The open platform company

Milestone Systems

XProtect® Enterprise to XProtect® Advanced VMS 2016 R2

System Migration Guide

Contents

Introduction

Milestone Systems A/S facilitates the migration from XProtect® Enterprise to XProtect® Expert or XProtect® Corporate, allowing full integration of existing XProtect Enterprise systems.

Only migration from XProtect Enterprise servers running XProtect Enterprise version 7.0 or later is supported.

When you start the migration, the recording of video on XProtect Enterprise servers stops. If you require access to the recordings on your XProtect Enterprise servers after the migration, this document will help you achieve this.

Access to old recordings from Milestone Mobile client and XProtect Web Client is not supported.

If you do not require access to the old recordings on your XProtect Enterprise servers, you are actually installing a new system. Then the process is to uninstall the old XProtect Enterprise system and delete the exiting recordings. For information about how to install the XProtect Advanced VMS, see the Milestone Advanced VMS administrator manual http://www.milestonesys.com/support/manuals-and-guides/.

Important: Milestone requires that you upgrade all your XProtect Smart Clients to the latest version as part of the migration.

To do the migration, what you actually do is that you add your XProtect Enterprise servers to your new XProtect Advanced VMS system as slave servers.

When you add cameras to XProtect Advanced VMS, the system applies the actual camera settings stored in the camera, such as image and stream settings - codec, resolution, and compression - as they were in XProtect Enterprise.

Users can access the databases in the XProtect Enterprise system by using the old system as a slave server. This allows users to connect to the XProtect Advanced VMS system and from there view recorded video from the old XProtect Enterprise servers, too.

In this way, you are able to provide users with access to recordings from both the new and the old systems, and gradually phase out the use of XProtect Enterprise servers and their recordings as they become obsolete.

This guide provides:

- Information about reuse.
- Important points to consider before you start the migration.
- Step by step process for migration, when you want to temporarily integrate existing XProtect Enterprise systems into XProtect Advanced VMS, providing access to recordings from both old and new systems for as long as required.

If you are lacking information about specific steps within Management Application or Management Client, please refer to the detailed administrator manual either as integrated help in your product or as download file from our website http://www.milestonesys.com/support/manuals-and-guides/.

What to consider before migrating

Before migrating, ask yourself the following questions:

How to handle existing system configuration

XProtect Advanced VMS is an altogether different platform. You cannot import your existing XProtect Enterprise configuration for reuse in XProtect Advanced VMS directly, but since camera settings are already stored in the cameras with XProtect Enterprise, they are maintained. Cameras' recording settings, scheduling, and such must be reconfigured and verified in XProtect Advanced VMS. Since the event server will be replaced, all history off alarms and events are not available:

- 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. Therefore one approach for grouping cameras is by camera types.
- 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 to ensure compatibility with XProtect Advanced VMS Products as well as the features they offer. 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 permissions must be defined through the Management Client. Once roles are defined, you can add users to the roles from Active Directory or create basic users.

Can I reuse existing cameras?

Before migrating, it is important that you verify that the XProtect Advanced VMS system also supports the cameras used in your XProtect Enterprise system. You can verify supported hardware on the Milestone website https://www.milestonesys.com/supported-hardware. Since the XProtect Advanced VMS system uses a different device pack, Milestone recommends that your cameras have the latest supported camera firmware version installed.

When you verify your cameras, also verify that the required functionality is supported. The use of a different device pack can cause slight differences in the way XProtect Advanced VMS supports exact functionality of some cameras compared to XProtect Enterprise.

For JPEG, XProtect Advanced VMS uses a recording frame rate of 5 frames per second, by default, when cameras are added. If you want a higher frame rate you can configure this in Management Client after cameras are added.

For MPEG-4/H.264, all frames are recorded by default.

Can I reuse existing servers?

XProtect Advanced VMS is a fully distributed system. As many recording servers as required can run under one XProtect Advanced VMS management server.

The administration interface of XProtect Advanced VMS, the Management Client, 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.

The 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.

To reuse existing servers requires that the OS is Windows 7 SP1 or Windows Server 2008 R2 or newer.

Information about the minimum system requirements for system components is available on our website http://www.milestonesys.com/SystemRequirements.

Archiving

Archiving is the automatic transfer of recordings from a camera's default recording storage to another location. In this way, the amount of recordings you are able to store are not limited by the size of the camera's default recording storage.

Archiving is not a requirement when using XProtect Advanced VMS. In case the hard disks you have allocated for the live database (default recording storage) are fast enough and able to contain the expected amount of data, the system can run without archiving.

If you are using the archiving feature in your current XProtect Enterprise system 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. If recording and archiving previously was done to the same disk you do not need to archive. Furthermore the live database in XProtect Advanced VMS processes tasks ten times faster compared to XProtect Enterprise.

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. You create storages per recording server, and for each camera or camera group, you specify which storage to use.

See the XProtect Advanced VMS Administrator manual for more information about storage and archiving.

Downtime while migrating?

If you want to reduce downtime while you migrate, you can install your XProtect Advanced VMS system on other hardware than your Enterprise system. You can do this in advance and thereby reduce the system downtime.

You can do this system configuration in advance:

- Authorize recording servers.
- Configure recording servers' storage and archiving.
- Create device groups.
- Add cameras.
- Create roles and users.

If minimum downtime is essential and you are going to migrate many cameras and other devices, Milestone recommends that you install on other hardware.

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.

Integrations to other applications

If you have created integrations between your current XProtect Enterprise system and 3rd party products, for example, access control systems or fire alarm systems, through the use of MIP SDK, the integrations should be carefully tested before migration to verify that they will also work with XProtect Advanced VMS.

Milestone recommends that you contact your solution provider to review your customized integrations for use with XProtect Advanced VMS.

Virus scanning

It is likely that virus scanning will use a considerable amount of system resources on scanning all the data being recorded or archived. Also, the virus scanning software may temporarily lock each file it scans. For performance reasons, Milestone recommends that you disable any virus scanning of camera databases and archiving locations, if archiving is enabled.

If you already have disabled virus scanning in your system, you should do the same on the new storage resources that you maybe set up in connection with the migration.

Migration steps in a single server system on the same hardware

The following checklist outlines what to do when you migrate a single server XProtect Enterprise system to a single server XProtect Advanced VMS system on the same hardware.

Depending on the number of cameras you are going to migrate, expect that your XProtect Smart Client users are not able to log into the system for about 30-60 minutes. Recording is only interrupted from when you stop the XProtect Enterprise camera feed until you activate the XProtect Advanced VMS default rules. If minimal downtime is required for your XProtect Smart Client users, Milestone recommends that you buy new hardware to preinstall the XProtect Advanced VMS system (see "Migration steps in a single server system to new hardware" on page xii).

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

☐ **2. Make notes of your existing XProtect Enterprise system users and their views in XProtect Smart Client**.

We recommend this step because XProtect Smart Client is being updated during this migration.
Camera names, IP addresses, storage, etc. you can still view in the Management Application.
Make sure that you have the user names and passwords for the cameras.

☐ **3. Prepare your XProtect Enterprise Image Server service configuration for use with XProtect Advanced VMS**.

1. In the Management Application, expand **Server Access** and change the port number to 81 (default is 80). Consider to change the server name to something recognizable (default is **Server**).

If downtime is acceptable and your server CPU load is high, you can speed up the installation time by stopping the services temporarily during the installation in the **Services** node.

☐ **4. Install XProtect Advanced VMS**.

Locate the installer file and your license file.

1. Start installation and follow the steps.
2. When you are asked about installation method, select **Single Server**.
3. Once the installation is running, you may be notified about updates to your .NET version. Accept that.
4. When the installation has completed successfully, click **Close**.

The first thing you need to do is to authorize the recording server.

1. Log into your XProtect Advanced VMS system's Management Client.
2. Select the recording server in the overview pane.
3. Right-click and select **Authorize Recording Server**.

☐ **5. Verify Recording Server storage and archiving in the XProtect Advanced VMS system**.

Even though configuration of archiving is not a requirement when using XProtect Advanced VMS, Milestone recommends that you verify that your system can actually run with the default configuration or change it.

To view the storage settings:

1. Select the recording server.
2. Select the **Storage** tab and verify the configuration.

☐ **6. Add the XProtect Enterprise server to the XProtect Advanced VMS system.**

1. Open your XProtect Advanced VMS system's Management Client.
2. In the **Tools** menu, select **Enterprise Servers.**
3. Specify the following:
   - IP address/host name of the XProtect Enterprise server. If you installed XProtect Advanced VMS on the same server, type ***hostname*** or ***IP address***.
   - Port number (81).
   - Select the required authentication method, **Basic** or **Windows**.
   - Specify a user with **Administrator Access** enabled in the XProtect Enterprise system.
4. If one or more involved Enterprise servers access the system through an internet connection, also specify the XProtect Advanced VMS management server's WAN address: Click **Network** and specify the WAN IP address of the management server. In this way, the XProtect Enterprise server can use the WAN address of the XProtect Advanced VMS management server when authenticating users.
5. Click **Close**.

☐ **7. Create roles in the XProtect Advanced VMS system and add users to them**.

When specifying the rights of the roles, make sure the role get access to:

- The required cameras, including any PTZ features.
- The XProtect Enterprise server slave.

You do it in this way:

1. In the Management Client, expand **Security**, right-click **Roles**, then select **Add Role**.

2. As a minimum, specify the following:
   - On the **Device** tab, provide access rights to the required cameras.
   - On the **PTZ** tab, provide access to PTZ features.
   - On the **Servers** tab, provide access to the XProtect Enterprise server slave. You can use the same user account, as when you added the XProtect Enterprise server to the XProtect Advanced VMS system.
3. Optionally:
   - On the **Overall Security** tab, specify the rights of this role for all current and future cameras in the system. Then you don't need to specify rights on the **Device** tab and **PTZ** tab.
   - You can create a **Smart Client Profile** to modify the user interface in XProtect Smart Client so it reflects their rights. Afterwards, on **Roles** > **Info** tab, you add this Smart Client Profile to one or more roles.
4. Add users/groups to roles on the **Users and Groups** tab.

☐ **8. Disable default rules**.

To prevent conflicts between the XProtect Advanced VMS recording server and the XProtect Enterprise server, disable the default recording rules:

1. Expand **Rules and Events** and select **Rules**.
2. Deactivate the following rules:
   - **Default Start Feed Rule**.
   - **Default Start Audio Feed Rule**.
   - **Default Record on Motion Rule**.

☐ **9. Specify device groups in the XProtect Advanced VMS system**.

You can create device groups up front or as part of the **Add Hardware** wizard below.

1. Expand **Devices**, right-click **Cameras** and select **Add Device Group**.
2. Create groups as required for your system.

☐ **10. Add the cameras you have previously only used on the XProtect Enterprise server, on the XProtect Advanced VMS recording server**.

Before you start the wizard, locate the camera user names and passwords.

1. Right-click the recording server you just added, and run the **Add Hardware** wizard to add cameras—chose between:
   - Express detection (the system scans automatically for new hardware on the recording server's local network)
   - Adding entire IP ranges in one go, or

- Individual IP addresses.

2. Fill out user name and password.
3. Select camera driver(s).
4. Specify a device group, that you want the camera(s) to belong to.
5. Repeat until you have added all your cameras.

☐ **11. Configure the cameras**.

1. Configure the cameras as required, such as adjusting the frame rate for JPEG cameras.
2. Verify that the automatic motion detection settings set up by default are sufficient, but in general verify all settings.

☐ **12. Activate licenses**.

When you have added the cameras, Milestone recommends that you activate the licenses.

1. Expand **Basics** and select **License Information**.
2. Review the status of your licenses.
3. You can activate licenses online or offline.

☐ **13. Stop XProtect Enterprise camera feed and recordings**.

1. In Management Application, go to **Scheduling and Archiving**.
2. Change the online schedule for all cameras to **Always off**.

☐ **14. Start XProtect Advanced VMS camera feed and recordings**.

In Management Client, enable the default recording rules:

1. Expand **Rules and Events** and select **Rules**.
2. Activate the following rules:
   - **Default Start Feed Rule**.
   - **Default Start Audio Feed Rule**.
   - **Default Record on Motion Rule**.

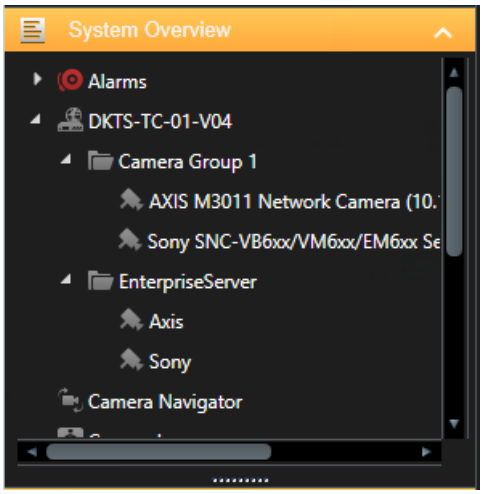
The system is now prepared for providing access to live feeds from the cameras straight from XProtect Advanced VMS, while also having access to old recordings—including archived recordings—supplied by the XProtect Enterprise server running as a slave under XProtect Advanced VMS.

Now you need to do some updates in XProtect Smart Client.

☐ **15. Log into XProtect Advanced VMS Smart Client as administrator**.

Use ***hostname*** or ***IP address*** and not localhost.

Click **Setup** and verify that you can see the cameras from the Enterprise server (in this example: **Enterprise Server**) in **System Overview** in the left side pane as well as the cameras you have added to your XProtect Advanced VMS system (in this example: **Camera Group 1**).



☐ **16. Re-establish XProtect Smart Client views**.

You need to create views for both the XProtect Enterprise cameras for playback of old recordings stored on the Enterprise server and views for the cameras coming through XProtect Advanced VMS for live viewing and playback of new recordings.

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. The XProtect Enterprise system is still installed and running, so you have the safety of being able to revert back to it before you progress further, if unexpected issues appear.

If you log into Smart Client using the Enterprise server on port 81, you only have access to the XProtect Enterprise system.

☐ **17. Verify that everything works as expected**.

For example, log into XProtect Smart Client as one of the XProtect Smart Client users being part of the role that has access to the Enterprise server.

Important: Migration completed.

Migration steps in a single server system to new hardware

The following checklist outlines what to do when you migrate a single server XProtect Enterprise system to a single server XProtect Advanced VMS system to new hardware.

Independent of the number of cameras, you can prepare your XProtect Advanced VMS system in advance and thereby reduce the downtime period for your XProtect Smart Client users significantly. As with migration on the same hardware, recording is also only interrupted from when you stop the XProtect Enterprise camera feed until you activate the XProtect Advanced VMS default rules.

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

☐ **2. Make notes of your existing XProtect Enterprise system users and their views in XProtect Smart Client**.

We recommend this step because XProtect Smart Client is being updated during this migration.
Camera names, IP addresses, storage, etc. you can still view in the Management Application.
Make sure that you have the user names and passwords for the cameras.

☐ **3. Install XProtect Advanced VMS on new hardware**.

Locate the installer file and your license files. Make sure that the user names and passwords for the cameras are available.

1. Start installation and follow the steps.
2. When you are asked about installation method, select **Single Server**.
3. Once the installation is running, you may be notified about updates to your .NET version. Accept that.
4. When the installation has completed successfully, click **Close**.

The first thing you need to do is to authorize the recording server.

1. Log into your XProtect Advanced VMS system's Management Client.
2. Select the recording server in the overview pane.
3. Right-click and select **Authorize Recording Server**.

☐ **4. Verify Recording Servers storage and archiving in the XProtect Advanced VMS system**.

Even though configuration of archiving is not a requirement when using XProtect Advanced VMS, Milestone recommends that you verify that your system can actually run with the default configuration or change it.

To view the storage settings:

1. Select the recording server.
2. Select the **Storage** tab and verify the configuration.

☐ **5. Go to the XProtect Enterprise server**.

☐ **6. Prepare your XProtect Enterprise Image Server service configuration for use with XProtect Advanced VMS**.

1. In the Management Application, expand **Server Access** and consider to change the server name to something recognizable (default is **Server**).

☐ **7. Go to the XProtect Advanced VMS system.**

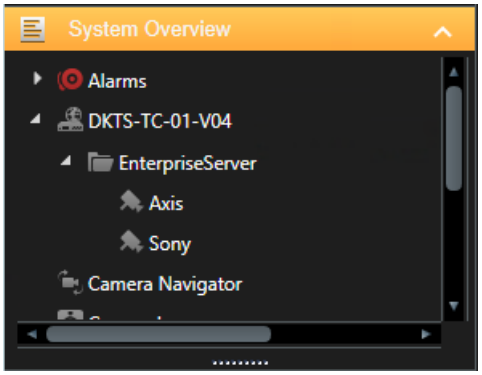
☐ **8. Add the XProtect Enterprise server to the XProtect Advanced VMS system**.

1. Open your XProtect Advanced VMS system's Management Client.
2. In the **Tools** menu, select **Enterprise Servers**.
3. Specify the following:
   - IP address/host name of the XProtect Enterprise server. If you installed XProtect Advanced VMS on the same server, type ***hostname*** or ***IP address***.
   - Port number (default is 80).
   - Select the required authentication method, **Basic** or **Windows**.
   - Specify a user with **Administrator Access** enabled in the XProtect Enterprise system.
4. If one or more involved Enterprise servers access the system through an internet connection, also specify the XProtect Advanced VMS management server's WAN address: Click **Network** and specify the WAN IP address of the management server. In this way the XProtect Enterprise can use the WAN address of the XProtect Advanced VMS management server when authenticating users.
5. Click **Close**.

☐ **9. Verify access to XProtect Enterprise cameras in XProtect Smart Client**.

Use ***hostname*** or ***IP address*** and not localhost.

Click **Setup** and verify that you can see the cameras from the Enterprise server (in this example: **Enterprise Server**) in **System Overview** in the left side pane.



☐ **10. Create roles in the XProtect Advanced VMS system and add users to them**.

When specifying the rights of the roles, make sure the role get access to:

- The required cameras, including any PTZ features.
- The XProtect Enterprise server slave.

You do it in this way:

1. In the Management Client, expand **Security**, right-click **Roles**, then select **Add Role**.
2. As a minimum, specify the following:
   - On the **Device** tab, provide access rights to the required cameras.
   - On the **PTZ** tab, provide access to PTZ features.
   - On the **Servers** tab, provide access to the XProtect Enterprise server slave. You can use the same user account, as when you added the XProtect Enterprise server to the XProtect Advanced VMS system.
3. Optionally:
   - On the **Overall Security** tab, specify the rights of this role for all current and future cameras in the system. Then you don't need to specify rights on the **Device** tab and **PTZ** tab.
   - On the **View Group** tab a view group for this role is created automatically. Decide if you want multiple roles for your XProtect Smart Client users with differentiated access rights to views.
   - You can create a **Smart Client Profile** to modify the user interface in XProtect Smart Client so it reflects their rights. Afterwards, on **Roles** > **Info** tab, you add this Smart Client Profile to one or more roles.
4. Add users/groups to roles on the **Users and Groups** tab.

☐ **11. Disable default rules**.

To prevent conflicts between the XProtect Advanced VMS recording server and the XProtect Enterprise server, disable the default recording rules:

1. Expand **Rules and Events** and select **Rules**.
2. Deactivate the following rules:
   - **Default Start Feed Rule**.
   - **Default Start Audio Feed Rule**.
   - **Default Record on Motion Rule**.

☐ **12. Specify device groups in the XProtect Advanced VMS system.**

You can create device groups up front or as part of the **Add Hardware** wizard below.

1. Expand **Devices**, right-click **Cameras** and select **Add Device Group**.
2. Create groups as required for your system.

☐ **13. Add the cameras you have previously only used on the XProtect Enterprise server, on the XProtect Advanced VMS recording server**.

Before you start the wizard, locate the camera user names and passwords.

1. Right-click the recording server you just added, and run the **Add Hardware** wizard to add cameras—chose between:
   - Express detection (the system scans automatically for new hardware on the recording server's local network)
   - Adding entire IP ranges in one go, or
   - Individual IP addresses.
2. Fill out user name and password.
3. Select camera driver(s).
4. Specify a device group, that you want the camera(s) to belong to.
5. Repeat until you have added all your cameras.

☐ **14. Configure the cameras**.

1. Configure the cameras as required, such as adjusting the frame rate for JPEG cameras.
2. Verify that the automatic motion detection settings set up by default are sufficient, but in general verify all settings.

☐ **15. Activate licenses**.

When you have added the cameras, Milestone recommends that you activate the licenses.

1. Expand **Basics** and select **License Information**.
2. Review the status of your licenses.
3. You can activate licenses online or offline.

Now you are ready for the actual migration.

☐ **16. On the XProtect Enterprise system, stop the camera feed and recordings**.

1. In Management Application, go to **Scheduling and Archiving**.
2. Change the online schedule for all cameras to **Always off**.

☐ **17. On the XProtect Advanced VMS system, start camera feed and recordings**.

In Management Client, enable the default recording rules:

1. Expand **Rules and Events** and select **Rules**.
2. Activate the following rules:
   - **Default Start Feed Rule**.
   - **Default Start Audio Feed Rule**.
   - **Default Record on Motion Rule**.

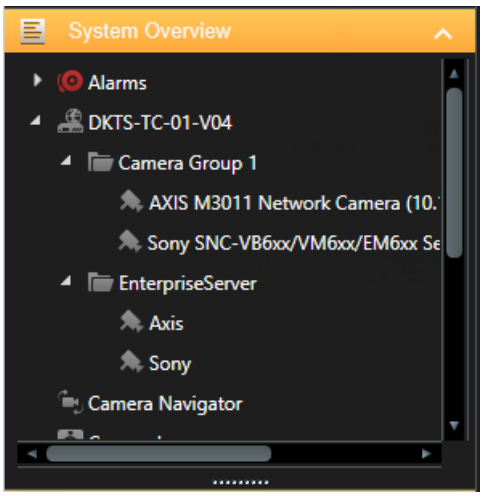
The system is now prepared for providing access to live feeds from the cameras straight from XProtect Advanced VMS, while also having access to old recordings—including archived recordings—supplied by the XProtect Enterprise server running as a slave under XProtect Advanced VMS.

Now you need to do some updates in XProtect Smart Client.

☐ **18. Log into XProtect Advanced VMS Smart Client as administrator**.

Use ***hostname*** or ***IP address*** and not localhost.

Click **Setup**. Previously you verified that you could see the cameras from the Enterprise server (in this example: **Enterprise Server**) in **System Overview** in the left side pane. Now you can verify that you can also see the cameras you have added to your XProtect Advanced VMS system (in this example: **Camera Group 1**).



☐ **19. Re-establish XProtect Smart Client views**.

You need to create views for both the XProtect Enterprise cameras for playback of old recordings stored on the Enterprise server and views for the cameras coming through XProtect Advanced VMS for live viewing and playback of new recordings.

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. The XProtect Enterprise system is still installed and running, so you have the safety of being able to revert back to it before you progress further, if unexpected issues appear.

☐ **20. Verify that everything works as expected**.

For example, log into XProtect Smart Client as one of the XProtect Smart Client users being part of the role that has access to the Enterprise server.

Important: Migration complete.

Migration steps in a distributed system

If your XProtect Enterprise system consists of multiple systems you have connected with the Master/Slave feature, the migration steps are almost the same. Multiple variations exist, but basically there are two scenarios:

1.

Buy one new server and install your XProtect Advanced VMS system, except the recording server, on this server. This is the distributed solution.

By not having a recording server on your management/event server you increase the performance and reduce downtime during the migration. On the master server and the slaves, you only install the recording server. You can now add the Enterprise servers and the newly installed recording servers to your XProtect Advanced VMS system. You will have your XProtect Enterprise system running in parallel with your XProtect Advanced VMS system in the phasing-out period. When the period ends, you un-install the XProtect Enterprise software.

Milestone recommends this migrating method.

2.

Reuse your hardware and install your XProtect Advanced VMS system on the same servers as your XProtect Enterprise system.

Then you install your XProtect Advanced VMS system on the master server as a single server option. On the slaves you only install the recording server. You can now add the Enterprise servers and the newly installed recording servers to your XProtect Advanced VMS system. You will have your XProtect Enterprise system running parallel with your XProtect Advanced VMS system in the phasing-out period. When the period ends you un-install the XProtect Enterprise software.

The table illustrates the two scenarios in an XProtect Enterprise system with one master and two slaves:

XProtect Enterprise setup	**XProtect Advanced VMS setup**
Master server Slave server Slave server	New hardware -> Distributed installation (Management server components except the recording server) Master server -> Recording server Slave server -> Recording server Slave server -> Recording server
	Master server -> Single server installation (including the recording server) Slave server -> Recording server Slave server -> Recording server

Below we list the high-level steps for our recommended migration method, where you maintain a distributed solution. You can find more details to each header in the single server sections:

☐ **1. Make notes of your existing XProtect Enterprise system users and their views in XProtect Smart Client**.

☐ **2. Install XProtect Advanced VMS except the recording server on new hardware**.

Locate the installer file and your license files. Make sure that the user names and passwords for the cameras are available.

1. Start installation and follow the steps.
2. When you are asked about installation method, select **Distributed**.
3. Once the installation is running, you may be notified about updates to your .NET version. Accept that.
4. When the installation has completed successfully, click **Close**.

☐ **3. Go to the administrative installation page and download the Recording Server installer**.

The administrative installation page can be found on the management server.

☐ **4. Go to the XProtect Enterprise server.**

☐ **5. Prepare your XProtect Enterprise Image Server service configuration for use with XProtect Advanced VMS**.

☐ **6. Install the XProtect Advanced VMS recording server which will eventually replace the 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.

Locate the installer file and your license files.

1. Start installation and follow the steps.
2. When you are asked about installation method, select **Typical**.
3. Specify management server address and Media database location. Click **Continue**.
4. An error message about the management server connection appears. Click **Yes** to continue.
5. Choose file location and product language. Click **Install**.
6. Once the installation is running, you may be notified about updates to your .NET version. Accept that.
7. When the installation of recorder and device pack has completed successfully, click **Close**.

Repeat the installation for all XProtect Enterprise servers.

☐ **7. Go to the XProtect Advanced VMS system**.

☐ **8. Authorize all recording servers in the XProtect Advanced VMS system**.

The first thing you need to do is to authorize the recording servers.

1. Log into your XProtect Advanced VMS system's Management Client.

2. Select the recording server in the overview pane.
3. Right-click and select **Authorize Recording Server**.

Repeat this step for all new recording servers.

☐ **9. Verify Recording Servers storage and archiving in the XProtect Advanced VMS system**.

☐ **10. Add the XProtect Enterprise server to the XProtect Advanced VMS system**.

☐ **11. Verify access to cameras in XProtect Smart Client**.

☐ **12. Create roles in the XProtect Advanced VMS system and add users to them**.

☐ **13. Disable default rules**.

☐ **14. Specify device groups in the XProtect Advanced VMS system**.

☐ **15. Add the cameras you have previously only used on the XProtect Enterprise server, on the XProtect Advanced VMS recording server**.

☐ **16. Configure the cameras**.

☐ **17. Activate licenses**.

Now you are ready for the actual migration.

☐ **18. Go to the XProtect Enterprise server**.

☐ **19. On the XProtect Enterprise system, stop the camera feed/recordings**.

☐ **20. Go to the XProtect Advanced VMS system**.

☐ **21. On the XProtect Advanced VMS system, start camera feed/recordings**.

☐ **22. Log into XProtect Advanced VMS Smart Client as administrator**.

☐ **23. Re-establish XProtect Smart Client views**.

☐ **24. Verify that everything works as expected**.

Removal of the XProtect Enterprise system

Eventually, the XProtect Enterprise server archives become so old that they are automatically deleted. When the last archive has expired, you should do the following:

If you installed XProtect Advanced VMS on the same hardware:

☐ **1. Go to the administrative installation page and download the Event Server installer**.

The administrative installation page can be found on the management server.

☐ **2. Remove the XProtect Enterprise system**.

1. Go to the Windows' **Add/Remove Programs** feature and **Uninstall** the XProtect Enterprise software.

The XProtect Advanced VMS event server is removed. You need to install it.

2. Run the downloaded Event Server installer.
3. After installation you can see the tray icon of the event server. Right click the icon to see the status, to make sure it is running.

If you installed XProtect Advanced VMS on new hardware:

☐ **1. Remove the XProtect Enterprise system**.

1. Go to the Windows' **Add/Remove Programs** feature and **Uninstall** the XProtect Enterprise software.

Repeat the uninstall step for all recording servers.

Post uninstall steps:

Finally, you need to remove the XProtect Enterprise server and XProtect Smart Client views from your XProtect Advanced VMS system.

☐ **1. Remove the XProtect Enterprise server from the XProtect Advanced VMS**.

1. In the Management Client's **Tools** menu, select **XProtect Enterprise Servers**.
2. Select the XProtect Enterprise server that you no longer want to connect to from the list, and click **Remove**.

Repeat the removal steps for all XProtect Enterprise servers.

☐ **2. Remove XProtect Smart Client views**.

1. Remove XProtect Smart Client views containing cameras from the XProtect Enterprise server you have just removed.

Remember to inform your users that from now on they only need the new views containing cameras from the XProtect Advanced VMS server.

Index