UNIFY **Harmonize** your enterprise

OpenScape Cordless IP V2 Security Checklist

Planning Guide

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.

unify.com

Contents

Contents

1 Introduction

1.1 History of Change

Date	Version	Description
2017-12	0.1	First Draft for OpenScape Cordless IP V2

1.2 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.

Figure: Usage of Security Checklists (SCL)
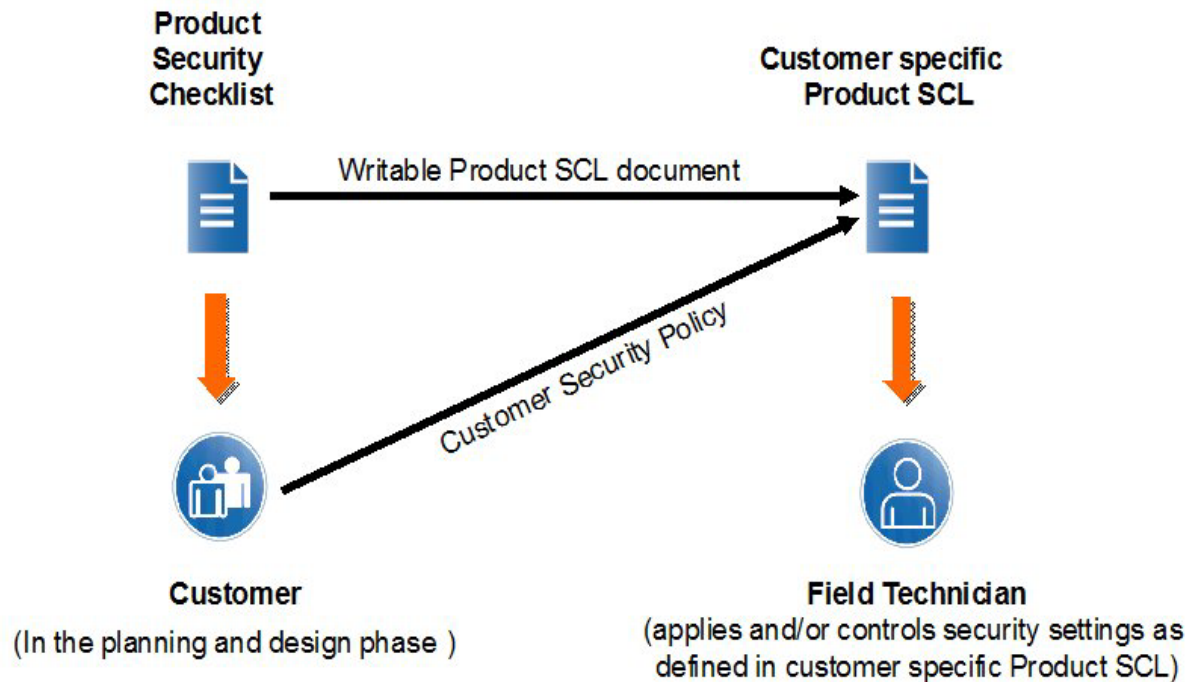
Update and Feedback

- 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 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 .

  They can be retrieved from the Unify partner portal http://www.unify.com/us/partners/partner-portal.aspxfor 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 (obso@unify.com).

1.3 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, analyse and resolve security vulnerabilities that emerge after products have been released, and to deliver guidance to customers how to mitigate or close these vulnerabilities.

Figure: Unify Baseline Security Policy- from Design to EOL
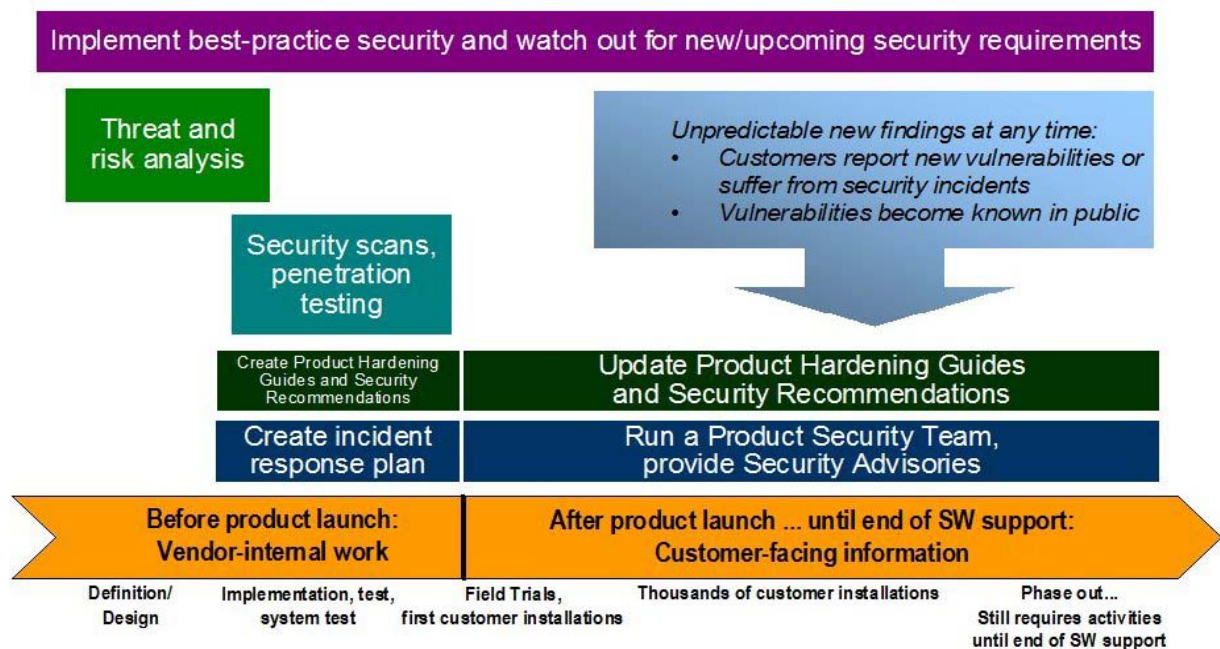
For more information about the Unify product security strategy we refer to the relevant Security Policies [1] and [2] in chapter 11 References.

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.

1.3.1 Security Implementation Checklist

The purpose of the Implementation Security Checklist is to assure that solutions that are being implemented in a secure way. The objective is to implement at least

fundamental security measures as part of the implementation of the whole solution.

Complementary the Product Security Checklists are issued for individual products which provide the complete collection of measure to secure each individual product. It's up to the individual customer to decide which of the Product SCL measures are appropriate within the respective project.

1.4 Customer Deployment - Overview

This Security Checklist covers the entire product and lists the 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 Remark		
Open issues to be resolved until		
Date		

2 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 Cordless IP V2.

2.1 Hardening Procedures of OpenScape Cordless IP V2 in General

OpenScape Cordless IP V2 offers two different deployment options which have to be considered.

Deployment	No. of BSIP2	Description
Small Solution	1 ... 10	One to 10 base stations. One base station running with All in one mode (The device is a Integrator/DECT manager) All other base stations running in Base only mode (The device acts as base station)
Medium Solution	1 ... 60	One BSIP2 running in Integrator/DECT Manager role Up to 60 base stations running in Base only mode

Figure: OpenScape Cordless IP Small Deployment
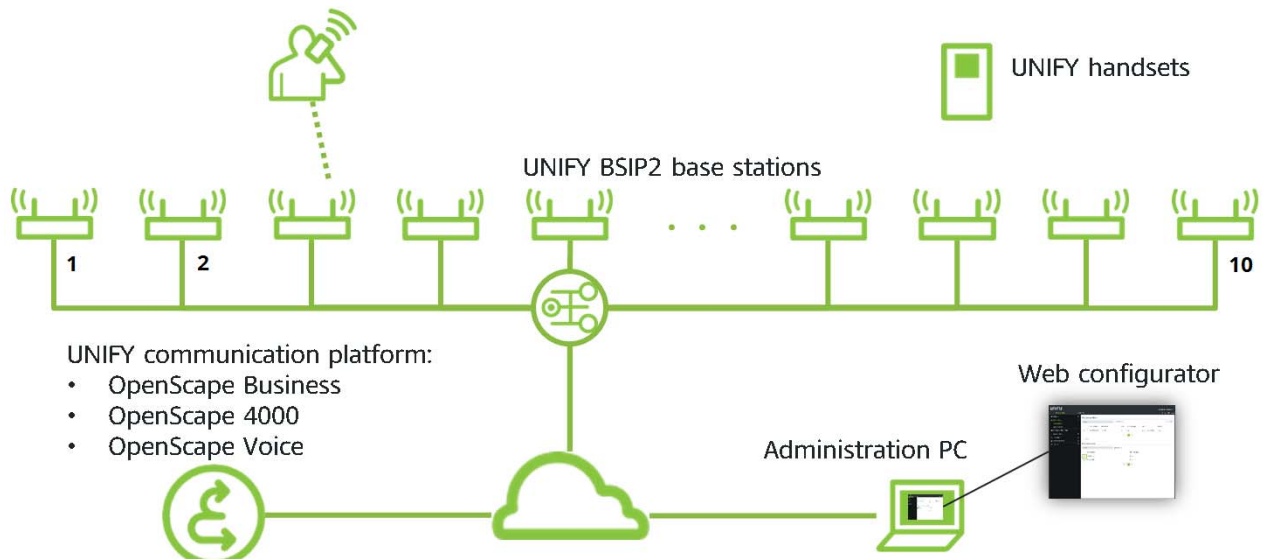
Figure: OpenScape Cordless IP Medium Deployment
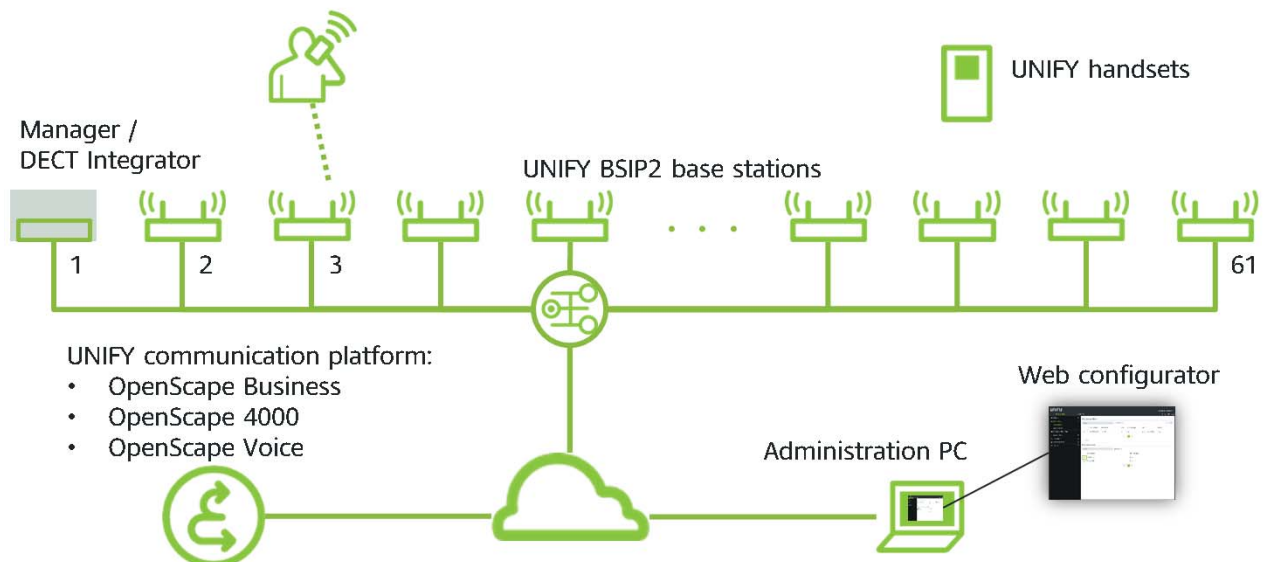
For safeguarding a OpenScape Cordless IP V2 solution all components have to be considered:

- Infrastructure (LAN, WAN)
  Physical and logical protection of the infrastructure against manipulation of features as well as sabotage

- OpenScape Cordless IP V2 system components
  Physical and logical protection of the system components against manipulation of features as well as sabotage.

- OpenScape Cordless IP V2 application
  Protection from unauthorized access and breach of confidentiality through individual passwords and protection of interfaces

- Administration PC
  Admission control by suitable password, provisioning with actual security updates, virus protection where required

- Subscriber terminals (e.g. DECT handsets):
  Access protection in case of absence, restriction of accessible phone numbers to protect against misuse and toll fraud

The recommended measures are listed in the following chapters.

2.2 Install latest (Up-to-date) Software

First point is to install only up-to-date software. The newest Software versions of software that is delivered by Unify always are available on Unify Software Server. We recommend to do also 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 (see [1] in chapter 11 References).

Table: CL-SW:

CL-SW: 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	See chapter "[System Update]" in OpenScape Cordless IP Administrator Documentation, [6] in chapter 11 References References Software Supply Server (SWS), see [5] in chapter 11 References		
OpenScape Cordless IP V2 (Medium Solution)			
Central Components	n/a		
Integrator (Update via **Settings** > **System** > **Firmware**)	Yes:	No:	Version

CL-SW: SW status All components	Up-to-date SW, SW that is delivered by Unify as well as additionally necessary Software.		
Base Stations (update automatically but should be checked in WBM: **Settings** > **Base stations** > **Administation**)	Yes:	No:	# of base stations checked
Administration PC components Operating System	Yes:	No:	Version
Browser	Yes:	No:	Type/Version
Customer Comments / Reasons			

INFO: Based on the SW installed, the necessary Patch management for the customer shall be defined.

Patch management is out of scope of this Product Security Checklist.

3 OpenScape Cordless IP V2

3.1 Connected PBX / VoIP Gateway / Communication Server

The terms "VoIP Gateway" and "PBX" are used as a synonym for the supported communication servers. The OpenScape Cordless IP system can be connected to the following communication servers:

- OSBiz:OpenScape Business
- OS4k: OpenScape 4000, OpenScape 4000
- OSV: OpenScape Voice

Please harden all products that are connected with OpenScape Cordless IP as the weakest product defines the security level of the whole system.

For details please refer to the Product Security Checklist of the concerned communication system (see [7] in chapter 11 References).

3.2 Connection to PBX / VoIP Gateway

The DECT subscribers of OpenScape Cordless IP the are represented by SIP users towards the PBX system.

OpenScape Cordless IP supports SIP over UDP or TCP. In that case the communication is not encrypted. Therefore the requirement from chapter 8.2.2 VoIP network separation and protection is essential.

In this case the communication between the Media Gateways has to be handled in same way as the connection to the PBX because it is not encrypted.

Therefore the requirements from chapter 8.2.2 VoIP network separation and protection are essential for the Media Gateway CrossLink Network too.

The best way is to place all Media Gateways and PBXs from one site in one separate network as described in 8.2.2 VoIP network separation and protection which is protected by a firewall.

3.3 Connection to DECT Network

3.3.1 DECT Network General

This network is solely used for the communication between the components of the OpenScape Cordless IP system (Integrator, DECT Manager) and the base stations (BSIP-Only). No Ethernet Layer3 components e.g. routers are allowed between components inside this network. For the DECT network, high requirements apply depending on the synchronization method used. As a minimum

requirement, a separate VLAN with highest priority (in case of LAN Synchronization) is required.

3.3.2 Synchronization via Ethernet (acc. IEEE 1588)

In contrast to an air based synchronization mechanisms, synchronization via Ethernet (acc. IEEE1588, PTP Precious Time Protocol) requires less configuration. The DECT network will be used for this synchronization mechanism.

The main advantages of synchronization via LAN are:

- more flexibility in the location of the DECT IP base station - no need to built synchronization chains as with synchronization via air,
- less DECT IP base stations may be required, because the overlapped area of DECT IP base station is less
- configuration of DECT IP systems is simplified, because all DECT IP base stations can be synchronized to only one synchronization master

On the other hand, great demands are made on the Ethernet characteristics like symmetry, packet loss, delay, jitter (variance of delay), … Therefore special requirements regarding the Ethernet components (especially the Ethernet switches used) have to be considered.

Exceeding of limits (especially of jitter) will lead to loss of synchronization, which will finally lead to a resynchronization process. During this resynchronization process the belonging Base Stations are unable to establish telephony connections.

To meet the special requirements regarding the network characteristics, it is strongly required to fulfil the requirements from chapter 8.2.3 DECT network separation and protection.

3.4 Connection to LDAP Server

The LDAP (Lightweight Directory Access Protocol) feature provides the phone user with the ability to query a centralized Directory Service (such as a Corporate Directory hosted on a remote LDAP server) and to display the directory entries that match the search criteria. It provides the user with a convenient method of finding and using telephone numbers.

The Directory Access feature does not support updating the central directory. The results of the queries are not stored persistently at the phone and queries have to be repeated if the data is needed again.

OpenScape Cordless IP uses an LDAP client to access a LDAP server (e.g. Built-in LDAP server of OpenScape Office or a Windows Directory Service) for phone book queries.

As OpenScape Cordless IP does not support LDAPS, the LDAP server must be kept inside the separated, access restricted network segment where OpenScape Cordless IP is located.

If it is not possible to place the LDAP server and the OpenScape Cordless IP system within the same separate, access restricted network segment, LDAP protocol must not be used.

CL-Sys-LDAP	Disable LDAP to external LDAP Server
Measures	Disable LDAP when LDAP server is not located within the same separate, access restricted network segment as the OpenScape Cordless IP system.
References	WBM: **Settings** > **Online Directories** > **Corporate**
Needed Access Rights	WBM Administration (User: admin)
Executed	Yes: No:
Customer Comments / Reasons	

3.5 Monitoring via SNMP

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. Additionally a SNMP server can send get or set advices to the monitored device.

OpenScape Cordless IP supports only SNMP v2. 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 are "public" (read only; get) and "private" (read and write access; get, set). As the community string is transmitted in clear text it can be eavesdropped easily.

Since OpenScape Cordless IP does not support changing the default community names and does not support configuration of a white list for allowed hosts, the SNMP server/host must be kept inside the separated, access restricted network segment where is located and the firewall should block all accesses to the SNMP port from unknown hosts.

CL-Sys-SNMP	Usage of SNMP
Measures	Do not use SNMP when SNMP server/host is not located within the same separate, access restricted network segment as the OpenScape Cordless IP system.
References	WBM: **Settings** > **System** > **System log** > **SNMP manager address**
Needed Access Rights	WBM administation (User:admin)

CL-Sys-SNMP	Usage of SNMP	
Executed	Yes:	No:
Customer Comments / Reasons		

3.6 Connection to SIP Server

DNS (Domain Name System) is used by OSCIP when the domain name (FQDN) is set in the SIP Server configuration. The system performs a DNS query to resolve this name into an IP address.

Attackers can exploit DNS queries to cause instability to the system. In order to secure the system from this kind of attacks, real IP addresses must be used instead of domain names, when the SIP Server is not located within the same, access restricted network segment as the OpenScape Cordless IP system.

If only real IP addresses were configured in the system, the use of the DNS SRV (DNS Service Records) feature is not possible.

CL-Sys-DNS	Usage of DNS in SIP Server Configuration	
Measures	Set real IP addresses in all DNS and SIP server fields when the SIP server is not located within the same, access restricted network segment as the OpenScape Cordless IP system. The use of the DNS SRV feature is not possible.	
References	See: • **Settings** > **Network** > I**P** • **Settings** > **Provider** or **PBX profiles** in OpenScape Cordless IP Administrator Documentation, [6] in chapter 11 References	
Needed Access Rights	WBM Administration (User: UnifyAdmin)	
Executed	Yes:	No:
Customer Comments / Reasons		

4 OpenScape Cordless IP Radio (DECT)

The OpenScape Cordless IP solution is already equipped ex-works with a variety of technical security features that are designed to meet the most important national and international legal requirements as well as other quality, privacy and information security standards.

The main security aspects that are implemented in OpenScape Cordless IP are summarized in the following. Thanks to these security features, OpenScape Cordless IP can be safely deployed even in customer networks with high security requirements:

• Compliance with relevant security standards in the DECT environment.

• Security for device logins, authentication and the transmission of radio signals.

• Administration Security.

• Protection against eavesdropping for OpenScape Cordless IP multi-cell systems

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.

In order to make the operation of the OpenScape Cordless IP even more secure, the following measures are strongly recommended.

5 3rd Party Components

5.1 Desktop PC for Administration

The general requirements for all PCs/Servers which run communication clients and applications are:

- The operating system version is released for the communication software (see sales information guide).
- Current security updates are installed (see item CL-SW in chapter 2.2 Install latest (Up-to-date) Software).
- A suitable virus protection SW shall be installed and active. This is especially true for mail servers and Windows PCs.
- The access to the system is protected by passwords according to the password rules defined in chapter 9.1 Password Policies.

CL-3d-PC-Adm	Administration PC Operating System Hardening
Measures	The operating system is released for this purpose.
	Current security updates are installed.
	A suitable virus protection software is installed and active.
	Access is protected by passwords according to the password policies in chapter 9.1 Password Policies.
References	• Product Release Note • Chapter 9.1 Password Policies
Needed Access Rights	Administrator
Executed	Yes: No:
Customer Comments / Reasons	

5.2 Web Browser

Web browsers are available on many systems. They contain a complex and error-prone software. Because in many cases a browser is the entry point to the system the hardening of the browser is essential. Many browsers e.g. can detect malware in download files, disable access to known malicious websites, and force secure communication.

5.2.1 Browser Hardening according to CIS

Browsers that are used / recommended for the system:

- Mozilla Firefox
- Internet Explorer
- Google Chrome

5.2.2 Application specific Differences to CIS Browser Hardening

Currently there are no product specific browser hardening measures known; neither exceptions nor additions.

6 Administration

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

- Secure access to the administration interface (HTTPS protocol)
- System access protection (user authentication, ...)

These overall concepts are applied in the following subchapters.

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

6.1 Administration Interface (HTTP/S)

Remote administration of OpenScape Cordless IP is offered via web service for use with a web-based client.

HTTP is a clear text protocol and therefore target of all known attacks on such protocols.If the WBM is accessed via HTTP the brower is automatically redirected to HTTPS.HTTPS means HTTP over a connection secured through SSL/TLS.

A self-signed server certificate for HTTPS encryption is delivered by default. This has to be accepted as trusted by the administrator in the browser. Since the web-server certificate and its private key are part of the general installation package, each customer gets the same key material.

For server authentication and against man-in-the-middle attacks, an individual certificate is necessary, which relies on a root certificate authority. This enables the browser, used for administration, to set up a secure end-to-end connection with OpenScape Cordless IP administration web service. It is recommended to the customer to use his/her individual certificate.

CL-ADM-HTTPS	Secure Access to Administration Web Service
Measures	Upload customer certificate.
References	**System** > **Web configurator** > **Web security ceritificate** (Note: Only PEM format with Certificate and unencrypted key are suported)
Needed Access Rights	WBM Standard (User: admin)
Executed	Yes: No:
Customer Comments / Reasons	

6.2 System Access Protection

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

- Authentication of users (user name, password)
- Authorization (roles and privileges)

These overall concepts are applied in the following subchapters.

6.2.1 User Authorization

OpenScape Cordless IP V2R0 does not offer different user roles. For V2R1 it is planned to offer two predefined users (as V1).

Username	WBM Mode	
admin	Administration	Full access to WBM; more or changed configuration options are available.

6.2.2 Password based Authentication

Fixed (default) passwords are a serious security risk. In any case, individual and safe password must be used for all users. After a new installation or a factory reset, the user is forced to change the password. This should be done according to the password policy (chapter 9.1 Password Policies).

CL-PW-Unify	Change Default Password for User "Unify"	
Measures	The default password for the WBM user "admin" must be changed.	
References	Password policy (chapter 9.1 Password Policies) Chapter default accounts (see 9.2 Default Accounts)	
Needed Access Rights	WBM Standard (User: admin)	
Executed	Yes:	No:
Customer Comments / Reasons		

6.3 SSH Interface

The Secure Shell interface (SSH) is reserved for technical specialists.It should only be activated for diagnosis purposes and a secure password according password policy should be chosen in (WBM: **Settings** > **System** > **Web Configurator** > **CLI access via ssh**).

7 Diagnostics

7.1 Logging

There are different stages of logging, which all should be considered. The syslog protocol is not encrypted and may contain sensitive information.

Therefore it is essential to keep the syslog server and the OpenScape Cordless IP system within the same separate, access restricted network segment. If this is not possible, syslog service must not be used.

CL-Log-IWU	Logging on IWU
Measures	Keep the syslog server within the same separate, access restricted network segment as the OpenScape Cordless IP system otherwise syslog service must be de-activated.
References	WBM: **System** > **System log** > **[] Activate system log**
Needed Access Rights	WBM Standard (User: admin)
Executed	Yes: No: De-activated:
Customer Comments / Reasons	

8 Infrastructure

8.1 Secure LAN Design

The Security Checklist is a help for the secure configuration of the OpenScape Cordless IP during the installation phase. The design phase of the customer network is before the installation phase. Thus in fact rules for the 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-LAN-SEC	Secure LAN Infrastructure
Measures	Keep OpenScape Cordless IP server and the corresponding communication system (e.g. OpenScape Voice,.) in the same separate, access restricted network segment, which is protected with a firewall. For Firewall configuration see port table in 9.3 Port Table
	Access to the separate, access restricted network segment where OpenScape Cordless IP server is located, only for authorized persons and trusted devices.
References	Chapter 1 and 2 in OpenScape Cordless IP Administrator Documentation, [6] in chapter 11 References
Needed Access Rights	IT service provider / Network administrator
Executed	Yes: No:
Customer Comments / Reasons	

8.2 Protection of internal LAN Communications

For the separate, access restricted network segment, 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.

The OpenScape Cordless IP internal infrastructure networks have to operate only within trusted environments.

8.2.1 Protection of LAN infrastructure

To assure the protection of the internal LAN communication the access to central components like switches and routers shall be restricted to technicians and administrators.

CL-LAN-PROT	Protect LAN Infrastructure
Measures	Access to routers and switches only for authorized persons and trusted devices.
References	
Needed Access Rights	IT service provider / Network administrator
Executed	Yes: No:
Customer Comments / Reasons	

8.2.2 VoIP network separation and protection

For the VoIP network, common requirements for a "VoIP ready" network apply. These networks have to be separated from other traffic by means of a specific VLAN.

To assure a logical or physical decoupling of voice and data network depending on the existing infrastructure a separate IP network or a dedicated VLAN should be used for the voice communication network. The voice communication network is the network between the PBX or the VoIP Gateway and the OpenScape Cordless IP system. The connection between base stations of the OpenScape Cordless IP system must also considered as voice network and should be handled in the same manner.

The communication related network should be protected by a firewall (see chapter 8.1 Secure LAN Design and chapter 8.3 LAN Interfaces and Ports - Firewall Concept).

CL-LAN-VoIP	Protect VoIP Network Infrastructure
Measures	Use separate IP network or VLAN for voice communication .
References	Chapter 4.5.1 "General Network Configuration" in OpenScape Cordless IP Administrator Documentation, [6] in chapter 11 References
Needed Access Rights	IT service provider / Network administrator

CL-LAN-VoIP	Protect VoIP Network Infrastructure	
Executed	Yes:	No:
Customer Comments / Reasons		

8.2.3 DECT network separation and protection

For the DECT network, higher requirements apply depending on the synchronization method used. As a minimum requirement, a separate VLAN with highest priority (in case of LAN Synchronization) is required.

To assure a logical or physical decoupling of voice and data network depending on the existing infrastructure a separate IP network or a dedicated VLAN should be used for the OpenScape Cordless IP system internal DECT network. The DECT network is the network between the OpenScape Cordless IP Media Gateway (BSIP-IWU) and the DECT base stations.

CL-LAN-DECT	Protect DECT Network Infrastructure	
Measures	Use separate IP network or VLAN for DECT network (communication between DECT base stations).	
References	Chapter 4.5.1 "General Network Configuration" in OpenScape Cordless IP Administrator Documentation, [6] in chapter 11 References	
Needed Access Rights	IT service provider / Network administrator	
Executed	Yes:	No:
Customer Comments / Reasons		

8.3 LAN Interfaces and Ports - Firewall Concept

Interfaces, which are not used, are deactivated by default and shall not be activated without explicit need. The ports used with OpenScape Cordless IP can be found in the addendum (chapter 9.3 Port Table). This information may be used for firewall configuration e.g. for network separation to increase security.

8.4 VPN connection (IPSec based)

VPNs (virtual private network) also known as secure tunnel can be realized in different ways. Most used Mechanism to build a VPN is using IPSec.

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

In VPN, the encryption of data occurs via different security mechanisms such as IPSec tunnelling, 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.

8.5 Backup and Restore

Backup archives contain configuration files. Even user passwords for SIP registration and DECT PIN's are stored within the backup. For handling of such backups special care is required in terms of where to store and access rights.

It is recommended to store the backup archives on a separate storage medium (like USB memory stick) and keep it in a secure place (like a safe) or store the backup archives on an encrypted area of the administration PC.

CL-LAN-Backup	Safe keeping of backup archives
Measures	Define a concept where to store the backup files for safe keeping.
References	Chapter 4.3.1.2 "Backup Config" in OpenScape Cordless IP Administrator Documentation, [6] in chapter 11 References
Needed Access Rights	IT service provider / Network administrator

CL-LAN-Backup	Safe keeping of backup archives	
Executed	Yes:	No:
Customer Comments / Reasons		

9 Addendum

9.1 Password Policies

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 normally mandated by technical means. OpenScape Cordless IP technically does not support the enforcement of the password policies depicted in chapter 9.1.1 PW Policy recommended. Therefore the system administrator is responsible to fit these requirements for the administration accounts. Since there are no other user accounts these policies are not relevant for end users.

If the default values don't fit with the customer's password policy, the values the customer wants to be configured shall be depicted in chapter 9.1.3 PW Policy agreed for customers deployment.

> *IMPORTANT:* The administrator is responsible for changing the password regularly.**Password Expiration Days** or **Password aging** is not supported.

9.1.1 PW Policy recommended

This Table is based on Unify's general security requirements for PW Policy.

Password characteristic	Guideline
General	• Use different passwords for different accounts • Store administrative passwords securely (e.g. in a password safe application or a safe)
Complexity	Min. 1 character from each of the following categories: • Upper-case letters (A-Z) only ASCII/basic Latin letters • Lower-case letters (a-z) only ASCII/basic Latin letters • Digits (0-9) • Special character (except $, %, blank (" "))
Exclusions	• no umlauted letters (Ä,Ö,Ü,.. and other non-standard letters) • no words found in dictionaries • no typical passwords (e.g. birthdays, car license number, names, 1234567, …) • Password must be different from UserID • Limited number of same or sequential characters in a row (max. 3)
Length	Depending on account type (min. 8 characters)

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

9.1.2 PIN Policy recommended

This Table is derived from Unify's general security requirements for PW Policy.

PIN charac-teristic	Guideline
General	• Use different PIN for different purpose • Store administrative PINs securely (e.g. in a password safe application or a safe)
Complexity	Digits (0-9)
Exclusions	• no typical PINs (e.g. birthdays, phone numbers, 1234567, …) • no patterns on the keyboard or phone dial pad • Limited number of same or sequential characters in a row (max. 2)
Length	8 characters

9.1.3 PW Policy agreed for customers deployment

In the following table please insert the values that have been agreed with the customer for the PW Policy.

Password Policy Topic	Agreed Value
Minimal Length	
Minimal number of upper case letters	
Minimal number of numerals	
Minimal number of special characters	
Maximal number of repeated characters	
Maximal number of sequential characters	

9.2 Default Accounts

Here the default accounts for OpenScape Cordless IP are listed. After the installation for each account, a default password is available.

> *INFO:* 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 base on unchanged default passwords.

#	User Name	Privileges	Unify Default PW (to be changed immediately)	Description
1	admin	WBM Admin	admin	Full access to WBM; more or changed configuration options are available.

9.3 Port Table

The OpenScape Cordless IP port list is published in the Interface Management Data Base (IFMDB).

For latest updates of the OpenScape Cordless IP port tables refer to the Interface Management Database (IFMDB) with Unify intranet link directly:

https://apps.g-dms.com/ifm/php/php_ifmdb/scripts/login.php

or via

Partner portal (http://www.unify.com/us/partners/partner-portal.aspx , [3] in chapter 11 References)

-> support -> service tools -> IFMDB

10 Abbreviations

ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
ARI	DECT terminology: Access Rights Identity
BIOS	Basic Input/Output System
BRI	ISDN Basic Rate Interface
BSIP	DECT Base Station for Cordless IP
CD-ROM	Compact Disc – Read-Only Memory
CIS	Center for Internet Security (https://www.cisecurity.org)
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)
COTS	Commercial off-the-shelf
CSCm	Customer Site Components Modular (located at User on customer Side)
CSTA	Computer Supported Telecommunications Applications
DECT	Digital Enhanced Cordless Telecommunications
DISA	Defence Information Systems Agency
DoD	Department of Defence
DSL	Digital Subscriber Line
EIC	DECT terminology: Equipment Installer's Code
EOL	End of Life
FM	Fault Management
HCIP	OpenScape Cordless IP
HFA	OpenScape Feature Access
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol

IEEE	Institute of Electrical and Electronics Engineers
IEEE 1588	IEEE "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems" see PTP
IFMDB	Interface Management Data Base
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Secure Internet Protocol
iRMC	integrated Remote Management Controller
IWU	HCIP specific: Interworking Unit
ISDN	Integrated Services Digital Network
KLIPS	Kernel IPSec Support
LAN	Local Area Network
LDAP	Lightweight directory access protocol
LDAPS	Lightweight directory access protocol over SSL
MGW	HCIP specific: Short term for "Media Gateway" (HCIP Server in Media Gateway mode)
MGW-IWU	HCIP specific: Short term for "Media Gateway-IWU" (HCIP Server in Management Server mode)
MS	Mircrosoft
NAT	Network Address Translation
OS	Operating System
OSO	OpenScape Office (PBX system)
OSV	OpenScape Voice (PBX system)
OBSO	OpenScape Baseline Security Office
PBX	Private Branch Exchange
PIN	Personal Identification Number
PSTN	Public Switch Telephony Network
PTP	Precision Time Protocol -> IEEE 1588
PW	Password
QM	Qualtiy Management
RFC	Request for Comments
SCL	Security Checklist
SEBA	Unify Partner Portal

SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management
SPE	Signalling and Payload Encryption
SQL	Structured Query Language
SSDP	Smart Service Delivery Platform
SSH	Secure Shell
SSL	Secure Socket Layer
SSO	Single Sign On
STIG	Security Technical Implementation Guide
SW	Software
SWS	Software Supply Server
TAPI	Telephony Application
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TLS	Transport Layer Security
UC	Unified Communication
UCC	Unified Communication and Collaboration
UDP	User Datagram Protocol
UM	User Management
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VPN	Virtual Private Network
WBM	Web Based Management
WL	Wireless Phone by Unify
WLAN	Wireless LAN

11 References

[1] Unify Security Advisories

http://www.unify.com/us/partners/partner-portal.aspx

-> sell -> document information -> search "security advisory"

[2] Security Policy - Vulnerability Intelligence Process,

http://wiki.unify.com/images/c/ce/Security_Policy_-
_Vulnerability_Intelligence_Process.pdf

[3] Interface Management Database (IFMDB)

available via SEBA Partner Portal

http://www.unify.com/us/partners/partner-portal.aspx

[4] Center of Internet Security – Security Benchmarks

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

[5] Software Supply Server

http://sw-download.unify.com:8080/en/p_nav1.html

[6] Administrator Documentation

Document number: A31003-C1010-M100-*-76A9

available via e-Doku or Partner Portal (SEBA)/ product information

http://www.unify.com/us/partners/partner-portal.aspx

[7] Related Security Checklists, Planning Guides

available via e-Doku or Partner Portal (SEBA) / product information

http://www.unify.com/us/partners/partner-portal.aspx

- **OpenScape Business V1 Security Checklist, Planning Guide**
  Document Number: A31001-P1030-P101-*-76A9
- **OpenScape Office V3 MX/LX Security Checklist, Planning Guide**
  Document Number: A31003-P3010-P101-*-7620
- **OpenScape 4000 V7 and Affiliated Products Security Checklist, Planning Guide**
  Document Number: A31001-H3170-P100-*-7620,
- **OpenScape Voice V8 Security Checklist, Planning Guide**
  Document Number: A31003-H8080-P101-*-76A9