A MITEL
PRODUCT
GUIDE

Unify OpenScape Xpert

OpenScape Xpert V7R5
Security Checklist

Planning Guide

05/2024

A31003-X2075-P100-02-76A9

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:

1. **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
2. **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.

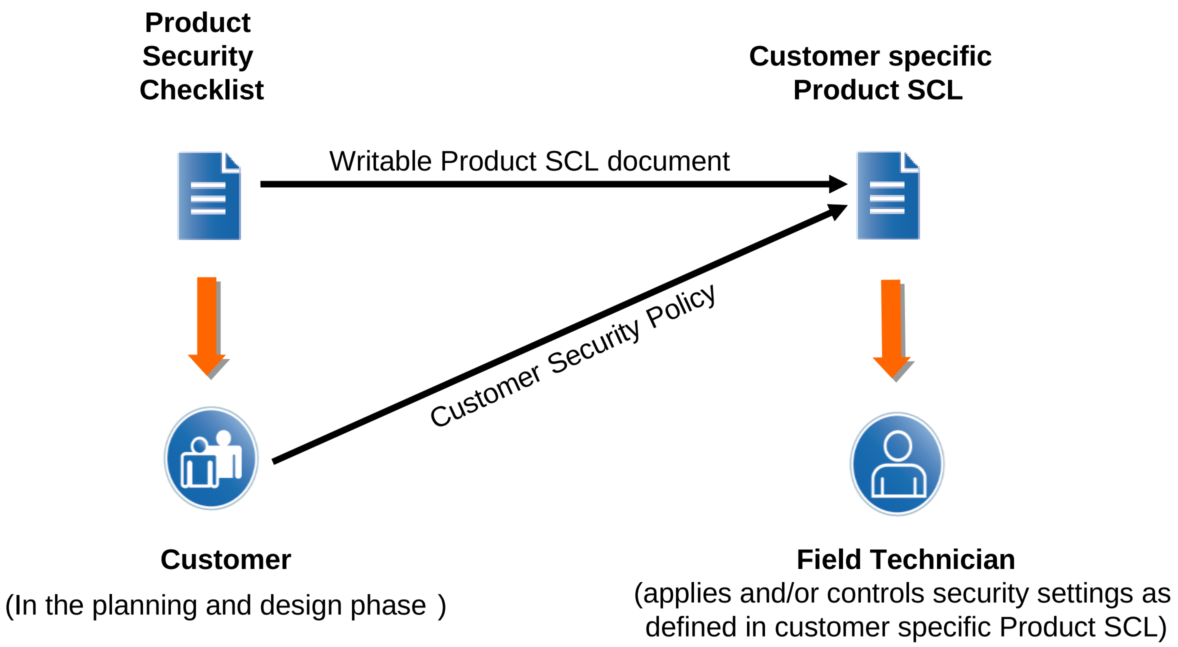
Product Security Checklist
Customer specific Product SCL
Writable Product SCL document
Customer Security Policy
Customer
(In the planning and design phase)
Field Technician
(applies and/or controls security settings as defined in customer specific Product SCL)

Figure 1: Usage of Security Checklists (SCL)

Update and Feedback

- By their nature, security-relevant topics are prone to continuous changes and updates. New findings, corrections and enhancements of this checklist are being included as soon as possible.
  Therefore, we recommend always using the latest version of the Security Checklists of the products that are part of your solution.
- 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).

1.2 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.

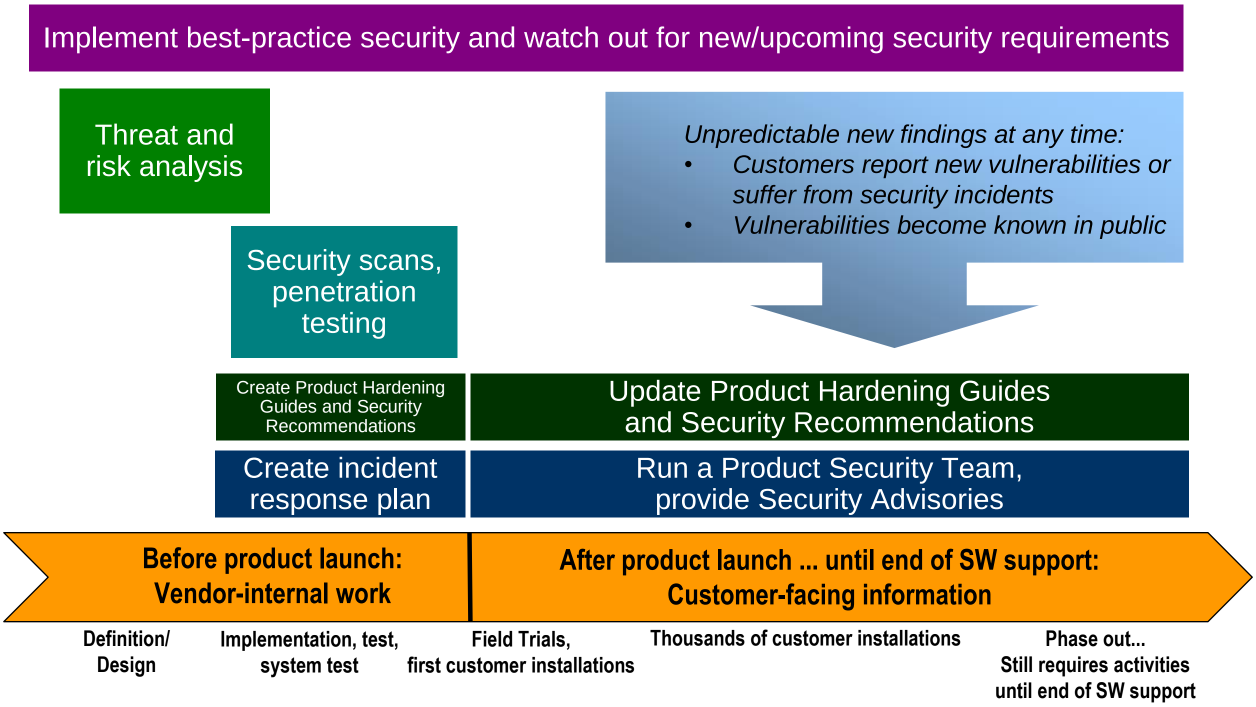
Implement best-practice security and watch out for new/upcoming security requirements
Threat and risk analysis
Security scans, penetration testing
Unpredictable new findings at any time:
• Customers report new vulnerabilities or suffer from security incidents
• Vulnerabilities become known in public
Create Product Hardening Guides and Security Recommendations
Update Product Hardening Guides and Security Recommendations
Create incident response plan
Run a Product Security Team, provide Security Advisories
Before product launch: Vendor-internal work
After product launch ... until end of SW support: Customer-facing information
Definition/ Design
Implementation, test, system test
Field Trials, first customer installations
Thousands of customer installations
Phase out... Still requires activities until end of SW support

Figure 2: Unify Baseline Security Policy - from Design to EOL

For more information about the Unify product security strategy we refer to the relevant Security Policies [3], [4], [5].

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. For OpenScape Xpert SM the Product Security Checklist is this document.

1.3 History of Change

Issue	Date	Summary
1	12/2022	First issue of the guide.
2	05/2024	Remove Center of Internet Security references.

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

2 Hardening Procedures in General

2.1 OSX Hardening

2.1.1 Disable Master password

Master password is sent to OSX clients with the configuration; therefore, its storage is not considered to be secure.

CL-DISABLE-MPWD	Disable Master password in SM
Measures	Master password should be disabled in the Management Portal
References	OpenScape Xpert Admin Help
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

2.1.2 Configure Call memory password

Call memory entries are part of the profile; therefore, it is protected by the profile credentials. Call memory password is just an additional layer: it protects accessing the Call memory entries on an unattended (but logged-in) profile.

Note: Call memory password is delivered with the profile to the client, its handling is not considered to be secure against high skilled hackers. The profile password protects the profile including the Call memory. Therefore, it is always recommended to log out or switch to Receive Calls Only mode when leaving the OSX client unattended.

CL- CALLMEMPWD	Enable Call memory password in SM
Measures	Call memory should be enabled in the Management Portal
References	OpenScape Xpert Admin Help
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

2.1.3 Use LDAP authentication for profiles

You can protect the profiles with a password that is stored (hashed) in the database. The option of assigning the profiles to LDAP users is also available; in this case the user credentials are stored wherever the LDAP server stores it (In a Windows environment typically, this place is the Active Directory). Because in this case the storage is out of the database, and often secured by the OS, it is considered more secure against some attacks. To make the LDAP traffic is encrypted, **configure LDAPS** as well.

CL-LDAP-PROF	Configure LDAP authentication for the profiles
Measures	Profile logins should be authenticated by the LDAP server using LDAPS.
References	OpenScape Xpert Admin Help
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

2.1.4 Change HTEMS certificates

Deploy HTEMS certificate according to the Service Manual to encrypt the traffic between SM, TT and MLC.

CL-HTEMS-CERT	Deploy certificates for HTEMS
Measures	Certificates are signed by organisation CA and deployed on SM, TTs and MLCs.
References	OpenScape Xpert Admin Help
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

2.1.5 Disable SHA1 signed certificate support

On OSXMP in System Properties/ Security tab the Accept SHA1 Algorithm for Certificate Signatures checkbox must be unchecked.

CL- DISABLE-SHA1	Disable SHA1 support
Measures	System Properties / Security tab / Accept SHA1 Algorithm for Certificate Signatures unchecked
References	OpenScape Xpert Admin Help
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐

Customer Comments / Reasons	

2.1.6 Configure OCSP validation for certificates

2.1.7 Enable/Disable unused interfaces on OSX Clients

If your setup does not absolutely require CTI, you should disable it. Same applies for the Thrift-based API, but here you have the option to enable TLS for it.

2.1.8 Harden OSX Client API interface

If the Thrift-based API of the OSX Client is enabled, it must be used with TLS. Therefore, on OSXMP in OSX Client properties, on the Interfaces tab at Thrift-based API group the Use TLS checkbox must be checked.

CL-OSXCLIENT-API	Check Use TLS on Interfaces tab of OSX Client properties
Measures	Use TLS is checked
References	OpenScape Xpert Admin Manual
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

Additionally, make sure to change deploy certificates as they are described in the Service Manual.

2.1.9 Configure Xpert Internal Communications Media Encryption

The voice data between OSX clients and MLC must be encrypted. Ensure the checkbox for Media Encryption (SRTP) is checked.

CL-INT-MEDIA-ENCRYPT	Enable media encryption (SRTP)
Measures	OSXMP / System Properties / Security tab / Internal Communication Setting / Media Encryption (SRTP) checked
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

2.1.10 Configure MLCs to use TLS for SIP

When the SIP proxy/registrar support it, enable TLS for SIP communication.

CL-SIP-TLS	Use TLS as SIP transport protocol
Measures	OSXMP / MLC / Connectivity / SIP Settings / SIP Transport Protocol is set to TLS
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

2.1.11 Enable full certificate check for SIP

TLS only provides real security if the certificates are valid. Enable full certificate validation for SIP connections in OSXMP.

CL-SIP-CERTCHECK	Enable full certificate check for SIP TLS connections
Measures	OSXMP / System Properties / Security tab / SIP Settings / TLS Authentication is set to FULL
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

2.1.12 Configure MLCs to use SRTP for Media Encryption

Unless a communication endpoint does not support it, enable SRTP for Media Encryption.

CL-MLC-SRTP	Use SRTP for voice data
Measures	OSXMP / MLC / Connectivity / SIP Settings / Media Encryption is set to SRTP
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

2.1.13 Configure Voice Recording to use secure communication

When Siprec is used for Voice recording ensure that secure communication channels are both set for SIP transport protocol (TLS) and Media Encryption (SRTP). This must be done on System Properties and in all Locations.

CL-SIPREC-ENCRYPT	Use TLS for SIP Transport protocol and enable media encryption
Measures	System Properties (Location) / Voice Recoding / SIP transport protocol is set to TLS and System Properties (Location) / Voice Recoding / Media Encryption is set to SRTP
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

2.1.14 Enable TLS for CSTA connections

When CSTA Line Monitoring is activated, enable TLS for CSTA connections unless the PBX does not support it.

CL-CSTA-TLS	Enable TLS for CSTA
Measures	OSXMP / System Properties / General tab / CSTA Settings / Use TLS for CSTA is enabled
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

3 System Manager Server Hardening

3.1 OSX System Manager Hardening

Each Windows server the OSX System Manager runs on shall be hardened. That may be more than one server in case of using the cluster feature of OSX.

Note: The cluster feature supports maximum 7 System Manager hosts in the OSX software version.

3.1.1 OS Hardening

Following OS is approved for the OpenScape Xpert System Manager server:

- Windows Server 2016 (64 bit)
- Windows Server 2019 (64 bit)

If the OS is not delivered by Unify, the hardening of the OS is up to the customer.

3.1.1.1 Updating SM OS with WSUS

The Windows 2016/2019 Standard Server 64 bit for SM can be updated via a WSUS server configured on the System Manager. For more information about WSUS in OSX environment please refer to the official OSX WSUS installation guide and the official WSUS site (see in References).

CL-SW status WSUS	**SW update executed**	
Measures	WSUS installed and configured.	
References	https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/plan/plan-your-wsus-deployment	
Needed Access Rights	Administrator	
SM1 (SMID):	Yes: ☐	No: ☐
SM2 (SMID):	Yes: ☐	No: ☐
SM3 (SMID):	Yes: ☐	No: ☐
SM4 (SMID):	Yes: ☐	No: ☐
SM5 (SMID):	Yes: ☐	No: ☐
SM6 (SMID):	Yes: ☐	No: ☐
SM7 (SMID):	Yes: ☐	No: ☐
Customer Comments / Reasons		

3.1.1.2 NLA for Remote Desktop

Turn on Network Level Authentication for Remote Desktops (or disable the Remote Desktop). This can be enabled in the group policy:

Network Level Authentication completes user authentication before you establish a remote desktop connection and the logon screen appears. This is a more secure authentication method that can help protect the remote computer from malicious users and malicious software.

CL-Windows NLA4RDP	**NLA is required**	
Measures	Set the following GPO to enabled on the domain controller: `Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\`**`Require user authentication for remote connections by using Network Level Authentication`**	
References	https://social.technet.microsoft.com/wiki/contents/articles/5490.configure-network-level-authentication-for-remote-desktop-services-connections.aspx	
Needed Access Rights	Administrator	
SM1 (SMID):	Yes: ☐	No: ☐
SM2 (SMID):	Yes: ☐	No: ☐
SM3 (SMID):	Yes: ☐	No: ☐
SM4 (SMID):	Yes: ☐	No: ☐
SM5 (SMID):	Yes: ☐	No: ☐
SM6 (SMID):	Yes: ☐	No: ☐
SM7 (SMID):	Yes: ☐	No: ☐
Customer Comments / Reasons		

3.1.1.3 SSL/TLS protocols and ciphers

MS supports a lot of SSL/TLS protocols and ciphers, several of them are outdated. These protocols are used in several Microsoft software such as Remote Desktop or IIS. Disable all the out-of-date protocols, such as:

- every SSL/TLS protocol before TLS 1.1
- RC4 ciphers
- any 64-bit block ciphers

You can disable them in the registry, but the easiest way of disabling them is using the free IIS Crypto GUI application from Nartac Software:

CL-Windows TLS Ciphers	**Old TLS protocols & ciphers are disabled**

Measures	Disable the above out-of-date TLS protocols and ciphers either through the registry or with the IIS Crypto GUI
References	https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel https://www.nartac.com/Products/IISCrypto/Download
Needed Access Rights	Administrator
SM1 (SMID):	Yes: ☐ No: ☐
SM2 (SMID):	Yes: ☐ No: ☐
SM3 (SMID):	Yes: ☐ No: ☐
SM4 (SMID):	Yes: ☐ No: ☐
SM5 (SMID):	Yes: ☐ No: ☐
SM6 (SMID):	Yes: ☐ No: ☐
SM7 (SMID):	Yes: ☐ No: ☐
Customer Comments / Reasons	

3.1.1.4 IP forwarding

IP Forwarding should be disabled on all SM hosts running Windows. By default, it is set to 0.

An attacker may use this flaw to route packets through this host and potentially bypass some firewalls/ routers/ NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

CL-Windows IP Forwarding	**IP forwarding disabled**
Measures	IPEnableRouter (IP forwarding) setting should be disabled on all SM hosts running Windows: On Windows, set the key 'IPEnableRouter' to 0 under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameter
References	http://technet.microsoft.com/en-us/library/cc962461.aspx
Needed Access Rights	Administrator

SM1 (SMID):
SM2 (SMID):
SM3 (SMID):
SM4 (SMID):
SM5 (SMID):
SM6 (SMID):
SM7 (SMID):
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐

Customer Comments / Reasons		

3.1.1.5 MS SQL Server uninstall on Windows Server

Sometimes Microsoft SQL server is preinstalled on Windows Servers. In that case the SQL Server must be uninstalled on all SM hosts.

CL-Windows SQL uninstall	CL-Windows SQL uninstall	
Measures	The SQL Server must be uninstalled on all SM hosts	
References		
Needed Access Rights	Administrator	
SM1 (SMID):	Yes: ☐	No: ☐
SM2 (SMID):	Yes: ☐	No: ☐
SM3 (SMID):	Yes: ☐	No: ☐
SM4 (SMID):	Yes: ☐	No: ☐
SM5 (SMID):	Yes: ☐	No: ☐
SM6 (SMID):	Yes: ☐	No: ☐
SM7 (SMID):	Yes: ☐	No: ☐
Customer Comments / Reasons		

3.1.1.6 Use firewall on the SM server

It is highly recommended to use the built-in firewall of Windows Server.

CL-SmFirewall	Configure a firewall on the SM
Measures	A firewall should be installed. The ports should be filtered
References	
Needed Access Rights	Administrator

SM1 (SMID):	Yes: ☐ No: ☐
SM2 (SMID):	Yes: ☐ No: ☐
SM3 (SMID):	Yes: ☐ No: ☐
SM4 (SMID):	Yes: ☐ No: ☐
SM5 (SMID):	Yes: ☐ No: ☐
SM6 (SMID):	Yes: ☐ No: ☐
SM7 (SMID):	Yes: ☐ No: ☐
Customer Comments / Reasons	

3.1.2 SM Installation hardening

3.1.2.1 Configuration HTTPS

Configure HTTPS (HTTP-Secure) according to the Service Manual to encrypt the traffic between the Wildfly server and the browser. Change the default self-signed certificate in https.keystore with the trusted CA signed certificate.

CL-HTTPS	Change self-signed certificates
Measures	The certificates in https.keystore is not the default installed certificates.
References	OpenScape Xpert Admin Help
Needed Access Rights	Administrator
SM1 (SMID):	Yes: ☐ No: ☐
SM2 (SMID):	Yes: ☐ No: ☐
SM3 (SMID):	Yes: ☐ No: ☐
SM4 (SMID):	Yes: ☐ No: ☐
SM5 (SMID):	Yes: ☐ No: ☐
SM6 (SMID):	Yes: ☐ No: ☐
SM7 (SMID):	Yes: ☐ No: ☐
Customer Comments / Reasons	

3.1.2.2 Use LDAPS authentication for OSXMP

The built-in Administrator account serves only for demonstration/marketing purposes, its credentials are not stored in a secure way and its password cannot be changed. Therefore, it must be disabled, and LDAP authentication must be configured as described in the Service Manual. LDAPS (Ldap - Secure) is highly recommended, since LDAP itself is a clear text protocol, and passwords are passed through it.

CL-LDAP-MP	Configure LDAPS authentication for MP
Measures	Login trials with the Administrator account should fail. Login with the configured LDAPS account should succeed. The LDAPS traffic between OSXMP and the LDAP server should be encrypted.
References	OpenScape Xpert Service Manual
Needed Access Rights	Administrator

SM1 (SMID):	Yes: ☐ No: ☐
SM2 (SMID):	Yes: ☐ No: ☐
SM3 (SMID):	Yes: ☐ No: ☐
SM4 (SMID):	Yes: ☐ No: ☐
SM5 (SMID):	Yes: ☐ No: ☐
SM6 (SMID):	Yes: ☐ No: ☐
SM7 (SMID):	Yes: ☐ No: ☐
Customer Comments / Reasons	

3.1.2.3 Change keystore fire default password

Change the default password of the .keystore file of Wildfly according to the Service Manual.

CL-KEYSTORE-PWD	Change default password of .keystore file
Measures	Wildfly .keystore password is changed. Wildfly service is restarted and the SM Administrator can login to the OSXMP.
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator
SM1 (SMID):	Yes: ☐ No: ☐
SM2 (SMID):	Yes: ☐ No: ☐
SM3 (SMID):	Yes: ☐ No: ☐
SM4 (SMID):	Yes: ☐ No: ☐
SM5 (SMID):	Yes: ☐ No: ☐
SM6 (SMID):	Yes: ☐ No: ☐
SM7 (SMID):	Yes: ☐ No: ☐
Customer Comments / Reasons	

3.1.2.4 Change Wildfly DB user default password

According to the Service Manual change the webuser password. It is saved into the vault.

CL-WILDFLY_DBUSERPWD	Change wildfly db user password
Measures	Password is changed. Wildfly restarted. SM Administrator login to OSXMP and save is successful.
Needed Access Rights	SM Administrator
References	OpenScape Xpert Service Manual

SM1 (SMID):
SM2 (SMID):
SM3 (SMID):
SM4 (SMID):
SM5 (SMID):
SM6 (SMID):
SM7 (SMID):
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐

Customer Comments / Reasons		

3.1.2.5 Set Activity Directory authentication for Database User (remote user)

According to the Service Manual activate the Active Directory authentication for Database user remoteuser.

CL-GSSAPI-REMOTEUSER	Activate GSSAPI plugin for remote user	
Measures	GSSAPI is activated for remote user. smdbtool commands can be executed	
References	OpenScape Xpert Service Manual	
Needed Access Rights	SM Administrator	

SM1 (SMID):
SM2 (SMID):
SM3 (SMID):
SM4 (SMID):
SM5 (SMID):
SM6 (SMID):
SM7 (SMID):
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐

Customer Comments / Reasons		

3.1.2.6 Change certificates for License Server

Deploy certificate according to the Service Manual to encrypt the traffic between System Manager Config Server and License Server.

CL-LIC-CERT	Deploy certificates for License Server
Measures	Certificates are signed by organisation CA and deployed on SM.
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator

SM1 (SMID):
SM2 (SMID):
SM3 (SMID):
SM4 (SMID):
SM5 (SMID):
SM6 (SMID):
SM7 (SMID):
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐

Customer Comments / Reasons		

3.1.2.7 Change certificates for Cluster DB replication

Deploy certificate according to the Service Manual to encrypt the traffic between System Managers Database Server.

CL-DB-CERT	Deploy certificates for Database Server	
Measures	Certificates are signed by organisation CA and deployed on SM.	
References	OpenScape Xpert Service Manual	
Needed Access Rights	SM Administrator	

SM1 (SMID):
SM2 (SMID):
SM3 (SMID):
SM4 (SMID):
SM5 (SMID):
SM6 (SMID):
SM7 (SMID):
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
	Yes: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐
		No: ☐

Customer Comments / Reasons		

4 MLC Server Hardening

4.1 OSX MLC Server Hardening

Each server the OpenScape Xpert - MLC runs on shall be hardened. That may be more than one server for distributed deployment of OpenScape Xpert – MLC and if so, the modifications should be applied on all servers.

General requirements for all PCs:

- The operating system version is released for the communication software (see sales information)
- Current security updates are installed (see chapter Hardening Procedures in General).

4.1.1 OS Hardening

The Multiline-Controller (MLC) should be installed on Debian 9 "Stretch" or on Debian 11 "Bullseye". In case of new installation, Debian 11 is hardly recommended. Install only the packages that are necessary for the MLC. Do not install any unnecessary software.

4.1.2 OS Update

The operating system should always be updated with the latest security updates.

The updates could be installed from the official Debian security repositories, for further information see http://www.debian.org/security/.

CL-MLC OS updates	OS updates are installed
Measures	all security updates are installed on MLC
Needed Access Rights	root
References	Debian security pages
Executed	Yes: □ No: □
Customer Comments / Reasons	

4.1.3 MLC hardening script

Run the prepared MLC hardening script (*/var/mlc/mlc.os.hardening.sh*). It disables the login with root accounts through ssh and sets up the following password policies:

- The password cannot contain the username or the reverse of the username
- The user can try to enter a password 3 times
- The minimum length of a password is 14 characters
- The number of characters that need to be different from the old password is 2
- At least 1 digit must be present in a password
- At least 1 other than digit character must be present in a password
- At least 1 upper case character must be present in a password
- At least 1 lower case character must be present in a password
- The maximum number of allowed consecutive repeating characters is 3
- The maximum number of allowed monotonic character sequences is 3
- The last 5 passwords will be remembered and cannot be reused
- The default blank password is not permitted
- The password is encrypted with SHA512

- A password will be valid for 90 days
- The user will be prompted of expiring password 14 days in advance
- These rules will be applied to all the new users and password as well as to the existing mlcadmin and mlcengr users
- An example password that fits all the policies: .2wsx3EDC4rfv5TGB

The passwords for the mlcadmin and mlcengr users are set to be expired. Although it is possible to change them on the next login, it is strongly advised to change at this time as from that point root login through ssh is not possible.

CL-MLC hardening Script	**MLC hardening script has run**
Measures	login with root is disabled. Password expiration is set to 90 days
Needed Access Rights	Root
References	Service manual in the Documents folder of the install CD.
Executed	Yes: ☐ No: ☐
Customer Comments / Reasons	

4.2 MLC Hardening

4.2.1 Install SIP certificate on MLC

To be able to use TLS as SIP transport protocol, install MLC certificates for SIP connection according to the Service Manual.

CL-SIP-CERT	Deploy certificates for SIP
Measures	Certificates are signed by organisation CA and deployed on MLCs
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator
Executed	Yes: ☐ No: ☐
Customer Comments / Reasons	

4.2.2 Install CSTA certificate on MLC

When CSTA Line Monitoring is enabled: to be able to use MTLS for CSTA connections, install MLC certificates for CSTA connection according to the Service Manual.

CL-CSTA-CERT	Deploy certificates for CSTA
Measures	Certificates are signed by organisation CA and deployed on MLCs
References	OpenScape Xpert Service Manual
Needed Access Rights	SM Administrator
Executed	Yes: ☐ No: ☐
Customer Comments / Reasons	

5 OSX Client Device Hardening

5.1 OSX Client Hardening

Each terminal device in OSX shall be hardened.

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

- The operating system version is released for the communication software (see sales information)
- Current security updates are installed (For Softclient: Windows security updates are installed, For OSX Client devices: the latest compatible OSX Client image is installed).

5.1.1 OS Hardening

The supported operating systems are:

- Debian V11 “bullseye” - only in case of OSX Client devices (🐧)
- Windows 10, 64 bit - only in case of Softclients (⊞)

In case of Softclients, the customer is responsible for hardening the computer and its OS.

5.1.1.1 Disable automatic VLAN discovery using LLDP-MED (OSX Client devices)

Automatic VLAN discovery using LLDP-MED feature must be disabled due to missing mandatory authentication.

Follow the Service Manual for configuration details.

CL-DISABLE-LLDP-MED	Disable automatic VLAN discovery using LLDP-MED
Measures	Dynamic VLAN assignment should not happen without mandatory authentication
References	Service manual
Needed Access Rights	Diagnosis Tool (+ttinstall)
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

5.1.1.2 Enable and configure Device Lock (OSX Client devices)

Plugging USB sticks and devices should be disabled as it is described in the Service Manual. Additional allowed devices can be configured.

CL-DEVICE-LOCK	Enable device lock
Measures	Plugging USB sticks/keyboards/mouse/etc should be unsuccessful
References	Service manual

Needed Access Rights	Diagnosis Tool (+ttinstall)
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

5.1.1.3 Configure Firewall according to customer requirements (OSX Client devices)

Unused services (CTI, TurretAPI, etc.) must be blocked in the firewall. Additional custom rules can also be set to accommodate unique site-specific security requirements.

Follow the Service Manual for configuration details.

CL-CONFIGURE-FIREWALL	Configure firewall
Measures	Unused services must be blocked in the firewall
References	Service manual
Needed Access Rights	root
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

5.1.1.4 Secure the BIOS (OSX Client devices)

Set up a BIOS password for both the supervisor and the user according to the password policy of your company.

Limit the User Access Level to [No Access] or [View Only].

Ensure that the correct storage device (CF card for N4, CFast card for N5, SSD for Incotel) is the first boot device.

Disable BBS popup if possible.

CL-CONFIGURE-BIOS	Configure BIOS
Measures	You will not be able to access the BIOS without a password. You can edit the BIOS settings only using the Supervisor password. You cannot boot from removable devices. The BBS popup option must not be available at startup.
References	Use the User Guide of the BIOS provider
Needed Access Rights	Local access for the BIOS
Configured	Yes: ☐ No: ☐
Customer Comments / Reasons	

6 References

[1] OpenScape Xpert Service Manual
OSX_Service_Manual_V7R1_Issue1.pdf in the Documents folder of the installation CD

[2] OpenScape Xpert Admin Help
OSX_Systemmanager_Help_V7R1.pdf in the Documents folder of the installation CD

[3] 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

[4] Support of Virus Protection Software for Server Applications
http://wiki.unify.com/images/2/21/Security_Policy_-_Support_of_Virus_Protection_Software_for_Server_Applications.pdf

[5] Secuity Policy - Vulnerability Intelligence Process,
http://wiki.unify.com/images/c/ce/Security_Policy_-_Vulnerability_Intelligence_Process.pdf

[6] Interface Management Database (IFMDB)
available via SEBA Portal
https://apps.g-dms.com/ifm/php/php_ifmdb/scripts/login.php

mitel.com