Milestone XProtect® VMS

Deployment Best Practice

Milestone Certified Integration Technician (MCIT)

Software release version: 2020 R1

Table of Contents

Document Purpose

This document is a reference for technicians and engineers to prepare, install, configure, and otherwise deploy Milestone XProtect VMS systems.

It is intended to supplement to Milestone manuals, guides, and whitepapers with practical advice and suggestions on how to best deploy XProtect VMS and provides context for these resources as well as additional references to eLearning courses and non-Milestone resources.

The tasks and steps presented in this document are targeted at the Milestone Certified Integration Technician (MCIT) level, and covers single-server to multi-server, medium-complexity installations.

Milestone Certified Integration Technicians and Engineers can use this document as a technical design and installation reference for the following tasks:

- Planning
- Installing
- Servicing
- Expanding

This document also provides insight and guidance to the XProtect VMS Deployment Checklist companion document for each of the steps taken to deploy XProtect VMS.

Finally, this document is used as a class handbook for the Technical Configuration 1 (TC1) class and acts as a self-study guide for the Milestone Certified Integration Technician (MCIT) Certification assessment.

Feedback and corrections

If you encounter information in this document that is unclear or incorrect, please notify us at deploymentfeedback@milestone.dk.

Accessing additional resources

The task descriptions in this document are intended to be brief yet comprehensive. To accomplish this, most tasks include a list of additional resources for more in-depth information and background.

There are four categories of additional resources:

- Milestone manuals and guides
- Milestone whitepapers and other Milestone documents
- Milestone eLearning courses
- Non-Milestone resources

Refer to the descriptions below for details on how to access each of these resources.

A. Milestone manuals and guides

You may download manuals and guides from the Milestone Documentation Portal: https://doc.milestonesys.com.

Select your download location and filter for the product you are looking for.

We recommend you download the relevant resources each time you start a new project to make sure you have the most recent versions readily available at all times.

These are the manual and guides referenced in this document:

Product filter/selection	Document title
XProtect Corporate	XProtect VMS Administrator manual
XProtect Corporate	XProtect Smart Client user manual
XProtect Corporate	XProtect VMS Activate licenses quick guide
XProtect Corporate	Register software licenses - Quick guide
XProtect Corporate	XProtect hardening guide
XProtect Corporate	Certificates Guide
XProtect Corporate	XProtect VMS system architecture document
XProtect Corporate	XProtect Smart Client - Hardware acceleration quick guide
XProtect Mobile	XProtect Web client user manual
XProtect Mobile	XProtect Mobile server administrator manual
XProtect Screen Recorder	XProtect Screen Recorder - Administrator manual

Note: Some documents, such as the XProtect® Smart Client User Manual, are available in many languages while others may be available in only a few. Select a language from the dropdown list to view the documents available in that language.

B. Milestone whitepapers and other Milestone documents

You can download whitepapers and other Milestone documents from the Milestone Content Portal > Assets section. Filter by asset category: documents.

https://content.milestonesys.com/media/?resetsearch&field=metaproperty_Assetcategory&value=Documents&multiple=false&filterType=add&hideFilter=false&filterkey=savedFilters

Filter on product, language, and/or asset type, or simply use the Search field to locate the documents.

While these documents change less frequently than the manuals and guides, we still recommend you download the latest versions every time you start a new project to make sure you have the latest information.

These are the white papers and other Milestone documents referenced in this document:

Product range	Asset type	Document title
XProtect VMS	White Paper	System Architecture Guide for IT Professionals
XProtect VMS	White Paper	Ensuring end-to-end protection of video
XProtect VMS	White Paper	Large-Scale VMS Design and Management White Paper
XProtect VMS	White Paper	XProtect Corporate Advanced Security
XProtect VMS	White Paper	Milestone Interconnect White Paper

Note: If the document does not show up in your search, try changing the language filter to English.

C. Milestone eLearning courses

You can access Milestone eLearning courses through the Learning & Performance home page: https://www.milestonesys.com/solutions/services/learning-and-performance/

Click the **Partner Learning Portal** link to access the eLearning courses.

You must log in with your My Milestone ID to access the eLearning. If you don't have a My Milestone ID, the Sign Up link on the home page will take you to the Create a Milestone logon page where you can create one.

These are the eLearning courses referenced in this document:

Training track	eLearning title
Milestone Integration Technician	Milestone Fundamentals of IP Surveillance Systems
Milestone Integration Technician	Getting Started with XProtect® VMS
Milestone Integration Technician	Navigating the XProtect VMS Management Client
Milestone Integration Technician	Getting Started with rules in XProtect® VMS
Milestone Integration Technician	Adding Cameras and Device Groups in XProtect® VMS Products
Milestone Integration Technician	Configuring and Using Enhanced PTZ
Milestone Integration Technician	Configuring and Using Alarms and Notifications
Milestone Integration Technician	Moving Hardware Devices
Milestone Integration Technician	Configuring XProtect® System Monitor
Milestone Integration Technician	Getting Started with XProtect Smart Client
Milestone Integration Technician	Configuring and Using Maps
Milestone Integration Technician	Configuring and Using XProtect Smart Map
Milestone Integration Technician	Getting Started with XProtect Web Client
Milestone Integration Technician	Configuring XProtect Mobile with Smart Connect
Milestone Integration Technician	Configuring and Using Push Notifications
Milestone Integration Technician	Configuring and Using Maps
Milestone Integration Technician	Using the Customer Dashboard
Ensuring Secure Systems	Identifying Cybersecurity Threats
Ensuring Secure Systems	Recording Server Data Encryption

D. Non-Milestone resources

For non-Milestone resources, simply click the link to view the linked article.

Preparing and Installing

1. Configure the network

1A. Confirm passwords and settings on existing network and server equipment

Before installing any new equipment, you should confirm what relevant network and server equipment is already installed and document key configuration parameters. These may include access credentials, network settings, operating system version, installed patches, and other settings that may be relevant for the installation. Doing this now may save you a lot of time tracking down the information later.

1B. Check switches

Depending on the choices made by the system designer, a Milestone XProtect® installation may use a dedicated network for surveillance devices (such as cameras) to insulate them from the client network where user workstations are connected, or devices and users may share the same network.

Separating the client network from the camera network and using a separate network interface card (NIC) for each network increases performance, stability, and security and makes it easier to dimension the network:

- Performance is increased by separating the traffic to and from recording servers so any high load on the client network does not impact the recording performance.
- Stability is increased because any network interference on the client network does not affect the camera network.
- Security is increased because users or equipment on the client network cannot contact the camera directly. This effectively prevents them from accidentally or intentionally interfering with the camera operation or gaining unauthorized access to the video feeds or camera settings. Further, isolating the camera network eliminates the possibility of devices sending any kind of information via the internet without your knowledge or permission.
- Dimensioning of the network is made easier because the load is separated onto several different networks, making it easier to calculate and measure the bandwidth usage, particularly on the critical camera network.

Systems that will be using external networked storage, such as a network attached storage (NAS) or storage area network (SAN), will also benefit from this connection using a dedicated NIC and being separate from other networks.

Before beginning the installation, it is best practice to verify both the existing and planned new network structure correspond to the design assumptions, that each network interface is capable of passing the calculated or estimated bandwidth, and that the required PoE budget is within the capabilities of each switch.

Additional resources:

- System Architecture Guide for IT Professionals
- eLearning: Exploring XProtect VMS System Architecture and Communication

1C. Determine IP address ranges

Milestone recommends you determine the IP addresses and address ranges for the surveillance system and implement any changes to existing networks before beginning installation of the Milestone system. This applies to both the IP addresses of the server(s) and the address range intended for devices (such as cameras). Doing this avoids having to make time-consuming changes during the installation phase.

For ease of design, documentation, and troubleshooting, Milestone recommends using static IP addresses for servers whenever possible. The IP addresses of devices (such as cameras) may be assigned either statically or dynamically (by a DHCP server), as customer or design requirements dictate.

Milestone supports both IPv4 and IPv6 throughout the system.

See also: 1E. Test the network > Dynamic Host Configuration Protocol (DHCP), 1E. Test the network > Domain Name Server (DNS)

Additional resources:

- eLearning: Milestone Fundamentals of IP Surveillance Systems
- IP Address - Wikipedia.org
- IPv6 Addressing - ipv6.com

1D. Configure the network

As with all high-bandwidth IT systems, Layer 3 routing should generally be avoided inside the LAN and used only when necessary, such as at the edge of the network (e.g., between a LAN and the internet) or to facilitate wireless access.

The issue is primarily one of performance. Naturally, the speed of the connection (upload and download) is critical, but even in situations where the bandwidth is plentiful, a routing engine—whether in a dedicated router or a Layer 3 switch—can process only a limited number of data packages per second, potentially limiting the number of camera feeds the connection can carry.

If the installation includes a router and/or a firewall, you should ensure the bandwidth and routing performance required for the application are available before proceeding with the installation, as changes become increasingly difficult and expensive if the original assumptions are proven faulty later on.

It is also important to be clear who is responsible for documenting and configuring the routing and firewall rules. Milestone uses a range of ports for the different services and functions which must be routed for the system to work correctly. While it is possible to change most of these, if desired, Milestone recommends using the default values unless there are significant reasons not to do so.

Milestone recommends using VPN tunnel connections between different sites if the connection is made through the internet. A site in this context may be a complete XProtect VMS installation, a recording server, one or more remote cameras, or one or more Smart Client users. While it is certainly possible to set up simple port forwarding to allow such traffic without the use of VPN, this is inherently less secure and is, therefore, not recommended in most cases.

Milestone considers it good practice to implement and test routing, firewall, wireless access points, and VPN settings and connections as early in the project as possible.

Additional resources:

- XProtect VMS Administrator manual > Ports used by the system
- System Architecture Guide for IT Professionals
- XProtect VMS hardening guide

1E. Test the network

Internet access

Internet access may be relevant in several respects with a Milestone XProtect system for:

- Software license registration
- Mobile client access (Mobile devices and browser-based access) from outside the LAN
- Smart Client or Management Client access from outside the LAN
- Access to devices (such as cameras) or recording servers located in other locations

Software license registration:

If possible, the Management Server should be set up so it can access the internet to enable online/automatic authentication of the license and the configuration. If this is not possible, manual offline authentication is possible.

Mobile client access:

If users should be able to access the system from mobile devices on the internet, port forwarding must be set up to allow the incoming connection to the XProtect Mobile server. In this case, Milestone highly recommends the XProtect Mobile server service be installed on a server in the DMZ for network security reasons.

Smart Client and Management Client access:

It is possible to set up access for these clients from the internet by configuring the necessary port forward rules in the edge router/firewall. However, because doing this will inevitably make the system vulnerable to unauthorized access, Milestone highly recommends using a secure VPN solution rather than simple port forwarding in these situations.

Remote devices or recording servers:

As with Smart Client access, it is possible to set up access to remote cameras or recording servers. In the case of remote devices, this requires configuring the necessary port forward rules in the edge router/firewall where the remote devices are located. For remote recording servers, port forwards are required at both ends. Because doing this will inevitably make the system vulnerable to unauthorized access, Milestone highly recommends using a secure VPN solution rather than simple port forwarding in these situations.

See also: 1D. Configure the network.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Basics > License Information
- System Architecture Guide for IT Professionals
- DMZ (computing) - Wikipedia.org
- Virtual private network - Wikipedia.org

Dynamic Host Configuration Protocol (DHCP)

In an XProtect VMS installation DHCP is typically used only on the client network but, in some cases, it may also be beneficial, or simply required by the customer, to use DHCP-assigned IP addresses on hardware devices (such as cameras).

If any IP addresses are assigned dynamically (i.e., by a DHCP server), it is important to verify the hostname resolves correctly from the DNS server or through NetBIOS, as relevant, before proceeding to install software or devices.

Note that Microsoft does not support NetBIOS for IPv6 and that NetBIOS does not resolve across different networks.

Milestone recommends using a static IP address in a dedicated range for hardware devices, unless there are specific requirements to do otherwise. Doing this makes troubleshooting easier and allows you to search and add cameras faster.

Milestone recommends always using static IP addresses for servers, per standard IT practice.

Additional resources:

- eLearning: Milestone Fundamentals of IP Surveillance Systems
- Connecting XProtect VMS to the Internet Guide
- Static vs. Dynamic IP Addresses - whatismyipaddress.com
- Dynamic Host Configuration Protocol - Wikipedia.org
- Hostname - Wikipedia.org
- NetBIOS - Wikipedia.org
- How NetBIOS name resolution really works - techrepublic.com

Domain Name Server (DNS)

If the installation depends on resolving device hostnames through a DNS server, you should verify that hostnames resolve correctly from the recording server before proceeding to install the device in the XProtect VMS. If the recording server cannot resolve the device IP address from the hostname, it will not be able to install the device.

It is possible to force a host (such as a workstation or server) to override the DNS lookup and resolve a domain- or hostname to a specific IP address. In Windows this is done by adding the domain- or hostname and IP address to the HOSTS file in %SystemRoot%\System32\drivers\etc\hosts. (Doing this requires administrator-level privileges.)

See also: 1E Test the network > Dynamic Host Configuration Protocol (DHCP)

Additional resources:

- Domain Name System - Wikipedia.org
- Hosts (file) - Wikipedia.org
- How to grant elevated privileges in Windows 10 - thewindowsclub.com

1F. Check Network Time Protocol (NTP) server

It is critical for the correct operation of a Milestone system that the date and time of all servers and workstations are accurate to within five minutes. If the installation makes use of onboard edge storage on devices (such as cameras), or if you intend to use the cameras' on-screen date and time stamps, it is further critical that the date and time in the edge device are as closely synchronized with the recording server as possible.

The XProtect VMS uses UTC time internally, so hosts can be in different time zones as long as the time zone is set correctly and the host or device is using the correct time for their time zone.

Milestone recommends always using an NTP time source for all time-critical hosts and devices. This may be either a public NTP server, such as time.microsoft.com, or a local time server. If a workstation or server is a member of a domain, it will usually synchronize to the domain server time automatically.

If a host does not have internet access and the host is not a member of a domain, Milestone recommends installing a local NTP server, either as a software or hardware solution. Similarly, it may be necessary to install a local NTP server for devices (such as cameras) to synchronize to, especially in systems where devices are isolated on a separate network where the Milestone Recording Servers are the only host they can access.

In this latter case, very often the only way to enable devices to synchronize their internal clocks is to install a software NTP on the recording server or add a hardware NTP server to the camera network.

Examples of local time servers are:

- NetTime (http://www.timesynctool.com) is a local time server application that can itself synchronize to one or more external sources or work as a free-running clock based on the host computer's internal clock.
- Ese ES-192/ES-194 (http://www.ese-web.com/es192.htm) is a stand-alone master clock network appliance that, once set, maintains time accuracy through the precision of the 50Hz/60Hz AC line frequency.
- Veracity Timenet Pro (http://www.veracityglobal.com/products/networked-video-integration-devices/timenet-pro.aspx) is a stand-alone master NTP reference clock network appliance that uses precision GPS satellite time as its reference signal.

Additional resources:

- XProtect VMS Administrator manual > Time servers (explained)
- Network Time Protocol - Wikipedia.org
- Time server - Wikipedia.org
- NIST Internet Time Servers - tf.nist.gov
- "It's Simple!" - Time Configuration in Active Directory - docs.microsoft.com
- System Architecture Guide for IT Professionals

1G. Check access to Microsoft Active Directory

Microsoft Active Directory® is a distributed directory service implemented by Microsoft for Windows domain networks. With Active Directory installed, you can add Active Directory groups and users to XProtect VMS roles in addition to Basic Users or Windows users defined locally on the Management Server.

Milestone recommends using Active Directory groups over individually defined users whenever possible, thereby keeping all individual user management in one central location.

To add Active Directory groups (or users) to the XProtect VMS, you must have a server with Active Directory installed and acting as domain controller available on your network.

Milestone recommends you verify that you have the necessary Active Directory groups for all user roles defined before you start configuring the XProtect VMS so you don't have to interrupt your work to take care of this later.

Additional resources:

- XProtect VMS Administrator manual > Before you start installation > Prepare Active Directory
- Active Directory - Wikipedia.org
- System Architecture Guide for IT Professionals

1H. Verify Microsoft SQL server access and permissions

Milestone uses an SQL server to store system configuration and log data. The system installer includes Microsoft SQL Server Express, which is free to use and typically supports up to 300 cameras.

For installations over 300 cameras, Milestone recommends using Microsoft SQL Server Essentials, Standard or Enterprise edition, on a dedicated server. These editions can handle databases over 10 GB in size, support multiple CPU cores and more than 1 GB memory per instance, and offer more comprehensive management and monitoring options, including scheduled backup functionality.

If you are using an existing SQL server for the installation, you should verify the connectivity and credentials to access the database. When installing or upgrading the Milestone XProtect software, the user account running the Management Server installer must have sysadmin credentials on the SQL. For normal operation (i.e., the user account used for the Management Server service itself), db_owner permissions are sufficient.

Because the entire system configuration is stored in the SQL server, Milestone recommends you configure a regular backup of the VMS configuration database to ensure you always have a backup that includes the latest changes. Further, Milestone recommends you implement a transaction log backup and shrink schedule, or change the SQL database backup type to Simple, to avoid continuous buildup of transaction logs.

Additional resources:

- System Architecture Guide for IT Professionals
- XProtect VMS Administrator manual > Before you start installation > Decide on a SQL Server edition
- Microsoft SQL Server - Wikipedia.org
- Server and Database Roles in SQL Server - docs.microsoft.com
- Milestone product system requirements - milestonesys.com

1I. Verify access to remote XProtect VMS systems that will be interconnected

Milestone Interconnect™ allows multiple remote sites running any paid-license XProtect VMS product to be linked with a central XProtect Corporate site.

If you are installing XProtect Corporate and the installation will be using Milestone Interconnect to connect to remote sites, you should verify you can successfully connect to, and view camera feeds from, each of the remote sites from the location of the XProtect Corporate Management Server through the XProtect® Smart Client.

By doing this as early in the project as possible, you help ensure against having to do time-consuming troubleshooting later on during the system-configuration phase of the project.

See also: 1D. Configure the network

Additional resources:

- System Architecture Guide for IT Professionals
- Milestone Interconnect White Paper

2. Configure cameras and other IP hardware devices

2A. Set a static IP address or configure DHCP and hostname

Most installations use a static IP address for hardware devices such as cameras and encoders, but in some cases the design may specify using dynamically assigned IP addresses.

If you use a static IP address, you simply configure the IP address, network mask, and optionally a gateway in the camera. Specifying the gateway is necessary only if you want the camera to access the internet (not recommended for security reasons) or the recording server is on a different network segment from the camera (not recommended for performance reasons).

If you need to assign the IP address dynamically, make sure to set or verify the hostname of the camera and confirm the camera is receiving an IP address in the correct IP range from the DHCP server and that the hostname of the camera resolves correctly from the recording server.

The easiest way to test this is to connect the camera to the intended camera network and ping the camera hostname from the recording server or another PC connected to the recording server network.

Also note that, if you use dynamically assigned IP addresses, because the IP address is by definition subject to change, you must specify the hostnames individually using the Manual detection mode in the XProtect VMS.

See also: 1C. Determine IP address ranges, 1E. Test the network > Dynamic Host Configuration Protocol (DHCP), 1E. Test the network > Domain Name Server (DNS)

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Hardware > Add hardware

2B. Set administrator account credentials

The XProtect VMS must access the device with administrator-level access. Most devices come with a preconfigured administrator account username. You may use the built-in administrator account or create a new one.

Some devices come with default passwords for the preconfigured user accounts. For security reasons, Milestone recommends you change any default passwords before deploying the camera, even if you will be deploying the camera to an isolated camera network that is reachable only by the recording server (recommended).

See also: 1B. Check switches

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Hardware > Add hardware

2C. Verify firmware version with Milestone Supported Devices list

The XProtect VMS Recording Server usually communicates with hardware devices through either a device driver developed specifically for individual devices or a series of similar devices from the same manufacturer.

Use the supported devices list on the Milestone website to verify whether your device is supported by a dedicated driver and what firmware versions the driver supports.

If the firmware currently installed in the hardware device is not in the list, you must install a supported version before installing the hardware device to the XProtect VMS. Milestone generally recommends you always install the latest supported firmware.

The list also notes whether the driver is included in the regular device pack or the legacy device pack (a device pack containing drivers for older devices). If you need to connect to devices supported in the legacy device pack, you must download and install this separately before or—optionally, for new installations—after installing the recording server.

Additional resources:

- XProtect VMS Administrator manual > Main system components > Recording Server
- Find hardware for XProtect® and Milestone Husky™ - milestonesys.com

2D. Mount cameras and other IP hardware devices

Since it is generally easier to correct problems before mounting a camera or other IP hardware device, Milestone generally recommends you complete steps 2A, 2B, and 2C before mounting the device.

When the device is mounted, you can perform location-specific tasks—such as adjusting the field of view (FoV) and focus to match the statement of work (SOW) or design specification, and connecting I/O and audio wires.

> **Note:** Depending on the device, the tools you have available, and your preferred method of working, it may be beneficial to defer this step until after you have added the device to the XProtect VMS. This way, if the installation includes access through a WiFi access point, or you choose to set up a temporary access point, you can use the XProtect Mobile client on a tablet when adjusting the FoV and focus.

2E. Configure additional device settings

In many cases, the steps above are all you need to do to make the hardware device ready to use. In some cases, however, you may need or want to do additional configuration, such as setting up onboard hardware motion detection, events, or analytics.

Milestone also generally recommends you disable any on-screen date and time stamps on cameras. The XProtect VMS will automatically timestamp all video, audio, and metadata when it is recorded. The timestamp is used for recording searches, playback, and evidence export.

If the on-screen time stamp is enabled, and the camera is not synchronized to the same time source as the recording server, the exported evidence will show two different times which may lead to confusion as to the time the evidence was recorded.

See also: 2A. Set a static IP address or configure DHCP and hostname, 2B. Set administrator account credentials, 2C. Verify firmware version with Milestone Supported Devices list, 2D. Mount cameras and other IP hardware devices

Additional resources:

- System Architecture Guide for IT Professionals > NTP

2F. Install Milestone Screen recorder

The Milestone XProtect Screen Recorder allows a Windows computer to act as an IP video camera, sending the contents of all monitors, or a specific monitor, to an XProtect VMS Recording Server.

The XProtect Screen Recorder consists of a small application you can download from the Milestone website and install on the Windows computer you want to record, and a hardware device driver included in the device pack installed on the Recording Server.

Additional resources:

- XProtect Screen Recorder - Administrator manual

3. Configure Windows servers

3A. Obtain or create server communication encryption certificates

If encryption is required for one or more XProtect server communication flows, obtaining the certificates may take some time. Starting the process of obtaining certificates even before you start installing the operating system may save you time and delays later on.

Milestone recommends that you establish a Public Key Infrastructure (PKI) for creating and distributing certificates. In a Windows domain, it is recommended to establish a PKI using the Active Directory Certificate Services (AD CS).

If you are unable to use a PKI, you must manually create and distribute certificates to use server encryption.

> Note: If you use manual distribution of certificates you are responsible for keeping the private certificates secure at all times. When you keep the private certificates secure, the client computers that trust the certificates are less vulnerable to attacks.

> Note: Starting with XProtect VMS version 2019R2, XProtect Mobile no longer includes the option to use auto-generated self-signed certificates for HTTPS encryption for client communication. Instead, a certificate must be implemented using a trusted CA the same way as for other system components. Because manually installing your own CA certificates on mobile devices can be challenging and is not regarded as secure, Milestone recommends obtaining server certificates for the mobile servers from a CA that is natively trusted by the mobile devices.

> Note: As server communication encryption is primarily relevant to services external to the management server, single-server installation can usually omit using management server communication encryption without compromising security.

Additional resources:

- XProtect VMS Administrator manual > Secure communication (explained)
- XProtect VMS certificates guide
- XProtect VMS hardening guide
- eLearning: Identifying Cybersecurity Threats
- eLearning: Recording Server Communication Encryption
- Public key infrastructure - Wikipedia.org
- Self-signed certificate - Wkipedia.org

3B. Install operating system environment

Installation is straightforward, as long as you pay attention to a few details.

Virtualization

All Milestone components can be deployed in a virtual environment, with various advantages and disadvantages.

Virtualization is often used to utilize hardware resources better, because typically the different virtual servers running on the hardware host server do not load the virtual server extensively and often not at the same time. This is also true for the Management Server and its various dependencies.

By contrast, the XProtect Recording Server service that records all the cameras and streaming video to clients is a comparatively high resource-demanding service that will consistently put a high load on CPU, memory, network, and the storage system.

Therefore, a usual advantage of using virtualization to a large extent does not apply to a recording server because, in most cases, it will use all available resources all the time, leaving nothing for other virtual servers to use.

Microsoft® Windows

Make sure the Windows version is supported for the component you are installing.

For recording servers, Milestone recommends setting the Windows Power Profile to “Full”, as the dynamic throttle mechanism may be slow to react and has been proven to be limiting Recording Server performance, especially in larger environments.

Windows server hostname

The XProtect VMS uses the server hostname in several respects—for example, for SQL server requests, for all Management Server services, for mobile and recording server communication, and as the default name when installing Recording Servers. So, while it is possible to update the system if you change the hostname of a server, Milestone recommends setting the hostname as desired before installing any Milestone software or Microsoft SQL.

XProtect VMS server hostnames should comply with Microsoft NetBIOS Computer Naming Conventions and be limited to 15 characters or less. Hostnames containing more than 15 characters will be truncated, which may cause problems and system errors, as multiple servers may appear to have identical names.

Milestone also recommends avoiding the use of the underscore (_) in hostnames, as this character is not supported by DNS servers.

See also: 1E. Test the network > Domain Name Server (DNS)

Additional resources:

- Milestone product system requirements - milestonesys.com
- XProtect VMS Administrator manual > Managing registered services
- XProtect VMS Administrator manual > Managing the SQL Server and databases > Changing the SQL Server and database addresses (explained)
- XProtect VMS Administrator manual > Moving the management server
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Change or verify the basic configuration of a recording server
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Failover servers > Change the management server address

3C. Set and verify network settings

As with all servers, make sure IP address, network mask, default gateway, and DNS server settings are set correctly. Milestone recommends using static IP addresses on your XProtect VMS servers.

It is possible to change the IP address of a server at any time; however, in many cases this will require some additional configuration to ensure the services communicate correctly. Consequently, Milestone recommends configuring the server as it is intended to run in production before installing any XProtect VMS software onto it.

See also: 1C. Determine IP address ranges, 1E. Test the network

3D. Check server access

Internet access

In most cases, the XProtect VMS servers do not require internet access for any purpose other than installing Windows updates. In this situation, an easy way to help protect the server from malicious software or unauthorized access may be to simply not allow it to access the internet.

The management server must have access to the internet if you intend to use online or automatic license activation. In the case of manually initiated online activation, the server needs access for only the few minutes the activation takes.

The management server must also have internet access if you intend to use the Milestone Customer Dashboard.

The XProtect Mobile server must have internet access if you need mobile and web clients to access the system from outside the network.

If you need Smart Client users to access the system from outside the network, Milestone highly recommends using a VPN connection for network security reasons. But, if you want simply to set up direct access through port forwarding, all recording servers as well as the management server must be set up with internet access.

Hostname lookup

All XProtect VMS server components and services, as well as Management Clients, must be able to successfully resolve the hostnames of any of the servers that host those services, even if the servers are added to the configuration using their IP address.

Therefore, when preparing a new server, it is good practice to verify it can resolve the hostnames of other servers and that other servers successfully resolve the hostname of the new server.

If the hostnames do not resolve through the DNS, or there is no DNS, you may edit the Windows HOSTS file manually.

See also: 11B. Activate license, 24B. Verify connectivity to Customer Dashboard, 25. Configure Mobile servers, 1E. Test the network

Additional resources:

- Milestone Customer Dashboard - milestonesys.com

3E. Add and verify user accounts and passwords

Management Server

On the server running the Management Server service, any Windows user that is a member of the Windows User Management Administrators user group will by default also be able to log in with the XProtect Management Client with full administrator credentials. To ensure you are never left with a system you cannot log into, this setting cannot be changed, so you will typically want to make sure you limit this access as much as possible.

In some systems—particularly smaller systems or demo systems with only a few users—it may sometimes be easiest to simply define additional users in Windows User Management and subsequently give those users permissions within the XProtect VMS.

This would be a good time to create those users. You can either define those users in the Guests group or create a custom group that has no critical permissions on the server itself.

If the server is on a domain with Microsoft Active Directory, you will, in almost all cases, want to use those AD groups (or individual users) to assign permissions within the XProtect VMS.

This is a good time to verify or add the AD groups you plan to use.

Other XProtect VMS servers

In most cases, there are not special requirements for users defined in Windows User Management or Active Directory on servers other than the server running the Management Server service.

There are, however, two notable exceptions:

- Servers used as recording servers that need access to a storage system that requires user authentication—for example, a network attached storage (NAS)—must have a Windows user defined that has full read, write, create, and delete file access on the NAS for the recorder server service to run under.
- Servers used as Failover Recording Servers must have a user created for the failover service to run under that allows the Failover Server service to start and stop the Failover Recording Server service.

See also: 1G. Check access to Microsoft Active Directory, 7. Install XProtect Recording Servers, 8. Install XProtect Failover Recording Servers

Additional resources:

- XProtect VMS Administrator manual > Before you start installation > Prepare Active Directory

3F. Enable remote management, such as Windows Remote Desktop

In many cases you will want to be able to manage any server remotely to perform Windows Updates, update the XProtect VMS software, and check on the status of the XProtect VMS server services. To allow this, you need to enable Windows Remote Desktop Protocol (RDP) or install some other form of remote access.

Additional resources:

- Remote Desktop Protocol - Wikipedia.org

3G. Check server time

It is essential that the server is set to the correct time and time zone. Recording Servers use the time to time stamp all recordings, while the Management Server uses the main system time and log entries. The time is converted to UTC time when stored, which allows the system to manage servers in different time zones seamlessly.

If you use a common time source for all servers (recommended), such as internet time or a local NTP time server, you should verify that the time updates correctly. If the server is on a domain, it will automatically synchronize to the domain server time.

Also note that if you log into the Management Server with the Management Client or Smart Client, and the workstation time deviates more than five minutes from the server time, the client will be denied access.

See also: 1F. Check Network Time Protocol (NTP) server

3H. Install all important Windows Updates

Milestone recommends always keeping your system current by installing all important updates from Microsoft.

3I. Check additional server software and settings

Depending on what you will be using the server for, the XProtect VMS may have specific requirements in addition to the version of Microsoft Windows itself. Minimally, you should verify the .Net version and Direct X version meet the requirements and that Intel Quicksync is enabled, if available.

If the server is equipped with NVIDIA graphics cards, you should verify the latest version of the NVIDIA driver software is installed.

If the server will be used as a Management Server, also verify that internet Information Services (IIS) is available, but not installed. (The Management Server installer will install and configure IIS automatically.)

Additional resources:

- Milestone product system requirements - milestonesys.com
- XProtect VMS Administrator manual > Before you start installation > Prepare your servers and network
- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Motion tab (devices) > Hardware acceleration (explained)
- Knowledge base article 000011033: Installation of XProtect VMS fails because automatic installation of IIS components failed (solution)

3J. Add anti-virus scan exceptions

If you run an anti-virus solution on the server, you must add the recommended exceptions to the real-time and disk scanning routines in order not to impact system performance.

The required exceptions include real-time and periodic scanning of the specific file extensions that are used by the XProtect Recording Server database (.blk, .idx, and .pic), and the folders and subfolders used by the various Management Server services, the Recording Server service, and the XProtect Mobile server service. Depending on the anti-virus software you may also need to exclude any real-time scanning of the IP ports those services use or the server processes themselves.

The exceptions must be added to all servers running an XProtect VMS server service or storage, including SAN or NAS servers.

The customer's organization may have strict guidelines regarding virus scanning, but it is important that you meet these requirements to prevent compromising the server, storage, and system performance.

Additional resources:

- XProtect VMS Administrator manual > Before you start installation > Virus scanning exclusions (explained)

3K. Enable SNMP traps

If the server is a management server and you will be using Simple Network Management Protocol (SNMP) traps, you must enable the SNMP agent in Windows.

See also: 24C. Verify SNMP trap connectivity

Additional resources:

- Simple Network Management Protocol - Wikipedia.org
- System Architecture Guide for IT Professionals > Mobile Server

4. Configure storage

4A. Prepare storage system

If you will be using RAID on your storage system, make sure it is set to a RAID stripe of 512kB or larger. Using a smaller block size may result in not getting the optimal performance out of the RAID system.

By default, Windows formats an NTFS disk with a 4 kB block size. For best performance, make sure your storage is formatted with NTFS 64 kB block size, regardless of the use of RAID and JBOD.

If you will be recording to a storage system running RAID 5 or RAID 6, you should take particular care to ensure the storage system has sufficient performance to meet the worst-case scenario of recording and playback while the RAID is recovering from a disk failure (rebuilding the RAID).

If the storage is intended for archiving only, it must have sufficient performance so that the recordings can be still transferred while the RAID is recovering from a disk failure. Milestone generally recommends you use archiving only if you will be storing the long-term storage on a physically different storage system than the recording database (for example, on a NAS system).

> **Note:** For performance and disk wear reasons, Milestone recommends you do not record or archive to the same physical disk that is used for the operating system (Windows), with the exception of high-performance, multi-disk RAID 10 systems.

> **Note:** For optimal performance, Milestone recommends you disable Windows indexing and disk compression on all video storage drives, as well as the drive containing the SQL database.

> **Note:** Milestone does not recommend using file systems other than NTFS, and explicitly does not recommend using Microsoft Resilient File System (ReFS) for the storage system at this time as it may result in degraded recording and playback performance over time.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage and archiving (explained)
- Knowledge base article 000001845: 'Media overflow' error messages in XProtect Corporate System Log
- XProtect VMS Administrator manual > Navigating the Management Client

4B. Verify access to remote storage

If you will be archiving to a NAS storage or recording or archiving to a SAN, you must make sure the user running the Recording Server service has full file access permissions on the storage resource.

For performance and database integrity reasons, Milestone strongly recommends you never record to a storage system that is not permanently and directly attached to the recording server, such as a NAS or USB drive. Doing so may result in loss of evidence and force the need for a database repair if the connection momentarily breaks.

> **Note:** In cases where the risk of losing connectivity is extremely small, it is generally acceptable to regard a redundant iSCSI connection as being a direct attached connection.

See also: 3E. Add and verify user accounts and passwords

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage and archiving (explained)

5. Install XProtect Management Server

5A. Prepare for installation

In preparation for installation, download the installation file from the Milestone website and make sure you have the .LIC software license file, unless you are installing the free XProtect Essential+ version.

> **Note**: Please refer to the Upgrade the System section if you are upgrading from a previous version of XProtect VMS.

> **Note**: If you are upgrading from a previous version and depend on XProtect Smart Client users being able to access the system immediately after the upgrade, you **must** upgrade the clients before upgrading the servers.

See also: "32E. Upgrade the system" on page 135

Additional resources:

- XProtect VMS Administrator manual > Before you start installation > Register Software License Code
- XProtect VMS Administrator manual > Before you start installation > Requirements for offline installation

5B. Import certificates on the management server

If available, import any certificates required on the server to the Windows Certificate Store.

Importing the certificates at this time allows enabling encryption from within the installer, if desired.

See also: 3A. Obtain or create server communication encryption certificates

Additional resources:

- XProtect VMS certificates guide

5C. Run the Management Server installer

For all situations other than a simple single-server installation, choose **Custom**.

If you are using an **existing SQL server**, make sure to run the Management Server **installer** under a user that has sysadmin permissions on the SQL server.

> **Note**: In rare situations, the system design document may specify that you install the Event Server or Log Server on a separate server for performance reasons. In these cases, make sure the users running those services have permissions to access the both the Management Server and the SQL database.

See also: 3E Add and verify user accounts and passwords, 1H Verify Microsoft SQL server access and permissions

Additional resources:

- XProtect VMS Administrator manual > Install a new XProtect system
- XProtect VMS Administrator manual > Before you start installation > Installation method
- System Architecture Guide for IT Professionals > System Components

5D. Select service user account

In a multi-server installation, there are some additional considerations to consider if installing in a workgroup environment or if installing as part of a Milestone Federated Arcitecture.

Workgroup:

In a Workgroup environment, Milestone generally recommends that all servers (Management Server, Recording and Failover Recording Servers, and Mobile servers) are installed to run under the same user name (for example, administrator), if possible.

The user must be a member of the administrators group in Windows user management on the server.

The reason for this is that the Data Collector service, which is installed along with all XProtect VMS servers, does not have permission to send data to the Management Server when running under the NETWORK SERVICE user in a Workgroup environment. This, in turn, results in the System Monitor and Customer Dashboard features (if available) not being able to monitor and display the health and performance of those servers.

If it is not possible to install a server (for example, a Recording Server) to run under the same user name as the Management Server, you should still install the Management Server to run under a specific user account. You can change the user running the Data Collector service after the installation completes.

Milestone Federated Architecture (MFA):

In an MFA system, all Management Servers must be installed to run under the same user name (for example, administrator). If you are installing in a Windows domain environment, the user must be a domain user and must be a member of the administrators group in Windows user management on the server.

See also: 3E. Add and verify user accounts and passwords

Additional resources:

- XProtect VMS Administrator manual > Before you start installation > Select service account
- XProtect VMS system architecture document

5E. Specify server encryption

If you will be using server communication encryption and have already imported the necessary certificates, the installer gives you the option to select the certificates and enable the encryption during the installation (default selection).

To simplify troubleshooting, Milestone suggests you do not enable server encryption until you have verified that servers and clients are communicating correctly.

> Note: In single-server installations, if you have not imported the Mobile server certificate prior to running the installer, you must clear the encryption option check box and will not be able to use HTTPS communication until a certificate is imported and enabled.

See also: 3A. Obtain or create server communication encryption certificates,5B. Import certificates on the management server

Additional resources:

- XProtect VMS Administrator manual > Secure communication (explained) > Management server encryption (explained)
- XProtect VMS Administrator manual > Secure communication (explained) > Encryption from the management server to the recording server (explained)
- XProtect VMS Administrator manual > Secure communication (explained) > Mobile server data encryption (explained)
- XProtect VMS certificates guide

5F. Verify the server is running

Once the install completes, verify the Management Server Manager and Event Server Manager notification area tray icons shows the server services have started correctly (the icon status is green).

Verify the Windows Firewall (if enabled) allows inbound access to all ports used by the Management Server.

Additional resources:

- XProtect VMS Administrator manual > Managing server services
- XProtect VMS Administrator manual > Managing server services > Server manager tray icons (explained)
- XProtect VMS Administrator manual > Ports used by the system

6. Install XProtect Mobile server

6A. Prepare for installation

Unless you are installing a single-server system, if you need to enable Mobile or Web Client access to the system, you must download and run the XProtect Mobile server installer on the server(s) where you want to run the XProtect Mobile server. In a system with only limited mobile access from internal WiFi or via VPN, this may be the management server itself if the server performance allows.

In installations where there will be a lot of mobile use, the XProtect Mobile server is usually installed on a separate server, or even multiple servers, for best performance and in order for the mobile traffic not to impact the performance of the management server.

In installations where mobile users will access the system from the internet directly (i.e., without a VPN), Milestone highly recommends locating the mobile server in the DMZ. The firewall should be configured to forward only the necessary ports originating from the mobile server to the XProtect VMS servers on the LAN.

6B. Import certificates on mobile servers

If available, import any certificates required on the server to the Windows Certificate Store.

Importing the Mobile server certificate at this time allows enabling encryption from within the installer, if desired.

> Note: If you have not imported the Mobile server certificate prior to running the installer, you must clear the encryption option checkbox and will not be able to use HTTPS communication until a certificate is imported and enabled.

See also: 3A. Obtain or create server communication encryption certificates

Additional resources:

- XProtect VMS Administrator manual > Secure communication (explained) > Mobile server data encryption (explained)

6C. Download and run XProtect Mobile server software from the Management Server

The XProtect Mobile server installation file is available on the Management Server admin download page: http://<management server>/installation/admin

> Note: If the servers are running in a Workgroup environment, Milestone recommends you install the Mobile Server to run under the same user name as the Management Server. Alternatively, you can change the user running the Milestone Data Collector service after the installation completes to ensure the System Monitor function is able to receive performance data from the server.

See also: 5D. Select service user account

Additional resources:

- XProtect VMS Administrator manual > Download Manager/download web page
- XProtect Mobile server administrator manual > Install XProtect Mobile server
- XProtect Mobile server administrator manual > XProtect Mobile (explained)
- DMZ (computing) - Wikipedia.org

6D. Specify mobile server encryption

Specify the certificate to use for HTTPS communication with XProtect Web Client and XProtect Mobile clients.

> Note: If you have not installed the Mobile server communication encryption certificates prior to running the installer, you must clear the encryption option checkbox and will not be able to use HTTPS communication until a certificate is imported and enabled.

See also: 6B. Import certificates on mobile servers

Additional resources:

- XProtect Mobile server administrator manual > Install XProtect Mobile server
- XProtect Mobile server administrator manual > Enable encryption > Enable encryption on the mobile server

.

6E. Specify URL and credentials to connect to the Management Server

The XProtect Mobile server needs to know how to contact the Management Server.

If you are installing the mobile server directly on the management server, the default options will work in almost all cases.

If you are installing on a separate server, you must specify the URL of the Management Server using either the server hostname or IP address, and you must specify the user account the Mobile server should log in as (for example, <hostname>\administrator). The user account must have administrator privileges.

Additional resources:

- XProtect VMS system architecture document

6F. Verify the server is running

Once the install completes, verify the XProtect Mobile server notification area tray icon shows the server service has started correctly (i.e., the icon status is green).

Log into the Mobile Server with the XProtect Web Client from the server hosting the Mobile Server to verify the Mobile Server is responding correctly. Any user that has Windows administrator rights on the management server will work.

Verify the Windows Firewall (if enabled) allows inbound access to all ports used by the Mobile server.

Repeat the XProtect Web Client login test, this time from a PC or server on the client network. Verify both HTTP and HTTPS logins are working, if both are allowed in the Windows firewall.

> Note: If a Mobile server certificate is not installed, the server notification area tray icon status will show yellow (not green) until either a certificate is imported and enabled or HTTPS communication is disabled via the Management Client.
>
> XProtect Web Client and XProtect Mobile clients will be able to use HTTP communication only if a certificate is imported and enabled.

Additional resources:

- XProtect VMS Administrator manual > Managing server services > Server manager tray icons (explained)
- XProtect VMS Administrator manual > Ports used by the system
- XProtect VMS Administrator manual > Secure communication (explained) > Mobile server encryption requirements for clients

7. Install XProtect Recording Servers

7A. Prepare for installation

Before installing a Recording Server, you should verify if the cameras you plan to use are supported in the device pack that comes with the Recording Server.

If you are installing the latest version for the software, the device pack will always be less than about four months old. If you are installing a Recording Server with an older version of the XProtect VMS or your device or device firmware is very recently released, you should download the newest device pack from the Milestone website.

If one or more of your hardware devices is listed as supported in the legacy device pack, you should make sure this is installed prior to installing the recording server.

In very rare cases, you can have a situation where the older firmware in a device is not compatible with the latest device packs but is supported in an older device pack. In these cases, Milestone will always recommend upgrading your device firmware to a version supported in the latest device pack. If, for some reason, that is undesirable, you may install an older device pack to overwrite the newer drivers.

For simplicity and ease of troubleshooting, Milestone recommends you always use the same device pack on all recording and Failover Recording Servers.

> **Note:** The Legacy Device Driver requires restarting the Recording Server Service or rebooting the server after installation, even if the installer does not prompt you to do this.

See also: 32D. Configure the Download Manager

Additional resources:

- XProtect VMS Administrator manual > Before you start installation > Device drivers (explained)
- XProtect VMS Administrator manual > Download manager/download web page > Device pack installer - must be downloaded
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Recording servers (explained)
- XProtect VMS system architecture document
- Knowledge base article 000006977: Legacy Device Pack: how to recognize the newly installed drivers

7B. Import certificates on recording servers

If available, import any certificates required on the server to the Windows Certificate Store.

Importing the certificates at this time allows enabling encryption from within the installer, if desired.

> Note: If you have already enabled management server communication encryption, you must ensure the recording server certificate is imported to the Windows Certificates Store and the CA is trusted on both the management server and recording server at this time.

See also: 3A. Obtain or create server communication encryption certificates

Additional resources:

- XProtect VMS Administrator manual > Secure communication (explained) > Encryption from the management server to the recording server (explained)
- XProtect VMS certificates guide

.

7C. Download and run the XProtect Recording Server installer from the Management Server

Unless you are installing a single server system, you must download and run the Recording Server installer on the server(s) you want to use as recording server(s).

The XProtect Recording Server installation file is available on the Management Server administrative installation page: http://<management server>/installation/admin

The typical installation option will install the Recording Server service under the NETWORK SERVICE user account. If you will be archiving recordings to a NAS or other external storage that requires user authentication, you must choose the custom installation option. This allows you to specify a user account for the Recording Server service that has access to the archive storage.

In all cases, you will need to specify a Recording Server name. The default option is the hostname of the recording server, but you can choose any name containing normal letters and numbers, including spaces. The name should ideally allow both system administrators and Smart Client users to easily identify the Recording Server by location or purpose.

You must also specify the hostname (or IP address) and port the Recording Server should use to contact the Management Server, as well as select a default path for recordings. Milestone recommends you do not store recordings on the physical drive that is used by the operating system (Windows).

> Note: If the servers are running in a Workgroup environment, Milestone recommends you install the Recording Servers to run under a user with the same user name as the Management Server, if possible. Alternatively, you can change the user running the Milestone Data Collector service after the installation completes to ensure the System Monitor function is able to receive performance data from the server.

See also: 4. Configure storage, 5C. Run the Management Server installer

Additional resources:

- XProtect VMS Administrator manual > Install new XProtect components > Install a recording server through Download Manager

7D. Specify recording server encryption

If you will be using recording server communication encryption and have already imported the necessary certificates, the installer gives you the option to select the certificates and enable the encryption during the installation (default selection).

To simplify troubleshooting, Milestone suggests you do not enable server encryption until you have verified that servers and clients are communicating correctly.

See also: 7B. Import certificates on recording servers

Additional resources:

- XProtect VMS Administrator manual > Install new XProtect components > Install a recording server through Download Manager
- XProtect VMS Administrator manual > Secure communication (explained) > Encryption from the management server to the recording server (explained)

7E. Verify the server is running

Once the install completes, verify the XProtect Recording Server notification area tray icon shows the server service has started correctly (i.e., the icon status is green).

Verify the Windows Firewall (if enabled) allows inbound access to all ports used by the Recording Server.

Additional resources:

- XProtect VMS Administrator manual > Managing server services > Server manager tray icons (explained)
- XProtect VMS Administrator manual > Ports used by the system

7F. Install a different device pack

After the installation completes, you can install a different device pack if necessary.

See also: 7A. Prepare for installation

7G. Add anti-virus scan exceptions

If you run an anti-virus solution on the server, and if you have not already done so, you must add the recommended exceptions to the real-time and disk scanning routines in order not to impact system performance.

See also: 3J. Add anti-virus scan exceptions

8. Install XProtect Failover Recording Servers

8A. Prepare for installation

In addition to the preparations discussed for a regular Recording Server, because a service running under the NETWORK SERVICE account does not have permissions to start and stop other services, you must make sure the Failover Recording Server has a user specified under Windows User Management that you can use to run the Failover Server service.

The user must be a member of the Administrators group or otherwise have administrator privileges. In a workgroup environment, the user name should be the same as that running the Management Server to ensure the System Monitor function is able to receive performance data from the server.

See also: 7A. Prepare for installation, 5C. Run the Management Server installer

Additional resources:

- XProtect VMS Administrator manual > Install new XProtect components > Install a failover recording server through Download Manager
- XProtect VMS system architecture document

8B. Import certificates on failover recording servers

If you imported any certificates when installing the recording servers, you should import the same certificates on the failover recording servers.

See also: 7B. Import certificates on recording servers

8C. Download and run the XProtect Recording Server installer from the Management Server

Download and run the Recording Server installer on the server(s) you want to use as failover recording server(s) and choose the failover installation option.

You must specify a Failover Recording Server name, the hostname (or IP address), and port of the Management Server, and select a default path for recordings, as you do for a regular Recording Server.

Specify the Windows user account you want the Recording Server to run under. If the servers are running in a Workgroup environment, the Recording Server must run under a user with the same user name as the Management Server.

> **Note:** You cannot use a recording server also as a failover recording server. It can be only one or the other.

See also: 7C. Download and run the XProtect Recording Server installer from the Management Server

Additional resources:

- XProtect VMS Administrator manual > Install new XProtect components > Install a failover recording server through Download Manager

8D. Specify recording server encryption

If you enabled recording server communication encryption on the recording servers, you should enable it on the failover recording servers also.

If you did not enable recording server communication encryption on the recording servers, you should also not enable it on the failover recording servers.

See also: 7D. Specify recording server encryption

8E. Verify the server is running

The Failover Recording Server consists of two server services:

- Failover Server, which monitors the Recording Servers and controls the Failover Recording Server start and stop, as well as the transfer of recordings back to the Recording Server once it recovers from a failover situation.
- Failover Recording Server, which takes over recording and streaming duties for a failed Recording Server.

Verify the XProtect Failover Server notification area tray icon shows the Failover Server has started correctly (i.e., the icon status is green).

Note that, since the Failover Recording Server is not active at this time, the XProtect Recording Server tray icon will indicate the Recording Server itself is not running.

Verify the Windows Firewall (if enabled) allows inbound access to all ports used by the Recording Server.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Failover servers > Failover recording server services (explained)
- XProtect VMS Administrator manual > Managing server services > Server manager tray icons (explained)
- XProtect VMS Administrator manual > Ports used by the system

8F. Install a different device pack

After the installation completes, you can install a different device pack, if necessary.

If the legacy device pack is installed on any recording server that will be associated with the failover server, you must also install it on the failover server.

For simplicity and ease of troubleshooting, Milestone recommends you always use the same device pack on all recording and Failover Recording Servers.

See also: 7A. Prepare for installation

8G. Add anti-virus scan exceptions

If you run an anti-virus solution on the server, and if you have not already done so, you must add the recommended exceptions to the real-time and disk scanning routines in order not to impact system performance.

See also:3J. Add anti-virus scan exceptions

9. Install XProtect Management Clients

9A. Prepare for installation

The XProtect Management Client is used by system administrators to manage the XProtect VMS. It is typically installed on the system administrator's workstation and is usually also installed on the Management Server itself to allow for local management (this is a default option in the installer).

Make sure the workstation(s) meet(s) the requirements of the Management Client in regard to Windows version, .Net version, and DirectX version.

Additional resources:

- Milestone product system requirements - milestonesys.com
- XProtect VMS Administrator manual > Management Client (explained)

9B. Import certificates on Management Client workstations

If you are manually distributing certificates, you must ensure the CA is trusted before proceeding.

See also: 3A. Obtain or create server communication encryption certificates, 7D. Specify recording server encryption

9C. Download and run the Management Client software from the Management Server

Download and run the Management Client installer on the workstation(s) you or the customer will be using for managing the XProtect VMS.

The XProtect Management Client installation file is available on the Management Server administrative installation page: http://<management server>/installation/admin

Note: If you have a newer version of the XProtect Management Client installed—for example, on your service laptop—it will usually work with older versions of the Management Server as well. If you have an older version installed, you will usually be prompted to upgrade before you can log into the system.

Note: Beginning with version 2017R1, the XProtect Mobile server plug-in is automatically installed with the Management Client installer, eliminating the need to do this step separately.

Configuring and Organizing

10. Configure global settings and behaviors

10A. Log in with the Management Client

With the Management Server installed, you can log in with the XProtect Management Client.

Windows Authentication and Windows Authentication (current user)

By default, only Windows users that are members of the Windows User Management Administrators user group on the server running the Management Server service are able to log into the XProtect VMS. To ensure you are never left with a system you cannot log into, this setting cannot be changed. You will typically want to make sure you limit this access as much as possible.

You can log in either with the Management Client installed on the server or one installed elsewhere, typically your normal workstation or laptop.

If you are already logged into Windows with credentials that meet the requirements described above, you can use the Windows Authentication (current user) option. Otherwise, you must choose Windows Authentication and specify those credentials. If you are not working directly on the management server, you may need to prefix the username with the hostname (or domain name) of the management server.

Common reasons why login fails:

- The time difference between the workstation and the management server is more than 5 minutes.
- The time zone settings are not correct on either the workstation or the server.
- The management server hostname does not resolve correctly from the workstation.
- The user is not a member of the Administrators group on the management server.
- You need to prefix the username with the server hostname (or domain name).
- A firewall on the management server is blocking access.
- The Management Server service is not started.
- The password is not correct.

10B. Basic authentication

The third login option available in the Management Client, Basic Authentication, is not relevant unless you configure a Basic user and assign it to a role with sufficient permissions.

Additional resources:

- XProtect VMS Administrator manual > Navigating the Management Client > Login overview

10C. Configure Management Client behavior

You can customize some Management Client behaviors on the Tools > Options > General tab.

Among these behaviors are your preferred number of log rows shown per page, the default preview frame rate, and maximum number of cameras in the preview pane. If you are managing the system remotely on a connection with limited bandwidth, Milestone recommends you adjust or disable the preview settings to prevent overloading the connection when the preview window is active.

You can also choose which select features should be enabled automatically when adding new cameras to the server, as well as changing the language of the Management Client interface.

It is a good idea to consider whether you need to change any of these settings before you proceed with configuring the server.

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system
- XProtect VMS Administrator manual > Setting options for the system > General tab (options)
- eLearning: Getting Started with XProtect VMS

10D. Configure Recording Server timeout settings

On the Tools > Options > General tab you can specify several general behaviors for all Recording Servers connected to this Management Server.

PTZ timeout settings

If you will be using PTZ cameras in the system, you can specify your preferred default PTZ timeout settings. These settings will apply unless you explicitly specify something else under the device properties for a specific PTZ camera.

> **Note:** The XProtect VMS will resume control of the PTZ camera from the user at the end of the timeout, which may not always be what the user expects. Milestone recommends the timeout values be determined in cooperation with the daily users to best set and meet their expectations.

Hardware device communication timeout settings

If some of your hardware devices (such as cameras) are located remotely from the Recording Server they are installed on, you may get an excessive number of communication timeout error messages due to the increased latency. To counter this, you can specify how long a communication error may exist before the system logs it as an error and triggers the Communication Error event.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Recording servers (explained)

10E. Configure Log Server settings

The Management Server has three main logs which are available through the Management Client interface.

You should verify the retention and logging level for each of the logs match what is required for the system on the Tools > Options > Server Logs tab.

> **Note:** User access logging is not enabled by default; you must enable it here if you need the system to log any operator user action other than login date, time, and IP address.

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system > Server Logs tab (options)

10F. Configure email notification settings

Milestone recommends configuring a number of rules to alert the system administrator by email when a server or hardware device error event occurs. Before you can do this, you must configure the mail server settings on the Tools > Options > Mail Server tab.

If you want to generate and attach AVI video clips to an email, you must also select which AVI codec the server should use for this on the Tools –> Options –> AVI Generation tab. Any codec you install on the Management Server will be available in the list.

By getting these settings taken care of at this time, you avoid getting interrupted when you make the actual email rules later on.

See also: 2020C. Create notification profiles

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system > Mail Server tab (options)
- XProtect VMS Administrator manual > Setting options for the system > AVI Generation tab (options)

10G. Verify bookmark default behavior

Users can use bookmarks to mark incidents in live or recorded video. When a user bookmarks an incident, the server automatically assigns it an ID and marks what user created it.

A bookmark video clip typically contains video from a few seconds before and a few seconds after the bookmarked incident to ensure that the incident is recorded, regardless of any delays. Bookmarks are searchable, so any user can easily find them later.

You should verify the default bookmark settings match your preferences for the installation. You do this on the Tools > Options > Bookmark tab.

Note: Bookmarks are not supported in all product versions.

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system > Bookmark tab (options)
- XProtect Smart Client User Manual > Bookmarks (configuration)

10H. Create Evidence Lock profiles

The evidence lock functionality allows users to protect video sequences from being deleted—for example, while an investigation or trial is ongoing. This protection also covers audio and other data from devices related to the selected cameras.

Once an evidence lock is in place, the system protects the data from being deleted. This means that users cannot delete the data until a user with sufficient user rights unlocks the evidence or the evidence lock expires based on the configured retention time.

User roles are assigned an evidence lock profile that contains one or more locking intervals, as appropriate for that user role. If you will be allowing users to create evidence locks, you must define the evidence lock profiles you will be assigning to the user roles on the Tools > Options > Evidence Lock tab.

Note: Evidence locks are not supported in all product versions.

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system > Evidence Lock tab (options)
- XProtect Smart Client User Manual > Evidence locks

10I. Add Audio Messages

Audio messages are typically short, but may also be longer, messages broadcast to one or more speakers connected to a hardware device, such as a camera, encoder, or audio-only IP device, triggered by rules.

If you will be using audio messages, you must upload the audio files on the Tools > Options > Audio Messages tab. Multiple file formats are supported.

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system > Audio messages tab (options)

10J. Configure Customer Dashboard connectivity

Enable access to the Customer Dashboard as required on the Tools > Options > Customer Dashboard tab.

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system > Customer Dashboard tab (options)
- Customer Dashboard - milestonesys.com

10K. Configure alarm and event settings

The alarms feature in the XProtect VMS provides the user with a central overview, control, and scalability of alarms.

If you will be using alarms, you should verify the default alarm retention times configured on the Tools > Options > Alarms and Events tab meet your system requirements.

Events used for alarms and rules are handled by the Event Server service that is typically installed on the management server.

Once an event has triggered the alarm or rule, it has usually outlived its purpose and, for that reason, is not stored or is stored for only a short time, by default. If, for any reason, you need to change if or how long one or more event types is stored, you can do so on the Tools > Options > Alarms and Events tab.

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system > Alarms and Events tab (options)
- XProtect Smart Client User Manual > Alarms and Events (configuration)

10L. Generic Event settings

Generic events allow you to trigger actions in the XProtect Event Server by sending simple strings via the IP network to your system. In this way, you may integrate the XProtect VMS with external sources, such as access control systems and alarm systems without a dedicated integration.

To avoid jeopardizing security, the Generic Event function is disabled by default and, when enabled, accepts only events originating on the management server itself (localhost) or explicitly specified IPv4 or IPv6 addresses.

If you will be using Generic Events, you must enable and configure the data source parameters, including the receiving port and allowed protocols and external sender IP addresses, on the Tools > Options > Generic Events tab.

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system > Generic Events tab (options)

11. Verify license and site information

11A. Review license information

Because the software license file determines what product you have installed, you should verify it matches what you expected.

You should also verify that the Milestone Care information is correct and that the license overview lists the expected number of hardware devices and Milestone Interconnect camera channels.

If what is shown under license information does not correspond to what was ordered, you must activate the license in order to update it with the latest information from the Milestone license server before contacting Milestone Partner Service and Sales Support.

Additional resources:

- XProtect VMS Administrator manual > Licenses (explained)
- XProtect VMS Administrator manual > Site Navigation: Basics > License Information

11B. Activate license

If what is listed under the Basics > License Information node doesn't match what you expect, you can update the XProtect VMS with the latest license information at this stage.

For easy maintenance and flexibility, if the management server has permanent access to the internet, Milestone recommends enabling automatic license activation so the server will always automatically activate and update the license whenever you add, remove, or replace any hardware device.

See also: 11A. Review license information

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Basics > License Information > Automatic license activation (explained)
- XProtect VMS Administrator manual > Site Navigation: Basics > License Information > Activate licenses online
- XProtect VMS Activate Licenses Quick Guide
- Register software license codes (SLCs) in Milestone Customer Dashboard - Quick guide

11C. Enter and verify the site information

You should enter the main site location, system administrator details, and any additional site information on the Basics > Site Information node as early as possible. Doing this allows all administrators working with the system to have full transparency into the current server hardware locations and contact persons.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Basics > Site information

12. Configure Recording Servers and Failover Recording Servers

12A. Define failover servers

If you installed any Failover Recording Servers, you should see them in the Management Client Servers > Failover Servers node. You can review the server information, including the recording storage location, on the Info tab.

Make sure the name of the server is one that makes sense and add a description of the location, intended use of the server, and anything else that may be useful when servicing the system months or years from now.

If you will use one or more Failover Servers as cold standby servers, you must create a failover server group and assign the Failover Servers you want to be part of that failover group. You must also determine the failover sequence (priority) before you can assign the failover group to the appropriate Recording Servers. Generally, the most efficient approach is to configure this before configuring the Recording Servers.

See also: 8. Install XProtect Failover Recording Servers, 12E. Assign Failover Servers to Recording Servers

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Failover servers > Failover recording server (explained)
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Failover servers > Failover steps (explained)
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Failover servers > Failover recording server functionality (explained)
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Failover servers > Group failover recording servers for cold standby

12B. Review and update recording server information

You can review the server information of each Recording Server you have installed on the Info tab when selecting the Recording Server in the Servers > Recording Servers node.

Make sure the name of the server is one that makes sense and add a description of the location, intended use of the server, and anything else that may be useful when servicing the system months or years from now.

See also: 7. Install XProtect Recording Servers

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Recording servers (explained)
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Info tab (recording server)

12C. Configure Recording Server storage settings

Select a Recording Server in the Servers > Recording Servers node and open the Storage tab to configure the storage settings.

In many cases, you can just edit the default storage to meet the specific requirements for the system. In other cases, you will need to create multiple different storage configurations to meet the different retention requirements of specific camera, microphone, speaker, and metadata groups.

Storage name and path

For ease of service, make sure your storage name describes the function of the storage as closely as possible.

Verify the recording path is correct. The path must refer to a disk system that is directly and permanently attached to the recording server (i.e., not, for example, a network or USB drive). Milestone also recommends that you do not assign a storage area to the physical disks used by the operating system but use a dedicated storage system to get the best performance.

You must make sure the disk system is formatted per Milestone recommendations and that any anti-virus scanning meets the Milestone recommendations (see references below).

Storage retention, signing, and encryption

Specify both the retention time and the maximum size you allow this storage to use on the disk.

With the exception of recordings that are protected by an Evidence Lock, whenever the configured retention time OR the maximum size is reached, the Recording Server will delete the oldest recording (first-in-first-out) or force an archiving if an archive exists (see the next step).

You can apply database signing and/or encryption if required by the system specification.

> **Note:** Not all XProtect VMS versions include database signing and encryption functionality.

See also: 3J. Add anti-virus scan exceptions, 4. Configure storage, 10H. Create Evidence Lock profiles, 12D. Configure archiving

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage tab (recording server)
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage tab (recording server) > Storage and Recording Settings properties
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage tab (recording server) > Add a new storage
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage tab (recording server) > Edit settings for a selected storage or archive
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage tab (recording server) > Enable digital signing for export

12D. Configure archiving

When you add an archive to a storage area, the recordings in that storage are automatically moved to an archive storage at intervals that you define. You can configure multiple archives for each storage (not supported in all product versions).

Archives are typically located on an external storage system but may also be located on the recording server hardware itself.

> Note: Milestone recommends you use archiving only if you need to physically move recordings to a different storage location for long-term storage or if the system requirements require grooming older recordings to save disk space.
>
> On larger systems, an ungraceful shutdown may, however, result in a prolonged recovery time as the Recording Server verifies and repairs the database.
>
> An ungraceful shutdown is any condition that prevents the Recording Server service from closing the database correctly. Typical examples are loss of power to a server not protected by a UPS, or forcefully killing the Recording Server service via the Windows Task Manager. Other examples include loss of communication with the disk system due to improper design (writing directly to a NAS) or due to hardware failure (for example, a disk controller failing).
>
> Upon restarting the server, the Recording Server service checks the integrity of each camera database and will initiate a repair routine if necessary. This usually takes only a few minutes, but in cases where the damage is so severe the database index has to be rebuilt, this can potentially take a long time. The risk of this, though small, can be minimized by using archiving to keep the database relatively small. Archiving once a day is typically sufficient for this purpose.

Archive name, path, and retention

When you add an archive to a storage configuration, you will need to specify the drive and path, retention time, and maximum size on disk, just as for the recording storage itself.

The archive path can be a UNC path pointing to a network storage. If you use network storage, you must make sure the user account running the Recording Server service has full permissions on that path.

An archive must always have a longer retention time than the recording storage itself. If you have multiple archives for the storage, each subsequent archive must have a longer retention time than the previous archive.

All retention times are accumulative—for example, if the storage retention is 7 days, the first archive is 30 days, and the second archive is 12 months. This is also how the data will be stored on the respective storage systems (paths).

Archive frequency

You must specify when the system should run the archive routine. Archiving can occur as frequently as you require, with a minimum of one hour between archiving.

Whenever an archive runs, only the data older than that specified for the storage or previous archive will be moved. You should therefore make sure that the storage or archive you will be archiving from has sufficient room to store the data stored within its specified retention time plus the data stored during the archive interval.

Archiving moves the data sequentially for one device at a time to achieve optimum performance from both the source and destination disk systems.

Archive grooming

Grooming allows you to remove video frames from the recordings when moving data onto an archive, thus allowing more data to be stored longer than if the full recording was archived.

The effective grooming result depends on the recording format. Recordings made in a frame-based codec format (such as MJPEG) can be groomed to any frame rate, while recordings made in a streaming codec format (such as MPEG4, H.264, and H.265) will be groomed to the nearest lower keyframe (I-frame).

> **Note:** Not all XProtect VMS versions include grooming functionality.

See also: 3J. Add anti-virus scan exceptions, 4. Configure storage, 7C. Download and run the XProtect Recording Server installer from the Management Server, 12C. Configure Recording Server storage settings

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage and archiving (explained)
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage tab (recording server) > Create an archive within a storage
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage tab (recording server) > Archive structure (explained)
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage tab (recording server) > Archive settings properties
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Storage tab (recording server) > Back up archived recordings

12E. Assign Failover Servers to Recording Servers

Select a Recording Server in the Servers > Recording Servers node and open the Failover tab to assign a Failover Server or failover server group to the Recording Server.

If you will be assigning a hot standby failover server to the Recording Server, simply select the Failover Server you want to assign to the Recording Server.

Cold standby failover servers are assigned by failover groups that can be added to multiple Recording Servers. Assuming you have already created the failover groups and assigned the Failover Recording Servers to the intended groups (see references below), you can now assign a primary failover server group and, optionally, also a secondary failover server group to the Recording Server.

If the system requirements state that not all cameras on the Recording Server should be part of the failover, you can specify which cameras to include in the advanced failover settings window.

See also: 12A. Define failover servers

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Recording servers > Failover tab (recording server)

12F. Enable certificates

Import any certificates that are still missing.

Verify all server communication encryption is enabled as required by the system design document.

Test connectivity for all servers and clients where encryption settings were changed.

> Note: Delaying enabling certificates beyond this point may cause the installation to not be in compliance with local data privacy laws and regulations.

See also: "3A. Obtain or create server communication encryption certificates" on page 27."5B. Import certificates on the management server" on page 36, "5E. Specify server encryption" on page 38, "7B. Import certificates on recording servers" on page 42, "7D. Specify recording server encryption" on page 44, "8B. Import certificates on failover recording servers" on page 46, "6B. Import certificates on mobile servers" on page 39, "6D. Specify mobile server encryption" on page 40

13. Add hardware devices

13A. Add and name hardware devices

IP hardware devices

In most cases, IP cameras, and possibly IP encoders, are the only hardware devices you will be adding to a Recording Server. Depending on how those devices are supported, they will use either a dedicated driver or the ONVIF driver.

Before installing, you should verify how the devices are supported and what firmware versions the driver supports. You can do this on the Milestone website: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

You can add devices by either IP address or hostname. If you will be adding the device by hostname, you must use the manual option.

After the hardware device has been detected, you have the option to select which functions you want to enable and to name both the hardware device and those device functions. Naming the device functions already at this point may be an advantage, especially if you are adding only a few devices or will be enabling audio or I/O functions, because you won't need to get back to it and work it out later.

The process is the same if you will be adding an IP I/O or audio-only device.

Each hardware device you add will consume one hardware device license.

DirectShow device

If you will be adding a DirectShow device—for example, to play back pre-recorded video clips as part of a demo system or to record video through a webcam driver—you should follow the instructions in KB00001020. You must use the manual detection option and explicitly specify using the DirectShowDriver in the hardware model dropdown list.

From there, the installation process and licensing are the same as for a physical hardware device. Once the DirectShow device has been added, you can specify the .AVI video file path, or webcam device or path, under the Settings tab.

Note that you can add only one DirectShow device to an XProtect VMS Recording Server, giving you up to eight video and audio channels.

Screen Recorders

XProtect Screen Recorder is a function that enables Milestone video management software (VMS) to inconspicuously capture screen recordings of any Microsoft® Windows-based PC or point-of-sale (POS) terminal. XProtect Screen Recorder is easily installed on computers that you want to monitor and recordings are fully synchronized with other video data.

Captured screen recordings are managed in the same way as video camera data in the software. Camera recordings can be viewed in live and playback mode and exported for evidence.

You can download the XProtect Screen Recorder software and manual from the Milestone website.

After the XProtect Screen Recorder is installed and configured on the PC you want to record, you can install the Screen Recorder driver on the Recording Server.

You must use the manual detection option and explicitly specify using the Screen Recorder driver in the hardware model dropdown list. Also remember to specify the correct password (leave the username blank) and the IP port. The default is port 52111.

From there, the installation process and licensing are the same as for a physical hardware device.

See also: 2C. Verify firmware version with Milestone Supported Devices list,2A. Set a static IP address or configure DHCP and hostname, 14A. Name hardware devices

Additional resources:

- Knowledge base article 000001020: Set up DirectShow Driver
- XProtect Screen Recorder - milestonesys.com
- XProtect Screen Recorder Administrator's Manual

13B. Disable all unused encoder video channels

If you are installing a multi-channel encoder or a DirectShow device, you should disable all the video channels you will not be using to prevent them showing up and causing unnecessary confusion in both the Management Client and operator client interfaces.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Enable/disable devices via device groups

14. Name and group devices

14A. Name hardware devices

The name of the hardware device itself is used only by system administrators in the Management Client. To make device management as easy as possible, the name should ideally reflect key information about the device, such as the make and model, IP address or hostname, and the location of the device.

You can add additional information under the description on the Info tab. This could include more details regarding precisely where the hardware device is located, who to contact for access, or information about warranty and servicing.

See also: 13A. Add and name hardware devices

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Hardware > Manage hardware

14B. Name cameras

Camera devices deliver video streams to the system that the client users can use to view live video or that the system can record for later playback by the client users. The camera name is visible both to system administrators in the Management Client and to all users who are permitted to access and view the camera.

To make the system as easy to use as possible, the camera name should ideally describe what the camera "is looking at" as precisely and as briefly as possible. If the camera has special capabilities, such as PTZ functionality, panoramic view, or thermal imaging, it is generally helpful for the user if such capabilities are also indicated within the camera name itself.

Because users and system administrators will be accessing and using cameras from the various client applications the exact same way regardless of make, model, and IP address, it is recommended not to include such information in the camera name.

Also, because it is usually obvious to a user when they are working with a camera, including the word "camera" in the camera name is often redundant and makes the name longer than needed. So in most cases, "camera" can be omitted to make the name shorter and easier to read.

Some examples of "good" camera names:

- Reception desk
- Reception entrance
- Reception elevator access
- Front entrance 180
- Front parking lot PTZ
- Market St. warehouse NW perimeter (thermal)

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Camera devices (explained)
- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Info tab (devices)

14C. Name microphones and speakers

Microphone devices deliver live audio streams to the system that the client users can listen to.

Speaker devices receive an audio stream only when it is started by the system—typically when a user presses the talk button in XProtect Smart Client, or when playing back a prerecorded audio file.

Both the microphone and speaker audio may be recorded for later playback.

The microphone and speaker names are visible both to system administrators in the Management Client and to all users who are permitted to access and use microphones and speakers.

To make the system as easy to use as possible, the microphone and speaker names should clearly and precisely communicate what the device is used for.

Because users and system administrators will be accessing and using cameras from the various client applications the exact same way regardless of make, model, and IP address, it is recommended not to include such information in the camera name. However, unlike most cameras, it may often be useful to include their functions ("speaker" or "mic") to mentally help keep those functions clear.

Some examples of "good" microphone and speaker names:

- Front entrance intercom mic
- Branch 32 teller windows 1-3 mic
- SAR-IF 149.080 MHz
- Front entrance intercom speaker

See also: 13. Add hardware devices

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Microphone devices (explained)
- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Speaker devices (explained)

14D. Name inputs and outputs

Input and output names are visible to system administrators in the Management Client, while outputs are also visible to users who are permitted to manually activate outputs.

Like microphones and speakers, good input and output names clearly and precisely communicate their uses.

Some examples of "good" input and output names:

- Duress Alarm
- Reception PIR
- Front entrance doorbell
- Front entrance door buzzer
- Main gate open

See also: 13. Add hardware devices

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Input devices (explained)
- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Output devices (explained)

14E. Name metadata channels

Metadata devices can deliver a data stream that, for example, describes the content or objects in the image (video analytics) or a GPS location. Metadata can be generated by the hardware device itself or by a third-party system or integration via a generic metadata driver.

Like microphones, speakers, inputs, and outputs, good metadata names clearly and precisely communicate their uses.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Metadata devices (explained)

14F. Disable unused devices

If not already done during the installation, any camera device (channel) on a multi-port encoder that is not used should be disabled. Likewise, all unused microphone, speaker, input, output, and metadata devices should be disabled (default setting).

See also: 13B. Disable all unused encoder video channels

14G. Create additional camera, microphone, speaker, input, output, and metadata device groups

Grouping of devices into device groups is part of the Add Hardware wizard but you can always modify the groups and add more groups, if needed. Each type of device (cameras, microphones, speakers, metadata, inputs, and outputs) has its own node under the Devices node.

Device groups can be used by system administrators for managing and changing settings on multiple devices at once, with rules and with roles (user permissions). They can also be used by Smart Client users when creating views or manually selecting a camera for viewing or sharing through the Smart Wall.

Thus, both system administrators and users can benefit from grouping devices into user-friendly categories—for example, based on location, function, or intended user access. Devices can exist in multiple groups and you can further organize them by creating subgroups and subgroups within subgroups.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with device groups

14H. Add devices to the relevant groups

After a device group is created, you can add devices to it.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with device groups > Specify which devices to include device group

15. Configure cameras

15A. Review and update device information

For each camera, microphone, speaker, input, output, and metadata device, you can add a short name and description in addition to the full name on the Info tab for each individual device (Devices > Cameras > Info tab).

The short name is useful if you use Smart Map in the Smart Client and you find the camera name is too long on the map. If you enter a short name, this will be displayed with the camera on the Smart Map instead of the full name, but with the full name still showing as a mouse-over tool tip.

The description allows you to add any details and notes that may be useful to you or other system administrators when servicing the system at a later date.

Add device positioning information

For camera devices you can enter GPS positioning coordinates, camera direction, field of view (FoV), and depth of field (distance from the camera lens to the center of focus). The XProtect VMS uses this information to place the camera on the Smart Map.

If a Smart Client user who has permissions to edit cameras and Smart Map adds or moves a camera, the new position will be reflected in the Management Client after a refresh.

You can verify the correct placement on Google Maps through the Preview button (requires internet access).

A camera is removed from a Smart Map only if it is disabled or deleted, or if the GPS coordinates are deleted in the Management Client. Smart Client users do not have permission to remove cameras from a Smart Map.

> **Note:** Not all XProtect VMS versions include Smart Map functionality.

See also: 13A. Add and name hardware devices

Additional resources:

- Milestone XProtect VMS Products - Administrator manual > Info tab (devices)
- eLearning: Adding Cameras and Device Groups in XProtect VMS Products
- eLearning: Configuring and Using XProtect Smart Map

15B. Configure general camera settings

Set up the general image settings for a camera or a camera group on the Devices > Cameras > Settings tab as required by the project documentation.

The general settings typically include image-related settings such as brightness, contrast, saturation, image rotation, auto iris, day/night mode, and shutter speed. On some devices, it may also include date and time stamp overlay settings and other settings that are common for all streams from the hardware device.

Selecting a group allows you to change settings all at once on all the cameras in that group and any subgroups. As most settings are hardware device driver specific, you can filter the group by hardware device in the dropdown list at the top of the Properties window.

> Note: There is no memory associated with a device group; it is simply a way to easily select a large group of devices. If the devices in the group currently have different values configured for a specific setting, the value field is shown as blank.

> Note: The ability to change some device properties—for example, resolution, rotation, brightness, and similar image settings—is limited to groups of 400 devices or less.

15C. Configure video streams

Configure the camera video stream(s) for a camera or a camera group on the Devices > Cameras > Settings tab as required by the project documentation.

The video stream settings typically include resolution, frame rate, codec, and streaming mode such as RTP/RTSP/TCP, HTTP streaming, RTP/UDP, RTP/UDP multicast, etc.

Many cameras and encoders support setting up multiple streams to use for different purposes. The XProtect Smart Client supports adaptive streaming which, if multiple live streams are available, allows the software to automatically request the live stream that is most optimal for a given view size and screen resolution.

EXAMPLE - Megapixel resolution:

When using megapixel resolutions in systems where the XProtect Smart Client is used to view the live stream from cameras, Milestone recommends defining one or more streams with a lower resolution—but typically the same codec, frame rate and streaming mode—if the camera supports this and the network bandwidth is available. Doing this will allow the Smart Client to automatically select the most optimal stream to display live for a given view and screen resolution.

EXAMPLE - Higher video quality for recorded video:

It may in some cases be desirable to record video in a higher resolution, a less compressed format (different codec), and/or different (often lower) frame rate than that used for live viewing. As this may greatly affect the amount of data recorded, this should be configured only if the project documentation specifies this or you can otherwise determine that the storage is dimensioned to accommodate this.

EXAMPLE - Lower latency video for PTZ cameras:

If operators will be manually controlling PTZ cameras, it may be desirable to use MJPEG compression for the live view stream(s) to lower the encoding and decoding latency. Depending on the maximum resolution of the monitors used on the Smart Client workstations, you may also be able to use a lower resolution for the live streams without it being visible to the operator.

Note: Not all XProtect VMS versions support multiple live streams to Smart Clients.

Video stream keyframe interval

Specify the keyframe interval or GOP (Group of Pictures) length for the stream or streams for each camera or group of cameras if relevant, and if the setting is available.

Milestone recommends using a GOP length of one second for most situations, but other configurations may be desirable for specific situations such as if you need more frequent keyframes for motion detection or have set up grooming for the archive (if supported) and need to ensure you have a certain number of keyframes per second available to meet the grooming specification.

Milestone discourages using very long keyframe intervals for both performance and evidence integrity reasons:

- The XProtect Smart Client requires a keyframe to start showing video, so a longer GOP may prolong the time before the video is displayed when changing views.
- The XProtect Smart Client needs to decode the entire GOP before showing the last frame when playing back video in reverse, so a longer keyframe interval may result in a sluggish playback performance.
- If the networks experience a packet drop, this will result in all video within the GOP being dropped, so a longer keyframe interval may result in evidence not being recorded. This will be especially pronounced if using a UDP streaming mode and the connection to the camera is poor.

Video stream bitrate control, priority, and limits

Verify and adjust bitrate controls, priorities, and limits for the stream or streams you need for each camera or group of cameras, if relevant, and if the setting is available.

Examples of bitrate control settings include fixed or variable bitrate, frame rate or image quality priority, target bitrate, and maximum bitrate.

See also: 15D. Configure streams

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Settings tab (devices)
- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Streams tab (devices) > Multi-streaming (explained)

15D. Configure streams

Add (or remove) and select the streams (defined under the Settings tab) you want to use for each camera or group of cameras on the Devices > Cameras > Streams tab. Cameras must be the same make and model within the group for the settings to be available.

Name video streams

You should name each video stream according to its intended use for later reference and to assist operators in selecting the correct live stream in the Smart Client.

Select video stream mode and options

Select the Live Mode and select which stream to use as the default live stream in clients and which stream the Recording Server should record. The recording stream is also the stream the Recording Server will use for software video motion detection (VMD).

> **Note:** Streams selected as default stream or recording stream will always be streaming (rules permitting) regardless of what Live Mode you select for that stream.

> **Note**: Setting the live mode of streams not selected as default or recording stream to "when needed" may save bandwidth as the stream is started only when actively viewed in the XProtect Smart Client. You must, however, make sure there is always sufficient bandwidth for all streams to run simultaneously to avoid dropped frames in those situations.

> **Note**: The default stream is always used by the XProtect Mobile server which transcodes (downscales and re-encodes in MJPEG) it. If you have multiple streams configured, you can often save processing power on the Mobile server by selecting a lower resolution stream without affecting the quality viewed on the XProtect Mobile client.

> **Note:** Not all XProtect VMS versions support multiple live streams to Smart Clients.

See also: 15B. Configure general camera settings , 15C. Configure video streams, 25D. Configure performance settings

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Streams tab (devices)
- eLearning: Improving XProtect Advanced performance with Multi-streaming

15E. Configure recording

Configure recording settings on the Devices > Cameras > Record tab for each camera or group of cameras.

Verify and adjust recording settings

Select recording settings, including the pre-buffer you want to have available for the camera device(s), and the recording frame rate you want to use as default.

The default pre-buffer is 3 seconds, stored in RAM (memory option).

> **Note:** The memory option uses very little RAM, even for a large number of cameras, but that you are limited to a maximum of 15 seconds for pre-buffer when using this option.

> **Note:** That selecting the disk option, depending on the recording rules you define later, may place an additional load and wear on the storage system because the pre-buffer is repeatedly written and deleted from the disk if it is not to be recorded (for example, if there was no motion).

> **Note:** If you are using other functions on the hardware device the camera is associated with and you want to define different recording rules for those, you must clear the Record on related devices check box under this tab.

Select recording storage

If you need to use a different storage for the selected camera device or camera device group, select this storage (defined previously) using the Select button.

See also: 12C. Configure Recording Server storage settings

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Record tab (devices)

15F. Configure 360° lens settings

In you are using an ImmerVision Enables® Panomorph 360° lens, you must configure it on the Devices > Cameras > Fisheye Lens tab for the Smart Client to correctly dewarp the image.

If you are using a different 360° lens, your camera manufacturer may have a Smart Client plug-in available you can install on the client workstation to enable the Smart Client to dewarp that image correctly.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices tabs > fisheye lens tab (devices)

15G. Configure privacy masking

Configure any camera privacy masks needed on the Devices > Cameras > Privacy Mask tab.

Privacy masks are overlaid on all video (live and playback).

> **Note:** The privacy mask behavior has recently changed:

> Versions 2017R3 and older have only one solid (black) privacy mask. If you change the privacy mask, the mask will change for all video, regardless of when it was recorded.
>
> Versions 2018R1 and newer have two privacy mask options, and either may be solid (gray) or blurred. The liftable mask may be removed by authorized users whereas the permanent mask may not. If you change a privacy mask, the change will NOT affect to already recorded video.

Permissions to lift the privacy mask are global for a role and are set under Roles > Overall Security > Cameras.

If you upgrade from 2017R3 or older to 2018R1 and newer, existing privacy masks will be converted to liftable masks.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Privacy masking tab (devices)

15H. Configure software Motion Detection

If you will be using software video motion detection (VMD) for triggering recording rules (or any other rules) or alarms, or want to enable users to search in-motion metadata through the Smart Client Sequence Explorer, you must configure motion detection for each camera on the Devices > Cameras > Motion tab.

If you will not be using software VMD, you may disable it to save server resources.

> **Note:** The preview image switches from the default live stream to the stream designated as the recording stream (if it is not the same stream) when you select the motion detection tab.

Verify motion detection and hardware acceleration options

Verify motion detection (VMD) is enabled (default setting)/disabled as desired for each camera or group of cameras.

If the server has one or more NVIDIA graphics cards and/or supports Intel Quick Sync, the Recording Server will use the graphics processing units (GPUs) for VMD when set to automatic (default setting). This will reduce the CPU load on the recording server during video motion analysis and improve the general performance of the recording server.

Since hardware acceleration is subject to the actual server and NVIDIA graphics card hardware and BIOS configuration, you should verify that each recording server is, in fact, using hardware acceleration as intended by verifying the CPU and GPU load on each recording server.

You can view the GPU load through the XProtect VMS System Monitor, Windows Task Manager or by using a third-party tool such as GPU-z.

Configure exclusion regions

Enable exclude regions and configure any area you prefer to except from VMD on each camera.

Areas covered by a permanent privacy masking are automatically exempted from VMD.

Select image processing, detection resolution and keyframe processing settings

By default, to save CPU/GPU power, video streams and Images are processed only every 500 mS for VMD purposes. You should adjust this if the specific application requires a more frequent processing rate, or can function with a less frequent rate.

Also, by default the Recording Server decodes only keyframes on streaming video formats (MPEG4/H.264/H.265) for VMD purposes. This means if you have a keyframe interval/GOP length of one second, the server will process only that one image per second even if you specify a more frequent processing interval on the Process image every (msec) dropdown list.

To further save CPU/GPU processing power, the Recording Server VMD, by default, processes only 12% of the pixels in the image. In some cases, particularly if you need to detect very minor changes in the image, you may need to increase the percentage of pixels used for VMD.

Verify and adjust settings as desired for each camera as needed.

> Note: Detecting motion more frequently and/or decoding the full stream (not only keyframes) for VMD will increase the GPU and/or CPU load on the recording server. Make sure the server hardware is specified to support this.

> Note: If the camera is configured to use a Smart Codec that dynamically adjusts the GOP, Milestone recommends using the full stream (not only keyframes) for VMD to ensure the Recording Server processes images frequently enough to provide reliable motion detection.

Determine motion detection sensitivity settings

By default, the motion sensitivity (i.e., how sensitive each pixel is to changes) is adjusted dynamically for each camera by an algorithm. This allows the sensitivity to change depending on the conditions—for example, between night and day, sun or rain, etc.

In some cases, if you are having difficulties getting reliable motion detection (i.e., too little or too much motion detected) at specific, critical conditions, it might be desirable to set a fixed level manually.

Adjust motion detection threshold

The motion detection threshold determines how many pixels must be above the motion sensitivity level before the Recording Server should regard it as a positive detection of motion.

Adjust the VMD threshold for each camera to the point where the number of false detections is at a minimum while actual motion is reliably detected.

See also: 15C. Configure video streams, 31A. Perform a walk test for all cameras with motion detection

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Motion tab (devices)
- XProtect Smart Client - Hardware acceleration guide
- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Motion tab (devices) > Hardware acceleration (explained)
- Intel Quick Sync Video and Milestone White Paper
- Product Update: Changing the industry with hardware accelerated decoding
- TechPowerUp GPU-Z - techpowerup.com

15I. Configure camera events

In addition to the events generated by the XProtect VMS, you can configure most hardware to trigger events on specific conditions. If you will be using events generated by the hardware device, you must add those events for each camera on the Devices > Cameras > Events tab.

Only events you have added to the configured events list will be available to use for rules and alarms.

Examples of camera-related hardware device events (alarms):

- Motion started (HW)
- Motion stopped (HW)
- Video loss
- Video resumed
- Tampering
- Scene change
- Temperature above range
- Temperature below range
- Temperature inside range
- SD card event started
- SD card event stopped
- Video analytics event started
- Video analytics event stopped
- Tripwire

- Illegal access
- Auto tracker event started
- Auto tracker event stopped
- Object removal event started
- Object removal event stopped

Refer to the supported devices list on the Milestone website for specific information on which events are supported by/for your specific hardware device.

> **Note:** Hardware device audio, I/O, and metadata events are not part of the camera-related hardware events but can be configured under their respective device groups.

See also: 16D. Configure microphone events, 17. Configure inputs and outputs, 21. Create rules

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices tab > Events tab (devices)
- Find hardware for XProtect® and Milestone Husky™ - milestonesys.com

15J. Configure PTZ presets

If the installation includes pan/tilt/zoom (PTZ) cameras and you will be creating rules to move the cameras to specific positions when a specific condition is met (or users will be using presets to manually move the camera to a specific position), you must create presets for each camera on the Devices > Cameras > Presets tab.

Create or import PTZ presets

You may have the option to either use the presets from the device (i.e., import the presets that are configured on the hardware device to the XProtect VMS) or to configure the presets directly on the Presets tab. On some hardware devices, you may have only one of these options available.

> **Note:** Users with sufficient permissions may also manage (create, edit, and delete) presets from the Smart Client.

Select default preset

An easy way to ensure a PTZ camera is not left in a useless position is to select a default preset and enable the Default Goto Preset when PTZ is done rule (the rule is disabled by default).

Adjust device-specific PTZ timeout settings

Verify the PTZ timeout settings and adjust as necessary for each PTZ camera.

See also: 10D. Configure Recording Server timeout settings > Verify PTZ session timeouts

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Presets tab (devices)

15K. Configure PTZ patrolling

Patrolling profiles are the definitions of how patrolling should take place. This includes the order in which the camera should move between preset positions and how long it should remain at each position.

Patrolling profiles may be started, paused, and stopped by rules or by users with adequate permissions.

Create PTZ Patrolling profiles

Create patrolling profiles for each PTZ camera as required by the system design requirements.

Configure preset order and time on position

Add presets, set the preset order, and specify the time on position for each patrol profile.

Configure custom transitions timing

By default, the time required for moving the camera from one preset position to another (the transition) is set to three seconds. During this time, motion detection is by default disabled on the camera since it will otherwise trigger a motion detection event.

> **Note:** If you time a specific transition to be longer and you are/will be using software motion detection for rules or alarms (including recording on motion), you must adjust the expected time for that transition to avoid triggering the motion event. Remember to include the time the camera takes to zoom and focus when you time the transition.

On some PTZ devices you can also adjust the transition speed if you want the camera to move at a slower speed between two presets—for example, to make a slow pan over a wide area. The option to set the transition speed is not available if you use presets imported from the hardware device.

> **Note:** Since software motion detection is disabled during transitions you must create a rule to record always if you want the slow pan to be recorded.

Select whether to customize transitions and specify the speed of expected transition time for each transition as required by the system design requirements. Be mindful that a PTZ camera on a patrol is looking only at a limited FoV at any given time. More presets in the patrol profile means less time overall at each preset.

See also: 21. Create rules

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices tabs > Patrolling tab (devices)

16. Configure microphones and speakers

This section is relevant only if the installation uses microphones and/or speakers.

As with cameras, you can add technical details and notes specific to each microphone or speaker device on the Devices > Microphones > Info tab and Devices > Speakers > Info tab.

You can also add a short name for use with Smart Map.

See also: 15A. Review and update device information

Additional resources:

- Milestone XProtect VMS Products - Administrator manual > About microphone devices
- Milestone XProtect VMS Products - Administrator manual > About speaker devices

16A. Verify microphone settings

Verify the microphone settings for each microphone or microphone group on the Devices > Microphones > Settings tab and change them as needed.

Selecting a group allows you to change settings on all the cameras in the group and any subgroups at once. Because most settings are hardware device driver specific, you can filter the group by hardware device in the dropdown list at the top of the Properties window.

> **Note:** Some microphone devices may not have any settings, in which case the Properties window will be blank.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Microphone devices (explained)

16B. Verify and adjust microphone recording settings

Configure recording settings on the Devices > Microphones > Record tab for each microphone or group of microphones.

See also: 15E. Configure recording

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Microphone devices (explained)

16C. Select microphone recording storage

Verify and, if necessary, change the recording storage for each microphone or group of microphones on the Devices > Microphones > Record tab.

See also: 15E. Configure recording

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Microphone devices (explained)

16D. Configure microphone events

In addition to the events generated by the XProtect VMS, you can configure some hardware to trigger events on specific audio-related conditions. If you will be using audio events generated by the hardware device, you must add those events for each camera on the Devices > Microphone > Events tab.

Only events you have added to the configured events list will be available to use for rules and alarms.

Examples of camera-related hardware device events (alarms):

- Audio falling
- Audio rising
- Audio passing
- Scream detection falling
- Scream detection rising

Refer to the supported devices list on the Milestone website for specific information on which events are supported by/for your specific hardware device.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Microphone devices (explained)
- XProtect VMS Administrator manual > Site Navigation: Devices tab > Events tab (devices)

16E. Verify speaker settings

Verify the Speaker settings for each microphone or microphone group on the Devices > Speakers > Settings tab and change them as needed.

Selecting a group allows you to change settings on all the cameras in the group and any subgroups at the same time. As most settings are hardware device driver specific, you can filter the group by hardware device in the dropdown list at the top of the Properties window.

> **Note:** Some microphone devices may not have any settings, in which case the Properties window will be blank.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Speaker devices (explained)

16F. Verify and adjust speaker recording settings

Configure recording settings for each speaker or group of speakers on the Devices > Speakers > Record tab.

See also: 15E. Configure recording

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Speaker devices (explained)

16G. Select speaker recording storage

Verify and, if necessary, change the recording storage for each speaker or group of speakers on the Devices > Speakers > Record tab.

See also: 15E. Configure recording

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Speaker devices (explained)

17. Configure inputs and outputs

This section is relevant only if the installation uses hardware (contact closure/dry contact) inputs and/or outputs.

As with cameras, you can add technical details and notes specific to each input or output device on the Devices > Input > Info tab and Devices > Output > Info tab.

You can also add short names for use with Smart Map.

See also: 15A. Review and update device information

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Input devices (explained)
- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Output devices (explained)

17A. Verify input settings

Verify the input settings for each input or input group on the Devices > Input > Settings tab and change them as needed.

Selecting a group allows you to change settings on all the cameras in the group and any subgroups at the same time. As most settings are hardware device driver specific, you can filter the group by hardware device in the dropdown list at the top of the Properties window.

> **Note:** Some input devices may not have any settings, in which case the Properties window will be blank.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Input devices (explained)

17B. Configure input events

Add the input events you will use to the configured events list. Only events you have added to the configured events list will be available to use for rules and alarms.

Most devices have both an input falling event and an input rising event available. In that case, you must add both to properly test the input is working and enable the XProtect VMS to reliably trigger on either event.

Examples of input events:

- Input falling event
- Input rising event

- Input activated

Refer to the supported devices list on the Milestone website for specific information on if and how many inputs are supported by/for your specific hardware device.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Input devices (explained)
- XProtect VMS Administrator manual > Site Navigation: Devices tab > Events tab (devices)

17C. Verify output settings

Verify the output settings for each input or input group on the Devices > Output > Settings tab and change them as needed.

Selecting a group allows you to change settings on all the cameras in the group and any subgroups at the same time. As most settings are hardware device driver specific, you can filter the group by hardware device in the dropdown list at the top of the Properties window.

Most output devices allow you to define a trigger time (the duration the output is held active when triggered), but the time interval you can choose varies between devices. Some output devices have additional settings, such as defining if the active output state is “closed” or “open”.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Output devices (explained)

17D. Test inputs and outputs

Before testing the inputs and outputs in the XProtect VMS, you should verify they work correctly when viewed/activated directly on the device. Typically, this functionality is available through the hardware device configuration web page.

To test an input:

- Select the input to test under Devices > Input.
- Activate and deactivate the input on the physical device.
- Verify the green indicator in the preview pane turns on and off accordingly. Each activation and deactivation are also displayed in the box next to the indicator light.

To test an output:

- Select the output to test under Devices > Output.
- Activate and deactivate the output via the controls in the in the preview pane:
- Click the elongated button above the check box to activate the output for the duration specified in the Properties pane.
- Select the check box to keep the output activated until you clear the box.

Note: Depending on the installation, the physical output may be wired to something that may be dangerous to life or property if triggered at the wrong time (for example, a garage door), or may cause unintended inconvenience (for example, an input to an intrusion alarm or panic alarm bell).

Therefore: MAKE SURE THE OUTPUT IS SAFE TO ACTIVATE BEFORE TESTING IT.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Devices: Working with devices > Input devices (explained) > Activate input manually for test

18. Configure client settings

18A. Create custom View Groups

The XProtect VMS automatically creates a view group for each role. Create any additional view groups required by the project documentation under the Client > View Groups node.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Clients: View Groups > View groups and roles (explained)

18B. Configure Smart Client Profiles

Smart Client profiles allow system administrators to control how XProtect Smart Client should look and behave and what features and panes the XProtect Smart Client users in a specific role have access to.

A Smart Client Profile can be used by multiple roles so there is no need to create a profile for each role unless they will have access to different Smart Client menus and features.

Create Smart Client profile

Unless you create specific Smart Client profiles for system administrators, you will typically want to keep the default Smart Client profile unchanged for that use.

Create any additional Smart Client profiles you need to meet the system user permission requirements under the Client > Smart Client Profiles node.

Add a detailed description and any other useful information under the Info tab.

> **Note:** Some product versions may have only a single or a limited number of Smart Client Profiles available.

Configure general and advanced settings and locks

Configure the general behavior that roles associated with the Smart Client profile should experience on the Client > Smart Client Profile > General tab. In most cases, you will want to hide and disallow any settings the user does not realistically need to perform their job.

If required, configure advanced settings (such as decoding performance and time zone settings) on the Client > Smart Client Profile > Advanced tab.

Lock any settings you do not want users to be able to change.

Configure Live, Playback and Setup tab settings and locks

On the Client > Smart Client Profile > Live / Playback / Setup tabs, configure whether the live, playback, and setup tabs should be available to roles associated with the Smart Client profile and configure which side pane menus under each of those tabs should be visible to the user.

Lock any settings you do not want users to be able to change.

Configure Export settings and locks

On the Client > Smart Client Profile > Export tab, configure whether the export function should be available for roles associated with the Smart Client profile and configure what export options should be available.

Lock any settings you do not want users to be able to change.

Configure timeline and view layout settings and locks

Configure the behavior of the Smart Client timeline for roles associated with the Smart Client profile on the Client > Smart Client Profile > Timeline tab.

Configure which view layouts you want users with permission to create views to be able to use on the Client > Smart Client Profile > View Layouts tab. This limitation is also carried over to users who use the XProtect Smart Wall function.

It is good practice to disable any views that contain more camera tiles than the client workstations are designed to be able to support. You might also disable any view layouts that do not match the available monitors. Lock any settings you do not want users to be able to change.

Configure Smart Map settings and locks

Configure the behavior of the Smart Map for roles associated with the Smart Client profile on the Client > Smart Client Profile > Smart Map tab. Lock any settings you do not want users to be able to change.

> **Note:** Not all XProtect VMS versions include Smart Client Profiles or are limited to a single profile.

See also: 22C. Create Roles

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Clients: Smart Client profiles > Smart Client profile properties

18C. Configure Matrix recipient details

With Matrix, rules configured in the XProtect VMS, as well as Smart Client users, can initiate any camera to be displayed at any user running a Matrix recipient's view.

The Matrix functionality can, to some degree, be used to substitute some of the Smart Wall functionality in XProtect VMS systems that do not have Smart Wall included. For XProtect Corporate systems, you should always use the superior XProtect Smart Wall functionality for user interaction.

The XProtect VMS supports two types of Matrix recipients: a stand-alone Matrix application and Smart Client Matrix. The stand-alone Matrix application had a number of design disadvantages and was terminated (end-of-life, with no support or updates) in 2012. Milestone highly discourages using the stand-alone Matrix application.

Configure XProtect Smart Client Matrix recipients as necessary on the Client > Matrix node.

See also: 18D. Configure Smart Walls

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Clients: Configuring Matrix
- Milestone Product Lifecycle - milestonesys.com

18D. Configure Smart Walls

XProtect Smart Wall is an advanced video wall product that provides excellent situation awareness in larger surveillance centers and helps the surveillance operators focus on what is important, ensuring higher efficiency and shorter response times.

Additional resources:

- XProtect VMS Administrator manual > Add-on products > XProtect Smart Wall (explained)

Create Smart Wall and Smart Wall presets

Create XProtect Smart Walls as needed on the Client > Smart Wall node and add detailed descriptions and any other useful information under the Info tab.

Define Smart Wall presets, if used, under the Client > Smart Wall > Presets tab.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Clients: Configuring Smart Wall > Configure Smart Walls

Add monitors and define monitor characteristics

Add Smart Wall monitors to the Smart Wall (right-click the Smart Wall under Client > Smart Walls).

Edit the Smart Wall layout under the Client > Smart Wall > Layout tab and configure the monitor information for each Smart Wall monitor (size and ratio).

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Clients: Configuring Smart Wall > Configure Smart Walls

Specify Smart Wall monitor layout

After updating the monitor information and while still editing the Smart Wall layout (see above), update the representation of the physical position of monitors relative to each other.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Clients: Configuring Smart Wall > Configure Smart Walls

Define Smart Wall monitor preset views

If you have defined Smart Wall presets (see above) for each Smart Wall monitor (not the Smart Wall itself), configure (edit) the desired layout for an easy preset under the Client > Smart Wall > Presets tab.

In addition to the layout, you can include any cameras you want the layout to show when the preset is triggered.

> **Note:** While users can manually drag any view layout to a Smart Wall Monitor and thus share any kind of view layout content—such as Carousels, Hotspots, Maps, Smart Map, and HTML pages—a Smart Wall preset is limited to containing only cameras.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Clients: Configuring Smart Wall > Configure Smart Walls

19. Configure software events

19A. Create User-defined Events

You can use user-defined events to allow users to manually trigger a rule. User-defined events are also exposed in the MIP-SDK, allowing third-party applications and integrations to trigger rules in the XProtect VMS.

Create any User-defined Events required for the installation on the Rules and Events > User-defined Events node.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Rules and events > User-defined events

19B. Configure Generic Events

Generic events allow you to trigger actions in the XProtect VMS by sending simple strings from any server, client, or device via the IP network to the XProtect Event Server (usually installed on the management server).

Configure Generic Event data settings if not done under 10I

To use Generic Events, you must enable Generic Events, specify event sources, and verify Generic Event settings under Tools > Options > Generic Events.

Create and define Generic Event

Create and define Generic Events as necessary on the Rules and Events > Generic Events node.

Verify if the expression matches the event string the external system is sending. If the system sends out several similar strings, verify that only the intended strings and string combinations give a positive match.

To determine the order in which the XProtect VMS searches for a match, assign the Generic Event a priority if you have multiple Generic Events and an event string is capable of triggering more than one of them. A higher number equals a higher priority.

> **Note:** If there is no risk that a Generic Event may be triggered by the wrong string, there is no need to change the priority (leave it at the default value of 1).
>
> There is no benefit or performance improvement of any kind in assigning a higher priority in those cases.

Test Generic Event

Test the Generic Event.

There are many ways of detecting when a Generic Event has been recognized. For testing, the two easiest ways are:

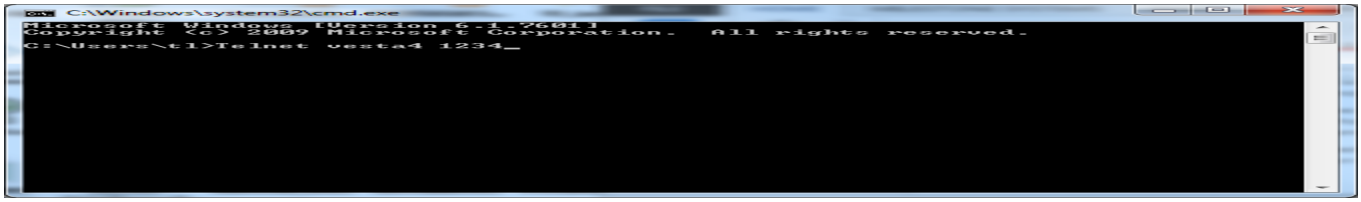
- Checking the Audit Log. This requires you to have User Access Logging enabled for the Audit Log.
- Checking the Rule Log. This requires you to define a rule that activates when the Generic Event is received and makes an entry in the rule log.

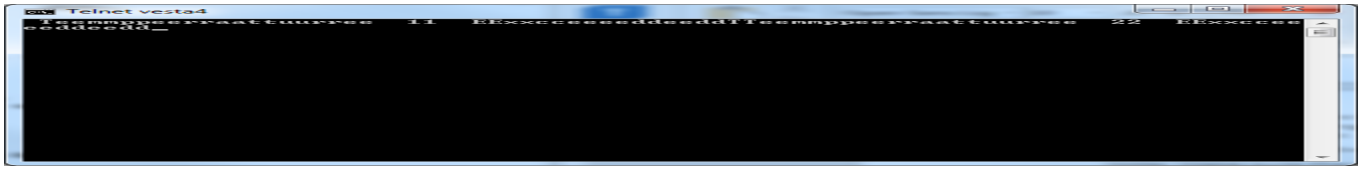
If you don't have access to the external system that will generate the Generic Event string, you can test the Generic Event from a command prompt by opening a Telnet connection to the Event Server on the port used for the Generic Event.

Once the connection is established, you can type or paste in the event string. Note that, depending on the configuration on the Tools > Options > Generic Event tab, you may receive an echo (so each character is shown double) or no feedback at all (no characters show as you type). You must abstract from this and simply type the string as it would be sent. Close the command prompt once the string is complete to force the connection shut.

EXAMPLE:

Expression: "Temperature 1 Exceeded" AND "Temperature 2 Exceeded"





Note: The Generic Event will trigger ONLY when the connection is closed (in this example, click the red X).

Note: Make sure the server/PC you are sending from is allowed as a Generic Event source in the Tools > Options > Generic Event tab.

Note: Telnet is usually disabled in Windows by default. You must turn on the Telnet Client feature on the PC you are testing from to use this test method.

See also: 5C. Run the Management Server installer, 10L. Generic Event settings, 10E. Configure Log Server settings, 21. Create rules

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Rules and events > Generic events

Defining and Monitoring

20. Create time and notification profiles

20A. Define single and recurring Time Profiles

Time profiles are one or more single or recurring time intervals that you can use in rules, roles, and alarms.

Create and define time profiles as needed on the Rules and Events > Rules and Events > Time Profiles node. Make sure the name clearly explains what each time profile covers; provide a detailed description if there is any ambiguity or details the name doesn't reflect.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Rules and events > Time profiles

20B. Define Day Length time profiles

Day length time profiles allow you to create a time profile that adjusts with the season. The profile uses GPS coordinates to determine the sunrise and sunset times each day. You can further set a fixed offset (positive or negative) for both sunrise and sunset to tailor the time profile to your exact application.

Create and define day length time profiles as needed on the Rules and Events > Rules and Events > Time Profiles node. Make sure the name clearly explains what each time profile covers; provide a detailed description if there is any ambiguity or details the name doesn't reflect.

> **Note:** Google Maps and Bing Maps each offer an easy way to obtain GPS coordinates for a location:
>
> Google Maps: Right-click on a location, select "What's here?" to display the GPS coordinates.
>
> Bing Maps: Right-click on a location. The GPS coordinates will show at the bottom of the pop-up window.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Rules and events > Time profiles > Day length time profiles (explained)

20C. Create notification profiles

Notification profiles allow you to set up email notifications that can be triggered by rules. You can include dynamic text (such as the Recording Server name or the trigger time) in both the subject and in the message text. You can also configure profiles to include still images and/or AVI video clips from the relevant camera with the email.

Create notification profiles as needed on the Rules and Events > Rules and Events > Notification Profiles node.

Note: You must configure the email server settings on the Tools > Options > Mail Server tab before you can use email notifications. Likewise, you must configure the AVI creation settings on the Tools > Options > AVI Generation tab before you can include AVI video clips with email notifications.

Note: Notifications containing H.265 encoded video require that the server that runs the Management Server service supports hardware acceleration.

Note: To prevent flooding email recipients with email notifications, you can define a fixed minimum time between emails for an email notification for situations where you predict the system may generate a lot of notifications in a short time—for example, if you trigger the notification based on motion detection or hardware device communication failures.

See also: 10F. Configure email notification settings

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Rules and events > Notification profiles > Notification profiles (explained)
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Notification profiles > Add notification profiles
- eLearning: Configuring and Using Alarms and Notifications

21. Create rules

21A. Verify default rules

Rules are a central element that controls all actions within the XProtect VMS.

The XProtect VMS includes a number of rules as part of the installation. Most of these rules are enabled by default to enable the most common basic features without your needing to set anything up. For example, rules for starting the video feeds to the cameras and recording when motion is detected are enabled by default.

Review the default rules on the Rules and Events > Rules node and determine which ones should be disabled, enabled, or modified to meet the behavior requirements of the installation.

Be aware that, because the rules in the most literal sense determine all actions, if you modify or deactivate the default rules, your system will respond accordingly. This means if you delete or disable all the default rules, the system will not do anything at all until you replace them with rules of your own.

Additional resources:

- XProtect VMS Administrator manual > Rules and events
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Rules (explained)
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Default rules (explained)
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Deactivate and activate a rule
- eLearning: Getting Started with rules in XProtect VMS

21B. Create video and audio feed start and recording rules

Create any additional rules on the Rules and Events > Rules node for starting video, audio, and metadata feeds needed to meet the requirements of the installation.

Create any additional rules for recording video, audio, and metadata needed to meet the requirements of the installation the same way.

Make sure to disable or modify any rules that may conflict with these additional rules. For example, if you create a rule to record a camera only when an external infrared (IR) sensor detects motion, you must disable the Default Record on Motion Rule and create in its place a new rule that includes only the cameras that should record on motion.

Also remember that if a video feed is not started, the XProtect VMS will not be able to show it live or record it.

See also: 21A. Verify default rules, 21C. Create other installation-specific rules

Additional resources:

- XProtect VMS Administrator manual > Rules and events
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Add a rule
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Edit, copy, and rename a rule
- eLearning: Getting Started with rules in XProtect VMS

21C. Create other installation-specific rules

Create all other rules needed to meet the requirements of the installation.

Note about rule complexity:

- If you require a complex system behavior, where a condition (event) will have multiple actions, it is good practice to create multiple simple rules rather than a single complex rule. Even though this results in more rules in your system, simpler rules are much easier to understand and thus maintain an overview of what your rules do.
- Keeping your rules simple also means that you have much more flexibility when it comes to deactivating/activating individual rule elements. With simple rules, you can deactivate/activate entire rules when required and copy and modify rules if new behaviors are required.

Note about rule names:

- Rules are sorted alphabetically by name. When you create rules, Milestone recommends you take extra care and follow a naming convention that will allow you and other system administrators to easily review the rules in order to understand the system behavior and to quickly find a rule if it needs to be modified or copied.
- One suggestion is to always start the rule name with its (primary) action—for example, “START FEED” or “RECORD”. If you do this, because the rules are always listed alphabetically, they will automatically be listed by their function.
- In addition, you should take care to give each rule a name that clearly explains the key behavior of the rule. This makes it relatively easy to get a good overview of how the system is configured, even if it has been a long time since the system was last serviced and/or if the system documentation is not fully updated or available. Remember to add any additional useful details in the description field.

Examples of rule names following this naming convention:

- EMAIL – Notify admin on disk free space threshold warning
- RECORD – Always on outdoor cameras
- RECORD – On motion on indoor cameras
- RECORD – On PTZ manual session
- RECORD AUDIO – On admin reception front door when is doorbell activated
- SMART WALL - Trigger lockdown preset on lockdown user-defined event

A naming convention is, of course, most effective if all system administrators use the same convention and strictly adhere to it. This also applies when servicing and expanding the system after the initial installation has been handed over to the customer.

Additional resources:

- XProtect VMS Administrator manual > Rules and events
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Add a rule
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Edit, copy, and rename a rule
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Rule complexity (explained)
- eLearning: Getting Started with rules in XProtect VMS

21D. Create system administrator email notification rules

Milestone recommends configuring rules to send an email notification to the system administrator(s) for all issues that may potentially affect the receiving, recording, or storage of evidence.

These rules may naturally vary for each installation but, at a minimum, will usually always include these ten situations.

Depending on whether your system uses archiving and/or recording server failover, there are four additional rules to consider (marked in gray):

Event	Event condition located under
Communication Error (Device)	Devices > Predefined Events
Feed Overflow Started	Devices > Predefined Events
Archive Unavailable	Recording Servers
Database Deleting Recordings Before Set Retention Size	Recording Servers
Database Deleting Recordings Before Set Retention Time	Recording Servers
Database Disk Full – Auto Archiving	Recording Servers
Database Disk Full - Deleting	Recording Servers

Database Full – Auto Archiving	Recording Servers
Database Repair	Recording Servers
Database Storage Unavailable	Recording Servers
Failover Started	Recording Servers
CPU Usage Critical	System Monitor > Server
Memory Usage Critical	System Monitor > Server
Service Available Critical	System Monitor > Server

See also: 10F. Configure email notification settings

Additional resources:

- XProtect VMS Administrator manual > Rules and events > Events overview

21E. Validate all rules

When you create a rule, the wizard ensures that all the rule's elements make sense. When a rule has existed for some time, one or more of the rule's elements may have been affected by other configurations and the rule may no longer work. For example, if a rule is triggered by a particular time profile, the rule does not work if you have deleted that time profile or if you no longer have permissions to it.

You can use rule validation to check the integrity of one or all rules by right-clicking on a rule and choosing to validate that rule or to validate all rules. If the rule (or any rules, if you choose to validate all rules) is missing information, the rule validation will point this out to you.

Note that you cannot validate whether configuration of prerequisites outside the rule itself may prevent the rule from working. For example, a rule specifying that recording should take place when motion is detected by a particular camera validates OK if the elements in the rule itself are correct, even if motion detection (which is enabled on a camera level, not through rules) has not been enabled for the relevant camera.

Also note that the rule validation can only check if each rule on its own is executable. Because the system cannot know when a rule may be triggered, it cannot tell you if any rules have conflicting actions. If you have conflicting rules, the software generally prioritizes an action over a non-action (such as recording over not recording) to help ensure the system will behave the same way at all times.

Using simple rules and having a good naming convention, as described above, is the best way to ensure you do not create conflicting rules.

See also: 21C. Create other installation-specific rules

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Validating rules (explained)
- XProtect VMS Administrator manual > Site Navigation: Rules and events > Rules > Rule complexity (explained)

22. Configure users and security

22A. Verify Windows users and groups

Windows users are either users or groups created in Microsoft Active Directory (AD) or local Windows users defined on the Management Server itself.

Active Directory allows you to piggyback on the process the customer already uses for managing access and permissions to their network resources. You therefore need to define permissions on the AD group level only once. As the manager of the Active Directory adds and removes users from the group, their access to and permissions in the XProtect VMS automatically change accordingly.

Verify Windows Active Directory groups and users (if not done under 1G)

Verify the AD user groups exist that are relevant for roles you plan to use in the XProtect VMS and that the AD is reachable from the Management Server. If you plan to add individual AD users to a role, this is a good time to ensure those users are created in the AD.

Create Windows users locally on the Management Server

If you plan to add local Windows users to a role, you must create them in Windows user management directly on the management server. Local Windows users are most commonly used in demo systems and systems with few users, as an alternative to Basic Users.

See also: 1G. Check access to Microsoft Active Directory, 22B. Create Basic Users

Additional resources:

- XProtect VMS Administrator manual > Before you start installation > Prepare Active Directory

22B. Create Basic Users

Whereas Windows users are authenticated by Active Directory or by Windows locally on the management server, based on their Windows login, Basic Users are authenticated within the XProtect VMS Management Server.

A Basic User is simply a username and password pair created in the XProtect VMS by the system administrator. Users cannot change their passwords themselves. Basic users are typically used in smaller systems where there is no Microsoft Active Directory server available for user management and authentication.

Create the Basic Users under Security > Basic Users, as required by the system design document.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Security > Basic users (explained)

22C. Create Roles

In the XProtect VMS, users are assigned to roles, which in turn determine what permissions each user has in the system. The XProtect VMS always has an Administrators role defined which cannot be deleted or modified.

Create additional roles as required by the system specification under Security > Roles.

Note that when you create a role, the system automatically creates a View Group for the role in which to create and store Smart Client views, in addition to the Private View Group each individual user has access to. You can remove the role View Group under Client > View Groups node if it is not required by the system specification.

See also: 18A. Create custom View Groups

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Security > Roles (explained)

22D. Assign client behavior and time profiles

Assign Smart Client profile

The Smart Client Profile determines how the XProtect Smart Client should look and behave for the users in that role.

Select the Info tab for the role and assign a Smart Client Profile to the role from the dropdown list.

Assign Default time profile

You can configure a number of security permissions to apply only during a specified time in a Time Profile. You can specify a specific time profile for each of those permissions, but to make configuration as easy as possible, use a general default time profile as the default setting.

Select the Info tab for the role and select from the dropdown list the time profile you want to use as the default time profile for the role.

Assign Evidence Lock profile

Assign the Evidence Lock profile you want to apply to the role.

Assign Smart Client login time profile

Using the "Only allow login within time profile" dropdown list, select a time profile for which users associated with this role can log in. The user is automatically logged off when the time interval specified in the time profile expires.

Note: Not all XProtect VMS versions include all the functions described in this section.

See also: 18B. Configure Smart Client Profiles, 20A. Define single and recurring Time Profiles, 10H. Create Evidence Lock profiles

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > Info tab (roles)

22E. Configure client permissions and login authorization requirements

Select what client applications users of the role are permitted to use—e.g., XProtect Smart Client, XProtect Mobile Client, and/or XProtect Web Client.

Select whether two-step login authorization (sometimes also referred to as "four-eye authorization" or "two-man rule") is required for users in this role. If selected, the XProtect Smart Client, XProtect Web Client, and the Management Client will ask for a second user, who must have user authorization privileges (typically by a supervisor or manager), to also provide their credentials before the user is logged in.

The Authorize users permission option is located on the Overall Security tab.

Select whether to make users anonymous during PTZ sessions. When this option is selected, the user will show up as "anonymous" instead of by user name on the "PTZ controlled by" and "PTZ session reserved by" notifications in the XProtect Smart Client (located in the PTZ menu on the camera's tool bar). The setting does not influence the (optional) Audit Log user access logging information.

See also: 22G. Define overall security settings for each role, 10E. Configure Log Server settings

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > Info tab (roles)

22F. Assign users and groups to each role

Add the users that should be associated with a role on the Users and Groups tab of the role. You can add Basic users that have already been created as well as Windows/Active Directory users and groups.

Note that users assigned to the BUILTIN\Administrators role will always have full system administrator permissions in the XProtect VMS (the role permission tabs are grayed out).

Also note that any user who is a member of the BUILTIN\Administrators group in Local Users and Groups in Windows user management—i.e., a user who can log into the physical server with Windows administrator privileges—is always assigned to the XProtect VMS Administrators role. You cannot remove those users from the role. This is a precaution to ensure that you never get into a situation where an administrator accidentally deletes all administrator users (including him/herself) and thereby is permanently locked out of the system with no option to get back in.

See also: 22A. Verify Windows users and groups, 22B. Create Basic Users

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > User and Groups tab (roles)

22G. Define overall security settings for each role

The settings on the Overall Security tab comprise the primary way of defining permissions for the role.

The XProtect VMS has a number of security groups, under which are a number of system components. For each component, you can configure the overall security to allow, deny, or remain undefined (no option selected).

Configure Overall Security settings for each role, as per your system design document, on the Overall Security tab for the role.

> **Note:** You can associate a user with more than one role, in which case you may end up having conflicting settings. In this case, the XProtect VMS will always prioritize an overall security setting (allow or deny) over any individual device/functional detail level permissions and will always prioritize the "deny" over the "allow" setting.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > Overall security tab (roles)

22H. Define detail security settings for each role

For each role, configure permissions for all functions for which there is no defined (allow/deny) overall security setting.

- Device access permissions (Security > Roles > Device tab for the role)
- PTZ permissions and priority (Security > Roles > PTZ tab for the role)
- Speaker access and priority (Security > Roles > Speech tab for the role)
- Smart Wall permissions (Security > Roles > Smart Wall tab for the role)
- Event activation permissions (Security > Roles > External Events tab for the role)
- View Group permissions (Security > Roles > View Group node)
- Matrix permissions (Security > Roles > Matrix node)
- Alarm permissions (Security > Roles > Alarm)

> **Note**: Only devices (cameras, microphones, speakers, inputs, outputs, and metadata) and device functions you explicitly permit access to will be available to users associated with the role.

> **Note**: You can select a device group to set permissions for all devices currently in that group.

Note: Event permissions include both pre-defined events (i.e., events native to the XProtect VMS, such as RequestPlayAudio, RequestStartRecording, and RequestStopRecording) and user-defined events (i.e., events defined by you or other system administrators on the Rules and Events > User-defined Events node).

See also: 22G. Define overall security settings for each role, 19A. Create User-defined Events; 18A. Create custom View Groups; 18C. Configure Matrix recipient details23. Define alarms

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > Device tab (roles)
- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > PTZ tab (roles)
- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > Speech tab (roles)
- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > Smart Wall tab (roles)
- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > External Events tab (roles)
- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > View Groups tab (roles)
- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > Matrix tab (roles)
- XProtect VMS Administrator manual > Site Navigation: Security > Roles settings > Alarms tab (roles)

22I. Verify effective roles

With the Effective Roles feature, you can view all roles of a selected user or group and thus verify their permissions match the requirements set forth in your system design document.

The function is located on the Tools > Effective Roles menu.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Security > View effective roles

23. Define alarms

23A. Add and remove alarm sounds

You can define alarms based on the events in the XProtect VMS for users to handle through the XProtect Smart Client, XProtect Web Client, and XProtect Mobile client.

If you will be using alarms with sound alerts, you should first verify the sounds you need are available in the system. On the Alarms > Sound Settings node, add and remove sounds to/from the list.

> Note: Sound files must be in Windows standard .WAV format or MP3 format and be less than 10 MB in size. The sound file is automatically uploaded to the Management Server and from there automatically distributed to the client workstations.

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Alarms > Alarms (explained)
- XProtect VMS Administrator manual > Site Navigation: Alarms > Sound Settings

23B. Configure alarm data settings

Verify and create alarm priorities

An alarm will always have an initial priority when triggered. Upon triggering, the associated sound file will play on the user workstations. Once triggered, users with permissions to manage the alarm can change the priority as needed to any other priority available in the list.

If the system design document requires additional or different alarm priorities, you must modify the settings on the Alarms > Alarm Data Settings > Alarm Data Levels tab.

> Note: To remove an alarm priority, click in the left-most (unnamed) column to select the priority and press the <delete> key on the keyboard.

Verify and create alarm states

The XProtect VMS has four built-in alarm states: new, in progress, on hold, and closed. In addition, you can add your own states to match the specific workflows used by the customer.

An alarm will always have an initial state of “New” when triggered. The alarm state will change to “In progress” once a user with permissions to manage the alarm selects it. The user can then change the state to any other priority available in the list as needed. The user closes the alarm by changing the state to “Closed”.

If the system design document requires additional or different alarm states, you must modify the settings on the Alarms > Alarm Data Settings > Alarm Data Levels tab.

To remove an alarm state, click in the left-most (unnamed) column to select the state and press the <delete> key on the keyboard. The built-in alarm states cannot be deleted.

Create alarm categories

Alarm categories can be used as levels, in addition to the alarm priority and alarm status, to classify or categorize alarms. The XProtect VMS does not have any default alarm categories defined.

If the system design document requires additional or different alarm categories, you must modify the settings on the Alarms > Alarm Data Settings > Alarm Data Levels tab.

To remove an alarm category, click in the left-most (unnamed) column to select the category and press the <delete> key on the keyboard.

Define alarm list columns

You can customize which information columns are available for the users when they view and manage alarms on the Alarms > Alarm Data Settings > Alarm List Configuration tab.

Edit the content of the "Selected columns" list to match the requirements in the system design document.

Enable and create reasons for closing alarms

Some customers may have an alarm-handling workflow that requires the operator to submit a reason when closing the alarm.

Enable the option and add the valid closing reasons to the list on the Alarms > Alarm Data Settings > Reasons for Closing tab, as defined by the system design document.

See also: 10K. Configure alarm and event settings

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Alarms > Alarm Data Settings

23C. Define alarm definitions

Create the alarm under Alarms > Alarm Definitions. Make sure to give it a descriptive name if your system design document doesn't already specify the name for the alarm.

Provide detailed instructions in the Instructions field for the operator to follow when handing the alarm, as defined by the customer in the system design document.

Configure trigger

Select the event that should trigger the alarm by selecting the event category, the event type, then the specific trigger event.

Configure activation period

By default, the alarm will always be active. Select a different time profile if the system design document calls for the alarm to be active only at selected times or select start and stop events if the alarm should be active only after another event (often from a third-party system integrated with the XProtect VMS) has occurred.

Configure operator action requirements

Some customers may have an alarm-handling workflow that requires the operator to react to an alarm within a certain time.

Select the required maximum reaction time in the Time Limit dropdown list, as specified by the customer in the system design document and select the event the XProtect VMS must trigger if the time is exceeded. The event is almost always a User-defined Event since this enables you, for example, to execute a rule to alert the operator or to send a notification to a supervisor.

Configure related cameras and maps

Select any cameras that are related to the alarm and are not implicitly related to the alarm event (software motion detection, for example, already includes the camera that detects the motion). The related cameras will show automatically when the operator handles the alarm.

If you have maps defined in the XProtect VMS that are relevant for the alarm, you can associate the map with the alarm on the related map dropdown list, so that it is displayed to the operator when they manage the alarm.

> **Note:** Maps are configured through the XProtect Smart Client.

Configure initial alarm owner, priority, and category

Configure the initial alarm owner (optional), initial alarm priority, and initial alarm category (optional), as specified in the system design document.

Configure events triggered by alarm

Select if other events should be triggered automatically when this alarm is triggered.

Also decide if the XProtect VMS should automatically close the alarm when the alarm condition is no longer relevant. For example, if the alarm is triggered by a "device not responding" event, auto-close will automatically close the alarm when the device starts responding. Note that not all events can auto-close, in which case the check box will be grayed out.

See also: 20A. Define single and recurring Time Profiles, 19A. Create User-defined Events, 28F. Create maps and Smart Map

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Alarms > Alarm configuration (explained)
- XProtect VMS Administrator manual > Site Navigation: Alarms > Add an alarm
- XProtect VMS Administrator manual > Site Navigation: Alarms > Alarm Definitions (properties)
- eLearning: Configuring and Using Alarms and Notifications

24. System performance and alerting

24A. Verify system performance via System Monitor

The System Monitor provides you with a quick, visual overview of the current state of your system's servers and cameras through colored tiles that represent the system hardware. In addition, you can enable saving historic system monitor data on the System Dashboard > System Monitor > Customize menu.

Even if you are not planning to use the historic data in the long term, Milestone recommends you enable it temporarily when you complete the system configuration to help validate the system is performing as expected. After the system has been running for a while, you can revisit this section to verify all values have remained satisfactory within the past 30 days (or however long the system has been running with a stable configuration). You can then disable the historical data option again if desired.

Recording the history will place an additional load the SQL server database and connection, so don't set the sampling interval shorter than you need it to be. Also, remember to disable the history again after that initial check if you do not intend to use it as part of a regular problem-prevention process.

> **Note:** The System Monitor uses the Data Collector service to collect and generate data. In very large systems, the CPU load on the management server CPU to process the data from thousands of cameras may be overly excessive relative to its benefits, especially if you already use an external SNMP or Microsoft System Center Operations Manager (SCOM) monitoring solution. In these cases, you may consider disabling the Data Collector service on all servers (Management Server, Recording Servers, mobile servers, etc.) to save resources.

Verify or customize system monitor thresholds

The System Monitor allows you to configure which system performance parameters you want to monitor, as well as the warning and critical levels for those parameters.

Verify or change which parameters to monitor and adjust the warning and critical alarm threshold values to best fit the needs of the installation on the System Dashboard > System Monitor Thresholds node for server, camera, disk, and storage (recording retention time).

Adjust the calculation interval for each parameter as desired to best meet the need for responsive updates while still avoiding false alerts stemming from irrelevant value fluctuations.

Verify service status, CPU and memory usage on all servers

Verify the CPU and memory utilization of all servers by selecting the System Dashboard > System Monitor > All servers tile. Both should read out normal (green) if the parameter is enabled. If the parameter is not enabled (see above), the status indicator will be gray.

Click the Details button for each critical server/service (at a minimum, the Management Server and all Recording Server services) and verify the actual CPU and memory usage values are within the expected range.

Verify free space and retention time on recording servers

Click the System Dashboard > System Monitor > All servers tile > Details button for each Recording Server and verify the actual disk read and write rates, as well as the network bandwidth usage values, are within the expected range.

To save time, you can combine this task with verifying the recording server CPU and memory utilization described above.

Verify frame rate and used space status for all cameras

Verify the camera frame rate status of all cameras by selecting the System Dashboard > System Monitor > All cameras tile. Both the Live FPS and Recording FPS should read out normal (green) if the parameter is enabled. If the parameter is not enabled (see above), the status indicator will be gray.

If the Live FPS shows a warning (yellow) or critical (red) state, the Recording Server is not receiving the frame rate you have configured. If the camera is intended to be started (check the rules), you should verify and troubleshoot your settings, network connection, camera capabilities/specification, etc. until what the server receives matches the configuration.

If the Recording FPS shows a warning or critical state and the camera should be recording (check the rules), you should verify the settings on the camera's settings, stream, and record tabs are correct and that the recording server storage system is able to process the amount of data sent to it.

Configure system performance email notification rules

If not done under section 21D.

See also: 15B. Configure general camera settings , 15C. Configure video streams, 15E. Configure recording, 21A. Verify default rules, 21B. Create video and audio feed start and recording rules, 21D. Create system administrator email notification rules

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: System Dashboard > System monitor (explained)
- XProtect VMS Administrator manual > Site Navigation: System Dashboard > Customize dashboard
- XProtect VMS Administrator manual > Site Navigation: System Dashboard > System monitor details (explained)
- XProtect VMS Administrator manual > Site Navigation: System Dashboard > System monitor thresholds (explained)

24B. Verify connectivity to Customer Dashboard

The Customer Dashboard allows you, as an integrator, to monitor the health of your customers' systems in real time, receive status updates, and keep track of technical incidents.

The Customer Dashboard information uses the System Monitor functionality and also provides you with the option to configure and receive system uptime reports and customizable notifications to help you address potential system issues before they disrupt a customer's business.

If you will be using the Customer Dashboard, you should verify the XProtect VMS is set up to send data to the portal on the Tools > Options > Customer Dashboard tab. You must activate the license before the Customer Dashboard starts receiving messages from the XProtect VMS:

- Log into the Customer Dashboard (https://online.milestonesys.com/) with your MyMilestone login.
- Add the customer to the Customers & Licenses > Customers tab, if the customer is not already in the list.
- Verify the Software License Code (SLC) is registered to your account under Customers and Licenses > Licenses tab. Select the license, then click the Details button and associate the license to the customer.
- Verify the server Monitoring Status is listed as "Monitored" on the Customer Dashboard > Server status page.

You can create error notification profiles on the Customer Dashboard > Error Notifications page to receive an email when any of the customer systems you are monitoring experiences a potential problem, and you can create filters to ignore errors you are not interested in receiving notifications for on the Customer Dashboard > Errors page.

The Customer Dashboard requires an active Milestone Care™ Plus subscription and that the management server has a permanent connection to the internet.

See also: 10J. Configure Customer Dashboard connectivity

Additional resources:

- XProtect VMS Administrator manual > Setting options for the system > Customer Dashboard tab (options)
- Customer Dashboard - milestonesys.com
- eLearning: Exploring the Milestone Reseller Portal

24C. Verify SNMP trap connectivity

The XProtect VMS supports Simple Network Management Protocol (SNMP), a standard protocol for monitoring and controlling network devices, managing their configuration, collecting statistics, and more.

The system acts as an SNMP agent which can generate an SNMP trap as a result of a triggered rule. A third-party SNMP management console can then receive information about the rule-triggering event and operators of the SNMP management console can configure their system for further action as required.

The implementation uses Microsoft® Windows® SNMP Service for triggering SNMP traps. This means that you must install the SNMP Service on recording servers. After configuring the SNMP Service through its own user interface, Recording Servers can send .mib (Management Information Base) files to the SNMP management console.

If the system design document requires sending SNMP traps, you must enable this in Windows if you did not already do that when you installed the server. Next, you must create rules to send SNMP traps, if you haven't already done so.

Configure the third-party SNMP management system to receive SNMP traps from the XProtect VMS Management Server and verify everything works as intended by forcing errors or situations that will trigger an SNMP trap to be sent, received, and displayed.

See also: 3K. Enable SNMP traps

24D. Check log files

Verify System Log is active and logging detail level is correct

Access the System Log under the Server Logs > System Log node and verify you have log entries and that the logging level details are as expected. As needed, force an error or situation that must trigger an entry into the log to verify the functionality.

Verify Audit Log is active and logging detail level is correct

Access the Audit Log under the Server Logs > Audit Log node and verify you have log entries and that the logging level details are as expected. As needed, force an error or situation that must trigger an entry into the log to verify the functionality.

Verify Rule Log is active and the information for each rule log entry is correct

If you have configured rules to make entries into the rule log, access the Rule Log under the Server Logs > Rule Log node and, to the extent possible, verify the functionality by forcing errors or situations that will trigger an entry into the log.

See also: 10E. Configure Log Server settings, 21C. Create other installation-specific rules

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: Logs > Logs (explained)
- XProtect VMS Administrator manual > Site Navigation: Server logs > System logs (properties)
- XProtect VMS Administrator manual > Site Navigation: Server logs > Audit log (properties)
- XProtect VMS Administrator manual > Site Navigation: Server logs > Rule-triggered logs (properties)

Extending and Maintaining

25. Configure Mobile servers

25A. Install XProtect Mobile server

If not already done.

This is required if users will access the XProtect VMS through the XProtect Web Client or XProtect Mobile client.

> **Note:** The single computer installation option automatically installs the XProtect Mobile server.

See also: 6. Install XProtect Mobile server

25B. Configure general settings

Access the general settings of the XProtect Mobile server on the Servers > Mobile Servers > General tab.

Verify mobile server name, description, and login method

Make sure the name of the server is one that makes sense also when the system is serviced at a later date. Add a description of the location, intended use for the server, and anything else that may be useful months or years from now.

Specify what login method to allow—Windows authentication, basic authentication, or both (Automatic).

Configure mobile server features and log settings

Configure the features you want the XProtect Mobile server to provide, or import and edit a configuration backup made from a different Mobile server:

- Disable XProtect Web Client access if this is not a requirement for the installation.
- The All cameras view is generally useful only in systems with a low number of cameras. In systems where you or the users themselves create customized views in the Smart Client, users have access to their normal Smart Client views in the XProtect Mobile client and the all cameras view can be disabled.
- Disable the actions (output and events) if remote users should not be allowed to trigger those.
- Enable keyframes if called for in the system design document, or if the bandwidth available to XProtect Web Client users is too limited for higher frame rates.
- Disable the built-in Administrators role from access to the Mobile server unless you are installing a small system with only a few users. With the exception of smaller installations, where security and user tracking is perhaps less critical, users should not normally use an administrator account for Smart Client or mobile viewing access to the XProtect VMS.

- For normal operations, you can usually ignore the Mobile server log (leave it at default settings).

If you have multiple mobile servers, they are each configured separately. Depending on your system requirements, you can configure each server with identical settings—for example, if you are simply dividing users onto different servers to share the load or using different settings because you need a different quality profile for some users.

If you have multiple Mobile servers that should be configured identically, complete all the steps in this section on one server, export the mobile server configuration, then import it to each of the other servers.

Additional resources:

- XProtect Mobile server administrator manual > Mobile server settings > General tab

25C. Configure connectivity settings

Access the connectivity settings of the XProtect Mobile server on the Servers > Mobile Servers > Connectivity tab.

Verify connection type and client timeout settings

Configure what connection type (HTTP and/or HTTPS) users are permitted to use.

> **Note:** If a certificate issued by a certificate authority (CA) trusted by the mobile device is not installed and enabled on the Mobile server, disallow HTTPS connections.

> **Note**: Milestone recommends not permitting HTTP connections if users can connect across open networks, such as the internet or open WiFi connections.

The client timeout (http) setting determines how often the XProtect Mobile client must indicate to the Mobile server that it is up and running. The default value (30 seconds) will work in most installations and should be increased only if you experience disconnect errors due to extreme latency that cannot be reduced. Be aware that the user experience will likely be greatly affected in networks with high latency.

Configure UPnP and internet access settings

When the Enable UPnP discoverability and Enable automatic port mapping check boxes are selected, and your network router has Universal Plug and Play (UPnP) support enabled, the router may automatically configure inbound access from the internet to the XProtect Mobile server. If any of the XProtect Mobile server settings (such as IP address or ports) change, the router will automatically update its port forward settings.

If the network consists of multiple layers of routers, and UPnP is enabled throughout the network and the Mobile server, you must enable the Configure customer internet access option in the Mobile server and manually specify the values you want the Mobile server to report to the UPnP-enabled network for the router chain to be configured correctly.

For security reasons, most customers prefer to disable UPnP throughout their network and simply configure port forwarding manually so they maintain complete control of the network at all times.

Therefore, unless the system design document explicitly specifies using UPnP to automatically configure inbound access, Milestone recommends you disable the UPnP discoverability option in the Mobile server and configure port forwarding manually as necessary.

Configure Smart Connect

Smart Connect allows you to send mobile users an email to add the XProtect Mobile server connection information to their XProtect Mobile client, so they don't have to manually type in technical details like IP address and ports.

After Smart Connect is enabled, you can specify one or more email addresses to send an invitation to. The XProtect VMS will relay the request to a Milestone server on the internet which in turn will generate and send the email to the users, or you can copy and paste the token into an email yourself.

The email from Milestone contains a link to install the XProtect Mobile app (the link automatically redirects the user to the appropriate app store for the device), and an "Add your server to XProtect Mobile" link. After the user has installed the app and clicks the link, the server is added to the server list in the app.

> **Note:** Smart Connect requires the Mobile server to have access to the internet (outbound connection), and the Software License Code (SLC) used to have a valid Milestone Care Plus subscription. If the XProtect Mobile server should be accessible from the Internet (inbound connection), this must be configured before sending the link to the user.

Verify firewall and router settings if not done under 1D

To enable inbound access in a non-UPnP network, simply configure inbound port forward in the routers manually, if you have not done so already. If you use UPnP, this should be configured automatically.

Make sure the Windows firewall and any third-party antivirus software that uses real-time port scanning are configured to allow inbound access to the XProtect Mobile server.

Test whether the XProtect Mobile server is accessible (i.e., that you can log in from a user account with the correct permissions) from any network the server should be accessible, including from the internet.

Confirm, by testing, that the XProtect Mobile server is not accessible (i.e., the server is unreachable, or access is denied) by user accounts (roles), clients, and networks that should not have access to the Mobile server.

See also: 1D. Configure the network, 1E. Test the network, 3J. Add anti-virus scan exceptions, 6F. Verify the server is running

Additional resources:

- XProtect Mobile server administrator manual > Mobile server settings > Connectivity tab
- XProtect Mobile server administrator manual > Enable encryption > Enable encryption on the mobile server > Edit certificate
- Universal Plug and Play - Wikipedia.org
- XProtect Mobile server administrator manual > Smart Connect (explained) > Set up Smart Connect
- eLearning: Configuring XProtect Mobile with Smart Connect

25D. Configure performance settings

Configure the Mobile server performance settings to meet any requirements in the system design document on the Servers > Mobile Servers > Performance tab.

> **Note:** The Mobile server transcodes video into MJPEG format. This allows the Mobile server to shift seamlessly between different streaming qualities and uses less CPU power to decode and display in the XProtect Mobile client and XProtect Web Client.

Additional resources:

- XProtect Mobile server administrator manual > Mobile server settings > Performance tab

25E. Configure Investigation settings

You can enable investigations so that people can use XProtect Web Client and XProtect Mobile to access recorded video, investigate incidents, and export and download video evidence.

Enable and configure investigations for each Mobile server as required on the Servers > Mobile Servers > Investigations tab.

> **Note:** While users create investigations and export data from the Web Client or Mobile client, the export itself is done by the Mobile server and all data is stored on the Mobile server. If users have access to log in to more than one Mobile server, they will see only investigations and exports made on that specific server.

Additional resources:

- XProtect Mobile server administrator manual > Mobile server settings > Investigations tab

25F. Configure Video Push

Video push lets a XProtect Mobile client user stream live video from the camera on their mobile device to an XProtect VMS Recoding Server via the XProtect Mobile server.

Video Push requires a Hardware Device License per channel. A Video Push channel is assigned to a specific XProtect Mobile server as well as a specific user login. A Video Push channel cannot be shared among multiple user logins.

> Note: If two users log in with the same credentials, they can both access the Video Push channel, but only one at a time (first come, first serve). If one user is already using the Video Push, and a second user tries to start a Video Push stream, the second user will receive an error message.

Enable Video Push and add Video Push channels

Enable Video Push on the Servers > Mobile Servers > Video Push tab, if required in the system design document, and add the number of Video Push channels you need.

This step establishes the channel, the IP port used by the channel, and the association to the user login. You can change the port number, if required by the customer's network design, but do not change the automatically generated MAC address.

> Note: While the port must be unique for each Mobile server, if you have multiple Mobile servers, as with all IP ports you can, of course, use the same ports on each Mobile server.

> Note: You can change the default password for the video push driver via the Change password button in the lower- right-hand corner.

Add Video Push device driver for each Video Push channel

Use the Add Hardware wizard to add a Video Push hardware device for each Video Push channel you created on the Recording Server where you want to record that channel.

You must use the manual detection method and specify the hostname (or IP address) of the Mobile server that will be hosting that Video Push channel, as well as the port number (defined above) for that channel. If you have changed the video push driver password, you must also specify this.

Once added, verify the video push video and audio streams are recorded to the intended storage configuration.

> Note: Make sure you explicitly specify to use the Video Push Driver in the hardware model dropdown list (auto-detect does not work with Video Push and other specialized device drivers for non-physical devices).

Find cameras for Video Push channels

Back on the Servers > Mobile Servers > Video Push tab, complete the association of the Video Push channel on the Mobile server to the Video Push device driver on the Recording Server.

Verify all channels are assigned a Video Push camera channel in the Camera Name column.

If you have multiple XProtect Mobile servers in the system, you must do this for each Mobile server.

See also: 13. Add hardware devices

Additional resources:

- XProtect Mobile server administrator manual > Using Video Push to stream video (explained) > Set up Video Push to stream video
- XProtect Mobile server administrator manual > Using Video Push to stream video (explained)
- Knowledge base article 000001226: About the MAC address used for Video Push driver

25G. Configure Push Notifications

You can enable XProtect Mobile to notify users when an event occurs, such as when an alarm triggers or something goes wrong with a device or server. Notifications are always delivered, regardless if the app is running or not.

Push notifications use cloud services from Apple (Apple Push Notification service, or APN), Google (Google Cloud Messaging Push Notification service), and Microsoft (Microsoft Azure Notification Hub).

Enable notifications if required by the system design document. As users log in for the first time, their devices are automatically added to the registered devices list. Once in the list, you can determine if the device should receive Push Notifications. Disable any devices that should NOT receive notifications.

> **Note:** Users can disable Push Notifications themselves globally in the Miscellaneous menu in the Mobile client app. Also, for each XProtect Mobile server a user has installed in their app, they can choose notification settings for each server under the Configuration > Notification settings for that server. Here, the user can choose whether to receive no alarms, all alarms (default setting), or only alarms that are assigned to them.

> **Note:** There is a limit to the number of notifications that a system is allowed to send during a period of time. If your system exceeds the limit, it can send only one notification every 15 minutes during the next period. The notification contains a summary of the events that occurred during the 15 minutes. After the next period, the limitation is removed.

> **Note:** Push Notifications require the Mobile server to have access to the internet (outbound connection), and the Software License Code (SLC) used to have a valid Milestone Care Plus subscription.

See also: 23C. Define alarm definitions

Additional resources:

- XProtect Mobile server administrator manual > Sending notifications (explained)
- XProtect Mobile server administrator manual > Mobile server settings > Notifications tab
- eLearning: Configuring and Using Push Notifications

26. Configure Milestone Interconnect

26A. Add Interconnected systems

Milestone Interconnect™ allows you to integrate a number of smaller, physically fragmented, and remote XProtect or Milestone Husky™ NVR installations with an XProtect Corporate central site.

Use the Add Hardware wizard to add remote sites as required by the system design document.

You must use the manual detection method and specify an administrator user account on the remote server to use for the connection. If you are specifying a Windows user account on the remote system, you must precede the user name with the hostname of that system (for example, XProtectVMS1\administrator).

Make sure you explicitly specify to use the correct driver manually in the hardware model dropdown list (auto-detect does not work with Video Push and other specialized device drivers for non-physical devices).

Milestone XProtect VMS Interconnect:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- Milestone Husky M500A, Milestone Husky M550A

Milestone XProtect Professional VMS Interconnect:

- XProtect Enterprise
- XProtect Professional
- XProtect Express
- XProtect Essential (paid versions)
- Milestone Husky M20, Milestone Husky M30, and Milestone Husky M50
- Milestone Arcus Embedded Interconnect
- Milestone Arcus embedded on third-party devices such as cameras and NAS devices
- Milestone Husky M10

Refer to the next step for more details about adding/enabling devices.

See also: 13. Add hardware devices, 26B. Select Interconnected cameras

Additional resources:

- XProtect VMS Administrator manual > Configuring Milestone Interconnect > Milestone Interconnect (explained)
- XProtect VMS Administrator manual > Configuring Milestone Interconnect > Add a remote site to your central Milestone Interconnect site

26B. Select Interconnected cameras

As with any multi-channel hardware device, you choose which associated logic devices (cameras, microphones, speakers, inputs, outputs, and metadata) you want to enable as part of the Add Hardware wizard process, or you can modify the selection at any later time.

Select which logic devices to enable and make sure they have "good" names.

> **Note:** Remote Interconnected systems do not require a Hardware Device License to add them, but instead require a Milestone Interconnect camera license for each remote camera channel you enable on the XProtect Corporate central site.

> **Note:** If you change the device configuration on the remote site (add, remove, enable, disable, or rename a device or event) you must update the configuration on the central site to reflect the new configuration on the remote site.

See also: 11A. Review license information, 13. Add hardware devices, 14. Name and group devices

Additional resources:

- XProtect VMS Administrator manual > Configuring Milestone Interconnect > Update remote site hardware

26C. Verify feed start and recording rules for Interconnected cameras

Combined with the settings on the remote system itself, the live streaming and recording possibilities are almost limitless. Typically, a remote system will be recording either on motion or always, while the default rules on the central system (assuming they have not been modified or disabled) will start the stream on all remote cameras (using a lot of bandwidth) and record those streams on motion.

Configure the start feed and recording rules for the Interconnected cameras to meet the requirements in the system design document.

Create any additional rules and alarms related to the events on the remote system.

See also: 21. Create rules, 23. Define alarms

Additional resources:

- XProtect VMS Administrator manual > Configuring Milestone Interconnect > Milestone Interconnect setups (explained)

26D. Verify user permissions to Interconnected cameras

Assign user permissions to Interconnected cameras, microphones, speakers, inputs, outputs, and metadata, as for any other device.

See also: 22. Configure users and security

27. Activate license

27A. Activate license

If you have not activated the license after adding hardware devices (Included Interconnected cameras), these will still be running in the grace period (normally 30 days).

Activate the license on the Basics > License Information > Activate License dropdown menu.

Activating the license will also reset the permitted changes without activation limit and update the license with any additional licenses that may have been purchased since the last activation.

If you forget to activate licenses before the grace period expires, they will stop sending video to the system. These licenses are shown in the Grace Period Expired column. See also Activate licenses after grace period.

See also: 11B. Activate license

27B. Enable automatic license activation

Enable automatic license activation on the Basics > License Information page as desired, if not already done. The management server must have permanent access to the internet to use this feature.

See also: 11B. Activate license

27C. Verify license information

After activating the license, review the license information again to ensure all hardware devices and features are registered as licensed. Also verify that the license and Milestone Care Plus expiration dates and the number of available licenses match what you have purchased.

See also: 11A. Review license information

28. Configure the Smart Client

28A. Check workstation hardware, software, and settings

Verify Windows version

Make sure the Windows version is compatible with the XProtect Smart Client version you are installing.

Milestone recommends you always keep your system current by installing all important updates from Microsoft.

Verify .Net version

Verify the required (or newer) .Net version is installed.

Verify DirectX version

Verify the required (or newer) DirectX version is installed.

Verify Graphics card capabilities

Verify the graphics card meets the requirements specified in the system design document.

Verify Intel Quicksync support

Make sure Intel Quicksync is supported and enabled if the system design document specifies using hardware decoding (recommended for all systems using MPEG4 or H.264 camera streams).

Check NVIDIA graphic card drivers

If the workstation has one or more NVIDIA graphics cards installed, the Smart Client may be able to use the NVIDIA GPU to decode the video streams. Verify the graphics card is identified as an NVIDIA card in the Windows Device Manager.

> **Note:** The NVIDIA Maxwell platform includes two product lines: GM107 and GM108. The GM108 line, used mostly in laptops, does not support hardware encoding and decoding. You may verify which line a given GPU belongs to directly with NVIDIA or by checking with a third-party tool such as GPU-Z. The additional resources section also includes a link to a third-party list of GM108 models that may be helpful, though it is not guaranteed to be complete.

> **Note:** Users of NVIDIA Optimus GPUs, used mostly in laptops, may experience crashes or slow frame rates on additional monitors. Milestone has published a KB article describing a solution.

Check network connectivity

Make sure the workstation can access the management server and all recording and failover recording servers. Also make sure the workstation has access to the internet, if this is a requirement.

Check workstation time

Verify the workstation is set to the correct time and time zone.

If the workstation is more than five minutes off from the server, the login may fail. Also, because the server time is converted to UTC time when stored and converted to the local time of the Smart Client (depending on your settings, this is the default behavior), all evidence search, and export will be incorrect if the workstation time is not correct, potentially rendering the evidence inadmissible in court.

If you use a common time source, such as internet time or a local NTP time server (recommended), you should verify that the time updates correctly. If the workstation is on a domain, it will automatically synchronize to the domain server time.

Check hostname lookup

XProtect Smart Client and XProtect Management Clients must be able to successfully resolve the hostnames of all XProtect VMS servers, even if users use the management server IP address to log into the client.

Therefore, when preparing a new workstation, it is good practice to verify it can resolve the hostnames of the management server and all recording and failover recording servers.

If the hostnames do not resolve through the DNS, or there is no DNS, you may edit the Windows HOSTS file manually.

> See also: 1F. Check Network Time Protocol (NTP) server, 3G. Check server time, 1E. Test the network > Dynamic Name Server (DNS)
>
> Additional resources:
>
> - Milestone product system requirements - milestonesys.com
> - XProtect Smart Client User Manual > Enabling hardware acceleration
> - TechPowerUp GPU-Z - techpowerup.com
> - NVIDIA GM108 Graphics Processing Unit (GPU) - videocardz.net
> - Knowledge base article 000006212: How to run the XProtect Smart Client on Nvidia Optimus hybrid graphic cards

28B. Import certificates on Smart Client workstations

If you are manually distributing certificates, you must ensure the CA is trusted before proceeding.

> See also:"3A. Obtain or create server communication encryption certificates" on page 27, "7D. Specify recording server encryption" on page 44, "12F. Enable certificates" on page 61

28C. Download and run Smart Client installer from the Management Server

XProtect Smart Client is a powerful, easy-to-use client application for a surveillance installation's daily operations. Its streamlined interface provides intuitive and powerful functions to manage any Milestone installation, regardless of its size.

Download and run the XProtect Smart Client installer on the workstation(s) you or the customer will be using for managing the XProtect VMS.

The XProtect Smart Client installation file is available on the Management Server admin download page: http://<management server>/installation

> Note: If you have a newer version of the XProtect Smart Client installed (for example, on your service laptop) it will usually work with older versions of the Management Server as well. If you have an older version installed, you may be prompted to upgrade when you log into the system.

See also: 10A Log in with the Management Client, 32E. Upgrade the system

Additional resources:

- XProtect Smart Client - milestonesys.com
- XProtect Smart Client User Manual > Application buttons (explained)
- XProtect Smart Client User Manual > Install XProtect Smart Client
- XProtect Smart Client User Manual > Logging in
- XProtect Smart Client User Manual > Getting to know your XProtect Smart Client > Modes in XProtect Smart Client (explained)
- XProtect Smart Client User Manual > Advanced mode overview (Live tab)

28D. Create views for each view group

The way video is displayed in XProtect Smart Client is called a view.

A view can contain video from up to 100 cameras, depending on your surveillance system. XProtect Smart Client can handle an unrestricted number of views, allowing you to switch between video feeds from various groups of cameras. The layout of each view can be customized to fit its content.

To help you maintain an overview, all views are placed in folders called groups. A group can contain any number of views and, if required, subgroups.

Create and populate views for each view group, so that users (guards, supervisors, managers, etc.) can immediately start using the system as soon as you hand it over to the customer.

Enable and test hardware acceleration, if required.

See also: 18A. Create custom View Groups, 22. Configure users and security

Additional resources:

- XProtect Smart Client User Manual > Views (configuration) > Views (explained)
- XProtect Smart Client User Manual > Views (configuration)
- XProtect Smart Client User Manual > Views (configuration) > Adding content to views
- XProtect Smart Client User Manual > Views (configuration) > Add overlay buttons to views
- XProtect Smart Client User Manual > Views (configuration) > Assign shortcut numbers to views
- XProtect Smart Client User Manual > Enabling hardware acceleration
- eLearning: Getting Started with XProtect Smart Client

28E. Verify hardware decoding/performance

If the workstation has Quicksync support or has NVIDIA graphics cards installed, select a view, and verify the hardware decoding is working correctly by temporarily enabling Level 2 Video diagnostics overlay on the Smart Client Settings > Advanced menu.

See also: 28A. Check workstation hardware, software, and settings > Verify Intel Quicksync support, 28A. Check workstation hardware, software, and settings > Check NVIDIA graphic card drivers

Additional resources:

- XProtect Smart Client User Manual > Settings window (explained) > Advanced settings

28F. Create maps and Smart Map

Create maps and Smart Map, as required by the system design document.

> **Note:** Not all XProtect VMS versions include Smart Map functionality.

See also: 18B. Configure Smart Client Profiles > Configure Smart Map settings and locks

Additional resources:

- XProtect Smart Client User Manual > Maps (configuration)
- XProtect Smart Client User Manual > Smart maps (configuration)
- eLearning: Configuring and Using Maps

28G. Verify user logins and permissions

Select a user from each of the roles you have defined. In turn, log into the Smart Client as a user under each role and verify the permissions are correct for each of the functions below, as relevant for the installation.

- Verify tab and pane permissions for all tabs
- Verify Setup menu permissions
- Verify access to Views
- Verify camera access permissions
- Verify privacy mask lift permissions
- Verify PTZ control and priority
- Verify Bookmark permissions
- Verify events activation permissions
- Verify Export permissions
- Verify Evidence Lock permissions
- Verify alarm management permissions

Note: Not all XProtect VMS versions include all these functions.

See also: 18B. Configure Smart Client Profiles, 22. Configure users and security, 23. Define alarms

Additional resources:

- XProtect Smart Client User Manual > Getting to know your XProtect Smart Client > Simplified mode overview
- XProtect Smart Client User Manual > Advanced mode overview (Live tab)
- XProtect Smart Client User Manual > Tabs in XProtect Smart Client > Live tab (explained)
- XProtect Smart Client User Manual > Tabs in XProtect Smart Client > Playback tab (explained)
- XProtect Smart Client User Manual > Searching in XProtect Smart Client
- XProtect Smart Client User Manual > Privacy Masking > Lift and apply privacy masks
- XProtect Smart Client User Manual > PTZ and fisheye lenses > PTZ images (explained)
- XProtect Smart Client User Manual > Bookmarks (configuration)
- XProtect Smart Client User Manual > Events (explained)
- XProtect Smart Client User Manual > Creating video evidence
- XProtect Smart Client User Manual > Alarms (explained)

28H. Verify audio permissions

Verify audio permissions for each microphone and speaker, if you are using audio in the system.

Check device microphone playback

Verify that users who should *not* be able to listen to incoming audio do not have access to the microphone device.

Verify that users who *should* be able to listen to incoming audio have access to the device and that audio is coming out of the speakers/headset as/when intended.

Evaluate if the sound quality and volume are satisfactory.

Verify for each camera in each view that the correct audio channel is playing back when the camera is selected.

Check device speaker output

Verify that users who should *not* be able to use outgoing audio do not have access to the speaker device.

Verify that users who *should* be able to use outgoing audio have access to the device, and that audio is coming out of the hardware device (i.e., the camera, encoder, or audio module) speaker when the user presses the TALK button and speaks into the microphone on the workstation.

Evaluate if the sound quality and volume are satisfactory.

Verify for each camera in each view that the correct speaker is selected when the camera is selected.

See also: 16. Configure microphones and speakers, 22. Configure users and security

Additional resources:

- XProtect Smart Client User Manual > Audio (configuration)
- XProtect Smart Client User Manual > Views (configuration) > Add overlay buttons to views

28I. Verify Smart Wall permissions

Verify permissions of any Smart Walls you have defined in the system.

Verify Smart Wall presets

Verify control of all Smart Walls, including testing each Smart Wall preset.

See also: 18D. Configure Smart Walls, 28G. Verify user logins and permissions

Additional resources:

- XProtect Smart Client User Manual > XProtect Smart Wall (configuration)

28J. Configure Smart Client Options

In addition to system administrators being able to customize the Smart Client features and settings for each role through Smart Client Profiles, users themselves are able to change any setting that isn't locked by the Smart Client Profile via the Settings menu.

However, a few settings that are directly tied to the workstation hardware accessories (such as joystick, keyboard shortcut, and alarm notification settings), are configurable directly in the Smart Client only when logged in as the user the settings should apply to.

Configure joystick settings

For relevant users and workstations, log in as the user (or have the user log in) and configure joystick settings on the Smart Client Settings > Joystick menu.

Because the capabilities of attached joysticks may vary, joystick settings are specific to the user and the workstation. If the user will be logging into multiple workstations that have joysticks attached, these settings are saved as independent profiles and therefore must be configured on each workstation.

Configure keyboard shortcuts

For relevant users and workstations, log in as the user (or have the user log in) and configure keyboard shortcuts on the Smart Client Settings > Keyboard menu.

Because keyboard layouts and capabilities may vary, keyboard settings are specific to the user and the workstation. If the user will be logging into multiple workstations, these settings are saved as independent profiles and therefore must be configured on each workstation.

Configure alarm sound notification

For relevant users and workstations, log in as the user (or have the user log in) and configure whether alarm sound notifications should be played back in the workstation speakers on the Smart Client Settings > Alarm menu.

Because not all workstations may have sound cards or speakers, or may be used for different purposes, Alarm notifications are specific to the user and the workstation. If the user will be logging into multiple workstations, these settings are saved as independent profiles and therefore must be configured on each workstation.

Verify Smart Client time zone settings

While you are logged in as a user, double-check that the time zone settings are configured as intended.

Even if the time zone setting is configured and locked through the Smart Client profile, this is an extra verification that the time the user will see, and will export evidence as, is correct.

See also: 18B. Configure Smart Client Profiles, 22C. Create Roles

Additional resources:

- XProtect Smart Client User Manual > Settings window (explained)
- XProtect Smart Client User Manual > Settings window (explained) > Joystick settings
- XProtect Smart Client User Manual > Settings window (explained) > Keyboard settings
- XProtect Smart Client User Manual > Settings window (explained) > Alarm Manager settings
- XProtect Smart Client User Manual > Settings window (explained) > Advanced settings

29. Configure Web Client

29A. Create browser shortcut

Create a browser and desktop shortcut on the laptop or workstation for all users who will be accessing the XProtect VMS through the XProtect Web Client.

See also: 25. Configure Mobile servers

29B. Verify user logins

Click the XProtect Web Client shortcut on the user laptop or workstation (see the previous step) to verify that it works correctly. Log in as the user (or have the user log in) and verify the user has access to the relevant features and camera views (and only those).

See also: 22C. Create Roles > Configure client permissions and login authorization requirement

Additional resources:

- XProtect Mobile client user manual > Get started
- eLearning: Getting Started with the XProtect Web Client

30. Configure Mobile client

30A. Install app from relevant online marketplace

Make sure all users who will be accessing the XProtect VMS through the XProtect Mobile client install the XProtect Mobile app on their mobile device.

You can simplify this process by sending the users a Smart Connect notification email.

See also: 25C. Configure connectivity settings > Configure Smart Connect

30B. Verify user logins

Verify that each user is able to log into the system from their mobile device. Verify the user has access to the relevant features and camera views (and only those).

See also: 22C. Create Roles > Configure client permissions and login authorization requirement

Additional resources:

- XProtect Mobile client user manual > Log in to the XProtect Mobile app

30C. Test Video Push

Verify that Video Push works for each user who has been given access to the feature.

See also: 25F. Configure Video Push

Additional resources:

- XProtect Mobile client user manual > Streaming video from your mobile device (explained)
- XProtect Mobile client user manual > Stream video from your device to your surveillance system

30D. Verify Push Notifications

Verify that Push Notifications works for each user who has been given access to the feature.

Make sure the Push Notifications settings on the user's mobile device is correct for the functionality you intend them to have.

See also: 25G. Configure Push Notifications

Additional resources:

- XProtect Mobile client - User manual > Turn on or turn off notifications
- XProtect Mobile client - User manual > Connection settings for a XProtect Mobile server > Notification settings
- XProtect Mobile client - User manual > React to a notification

31. Hand off to the customer

31A. Perform a walk test for all cameras with motion detection

For all cameras that are set to record, or in other ways use video motion detection for event control, walk through all areas where you need the camera to detect motion. Make sure to cover edges of the area and repeat the test walking both directions, as appropriate.

Be careful not to walk or move faster than typical motion in the field of view would be, as faster motion more easily triggers detection. If the light condition varies significantly (for example, night and day), repeat the test under as many different conditions as you can.

If a camera is installed for a specialized purpose, you should adapt the test to the best fit. For example, if the camera is intended primarily for recording vehicle traffic, you should drive rather than walk for that test.

Confirm or re-adjust motion detection settings for each camera

Confirm, either by looking at the recordings (if recording on motion detection) or by having a colleague monitor the motion detection level in real time during the walk test, that the motion is detected correctly and that false detections are at a minimum.

Adjust the settings as necessary and re-do the test. Evaluate if the results are satisfactory or if the motion detection needs to be supplemented or replaced with other detection options to meet the surveillance objectives specified in the system design document.

31B. Create a configuration report

Create a configuration report to go with the installation documentation on the System Dashboard > Configuration Reports node in the XProtect Management Client. Make sure to fill out the Front Page information as completely as possible, including adding your company logo. Include only report categories where you have made configurations in the export.

The configuration report is a great document to supplement all your other project and installation documentation, and it includes fields both you and the customer can sign as part of the Final Acceptance Test handover process.

31C. Make a configuration backup

Make a backup of the configuration with the File > Configuration Backup function.

The configuration backup is a convenient tool to have in case the system has to be reverted to the original configuration after the handover to the customer. Take a copy with you for safekeeping and leave a copy by the management server for convenience.

If you are using a full version of Microsoft SQL (i.e., not SQL Express), Milestone highly recommends you also set up scheduled backups of the SQL database to a separate location, so you will always have a recent copy to revert to in case of a catastrophic event.

31D. Perform Final Acceptance Test

Perform a Final Acceptance Test (FAT) with the customer, covering all the relevant items in this document.

Following the FAT, both you and the customer may sign the document to confirm you agree the system is installed and configured in accordance with the system design document agreed upon at the start of the project.

31E. Perform customer operator and staff training

A well-trained customer staff is essential for a successful customer experience and future business.

Train the customer's system administrators to the agreed-upon level.

Train the customer's user staff (guards, operators, super-users, supervisors, managers, etc.) who will be using the XProtect VMS on a daily or occasional basis to monitor, investigate, and export evidence.

You may also consider utilizing the free operator eLearning available on Milestone's website.

31F. Confirm Statement of Work fulfilment

Following the FAT and customer training, the customer should confirm the Statement of Work (SOW) is completed and sign off on the handover document to close the project.

See also: 15H. Configure software Motion Detection, 15I. Configure camera events, 32G. Perform SQL server maintenance, 32I. Manage profitability and customer expectations

Additional resources:

- XProtect VMS Administrator manual > Site Navigation: System dashboard > Configuration reports (explained)
- XProtect VMS Administrator manual > Backing up and restoring system configuration > Backing up and restoring your system configuration (explained)
- Customer Learning Portal - learn.milestonesys.com
- XProtect VMS Administrator manual > Backing up and restoring system configuration > Scheduled backup and restore of system configuration (explained)

32. Additional XProtect VMS service, upgrade, and expansion proficiencies

32A. Replace a hardware device

If you need to replace a hardware device (because the old device has stopped working or you are upgrading to an improved device from the same or a different manufacturer), the Replace Hardware wizard allows you to retain many of the settings from the old device as well as all recordings, View Group settings, and user permissions.

On the Servers > Recording Servers node in the Management Client, select the Recording Server the old device is installed to. Right-click on the old device and select Replace Hardware to start the wizard.

Additional resources:

- XProtect VMS Administrator manual > Replace hardware

32B. Move a hardware device to another Recording Server

If you need to move a hardware device to a different Recording Server, the Move Hardware wizard allows you to do so while retaining all settings and all recordings.

On the Servers > Recording Servers node in the Management Client, select the Recording Server the hardware device is currently installed to. Right-click on the device and select Move Hardware to start the wizard.

> **Note:** When moving a device, any users viewing the live feed from that device may experience a short interruption until the client updates with the new location of the device.

> **Note:** Existing recordings are not moved. When a user accesses those recordings, the new recording server connects to the original recording server via port 5210 and streams the recordings to the user client.

See also: 12C. Configure Recording Server storage settings

Additional resources:

- XProtect VMS Administrator manual > Move hardware

32C. Save and load a system configuration

You can make a manual backup of the system configuration at any time.

To load a system configuration backup, you must be working directly on the Management Server desktop, either locally or by remote desktop connection.

Right-click the Management Server notification area tray icon and select Restore Configuration to start the process.

See also31C. Make a configuration backup, 5F. Verify the server is running

Additional resources:

- XProtect VMS Administrator manual > Backing up and restoring system configuration > Restore system configuration from a manual backup

32D. Configure the Download Manager

The Download Manager determines what is available on the Management Server download web page.

Install Server-Side installers

You can add additional components to the download web page by downloading a server-side installer for that component from the Milestone website download section.

For example, you may want to download and install "Server-Side XProtect Smart Client 64-bit" for a newer product version to allow users to upgrade their Smart Client to the new version before you upgrade the servers to maintain maximum compatibility and minimize interruptions to the production environment.

Manage access to downloads

You can manage what components are made available on both the user application installation page and the administrator application installation page through the Download Manager.

The Download Manager is a separate application that is installed automatically along with the Management Server.

Start the Download Manager from the application start menu/page when connected directly to the Management Server (locally or by remote desktop connection).

See also: 28C. Download and run Smart Client installer from the Management Server

Additional resources:

- XProtect VMS Administrator manual > Download Manager/download web page

32E. Upgrade the system

To upgrade to a larger product within the XProtect VMS family, if the system is already on the same version as the license you have for the larger version, simply load the license file to enable the features.

The process for upgrading the system to a newer version of the same or larger XProtect VMS product is the same and, with a few additions, similar to installing the product for the first time. When upgrading, the configuration is retained from the current version.

Prepare to upgrade to a new version

When upgrading the software, you should pay special attention to:

- Verify the newer XProtect VMS version is supported with the Windows version currently running on servers and workstations.
- Verify if the newer XProtect VMS version requires upgrading other software, such as .NET or DirectX, on servers or workstations. Also, verify if the newer XProtect VMS version supports the version of SQL server currently installed (see below).
- For systems where users are depending on accessing the servers immediately after the upgrade, you must upgrade all XProtect Smart Clients to the new version **before** installing the server software. This will allow you to upgrade clients at times convenient to users and, critically, ensure the clients will work with the new server versions.
- Save the system configuration and retain a copy in a safe location.
- Make or verify you have an up-to-date backup of the SQL database.
- Verify what user accounts are currently used for the Management Server, Recording Server, and Failover Server services. If these differ from the default option (NETWORK SERVICE), you must select the custom installation option for that component and verify the new installation uses the same user.
- Determine how to handle existing log files when upgrading from 2018R2 or older to 2018R3 or newer.
- Determine if and when to enable management server and recording server communication encryption when upgrading from 2019R1 or older to 2019R2 or newer.

> **Note:** If you are upgrading from XProtect VMS version 2017R3 or older to version 2018R1 or newer, make sure to determine if you need to install the legacy device pack before installing recording servers and failover recording servers.

Additional considerations when upgrading a multi-server workgroup environment:

- In a multi-server workgroup installation, all server services (Management Server, Recording Servers, etc.) should usually be installed to run under user accounts with the same user name to ensure the System Monitor and Customer Dashboard functions work correctly.
- If the server services are currently running under different user account names for a reason—for example to have access to a NAS or and external SQL database—you should also verify what user account the Milestone Data Collector service is running under. This would usually be an account with the same user name as that used for the Management Server. Make sure to replicate these settings for the upgrade installation.
- If the server services are installed under the NETWORK SERVICE, the Data Collector service is likely not working (if the current version has that feature). To make it work after the upgrade (if that is required), make sure to install all servers to run under user accounts with the same user name, or manually change the user of the Data Collector service to match that of the Management Server after completing the installation.

Upgrade the SQL server

If the SQL server needs to be upgraded (only necessary if the current version is not supported by the new version), the process depends on the circumstances for the installation:

- If you are currently using SQL Express installed on the management server itself, simply choose to install the new version and use the existing database in the Management Server installer.
- If you use a full version of SQL or if SQL Express is not installed on the management server itself, you must upgrade it manually prior to running the Management Server installer.

Note: In XProtect® 2018 R3 there is no option from the Management Server tray icon to change the location of the Log Server SQL. Milestone has published a KB describing a workaround.

Handle old log entries

If you are upgrading from XProtect VMS version 2018R2 or older to version 2018R3 or newer, the old log files are not carried over due to new functionality added in 2018R3. This change has several implications when upgrading:

- If the old logs are important to you, Milestone recommends you export them before upgrading. They will not be accessible via the Management Client after the upgrade. If exporting the logs is not an option and access is nevertheless required after upgrading, Milestone has published a KB article describing a workaround to access the logs though a separate installation of a free XProtect Essential+ 2018R2.
- The old logs are not deleted automatically from SQL and will stay there until manually deleted. If you need to free up space before upgrading you can shrink the log files by setting the maximum number of log entries to "1" for each of the logs in Tools > Options > Server Logs and wait for an hour or so for the log cleanup process to execute before upgrading.

If you are upgrading from XProtect VMS version 2019R1 or newer, and the system was previously upgraded from version 2018R2 or older, Milestone recommends checking whether the old log files are still present in the SQL database. If found, and if it there is no longer a requirement to retain them, the old log database should be deleted from the SQL server.

Handle Mobile Server HTTPS certificates

If you are upgrading from XProtect VMS version 2019R1 or older to version 2019R2 or newer:

Starting with XProtect VMS version 2019R2, XProtect Mobile no longer includes the option to use auto-generated self-signed certificates for HTTPS encryption for client communication. Instead, a certificate must be implemented using a trusted CA the same way as for other system components.

Install (upgrade to) a new version

Milestone recommends you install the new version in this order to upgrade:

- Upgrade all Smart Clients for all users depending on access to the system after the upgrade. Milestone recommends using the Download Manager and Software Upgrade Manager to more easily complete this.
- Install (upgrade) the Management Server. Make sure to select to re-use the existing SQL database.
  Note that the user performing the install must have sysadmin privileges on the SQL server.
- Install (upgrade) Management Clients on workstations you will be using during the upgrade.
- Install (upgrade) Failover Recording Servers.
- Install (upgrade) Recording Servers.
- Install (upgrade) XProtect Mobile servers.
- Install (upgrade) any remaining XProtect Smart Clients.
- Install (upgrade) any remaining Management Clients.
- Install (upgrade) XProtect Mobile clients.
- In the Management Client Tools > Options > Server Logs, clear the "Allow 2018 R2 and earlier components to write logs" check box (if selected) unless it is still required.
- Verify everything is working correctly.
- Save the system configuration and retain a copy in a safe location.

Note: If you are upgrading from XProtect VMS version 2018R1 or older to version 2018R2 or newer, all management and client access to older Recording Servers will be lost once the new Management Server is installed unless these have been patched with hotfix 162666. To avoid this, either install the hotfix or download and install the XProtect VMS 2018R2 Recording Servers before installing the Management Server.

Note: If the XProtect VMS version you are upgrading from is significantly older (e.g., several years) than the version you are upgrading to, you should contact Milestone Technical Support to verify what the best approach is.

Note: If you are upgrading from an XProtect Professional VMS system (XProtect Essential, XProtect Express, XProtect Professional, or XProtect Enterprise), you should refer to the directions in the system migration guide (see resource list) and proceed to install the XProtect VMS as a new installation.

See also: 3B. Install operating system environment, 3I. Check additional server software and settings, 28A. Check workstation hardware, software, and settings, 32D. Configure the Download Manager, 28C. Download and run Smart Client installer from the Management Server, 32G. Perform SQL server maintenance, 32C. Save and load a system configuration, 3A Obtain or create server communication encryption certificates, 12F enable certificates, 5. Install XProtect Management Server, 9. Install XProtect Management Clients, 8. Install XProtect Failover Recording Servers, 7. Install XProtect Recording Servers, 6. Install XProtect Mobile server, 30A. Install app from relevant online marketplace

Additional resources:

- XProtect VMS Administrator manual > Upgrade (explained)
- XProtect VMS Administrator manual > Upgrade best practices
- XProtect VMS Administrator manual > Before you start installation > Device drivers (explained)
- XProtect VMS Administrator manual > Site Navigation: Server logs > Export logs
- XProtect VMS Administrator manual > Site Navigation: Server logs > Allow 2018 R2 and earlier components to write logs
- XProtect VMS system migration guide
- Knowledge base article 000004420: XProtect® VMS: .NET security vulnerability (hotfixes for 2016 R1 - 2018 R1)
- Troubleshooting assistant: Milestone Support hotfix 261666 installation walkthrough
- Knowledge base article 000006988: How to access old logs on a new XProtect 2018 R3 installation

32F. Explain and manage key system behaviors

Milestone has identified a number of key system behaviors you should understand and be able to explain to the customer's system administrators, risk managers, and Smart Client users.

Explain daylight-saving behavior

Explain the daylight-saving behavior of the XProtect VMS as it applies in spring and fall.

Explain how to search for evidence in the "hour that occurs twice" when daylight saving is adjusted back an hour.

Explain risks and possible consequences if the Windows time on a server or a client workstation uses different daylight-saving settings than the rest of the system.

Explain cold and hot failover server behavior

Explain the difference between cold and hot failover server.

> **Note:** Not all XProtect VMS versions include failover server functionality.

Additional resources:

- XProtect VMS Administrator manual > Daylight saving time (explained)
- XProtect VMS Administrator manual > Site Navigation: Servers and hardware: Failover servers > Failover recording server (explained)

32G. Perform SQL server maintenance

Backup SQL database

In addition to backing up the configuration manually from the Management Client, you can also back it up directly on the SQL server using Microsoft® SQL Server Management Studio. This also allows you to back up log files (including audit logs), if desired.

If you are using a full version of Microsoft SQL (i.e., not SQL Express), Milestone highly recommends you also set up scheduled backups of the SQL database to a backed-up location, so you will always have a recent copy to revert to in case of a catastrophic event.

Shrink SQL transaction log

Each time SQL makes a database change, it also logs this in its transaction log. A configuration change in the Management Client or Smart Client, or an entry in the XProtect VMS log, results in one or more entries or changes in the SQL database.

In systems with a lot of activity, the transaction log builds up over time and may reach a point where it has filled up the disk, potentially causing Windows to stop working.

To avoid such a scenario, Milestone recommends you monitor the available disk space on your SQL server and, as necessary, shrink the SQL Server transaction log at regular intervals using Microsoft® SQL Server Management Studio.

Additional resources:

- XProtect VMS Administrator manual > Backing up and restoring system configuration > Scheduled backup and restore of system configuration (explained)
- How to schedule and automate backups of SQL Server databases in SQL Server Express - support.microsoft.com
- Understanding SQL Server Backups - docs.microsoft.com
- Shrinking the Transaction Log - docs.microsoft.com

32H. Perform critical server maintenance

Milestone has identified a number of critical maintenance tasks you should be prepared to execute as part of a planned system maintenance or expansion, or in case of a major failure.

Replace a (failed) management server

If the XProtect Management Server is running in a virtualized environment, using the tools available within this environment is usually the fastest way to migrate the Management Server.

If the XProtect Management Server is running in a non-virtual environment, and the server is still running (or you have a current backup) and the hardware and software configuration should remain the same, backing up and restoring the entire server installation may be the easiest and fastest way to migrate to a new server.

If none of these situations apply:

- Make a configuration backup or locate the most recent configuration backup file.
- Install the XProtect Management Server on the new server.
- Restore the backed-up system configuration to the new system.

Replace a (failed) recording server

If the recording server is still working and you simply want to replace it with different hardware, the best approach is to install the Recording Server as a new server, configure the storage, and move the hardware devices to the new server using the Move Hardware wizard.

Once you reach the maximum retention time of all the storage configurations on the old server, you should use the Management Client to delete it from the system before taking the old server offline.

If a recording server is malfunctioning and you want to replace it with a new server that inherits the settings of the old Recording Server, follow these steps:

- Remove the old recording server from the network or take other steps to make sure it will never be online at the same time as the new recording server.
- Retrieve the Recording Server ID from the old recording server (the server does not need to be online).
- Install the XProtect Recording Server software on the new recording server.
- Stop the Recording Server service on the new recording server.
- Replace the Recording Server ID on the new recording server.
- Start the Recording Server service on the new recording server. The new Recording Server will automatically retrieve the configuration of the old Recording Server from the Management Server.
- Verify everything is working as intended. Make particularly sure the storage configuration matches the hardware and storage configuration on the new recording server.

Replace a storage system

When replacing a storage system on a running recording server, Milestone recommends you keep the existing storage system running in parallel and follow these steps to ensure all recordings remain intact and available to users:

- Create new storage configuration settings on the Servers > Recording Servers > Storage tab for the new storage system.
- Move all devices to the new storage system (on the Record tab for each device or device group).
- After you reach the maximum retention time of all the storage configurations on the old storage system, you can remove the storage configurations from the Recording Server and take the old storage system offline.

If a storage system has experienced a catastrophic failure and you are unable to bring it back online, do the first two steps. The final step does not apply since the storage no longer is available and all recordings are lost.

See also: 3. Configure Windows servers, 5. Install XProtect Management Server, 32C. Save and load a system configuration, 7. Install XProtect Recording Servers, 32B. Move a hardware device to another Recording Server, 12C. Configure Recording Server storage settings, 15E. Configure recording > Select recording storage

Additional resources:

- XProtect VMS Administrator manual > Moving the management server
- XProtect VMS Administrator manual > Replace a recording server

32I. Manage profitability and customer expectations

Good project management, and by extension good project documentation, is key to maintaining customer expectations and project profitability, both of which are, of course, critical to grow the business.

Explain the importance of a Statement of Work (SOW)

When finalizing the project documentation prior to the installation, be sure to include a detailed Statement of Work (SOW). The SOW sets the customer's expectations in writing, with specific details on how the project will be installed. Any work requested by the customer beyond what is documented is a change order and additional billable work.

A SOW may often be vague in the initial phase, gradually getting more detailed until a bid can be submitted and the project secured. After that, the SOW should get more detailed as the customer's requirements are settled in full until the point when it contains a full "to-be-built" specification the integrator and customer can both sign off on.

For the part of the project that applies to the Milestone system, the SOW (or more commonly in larger projects, a sub-document or appendix to the SOW) should contain sufficient detail in all sections of the document to enable the installation team to install the system from the document with minimal interaction from the customer.

The SOW also provides the template for the final acceptance test.

Explain the importance of acceptance testing (Final Acceptance Test, FAT)

The Final Acceptance Test (FAT) is the last step before the customer takes ownership of the installation.

If sufficiently detailed, the SOW and the associated sequential checklist (i.e., this document) contain everything that was agreed upon when the customer accepted the scope and price of the proposed project.

Going through each of the steps in the SOW together with the customer is your proof that the project delivered is the project the customer bought.

Getting the customer's signature on the FAT document swiftly and without need for major corrections is therefore key in closing the project to everyone's satisfaction and, typically, critical for the customer to release the final payment to your company.

It is also a great time to suggest and secure a contract for additional work that might not have been included in the original project (including change orders) or that addresses additional needs the customer might have.

See also: 31D. Perform Final Acceptance Test, 31F. Confirm Statement of Work fulfilment

Additional resources:

- Statement of work - Wikipedia.org
- Acceptance testing - Wkipedia.org