

MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile server 2024 R2

Administrator manual



Contents

Copyright, trademarks, and disclaimer	5
Overview	6
What's new?	6
XProtect Mobile	7
Requirements and considerations	8
Before you install the XProtect Mobile server	8
Requirements for notifications setup	8
Requirements for Smart Connect setup	8
Requirements for user's two-step verification setup	9
Requirements for Video Push setup	9
Requirements for direct streaming	9
Requirements for using Share	9
Installation	11
Install the XProtect Mobile server	11
Configuration	14
Mobile server settings	14
Connection information	14
General tab	15
Connectivity tab	17
Server Status tab	19
Performance tab	20
Investigations tab	23
Video Push tab	25
Notifications tab	26
Two-step verification tab	27
Direct streaming	29
Adaptive streaming	30
Mobile server data encryption (explained)	31

- Enable encryption on the mobile server33
- Milestone Federated Architecture and parent/child sites34
- Smart Connect34
 - Set up Smart Connect35
 - Enable Universal Plug and Play discoverability on your router35
 - Enable connections on complex network35
 - Configure connection settings36
 - Send an email message to users36
- Notifications36
 - Set up push notifications on XProtect Mobile server37
 - Enable sending push notifications to specific or all mobile devices38
 - Stop sending push notifications to specific or all mobile devices38
 - Remove one or all registered devices from the Registered devices list38
- Set up investigations39
- Using Video Push to stream video41
 - Set up Video Push to stream video41
 - Add a Video Push channel for streaming video41
 - Edit a Video Push channel42
 - Remove a Video Push channel42
 - Change password42
 - Add the Video Push Driver as a hardware device on the recording server43
 - Add the Video Push Driver device to the channel for Video Push44
 - Enable audio for existing video push channel44
- Set up users for two-step verification via email45
 - Enter information about your SMTP server45
 - Specify the verification code that will be sent to users45
 - Assign verification method to users and Active Directory groups46
- Actions46
- Mobile device management (MDM)47
 - Configure mobile server details on MDM platform (administrators)47

- Naming an output for use in XProtect Mobile client and XProtect Web Client48
- External IDP and XProtect Mobile49
 - Configure external IDP login for XProtect Web Client49
- Add Emergency Alert alarms50
- Maintenance51**
 - Mobile Server Manager51
 - Access XProtect Web Client51
 - Start, stop and restart Mobile Server service52
 - Change data protection password52
 - Show/edit port numbers53
 - Accessing logs and investigations53
 - Change investigations folder54
 - Show status54
 - Use a load balancer for the mobile server55
 - Migrate a mobile server to another host56
- Troubleshooting58**
 - Troubleshooting XProtect Mobile58
- Appendices61**
 - Appendix A61
 - Appendix B64

Copyright, trademarks, and disclaimer

Copyright © 2024 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

What's new?

In XProtect Mobile server 2023 R3

Connection information:

- Check if the mobile server is accessible from the internet. See [Connection information on page 14](#).

Alarms:

- Add Emergency Alert alarms to enable the users to receive alarm notifications of the highest severity level in the XProtect Mobile client. See [Add Emergency Alert alarms on page 50](#).

In XProtect Mobile server 2023 R2

Bookmarks and live video sharing:

- To share bookmarks and live video in the XProtect Mobile client, you must enable encryption on the management server. See [Requirements for using Share on page 9](#).

Notifications:

- You can remove device registration data from the VMS database. See [Remove one or all registered devices from the Registered devices list on page 38](#).

In XProtect Mobile server 2022 R3

External IDP:

- You can now log in to XProtect Web Client and the XProtect Mobile client with an external IDP. See [External IDP and XProtect Mobile on page 49](#)

Mobile device management (MDM):

- The XProtect Mobile client now supports mobile device management (MDM). With MDM, you can manage and secure devices, apps, and data from a unified console. For more information, see [Mobile device management \(MDM\) on page 47](#)

Push notifications:

- When you enable this feature, a warning informs you that your system may not be GDPR-compliant

In XProtect Mobile server 2022 R2

Notifications:

- Notifications are disabled by default

Installation:

- When installing Mobile Server, you can connect to the surveillance system with a basic user

XProtect Mobile

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.

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.

XProtect Mobile server

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

An 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 an XProtect Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats, allowing the streaming of video on the mobile device.

XProtect Mobile plug-in

The XProtect Mobile plug-in is part of the XProtect Mobile Server component. The XProtect Mobile plug-in allows you to view and manage the mobile servers in your VMS system from the **Servers** node in XProtect Management Client.

You install the XProtect Mobile plug-in on any computer with XProtect Management Client from which you want to manage the mobile servers.

Mobile Server Manager

Use the Mobile Server Manager to get information about the service, check the state of the Mobile Server service, view logs or status messages, and starting and stopping the service.

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

Requirements and considerations

Before you install the XProtect Mobile server

For information about the system requirements for the various VMS applications and system components, go to the Milestone website (<https://www.milestonesys.com/systemrequirements/>).

Milestone recommends that you install the XProtect Mobile server on a separate computer. Before you install and start using the XProtect Mobile Server component, make sure of the following:

- You have set up cameras and views in XProtect Management Client.
- The mobile server computer resolves the host names of the computers that run the other VMS server components.
- The management server computer resolves the host name of the mobile server computer.
- You have a running VMS installed.
- You have configured at least one VMS user. To connect to the surveillance system, the role to which this user is added requires permissions for the management server:
 - **Connect**
 - **Read**
 - **Edit**
- If you are upgrading your system, make sure that the version of the XProtect Mobile plug-in matches the version of the mobile server. Your system might not function properly if the versions of the plug-in and mobile servers are not identical.

Requirements for notifications setup

To notify users when an event occurs:

- You must associate one or more alarms with one or more events and rules. This is not required for system notifications
- You have an up-to-date Milestone Care™ agreement with Milestone Systems
- Your system must have access to the Internet

For more information, see:

[Set up push notifications on XProtect Mobile server on page 37](#)

[Notifications tab on page 26](#)

Requirements for Smart Connect setup

To use Smart Connect and verify that you have configured XProtect Mobile correctly, you must have:

- A public IP address for your XProtect Mobile server. The address can be static or dynamic, but typically it's a good idea to use static IP addresses
- A valid license for Smart Connect
- An up-to-date Milestone Care™ agreement with Milestone Systems

Requirements for user's two-step verification setup

To set up users for two-step verification via email:

- 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 service to enable the two-step verification feature.

For more information, see:

[Set up users for two-step verification via email on page 45](#)

[Two-step verification tab on page 27](#)

Requirements for Video Push setup

To stream video from a mobile device's camera to the XProtect surveillance system, you must have:

- A device license for each channel you use.

Requirements for direct streaming

XProtect Mobile supports direct streaming in live mode. 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 or the H.265 codec.



XProtect Web Client supports H.264 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**.

Requirements for using Share

Users can share bookmarks and live video while using the XProtect Mobile client app. These functionalities are available after:

- You have enabled encryption on the management server.

Installation

Install the XProtect Mobile server

Once you have installed the XProtect Mobile server, you can use the 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 the 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.

Download the XProtect Mobile server installer

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. Select **All Languages** for the XProtect Mobile server installer.

Install the XProtect Mobile server

1. Run the downloaded file. Then, select **Yes** to all warnings.
2. Select a language for the installer. Then, select **Continue**.
3. Read and accept the license agreement. Then, select **Continue**.
4. Select the installation type:
 - Select **Typical** to install XProtect Mobile server and plug-in
 - Select **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 an 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.

5. For custom installation only: Select the components that you want to be installed. Then, select **Continue**.

6. Select the service account for the mobile server. Then, select **Continue**.



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

7. For custom installation only: Log in with an existing VMS user account when connecting to the surveillance system:

- **Service account** is the account you selected in step 8. To connect using this account, make sure that the service account is a member of a domain to which the management server has access
- **Basic user.** Use a basic user when the service account is not a member of a domain to which the management server has access



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

Select **Continue**.

8. In the **Server URL** field, fill in the primary management server address.

For custom installation only: Specify the connection ports for communication with the mobile server. Then, select **Continue**. In a typical installation, the connection ports get the default port numbers (8081 for HTTP port and 8082 for HTTPS port).

9. On the **Assign a mobile server data protection password** page, enter a password to encrypt your investigations. As a system administrator, you will need to enter this password to access the mobile server data in case of system recovery or when expanding your system with additional mobile servers.



You must save this password and keep it safe. Failure to do so may compromise your ability to recover mobile server data.

If you do not want your investigations to be password-protected, select **I choose not to use a mobile server data protection password, and I understand that investigations will not be encrypted**.

Click **Continue**.

10. Specify the mobile server encryption. Then, select **Continue**.

On the **Select encryption** page, you can secure the communication flows:

- Between the mobile servers and the recording servers, data collectors, and the management server. To enable encryption for internal communication flows, in the **Server certificate** section, select a certificate

- Between the mobile servers and clients. To enable encryption between the mobile server and clients that retrieve data streams from the mobile server, in the **Streaming media certificate** section, select a certificate



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](#).

For more information about establishing secure communication in your system, see:

- [Mobile server data encryption \(explained\)](#)
- [The Milestone guide about certificates](#)

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 33](#)).

11. Select the file location and product language and then select **Install**.

When the installation is completed, a list of successfully installed components appears.

Configuration

Mobile server settings

In Management Client, you can configure and edit a list of XProtect Mobile server settings. You can access these settings on 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 (see [Connectivity tab on page 17](#))
- Set up the Smart Connect feature (see [Connectivity tab on page 17](#))
- See the current status of the server and the list of 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 notifications and push notifications (see [Notifications tab on page 26](#))
- Enable and configure an additional login step for users (see [Two-step verification tab on page 27](#))

Connection information

The following tables describe the statuses and messages of the mobile server that are visible on all tabs.

The server is accessible through the internet

Color	Status	Description
Orange	N/A	The mobile server has not been configured to be accessible from outside the local network.
Red	No	The XProtect Web Client and XProtect Mobile client users cannot connect to the mobile server from the internet.
Green	Yes	The XProtect Web Client and XProtect Mobile client users can connect to the mobile server from the internet.

Connection to server

Color	Message	Description
Orange	HTTPS invalid certificate	The XProtect Mobile plug-in does not recognize the certificate of the mobile server.
Orange	HTTP/HTTPS Unreachable	XProtect Management Client cannot reach the mobile server.
Red	HTTP/HTTPS Not connected	XProtect Management Client has detected the mobile server but cannot connect to it.
Green	HTTP/HTTPS	XProtect Management Client has established a connection with the mobile server.

General tab

The following table describes the settings on this tab.

General

Name	Description
Server name	Enter the 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.

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 the All cameras view for XProtect Mobile client	This view displays all the cameras that a user is allowed to view on a recording server. This feature is enabled by default.
Enable bookmarks	Enable the bookmarks feature to quickly locate video sequences in XProtect Mobile client and XProtect Web Client. This feature is enabled by default.
Enable actions (outputs and events)	<p>Enable access to actions in XProtect Mobile client and XProtect Web Client. This feature is enabled by default.</p> <p>If you disable this feature, the client users are not able to see output and events, even if these are configured correctly.</p>
Enable incoming audio	Enable the incoming audio feature in XProtect Web Client and XProtect Mobile client. This feature is enabled by default.
Enable push-to-talk	Enable the 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 36](#)
- [Send an email message to users on page 36](#)
- [Enable connections on complex network on page 35](#)
- [Enable Universal Plug and Play discoverability on your router on page 35](#)

For more information, see [Smart Connect on page 34](#).



You can configure how the XProtect Mobile client and XProtect Web Client users should connect to the XProtect Mobile server when you open the **Server Configurator** during installation or by right-clicking the Mobile Server Manager tray icon after installation. The connection type can either be HTTPS or HTTP. For more information, see [Enable encryption on the mobile server on page 33](#).

General

Name	Description
Client timeout	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

Name	Description
	<p>and running. The default value is 30 seconds.</p> <p>Milestone recommends that you do not increase the time frame.</p>
<p>Enable UPnP-discoverability</p>	<p>This makes the XProtect Mobile server discoverable on the network by means of the UPnP protocols.</p> <p>The XProtect Mobile client has scanning functionality for finding XProtect Mobile servers based on UPnP.</p>
<p>Enable automatic port mapping</p>	<p>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.</p> <p>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.</p>
<p>Enable Smart Connect</p>	<p>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.</p>

Internet access

Name	Description
<p>Configure custom internet access</p>	<p>Provide the IP address or hostname and the port number 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.</p>
<ul style="list-style-type: none"> • HTTP • HTTPS 	<p>Select the type of connection.</p>
<p>Select to retrieve IP address dynamically</p>	<p>Select the check box, if your IP addresses often change.</p>

Name	Description
Use the configured URL address only	Select the check box to connect to the mobile server with a custom-specified IP address or hostname only.
Server addresses	Lists all the URL 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	<p>Shows the current relation between the XProtect Mobile server and the XProtect Mobile client or XProtect Web Client user in question. Possible states are:</p> <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 (for XProtect Expert and XProtect Corporate only). This feature is enabled by default.
Enable adaptive streaming	Enable adaptive streaming in XProtect Web Client and XProtect Mobile client (for XProtect Expert and XProtect Corporate only). 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

Name	Description
	Mobile server performance.
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
- Investigate incidents
- Prepare and download video evidence

Name	Description
Enable investigations	Select this check box to allow users to create investigations.

Name	Description
Investigations folder	Shows where your video exports are saved on your hard drive.
View investigations made by other users	Select this check box to allow users to access investigations that they did not create.
Enable the size limit of investigations folder	Select this check box to set a size limit on the investigations folder and enter the maximum number of megabytes that the investigations folder can contain. The default size is 2000 MB.
Enable the investigation retention time	Select this check box to set a retention time for investigations. By default, the retention time is seven days.
Export formats	<p>Select the check box of the export format that you want to use. The available export formats are:</p> <ul style="list-style-type: none"> • AVI format • XProtect format • MKV format <p>By default, the check boxes are cleared.</p>
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	<p>Select the compression format to use when preparing AVI packages for download.</p> <p>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.</p>
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.

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 XProtect , 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 41](#)), 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.

By default, notifications are disabled.

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 38](#)

The following table describes the settings on this tab.

Name	Description
Notifications	Select this check box to turn on notifications.
Maintain device registration	Select this check box to store information about the devices and users who connect to this server. The system sends notifications to these devices. 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.

Registered devices

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

Two-step verification tab



Available functionality depends on the system you are using. See the complete feature list, which is available on the product overview page on the Milestone website (<https://www.milestonesys.com/products/software/xprotect-comparison/>).

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 45](#).

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. The 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.


Name	Description
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	<p>Enter the message you want to send. Example: Your code is {0}.</p> <div style="border: 1px solid #0070C0; background-color: #D9E1F2; padding: 5px; margin-top: 10px;">  <p>If you forget to include the {0} variable, the code is added at the end of the text by default.</p> </div>

Verification code settings

Name	Description
Reconnection timeout (0-30 minutes)	<p>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.</p> <p>This setting does not apply to XProtect Web Client.</p>
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 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:

Name	Description
	<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 style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6;">  Windows groups do not support two-step verification. </div>
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 the user name and password
User details	<p>Enter the email address to which each user will receive codes.</p>

Direct streaming

XProtect Mobile supports direct streaming in live mode.

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. XProtect® Mobile client also supports the use of the H.265 codec. 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 the XProtect Mobile client.

In Management Client, you can enable or disable direct streaming for clients (see [Mobile server settings on page 14](#)).

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 9](#))
- 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 with the server or with the camera has been lost
- You use the privacy masking feature during live video

Adaptive streaming

XProtect Mobile supports adaptive streaming in live mode.

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 that are running XProtect Mobile client and XProtect Web Client.

To take advantage of adaptive streaming, your cameras must have multiple streams defined with different resolutions. In this case, the feature enables 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 14](#)).

Mobile server data encryption (explained)

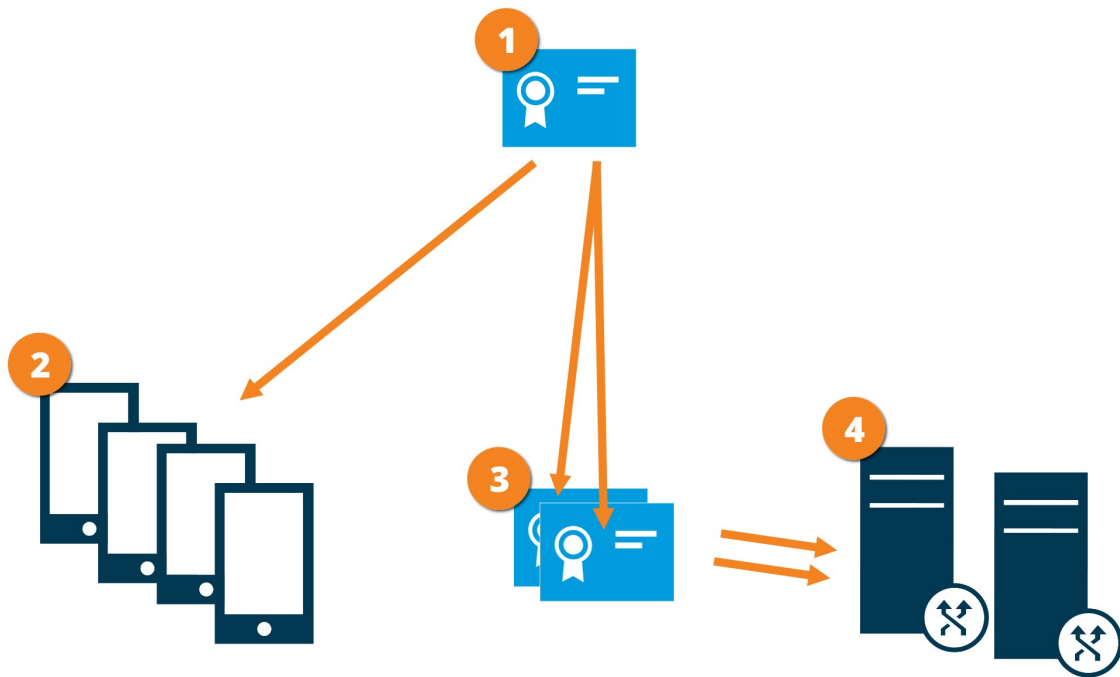
For security reasons, Milestone recommends that you use secure communication between the mobile server and clients when you manage user account settings.

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

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.



- ❶ 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)
- ❷ The CA certificate must be trusted on all clients. In this way, clients can verify the validity of the certificates issued by the CA
- ❸ The CA certificate is used to establish a secure connection between the mobile server and clients and services
- ❹ 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

For more information, see the [certificates guide about how to secure your XProtect VMS installations](#).

Enable encryption on the mobile server

To use an HTTPS protocol for establishing a 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 the [certificates guide about how to secure your XProtect VMS installations](#).



When you configure encryption for a server group, it must either be enabled with a certificate belonging to the same CA certificate or, if the encryption is disabled, then it must be disabled on all computers in the server group.



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.

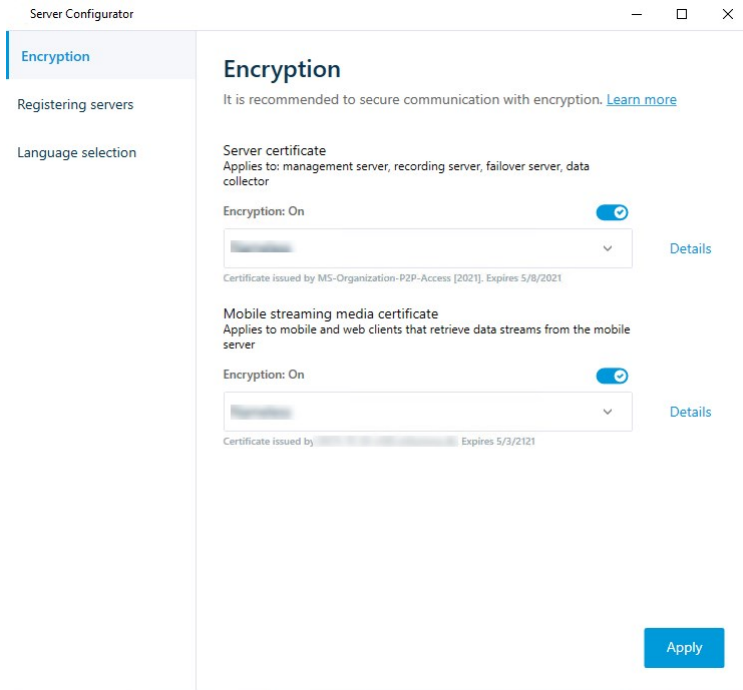
Steps:

1. On a computer with a mobile server installed, open the **Server Configurator** from:
 - The Windows Start menuor
 - The Mobile Server Manager by right-clicking the Mobile Server Manager icon on the computer task bar
2. In the **Server Configurator**, under **Mobile streaming media certificate**, turn on **Encryption**.
3. Click **Select certificate** to open a list with unique subject names of certificates that have a private key and that are installed on the local computer in the Windows Certificate Store.
4. Select a certificate to encrypt the communication of XProtect Mobile client and XProtect Web Client with the mobile server.

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

The Mobile Server service user has been given access to the private key. It is required that this certificate

be trusted on all clients.



5. Click **Apply**.



When you apply certificates, the Mobile Server service restarts.

Milestone Federated Architecture and parent/child sites

Milestone Federated Architecture links multiple individual systems into a federated site hierarchy of parent/child sites.

To gain access to all sites with your XProtect Mobile or XProtect Web Client, install the XProtect Mobile server only on the parent site.

Users of XProtect Mobile client or XProtect Web Client must connect to the management server on the parent site.

Smart Connect

Smart Connect enables you to 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

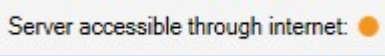
To set up the Smart Connect feature, do the following:

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 the 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: 

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
 - 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 8](#)

[Connectivity tab on page 17](#)

Notifications

You can enable XProtect Mobile to notify users when an event occurs, such as when an alarm triggers or something goes wrong with a device or server.

Notifications are always delivered, regardless if the app is running or not. 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.

By default, notifications are disabled.

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 8](#) and [Notifications tab on page 26](#).

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. Read the warning about your personal data and select **Yes** if you want to proceed.
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. Read the warning about your personal data and select **Yes** if you want to proceed

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.

Remove one or all registered devices from the Registered devices list

When you uninstall the XProtect Mobile app or disable the device, the device data may still be kept in the VMS database.

The VMS removes the device registration data when:

- You remove a user from the system.
- Milestone Care Plus has not been renewed for more than 180 days.

However, there are scenarios when the device registration data is not automatically removed.

You must manually remove one or all registered devices when:

- A user has lost his phone.
- You want to uninstall the mobile server completely and remove its data.
- A user has stopped using the XProtect Mobile client app or notifications.
- You have added an Active Directory (AD) group to a VMS role and the permissions for a user have changed. When you add an AD group, the VMS does not see the users in that role. If you remove a user from an AD group or restrict the user from using the mobile server, you must also manually remove the user's device from the list.

To remove a registered device:

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 device and then select **Remove**.
 - For all devices, select **Remove all**.


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 **Enable investigations** check box. By default, the check box is selected.
3. In the **Investigations folder** field, specify where to store video for investigations.
4. 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.
5. Select the **Enable the size limit of investigations folder** check box to set the maximum number of megabytes that the investigation folder can contain.
6. Select the **Enable the investigation retention time** check box to set a retention time for investigations. By default, the retention time is set to seven days.

- Under **Export formats**, select the check box of the export format that you want to use. The available export formats are:
 - **AVI format**
 - **XProtect format**
 - **MKV format**


 By default, the check boxes are cleared.

- (Optional) To include the date and time that a video was downloaded, select the **Include timestamps for AVI exports** check box.
- 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.

- 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.

 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 **XProtect**, **AVI**, or **MKV** fields for exports

Using Video Push to stream video

You can set up Video Push so that users can keep others informed about a situation or record a 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 9](#).

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 Servers**, then select the mobile server.
2. On the **Video Push** tab, select the **Video Push** check box.
3. Under **Channels mapping**, in the bottom-left corner, click **Add** to add a video push channel.
4. In the dialog box that appears, 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.



When you add a new Video Push channel on the mobile server, the system generates the port number and the MAC address of the channel that are used when the channel is added as a hardware device on the recording server. The system also generates the password that is used for connecting the Recording Server with the Mobile Server. The default password is **Milestone**.

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.
7. To save the channel, click **Save** in the upper-left corner of the navigation pane.

Edit a Video Push channel

You can edit the configuration details of a Video Push channel that you added:

1. Under **Channels mapping**, select the channel to edit, then click **Edit**.
2. When you are done with editing, click **OK** to close the Video Push Channel dialog box.
3. To save the edits, click **Save** in the upper-left corner of the navigation pane.



When you edit the port number and the MAC address of a Video Push channel, make sure to also replace the Video Push channel configuration details that you previously added on the recording server with the new information. Otherwise, the connection between the Recording Server and the Mobile Server will be broken.

Remove a Video Push channel

You can remove channels that you no longer use:

1. Under **Channels mapping**, select the channel to remove, then click **Remove**.
2. To save the change, click **Save** in the upper-left corner of the navigation pane.

Change password

You can change the automatically-generated password that is used to connect the Recording Server with the Mobile Server:

1. Under **Channels mapping**, in the bottom-right corner, click **Change password**.
2. In the **Change Video Push password** dialog box, type the new password in the first field, then repeat the new password in the second field, then click **OK**.
3. To save the change, click **Save** in the upper-left corner of the navigation pane.



When you change the Video Push channel password, the change will be applied to all Video Push channels that already exist in the list or will be added in the future. Even if you remove all existing Video Push channels from the list, the new password remains active and will be applied to future channels.



After the change is saved, all existing Video Push channels stop working because the connection between the Recording Server and the Mobile Server is broken. To restore this connection, in the navigation pane, by right-clicking the **Recording servers** tab, you must run the **Replace Hardware** wizard and enter the new password for the Video Push Driver that you added as a hardware device on the Recording Server.

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 the login credentials for the Video Push Driver:
 - User name: Leave the field blank to use the default user name.
 - Password: Enter **Milestone** - the password that is generated by the system. If you have changed it when adding the Video Push channel on the mobile server, enter the password that you prefer using. Then click **Next**



These credentials are for the hardware, not for the user. The credentials are not related to the user account that is used for accessing the Video Push channel.

5. In the list of drivers, expand **Milestone**, select the **Video Push Driver** check box, and click **Next**.
6. In the **Address** field, enter the IP address of the computer where the XProtect Mobile server is installed.



It is recommended that you use the MAC address generated by the system. Change it only if you experience problems with the Video Push Driver device or, for example, if you have edited the port number and the MAC address of the Video Push channel on the mobile server.

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 9](#)), 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.
For more information, see [Client tab \(devices\)](#).
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 the complete feature list, which is available on the product overview page on the Milestone website (<https://www.milestonesys.com/products/software/xprotect-comparison/>).

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 45](#).
2. [Specify the verification code that will be sent to users on page 45](#).
3. [Assign verification method to users and Active Directory groups on page 46](#).

See also [Requirements for user's two-step verification setup on page 9](#) and [Two-step verification tab on page 27](#).

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 more information, see [Two-step verification tab on page 27](#).

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 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 27](#).

Assign verification 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 **Verification method** column, select a verification method for each user or group.
2. In the **User details** field, add the delivery details, such as the 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 27](#).

Actions

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](#).

Mobile device management (MDM)

Mobile device management (MDM) is a software that secures, monitors, manages, and supports mobile devices deployed across mobile operators, service providers, and enterprises.

Typically, the MDM solutions include a server component, which sends out the management commands to the mobile devices, and a client component, which runs on the managed device and receives and implements the management commands.

You can distribute the XProtect Mobile client and add custom policies to the devices in your organization.



To use the MDM functionality on a mobile device, you must configure the mobile server details on the MDM software platform. The mobile server details include the server name, the server address, the server port, and the connection type protocol.



If you have updated the details of an already added mobile server, the operator must manually delete this server from the **Servers** list and restart the XProtect Mobile app.

Configure mobile server details on MDM platform (administrators)

To distribute and manage the XProtect Mobile client to mobile devices from an MDM platform, you need to add the server details. For more information about the configuration, check the documentation about your MDM software.



If you haven't typed in any of the mandatory server details or have provided incorrect details, the mobile server won't be added to the XProtect Mobile app.

For Android users

You can specify the server details in the user interface of your MDM platform. You have the option to upload a managed configuration file with the server details.

Server details:

- **Server name** - (Mandatory) Type in the server name
- **Server address** - (Mandatory) Type in the server address
- **Server port** - (Mandatory) Type in the server port number
- **Connection protocol type** - Enable when you use an HTTPS connection. Disable when you use an HTTP connection. By default, the HTTPS connection is enabled

To upload the file to your MDM platform:

1. At the back of this manual, in Appendix A, find the managed configuration template for Android devices. Copy the content.
2. Open a text editor of your choice and paste the content.
3. Specify the server details in the **android:description** fields.
4. Save the file as .XML.
5. Open your MDM platform and upload the managed configuration file.

For iOS users

To manage iOS devices from an MDM platform, you need to specify the connection details in the managed configuration file.

1. At the back of this manual, in Appendix B, find the managed configuration template for iOS devices. Copy the content.
2. Open a text editor of your choice and paste the content.
3. Specify the server details:
 - **versionConfig** - (Mandatory) Type in the default version of the app configuration **1.0.0**
 - **serverNameConfig** - (Mandatory) Type in the server name
 - **serverAddressConfig** - (Mandatory) Type in the server address
 - **serverPortConfig** - (Mandatory) Type in the server port number
 - **serverConnectionProtocolTypeConfig** - The default connection type is **HTTPS**, to use a non-secure connection, type in **HTTP**
4. Save the file as .XML.
5. Open your MDM platform and upload the managed configuration file.

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

To get actions to show correctly together with the 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 - 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 - 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 [Outputs](#).

External IDP and XProtect Mobile

IDP is an acronym for Identity Provider. An external IDP is an external application and service where you can store and manage user identity information and provide user authentication services to other systems. You can associate an external IDP with the XProtect VMS.

You can log in to XProtect Web Client or the XProtect Mobile client via an external IDP with XProtect 2022 R3 and later.



To log in with an external IDP to XProtect Web Client or the XProtect Mobile client, you must use an HTTPS connection.

Before you configure external an IDP login for XProtect Web Client and the XProtect Mobile client, make sure that you have:

- Configured an external IDP
- Registered claims
- Mapped claims to roles

For more information, see the [administrator manual for XProtect VMS](#).

To log in to XProtect Web Client via an external IDP, you need additional configuration. See [Configure external IDP login for XProtect Web Client on page 49](#).

Configure external IDP login for XProtect Web Client

The option to log in via an external IDP to XProtect Web Client is available for HTTPS connections only.

1. In Management Client, select **Tools > Options** and open the **External IDP** tab.
2. In the **Redirect URIs for web clients** section, select **Add**.
3. Enter the addresses for XProtect Web Client in the format **https://[address]:[port number]/index.html**:
 - For the address, enter the host name or the IP address of the computer on which the mobile server is running
 - For the port number, enter the port that XProtect Web Client uses to communicate with the mobile server. For HTTPS connections, the default port number is 8082

Add Emergency Alert alarms

When a potential threat is detected, Emergency Alert enables XProtect Mobile client users to receive alarm notifications of the highest severity level, view the alarm details, and immediately act. Emergency Alert is a type of alarm you define in XProtect Management Client.



For this functionality to work, it requires push notifications. Push notifications are available only if you have purchased a Milestone Care Plus license.



The feature is only available in certain XProtect VMS products. See the complete feature list, which is available on the product overview page on the Milestone website (<https://www.milestonesys.com/products/software/xprotect-comparison/>).

To add such an alarm, you must:

1. Add a new alarm category with level 99 in **Alarms > Alarm Data Settings**. You can create as many categories with level 99 as you need.
2. Add an alarm definition with this category.

Maintenance

Mobile Server Manager

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 the mobile server functionalities.

You can:

- [Access XProtect Web Client on page 51](#)
- [Start, stop and restart Mobile Server service on page 52](#)
- [Change data protection password on page 52](#)
- [Show/edit port numbers on page 53](#)
- [Enable encryption on the mobile server on page 33](#) using the **Server Configurator**
- Open today's log file (see [Accessing logs and investigations on page 53](#))
- Open Log folder (see [Accessing logs and investigations on page 53](#))
- Open investigations folder (see [Accessing logs and investigations on page 53](#))
- [Change investigations folder on page 54](#)
- See XProtect Mobile Server status (see [Show status on page 54](#))

Access XProtect Web Client

If you have an 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 an 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 an XProtect Mobile server is installed, you can access it from a browser. Continue with step 4 in this process.
4. Open an Internet browser (Microsoft Edge, 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

Change data protection password

The mobile server data protection password is used to encrypt investigations. As a system administrator, you will need to enter this password to access the mobile server data in case of system recovery or when expanding your system with additional mobile servers.

To change the mobile server data protection password:

1. Right-click the Mobile Server Manager icon and select **Change data protection password settings**. A dialog box appears.
2. In the **New password** field, enter your new password.
3. Re-enter the new password in the **Confirm new password** field.
4. (Optional) If you do not want your investigations to be password protected, select **I choose not to use a mobile server data protection password, and I understand that investigations will not be encrypted**.
5. Click **OK**.



You must save this password and keep it safe. Failure to do so may compromise your ability to recover mobile server data.

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**.

Accessing logs and investigations

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**

Audit logs are created for every action that is not already logged by the Management Server or the Recording Server.

The following actions are always logged (even when extended audit logging is not enabled):

- All administration (these audit log messages contain the old value and the new value)
- All actions regarding creating, editing or deleting investigations as well as preparation and download of exported material, changing relevant pieces of the configuration. The audit log contains details about what has been done.



Video push streaming is logged only when extended audit logging is enabled.



If you uninstall the XProtect Mobile server from your system, its log files are not deleted. Administrators with proper user permissions 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

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.

Name	Description
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.

Use a load balancer for the mobile server

As an additional security step, XProtect Mobile uses IDs in the communication between the server and the mobile app. When a user connects to a mobile server from the XProtect Mobile app for the first time, the server ID of the mobile server is copied to the user's device. Every time a connection to a mobile server is attempted, the server IDs are compared with those obtained initially.

By default, every server has a unique server ID. To add a mobile server to a load-balancing group, you must ensure that the mobile server's ID matches the ID used by the other mobile servers in the group.

On a host in the load-balancing group

To copy the server IDs from a host:

1. Go to C:\ProgramFiles\Milestone\Milestone Mobile Server and copy the **VideoOS.MobileServer.Service.exe.config** file.
2. Paste the file on your desktop and open it with a text editor of your choice.
3. Search the file for the `ServerSettings` tag. It should look like this:

```
<ServerSettings>
  <Identification>
    <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
    <add key="ServiceIdS" value="10353810-803F-4880-BC22-417B37F1A1C8">
    <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
  </Identification>
  ---
</ServerSettings>
```

4. Copy the **ServiceID** and **ReportedServiceID** values.

On the other hosts that are part of the group

On a host that is part of the load-balancing group:

1. Go to C:\ProgramFiles\Milestone\Milestone Mobile Server and open the **VideoOS.MobileServer.Service.exe.config** file with a text editor of your choice.
2. Search the file for the `ServerSettings` tag and replace the **ServiceID** and **ReportedServiceID** values with those from the original configuration file.
3. To apply the changes, restart the Mobile Server service.
4. Ask the XProtect Mobile client users to add the mobile server again.

Repeat the steps on all hosts that are part of the load-balancing group.

Migrate a mobile server to another host

As an additional security step, XProtect Mobile uses IDs in the communication between the server and the mobile app. When a user connects to a mobile server from the XProtect Mobile app for the first time, the server ID of the mobile server is copied to the user's device. Every time the app tries to connect to a mobile server, it compares the server IDs with the ones it got initially. If the server IDs do not match, the connection fails.

When you migrate the mobile server to another host and keep its original address, you must keep the old server's server ID.

On the old host

Before you migrate your mobile server, you must:

1. Go to C:\ProgramFiles\Milestone\Milestone Mobile Server and copy the **VideoOS.MobileServer.Service.exe.config** file and open it with a text editor of your choice.
2. Search the file for the `ServerSettings` tag. It should look like this:

```
<ServerSettings>
  <Identification>
    <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
    <add key="ServiceIds" value="10353810-803F-4880-BC22-417B37F1A1C8">
    <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
  </Identification>
  ---
</ServerSettings>
```

3. Copy the **ServiceID** and **ReportedServiceID** values.

You are now ready to migrate your mobile server.

On the new host

After you have installed and configured the mobile server on the new host:

1. Go to `C:\ProgramFiles\Milestone\Milestone Mobile Server` and open the **VideoOS.MobileServer.Service.exe.config** file with a text editor of your choice.
2. Search the file for the `ServerSettings` tag and replace the **ServiceID** and **ReportedServiceID** values with those from the original configuration file.
3. To apply the changes, restart the Mobile Server service.
4. Ask the XProtect Mobile client users to add the mobile server again.

Troubleshooting

Troubleshooting XProtect Mobile

Connections

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 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 14](#)).

The server address field must contain a valid host name when applied in the iOS device. Valid host names can contain the ASCII letters 'a' through 'z' (case-insensitive), the digits '0' through '9', dot and the hyphen ('-').

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 the XProtect Mobile server, you must manually enable TCP and UDP communications.

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 are not applicable for the XProtect Mobile server. You must manually create a 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.

I have not changed the address of the mobile server but the XProtect Mobile client users can no longer connect to it. Why?

The XProtect Mobile clients connect to the mobile server using a unique service ID. Even if the host name and IP address of the mobile server computer remain the same, the service ID might not match with the one stored on the clients, for example, when:

- You have reset your computer and reinstalled the mobile server.
- You have moved the mobile server to another computer but kept its original configuration.

To reestablish the connection, you can:

- Update the service ID on the new mobile server, so that it matches the service ID from the previous configuration. See <https://developer.milestonesys.com/s/article/unable-to-establish-connection-to-XProtect-Mobile-Server-using-Android-iOS-client>.
- Ask the XProtect Mobile client users to reconnect to the mobile server.

Image quality

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. For more information, see the [user manual for XProtect Smart Client](#).

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.

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 the 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

Does my processor support hardware-accelerated decoding?

Only newer processors from Intel support hardware-accelerated decoding. Check the Intel website (https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&0_QuickSyncVideo=True) 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 on page 54](#)).

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 on your system. These drivers are not available from Windows Update.

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.

Notifications

I made no changes in the notification configuration but the registered devices stopped receiving notifications. Why?

If you have updated your license or renewed your Milestone Care subscription, you need to restart the Mobile Server service.

Appendices

Appendix A

Managed configuration template for Android

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<restrictions xmlns:android="http://schemas.android.com/apk/res/android">
```

```
<restriction
```

```
  android:defaultValue="1.0.0"
```

```
  android:description="The current version of the app configuration"
```

```
  android:key="version_config"
```

```
  android:restrictionType="hidden"
```

```
  android:title="Version" />
```

```
</restriction
```

```
android:description="(Mandatory) Enter the server name."
```

```
android:key="server_name_config"
```

```
android:restrictionType="string"
```

```
android:title="Server name" />
```

```
<restriction
```

```
android:description="(Mandatory) Enter the server address."
```

```
android:key="server_address_config"
```

```
android:restrictionType="string"
```

```
android:title="Server address" />
```

```
<restriction
```

```
android:description="(Mandatory) Enter the server port."
```

```
android:key="server_port_config"
```

```
android:restrictionType="integer"
```

```
android:title="Server port" />
```

```
<restriction
```

```
    android:description="Enable when you use an HTTPS connection. Disable  
    when you use an HTTP connection."
```

```
    android:key="server_secure_connection_config"
```

```
    android:restrictionType="bool"
```

```
    android:title="Connection protocol type"
```

```
    android:defaultValue="true"/>
```

```
</restrictions>
```

Appendix B

Managed configuration template for iOS

```
<managedAppConfiguration>
```

```
<version>1</version>
```

```
<bundleId>com.milestonesys.XProtect</bundleId>
```

```
<dict>
```

```
<string keyName="versionConfig">
```

```
<defaultValue>
```

```
<value>1.0.0</value>
```

```
</defaultValue>
```

```
</string>
```

```
<string keyName="serverNameConfig">
```

```
</string>
```

```
<string keyName="serverAddressConfig">
```

```
</string>
```



```
<string keyName="serverPortConfig">
```

```
</string>
```

```
<string keyName="serverConnectionProtocolTypeConfig">
```

```
<defaultValue>
```

```
<value>HTTPS</value>
```

```
</defaultValue>
```

```
</string>
```

```
</dict>
```

```
<presentation defaultLocale="en-US">
```

```
<field keyName="versionConfig" type="input">
```

```
<label>
```

```
<language value="en-US">Version</language>
```

```
</label>
```

```
<description>
```

```
        <language value="en-US">The current version of the app  
configuration</language>
```

```
    </description>
```

```
</field>
```

```
<fieldGroup>
```

```
  <name>
```

```
    <language value="en-US">Mobile server</language>
```

```
  </name>
```

```
  <field keyName="serverNameConfig" type="input">
```

```
    <label>
```

```
      <language value="en-US">Server name</language>
```

```
    </label>
```

```
    <description>
```

```
      <language value="en-US">(Mandatory) Enter the server  
name.</language>
```

```
</description>
```

```
</field>
```

```
<field keyName="serverAddressConfig" type="input">
```

```
<label>
```

```
<language value="en-US">Server address</language>
```

```
</label>
```

```
<description>
```

```
<language value="en-US">(Mandatory) Enter the server  
address.</language>
```

```
</description>
```

```
</field>
```

```
<field keyName="serverPortConfig" type="input">
```

```
<label>
```

```
<language value="en-US">Server port</language>
```

```
</label>
```

```
<description>
```

```
      <language value="en-US">(Mandatory) Enter the server  
port.</language>
```

```
</description>
```

```
</field>
```

```
<field keyName="serverConnectionProtocolTypeConfig" type="input">
```

```
<label>
```

```
      <language value="en-US">Connection protocol type</language>
```

```
</label>
```

```
<description>
```

```
      <language value="en-US">To specify the connection protocol  
type, enter HTTPS or HTTP.</language>
```

```
</description>
```

```
</field>
```

```
</fieldGroup>
```

```
</presentation>
```

```
</managedAppConfiguration>
```



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/>.

