privileges	User Name	PW Policy configured	Unify Default PW (to be changed immediately)	Description
myPortal Smart	User	<phone number>	see chapter 12.1.2.6	No default	Client access to UC Smart server
myPortal @work	User	<phone number>	see chapter 12.1.2.6	No default	Client access to UC Smart server
UC Smart Assistant	User	<phone number>	see chapter 12.1.2.6	No default	Web based administration of some myPortal Smart functions.
myPortal to go	User	<phone number>	see chapter 12.1.2.6	No default	Mobile Client for UC Smart functions
myPortal for openStage	User	<phone number>	see chapter 12.1.2.6	No default	Desk phone Client for UC Smart functions
OpenScape Business Attendant	User	<phone number>	see chapter 12.1.2.6	No default	Account used for authentication of the UC functions within client
OpenScape Business Busy Lamp Field	User	<phone number>	see chapter 12.1.2.6	No default	Account used for authentication of the UC functions within client

Application Launcher	User	<phone number>	see chapter 12.1.2.6	No default	Account used for authentication in general
3 <sup>rd</sup> party client at WebServices Interface	User	<phone number>	see chapter 12.1.2.6	No default	Account is used within (WSI) for authentication of the 3 <sup>rd</sup> party application

### 12.2.2.3 Smart VM

Type	Necessary privileges	User Name	PW Policy configured	Unify Default PW (to be changed immediately)	Description
Smart Voicemail Box	User	<phone number>	see chapter 12.1.2.8	123456	User account for access to VM Box and VM Box configuration

### 12.2.2.4 Phone devices and services

Client Type	Necessary privileges	User Name	PW Policy configured	Unify Default PW (to be changed immediately)	Description
OpenStage OpenScape Phone	administrator	administrator	see security policy for devices	123456	
OpenStage OpenScape Phone	user	user	see security policy for devices	123456	
Phone	OSBiz Subscriber	<phone number>	See chapter 12.1.2.9	00000	Individual Phone Lock Code,
Phone	OSBiz Subscriber	<phone number>	See chapter 12.1.2.9	00000	DISA PIN
Phone	OSBiz Subscriber	<phone number>	See chapter 12.1.2.9	00000	Desktop sharing PIN
Phone	OSBiz Subscriber	<phone number>	See chapter 12.1.2.9	00000	Flex call PIN

## 12.2.3 Operating System Accounts

Linux Operating Systems for OpenScape Business S / UC Booster Server and Microsoft Windows Operating System for servers / clients are not delivered with the OpenScape Business SW. In these cases, no default passwords are used for operating system access

OpenScape Business X models are delivered as appliances on base of an embedded Linux Operating System. The same applies for the Xpressions Compact card. Default accounts for OS administrations are implemented within both appliances.

### 12.2.3.1 OpenScape Business X

Within OpenScape Business X models a root account is available for OS access via SSH. This access can only be used by development in case of extended trouble shooting. For normal administration this account is not necessary.

The SSH access to Operation System X is disabled within factory delivery. It has to be enabled explicitly within the firewall settings of the Administration Portal of an OpenScape Business X model. The firewall settings apply to the main board OS as well as to the UC Booster Server card OS.

**Note:**

The root account password is not published; it changes from SW version to SW version.

**Measures:**

In case of a compromised root password please contact the Unify service organization and open a priority 1 ticket. Unify service organization will help on deciding the next steps such as

- update to latest SW version of OpenScape Business
- update to a specific HotFix of OpenScape Business
- close ssh port
- disable RSP access
- change admin access

## 12.3 Certificates

A certificate guarantees the ownership of e.g. a public key to a person or organization.

### Credentials used for OpenScape Business V3

**Since the default certificates don't even fulfill minimum security requirements, it is necessary to change the default certificates into customer specific certificates immediately after installation process.**

**Be aware that most successful attacks to Unify systems are based on unchanged default values.**

TLS certificates are used in OpenScape Business V3 for several connections:

#	Interface	Customer requirement for OSBiz V3 credentials	Expiration Date for Customer specific key material	Unify Default credentials	Usage
1	HTTPS			Unify default certificate	Server authentication for <ul style="list-style-type: none"><li>• Administration Portal (WBM)</li><li>• WebServices (WSI)</li><li>• UC Suite Clients</li><li>• UC Smart Client</li><li>• Application Launcher</li><li>• myPortal to go</li></ul>
2	TLS /SRTP			Generated via lightweight CA	Signaling and payload encryption for secure voice calls with HFA Phones
3	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.

Imported customer certificates can also be used instead of the Unify defaults.

## 12.4 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 Unify Partner Portal (SEBA) within the link:

<http://www.unify.com/us/partners/partner-portal.aspx>

Within the Partner Portal navigate to:

-> **Support** -> **service tools** -> **Interface Management Database (IFMDB)**

### 12.4.1 IFMDB Report relevant for security Checklist

To get all information that is necessary for the Security Checklist Port Table you should go the following way in IFMDB:

1. Choose **"Firewall Scenario Report"**
2. Within **Firewall Scenario Report** page:
  - a. Choose OpenScape Business as entity for the **left side** of the firewall (use filter to reduce entity options) and mark the button **Sel** in the last column. Afterwards press button **Continue** at the left lower corner of the page.
  - b. Choose OpenScape Business as entity for the **right side** of the firewall (use filter to reduce entity options) and mark the button **Sel** in the last column. Afterwards press button **Continue** at the left lower corner of the page.
  - c. Select the required versions within the **Review** page by unchecking the green buttons. Afterwards press button **Continue** at the left lower corner of the page

Left side of the FW	Right side of the FW
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input checked="" type="radio"/>

- d. Select the required report Format within the **Format/Style** by selecting the appropriate radio buttons. If you are not sure which report fits the best, click to the exclamation mark in the last column labeled with **Info** to get more information about the report and its handling.

Left side

Right Side

Review

Format / Style

Firewall Scenario Report

Confidentiality Class: 1. Selective Customer

Information

Detail level:

☐ low
☒ medium
☐ high

Show connection results:

☒ matching
☒ fuzzy matching
☒ non-matching

Format		Style / Description	Info
Display	Excel		
<input type="radio"/>	<input type="radio"/>	AF002 / Standard FWS table	!
<input checked="" type="radio"/>	<input type="radio"/>	AF004 / Communication Table for Firewall (FW) Configuration & OBSO Security Checklists	!
<input type="radio"/>	<input type="radio"/>	AF006 / Communication table for system under test on the left side of firewall.	!

↑

↑

Please select one of the following report styles and output formats (Display / Excel file)

press button **Continue** at the left lower corner of the page to get the port list

## 12.4.2 Port of miscellaneous applications and services

## 13 Abbreviations

AP	Access Point
BIOS	Basic Input/Output System
BRI	ISDN Basic Rate Interface
CIS	Center of Internet Security ( <a href="https://www.cisecurity.org">https://www.cisecurity.org</a> )
CLA	Customer License Agent (location of license File on customer Side)
CLC	Customer License Client (located at Product on Customer Side)
CLM	Customer License Management (located at User on Customer Side)
CLS	Customer License Server (located on Unify Side)
CSCm	Customer Site Components Modular (located at User on customer Side)
CMP	Common Management Platform
CSTA	Computer Supported Telecommunications Applications
DECT	Digital Enhanced Cordless Telecommunications
DISA	Direct Inward System Access
FM	Fault Management
HFA	HiPath Feature Access
HLP	Client component of License Management (CLC component)
HMP	(CLM and CSCm components for License Management
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IFMDB	Interface Management Data Base
IP	Internet Protocol
IPSec	Secure Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LDAP	Lightweight directory access protocol
LDAPS	Lightweight directory access protocol secured
MS	Microsoft
NAT	Network Address Translation
OS	Operating System
PSTN	Public Switch Telephony Network
PW	Password
QM	Quality Management
RSP	Remote Service Platform
SCL	Security Checklist
SEBA	Unify Partner Portal
SF	Security Foundation)
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

SQL	Structured Query Language
SSDP	Smart Service Delivery Platform
SSH	Secure Shell
SSO	Single Sign On
SW	Software
TAPI	Telephony Application
TDM	Time Division Multiplex
TLS	Transport Layer security
UM	User Management
URL	Uniform Resource Locator
VM	Virtual Machine
VPN	Virtual Private Network
WL	Wireless Phone by Unify
WLAN	Wireless LAN



# 14 References

Link to OpenScape Business V3 Product Information:

[https://enterprise-businessarea.unify.com/productinfo/producthomepageservice.jsp?mainTab=external\\_productversion&pvid=683200&pid=440100&clienttype=topnet](https://enterprise-businessarea.unify.com/productinfo/producthomepageservice.jsp?mainTab=external_productversion&pvid=683200&pid=440100&clienttype=topnet)

- [1] **OpenScape Business V3 Administrator Documentation**  
available via e-Doku or SEBA Portal / product information
- [2] **Manager E Administrator Documentation**  
available via e-Doku or SEBA Portal / product information
- [3] **OpenScape Business V3 Service Manual**  
available via e-Doku or SEBA Portal / product information
- [4] Xpressions Compact V3 Installation and Administration Manual  
available via e-Doku or SEBA Portal / product information
- [5] **Support of Operating System Updates for Server Applications**  
[http://wiki.unify.com/images/c/c0/Security\\_Policy\\_-\\_Support\\_of\\_Operating\\_System\\_Updates\\_for\\_Server\\_Applications.pdf](http://wiki.unify.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.unify.com/images/2/21/Security\\_Policy\\_-\\_Support\\_of\\_Virus\\_Protection\\_Software\\_for\\_Server\\_Applications.pdf](http://wiki.unify.com/images/2/21/Security_Policy_-_Support_of_Virus_Protection_Software_for_Server_Applications.pdf)
- [7] **Unify Security Advisories**  
<http://www.unify.com/us/partners/partner-portal.aspx>  
-> sell -> document information -> search "security advisory"
- [8] **Security Policy - Vulnerability Intelligence Process,**  
[http://wiki.unify.com/images/c/ce/Security\\_Policy\\_-\\_Vulnerability\\_Intelligence\\_Process.pdf](http://wiki.unify.com/images/c/ce/Security_Policy_-_Vulnerability_Intelligence_Process.pdf)
- [9] **Security Checklist – OpenStage and DeskPhone IP HFA V3**  
[https://enterprise-businessarea.unify.com/productinfo/document/-WOWUMIIqKg\\_/OpenScape%20Desk%20Phone%20IP\\_OpenStage%20HFA%20V3%2C%20Security%20Checklist%2C%20Issue%203.pdf](https://enterprise-businessarea.unify.com/productinfo/document/-WOWUMIIqKg_/OpenScape%20Desk%20Phone%20IP_OpenStage%20HFA%20V3%2C%20Security%20Checklist%2C%20Issue%203.pdf)
- [10] **Security Checklist – OpenScape DeskPhone IP OpenStage SIP V3**  
[https://enterprise-businessarea.unify.com/productinfo/document/frmwTZorags\\_/OpenScape%20Desk%20Phone%20IP\\_OpenStage%20SIP%20V3%2C%20Security%20Checklist%2C%20Issue%204.pdf](https://enterprise-businessarea.unify.com/productinfo/document/frmwTZorags_/OpenScape%20Desk%20Phone%20IP_OpenStage%20SIP%20V3%2C%20Security%20Checklist%2C%20Issue%204.pdf)
- [11] **Interface Management Database (IFMDB)**  
available via SEBA Partner Portal  
<http://www.unify.com/us/partners/partner-portal.aspx>
- [12] **Center of Internet Security – Security Benchmarks**  
<https://benchmarks.cisecurity.org/en-us/?route=downloads.multiform>
- [13] **RSPssh Installation Guide**  
[https://enterprise-businessarea.unify.com/productinfo/document/ZHuC2YAeIO4\\_/Remote%20Service%20Platform%20V3%20Getting%20Started%20Guide%20-%20RSPssh.pdf](https://enterprise-businessarea.unify.com/productinfo/document/ZHuC2YAeIO4_/Remote%20Service%20Platform%20V3%20Getting%20Started%20Guide%20-%20RSPssh.pdf)
- [14] A31003-S2530-M100-13-76A9, 02/2014 HiPath Xpressions Compact V3.0, Administrator Documentation
- [15] A31003-P3020-J101-05-7631, 05/2016 OpenScape Business V3, Installing OpenScape Business S

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Copyright © Unify Software and Solutions GmbH & Co. KG, 04/2023  
All rights reserved.

Reference No.: A31003-P3030-P100-05-76A9

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.

[atos.net](https://atos.net)

The logo for Atos, featuring the word "Atos" in a bold, white, sans-serif font. The letter 'o' is stylized with a circular graphic element inside it.