



The open platform company

Milestone Systems

XProtect[®] Advanced VMS

Hardening Guide

Copyright, trademarks and disclaimer

Copyright © 2017 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 reserve 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.

Changes to this document

Document version	Release	Comments
Version 1	2016 R2	This document applies to XProtect Advanced VMS versions 2016 R3 and before.
Version 2	2016 R3	<p>This document applies to XProtect Advanced VMS versions 2016 R3 and before.</p> <p>These are the changes to the document:</p> <ul style="list-style-type: none">• Added Changes to this document topic• Added Kerberos support (see "About Kerberos authentication" on page 20)• Updated port numbers in Use firewalls to limit IP access to servers and computers (on page 22)

Contents

Introduction.....	8
What is "hardening?"	8
Target audience.....	8
Resources and references.....	9
Hardware and device components.....	9
Cyber threats and cyber risks	10
Cyber Risk Management Framework.....	11
Hardening system components.....	14
General setup.....	15
Servers, Workstations, Clients and Applications	17
Basic steps	17
Establish surveillance and security objectives	17
Establish a formal security policy and response plan.....	17
Use Windows users with Active Directory.....	18
About Kerberos authentication	20
Use Windows update	21
Keep software and device firmware updated.....	21
Use secure and trusted networks connection	22
Use firewalls to limit IP access to servers and computers	22
Use antivirus on all servers and computers	30
Monitor logs in the VMS for signs of suspicious activity.....	30
Advanced steps	32
Adopt standards for secure network and VMS implementations	32
Establish an incident response plan.....	32
Protect sensitive VMS components	33

- Follow Microsoft OS Security best practices 33
- Use tools to automate or implement the security policy 33
- Follow established network security best practices..... 34
- Devices and network..... 35**
 - Devices - basic steps 35**
 - Use strong passwords instead of default passwords 35
 - Stop unused services and protocols..... 35
 - Create dedicated user accounts on each device..... 36
 - Network - basic steps 37**
 - Use a firewall between the VMS and the Internet 37
 - Connect the camera subnet to the recording server subnet only 37
 - Devices - advanced steps 38**
 - Use Simple Network Management Protocol to monitor events..... 38
 - Network - advanced steps 38**
 - Use secure wireless protocols..... 38
 - Use port-based access control 38
 - Run the VMS on a dedicated network 39
- Milestone Servers..... 40**
 - Basic steps 40**
 - Use physical access controls and monitor the server room..... 40
 - Use encrypted communication channels..... 40
 - Advanced steps 40**
 - Run services with service accounts 40
 - Run components on dedicated virtual or physical servers 41
 - Restrict the use of removable media on computers and servers..... 41
 - Use individual administrator accounts for better auditing 41
 - Use subnets or VLANs to limit server access..... 41
 - Enable only the ports used by Event Server..... 42

- SQL Server..... 42**
 - Run the SQL Server database on a separate server 42
- Management Server..... 42**
 - Adjust the token time-out..... 42
 - Enable only the ports used by the management server 43
 - Disable non-secure protocols 43
- Recording Server 44**
 - Use separate network interface cards 44
- Milestone Mobile server component 44**
 - Only enable ports that Milestone Mobile server uses 44
 - Use a "demilitarized zone" (DMZ) to provide external access..... 44
 - Disable non-secure protocols 45
- Log Server 45**
 - Install Log Server on a separate SQL Server..... 45
 - Limit the IP access to Log Server 45
- Client programs..... 46**
 - Basic steps (all client programs) 46**
 - Use Windows users with AD 46
 - Restrict permissions for client users..... 46
 - Always run clients on trusted hardware on trusted networks..... 48
 - XProtect Smart Client - advanced steps 48**
 - Restrict physical access to any computer running XProtect Smart Client48
 - Always use a secure connection by default, particularly over public networks 48
 - Activate login authorization..... 49
 - Do not store passwords 50
 - Turn on only required client features..... 51
 - Use separate names for user accounts 52

- Prohibit the use of removable media 52
- Milestone Mobile client - advanced steps..... 53**
 - Always use the Milestone Mobile client on secure devices 53
 - Download the Milestone Mobile client from authorized sources..... 53
 - Mobile devices should be secured 53
- XProtect Web Client - advanced steps 54**
 - Always run XProtect Web Client on trusted client computers 54
 - Use certificates to confirm the identity of a Milestone Mobile server .. 54
 - Use only supported browsers with the latest security updates..... 55
- Management Client - advanced steps 55**
 - Use Management Client profiles to limit what administrators can view55
 - Allow administrators to access relevant parts of the VMS 56
 - Run the Management Client on trusted and secure networks 56
- Appendix 1 - Resources..... 57**
- Appendix 2 - Acronyms 59**
- Index 60**

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:
 - a Harden the servers (physical and virtual) and client computers and devices
 - b Harden the network
 - c 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 Advanced 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 57) for a list of references and Appendix 2 - Acronyms (on page 59) 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 Advanced 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 Advanced VMS installation. For example, cameras often have default passwords. Some manufacturers publish

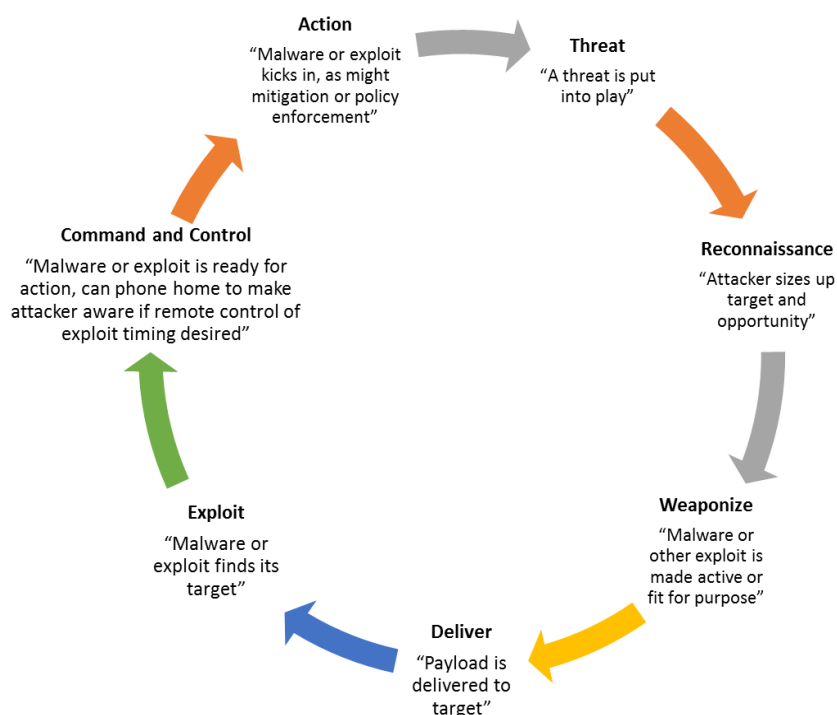
these passwords online so that they're easy for customers to find. Unfortunately, that means the passwords are also available to attackers.

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 Advanced VMS and Windows configurations.

The risk and threat assessment process includes the following steps:

- Identify information and security risks
- Assess and prioritize risks

XProtect Advanced VMS - Hardening Guide

- 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.

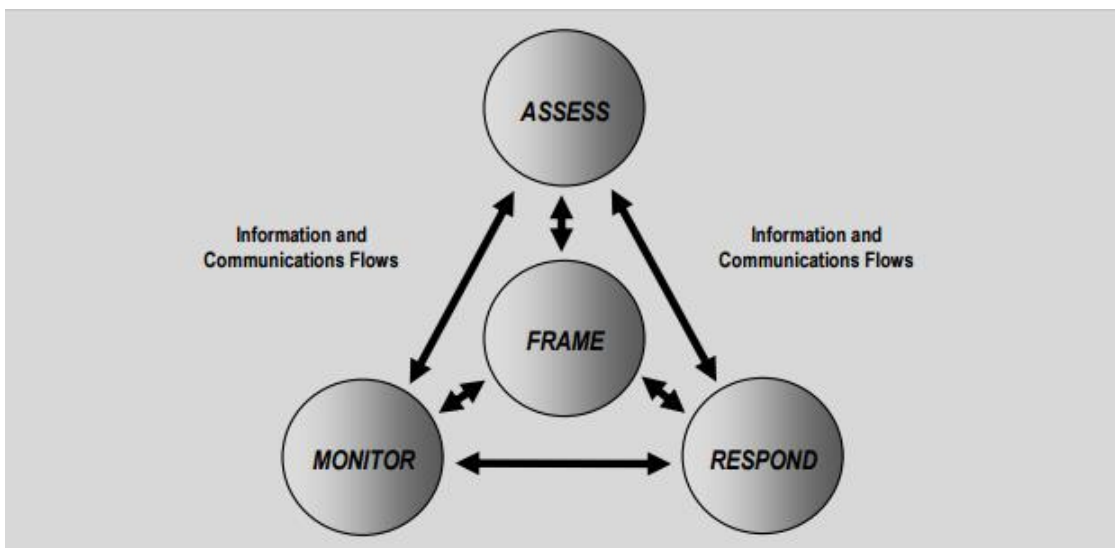
Cyber Risk Management Framework

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 provides references for detailed security plans.

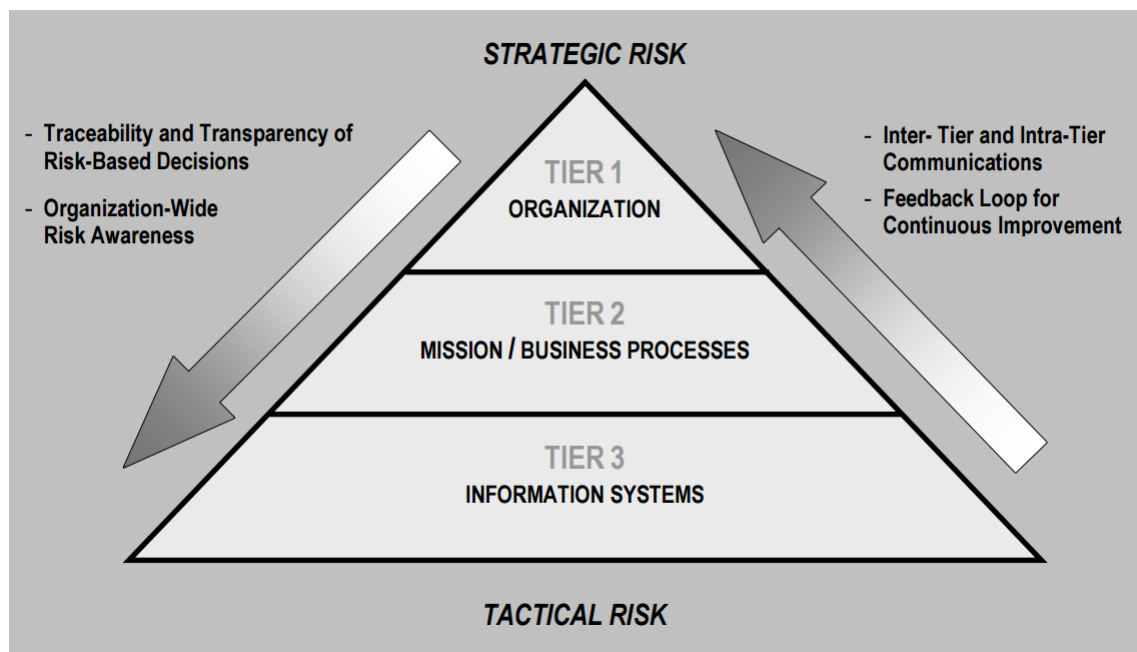


High-level view of risk management (SP 800-39, page 8 <http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf>)

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.

XProtect Advanced VMS - Hardening Guide

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.

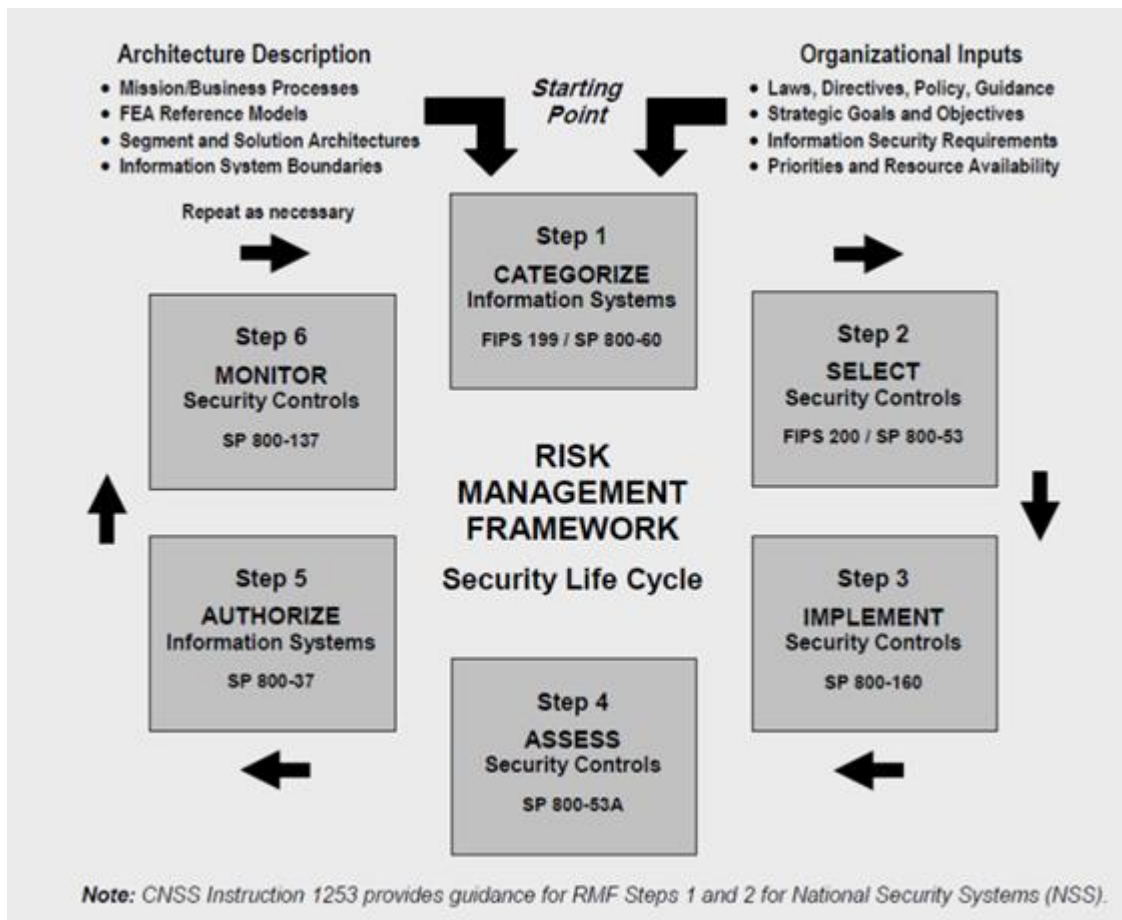


Balancing security and business goals (SP 800-39, page 9 <http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf>)

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.

XProtect Advanced VMS - Hardening Guide

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 Advanced 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) 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.

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 57) 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.

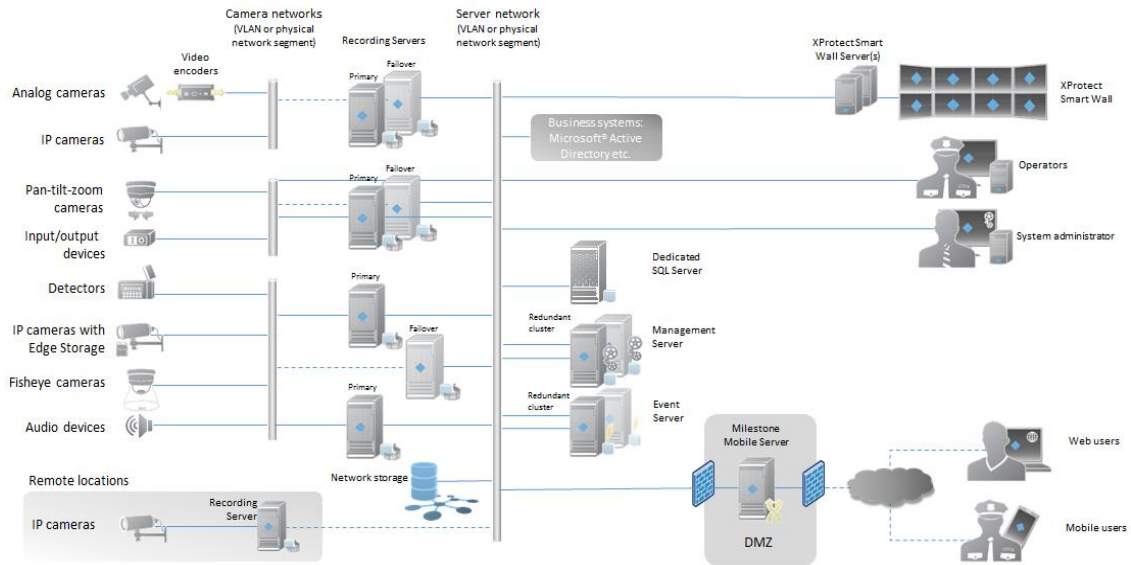
(AC3, AC4, AC6, CA3, CM3, CM6, CM7, IR4, SA9, SC7, SC28, SI3, SI 8 in Appendices D and F in NIST SP 800-53 Rev4
<http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf> (AC Access Controls), (CM Configuration Management) (IR Incident Response) (SA System and Service Acquisition) (SI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

XProtect Advanced VMS - Hardening Guide

The figure shows an example of a general setup.



Servers, Workstations, Clients and Applications

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

- The XProtect Advanced 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

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

XProtect Advanced VMS - Hardening Guide

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 Advanced 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 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 (NTLM) for login, Kerberos (see "About Kerberos authentication" on page 20), or other SSP options from Microsoft.

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.

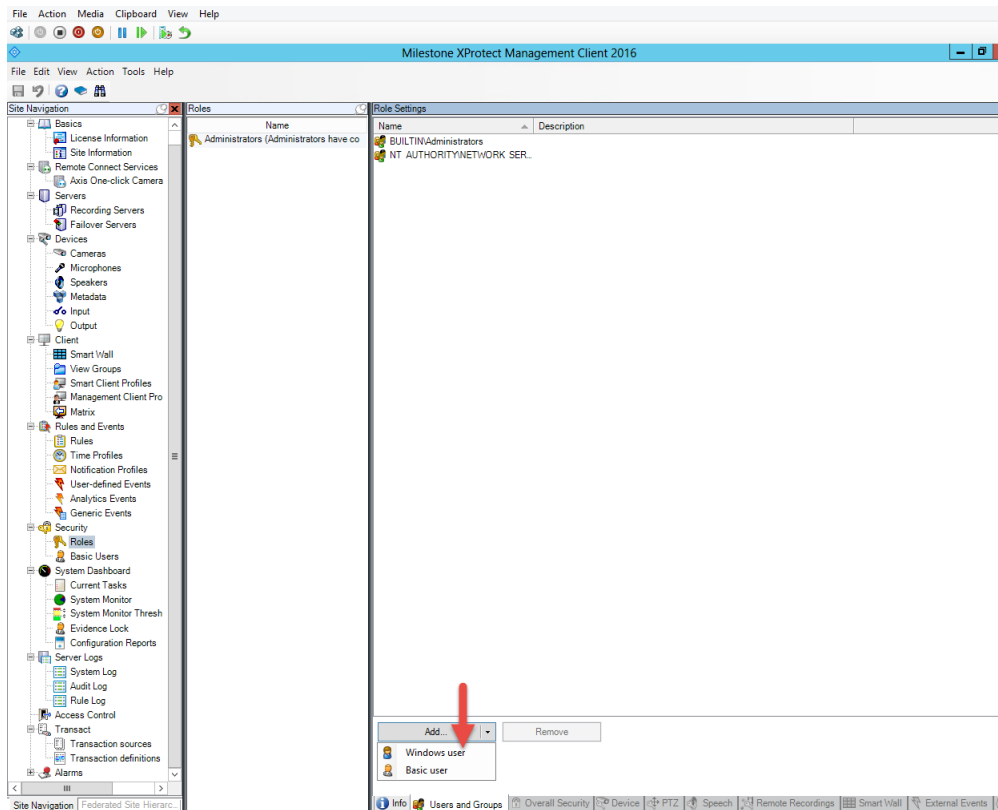
Windows users have the advantage of being authenticated via the directory as a single authoritative source and enterprise service for the network and not ad hoc for their local machine. This lets you use role based access controls to assign permissions to users and groups consistently across the domain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

XProtect Advanced VMS - Hardening Guide

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**

About Kerberos authentication

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 video management software 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 hostname 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 Advanced 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 Advanced 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 Advanced 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 Advanced VMS product.
3. In the **Device pack** column, select the version of the current device pack.

XProtect Advanced VMS - Hardening Guide

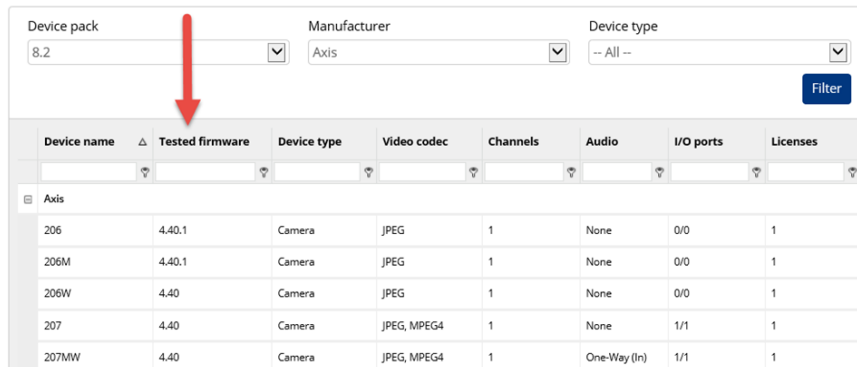
4. Select the manufacturer of your device, and then click **Filter**. The version of the firmware that the device pack supports is listed in the **Tested Firmware** column.

Below is an extensive list of supported devices and firmware versions.

Please remember that throughout the year there will be new releases of device packs that will allow for integration with new cameras models and devices.

Number of supported manufacturers: 129

Number of supported devices: 254 (plus various devices in series and non-listed OEM devices)



The screenshot shows a web interface with three dropdown menus: 'Device pack' (set to 8.2), 'Manufacturer' (set to Axis), and 'Device type' (set to -- All --). A blue 'Filter' button is to the right. Below is a table with columns: Device name, Tested firmware, Device type, Video codec, Channels, Audio, I/O ports, and Licenses. The table lists several Axis camera models.

Device name	Tested firmware	Device type	Video codec	Channels	Audio	I/O ports	Licenses
Axis							
206	4.40.1	Camera	JPEG	1	None	0/0	1
206M	4.40.1	Camera	JPEG	1	None	0/0	1
206W	4.40	Camera	JPEG	1	None	0/0	1
207	4.40	Camera	JPEG, MPEG4	1	None	1/1	1
207MW	4.40	Camera	JPEG, MPEG4	1	One-Way (In)	1/1	1

Learn more

The following control(s) provide additional guidance:

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

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 (TLS, currently 1.2) with valid certificates that meet industry best practices, such as from Public-Key Infrastructure (X.509) and CA/Browser Forum.

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

XProtect Advanced VMS - Hardening Guide

- 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 Advanced 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.

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.
443	HTTPS	IIS	XProtect Smart Client and the Management Client	Authentication of basic users.
6473	TCP	Management Server service	Management Server tray controller, local connection only.	Showing status and managing the service.

XProtect Advanced VMS - Hardening Guide

Port number	Protocol	Process	Connections from...	Purpose
7475	TCP	Management Server service	Windows SNMP Service	<p>Communication with the SNMP extension agent.</p> <p>Do not use the port for other purposes even if your system does not apply SNMP.</p> <p>In XProtect Advanced VMS 2014 systems or older, the port number was 6475.</p>
8080	TCP	Management server	Local connection only.	Communication between internal processes on the server.
9993	TCP	Management Server service	Recording Server services	Authentication, configuration, token exchange.
12345	TCP	Management Server service	XProtect Smart Client	<p>Communication between the system and Matrix recipients.</p> <p>You can change the port number in the Management Client.</p>

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.

XProtect Advanced VMS - Hardening Guide

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. 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. 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. 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. 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. The port is disabled per default.

XProtect Advanced VMS - Hardening Guide

Port number	Protocol	Process	Connections from...	Purpose
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.
7474	TCP	Recording Server Service	Windows SNMP service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. In XProtect Advanced VMS 2014 systems or older, the port number was 6474.
7563	TCP	Recording Server Service	XProtect Smart Client, Management Client	Retrieving video and audio streams, PTZ commands.
8966	TCP	Recording Server Service	Recording Server tray controller, local connection only.	Showing status and managing the service.
11000	TCP	Recording Server Service	Failover recording servers	Polling the state of recording servers.
65101	UDP	Recording Server service	Local connection only	Listening for event notifications from the drivers.

Note that 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. The port is disabled per 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.

XProtect Advanced VMS - Hardening Guide

Port number	Protocol	Process	Connections from...	Purpose
7474	TCP	Recording Server Service	Windows SNMP service	Communication with the SNMP extension agent. 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 tray controller, local connection only.	Showing status and managing the service.
8967	TCP	Failover Server Service	Failover Server tray controller, 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.

Note that 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	Mobil Server management (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.

XProtect Advanced VMS - Hardening Guide

LPR Server service

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

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. You can change the port number in the Management Client.

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.

XProtect Advanced VMS - Hardening Guide

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.

Note that only a few camera models are able to establish outbound connections.

Client components (outbound connections)

XProtect Smart Client, XProtect Management Client, Milestone Mobile server

Port number	Protocol	Connections to...	Purpose
80	HTTP	Management server service	Authentication
443	HTTPS	Management server service	Authentication of basic users.
7563	TCP	Recording server service	Retrieving video and audio streams, PTZ commands.
22331	TCP	Event Server service	Alarms.

Web Client, Milestone Mobile client

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

XProtect Advanced VMS - Hardening Guide

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

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 Advanced VMS Administrator Guide.

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 Advanced 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 Advanced VMS does not support syslog.

Milestone recommends that you use the Audit Log in XProtect Advanced 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 Advanced VMS products. This includes the times of the activities and the source IP addresses.

The client components are XProtect Smart Client, Web Client, the Milestone 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.

XProtect Advanced VMS - Hardening Guide

- 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 Advanced VMS, follow these steps:

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

Level	UTC Time	Local Time	Description	Category	Permission	ID	User	User Location	Relevance
	06-01-2016 15:12:04	06-01-2016 16:12:04	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	10.100.0.46	Management
	06-01-2016 11:48:40	06-01-2016 12:48:40	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	06-01-2016 11:39:33	06-01-2016 12:39:33	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	06-01-2016 08:12:39	06-01-2016 09:12:39	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	06-01-2016 07:40:33	06-01-2016 08:40:33	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	06-01-2016 04:36:39	06-01-2016 05:36:39	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	06-01-2016 03:41:32	06-01-2016 04:41:32	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	06-01-2016 01:00:39	06-01-2016 02:00:39	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	05-01-2016 23:42:32	06-01-2016 00:42:32	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	05-01-2016 21:24:38	05-01-2016 22:24:38	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	05-01-2016 19:43:32	05-01-2016 20:43:32	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	05-01-2016 17:48:37	05-01-2016 18:48:37	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	05-01-2016 15:44:31	05-01-2016 16:44:31	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	05-01-2016 14:12:37	05-01-2016 15:12:37	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	05-01-2016 11:45:31	05-01-2016 12:45:31	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	05-01-2016 10:36:37	05-01-2016 11:36:37	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	05-01-2016 07:46:31	05-01-2016 08:46:31	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	05-01-2016 07:00:36	05-01-2016 08:00:36	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	05-01-2016 03:47:31	05-01-2016 04:47:31	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	05-01-2016 03:24:35	05-01-2016 04:24:35	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	04-01-2016 23:48:34	05-01-2016 00:48:34	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	04-01-2016 23:48:30	05-01-2016 00:48:30	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	04-01-2016 20:12:33	04-01-2016 21:12:33	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	04-01-2016 19:49:30	04-01-2016 20:49:30	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	04-01-2016 16:36:33	04-01-2016 17:36:33	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	04-01-2016 15:50:30	04-01-2016 16:50:30	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	04-01-2016 13:00:32	04-01-2016 14:00:32	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	04-01-2016 11:51:29	04-01-2016 12:51:29	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	04-01-2016 09:24:32	04-01-2016 10:24:32	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	04-01-2016 08:35:07	04-01-2016 09:35:07	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	10.10.48.50	Management
	04-01-2016 07:52:29	04-01-2016 08:52:29	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	04-01-2016 05:48:31	04-01-2016 06:48:31	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management
	04-01-2016 03:53:29	04-01-2016 04:53:29	User successfully logged in	Security	Granted	4016	NT AUTHORITY\SYSTEM	fe80:6068:950f:bf...	Management
	04-01-2016 02:12:31	04-01-2016 03:12:31	User successfully logged in to the system from the	Security	Granted	4015	MILESTONE\SYSTEMS	..:1	Management

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

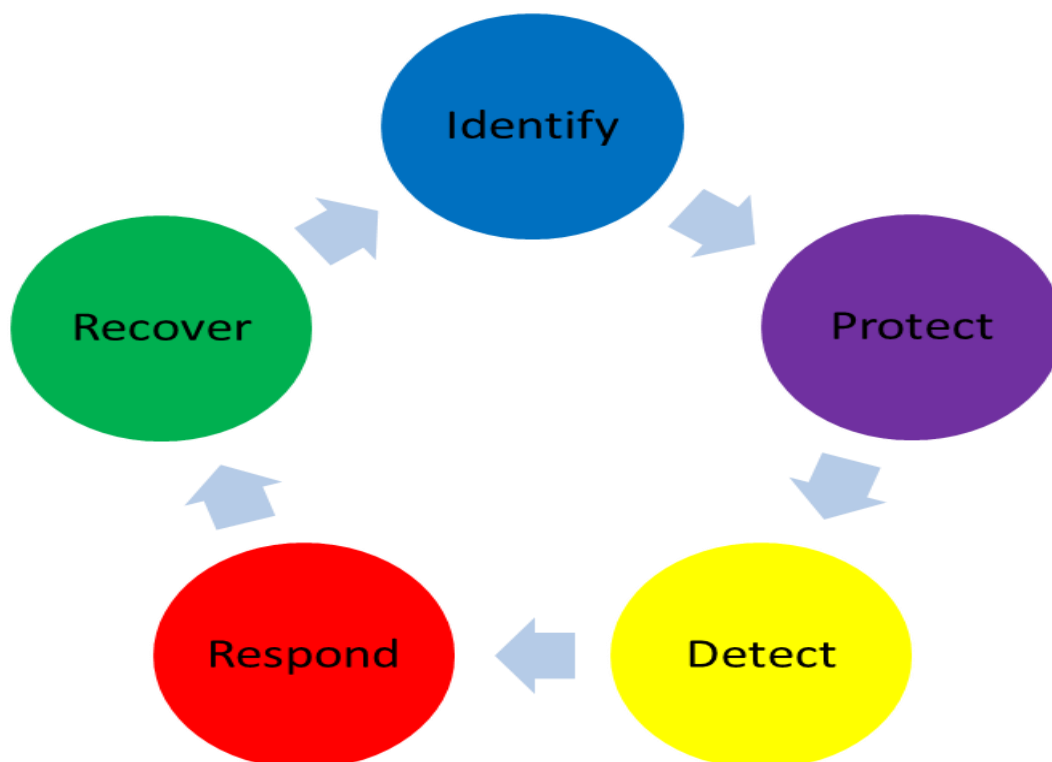
Adopt standards for secure network and VMS implementations

Milestone recommends that you adopt standards for secure networking and XProtect Advanced 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.



XProtect Advanced VMS - Hardening Guide

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 and Security Content Automation Protocol (SCAP) Validation Program.) 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, SP 800-41-rev1 (specific to firewalls), and ICS-CERT 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 Advanced 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.

Devices - basic steps

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.

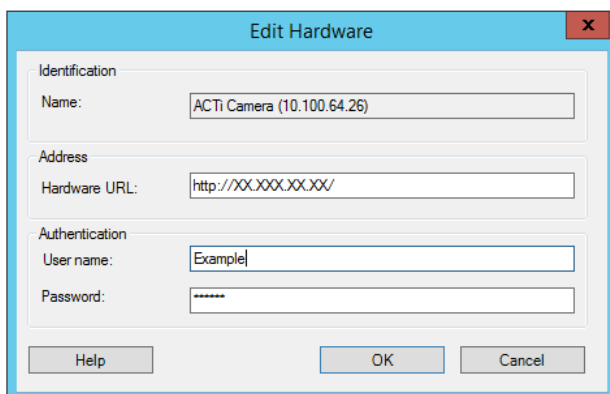
You can change the user name and password for a device before or after you add it in Management Client.

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:

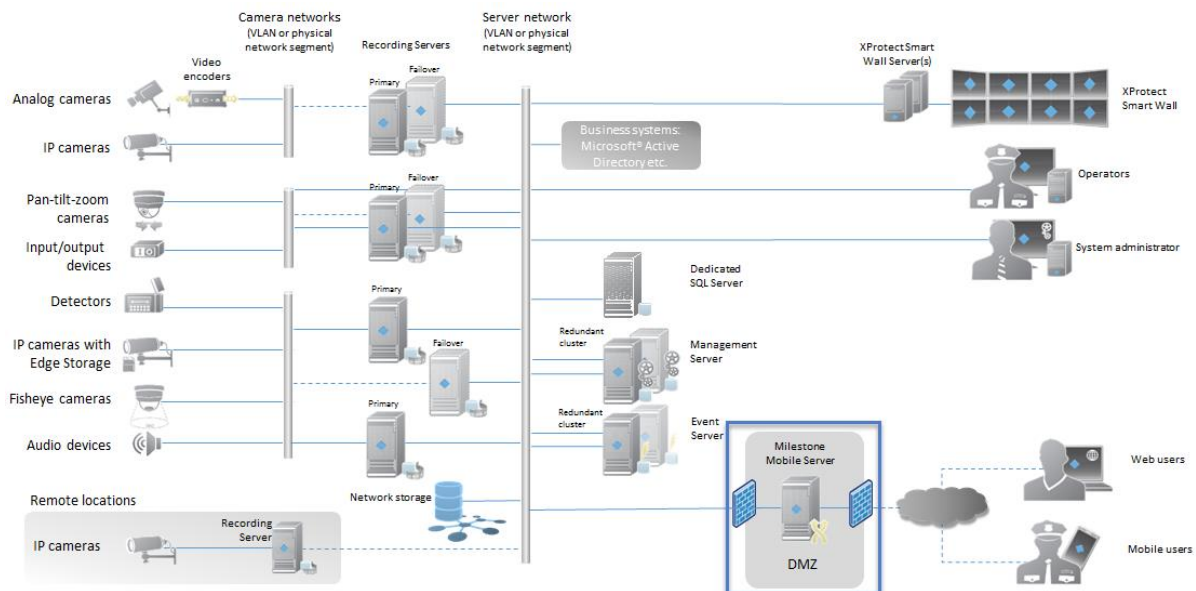
- NIST SP 800-53 AC-2 **Account Management**
- NIST SP 800-53 AC-4 **Least Privilege**

Network - basic steps

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 44).

Learn more

The following control(s) provide additional guidance:

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

Devices - advanced steps

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.

Learn more

The following control(s) provide additional guidance:

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

Network - advanced steps

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.

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, 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**

XProtect Advanced VMS - Hardening Guide

- 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 Advanced 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

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

Run services with service accounts

Milestone recommends that you create service accounts for services related to XProtect Advanced 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 [About Kerberos authentication](#) (on page 20). 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:

XProtect Advanced VMS - Hardening Guide

- 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 Advanced 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 Advanced 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 Advanced 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:

XProtect Advanced VMS - Hardening Guide

- 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 Advanced 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

Run the SQL Server database on a separate server

Milestone recommends that you make the SQL Server 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 database on a separate server, and not on the management server.

SQL 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

XProtect Advanced 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

XProtect Advanced VMS - Hardening Guide

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 Advanced VMS.

The management server ports used in XProtect Advanced 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), 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**

Recording Server

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**

Milestone Mobile server component

Only enable ports that Milestone Mobile server uses

Milestone recommends that you enable only the ports that Milestone 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 Milestone 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 the section in this document titled **Disable non-secure protocols (on page 43)**.

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**

Log Server

Install Log Server on a separate SQL Server

Milestone recommends that you install the Log Server on a separate SQL Server. If the Log Server is affected by a performance issue, for example, due to flooding or other reasons, and uses the same database as the management server, both 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 80.

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

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 \(AD\)](#) (see "Use Windows users with Active Directory" on page 18).

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.

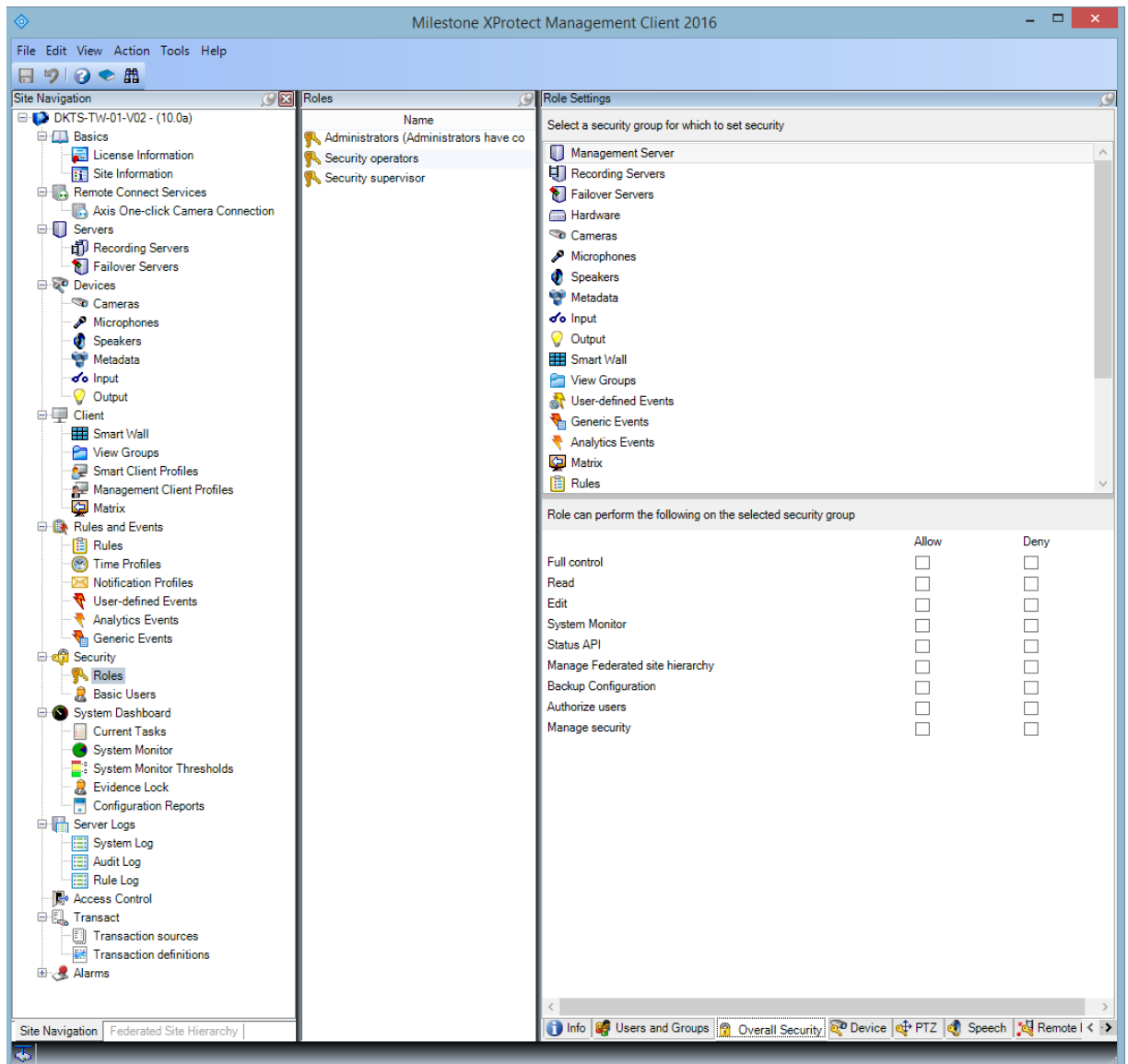
The following instructions describe how to do this. Additional information is available in the [Advanced Security Management white paper](#).

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.

XProtect Advanced VMS - Hardening Guide

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. 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**

XProtect Smart Client - advanced steps

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.

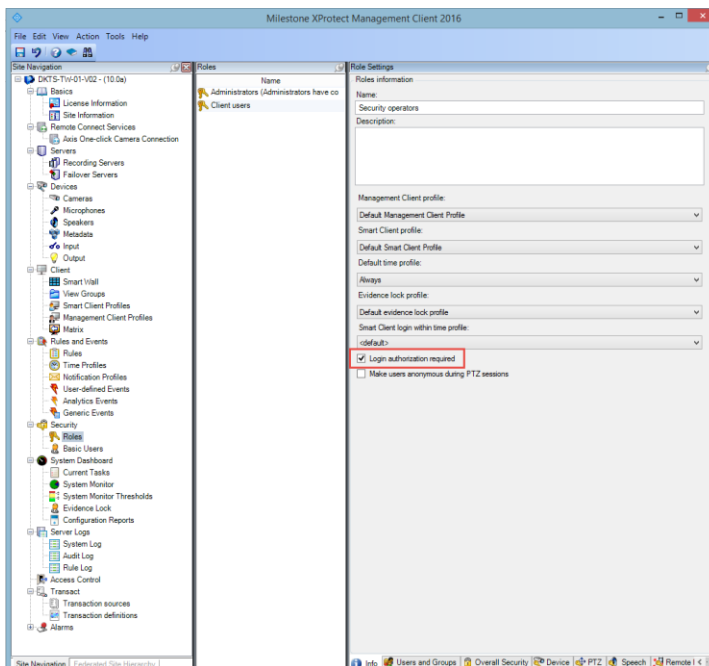
You set up login authorization on the roles. Users associated with the role are prompted for a second user (a supervisor) to authorize their access to the system.

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.

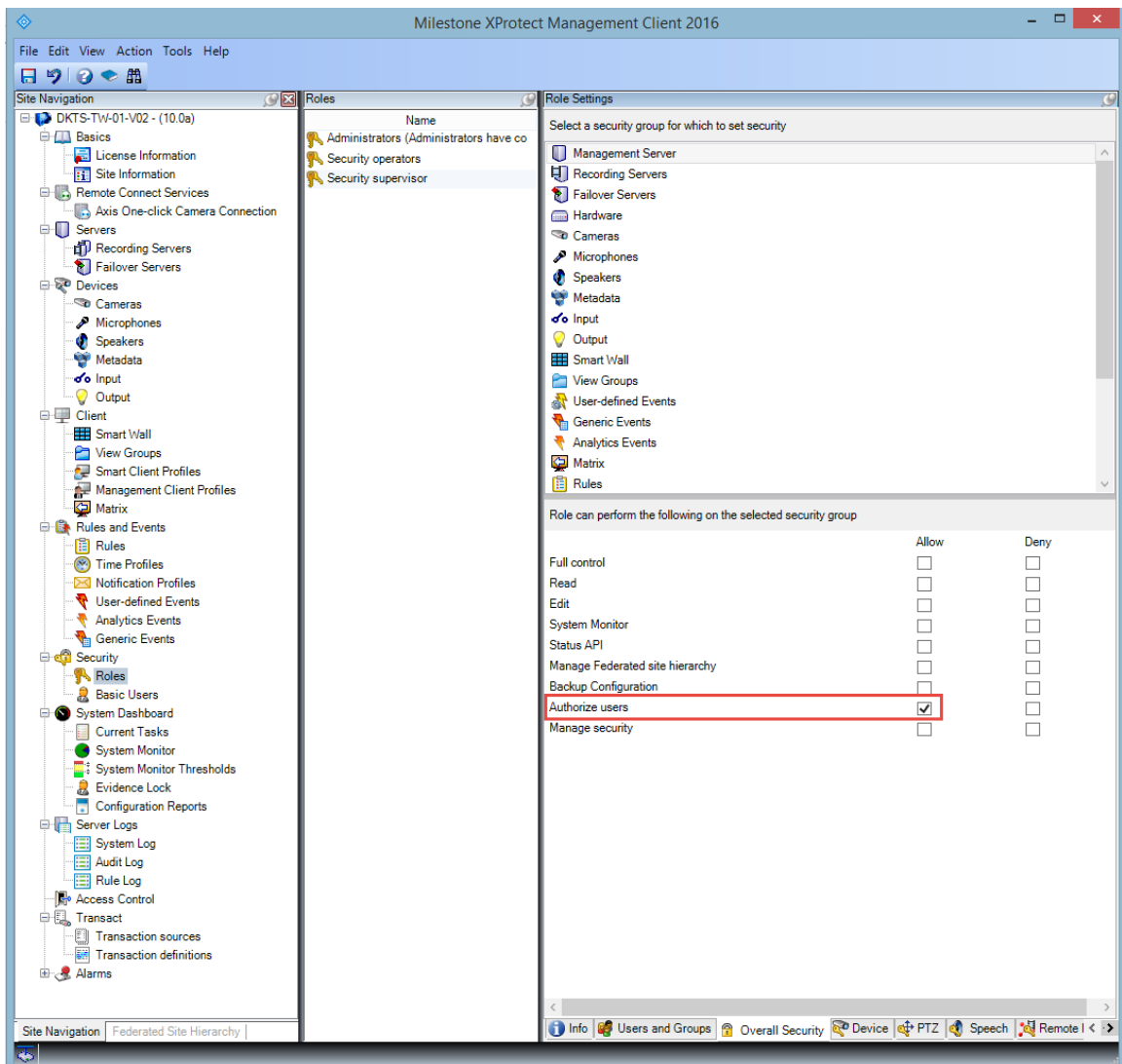


To configure the roles that authorize and grant access, follow these steps:

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.

XProtect Advanced VMS - Hardening Guide

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

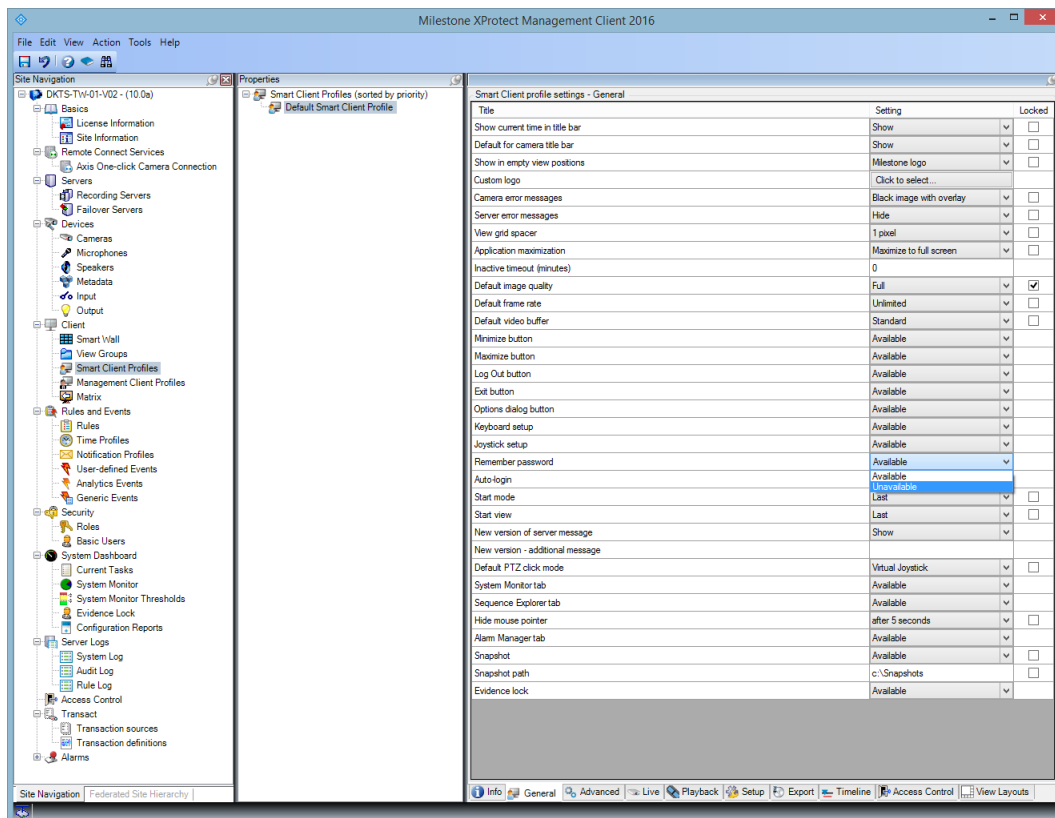
XProtect Smart Client provides the option to remember passwords for users. To reduce the risk of unauthorized access, Milestone recommends that you do not use this feature.

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

XProtect Advanced VMS - Hardening Guide

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.

XProtect Advanced VMS - Hardening Guide

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**

Milestone Mobile client - advanced steps

SP 800-124 revision 1 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

Milestone recommends that you always use the Milestone 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 Milestone 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) (or connect through VPN) 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

XProtect Advanced VMS - Hardening Guide

security policy to prohibit the Milestone 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**

XProtect Web Client - advanced steps

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 HTTPS and the latest TLS. 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 Milestone 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 certificates** section in the **Milestone Mobile Server 2016 - Administrator Guide**.

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 Internet Explorer
- 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**

Management Client - advanced steps

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 Help for Management Client.

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**

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
5. Cloud Security Alliance (CSA) and the Cloud Controls Matrix
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), 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
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, 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>

XProtect Advanced VMS - Hardening Guide

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
21. SANS institute website and the SANS Critical Security Controls
22. XProtect® Corporate – Advanced Security Management

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

Index

Use a firewall between the VMS and the Internet • 37

A

About Kerberos authentication • 3, 18, 19, 40

Activate login authorization • 49

Adjust the token time-out • 42

Adopt standards for secure network and VMS implementations • 32

Advanced steps • 32, 40

Allow administrators to access relevant parts of the VMS • 56

Always run clients on trusted hardware on trusted networks • 48

Always run XProtect Web Client on trusted client computers • 54

Always use a secure connection by default, particularly over public networks • 48

Always use the Milestone Mobile client on secure devices • 53

Appendix 1 - Resources • 9, 14, 57

Appendix 2 - Acronyms • 9, 59

B

Basic steps • 17, 40

Basic steps (all client programs) • 46

C

Changes to this document • 3

Client programs • 46

Connect the camera subnet to the recording server subnet only • 37

Index

Copyright, trademarks and disclaimer • 2

Create dedicated user accounts on each device • 36

Cyber Risk Management Framework • 11

Cyber threats and cyber risks • 10

D

Devices - advanced steps • 38

Devices - basic steps • 35

Devices and network • 35

Disable non-secure protocols • 43, 45

Do not store passwords • 50

Download the Milestone Mobile client from authorized sources • 53

E

Enable only the ports used by Event Server • 42

Enable only the ports used by the management server • 43

Establish a formal security policy and response plan • 17

Establish an incident response plan • 32

Establish surveillance and security objectives • 17

F

Follow established network security best practices • 34

Follow Microsoft OS Security best practices • 33

G

General setup • 15

H

Hardening system components • 14

XProtect Advanced VMS - Hardening Guide

Hardware and device components • 9

I

Install Log Server on a separate SQL Server • 45

Introduction • 8

K

Keep software and device firmware updated • 21

L

Limit the IP access to Log Server • 45

Log Server • 45

M

Management Client - advanced steps • 55

Management Server • 42

Milestone Mobile client - advanced steps • 53

Milestone Mobile server component • 44

Milestone Servers • 40

Mobile devices should be secured • 53

Monitor logs in the VMS for signs of suspicious activity • 30

N

Network - advanced steps • 38

Network - basic steps • 37

O

Only enable ports that Milestone Mobile server uses • 44

P

Prohibit the use of removable media • 52

Protect sensitive VMS components • 33

R

Recording Server • 37, 44

Resources and references • 9

Index

Restrict permissions for client users • 46

Restrict physical access to any computer running XProtect Smart Client • 48

Restrict the use of removable media on computers and servers • 41

Run components on dedicated virtual or physical servers • 41

Run services with service accounts • 40

Run the Management Client on trusted and secure networks • 56

Run the SQL Server database on a separate server • 42

Run the VMS on a dedicated network • 39

S

Servers, Workstations, Clients and Applications • 17

SQL Server • 42

Stop unused services and protocols • 35

T

Target audience • 8

Turn on only required client features • 51

U

Use a • 44

Use antivirus on all servers and computers • 30

Use certificates to confirm the identity of a Milestone Mobile server • 54

Use encrypted communication channels • 40

Use firewalls to limit IP access to servers and computers • 3, 22

Use individual administrator accounts for better auditing • 41

XProtect Advanced VMS - Hardening Guide

Use Management Client profiles to limit what administrators can view • 55

Use only supported browsers with the latest security updates • 55

Use physical access controls and monitor the server room • 40

Use port-based access control • 38

Use secure and trusted networks connection • 22

Use secure wireless protocols • 38

Use separate names for user accounts • 52

Use separate network interface cards • 44

Use Simple Network Management Protocol to monitor events • 38

Use strong passwords instead of default passwords • 35

Use subnets or VLANs to limit server access • 41

Use tools to automate or implement the security policy • 33

Use Windows update • 20

Use Windows users with Active Directory • 18, 46

Use Windows users with AD • 46

W

What is • 8

X

XProtect Smart Client - advanced steps • 48

XProtect Web Client - advanced steps • 54

About Milestone Systems

Milestone Systems is a global industry leader in open platform IP video management software, founded in 1998 and now operating as a stand-alone company in the Canon Group. Milestone technology is easy to manage, reliable and proven in thousands of customer installations, providing flexible choices in network hardware and integrations with other systems. Sold through partners in more than 100 countries, Milestone solutions help organizations to manage risks, protect people and assets, optimize processes and reduce costs. For more information, visit: <http://www.milestonesys.com>.

