

Milestone Systems

XProtect® Mobile client 2022 R3

User manual



Contents

Copyright, trademarks, and disclaimer	5
Supported VMS products and versions	6
Overview	7
What's new?	7
In XProtect Mobile client 2022 R3	7
Server and client components of XProtect Mobile (explained)	
XProtect Access and XProtect Mobile (explained)	g
Requirements and considerations	12
Before you start (administrators)	12
Requirements for listening to audio	12
Requirements for using push-to-talk	13
Requirements for using video push	14
Requirements for direct streaming	14
Installation	15
Installing XProtect Mobile Server components (administrators)	15
Install XProtect Mobile on a mobile device	17
Configuration	18
Configure user profiles on server (administrators)	18
Select a language for the app	18
Buttons and settings overview	18
Connection settings for a mobile server (explained)	26
Connect your mobile device to a mobile server or disconnect a mobile server	28
View and edit connections to mobile servers	31
Enable access request notifications in XProtect Mobile	32
Enable or disable notifications	33
External IDP and XProtect Mobile client (explained)	35
Using biometrics or device credentials to secure the app (explained)	35
Streaming video from your mobile device (explained)	36

	Set up video streaming on your mobile device	37
	Listening to incoming audio (explained)	38
	Push-to-talk (explained)	38
	Mobile device management (MDM) (explained)	40
	Direct streaming (explained)	40
	Adaptive streaming (explained)	41
o	peration	42
	Logging in and out	42
	Change password in XProtect Mobile client	45
	Viewing live video	46
	Bookmarks (usage)	48
	Bookmarks (explained)	48
	View the bookmark details or play the bookmark video clip	49
	Add or edit bookmarks	50
	Delete bookmarks	52
	Use the filter	52
	Filter your views	52
	Filter your bookmarks	53
	Interact with live video in full screen	55
	Use picture-in-picture	57
	Take a snapshot	57
	Find and view video recordings	58
	Using the playback timeline (explained)	60
	View or create an investigation	63
	Stream video from your device to your surveillance system	64
	View alarms	65
	Using actions in XProtect Mobile	66
	View and trigger actions	67
	React to a notification	67
	View doors and take action	68

Respond to access requests	69
Investigate access control events	70

Copyright, trademarks, and disclaimer

Copyright © 2022 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.

Supported VMS products and versions

This manual describes features supported by the following XProtect VMS products:

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

Milestone tests the features described in this manual with the above-mentioned XProtect VMS products in the current release version and the two previous release versions.

If new features are only supported by the current release version and not any previous release versions, you can find information about this in the feature descriptions.

You can find the documentation for XProtect clients and add-ons supported by the retired XProtect VMS products mentioned below on the Milestone download page (https://www.milestonesys.com/downloads/).

- XProtect Enterprise
- · XProtect Professional
- XProtect Express
- XProtect Essential

Overview

What's new?

In XProtect Mobile client 2022 R3

For Android and iOS users

Log in with an external IDP:

• You can log in to the XProtect Mobile app using an external IDP. With this alternative login method you can be authorized to access the app without the required login credentials of a basic user or a Windows user. For more information, see External IDP and XProtect Mobile client (explained) on page 35.

New user experience:

- The login procedure splits into two:
 - On the **Add servers** screen, you can enter your server details and continue your login or choose to save the details and continue login later. For more information, see Connect your mobile device to a mobile server or disconnect a mobile server on page 28.
 - On the **Login** screen, you can enter your user credentials or choose to log in with an external IDP. For more information, see Logging in and out on page 42.
- The new user menu contains the following buttons and settings:
 - · Log out
 - · Change password
 - Disconnect from server
 - Go to the app settings.

For more information, see Buttons and settings overview on page 18.

Using biometrics or device credentials to secure the app:

• You can now use biometrics or your device credentials to verify your identity before you open the app. Quick authentication based on your fingerprint, facial recognition, or device credentials facilitates access to the XProtect Mobile client and improves the security of the app. For more information, see Using biometrics or device credentials to secure the app (explained) on page 35.

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) (explained) on page 40.

Notifications:

- To receive notifications, you are no longer required to save your user credentials. If you haven't saved your user credentials, you'll be prompted to enter your credentials or use your external IDP login method each time before you open a received notification.
- To receive notifications, you must enable the notifications setting on the app level (Android), mobile device, and server level.

For more information, see Enable or disable notifications on page 33.

For Android users

Time picker (Android):

• The time picker has a new and simplified interface. For more information, see Using the playback timeline (explained) on page 60.

In XProtect Mobile client 2022 R2

Notifications:

• By default, notifications are disabled when you add a server. For more information, see Enable or disable notifications on page 33.

In XProtect Mobile client 2022 R1

Bookmarks:

- You can edit the start time, the event time, or the end time of bookmarks.
- To find a specific bookmark, you can search and use filtering. There are three options for filtering bookmarks:
 - You can enter a keyword from the headline or description of the bookmark or enter the complete bookmark ID.
 - You can select specific cameras.
 - You can select a predefined time interval. You can also customize the time interval that you want to apply as a filter.

Video diagnostics overlay:

• You can enable this setting to view the FPS (frames per second), the codec, the resolution, and the type of streaming of the video stream in the selected view. The feature displays the information as an overlay to the video and can help you to troubleshoot XProtect Mobile client issues related to the video stream and performance issues.

Direct streaming:

• The feature is also available in XProtect Professional+ and XProtect Express+.

Adaptive streaming:

• The feature is also available in XProtect Professional+ and XProtect Express+.

Server and client components of XProtect Mobile (explained)

In the free XProtect Mobile app, you can:

- · View live video and video recordings.
- Play incoming and outgoing audio in live video and video recordings.
 - Use the push-to-talk (PTT) feature while you are watching live video from one camera.
 - Play back incoming and outgoing audio in playback mode.
- Use video push to stream live video with audio from the camera on your mobile device to your XProtect surveillance system.
- Use bookmarks to quickly locate relevant video sequences in live videos and video recordings.
- Create investigations.
- Activate actions that trigger events in your video surveillance system.
- · View videos for alarms that are triggered by various events.

XProtect Mobile has five components:

- XProtect Mobile client is a mobile surveillance app that you can install and use on your Android or iOS
 device. You can use as many installations of XProtect Mobile client as you need. For more information,
 see Installing XProtect Mobile Server components (administrators) on page 15
- · XProtect Web Client lets you view live video in your web browser and lets you download recordings
- The XProtect Mobile server is responsible for giving the XProtect Mobile client and XProtect Web Client users access to the system
- XProtect Mobile plug-in
- Mobile Server Manager

In addition to acting as a system gateway for XProtect Mobile client and XProtect Web Client, the mobile server can transcode video as the original camera video stream, in many cases, is too large to fit the bandwidth available for the client users.

XProtect Mobile supports direct streaming and adaptive streaming in live mode.

For more information, see the administrator manual for XProtect VMS.

XProtect Access and XProtect Mobile (explained)



The use of XProtect Access requires that you have purchased a base license that allows you to access this feature within your XProtect system. You also need an access control door license for each door you want to control.

With XProtect Access and the XProtect Mobile app installed on your smartphone or tablet, you get:

- Live monitoring of events at access points
- Operator aided passage for access requests
- Investigation of events at access points
- Centralized overview and control of door states
- Cardholder information

Access requests

When you get an access request on your device, it may look like this:

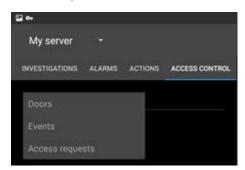


Access requests let you:

- View the state of the door, for example, **Closed**, **Locked**.
- View live video.
- View the cardholder details, for example, picture and authority level.

- Lock doors and grant access to cardholders by unlocking doors.
- Listen to incoming audio in live mode.
- Use the push-to-talk (PTT) feature while you are watching live video from one camera.

Access requests are listed under **Access requests** for two minutes. After that, they appear only in the **Events** list, where you can watch the video recorded when the cardholder tried to gain access.



Requirements and considerations

Before you start (administrators)

To use the XProtect Mobile app for access control purposes, you need:

- A Milestone Care Plus service agreement
- Licenses required for using XProtect Access. This includes a base license and a door license for each door
- An access control system that is configured and integrated with your VMS
- If you are using one of the products listed below, you must configure the user profiles to enable access control and access requests:
 - XProtect Corporate
 - XProtect Expert
 - · XProtect Professional+
 - XProtect Express+
 - XProtect Essential+

If you are using XProtect Essential+, also see Configure user profiles on server (administrators) on page 18.

- You must download the XProtect Mobile app from App Store^{5M} or Google Play and install it on your smartphone or tablet.
- In the XProtect Mobile app:
 - 1. You must specify the server settings of the mobile server (see Connect your mobile device to a mobile server or disconnect a mobile server on page 28).
 - 2. In the server settings, you must enable access request notifications (see Enable access request notifications in XProtect Mobile on page 32).



If you have enabled the Operator login required option, the access control system will not be available in XProtect Mobile client. For more information, see the administrator manual for XProtect VMS.

Requirements for listening to audio

To listen to incoming audio from the cameras in your XProtect VMS through a mobile device, you must have:

• A microphone attached to a camera.



When a camera in your surveillance system has a microphone attached, you can play audio without any additional settings needed. The audio icon on the camera toolbar shows whether the audio feature is available.

• Sufficient user permissions.



Access to the incoming audio feature may be restricted depending on your user permissions. Ask your system administrator if in doubt.

• HTTP or HTTPS with CA certificate connection.

If you want to use an HTTPS connection, a digital certificate from a certificate authority (CA) must be installed on your XProtect Mobile server.



CAs issue digital certificates that verify the identities of users and websites that exchange data on the internet. Examples of CAs are companies like Comodo, Symantec, and GoDaddy. For detailed information about certificates, see the topic about enabling encryption in the guide about certificates.

Requirements for using push-to-talk

To use the push-to-talk (PTT) feature on your mobile device in your XProtect VMS, you must have:

- Cameras that have speakers attached.
- Sufficient user permissions.



Access to the push-to-talk feature may be restricted depending on your user permissions. Ask your system administrator if in doubt.

- Allowed the XProtect Mobile app to use the microphone of your mobile device.
- HTTP or HTTPS with CA certificate connection.

If you want to use an HTTPS connection, a digital certificate from a certificate authority (CA) must be installed on your XProtect Mobile server.

Requirements for using video push

To use video push and to stream video with audio, you must allow the XProtect Mobile app to access the camera and microphone of your mobile device.

Requirements for direct streaming

XProtect Mobile supports direct streaming in live mode.

You can use direct streaming to monitor more than 100 concurrent live video streams at Full HD 30 FPS. To do this, you must:

- Use cameras that support the H.264 codec or the H.265 codec.
- Allow direct streaming on your mobile device (see Buttons and settings overview on page 18).

For more information, see the administrator manual for XProtect VMS.

Installation

Installing XProtect Mobile Server components (administrators)

This information is primarily for system administrators. For detailed feature descriptions and procedures for configuration and maintenance, see the administrator manual for XProtect VMS.

You can install the XProtect Mobile Server component when you install version 2013 and all later versions of XProtect products:

- XProtect Corporate
- XProtect Expert
- · XProtect Professional+
- XProtect Express+
- XProtect Essential+
- · Milestone Husky
- Milestone Arcus

To get the most out of XProtect Mobile, make sure that you're using the latest version of your VMS product. Information about the products is available on the Milestone website (https://www.milestonesys.com/solutions/platform/product-index/).

You can also download XProtect Mobile Server for free from the download page on the Milestone website (https://www.milestonesys.com/downloads/).

Where to install the XProtect Mobile Server component

Install the XProtect Mobile Server component on the computer that runs your surveillance system or on a dedicated computer.

If you plan to have more than ten cameras in your system showing video simultaneously, Milestone recommends that you install XProtect Mobile Server on a dedicated computer.

You can install the XProtect Mobile server in various ways:

Installation method		
XProtect product	Installation on the same computer as the VMS	Installation on a dedicated computer
 XProtect Corporate XProtect Expert XProtect Professional+ XProtect Express+ XProtect Express+ 	Complete a Single Computer installation of the XProtect VMS software. This installation includes the XProtect Mobile Server.	Run the separate XProtect Mobile Server installer.

Installing the XProtect Mobile plug-in component

You should install the XProtect Mobile plug-in on all computers that run the Management Client:

- 1. Run the XProtect Mobile installer.
- 2. Choose a **Custom** installation and select the plug-in (32-bit or 64-bit). It is safe to install both.
- 3. Restart Management Client.

Operating systems

XProtect Mobile supports the following operating systems for mobile devices:

Operating system	Devices
Android 9.0 or newer	Smartphones and tablets with Android installed
iOS 14.0 or newer	iPhone, iPad, and iPod Touch

Install XProtect Mobile on a mobile device

On your mobile device, download the free XProtect Mobile application from Google Play or App Storesm.

- Find the app in the app store by searching for "XProtect Mobile" and then install it on your mobile device.
 The XProtect Mobile logo icon appears on the screen of your device.
- 2. To run XProtect Mobile, tap the icon.



By default, a Milestone demo server installs. Use the server to test the app. The server is just for testing, so there are some things you can't do. For example, you can't use pan-tilt-zoom controls.

You can't delete or edit the demo server, but you can hide it from the server list. To hide the server, go to **Settings**, under **General**, enable the **Hide demo server** setting.

To view videos from your cameras, connect the app to one or more mobile servers (see Connect your mobile device to a mobile server or disconnect a mobile server on page 28).

Configuration

Configure user profiles on server (administrators)

You must enable certain user permissions to ensure that users of XProtect Mobile can use access control and view and respond to access requests on their smartphones or tablets. Depending on your VMS, the setup differs slightly.

In Management Client:

- 1. Expand Security and select Roles.
- 2. Select the role that you want to modify.
- 3. In Role Settings, click the Access Control tab.
- 4. If not already selected, select these check boxes:
 - Use access control Required to view access control features in XProtect Mobile
 - Receive notifications Required to receive access requests as push notifications
- 5. For each required role, repeat the steps above.
- 6. Save the changes.

Select a language for the app

By default, the XProtect Mobile app uses the language of your device. For example, if your device uses French, the XProtect Mobile client displays in French.

To use a different language, change the language of your device. Then, restart the XProtect Mobile app to apply the change.



To use the XProtect Mobile client in a specific language, your device must support that language.

Buttons and settings overview

This topic lists and describes buttons and settings in the XProtect Mobile app. If you see something in the app that you're not sure how to use, you can look it up here.

When you start the app, the **Servers** screen contains the following buttons and settings:

Name	Description		
Add server (Android)	Scan the local network for available mobile servers. The XProtect Mobile client has a scanning functionality for finding XProtect Mobile servers based on UPnP.		
(Android) Edit (iOS)	 Add server (iOS) - Scan the local network for mobile servers. Edit - Edit settings for the server. Delete - Delete the server from the list. Connect or Disconnect (Android) - Connect to the mobile server or disconnect the server you are currently connected to. 		
(Android) Settings (iOS)	 General settings: Stay awake - Enable to keep the screen awake while streaming video. Hide demo server - Enable to hide the demo server from the server list. Provide usage data - Enable to help us deliver excellent services to you. You must not enable data collection if you want the system to have an EU GDPR-compliant installation. For more information about data protection and the usage data collection, see the GDPR privacy guide. Push notifications (Android) - Enable to receive push notifications in the app. To receive push notifications, you must also enable the notifications setting for the app on your mobile device and on the mobile server (see Enable or disable notifications on page 33). Enable use of biometrics or your device credentials for this app - Use biometric sensors or your device credentials to unlock the app. To use the feature in the app, you must enable the setting about biometrics and security on your mobile device. 		

Name	Description
	Video quality settings:
	Frames per second - Lower FPS will reduce the bandwidth usage.
	Optimize bandwidth or image quality - Enable to reduce bandwidth usage. Disable to increase image quality.
	• Use lower video resolution - Enable to allow for higher FPS rates.
	 Allow direct streaming on device - Allow to improve the video quality. Direct streaming is only available if enabled on the server.
	 Use keyframes only in live video from multiple cameras - Enable to use keyframes only and to reduce the usage of CPU power. Disable to use all frames and higher FPS rates.
	 Video diagnostics overlay - Enable to view the FPS (frames per second), the codec, the resolution, and the type of streaming of the video stream in the selected view. The feature displays the information as an overlay to the video and can help you to troubleshoot XProtect Mobile client issues related to the video stream and performance issues.
	Controls settings:
	Autohide video controls - Hide the video controls after a period without activity.
	Default PTZ controls - Select the preferred default setting for the PTZ control.
	Find more information about using the XProtect Mobile app by tapping the Help link.

When you tap ${\bf Add}\ {\bf server},$ the ${\bf Add}\ {\bf servers}$ screen contains the following settings:

Name	Description
Add server with	Add a server using a unique server identifier. This connection method uses the Address book service and requires a Milestone Care Plus subscription package.
Add server manually	Enter a name for the server, its IP address or its host name, and select the type of connection that you will use to connect the XProtect Mobile client to the mobile server. By default, the HTTPS connection is selected

After logging in to a mobile server:

- The user menu in the upper left-hand corner contains the following:
 - Your user name and login authentication type.
 - Log out Tap the button to log out from the server. Logging out will remove your saved user credentials for this mobile server (see Logging in and out on page 42).
 - Change password As a basic user, you can change your password whenever you want to (see Change password in XProtect Mobile client on page 45).
 - The name of the mobile server your mobile device is currently connected to.
 - Disconnect from server Disconnect from the server you are currently connected to. (see Connect your mobile device to a mobile server or disconnect a mobile server on page 28).
 - **Go to the app settings** Tap the link to go to the XProtect Mobile app settings.
- The top bar in Android and the bottom tabs in iOS can contain the following options:



The options are available only if you have been given permission to view them, which happens in Management Client.

Name	Description
(Android)	Filter camera views or bookmarks. By default, all views and bookmarks are selected.
Q	 Search for a view or a specific camera. Enter ptz to find all your PTZ cameras. Enter audio to find all your cameras that have microphones attached. Enter ptt to find all your cameras that have speakers.
Views (Android)	View the available views of cameras on the Home screen. Select the view that you want to play video from (live or recorded). The available views are organized in folders: . (Android) . (iOS)

Name	Description
	These folders can contain other folders with views or separate views with cameras - (Android) or (iOS). The views can only contain cameras.
Cameras (Android) (iOS)	View the available cameras listed in the All cameras view.
Investigations (Android)	View investigations created in XProtect Web Client or XProtect Mobile client.
Bookmarks (Android) (iOS)	 View the list of bookmarks. You can also: Edit the bookmark details - (Android) or Edit (iOS). Delete the bookmark - (Android) or Delete (iOS).
Actions (Android) (iOS)	Access outputs and events to activate them.
Alarms (Android)	View and react to alarms.
(Android)	Video push lets you use the camera on your mobile device to stream video with audio to your surveillance system. On the Video push screen, go to (Android) or Settings (iOS) to view or change: • Video resolution - Select the resolution of the video stream to push.

Name	Description
	 Automatic image quality - Enable to adjust the image quality automatically. If you disable the setting, then you can set the image quality to Low, Medium, or High.
	• Location data - Add location data to the video stream.
	XProtect Corporate
	XProtect Expert
	XProtect Professional+
	XProtect Express+
	XProtect Essential+

In live mode, you can use these buttons to do the following:

Name	Description
(Android) (iOS)	View a list of actions for the selected camera.
(Android)	Go to PTZ mode. Shows PTZ controls on the screen so you can pan, tilt and zoom in on the selected camera. Dimmed for non-PTZ cameras.
(Android)	View the PTZ preset positions on the selected camera (for PTZ cameras only).
(Android)	Take a snapshot of the current frame. Snapshots are saved as follows: • Snapshots are saved to your device's SD card at /mnt/sdcard/Milestone (Android).

Name	Description
	 Snapshots are saved to your device's Photo Library and can be accessed by tapping Photos on your device (iOS). You cannot change the save locations.
(Android)	Start or stop listening to incoming audio from cameras that have microphones attached.
\$	Start or stop using the push-to-talk (PTT) feature with cameras that have speakers.
(Android)	Add a bookmark to live videos to quickly locate relevant video sequences (see Viewing live video on page 46).
(Android)	Switch from live mode to playback mode.

In playback mode, you can use these buttons to do the following:

Name	Description
(Android)	View a list of created video recordings.
(Android)	Turn on and turn off a small picture-in-picture (PiP) for live mode. Tap the button again or double-tap the PiP view to return to live mode.
(Android)	Create an investigation.

Name	Description
(iOS)	
(Android)	Play a video recording forwards.
(Android)	Play a video recording backward.
(Android) (iOS)	Pause playing a video recording.
► K (Android)	Go forward to the next sequence or go back to the previous sequence.
(Android)	Go one frame forward or one frame backward in the sequence.
10-55-2019 10-05-2019	Drag the time scroller to go to a specific time in a video recording. Tap the time indicator to open the time picker.
X1	Open a selection of playback speeds.
(Android) (iOS)	Play back audio from cameras that have microphones and speakers attached.
(Android)	Take a snapshot in playback mode.

Name	Description
(Android)	Add a bookmark to recorded videos to quickly locate video sequences (see Find and view video recordings on page 58).
(Android)	Go back to live mode.

Connection settings for a mobile server (explained)

When you add a mobile server to your XProtect Mobile app manually, you must configure a list of settings.

Settings on the Add servers screen

Setting	Description	
Server name	The name of the server. The name displays in the list of servers on your device and can be anything you want.	
Address	The address of the computer where XProtect Mobile Server is running. The server address can be an IP address or a host name.	
https:// or http://	The type of connection that you will use to connect the XProtect Mobile client to the mobile server. By default, the HTTPS connection is selected.	
	If you select the HTTP connection type, you must ensure that the mobile server also uses an HTTP connection. Otherwise, the XProtect Mobile app and the server cannot communicate.	
	If in doubt, ask your system administrator.	
Port	The port number that the XProtect Mobile client uses to communicate with the server. For	

Setting	Description	
	HTTP connections, the default port is 8081. For HTTPS connections, the default port is 8082.	
number	If you edit the port number, you must also edit the corresponding port number on the mobile server side. Otherwise, the XProtect Mobile app and the server cannot communicate.	
Continue login	Go to the Login screen.	
Save and log in later	Save the mobile server details and log in later.	



If you use an MDM functionality on your mobile device, the mobile server details will be entered automatically.

Settings on the Login screen

Setting	Description
Windows user Basic user	Your login authentication type. Select whether you log in as a Windows user or as a basic user.
User name	A mandatory login credential.
Password	A mandatory login credential.

Setting	Description
	The user name and password can be based on either basic users set up in Management Client or on Windows users. Windows user credentials are specific to a machine or a domain.
Remember me	Indicate whether you want to remember your user name and password for the next time you connect to an already added server. By default, the setting is enabled.
Log in	Log in to the XProtect Mobile client.
Change password	As a basic user, you can change your password whenever you want to (see Logging in and out on page 42).
Log in with [Name of an external IDP]	If your system administrator has configured a login with an external IDP, use this option to log in to the XProtect Mobile client. For more information, see External IDP and XProtect Mobile client (explained) on page 35.

Connect your mobile device to a mobile server or disconnect a mobile server

You can connect your mobile device to more than one mobile server.

Requirements:

- Get server and user details from your system administrator.
- You have installed and opened the app.
- If you want to use an HTTPS connection, a digital certificate from a certificate authority (CA) must be installed on your XProtect Mobile server.



You cannot connect to the mobile server through your XProtect Mobile app if you use a self-signed certificate. If in doubt, ask your system administrator

Connect to a server that you have not used before

- 1. Open the XProtect Mobile app.
- 2. On the Servers screen:
 - Android Tap Add server to scan the local network for mobile servers.
 - iOS Tap Edit, then tap Add server to scan the local network for mobile servers.



The XProtect Mobile client has a scanning functionality for finding XProtect Mobile servers based on UPnP and it lists these servers under New

servers. Select one or more servers, and then tap to save.





The Already added servers group lists the servers that you have connected to your mobile device before.

- 3. If you choose to add the server manually, tap Add server manually. On the Add servers screen specify the following settings:
 - In the Server name field, enter a name for the server. The server name shows in the list of servers on your device, and it can be anything you want.
 - In the Address field, enter the server IP address or the server host name.
 - Specify the connection type protocol. By default, the connection type is set to HTTPS.



To connect to a mobile server with an HTTP connection setting configured, you must set the connection type protocol to HTTP on the app side. If in doubt, contact your system administrator.



If you use an MDM functionality on your mobile device, the mobile server details will be entered automatically. For more information, see Mobile device management (MDM) (explained) on page 40.

• To continue login, tap Continue login and follow the instructions to log in to the server (see Logging in and out on page 42). To save the server details and log in later, tap Save and log in later.

Connect to a server that you have used before

- 1. Open the XProtect Mobile app.
- 2. From the list of servers in your network, tap the mobile server you want to connect to.
 - If you have previously enabled **Remember me** for this mobile server, tap the server to log in.
 - If you haven't enabled the **Remember me** setting, tap the server and follow the instructions to log in to the mobile server (see Logging in and out on page 42).

Connect by entering the unique identifier for the server



This connection method uses the Address book service and requires a Milestone Care Plus subscription package.

Ask your system administrator for the unique identifier for the server.

- 1. Open the XProtect Mobile app.
- 2. On the **Servers** screen:
 - Android Tap Add server to scan the local network for mobile servers.
 - iOS Tap Edit, then tap Add server to scan the local network for mobile servers.
- 3. On the Add servers screen, tap Add server with ID.
- 4. Enter the server ID and tap Add server.
- 5. To continue login, on the **Servers** screen, tap the mobile server. Then, follow the instructions to log in to the mobile server (see Logging in and out on page 42).

Connect from an email



This connection method uses the Address book service and requires a Milestone Care Plus subscription package.

Your system administrator can send you an email that contains a unique identifier for the server. Use the identifier to connect your mobile device to a mobile server.

- 1. On your mobile device, find the email from your system administrator.
- 2. If XProtect Mobile is not installed, tap the **Download XProtect Mobile** link to go to the store where you can download it. Then, install the app on your device.

- 3. In the same email, tap Add your server to XProtect Mobile.
- 4. To continue login, on the Servers screen, tap the mobile server. Then, follow the instructions to log in to the mobile server (see Logging in and out on page 42).

Disconnect a mobile server

If you want to disconnect your mobile device from a server:

- Android and iOS After you log in to the mobile server, on the server screen:
 - 1. In the upper left-hand corner, tap the user menu.
 - 2. Tap Disconnect from server.
- Android After you log in to the mobile server, go back to the Servers screen:
 - 1. In the servers list, go to the server you want to disconnect.
 - 2. Tap and then tap **Disconnect**.



If you have enabled the Remember me setting, on your next login, your user credentials will remain saved for the disconnected server.

View and edit connections to mobile servers

If, for example, you want to change the type of connection or select another server as the default server, you can view and change settings for your connections to mobile servers.

- 1. On the **Servers** screen:
 - Android In the list of servers, tap for the relevant mobile server, then tap **Edit** to open the Edit server screen.
 - iOS Tap Edit, then tap the relevant mobile server to open the Edit server screen.
- 2. On the **Edit server** screen, view or edit the server settings:
 - Automatic connection Enables you to connect to the mobile server even if the server address has changed. By default, this setting is enabled.
 - Secure connection Use HTTPS when you connect to a server. By default, the HTTPS connection is enabled.



If you want to use an HTTPS connection, a digital certificate from a certificate authority (CA) must be installed on your XProtect Mobile server. You cannot connect to the mobile server through your XProtect Mobile app if you use a self-signed certificate. If in doubt, ask your system administrator.

- **Server connections** Lists the available server addresses.
 - To add mobile server addresses manually, tap Add address. Enter the server address and the port number for the mobile server, and then tap Add address (Android) or Save (iOS).
 - To edit mobile server addresses:
 - Android Tap for the relevant server address and tap **Edit**. Edit the address and the port number, and tap Save address.
 - iOS Tap Edit, tap the relevant server address, and tap Edit. Edit the address and the port number, and tap Save.
 - To delete mobile server addresses:
 - Android Tap for the relevant server address and tap **Delete**. Then, tap **Yes** to
 - iOS Tap Edit, tap the red minus icon for the relevant server address, and tap Delete. Then, tap Done.
- Default server Enable the setting if you want to always connect to this mobile server when you start XProtect Mobile.
- Save server settings Tap the button to save your edits.

Enable access request notifications in XProtect Mobile



To receive notifications from your VMS, you have to purchase a Milestone Care Plus license. Access request notifications are disabled by default.

In addition to the security settings on the server, you must also enable access request notifications in the server settings in the XProtect Mobile app. You must do this for all servers that the app is connected to.

- 1. Open your XProtect Mobile app, and then do the following:
 - Android In the list of servers, go to the server you want to connect to, tap
 - iOS In the list of servers, in the upper right-hand corner, tap Edit, and then tap the server that you want to connect to.
- 2. Under **Notifications**, enable the **Receive notifications** option per that server.
- 3. Tap Notification settings (iOS) or Tap to configure (Android) and enable Access requests.
- 4. Tap Done.
- 5. On the Edit server screen, tap Save (iOS) or Save server settings (Android).



If you have enabled the notifications setting but you haven't saved your user credentials, you are prompted to enter your credentials or use your external IDP login method each time before you open a received notification.

If you disable Access requests, you will not be notified about any access requests, and the list of access requests will disappear from the XProtect Mobile app.

Enable or disable notifications

If you have configured events and alarms in your surveillance system, XProtect Mobile can send you a notification when events trigger alarms or when something goes wrong with a device or server. If you have the app open, XProtect Mobile displays the notification in the app.

If you want XProtect Mobile to notify you even when you don't have the app open, you must enable push notifications. Push notifications are sent to your mobile device. Settings for notifications on your mobile device determine how you are notified. For example, it can display a banner or play a distinctive sound.



Push notifications are available only if you have purchased a Milestone Care Plus license.

To receive notifications, you must enable the notifications setting on the app level (Android), mobile device, and server level.

Steps to enable or disable notifications on app level (Android) and mobile device level



By default, in the XProtect Mobile client, the notifications setting is enabled on the app (Android) and device level.

For Android users

- 1. Open your XProtect Mobile app.
- 2. On the **Servers** screen, tap
- 3. On the **Settings** screen, go to **Push notifications** and enable or disable the setting. To receive push notifications, you must also enable the notifications setting for the app on your mobile device.

For Android and iOS users

- 1. Go to the settings of your device. Tap XProtect Mobile, then tap Notifications.
- 2. Enable or disable the Allow Notifications setting.

Steps to enable or disable notifications on server level



By default, in the XProtect Mobile client, the notifications setting is disabled when you add

- 1. Open XProtect Mobile, and then do the following:
 - Android From the list of servers, go to the server you want to connect to, tap then tap Edit.
 On the Edit server screen, under Notifications, enable or disable Receive notifications per that server. If you haven't enabled the Push notifications setting in the app, tap the Go to the app settings link. To receive push notifications, you must also enable the notifications setting for the app on your mobile device.
 - iOS From the list of servers, in the upper right-hand corner, tap Edit. Tap the server that you
 want to connect to, and then under Notifications, enable or disable Receive notifications per that
 server. If you haven't enabled the notifications setting for the XProtect Mobile app on your mobile
 device, tap the Go to the mobile device settings link.



If you disable **Receive notifications**, you will receive server status notifications only. If you have enabled the notifications setting but you haven't saved your user credentials, you are prompted to enter your credentials or use your external IDP login method each time before you open a received notification.

- 2. To specify the alarms that you will be notified about, tap Notification settings (iOS) or Tap to configure (Android), and then do one of the following:
 - Enable Alarms:
 - Select All alarms You will be notified when any alarm is triggered, regardless of the alarm's owner or source.
 - Select My alarms You will be notified when an alarm that you own is triggered or when someone assigns an alarm to you.
 - Disable Alarms You will not be notified when events trigger alarms. However, you will be able to see those alarm events listed under Alarms.
- 3. To save your changes:
 - Android Tap Save server settings.
 - iOS Tap Done.

External IDP and XProtect Mobile client (explained)

XProtect Mobile client supports login with an external IDP.

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 the XProtect Mobile client via an external IDP with XProtect 2022 R3 and later.



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

For more information, see the topic about the login with an external IDP in the administrator manual about the XProtect VMS.

Using biometrics or device credentials to secure the app (explained)

The XProtect Mobile client supports using biometrics or device credentials for identity verification.

To easily and securely verify your identity when you open the app, you can use:

- Biometric authentication Using your fingerprint or facial recognition
- Your device credentials PIN, passcode, or other unlock pattern.

You can enable or disable the feature anytime from the app settings.



To use the feature in the app, you must enable the setting on your mobile device.

Steps to enable the feature for the XProtect Mobile app

In the app, on the **Settings** screen:

- 1. Under the **General** settings, go to the **Enable use of biometrics or your device credentials for this app** setting.
- 2. Enable the setting. By default, the setting is disabled.

Streaming video from your mobile device (explained)

Video push lets you stream live video with audio from the camera on your mobile device to your XProtect surveillance system.

This is useful, for example, to collect evidence when you examine an incident.



"When would I want to stream video from my mobile device?"

- A crowd is forming at an entrance, and you want to show the control room.
- You have witnessed a crime and want footage of the perpetrator.
- You are interviewing a witness and want to record the response.
- A guard is handling a situation, and you want to document his actions.

Your administrator must set up video push

Before you can use video push, your administrator must do the following in Management Client:

- Add a channel to the mobile server.
- Add the Video Push Driver as a hardware device.
- Enable the microphone related to the camera that you use for video streaming.
- Specify the users who can stream video from a device.



Video push is available in landscape and portrait mode.

For more information, see the administrator manual for XProtect VMS.

Set up video streaming on your mobile device

Settings for Android

On the **Video Push** screen, tap



On the Video push settings screen, specify the following:

- Video resolution The options for setting the resolution of the video stream are Low, Medium, High, or HD.
- Automatic image quality Enable to adjust the image quality of the video stream automatically.
- You can also set the image quality of the video stream to Low, Medium, or High.
- Location data Enable to include details about where you are while you stream the video. This requires that you turn on location information on your device. Only available for:
 - XProtect Corporate
 - XProtect Expert
 - · XProtect Professional+
 - XProtect Express+
 - XProtect Essential+

Settings for iOS

On the Video Push screen, tap Settings.

On the Video push settings screen, specify the following:

- Video resolution The options for setting the resolution of the video stream are Low, Medium, High, or HD.
- Image quality Select whether to allow XProtect Mobile to adjust the image quality automatically or to set it to Low, Medium, or High. By default, the Automatic image quality is enabled. This can affect the quality of the video.



The XProtect Mobile client will change the compression of the images trying to maintain a stable number of frames per second even on slow connections. This is different from the server-side quality of service, which is used when viewing live video.

- Location data Enable to include details about where you are while you are streaming the video. Only available for:
 - XProtect Corporate
 - XProtect Expert
 - XProtect Professional+
 - XProtect Express+
 - XProtect Essential+

Listening to incoming audio (explained)

XProtect Mobile client supports incoming audio when you:

• View live video (see Viewing live video on page 46).



You can play the incoming live audio from microphones attached to cameras even when there is no live video streaming from these cameras.

• Play back video recordings (see Find and view video recordings on page 58).

The incoming audio is also available in:

- Investigations (see View or create an investigation on page 63)
- Alarms (see View alarms on page 65)
- Access control (see View doors and take action on page 68, Respond to access requests on page 69, Investigate access control events on page 70)
- Bookmarks (see Bookmarks (usage) on page 48).

Push-to-talk (explained)

The feature allows you to communicate through the XProtect VMS from the microphone of your mobile device with people near a video camera with audio equipment. You can also listen to the recorded conversations in playback mode.

XProtect Mobile client supports the push-to-talk (PTT) feature:

- While you are watching live video from one camera (see Viewing live video on page 46).
- When you play the recorded outgoing audio in video recordings (see Find and view video recordings on page 58).
- In investigations (see View or create an investigation on page 63).

- In alarms (see View alarms on page 65).
- In access control (see View doors and take action on page 68, Investigate access control events on page 70 and Respond to access requests on page 69).



You must allow the XProtect Mobile app to have access to the microphone of your mobile device (see Requirements for using push-to-talk on page 13).

When the push-to-talk (PTT) feature is available for use, you will see the **Push-to-talk** button on the camera toolbar. Its icon has the following states:

Icon	Description
(Available)	In live mode, it shows that the push-to-talk (PTT) feature is available and that you fulfilled the necessary requirements for using it. Tap and hold to start using push-to-talk. Release the button to end transmitting audio.
(Active)	In live mode, it shows that you are currently using the push-to- talk (PTT) feature. The microphone of your mobile device and the speaker of the video camera are in an active state. The blue pulsating circle indicates the sound level.
(Disabled)	In live mode, it shows that the push-to-talk (PTT) feature is available but that you did not fulfill the necessary requirements for using it (see Requirements for using push-to-talk on page 13).
(Android) (Android)	In playback mode, when you tap (Android) or (iOS), it shows that you can listen to incoming and outgoing recorded audio while playing back a video recording and that you can select the audio source that you want to listen to.

Rules for interrupting push-to-talk

Based on the level of your user permissions (Administrators or Operators), there are two rules for interrupting a push-to-talk session in live mode:

- Users with the same level of user permissions cannot interrupt each other.
- Users with a lower level of user permissions (Operators) cannot interrupt users with a higher level of user permissions (Administrators).

Mobile device management (MDM) (explained)

XProtect Mobile client supports 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.



To use the MDM functionality on your mobile device, the administrator of your XProtect VMS 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 the administrator has updated the details of an already added mobile server, you must delete this server from the servers list manually and restart the XProtect Mobile app.

For more information, see the topic about configuring the mobile server details on the MDM platform in the manual about the mobile server.

Direct streaming (explained)

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. 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.

You can use direct streaming in the single-camera view, the grid view, and picture-in-picture (PiP).

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 14).
- The codec of the streaming camera is different than H.264 or H.265.
- The video cannot start playing for more than four seconds.
- The connection with the server or with the camera has been lost.
- You use the privacy masking feature during live video.

Adaptive streaming (explained)

XProtect Mobile supports adaptive streaming in live mode.

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 allows you to:

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



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



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

For more information, see the administrator manual for XProtect VMS.

Operation

Logging in and out

You can log in to the XProtect Mobile client as a basic user or as a Windows user, or you can log in with an external IDP. Your system administrator defines the authentication login method in XProtect Management Client.



Milestone recommends that you use a secure connection when you manage your user credentials

Steps to log in as a basic user for the first time

To log in as a basic user for the first time, you must change the temporary password that your system administrator has given you:

- 1. Tap the XProtect Mobile app icon. Then, tap Add servers.
- 2. From the list of servers in your network, tap the mobile server you want to connect to.
- 3. On the Add servers screen, enter the server details and tap Continue login.
- 4. On the **Login** screen:
 - 1. Select Basic user as your authentication login method.



Your system administrator must define the user profile in the surveillance system.

- 2. Enter your user name and temporary password and tap Log in. A dialog box appears.
- 3. Tap **Continue** to open a new window.
- 5. Follow the instructions in the Set a new password wizard and save your new password.
- 6. After saving your changes, you will be redirected back to:
 - Android The **Login** screen to continue your login as a basic user.
 - iOS The **Servers** screen to continue your login as a basic user. On the **Servers** screen, tap the relevant server to open the **Login** screen.
- 7. On the **Login** screen, enter your user name and new password. By default, the **Remember me** setting is enabled.
- 8. Tap Log in.

Steps to log in as a basic user

- 1. Tap the XProtect Mobile app icon.
- 2. On the **Servers** screen:
 - If you want to log in to a new mobile server, tap Add server to open the Add server screen. Follow
 the instructions to connect your mobile device to the mobile server (see Connect your mobile
 device to a mobile server or disconnect a mobile server on page 28). Then, continue with step
 three of this procedure.
 - If you want to log in to an already added server, from the list of servers, tap the relevant mobile server.
 - If you have enabled the **Remember me** setting, you log in to the server directly.
 - If you haven't enabled the **Remember me** setting, continue with step three of this procedure.
- 3. On the Login screen:
 - 1. Select **Basic user** as your authentication login method.



Your system administrator must define the user profile in the surveillance system.

- 2. Enter your user credentials. By default, the **Remember me** setting is enabled.
- 3. Tap Log in.
- 4. (Optional) If your system administrator has set up two-step verification for your user account, you are asked for a verification code, which the system sends to your email address. If in doubt, ask your system administrator for the email address.
 - 1. Open your email program and make a note of the numbers.
 - 2. Enter the code in the XProtect Mobile app and tap Log in.



If you do not use the verification code within a specific period of time (the default period of time is five minutes), the verification code times out. You can then request a new code on the screen where you enter the code.



If you exceed the number of allowed code entry attempts (the default number is three), you will be blocked from making more attempts. In that case, you must log out of the XProtect Mobile app and log in again.



If your system administrator forces you to change your password on the next login, follow the steps listed above to log in.



If you use an MDM functionality on your mobile device, the mobile server details will be entered automatically and after you tap on the relevant mobile server, you'll go to the **Login** screen directly. For more information, see Mobile device management (MDM) (explained) on page 40.

Steps to log in as a Windows user:

- 1. Tap the XProtect Mobile app icon.
- 2. On the **Servers** screen:
 - If you want to log in to a new mobile server, tap Add server to open the Add server screen. Follow
 the instructions to connect your mobile device to the mobile server (see Connect your mobile
 device to a mobile server or disconnect a mobile server on page 28). Then, continue with step
 three of this procedure.
 - If you want to log in to an already added server, from the list of servers, tap the relevant mobile server.
 - If you have enabled the **Remember me** setting, you log in to the server directly.
 - If you haven't enabled the **Remember me** setting, continue with step three of this procedure.
- 3. On the Login screen:
 - 1. Select Windows user as your authentication login method.



Your system administrator must define the user profile in the surveillance system.

- 2. Enter your user credentials. Windows user credentials are specific to a machine or a domain. By default, the **Remember me** setting is enabled.
- 3. Tap Log in.



If you use an MDM functionality on your mobile device, the mobile server details will be entered automatically and after you tap on the relevant mobile server, you'll go to the **Login** screen directly. For more information, see Mobile device management (MDM) (explained) on page 40.

Steps to log in with an external IDP

- 1. Tap the XProtect Mobile app icon.
- 2. On the Servers screen:
 - If you want to log in to a new mobile server, tap Add server to open the Add server screen. Follow
 the instructions to connect your mobile device to the mobile server (see Connect your mobile
 device to a mobile server or disconnect a mobile server on page 28). Then, continue with step
 three of this procedure.
 - If you want to log in to an already added server, from the list of servers, tap the relevant mobile server.
- 3. On the Login screen, tap Log in with [Name of an external IDP] (see External IDP and XProtect Mobile client (explained) on page 35.



If you use an MDM functionality on your mobile device, the mobile server details will be entered automatically and after you tap on the relevant mobile server, you'll go to the **Login** screen directly. For more information, see Mobile device management (MDM) (explained) on page 40.

Steps to log out from the XProtect Mobile server

- 1. In the app, go to the server screen.
- 2. In the upper left-hand corner, tap the user menu.
- 3. Tap Log out.



Logging out will remove your saved user credentials for this mobile server.

Change password in XProtect Mobile client

Changing your password often increases the security of your XProtect VMS system. If you log in as a basic user, you can change your password whenever you want to, or your system administrator can force you to change your password. If you use the Windows authentication method, only your system administrator can change your password.



To be able to manage your user credentials, you must use XProtect VMS 2021 R1 or later.

To change your password for an already added mobile server:

- 1. Open the XProtect Mobile app, then on the Servers screen, tap the relevant mobile server.
 - If you have saved your user credentials, the server screen displays.
 - 1. In the upper left-hand corner of the server screen, tap the user menu.
 - 2. In the user menu, tap **Change password** to open a new browser window.
 - If you haven't saved your user credentials, on the **Login** screen:
 - 1. Select the **Basic user** authentication.
 - 2. Tap **Change password** to open a new browser window.
- 2. Follow the instructions in the Set a new password wizard and save your new password.
- 3. After saving your changes, you'll be redirected to the **Servers** screen in the XProtect Mobile app.
- 4. Tap the relevant mobile server. The **Login** screen displays.
- 5. On the **Login** screen, in the **User name** and **Password** fields, enter your user credentials. By default, the **Remember me** setting is enabled.
- 6. Tap Log in.



If you have forgotten your current password, you must contact your system administrator. The system administrator will force you to change your password on your next login.



Your account will be locked out if you have made many unsuccessful login attempts. You can either wait for the lockout time to expire or contact your system administrator. The administrator can enable your account again and, in addition, may force you to change your password on the next login.

Viewing live video

You can view video only on cameras that are set up in views in XProtect Smart Client. You cannot create views in XProtect Mobile. Also, the XProtect Mobile client displays only video. If a view in XProtect Smart Client contains other types of content, such as maps, text, or HTML pages, the content does not display.

When you connect to a server, the XProtect Mobile client lists your views.

- Android To access your views, tap Views.
- iOS To access your views, tap

On the **Home** screen, the available views are organized in folders:

- . (Android)
- . (iOS)

These folders can contain other folders with views or separate views with cameras - (Android) or (iOS). The views can only contain cameras.

The list of views offers the following information:

- The name of the folder. This can be **Shared** with views that everyone can access, or **Private** with views that you have set up in XProtect Smart Client, and only you can access.
- The name of the view. For example, Building A.
- The number of cameras available in the view.

Start viewing live video from a camera

- 1. Tap a view to display the cameras that it contains.
- 2. Tap the preview image for the camera.
- 3. Optional. Tap (Android) or (iOS) to start playing audio. Tap (Android) or (iOS) to stop playing audio (Only for cameras that have microphones attached).
- 4. Optional. Tap and hold to start push-to-talk. Release the icon to end transmitting audio (Only for cameras that have speakers).
- 5. Optional. Tap (Android) or (iOS) to add a bookmark to quickly locate relevant video sequences (see Bookmarks (usage) on page 48).

Stop viewing live video from a camera, or view another camera

To stop viewing live video:

- Android Tap \leftarrow
- iOS Tap

To view video from another camera in the view:

• Swipe right or left.

Camera indicators

The camera indicators show you if the camera is detecting motion, recording video, or both. The camera indicators are visible in the camera title bar.

Symbol	Is motion being detected?	Is the video being recorded?
鋏●	\otimes	\otimes
<u>₹</u>	\odot	\otimes
鉄	\otimes	\odot
<u>₹</u>	\odot	\odot

Search for a specific camera

If you have lots of views and cameras, you can find a camera by searching for the camera name.

- 1. Above the list of views, tap
- 2. Enter the name of the camera.

Bookmarks (usage)

This 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/solutions/platform/product-index/).

You can use bookmarks to quickly locate relevant video sequences. You can use the feature in both live mode (see Viewing live video on page 46) and playback mode (see Find and view video recordings on page 58) or while you use video push (see Stream video from your device to your surveillance system on page 64).

Bookmarks (explained)

A bookmark is, essentially, a small video clip. When you bookmark an incident, the system automatically assigns it an ID and adds the user who created the bookmark.

A bookmark video clip typically contains video from a few seconds before and a few seconds after the bookmarked incident (the time interval is specified by the system administrator) to ensure that the incident is recorded, regardless of any delays.



Depending on your user permissions, you may not be able to add bookmarks from certain cameras due to restrictions. You may be able to view bookmarks even if you cannot add them, and the other way around.

View the bookmark details or play the bookmark video clip

In the XProtect Mobile app, you can create detailed bookmarks to make it easier to find the bookmarks after you have created them.

To view the details of the bookmark that you have added and to play the bookmark video clip:

- 1. On the **Home** screen, tap **Bookmarks** (Android) or (iOS) to open the bookmarks list.
- 2. On the **Bookmarks** screen, select **All bookmarks** to open the complete list of bookmarks created by all users or **My bookmarks** to open a list of bookmarks that only shows those bookmarks that you have created yourself.
- 3. Optional. If the list of bookmarks is too long, tap Load more.
- 4. Optional. To make the search easier, you can filter the list of bookmarks (see Filter your bookmarks on page 53).

- $5. \ \ \, \text{Navigate to the bookmark that you want to view, then tap on it. The \textbf{Bookmark details}} \, \text{screen opens.}$
- 6. To play the bookmark video clip, tap on the video.
- 7. On the **Bookmark details** screen, you can view:

Name	Description
Headline	The headline of the bookmark that must contain a maximum of 50 characters. The field is required.
Description	The additional description of the bookmark. The field is optional.
Start time	The suggested start time of the bookmark clip is a number of seconds before the time of the bookmark event. The start time is specified by the system administrator.
Bookmark event	The time in the video clip that shows when the bookmark event was triggered.
End time	The suggested end time of the bookmark clip is a number of seconds after the time of the bookmark event. The end time is specified by the system administrator.
Bookmark ID	A unique ID number that is assigned to the bookmark automatically.
Added by	The user who has created the bookmark.
Camera name	The name of the camera that streams the bookmark video clip.
Duration	The duration of the bookmark video clip.
See live video	Tap to return to the video in live mode.

Add or edit bookmarks

You can add bookmarks to live videos and video recordings.

Steps to add bookmarks to videos in live mode:

- 1. Tap **Views** (Android) or (iOS), then select the required camera in the view.
- 2. Tap (Android) or (iOS). The bookmark is added with the name **Quick bookmark** assigned by the system automatically.
- 3. Optional. To change the bookmark name, tap **Edit** on the success message. The **Edit bookmark** screen opens.
 - 1. In the **Headline** field, enter a name for the bookmark. You can also change the name later.
 - 2. Optional. Describe the incident. You can also change the description later.
 - 3. Tap Save.



The **Duration** of a bookmark clip is determined on the surveillance system server.

Steps to add bookmarks to videos in playback mode:

- 1. Select the required camera in the view and switch to playback mode.
- 2. Tap (Android) or (iOS). The **Add bookmark** screen opens.
- 3. In the **Headline** field, enter a name for the bookmark. You can also change the name later.
- 4. Optional. In the **Description** field, describe the incident. You can also change the description later.
- 5. Tap (Android) or **Save** (iOS).

The **Duration** of a bookmark clip is determined on the surveillance system server.



Depending on your user permissions, you can find the added bookmarks on the timeline of the video recording.

Steps to edit bookmarks

- 1. On the **Bookmarks** screen, navigate to the bookmark that you want to edit, then tap on it. The **Bookmark details** screen opens.
- 2. To edit the bookmark, tap (Android) or **Edit** (iOS). The **Edit bookmark** screen opens.
- 3. In the Headline field, enter a name for the bookmark.
- 4. Optional. Describe the incident.

- 5. Optional. Although the time of the bookmark event and the start and end time of the video clip are specified by the system administrator, you can adjust these settings. To do that, navigate to the time setting that you want to edit and tap . The Edit time frame screen opens. The time setting that you want to edit is highlighted in yellow.
 - 1. Drag the time indicator of the setting to the desired position on the timeline. You can also edit the time frame by tapping on the timeline to open the time picker.
 - 2. Optional. On the **Edit time frame** screen, repeat the step above to edit the other two time settings of the bookmark. The bookmark event time must be between the start time and the end time of the video clip.
- 6. Tap (Android) or **Save** (iOS).



The **Duration** of a bookmark clip is determined on the surveillance system server.

Delete bookmarks

Depending on your user permissions, you can delete bookmarks created by yourself or others. If you delete a bookmark, it is removed from the database, and you can no longer access it.

Steps to delete bookmarks:

- 1. On the **Edit bookmarks** screen, tap (Android) or **Delete** (iOS).
- 2. On the confirmation message, tap **Delete**.
- 3. Optional. Tap the bookmark you want to delete and swipe it to the left.

Use the filter

Filter your views

If you want to see a particular type of view only, or if you want to display fewer views, you can apply a filter. All views are displayed when you tap the filter, regardless of whether they are shown or filtered. You can always choose to include a view again.

How you filter views depends on the operating system on your device. To filter views:

1. On the **Home** screen:

- Android In the upper-right corner, tap . If a filter is already applied, the icon has a check
- iOS In the upper-right corner, tap . If a filter is already applied, the icon is blue
- 2. To include or exclude a view, tap the view or use the slider.
- 3. To apply the filter and return to the list of views:
 - Android In the upper-right corner, tap
 - iOS In the upper-right corner, tap **Done**.

Discard filter selections

If you haven't saved your selections yet, you can discard them:

- Android In the upper-left corner, tap
- iOS Undo your selections manually.

Filter your bookmarks

To find a specific bookmark, you can search and use filtering. There are three options for filtering bookmarks:

- You can enter a keyword from the headline, the description, or the complete ID of the bookmark.
- You can select specific cameras.
- You can select a predefined time interval. You can also customize the time interval that you want to apply as a filter.

Steps to filter bookmarks by a keyword

- 1. On the **Bookmarks** screen:
 - Android In the upper-right corner, tap ... If a filter is already applied, the icon has a check
 - iOS In the upper-right corner, tap . If a filter is already applied, the icon is blue
- 2. On the **Filter bookmarks** screen, in the **Keywords** field, enter a keyword from the headline or description of the bookmark or enter the complete bookmark ID.

- 3. To apply the filter and return to the list of bookmarks:
 - Android In the upper-right corner, tap
 - iOS In the upper-right corner, tap Apply.
- 4. Optional. To undo your filter selection, tap Clear all filters.

Steps to filter bookmarks by selected cameras

- 1. On the **Bookmarks** screen:
 - Android In the upper-right corner, tap . If a filter is already applied, the icon has a check
 - iOS In the upper-right corner, tap . If a filter is already applied, the icon is blue
- 2. On the **Filter bookmarks** screen, tap **Select cameras**. The **Cameras** screen opens, and the list of all available cameras is displayed.
- 3. Optional. To quickly find specific cameras, use the Search option.
- 4. From the camera list, select the cameras that you want to apply as a filter. To undo your selection, tap the selected cameras.
- 5. Optional. To select all cameras in the list, use the **Select all** option. To undo your selection, tap **Deselect all**.
- 6. To navigate back to the **Filter bookmarks** screen after you have finished your selection, tap (Android) or **Filters** (iOS).
- 7. To apply the selected cameras as a filter and return to the list of bookmarks:
 - Android In the upper-right corner, tap
 - iOS In the upper-right corner, tap Apply.
- 8. Optional. To undo your filter selection, tap Clear all filters.

Steps to filter bookmarks by predefined or custom time intervals

You can filter the list of your bookmarks by using a specific time frame with predefined or custom time intervals between the start time and the end time of the video sequences that you have bookmarked. The default duration of the time frame is set to **2 hours**.

1. On the Bookmarks screen:

- Android In the upper-right corner, tap . If a filter is already applied, the icon has a check
- iOS In the upper-right corner, tap . If a filter is already applied, the icon is blue
- 2. On the **Filter bookmarks** screen, to specify the time frame:
 - Android Select the **Show specific time frame** check box.
 - iOS Enable the **Show specific time frame** setting.
- 3. To open the list of predefined time intervals:
 - Android Tap the Predefined time intervals list.
 - iOS Tap the Predefined time intervals link.
- 4. Select one of the following time intervals:
 - Last 2 hours
 - · Last 6 hours
 - · Last 12 hours
 - · Last 24 hours
 - Yesterday
 - Last 7 days
- 5. Optional. To customize the time interval between the start time and the end time of the video sequence that you have bookmarked, tap
- 6. To apply the filter and return to the list of bookmarks:
 - Android In the upper-right corner, tap
 - iOS In the upper-right corner, tap Apply.
- 7. Optional. To undo your filter selection, tap Clear all filters.

Interact with live video in full screen

Use pan-tilt-zoom controls and PTZ presets

If you're viewing video from a pan-tilt-zoom (PTZ) camera, tap (Android) or (iOS) to use the PTZ controls. Tap controls once to pan or zoom one step.

If your administrator created PTZ presets for the PTZ camera in Management Client, you can use PTZ presets on your device in PTZ mode. PTZ presets are predefined positions in the view.

How you access PTZ presets depends on the operating system on your device.

- Android Tap
- iOS Tap

From the PTZ presets list, select a preset to start using it.

Zoom in or out

You can zoom in or out to get a better look at the video.

- To zoom in, pinch out or tap
- To zoom out, pinch in or tap

XProtect Mobile uses digital zoom.

Crop or fit images to the screen

You can resize images to fit them to your screen, or you can crop them. By default, images are fitted to the screen.

The outer parts of images are removed. Tap twice to crop images to fill the screen and preserve the image's aspect ratio.

Display other cameras in the view

If your view contains other cameras, you can swipe right or left to display their video.

Switch to playback mode

If you are recording and something happens that you want to review, you can switch to playback mode to review the footage or start an investigation.

To switch to playback mode:

- Android Tap
- iOS Tap



To keep an eye on the live video while you are investigating, turn on picture-in-picture by tapping . To turn off the picture-in-picture option, tap again.

Use picture-in-picture

If you see something that you want to investigate, but you don't want to stop observing the current situation, you can display live video using picture-in-picture (PiP) and play back video at the same time.

To turn on picture-in-picture (PiP):

- 1. Switch from live mode to playback mode by tapping (Android) or (iOS).
- 2. Depending on the operating system on your device:
 - Android Tap
 - iOS Tap



Incoming audio is not available in PiP.



To move the PiP window, tap and hold, and drag the PiP window to the preferred place on the screen.

Return to live video

To view the live video in full screen:

- Double-tap the PiP window.
- Tap \leftarrow (Android) or \triangleleft (iOS).

Take a snapshot

When you view a live video or play it back, and you find something that is of interest, you can take a snapshot of that content on your device.



If you don't have sufficient user permissions, you will not be able to take snapshots when using the XProtect Mobile app. If in doubt, ask your system administrator.

Snapshots are saved on your mobile device.

- Android View snapshots on your device's SD card at /mnt/sdcard/Milestone.
- iOS View snapshots in the **Photo Library**.



You cannot change the save locations.

To take a snapshot in live mode or playback mode:

- Android Tap
- iOS Tap 🖾.

Find and view video recordings

In playback mode, you can access the recorded video from a camera.

View video recordings from a camera

How you access recordings depends on the operating system of your device.

- 1. In the view that contains the camera, tap the preview image for the camera.
- 2. Tap (Android) or (iOS).
- 3. To view a list of recordings from the camera:
 - Android Tap
 - iOS Tap

Playing back recorded video

Use the timeline controls to play back the recorded video. Controls are shown or hidden depending on what you are doing.

- Tap to open the time picker or scroll the timeline to go to a specific time in the recording (see Using the playback timeline (explained) on page 60).
- Speed up or slow down the playback.
- (Android) or (iOS) Play the video backward or forwards, and pause the video by tapping

- (iOS).
- (Android) or (iOS) Go to the previous or next sequence.
- (Android) or (iOS) Go one frame forward or one frame backward in the sequence.

In playback mode, you can also:

- Hide or display live video from the camera in a picture-in-picture window (see Use picture-in-picture on page 57).
- (Android) or (iOS) Add a bookmark to quickly locate relevant video sequences (see Bookmarks (usage) on page 48).



Depending on your user permissions, you can find the added bookmarks on the timeline of the video recording.

Playing back audio in video recordings (For cameras that have microphones and speakers attached)

To listen to recorded incoming audio and outgoing audio, tap (Android) or (iOS) to open the **Audio** sources list and select the audio device that you want to listen to while playing back the video recording.

The options are:

- All sources Listen to both the recorded incoming and outgoing audio.
- Microphone Listen to the incoming audio only.
- Speaker Listen to the outgoing audio only.
- Audio off (default)



You can play back audio only when there is a video recording, and you play the recording forward at normal speed.

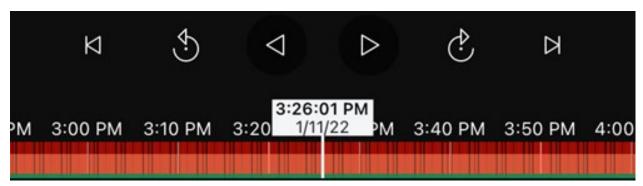
Load more recordings

In the **Recent history** (iOS) or **History** (Android) lists, if you don't find the sequence that you want and more recordings are available, you can load more and keep investigating.

• Android and iOS - Tap Load more.

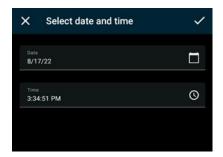
Using the playback timeline (explained)

On the timeline bar, you can specify the time of the recording, when you want to play back a recording, or when you want to view an investigation.

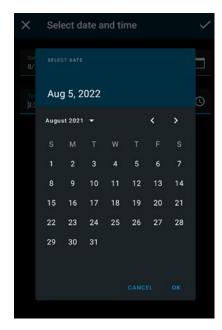


To do that in playback mode:

• (Android) On the timeline bar, tap the time indicator to open the time picker. On the **Select date and time** screen:



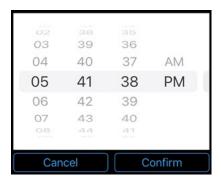
• To select the date, tap . After selecting the date, tap **OK**. You can also type the desired date into the **Date** field.



• To select the start time, tap . After selecting the time, tap **OK**. You can also type the desired start time into the **Time** field.



- To save your changes, tap . The recording loads at the selected start time and date.
- (iOS) On the timeline bar, tap the time indicator to open the time picker and select the start time of that part in the recording that you want to play back. Then tap **Confirm**. The recording loads at the selected start time.



• On the timeline bar, drag the time scroller to the right or to the left to adjust the start time of that part in the recording that you want to play back. In the center of the time scroller, the time indicator shows the selected time in the recording. While you drag the time scroller, you see the frames currently selected in the recording. When you stop dragging the time scroller, the recording that you want to play back loads at the selected start time.

The maximum time period displayed on the timeline is 24 hours, with a four-hour time interval between frames. The minimum time interval between frames is one minute.

Colors in the timeline

- Light red indicates recordings.
- · Red indicates motion.
- Light green indicates incoming audio.
- Green indicates outgoing audio.

In an investigation, you can follow the same steps to specify the time in the investigation that you want to view.

View or create an investigation

If you are using investigations in XProtect Web Client, you can use XProtect Mobile to view and create investigations. You can preview video from investigations, but you cannot download it to your mobile device.

View ongoing and completed investigations

How you access investigations depends on the operating system of your mobile device.



You can quickly refresh the list of investigations by swiping down from the top. You need to be at the top of the list. Otherwise, you will scroll instead.

- 1. To go to investigations:
 - Android Tap Investigations.
 - iOS On the **Navigation** pane, tap
- 2. Optional: On the **Investigations** screen, you can filter investigations:
 - My investigations View your investigations.
 - **All investigations** View your investigations and those that other people created. Your administrator must enable you to do this.
- 3. To see the details of an investigation, tap the investigation.
- 4. To view the video in the investigation:
 - Tap (Android) or (iOS).
- 5. To go to a specific time period in the investigation, on the timeline bar, tap to open the time picker or scroll the timeline to go to a specific time in the recording (see Using the playback timeline (explained) on page 60).

Create an investigation

When you create an investigation, the video is saved on the mobile server that you are connected to, not on your mobile device. To view the video on your device, you must connect to the server.

- 1. Find the camera that recorded the video, then tap the preview image to maximize it.
- 2. Tap (Android) or (iOS), then:
 - Android Tap
 - iOS Tap
- 3. Specify the time to define the period to investigate.
- 4. Tap Create.

Listen to audio in an investigation

If you create an investigation from a camera with audio devices (microphone and speaker) attached, you can listen to incoming and outgoing recorded audio when you play the recording forward at normal speed (see Find and view video recordings on page 58).

Stream video from your device to your surveillance system

If your system administrator has set up video push in Management Client and has enabled you to use video push, you can stream video with audio from your device to your surveillance system. For more information, see Streaming video from your mobile device (explained) on page 36 and Requirements for using video push on page 14.

How you access and use video push depends on the operating system on your device:

- 1. Access video push:
 - Android In the bottom-right corner, tap
 - iOS In the navigation bar, tap
- 2. Stream the video from the front-facing or back-facing camera of your device:
 - Android and iOS tap
- 3. Start streaming video:
 - Android Tap
 - iOS Tap
- 4. Optional. Start audio in the video push:

- Android and iOS Tap
- 5. Optional. Stop audio in the video push:
 - Android and iOS Tap
- 6. Stop recording:
 - Android Tap
 - iOS Tap

Bookmark an interesting moment

If you see something that you will want to investigate later, you can bookmark the moment in the video while you are streaming the video from your device to your surveillance system.

To add a bookmark:

- Android In the upper-right corner, tap
- iOS In the upper-left corner, tap Bookmark.

On the **Bookmarks** screen, you can view, edit, or delete the bookmark that you have added. For more information, see Bookmarks (usage) on page 48.

Investigate the video you streamed

XProtect Mobile records the video that you stream so that you can investigate it.

- 1. Go to the view with the video push camera.
- 2. Tap the camera to go to full screen.
- 3. To play back the recording, tap (Android) or (iOS).
- 4. Use the playback controls to investigate the video.

View alarms

Alarms can be triggered by various events:

- A camera stops working.
- A pane of glass gets shattered or broken.
- A locker gets broken into.
- A blacklisted license plate is seen on camera.



To view alarms, ask your system administrator to set up alarms and give you the required user permissions.

To view an alarm:

- 1. Open Alarms:
 - Android Tap Alarms.
 - iOS Tap 🚨.
- 2. From the All alarms list, find the alarm you want to play video for and tap it.
- 3. View the details of the alarm:
 - · Type of the event
 - Time of the occurrence
 - · State of the alarm
 - · To whom it is assigned
 - · Priority of the alarm
- 4. To play the video:
 - Android Tap
 - iOS Tap
- 5. Play the video backward or forward and check when the image that you are seeing was taken.
- 6. Optional. If the camera has audio devices (microphone and speaker) attached, you can listen to incoming and outgoing recorded audio when you play the video recording forward at normal speed (see Find and view video recordings on page 58).
- 7. To save the video for later or share it with others:
 - Android Tap
 - iOS -
- 8. Specify the time to define the period to investigate.
- 9. Tap Create.

Using actions in XProtect Mobile

If your system administrator has given you permission, you can trigger actions if you need to. In the clients, actions are outputs and events that you can activate. For example, you can:

- Start or stop recording.
- Switch to a different frame rate.
- Trigger SMS and email notifications.
- Move PTZ cameras to PTZ preset positions.
- Activate hardware output.

View and trigger actions

You can view and trigger actions in several places:

- · The list of views
- · When you view live video
- The Actions screen

View actions on the Actions screen

- 1. To view the list of actions that are grouped by **Outputs** and **Events**:
 - Android Tap Actions.
 - iOS Tap 💆

Trigger an action

- 1. There are two ways to trigger an action:
 - Android and iOS In the list of actions, tap the action, and then confirm that you want to trigger the action.
 - Android and iOS In live mode, on the camera toolbar, tap (Android) or (iOS) and select the action that is associated with the camera and that you want to trigger.

React to a notification

XProtect Mobile can notify you when something requires your attention even when you're not using the app. For example, the system can notify you when an alarm is triggered.

React now or later

To react immediately, tap the notification to open XProtect Mobile and investigate what happened. When you do this, XProtect Mobile does not store the notification.

If you don't want to react immediately, you can view the notification later:

- Android Go to the Notification Area. Open the notification drawer to see the details.
- iOS Go to the lock screen or the Notification Center.

View doors and take action

You can check the door's state, for example, **Closed**, **Unlocked**, and view live video or play back recorded video from the cameras monitoring the door. If the cameras have audio devices attached, you can also:

- Listen to the incoming audio and use the push-to-talk (PTT) feature in live mode.
- Listen to the incoming and outgoing audio in playback mode.

Based on the state of the door, you can either lock or unlock it.



Lock and **Unlock** are the standard options, but other commands may be defined in your access control system.

- 1. Open Access control:
 - Android Tap **Access Control**, then tap and select **Doors**.
 - iOS Tap , then tap **Doors**.

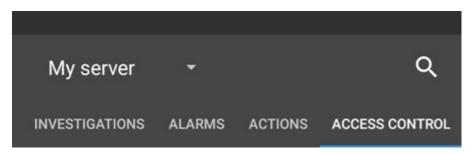
A list of doors appears.

- 2. Tap the door that you want to view.
- 3. View video in live mode from the camera monitoring the door.
- 4. Optional. Tap (Android) or (iOS) to start playing incoming audio. Tap (Android) or (iOS) to stop playing audio (Only for cameras that have microphones attached).
- 5. Optional. Tap and hold to start push-to-talk. Release the icon to end transmitting audio (Only for cameras that have speakers).
- 6. If required, Lock or Unlock the door. The state of the door changes.
- 7. To play back the video, tap the live image and then tap (Android) or (iOS). You can see the video stream in live mode even when you are in playback mode.
- 8. Optional. If the camera has audio devices (microphone and speaker) attached, you can listen to incoming and outgoing recorded audio when you play the video recording forward at normal speed (see Find and view video recordings on page 58).

Respond to access requests

When someone tries to enter a building using a door controller and access is denied, an access request is sent to your app. Depending on your access control system, you can respond by, for example, unlocking the door to let the person enter.

1. If you are using a VMS that supports push notifications, open the access request from the notification bar. This example is from an Android tablet. It may look different on iOS.



Or:

- 1. Open the app, and in the list of servers, tap the server that you want to connect to.
- 2. Open Access control:
 - Android Tap the **Access Control** tab, then tap and select **Access requests**.
 - iOS Tap , then tap Access requests.
- 3. Tap an access request to open it. After opening the access request, you will see:
 - Live video from the cameras at the door.
 - Details about the person who tries to enter.



- 4. To switch cameras, swipe the live image left. If there are more than two, swipe several times.
- 5. Optional. Tap (Android) or (iOS) to start playing incoming audio. Tap (Android) or (iOS) to stop playing audio (Only for cameras that have microphones attached).
- 6. Optional. Tap and hold to start push-to-talk. Release the icon to end transmitting audio (Only for cameras that have speakers).
- 7. Now you can either **Lock** or **Unlock** the door.

- 8. To play back the video before or at the time when the cardholder tried to enter:
 - 1. Tap the live image. The live video feed displays in a bigger view.
 - 2. Tap (Android) or (iOS) to switch to playback mode. In the changed view, you can still view the live video at the top.
 - 3. Optional. If the camera has audio devices (microphone and speaker) attached, you can listen to the incoming and outgoing recorded audio when you play the video recording forward at normal speed (see Find and view video recordings on page 58).

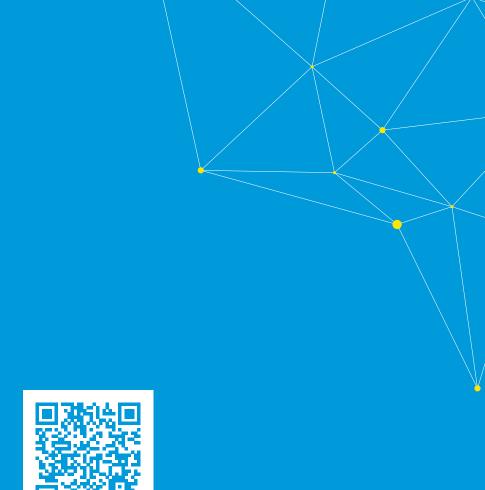
Investigate access control events

You may want to check who entered a building during the last hour or who was denied access. Other examples of access control events are **Door controller tampering** and **Door controller power failure**. Such events are defined in the access control system.



By default, all access control events from the last 30 days are displayed.

- 1. Open Access control:
 - Android Tap the **Access Control** tab, then tap and select **Events**.
 - iOS Tap **!**, then tap **Events**.
- 2. Optional. If the event is not in the list, tap Load more at the bottom of the list to view more events.
- 3. Tap an event to view details about it. For example, if the event is **Door Locked**, tap **View door** to check the state of the door or to lock or unlock the door.
- 4. To play back the video recorded at the time of the event:
 - Android Tap
 - iOS Tap
- 5. Optional. If the camera has audio devices (microphone and speaker) attached, you can listen to two-way recorded audio when you play the video recording forward at normal speed (see Find and view video recordings on page 58).



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/.







