

MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile Server 2020 R2

Administrator manual



Contents

Copyright, trademarks, and disclaimer	5
Overview	6
XProtect Mobile (explained)	6
XProtect Mobile server (explained)	6
Product comparison chart	6
Requirements and considerations	10
Prerequisites for using XProtect Mobile	10
XProtect Mobile system requirements	10
Requirements for notifications setup	10
Requirements for Smart Connect setup	11
Requirements for user's two-step verification setup	11
Requirements for Video Push setup	11
Mobile server encryption requirements for clients	11
Requirements for direct streaming	11
Installation	13
Install XProtect Mobile server	13
Configuration	15
Mobile server settings	15
General tab	15
Connectivity tab	17
Server Status tab	19
Performance tab	20
Investigations tab	23
Video Push tab	25
Notifications tab	25
Two-step verification tab	26
Direct streaming (explained)	29
Adaptive streaming (explained)	30

Secure communication (explained)	30
Management server encryption (explained)	31
Encryption from the management server to the recording server (explained)	32
Encryption between the management server and the Data Collector Server (explained)	34
Encryption to clients and servers that retrieve data from the recording server (explained)	35
Mobile server data encryption (explained)	37
Mobile server encryption requirements for clients	38
Enable encryption	38
Enable encryption to and from the management server	38
Enable server encryption for recording servers or remote servers	39
Enable encryption to clients and servers	40
Enable encryption on the mobile server	42
Edit certificate	42
Milestone Federated Architecture and master/slave servers (explained)	43
Smart Connect (explained)	43
Set up Smart Connect	44
Enable Universal Plug and Play discoverability on your router	44
Enable connections on complex network	44
Configure connection settings	45
Send an email message to users	45
Sending notifications (explained)	45
Set up push notifications on XProtect Mobile server	46
Enable sending push notifications to specific or all mobile devices	47
Stop sending push notifications to specific or all mobile devices	47
Set up investigations	47
Using Video Push to stream video (explained)	48
Set up Video Push to stream video	49
Add a Video Push channel for streaming video	49
Remove a Video Push channel	49
Add the Video Push Driver as a hardware device on the Recording Server	49

Add the Video Push Driver device to the channel for Video Push	51
Enable audio for existing video push channel	51
Set up users for two-step verification via email	51
Enter information about your SMTP server	52
Specify the verification code that will be sent to users	52
Assign login method to users and Active Directory groups	52
Actions (explained)	53
Naming an output for use in XProtect Mobile client and XProtect Web Client (explained)	53
Maintenance	54
Mobile Server Manager (explained)	54
Access XProtect Web Client	54
Start, stop and restart Mobile Server service	55
Fill in/edit management server address	55
Show/edit port numbers	55
Edit certificate	56
Accessing logs and investigations (explained)	56
Change investigations folder	56
Show status (explained)	57
Troubleshooting	58
Troubleshooting XProtect Mobile	58

Copyright, trademarks, and disclaimer

Copyright © 2020 Milestone Systems A/S

Trademarks

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

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

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

Disclaimer

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

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

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

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

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

Overview

XProtect Mobile (explained)

XProtect Mobile consists of five components:

- XProtect Mobile client

The XProtect Mobile client is a mobile surveillance app that you can install and use on your Android or Apple device. You can use as many installations of XProtect Mobile client as you need.

For more information, download the XProtect Mobile Client User Manual from the Milestone Systems website (<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>).

- XProtect Web Client

XProtect Web Client lets you view live video in your web browser and lets you download recordings. XProtect Web Client is installed automatically together with the installation of the XProtect Mobile server.

For more information, download the XProtect Web Client User Manual from the Milestone Systems website (<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>).

- XProtect Mobile server
- XProtect Mobile plug-in
- Mobile Server Manager

This manual covers the XProtect Mobile server, XProtect Mobile plug-in, and Mobile Server Manager.

XProtect Mobile server (explained)

The XProtect Mobile server handles logins to the system from the XProtect Mobile client or XProtect Web Client.

A XProtect Mobile server distributes video streams from recording servers to the XProtect Mobile client or XProtect Web Client. This offers a secure setup where recording servers are never connected to the internet. When a XProtect Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats allowing streaming of video on the mobile device.

You must install the XProtect Mobile server on any computer from which you want to access recording servers. When you install the XProtect Mobile server, log in using an account that has administrator rights. Otherwise, installation will not complete successfully (see Install XProtect Mobile server on page 13).

The XProtect Mobile server supports direct streaming and adaptive streaming in live mode (for XProtect Expert and XProtect Corporate only).

Product comparison chart

XProtect VMS includes the following products:

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

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

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

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

Name	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
SNMP notification	-	-	-	✓	✓
Time controlled user access rights	-	-	-	-	✓
Reduce frame rate (grooming)	-	-	-	✓	✓
Video data encryption (recording server)	-	-	-	✓	✓
Database signing (recording server)	-	-	-	✓	✓
PTZ priority levels	1	1	3	32000	32000
Extended PTZ (Reserve PTZ session and patrolling from XProtect Smart Client)	-	-	-	✓	✓
Evidence lock	-	-	-	-	✓
Bookmark function	-	-	Manual only	Manual and rule-based	Manual and rule-based
Live multi-streaming or multicasting / Adaptive streaming	-	-	-	✓	✓
Direct streaming	-	-	-	✓	✓
Overall security	Client user rights	Client user rights	Client user rights	Client user rights	Client user rights/ administrator user rights

Name	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
XProtect Management Client profiles	-	-	-	-	✓
XProtect Smart Client profiles	-	-	3	3	Unrestricted
XProtect Smart Wall	-	-	-	optional	✓
System Monitor	-	-	-	✓	✓
Smart map	-	-	-	✓	✓
Two-step verification	-	-	-	-	✓
DLNA support	-	✓	✓	✓	✓
Privacy masking	-	✓	✓	✓	✓
Device password management			✓	✓	✓

Requirements and considerations

Prerequisites for using XProtect Mobile

Before you can start using XProtect Mobile, you must make sure that you have the following:

- A running VMS installed and configured with at least one user
- Cameras and views set up in XProtect Smart Client
- A mobile device running Android or iOS with access to Google Play or App StoreSM from which you can download the XProtect Mobile client application
- A web browser for running XProtect Web Client

To read more about requirements, see XProtect Mobile system requirements on page 10.

XProtect Mobile system requirements

For information about the **minimum** system requirements to the various components, visit the Milestone website (<https://www.milestonesys.com/systemrequirements/>).

- To find requirements for XProtect Mobile client, select the **XProtect Mobile** product icon
- To find requirements for XProtect Web Client, select the **XProtect Web Client** product icon
- To find requirements for XProtect Mobile server, select the icon of the XProtect product that you have installed
- The requirements for XProtect Mobile plug-in are:
 - A running Management Client
 - The Milestone plug-in is installed to integrate with your VMS

Requirements for notifications setup

- You must associate one or more alarms with one or more events and rules. This is not required for system notifications
- Make sure that your Milestone CareTM agreement with Milestone Systems is up-to-date
- Your system must have access to the Internet

For more information, see:

Set up push notifications on XProtect Mobile server on page 46

Notifications tab on page 25

Requirements for Smart Connect setup

- Your XProtect Mobile server must use a public IP address. The address can be static or dynamic, but typically it's a good idea to use static IP addresses
- You must have a valid license for Smart Connect

Requirements for user's two-step verification setup

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

For more information, see:

Set up users for two-step verification via email on page 51

Two-step verification tab on page 26

Requirements for Video Push setup

- Each channel requires a hardware device license
- To enable audio with video push:
 1. Download and install Milestone XProtect Device Pack 10.3a version or later.
 2. Download and install XProtect Mobile Server Installer.exe 13.2a or later.
 3. Restart the Recording Server service.

Mobile server encryption requirements for clients

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

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

Requirements for direct streaming

XProtect Mobile supports direct streaming in live mode (for XProtect Expert and XProtect Corporate only).

Camera configuration requirements for direct streaming

To use direct streaming in XProtect Web Client and XProtect Mobile client, you must have the following camera configuration:

- The cameras must support the H.264 codec (for all clients) or the H.265 codec (for the XProtect Mobile client only)
- It is recommended that you set the **GOP size** value to **1 second** and the **FPS** setting must have a value that is higher than **10 FPS**

Installation

Install XProtect Mobile server

Once you have installed XProtect Mobile server, you can use XProtect Mobile client and XProtect Web Client with your system. To reduce the overall use of system resources on the computer running the management server, install XProtect Mobile server on a separate computer.

The management server has a built-in public installation webpage. From this webpage, administrators and end-users can download and install the required XProtect system components from the management server or any other computer in the system.



XProtect Mobile server is automatically installed when you install the "single computer" option.

To install the XProtect Mobile server:

1. Enter the following URL in your browser: *http://[management server address]/installation/admin* where the [management server address] is the IP address or the host name of the management server.
2. Click **All Languages** for the XProtect Mobile server installer.
3. Run the downloaded file. Then, click **Yes** to all warnings. Then, unpacking starts.
4. Select a language for the installer. Then, click **Continue**.
5. Read and accept the license agreement. Then, click **Continue**.
6. For secure communication, select the certificate used to connect to the management server.
7. Select the installation type:
 - Click **Typical** to install XProtect Mobile server and plug-in
 - Click **Custom** to install only the server or only the plug-in. For example, installing only the plug-in is useful if you want to use Management Client to manage XProtect Mobile servers, but don't need XProtect Mobile server on that computer



XProtect Mobile plug-in is required on the computer running Management Client to manage XProtect Mobile servers in Management Client.

8. For custom installation only: Select the components that you want to be installed. Then, click **Continue**.
9. Specify the mobile server encryption. Then, click **Continue**.

On the **Specify mobile server encryption** page, you can secure the communication between the mobile server and the clients and services.



If you do not enable encryption, some features in some clients will not be available. For more information, see Mobile server encryption requirements for clients on page 38.

Select a valid certificate in the list. For more information about establishing secure communication in your system, see Mobile server data encryption (explained) on page 37 or the *Milestone Certificate guide* (English only).

You can also enable encryption after the installation completes from the Mobile Server Manager tray icon in the taskbar of your operating system (see Enable encryption on the mobile server on page 42).

10. Select the service account for the mobile server. Then, click **Continue**.



To change or edit the service account credentials at a later stage, you will have to reinstall the mobile server.

11. In the **Server URL** field, fill in the primary management server address.
12. For custom installation only: Specify the connection ports for communication with the mobile server. Then, click **Continue**.



In a typical installation, the connection ports get the default port numbers (8081 for HTTP port and 8082 for HTTPS port).

13. Select the file location and product language and then, click **Install**.
14. When the installation is completed, a list of successfully installed components appears. Then, click **Close**.

You are ready for configuring XProtect Mobile (see Mobile server settings on page 15).

Configuration

Mobile server settings

In Management Client you can configure and edit a list of XProtect Mobile server settings accessible through tabs at the bottom toolbar of the mobile server **Properties** section. From there, you can:

- Enable or disable server features general configuration (see General tab on page 15)
- Configure server connectivity settings and set up Smart Connect feature (see Connectivity tab on page 17)
- See server current status and listed active users (see Server Status tab on page 19)
- Set up performance parameters to enable direct streaming and adaptive streaming, or to set transcoded video stream limitations (see Performance tab on page 20)
- Configure investigation settings (see Investigations tab on page 23)
- Configure Video Push settings (see Video Push tab on page 25)
- Set up, turn on and turn off system and push notifications (see Notifications tab on page 25)
- Enable and configure an additional login step for users (see Two-step verification tab on page 26)

General tab

The following table describes the settings on this tab.

General

Name	Description
Server name	Enter a name of the XProtect Mobile server.
Description	Enter an optional description of the XProtect Mobile server.
Mobile server	See the name of the currently selected XProtect Mobile server.
Login method	Select the authentication method to use when users log in to the server. You can choose between: <ul style="list-style-type: none">• Automatic• Windows authentication• Basic authentication

Features

The following table describes how you control the availability of XProtect Mobile features.

Name	Description
Enable XProtect Web Client	Enable access to XProtect Web Client. This feature is enabled by default.
Enable all cameras view	Include the All Cameras view. This view displays all of the cameras that a user is allowed to view on a recording server. This feature is enabled by default.
Enable actions (outputs and events)	Enable access to actions in XProtect Mobile client and XProtect Web Client. This feature is enabled by default. If you disable this feature, the client users are not able to see output and events, even if these are configured correctly.
Enable incoming audio	Enable incoming audio feature in XProtect Web Client and XProtect Mobile client. This feature is enabled by default.
Enable push-to-talk	Enable push-to-talk (PTT) feature in XProtect Web Client and XProtect Mobile client. This feature is enabled by default.
Deny the built-in Administrator role access to the XProtect Mobile server	Enable this to prevent users assigned to the built-in administrator role from accessing video on XProtect Mobile client or XProtect Web Client.

Log settings

You can see the log settings information.

Name	Description
Log file location	See where the system saves log files.
Keep logs for	See the number of days to keep logs for. The default is three days.

Configuration backup

If your system has multiple XProtect Mobile servers, you can use the backup function to export the current settings and import them on other XProtect Mobile servers.

Name	Description
Import	Import an XML file with a new XProtect Mobile server configuration.
Export	Export your XProtect Mobile server configuration. Your system stores the configuration in an XML file.

Connectivity tab

Settings on the **Connectivity** tab are used in the following tasks:

- Configure connection settings on page 45
- Send an email message to users on page 45
- Enable connections on complex network on page 44
- Enable Universal Plug and Play discoverability on your router on page 44

For more information, see Smart Connect (explained) on page 43.

General

Name	Description
Connection type	Choose how XProtect Mobile client and XProtect Web Client users should connect to the XProtect Mobile server. You can choose between the following options: HTTP only , HTTP and HTTPS or HTTPS only . For more information, see Mobile server encryption requirements for clients on page 38.
Client timeout (HTTP)	Set a time frame for how often the XProtect Mobile client and XProtect Web Client must indicate to the XProtect Mobile server that they are up and running. The default value is 30 seconds. Milestone recommends that you do not increase the time frame.
Enable UPnP	This makes the XProtect Mobile server discoverable on the network by means of the

Name	Description
discover-ability	UPnP protocols. The XProtect Mobile client has scanning functionality for finding XProtect Mobile servers based on UPnP.
Enable automatic port mapping	When the XProtect Mobile server is installed behind the firewall, a port mapping is required in the router, so clients can still access the server from the internet. The Enable automatic port mapping option enables the XProtect Mobile server to do this port mapping by itself provided that the router is configured for it.
Enable Smart Connect	Smart Connect enables you to verify that you have configured the XProtect Mobile server correctly without logging in with a mobile device or a tablet to do the validation. It also simplifies the connection process for the client users.

Internet Access

Name	Description
Configure custom internet access	If you use UPnP port mapping, to direct connections to a specific connection, select the Configure custom Internet access check box. Then provide the IP address or host name , and the port to use for the connection. For example, you might do this if your router does not support UPnP, or if you have a chain of routers.
Disable default address	Disable the default IP addresses to connect to the mobile server only with a custom IP address or host name.
Select to retrieve IP address dynamically	If your IP addresses often change, select the Select to retrieve IP address dynamically check box.
HTTP port	Enter the port number for the HTTP connection.
HTTPS port	Enter the port number for the HTTPS connection.
Server addresses	Lists all the IP addresses that are connected to the mobile server.

Smart Connect notification

Name	Description
Email invitation to	Enter the email address for the recipient of the Smart Connect notification.
Email language	Specify the language used in the email.
Smart Connect token	A unique identifier that users of mobile devices can use to connect to the XProtect Mobile server.
Link to Smart Connect	A link that users of mobile devices can use to connect to the XProtect Mobile server.

Server Status tab

See the status details for the XProtect Mobile server. The details are read-only:

Name	Description
Server active since	Shows the time and date when the XProtect Mobile server was last started.
CPU usage	Shows current CPU usage on the mobile server.
External bandwidth	Shows the current bandwidth in use between the XProtect Mobile client or XProtect Web Client and the mobile server.

Active users

See the status details of the XProtect Mobile client or XProtect Web Client currently connected to the XProtect Mobile server.

Name	Description
User Name	Shows the user name for each XProtect Mobile client or XProtect Web Client user connected to the mobile server.
State	Shows the current relation between the XProtect Mobile server and the XProtect Mobile client or XProtect Web Client user in question. Possible states are: <ul style="list-style-type: none"> • Connected: An initial state when the clients and the server exchange keys and encrypting credentials • Logged In: The XProtect Mobile client or XProtect Web Client user is logged into the XProtect system
Video bandwidth usage (kB/s)	Shows the total bandwidth of the video streams that are currently open for each XProtect Mobile client or XProtect Web Client user.
Audio bandwidth usage (kB/s)	Shows the total bandwidth of the audio streams that are currently open for each XProtect Web Client user.
Transcoded video streams	Shows the total number of transcoded video streams that are currently open for each XProtect Mobile client or XProtect Web Client user.
Direct video streams	Shows the total number of direct video streams that are currently open for each XProtect Mobile client or XProtect Web Client user (for XProtect Expert and XProtect Corporate only).
Transcoded audio streams	Shows the total number of transcoded audio streams that are currently open for each XProtect Web Client user.

Performance tab

On the **Performance** tab, you can set the following settings and limitations on the XProtect Mobile server's performance:

Video streaming settings (for XProtect Expert and XProtect Corporate only)

Name	Description
Enable direct streaming	Enable direct streaming in XProtect Web Client and XProtect Mobile client. This feature is enabled by default.
Enable adaptive streaming	Enable adaptive streaming in XProtect Web Client and XProtect Mobile client. This feature is enabled by default.
Streaming modes	<p>After you enable the adaptive streaming feature, you can select the type of the streaming mode from the list:</p> <ul style="list-style-type: none"> • Optimize video quality (default) - selects the stream with the lowest available resolution that is equal to or higher than the requested resolution • Optimize server performance - reduces the requested resolution and then selects the stream with the lowest available resolution that is equal to or higher than the reduced request • Optimize resolution for low bandwidth - selects the stream with the lowest available resolution (recommended if you use 3G or an unstable network)

Transcoded video stream limitations**Level 1**

Level 1 is the default limitation placed on the XProtect Mobile server. Any limitations that you set here are always applied to the XProtect Mobile's transcoded video streams.

Name	Description
Level 1	Select the check box to enable the first level of limitations to XProtect Mobile server performance.

Name	Description
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the XProtect Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the XProtect Mobile server to clients.

Level 2

If you want to enforce a different level of limitations than the default one in **Level 1**, select the **Level 2** check box. You cannot set any settings higher than what you have set them to in the first level. If you, for example, set the Max FPS to 45 on **Level 1**, you can set the Max FPS on **Level 2** only to 44 or below.

Name	Description
Level 2	Select the check box to enable the second level of limitations to XProtect Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the XProtect Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the XProtect Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the XProtect Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the XProtect Mobile server to clients.

Level 3

You can also select a **Level 3** check box to create a third level for limitations. You cannot set any settings higher than what you have set them to in **Level 1** and **Level 2**. If you, for example, set the **Max FPS** to 45 on **Level 1** and to level 32 on **Level 2**, you can set the **Max FPS** on **Level 3** only to 31 or less.

Name	Description
Level 3	Select the check box to enable the third level of limitations to XProtect Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the XProtect Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the XProtect Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the frames per second (FPS) to send from the XProtect Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the XProtect Mobile server to clients.



The system does not instantly switch from one level to another level. If your CPU or bandwidth threshold goes less than five percent above or below the indicated levels, the current level stays in use.

Investigations tab

Investigations settings

You can enable investigations so that people can use the XProtect Mobile client or XProtect Web Client to access recorded video and investigate incidents, and to prepare and download video evidence.

Name	Description
Investigations folder	Shows where your video exports are saved on your hard drive.
Limit size of investigations	Enter the maximum number of megabytes that the investigations folder can contain. Default size is 2000 MB.

Name	Description
folder to	
View investigations made by other users	Select this check box to allow users to access investigations that they did not create.
Include timestamps for AVI exports	Select this check box to include the date and time that the AVI file was downloaded.
Used codec for AVI exports	Select the compression format to use when preparing AVI packages for download. The codecs that you can choose from can differ depending on your operating system. If you do not see the codec you want, you can add it to the list by installing it on the computer where the XProtect Mobile server is running.
Used audio bit for AVI exports	Select from the list the appropriate audio bit rate when audio is included in your video export. The default is 160000 Hz.
Keep or delete data when exports fail (MKV and AVI)	Select whether to keep the data that was not successfully prepared for download in an investigation or delete it.

Investigations

Name	Description
Investigations	Lists the investigations that have been set up so far in the system. Use the Delete or Delete all buttons if you no longer want to keep an investigation. This can be useful if, for example, you want to make more disk space available on the server.
Investigation details	To delete individual video files that were exported for an investigation, but keeping the investigation, select the investigation in the list. In the Investigation details group, select the delete icon to the right of the Database , AVI , or MKV fields for exports.

Video Push tab

You can specify the following settings if you enable Video Push:

Name	Description
Video Push	Enable Video Push on the mobile server.
Number of channels	Shows the number of enabled Video Push channels in your XProtect system.
Channel	Shows the channel number for the relevant channel. Non-editable.
Port	Port number for the relevant Video Push channel.
MAC Address	MAC address for the relevant Video Push channel.
User Name	Enter the user name associated with the relevant Video Push channel.
Camera Name	Shows the name of the camera if the camera has been identified.

Once you have completed all necessary steps (see Set up Video Push to stream video on page 49), select **Find Cameras** to search for the relevant camera.

Notifications tab

Use the **Notifications** tab to turn on or turn off system notifications and push notifications.

If you turn on notifications, and have configured one or more alarms and events, XProtect Mobile notifies users when an event occurs. When the app is open, notifications are delivered in XProtect Mobile on the mobile device. Push notifications notify users who don't have the XProtect Mobile open. These notifications are delivered to the mobile device.

For more information, see: Enable sending push notifications to specific or all mobile devices on page 47

The following table describes the settings on this tab.

Name	Description
Notifications	Select this check box to turn on notifications.
Maintain device registration	<p>Select this check box to store information about the devices and users who connect to this server. The system sends notifications to these devices.</p> <p>If you clear this check box, you also clear the list of devices. For users to start receiving notifications again, you must select the check box, and the users must connect their devices to the server again.</p>

Registered devices

Name	Description
Enabled	Select this check box to start sending notifications to the device.
Device Name	<p>A list of the mobile devices that have connected to this server.</p> <p>You can start or stop sending notifications to specific devices by selecting or clearing the Enabled check box.</p>
User	Name of the user that will receive notifications.

Two-step verification tab



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

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


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

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

For more information, see Set up users for two-step verification via email on page 51.

The following tables describe the settings on this tab.


Provider settings > Email

Name	Description
SMTP server	Enter the IP address or host name of the simple mail transfer protocol (SMTP) server for two-step verification emails.
SMTP server port	Specify the port of the SMTP server for sending emails. Default port number is 25 without SSL and 465 with SSL.
Use SSL	Select this check box if your SMTP server supports SSL encryption.
User name	Specify the user name for logging in to the SMTP server.
Password	Specify the password for logging in to the SMTP server.
Use Secure Password Authentication (SPA)	Select this check box if your SMTP server supports SPA.
Sender's email address	Specify the email address for sending verification codes.
Email subject	Specify the subject title for the email. Example: Your two-step verification code.
Email text	<div>Enter the message you want to send. Example: Your code is {0}.</div> <div> If you forget to include the {0} variable, the code is added at the end of the text by default.</div>

Verification code settings

Name	Description
Reconnection timeout (0-30 minutes)	Specify the period within which XProtect Mobile client users do not have to reverify their login in case of, for example, a disconnected network. The default period is three minutes. This setting does not apply to XProtect Web Client.
Code expires after (1-10 minutes)	Specify the period within which the user can use the received verification code. After this period, the code is invalid and the user has to request for a new code. The default period is five minutes.
Code entry attempts (1-10 attempts)	Specify the maximum number of code entry attempts before the provided code becomes invalid. The default number is three.
Code length (4-6 characters)	Specify the number of characters for the code. The default length is six.
Code composition	Specify the complexity of the code that you want the system to generate. You can select among: <ul style="list-style-type: none"> • Latin uppercase (A-Z) • Latin lowercase(a-z) • Digits (0-9) • Special characters (!@#...)

User settings

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

Name	Description
Verification method	<p>Select a verification setting for each user or group. You can select among:</p> <ul style="list-style-type: none"> • No login: the user cannot log in • No two-step verification: the user must enter user name and password • Email: the user must enter a verification code in addition to user name and password
User details	Enter the email address to which each user will receive codes.

Direct streaming (explained)

XProtect Mobile supports direct streaming in live mode (for XProtect Expert and XProtect Corporate only).

Direct streaming is a video streaming technology that transfers video from an XProtect system to the clients directly in H.264 codec, which is supported by most modern IP cameras. Direct streaming does not require any transcoding and, therefore, removes some of the stress on the XProtect system.

The direct streaming technology is in contrast to the transcoding setting in XProtect, in which an XProtect system decodes video from the codec that is used on the camera into JPEG files. Enabling the feature results in reduced CPU usage for the same configuration of cameras and video streams. Direct streaming also increases streaming performance for the same hardware – up to five times as many concurrent video streams compared to transcoding.

You can also use the direct streaming feature to transfer video from cameras that support the H.265 codec directly to XProtect Mobile client.

In Management Client, you can enable or disable direct streaming for clients (see Mobile server settings on page 15).

The video stream falls back from direct streaming to transcoding if:

- The direct streaming feature has been disabled in Management Client or the requirements have not been fulfilled (see Requirements for direct streaming on page 11)
- The codec of the streaming camera is different than H.264 (for all clients) or H.265 (for the XProtect Mobile client only)
- The video cannot start playing for more than ten seconds
- The frame rate of the streaming camera is set to **one** frame per second (1 FPS)
- The connection to the server or with the camera has been lost
- You use the privacy masking feature during live video

Adaptive streaming (explained)

XProtect Mobile supports adaptive streaming in live mode (for XProtect Expert and XProtect Corporate only).

Adaptive streaming is useful when you view multiple live video streams in the same view of cameras. The feature optimizes the performance of the XProtect Mobile server and improves the decoding capability and performance of devices running XProtect Web Client.

To take advantage of adaptive streaming, your cameras must have multiple streams defined with different resolutions. In this case, the feature allows you to:

- Optimize video quality - selects the stream with the lowest available resolution that is equal to or higher than the requested resolution
- Optimize server performance - reduces the requested resolution and then selects the stream with the lowest available resolution that is equal to or higher than the reduced request
- Optimize resolution for low bandwidth - selects the stream with the lowest available resolution (recommended if you use 3G or an unstable network)



When zooming, the live video stream requested is always the one with the highest available resolution.



Bandwidth usage is often reduced when the resolution of the requested streams is reduced. Bandwidth usage also depends on other settings in the configurations of the defined streams.

You can enable or disable adaptive streaming, and set the preferred streaming mode of the feature on the **Performance tab** of the mobile server settings in Management Client (see Mobile server settings on page 15).

Secure communication (explained)

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

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

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

A certificate authority (CA) can issue certificates to web services on servers using a CA certificate. This certificate contains two keys, a private key and public key. The public key is installed on the clients of a web service (service clients) by installing a public certificate. The private key is used for signing server certificates that must be installed on the server. Whenever a service client calls the web service, the web service sends the server certificate

including the public key to the client. The service client can validate the server certificate using the already installed public CA certificate. The client and the server can now use the public and private server certificate to exchange a secret key and thereby establish a secure SSL/TLS connection.

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



Certificates have an expiry date. XProtect VMS will not warn you when a certificate is about to expire. If a certificate expires:

- The clients will no longer trust the recording server with the expired certificate and thus cannot communicate with it.
- The recording servers will no longer trust the management server with the expired certificate and thus cannot communicate with it.
- The mobile devices will no longer trust the mobile server with the expired certificate and thus cannot communicate with it.

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

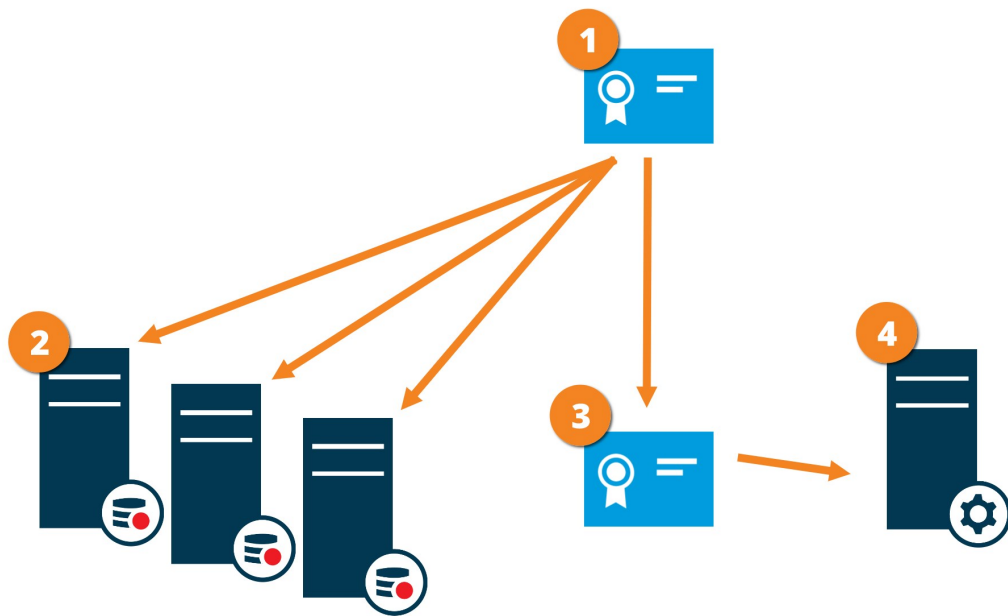
When you renew a certificate with the same subject name and add it to the Windows Certificate Store, the servers will automatically pick up the new certificate. This makes it easier to renew certificates for many servers without having to re-select the certificate for each server and without restarting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

Management server encryption (explained)

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

Certificate distribution for management servers

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



- ❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (management server) and by the party that verifies the certificate (recording servers)
- ❷ The CA certificate must be trusted on all recording servers. In this way the recording servers can verify the validity of the certificates issued by the CA
- ❸ The CA certificate is used to establish secure connection between the management server and the recording servers
- ❹ The CA certificate must be installed on the computer on which the management server is running

Requirements for the private management server certificate:

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

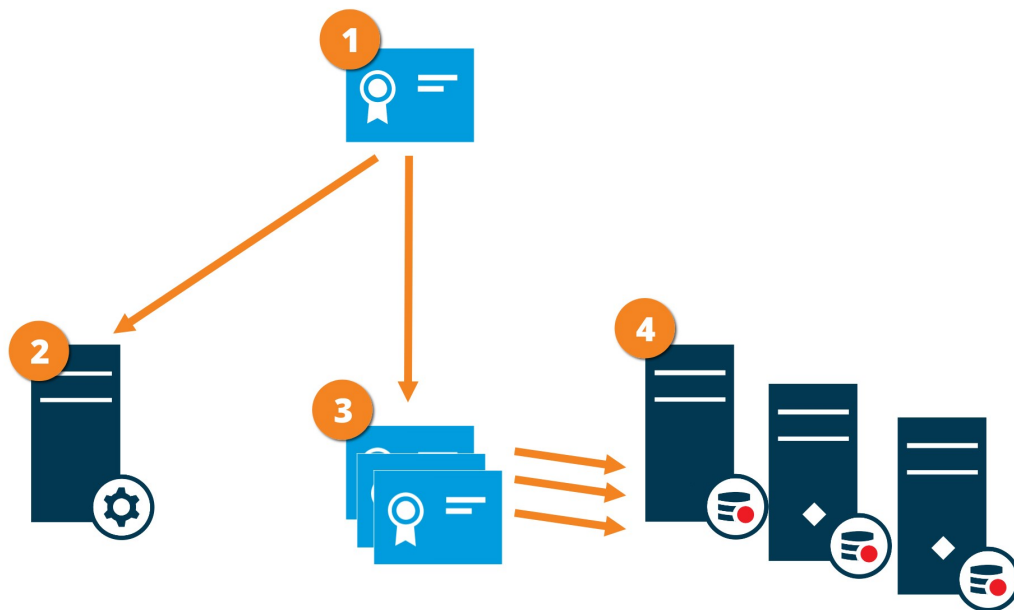
Encryption from the management server to the recording server (explained)

You can encrypt the two-way connection between the management server and the recording server. When you enable encryption on the management server, it applies to connections from all the recording servers that connect to the management server. Encryption of this communication must follow the encryption setting on the

management server. So, if management server encryption is enabled, this must also be enabled on the recording servers, and vice-versa. Before you enable encryption, you must install security certificates on the management server and all recording servers, including failover recording servers.

Certificate distribution

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



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

Requirements for the private recording server certificate:

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

Encryption between the management server and the Data Collector Server (explained)

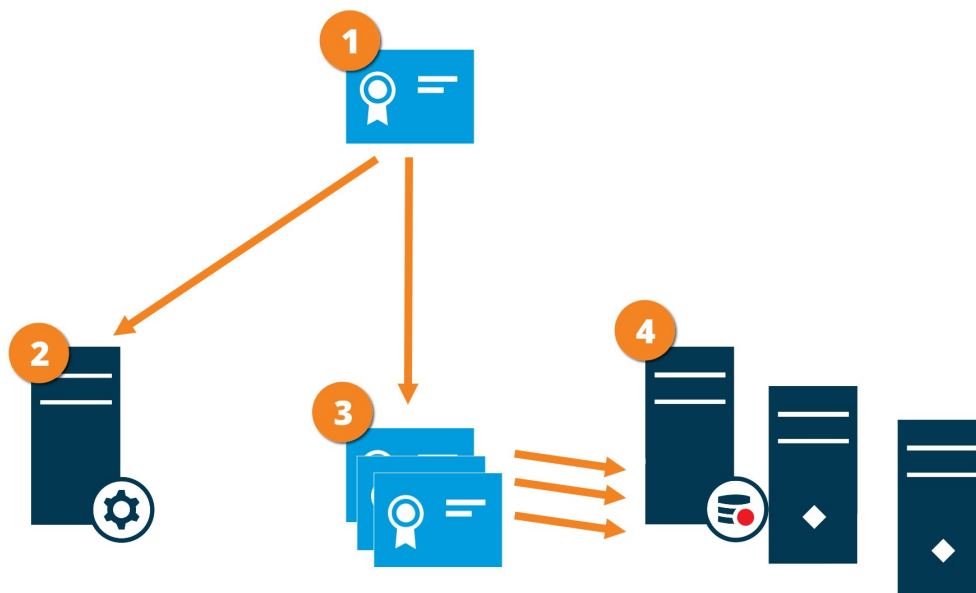
You can encrypt the two-way connection between the management server and the Data Collector affiliated when you have an external server of the following type:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

When you enable encryption on the management server, it applies to connections from all the Data Collector servers that connect to the management server. Encryption of this communication must follow the encryption setting on the management server. So, if management server encryption is enabled, this must also be enabled on the Data Collector servers affiliated with each external server, and vice-versa. Before you enable encryption, you must install security certificates on the management server and all Data Collector servers affiliated with the external servers.

Certificate distribution

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



- ❶ A CA certificate acts as a trusted third party, trusted by both the subject/owner (data collector server) and by the party that verifies the certificate (management server)
- ❷ The CA certificate must be trusted on the management server. In this way the management server can verify the validity of the certificates issued by the CA
- ❸ The CA certificate is used to establish secure connection between the data collector servers and the management server
- ❹ The CA certificate must be installed on the computers on which the data collector servers are running

Requirements for the private data collector server certificate:

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

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

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

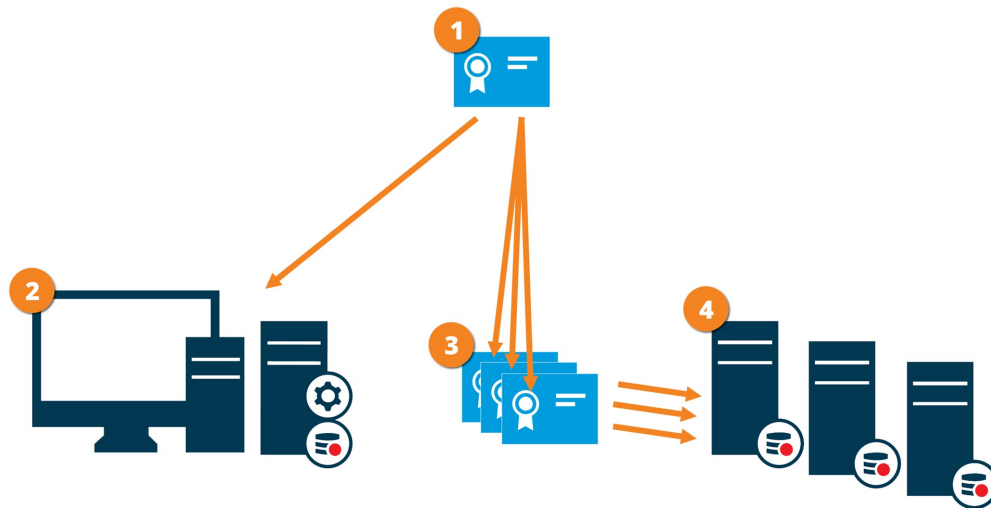
- XProtect Smart Client
- Management Client
- Management Server (for System Monitor and for images and AVI video clips in email notifications)
- XProtect Mobile Server
- XProtect Event Server
- XProtect LPR
- ONVIF Bridge
- XProtect DLNA Server
- Sites that retrieve data streams from the recording server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



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

Certificate distribution

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



- ❶ A CA certificate acts as a trusted third-party, trusted by both the subject/owner (recording server) and by the party that verifies the certificate (all clients)
- ❷ The CA certificate must be trusted on all clients. In this way the clients can verify the validity of the certificates issued by the CA
- ❸ The CA certificate is used to establish secure connection between the recording servers and all clients and services
- ❹ The CA certificate must be installed on the computers on which the recording servers are running

Requirements for the private recording server certificate:

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



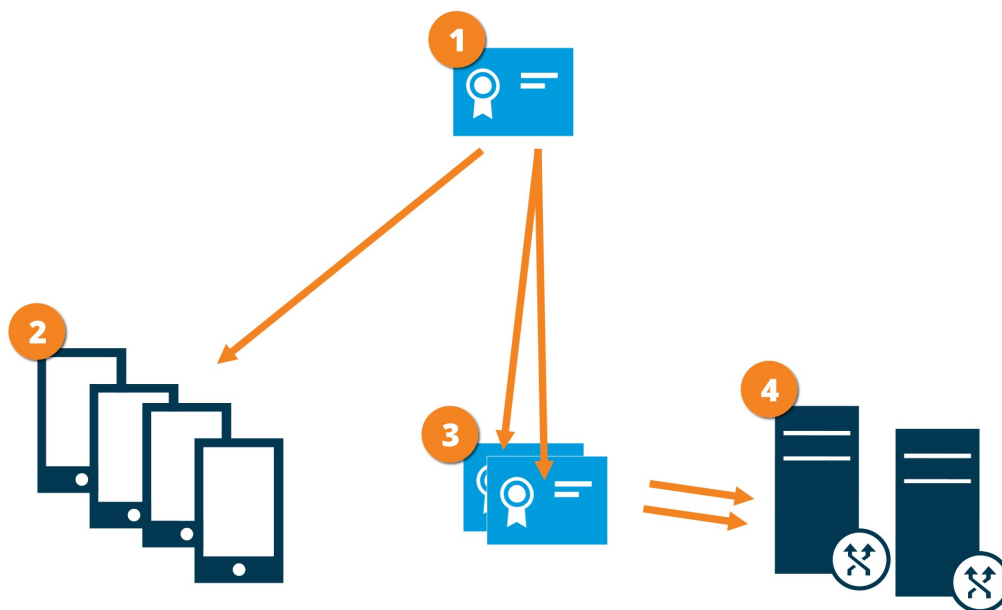
If you enable encryption on the recording servers and your system applies failover recording servers, Milestone recommends that you also prepare the failover recording servers for encryption.

Mobile server data encryption (explained)

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

Certificate distribution for mobile servers

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



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

Requirements for the CA certificate:

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

Mobile server encryption requirements for clients

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

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

Enable encryption

Enable encryption to and from the management server

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see Management server encryption (explained) on page 31.

Prerequisites:

- A server authentication certificate is trusted on the computer that hosts the management server

First, enable encryption on the management server.

Steps:

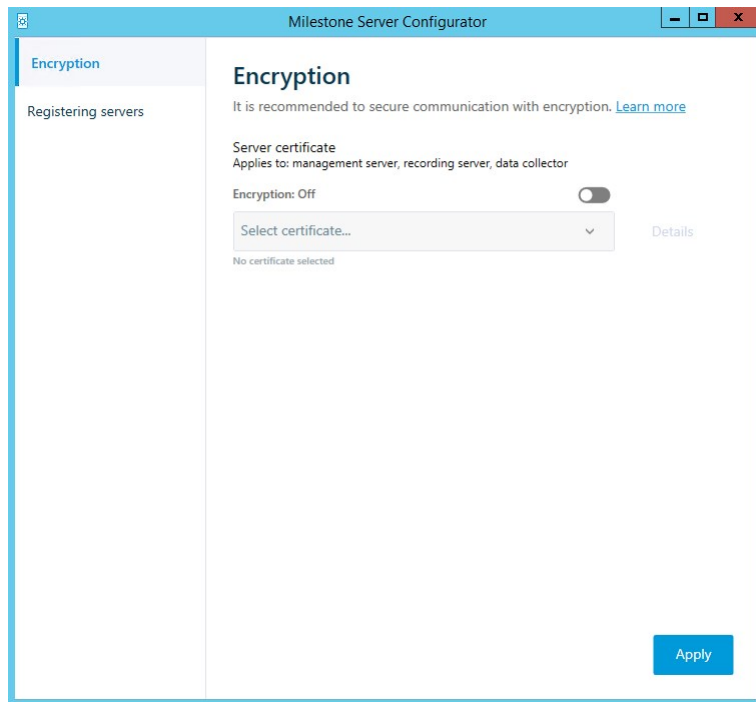
1. On the computer that runs the management server, right-click the Management Server Manager icon in the notification area and select **Server Configurator**.

The **Server Configurator** window appears. The options in this window depend on what servers are installed on the computer.

2. Under **Server certificate**, turn on encryption and select the certificate to encrypt communication between the recording server, management server and data collector server.

When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.

To complete the enabling of encryption, the next step is to update the encryption settings on each recording server and each server with a data collector (Event Server, Log Server, LPR Server, and Mobile Server). For more information, see [Enable server encryption for recording servers or remote servers](#) on page 39.

Enable server encryption for recording servers or remote servers

You can encrypt the two-way connection between the management server and the recording server or other remote servers with the data collector (Event Server, Log Server, LPR Server, and Mobile Server).

If your system contains multiple recording servers or remote servers, you must enable encryption on all of them. For more information, see [Encryption from the management server to the recording server \(explained\)](#) on page 32 and [Encryption between the management server and the Data Collector Server \(explained\)](#) on page 34.

Prerequisites:

- You have enabled encryption on the management server, see [Enable encryption](#) on page 38

Steps:

1. On each computer that runs a recording server or remote server with a data collector, open the **Server Configurator** from the Windows startup menu.

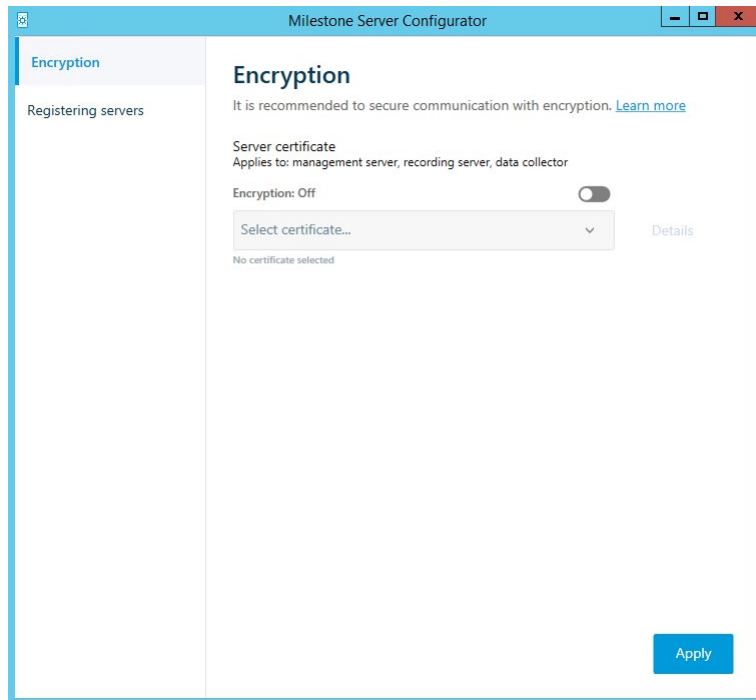
The options in this window depend on what servers are installed on the computer.

2. In the **Server Configurator**, under **Server certificate**, turn on encryption and select the certificate to encrypt communication between the recording server, management server and data collector server.

When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

The recording server service user has been given access to the private key. It is required that this certificate is trusted on all clients.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.



When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

Enable encryption to clients and servers

You can encrypt connections from the recording server to clients and servers that stream data from the recording server. For more information, see Encryption to clients and servers that retrieve data from the recording server (explained) on page 35.

Prerequisites:

- The server authentication certificate to be used is trusted on all computers running services that retrieve

data streams from the recording server

- XProtect Smart Client and all services that retrieve data streams from the recording server must be version 2019 R1 or later
- Some third-party solutions created using MIP SDK versions earlier than 2019 R1 may need to be updated

Steps:

1. On each computer that runs a recording server or remote server with a data collector, open the **Server Configurator** from the Windows startup menu.

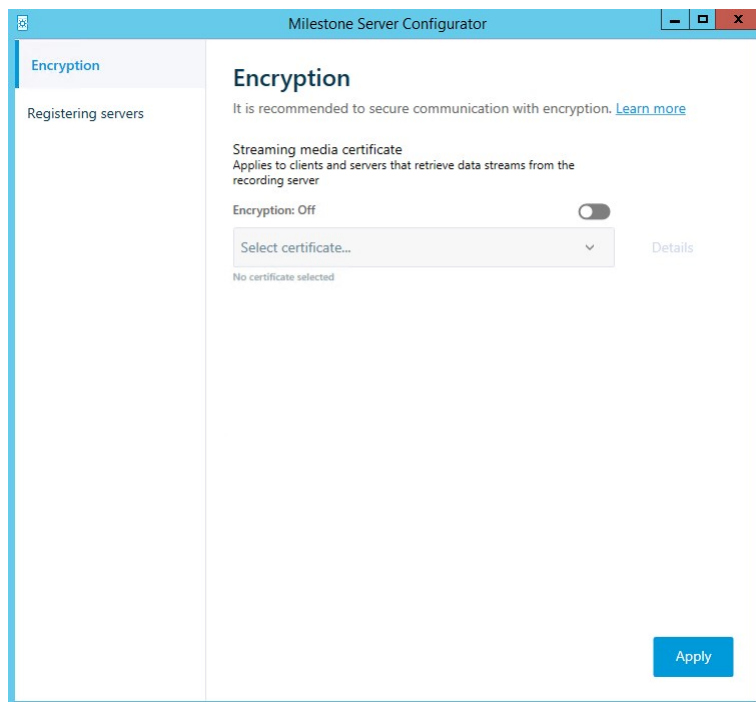
The options in this window depend on what servers are installed on the computer.

2. In the **Server Configurator**, under **Streaming media certificate**, turn on encryption and select the certificate to encrypt communication between the clients and servers that retrieve data streams from the recording server.

When you select a certificate, a list appears with unique subject names of certificates installed on the local computer in the Windows Certificate Store that has a private key.

The recording server service user has been given access to the private key. It is required that this certificate is trusted on all clients.

Select **Details** to view Windows Certificate Store information about the selected certificate.



3. Click **Apply**.



When you apply certificates, the recording server will be stopped and restarted. Stopping the Recording Server service means that you cannot record and view live video while you are verifying or changing the recording server's basic configuration.

To verify if the recording server uses encryption, see View encryption status to clients.


Enable encryption on the mobile server

To use an HTTPS protocol for establishing secure connection between the mobile server and clients and services, you must apply a valid certificate on the server. The certificate confirms that the certificate holder is authorized to establish secure connections. For more information, see Mobile server data encryption (explained) on page 37 and Mobile server encryption requirements for clients on page 38.



Certificates issued by CA (Certificate Authority) have a chain of certificates and on the root of that chain is the CA root certificate. When a device or browser sees this certificate, it compares its root certificate with pre-installed ones on the OS (Android, iOS, Windows, etc.). If the root certificate is listed in the pre-installed certificates list, then the OS ensures the user that the connection to the server is secure enough. These certificates are issued for a domain name and are not free of charge.


To enable encryption, after the mobile server has been installed:

1. On a computer with a mobile server installed, right-click the Mobile Server Manager tray icon in the taskbar of the operating system and select **Edit certificate**.
2. Select the **Encrypt the connections for clients and services that retrieve data streams from the mobile server** check box.
3. To select a valid certificate, click . A Windows Security dialog box opens.
4. Select the certificate that you want to apply.
5. Click **OK**.

Edit certificate

If the certificate that you use for secure connection has expired, you can select another certificate that is installed on the computer on which the mobile server is running.

To change a certificate:

1. On a computer with a mobile server installed, right-click the Mobile Server Manager tray icon in the taskbar of the operating system and select **Edit certificate**.
2. To select a valid certificate, click . A Windows Security dialog box opens.
3. Select the certificate that you want to apply.
4. Click **OK**.

A message informs you that the certificate has been installed and that the Mobile Server service has been restarted to apply the change.

Milestone Federated Architecture and master/slave servers (explained)

If your system supports Milestone Federated Architecture or servers in a master/slave setup, you can access such servers with your XProtect Mobile client or XProtect Web Client. Use this functionality to gain access to all cameras on all slave servers by logging in to the master server.

If in a Milestone Federated Architecture setup, you gain access to child sites via the central site. Install the XProtect Mobile server only on the central site.

This means that when users of XProtect Mobile client or XProtect Web Client log in to a server to see cameras from all servers in your system, they must connect to the IP address of the master server. Users must have administrator rights on all servers in the system in order for the cameras to show up in the XProtect Mobile client or XProtect Web Client.

Smart Connect (explained)

Smart Connect enables you verify that you have configured the XProtect Mobile correctly without logging in with a mobile device or a tablet to do the validation. It also simplifies the connection process for the XProtect Mobile client and XProtect Web Client users.

This feature requires that your XProtect Mobile server uses a public IP address and that your system is licensed with a Milestone Care Plus subscription package.

The system gives you instant feedback in the Management Client if the remote connectivity setup has been set up successfully and confirms that the XProtect Mobile server is accessible from the Internet.

Smart Connect enables the XProtect Mobile server to switch seamlessly between internal and external IP addresses and connect to the XProtect Mobile from any location.

To make it easier to set up customers' mobile clients, you can send an email directly from within the Management Client to the end-user. The email includes a link that adds the server directly to XProtect Mobile. This completes the setup without any need to enter network addresses or ports.

Set up Smart Connect


To set up the Smart Connect feature, do the following:

1. In Management Client, in the navigation pane, expand **Servers**, and select **Mobile Servers**.
2. Select the mobile server and click the **Connectivity** tab.
3. Enable Universal Plug and Play discoverability on your router.
4. Configure connection settings.
5. Send an email message to users.
6. Enable connections on complex network.

Enable Universal Plug and Play discoverability on your router

To make it easy to connect mobile devices to XProtect Mobile servers, you can enable Universal Plug and Play (UPnP) on your router. UPnP enables XProtect Mobile server to configure port forwarding automatically. However, you can also manually set up port forwarding on your router by using its web interface. Depending on the router, the process for setting up port mapping can differ. If you are not sure how to set up port forwarding on your router, see the documentation for that device.



Every five minutes, the XProtect Mobile Server service verifies that the server is available to users on the Internet. The status displays in the upper-left corner of the **Properties** pane: **Server accessible through internet:** .

Enable connections on complex network

If you have a complex network where you have custom settings, you can provide the information users need to connect.

On the **Connectivity** tab, in the **Internet Access** group, specify the following:

- If you use UPnP port mapping, to direct connections to a specific connection, select the **Configure custom Internet access** check box. Then provide the **IP address or host name**, and the port to use for the connection. For example, you might do this if your router does not support UPnP, or if you have a chain of routers
- If your IP addresses often change, select the **Check to retrieve IP address dynamically** check box

Configure connection settings

1. In Management Client, in the navigation pane, expand **Servers**, and select **Mobile Servers**.
2. Select the server and click the **Connectivity** tab.
3. Use the options in the **General** group to specify the following:
 - To make it easy for XProtect Mobile client and XProtect Web Client users to connect to XProtect Mobile servers, select the **Enable Smart Connect** check box
 - Specify the protocol to use in the **Connection type** field
 - Before you turn on secure connections, make sure that you are familiar with digital certificates. To learn how to add a certificate in XProtect Mobile server, see Edit certificate on page 42
 - Set a time frame for how often the XProtect Mobile client and XProtect Web Client must indicate to the mobile server that they are up and running
 - To make the XProtect Mobile server discoverable on the network by means of the UPnP protocols, select the **Enable UPnP discoverability** check box
 - To enable the XProtect Mobile server, do the port mapping by itself if the router is configured for it, select the **Enable automatic port mapping** check box

Send an email message to users

To make it easier to set up XProtect Mobile client and XProtect Web Client, you can send an email directly from within the Management Client to the end-user. The email includes a link that adds the server directly to XProtect Mobile. This completes the setup without any need to enter network addresses or ports.

1. In the **Email invitation to** field, enter the email address for the recipient of the Smart Connect notification, and then specify a language.
2. Next, do one of the following:
 - To send the message, click **Send**
 - Copy the information to the messaging program you use

For more information, see:

Requirements for Smart Connect setup on page 11

Connectivity tab on page 17

Sending notifications (explained)

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. When XProtect Mobile is open on the mobile device, the app delivers the notification. System notifications are also delivered even when the app is not running. Users can specify the types of notifications they want to receive. For example, a user can choose to receive notifications for the following:

- All alarms
- Only alarms assigned to them
- Only alarms related to the system

These might be when a server goes offline or comes back online.

You can also use push notifications to notify users who don't have XProtect Mobile open. These are called push notifications. Push notifications are delivered to the mobile device, and are a great way to keep users informed while they're on the go.

Using push notifications



To use push notifications, your system must have access to the Internet.

Push notifications use cloud services from Apple, Microsoft, and Google:

- Apple Push Notification service (APN)
- Microsoft Azure Notification Hub
- Google Cloud Messaging Push Notification service

There is a limit to the number of notifications that your 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.

See also Requirements for notifications setup on page 10 and Notifications tab on page 25.

Set up push notifications on XProtect Mobile server

To set up push notifications, follow these steps:

1. In Management Client, select the mobile server, and then click the **Notifications** tab.
2. To send notifications to all mobile devices that connect to the server, select the **Notifications** check box.
3. To store information about the users and mobile devices that connect to the server, select the **Maintain device registration** check box.



The server sends notifications only to the mobile devices in this list. If you clear the **Maintain device registration** check box and save the change, the system clears the list. To receive push notifications again, users must reconnect their device.

Enable sending push notifications to specific or all mobile devices

To enable XProtect Mobile, notify users when an event occurs by sending push notifications to specific or all mobile devices:

1. In Management Client, select the mobile server, and then click the **Notifications** tab.
2. Do one of the following:
 - For individual devices, select the **Enabled** check box for each mobile device listed in the **Registered devices** table
 - For all mobile devices, select the **Notifications** check box

Stop sending push notifications to specific or all mobile devices

There are several ways to stop sending push notifications to specific or all mobile devices.

1. In Management Client, select the mobile server, and then click the **Notifications** tab.
2. Do one of the following:
 - For individual devices, clear the **Enabled** check box for each mobile device. The user can use another device to connect to the XProtect Mobile server
 - For all devices, clear the **Notifications** check box

To temporarily stop for all devices, clear the **Maintain device registration** check box and then save your change. The system sends notifications again after users reconnect.

Set up investigations

Set up investigations so that people can use XProtect Web Client or XProtect Mobile to access recorded video and investigate incidents, and to prepare and download video evidence.

To set up investigations, follow these steps:

1. In Management Client, click the mobile server, and then click the **Investigations** tab.
2. Select the **Enabled** check box. By default, the check box is selected.
3. In the **Investigations folder** field, specify where to store video for investigations.
4. In the **Limit size of investigations folder to** field, enter the maximum number of megabytes that the investigation folder can contain.
5. Optional: To allow users to access investigations that other users create, select the **View investigations made by other users** check box. If you do not select this check box, users can see only their own investigations.
6. Optional: To include the date and time that a video was downloaded, select the **Include timestamps for AVI exports** check box.

7. In the **Used codec for AVI exports** field, select the compression format to use when preparing AVI packages for download.



The codecs in the list can differ, depending on your operating system. If you do not see the codec you want to use, you can install it on the computer where Management Client is running, and it will display in this list.



Additionally, codecs can use different compression rates, which can affect video quality. Higher compression rates reduce storage requirements but can also reduce quality. Lower compression rates require more storage and network capacity but can increase quality. It's a good idea to research the codecs before you select one.

8. From the **Used audio bit rate for AVI exports** list, select the appropriate audio bit rate when audio is included in your video export. The default is 160000 Hz.
9. In the **Keep or delete data when exports fail (MKV and AVI)** field, specify whether to keep the data that was successfully downloaded, although it can be incomplete, or delete it.



To enable users to save investigations, you must grant the **Export** permission to the security role assigned to the users.

Clean up investigations

If you have investigations or video exports that you no longer need to keep, you can delete them. For example, this can be useful if you want to make more disk space available on the server.

- To delete an investigation, and all of the video exports that were created for it, select the investigation in the list, and then click **Delete**.
- To delete individual video files that were exported for an investigation, but keeping the investigation, select the investigation in the list. In the **Investigation details** group, click the **Delete** icon to the right of the **Database**, **AVI**, or **MKV** fields for exports.

Using Video Push to stream video (explained)

You can set up Video Push so that users can keep others informed about a situation, or record video to investigate it later, by streaming video from their mobile device's camera to your XProtect surveillance system. The video stream may have audio as well.

See also Video Push tab on page 25 and Requirements for Video Push setup on page 11.

Set up Video Push to stream video

To let users stream video from their mobile devices to the XProtect system, set up Video Push on the XProtect Mobile server.

In Management Client, perform these steps in the following order:

1. On the **Video Push** tab, select the **Video Push** check box to enable the feature.
2. Add a Video Push channel for streaming video.
3. Add the Video Push Driver as a hardware device on the Recording Server. The driver simulates a camera device so that you can stream video to the Recording Server.
4. Add the Video Push Driver device to the channel for Video Push.

Add a Video Push channel for streaming video

To add a channel, follow these steps:

1. In the navigation pane, select **Mobile Server**, then select the mobile server.
2. On the **Video Push** tab, select the **Video Push** check box.
3. In the bottom-right corner, click **Add** to add a video push channel under **Channels mapping**.
4. Enter the user name of the user account (added under **Roles**) that will use the channel. This user account must be allowed to access the XProtect Mobile server and the recording server (on the **Overall Security** tab).



To use Video Push, users must log in to XProtect Mobile on their mobile device using the user name and password for this account.

5. Make a note of the port number. You will need it when you add the Video Push driver as a hardware device on the recording server.
6. Click **OK** to close the Video Push Channel dialog box and to save the channel.

Remove a Video Push channel

You can remove channels that you no longer use:

- Select the channel to remove, then click **Remove** in the bottom-right corner

Add the Video Push Driver as a hardware device on the Recording Server

1. In the navigation pane, click **Recording Servers**.
2. Right-click the server that you want to stream video to and click **Add Hardware** to open the **Add Hardware** wizard.

3. Select **Manual** as the hardware detection method and click **Next**.
4. Enter login credentials for the camera:
 - For user name, enter the factory defaults or the user name specified on the camera
 - For password: Enter **Milestone**, and then click **Next**



These credentials are for the hardware, not the user. The credentials are not related to the user name for the channel.

5. In the list of drivers, expand **Milestone**, select the **Video Push Driver** check box, and click **Next**.



The system generates a MAC address for the Video Push Driver device. We recommend that you use this address. Change it only if you experience problems with the Video Push Driver device or, for example, if you need to add a new address and port number.

6. In the **Address** field, enter the IP address of the computer where XProtect Mobile server is installed.
7. In the **Port** field, enter the port number for the channel that you created for streaming video. The port number was assigned when you created the channel.
8. In the **Hardware model** column, select **Video Push Driver**, and then click **Next**.
9. When the system detects the new hardware, click **Next**.
10. In the **Hardware name template** field, specify whether to display either the model of the hardware and the IP address, or the model only.
11. Specify whether to enable related devices by selecting the **Enabled** check box. You can add related devices to the list for **Video Push Driver**, even though they are not enabled. You can enable them later.



If you want to use location information when you stream video, you must enable the **Metadata** port.



If you want to play audio when you stream video, you must enable the microphone related to the camera that you use for video streaming.

12. Select the default groups for the related devices on the left or select a specific group in the **Add to Group** field. Adding devices to a group can make it easier to apply settings to all devices at the same time or replace devices.


Add the Video Push Driver device to the channel for Video Push

To add the Video Push Driver device to the channel for video push, follow these steps:

1. In the **Site navigation** pane, click **Mobile Servers**, and then click the **Video Push** tab.
2. Click **Find Cameras**. If successful, the name of the Video Push Driver camera displays in the **Camera Name** field.
3. Save your configuration.

Enable audio for existing video push channel

After you have fulfilled the requirements for enabling audio in video push (see Requirements for Video Push setup on page 11), in Management Client:

1. In the **Site Navigation** pane, expand the **Servers** node and click **Recording Servers**.
2. In the overview pane, select the relevant recording server folder, then expand the **Video Push Driver** folder and right-click the video push - related microphone.
3. Select **Enabled** to enable the microphone.
4. In the same folder, select the video push - related camera.
5. In the **Properties** pane, click the **Client** tab (see Client tab properties).
6. On the right-hand side of the **Related microphone** field, click . The **Selected device** dialog box opens.
7. On the **Recording servers** tab, expand the recording server folder and select the video push related microphone.
8. Click **OK**.

Set up users for two-step verification via email



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

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

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

In Management Client, perform these steps:

1. Enter information about your SMTP server on page 52.
2. Specify the verification code that will be sent to users on page 52.
3. Assign login method to users and Active Directory groups on page 52.

See also Requirements for user's two-step verification setup on page 11 and Two-step verification tab on page 26.

Enter information about your SMTP server

The provider uses the information about the SMTP server:

1. In the navigation pane, select **Mobile Servers** and select the relevant mobile server.
2. On the **Two-step verification** tab, select the **Enable two-step verification** check box.
3. Below **Provider settings**, on the **Email** tab, enter information about your SMTP server and specify the email that the system will send to client users when they log in and are set up for a secondary login. For details about each parameter, see Two-step verification tab on page 26.

For more information, see Two-step verification tab on page 26.

Specify the verification code that will be sent to users

To specify the complexity of the verification code:

1. On the **Two-step verification** tab, in the **Verification code settings** section, specify the period within which XProtect Mobile client users do not have to reverify their login in case of, for example, a disconnected network. The default period is three minutes.
2. Specify the period within which the user can use the received verification code. After this period, the code is invalid, and the user must request for a new code. The default period is five minutes.
3. Specify the maximum number of code entry attempts before the provided code becomes invalid. The default number is three.
4. Specify the number of characters for the code. The default length is six.
5. Specify the complexity of the code that you want the system to generate.

For more information, see Two-step verification tab on page 26.

Assign login method to users and Active Directory groups

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

1. In the **Login method** column, select a verification method for each user or group.
2. In the **Details** field, add the delivery details such as email addresses of individual users. Next time the user logs into XProtect Web Client or the XProtect Mobile app, he or she is asked for a secondary login.

3. If a group is configured in Active Directory, the XProtect Mobile server uses details, such as email addresses, from Active Directory.



Windows groups do not support two-step verification.

4. Save your configuration.

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

For more information, see Two-step verification tab on page 26.

Actions (explained)

You can manage the availability of the **Actions** tab in the XProtect Mobile client or XProtect Web Client by enabling or disabling **Actions** on the **General** tab. **Actions** are by default enabled, and all available actions for the connected devices are shown here.

For more information, see General tab on page 15.

Naming an output for use in XProtect Mobile client and XProtect Web Client (explained)

To get actions to show correctly together with current camera, you must create an output group that has the same name as the camera.

Example:

When you create an output group with outputs attached to a camera named "AXIS P3301, P3304 - 10.100.50.110 - Camera 1", you must enter the same name in the **Name** field (under the **Device group information**).

In the **Description** field, you can add a further description, for example "AXIS P3301, P3304 - 10.100.50.110 - Camera 1 - Light switch".



If you do not follow these naming conventions, actions are not available in the action list for the associated camera's view. Instead, actions appear in the list of other actions on the **Actions** tab.

For more information, see Output devices (explained).

Maintenance

Mobile Server Manager (explained)

The Mobile Server Manager is a tray-controlled feature connected to the mobile server. Right-clicking the Mobile Server Manager tray icon in the notification area opens a menu from which you can access mobile server functionality.

You can:

- Access XProtect Web Client on page 54
- Start, stop and restart Mobile Server service on page 55
- Fill in/edit management server address on page 55
- Show/edit port numbers on page 55
- Edit certificate on page 42
- Open today's log file (see Accessing logs and investigations (explained) on page 56)
- Open Log folder (see Accessing logs and investigations (explained) on page 56)
- Open investigations folder (see Accessing logs and investigations (explained) on page 56)
- Change investigations folder on page 56
- See XProtect Mobile Server status (see Show status (explained) on page 57)

Access XProtect Web Client

If you have a XProtect Mobile server installed on your computer, you can use the XProtect Web Client to access your cameras and views. Because you do not need to install XProtect Web Client, you can access it from the computer where you installed the XProtect Mobile server, or any other computer you want to use for this purpose.

1. Set up the XProtect Mobile server in the Management Client.
2. If you are using the computer where XProtect Mobile server is installed, you can right-click the Mobile Server Manager tray icon in the notification area and select **Open XProtect Web Client**.
3. If you are not using the computer where XProtect Mobile server is installed, you can access it from a browser. Continue with step 4 in this process.
4. Open an Internet browser (Internet Explorer, Mozilla Firefox, Google Chrome or Safari).

5. Enter the external IP address, that is, the external address and port of the server on which the XProtect Mobile server is running.

Example: The XProtect Mobile server is installed on a server with the IP address 127.2.3.4 and is configured to accept HTTP connections on port 8081 and HTTPS connections on port 8082 (default settings of the installer).

In the address bar of your browser, enter: **http://127.2.3.4:8081** if you want to use a standard HTTP connection or **https://127.2.3.4:8082** to use a secure HTTPS connection. You can now begin using XProtect Web Client.

6. Add the address as a bookmark in your browser for easy future access to XProtect Web Client. If you use XProtect Web Client on the local computer on which you installed the XProtect Mobile server, you can also use the desktop shortcut which the installer creates. Click the shortcut to launch your default browser and open XProtect Web Client.



You must clear the cache of Internet browsers running the XProtect Web Client before you can use a new version of the XProtect Web Client. System administrators must ask their XProtect Web Client users to clear their browser cache after upgrading or force this action remotely (you can do this action only in Internet Explorer in a domain).

Start, stop and restart Mobile Server service

If needed, you can start, stop and restart the Mobile Server service from the Mobile Server Manager.

- To perform any of these tasks, right-click the Mobile Server Manager icon and select **Start Mobile Server service**, **Stop Mobile Server service** or **Restart Mobile Server service**, respectively

Fill in/edit management server address

1. Right-click the Mobile Server Manager icon and select **Management server address**.
2. In the **Server URL** field, fill in the server's URL address.
3. Click **OK**.


Show/edit port numbers

1. Right-click the Mobile Server Manager icon and select **Show/edit port numbers**.
2. To edit the port numbers, enter the relevant port number. You can indicate a standard port number for HTTP connections or a secured port number for HTTPS connections, or both.
3. Click **OK**.

Edit certificate

If the certificate that you use for secure connection has expired, you can select another certificate that is installed on the computer on which the mobile server is running.

To change a certificate:

1. On a computer with a mobile server installed, right-click the Mobile Server Manager tray icon in the taskbar of the operating system and select **Edit certificate**.
2. To select a valid certificate, click . A Windows Security dialog box opens.
3. Select the certificate that you want to apply.
4. Click **OK**.

A message informs you that the certificate has been installed and that the Mobile Server service has been restarted to apply the change.

Accessing logs and investigations (explained)

The Mobile Server Manager lets you quickly access the log file of the day, open the folder where log files are saved, and open the folder where investigations are saved.

To open any one of these, right-click the Mobile Server Manager icon and select:

- **Open today's log file**
- **Open Log folder**
- **Open Investigation folder**



If you uninstall the XProtect Mobile server from your system, its log files are not deleted. Administrators with proper user rights can access these log files at a later time or decide to delete them if they are not needed any longer. The default location of the log files is in the **ProgramData** folder. If you change the default location of log files, existing logs are not copied to the new location nor are they deleted.

Change investigations folder

The default location of investigations is in the **ProgramData** folder. If you change the default location of the investigations folder, the existing investigations are not automatically copied to the new location nor are they deleted. To change the location where you save the investigation exports on your hard disk:

1. Right-click the Mobile Server Manager icon and select **Change investigations folder**.

The **Investigations location** window opens.

2. Next to the **Folder** field that shows the current location, click the folder icon to browse for an existing folder or create a new folder > Click **OK**.
3. From the **Old investigations** list, select the action that you want to apply to the existing investigations that are stored in the current location. The options are:

- **Move:** Moves the existing investigations to the new folder



If you do not move the existing investigations to the new folder, you will no longer be able to see them.

- **Delete:** Deletes the existing investigations
- **Do nothing:** The existing investigations remain in the current folder location. You will no longer be able to see them after you have changed the default location of the investigations folder

4. Click **Apply** > Click **OK**.

Show status (explained)

Right-click the Mobile Server Manager icon and select **Show Status** or double-click the Mobile Server Manager icon to open a window that shows the status of the XProtect Mobile server. You can see the following information:

Name	Description
Server running since	Time and date of the time when the XProtect Mobile server was last started.
Connected users	Number of users currently connected to the XProtect Mobile server.
Hardware decoding	Indicates if hardware accelerated decoding is in action on the XProtect Mobile server.
CPU usage	How many % of the CPU is currently being used by the XProtect Mobile server.
CPU usage history	A graph detailing the history of CPU usage by the XProtect Mobile server.

Troubleshooting

Troubleshooting XProtect Mobile

Connections

1. **Why can't I connect from my XProtect Mobile client to my recordings/XProtect Mobile server?**

In order to connect to your recordings, the XProtect Mobile server must be installed on the server that runs your XProtect system or alternatively on a dedicated server. The relevant XProtect Mobile settings are also needed in your XProtect video management setup. These are installed as either plug-ins or as part of a product installation or upgrade. For details on how to get the XProtect Mobile server and how to integrate the XProtect Mobile client-related settings in your XProtect system, see the configuration section (see Mobile server settings on page 15).

2. **I just turned on my firewall, and now I can't connect a mobile device to my server. Why not?**

If your firewall was turned off while you installed XProtect Mobile server, you must manually enable TCP and UDP communications.

3. **How to avoid the security warning when I run XProtect Web Client through an HTTPS connection?**

The warning appears because the server address information in the certificate is incorrect. The connection will still be encrypted.

The self-signed certificate in the XProtect Mobile server needs to be replaced with your own certificate matching the server address used to connect to the XProtect Mobile server. These certificates are obtained through official certificate signing authorities such as Verisign. Consult the chosen signing authority for more details.

XProtect Mobile server does not use Microsoft IIS. This means that instructions provided for generating certificate signing request (CSR) files by the signing authority using the IIS is not applicable for the XProtect Mobile server. You must manually create CSR-file using command line certificate tools or other similar third-party application. This process should be performed by system administrators and advanced users only.

Image quality

1. **Why is the image quality sometimes poor when I view video in the XProtect Mobile client?**

The XProtect Mobile server automatically adjusts image quality according to the available bandwidth between the server and client. If you experience lower image quality than in the XProtect® Smart Client, you might have too little bandwidth to get full resolution images through the XProtect Mobile client. The reason for this can either be too little upstream bandwidth from the server or too little downstream bandwidth on the client. See the **XProtect Smart Client User Manual** which you can download from our website (<https://www.milestonesys.com/support/help-yourself/manuals-and-guides/>).

If you are in an area with mixed wireless bandwidth, you may notice that the image quality improves when you enter an area with better bandwidth.

2. **Why is the image quality poor when I connect to my XProtect video management system at home through Wi-Fi at my office?**

Check your home internet bandwidth. Many private internet connections have different download and upload bandwidths often described as, for example, 20 Mbit/2 Mbit. This is because home users rarely need to upload large amounts of data to the internet but consume a lot of data instead. The XProtect video management system needs to send video to the XProtect Mobile client and is limited by your connection's upload speed. If low image quality is consistent on multiple locations where the download speed of the XProtect Mobile client's network is good, the problem might be solved by upgrading the upload speed of your home internet connection.

Hardware accelerated decoding

1. **Does my processor support hardware-accelerated decoding?**

Only newer processors from Intel support hardware accelerated decoding. Check Intel website (<https://ark.intel.com/Search/FeatureFilter?productType=processors/>) if your processor is supported.

In the menu, make sure **Technologies > Intel Quick Sync Video** is set to **Yes**.

If your processor is supported, hardware-accelerated decoding is enabled by default. You can see the current status in **Show status** in the Mobile Server Manager (see Show status (explained) on page 57).

2. **Does my operating system support hardware-accelerated decoding?**

All the operating systems that XProtect supports also support hardware acceleration.

Make sure you install the newest graphic drivers from the Intel website on your system. These drivers are not available from Windows Update.

Hardware-accelerated decoding is not supported, if the mobile server is installed in a virtual environment.

3. **How do I disable hardware-accelerated decoding on the mobile server? (Advanced)**

If the processor on the mobile server supports hardware accelerated decoding, it is by default enabled. To turn hardware-accelerated decoding off, do the following:

1. Locate the file VideoOS.MobileServer.Service.exe.config. The path is typically: C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config.
2. Open the file in Notepad or a similar text editor. If necessary, associate the file type .config with Notepad.
3. Locate the field <add key="HardwareDecodingMode" value="Auto" />.
4. Replace the value "Auto" with "Off".
5. Save and close the file.



helpfeedback@milestone.dk

About Milestone

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

