OpenScape Xpressions V7

Security Checklist

Planning Guide
03/2025

A31003-S2370-P102-17-7620

Mitel

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

Contents

History of Changes

Date	Changes	Reason
2012-06-12	REMOVED: Security Measures for SSH	–
2012-06-27	REMOVED: Security Measures for the Web Server according to CIS	–
2013-04-04	ADDED: Deviations from the OS Benchmarks for Microsoft Windows Server 2008	CQ00251551
2013-05-02	ADDED: New Security Measure for PostgreSQL Database.	CQ00258685
2016-11-24	ADDED: Protection against Toll Fraud	NA15149433
2016-12-05	UPDATED: Protection against Toll Fraud	review
2017-04-27	REMOVED: Deviations from the OS Benchmarks for Microsoft Windows Server 2003 ADDED: Deviations from the OS Benchmarks for Microsoft Windows Server 2012 and 2012 R2	UCBE-11165
2017-04-27	UPDATED: Protection against Toll Fraud	review
2017-05-19	ADDED: Security Measures for HTTPS	UCBE-11393
2019-09-23	UPDATED: Protection against Toll Fraud regarding NCO Locations for different Country Codes	UCBE-20959
2020-02-19-	UPDATED: 3.12 Security Measures for HTTP	UCBE-22124
2020-03-10	UPDATED: 3.1 Security Measures for the Server Operating System according to CIS	UCBE-19992
2021-12-07	ADDED: 6.1 End of life / End of support of Apache Tomcat server	UCBE-28858
2021-12-17	UPDATED: 6.1 End of life / End of support of Apache Tomcat server	UCBE-29002
2023-01-06	UPDATED: 4.1 Security Measures for PC Operating Systems	DOCLOC-6610
2024-04-24	UPDATED: 3.1 OS Hardening, 5.1 Virtualization Hardening, 5.2 Web Browsers Hardening, 5.3.1 Security Measures for the Microsoft SQL Database	DOCLOC-8565
2025-03-06	Updated: 5.1 Virtualization Hardening	DOCLOC-9418

1 General Notes

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

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

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

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

The Security Checklists can be used for two purposes:

1. **In the Planning and Design Phase of a particular Customer Project**

   Use the Security Checklists of every relevant product to evaluate, if all products that make part of the solution can be aligned with the customer’s security requirements – and document in the Checklist, how they can be aligned.

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

   - During installation/setup of the solution
   - During the operation

2. **During Installation and during major Enhancements or Software Upgrade Activities**

   The Security Checklists (ideally documented as described in step 1) are used to apply and/or control the security settings of every individual product.

Update and feedback

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

  Therefore, we recommend using always the latest version of the Security Checklists of the products that are part of your solution. They can be retrieved from the partner portal at the relevant product information site.

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

  Please contact the OpenScale Baseline Security Office.

1.1 Customer Deployment – Overview

This Security Checklist covers the product OpenScape Xpressions 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 resolved until		
Date		

2 Overview of OpenScape Xpressions

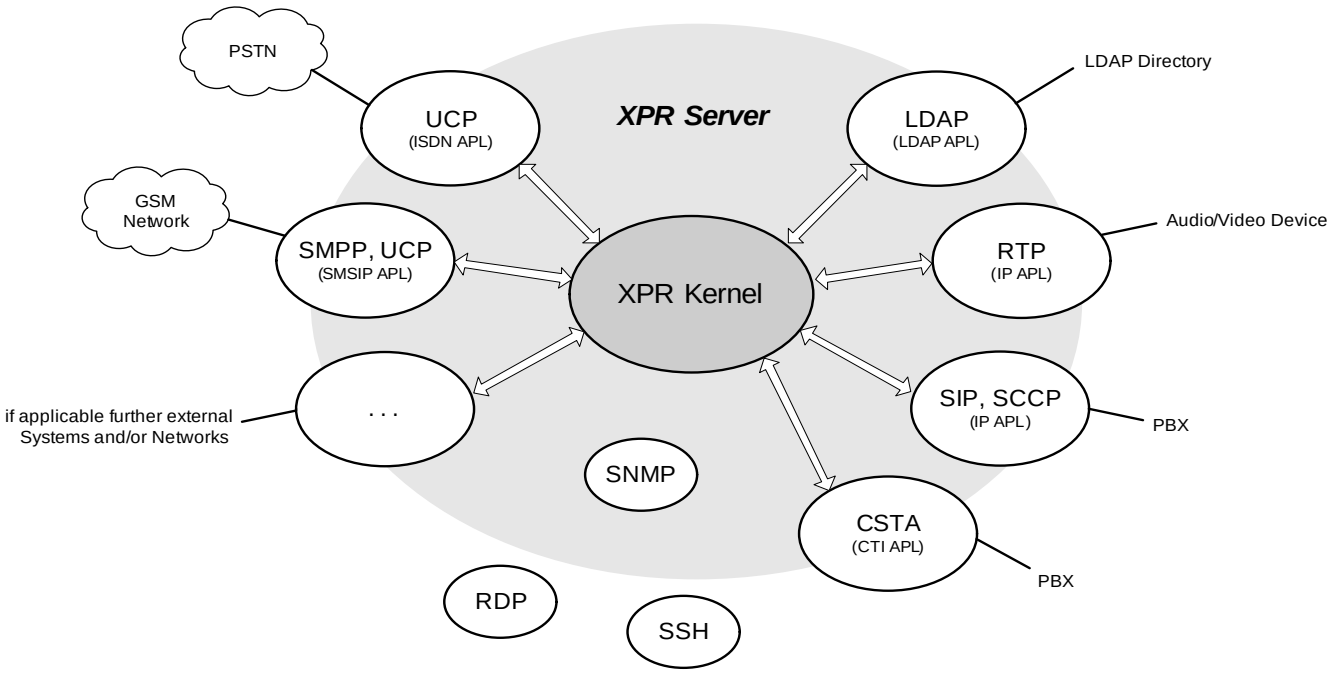
NOTE: This document only applies to OpenScape Xpressions as voice-only solution. Please follow chapter C *Configuring OpenScape Xpressions as Voice-only System* in the OpenScape Xpressions Server Installation manual to install OpenScape Xpressions as a voice only solution.

Central OpenScape Xpressions component is the XPR kernel.

Access to the XPR kernel is provided by different, optional Access Protocol Layers (APLs) that integrate protocols such as SIP, RTP or LDAP. These access protocol layers enable external systems or networks and OpenScape Xpressions to communicate with each other via the relevant protocols.

Furthermore, you can use default network protocols to access the computer system of OpenScape Xpressions – e.g. by means of the Remote Desktop Protocol (RDP) or Secure Shell (SSH).

Beyond that, OpenScape Xpressions can use SNMP implemented within the operating system.



The basic requirement for operating OpenScape Xpressions securely is that all OpenScape Xpressions components are operated with the latest software respectively.

Check-1		
Server components of OpenScape Xpressions		
OpenScape Xpressions	No	Yes
Client components of OpenScape Xpressions		
Web Assistant	No	Yes
Components by 3rd-party producers		
Server operating systems	No	Yes
Client operating systems	No	Yes
Web browser	No	Yes

3 Securing the Server Components

3.1 OS Hardening

You can use the server components of OpenScape Xpressions under one of the following server operating systems:

- Microsoft Windows Server 2012 and 2012 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2016 RTM (Release 1607)

OpenScape Xpressions is delivered as an application. The customer is responsible for providing the operating system and applying suitable hardening measures.

We recommend to apply hardening measures according to best practice standards like e.g. the Benchmarks issued by the Center of Internet Security (CIS).

3.2 Security Measures for OpenScape Xpressions Services

All OpenScape Xpressions services operate under the **LocalSystem** Windows account, which has been given extensive system privileges.

Check-2	
Possible consequences	An attacker gains full control of the XPR server after successfully attacking one of these services – e.g. by a buffer overflow.
Hardening measures	Start the XPR server services in the context of a Windows account that has been assigned restricted privileges. In doing so, use the minimum-privileges principle by assigning the account used only privileges actually required. You find information about this in the *OpenScape Xpressions, Server Installation* manual in the following chapter: 4.5.4 Assigning a Service Account
Hardening measures configured	No Yes
Remarks	

3.3 Security Measures for CSTA

An attacker can use spied-out authentication data to insert falsified CSTA messages in the communication between OpenScape Xpressions and PBX.

Check-3	
Possible consequences	An attacker floods the PBX with falsified CSTA messages and makes the associated service unavailable for proper CSTA communication.
Hardening measures	Use an IPSec-based VPN tunnel to transmit CSTA data encrypted. You find information about configuring IPSec in the *OpenScape Xpressions, Server Installation* manual in the following chapter: D.15 IPSec Configuration
Hardening measures configured	No Yes
Remarks	

3.4 Security Measures for LDAP

An attacker can read the LDAP user passwords transmitted using LDAP.

Check-4	
Possible consequences	An attacker can read the confidential LDAP user passwords. However, the attacker cannot change the read LDAP user passwords, because LDAP has read-only privileges for the Active Directory.
Hardening measures	Use LDAP via SSL for transmitting the LDAP user passwords encrypted. Please note that all other LDAP data is still transmitted unencrypted. Activate LDAP via SSL using the registry key **UseSSL** of the LDAP APL. You find information about this in the *OpenScape Xpressions, Server Administration* manual in the following chapter: 19.13 LDAP and SSL Encryption
Hardening measures configured	No Yes
Remarks	

3.5 Security Measures for RTP

An attacker can intercept and change voice, video and DTMF data transmitted by RTP.

Check-5	
Possible consequences	An attacker can intercept confidential data – e.g. simple audio or video communication, but also PINs or credit card numbers transmitted using DTMF. Changing intercepted data is possible also.
Hardening measures	Use SRTP to transmit the RTP data encrypted. You find information about this in the *OpenScape Xpressions, Server Administration* manual in the following chapter: 10.10.4.2 Properties of SIP-based Devices (Security)
Hardening measures configured	No Yes
Remarks	

3.6 Security Measures for SCCP

An attacker can use spied-out authentication data to insert falsified SCCP messages in the communication between OpenScape Xpressions and Cisco Call Manager.

Check-6	
Possible consequences	An attacker floods the Cisco Call Manager with falsified SCCP messages and makes the associated service unavailable for proper SCCP communication. An attacker can influence billing.
Hardening measures	Use TLS by means of Stunnel to transmit the SCCP data encrypted. You find information about this in the *OpenScape Xpressions, Server Installation* manual in the following chapter: 4.5.11.1 Configuring stunnel
Hardening measures configured	No Yes
Remarks	

3.7 Security Measures for SIP

An attacker can use spied-out authentication data to insert falsified SIP messages in the communication between OpenScape Xpressions and SIP server (PBX).

Check-7	
Possible consequences	An attacker floods the SIP server (PBX) with falsified SIP messages and makes the associated service unavailable for proper SIP communication. An attacker can influence billing.
Hardening measures	Use TLS to transmit the SIP data encrypted. The keys for RTP communication are then transmitted encrypted also. You find information about this in the *OpenScape Xpressions, Server Administration* manual in the following chapter: 10.10.4.2 Properties of SIP-based Devices (SIP tab)
Hardening measures configured	No Yes
Remarks	

3.8 Security Measures for SMPP

An attacker can read SMS data transmitted using SMPP.

Check-8	
Possible consequences	An attacker can read confidential data.
Hardening measures	Use an IPSec- or Stunnel (TLS)-based VPN tunnel to transmit SMS data encrypted. You find information about configuring IPSec in the *OpenScape Xpressions, Server Installation* manual in the following chapter: D.15 IPSec Configuration
Hardening measures configured	No Yes
Remarks	

An attacker can change the SMS data of SMPP-based communication.

Check-9	
Possible consequences	An attacker can falsify the information sent in an SMS message.
Hardening measures	Use an IPSec- or Stunnel (TLS)-based VPN tunnel to transmit SMS data encrypted. You find information about configuring IPSec in the *OpenScape Xpressions, Server Installation* manual in the following chapter: D.15 IPSec Configuration
Hardening measures configured	No Yes
Remarks	

3.9 Security Measures for SMTP, POP3 and IMAP

An attacker can wiretap messages transmitted using SMTP, POP3 or IMAP.

Check-10	
Possible consequences	An attacker can read confidential data.
	Use SSL for the SMTP APL to transmit data securely. You find information about this in the *OpenScape Xpressions, Server Administration* manual in the following SMTP APL chapter: 12.1.5 Secure Sockets
Hardening measures	
Hardening measures configured	No Yes
Remarks	

3.10 Security Measures for SNMP

An attacker can use spied-out authentication data to insert falsified SNMP messages in the communication between SNMP server and client.

Check-11	
Possible consequences	An attacker influences SNMP-based checking and control of OpenScape Xpressions.
Hardening measures	Use TLS by means of Stunnel to transmit the SNMP data encrypted. You find information about this in the *OpenScape Xpressions, Server Installation* manual in the following chapter: 4.5.11.1 Configuring stunnel
Hardening measures configured	No Yes
Remarks	

3.11 Security Measures for UCP

An attacker can read SMS data transmitted using UCP.

Check-12	
Possible consequences	An attacker can read confidential data.
Hardening measures	Use an IPSec- or TLS-based VPN tunnel to transmit SMS data encrypted. You find information about configuring IPSec in the *OpenScape Xpressions, Server Installation* manual in the following chapter: D.15 IPSec Configuration
Hardening measures configured	No Yes
Remarks	

An attacker can change the SMS data of UCP-based communication.

Check-13	
Possible consequences	An attacker can falsify the information sent in an SMS message.
Hardening measures	Use an IPSec- or TLS-based VPN tunnel to transmit SMS data encrypted. You find information about configuring IPSec in the *OpenScape Xpressions, Server Installation* manual in the following chapter: D.15 IPSec Configuration
Hardening measures configured	No Yes
Remarks	

3.12 Security Measures for HTTPS

TLS v1.2 is now enabled by default.

TLS 1.0 and 1.1 are disabled and can only be enabled via registry keys.

Check-14	
Possible consequences	The attacker could access confidential user data.

Hardening measures	Check if TLS 1.0 or 1.1 are disabled.
	The following DWORD regkeys must be set to 0 or should not exist :
	`MRS Globals\SSL_TLSv1_Enable`
	`MRS Globals\SSL_TLSv1_1_Enable`
	and
	`WebApl\SSL_TLSv1_Enable`
	`WebApl\SSL_TLSv1_1_Enable`

Hardening measures configured	No Yes
Remarks	Disabling TLS v1 can break compatibility with older browser (eg IE 10 or below) and with OS UC WebClient.

4 Securing the Client Components

Check-15	
Possible consequences	An attacker can falsify the information sent in an SMS message.
Hardening measures	Use an IPSec- or TLS-based VPN tunnel to transmit SMS data encrypted. You find information about configuring IPSec in the *OpenScape Xpressions, Server Installation* manual in the following chapter: D.15 IPSec Configuration
Hardening measures configured	No Yes
Remarks	

4.1 Security Measures for PC Operating Systems

Harden all client PCs that host client components of OpenScape Xpressions.

Check-16	**Installing all security updates for the client PC operating systems**
Hardening measures configured	No Yes
Remarks	

Check-17	**Installing and activating current virus protection on the client PCs**
Hardening measures configured	No Yes
Remarks	

5 Securing 3rd-Party Components

5.1 Virtualization Hardening

You can use the server components of OpenScape Xpressions in a virtual environment.

We recommend hardening the virtualization infrastructure according to security guidelines provided by the virtualization vendor. As an alternative, best practice standards like the Benchmarks issued by the Center of Internet Security (CIS) should be considered.

5.2 Web Browsers Hardening

Clients of OpenScape Xpressions are based on web browsers.

We recommend hardening web browsers according to best practice standards, such as the Benchmarks issued by the Center for Internet Security (CIS).

5.3 Security Measures for the System Databases

OpenScape Xpressions uses the following databases:

- PostgreSQL
- Microsoft SQL

5.3.1 Security Measures for the Microsoft SQL Database

We recommend hardening the Microsoft SQL Database according to best practice standards, such as the Benchmarks issued by the Center for Internet Security (CIS).

5.3.2 Security Measures for the PostgreSQL Database

You use the PostgreSQL database when deploying the Web Client with OpenScape Xpressions.

Check-18	
Possible consequences	An attacker can access confidential data.
Hardening measures	Limit the access for the database by restricting the TCP/IP addresses, OpenScape Xpressions is listening to for database access. For this, search in the following file for the parameter **listen_addresses** and change its setting to **'127.0.0.1'.** Also include the quotation marks. `xpr\postgresql\data\postgresql.conf`
Hardening measures configured	No Yes
Remarks	

6 Securing the Infrastructure

OpenScape Xpressions uses different system ports for communicating with other components. You find information about these ports in the *OpenScape Xpressions, Server Administration* manual in the following chapters:

- 7.6.1 Firewalls between Nodes of a distributed XPR Server
- 7.7 TCP / IP ports used by the XPR Server

Block in your network **all** system ports not specified in the mentioned chapters.

The OpenScape Xpressions, Server Administration manual is available via E-Docu or the partner portal.
https://www.unify.com/us/partners/partner-portal.aspx

6.1 End of life / End of support of Apache Tomcat server

Apache Tomcat server may have unfixed vulnerabilities that are impacting OpenScape Xpressions.

Apache Tomcat server is no longer maintained by OpenScape Xpressions since it was part of UCC Components that is out of support and OpenScape UC integration must be used on its place.

For this reason, we strongly recommend to uninstall any UCC components installed on OS Xpressions server and if it is not possible, at least block the access to ports 7789 and 8443 on OS Xpressions server.

7 Securing the User Interfaces

OpenScape Xpressions deploys administrator and system user interfaces. You must protect these two interface types from unauthorized access.

7.1 Security Measures for the Administrator Interface

If the administrator interface of OpenScape Xpressions is protected insufficiently, an attacker can use it to access the XPR server configuration.

Check-19	
Possible consequences	An attacker gains full control of the XPR server and its services. An attacker can access user data – e.g. in e-mail or voicemail inboxes.
Hardening measures	Protect the administrator interface from unauthorized access. To do this, heed the following useful points: • Authentication of users by user name and password Verify that users do not deploy trivial passwords and configured passwords are changed in regular, relatively short intervals. Have user accounts locked after wrong passwords were entered several times. You find information about this in the *OpenScape Xpressions, Server Administration* manual in the following chapter: 4.8 Password Handling in the XPR Server • Authorization by user groups and privileges Assign users only those system privileges they actually need for their work. You find information about this in the *OpenScape Xpressions, Web Assistant* in the following chapter: 4.2.1 User Administration • Audit Use audit logging to log system changes and, if required, to trace them. You find information about this in the *OpenScape Xpressions, Server Administration* manual in the following chapter: 31.4 LogTool
Hardening measures configured	No Yes
Remarks	

7.2 Security Measures for the User Interfaces

If the user interfaces of OpenScape Xpressions are protected insufficiently, an attacker can access data and services of individual users.

Check-20	
Possible consequences	An attacker can access data of individual users – e.g. in e-mail or voicemail inboxes. An attacker can perform services on behalf of an individual user – e.g. sending e-mails or voicemails.
Hardening measures	Protect the user interfaces from unauthorized access. To do this, heed the following useful points: • Authentication of users by user name and password / PIN Verify that users do not deploy trivial passwords / PINs and configured passwords are changed in regular, relatively short intervals. Have user accounts locked after wrong passwords / PINs were entered several times. You find information about this in the *OpenScape Xpressions, Server Administration* manual in the following chapters: - 4.7 PIN Handling in the XPR Server - 4.8 Password Handling in the XPR Server • Authorization by user groups and privileges Assign users only those system privileges they actually need for their work. You find information about this in the *OpenScape Xpressions, Web Assistant* in the following chapter: 4.2.1 User Administration
Hardening measures configured	No Yes
Remarks	

8 Protection against Toll Fraud

Toll fraud can cause considerable financial losses. The measures listed below shall be taken to protect against unauthorized access of the Xpressions system.

8.1 Securing Mailboxes

With the feature CLIP-No-Screening for one-number-services (ONS) everybody can spoof an internal number and gets the privilege to dial out an expensive number abroad.

Furthermore attackers make short test calls (mostly late in the evening or on weekends) and try to get access to the mailbox.
If it is reported (e.g. from the cleaning personal or the security) that short ringing of the phones is heard, then this is a sign of being attacked.

Especially mailboxes with which an outgoing call can be established present a high risk.

See below how to make the system more secure:

- Prevent to use / deploy / install unused mailboxes or at least keep the number small and monitor them.
- Use a strong password and pin.
  Also for unused mailboxes a strong password / pin should be assigned.
  It is better to prevent to have unused mailboxes.
- Change the password regulary
- Change immediately password / pin when you are informed about an attack.
- Keep well known numbers confidential (inform employees not to provide information about well known numbers or reference numbers outside).
  These numbers include dialable numbers outside of the system, that provide remote access to the mailboxes.
- Lock the mailbox if there are too many invalid log-in attempts (e.g. allow only 3 attempts) refer also to section Section 8.6.2, “PIN policy”.
- Call Transfer to External should be disabled by default.
- Call Transfer to External should be allowed only for internal callers.
- Trusted numbers should be disabled.
- Use different NCO Locations for different Country Codes.
- In case NCO Ranges are used, always define the Country code outside the Ranges.

Refer also to Chapter 7, “Securing the User Interfaces”.

8.2 Securing Server Components

Refer to Chapter 3, “Securing the Server Components”.

8.3 Securing Client Components

Refer to Chapter 4, “Securing the Client Components”.

8.4 Securing 3rd-Party Components

Refer to Chapter 5, “Securing 3rd-Party Components”.

8.5 Securing the infrastructure

Refer to Chapter 6, “Securing the Infrastructure”.

8.6 Password / PIN Policy

8.6.1 Password policy

Minimum length: 8

Must include at least:

- Upper case letters : 1
- Lower case letters : 1
- Numbers : 1
- Special Characters : 1

Furthermore the following should be applied:

Maximum identical characters in a row: 3

Maximum sequentical characters in a row: 3

Number of old password to consider : 5

Must change password after : 90 days

Cannot change password again before : 1 day

Default password must be changed after login : yes

8.6.2 PIN policy

Minimum length : 8

Number of stored PINs : 5

PIN expiration : 90 days

Maximum tolerated login failures : 3

8.7 General hints

- Do not use default passwords
- Change passwords / pins regulary or force the users to do this via a policy
- Use strong passwords / pins (use a policy for this)
- Do not allow many attempts for a password, if there are too many wrong password attempts lock the service / device / mailbox etc. and generate an alert or alarm or at least log it.
- Do not deploy unused mailboxes, or at least keep them to a minimum and monitor them
- Use Firewalls
- keep permissions to a minimum
- update software regulary, especially when there are security fixes
- Keep information confidential, especially about phone numbers.