Milestone Systems

Migrating from XProtect® Enterprise
to XProtect® Advanced VMS

System Migration Guide

milestone

The Open Platform Company

Contents

Copyright, trademarks and disclaimer

Copyright

Trademarks

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

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

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

Disclaimer

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

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

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

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

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

Introduction

Milestone's premium IP video platform, XProtect® Advanced VMS, raises system operation for large installations to new heights of flexibility and ease-of-use.

Organizations currently using XProtect® Enterprise—Milestone's other comprehensive multi-server IP video management system—may want to migrate to XProtect Advanced VMS for even greater flexibility, including:

- Fully distributed server architecture
- Innovative centralized management
- Failover redundancy
- Milestone Federated Architecture™
- Time based user rights
- Smart Wall functionality

Before surveillance system administrators begin migrating complex video surveillance setups in mission-critical environments, it is natural for them to ask for example:

- How to prepare the upgrade?
- How to ensure access to recordings from both the old and the new systems?
- To what extent can existing hardware be used?

This migration guide provides the answers, including:

- Information about reuse of existing hardware
- Important points to consider before migrating
- Best-practice advice on how to go about the upgrade, including a suggested strategy for temporarily integrating existing XProtect Enterprise setups into XProtect Advanced VMS, thus providing access to recordings from both old and new systems for as long as required
- Useful tips.

Product overview

This system is a fully distributed solution, designed for large multi-site and multiple server installations requiring 24/7 surveillance, with support for devices from different vendors. The solution offers centralized management of all devices, servers, and users, and empowers an extremely flexible rule system driven by schedules and events.

Your system consists of the following main elements:

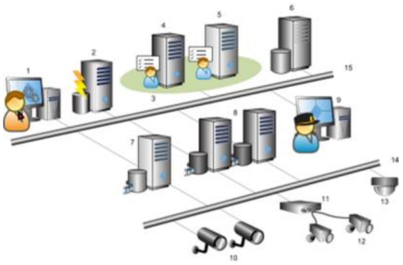
- The **management server** - the center of your installation
- One or more **recording servers**
- One or more **Management Clients,** which are unlicensed and can be downloaded and installed for free (as many times as needed).
- A **Download Manager**
- One or more **XProtect® Smart Clients**, which are unlicensed and can be downloaded and installed for free (as many times as needed). Possibly also one or more **XProtect Web Clients** and/or **Milestone Mobile clients**, which are also free of charge.

Your system also includes fully integrated Matrix functionality for distributed viewing of video from any camera on your surveillance system to any computer with XProtect Smart Client installed.

The system also offers the possibility of including the standalone XProtect® Smart Client – Player when you export video evidence from the XProtect Smart Client. XProtect Smart Client – Player allows recipients of video evidence (such as police officers, internal or external investigators, etc.) to browse and play back the exported recordings without having to install any software on their computers.

Finally, your system handles an unlimited number of cameras, servers, and users—across multiple sites if required. Your system can handle IPv4 as well as IPv6.

A typical system setup



Example of a system setup. The number of cameras and recording servers, as well as the number of connected clients, can be as high as you require.

Legend:

1. Management Client(s)
2. Event server
3. Microsoft cluster
4. Management server

5. Management failover server
6. SQL server
7. Failover recording server
8. Recording server(s)
9. XProtect Smart Client
10. IP video cameras
11. Video server
12. Analog cameras
13. PTZ IP camera
14. Camera network
15. Server network

Management server

What? Stores the surveillance system's configuration in a relational database, either on the management server computer itself or on a separate SQL Server on the network. Also handles user authentication, user rights, etc. To enhance system performance, several management servers can be run as a Milestone Federated Architecture™.

Where? Runs as a service, and is typically installed on a dedicated server.

- **What comes along with the management server?** When you install the management server, you also get the following integrated components as well (if you select a single server management server installation):

  The **event server**

  - **What?** Stores and handles incoming alarms and map functionality, and receives analytic and generic events from system servers (including any XProtect servers in a possible federated hierarchy). This enables powerful monitoring and instant overview of alarms and maps and possible technical problems within your systems. If your setup does not have an event server installed, neither of the features mentioned under this bullet will work.
  - **Where?** Usually installed on the same server as the management server and runs as a service.

  The **log server**

  - **What?** Provides the necessary functionality for logging information from your system.
  - **Where?** Usually installed on the same server as the management server and runs as a service.

  The **service channel**

  - **What?** Enables automatic and transparent configuration communication between servers and clients in your system.
  - **Where?** Usually installed on the same server as the management server and runs as a service.

Recording server

What? Used for recording video and for communicating with cameras and other devices. In large installations, more than one recording server is often used on the surveillance system. Failover recording servers can be set up to take over if a recording server becomes temporarily unavailable.

Where? Recording servers as well as failover recording servers run as services, and are typically installed on separate servers rather than on the management server itself.

Management Client

What? Feature-rich administration client for configuration and day-to-day management of the system. Available in several languages.

Where? Typically installed on the surveillance system administrator's workstation or similar.

Download Manager

What? Lets surveillance system administrators manage which system-related components (e.g. particular language versions of clients) your organization's users will be able to access from a targeted web page generated by the management server. Refer to Download Manager/download web page.

Where? Automatically installed on the management server during the installation process.

Access clients

- **XProtect Smart Client**

  What? XProtect Smart Client is the main client application that provides intuitive control over your system setup. It gives access to live and recorded video, instant control of cameras and connected security devices, and a comprehensive overview of recordings. It has an adaptable user interface that can be optimized for individual operators' tasks and adjusted according to specific skills and authority levels.

  Where? XProtect Smart Client must be installed on all client computers.

  How? Users connect to the management server for initial authentication, then transparently to the recording servers for video recordings, etc.

- **XProtect Web Client**

  What? XProtect Web Client is a web-based client application for viewing, playing back and sharing video. It provides instant access to the most commonly used functions, and is quick to learn and simple to operate for users of all levels. It connects to your setup through almost any browser and computer.

  Where? XProtect Web Client is free of charge and does not have to be installed on any client computer(s). However, you must integrate one or more Milestone Mobile servers in your XProtect® setup.

How? Users access XProtect Web Client via a URL (using the IP-address of the Milestone Mobile server) and may monitor the XProtect system from any computer or tablet connected to the Internet.

- **Milestone Mobile client**

  What? Milestone Mobile client is a mobile application which allows you to view live video from one or multiple cameras, use Video push, play back video recordings, and more.

  Where? Milestone Mobile client is free of charge and must be installed on users' smartphones or tablets (or even portable music players running iOS) from management server's download web page. You must integrate one or more Milestone Mobile servers in your XProtect setup.

  How? The Milestone Mobile client is available for free download on Google Play and the App Store℠ .

Integrate XProtect Enterprise

In addition to the elements in the illustration in Access during migration (on page 18), it is also possible to add existing XProtect Enterprise servers to an XProtect Advanced VMS system. When this is the case, the XProtect Enterprise servers will run as slave servers on the XProtect Advanced VMS system.

Although you cannot re-use XProtect Enterprise configuration or databases in XProtect Advanced VMS, you can run XProtect Enterprise servers as slave servers under XProtect Advanced VMS. This allows users to be connected to the XProtect Advanced VMS system and to view video from XProtect Enterprise servers too.

That way, you are able to provide users with access to recordings from both systems, and gradually phase out use of XProtect Enterprise servers and their recordings as they become obsolete. This method is described in Access during migration (on page 18).

What to consider before migrating

Before migrating, ask yourself the following questions:

Reuse existing servers?

XProtect Advanced VMS is a fully distributed system. As many recording servers as required can run under an XProtect Advanced VMS management server. And each of the recording servers can run as many cameras as required. The same applies for failover servers.

XProtect Advanced VMS's administration interface can be installed as a client on any computer. When migrating to XProtect Advanced VMS you may also use the occasion to rethink and optimize the way you use your servers.

Consequently, minimum system requirements for running XProtect Enterprise and XProtect Advanced VMS servers differ only slightly. In many cases, you are able to reuse your existing servers. See the following minimum system requirements for relevant components:

Computer running management server

Name	Description
CPU	Intel® Xeon®, minimum 2.0 GHz (Dual Core recommended)
RAM	Minimum 1 GB (2 GB or more recommended)
Network	Ethernet (1 Gbit recommended)
Graphics Adapter	Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
Hard Disk Space	Minimum 50 GB free (depends on number of servers, cameras, rules, and logging settings

Operating System	‣ Microsoft® Windows® 8 Enterprise (32 bit or 64 bit) ‣ Microsoft Windows 8 Professional (32 bit or 64 bit) ‣ Microsoft Windows 7 Ultimate (32 bit or 64 bit) ‣ Microsoft Windows 7 Enterprise (32 bit or 64 bit) ‣ Microsoft Windows 7 Professional (32 bit or 64 bit) ‣ Microsoft Windows Server 2012 (64 bit): Standard and Datacenter. ‣ Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. ‣ Microsoft Windows Server 2008 (32 or 64 bit) ‣ Microsoft Windows Server 2003 (32 or 64 bit) To run clustering/failover recording servers, you also need a Microsoft Windows Server 2003/2008 Enterprise or Data Center edition.
Software	Microsoft® .NET 3.5 SP1 and .NET 4.0 and Internet Information Services (IIS) 5.1 or newer

Computer running recording server or failover recording server

Name	Description
CPU	Dual Core Intel Xeon, minimum 2.0 GHz (Quad Core recommended)
RAM	Minimum 1 GB (2 GB or more recommended)
Network	Ethernet (1 Gbit recommended)
Graphics Adapter	Onboard GFX, AGP, or PCI-Express, minimum 1024 x 768, 16-bit color
Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
Hard Disk Space	Minimum 100 GB free (depends on number of cameras and recording settings)

Operating System	Microsoft® Windows® 8 Enterprise (32 bit or 64 bit) Microsoft Windows 8 Professional (32 bit or 64 bit) Microsoft Windows 7 Ultimate (32 bit or 64 bit) Microsoft Windows 7 Enterprise (32 bit or 64 bit) Microsoft Windows 7 Professional (32 bit or 64 bit) Microsoft Windows Server 2012 (64 bit): Standard and Datacenter. Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. Microsoft Windows Server 2008 (32 or 64 bit) Microsoft Windows Vista® Business (32 or 64 bit) Microsoft Windows Vista Enterprise (32 or 64 bit) Microsoft Windows Vista Ultimate (32 or 64 bit) Microsoft Windows Server 2003 (32 or 64 bit)
Software	Microsoft® .NET 4.0 Framework.

IMPORTANT: When you format the hard disk of a recording/failover recording server device, you must change its **Allocation unit size** setting from 4 to 64 kilobytes. This is to significantly improve recording performance of the hard disk. You can read more about allocating unit sizes and find help at http://support.microsoft.com/kb/140365/en-us.

Computer running XProtect Smart Client

Name	Description
CPU	Intel Core2 Duo, minimum 2.0 GHz (Quad Core recommended for larger views)
RAM	Minimum 512 MB (1 GB recommended for larger views, 1 GB recommended on Microsoft® Windows® Vista®)
Network	Ethernet (100 Mbit or higher recommended)
Graphics Adapter	AGP or PCI-Express, minimum 1280 x 1024, 16 bit colors
Hard Disk Space	Minimum 500 MB free

Operating System	- Microsoft® Windows® 8 Professional (32 bit or 64 bit*) - Microsoft Windows 8 Enterprise (32 bit or 64 bit*) - Microsoft Windows 7 Professional (32 bit or 64 bit*) - Microsoft Windows 7 Enterprise (32 bit or 64 bit*) - Microsoft Windows 7 Ultimate (32 bit or 64 bit*) - Microsoft Windows Server 2012 (64 bit): Standard and Datacenter. - Microsoft Windows Server 2008 R2 (64 bit): Standard, Web, High Performance Computing (HPC), Enterprise, and Datacenter. - Microsoft Windows Server 2008 - Microsoft Windows Server 2003 (32 bit or 64 bit*) - Microsoft Windows Vista Ultimate (32 bit or 64 -bi*) - Microsoft Windows Vista Enterprise (32 bit or 64 bit*) - Microsoft Windows Vista Business (32 bit or 64 bit*) - Microsoft Windows XP® Professional (32 bit or 64 bit*). *Running as a 32 bit service/application
Software	Microsoft® .NET 4.0 Framework, DirectX 9.0 or newer, and Windows Help (WinHlp32.exe) which you can download from http://www.microsoft.com/downloads/.

Reuse existing cameras?

Although XProtect Advanced VMS already supports more than 1500 different camera models, it currently does not support as many different camera makes and models as XProtect Enterprise. This is due to the fact that the camera drivers need to be ported from one platform to another.

Before migrating, it is important that you verify that the cameras used in your XProtect Enterprise setup is also supported by XProtect Advanced VMS. This is quickly verified on the Milestone website. Go to www.milestonesys.com's **Support and Services** > **Support** > **Supported Hardware** and find your relevant software version.

When verifying your cameras, also verify that required functionality (e.g. input) is supported. There are slight differences in the way exact functionality of certain cameras is supported by XProtect Advanced VMS compared to XProtect Enterprise.

If a camera you require is not currently supported by XProtect Advanced VMS, contact your Milestone representative. Support for the camera may be imminent; and if not, your Milestone representative will be able to forward a request for supported by XProtect Advanced VMS.

Reuse existing system configuration?

XProtect Advanced VMS is an altogether different system. You cannot import your existing XProtect Enterprise configuration for reuse in XProtect Advanced VMS. Cameras' recording settings, scheduling, etc. must be configured anew in XProtect Advanced VMS. Fortunately, this is made easy:

- When configuring XProtect Advanced VMS through the Management Client, you are able to group cameras, and configure common settings for all cameras within a group in one go.
- XProtect Advanced VMS uses the concept of time profiles, with which you can quickly and easily set up even detailed scheduling for your cameras.

XProtect Smart Client users should upgrade their XProtect Smart Clients to the latest version when migrating to XProtect Advanced VMS. The latest version is required in order to benefit from XProtect Advanced VMS features such as archiving schedules, user defined events, bookmarks, multicasting, edge storage, Smart Client profiles, system dashboard, video wall handling through XProtect Smart Wall (an add-on product), etc. Also, new Smart Client views containing the cameras from XProtect Advanced VMS must be created.

In XProtect Advanced VMS, roles determine which features users have access to. Roles with appropriate rights must therefore be defined through the Management Client. Once roles are defined, you can easily add users to the roles from Active Directory.

Downtime while migrating?

If you have an XProtect Advanced VMS management server and an XProtect Advanced VMS recording server with a camera configuration identical to that on your currently running XProtect Enterprise server, downtime can be avoided by running XProtect Advanced VMS in parallel with XProtect Enterprise during the switch.

Without parallel servers, it will not be possible to avoid downtime completely, although you can minimize the effects of downtime by performing the migration at night, during closing hours, or at another time at which video surveillance is not critical to your organization.

See also the smooth integration strategy outlined in Access during migration (on page 18). In short, the strategy involves installing and configuring an XProtect Advanced VMS recording server on the server previously running as XProtect Enterprise server.

Customized integrations to other applications

If customized integrations between your current XProtect Enterprise setup and other applications (for example access control systems, fire alarm systems, or similar) have been made through the Milestone Software Development Kit (SDK) and/or Application Programming Interface (API), the integrations should be carefully tested to verify that they will also work with XProtect Advanced VMS. Some customized integrations may have to be re-programmed.

When developers review your customized integrations for use with XProtect Advanced VMS, it is highly recommended that they work with the latest available Milestone SDK.

Tip: XProtect Advanced VMS features user-defined events, which let developers create customized surveillance system events based on data from other applications.

Important differences and more

A few other things to consider before migrating:

Recording frame rate

By default, XProtect Advanced VMS uses a recording frame rate of 5 frames per second. If you are used to a higher recording frame rate in your XProtect Enterprise setup (for example, XProtect Enterprise versions earlier than 7.0 store video recordings with the full frame rate), you may initially find that video from some or all cameras has a lower frame rate when recorded by XProtect Advanced VMS.

You can of course configure a higher recording frame rate for your cameras in XProtect Advanced VMS.

Remember that XProtect Advanced VMS lets you group cameras, and configure common settings for all cameras within a group in one go.

Archiving

Archiving is the automatic transfer of recordings from a camera’s default database to another location. This way, the amount of recordings you are able to store will not be limited by the size of the camera’s default database.

If you are using the archiving feature in your current XProtect Enterprise setup and have allocated disks for this purpose, it is possible to re-use these disks with XProtect Advanced VMS, as the disk specifications basically are identical for the two systems.

Different from XProtect Enterprise, the archiving process in XProtect Advanced VMS supports multi-stage storage architecture where the recordings can be archived again and again to new storage areas. The **Live** database is automatically segmented in 1 hour segments, keeping the size of the open **Live** databases as small as possible in order to keep a potential database repair after a failure as short as possible. Definition and configuration of **Live** databases and archives are defined as part of a **Storage Container**. Cameras that should store video or audio recordings are then set to use one of the defined storage containers, making the storage configuration on the individual devices very simple. In addition, it is possible to use the following features when archiving:

- **Signing:** can be enabled if you want to write a digital signature to database files containing recorded data. This allows the XProtect Smart Client and the XProtect Smart Client – Player to verify that the contents of imported and opened databases have not been tampered with and that no database files have been removed.

- **Encryption:** can be enabled per storage container which then encrypts video and audio data recorded in the live database from the cameras using the storage container. The encryption is kept and transferred with the recordings once they are archived. If the archiving function also grooms the video recordings the encryption is still kept as it is the individual records inside the database that are encrypted.

- **Grooming:** a method to decrease the frame rate of the recorded video over time in order to save space on the storage system while still keeping a record of what has happened in the past. XProtect Advanced VMS is able to groom video recordings each time they are archived.

As XProtect Advanced VMS supports multi-stage archive the grooming can be done as many times as there are archives, reducing the frame rate again and again over time. For JPEG recordings it is possible to groom to any frame rate lower than the frame rate currently recorded in the database, but for MPEG and H.264 recordings, grooming can only be done to key-frames and below (e.g. a key-frame every 1 second or less).

- **Background Repair:** the recording servers are able to repair the databases in the background, both in start-up scenarios and on the fly if it detects databases that might be corrupted. During a start-up with corrupted databases, these databases are moved to a subfolder where new databases are created and the recording server starts as normally. Once the recording server is up and running, these corrupted databases will be repaired in the background and merged into the new database. Users of the Management Client will experience corrupt databases that are being repaired as gaps in the recordings. Once the databases are repaired, one by one, their contained recordings will be browsable by the clients without any further actions. This function ensures that the start-up time for recording servers are the same regardless if there are corrupted databases that should be repaired or not.
- **System Monitor:** This offers an excellent overview of system information and makes it possible to create reports on all management servers, recording servers, failover servers, and cameras in your surveillance setup. All servers display/can report on CPU usage and available memory information. Furthermore, recording servers also display connection status information.

Archiving is not necessarily a must when using XProtect Advanced VMS. In case the hard disks you have allocated for the live database are fast enough and able to contain the expected amount of data, the system can run without archiving. This is possible due to the automatic 1 hour segment division of the live database, which keeps a potential database repair after a failure as short as possible, as only the last (hour) segment of the database needs to be repaired.

Virus scanning

For performance reasons it is highly recommended that you disable any virus scanning of camera databases and archiving locations. It is likely that virus scanning will use a considerable amount of system resources on scanning all the data being archived. Also, the virus scanning software may temporarily lock each file it scans. Not disabling virus scanning will in most cases result in considerable performance degradation.

Access during migration

One strategy/key issue when migrating is the ability to provide access to recordings from both the **old** and the **new** system.

XProtect Advanced VMS allows full integration of existing XProtect Enterprise (6.0 or later) setups, thus allowing you to provide access to recordings from both old and new systems for as long as required. The following checklist outlines what to do:

☑ You may check the boxes in this list as you go along.

□ **Install your XProtect Advanced VMS management server on a dedicated server.**

□ **Change your XProtect Enterprise Image Server service configuration** so it uses port 81 instead of port 80. This will prepare it for use with XProtect Advanced VMS.

□ Use XProtect Advanced VMS's Management Client to **add the XProtect Enterprise server to the XProtect Advanced VMS system as a slave**.

This will provide access to recordings from your existing XProtect Enterprise server through XProtect Advanced VMS, including archived recordings. If you have used archiving on your XProtect Enterprise server, you will potentially be able to supply old XProtect Enterprise recordings though your new XProtect Advanced VMS system for a considerable period of time.

Only XProtect Enterprise servers running XProtect Enterprise version 6.0 or later can be used as slaves on an XProtect Advanced VMS system.

How to add XProtect Enterprise servers: In the Management Client's **Tools** menu, select **Enterprise Servers…**, click **Add…**, specify the IP address/host name of the XProtect Enterprise server, specify port number (81), select required authentication method and specify/select a user identity with unlimited access to both the XProtect Enterprise and XProtect Advanced VMS systems, click **OK**.

When you have added the XProtect Enterprise server as a slave, you must let the XProtect Enterprise server know that authentication of users connecting with XProtect Smart Clients will now be handled by the XProtect Advanced VMS management server. You can do this through XProtect Advanced VMS's Management Client.

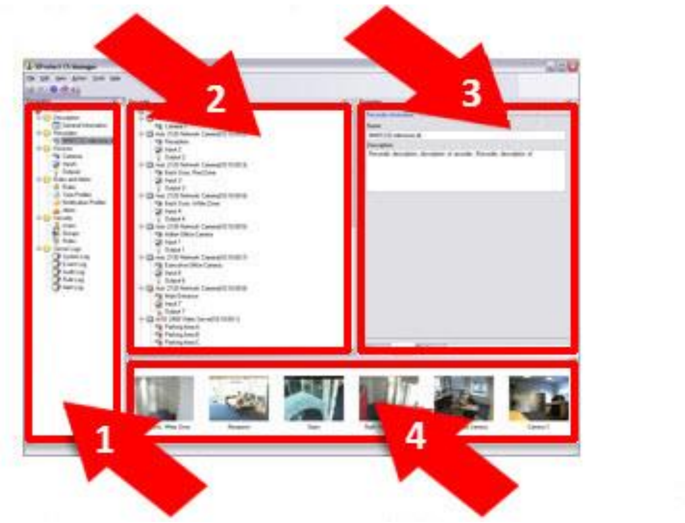
How to let XProtect Enterprise servers know: In the Management Client's **Tools** menu, select **XProtect Enterprise Servers…**, click **Network…**, and specify the LAN and/or WAN IP address of the XProtect Advanced VMS management server. If all involved servers are placed on your local network, you can just specify the management server's LAN address. If one or more involved servers access the system through an internet connection, also specify the management server's WAN address.

□ Use XProtect Advanced VMS's Management Client to **set up XProtect Advanced VMS roles**, and add users to them. When specifying the rights of the roles, make sure they get access to 1) the required cameras, including any PTZ features, 2) the required parts of the XProtect Smart Client, 3) the XProtect Enterprise server slave. This will allow users with the roles in question—from their XProtect Smart Clients—to view cameras from the XProtect Enterprise server through XProtect Advanced VMS.

How to add roles: In the Management Client's navigation pane, expand **Security**, right-click **Roles**, then select **Add Role…**

How to specify roles' rights: In the Management Client's navigation pane, expand **Security**, select **Roles**, and select the required role from the list in the overview pane. Specify required rights on the tabs in the properties pane. Exact requirements differ from organization to organization, but you should as a minimum define rights on the following tabs: **Device** (access to cameras), **Application** (access to XProtect Smart Client), and **Enterprise Server** (access to the XProtect Enterprise slave server). Repeat for each role you have added.

How to add users/groups to roles: In the Management Client's navigation pane, expand **Security**, select **Roles**, and select the required role from the list in the overview pane. Select the **Users and Groups** tab in the properties pane, then click **Add….**



1. Site Navigation Pane and Federated Sites Hierarchy Pane
2. Overview Pane
3. Properties Pane
4. Preview Pane

□ **Create new XProtect Smart Client views** identical to the ones your users already have for accessing the cameras from XProtect Enterprise. Only this time you create the views with the cameras coming through XProtect Advanced VMS.

Your users now have access to both the old and the new system. From this point they will not connect directly to the XProtect Enterprise server anymore, all client connections will take place through the XProtect Advanced VMS management server.

Tip: The entire XProtect Enterprise system will still run. Thus you have the safety of easily being able to revert back to it before you progress further, should any unexpected issues arise and require solving.

□ When you have verified that everything works to your satisfaction, you are ready to **install the XProtect Advanced VMS recording server which will eventually replace the XProtect Enterprise server**. You can install it on either the same physical server as the existing XProtect Enterprise server, or on a new server parallel to the existing XProtect Enterprise server.

If installing the XProtect Advanced VMS recording server on the same physical server as the existing XProtect Enterprise server, note that some of the required updates (such as .NET and the latest patches from Microsoft) are likely to require restart of the server.

Also note that if you install XProtect Advanced VMS recording server on the same physical server as the existing XProtect Enterprise server, while the XProtect Enterprise server is recording, the installation is likely to take considerably longer than if the XProtect Enterprise server is temporarily stopped. This is simply a question of CPU and disk load.

Remember to authorize each recording server through the Management Client. By authorizing recording servers before they can be used, you have full control over which recording servers are able to send information to the management server.

How to authorize: In the Management Client's navigation pane, right-click the required recording server, select **Authorize Recording Server**.

□On the XProtect Advanced VMS recording server installed in the previous step, you can now **add and configure the cameras you have previously only used on the XProtect Enterprise server.**

How to add and configure: Use the Management Client's **Add Wizard** to add cameras—the wizard lets you add entire IP ranges in one go. Then configure the cameras as required.

Tip: You can add and configure the cameras in XProtect Advanced VMS even though the XProtect Enterprise server is running with the same cameras.

While adding and configuring the cameras, disable XProtect Advanced VMS's default **Start Feed**, **Start Audio Feed** and **Record on Motion** rules to prevent conflicts between the XProtect Advanced VMS recording server and the XProtect Enterprise server.

How to disable: In the Management Client's navigation pane, expand **Rules and Alerts,** select **Rules**, and, in the overview pane, select **Rules**, then, in the properties pane, clear the **Active** box.

□ Once you have added and configured the cameras on the XProtect Advanced VMS recording server, you can **stop camera feeds through the XProtect Enterprise server.**

How to stop camera feed: If using an XProtect Enterprise version earlier than 7.0, open XProtect Enterprise's Administrator Application, and click **Scheduler…**. In the **Camera/Alert Scheduler** window, select **Clear**, clear all activity for a camera, and then **Copy and Paste to All** feature. If using XProtect Enterprise version 7.0 or later, open the Management Application, expand **Advanced Configuration**, click **Scheduling and Archiving**, and change the **Online** setting for all cameras to **Always off**.

□ XProtect Advanced VMS's default rules, such as **Start Feed**, **Start Audio Feed** and **Record on Motion** can now be enabled. If any **changes to image resolution and/or protocols** are required, this is the time to apply them.

Users now have access to live feeds from the cameras straight from XProtect Advanced VMS, while also having access to recordings—including archived recordings—supplied by the XProtect Enterprise server running as a slave under XProtect Advanced VMS.

□ Eventually, the XProtect Enterprise server's archives will become so old that they are automatically deleted. When the last archive has expired, you can **remove the XProtect Enterprise server** or—if installed on the same physical server as the XProtect Advanced VMS recording server—remove the XProtect Enterprise software using Windows' **Add/Remove Programs** feature.

Tip: If removing the XProtect Enterprise software, manually delete the **XProtect Enterprise** installation folder, database folders and archive folders after using Windows' **Add/Remove Programs** feature.

Also remember to remove the XProtect Enterprise slave server setting from XProtect Advanced VMS.

How to remove XProtect Enterprise slaves: In the Management Client's **Tools** menu, select **XProtect Enterprise Servers…**, select the no longer required XProtect Enterprise server from the list, then click **Remove**.

At this stage you can also remove old XProtect Smart Client views (i.e. those containing cameras from the now removed XProtect Enterprise server). Remember to inform your users that from now on they only need the new views (i.e. those containing cameras from the XProtect Advanced VMS server).

Index

About Milestone Systems

Founded in 1998, Milestone Systems is the global industry leader in open platform IP video management software. The XProtect platform delivers powerful surveillance that is easy to manage, reliable and proven in thousands of customer installations around the world. With support for the widest choice in network hardware and integration with other systems, XProtect provides best-in-class solutions to video enable organizations – managing risks, protecting people and assets, optimizing processes and reducing costs. Milestone software is sold through authorized and certified partners. For more information, visit:

www.milestonesys.com.