MAKE THE
WORLD SEE

# Milestone Systems

XProtect® VMS

Hardening guide

milestone

# Changes to this document

| Document version | Release | Comments |
|---|---|---|
| Version 12 | 2020 R1 | Microsoft Internet Explorer no longer supported. Microsoft Edge is supported. See Use only supported browsers with the latest security updates on page 81. |
| Version 11 | 2019 R3 | Port 5432 is disabled by default. See Use firewalls to limit IP access to servers and computers on page 43.<br><br>Added information on Disable IIS header information on page 62. |
| Version 10 | 2019 R2 | Added section Secure communication (explained) on page 25<br><br>• Management server encryption (explained) on page 26<br>• Encryption from the management server to the recording server (explained) on page 27<br>• Mobile server data encryption (explained) on page 30<br><br>Added hardening information for the SQL Server and database connection in Connection to the SQL Server and database on page 59.<br><br>Added hardening information for Recording Server in Harden Network Attached Storage (NAS) to store recorded media data on page 65. |
| Version 9 | 2019 R1 | Added encryption from the recording server to all clients, described here: Encryption from the management server to the recording server (explained) on page 27 |
| Version 8 | 2018 R3 | Added design recommendations, described here: Privacy by design on page 18.<br><br>Log Server uses port number 22337, described here: Use firewalls to limit IP access to servers and computers on page 43 and Limit the IP access to Log Server on page 70.<br><br>Mobile server no longer uses port 8000 for communication with Tray Manager. This was removed from Use firewalls to limit IP access to servers and computers on page 43.<br><br>New recommendation for scanning for devices, described in Scanning for devices on page 42. |
| Version 7 | 2018 R2 | No changes to this document |

| Document version | Release | Comments |
|---|---|---|
| Version 6 | 2018 R1 | Clarified the need to add specific firewall rules to the Management Server, described here: Use firewalls to limit IP access to servers and computers on page 43. |
| Version 5 | 2018 R1 | No changes to this document |
| Version 4 | 2017 R3 | No changes to this document |
| Version 3 | 2017 R2 | This document applies to XProtect VMS versions 2017 R2 and before.<br>These are the changes to the document:<br>• Added Two-step verification for Milestone Mobile (see Set up users for two-step verification via email on page 66)<br>• Storage and Recording Settings properties on page 63 |
| Version 2 | 2016 R3 | This document applies to XProtect VMS versions 2016 R3 and before.<br>These are the changes to the document:<br>• Added Changes to this document topic<br>• Added Kerberos support (see Kerberos authentication (explained) on page 32)<br>• Updated port numbers in Use firewalls to limit IP access to servers and computers on page 43 |
| Version 1 | 2016 R2 | This document applies to XProtect VMS versions 2016 R3 and before. |

# Contents

**Changes to this document** ..... **2**

**Copyright, trademarks, and disclaimer** ..... **8**

**Introduction** ..... **9**

What is "hardening?" ..... 9

Target audience ..... 9

Resources and references ..... 10

Hardware and device components ..... 10

Cyber threats and cyber risks ..... 11

Cyber Risk Management Framework ..... 12

Hardening system components ..... 15

**General setup** ..... **17**

Privacy by design ..... 18

**Servers, Workstations, Clients and Applications** ..... **22**

Basic steps ..... 22

Establish surveillance and security objectives ..... 22

Establish a formal security policy and response plan ..... 23

Use Windows users with Active Directory ..... 23

Secure communication (explained) ..... 25

Management server encryption (explained) ..... 26

Encryption from the management server to the recording server (explained) ..... 27

Encryption to clients and servers that retrieve data from the recording server (explained) ..... 28

Mobile server data encryption (explained) ..... 30

Mobile server encryption requirements for clients ..... 31

Kerberos authentication (explained) ..... 32

Use Windows update ..... 33

Keep software and device firmware updated ..... 33

Use antivirus on all servers and computers ..... 34

Monitor logs in the VMS for signs of suspicious activity ..... 35

Advanced steps ..... 36
Adopt standards for secure network and VMS implementations ..... 37
Establish an incident response plan ..... 37
Protect sensitive VMS components ..... 38
Follow Microsoft OS Security best practices ..... 38
Use tools to automate or implement the security policy ..... 38
Follow established network security best practices ..... 39
**Devices and network ..... 40**
Basic steps – Devices ..... 40
Use strong passwords instead of default passwords ..... 40
Stop unused services and protocols ..... 40
Create dedicated user accounts on each device ..... 41
Scanning for devices ..... 42
Basic steps – Network ..... 42
Use secure and trusted networks connection ..... 42
Use firewalls to limit IP access to servers and computers ..... 43
Use a firewall between the VMS and the Internet ..... 53
Connect the camera subnet to the recording server subnet only ..... 54
Advanced steps – Devices ..... 54
Use Simple Network Management Protocol to monitor events ..... 54
Advanced steps – Network ..... 55
Use secure wireless protocols ..... 55
Use port-based access control ..... 55
Run the VMS on a dedicated network ..... 56
**Milestone Servers ..... 57**
Basic steps – Milestone servers ..... 57
Use physical access controls and monitor the server room ..... 57
Use encrypted communication channels ..... 57
Advanced steps – Milestone servers ..... 57
Run services with service accounts ..... 58

Run components on dedicated virtual or physical servers ..... 58
Restrict the use of removable media on computers and servers ..... 58
Use individual administrator accounts for better auditing ..... 58
Use subnets or VLANs to limit server access ..... 59
Enable only the ports used by Event Server ..... 59
SQL Server ..... 59
Connection to the SQL Server and database ..... 59
Run the SQL Server and database on a separate server ..... 60
Management Server ..... 60
Adjust the token time-out ..... 60
Enable only the ports used by the management server ..... 61
Disable non-secure protocols ..... 61
Disable legacy remoting channel ..... 62
Disable IIS header information ..... 62
Recording Server ..... 63
Storage and Recording Settings properties ..... 63
Use separate network interface cards ..... 65
Harden Network Attached Storage (NAS) to store recorded media data ..... 65
Milestone Mobile server component ..... 65
Only enable ports that Milestone Mobile server uses ..... 65
Use a "demilitarized zone" (DMZ) to provide external access ..... 66
Disable non-secure protocols ..... 66
Set up users for two-step verification via email ..... 66
Requirements ..... 67
Two-step verification tab ..... 68
Log Server ..... 70
Install Log Server on a separate server with SQL Server ..... 70
Limit the IP access to Log Server ..... 70
**Client programs ..... 71**
Basic steps (all client programs) ..... 71

Use Windows users with AD ..... 71
Restrict permissions for client users ..... 71
Always run clients on trusted hardware on trusted networks ..... 73
Advanced steps – XProtect Smart Client ..... 73
Restrict physical access to any computer running XProtect Smart Client ..... 73
Always use a secure connection by default, particularly over public networks ..... 74
Activate login authorization ..... 74
Do not store passwords ..... 77
Turn on only required client features ..... 78
Use separate names for user accounts ..... 78
Prohibit the use of removable media ..... 79
Advanced steps – Milestone Mobile client ..... 79
Always use the Milestone Mobile client on secure devices ..... 79
Download the Milestone Mobile client from authorized sources ..... 80
Mobile devices should be secured ..... 80
Advanced steps – XProtect Web Client ..... 80
Always run XProtect Web Client on trusted client computers ..... 80
Use certificates to confirm the identity of a Milestone Mobile server ..... 81
Use only supported browsers with the latest security updates ..... 81
Advanced steps – Management Client ..... 82
Use Management Client profiles to limit what administrators can view ..... 82
Allow administrators to access relevant parts of the VMS ..... 82
Run the Management Client on trusted and secure networks ..... 83
**Product comparison chart ..... 84**
**Appendix 1 - Resources ..... 87**
**Appendix 2 - Acronyms ..... 89**

# Copyright, trademarks, and disclaimer

Copyright © 2020 Milestone Systems A/S

### Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

### Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserves the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third-party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file 3rd_party_software_terms_and_conditions.txt located in your Milestone system installation folder.

# Introduction

This guide describes security and physical security measures and best practices that can help secure your XProtect video management software (VMS) against cyber-attacks. This includes security considerations for the hardware and software of servers, clients and network device components of a video surveillance system.

This guide adopts standard security and privacy controls and maps them to each of the recommendations. That makes this guide a resource for compliance across industry and government security, and network security requirements.

## What is "hardening?"

Developing and implementing security measures and best practices is known as "hardening." Hardening is a continuous process of identifying and understanding security risks, and taking appropriate steps to counter them. The process is dynamic because threats, and the systems they target, are continuously evolving.

Most of the information in this guide focuses on IT settings and techniques, but it's important to remember that physical security is also a vital part of hardening. For example, use physical barriers to servers and client computers, and make sure that things like camera enclosures, locks, tamper alarms, and access controls are secure.

The following are the actionable steps for hardening a VMS:

1. Understand the components to protect
2. Harden the surveillance system components:
    1. Harden the servers (physical and virtual) and client computers and devices
    2. Harden the network
    3. Harden the cameras
3. Document and maintain security settings on each system
4. Train and invest in people and skills, including your supply chain

### Target audience

Everyone in an organization must understand at least the basics about network and software security. Attempts to compromise critical IT infrastructure are becoming more frequent, so everyone must take hardening and security seriously.

This guide provides basic and advanced information for end users, system integrators, consultants, and component manufacturers.

- Basic descriptions give general insight into security
- Advanced descriptions give IT-specific guidance for hardening XProtect VMS products. In addition to software, it also describes security considerations for the hardware and device components of the system.

## Resources and references

The following organizations provide resources and information about best practices for security:

- International Standards Organization (ISO),
- United States (US) National Institute of Standards and Technology (NIST)
- Security Technical Implementation Guidelines (STIGs) from the US Defense Information Systems Administration (DISA)
- Center for Internet Security
- SANS Institute
- Cloud Security Alliance (CSA)
- Internet Engineering Task Force (IETF)
- British Standards

Additionally, camera manufacturers provide guidance for their hardware devices.

See Appendix 1 - Resources on page 87 for a list of references and Appendix 2 - Acronyms on page 89 for a list of acronyms.

This guide leverages country, international, and industry standards and specifications. In particular, it refers to the United States Department of Commerce National Institute of Standards and Technology Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf).

The NIST document is written for the US Federal government; however, it is generally accepted in the security industry as the current set of best practices.

This guide refers and links to additional information about security controls. The guidance can be cross-referenced to industry-specific requirements and other international security and risk management standard and frameworks. For example, the current NIST Cybersecurity Framework uses SP 800-53 Rev4 as a basis for the controls and guidance. Another example is Appendix H in SP 800-53 Rev 4, which contains a reference to ISO/IEC 15408 requirements, such as Common Criteria.

## Hardware and device components

In addition to software, the components of an XProtect VMS installation typically include hardware devices, such as:

- Cameras
- Encoders
- Networking products

- Storage systems
- Servers and client computers (physical or virtual machines)
- Mobile devices, such as smartphones

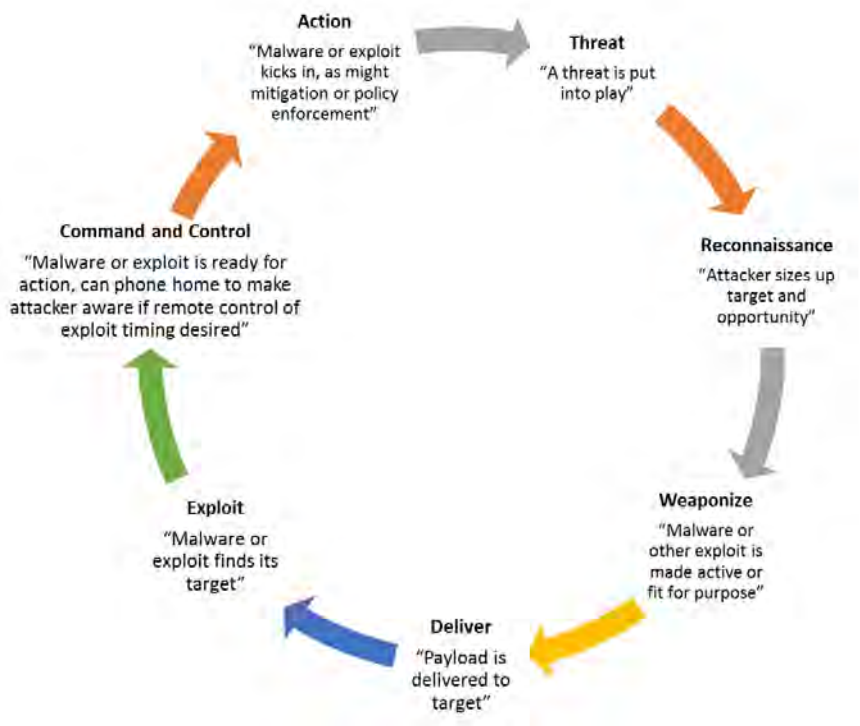
It is important to include hardware devices in your efforts to harden your XProtect VMS installation. For example, cameras often have default passwords. Some manufacturers publish these passwords online so that they're easy for customers to find. Unfortunately, that means the passwords are also available to attackers.

This document provides recommendations for hardware devices.

## Cyber threats and cyber risks

There are many sources of threats to a VMS, including business, technology, process and human attacks or failures. Threats take place over a lifecycle. The threat lifecycle, sometimes called the "cyber kill" or "cyber threat chain," was developed to describe the stages of advanced cyber threats.

Each stage in the threat lifecycle takes time. The amount of time for each stage is particular to the threat, or combination of threats, and its actors and targets.




The threat lifecycle is important for risk assessment because it shows where you can mitigate threats. The goal is to reduce the number of vulnerabilities, and to address them as early as possible. For example, discouraging an attacker who is probing a system for vulnerabilities can eliminate a threat.

Hardening puts in place actions that mitigate threats for each phase in the threat lifecycle. For example, during the reconnaissance phase an attacker scans to find open ports and determine the status of services that are related to the network and the VMS. To mitigate this, hardening guidance is to close unnecessary system ports in XProtect VMS and Windows configurations.

The risk and threat assessment process includes the following steps:

- Identify information and security risks
- Assess and prioritize risks
- Implement policy, procedures, and technical solutions to mitigate these risks

The overall process of risk and threat assessment, and the implementation of security controls, is referred to as a risk management framework. This document refers to NIST security and privacy controls and other publications about risk management frameworks.

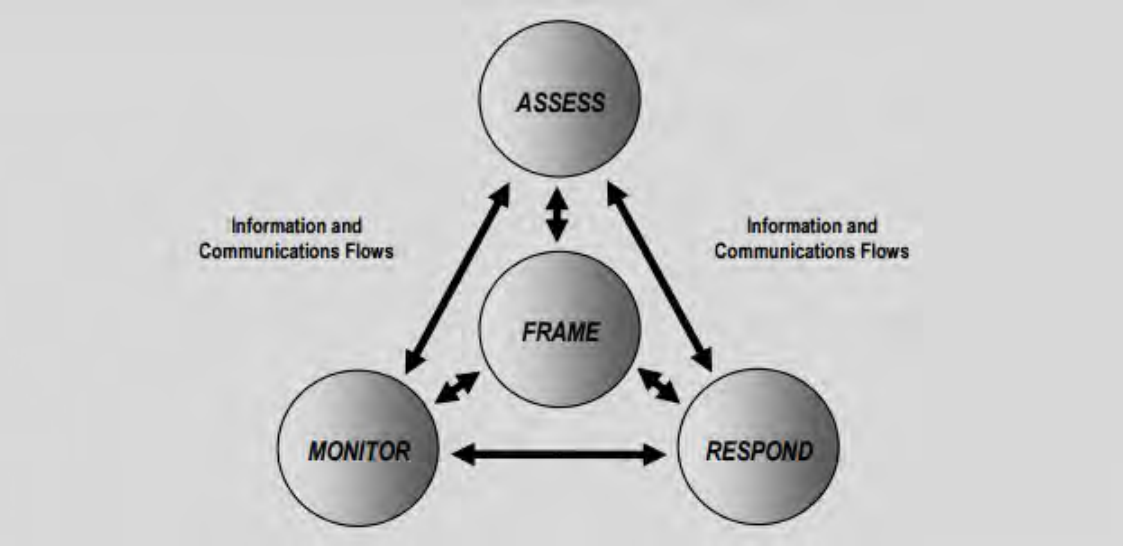
## Cyber Risk Management Framework

The security and privacy controls in SP 800-53 Revision 4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) are part of an overall risk management framework from NIST. The NIST document SP800-39 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf) is a guide to applying a risk management framework. SP800-36 is a foundational document for the NIST Cybersecurity Framework, which is described in Cybersecurity Framework (http://www.nist.gov/cyberframework/).

The figures here show:

- An overview of the risk management process. It shows a high-level, overall approach.
- Risk management at a business level, taking strategic and tactical considerations into account.
- The lifecycle of a risk management framework, and the NIST documents that provides details for each of the steps in the lifecycle.

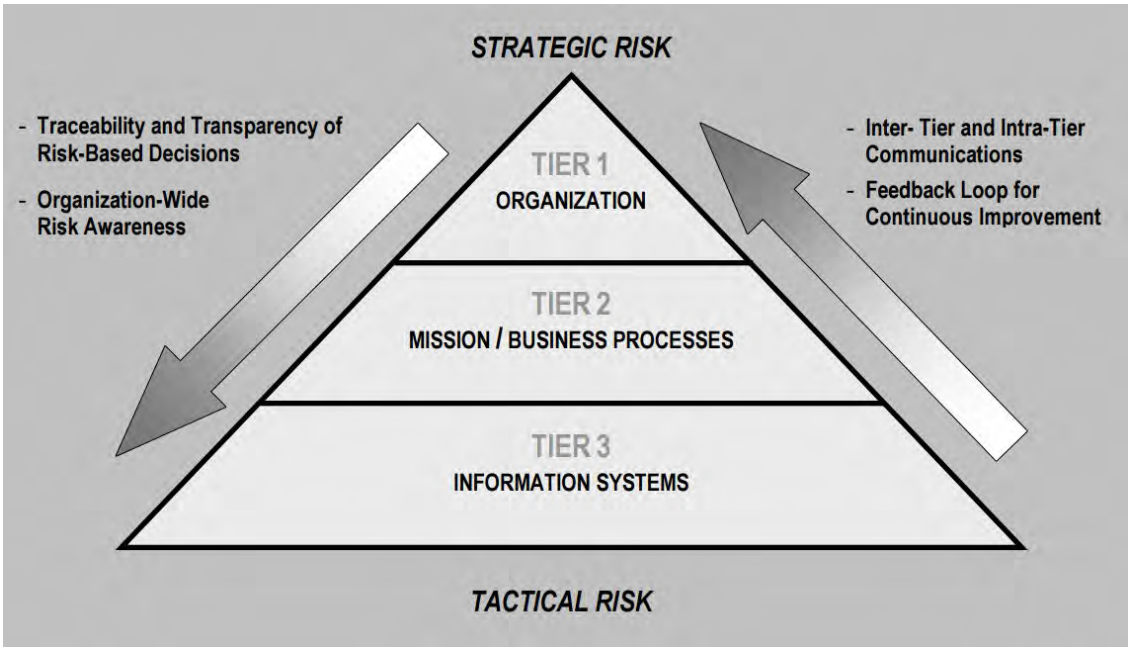
Security and privacy controls represent specific actions and recommendations to implement as part of a risk management process. It's important that the process includes the assessment of the organization, the particular requirements of a given deployment, and the aggregation of these activities into a security plan. SP 800-18 Revision 1 (http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf) provides references for detailed security plans.




High-level view of risk management (SP 800-39, page 8 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

The process is interactive, and responses and their outcomes are iterative. Security threats, risks, responses and results are dynamic and adapt, and as a result so must a security plan.

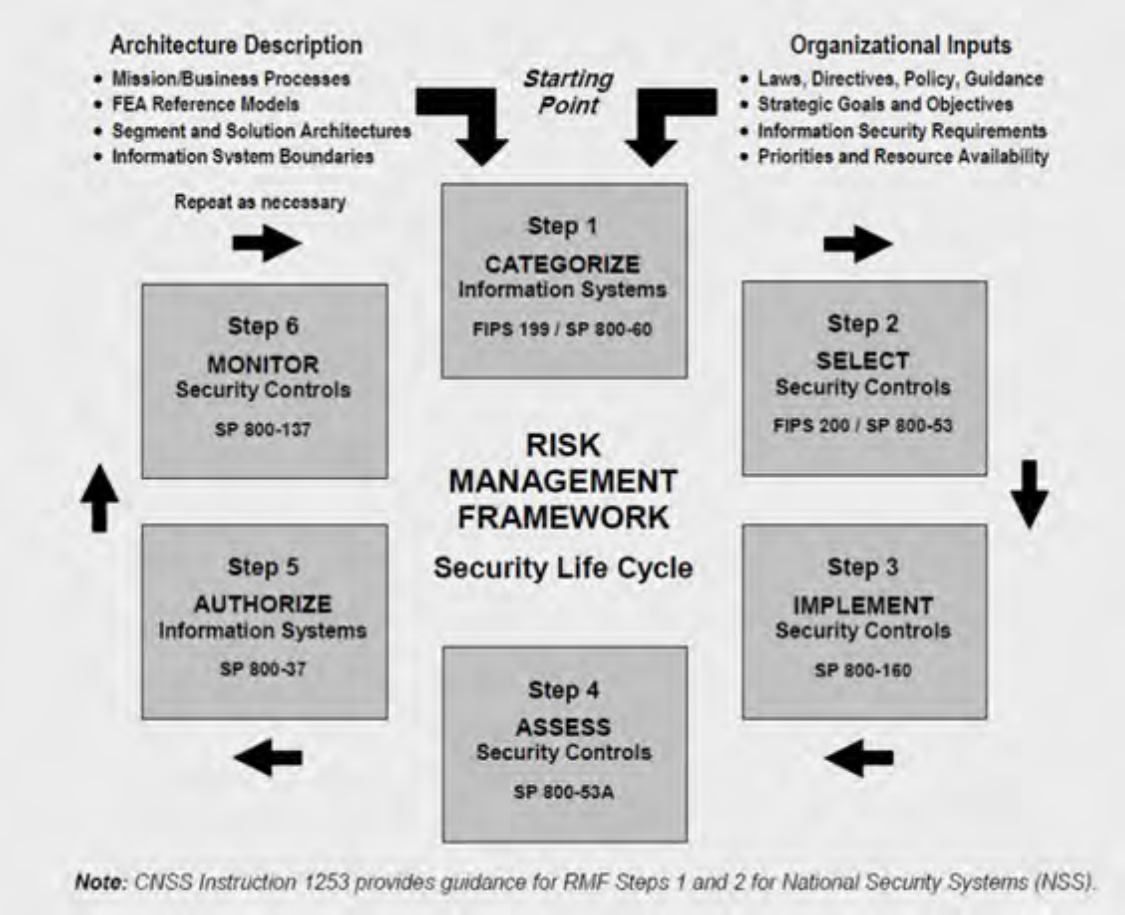
This diagram shows how a risk management framework considers IT systems, business processes, and the organization as a whole to find a balance for the security plan.




Balancing security and business goals (SP 800-39, page 9 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

When hardening a system, you balance the impact on business productivity and usability for the sake of security, and vice versa, in the context of the services you deliver. Security guidance is not isolated from other business and IT activities.

For example, when a user enters their password incorrectly on three consecutive attempts, the password is blocked and they cannot access the system. The system is secure from brute-force attacks, but the unlucky user cannot use the device to do their work. A strong password policy that requires 30 character passwords, and changing passwords every 30 days is a best practice, but it's also difficult to use.




Example of a risk management framework (SP 800-53 Rev 4, page 8 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf))

To document its risk management framework, NIST produced multiple special publications. It includes the following components:

1. Categorization (identification of risk level)
2. Selection of security and privacy controls
3. Implementation

4. Assessment of the effectiveness of security controls
5. Creating an improved system security profile, and what's called an Authority to Operate (ATO)
6. Monitoring and evaluating through iterations

The risk management framework helps put a security plan and guidance in a security context.

## Hardening system components

To harden system components, you change configurations to reduce the risk of a successful attack. Attackers look for a way in, and look for vulnerabilities in exposed parts of the system. Surveillance systems can involve 100s or even 1000s of components. Failure to secure any one component can compromise the system.

The need to maintain configuration information is sometimes overlooked. XProtect VMS provides features for managing configurations, but organizations must have a policy and process in place, and commit to doing the work.

Hardening requires that you keep your knowledge about security up-to-date:

- Be aware of issues that affect software and hardware, including operating systems, mobile devices, cameras, storage devices, and network devices. Establish a point-of-contact for all of the components in the system. Ideally, use reporting procedures to track bugs and vulnerabilities for all components.
- Keep current on Common Vulnerabilities and Exposures (CVEs) (described in Common Vulnerabilities and Exposures (https://cve.mitre.org/)) for all system components. These can relate to the operating systems, devices that have hard-coded maintenance passwords, and so on. Address vulnerabilities for each component, and alert manufacturers to vulnerabilities.
- Review Milestone Knowledge Base (KB) articles, and regularly review logs for signs of suspicious activity. For more information, see the *Milestone Knowledge Base* (https://force.milestonesys.com/support/MccKnowledgeBase).
- Maintain up-to-date configuration and system documentation for the system. Use change-control procedures for the work you perform, and follow best practices for configuration management, as described in SP 800-128 (http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf).

The following sections provide basic and advanced hardening and security recommendations for each system component. The sections also contain examples of how these relate to specific security controls described in the NIST Special Publication 800-53 Revision 4, titled *Security and Privacy Controls for Federal Information Systems and Organizations*.

In addition to the NIST document, the following sources are referenced:

- Center for Internet Security
- SP 800-53
- ISO 27001
- ISO/IEC 15408 (also known as Common Criteria, ISO/IEC 15408-1:2009 (http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341)) .

Appendix 1 - Resources on page 87 in this document provides recommendations from camera manufacturers. This is a relatively new effort from manufacturers, so limited resources are available. For the most part, the recommendations can be generalized across camera manufacturers.

# General setup

To help secure your surveillance system, Milestone recommends the following:

- Restrict access to servers. Keep servers in locked rooms, and make it difficult for intruders to access network and power cables.

  (PE2 and PE3 in Appendices D and F in NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) (PE Physical and Environment Protection).)

- Design a network infrastructure that uses physical network or VLAN segmentation as much as possible.

  (SC3 in Appendices D and F in NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) (SC System and Communication Protection).)

  - Separate the camera network from the server network by having two network interfaces in each recording server: one for the camera network, and one for the server network.
  - Put the mobile server in a "demilitarized zone" (DMZ) with one network interface for public access, and one for private communication to other servers.

    (SC7 in Appendices D and F NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf).)

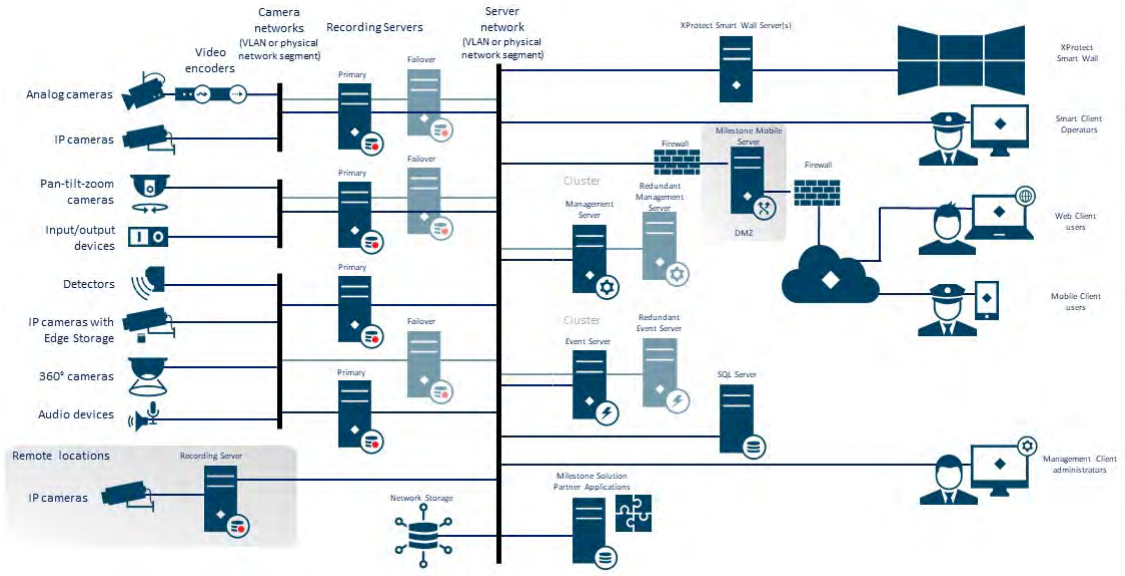
  - Many precautions can be taken when it comes to general set up. In addition to firewalls, these include techniques to segment the network and control access to the servers, clients and applications.

    (AC3, AC4, AC6, CA3, CM3, CM6, CM7, IR4, SA9, SC7, SC28, SI3, SI 8 in Appendices D and F in NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) (AC Access Controls), (CM Configuration Management) (IR Incident Response) (SA System and Service Acquisition) (SI Systems and Information Integrity).)

- Configure the VMS with roles that control access to the system, and designate tasks and responsibilities.

  (AC2, AC3, AC6, AC16, AC25, AU6, AU9, CM5, CM11, IA5, PL8, PS5, PS7, SC2, SI7, in Appendices D and F in NIST SP 800-53 Rev4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) (AU Audit and Accountability) (IA Identification and Authentication) (PL Planning).)

The figure shows an example of a general setup.




# Privacy by design

Milestone products are designed to deliver secure, end-to-end communication. Milestone products are designed to protect privacy and to secure data. Data protection is always important, but especially if you intend to be General Data Protection Regulation (GDPR) compliant in the EU.

According to GDPR, the controller of personal data, when processing such data, has an obligation to implement technical or organizational measures which are designed to implement the data protection principles set out in GDPR. GDPR refers to this as privacy by design.

In the context of a surveillance camera, a relevant example of privacy by design would be a feature that digitally allows the user to restrict image capture to a certain perimeter, preventing the camera from capturing any imagery outside this perimeter that would otherwise be captured.

In XProtect, there is support for privacy masking in two forms – permanent masks that cannot be removed, and liftable masks that (with the right permissions) can be lifted to reveal the image behind the mask.

The controller also has an obligation to implement technical or organizational measures which by default ensure the least privacy intrusive processing of the personal data in question. GDPR refers to this as privacy by default. In the context of a camera, a relevant example of privacy by default could be using privacy masking to keep a sensitive area within the view of the camera private.

**What should you do to ensure privacy by design?**

- Consider the resolution of different points in the camera scene and document these settings

  Different purposes require different image qualities. When identification is not necessary, the camera resolution and other modifiable factors should be chosen to ensure that no recognizable facial images are captured.

- Encrypt your recordings

  Milestone recommends that you secure your recordings by enabling at least Light encryption on your recording servers' storage and archives. Milestone uses the AES-256 algorithm for encryption. When you select Light encryption, only a part of the recording is encrypted. When you select Strong encryption, the entire recording is encrypted.

- Secure the network

  Milestone recommends that you select cameras that support HTTPS. It is recommended that you set the cameras on separate VLANs and use HTTPS for your camera to recording server communication.

  It is recommended that XProtect Smart Clients and XProtect Smart Walls are on the same VLAN as the servers.

  Use a VPN encrypted network or similar if using Smart Client or Smart Wall from a remote location.

- Enable and document the intended retention time

  According to Article 4(1)(e) of the GDPR, recordings must not be retained longer than necessary for the specific purposes for which they were made. Milestone recommends that you set the retention time according to regional laws and requirements, and in any case, to set the retention time to a maximum of 30 days.

- Secure exports

  Milestone recommends that you only allow access to export functionality for a select set of users that need this permission.

  Milestone also recommends that the Smart Client profile is changed to only allow export in XProtect Format with encryption enabled. AVI and JPEG exports should not be allowed, because they can not be made secure. This makes export of any evidence material password protected, encrypted and digitally signed, making sure forensic material is genuine, untampered with and viewed by the authorized receiver only.

- Enable privacy masking – permanent or liftable

  Use privacy masking to help eliminate surveillance of areas irrelevant to your surveillance target.

  Milestone recommends that you set a liftable blurring mask for sensitive areas and in places where person identification is not allowed. Create then a second role that can authorize the mask to be lifted.

- Restrict access rights with roles

  Apply the principle of least privilege (PoLP).

  Milestone recommends that you only allow access to functionality for a select set of users that need this permission. By default, only the system administrator can access the system and perform tasks. All new roles and users that are created have no access to any functions until they are deliberately configured by an administrator.

  Set up permissions for all functionality, including: viewing live video and recordings, listening to audio, accessing metadata, controlling PTZ cameras, accessing and configuring Smart Wall, lifting privacy masks, working with exports, saving snapshots, and so on.

  Grant access to only the cameras that the specific operator needs to access, and restrict access to recorded video, audio, and metadata for operators, either completely, or grant access to only the video, audio, or metadata recorded in the past few hours or less.

  Regularly assess and review roles and responsibilities for operators, investigators, system administrators and others with access to the system. Does the principle of least privilege still apply?

- Enable and use two-step verification

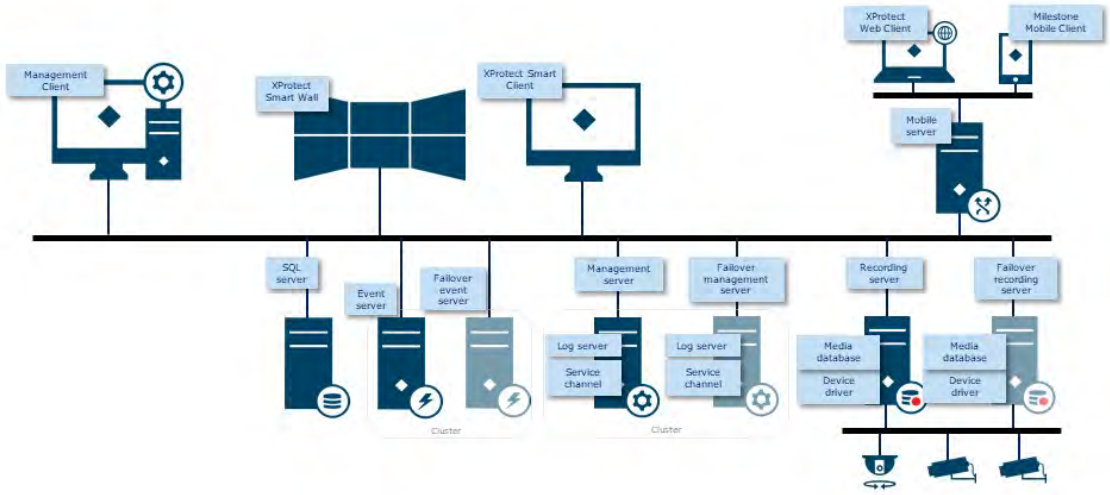
  Milestone recommends that you specify an additional login step for users of XProtect Mobile or XProtect Web Client by enabling two-step verification.

- Restrict administrator permissions

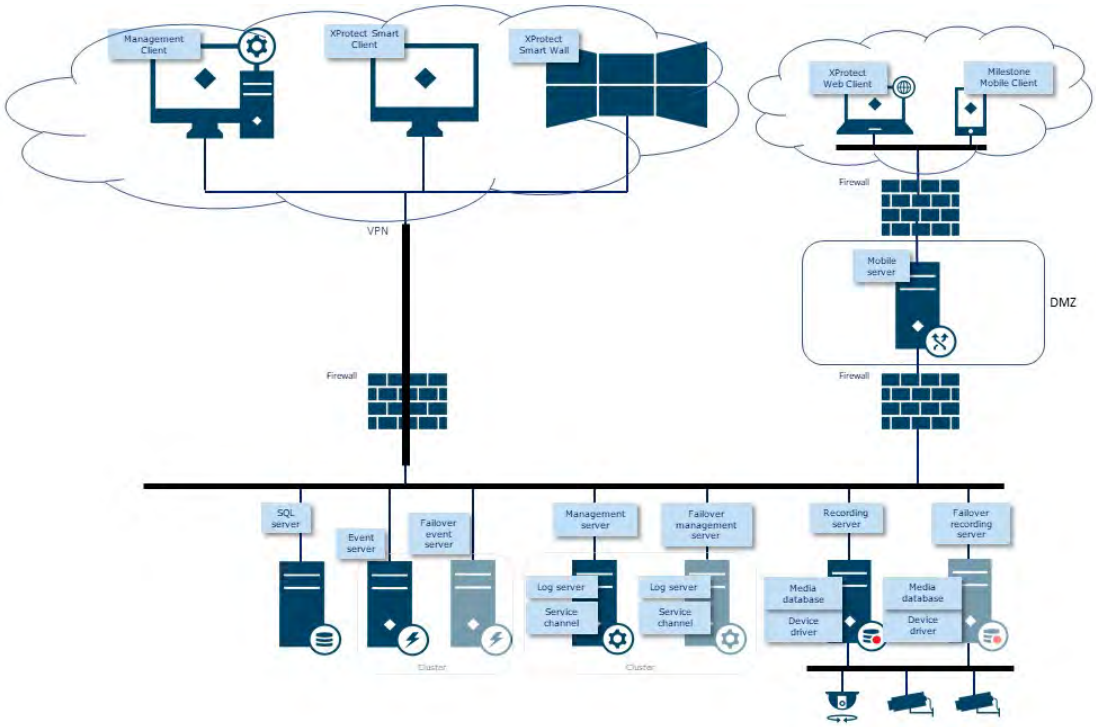
  Milestone recommends that you limit the number of users that have an Administrator role. If you need to create multiple Administrator roles, you can restrict their access by creating Administrator roles that can manage only select parts of the system, such as certain devices or functions.

  Milestone also recommendsthat the VMS administrator does not have full administrator rights on the storage that contains recorded video, and the storage administrator should not have access to the VMS or backup administration.

For security, segment the network so there is a client/management network, and camera networks behind the recording servers:




For greater security, put the mobile server in a "demilitarized zone" (DMZ) with one network interface for public access, and one for private communication to other servers, and use VPN encrypted networks for external connections or to increase security for less secure internal networks:



# Servers, Workstations, Clients and Applications

This section provides hardening guidance based on Microsoft Windows and the services that XProtect VMS uses. This includes:

- The XProtect VMS product, for example XProtect® Corporate or XProtect® Enterprise running on Windows Servers
- The device pack installed on the recording servers
- The server hardware or virtual platforms, and operating systems and services
- The client computers for XProtect® Smart Client and XProtect® Web Client
- Mobile devices and their operating systems and applications

## Basic steps

Establish surveillance and security objectives ..... 22
Establish a formal security policy and response plan ..... 23
Use Windows users with Active Directory ..... 23
Secure communication (explained) ..... 25
Kerberos authentication (explained) ..... 32
Use Windows update ..... 33
Keep software and device firmware updated ..... 33
Use antivirus on all servers and computers ..... 34
Monitor logs in the VMS for signs of suspicious activity ..... 35

### Establish surveillance and security objectives

Before implementing the VMS, Milestone recommends that you establish surveillance objectives. Define goals and expectations related to capturing and using video data and related metadata. All stakeholders should understand the surveillance objectives.

Specifics of surveillance objectives can be found in other documents, for example BS EN 62676-1-1: *Video surveillance systems for use in security applications.System requirements. General*.

When surveillance objectives are in place, you can establish the security objectives. Security objectives support the surveillance objectives by addressing what to protect in the VMS. A shared understanding of security objectives makes it easier to secure the VMS and maintain data integrity.

With the surveillance and security objectives in place, you can more easily address the operational aspects of securing the VMS, such as how to:

- Prevent data from being compromised
- Respond to threats and incidents when they occur, including roles and responsibilities.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 PL-2 *System Security Plan*
- NIST SP 800-53 SA-4 *Acquisition Process*

## Establish a formal security policy and response plan

In compliance with NIST SP 800-100 Information Security Handbook: A Guide for Managers (http://csrc.nist.gov/publications/nistpubs/800-100/sp800-100-mar07-2007.pdf), Milestone recommends that you establish a formal security policy and a response plan that describe how your organization addresses security issues, in terms of practical procedures and guidelines. For example, a security policy can include:

- A password policy defined by the internal IT department
- Access control with ID badges
- Restrictions for smartphones from connecting to the network

Adopt existing IT policies and plans if they adhere to security best practices.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 IR-1 *Incident Response Policy and Procedures*
- NIST SP 800-53 PM-1 *Information Security Program Plan*

## Use Windows users with Active Directory

There are two types of users in XProtect VMS:

- Basic user: a dedicated VMS user account authenticated by a combination of username and password using a password policy. Basic users connect to the VMS using a secure socket layer (SSL) with current Transport Layer (TLS) security protocol session (https://datatracker.ietf.org/wg/tls/charter/) for login, encrypting the traffic contents and username and password.
- Windows user: the user account is specific to a machine or a domain, and it is authenticated based on the Windows login. Windows users connecting to the VMS can use Microsoft Windows Challenge/Response (NTML) for login, Kerberos (see Kerberos authentication (explained) on page 32), or other SSP options from Microsoft (https://msdn.microsoft.com/en-us/library/windows/desktop/aa380502(v=vs.85).aspx).

Milestone recommends that, whenever possible, you use Windows users in combination with Active Directory (AD) to authorize access to the VMS. This allows you to enforce:

- A password policy that requires users to change their password regularly
- Brute force protection, so that the Windows AD account is blocked after a number of failed authentication attempts, again in line with the organization password policy
- Multi-factor authentication in the VMS, particularly for administrators
- Role-based permissions, so you can apply access controls across your domain

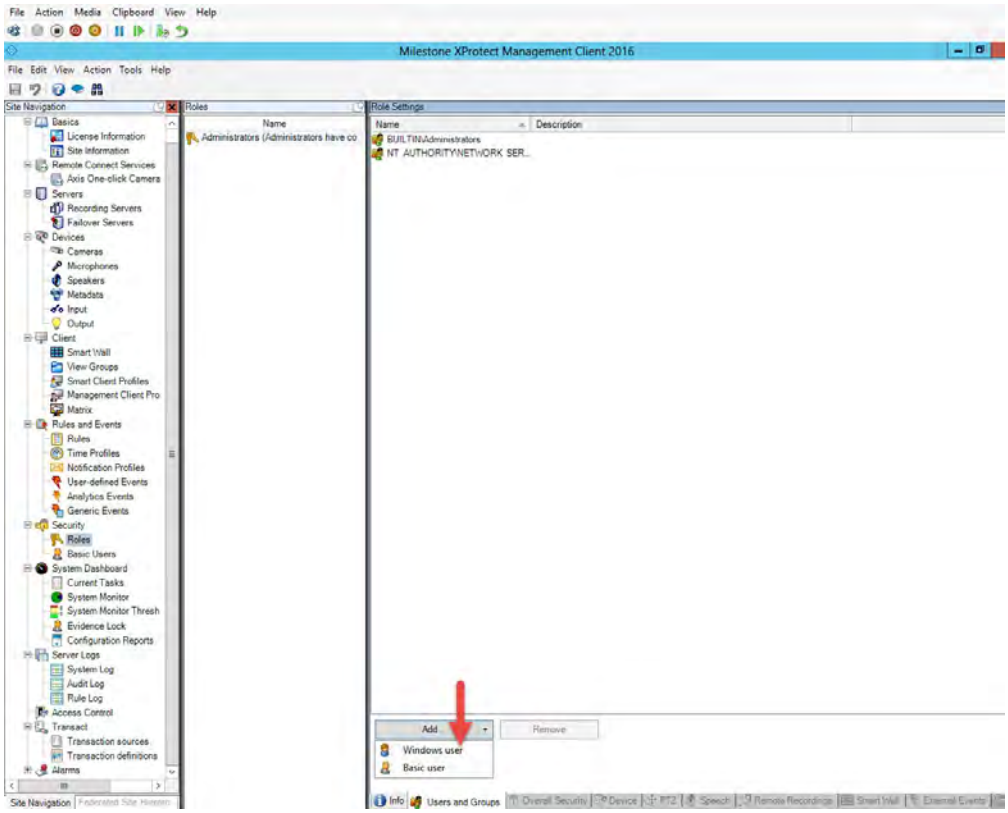
If your organization does not use AD, you can add Windows users to workgroups on the management server instead. Workgroups give you some of the same advantages as Windows users with AD. You can enforce a password policy, which helps protect against brute force attacks, but Milestone recommends that you use a Windows Domain because this gives you central control over user accounts.

Windows users have the advantage of being authenticated via the directory as a single authoritative source and enterprise service for the network and not ad hoc for their local machine. This lets you use role based access controls to assign permissions to users and groups consistently across the domain and the computers on the network.

If you use local Windows users, the user must create a local user name and password on each machine, which is problematic from security and usability perspectives.

To add Windows users or groups to roles in Management Client, follow these steps:

1. Open Management Client.
2. Expand the **Security** node.



3. Select the role to which you want to add the Windows users.
4. On the **Users** and **Groups** tab, click **Add**, and select **Windows user**. A pop-up window appears.
5. If the domain name does not appear in the **From this location** field, click **Locations**.
6. Specify the Windows user, and then click **OK**.

To verify that the Windows user is an AD user, the domain name must appear as a prefix, for example "Domain\John".

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 SA-5 *Information System Documentation*
- NIST SP 800-53 SA-13 *Trustworthiness*

## Secure communication (explained)

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or its predecessor, Secure Sockets Layer (SSL).

In XProtect VMS, the secure communication is obtained by using SSL/TLS with asymmetric encryption (RSA).

SSL/TLS uses a pair of keys—one private, one public—to authenticate, secure, and manage secure connections.

A certificate authority (CA) can issue certificates to web services on servers using a CA certificate. This certificate contains two keys, a private key and public key. The public key is installed on the clients of a web service (service clients) by installing a public certificate. The private key is used for signing server certificates that must be installed on the server. Whenever a service client calls the web service, the web service sends the server certificate including the public key to the client. The service client can validate the server certificate using the already installed public CA certificate. The client and the server can now use the public and private server certificate to exchange a secret key and thereby establish a secure SSL/TLS connection.

For more information about TLS: https://en.wikipedia.org/wiki/Transport_Layer_Security

Certificates have an expiry date. XProtect VMS will not warn you when a certificate is about to expire. If a certificate expires:
- The clients will no longer trust the recording server with the expired certificate and thus cannot communicate with it.
- The recording servers will no longer trust the management server with the expired certificate and thus cannot communicate with it.
- The mobile devices will no longer trust the mobile server with the expired certificate and thus cannot communicate with it.

To renew the certificates, follow the steps in this guide as you did when you created certificates.

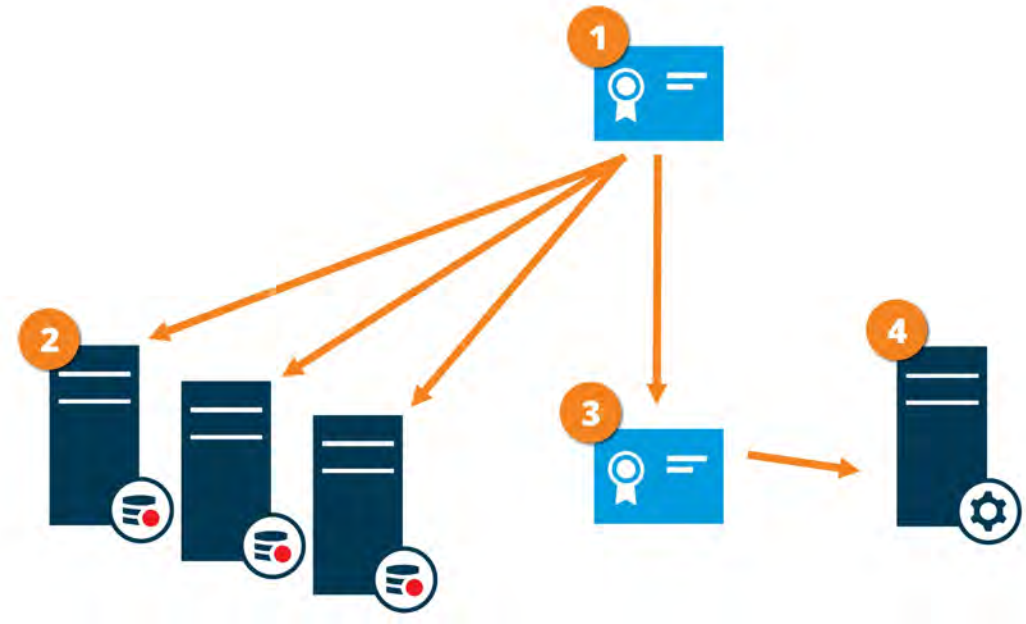
When you renew a certificate with the same subject name and add it to the Windows Certificate Store, the servers will automatically pick up the new certificate. This makes it easier to renew certificates for many servers without having to re-select the certificate for each server and without restarting the services.

### Management server encryption (explained)

You can encrypt the two-way connection between the management server and the recording server. When you enable encryption on the management server, it applies to connections from all the recording servers that connect to the management server. If you enable encryption on the management server, you must also enable encryption on all of the recording servers. Before you enable encryption, you must install security certificates on the management server and all recording servers.

#### Certificate distribution for management servers

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication to the management server.




❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (management server) and by the party that verifies the certificate (recording servers)

❷ The CA certificate must be trusted on all recording servers. In this way the recording servers can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish secure connection between the management server and the recording servers

❹ The CA certificate must be installed on the computer on which the management server is running

Requirements for the private management server certificate:

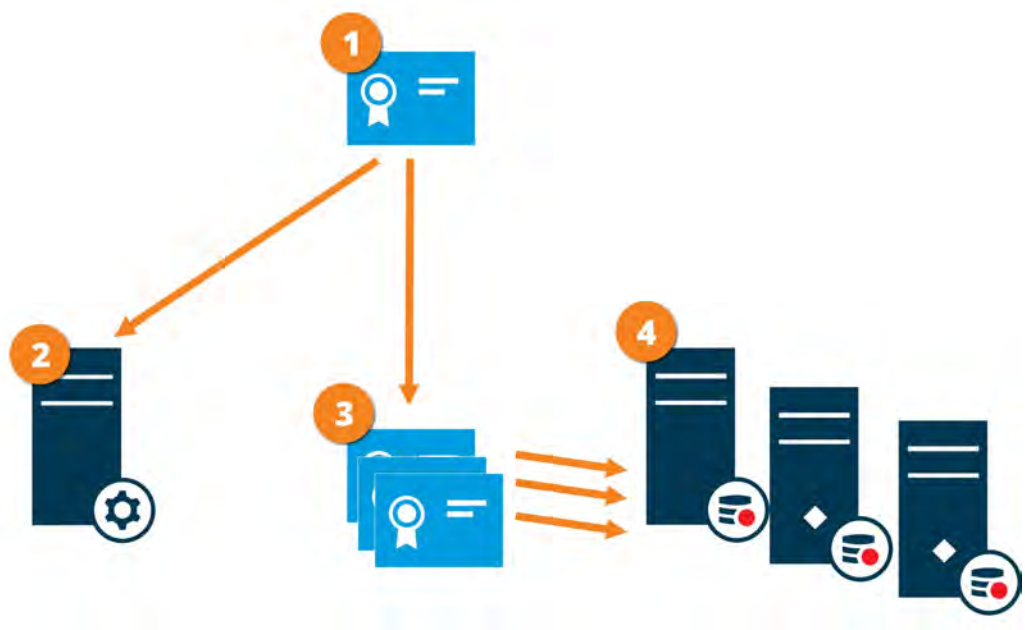
- Issued to the management server so that the management server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on the management server itself, by trusting the CA certificate that was used to issue the management server certificate
- Trusted on all recording servers connected to the management server, by trusting the CA certificate that was used to issue the management server certificate

### Encryption from the management server to the recording server (explained)

You can encrypt the two-way connection between the management server and the recording server. When you enable encryption on the management server, it applies to connections from all the recording servers that connect to the management server. Encryption of this communication must follow the encryption setting on the management server. So, if management server encryption is enabled, this must also be enabled on the recording servers, and vice-versa. Before you enable encryption, you must install security certificates on the management server and all recording servers, including failover recording servers.

**Certificate distribution**

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication from the management server.




1 A CA certificate acts as a trusted third party, trusted by both the subject/owner (recording server) and by the party that verifies the certificate (management server)

2 The CA certificate must be trusted on the management server. In this way the management server can verify the validity of the certificates issued by the CA

3 The CA certificate is used to establish secure connection between the recording servers and the management server

4 The CA certificate must be installed on the computers on which the recording servers are running

Requirements for the private recording server certificate:

- Issued to the recording server so that the recording server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on the management server, by trusting the CA certificate that was used to issue the recording server certificate

### Encryption to clients and servers that retrieve data from the recording server (explained)

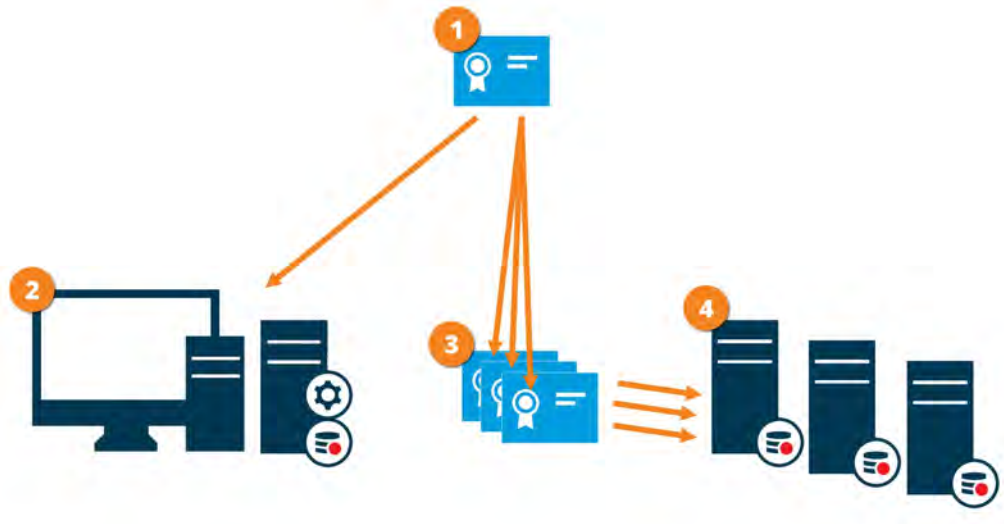
When you enable encryption on a recording server, communication to all clients, servers, and integrations that retrieve data streams from the recording server are encrypted. In this document referred to as 'clients':

- XProtect Smart Client
- Management Client
- Management Server (for System Monitor and for images and AVI video clips in email notifications)
- XProtect Mobile Server
- XProtect Event Server
- XProtect LPR
- ONVIF Bridge
- XProtect DLNA Server
- Sites that retrieve data streams from the recording server through Milestone Interconnect
- Some third-party MIP SDK integrations

> ⚠ For solutions built with MIP SDK 2018 R3 or earlier that accesses recording servers: If the integrations are made using MIP SDK libraries, they need to be rebuilt with MIP SDK 2019 R1; if the integrations communicate directly with the Recording Server APIs without using MIP SDK libraries, the integrators must add HTTPS support themselves.

**Certificate distribution**

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication to the recording server.




1 A CA certificate acts as a trusted third-party, trusted by both the subject/owner (recording server) and by the party that verifies the certificate (all clients)

❷ The CA certificate must be trusted on all clients. In this way the clients can verify the validity of the certificates issued by the CA

❸ The CA certificate is used to establish secure connection between the recording servers and all clients and services

❹ The CA certificate must be installed on the computers on which the recording servers are running

Requirements for the private recording server certificate:

- Issued to the recording server so that the recording server's host name is included in the certificate, either as subject (owner) or in the list of DNS names that the certificate is issued to
- Trusted on all computers running services that retrieve data streams from the recording servers, by trusting the CA certificate that was used to issue the recording server certificate
- The service account that runs the recording server must have access to the private key of the certificate on the recording server.

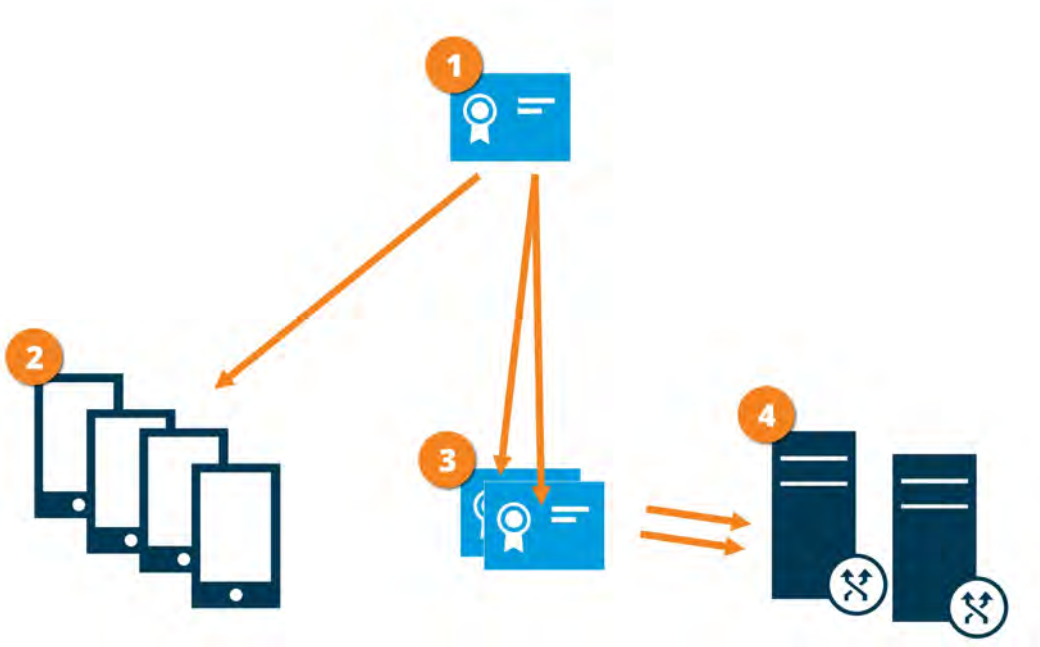
> If you enable encryption on the recording servers and your system applies failover recording servers, Milestone recommends that you also prepare the failover recording servers for encryption.

### Mobile server data encryption (explained)

In XProtect VMS, encryption is enabled or disabled per mobile server. When you enable encryption on a mobile server, you will have the option to use encrypted communication with all clients, services, and integrations that retrieve data streams.

#### Certificate distribution for mobile servers

The graphic illustrates the basic concept of how certificates are signed, trusted, and distributed in XProtect VMS to secure the communication with the mobile server.




1. A CA certificate acts as a trusted third party, trusted by both the subject/owner (mobile server) and by the party that verifies the certificate (all clients)
2. The CA certificate must be trusted on all clients. In this way clients can verify the validity of the certificates issued by the CA
3. The CA certificate is used to establish secure connection between the mobile server and clients and services
4. The CA certificate must be installed on the computer on which the mobile server is running

**Requirements for the CA certificate:**

- The mobile server's host name must be included in the certificate, either as subject/owner or in the list of DNS names that the certificate is issued to
- The certificate must be trusted on all devices that are running services that retrieve data streams from the mobile server
- The service account that runs the mobile server must have access to the private key of the CA certificate

### Mobile server encryption requirements for clients

If you do not enable encryption and use an HTTP connection, the push-to-talk feature in XProtect Web Client will not be available.

If you select a self-signed certificate for the encryption of the mobile server, XProtect Mobile client will not be able to connect with the mobile server.

## Kerberos authentication (explained)

Kerberos is a ticket-based network authentication protocol. It is designed to provide strong authentication for client/server or server/server applications.

Use Kerberos authentication as an alternative to the older Microsoft NT LAN (NTLM) authentication protocol.

Kerberos authentication requires mutual authentication, where the client authenticates to the service and the service authenticates to the client. This way you can authenticate more securely from XProtect clients to XProtect servers without exposing your password.

To make mutual authentication possible in your XProtect VMS you must register Service Principal Names (SPN) in the active directory. An SPN is an alias that uniquely identifies an entity such as a XProtect server service. Every service that uses mutual authentication must have an SPN registered so that clients can identify the service on the network. Without correctly registered SPNs, mutual authentication is not possible.

The table below lists the different Milestone services with corresponding port numbers you need to register:

| Service | Port number |
|---|---|
| **Management server - IIS** | 80 - Configurable |
| **Management server - Internal** | 8080 |
| **Recording server - Data Collector** | 7609 |
| **Failover Server** | 8990 |
| **Event Server** | 22331 |
| **LPR Server** | 22334 |

The number of services you need to register in the active directory depends on your current installation. Data Collector is installed automatically when installing Management Server, Recording Server, Event Server, LPR Server or Failover Server.

You must register two SPNs for the user running the service: one with the host name and one with the fully qualified domain name.

If you are running the service under a network user service account, you must register the two SPNs for each computer running this service.

This is the Milestone SPN naming scheme:

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

The following is an example of SPNs for the recording server service running on a computer with the following details:

```
Hostname: Record-Server1
Domain: Surveillance.com
```

SPNs to register:
`VideoOS/Record-Server1:7609`
`VideoOS/Record-Server1.Surveillance.com:7609`

## Use Windows update

Milestone recommends that you use Windows Update to protect your VMS against vulnerabilities in the operating system by making sure that the latest updates are installed.XProtect VMS is Windows-based, so security updates from Windows Update are important.

Updates can require a connection to the Internet, so Milestone recommends that this connection is open only as required, and that it is monitored for unusual traffic patterns.

Windows Updates often require a restart. This can be a problem if high-availability is required, because the server cannot receive data from devices while it restarts.

There are several ways to avoid this, or minimize the impact. For example, you can download updates to the server, and then apply them at a time when a restart will disrupt surveillance as little as possible.

If high availability is a concern, Milestone recommends that you run management server and event servers in clusters that include one or more failover servers. The failover server will take over while the recording server restarts, and surveillance is not interrupted. Do not include recording servers in the cluster. For recording servers, use a failover recording server.

Before implementing Windows updates across the organization, Milestone recommends that you verify the updates in a test environment. See NIST 800-53 CM-8 *Information system component inventory and sandboxing and SC-44 Detonation Chambers*.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SI-2 *Flaw Remediation*

## Keep software and device firmware updated

Milestone recommends that you use the latest version of XProtect VMS and firmware for the hardware devices, for example the cameras. This will ensure that your system includes the latest security fixes.

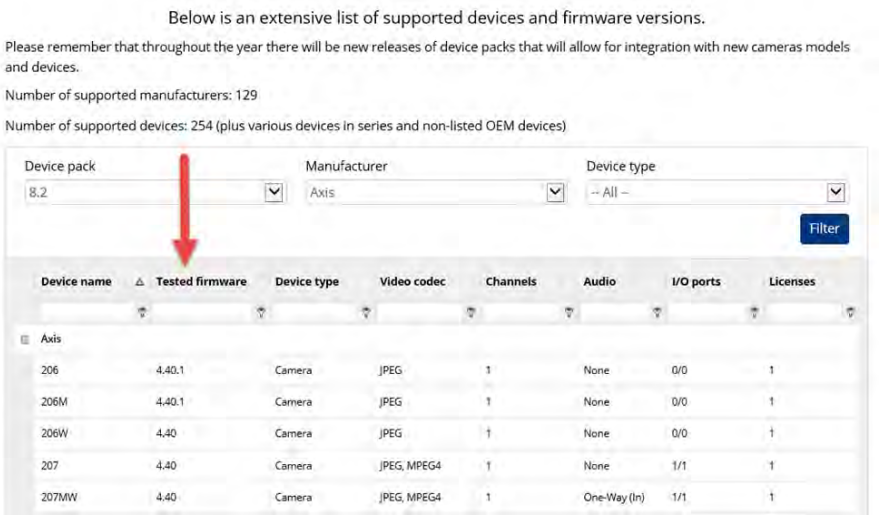
For hardware, network components, and operating systems, check the CVE database as well as any updates pushed out by manufacturers.

Before you upgrade the device firmware, verify that XProtect VMS supports it. Also, make sure that the device pack installed on the recording servers supports the device firmware.

Do this in a test environment for configuration, integration and testing before putting it into the production environment.

To verify that the VMS supports a device, follow these steps:

1. Open this link (https://www.milestonesys.com/solution-partners/supported-hardware/).
2. Click the link that matches your XProtect VMS product.
3. In the **Device pack** column, select the version of the current device pack.
4. Select the manufacturer of your device, and then click **Filter**. The version of the firmware that the device pack supports is listed in the **Tested Firmware** column.




**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SI-2 *Flaw Remediation*

## Use antivirus on all servers and computers

Milestone recommends that you deploy anti-virus software on all servers and computers that connect to the VMS. Malware that gets inside your system can lock, encrypt, or otherwise compromise data on the servers and other devices on the network.

If mobile devices connect to the VMS, this includes ensuring that the devices have the latest operating systems and patches (though not directly anti-virus) installed.

When you do virus scanning, do not scan recording server directories and subdirectories that contain recording databases. In addition, do not scan for viruses on archive storage directories. Scanning for viruses on these directories can impact system performance.

For information about the ports, directories, and subdirectories to exclude from the virus scan, see the section *About virus scanning* in the *XProtect VMS - Administrator manual*.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 PL-8 *Information Security Architecture*
- NIST SP 800-53 SI-2 *Flaw remediation*
- NIST SP 800-53 SI-3 *Malicious Code Protection*
- NIST SP 800-53 SI *Information Systems Monitoring*

## Monitor logs in the VMS for signs of suspicious activity

XProtect VMS provides features for generating and viewing logs that provide information about patterns of use, system performance, and other issues.Milestone recommends that you monitor the logs for signs of suspicious activities.

There are tools that leverage logs for operational and security purposes. Many businesses use syslog servers to consolidate logs. You can use syslog to note activities at a Windows level, however, XProtect VMS does not support syslog.

Milestone recommends that you use the Audit Log in XProtect VMS, and enable user access logging in Management Client. By default, the Audit Log notes only user logins. However, you can turn on user access logging so that the Audit Log notes all user activities in all of the client components of XProtect VMS products. This includes the times of the activities and the source IP addresses.

The client components are XProtect Smart Client, Web Client, the XProtect Management Client component, and integrations made by using the MIP SDK. Examples of activities are exports, activating outputs, viewing cameras live or in playback, and so on.

The Audit log does not note unsuccessful login attempts, or when the user logs out.

Logging all user activities in all clients increases the load on the system, and can affect performance.

You can adjust the load by specifying the following criteria that controls when the system will generate a log entry:

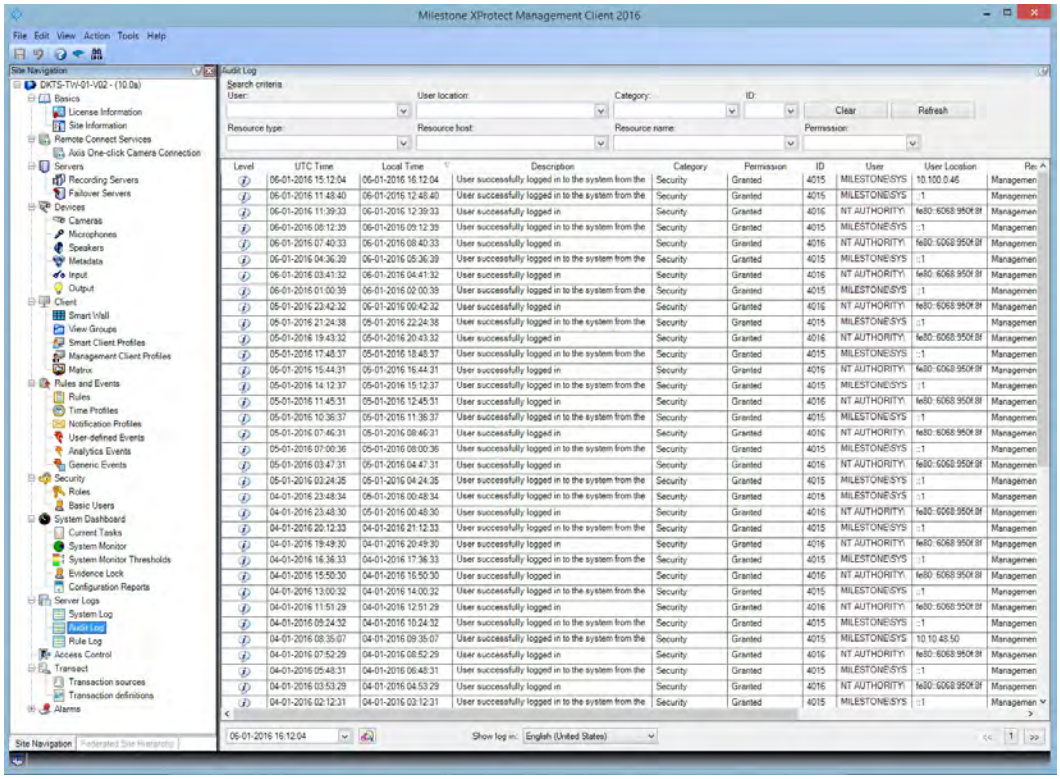
- The number of seconds that comprise one sequence. The VMS generates one log entry when a user plays video within the sequence.
- The number of frames that a user must view when playing back video before the VMS generates a log entry.

To turn on and configure extended user access logging, follow these steps:

1. In Management Client, click **Tools**, and select **Options**.
2. On the **Server Logs** tab, under **Log settings**, select **Audit Log**.
3. Under **Settings**, select the **Enable user access logging** check box.
4. Optional: To specify limitations for the information that is noted, and reduce impact on performance, make selections in the **Playback sequence logging length** and **Records seen before logging** fields.

To view the Audit Log in XProtect VMS, follow these steps:

1. Open Management Client.
2. Expand the **Server Logs** node.
3. Click **Audit Log**.




**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AU-3 *Content of Audit Records*
- NIST SP 800-53 RA-5 *Vulnerability Scanning*
- NIST SP 800-53 AU-6 *Audit Review, Analysis and Reporting*

# Advanced steps

Adopt standards for secure network and VMS implementations ..... 37
Establish an incident response plan ..... 37
Protect sensitive VMS components ..... 38
Follow Microsoft OS Security best practices ..... 38
Use tools to automate or implement the security policy ..... 38
Follow established network security best practices ..... 39

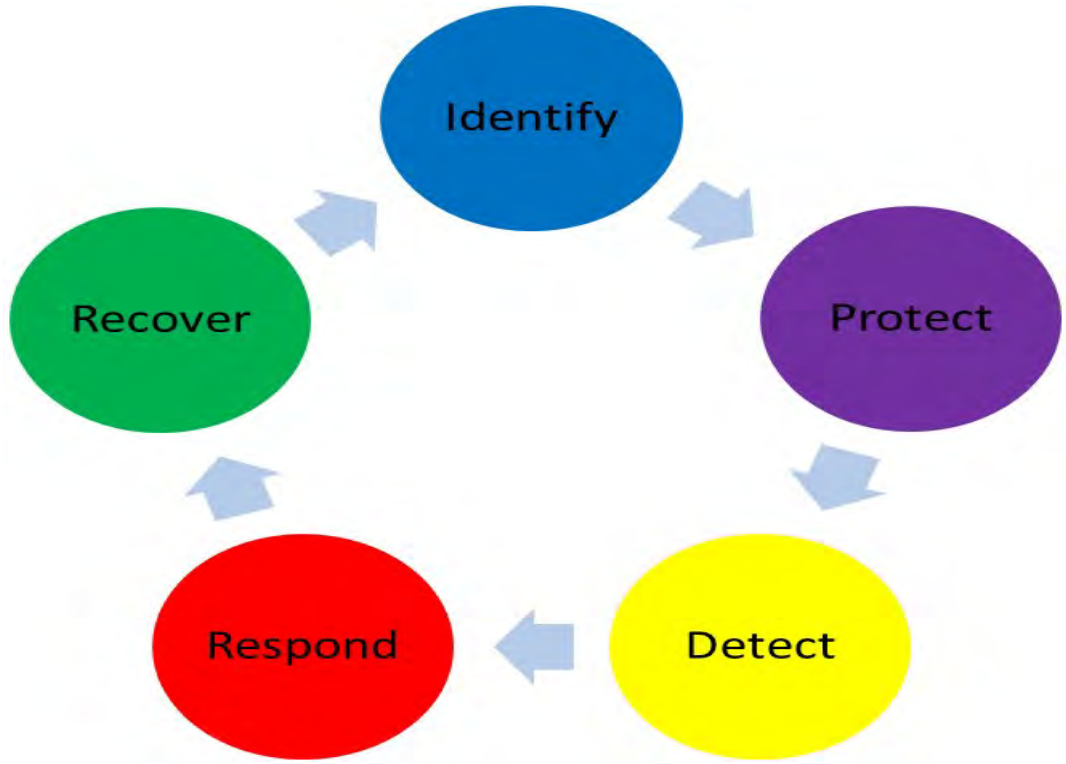
## Adopt standards for secure network and VMS implementations

Milestone recommends that you adopt standards for secure networking and XProtect VMS implementations. The use of standards is a basic component of Internet and network engineering, and the basis of interoperability and system conformance. This also applies to the use of cryptographic solutions, where standards-based cryptography is the most commonly accepted approach.

## Establish an incident response plan

Milestone recommends you start with a set of policies and procedures and establish an incident response plan. Designate staff to monitor the status of the system and respond to suspicious events. For example, activities that happen at unusual times. Establish a security Point of Contact (POC) with each of your vendors, including Milestone.

The following image is adapted from the NIST Cybersecurity Framework (http://www.nist.gov/cyberframework/). It shows the lifecycle that needs to be considered when creating a plan. The supporting material in the framework provide details about the lifecycle and security controls for incident response plans.




**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 IR 1-13 *Incident Response*

## Protect sensitive VMS components

Milestone recommends that you use physical access control, and use the VMS to monitor and protect its sensitive VMS components. Physical restriction and role-based physical access control are countermeasures that keep servers and workstations secure.

Administrators and users should only have access to the information they need in order to fulfill their responsibilities. If all internal users have the same access level to critical data, it's easier for attackers to access the network.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 PE-1 *Physical and Environmental Protection Policy and Procedures*
- NIST SP 800-53 PE-2 *Physical Access Authorizations*
- NIST SP 800-53 PE-3 *Physical Access Control*
- NIST SP 800-53 AC-4 *Least Privilege*

## Follow Microsoft OS Security best practices

Milestone recommends that you follow the security best practices for Microsoft operating systems (OS) to mitigate OS risks and maintain security. This will help you keep the Microsoft servers and client computers secure.

For more information, see *Microsoft Security Update Guide* (https://technet.microsoft.com/en-us/security/dn550891.aspx).

## Use tools to automate or implement the security policy

Milestone recommends that you find one or more tools to help you automate and implement the security policy. Automation reduces the risk of human error and makes it easier to manage the policy. For example, you can automate the installation of security patches and updates on servers and client computers.

One way to implement this recommendation is to combine the Microsoft Security Configuration Manager (SCCM) with the Security Content Automation Protocol (SCAP).(See for example, *Geek of All Trades: Automate Baseline Security Settings* (https://technet.microsoft.com/en-us/magazine/ff721825.aspx) and *Security Content Automation Protocol (SCAP) Validation Program* (http://scap.nist.gov/validation/).) This gives you a framework to create, distribute, and validate security settings on computers across your network.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST SP 800-53 CM-2 *Baseline Configuration*
- NIST SP 800-53 CM-3 *Configuration Change Control*

## Follow established network security best practices

Milestone recommends that you follow IT and vendor best practices to ensure that devices on your network are securely configured. Ask your vendors to provide this information. It is important to open and maintain a security dialogue, and a discussion of best practices is a good place to start.

It is important to deny access to the VMS by not using vulnerable network settings. For more information, see *SP 800-128* (http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf), *SP 800-41-rev1* (http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf) (specific to firewalls), and *ICS-CERT Standards and References* (https://ics-cert.us-cert.gov/Standards-and-References) (general list).

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 MA-3 *Maintenance Tools*

# Devices and network

This section provides guidance for hardening the devices and network components related to XProtect VMS. This includes key parts of the system such as the cameras, storage, and the network.

Surveillance systems often include cameras at the edge of the network. Cameras and their network connections, if left unprotected, represent a significant risk of compromise, potentially giving intruders further access to the system.

## Basic steps – Devices

Use strong passwords instead of default passwords ..... 40

Stop unused services and protocols ..... 40

Create dedicated user accounts on each device ..... 41

Scanning for devices ..... 42

### Use strong passwords instead of default passwords

Milestone recommends that you change the default passwords on devices, for example, on a camera. Do not use default passwords because they are often published to the Internet and are readily available.

Instead, use strong passwords for devices. Strong passwords include eight or more alpha-numeric characters, use upper and lower cases, and special characters.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 IA-4 *Authenticator Management*
- NIST 800-53 IA-8 *Authenticator Feedback*
- NIST 800-53 SI-11 *Error Handling*

### Stop unused services and protocols

To help avoid unauthorized access or information disclosure, Milestone recommends that you stop unused services and protocols on devices. For example, Telnet, SSH, FTP, UPnP, Ipv6, and Bonjour.

It is also important to use strong authentication on any services that access the VMS, network, or devices. For example, use SSH keys instead of user names and passwords, and use certificates from a Certificate Authority for HTTPS. For more information, see the hardening guides and other guidance from the device manufacturer.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-17 *Remote Access (Disable Unused Protocols)*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 CM-7 *Least Functionality*
- NIST SP 800-53 IA-2 *Identification and Authentication*
- NIST SP 800-53 SA-9 *External Information Services*

## Create dedicated user accounts on each device

All cameras have a default user account with a user name and password that the VMS uses to access the device. For auditing purposes, Milestone recommends that you change the default user name and password.

Create a user account specifically for use by the VMS, and use this user account and password when you add the camera to the VMS. When a recording server connects to the camera, it uses the user name and password you have created. If the camera has a log, this log shows that the recording server has connected to the camera.

With a dedicated user name and password, the device logs can help you determine whether a recording server or a person accessed the camera. This is relevant when investigating potential security issues affecting devices.

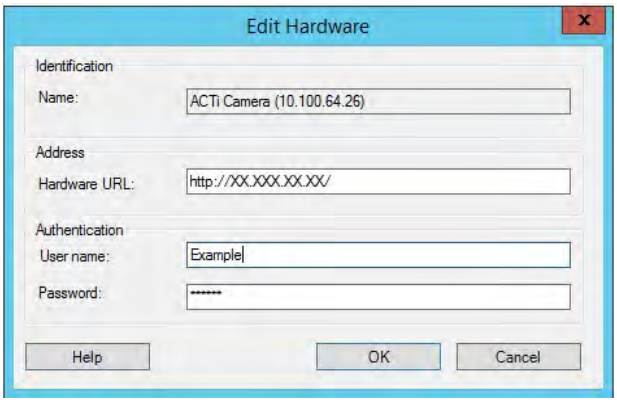
You can change the user name and password for a device before or after you add it in Management Client.

To change the user name and password before you add the device, follow these steps:

1. Go to the device's web interface, and change the default user name and password.
2. In Management Client, add the device, and specify the user name and password.

To change the user name and passwords of devices that are already added, follow these steps:

1. In Management Client, in the Site Navigation pane, expand the **Servers** node and select **Recording Servers**.
2. In the Recording Server pane, expand the recording server that contains the device, and then right-click the device and select **Edit hardware**.




3. Under **Authentication**, enter the new user name and password.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-4 *Least Privilege*

## Scanning for devices

Scanning for devices (for example, **Express** scan or **Address range scanning** when adding hardware) is done using broadcasts that may contain user names and passwords in plain text.

Unless this is an initial setup, this functionality should not be used for adding devices to the system. Use the **Manual** option instead and manually select the driver.

On sensitive systems, the **Automatic device discovery** functionality should be disabled on XProtect Professional VMS (located on **Settings** > **Connecting hardware devices**), because it will periodically send broadcasts that may contain user names and passwords.

# Basic steps – Network

Use secure and trusted networks connection ..... 42

Use firewalls to limit IP access to servers and computers ..... 43

Use a firewall between the VMS and the Internet ..... 53

Connect the camera subnet to the recording server subnet only ..... 54

## Use secure and trusted networks connection

Network communications must be secure, whether or not you are on a closed network. By default, secure communications should be used when accessing the VMS. For example:

- VPN tunnels or HTTPS by default
- Latest version of the Transport Layer Security (https://datatracker.ietf.org/wg/tls/charter/) (TLS, currently 1.2) with valid certificates that meet industry best practices, such as from Public-Key Infrastructure (X.509) (https://datatracker.ietf.org/wg/ipsec/documents/) and CA/Browser Forum (https://cabforum.org/).

Otherwise, credentials may be compromised and intruders might use them to access the VMS.

Configure the network to allow client computers to establish secure HTTPS sessions or VPN tunnels between the client devices and the VMS servers.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SI-2 *Flaw remediation*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 SC-23 *Session Authenticity*

## Use firewalls to limit IP access to servers and computers

Milestone recommends that you use secure connections, and the following additional steps:

- Use secure device authentication
- Use TLS
- Use device whitelisting to authenticate devices
- Use firewalls to limit network communication between servers and client computers and programs.

All XProtect components and the ports needed by them are listed in individual sections below. To ensure, for example, that the firewall blocks only unwanted traffic, you need to specify the ports that the XProtect VMS uses. You should only enable these ports. The lists also include the ports used for local processes.

They are arranged in two groups:

- Server components (services)—Offer their service on particular ports which is why they need to listen for client requests on these ports. Therefore, these ports need to be opened in the Windows Firewall for inbound connections.
- Client components (clients)—Initiate connections to particular ports on server components. Therefore, these ports need to be opened for outbound connections. Outbound connections are typically open by default in the Windows Firewall.

If nothing else is mentioned, ports for server components must be opened for inbound connections, and ports for client components must be opened for outbound connections.

Do keep in mind that server components can act as clients to other server components as well.

The port numbers are the default numbers, but this can be changed. Contact Milestone Support, if you need to change ports that are not configurable through the Management Client.

### Server components (inbound connections)

Each of the following sections list the ports which need to be opened for a particular service. In order to figure out which ports need to be opened on a particular computer, you need to consider all services running on this computer.

Restrict remote access to the Management Server by adding firewall rules to only allow Recording Servers to connect to TCP port 9993.

### Management Server service and related processes

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **80** | HTTP | IIS | All XProtect components | Main communication, for example, authentication and configurations. |
| | | | The Management Server service and Recording Server services | Handles registration of recording servers and management servers via the Authorization Server service. |
| **443** | HTTPS | IIS | XProtect Smart Client and the Management Client | Authentication of basic users. |
| | | | The Management Server service and Recording Server services | Handles registration of recording servers and management servers via the Authorization Server service. |
| **6473** | TCP | Management Server service | Management Server Manager tray icon, local connection only. | Showing status and managing the service. |
| **8080** | TCP | Management server | Local connection only. | Communication between internal processes on the server. |
| **9000** | HTTP | Management server | Recording Server services | Web service for internal communication between servers. |
| **9993** | TCP | Management Server service | Recording Server services | Authentication, configuration, token exchange. |

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **12345** | TCP | Management Server service | XProtect Smart Client | Communication between the system and Matrix recipients.<br>You can change the port number in the Management Client. |
| **12974** | TCP | Management Server service | Windows SNMP Service | Communication with the SNMP extension agent.<br>Do not use the port for other purposes even if your system does not apply SNMP.<br>In XProtect 2014 systems or older, the port number was 6475.<br>In XProtect 2019 R2 systems and older, the port number was 7475. |

**SQL Server service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **1433** | TCP | SQL Server | Management Server service | Storing and retrieving configurations. |
| **1433** | TCP | SQL Server | Event Server service | Storing and retrieving events. |
| **1433** | TCP | SQL Server | Log Server service | Storing and retrieving log entries. |

**Data Collector service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **7609** | HTTP | IIS | On the management server computer: Data Collector services on all other servers.<br>On other computers: Data Collector service on the Management Server. | System Monitor. |

**Event Server service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **1234** | TCP/UDP | Event Server Service | Any server sending generic events to your XProtect system. | Listening for generic events from external systems or devices.<br>Only if the relevant data source is enabled. |
| **1235** | TCP | Event Server service | Any server sending generic events to your XProtect system. | Listening for generic events from external systems or devices.<br>Only if the relevant data source is enabled. |
| **9090** | TCP | Event Server service | Any system or device that sends analytics events to your XProtect system. | Listening for analytics events from external systems or devices.<br>Only relevant if the Analytics Events feature is enabled. |
| **22331** | TCP | Event Server service | XProtect Smart Client and the Management Client | Configuration, events, alarms, and map data. |
| **22333** | TCP | Event Server service | MIP Plug-ins and applications. | MIP messaging. |

**Recording Server service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **25** | SMTP | Recording Server Service | Cameras, encoders, and I/O devices. | Listening for event messages from devices.<br>The port is disabled by default. |
| **5210** | TCP | Recording Server Service | Failover recording servers. | Merging of databases after a failover recording server had been running. |
| **5432** | TCP | Recording Server Service | Cameras, encoders, and I/O devices. | Listening for event messages from devices.<br>The port is disabled by default. |
| **7563** | TCP | Recording Server Service | XProtect Smart Client, Management Client | Retrieving video and audio streams, PTZ commands. |
| **8966** | TCP | Recording Server Service | Recording Server Manager tray icon, local connection only. | Showing status and managing the service. |
| **9001** | HTTP | Recording Server Service | Management server | Web service for internal communication between servers.<br>If multiple Recording Server instances are in use, every instance needs its own port. Additional ports will be 9002, 9003, etc. |
| **11000** | TCP | Recording Server Service | Failover recording servers | Polling the state of recording servers. |

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **12975** | TCP | Recording Server Service | Windows SNMP service | Communication with the SNMP extension agent.<br>Do not use the port for other purposes even if your system does not apply SNMP.<br>In XProtect 2014 systems or older, the port number was 6474.<br>In XProtect 2019 R2 systems and older, the port number was 7474. |
| **65101** | UDP | Recording Server service | Local connection only | Listening for event notifications from the drivers. |

In addition to the inbound connections to the Recording Server service listed above, the Recording Server service establishes outbound connections to the cameras.

**Failover Server service and Failover Recording Server service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **25** | SMTP | Recording Server Service | Cameras, encoders, and I/O devices. | Listening for event messages from devices.<br>The port is disabled by default. |
| **5210** | TCP | Recording Server Service | Failover recording servers | Merging of databases after a failover recording server had been running. |
| **5432** | TCP | Recording Server Service | Cameras, encoders, and I/O devices. | Listening for event messages from devices.<br>The port is disabled by default. |

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **7474** | TCP | Recording Server Service | Windows SNMP service | Communication with the SNMP extension agent.<br>Do not use the port for other purposes even if your system does not apply SNMP. |
| **7563** | TCP | Recording Server Service | XProtect Smart Client | Retrieving video and audio streams, PTZ commands. |
| **8844** | UDP | Failover recording servers | Local connection only. | Communication between the servers. |
| **8966** | TCP | Failover Recording Server Service | Failover Recording Server Manager tray icon, local connection only. | Showing status and managing the service. |
| **8967** | TCP | Failover Server Service | Failover Server Manager tray icon, local connection only. | Showing status and managing the service. |
| **8990** | TCP | Failover Server Service | Management Server service | Monitoring the status of the Failover Server service. |
| **9001** | HTTP | Failover Server Service | Management server | Web service for internal communication between servers. |

**Log Server service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **22337** | HTTP | Log Server service | All XProtect components except for Management Client and the recording server. | Write to, read from, and configure the log server. |

In addition to the inbound connections to the Failover Recording Server service listed above, the Recording Server service establishes outbound connections to the cameras.

**Mobile Server service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **8000** | TCP | Mobile Server service | Mobile Server Manager tray icon, local connection only. | SysTray application. |
| **8081** | HTTP | Mobile Server service | Mobile clients, Web clients, and Management Client. | Sending data streams; video and audio. |
| **8082** | HTTPS | Mobile Server service | Mobile clients and Web clients. | Sending data streams; video and audio. |

**LPR Server service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **22334** | TCP | LPR Server Service | Event server | Retrieving recognized license plates and server status.<br>In order to connect, the Event server must have the LPR plug-in installed. |
| **22334** | TCP | LPR Server Service | LPR Server Manager tray icon, local connection only. | SysTray application |

**Milestone ONVIF Bridge service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **580** | TCP | ONVIF Bridge Service | ONVIF clients | Authentication and requests for video stream configuration. |
| **554** | RTSP | RTSP Service | ONVIF clients | Streaming of requested video to ONVIF clients. |

**XProtect DLNA Server service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **9100** | HTTP | DLNA Server Service | DLNA device | Device discovery and providing DLNA channels configuration. Requests for video streams. |
| **9200** | HTTP | DLNA Server Service | DLNA device | Streaming of requested video to DLNA devices. |

**XProtect Screen Recorder service**

| Port number | Protocol | Process | Connections from... | Purpose |
|---|---|---|---|---|
| **52111** | TCP | XProtect Screen Recorder | Recording Server Service | Provides video from a monitor. It appears and acts in the same way as a camera on the recording server.<br>You can change the port number in the Management Client. |

**Server components (outbound connections)**

**Management Server service**

| Port number | Protocol | Connections to... | Purpose |
|---|---|---|---|
| **443** | HTTPS | Milestone Customer Dashboard via<br>https://service.milestonesys.com/ | Send status, events and error messages from the XProtect system to Milestone Customer Dashboard. |
| **443** | HTTPS | The License server that hosts the License Management service. Communication is via https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx | Activating licenses. |

**Log Server service**

| Port number | Protocol | Connections to... | Purpose |
|---|---|---|---|
| 443 | HTTP | Log server | Forwarding messages to the log server. |

**Cameras, encoders, and I/O devices (inbound connections)**

| Port number | Protocol | Connections from... | Purpose |
|---|---|---|---|
| 80 | TCP | Recording servers and failover recording servers | Authentication, configuration, and data streams; video and audio. |
| 443 | HTTPS | Recording servers and failover recording servers | Authentication, configuration, and data streams; video and audio. |
| 554 | RTSP | Recording servers and failover recording servers | Data streams; video and audio. |

**Cameras, encoders, and I/O devices (outbound connections)**

| Port number | Protocol | Connections to... | Purpose |
|---|---|---|---|
| 25 | SMTP | Recording servers and failover recording servers | Sending event notifications (deprecated). |
| 5432 | TCP | Recording servers and failover recording servers | Sending event notifications.<br>The port is disabled by default. |
| 22337 | HTTP | Log server | Forwarding messages to the log server. |

Only a few camera models are able to establish outbound connections.

**Client components (outbound connections)**

**XProtect Smart Client, XProtect Management Client, XProtect Mobile server**

| Port number | Protocol | Connections to... | Purpose |
|---|---|---|---|
| 80 | HTTP | Management Server service | Authentication |
| 443 | HTTPS | Management Server service | Authentication of basic users. |

| Port number | Protocol | Connections to... | Purpose |
|---|---|---|---|
| **7563** | TCP | Recording Server service | Retrieving video and audio streams, PTZ commands. |
| **22331** | TCP | Event Server service | Alarms. |

**XProtect Web Client, XProtect Mobile client**

| Port number | Protocol | Connections to... | Purpose |
|---|---|---|---|
| **8081** | HTTP | XProtect Mobile server | Retrieving video and audio streams. |
| **8082** | HTTPS | XProtect Mobile server | Retrieving video and audio streams. |

**Learn more**

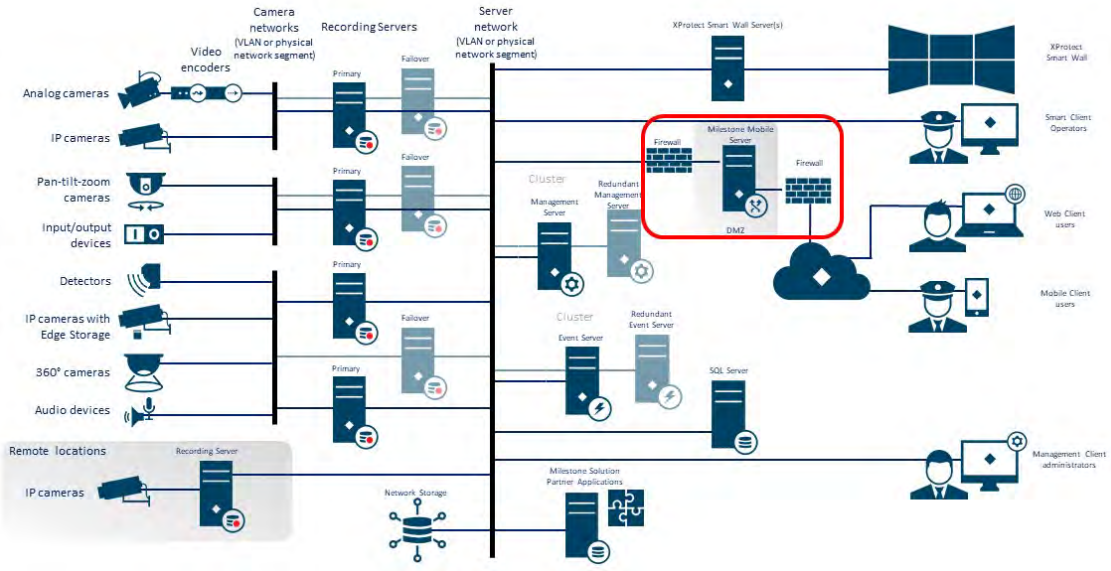
The following control(s) provide additional guidance:

- NIST SP 800-53 CA-3 *System Interconnections*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 SC-7 *Boundary Protection*

## Use a firewall between the VMS and the Internet

The VMS should not connect directly to the Internet. If you expose parts of the VMS to the Internet, Milestone recommends that you use an appropriately configured firewall between the VMS and the Internet.

If possible, expose only the Milestone Mobile server component to the Internet, and locate it in a demilitarize zone (DMZ) with firewalls on both sides. This is illustrated in the following figure.




**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 CA-3 *System Interconnections*

## Connect the camera subnet to the recording server subnet only

Milestone recommends that you connect the camera subnet only to the recording server subnet. The cameras and other devices need to communicate only with the recording servers. For more information, see Recording Server on page 63.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 SC-7 *Boundary Protection*

# Advanced steps – Devices

## Use Simple Network Management Protocol to monitor events

Milestone recommends that you use Simple Network Management Protocol (SNMP) to monitor events on the devices on the network. You can use SNMP as a supplement for syslog. SNMP works in real-time with many types of events that can trigger alerts, for example if a device is restarted.

For this to work, the devices must support logging via SNMP.

There are multiple versions of SNMP protocols available. Versions 2c and 3 are the most current. Implementation involves a suite of standards. A good overview can be found on the SNMP reference site (http://www.snmp.com/protocol/snmp_rfcs.shtml).

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SI-4 *Event Monitoring*

# Advanced steps – Network

Use secure wireless protocols ..... 55

Use port-based access control ..... 55

Run the VMS on a dedicated network ..... 56

## Use secure wireless protocols

If you use wireless networks, Milestone recommends that you use a secure wireless protocol to prevent unauthorized access to devices and computers. For example, use standardized configurations. The NIST guidance on wireless local area networks provides specific details on network management and configuration. For more information, see *SP 800-48 revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks* (http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf).

Additionally, Milestone recommends that you do not use wireless cameras in mission-critical locations. Wireless cameras are easy to jam, which can lead to loss of video.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-18 *Wireless Access*
- NIST SP 800-53 SC-40 *Wireless Link Protection*

## Use port-based access control

Use port-based access control to prevent unauthorized access to the camera network. If an unauthorized device connects to a switch or router port, the port should become blocked. Information about how to configure switches and routers is available from the manufacturers. See *SP 800-128, Guide for Security-Focused Configuration Management of Information Systems* (http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf), for information about configuration management of information systems.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST 800-53 CM-2 *Baseline Configuration*
- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

## Run the VMS on a dedicated network

Milestone recommends that, whenever possible, you separate the network where the VMS is running from networks with other purposes. For example, a shared network such as the printer network should be isolated from the VMS network. In addition, XProtect VMS deployments should follow a general set of best practices for system interconnections.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 CA-3 *System Interconnections*

# Milestone Servers

This section contains guidance on how to protect the Milestone servers.

## Basic steps – Milestone servers

Use physical access controls and monitor the server room ..... 57

Use encrypted communication channels ..... 57

### Use physical access controls and monitor the server room

Milestone recommends that you place the hardware with the servers installed in a designated server room, and that you use physical access controls. In addition, you should maintain access logs to document who has had physical access to the servers. Surveillance of the server room is also a preventive precaution.

Milestone supports integration of access control systems and their information. For example, you can view access logs in XProtect Smart Client.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 PE-3 *Physical Access Control*

### Use encrypted communication channels

Milestone recommends that you use a VPN for communication channels for installations where servers are distributed across untrusted networks. This is to prevent attackers from intercepting communications between the servers. Even for trusted networks, Milestone recommends that you use HTTPS for configuration of cameras and other system components.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 AC-4 *Information Flow Enforcement*
- NIST 800-53 AC-17 *Remote Access*

## Advanced steps – Milestone servers

Run services with service accounts ..... 58

Run components on dedicated virtual or physical servers ..... 58

Restrict the use of removable media on computers and servers ..... 58

Use individual administrator accounts for better auditing ..... 58

Use subnets or VLANs to limit server access ..... 59

Enable only the ports used by Event Server .....59

## Run services with service accounts

Milestone recommends that you create service accounts for services related to XProtect VMS, instead of using a regular user account. Set up the service accounts as domain users, and only give them the permissions required to run the relevant services. See Kerberos authentication (explained) on page 32. For example, the service account should not be able to log on to the Windows desktop.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 AC-5 *Separation of Duties*
- NIST 800-53 AC-6 *Least Privilege*

## Run components on dedicated virtual or physical servers

Milestone recommends that you run the components of XProtect VMS only on dedicated virtual or physical servers without any other software or services installed.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 CM-9 *Configuration Management Plan*

## Restrict the use of removable media on computers and servers

Milestone recommends that you restrict the use of removable media, for example USB keys, SD cards, and smartphones on computers and servers where components of XProtect VMS are installed. This helps prevent malware from entering the network. For example, allow only authorized users to connect removable media when you need to transfer video evidence.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 MP-7 *Media Use*

## Use individual administrator accounts for better auditing

As opposed to shared administrator accounts, Milestone recommends using individual accounts for administrators. This lets you track who does what in XProtect VMS. This helps prevent malware from entering the network. You can then use an authoritative directory such as Active Directory to manage the administrator accounts.

You assign administrator accounts to roles in Management Client under **Roles**.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 AC-5 *Separation of Duties*
- NIST 800-53 CM-9 *Configuration Management Plan*

## Use subnets or VLANs to limit server access

Milestone recommends that you logically group different types of hosts and users into separate subnets. This can have benefits in managing privileges for these hosts and users as members of a group with a given function or role. Design the network so that there is a subnet or VLAN for each function. For example, one subnet or VLAN for surveillance operators and one for administrators. This allows you to define firewall rules by group instead of for individual hosts.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CSC 11: *Secure Configurations for Network Devices such as Firewalls, Routers, and Switches*
- NIST SP 800-53 SC-7 *Boundary Protection*

## Enable only the ports used by Event Server

Milestone recommends that you enable only the ports used by event server, and block all other ports, including the default Windows ports.

The event server ports used in XProtect VMS are: 22331, 22333, 9090, 1234, and 1235.

The ports used depend on the deployment. If in doubt, contact Milestone Support.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 CSC 11: *Secure Configurations for Network Devices such as Firewalls, Routers, and Switches*

# SQL Server

## Connection to the SQL Server and database

Communication between the Milestone XProtect VMS and the SQL Server and database can potentially be tampered by an attacker because the certificate is not validated.

To mitigate this, you must first set up verifiable server certificates. After the certificates are set up, you must modify the ConnestionString in the Windows registry by removing trustServerCertificate=true, as follows:

Registry key: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\Common\ConnectionString

- Current

  connection string: Data Source=localhost;initial catalog='Surveillance';Integrated Security=SSPI;encrypt=true;trustServerCertificate=true

- Hardened

  connection string: Data Source=localhost;initial catalog='Surveillance';Integrated Security=SSPI;encrypt=true

This results in encryption occurring only if there is a verifiable server certificate, otherwise the connection attempt fails.

This issue is described in detail in the article Using Encryption Without Validation.

## Run the SQL Server and database on a separate server

Milestone recommends that you make the SQL Server and database redundant. This reduces the risk of real or perceived downtime.

To support Windows Server Failover Clustering (WSFC), Milestone recommends that you run the SQL Server and database on a separate server, and not on the management server.

SQL Server must run in WSFC setup, and the management and event servers must run in a Microsoft Cluster setup (or similar technology). For more information about WSFC, see *Windows Server Failover Clustering (WSFC) with SQL Server* (https://msdn.microsoft.com/en-us/library/hh270278.aspx).

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 SC-7 *Boundary Protection*
- NIST 800-53 CM-9 *Configuration Management Plan*

# Management Server

Adjust the token time-out ..... 60

Enable only the ports used by the management server ..... 61

Disable non-secure protocols ..... 61

Disable legacy remoting channel ..... 62

Disable IIS header information ..... 62

## Adjust the token time-out

XProtect VMS uses session tokens when it logs in to the management server using SSL (basic users) or NTLM (Windows users) protocols. A token is retrieved from the management server and used on the secondary servers, for example the recording server and sometimes also the event server. This is to avoid that NTLM and AD lookup

is performed on every server component.

By default, a token is valid for 240 minutes. You can adjust this down to 1 minute intervals. This value can also be adjusted over time. Short intervals increase security, however, the system generates additional communication when it renews the token.

The best interval to use depends on the deployment. This communication increases the system load and can impact performance.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 IA-5 *Authenticator Management*

## Enable only the ports used by the management server

Milestone recommends that you enable only the ports used by the management server, and that you block all other ports, including the default Windows ports. This guidance is consistent for the server components of XProtect VMS.

The management server ports used in XProtect VMS are: 80, 443, 1433, 7475, 8080, 8990, 9993, 12345.

The ports used depend on the deployment. If in doubt, contact Milestone Support.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 SC-7 *Boundary Protection*

## Disable non-secure protocols

When a basic user logs in to the management server through IIS, the Management Client will use any protocol available.Milestone recommends that you always implement the latest version of the Transport Layer Security (TLS, currently 1.2) (https://datatracker.ietf.org/wg/tls/charter/), and disable all improper cipher suites and obsolete versions of SSL/TLS protocols. Perform actions to block non-secure protocols at the OS level. This prevents the Management Client from using protocols that are not secure. The OS determines the protocol to use.

The protocols used depend on the deployment. If in doubt, contact Milestone Support.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 AC-17 *Remote Access (Disable Unused Protocols)*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

## Disable legacy remoting channel

Communication between the recording servers and the management server has become more secure with the solution implemented in 2019 R2. If you upgrade from a previous XProtect VMS release, the management server still starts the legacy 3rd party technology to be able to communicate with recording servers on older releases.

When all recording servers in your system are upgraded to version 2019 R2 or later, you can configure the management server to not start the legacy remoting channel, to make your system less vulnerable, Milestone recommends that you set **UseRemoting** to **False** in the management server configuration file.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 AC-17 *Remote Access (Disable Unused Protocols)*
- NIST 800-53 CM-6 *Configuration Settings*

## Disable IIS header information

For security purposes, Milestone recommends that you disable the X-Powered-By HTTP and X-AspNet-Version headers.

The HTTP header X-Powered-By reveals the version of IIS being used on the server. Disable this header by doing the following:

1. Open the IIS Manager.
2. Select the Default website.
3. Select **HTTP Response Headers**.
4. Select the **X-Powered-By** HTTP header and select **Remove**.

The HTTP header X-AspNet-Version reveals the version of ASP.NET being used by the Management Server application pool. Disable this header by doing the following:

1. Open the web.config file located in %windir%\Microsoft.NET\Framework\v4.0.30319\CONFIG.
2. After the `<system.web>` tag, add this: `<httpRuntime enableVersionHeader="false" />`
3. Save the file.

The SERVER header variable should not be removed, because it will cause functionality within Management Server to break.

# Recording Server

Storage and Recording Settings properties ....63
Use separate network interface cards ....65
Harden Network Attached Storage (NAS) to store recorded media data ....65

## Storage and Recording Settings properties

Available functionality depends on the system you are using. See https://www.milestonesys.com/solutions/platform/product-index/ for more information.

In the **Storage and Recording Settings** dialog box, specify the following:

| Name | Description |
|---|---|
| **Name** | Rename the storage if needed. Names must be unique. |
| **Path** | Specify the path to the directory to which you save recordings in this storage. The storage does not necessarily have to be located on the recording server computer.<br><br>If the directory does not exist, you can create it. Network drives must be specified by using UNC (Universal Naming Convention) format, example: \\server\volume\directory\. |
| **Retention time** | Specify for how long recordings should stay in the archive before they are deleted or moved to the next archive (depending on archive settings).<br><br>The retention time must always be longer than the retention time of the previous archive or the default recording database. This is because the number of retention days specified for an archive includes all the retention periods stated earlier in the process. |

| Name | Description |
|---|---|
| **Maximum size** | Select the maximum number of gigabytes of recording data to save in the recording database.<br><br>Recording data in excess of the specified number of gigabytes is auto-moved to the first archive in the list - if any is specified - or deleted.<br><br>When less than 5GB of space is free, the system always auto-archives (or deletes if no next archive is defined) the oldest data in a database. If less than 1GB space is free, data is deleted. A database always requires 250MB of free space. If you reach this limit (if data is not deleted fast enough), no more data is written to the database until you have freed enough space. The actual maximum size of your database is the amount of gigabytes you specify, minus 5GB. |
| **Signing** | Enables a digital signature to the recordings. This means, for example, that the system confirms that exported video has not been modified or tampered with when played back.<br><br>The system uses the SHA-2 algorithm for digital signing. |
| **Encryption** | Select the encryption level of the recordings:<br><br>• **None**<br>• **Light (Less CPU usage)**<br>• **Strong (More CPU usage)**<br><br>The system uses the AES-256 algorithm for encryption.<br><br>If you select **Light**, a part of the recording is encrypted. If you select **Strong**, the whole recording is encrypted.<br><br>If you choose to enable encryption, you must also specify a password below. |
| **Password** | Enter a password for the users allowed to view encrypted data.<br><br>Milestone recommends that you use strong passwords. Strong passwords do not contain words that can be found in a dictionary or are part of the user's name. They include eight or more alpha-numeric characters, upper and lower cases, and special characters. |

## Use separate network interface cards

Milestone recommends that you use multiple network interface cards (NICs) to separate the communication between recording servers and devices from the communication between recording servers and client programs. Client programs do not need to communicate directly with devices.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*

## Harden Network Attached Storage (NAS) to store recorded media data

The Recording Server can use Network Attached Storage (NAS) to store recorded media data.

If you choose to use NAS, it can be hardened by using SMB 3.0 security enhancements, as described in this document on SMB security enhancements.

# Milestone Mobile server component

Only enable ports that Milestone Mobile server uses ..... 65

Use a "demilitarized zone" (DMZ) to provide external access ..... 66

Disable non-secure protocols ..... 66

Set up users for two-step verification via email ..... 66

## Only enable ports that Milestone Mobile server uses

Milestone recommends that you enable only the ports that XProtect Mobile server uses, and block all other ports, including the default Windows ports.

By default, mobile server uses ports 8081 and 8082.

The ports used depend on the deployment. If in doubt, contact Milestone Support.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 SC-7 *Boundary Protection*

## Use a "demilitarized zone" (DMZ) to provide external access

Milestone recommends that you install XProtect Mobile server in a DMZ, and on a computer with two network interfaces:

- One for internal communication
- One for public Internet access

This allows mobile client users to connect to Milestone Mobile server with a public IP address, without compromising the security or availability of the VMS network.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*

## Disable non-secure protocols

Milestone recommends that you use only the necessary protocols, and only the latest versions. For example, implement the latest version of the Transport Layer Security (TLS, currently 1.2) and disable all other cipher suites and obsolete versions of SSL/TLS protocols. This requires configuration of Windows and other system components, and the proper use of digital certificates and keys.

The same recommendation is given for the management server. For more information, see Disable non-secure protocols on page 61.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 AC-17 *Remote Access (Disable Unused Protocols)*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

## Set up users for two-step verification via email

Available functionality depends on the system you are using. See https://www.milestonesys.com/solutions/platform/product-index/ for more information.

To impose an additional login step on users of the XProtect Mobile client or XProtect Web Client, set up two-step verification on the XProtect Mobile server. In addition to the standard user name and password, the user must enter a verification code received by email.

Two-step verification increases the protection level of your surveillance system.

### Requirements

- You have installed an SMTP server.
- You have added users and groups to your XProtect system in the Management Client on the **Roles** node in the **Site Navigation** pane. On the relevant role, select the **Users and Groups** tab.
- If you upgraded your system from a previous version of XProtect, you must restart the mobile server to enable the two-step verification feature.

In Management Client or Management Application, perform these steps:

1. Enter information about your SMTP server.
2. Specify the settings for the verification code that will be sent to the client users.
3. Assign login method to users and domain groups.

This topic describes each of these steps.

#### Enter information about your SMTP server

The provider uses the information about the SMTP server:

1. In the navigation pane, select **Mobile Servers**, and select the relevant mobile server.
2. On the **Two-step verification** tab, select the **Enable two-step verification** check box.
3. Below **Provider settings**, on the **Email** tab, enter information about your SMTP server and specify the email that the system will send to client users when they log in and are set up for a secondary login. For details about each parameter, see Two-step verification tab on page 68.

#### Specify the verification code that will be sent to the users

To specify the complexity of the verification code:

1. On the **Two-step verification** tab, in the **Verification code settings** section, specify the period within which Milestone Mobile client or XProtect Web Client users, do not have to reverify its login in case of, for example, a disconnected network. Default period is 3 minutes.
2. Specify the period within which the user can use the received verification code. After this period, the code is invalid and the user has to request for a new code. Default period is 5 minutes.
3. Specify the maximum number of code entry attempts, before the user will be blocked. Default number is 3.
4. Specify the number of characters for the code. Default length is 6.
5. Specify the complexity of the code that you want the system to compose.

#### Assign login method to users and Active Directory groups

On the **Two-step verification** tab, in the **User settings** section, the list of users and groups added to your XProtect system appears.

1. In the **Login method** column, select between no login, no two-step verification, or delivery method of codes.
2. In the **Details** field, add the delivery details such as email addresses of individual users. Next time the user logs into XProtect Web Client or the XProtect Mobile client, he or she is asked for a secondary login.
3. If a group is configured in Active Directory, the Mobile server uses details, such as email addresses, from Active Directory.

   Windows groups do not support two-step verification.
4. Save your configuration.

You have completed the steps for setting up your users for two-step verification via email.

### Two-step verification tab

Available functionality depends on the system you are using. See https://www.milestonesys.com/solutions/platform/product-index/ for more information.

Use the **Two-step verification** tab to enable and specify an additional login step on users of:

- XProtect Mobile app on their iOS or Android mobile devices
- XProtect Web Client

The first type of verification is a password. The second type is a verification code, which you can configure to be sent to the user via email.

For more information, see Set up users for two-step verification via email on page 66.

The following tables describe the settings on this tab.

**Provider settings** > **Email**

| Name | Description |
|---|---|
| **SMTP server** | Enter the IP address or host name of the simple mail transfer protocol (SMTP) server for two-step verification emails. |
| **SMTP server port** | Specify the port of the SMTP server for sending emails.<br>Default port number is 25 without SSL and 465 with SSL. |
| **Use SSL** | Select this check box if your SMTP server supports SSL encryption. |
| **User name** | Specify the user name for logging in to the SMTP server. |
| **Password** | Specify the password for logging in to the SMTP server. |
| **Use Secure Password Authentication (SPA)** | Select this check box if your SMTP server supports SPA. |
| **Sender's email address** | Specify the email address for sending verification codes. |
| **Email subject** | Specify the subject title for the email. Example: Your two-step verification code. |

| Name | Description |
|---|---|
| Email text | Enter the message you want to send. Example: Your code is {0}.<br> If you forget to include the {0} variable, the code is added at the end of the text by default. |

Verification code settings

| Name | Description |
|---|---|
| Reconnection timeout (0-30 minutes) | Specify the period within which XProtect Mobile client users do not have to reverify their login in case of, for example, a disconnected network. The default period is three minutes.<br>This setting does not apply to XProtect Web Client. |
| Code expires after (1-10 minutes) | Specify the period within which the user can use the received verification code. After this period, the code is invalid and the user has to request for a new code. The default period is five minutes. |
| Code entry attempts (1-10 attempts) | Specify the maximum number of code entry attempts before the the provided code becomes invalid. The default number is three. |
| Code length (4-6 characters) | Specify the number of characters for the code. The default length is six. |
| Code composition | Specify the complexity of the code that you want the system to generate. You can select among:<br>• **Latin uppercase (A-Z)**<br>• **Latin lowercase(a-z)**<br>• **Digits (0-9)**<br>• **Special characters (!@#...)** |

User settings

| Name | Description |
|---|---|
| Users and groups | Lists the users and groups added to the XProtect system.<br>If a group is configured in Active Directory, the mobile server uses details, such as email addresses, from Active Directory.<br> Windows groups do not support two-step verification. |

| Name | Description |
|---|---|
| Verification method | Select a verification setting for each user or group. You can select among:<br>• **No login**: the user cannot log in<br>• **No two-step verification**: the user must enter user name and password<br>• **Email**: the user must enter a verification code in addition to user name and password |
| User details | Enter the email address to which each user will receive codes. |

# Log Server

Install Log Server on a separate server with SQL Server ..... 70

Limit the IP access to Log Server ..... 70

## Install Log Server on a separate server with SQL Server

For very large systems with many transactions to and from the log server's SQL database, Milestone recommends that you install the Log Server component on a separate server with its own SQL Server and store logs in an SQL database on that local SQL Server. If the Log Server is affected by performance issues, for example, due to flooding or other reasons, and uses the same SQL Server as the management server, both services can be affected.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*
- NIST SP 800-53 CM-9 *Configuration Management Plan*

## Limit the IP access to Log Server

Milestone recommends that only VMS components can contact the Log Server.Log Server uses port 22337.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

# Client programs

This section provides guidance about how to protect the Milestone client programs.

The client programs are:

- XProtect Smart Client
- XProtect Web Client
- XProtect Management Client
- Milestone Mobile client

## Basic steps (all client programs)

Use Windows users with AD ..... 71

Restrict permissions for client users ..... 71

Always run clients on trusted hardware on trusted networks ..... 73

### Use Windows users with AD

Milestone recommends that, whenever possible, you use Windows users in combination with Active Directory (AD) to log in to the VMS with the client programs. This enables you to enforce a password policy, and apply user settings consistently across the domain and network. It also provides protection against brute force attacks. For more information, see Use Windows users with Active Directory on page 23.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 SA-5 *Information System Documentation*
- NIST 800-53 SA-13 *Trustworthiness*

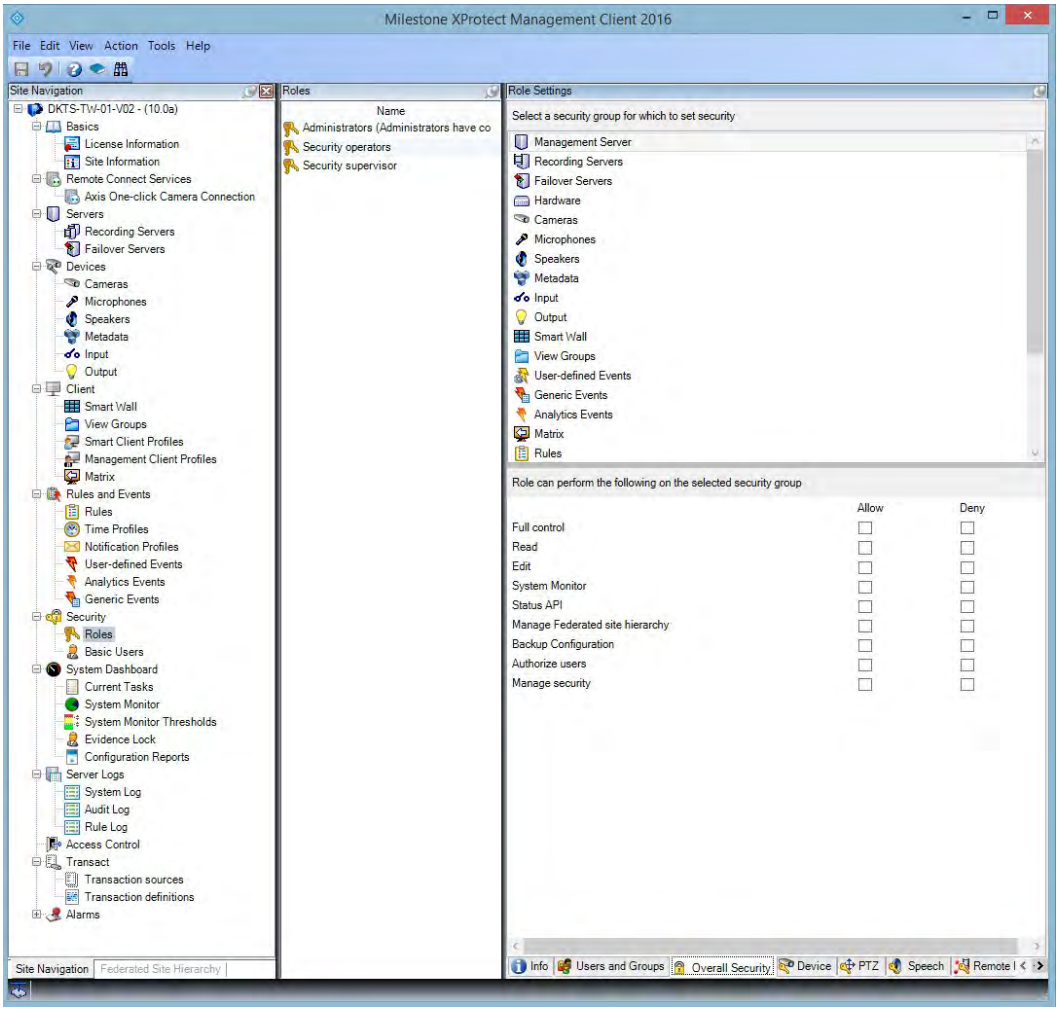
### Restrict permissions for client users

Milestone recommends that administrators specify what users can do in Management Client or XProtect Smart Client.

The following instructions describe how to do this. Additional information is available in the Advanced Security Management white paper (https://www.milestonesys.com/files/White%20papers/XProtect_Corporate_Advanced_Security_Management.pdf).

To restrict client user permissions, follow these steps:

1. Open Management Client.
2. Expand the **Security** node, select **Roles**, and then select the role that the user is associated with.
3. On the tabs at the bottom, you can set permissions and restrictions for the role.




By default, all users associated with the Administrator role have unrestricted access to the system. This includes users who are associated with the Administrator role in AD as well as those with the role of administrator on the management server.

### Learn more

The following documents provide additional information:

- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

## Always run clients on trusted hardware on trusted networks

Milestone recommends that you always run XProtect clients on hardware devices with the proper security settings. Specific guidance for mobile devices is available in SP 800-124 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf). These settings are specific to the device.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*
- NIST SP800-53 CM-6 *Configuration Settings*

# Advanced steps – XProtect Smart Client

Restrict physical access to any computer running XProtect Smart Client ..... 73
Always use a secure connection by default, particularly over public networks ..... 74
Activate login authorization ..... 74
Do not store passwords ..... 77
Turn on only required client features ..... 78
Use separate names for user accounts ..... 78
Prohibit the use of removable media ..... 79

## Restrict physical access to any computer running XProtect Smart Client

Milestone recommends that you restrict physical access to computers running XProtect Smart Client. Allow only authorized personnel to access the computers. For example, keep the door locked, and use access controls and surveillance.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 PE-1 *Physical and Environmental Protection Policy and Procedures*
- NIST SP 800-53 PE-2 *Physical Access Authorizations*
- NIST SP 800-53 PE-3 *Physical Access Control*
- NIST SP 800-53 PE-6 *Monitoring Physical Access*

## Always use a secure connection by default, particularly over public networks

If you need to access the VMS with XProtect Smart Client over a public or untrusted network, Milestone recommends that you use a secure connection through VPN. This helps ensure that communication between XProtect Smart Client and the VMS server is protected.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-17 *Remote Access*
- NIST SP 800-53 CM-6 *Configuration Settings*

## Activate login authorization

Login authorization requires a user to log in on XProtect Smart Client or Management Client, and another user who has an elevated status, such as a supervisor, to provide approval.

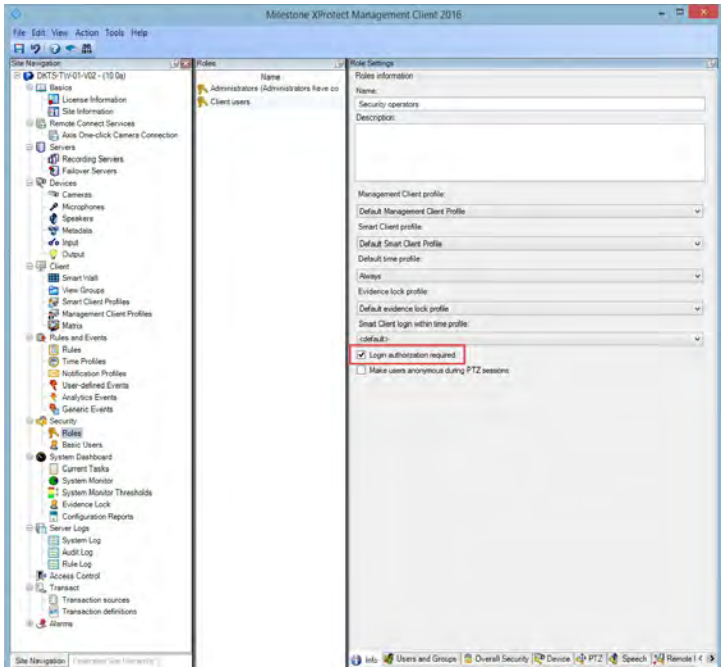
You set up login authorization on the roles. Users associated with the role are prompted for a second user (a supervisor) to authorize their access to the system.

Login authorization is currently not supported by mobile client, XProtect Web Client, and any Milestone Integration Platform (MIP) SDK integrations.

To turn on login authorization for a role, follow these steps:

1. Open Management Client.
2. Expand the **Security** node, select **Roles**, and then select the relevant role.

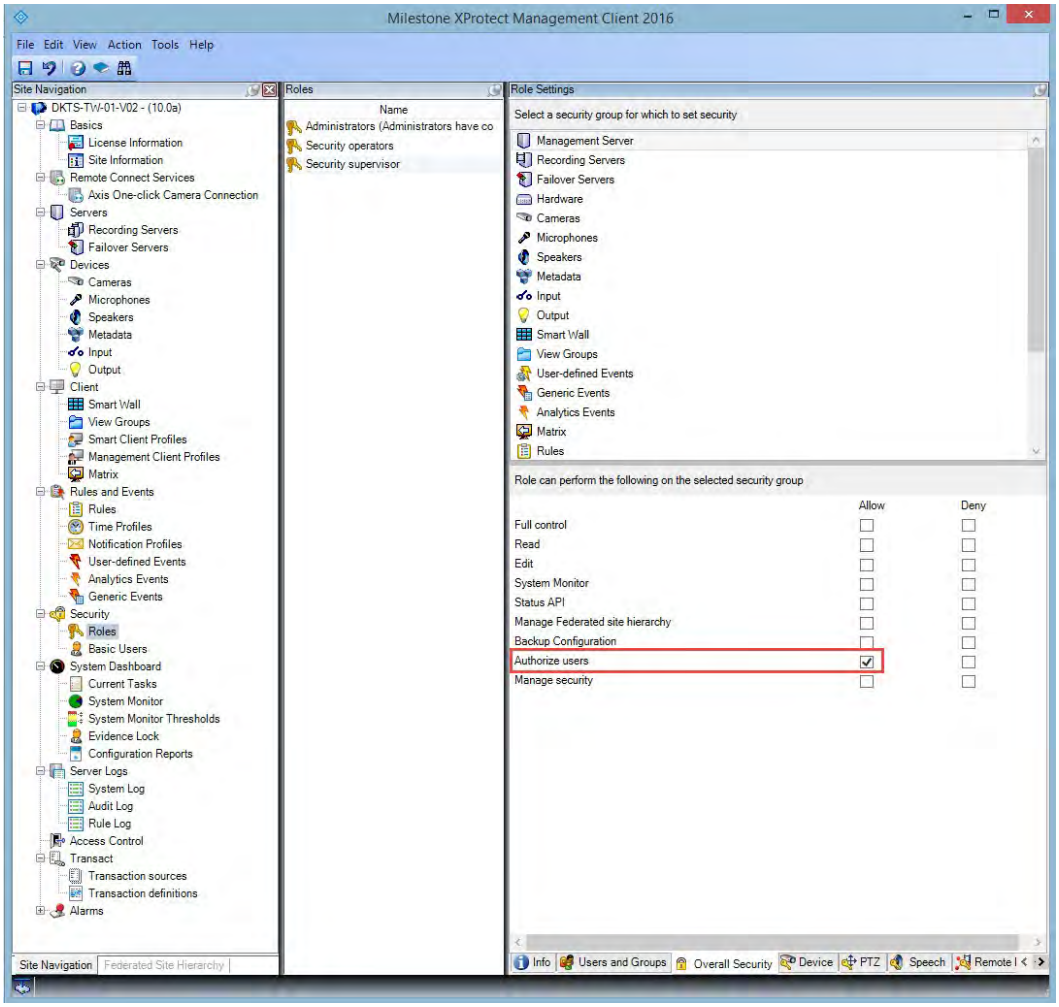
   Select the **Login authorization required** check box.




To configure the roles that authorize and grant access, follow these steps:

1. To create a new role, for example "Security supervisor", expand the **Security** node, right-click **Roles** and create a new role.
2. Click the **Overall Security** tab, and select the **Management Server** node.

   Select the **Allow** check box next to the **Authorize users** check box.




### Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-6 *Least Privilege*
- NIST SP 800-53 AC-17 *Remote Access*
- NIST SP 800-53 CM-6 *Configuration Settings*

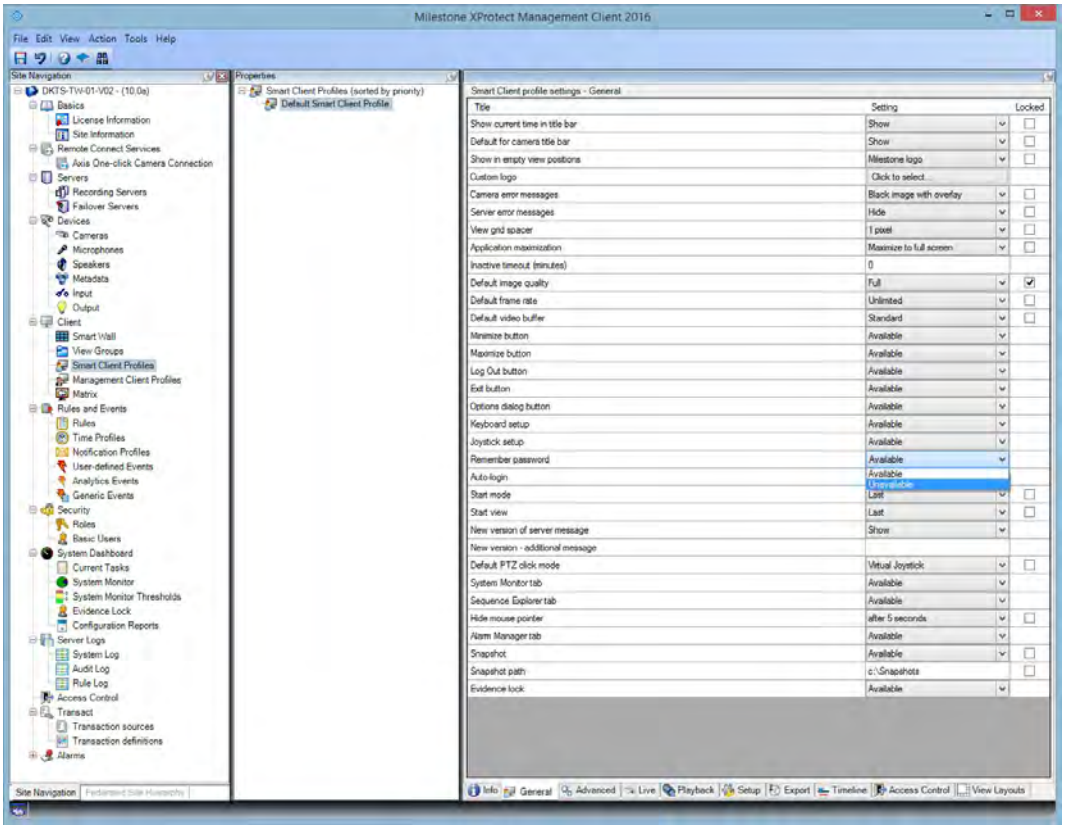
## Do not store passwords

XProtect Smart Client provides the option to remember passwords for users. To reduce the risk of unauthorized access, Milestone recommends that you do not use this feature.

To turn off the remember password feature, follow these steps:

1. Open Management Client.
2. Expand the **Client** node, select **Smart Client Profiles**, and then select the relevant Smart Client profile.
3. In the **Remember password** list, select **Unavailable**.

> The **Remember password** option is not available the next time a user with this profile logs into XProtect Smart Client.




### Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 IA-1 *Identification and Authentication Policy and Procedures*

## Turn on only required client features

Turn on only required features, and turn off features that a surveillance operator does not need. The point is to limit opportunities for misuse or mistakes.

You can turn on and turn off features in XProtect Smart Client and in XProtect Management Client.

In Management Client, configure Smart Client profiles to specify sets of permissions for users who are assigned to the profile.Smart Client profiles are similar to Management Client profiles, and the same user can be assigned to each type of profile.

To configure a Smart Client profile, follow these steps:

1. Open Management Client.
2. Expand the **Client** node, select **Smart Client Profiles**, and then select the relevant Smart Client profile.
3. Use the tabs to specify settings for features in Smart Client. For example, use the settings on the Playback tab to control features used to investigate recorded video.

Before you assign a user to a Smart Client profile, ensure that the permissions for the user's role are appropriate for the profile. For example, if you want a user to be able to investigate video, make sure that the role allows the user to play back video from cameras, and that Sequence Explorer tab is available on the Smart Client profile.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-6 *Least Privilege*
- NIST SP 800-53 CM-6 *Configuration Settings*

## Use separate names for user accounts

Milestone recommends that you create a user account for each user, and use a naming convention that makes it easy to identify the user personally, such as their name or initials. This is a best practice for limiting access to only what is necessary, and it also reduces confusion when auditing.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-1 *Configuration Management Policy and Procedures*

- NIST 800-53 CM-2 *Baseline Configuration*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

## Prohibit the use of removable media

For video exports, establish a chain of procedures that are specific to evidence.Milestone recommends that the security policy allows only authorized XProtect Smart Client operators to connect removable storage devices such as USB flash drives, SD cards, and smartphones to the computer where XProtect Smart Client is installed.

Removable media can transfer malware to the network, and subject video to unauthorized distribution.

Alternatively, the security policy can specify that users can export evidence only to a specific location on the network, or to a media burner only. You can control this through the Smart Client profile.

**Learn more**

The following control(s) provide additional guidance:

- NIST SO 800-53 MP-7 *Media Use*
- NIST SP 800-53 SI-3 *Malicious Code Protection*

# Advanced steps – Milestone Mobile client

SP 800-124 revision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf) provides guidance that is specifically for mobile devices. The information it contains applies to all topics in this section.

Always use the Milestone Mobile client on secure devices ..... 79

Download the Milestone Mobile client from authorized sources ..... 80

Mobile devices should be secured ..... 80

## Always use the Milestone Mobile client on secure devices

Milestone recommends that you always use the XProtect Mobile client on secure devices that are configured and maintained according to a security policy. For example, ensure that mobile devices do not allow users to install software from unauthorized sources. An enterprise app store is one example of a way to constrain device applications as part of overall mobile device management.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*
- NIST SP800-53 CM-6 *Configuration Settings*

## Download the Milestone Mobile client from authorized sources

Milestone recommends that you download the XProtect Mobile client from one of these sources:

- Google Play Store
- Apple App Store
- Microsoft Windows Store.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 *Boundary Protection*
- NIST SP 800-53 CM-6 *Configuration Settings*

## Mobile devices should be secured

If you want to access the VMS with a mobile device over a public or untrusted network, Milestone recommends that you do so with a secure connection, use proper authentication and Transport Layer Security (TLS) (https://datatracker.ietf.org/wg/tls/charter/) (or connect through VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) and HTTPS. This helps protect communications between the mobile device and the VMS.

Milestone recommends that mobile devices use screen-lock. This helps prevent unauthorized access to the VMS, for example, if the smart phone is lost. For maximum security, implement a security policy to prohibit the XProtect Mobile client from remembering the user name and password.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 AC-17 *Remote Access*
- NIST SP 800-53 CM-6 *Configuration Settings*

# Advanced steps – XProtect Web Client

Always run XProtect Web Client on trusted client computers ..... 80

Use certificates to confirm the identity of a Milestone Mobile server ..... 81

Use only supported browsers with the latest security updates ..... 81

## Always run XProtect Web Client on trusted client computers

Always securely connect all components of the VMS. Server-to-server and client-to-server connections should use proper authentication and Transport Layer Security (TLS) (https://datatracker.ietf.org/wg/tls/charter/) (or connect through VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) and HTTPS. Always run XProtect Web Client on

trusted computers, for example, do not use a client computer in a public space.Milestone recommends that you educate users about the security measures to remember when using browser-based applications, such as XProtect Web Client. For example, make sure they know to disallow the browser from remembering their password.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 IA-2 *Identification and Authentication*

## Use certificates to confirm the identity of a Milestone Mobile server

This document emphasizes the use of the latest TLS. With that comes the need for the proper use of certificates and the implementation of the TLS cipher suite.Milestone recommends that you install a certificate on the XProtect Mobile server to confirm the identity of the server when a user tries to connect through XProtect Web Client.

For more information, see the *Edit certificate* section in the *XProtect VMS - Administrator manual*.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 IA-2 *Identification and Authentication*

## Use only supported browsers with the latest security updates

Milestone recommends that you install only one of the following browsers on client computers. Make sure to include the latest security updates.

- Apple Safari
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST SP 800-53 CM-2 *Baseline Configuration*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 PL-8 *Information Security Architecture*
- NIST SP 800-53 SI-3 *Malicious Code Protection*

# Advanced steps – Management Client

Use Management Client profiles to limit what administrators can view ..... 82

Allow administrators to access relevant parts of the VMS ..... 82

Run the Management Client on trusted and secure networks ..... 83

## Use Management Client profiles to limit what administrators can view

Milestone recommends that you use Management Client profiles to limit what administrators can view in the Management Client.

Management Client profiles allow system administrators to modify the Management Client user interface. Associate Management Client profiles with roles to limit the user interface to represent the functionality available for each administrator role.

Display only the parts of the VMS that administrators need to perform their duties.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST 800-53 CM-2 *Baseline Configuration*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

## Allow administrators to access relevant parts of the VMS

If you have a setup that requires multiple administrators, Milestone recommends that you configure different administrator rights for administrators who use the Management Client.

To define administrator permissions, follow these steps:

1. In Management Client, expand the **Security** node, select **Roles**, and then select the relevant administrator role.

   You cannot modify the built-in administrator role, so you must create additional administrator roles.

2. On the **Overall Security** tab, specify the actions that the administrator can take for each security group.
3. On the other tabs, specify the security settings for the role in the VMS.

   For more information about security settings for roles, see the *XProtect VMS - Administrator manual*.

4. On the **Info** tab, associate the role with a Management Client profile.

You can turn on or turn off features by using the Management Client profile. Before you assign a user to a Management Client profile, ensure that the permissions for the user's role are appropriate for the profile. For example, if you want a user to be able to manage cameras, make sure that the role allows the user to do this, and that cameras are enabled on the Management Client profile.

**Learn more**

The following control(s) provide additional guidance:

- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-1 *Configuration Management Policy and Procedures*
- NIST 800-53 CM-2 *Baseline Configuration*
- NIST 800-53 CM-6 *Configuration Settings*
- NIST 800-53 CM-7 *Least Functionality*

## Run the Management Client on trusted and secure networks

If you access the Management Server with Management Client over HTTP, the plain text communication can contain unencrypted system details.Milestone recommends that you run the Management Client only on trusted and known networks. Use a VPN to provide remote access.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 *Account Management*
- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 IA-2 *Identification and Authentication*

# Product comparison chart

XProtect VMS includes the following products:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

The complete feature list is available on the product overview page on the Milestone website (https://www.milestonesys.com/solutions/platform/product-index/).

Below is a list of the main differences between the products:

| Name | XProtect Essential+ | XProtect Express+ | XProtect Professional+ | XProtect Expert | XProtect Corporate |
|---|---|---|---|---|---|
| Sites per SLC | 1 | 1 | Multi-site | Multi-site | Multi-site |
| Recording servers per SLC | 1 | 1 | Unrestricted | Unrestricted | Unrestricted |
| Hardware devices per recording server | 8 | 48 | Unrestricted | Unrestricted | Unrestricted |
| Milestone Interconnect™ | - | Remote site | Remote site | Remote site | Central/remote site |
| Milestone Federated Architecture™ | - | - | - | Remote site | Central/remote site |
| Recording server failover | - | - | - | Cold and hot standby | Cold and hot standby |
| Remote connect services | - | - | - | - | ✓ |
| Edge storage support | - | - | ✓ | ✓ | ✓ |
| Multi-stage video storage | Live databases + 1 archive | Live databases + 1 archive | Live databases + 1 archive | Live databases + unrestricted archives | Live databases + unrestricted archives |
| SNMP notification | - | - | - | ✓ | ✓ |

| Name | XProtect Essential+ | XProtect Express+ | XProtect Professional+ | XProtect Expert | XProtect Corporate |
|---|---|---|---|---|---|
| Time controlled user access rights | - | - | - | - | ✓ |
| Reduce frame rate (grooming) | - | - | - | ✓ | ✓ |
| Video data encryption (recording server) | - | - | - | ✓ | ✓ |
| Database signing (recording server) | - | - | - | ✓ | ✓ |
| PTZ priority levels | 1 | 1 | 3 | 32000 | 32000 |
| Extended PTZ (Reserve PTZ session and patrolling from XProtect Smart Client) | - | - | - | ✓ | ✓ |
| Evidence lock | - | - | - | - | ✓ |
| Bookmark function | - | - | Manual only | Manual and rule-based | Manual and rule-based |
| Live multi-streaming or multicasting | - | - | - | ✓ | ✓ |
| Overall security | Client user rights | Client user rights | Client user rights | Client user rights | Client user rights/ administrator user rights |
| XProtect Management Client profiles | - | - | - | - | ✓ |
| XProtect Smart Client profiles | - | - | 3 | 3 | Unrestricted |
| XProtect Smart Wall | - | - | - | optional | ✓ |
| System Monitor | - | - | - | ✓ | ✓ |
| Smart map | - | - | - | ✓ | ✓ |
| Two-step verification | - | - | - | - | ✓ |

| Name | XProtect Essential+ | XProtect Express+ | XProtect Professional+ | XProtect Expert | XProtect Corporate |
|---|---|---|---|---|---|
| DLNA support | - | ✓ | ✓ | ✓ | ✓ |
| Privacy masking | - | ✓ | ✓ | ✓ | ✓ |
| Device password management | | | ✓ | ✓ | ✓ |

# Appendix 1 - Resources

1. *Axis Communications: Hardening Guide* (http://www.axis.com/files/sales/axis_hardening_guide_1488265_en_1510.pdf)
2. *Bosch Security Systems: Bosch IP Video and Data Security Guidebook* (http://resource.boschsecurity.com/documents/data_security_guideb_special_enus_22335871499.pdf)
3. *British Standard BS EN 62676-1-1: Video surveillance systems for use in security applications, Part 1-1: System requirements – General* (http://shop.bsigroup.com/browse-by-subject/security/electronic-security-systems/cctvstandards/)

   Describes the minimum requirements for a video surveillance system. See also related standards.
4. *Center for Internet Security: The CIS Critical Security Controls for Effective Cyber Defense* (https://www.cisecurity.org/critical-controls.cfm)
5. *Cloud Security Alliance (CSA)* (https://cloudsecurityalliance.org/) and the *Cloud Controls Matrix* (https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/)
6. *Defense Information Systems Agency (DISA): Security Technical Implementation Guides (STIGs)* (http://iase.disa.mil/stigs/pages/index.aspx)
7. *Internet Engineering Task Force (IETF)* (https://www.ietf.org/), multiple references
8. *ISO/IEC 15048 Information technology - Security techniques - Evaluation criteria for IT security* (http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341)
9. *ISO/IEC 31000, Risk management – Principles and guidelines* (http://www.iso.org/iso/home/standards/iso31000.htm)
10. *ISO/IEC 31010, Risk management – Risk assessment techniques* (http://www.iso.org/iso/catalogue_detail?csnumber=51073)
11. *ISO 27001: A standard and framework for managing threats in an information security management system (ISMS)* (http://www.iso.org/iso/iso27001)
12. *ISO 27002: Information technology — Security techniques — Code of practice for information security controls* (https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en)
13. *Microsoft Security Update Guide* (https://technet.microsoft.com/en-us/security/dn550891.aspx)

    See also *Why We're Not Recommending "FIPS Mode" Anymore* (http://blogs.technet.com/b/secguide/archive/2014/04/07/why-we-re-not-recommending-fips-mode-anymore.aspx) and *Automating security configuration tasks* (https://technet.microsoft.com/en-us/library/bb490776.aspx), among others
14. *National Institute of Standards and Technology: Computer Security Division Computer Security Resource Center* (http://csrc.nist.gov/)
15. *National Institute of Standards and Technology: Cybersecurity Framework* (http://www.nist.gov/cyberframework/)

16. *National Institute of Standards and Technology: Guide for Applying the Risk Management Framework to Federal Information Systems* (http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)

17. *National Institute of Standards and Technology: Managing Information Security Risk* (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf)

18. *National Institute of Standards and Technology: Security and Privacy Controls for Federal Information Systems and Organizations SP 800-53- Revision 4* (http://dx.doi.org/10.6028/nist.sp.800-53r4) and *Pre-Draft Revision 5* (http://csrc.nist.gov/groups/sma/fisma/sp800-53r5_pre-draft.html)

19. *NIST SP 800-100 Information Security Handbook: A Guide for Managers* (http://csrc.nist.gov/publications/nistpubs/800-100/sp800-100-mar07-2007.pdf)

20. *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf)

21. *SANS Institute* website (https://sans.org) and the *SANS Critical Security Controls* (https://www.sans.org/critical-security-controls/)

22. *XProtect® Corporate – Advanced Security Management* (https://www.milestonesys.com/files/White%20papers/XProtect_Corporate_Advanced_Security_Management.pdf)

# Appendix 2 - Acronyms

AD – Active Directory

CSA – Cloud Security Alliance

CVE – Common Vulnerabilities and Exposures

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

IEC – International Electrotechnical Commission

IETF – Internet Engineering Task Force

IP – Internet Protocol

ISO – International Standards Organization

IT – Information Technology

KB – Knowledge Base

NIST – National Institute of Standards and Technology

RSTP – Rapid Spanning Tree Protocol

SMTP – Simple Mail Transfer Protocol

SSL – Secure Socket Layer

STIG – Security Technical Information Guide

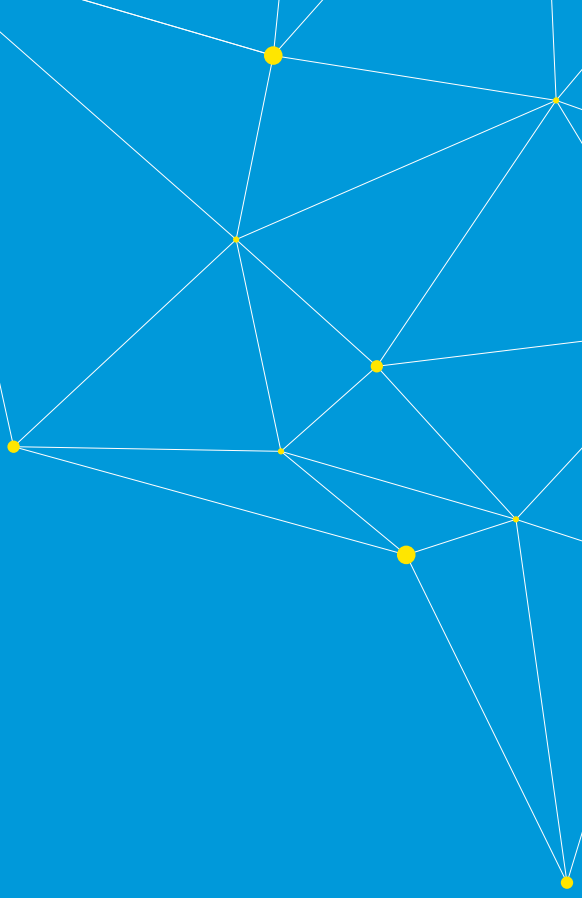
TCP – Transmission Control Protocol

TLS- Transport Layer Security

UDP – User Datagram Protocol

VMS – Video Management Software

VPN – Virtual Private Network



helpfeedback@milestone.dk

**About Milestone**

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.