A MITEL
PRODUCT
GUIDE

Mitel OpenScape Concierge

OpenScape Concierge V5R0

Security Checklist

Planning Guide

03/2025

A31003S2250P1000676A9

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively "Unify") or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

1 Introduction

1.1 General Remarks

Information and communication and their seamless integration in “Unified Communications and Collaboration“ (UCC) are important, valuable assets forming the core parts of an enterprise business. These assets require every enterprise provide specific levels of protection, depending on individual requirements to availability, confidentiality, integrity and compliance for the communication system and IT infrastructure it utilizes.

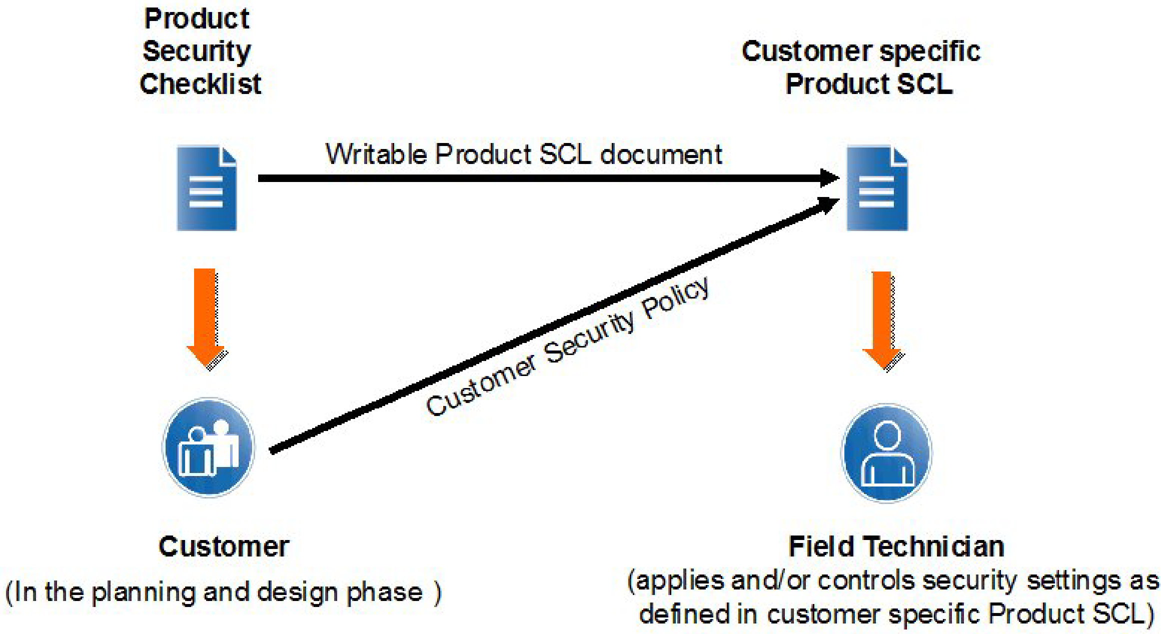
Unify attempts to provide a common standard of features and settings of security parameters within delivered products. Beyond this, we generally recommend

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

Product Security Checklists are published as a basis to support the customer and service department in both direct and indirect channels, as well as self- maintainers, to document security setting agreements and discussions.

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:
  - During installation/setup of the solution
  - 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.


Product Security Checklist
Customer specific Product SCL
Writable Product SCL document
Customer Security Policy
Customer
(In the planning and design phase)
Field Technician
(applies and/or controls security settings as defined in customer specific Product 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 using always 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 http://www.unify.com/us/ partners/partner-portal.aspx for the entire product.
- We encourage you to provide feedback in any cases of unclarity, or problems with the application of this checklist.
  Please contact the OpenScape Baseline Security Office

1.2 Security Strategy for Unify Products

Reliability and security is a key requirement for all products, services and solutions delivered by Unify. This requirement is supported by a comprehensive security software development lifecycle that applies to all new products or product versions being developed from design phase until end of life of the product.

Products of Unify are developed according to the Baseline Security Policy, which contains the technical guidelines for the secure development, release and sustaining of the company’s products. It defines the fundamental measures for software security that are taken throughout the whole lifecycle of a product, from design phase until end of life:

Product planning and design

Threat and Risk analysis (Theoretical Security Assessment) to determine the essential security requirements for the product.

Product development and test

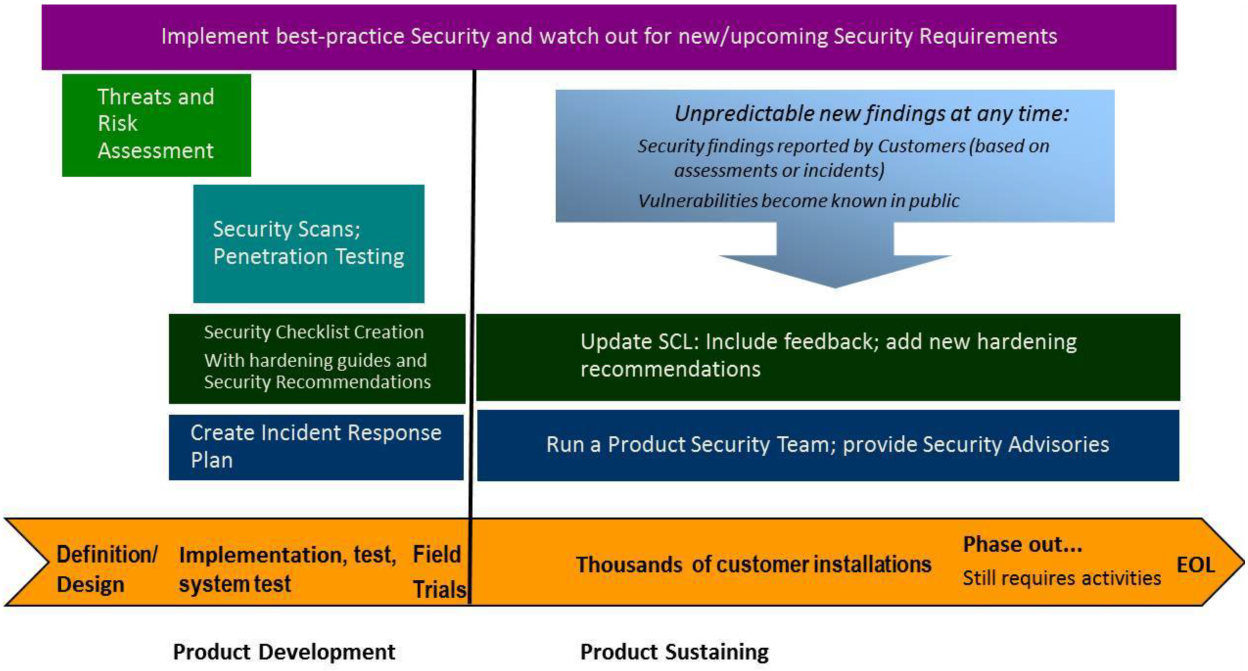
Penetration Tests (Practical Security Assessment) to discover implementation vulnerabilities and to verify the hardening of the default system configuration.

Installation and start of operation

Hardening Guides (Security Checklist) to support the secure configuration of the product according to the individual customer's security policy.

Operation and maintenance

Proactive Vulnerability Management to identify, analyze and resolve security vulnerabilities that emerge after products have been released, and to deliver guidance to customers how to mitigate or close these vulnerabilities


Implement best-practice Security and watch out for new/upcoming Security Requirements
Threats and Risk Assessment
Security Scans; Penetration Testing
Security Checklist Creation With hardening guides and Security Recommendations
Create Incident Response Plan
Unpredictable new findings at any time:
Security findings reported by Customers (based on assessments or incidents)
Vulnerabilities become known in public
Update SCL: Include feedback; add new hardening recommendations
Run a Product Security Team; provide Security Advisories
Definition/ Design
Implementation, test, system test
Field Trials
Thousands of customer installations
Phase out...
Still requires activities
EOL
Product Development
Product Sustaining

For more information about the Unify product security strategy we refer to the relevant Security Policies (see References [8], [9], [10]).

As we at Unify define a secure product, our products are not secure, but - they can be installed, operated and maintained in a secure way. The level of the products security should be scheduled by the customer.

The necessary information for that is drawn up in the Product Security Checklist. The Product Security Checklist is this paper. The security Checklist is a living document that integrates feedbacks and new security aspects during the whole product sustaining phase. To keep the Unify product on the security level scheduled at installation time it is also necessary to apply new security aspects to the product during its live time. Additional security offers for the operations and maintenance phase of the product as described above in this chapter should also be applied.

1.3 History of Change

Date	Version	Description
2018-10-22	0.1	Initial creation
2017-12-17	0.2	Update OS-Hardening
2018-12-21	0.3	Re-branding, style
2019-05-03	1.0	Preliminary
2022-01-19	2.0	Review
2023-19-05	2.0	Review and updated the chapters: 5.9.1 Communication between OpenScape Concierge V5 Services and the OSCC Informix database, 5.9.2 Communication between Concierge ConfigSync Server and OSCC Server, 5.9.3 Communication between Contact Center Node and OSCC Server

1.4 Customer Deployment - Overview

This Security Checklist covers the product and lists their security relevant topics and settings in a comprehensive form.

	Customer	Supplier
Company		
Name		
Address		

	Customer	**Supplier**
Telephone		
E-mail		
Covered Systems (e.g. System, SW version, devices, MAC/IP- addresses)		
Referenced Master Security Checklist	Version:	
	Date:	
General Remark		
Open issues to be resolved until		
Date		

1.5 Untreated topics

This Security Checklist is not handling following topics:

- Security of license management through CLA/CLM
- Details of security of remote access through SSDP (RSPSSH)

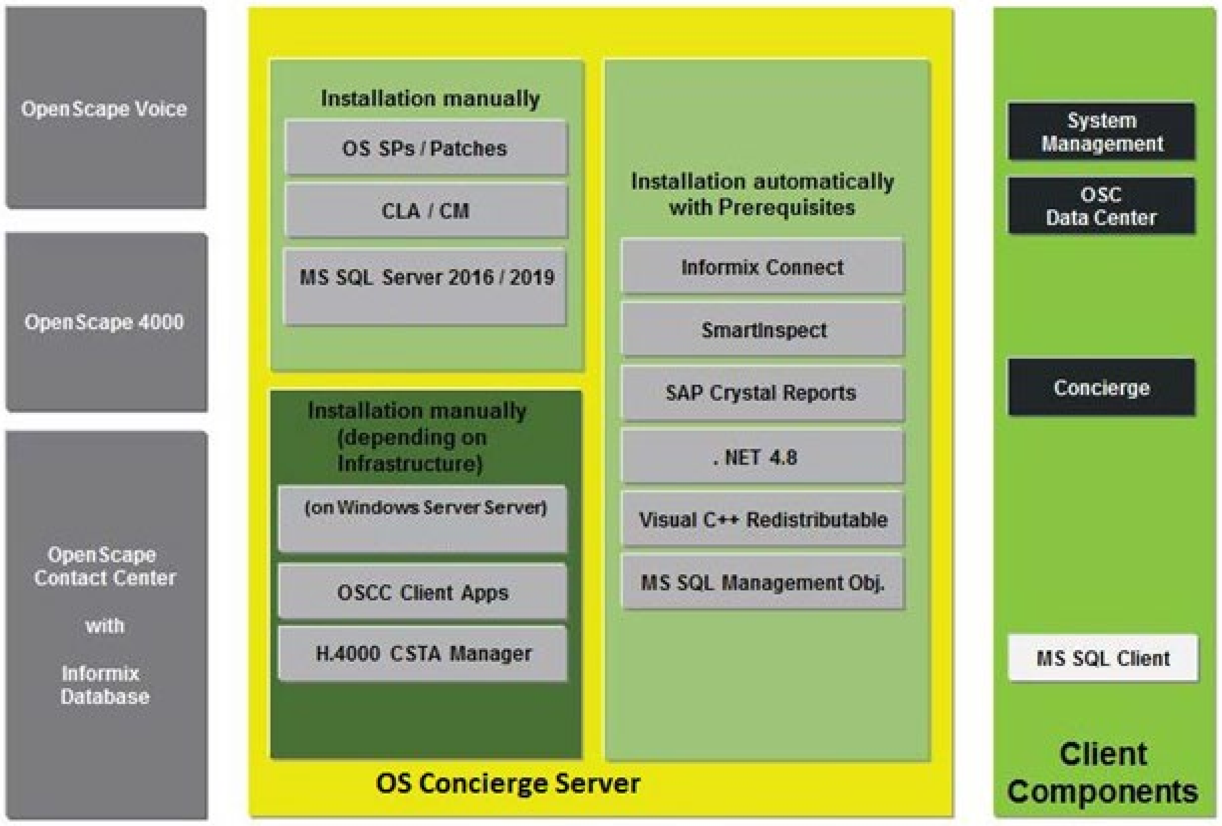
These topics will be handled in separate Security Checklists.

2 SF - OpenScape Concierge V5R0 Hardening Procedures in General

In this section an overview of OpenScape Concierge V5R0 including Concierge is given followed by most basic hardening measures.

2.1 Essential software modules of OpenScape Concierge V5R0

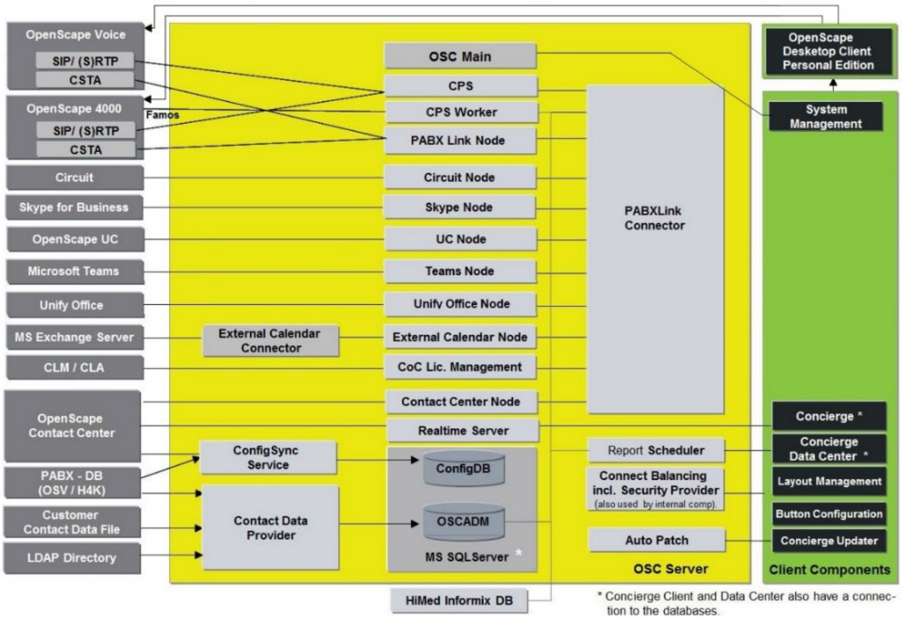
The following graphic shows the essential software modules of OpenScape Concierge V5R0. Most of them are installed by OpenScape Concierge V5R0 server setup, but there is also software that must be installed manually depending on selected deployment. For details see server setup document [2].



2.2 Components of OpenScape Concierge V5R0

The following overviews show the essential software modules and components of OpenScape Concierge V5R0.

2.2.1 Components of OS Concierge Server



* Concierge Client and Data Center also have a connection to the databases.

OSC Main is the central service to start and stop the applications.

The modules Contact Data Provider (CDP), Concierge Provider Service (CPS) and the database **OSCADM** are only active with Concierge deployment – depending on the infrastructure this is also valid for the connectors to UC Node and External Calendar Node.

If an OS Concierge standby server exists in the deployment, it will have the same components.

2.3 Basic measures for OpenScape Concierge V5R0

The recommended measures are listed in the following sections.

Some protocols like CSTA and DNS SRV don’t provide support for encryption. Additively OS Concierge doesn’t support encryption for SIP. It is recommended to handle this by infrastructure – specifically by establishing VPN connections or VLAN’s between the servers to reach a higher degree of security (see section 6.4 VPN connection (IPSec based)).

Install only up-to-date software. The newest versions of software that is delivered by Unify always are available on Unify Software Server. We recommend the installation of up-to-date software versions and patches of additionally needed 3rd party software. Please also take into account manufacturer advisories as well as Unify security advisories

CL-SF: SW status **All components**	**Up-to-date SW, SW that is delivered by Unify as well as additionally necessary Software**
Measures	Up-to-date SW installed for the below listed components. SW that is delivered by Unify can be downloaded from the SW Server.
References	Release notes
OpenScape Concierge V5R0	Yes: □ No: □
Central components	
OS Concierge Server	Yes: □ No: □ Version:
OS Concierge standby server	Yes: □ No: □ Version:
Further 3rd party components on servers	
Browser	Yes: □ No: □ Version:
OS SPs / Patches	Yes: □ No: □ Version:
IIS	Yes: □ No: □ Version:
.NET	Yes: □ No: □ Version:
Java RE	Yes: □ No: □ Version:
OSCC Client Apps	Yes: □ No: □ Version:
H.4000 CSTA Manager	Yes: □ No: □ Version:
Virus protection	Yes: □ No: □ Version:
Clients	

CL-SF: SW status **All components**	**Up-to-date SW, SW that is delivered by Unify as well as additionally necessary Software**
Concierge	Yes: □ No: □ Version:
Configuration Management	Yes: □ No: □ Version:
Concierge Data Center	Yes: □ No: □ Version:
Layout Manager	Yes: □ No: □ Version:
Button Config	Yes: □ No: □ Version:
System Management	Yes: □ No: □ Version:
Further 3rd party components on clients	
Browser	Yes: □ No: □ Version:
OS SPs / Patches	Yes: □ No: □ Version:
Java RE	Yes: □ No: □ Version:
MS SQL Client	Yes: □ No: □ Version:
Virus protection	Yes: □ No: □ Version:
Customer Comments / Reasons	

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

3 SF - Server Hardening

Each server, the OpenScape Concierge V5R0 runs on, shall be hardened. That may be more than one server for distributed deployment of OpenScape Concierge V5R0.

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

- The operating system version is released for the communication software (see release notes [4])
- Current security updates are installed (see section 2 SF - OpenScape Concierge V5R0 Hardening Procedures in General)
- Suitable virus protection software shall be installed and active (see 3.5 SF - Virus Protection). This is especially true for mail servers and Windows PCs.
- The access to the system is protected by passwords according to the password rules fixed in 7.1 SF - Password Policies.
- After Installation all software that were necessary as installation help (diagnostic tools like Wireshark, putty, old SW Versions ...) shall be removed from Server.

3.1 Bios Settings

BIOS Settings are general security task independent of the specific application on the server.

3.1.1 BIOS Password

Set BIOS Password on OpenScape Concierge Server according to your password policy, in order to avoid unauthorized change of BIOS configuration. BIOS Password can be changed within the BIOS settings. The computer displays how to enter the BIOS during start-up phase.

Setting Boot password **for rebooting** is not recommended, because it would not allow rebooting the server without physical access to the system keyboard to enter the boot password.

Setting BIOS password **for BIOS changes** is recommended.

CL-BIOS Protect BIOS settings **OpenScape Concierge V5R0**	**Setting BIOS password for BIOS changes**
Measures	• BIOS password is necessary to change the setting in the BIOS is configured in the BIOS settings. • BIOS Manufacture supports this feature
References	
Needed Access Rights	BIOS access
Executed	Yes: □ No: □
Customer Comments / Reasons	

3.1.2 Boot device

Disable booting from USB-Device, Floppy or CD-ROM. This option can be changed within the BIOS settings. The computer displays how to enter the BIOS during start-up. Booting from CD-ROM may be necessary for software installation and upgrade. If you install software from a CD-ROM please take in account that booting from CD-ROM must be enabled.

Disable booting from Network or USB-Device. This option can be changed within the BIOS settings. The computer displays how to enter the BIOS during start up.

CL-BIOS boot device **OpenScape Contact** **OpenScape Concierge V5R0**	**Setting Boot device in BIOS**
Measures	• Boot device is configured in the BIOS settings
References	
Needed Access Rights	BIOS access. If configured, the BIOS password is needed for this.
Executed	Yes: □ No: □
Customer Comments / Reasons	

3.1.3 BIOS write protection

Depending on the Main board manufacture it might be possible to active write protection for the BIOS by jumper settings on the main board. This jumper must be considered in case of BIOS updates.

CL-BIOS write protection **OpenScape Contact** **OpenScape Concierge V5R0**	**Setting write protection**
Measures	• Jumper on main board is set
References	
Needed Access Rights	BIOS access.
Executed	Yes: □ No: □
Customer Comments / Reasons	

3.2 SF - OS Hardening

OpenScape Concierge V5R0 software must be installed on a server machine that runs following operating system:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

If the OS is not delivered by Unify, the hardening of the OS is up to the customer. In that case Unify proposes the below measures for the hardening of the OS as well, but it is up to the customer to execute the OS hardening.

This includes ensuring that the latest Windows updates are installed [8] , virus protection software is installed [9], and that access to the system is protected by passwords that meet the security requirements of your organization. For a list of the hot fixes that have been tested for each supported operating system, contact your support representative.

We recommend that you install the operating system and then the OpenScape Concierge Server software **before** hardening the OpenScape Concierge Server machine.

NOTE:
Some settings might result in system overheads in terms of resource consumption (CPU, memory, disk space, etc.). The customer must be aware of the potential impacts of these settings on the overall performance of the machine and consider tradeoffs in terms of balancing the security concerns versus the quality of service provided by the application running on the server machine.

Mandatorily the below hardening advisories shall be applied for OS that is delivered by Unify.

3.3 Clean Customer Deployment

CL-Clean deployment OpenScape Concierge V5R0 Server PCs	**All SW coming from Unify that is not necessary for the customer deployment has to be removed from the OpenScape Concierge V5R0 Server.**
Measures	After Installation all software that was necessary as installation help (diagnostic tools like Wireshark, putty, old SW Versions ...) shall be removed from Server
References	
Needed Access Rights	Windows administration
Executed	
OS Concierge Server	Yes: □ No: □
Remote Agent server	Yes: □ No: □
Reporter server	Yes: □ No: □
OS Concierge standby server	Yes: □ No: □
Remote Agent standby server	Yes: □ No: □
Reporter standby server	Yes: □ No: □
Customer Comments / Reasons	

3.4 OpenScape Concierge V5R0 Protection on Server Level

Whether the user accounts on Operating System Level shall be content of the Security Checklist or not, depends on the customer deployment. Many customers make these themselves. Nevertheless, the customer shall be aware, that the security of server access on OS level is not independent of the security of OpenScape Concierge V5R0.

- Access right settings for user accounts (read/write access to file system) (details see also section 5.1 System Access Protection)
- OS Password policies (details see 5.1System Access Protection)
- Default PW replacement (details see also 7.2SF - Default Accounts

OpenScape Concierge V5R0 Data Protection on Server:

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

Which default OS accounts are necessary is depicted in the appendix in Section 7.2 SF - Default Accounts

CL-1 CL-SrvPwd **OpenScape Concierge V5R0 Server PCs**	**Access to the server / PCs are protected by passwords.**
Measures	• Customer specific PW policy is defined as depicted in addendum section 7.1. • Default accounts are depicted in addendum section 7.2. • The default passwords are replaced by individual passwords.
References	• Valid PW policies see section 7.1 • Default Accounts see section 7.2
Needed Access Rights	Windows administration
Executed	
OS Concierge Server	Yes: □ No: □
Remote Agent server	Yes: □ No: □
Reporter server	Yes: □ No: □
OS Concierge standby server	Yes: □ No: □
Remote Agent standby server	Yes: □ No: □
Reporter standby server	Yes: □ No: □
Customer Comments / Reasons	

3.5 SF - Virus Protection

Unify Baseline Security Policy recommendation can be found in [9].

Virus Protection is recommended for all Unify products.

OpenScape Concierge V5R0 was tested with Crowstrike 6.42.15610.0.

CL-VirusProtect OpenScape Concierge V5R0 Server PCs	**Virus protection software is installed and active.**
Measures	- Virus scanner to be used (Crowstrike v6.42.15610.0)
References	https://nuxeo.unify.com/nuxeo/site/proxy/internal/nxdoc/view/RAW/d0255f02-bf4e-4563-92ad-988272894a76
Needed Access Rights	Windows administration
Executed	
OS Concierge Server	Yes: □ No: □
Remote Agent server	Yes: □ No: □
Reporter server	Yes: □ No: □
OS Concierge standby server	Yes: □ No: □
Remote Agent standby server	Yes: □ No: □
Reporter standby server	Yes: □ No: □
Customer Comments / Reasons	

3.6 File and Print services

OpenScape Concierge V5R0 installer puts all related Concierge client software into folder ***C:\Program Files (86x)\OpenScape Contact Center Extension\ClientSetups***, which normally is published as a shared drive.

Print services are not required and therefore don't have to be published as shared service.

3.6.1 Share-Mode (File Service)

The "\netsetup" share provides client software installer. The initial installation can be done by accessing this shared folder. Clients also check at their start, if under \\<OS Concierge Servername>\netsetup there's any updated software. If so, then the new version is shown to the user who then easily can update their client.

- The service can be switched off, if customer security policy requires that. The functions mentioned above are not available in this case. In this case the software and any updates must be distributed through any other solution (e.g. by distributing it on a different server or by CD).
- If Share-Mode is not switched off:
  - The directory shall be read-only.

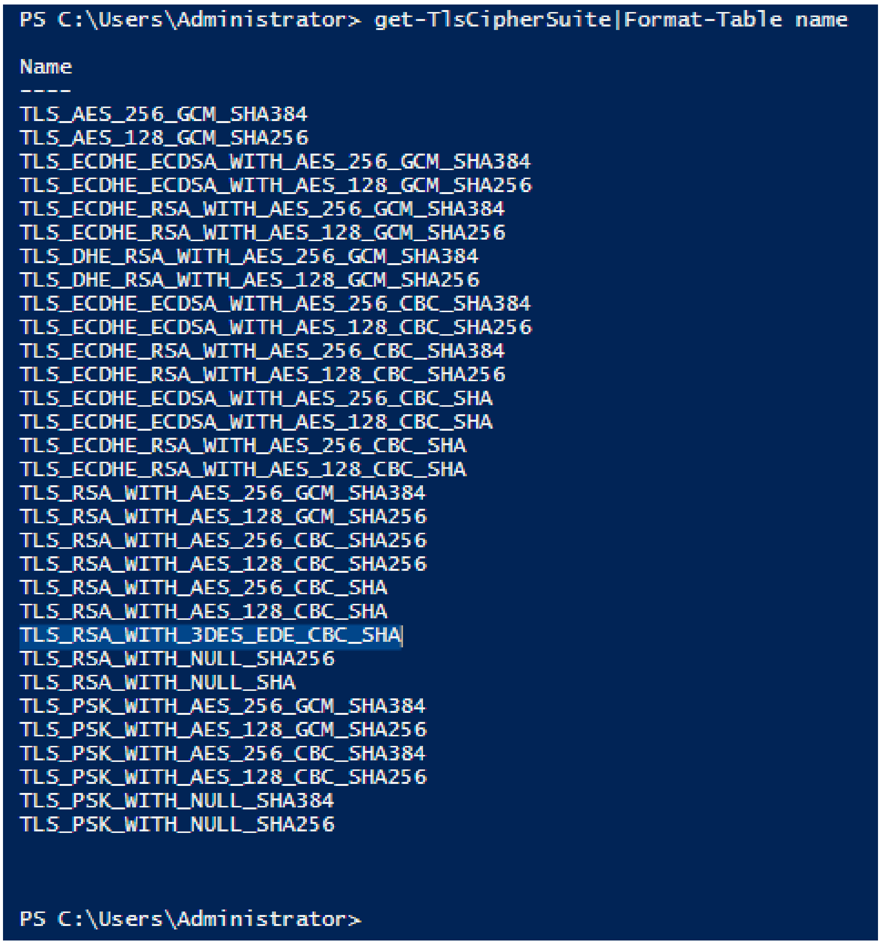
CL-SharedFolder OpenScape Concierge V5R0	**Secure shared folder .**
Measures	• Share-Mode is deactivated or • Security Measures as described in Customer Comments are done, because service is needed
References	See section **"Client updates and patches"** in [3]
Needed Access Rights	Windows administration
Executed	Yes: □ No: □
Customer Comments / Reasons	

3.7 Disabling Insecure Ciphers

To list all enabled ciphers in the Windows Operational System, use the following Windows PowerShell command:

```
Get-TlsCipherSuite|Format-Table name
```

You will see a list like this:



```
PS C:\Users\Administrator> get-TlsCipherSuite|Format-Table name

Name
----
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
TLS_PSK_WITH_AES_256_GCM_SHA384
TLS_PSK_WITH_AES_128_GCM_SHA256
TLS_PSK_WITH_AES_256_CBC_SHA384
TLS_PSK_WITH_AES_128_CBC_SHA256
TLS_PSK_WITH_NULL_SHA384
TLS_PSK_WITH_NULL_SHA256


PS C:\Users\Administrator>
```

To remove vulnerabilities it is recommended to disable the cipher called "**`TLS_RSA_WITH_3DES_EDE_CBC_SHA`**" or any other deprecated cipher when necessary. To do so, use the windows PowerShell command below:

```
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_3DES_EDE_CBC_SHA"
```

NOTE: For this to take effect, the server machine must be restarted.

4 OpenScape Concierge V5R0

4.1 Secured connection with OS Concierge Server

In the OS Concierge Systemmanagement the setting of the security can be adapted.

TLS Versions 1.1 and V1.2 are available.

The default setting: TLS Version 1.2 only is activated.

NOTE:
To ensure maximum security, it is advised to use TLS 1.2 as the default and disable older versions such as TLS 1.0 and TLS 1.1 in the operating system. Microsoft provides specific guides on how to accomplish this. This measure is important because some third-party entities may try to negotiate TLS versions below 1.2 with the operating system, which can lead to security vulnerabilities.

The certificate validation is configured in the OS Concierge Systemmanagement.

The following settings are possible: None, Server validation, Chain validation.

The default setting: Server validation.

CL-OS Concierge Server1 OpenScape Concierge V5R0	Secured connection with OS Concierge Server.
Measures	• Use the maximal validation of the certificate. Activate certificate validation with chain.
References	
Needed Access Rights	OS Concierge administration
Executed	Yes: □ No: □ Deactivated: □
Customer Comments / Reasons	

The default server certificate which comes with the installation should be replaced by a new one which contains the server name and is signed by a trusted CA.

CL-OS Concierge Server2 OpenScape Concierge V5R0	Secured connection with OS Concierge Server.
Measures	• Replace the default certificate by a CA signed one.
References	
Needed Access Rights	OS Concierge administration
Executed	Yes: □ No: □ Deactivated: □

CL-OS Concierge Server2 OpenScape Concierge V5R0	Secured connection with OS Concierge Server.
Customer Comments / Reasons	

The OS Concierge Server uses the configured Cipher Suite of the Windows OS. The Cipher Suite is configured via the group policy (Key SSL Cipher Suite Order).

The default setting: OS Concierge uses the default group policy of the OS.

4.2 Connection to Mail Server

The server side OS Concierge Provider Service (CPS) connects as a client to a mail server. It uses SMTP to send status information to target accounts in case a component fails.

4.2.1 SMTP Interface

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.

The SMTP extension (ESMTP) provides a mechanism for e-mail clients to specify a security mechanism to a corporate e-mail server, authenticate the exchange, and negotiate a security profile (Simple Authentication and Security Layer, SASL) for subsequent message transfers. An authenticated logon to SMTP is provided through the “Auth-Login” mechanism.

SMTP can only be used with encryption when the used mail server supports that.

Default Settings:

SMTP communicates in plaintext and has no authentication. All SMTP transmissions are in clear text, and user names, passwords, commands and data can be easily read by anyone able to perform packet capture (sniffing) on the network.

CL-SMTP1 OpenScape Concierge V5R0	SMTP Interface secured.
Measures	• Use authentication mechanisms at the SMTP server (for configuration of Concierge on OS Concierge Server see [6] • Select secure communication (TLS protocol or VPN tunnel – see section 6.4) between SMTP server and OS Concierge
References	
Needed Access Rights	OS Concierge administration
Executed	Yes: □ No: □ Deactivated: □
Customer Comments / Reasons	

CL-SMTP1 OpenScape Concierge V5R0	SMTP Interface secured.

4.3 Connection to MS Exchange

OS Concierge Server's external calendar node connects to the external MS-Exchange Server to read calendar entries. It communicates with the Exchange server over Exchange Web Services by using HTTP/S protocol. The customer site Exchange server has an account that is used by the OS Concierge Server. Additionally, it is possible to use integrated or form based authentication.

The following calendar systems are supported:

- Exchange 2013/2016/2019 via EWS

NOTE: The authentication protocols supported are Kerberos, NTLM, and OAUTH. For more details about Kerberos Authentication, please verify item **6.4.9 of OpenScape Concierge V5R0 Plus and Professional Administrator Documentation** and consult the respective documentation from Microsoft.

4.3.1 EWS (Exchange Web Services)

Default Settings

The EWS communicates in plaintext. Authentication is done by username and password. The authentication uses basic authentication.

CL-EWS1 OpenScape Concierge V5R0	EWS Interface secured.
Measures	• Activate HTTPS for EWS (see Concierge configuration [6]) • Communicate with EWS in a VPN tunnel between the MS-Exchange server and OS Concierge (see section 6.4)
References	
Needed Access Rights	Exchange administration, OS Concierge administration
Executed	Yes: □ No: □ Deactivated: □
Customer Comments / Reasons	

4.4 Connection to LDAP Server

The server side search node of the OS Concierge Server performs searches in external LDAP Server as a client. Also, the Contact Data Provider of OS Concierge Server can connect to external LDAP Server as a client to create and maintain the concierge telephone book. Information about internal contacts, email addresses and telephone numbers will be transmitted.

4.4.1 LDAP Interface

Lightweight Directory Access Protocol (LDAP) is a protocol that queries information from a directory service. It is a simplified version of the Directory Access Protocol (DAP), which was defined in the X.500 standard.

Authentication in LDAP works as follows:

1. Simple bind:
   - The client authentication at the server works with a distinguished name (DN).
   - It is also possible to use the DN and a password. The password is transmitted in plain text.
   - The password can also be encrypted.
2. Anonymous bind:
   - Here the DN and the Password field are empty.

Default Settings

LDAP communicates in plaintext. Authentication is not used (anonymous access).

CL-LDAP1 **OpenScape Concierge V5R0**	**LDAP Interface secured (client side)**
Measures	• If LDAPS is not possible, limit accessible data on LDAP server as much as possible. • If LDAPS is not possible, communicate with LDAP in a VPN tunnel between the external LDAP server and OS Concierge (see section 6.4) • Switch on authentication mechanisms at the LDAP server • Activate LDAPS to communicate with the external LDAP server (for configuration see [5] and [6])
References	
Needed Access Rights	LDAP administration, OS Concierge administration
Executed	Yes: □ No: □ Deactivated: □
Customer Comments / Reasons	

4.5 Connection to DNS Server

OS Concierge uses DNS SRV to locate available CSTA and SIP services. If the deployment is designed with geo-separated OSVs, DNS SRV is used to transmit which of the OSV nodes is primarily used by the agents.

4.5.1 DNS SRV Interface

The DNS SRV mechanism extends the normal DNS. The response could be manipulated.

Default Settings

DNS SRV communicates in plaintext. Authentication is not supported by DNS (anonymous access).

CL-DNS SRV1 **OpenScape Concierge V5R0**	**DNS SRV Interface secured**
Measures	• Communicate with DNS in a VPN tunnel between the DNS server and OS Concierge (see section 6.4)
References	
Needed Access Rights	Windows administration
Executed	Yes: □ No: □ Deactivated: □
Customer Comments / Reasons	

4.6 Connection to PABX

PABX Link Connector makes connections available over different interfaces to the OS Concierge Server and the OS Concierge clients.

Computer-supported telecommunications applications (CSTA) provide an abstraction layer for telecommunication applications, which is independent of underlying signaling protocols and independent of devices. The objective of CSTA is to develop and refine a standardized CTI (Computer Telephony Integration) interface to provide third party interactions between computer applications and the telecommunications network.

4.6.1 CSTA Interface

CSTA is used between OS Concierge and PABX to transmit subscriber events. Information about who calls whom and other events are transmitted. In case of an H4k, the data is transmitted over the CSTA ANSI protocol which is not human readable. If an OSV is used, the data is transmitted over XML statements.

OpenScape Concierge V5R0 server must be in the same internal IP network as the CSTA communication partner (i.e. the PBX). Protection of this internal network through an external firewall is required due to unencrypted usage of CSTA interface. Access to this network is restricted to authorized network administrators. In addition to firewall configuration, usage of IP Sec between OpenScape Concierge V5R0 and CSTA communication partner should be considered.

Default Settings

CSTA doesn't support authentication and encryption.

CL-CSTA1 **Sample Product Vxy**	**Protect infrastructure for CSTA**
Measures	• Keep OpenScape Concierge V5R0 servers as listed above (CL-1) in the same internal network and protect it with a firewall. • Access to the internal network only for authorized persons and trusted devices • Usage of IPSec for CSTA Protocol (for VPN see section 6.4)
References	
Needed Access Rights	Windows administration
Executed	Yes: □ No: □ Deactivated: □
Customer Comments / Reasons	

4.7 Connection to MS SQL

OpenScape Concierge V5R0 accesses MS SQL as a client. Configuration data and runtime related data is stored and managed there. Connections to MS SQL shall support TLS encryption.

NOTE:
To enhance security, it is advisable to configure "Force Encryption" as "Yes" in the SQL Server Configuration Manager, found under Network Protocols, after installation. Additionally, it is recommended to install the latest security updates for SQL from Microsoft

NOTE:
Enabling the "Receive updates for other Microsoft products" option in Windows is highly recommended to ensure that SQL and other Windows components are always up to date with the latest versions.

CL-SQLDB-CONN1 **OpenScape Concierge V5R0**	**SQL connection secured**
Measures	• Connection to ConfigDB and OSCADM is encrypted. • All OS Concierge components support encrypted database connections.
References	http://support.microsoft.com/kb/316898 http://msdn.microsoft.com/en-us/library/ms191192(v=sql.110).aspx#ConfigureServerConnections
Needed Access Rights	Database administration, OS Concierge administration
Executed	Yes: □ No: □ Deactivated: □
Customer Comments / Reasons	

NOTE: Some Windows versions are still using the unsafe Cipher called "`TLS_RSA_WITH_3DES_EDE_CBC_SHA`" including the SQL server, therefore it is recommended to disable this Cipher in the operational System. For more information, see the item 3.7.

4.8 Monitoring of device data via SNMP

Here the host side (e.g. Fault Management, Accounting Management) of the monitoring is described. For each monitored device the host has to be adapted to the SNMP possibilities of the monitored device. For the monitored device this sub section should be found in Administration 5.2.

This step is an administrative task, which is not performed once after installation but continuously during the operation of OpenScape Concierge V5R0 whenever new network elements are added for monitoring. It also involves the network elements themselves (see the security checklists of the monitored devices).

The Simple Network Management Protocol (SNMP) can be used for sending error messages from the monitored device to the SNMP server /host by trap. From the standard security point of view this is unproblematic.

If the SNMP server/host sends “get” or “set” advices to the monitored devices there is a risk for them. Thus in this case the SNMP interface should be configured more secure.

The OS Concierge Server supports only read-only access.

Details: see section 5.2.

4.9 Connection with OpenScape Contact Center

The Concierge Professional provides the possibility to enable the integration between OpenScape Concierge and Open Scape Contact Center (OSCC) through the OpenScape Concierge Contact Center Node.

4.9.1 Communication between OpenScape Concierge V5 Services and the OSCC Informix database

As there is a direct connection between OpenScape Concierge Server and the OSCC IBM Informix database, both Systems OpenScape Concierge Server and OSCC Server should reside in the same subnet protected by a firewall.

4.9.2 Communication between Concierge ConfigSync Server and OSCC Server

As there is a direct connection between the OpenScape Concierge ConfigSync Server and the OSCC IBM Informix database, it is also recommended to ensure that both systems (OpenScape Concierge Server and OSCC) are running on the same subnet and protected by a firewall.

4.9.3 Communication between Contact Center Node and OSCC Server

Any communication between OpenScape Concierge and other applications should be encrypted. Therefore, it is recommended to enable the enhanced security option in OpenScape Contact Center.

For more information consult the item “20.3.4 Configuring the enhanced security option from the OpenScape Contact Center Manager Administration Guide”.

NOTE:
No configuration is required on the OpenScape Concierge side. However, it is strongly recommended to keep the OpenScape Client updated in accordance with the OpenScape Contact Center.

5 Administration

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

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

These overall concepts are applied in the following three subsections.

Afterwards the hardening of specific protocols and products used for administration is handled.

5.1 System Access Protection

Every Unify product has a User Role Concept, where access privileges are assigned to user roles. Which roles are predefined in the product is depicted in the products documentation (see Administrator documentation [1]).

5.1.1 Password based Authentication

Fixed passwords are a serious security risk. In any case, individual and safe passwords must be used for all users. Every user shall only get those rights or roles, which are necessary for him (see 7.2 SF - Default Accounts).

System Management and Configuration Management have got the same password policy. In case of installation of Concierge, the installed Concierge Data Center uses same password policy, too.

CL Pwd1 **OpenScape Concierge V5R0**	**Overall customer specific password concept**
Measures	Rules for customer specific password handling are defined see 7.1SF - Password Policies. and applied for administration
References	
Needed Access Rights	Windows administration
Executed	Yes: □ No: □
Customer Comments / Reasons	

A new password has to be entered after the first start according to Password Policy (see section 7.1)

CL chgDefPwd **OpenScape Concierge V5R0**	**Change all default PW into customer individual passwords**
Measures	Implement individual passwords for • Predefined Users like Basic user, Advanced user, Expert user • Customer specific Users

CL chgDefPwd **OpenScape Concierge V5R0**	**Change all default PW into customer individual passwords**
References	
Needed Access Rights	Windows administration
Executed	Yes: □ No: □
Customer Comments / Reasons	

5.2 SF - Monitoring via SNMP

Here the side of the monitored device is described. OS Concierge can be monitored by using SNMP v2 or v3. SNMP version can be selected in System Management and v2 is default. For Software Subscription Licensing the OSV CMP analyses data from OS Concierge by using SNMPv1 or v2.

The Simple Network Management Protocol (SNMP) can be used for sending error messages from the monitored device to the SNMP server/host by trap. From the standard security point of view this is unproblematic.

If the SNMP server sends get or set advices to the monitored devices there is a risk for them. Thus, in this case the SNMP interface should be configured more secure. Details see below.

5.2.1 SNMP v2

In practical experience the SNMP v2c version from 1996 is used equivalent to SNMP v2. From the security point of view this version provides the same as SNMP v1.

Communities:

A community string is available in SNMP v2. It is comparable with a user ID or 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. Normally trap managers also make use of the community string.

Default is normally “public”.

Allowed Hosts:

The community string is transmitted in the form of clear text. Therefore, it can be eavesdropped easily. Thus, also IP addresses of systems that may contact the monitored system via SNMP shall be defined.

CL-SF: SNMPv1/v2 OpenScape Concierge V5R0	SNMP (v2c) security settings
Measures	• Set individual Community String name; delete default community string names. • Restrict hosts that may contact the monitored system by giving the hosts IP addresses
References	
Needed Access Rights	OS Concierge administration
Executed	Yes: □ No: □ Deactivated: □
Customer Comments / Reasons	

5.2.2 SNMP v3

This step is an administrative task, which is not performed once after installation but continuously during the operation of OpenScape FM whenever new network elements are added for monitoring. It also involves the network elements themselves. They have to be configured to use SNMPv3. Other SNMP versions should be deactivated.

New security aspects of SNMP v3:

SNMPv3 contains new Security models

- User-based Security Model (USM)
  - secure authentication
  - encrypted communication

- View-based Access Control Model (VACM)
  - Access Control for sub trees of MIB

Security targets (see. RFC 2571 and RFC 3411)

- Creation of a Security Model in Security Subsystem
- Target of SNMPv3-Frameworks is the protection against
  - The forgery of information
  - An un-allowed access
  - The manipulation of the message
  - The unwanted publication of information

Design of the User Security Model with the consideration of diverse security problems

- Change of information (data integrity)
- Masquerading (authentication of sender)
- Confidentiality of information (Disclosure, Data Confidentiality)
  - Replay-Attacks (Message Timeliness)

Agreement of required security parameters (definition security level)

- NoAuthNoPriv (no authentication, no encryption)
- AuthNoPriv (Authentication but no encryption)
- AuthPriv (Authentication and encryption). This is the recommended setting.

Two possibilities to restrict user Access (authorization)

- Lock access to sub trees of the MIB for user groups
- Restrict privileges (get, set, trap) to sub trees of the MIB for user groups.

CL-SF: SNMPv3 **OpenScape Concierge V5R0**	**SNMP (v3) security settings**
Measures	• Activate secure Authentication (thus no community string in SNMP v3) and configure passphrase in System Management • Activate Encrypted Communication • Define access classes for MIB sub trees
References	
Needed Access Rights	OS Concierge administration
Executed	Yes: □ No: □
Customer Comments / Reasons	

CL-SF: SNMPv3 OpenScape Concierge V5R0	SNMP (v3) security settings

5.3 Web Services (HTTP/S)

Web Services are offered by OpenScape Concierge V5R0:

- by the AutoUpdate of the OpenScape Concierge Client

HTTP is a clear text protocol and therefore target of all known attacks on such protocols. It is recommended to use additional security mechanisms and replace HTTP with HTTPS.

HTTPS means HTTP over a connection secured through TLS. The security strength of HTTPS depends heavily on which TLS cipher suite is negotiated, which kind of authentications is established (none, server only, client and server) and the strength of the certificates used for authentication.

NOTE:
For security purposes, it is crucial to encrypt all communication between the client and the server. As such, we highly recommend enabling the HTTPS protocol during automatic updates for the Concierge client. You can find instructions on how to do this in item 6.1.3.3 of the "Concierge Configuration Guide".

The default TLS certificate is self-signed and is not trusted. Install a valid certificate signed by a commonly trusted certificate authority. To be valid, the certificate must be:

- Signed by a trusted certificate authority
- Not expired.
- Having a common name that matches the host name of the web server, such as www.example.com.

CL-HTTP OpenScape Concierge V5R0	Secure Access to Web Services
Measures	- HTTPS only' is activated. - Cookies are disabled (recommended if HTTP is used)
References	
Needed Access Rights	OS Concierge administration
Executed	Yes: □ No: □
Customer Comments / Reasons	Describe measures taken:

6 Infrastructure

6.1 Secure LAN Design

The Security Checklist is a help for the secure configuration of the OpenScape Concierge V5R0 during the installation phase. The design phase of the customer network is before the installation phase. Thus, in fact rules for network design are not the focus of this document.

Practical experience has shown that it might be necessary to have information about a secure network design, because dependent on this network design communication connections have to be secured or not.

CL secure LAN Design OpenScape Concierge V5R0	Secure LAN Infrastructure
Measures	• Keep OpenScape Concierge Servers (Main server and Standby servers) in the same internal network, which is protected with a firewall. For Firewall configuration see IFMDB [12]. • Access to the internal network where OpenScape Concierge Servers are located, only for authorized persons and trusted devices.
References	
Needed Access Rights	Windows administration
Executed	Yes: □ No: □
Customer Comments / Reasons	

6.2 Protection of internal LAN Communications

For the internal IP network, the requirements according to the administrator documentation have to be met. Access to central components like switches and routers shall be restricted to technicians and administrators.

A logical or physical decoupling of voice and data network should be considered depending on the existing infrastructure. The IT service provider of the customer may have to be involved.

CL-VLAN **LAN infrastructure**	**Protect infrastructure**
Measures	• Access to routers and switches only for authorized persons and trusted devices • Use separate VLAN for voice communication (optional)
References	
Needed Access Rights	Windows administration
Executed	Yes: □ No: □
Customer Comments / Reasons	

6.3 LAN Interfaces and Ports – Firewall Concept

Interfaces, which are not used, shall be deactivated by default in the firewall and shall not be activated without explicit need. The ports used with OpenScape Concierge V5R0 can be found in the IFMDB (see [12]). This information may be used for external firewall configuration e.g. for network separation to increase security.

The firewall shall only those ports and IP addresses which are needed to enable communication between clients and servers.

6.4 VPN connection (IPSec based)

VPNs (virtual private network) also known as secure tunnel can be realized in different ways. Most used Mechanism to realize a VPN with IPSec (see [14]).

Many modern Operating systems contain components, with which a VPN can be built. Linux contains an IPSec implementation since Kernel 2.6. Elder kernel versions need the KLIPS-IPSec-Kernel module, by openswan.

VPN offers you:

- 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 remote access e.g. when an employee leaves the company.

In VPN, the encryption of data occurs via different security mechanisms such as IPSec tunneling, Security Associations and authentication methods (peer-to-peer, digital signatures).

IPSec is used to encrypt data and can generally be implemented with and without tunnels. IPSec is an option for implementing VPN. You can encrypt the entire IP packet here with the IP header: this occurs in tunnel mode.

Tunnels must always be configured for both VPN peers.

IPSec supports the automatic key management system, Internet Key Exchange (IKE). This is a standard that is integrated in IPSec.

CL-VPN1 OpenScape Concierge V5R0 external router	**Networking and remote access allowed via VPN only**
Measures	Recommended operation mode: • IKE(Internet-Key-Exchange-Protocol) "Main Mode" with Perfect Forward Secrecy and DH Group 2 / 5 (provides automatic key exchange management) (Default) • Encryption with AES (check setting in the VPN Client) A) Pre-shared Key (Recommended only for a limited number of devices) • Chose key word according to password recommendation (section 7.1 SF - Password Policies) • A secure transmission and storage of the key word has to be guaranteed. B) Certificates may be used for increased security requirements or with an existing PKI Infrastructure • Recommended operation mode: RSA and hash function with SHA-256 • Configuration is more complex (expert mode). Documentation of certificates and serial numbers and safe storage has to be guaranteed

CL-VPN1 OpenScape Concierge V5R0 external router	Networking and remote access allowed via VPN only
References	
Needed Access Rights	Windows administration
Executed	Yes: □ No: □ No network/remote access: □
Customer Comments / Reasons	Pre-shared key □ Certificates □

6.4.1 Remote agents

Remote agents shall be connected via VPN to protect confidentiality. With that, an encrypted tunnel is set up for communication. This can be done e.g. by an existing VPN Router.

CL-VPN3 LAN Infrastructure	Access for external subscribers only via VPN
Measures	• provide remote agents' tunnel by configuration of VPN router
References	
Needed Access Rights	Windows administration
Executed	Yes: □ No: □ No ext. subscriber: □
Customer Comments / Reasons	Shall remote agents' VPN be configured via VPN router?

6.4.2 SIP

A trunk is established between CPS (Concierge Provider Service) and PABX.

OS Concierge does support TLS for SIP.
OS Concierge does support SRTP.
VPN tunnel between PABX and OS Concierge servers can be used if additional security is required.

CL- VPN4 **OpenScape Concierge V5**	**Signaling and Payload Encryption**
Measures	• Use VPN tunnel between PABX and OS Concierge Servers
References	
Needed Access Rights	Windows administration
Executed	Yes: □ No: □
Customer Comments / Reasons	

7 Addendum

7.1 SF - Password Policies

The Unify Password Policy depicted in https://hisat.global-intra.net/wiki/index.php/General_Security_Requirements is recommended for/from Unify products.

The OpenScape Concierge system does not enforce a password policy for the accounts that are created for the OpenScape Concierge system.

It is the responsibility of the customer to ensure that any passwords that are created are as secure as possible and are changed periodically. We recommend adhering to the password policy guidelines described in section 7.1.1 PW Policy supported by OpenScape Concierge V5R.

7.1.1 PW Policy supported by OpenScape Concierge V5R0

All rules that are required by Service foundation Security are marked with SF. Please enter the agreed password policy in the last column of the table below.

	Password policy for OpenSsape Concierge V5	Password Default value	Customer setting
1	Minimal PW Length	8 SF[1]	
2	Maximal PW Length	16	
3	Minimal number of upper-case letters	1 SF[2]	
4	Minimal number of lower-case letters	1 SF	
5	Minimal number of numerals	1 SF	
6	Minimal number of special characters	1 SF[3]	
7	Maximal number of repeated characters	3 SF	
8	Maximal number of sequential characters	3 SF	
9	Account name (reversed too) may not be part of password	True	
10	Use blacklist of strings which may not be contained in password	False	
11	Minimum character count for changed characters	4 SF	
12	Password History	5 SF[1]	
13	Maximum password age standard in days	90 SF[1]	

[1] For SF there is a differentiation of the default value for regular users, admin accounts, service accounts, super users, computer system accounts and windows domain admins. Details see Implement Security checklist.

[2] For SF only 3 rules from Rule 3 to Rule 6 have to be fulfilled

[3] For SF not allowed are $ % blank (" ") and “Umlaute” that are Ö Ä Ü ü ä ö and other non-standard letters

[4] For SF: not allowed are words found in dictionaries, no typical PW as Birthdays, car license numbers, names…

[5] For SF: no patterns on the display

7.2 SF - Default Accounts

Here the Default Accounts for the OpenScape Concierge V5R0 inclusively user accounts of systems that can access OpenScape Concierge V5R0 are listed. This includes user accounts as well as machine accounts that are used for authentication between SW applications.

After the installation for each account, a default password is available.

IMPORTANT

Since the default PW 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.

7.2.1 OpenScape Concierge V5R0 accounts

	User Name	Necessary privileges	PW Policy configured	Unify Default PW (to be changed immediately)	Description
1	systemmanager	System management	Yes, as agreed in section 7.1	manager	Account of the System Management application
2	default\manager	Tenant management	Yes, as agreed in section 7.1	manager	Default account of the Configuration Management application, if no tenant is configured
3	<tenant-name>\ manager	Tenant management	Yes, as agreed in section 7.1	manager	Default account of the Configuration Management for each configured tenant. “<tenant-name>” is to replace by configured name of tenant.

	User Name	Necessary privileges	PW Policy configured	Unify Default PW (to be changed immediately)	Description

7.2.2 Windows Server 2019/2022 R0 Accounts Server OpenScape Concierge

Operating System normally is not delivered with the Unify System, thus in most cases we don't have default passwords.

	User Name	Necessary privileges	PW Policy configured	Unify Default PW (to be changed immediately)	Description
1	Administrator	Windows administration	see section 7.1		Default administrator account, shall be re-named during the OS hardening procedure.
2	CoCUSER	Windows administration	see section 7.1		Used to start application critical services (MDC, call center node) and to connect to SQL server.
3	SvcRSPSSH	Windows administration	see section 7.1		Used for file transfer, log data in context of SSDP.

7.3 SF - Certificate Handling

A certificate guarantees the ownership of e.g. a public key to a person or organization.

OpenScape Concierge V5R0 supports certificate handling for accessing Reporter application by internet browsers. To use this feature, on IIS a certificate for server authentication and on internet browsers the appropriate chain of certificates has to be installed for verifying it.

7.4 Protection Against DLL Injection

The OpenScape Concierge includes a robust DLL injection prevention system that alerts the user when a potentially hijacked DLL is being executed. If the Concierge identifies a possibly malicious DLL, please verify the DLL’s safety by running a trusted antivirus scan.

8 References

[1] OpenScape Concierge V5R0 Administrator Documentation available via e-Doku or Partner Portal (SEBA)/ product information
http://www.unify.com/us/partners/partner-portal.aspx

[2] OpenScape Concierge V5R0 Server Setup
available via E-Doku or Partner Portal (SEBA)/ product information
http://www.unify.com/us/partners/partner-portal.aspx

[3] OpenScape Concierge V5R0 Client Setup
available via E-Doku or Partner Portal (SEBA)/ product information
http://www.unify.com/us/partners/partner-portal.aspx

[4] OpenScape Concierge V5R0 Release Notes
available via E-Doku or Partner Portal (SEBA)/ product information
http://www.unify.com/us/partners/partner-portal.aspx

[5] OpenScape Concierge V5R0 Configuration Applications
available via E-Doku or Partner Portal (SEBA)/ product information
http://www.unify.com/us/partners/partner-portal.aspx

[6] OpenScape Concierge V5R0 Configuration Concierge
available via E-Doku or Partner Portal (SEBA)/ product information
http://www.unify.com/us/partners/partner-portal.aspx

[7] OpenScape Concierge V5R0 Trouble Shooting
available via E-Doku or Partner Portal (SEBA)/ product information
http://www.unify.com/us/partners/partner-portal.aspx

[8] 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

[9] Unify Security Advisories
http://www.unify.com/us/partners/partner-portal.aspx
-> sell -> document information -> search “security advisory”

[10] Security Policy - Vulnerability Intelligence Process,
https://networks.unify.com/security/advisories/Security_Policy_Vulnerability_Intelligence_Process.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] Creating a VPN connection
http://technet.microsoft.com/en-us/library/cc726062%28v=ws.10%29.aspx

mitel.com