AXIS Camera Station Pro

User manual

About

AXIS Camera Station Pro is a video management solution for monitoring, recording, and managing video feeds from Axis network cameras. It supports access control, multi-site management, AXIS Audio Manager integration, and third-party system integration.

It's compatible with all maintained AXIS OS versions on the active, Long-Term Support (LTS) and Product Specific Support (PSS) tracks*. For more information, see AXIS Camera Station Pro release notes or the *AXIS OS Portal*. To check which products work with AXIS Camera Station Pro, see *Compatible products*.

*We aim to support compatibility with older AXIS OS versions whenever commercially viable.

Access options

AXIS Camera Station Pro server – manages all communication with cameras, video encoders, and auxiliary devices in your system. For information about system requirements and capacity planning, see *Hardware guidelines* in the *AXIS Camera Station Pro – Installation and migration guide*.

AXIS Camera Station Pro client – provides access to recordings, live video, logs, and configuration. You can install it on any computer, enabling remote viewing and control from anywhere on the internet or corporate network.

Web client for AXIS Camera Station – provides access to AXIS Camera Station Pro recordings and live video in your web browser. See the *Web client for AXIS Camera Station user manual* for more information.

AXIS Camera Station Pro mobile app – provides access to recordings and live video on multiple systems. You can install the app on Android and iOS devices and enable remote viewing from other locations.

Download options

Go to the *AXIS Camera Station Pro download page* to download, update, or try it for free for 90 days.

- **Free, fully featured 90-day trial:** Try AXIS Camera Station Pro for free for 90 days. No license needed.
- **Update your client only – Offline:** Updates the client, the part of AXIS Camera Station Pro you interact with directly. Use this if you only need to update the client, not the server.
- **Update your client and server – Offline:** A compressed update package for both the client and the server. After downloading, extract the .zip file to access the .msi and .cab files, then run the .msi file to start the update.
- **Update your client and server – Online:** Downloads, extracts, and installs the update automatically. Run the .exe file and follow the on-screen instructions. Keep your computer connected to the internet throughout the installation.
- **Mobile app for iOS:** The AXIS Camera Station Pro mobile app for iPhones and iPads. Available on App Store.
- **Mobile app for Android:** The AXIS Camera Station Pro mobile app for Android phones and tablets. Available on Google Play.

Tutorial videos

For more in-depth examples of how to use the system, go to *AXIS Camera Station Pro tutorial videos*.

System features

For more information about the system features, go to *AXIS Camera Station Pro Feature Guide*.

What's new?

For the new features in each AXIS Camera Station Pro release, go to *What's new in AXIS Camera Station Pro*.

Helpful links for an administrator

- *Connect to a server, on page 8*
- *Configure devices, on page 42*
- *Configure storage, on page 67*
- *Configure recording and events, on page 72*
- *Configure connected services, on page 109*
- *Configure server, on page 111*
- *Configure security, on page 121*

More manuals

- *Web client for AXIS Camera Station*
- *AXIS Camera Station Pro Integrator Guide*
- *AXIS Camera Station Mobile App*
- *AXIS Camera Station Pro tutorial videos*
- *AXIS Camera Station Pro Troubleshooting Guide*
- *AXIS Camera Station Pro System Hardening Guide*

Helpful links for an operator

- *Connect to a server, on page 8*
- *Configure client, on page 105*
- *Live view, on page 12*
- *Playback recordings, on page 24*
- *Export recordings, on page 26*

Quick start

Use this guide to get your system up and running.

Before you start:

- Configure the network for your installation. See *Network configuration*.
- Configure your server ports if needed. See *Server port configuration*.
- Make sure your system is secure. See *Security considerations*.

For administrators:

1. *Start the video management system*
2. *Add devices*
3. *Configure recording method, on page 6*

For operators:

1. *View live video, on page 6*
2. *View recordings, on page 6*
3. *Export recordings, on page 6*
4. *Play and verify recordings in AXIS File Player, on page 6*

Start the video management system

Double-click the AXIS Camera Station Pro client icon to start the client. When you start the client for the first time, it attempts to log in to the AXIS Camera Station Pro server installed on the same computer as the client.

Once the client opens, it asks you to license your system. Click **License now** to go to the **Manage licenses** page, where you can register the server with an organization. See *Manage connected services, on page 109* and *Manage licenses, on page 119* for more information.
You must register and connect the system to an organization to access connected services, such as the VMS web client, system health monitoring, and online licensing.

You can connect to multiple AXIS Camera Station Pro servers in different ways. See *Connect to a server*.

Add devices

The first time you start AXIS Camera Station Pro, the **Add devices** page opens and searches the network for devices to add. See *Add devices*.

1. Select the devices you want to add from the list. If you can't find a device, click **Manual search** or type to filter.
2. Click **Add**.
3. Click **Close** to skip configuration and continue later. To continue with the configuration now:
   3.1. Choose **Quick configuration** or **Site Designer configuration**. See *Import AXIS Site Designer projects, on page 45* for more information.
   3.2. Select **Add image overlay for date, time, and text** to add overlays to any Axis cameras that don't already have one.
   3.3. Click **Next**.
   3.4. Select your **Recording method** preference.
   3.5. Click **Next**.
   3.6. Choose your **Retention time** and **Recording storage**, and click **Finish** to apply the configuration.

Configure recording method

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera.
3. Turn on **Motion detection**, or **Continuous**, or both.
4. Click **Apply**.

View live video

1. Open a **Live view** tab.
2. Select a camera to view its live video.

See *Live view, on page 12* for more information.

View recordings

1. Open a **Recordings** tab.
2. Select the camera you want to view recordings from.

See *Recordings, on page 24* for more information.

Export recordings

1. Open a **Recordings** tab.
2. Select the camera you want to export recordings from.
3. Click  to display the selection markers.
4. Drag the markers to include the recordings that you want to export.
5. Click  to open the **Export** tab.
6. Click **Export...**

See *Export recordings, on page 26* for more information.

Play and verify recordings in AXIS File Player

1. Go to the folder with the exported recordings.
2. Double-click AXIS File Player.
3. Click  to show the recording's notes.
4. To verify the digital signature:
   4.1. Go to **Tools > Verify digital signature**.
   4.2. Select **Validate with password** and enter your password.
   4.3. Click **Verify** to see the verification results.

Note

- A digital signature is different from signed video. Signed video lets you trace a recording back to the camera it came from, so you can verify it wasn't tampered with. See *Signed video* and the camera's user manual for more information.
- If stored files don't have any connection with an AXIS Camera Station database (non-indexed files), you need to convert them to make them playable in AXIS File Player. Contact Axis Technical support for help converting your files.

Network configuration

Configure proxy or firewall settings before using AXIS Camera Station Pro if the client, server, and connected network devices are on different networks.

Client proxy settings

If a proxy server is between the client and the server, configure the proxy settings in Windows on the client computer. Contact Axis support for more information.

Server proxy settings

If the proxy server is between the network device and the server, you must configure the proxy settings in Windows on the server. Contact Axis support for more information.

NAT and Firewall

When a NAT or firewall separates the client and the server, configure it to ensure that the HTTP port, TCP port, and streaming port specified in AXIS Camera Station Pro Service Control can pass through. Contact your network administrator for help.

See *Port list for AXIS Camera Station Pro, on page 191* for more information.

Server port configuration

The AXIS Camera Station Pro server uses ports 29202 (TCP) and 29204 (HTTPS) for server-client communication. You can change the ports in AXIS Camera Station Pro Service Control if needed.

Note

Only change the ports if you intend to use AXIS Camera Station Pro without Axis Secure Remote Access v2 or any other Axis cloud services

For more information, see *General* or *FAQ*.

Security considerations

To prevent unauthorized access to cameras and recordings:

- Use strong passwords for all network devices (cameras, video encoders, and auxiliary devices).
- Install the AXIS Camera Station Pro server, cameras, video encoders, and auxiliary devices on a secure network, separate from the office network. You can install the AXIS Camera Station Pro client on a computer on another network, for example, a network with internet access.
- Make sure all users have strong passwords.

Connect to a server

The AXIS Camera Station Pro client lets you connect to a single server or multiple servers in different ways:

Last used servers – Connect to the servers used in the previous session.

This computer – Connect to the server installed on the same computer as the client.

Remote server – See *Connect to a remote server, on page 8*.

Axis Secure Remote Access v2 – See *Sign in to AXIS Secure Remote Access v2, on page 8*.

Note

- The first time you connect to a server, the client checks the server certificate ID. To make sure you're connecting to the correct server, compare the certificate ID with the one displayed in AXIS Camera Station Pro Service Control. See *General, on page 191* for more information.
- The client and server must have the same version. If there's a version mismatch when connecting to a local system or one with port mapping, the client can download the correct version to match the server and then switches to that version.
- For a client to connect to multiple servers, each server must have the same version. By default, the client shortcut uses the latest version.

Server list	To connect to servers from a server list, select one from the **Server list** drop-down menu. Click to create or edit the server lists. See *Server lists*.
Import server list	To import a server list file exported from AXIS Camera Station Pro, click **Import server list** and browse to an .msl file. See *Server lists*.
Delete saved passwords	To delete saved usernames and passwords for all connected servers, click **Delete saved passwords**.

Connect to a remote server

1. Select **Remote server**.
2. Select a server from the **Remote server** drop-down list or enter the IP or DNS address. If the server isn't listed, click to refresh the list of all the available remote servers. If the server is configured to accept clients on a different port than the default port number 29202, enter the IP address followed by the port number, for example, 192.168.0.5:46001.
3. Do one of the following:
   - Select **Log in as current user** to log in as the current Windows® user.
   - Clear **Log in as current user** and click **Log in**. Select **Other user** and provide another username and password to log in with different credentials.

Sign in to AXIS Secure Remote Access v2

1. Click the **Sign in to AXIS Secure Remote Access v2** link.
2. Enter your My Axis account credentials.
3. Click **Sign in**.
4. Select an organization and click **OK**.
5. Select the server you want to log in to.
6. Log in using your server credentials.

Note

Your server credentials are different from your My Axis account credentials.

The status bar at the bottom of the AXIS Camera Station Pro client shows the Axis Secure Remote Access v2 usage. **Data used this month** shows the total amount of relayed data used by the organization during the month. The counter resets on the first of every month at midnight.

Axis Secure Remote Access v2 on mobile devices

To log in to your server using Axis Secure Remote Access v2 on a mobile device (iOS and Android):

1. Go to *axis.com/products/axis-camera-station/overview* and download the AXIS Camera Station Mobile app.
2. Install and open the mobile app.
3. Sign in to Axis Secure Remote Access v2 with your My Axis account credentials.
4. Select the server you want to log in to.
5. Log in using your server credentials.

Note

- Your server credentials are different from your My Axis account credentials.
- You need to be invited to join the organization as a user before you can sign in with your My Axis account.

The mobile app shows the total amount of relayed data used by the organization during the month. For more information, read the *AXIS Camera Station Mobile app user manual*.

Client proxy settings

If a proxy server is between the AXIS Camera Station Pro client and the AXIS Camera Station Pro server, you must configure the proxy settings in Windows on the client computer. Contact Axis support for more information.

AXIS Camera Station Pro client

Tabs

Live view	View live video from connected cameras. See *Live view*.
Recordings	Search, play, and export recordings. See *Recordings*.
Smart search 1	Locate events in recorded video using motion search. See *Smart search 1*.
Data search	Search for data from an external source or system and track what happened at the time of each event. See *Data search, on page 39*.
Configuration	Manage connected devices and configure client and server settings. See *Configuration*.
Hotkeys	View and configure hotkeys. See *Hotkeys*.
Logs	Alarm, event, and audit logs. See *Logs*.
Access management	Configure and manage the system's cardholders, groups, doors, zones, and access rules. See *Access management, on page 163*.
Smart search 2	Use advanced filters to find vehicles and persons based on characteristics. See *Smart search 2, on page 34*.
System health monitoring	Monitor the health data from a single or multiple AXIS Camera Station Pro systems. See *System Health Monitoring BETA, on page 174*.
Live view alerts	Automatically navigate to the Live view alerts tab of the camera or view when the Live view action is triggered. See *Create live view actions*.
Recording alerts	In the Alarms or Logs tab, select one alarm and click **Go to recordings** to open the Recording alerts tab. See *Alarms* and *Logs*.

Main menu

	Open the main menu.
Servers	Connect to a new AXIS Camera Station Pro server and view the server lists and the connection status for all servers. See *Configure server*.
Actions	Start or stop a recording manually and change the status of I/O ports. See *Record manually* and *Monitor I/O ports*.
Help	Access help and support options. Go to **Help** > **About** to see which AXIS Camera Station Pro client version you're using.

Log out	Log out and disconnect from the server.
Exit	Exit and close the AXIS Camera Station Pro client.

Title bar

? or F1	Open help.
	Enter full screen mode.
 or ESC	Exit full screen mode.

Status bar

- The warning icon indicates a time mismatch between the client and server. Make sure their times are synchronized to avoid timeline issues.
- The server connection status shows the number of connected servers. See *Connection status*.
- The license status shows the number of unlicensed devices. See *Manage licenses*.
- The Secure Remote Access v2 usage shows how much data you've used this month.
- **AXIS Camera Station Pro update available** indicates that a new version is available. Only visible when you're logged in as administrator. See *Update AXIS Camera Station Pro, on page 115*.

Alarms and Tasks

- The Alarms and Tasks tabs show triggered events and system alarms. See *Alarms* and *Tasks*.

Live view

The live view shows live video from connected cameras. When you connect to multiple AXIS Camera Station Pro servers, it displays all views and cameras grouped by server name.

Views provide access to all the cameras and devices added to AXIS Camera Station Pro. A view can consist of one or several cameras, a sequence of items, a map, or a web page. The live view updates the views automatically when you add or remove devices from the system.

With the AXIS Audio Manager Pro integration, you can also set up and add audio zones with paging interfaces in the live view. For more information, see *Use paging interfaces in split views, on page 19*

All users can access views. For information about user access rights, see *User permissions, on page 121*.

To configure the live view, see *Client settings*.

Multiple monitors

To open a view on another screen:

1. Open a **Live view** tab.
2. Select one or more cameras, views, or sequences.
3. Drag and drop them onto the other screen.

To open a view on a monitor connected to an Axis video decoder:

1. Open a **Live view** tab.
2. Select one or more cameras, views, or sequences.
3. Right-click your selection and select **Show on AXIS T8705** or **Show on AXIS D1110**, depending on which video decoder you're using.

Note

- AXIS T8705 supports Axis cameras only.
- AXIS D1110 supports up to 9 streams in one split view.

Manage views in live view

+	Add a new split view, sequence, camera view, map, web page, or folder.
✎	Edit a view or a camera name. To edit camera settings, see *Edit camera settings*
🗑	Remove a view. You need permissions to edit the view and all secondary views to remove it. To remove cameras from AXIS Camera Station Pro, see *Cameras, on page 48*.
🔒	As an administrator, you can lock the view to prevent operators from moving or editing it.

Image management in live view

Navigate	To go to the camera view, right-click an image in a split view and select **Navigate**.
Take snapshot	To take a snapshot, right-click an image and select **Take snapshot**. The system saves the snapshot to the folder specified in **Configuration > Client > Settings**.

	Note AXIS Camera Station Pro typically uses the video stream when you take snapshots, so you get a snapshot with the same resolution as the video stream. However, for panoramic and fisheye cameras, which require stitching or dewarping, the snapshot is taken on the client side directly from the screen. This can result in lower resolution images, especially in views with multiple cameras where each image appears smaller on the screen.
Add snapshot to Export	To add a snapshot to the export list, right-click an image and select **Add snapshot to Export**.
Show on	To open a view on another screen, right-click the image and select **Show on**.
Use Mechanical PTZ	Available for PTZ cameras and for cameras that have digital PTZ configured in the camera's web interface. To use mechanical PTZ, right-click the image and select **Use Mechanical PTZ**. Use the mouse to zoom, pan and tilt.
Zoom	Use the mouse wheel to zoom in and out. Alternatively, press Ctrl + [+] to zoom in and Ctrl + [-] to zoom out.
Area zoom	To magnify an area, draw a rectangle in the area you want to magnify. To zoom out, use the mouse wheel. To magnify an area near the center of the image, use the right mouse button and drag to draw a rectangle.
Pan and tilt	Click the image where you want to point the camera. To pan and tilt continuously, move the cursor to the center of the image to show the navigation arrow. Click and hold to pan in the direction of the arrow. To pan and tilt at a higher pace, click and hold to make the navigation arrow longer.
Set focus	To adjust the focus for an AXIS device, right-click the image and select **Set focus**. Use the **Near** and **Far** bars to adjust the focus manually, or click **AF** to focus automatically. To adjust the focus for an ONVIF device, right-click the image and select **Set focus**. Select a **Focus mode**. The dialog updates depending on which mode you choose: • **Absolute**: Set the focus to a specific position by entering a value and clicking **Apply**. • **Relative**: Adjust the focus incrementally. Use **Near** for objects close to the camera and **Far** for objects further away. • **Continuous**: Move the focus using **Nearer** or **Further** and click **Stop** when done. • To focus automatically, click **AF**.
Focus recall zone	To add or remove a focus recall zone, right-click the image and select **Focus recall zone**.

Autotracking on/off	To turn on or off autotracking for an Axis PTZ camera with AXIS PTZ Autotracking configured, right-click the image and select **Autotracking on/off**.
Presets	To go to a preset position, right-click the image, select **Presets**, and select a preset. To create presets, see *PTZ presets*.
Add preset	To add a preset, drag the image view to the desired position, right-click, and select **Presets > Add preset**.
Absolute PTZ Move	Available for ONVIF devices that support absolute PTZ positioning. Use this to move the camera to precise, repeatable coordinates. To use Absolute PTZ, right-click the camera in live view and select **Absolute PTZ Move**. Select a coordinate system: **Generic** for standard coordinates or **Spherical** for degree-based coordinates. Enter position values for pan, tilt, and zoom, set the movement speed, and click **OK** or **Send**.
Stream profile	To set the stream profile, right-click an image and select **Stream profile**. See *Stream profiles*.

Add digital presets

PTZ control

Note

As an administrator, you can turn off mechanical PTZ for users. See *User permissions*.

Recording and instant replay in live view

	To go to the Recordings tab, select a camera or a split view and click  .
	Indicates an ongoing recording in the live view.
	Indicates that motion is detected.

	To play an ongoing recording, hover over the image and click **Instant replay**. The Recordings tab opens and plays the last 5 seconds of the recording.
REC	To record manually from the live view, hover over the image and click **REC**. The button turns yellow to indicate that the recording is ongoing. To stop recording, click **REC** again.

To configure manual recording settings such as resolution, compression, and frame rate, see *Recording method*. For more information about recording and playback, see *Playback recordings*.

Note

As an administrator, you can turn off the manual recording feature for users. See *User permissions*.

Audio in live view

Audio is available if the camera has audio capabilities and you have turned on audio in the profile used for the live view.

Go to **Configuration > Devices > Stream profiles** and configure audio for the camera. See *Stream profiles, on page 49*.

Volume	To change the volume in a view, hover the image, then hover the speaker button and then use the slider to change the volume. To mute or unmute audio, click .
Listen to this view only	To mute other views and listen to this view only, hover the image and click .
Speak through the speaker	To speak through the configured speaker in full-duplex mode, hover the image and click .
Push-to-talk	To speak through the configured speaker in simplex and half-duplex modes, hover the image and click and hold . To show the **Push-to-talk** button for all duplex modes, turn on **Use push-to-talk for all duplex modes** under **Configuration > Client > Streaming > Audio**. See *Streaming, on page 108*.

Note

As an administrator you can turn off audio for users. See *User permissions*.

Onscreen control in live view

Note

Onscreen control requires firmware 7.40 or later.

	To access the available camera features in the live view, click .

Split view

A split view shows multiple views in the same window. You can use camera views, sequences, web pages, maps, and other split views in a split view.

Note

When connecting to multiple AXIS Camera Station Pro servers, you can add any view, camera, device, or audio zone from other servers to your split view.

To add a split view:

1. In the **Live view** tab, click +.
2. Select **New Split View**.
3. Enter a name for the split view.
4. Select a layout from the **Template** drop-down menu.
5. Drag and drop cameras or views from the side panel to the grid, or double-click to add them to the first available slot.
6. Click **Save view**.

To edit a camera or view in the grid, select it. Under **Select item to configure** you can:

- Click **Remove** to remove it from the grid.
- Select a **PTZ preset** from the drop-down menu.

To add a hotspot:

- Select a frame and click **Set hotspot** under the **Hotspot** section.

To display triggered video streams automatically in the hotspot:

- Select **Dynamic hotspot content** and configure the settings. See *Dynamic hotspot, on page 16* for more information.

To set the stream profile for a camera:

- Right-click it in the grid view and select **Stream profile**. See *Stream profiles, on page 49*.

Dynamic hotspot

Use dynamic hotspots to monitor multiple events at once. When action rules are triggered, video streams appear automatically in the hotspot. For example, if motion is detected at three different entrances, all three camera views appear at the same time.

The hotspot adjusts its grid based on how many views are active. Each view shows a countdown timer and disappears when the countdown ends.

Note

For cameras triggered by stateful live view actions, the countdown starts when the action is no longer active. For other cameras and views, the countdown starts immediately.

Create a dynamic hotspot

To add a new view with a dynamic hotspot:

1. In the **Live view** tab, click +.
2. Click **Add hotspot**.
3. Select **Dynamic hotspot content**.
4. Configure the settings:
   - **Number of split view cells**: The number of cells in the grid, even when no views are active. Range: 1 to 144.
   - **Countdown in seconds**: How long each triggered view stays visible. Set to 0 to keep views visible until manually removed. Range: 0 to 999.

- **Seconds remaining when countdown appears in view**: Controls when the countdown timer appears on screen. Set to 0 to always show it. Note that displaying the timer uses system resources. Range: 0 to 999.
- **Mute audio on incoming views**: New streams start muted. You can unmute them individually.
- **Allow adding views with click on view**: Manually add views to the hotspot by clicking them, alongside triggered views.
- **Allow adding views with hotkey**: Use keyboard shortcuts to add defined views to the hotspot, alongside triggered views.

5. Click **Save view**.

To add a dynamic hotspot to an existing view:

1. In the **Live view** tab, click **Edit view**.
2. Click **Add hotspot**.
3. Select **Dynamic hotspot**.
4. Configure the settings as described in step 4 above.
5. Click **Save view**.

Note

You can convert an existing hotspot to a dynamic hotspot by editing the hotspot in the **Live view** tab.

Control and manage views

Each cell in a dynamic hotspot includes:

- **Countdown indicator**: Shows the remaining time before the view disappears.
- **Pause button**: Pause the countdown to keep a view visible longer.
- **Close button**: Immediately remove a view from the hotspot.
- **Flash indicator**: The countdown border flashes when a view is re-triggered.

These controls are hidden when you expand a cell to single view or switch to playback mode. Double-click any cell to expand it to full view. While expanded, the countdown pauses automatically. The dynamic hotspot continues updating in the background, and when you return to the grid view, you'll see the active views.

Note

When you switch to playback mode, the camera streams become fixed and won't update. Switch back to live view to resume normal operation.

Door dashboard in split view

If you have configured a door, you can assist cardholders and monitor the door and lock status and recent transactions in a split view.

1. Add a door. See *Add a door, on page 133*.
2. Add the door dashboard to a split view, see *Split view, on page 16*.

Dashboard	To view door details and lock status, open the **Dashboard** tab. The dashboard displays the following information: • Access control events with cardholder details and photos, for example, when a cardholder swipes a card. • Alarms with alarm trigger information, for example, when a door is open too long. • The latest transaction.
	To bookmark an event and make it available on the **Transactions** tab, click .
Access	To manually grant access, click **Access**. This unlocks the door as if someone presented their credentials. The door automatically locks again after a set time.
Lock	To manually lock the door, click **Lock**.
Unlock	To manually unlock the door, click **Unlock**. The door stays unlocked until you manually lock it again.
Lockdown	To prevent access to the door, click **Lockdown**.
Transactions	To view recent transactions and saved transactions, open the **Transactions** tab.

Monitor and assist in door dashboard

AXIS Data Insights Dashboard in a split view

The AXIS Data Insights Dashboard displays analytics data from your devices in graphs and charts. To add a dashboard to a split view:

1. Configure a dashboard. See *AXIS Data Insights Dashboard, on page 158*.
2. On the **Live view** tab, click .
3. Select **New Split View**.
4. Expand the **Dashboards** folder.
5. Drag and drop a dashboard to the grid.
6. Click **Save view**.

Dashboards	
Audio analytics	Displays data from AXIS Audio Analytics events.
Crossline counting	Displays data from AXIS Object Analytics crossline counting scenario.

Dashboards	
Generic	Displays data from all supported data sources.
Image health	Displays data from AXIS Image Health Analytics events.
Occupancy in area	Displays occupancy data from AXIS Object Analytics occupancy in area scenario.
In and Out counting	Displays data from AXIS Object Analytics crossline counting scenario, AXIS People Counter, and AXIS P8815-2 3D Counter.
Air Quality Monitor	Displays live indoor air quality data from AXIS Air Quality Sensors.
Air Quality Monitor Detailed	Displays aggregated data from AXIS Air Quality Sensors.

Use paging interfaces in split views

You can use paging interfaces to make live announcements, make calls, or play audio files from audio devices. This requires the AXIS Audio Manager Pro integration. For more information, see *Configure AXIS Audio Manager Pro, on page 154*.

To use paging interfaces:

1. Edit or add a new split view.
2. Drag and drop one or multiple audio zones to the grid to turn it into a paging interface.

Note

Audio zones in AXIS Camera Station Pro are identical to the zones you have set up on your AXIS Audio Manager Pro server.

3. Select **Speak**, **Call**, or **Play a file**:
   - Select **Speak** for one-way communication such as live announcements.
   - Select **Call** for two-way communication, for example when you want to talk to someone through an intercom.
   - Select **Play a file** to play a file from the AXIS Audio Manager Pro server through the speaker.

Sequence

A sequence switches between views automatically.

Note

When connecting to multiple AXIS Camera Station Pro servers, you can add any view, camera or device from other servers to your sequence.

To add a sequence:

1. In the **Live view** tab, click +.
2. Select **New sequence**.
3. Enter a name for the sequence.
4. Drag and drop one or multiple views or cameras to the sequence view.
5. Arrange the views in the order you want them to appear.
6. Click a view to edit its settings.
7. Click **Save view**.

PTZ preset	For cameras with PTZ capabilities, select which PTZ preset the camera moves to when this view is active.
Dwell time	The number of seconds each view is shown before switching to the next. You can set this individually for each view.

Note

- You can't add a sequence view into another sequence view.
- You can't add component views from a remote server directly. As a workaround, add the component view to a single split view first, then add that split view from the remote server.
- Timeline playback might behave unexpectedly. Playback shows all cameras in the sequence, but only one is active at a time.

Use the sequence bar

When viewing a sequence, a bar at the bottom of the view lets you control playback manually:

- Use **[>]** and **[<]** to navigate to the next or previous view.
- Use **Hold** or **Continue** to pause and resume the sequence.
- A countdown shows how many seconds are left until the next automatic switch.
- Right-click the sequence to hide the bar.
- When the sequence is open in the **Recording** tab, it's set to **Hold** automatically and can only be navigated manually with the next and previous buttons.

Camera view

A camera view displays live video from one camera. You can use camera views in split views, sequences, and maps.

Note

When connecting to multiple AXIS Camera Station Pro servers, the list shows all cameras from all connected servers.

To add a camera view:

1. In the Live view or Recordings tab, click +.
2. Select **New Camera View**.
3. Select the camera from the drop-down menu, and click **OK**.

Map

A map is an imported image where you can place camera views, split views, audio zones, sequences, web pages, other maps, and doors. The map gives a visual overview and a way to locate and access individual devices. You can create several maps and arrange them on an overview map for large installations.

Action buttons are also available in the map view. See *Create action button triggers*.

Note

When connecting to multiple AXIS Camera Station Pro servers, you can add any view, camera or device from other servers to your map view.

To add a map:

1. In the **Live view** tab, click +.
2. Select **New map**.

3. Enter a name for the map.
4. Click **Choose image** and find your map file. The file must be no larger than 20 MB. Supported formats: BMP, JPG, PNG, and GIF.
5. Drag the views, cameras, other devices, and doors onto the map.
6. Click an icon on the map to edit its settings.
7. Click **Add label**, enter a label name, and set the size, rotation, style, and color of the label.
8. Click **Save view**.

Note

- You can edit some settings for multiple icons and labels at the same time.
- All devices that your user account can't access are removed from the map when you edit it.
- You can't add component views from a remote server directly. As a workaround, add the component view to a single split view first, then add that split view from the remote server to the map.

Icon settings

Click an icon on the map to open its settings.

	The physical state of the door when the door is configured with a door monitor.
	The physical state of the lock when the door is configured without a door monitor.
	A red warning triangle indicates a tampering alert on a door, reader, or door controller.
Icon	Select the icon you want to use. This option is only available for cameras and other devices.
Size	Adjust the slider to change the size of the icon.
Color	Click  to change the color of the icon.
Name	Turn on this option to display the icon name. Select **Bottom** or **Top** to change the position of the icon name.
Coverage area	Available for supported devices. Turn on this option to show the coverage area of the device on the map. You can edit the **Range**, **Width**, **Direction**, and color of the coverage area. Turn on **Flash** to make the coverage area flash when a recording is triggered by motion detection or other action rules. To turn off flashing coverage areas globally for all devices, see *Client settings, on page 105*.
Direction arrow	Shows arrows pointing in the direction of each camera's field of view. You can show arrows with or without coverage areas.
Show recording indicators	Controls which recording indicators are visible on the icon. Turn on **Small indicators** to show a compact version of the indicators. Use the individual toggles to show or hide indicators for **Recording**, **Motion detected**, **Object detected**, and **Action rule active**. This setting is stored on the server, so all clients share the same configuration.

Label	A label has a text, size, rotation, and color. You also have the option to underline and italicize the content of the label.
Remove	Click to remove the icon from the map.

Navigate the map

Zoom and move
- You can zoom and move the map using a mouse, keyboard, or joystick. Touch isn't currently supported.

Mouse
- Scroll the mouse wheel to zoom in and out.
- When zoomed in, drag to move around the map.

Keyboard
- Press Ctrl + [+] to zoom in and Ctrl + [-] to zoom out.
- Use Ctrl + arrow keys to pan and tilt.

Joystick
- Twist the joystick head to zoom in and out.
- Tilt the joystick to pan and tilt.

Take a snapshot
- Right-click the map to open the context menu. You can save a snapshot of the map to your disk, or add it to the **Export** tab. The snapshot captures the map exactly as it appears at that moment, including all current camera statuses and indicator states.

Web page

A web page view displays a page from the Internet. You can add a web page to a split view or a sequence, for example.

To add a web page:

1. In the **Live view** tab, click .
2. Select **New web page**.
3. Enter a name for the web page.
4. Enter the webpage URL.
5. Click **OK**.

Folders

Use folders to categorize items in a tree view navigation. Folders can contain split views, sequences, camera views, maps, webpages, and other folders.

To add a folder:

1. In the Live view or Recordings tab, click .

2. Select **New Folder**.
3. Enter a name for the folder, and click **OK**.

Recordings

From the **Recordings** tab, you search, play back, and export recordings. The tab consists of a main view and two panels where you can find views, images, playback tools, and cameras from connected servers grouped by server name. See *Live view*.

From the main view, you can manage the image in the same way as in the live view. For more information, go to *Image management in live view, on page 12*.

To change the recording method and settings such as resolution, compression and frame rate, see *Recording method*.

Note

You can't manually delete recordings from AXIS Camera Station Pro. To delete old recordings, change the retention time under **Configuration > Storage > Selection**.

Playback recordings

Recordings from multiple cameras can play at the same time when you put the playback marker over multiple recordings in the timeline.

You can display live and recorded video at the same time when you use multiple monitors.

Playback timeline

Hover over a recording in the timeline to show the recording type and time. To get a better view and find recordings, you can zoom in, zoom out, and drag the timeline. The playback pauses temporarily when you drag the timeline and resumes when you release. Scrub the timeline to get an overview of the content and find specific moments.

- A red line indicates a motion detection recording.
- A blue line indicates a recording triggered by an action rule.

Find recordings

	Click to select a date and time in the timeline.
	Filter which recording types appear in the timeline.
	Use to find saved bookmarks. See *Bookmarks*.
	Click to open a list of recordings and bookmarks created with the Axis body worn camera. Here you can search for date and time, recording activation method, and any categories and notes that the camera user added in AXIS Body Worn Assistant.
 Smart search 1	Search for recordings using Smart search 1. See *Smart search 1*.

Playback recordings

	Play the recording.
	Pause the recording.
	Jump to the start of the ongoing or previous recording or event. Right-click to go to recordings, events, or both.

	Jump to the start of the next recording or event. Right-click to go to recordings, events, or both.
	Go to the previous frame in a recording. Pause the recording to use this feature. Right-click to set how many frames to skip (up to 20 frames).
	Go to the next frame in a recording. Pause the recording to use this feature. Right-click to set how many frames to skip (up to 20 frames).
	Change the playback speed using the multipliers in the drop-down menu.
	Mute audio. Only recordings with audio have this feature.
Audio slider	Slide to change the audio volume. Only recordings with audio have this feature.
Show all body worn metadata	Show the metadata for a body worn system and display notes and categories from AXIS Body Worn Assistant.
Pan, tilt and zoom	Click the image and scroll to zoom in and out. To zoom in on a specific area, place the cursor there before scrolling.

Bookmarks

Note

- You can't delete a locked recording unless you manually unlock it.
- Locked recordings are deleted when the associated camera is removed from the system.

	Click to show all the bookmarks. To filter the bookmarks, click the icon.
	Add a new bookmark.
	Means that it's a locked recording. The recording includes at least 2.5 minutes of video before and after the bookmark.
	Edit the bookmark name and description, or lock and unlock the recording.
	Remove a bookmark. To remove multiple bookmarks, select them while holding Ctrl or Shift, and click **Remove**.
Prevent recording deletion	Select to lock the recording. Clear to unlock it.

Add bookmarks

1. Go to the recording.
2. In the timeline, zoom in and out and move the timeline to put the marker at your desired position.
3. Click  .
4. Enter the bookmark name and description. Use keywords to make the bookmark easy to find.

5. Select **Prevent recording deletion** to lock the recording.

Note

To unlock the recording, clear **Prevent recording deletion** or delete the bookmark.

6. Click **OK** to save the bookmark.

Event categories

Assign categories to recordings to make it easier to find specific types of events. Before you start, make sure you have the appropriate user permissions. See *User or group privileges, on page 122*.

Assign event categories

1. In the **Recordings** tab, locate the recording you want to assign a category to.
2. Right-click the recording in the timeline and select **Categorize event**.
3. Add one or multiple categories.
4. Click **OK**.

When you categorize an event, the selected categories appear on the recording preview thumbnail. If you assigned a color to the category, the timeline displays that color.

Remove event categories

1. In the **Recordings** tab, locate the recording you want to remove categories from.
2. Right-click the recording in the timeline and select **Categorize event**.
3. In the list of assigned categories, select the category you want to remove.
4. Click **Remove**.
5. Repeat steps 3-4 for each category you want to remove.
6. Click **OK**.

Note

You can only use the **Remove** button if you have permission to remove categories or if you select an unassigned category from the list.

See *Configure event categories, on page 80* for more information.

Export recordings

From the **Export** tab, you can export recordings to a local storage device or network location. You can also find information and a preview of the recording here. You can export multiple files at the same time in .asf, .mp4, and .mkv formats.

To play your recordings, use Windows Media Player (.asf) or AXIS File Player (.asf, .mp4, .mkv). AXIS File Player is a free video and audio playback software that doesn't require installation.

Note

In AXIS File Player, you can change the playback speed of recordings in the .mp4 and .mkv formats, but not in .asf format.

Before you start, make sure you have permission to export. See *User permission for exporting, on page 29*.

To export a recording:

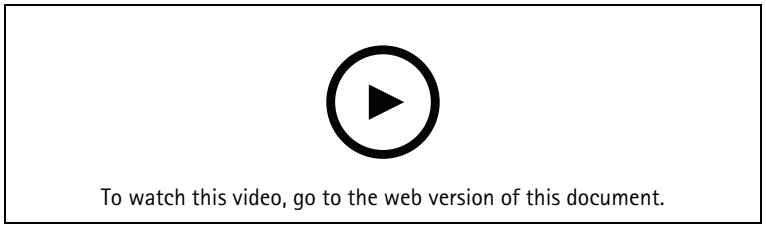
1. In the **Recordings** tab, select a camera or a view.
2. Add the recordings to the export list. Recordings in the timeline that aren't included in the export get a striped color.
   2.1. Click  to show the selection markers.
   2.2. Move the markers to include the recordings that you want to export.

2.3. Click to open the **Export** tab.

3. Click **Export...**
4. Select a folder to export the recordings to.
5. Click **OK**. The export task appears in the **Tasks** tab.

The export folder includes:

- The recordings in the selected format.
- A .txt file with notes if you select **Include notes**.
- AXIS File Player if you select **Include AXIS File Player**.
- An .asx playlist file if you select **Create playlist(.asx)**.



Export recordings

Recordings tab	
	To select multiple recordings, click and move the selection markers to the desired start and end points.
	To export recordings within the selection markers, click .
Add recordings	To add a single recording, right-click a recording and select **Export > Add recordings**.
Add event recordings	To add all recordings that occurred within the time of an event, right-click a recording and select **Export > Add event recordings**.
Remove recordings	To remove a single recording from the export list, right-click a recording and select **Export > Remove recordings**.
Remove recordings	To remove multiple recordings within the selection markers from the export list, right-click outside of a recording and select **Export > Remove recordings**.

Export tab	
Audio	To exclude audio from an exported recording, clear the checkbox in the **Audio** column. To always include audio in exported recordings, go to **Configuration** > **Server** > **Settings** > **Export** and select **Include audio when adding recordings to export**.
	To edit the recording, select a recording and click . See *Edit recordings before exporting, on page 29*.

Export tab	
	To edit the notes for the recording, select a recording and click  .
	To remove the recording from the export list, select a recording and click  .
Switch to export	If the **Incident report** tab is open, click **Switch to export** to go back to the **Export** tab.
Preferred stream profile	Select the stream profile in the **Preferred stream profile** field.
Preview	To preview a recording, click the recording in the exported list to play it. You can only preview multiple recordings if they're from the same camera.
Save	To save the export list to a file, click **Save**.
Load	To include a previously saved export list, click **Load**.
Name of export	Enter a custom name for the exported folder and files, or leave it blank to use the default naming convention in AXIS Camera Station Pro.
Append camera name and timestamp	Select this option to append the camera name and timestamp to the name of the exported folder and files.
Adjust start and end time	To adjust the recording start and end time, go to the timeline in the preview and adjust the start and end times. The timeline shows up to thirty minutes of recording before and after the selected recording.
Add snapshot	To add a snapshot, drag the timeline in the preview to a specific location, right-click the preview, and select **Add snapshot**.

Advanced settings	
Include notes	Select **Include notes** to include recording notes as a .txt file in the exported folder and as a bookmark in AXIS File Player.
Include AXIS File Player	To include AXIS File Player with the exported recordings, select **Include AXIS File Player**.
Create playlist(.asx)	To create a playlist in .asx format used by Windows Media Player, select **Create playlist(.asx)**. The recordings play in the order in which they were recorded.
Add digital signature	To prevent image tampering, select **Add digital signature**. This option is only available for recordings in the .asf format. See *Play and verify exported recordings, on page 30*.
Export to Zip file	To export to a Zip file, select **Export to Zip file** and enter a password if needed.

Advanced settings	
Export format	From the **Export format** drop-down menu, select a format to export the recordings to. Exported recordings don't include audio in G.711 or G.726 format if you select MP4.
Edited video encoding	For edited videos, you can set the video encoding format to `Automatic`, `H.264`, or `M-JPEG` under **Edited video encoding**. Select `Automatic` to use M-JPEG for M-JPEG format and H.264 for all other formats.

User permission for exporting

To export recordings or generate incident reports, you need the appropriate permissions. You can have permission for either or both. When you click in the **Recordings** tab, the connected export tab opens.

To configure the permissions, go to *User permissions, on page 121*.

Edit recordings before exporting

Blur a moving object

1. In the **Export** tab or **Incident report** tab, select a recording and click .
2. Move the timeline to the first occurrence of the moving object you want to cover.
3. Click **Bounding boxes > Add** to add a new bounding box.
4. Go to **Bounding box options > Size** to adjust the size.
5. Move the bounding box and put it over the object.
6. Go to **Bounding box options > Fill** and set it to **Pixelated** or **Black**.
7. When the recording plays, right-click the object and select **Add key frame**.
8. To add continuous key frames, move the bounding box to cover the object while the recording plays.
9. Move the timeline and make sure that the bounding box covers the object throughout the recording.
10. To set an end point, right-click the diamond shape in the last key frame and select **Set end**. This removes the key frames after the end point.

Note

You can add multiple bounding boxes in the video. If bounding boxes overlap, the overlapped area uses the fill in this order: Black, Pixelated, then Clear.

Remove all	To remove all bounding boxes, click **Bounding boxes > Remove all**.
Remove key frame	To remove a key frame, right-click the key frame and select **Remove key frame**.

Show a moving object with blurred background

1. Create a bounding box. See *Blur a moving object, on page 29*.
2. Go to **Bounding box options > Fill** and set it to **Clear**.
3. Go to **Video background** and set it to **Pixelated** or **Black**.

Pixelate all but this	Select multiple bounding boxes in the list, right-click and select **Pixelate all but this**. The selected bounding boxes turn **Clear** and the unselected ones turn **Pixelated**.

Generate bounding boxes

To generate bounding boxes from analytics data, make sure the camera's analytics are turned on. See *Stream profiles, on page 49*.

1. In the **Export** tab or **Incident report** tab, click .
2. Click **Generate bounding boxes**.
3. Make sure the bounding boxes cover the moving object. Adjust if necessary.
4. Select a fill for the bounding boxes or video background.

Improve video editing with AXIS Video Content Stream

To improve video editing, install the application AXIS Video Content Stream 1.0 on cameras with firmware 5.50 to 9.60. AXIS Camera Station Pro starts the installation automatically when you add a camera to the system. See *Install camera applications*.

Edit recordings before export

Play and verify exported recordings

To prevent image tampering, you can add a digital signature to exported recordings with or without a password. Use AXIS File Player to verify the digital signature and check for changes to the recording.

1. Go to the folder with the exported recordings. If the exported Zip file is password protected, enter your password to open the folder.
2. Open AXIS File Player. The exported recordings play automatically.
3. In AXIS File Player, click to view the recording notes.
4. To verify the digital signature of recordings exported with **Add digital signature**:
   4.1. Go to **Tools > Verify digital signature**.
   4.2. Select **Validate with password** and enter your password if it's password protected.
   4.3. To see the verification results, click **Verify**.

Export incident reports

From the **Incident report** tab, you can export incident reports to a local storage device or network location. You can include recordings, snapshots, and notes in your incident reports.

Before you start, make sure you have permission to export. See *User permission for exporting, on page 29*.

Incident reporting

Generate incident reports

1. In the **Recordings** tab, select a camera or a view.
2. Add the recordings to the export list. See *Export recordings, on page 26*.
3. Click **Switch to incident report** to go to the **Incident report** tab.
4. Click **Create report**.
5. Select a folder to save the incident report to.
6. Click **OK**. The incident report export task appears in the **Tasks** tab.

The export folder includes:

- AXIS File Player.
- The recordings in the selected format.
- A .txt file if you select **Include notes**.
- The incident report.
- The playlist if you export multiple recordings.

Audio	To exclude audio from an exported recording, clear the checkbox in the **Audio** column. To always include audio in exported recordings, go to **Configuration** > **Server** > **Settings** > **Export** and select **Include audio when adding recordings to export**.
	To edit the recording, select a recording and click . See *Edit recordings before exporting, on page 29*.
	To edit the notes for the recording, select a recording and click .
	To remove a recording from the export list, select a recording and click .
Switch to incident report	If the **Export** tab is open, click **Switch to incident report** to go to the **Incident report** tab.
Preferred stream profile	Select the stream profile in the **Preferred stream profile** drop-down list.
Preview	To preview a recording, click it in the export list to play it. You can only preview multiple recordings if they're from the same camera.
Save	To save the incident report to a file, click **Save**.
Load	To load a previously saved incident report, click **Load**.

Description	The **Description** field automatically fills with predefined data from the description template. You can also add additional information to include in the incident report.
Category	Select a category that the report belongs to.
Reference ID	A **Reference ID** is automatically generated. You can change it manually if needed. The ID is unique and identifies the incident report.
Include notes	Select **Include notes** to include recording notes as a . txt file in the exported folder and as a bookmark in AXIS File Player.
Edited video encoding	For edited videos, you can set the video encoding format to `Automatic`, `H.264`, or `M-JPEG` under **Edited video encoding**. Select `Automatic` to use M-JPEG for M-JPEG format and H.264 for all other formats.
Adjust start and end time	To adjust the recording start and end time, go to the timeline in the preview and adjust the start and end times. The timeline shows up to thirty minutes of recording before and after the selected recording.
Add snapshot	To add a snapshot, move the timeline in the preview to a specific location, right-click the preview, and select **Add snapshot**.

Record manually

Note

When you connect to multiple AXIS Camera Station Pro servers, you can manually start and stop a recording on any connected server. To do this, select the server from the **Selected server** drop-down list.

To manually start and stop a recording from the main menu:

1. Go to ☰ > **Actions** > **Record manually**.
2. Select one or more cameras.
3. Click **Start** to start the recording.
4. Click **Stop** to stop the recording.

To start and stop a manual recording from the **Live view** tab:

1. Go to **Live view**.
2. Hover over the camera's live view frame.
3. Click **REC** to start the recording. A red indicator appears in the view frame while recording.
4. Click **REC** to stop the recording.

Smart search 1

Use Smart search 1 to find parts of a recording where movement occurred in a defined area.

To increase search speed, select **Include analytics data** in the stream profile settings. See *Stream profiles*.

To use Smart search 1:

1. Click + and open a **Smart search 1** tab.
2. Select the camera you want to search.
3. Adjust the area of interest. You can add up to 20 points to the shape. To remove a point, right-click it.
4. Use the **Short-lived objects filter** and **Small objects filter** to filter out unwanted results.
5. Select the date and time range for the search. Use the Shift key to select a range of dates.
6. Click **Search**.

The search results appear on the **Results** tab. You can right-click one or more results to export the recordings.

Short-lived objects filter	The minimum time that an object must be in the area of interest to be included in the search results.
Small objects filter	The minimum size that an object must have to be included in the search results.

Smart search 1

Smart search 2

Use Smart search 2 to find moving persons and vehicles in recordings.

Note

Smart search 2 requires the following:

- Streaming analytics metadata over RTSP.
- AXIS Video Content Stream on cameras with AXIS OS earlier than 9.60. See *Install camera applications, on page 62*.
- Time synchronization between the AXIS Camera Station Pro server and cameras.

When you turn on Smart search 2 for an Axis camera, AXIS Camera Station Pro starts recording metadata from that camera and uses it to classify objects in the scene. This lets you use filters to find things of interest.

Note

- We recommend that you use continuous recording as motion detection can result in detections without video.
- Use H.264 format if you want to preview recordings in the search result.
- Make sure that the lighting conditions meet the camera's specifications for optimal color classification. Use additional lighting if needed.

Workflow

1. *Configure smart search 2, on page 155*
2. Configure time synchronization between the AXIS Camera Station Pro server and cameras. See *Time synchronization, on page 66*.
3. Create a filter or load an existing filter. See *Search with filters, on page 34*.
4. Manage search results. See *Smart search results, on page 38*.

Search with filters

1. Go to **Configuration > Smart search 2 > Settings** and select the cameras you want to use in Smart search 2.
2. Click + and open the **Smart search 2** tab.
3. Define your search criteria.
4. Click **Search**.

If the search takes longer than expected, try one or more of the following to speed it up:

- Turn on background server classification for important or frequently used cameras.
- Apply incoming filters to cameras to reduce irrelevant detections.
- Shorten the search time period.
- Reduce the numbers of cameras in the search.
- Define area, object direction, size, and duration to narrow down the amount of data.

Cameras	To limit the search by camera, click **Cameras** and select the cameras you want to include in the search.
Search interval	To limit the search by time, click **Search interval** and select a time range, a specific time interval over multiple days, or create a custom interval.

Person	To detect persons, click **Object characteristics** > **Pre-classified**, select **Person** and the clothing colors. You can select multiple colors.
Vehicle	To detect vehicles, click **Object characteristics** > **Pre-classified** and select the vehicle types and colors. You can select multiple vehicle types and vehicle colors.
Visual similarity	You can use a search result with a person in the image to search for visually similar persons. Open the context menu in a search result item and select **Use as visual similarity reference**. Then click **Search**. Note Similarity search creates abstract representations from cropped low-resolution images of people and compares them to other representations. When two representations are similar, you get a hit on your search. Similarity search doesn't use biometric data to identify a person but can, for example, recognize someone's general shape and color of clothing.
Free text search	Free text search lets you describe what you're looking for in the recordings using natural language (English only). See *Free text search, on page 36*.
Area	To filter by area, click **Area**, select a camera, and turn on **Filter by area on this camera**. Adjust the area of interest in the image and add or remove points if you need to.
Line crossing	To filter by line crossing, click **Line crossing**, select a camera, and turn on **Filter by line crossing on this camera**. Adjust the line in the image and add or remove points if you need to.
Size	To filter by size, click **Size**, select the camera, and turn on **Filter by size on this camera**. Adjust the minimum height and width as a percentage of the total image.
Duration	To filter by duration, click **Duration**, select the camera and turn on **Filter by duration on this camera**. Adjust the minimum duration in seconds.
Speed	To filter by speed, click **Speed**, select the camera, and turn on **Filter by speed on this camera**. Specify the speed range you want to include in the filter. Note The speed filter is available for radar devices and fusion cameras that can detect speed.
Unknown object detections	To include the detections that Smart search 2 classifies as unknown, select **Object characteristics** and then **Unknown object detections**.
	To save a filter, click , type a filter name, and click **Save**.

	Select **Share with other users** to share the filter with other users. To replace an existing filter, click , select an existing filter, and click **Replace**.
	To load a recent search, click > **Recent searches** and select a search. To load a saved filter, click > **Saved filters** and select a filter. To load a filter shared by another user, click > **Shared filters** and select a filter.
	To reset a filter, click and click **Reset**.

Free text search

Free text search lets you describe what you're looking for in the recordings using natural language.

Note

- Free text search requires a minimum of 16 GB RAM.
- Free text search requires an internet connection.
  - Free text search uses the internet connection to download the AI model from axis.com when you set it up for the first time and when Axis upgrades the model.
  - Free text search connects once a week to Axis cloud services to check if the AI models require any updates to comply with future regulations or requirements. If the connection fails, you won't be able to use free text search until your system reconnects.
  - Free text search performs all processing locally on your server and **doesn't** use the internet connection to send any video, images, or prompt texts.

To turn on free text search:

1. Open a **Configuration** tab.
2. Go to **Smart search 2** > **Settings**.
3. Under Free text search, select **Use free text search**. The system downloads the required files from axis.com.

To search:

1. Open a **Smart search 2** tab.
2. Click **Object characteristics**.
3. Click **Free text**.
4. Click **Show** to read information about the intended use, limitations, and responsible use.
5. Enter what to include and exclude in your search.
6. Click **Search**.

Prompting guidelines

We recommend using the following structure for your prompts:

```
{person, vehicle or other object} + {specific action or attributes of the person, vehicle, or object}
```

Describe the object with a few key descriptors. For example:

Prompt	Comment
A lady in a red sweater and black hat	About right
Lady in red	A little too vague
A lady approximately 156 cm tall, with a maroon cardigan with yellow accents and a late 80's inspired black sun hat with a tan trim	Far too much detail

Describe the situation as if you were talking to someone who isn't a surveillance expert. For example:

Prompt	Comment
A yellow pickup truck parked by a tree	About right
An unmanned vehicle, license plate: CHY67F, class: pickup, color: yellow, position: Adjacent to mighty poplar tree.	Too much like a police report

Good descriptors that free text search has a good chance of understanding:

Descriptor	Example
Object class	Person, Car, Bicycle, Animal
Color	Yellow
Weather	Sunny
Well known brands (car brands, logos)	UPS truck

Bad descriptors:

Descriptor	Example
Text	A shop sign which says 'No admittance to dancing bears'
Emotional cues	An angry looking man
Counting	14 people milling around a town square
Regional slang	A red hoover

Search query moderation

Searches containing insulting, harmful, or toxic content may be blocked to maintain a safe and respectful environment. Our system uses a natural language processing model and a custom list of prohibited search categories and words to evaluate each search query.

If you disagree with a blocked word or want to suggest a new one, you can provide anonymous feedback through the user interface of the smart search, which goes to our team for review.

Note

- Free text search supports only English.
- Free text search understands still images. It can be challenging to get good results for actions like falling, running, or stealing because these require more context.
- Free text search uses cropped images and might not include the surrounding environment. You might get less accurate results when using scene descriptors like city, urban, park, garden, lake, and beach.
- For more detailed information on the free text search feature, including its limitations and best practices, refer to our white paper *Free-text search in AXIS Camera Station Pro*.

Smart search results

	To group detections that are likely to belong to the same event, group them in time intervals. Select an interval from the drop-down menu.
Latest first	Smart search 2 shows search results in descending order with the latest detections first. Click **Oldest first** to show the oldest detections first.
Confidence level	To further filter the search results, click **Confidence level** and set the confidence level. A high confidence level filters out uncertain classifications.
Columns	To adjust the size of the thumbnails in the search result, click **Columns** and change the number of columns.
Detection view	To show a cropped view of the detected object as a thumbnail, select **Detection view**.

Limitations

- Smart search 2 supports only the primary (non-cropped) view area.
- Smart search 2 supports only non-cropped capture modes.
- Using Smart search 2 with mirrored and rotated camera streams for devices with ARTPEC-7 or higher and firmware version lower than 10.6 can cause some problems.
- High or very variable network latency can cause time synchronization issues and affect the classification of detections based on analytics metadata.
- Classification of object types and detection accuracy are negatively affected by low image quality due to high compression levels, weather conditions such as heavy rain or snow, and cameras with low resolution, heavy distortion, large field of view, or excessive vibrations.
- Smart search 2 may not detect small and distant objects.
- Color classification doesn't work in darkness or with IR illumination.
- Body worn cameras aren't supported.
- Radar can only detect persons and other vehicles. It's not possible to turn on background server classification for radar.
- Object classification behavior is unpredictable for thermal cameras.
- Smart search 2 doesn't detect moving objects when a PTZ preset position changes and for a short period after the position changes.
- Line crossing and area filters don't follow PTZ position changes.

Data search

Data search lets you find data from an external source. A source is a system or device that generates data about events. See *External data sources, on page 65* for more information.
For example:

- An event generated by an access control system.
- A license plate captured by AXIS License Plate Verifier.
- A speed captured by AXIS Speed Monitor.

To change how long AXIS Camera Station Pro keeps external data, go to **Configuration > Server > Settings > External data**.

To search data:

1. Click + and select **Data search**.
2. Select a search interval .
3. Select a data source type from the drop-down list.
4. Click **Search options** and apply any additional filters. Available filters vary depending on the data source type.
5. Enter any keywords in the search field. See *Optimize your search, on page 40*.
6. Click **Search**.

Data search bookmarks the data generated from the source if you've configured it with a view. Click the data in the list to go to the recording associated with the event.

Time interval	
Live	To search real-time data, select **Live** as the time interval. Data search can display a maximum of 3000 live data events. Live mode doesn't support search operators.
Last hour – Last 30 days	To search data from a preset time range, select one of the available options: last hour, 4 hours, 12 hours, 24 hours, 48 hours, 7 days, or 30 days.
Custom	To search data within a specific time range, select **Custom** and set a start and end date and time.

You can filter the search result on different types of sources:

Data source type	
All data	This option includes data from both component and external sources.
Access control	Use this option to include data only from this component. Access control lets you filter on doors and zones, cardholders, and event types.
Third-party	Use this option to include data from third-party sources other than the configured components.

Depending on the data source, you can get different items in your search result. For example:

Search results	
Server	The server that the event data is sent to. Only available when connecting to multiple servers.
Location	The name of the door and the name of the door controller with IP address.
Enter speed	The speed (kilometers per hour or miles per hour) when the object enters the Radar Motion Detection (RMD) zone.
Classification	The object classification. For example: Vehicle.

To export the search results to a PDF or text file, click **Download search result**. You can rearrange columns and adjust column widths to improve the table layout in the PDF output. The PDF includes up to 10 columns.

Optimize your search

You can use the following search operators for more precise results:

Use quotation marks `" "` for exact matches with keywords	• A search for `"door 1"` returns results containing "door 1". • A search for `door 1` returns results containing both "door" and "1".
Use `AND` to find matches containing all keywords.	• A search for `door AND 1` returns results containing both "door" and "1". • A search for `"door 1" AND "door forced open"` returns results containing both "door 1" and "door forced open".
Use `OR` or `|` to find matches containing any keyword.	• A search for `"door 1" OR "door 2"` returns results containing "door 1" or "door 2". • A search for `door 1 OR door 2` returns results containing "door" or "1" or "2".
Use parentheses `( )` together with `AND` or `OR`.	• A search for `(door 1 OR door 2) AND "Door forced open"` returns results containing one of the following: – "door 1" and "Door forced open" – "door 2" and "Door forced open" • A search for `door 1 AND (door (forced open OR open too long))` returns results containing one of the following: – "door 1" and "door forced open" – "door 1" and "door open too long"
Use >, >=, <, or <= to filter numbers in a specific column.	• A search for `[Max speed] > 28` returns results containing a number greater than 28 in the Max speed column. • A search for `[Average speed] < = 28` returns results containing a number less than or equal to 28 in the Average speed column.

Use `CONTAINS` to search for text in specific column.	• A search for `[Cardholder] CONTAINS Oscar` returns data where 'Oscar' is in the Cardholder column. • A search for `[Door] CONTAINS "door 1"` returns data where 'door 1' is in the Door column.
Use = for exact matches in a specific column.	A search for `[CardholderId] = ABC123` returns results that match "ABC123" in the "Cardholder" column only.

Configuration

On the Configuration tab, you can manage connected devices and configure settings for the client and servers.

Click + and select **Configuration** to open the **Configuration** tab.

Configure devices

In AXIS Camera Station Pro, a device refers to a network product with an IP address. A camera refers to a video source, such as a network camera or a video port (with a connected analog camera) on a multi-port video encoder. For example, a 4-port video encoder is one device with four cameras.

Note

- AXIS Camera Station Pro only supports devices with IPv4 addresses.
- Some video encoders have one IP address for each video port. In this case, AXIS Camera Station Pro treats each video port as one device with one camera.

In AXIS Camera Station Pro, a device can be:

- A network camera.
- A video encoder with one or more video ports.
- An auxiliary non-camera device, for example an I/O audio device, a network speaker, or a door controller.
- An intercom.

From here, you can:

- Add cameras and devices without video capabilities. See *Add devices*.
- Edit preferences of connected cameras. See *Cameras*.
- Edit preferences of non-camera devices. See *Other devices*.
- Edit stream profiles for resolution, format, and more. See *Stream profiles*.
- Adjust image settings in real time. See *Image configuration*.
- Add or remove PTZ presets. See *PTZ presets*.
- Manage and maintain connected devices. See *Device management*.
- Manage external data sources. See *External data sources, on page 65*.

Add devices

Note

- The system considers view areas as individual cameras. You must create view areas in the camera before using them. See *Use view areas*.
- When you add a device, the device synchronizes its time with the AXIS Camera Station Pro server.
- We recommend that you don't use special characters such as å, ä, and ö in a device's hostname.

1. Find your devices, video streams, or prerecorded videos.
   - *Find your devices, on page 44*
   - *Find your video streams, on page 44*
   - *Find prerecorded videos, on page 44*
2. *Add devices, video streams, or prerecorded videos, on page 45*

You must resolve any issues shown in the device status column before you can add a device.

(empty)	If there's no status, you can add the device to AXIS Camera Station Pro.
Communicating	AXIS Camera Station Pro server is trying to access the device.
Device certificate not trusted	AXIS Camera Station Pro can't verify that the HTTPS certificate on the device is signed by a trusted issuer. Click the link to issue a new HTTPS certificate or tell AXIS Camera Station Pro to trust the existing one.
Certificate authority has expired	The certificate authority that issued the device certificate is no longer valid. Click the link to issue a new HTTPS certificate or tell AXIS Camera Station Pro to trust the existing one.
Address mismatch in device certificate	The device address doesn't match the address in the certificate. Click the link to issue a new HTTPS certificate or tell AXIS Camera Station Pro to trust the existing one.
Communication error	AXIS Camera Station Pro can't contact the device.
Enter password	AXIS Camera Station Pro doesn't know which credentials to use to access the device. Click the link to enter a username and password for an administrator account on the device. By default, AXIS Camera Station Pro will use this username and password for all devices on which the user exists.
Set password	The root account and password aren't set up, or the device still uses the default password. Click the link to set the root user password. • Enter your password or click **Generate** to get a password. We recommend saving a copy of the generated password. • Select to use this password for all devices with the `Set password` status. • If the device enforces a password policy, a password policy indicator will show whether your password meets the requirements. See *User management, on page 59* for more information.
Model not supported	AXIS Camera Station Pro doesn't support the device model.
Obsolete firmware	The device's firmware is outdated. Update it before you add a device.
Faulty device	The device parameters retrieved by AXIS Camera Station Pro are corrupt.
Set tilt orientation	Click the link to select tilt orientation: Ceiling, Wall, or Desk, depending on how the camera is mounted. Some camera models require tilt orientation to be set.
Unsupported ONVIF device	AXIS Camera Station Pro doesn't support this third-party device.
Unsupported device	AXIS Camera Station Pro doesn't support this type of device.

Note

New HTTPS certificates are issued by AXIS Camera Station Pro and will auto-renew.

Find your devices

To find devices that aren't listed:

1. Go to **Configuration > Devices > Add devices**.
2. Click **Cancel** to stop the ongoing network search.
3. Click **Manual search**.
4. To find multiple devices in one or more IP ranges:
   4.1. Select **Search one or more IP ranges**.
   4.2. Type the IP range. For example: 192.168.10.*, 192.168.20-22.*, 192.168.30.0-50
   - Use a wildcard for all addresses in a group.
   - Use a dash for a range of addresses.
   - Use a comma to separate multiple ranges.

   4.1. To change the default port 80, enter the port range. For example: 80, 1080-1090
   - Use a dash for a range of ports.
   - Use a comma to separate multiple ranges.

   4.1. Click **Search**.
5. To find one or more specific devices:
   5.1. Select **Enter one or more hostnames or IP addresses**.
   5.2. Enter the hostnames or IP addresses separated by comma.
   5.3. Click **Search**.
6. Click **OK**.

Find your video streams

You can add video streams that support the following:

- Protocol: RTSP, HTTP, HTTPS
- Video encoding: M-JPEG for HTTP and HTTPS, H.264 for RTSP
- Audio encoding: AAC and G.711 for RTSP

Supported video stream URL schemes:

- `rtsp://<address>:<port>/<path>`
  For example: `rtsp://<address>:554/axis-media/media.amp`
- `http://<address>:80/<path>`
  For example: `http://<address>:80/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`
- `https://<address>:443/<path>`
  For example: `https://<address>:443/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

1. Go to **Configuration > Devices > Add devices**.
2. Click **Enter stream URLs** and enter one or more stream URLs separated by comma.
3. Click **Add**.

Find prerecorded videos

You can add prerecorded videos in .mkv format to AXIS Camera Station Pro.

Requirements:

- Video encoding: M-JPEG, H.264, H.265
- Audio encoding: AAC

1. Create a folder **PrerecordedVideos** under `C:\ProgramData\Axis Communications\AXIS Camera Station Server`.
2. Add a .mkv file to the folder.
3. To dewarp the prerecorded video, add a .dewarp file with the same name as the .mkv file to the folder. See *Image configuration, on page 53* for more information.
4. Go to **Configuration > Devices > Add devices** and turn on **Include prerecorded video**.
   You can find your prerecorded video and several prerecorded videos provided by the system.

Add devices, video streams, or prerecorded videos

1. In a multi-server system, select a server from the **Selected server** drop-down list.
2. Go to **Configuration > Devices > Add devices**.
3. Select the devices, video streams, or prerecorded videos. Click **Add**.
4. Click **Close** to skip configuration and continue later. To continue with the configuration:
   4.1. Choose **Quick configuration** to configure the basic settings. If you're importing an AXIS Site Designer project, choose **Site Designer configuration**. See *Import AXIS Site Designer projects* for more information.
   4.2. Select **Add image overlay for date, time, and text** to add overlays to Axis cameras that don't already have one.
   4.3. Click **Next**.
   4.4. Select your **Recording method** preference.
   4.5. Click **Next**.
   4.6. Choose your **Retention time** and **Recording storage**, and click **Finish** to apply the configuration.

Import AXIS Site Designer projects

AXIS Site Designer is an online design tool that helps you build a site with Axis products and accessories.

If you've created a site in AXIS Site Designer, you can import the project settings to AXIS Camera Station Pro. You can access the project using an access code or a downloaded setup file.

To import an AXIS Site Designer project to AXIS Camera Station Pro:

1. Generate an access code or download a project file:
   1.1. Sign in to *http://sitedesigner.axis.com* with your My Axis account.
   1.2. Select a project and go to the project page.
   1.3. Click **Share**.
   1.4. Click **Generate code** if your AXIS Camera Station Pro server has an internet connection, or click **Download settings file** if it doesn't.
2. In the AXIS Camera Station Pro client, go to **Configuration > Devices > Add devices**.
3. Select the devices, and click **Add**.
4. Select **Site Designer configuration** and click **Next**.
5. Select **Access code** and enter the access code. To use the downloaded setup file instead, select **Choose file**.
6. Click **Import**. AXIS Camera Station Pro tries to match the project with the selected devices by IP address or product name. If the match fails, select the correct devices from the drop-down menu.

7. Click **Next**.
8. Select your **Recording method** preference. These settings apply to cameras that don't match the project configuration.
9. Click **Next**.
10. Choose your **Retention time** and **Recording storage**, and click **Finish** to apply the configuration.

AXIS Camera Station Pro imports the following settings from the AXIS Site Designer project:

	Encoders, video decoders, door controllers, radar detectors, and speakers	Cameras, intercoms, and F/FA series
Schedules with name and time slots	✓	✓
Maps with name, icon color, icon location, and item name	✓	✓
Name	✓	✓
Description	✓	✓
Continuous recording: schedule and recording profile including frame rate, resolution, video encoding, and compression		✓
Motion triggered recording: schedule and recording profile including frame rate, resolution, video encoding, and compression		✓
Zipstream strength		✓
Audio settings for live view and recordings		✓
Retention time for recordings		✓

Note

- If you've defined one of the recording profiles or if there are two identical recording profiles in the AXIS Site Designer project, AXIS Camera Station Pro sets the profile to medium.
- If you've defined both recording profiles in the AXIS Site Designer project, AXIS Camera Station Pro sets the continuous recording profile to medium and the motion-triggered recording to high.
- AXIS Camera Station Pro optimizes the aspect ratio, so the resolution may differ from the AXIS Site Designer project.
- AXIS Camera Station Pro can set the audio settings if the device has a built-in microphone or speaker. To use an external audio device, turn it on after installing it.
- AXIS Camera Station Pro doesn't apply audio settings to intercoms even if the settings in AXIS Site Designer differ. On intercoms, audio is always on, but only in live view.

Add third-party devices

You can add third-party devices to AXIS Camera Station Pro in the same way you add Axis products. See *Add devices*.

Note

You can also add third-party devices as video streams in AXIS Camera Station Pro. See *Find your video streams, on page 44*.

AXIS Camera Station Pro supports the following functions for third-party devices according to IEC62676-2-31 and IEC62676-2-32:

- Camera discovery
- Video encoding: M-JPEG, H.264
- Audio encodings: G.711 (one-way, from the device to AXIS Camera Station Pro)
- One video profile per camera
- Live view
- Continuous and manual recordings
- Playback
- Recording exports
- Device event triggers
- PTZ

Use view areas

Some camera models support view areas. AXIS Camera Station Pro lists view areas as individual cameras on the **Add devices** page. See *Add devices*.

Note

- All view areas in a network camera count as one camera in the total number of cameras allowed by the AXIS Camera Station Pro license.
- The number of cameras you can add depends on your license.

To use view areas in AXIS Camera Station Pro, you must first turn them on in the camera:

1. Go to **Configuration > Devices > Cameras**.
2. Select the camera and click the link in the Address column.
3. In the camera's configuration page, enter the username and password to log in.
4. Click **Help** for instructions on where to find the setting. The location differs depending on the camera model and firmware.

Replace a device

You can replace a device and keep the existing configuration and recordings. The number of configured video streams on the new camera must be the same as on the old one.

To replace a device:

1. If the device you're replacing uses cloud storage, go to **Cloud storage** in My Systems and turn off cloud storage for the device.
2. Open a **Configuration** tab and go to **Devices** > **Management**.
3. Select the device you want to replace and click  .
4. In the **Replace device** dialog, select the device you want to replace the old one with.

5. Click **Finish**.
6. The **Replaced device** dialog appears to confirm the device was successfully replaced. Click **OK**.
7. If the replaced device was using cloud storage, restart the service on your AXIS Camera Station Pro server. Then turn on cloud storage for the device in My Systems. See *Turn on cloud storage for your individual cameras*.
8. Check the new device's configuration to make sure the settings are correct and it functions normally. If applicable:
   8.1. Reconfigure PTZ presets on the device.
   8.2. Add any removed I/O ports and update related action rules.
   8.3. Reconfigure motion settings if the old camera used built-in video motion detection instead of the video motion detection ACAP application.
   8.4. Insert an SD card or turn off **Failover recording** in the storage selection settings if the old camera used failover recording.

Cameras

Go to **Configuration > Devices > Cameras** to view the list of all cameras added to the system.

On this page, you can:

- Click a camera's address to open its web interface. This requires that there's no NAT or firewall between the AXIS Camera Station Pro client and the device.
- Edit the camera settings. See *Edit camera settings*.
- Remove cameras. This also deletes all recordings associated with the deleted cameras, including locked ones.

Edit camera settings

To edit camera settings:

1. Go to **Configuration > Devices > Cameras**.
2. Select a camera and click **Edit**.

Enabled	To prevent recording and viewing of the video stream, clear **Enabled**. You can still configure recording and live view.
Channel	When **Channel** is available for multiport video encoders, select the port number. When **Channel** is available for view areas, select the number corresponding to the view area.

Other devices

Go to **Configuration > Devices > Other devices** to view a list of devices without video capabilities. The list includes door controllers, audio devices, and I/O modules.

For information about supported products, go to *www.axis.com*. See *Use audio from other devices*.

On this page, you can:

- Click a device's address to open its web interface. This requires that there's no NAT or firewall between the AXIS Camera Station Pro client and the device.
- Edit the device settings, such as device name, address, and password.
- Remove devices.

Edit other device settings

To change the name of a non-camera device:

1. Go to **Configuration > Devices > Other devices**.
2. Select a device and click **Edit**.
3. Enter the new name for the device.

Stream profiles

A stream profile is a group of settings that affect the video stream, such as resolution, video format, frame rate, and compression. Go to **Configuration > Devices > Stream profiles** to open the **Stream profiles** page. The page shows a list of all cameras.

The following profiles are available in live view and recording settings:

High – Optimized for the highest quality and resolution.

Medium – Optimized to balance high quality with performance.

Low – Optimized for performance.

Note

The stream profile is set to **Automatic** in live view and recordings by default. The stream profile changes automatically to **High**, **Medium**, or **Low** depending on the available size for the video stream.

Stream profiles on the camera

AXIS Camera Station Pro automatically adds stream profiles to the camera to help you set up recording rules directly on it. The profiles appear in the camera's web interface under **Stream profiles** and are named after the camera and profile level, for example, "Camera 1_ACS_Pro_High".

The profiles on the camera are added or updated when:

- A camera is added to AXIS Camera Station Pro.
- Stream profiles are changed in AXIS Camera Station Pro.
- The nightly refresh runs.

When a camera is removed from AXIS Camera Station Pro, the stream profiles created by AXIS Camera Station Pro are deleted from the camera.

Note

Stream profiles using M-JPEG or MPEG-4 formats aren't added to the camera.

Edit stream profiles

1. Go to **Configuration > Devices > Stream profiles**, and select the cameras you want to configure.
2. Under **Video profiles**, configure resolution, video format, frame rate, and compression.
3. Under **Audio**, configure the microphone and speaker.
4. Under **Advanced**, configure analytics data, FFmpeg streaming, PTZ autotracking object indicators, and customized stream settings. These settings aren't available for all products.
5. Click **Apply**.

Video profiles

Encoder	• Available options depend on the video encoder configurations on the device. Only available for third-party devices. • You can only use a video encoder configuration for one video profile. • If the device has only one encoder configuration, only the **Medium** profile is available.
Resolution	Available options depend on camera model. A higher resolution gives an image with more details but requires more bandwidth and storage space.
Format	Available options depend on camera model. Most cameras support **H.264** and **M-JPEG**. H.264 requires less bandwidth and storage space than M-JPEG. Some cameras also support **H.265**, which offers slightly better compression but requires more processing power. Our latest generation cameras support AV1, which offers good compression and a number of new functions, such as togglable overlays. For more information about AV1, see the *AV1 product page*. To check if your camera supports AV1, see the *compatible cameras page*.
Frame rate	The actual frame rate depends on camera model, network conditions, and computer configuration.
Compression	Lower compression improves image quality, but requires more bandwidth and storage space.

Note

- Only cameras with firmware 5 and above appear in the audio drop-down lists.
- If more than 5 cameras use the same audio source, the source camera can become overloaded and perform less efficiently.

Zipstream

Strength	Zipstream strength determines the level of bitrate reduction in an H.264 or H.265 stream in real time. This option is only available for Axis devices that support Zipstream.	**Default**	Use the Zipstream setting configured through the device's web interface page.
		Off	None
		Low	No visible effect in most scenes.
		Medium	Visible effect in some scenes: less noise and slightly lower level of detail in regions of lower interest.
		High	Visible effect in many scenes: less noise and lower level of detail in regions of lower interest.
		Higher	Visible effect in even more scenes: less noise and lower level of detail in regions of lower interest.
		Extreme	Visible effect in most scenes: less noise and lower level of detail in regions of lower interest.
Optimize for storage	Zipstream optimizes the video stream for storage using the **Optimize for storage** profile. This profile uses more advanced compression tools to reduce storage use beyond the default Zipstream setting and can further reduce the bitrate even for scenes with a lot of motion. • The asf format doesn't support B-frames used by this feature. • This feature doesn't affect video recorded to AXIS S30 series recorders. • This feature requires AXIS OS 11.7.59 or later.		

Audio

Microphone:	To associate a microphone to the camera, select **Built-in microphone or line in** or other device's microphone. See *Use audio from other devices*.
Speaker:	To associate a speaker to the camera, select **Built-in speaker or line out** or other device's speaker. Use a microphone connected to the computer to make spoken announcements. See *Use audio from other devices*.
Use microphone for:	Turn on microphone audio for one or two streams. You can turn on audio for live view and recordings, live view only, or recordings only.

When connected to AXIS Audio Manager Pro, you can also select audio devices from the AXIS Audio Manager Pro server as the audio device associated with a camera. For more information, see *Configure AXIS Audio Manager Pro, on page 154*.

Advanced

Include analytics data	To allow data gathering for smart search during video streaming, select **Include analytics data**. Only available for Axis devices that support analytics data. Data gathering for *Smart search 1* can add latency in live video streaming.
Use FFmpeg	To improve compatibility with third-party devices, select **Use FFmpeg** to turn on FFmpeg streaming. Only available for third-party devices.
Show PTZ autotracking object indicators	To show the object indicators that are detected by a PTZ camera in live view, select **Show PTZ autotracking object indicators** and set the video stream buffer time to up to 2000 milliseconds. Only available for Axis PTZ cameras with AXIS PTZ Autotracking. For a complete workflow to set up AXIS PTZ Autotracking in AXIS Camera Station Pro, see *Set up AXIS PTZ Autotracking*.
Stream customization	To customize the stream settings for a specific profile, enter the settings separated by `&` for the profile. For example, enter `overlays=off&color=0` to hide the overlays on that camera. The custom settings override any existing settings. Don't include sensitive information in the custom settings.

To **customize profile settings** for resolution, frame rate, compression, video format, and audio, select the camera to configure. For cameras of the same model that have the same configuration capabilities, multiple cameras can be configured at the same time. See *Configuration settings*.

To **customize profile settings for recordings**, see *Recording method*.

You can **limit the resolution and frame rate for Live view to reduce bandwidth consumption**, for example, if the connection between the AXIS Camera Station Pro client and AXIS Camera Station Pro server is slow. See Bandwidth usage in *Streaming*.

Use audio from other devices

You can use audio from other non-camera or auxiliary devices with video from a network camera or video encoder for live viewing or recording.

1. Add the non-camera device to AXIS Camera Station Pro. See *Add devices*.
2. Configure the camera to use audio from the device. See *Stream profiles*.
3. Turn on audio for live view or recording. See *Stream profiles*.

You can find the following examples in *AXIS Camera Station Pro video tutorials*:

- Set up audio devices and make live announcements.
- Create an action button to manually play audio when motion is detected.
- Automatically play audio when motion is detected.
- Add an audio clip to speaker and AXIS Camera Station Pro.

Image configuration

You can configure the image settings for the cameras connected to AXIS Camera Station Pro.

Note

Changes to image configuration take effect immediately.

To configure the image settings:

1. Go to **Configuration > Devices > Image configuration**. AXIS Camera Station Pro displays a list of all cameras.
2. Select the camera to show the video feed below the list in real time. Use the **Type to search** field to find a specific camera in the list.
3. Configure the image settings:

Brightness – Adjust the image brightness. A higher value gives a brighter image.

Color level – Adjust the color saturation. Select a lower value to reduce color saturation. Color level 0 gives a black and white image. The maximum value gives maximum color saturation.

Sharpness – Adjust the amount of sharpening applied to the image. Increasing sharpness might increase image noise, especially in low light situations. High sharpness might also introduce image artifacts around areas with high contrast, for example sharp edges. Lower sharpness reduces image noise, but makes the image less sharp.

Contrast – Adjust the image contrast.

White balance – Select the white balance option in the drop-down list. White balance is used to make colors in the image look consistent regardless of the light source's color temperature. When selecting **Automatic** or **Auto**, the camera identifies the light source and compensates for its color automatically. If the result isn't satisfactory, select an option corresponding to the type of light source. Available options depend on camera model.

Rotate image – Set image rotation degrees.

Automatic image rotation – Turn on to adjust the image rotation automatically.

Mirror image – Turn on to mirror the image.

Backlight compensation – Turn on if a bright light source, such as a light bulb, makes other areas of the image appear too dark.

Dynamic contrast (Wide dynamic range) – Turn on to improve exposure when there's a considerable contrast between light and dark areas in the image. Use the slider to adjust the level. Turn off in low light conditions.

Custom dewarp settings – You can import a .dewarp file that contains the lens parameters, optical centers, and tilt orientation of the camera. Click **Reset** to reset the parameters to their original values.

To configure custom dewarp settings:

1. Create a .dewarp file including the following parameters:
   - Required: `RadialDistortionX`, `RadialDistortionY`, `RadialDistortionZ`, and `TiltOrientation`. The possible values for `TiltOrientation` is `wall`, `desk`, and `ceiling`.
   - Optional: `OpticalCenterX` and `OpticalCenterY`. If you want to set the optical centers, you must include both of the two parameters.
2. Click **Import** and navigate to the .dewarp file.

The following is an example of a .dewarp file:

```
RadialDistortionX=-43.970703 RadialDistortionY=29.148499 RadialDistortionZ=715.732193
TiltOrientation=Desk OpticalCenterX=1296 OpticalCenterY=972
```

PTZ presets

Pan, tilt, zoom (PTZ) is the ability to pan (move left and right), tilt (move up and down), and zoom in and out.

Go to **Configuration > Devices > PTZ presets**. AXIS Camera Station Pro displays a list of cameras that support PTZ. Click a camera to view all presets available for the camera. Click **Refresh** to update the preset list.

You can use PTZ with:

- PTZ cameras, that is, cameras with built-in mechanical PTZ
- Fixed cameras with digital PTZ turned on.
- ONVIF cameras that support PTZ presets.

Digital PTZ can be turned on from the camera's built-in configuration page. For more information, see the camera's user manual. To open the configuration page, go to the device management page, select the camera, and click the link in the **Address** column.

PTZ presets can be configured in AXIS Camera Station Pro and the camera's configuration page. We recommend configuring PTZ presets in AXIS Camera Station Pro.

- When a PTZ preset is configured in the camera's configuration page, you can only view the stream within the preset. PTZ movements in live view can be seen and are recorded.
- When a PTZ preset is configured in AXIS Camera Station Pro, you can view the complete stream of the camera. PTZ movements in live view aren't visible or recorded.

Note

PTZ can't be used while the camera's control queue is on. For information about the control queue and how to turn it on and off, see the camera's user manual.

To add a preset:

1. Go to **Configuration > Devices > PTZ presets** and select a camera in the list.
2. For cameras with mechanical PTZ, use the PTZ controls to move the camera view to the desired position. For cameras with digital PTZ, use the mouse wheel to zoom in and drag the camera view to the desired position.
3. Click **Add** and enter a name for the new preset.
4. Click **OK**.

- To remove a preset, select it and click **Remove**. This will remove the preset from both AXIS Camera Station Pro and the camera.

Device management

Device management provides tools for administration and maintenance of devices connected to AXIS Camera Station Pro.

Go to **Configuration > Devices > Management** to open the **Manage devices** page.

If you've set up automatic checks for new firmware versions in *Firmware upgrade settings, on page 110*, a link displays when new firmware versions are available for devices. Click the link to upgrade the firmware versions. See *Upgrade firmware*.

If you've set up automatic checks for new software versions in *Update AXIS Camera Station Pro, on page 115*, a link displays when a new AXIS Camera Station Pro version available. Click the link to install the new version.

AXIS Camera Station Pro displays a list of all added devices. Use the **Type to search** field to find devices in the list. To hide or show columns, right-click the header row and select which columns to show. Drag and drop the headers to display the columns in a different order.

The device list includes the following information:

- **Name:** The name of the device or a list of all associated camera names when the device is a video encoder with multiple connected cameras, or a network camera with multiple view areas.
- **MAC address:** The MAC address of the device.
- **Status:** The status of the device.
  - **OK:** The standard state for an established device connection.
  - **Maintenance:** The device is under maintenance and temporarily inaccessible.
  - **Not accessible:** No connection can be established with the device.
  - **Not accessible over set hostname:** No connection can be established with the device via its hostname.
  - **Server not accessible:** No connection can be established with the server that the device is connected to.
  - **Enter password:** The device can't be reached until valid credentials are entered. Click the link to provide valid user credentials. If the device supports encrypted connections, the password is sent encrypted by default.
  - **Set password:** The root account and password aren't set up, or the device still uses the default password. Click the link to set the root user password.
    - Enter your password or click **Generate** to automatically generate a password up to the length allowed by the device. We recommend saving a copy of the generated password.
    - Select to use this password for all devices with the `Set password` status.
    - Select **Enable HTTPS** to turn on HTTPS if the device supports it.
  - **Password type: unencrypted:** No connection is established with the device as the device has previously connected using an encrypted password. For security reasons, AXIS Camera Station Pro doesn't allow use of unencrypted passwords for devices that have previously used encrypted passwords. For devices supporting encryption, the connection type is configured on the device's configuration page.
  - **Certificate error:** There's an error with the certificate on the device.
  - **Certificate about to expire:** The certificate on the device is about to expire.
  - **Certificate has expired:** The certificate on the device has expired.
  - **HTTPS certificate not trusted:** The HTTPS certificate on the device isn't trusted by AXIS Camera Station Pro. Click the link to issue a new HTTPS certificate.
  - **HTTP failed:** No HTTP connection can be established with the device.
  - **HTTPS failed:** No HTTPS connection can be established with the device.
  - **HTTP and HTTPS failed (ping or UDP OK):** No HTTP and HTTPS connection can be established with the device. The device responds to ping and User Datagram Protocol (UDP) communication.
- **Address:** The address of the device. Click the link to go to the device's configuration page. It shows the IP address or hostname depending on which one is used when adding the device. See *Device configuration tab, on page 65*.

- **Hostname:** The hostname of the device if available. Click the link to go to the device's configuration page. The hostname displayed is the fully qualified domain name. See *Device configuration tab, on page 65*.
- **Manufacturer:** The manufacturer of the device.
- **Model:** The model of the device.
- **Firmware:** The version of firmware the device is currently using.
- **DHCP:** Indicates whether the device is connected to the server using DHCP.
- **HTTPS:** The HTTPS status of the device. See HTTPS status in *Security, on page 63*.
- **IEEE 802.1X:** The IEEE 802.1X status of the device. See IEEE 802.1X status in *Security, on page 63*.
- **Server:** The AXIS Camera Station Pro server the device is connected to.
- **Tags:** (Hidden by default) The tags added to the device.
- **UPnP Friendly Name:** (Hidden by default) The UPnP name. This is a descriptive name used to make it easier to identify the device.

You can perform the following actions on devices:

- Assign IP address to devices. See *Assign IP address*.
- Set password for devices. See *User management*.
- Upgrade firmware for devices. See *Upgrade firmware*.
- Restart devices.
- Restore devices: resets most settings to their factory default values, including the password. The following settings aren't reset: uploaded camera applications, boot protocol (DHCP or static), static IP address, default router, subnet mask, and system time.

Note

- To prevent unauthorized access, always set a new password after restoring a device.
- If the device you're resetting uses cloud storage, go to **Cloud storage** in My Systems and turn off cloud storage for the device before you reset it. Once the device is reset, restart the service on your AXIS Camera Station Pro server and turn on cloud storage for the device in My Systems. See *Turn on cloud storage for your individual cameras*.
- Install camera application on devices. See *Install camera applications*.
- Reload devices after changing settings from the device's configuration page.
- Configure devices. See *Configure devices*.
- User management. See *User management*.
- Manage certificates. See *Security, on page 63*.
- Collect device data. See *Collect device data*.
- Select to use IP address or hostname. See *Connection, on page 64*.
- Tag devices. See *Tags*.
- Enter device credentials. Right-click a device and select **Advanced > Enter device credentials** to enter the password for the device.
- Go to the device's configuration tab and configure your device. See *Device configuration tab, on page 65*.

Assign IP address

AXIS Camera Station Pro can assign IP address to multiple devices. You can obtain new IP addresses automatically from a DHCP server or assign them from an IP address range.

Assigning IP addresses

1. Go to **Configuration > Devices > Management** and select the devices to configure.
2. Click  , or right-click and select **Assign IP address**.
3. If some of the devices can't be configured, for example if the devices are inaccessible, the Invalid devices dialog will appear. Click **Continue** to skip the devices that can't be configured.
4. If you select one device to assign an IP address, click **Advanced** to open the **Assign IP address** page.
5. Select **Obtain IP addresses automatically(DHCP)** to obtain the IP addresses automatically from a DHCP server.
6. Select **Assign the following IP address range** and specify the IP range, subnet mask, and default router. To specify the IP range:
   - Use wildcards. For example: 192.168.0.* or 10.*.1.*
   - Write the first and last IP addresses separated by a dash. For example: 192.168.0.10-192.168.0.20 (this address range can be shortened to 192.168.0.10-20) or 10.10-30.1.101
   - Combine wildcards and range. For example: 10.10-30.1.*
   - Use a comma to separate multiple ranges. For example: 192.168.0.*,192.168.1.10-192.168.1.20

Note

To assign an IP address range, the devices must be connected to the same AXIS Camera Station Pro server.

7. Click **Next**.
8. Review the current IP addresses and the new IP addresses. To change the IP address for a device, select the device and click **Edit IP**.
   - The **Current IP address** section shows the current IP address, subnet mask, and default router.
   - Edit the options in the **New IP address** section, and click **OK**.
9. Click **Finish** when satisfied with the new IP addresses.

Configure devices

You can configure some settings on multiple devices at the same time by copying device settings from one device, or by applying a configuration file.

Note

To configure all settings on a single device, go to the device's configuration page. See *Device configuration tab, on page 65*.

- For information on configuring devices, see *Configuration methods*.
- For information on creating a configuration file, see *Create configuration file*.
- For information on which settings can be copied, see *Configuration settings*.

Configuration methods

There are different methods to configure devices. AXIS Device management configures all devices according to the settings in the method. See *Configure devices*.

Use configuration of the selected device

Note

This method is only available for a single device and reuses some or all of its existing settings.

1. Go to **Configuration > Devices > Management**.
2. Right-click one device and select **Configure Devices > Configure**.
3. Select the settings you want to apply. See *Configuration settings, on page 58*.
4. Click **Next** to verify the settings to be applied.
5. Click **Finish** to apply the settings to the device.

Copy configuration from another device

1. Go to **Configuration > Devices > Management**.
2. Right-click the devices and select **Configure Devices > Configure**. Devices of different models and firmware can be selected.
3. Click **Device** to show devices with reusable configurations.
4. Select a device to copy settings from and click **OK**.
5. Select the settings you want to apply. See *Configuration settings, on page 58*.
6. Click **Next** to verify the settings to be applied.
7. Click **Finish** to apply the settings to the devices.

Use configuration file

A configuration file contains settings from one device. It can be used to configure multiple devices at the same time and reconfigure a device, for example if the device is reset to its factory default settings. A configuration file created from a device can be applied to devices with different models or firmware even if some settings don't exist on all devices.

If some settings don't exist or can't be applied, the task status shows as **Error** in the **Tasks** tab at the bottom of the AXIS Camera Station Pro client. Right-click the task and select **Show** to display information about the settings that couldn't be applied.

Note

This method should only be used by experienced users.

1. Go to **Configuration > Devices > Management**.
2. Right-click the devices and select **Configure Devices > Configure**.
3. Click **Configuration File** to go to the configuration file. To learn how to create a configuration file, see *Create configuration file, on page 58*.
4. Browse to the .cfg file and click **Open**.
5. Click **Next** to verify the settings to be applied.
6. Click **Finish** to apply the settings to the devices.

Create configuration file

A configuration file contains settings from one device. You can then apply these settings to other devices. To learn how to use the configuration file, see *Configuration methods*.

The settings shown are the device settings accessible through AXIS Device Management. To find a particular setting, use the **Type to search** field.

To create a configuration file:

1. Go to **Configuration > Devices > Management**.
2. Select the device to create the configuration file from.
3. Right-click and select **Configure Devices > Create Configuration File**.
4. Select the settings to include and change their values as required. See *Configuration settings*.
5. Click **Next** to verify the settings.
6. Click **Finish** to create the configuration file.
7. Click **Save** to save the settings to a .cfg file.

Configuration settings

When you configure devices, you can configure the parameters, action rules, and additional settings of the devices.

Parameters

Parameters are internal settings that control device behavior. For general information about parameters, see the product's user manual available at *www.axis.com*

Note

- Parameters should only be modified by experienced users.
- Not all device parameters are accessible from AXIS Device Management.

You can insert variables in some text fields. The variables are replaced with text before being applied to a device. To insert a variable, right-click the text field and select:

- **Insert device serial number variable:** Replaced with the serial number of the device that the configuration file is applied to.
- **Insert device name variable:** Replaced with the name of the device used when applying the configuration file. The device name can be found in the **Name** column in the **Device management** page. To rename a device, go to the **Cameras** or **Other devices** page.
- **Insert server name variable:** Replaced with the name of the server used when applying the configuration file. The server name can be found in the **Server** column in the **Device management** page. To rename a server, go to AXIS Camera Station Pro Service Control.
- **Insert server time zone variable:** Replaced with the POSIX time zone of the server used when applying the configuration file. You can use this with the POSIX time zone parameter to set the correct time zone of all devices in a network with servers in different time zones.

Action rules

Action rules can be copied between devices. Action rules should only be modified by experienced users. For general information about action rules, see *Action rules*.

Additional settings

- **Stream profiles:** A stream profile is a preconfigured live view configuration profile for video encoding, image, and audio settings. Stream profiles can be copied between devices.
- **Motion detection windows:** Motion detection windows define specific areas in the camera's field of view. Typically, alarms are generated whenever movement occurs (or stops) within the specified areas. Motion detection windows can be copied between devices.

User management

Go to **Configuration > Devices > Management** to manage users of the devices.

When you set password or remove users for multiple devices, users that aren't present on all devices are indicated with  . Each user appears only once, even if they have different roles on different devices.

Note

The accounts are device specific and aren't related to the user accounts of AXIS Camera Station Pro.

Password policy

Some devices require passwords to meet specific criteria. When one or more selected devices enforce a password policy, the password strength indicator is replaced by a password policy indicator showing whether your password meets the active policy.

- If no policy is required, or the device is ONVIF, the password strength indicator is shown as usual.
- If you've selected multiple devices with different policies, the password must satisfy all of them.
- If the password doesn't meet the requirements, **Non-compliant** is shown. Hover over the info icon to see the specific requirements:

Length policy – Password must be at least 15 characters long.

Complexity policy – Password must be at least 12 characters long and include one uppercase letter, one lowercase letter, one numeric digit, and one special character.

Both policies – Both length and complexity requirements must be met.

Set password

Note

- Devices with firmware 5.20 and later support 64-character passwords. Devices with earlier firmware versions support 8-character passwords. We recommend setting passwords on devices with older firmware separately.
- When setting a password on multiple devices that support different password lengths, the password must fit within the shortest supported length.
- To prevent unauthorized access and increase security, we strongly recommend that all devices added to AXIS Camera Station Pro are password protected.

The following characters can be used in passwords:

- Letters A-Z, a-z
- Numbers 0-9
- Space, comma (,), period (.), colon (:), semicolon (;)
- !, ", #, $, %, &t, ', (, +, *, -,), /, <, >, =, ?, [, \, ^, -, `, {, |, ~, @,], }

To set a password for users on devices:

1. Go to **Configuration > Devices > Management > Manage devices**.
2. Select the devices and click . You can also right-click the devices and select **User Management > Set password**.
3. Select a user.
4. Enter your password or click **Generate** to generate a strong password.
5. Click **OK**.

Note

If you select **Use this password for all devices without a factory default password**, the password is applied to all devices with the **Set password** status. If the password length exceeds the maximum supported by a device, you'll be informed before the dialog opens and can choose to continue without those devices.

Add user

To add local or Active Directory users to AXIS Camera Station Pro:

1. Go to **Configuration > Devices > Management > Manage devices**.
2. Right-click the devices and select **User Management > Add user**.
3. Enter a username and password, and confirm the password. For a list of valid characters, see the **Set password** section above.
4. Select the user access rights from the **Role** drop-down list:
   - **Administrator:** Unrestricted access to the device.
   - **Operator:** Access to the video stream, events, and all settings except System Options.
   - **Viewer:** Access to the video stream.
5. Select **Enable PTZ control** to allow the user to pan, tilt, and zoom in live view.
6. Click **OK**.

Remove user

To remove users from the devices:

1. Go to **Configuration > Devices > Management > Manage devices**.
2. Right-click the devices and select **User Management > Remove user**.
3. Select the user you want to remove from the **User** drop-down list.
4. Click **OK**.

List users

To list all users on the devices and their access rights:

1. Go to **Configuration > Devices > Management > Manage devices**.
2. Right-click the devices and select **User Management > List users**.
3. Use the **Type to search** field to find users in the list.

Upgrade firmware

Firmware is software that determines the functionality of your Axis device. Keeping your firmware up to date ensures your device has the latest features and improvements.

New firmware can be downloaded using AXIS Camera Station Pro or imported from a file on a hard drive or memory card. Firmware versions that are available for download are shown with the text **(Download)** after their version numbers. Firmware versions that are available on the local client are shown with the text **(File)** after their version numbers.

When you upgrade firmware, you can select the upgrade type:

- **Standard:** Upgrade to the selected firmware version and keep the existing setting values.
- **Factory default:** Upgrade to the selected firmware version and reset all settings to the factory default values.

To upgrade firmware:

1. Go to **Configuration > Devices > Management** and select the devices to configure.
2. Click  , or right-click and select **Upgrade firmware**.
3. If some of the devices can't be configured, for example if the devices are inaccessible, the **Invalid devices** dialog will appear. Click **Continue** to skip the devices that can't be configured.
4. The device isn't accessible during the firmware upgrade. Click **Yes** to continue. If you don't want to see this message again, select **Do not show this dialog again** and click **Yes**.
5. The **Upgrade firmware** dialog lists the device model, number of devices of each model, the existing firmware version, available firmware versions to upgrade, and the upgrade type. By default, the devices in the list are preselected when new firmware versions are available for download, and the latest firmware version is preselected for each device.
   5.1. To update the list of firmware versions available for download, click **Check for updates**. To browse for one or more firmware files stored on the local client, click **Browse**.
   5.2. Select the devices, the firmware versions that you want to upgrade, and the upgrade type.
   5.3. Click **OK** to start upgrading the devices in the list.

Note

By default, firmware updates are done for all the selected devices at the same time. The update order can be changed. See *Firmware upgrade settings*.

Install camera applications

A camera application is software that can be uploaded to and installed on Axis network video products. Applications add functionality to the device, for example detection, recognition, tracking, or counting capabilities.

Some applications can be installed directly from AXIS Camera Station Pro. Other applications must first be downloaded from *www.axis.com/global/en/products/analytics-and-other-applications* or from the application vendor's website.

Applications can be installed on devices with support for AXIS Camera Application Platform. Some applications also require a specific firmware version or camera model.

If the application requires a license, you can install the license key file at the same time as the application or later using the device's configuration page.

To obtain the license key file, the license code included with the application must be registered at *www.axis.com/se/sv/products/camera-applications/license-key-registration#/registration*

If an application can't be installed, go to *www.axis.com* and check if the device model and firmware version support AXIS Camera Application Platform.

Available camera applications:

AXIS Video Motion Detection 4 – An application that detects moving objects within an area of interest. The application doesn't require a license and can be installed on cameras with firmware 6.50 and later. You can also check the firmware release notes for your product to verify if it supports video motion detection 4.

AXIS Video Motion Detection 2 – An application that detects moving objects within an area of interest. The application doesn't require a license and can be installed on cameras with firmware 5.60 and later.

AXIS Video Content Stream – An application that lets Axis cameras send motion tracking data to AXIS Camera Station Pro. It can be installed on cameras with firmware between 5.50 and 9.59. AXIS Video Content Stream can only be used with AXIS Camera Station Pro.

Other applications – Any application you want to install. Download the application to your local computer before you start the installation.

To install camera applications:

1. Go to **Configuration > Devices > Management**.
2. Select the cameras you want to install the applications on. Click  or right-click and select **Install camera application**.
3. Select the camera application you want to install. If you want to install other applications, click **Browse** and navigate to the local application file. Click **Next**.
4. If you have the application installed, you can select **Allow application overwrite** to reinstall the application, or select **Allow application downgrade** to install a previous version of the application.

Note

Downgrading or overwriting the application resets its settings on the devices.

5. If a license is required for the application, the **Install licenses** dialog appears.
   5.1. Click **Yes** to start installing a license, and then click **Next**.
   5.2. Click **Browse** and navigate to the license file, and then click **Next**.

Note

Installing AXIS Video Motion Detection 2, AXIS Video Motion Detection 4, or AXIS Video Content Stream doesn't require a license.

6. Review the information and click **Finish**. The status of the camera changes from `OK` to `Maintenance` and back to `OK` when the installation is done.

Security

The AXIS Camera Station Pro certificate authority (CA) automatically signs and distributes client and server certificates to devices when you turn on HTTPS or IEEE 802.1X. The CA ignores preinstalled certificates. For more information on how to configure certificates, see *Certificates, on page 124*.

Manage HTTPS or IEEE 802.1X certificates

Note

Before enabling IEEE 802.1X, make sure the time on the Axis devices is synchronized in AXIS Camera Station Pro.

1. Go to **Configuration > Devices > Management**.
2. Right-click the devices:
   - Select **Security > HTTPS > Enable/Update** to turn on HTTPS or update the HTTPS settings for the devices.
   - Select **Security > IEEE 802.1X > Enable/Update** to turn on IEEE 802.1X or update the IEEE 802.1X settings for the devices.
   - Select **Security > HTTPS > Disable** to turn off HTTPS for the devices.
   - Select **Security > IEEE 802.1X > Disable** to turn off IEEE 802.1X for the devices.
   - Select **Certificates...** to get an overview, delete certificates, or get detailed information about a specific certificate.

Note

When the same certificate is installed on several devices, it appears as one item. Deleting it removes the certificate from all devices it's installed on.

Status of HTTPS and IEEE 802.1X

On the Device management page, the status of HTTPS and IEEE 802.1X is listed.

	Status	Description
HTTPS	On	AXIS Camera Station Pro uses HTTPS to connect to the device.
	Off	AXIS Camera Station Pro uses HTTP to connect to the device.
	Unknown	The device is unreachable.
	Unsupported firmware	HTTPS isn't supported because the device firmware is too old.
	Unsupported device	HTTPS isn't supported on this device model.
IEEE 802.1X	Enabled	IEEE 802.1X is active on the device.
	Disabled	IEEE 802.1X isn't active but ready to be activated on the device.
	Unsupported firmware	IEEE 802.1X isn't supported because the device firmware is too old.
	Unsupported device	IEEE 802.1X isn't supported on this device model.

Collect device data

This option is typically used for troubleshooting. Use it to generate a .zip file with a data collection report for a specific location on your devices.

To collect device data:

1. Go to **Configuration > Devices > Management**.
2. Right-click the devices, and select **Collect device data**.
3. In the **Data source on selected devices** section:
   - Click **Preset** and select one from the drop-down list of commonly used commands.

   Note

   Some presets don't work on all devices. For example, PTZ status doesn't work on audio devices.
   - Click **Custom** and specify the URL path to your data collection source on the selected servers.
4. In the **Save as** section, specify the file name and folder location for your data collection .zip file.
5. Select **Automatically open folder when ready** to open the specified folder when the data collection is done.
6. Click **OK**.

Connection

To communicate with devices using the IP address or hostname:

1. Go to **Configuration > Devices > Management**.
2. Select the devices, right-click, and select **Connection**.
   - To connect to the devices by using the IP address, select **Use IP**.
   - To connect to the devices by using the hostname, select **Use hostname**.
   - To change credentials, or address and port settings, select **Edit**.

Tags

Tags help you organize devices on the **Device management** page. A device can have multiple tags.

You can tag devices by model, location, or other criteria. For example, when devices are tagged by camera model, you can quickly find and upgrade all cameras of that model.

To tag a device:

1. Go to **Configuration > Devices > Management**.
2. Right-click a device and select **Tag devices**.
3. Select **Use existing tag** and select a tag, or select **Create a new tag** and enter a name for it.
4. Click **OK**.

To remove a tag from a device:

1. Go to **Configuration > Devices > Management** and click  at the top right.
2. In the **Tags** folder, select a tag. All devices associated with the tag are now displayed.
3. Select the devices, right-click, and select **Untag devices**.
4. Click **OK**.

To manage a tag:

1. Go to **Configuration > Devices > Management** and click  at the top right.
2. In the **Device tags** page:
   - Right-click **Tags** and select **New tag** to create a tag.
   - Right-click a tag, select **Rename tag** and enter a new name to rename a tag.
   - Right-click a tag, select **Delete** to delete a tag.

- Click to pin the **Device tags** page.
- Click a tag to display all devices associated with it, and click **All devices** to display all devices connected to AXIS Camera Station Pro.
- Click **Warnings/Errors** to display devices that need attention, for example devices that are inaccessible.

Device configuration tab

To configure all settings on a single device:

1. Go to **Configuration > Devices > Management**.
2. Click the device's address or hostname to go to the device's configuration tab.
3. Change the settings. For information on configuring your device, see the device's user manual.
4. Close the tab. The device reloads to apply the changes in AXIS Camera Station Pro.

Limitations

- Auto authentication for third-party devices isn't supported.
- We can't guarantee general support for third-party devices.
- The device configuration tab with active video streams increases the load and might impact the performance of the server machine.

External data sources

An external data source is a system or source that generates data that can be used to track what happened at the time of each event. See *Data search, on page 39*.

Go to **Configuration > Devices > External data sources** to view a list of all external data sources. Click a column heading to sort by the content of the column.

Item	Description
Name	The name of the external data source.
Source key	The unique identifier of the external data source.
View	The view that the external data source is linked to.
Server	The server that the data source is connected to. Only available when connecting to multiple servers.

An external data source is added automatically when:

- A door is created under **Configuration > Access control > Doors and zones**.
  For a complete workflow on how to set up an Axis network door controller in AXIS Camera Station Pro, see *Set up an Axis network door controller*.
- The first event is received by the device that is configured with AXIS License Plate Verifier.
  For a complete workflow to set up AXIS License Plate Verifier in AXIS Camera Station Pro, see *Set up AXIS License Plate Verifier*.

If an external data source is configured with a view, the data generated from the data source is automatically bookmarked in the timeline of the view in the **Data search** tab. To connect a data source to a view:

1. Go to **Configuration > Devices > External data sources**.
2. Select an external data source and click **Edit**.
3. Select a view from the **View** drop-down list.
4. Click **OK**.

Time synchronization

Go to **Configuration > Devices > Time synchronization** to open the **Time synchronization** page.

AXIS Camera Station Pro displays a list of all added devices. Right-click the header row and select which columns to show. Drag and drop the headers to display the columns in a different order.

The device list includes the following information:

- **Name:** The name of the device or a list of all associated camera names when the device is a video encoder with multiple connected cameras, or a network camera with multiple view areas.
- **Address:** The address of the device. Click the link to go to the device's configuration page. It shows the IP address or hostname depending on which one is used when adding the device. See *Device configuration tab, on page 65*.
- **MAC address:** The MAC address of the device.
- **Model:** The model of the device.
- **Enabled:** Shows if the time synchronization is turned on.
- **NTP source:** The NTP source configured for the device.
  - **Static:** The NTP servers on the device are specified manually under **Primary NTP server** and **Secondary NTP server**.
  - **DHCP:** The device receives the NTP server dynamically from the network. **Primary NTP server** and **Secondary NTP server** are not available when **DHCP** is selected.
- **Primary NTP server:** The primary NTP server configured for the device. Only available when **Static** is selected.
- **Secondary NTP server:** The secondary NTP server configured for the device. Only available for Axis devices that support secondary NTP and when **Static** is selected.
- **Server time offset:** The time difference between the device and the server.
- **UTC time:** The coordinated universal time on the device.
- **Synced:** Indicates whether the time synchronization settings are applied. Only available for devices with firmware 9.1 or later.
- **Time to next sync:** The remaining time to next synchronization.

The Windows Time service (W32Time) uses the Network Time Protocol (NTP) to synchronize the date and time for AXIS Camera Station Pro server. The following information is displayed:

- **Server:** The AXIS Camera Station Pro server on which the Windows Time service is running.
- **Status:** The status of the Windows Time service. Either `Running` or `Stopped`.
- **NTP server:** The NTP server configured for the Windows Time service.

Configure time synchronization

1. Go to **Configuration > Devices > Time synchronization**.
2. Select your devices and select **Enable time synchronization**.
3. Select the NTP source **Static** or **DHCP**.
4. If you've selected **Static**, configure the primary and secondary NTP server.
5. Click **Apply**.

Send alarm when the time difference between server and device is more than 2 seconds	Select this to receive an alarm if the time difference between the server and device is more than 2 seconds.
Set the time zone manually through the device interface	Select this option if you don't want to use the server's time zone and use another one at the device's location instead. If you choose this option, you must set the time zone manually through the device's web interface.

Configure storage

Go to **Configuration > Storage > Management** to open the **Manage storage** page. Here you get an overview of the local storage and network storage in AXIS Camera Station Pro.

List	
Location	The path and name of the storage.
Allocated	The maximum amount of storage allocated to recordings.
Used	The amount of storage space currently used for recordings.

List	
Status	The storage status. Possible values are: • **OK** • **Storage full:** The storage is full. The system overrides the oldest, unlocked recordings. • **Unavailable:** The storage information is currently unavailable. For example, if a network storage was removed or disconnected. • **Intruding data:** Data from other applications use storage space allocated for AXIS Camera Station Pro. Or, there are recordings with no database connection, so-called non-indexed recordings, in the storage space allocated for AXIS Camera Station Pro. • **No permissions:** The user has no read or write permission to the storage. • **Low space:** The drive has less than 15 GB of free space, which AXIS Camera Station Pro considers too low. To prevent errors or corruption, AXIS Camera Station Pro performs a forced cleanup, regardless of the placement of the storage slider, to protect the drive. During the forced cleanup, AXIS Camera Station Pro prevents recording until more than 15 GB of storage is available. • **Insufficient capacity**: The total disk size is less than 32 GB, which isn't enough for AXIS Camera Station Pro. AXIS OS Recorders supporting RAID can also have the following statuses: • **Online:** The RAID system works as it should. There's a redundancy in case one of the physical disks in the RAID system breaks down. • **Degraded:** One of the physical disks in the RAID system is broken. It's still possible to record and play recordings from the storage, but there's no redundancy. If another physical disk breaks, the RAID status changes to **Failure**. We recommend replacing the broken physical disk as soon as possible. After you replace a broken disk, the RAID status changes from **Degraded** to **Syncing**. • **Syncing:** The RAID disks are synchronizing. It's possible to record and play recordings from the storage, but there's no redundancy if a physical disk breaks down. Once the physical disks have synchronized, there's redundancy in the RAID system, and the RAID status changes to **Online**. Important Never remove a RAID disk while synchronizing. This can lead to disk failure. • **Failure:** Several physical disks in the RAID system have failed. When this happens, all recordings in the storage are lost, and recording is only possible once you replace the broken physical disks.
Server	The server where the local storage or network storage is.

Overview	
Used	Amount of storage space currently used by indexed recordings. If a file is in the recording directory but not indexed in the database, the file belongs to the **Other data** category. See *Manage storage, on page 69*.
Free	Amount of storage space left on the storage location. This is the same amount as "Space free" shown in Windows properties for the storage location.

Overview	
Other data	Amount of storage space taken up by the files other than indexed recordings and therefore unknown to AXIS Camera Station Pro. Other data = Total capacity - used space - free space.
Total capacity	The total amount of storage space. This is the same amount as "Total size" shown in Windows properties for the storage location.
Allocated	The amount of storage space that AXIS Camera Station Pro can use for recordings. You can adjust the slider and click **Apply** to adjust the allocated space.

Network storage	
Path	The path of the network storage path.
Username	The username used to connect to the network storage.
Password	The password for the username used to connect to the network storage.

Manage storage

Go to **Configuration > Storage > Management** to open the **Manage storage** page. Here you can specify the folder to store recordings. To prevent storage from filling up, set a maximum percentage of total capacity for AXIS Camera Station Pro to use. You can add additional local storage and network drives for security and more space.

Note

- When connected to multiple AXIS Camera Station Pro servers, select the server from the **Selected server** drop-down menu to manage the storage.
- When the service uses the system account to log in, you can't add network drives that link to shared folders on other computers. See *Network storage isn't accessible*.
- You can't remove the local storage or network storage if cameras are set to record to it or it contains recordings.

Add a local storage or shared network drive

1. Go to **Configuration > Storage > Management**.
2. Click **Add**.
3. To add a local storage, select **Local storage** and select a storage location from the drop-down menu.
4. To add a shared network drive, select **Shared network drive** and enter the path. For example: \\ip_address\share.
5. Click **OK** and enter the username and password for the shared network drive.
6. Click **OK**.

Remove a local storage or shared network drive

To remove a local storage or shared network drive, select it from the storage list and click **Remove**.

Move recordings to a new folder

1. Go to **Configuration > Storage > Management**.
2. Select a local storage or shared network drive from the storage list.
3. Under **Overview**, enter a folder name in **Move recordings to a new folder** to change the storage location for recordings. This also moves existing recordings from the previous folder to the new folder.

4. Click **Apply**.

Adjust storage capacity

1. Go to **Configuration > Storage > Management**.
2. Select a local storage or shared network drive from the storage list.
3. Under **Overview**, move the slider to set the maximum space that AXIS Camera Station Pro can use.
4. Click **Apply**.

Note

- We recommend leaving at least 5% of the disk space free for optimal performance.
- The minimum storage requirement for a storage added to AXIS Camera Station Pro is 32 GB with at least 15 GB of free space available.
- If there's less than 15 GB of free space available, AXIS Camera Station Pro automatically deletes old recordings to free up space.

Collect non-indexed files

Non-indexed files can make up a substantial part of **Other data** on the storage. A non-indexed file is any data in the recording folder that isn't part of the current database. The file can contain recordings from previous installations or data lost when a restore point was used.

The system doesn't delete collected files, but collects and places them in the **Non-indexed files** folder on the recording storage. The storage can be located on the same computer as the client, or on a remote server depending on your configuration. To access the **Non-indexed files** folder, you need access to the server. AXIS Camera Station Pro organizes the data by server first, then by devices connected to that server.

You can look for a lost recording or log, or delete the contents to free up space.

To collect non-indexed files for review or removal:

1. Go to **Configuration > Storage > Management**.
2. Select a local storage or shared network drive from the storage list.
3. Under **Collect non-indexed files**, click **Collect** to start the task.
4. When the task is complete, go to **Alarms and Tasks > Tasks** and double-click the task to view the result.

Select storage devices to connect

Note

Recordings are stored as .acsm files and must be converted before you can play them. Contact Axis Technical support for help converting your files.

Go to **Configuration > Storage > Selection** to open the **Select storage** page. This page shows a list of all cameras in AXIS Camera Station Pro. Here you can specify how many days to keep recordings for specific cameras. When selected, you can see the storage information under **Recording Storage**. You can configure multiple cameras at the same time.

Name	The name of the device or a list of all associated camera names when the device is a video encoder with multiple connected cameras, or a network camera with multiple view areas.
Address	The address of the device. Click the link to go to the device's configuration page. It shows the IP address or hostname depending on which one was used when you added the device. See *Device configuration tab, on page 65*.
MAC address	The MAC address of the device.
Manufacturer	The manufacturer of the device.
Model	The model of the device.

Used storage	The amount of storage space currently used for recordings.
Location	The path and name of the storage.
Retention time	The retention time configured for the camera.
Oldest recording	The time of the oldest recording from the camera kept in the storage.
SD card playback	Indicates whether the camera is configured to play back recordings directly from its SD card in AXIS Camera Station Pro, without copying them to the server.
Failover recording	Indicates whether the camera uses failover recording.
Copy to ACS Pro	Indicates whether SD card recordings are copied to the AXIS Camera Station Pro.
Fallback recording	Indicates whether the camera uses fallback recording.
Server	The server where the local storage or network storage is.

The storage settings for each camera were configured when the cameras were added to AXIS Camera Station Pro. To edit storage settings for a camera:

1. Go to **Configuration > Storage > Selection**.
2. Select the camera to edit the storage settings.
3. Under **Recording storage**, set storage location and retention time.
4. Under **SD card storage**, select **Playback of SD card recordings**, **Failover recording**, and **Copy SD card recordings to ACS Pro server** as needed.
5. Click **Apply**.

Recording storage

Note

- To use SD card storage, the device must support VAPIX and use an Axis SD card.
- SD card features don't work with M-JPEG.
- Recordings on the SD card aren't deleted by AXIS Camera Station Pro. Their retention is controlled by the SD card retention time on the camera.

Store to	Select the storage location for recordings from the drop-down menu. Available options are the local storage and network storage that were created.
Retention time	• **Unlimited**: Keep recordings until the storage is full. • **Limited**: Set the maximum number of days to keep recordings. Note If the amount of storage space reserved for AXIS Camera Station Pro becomes full, the system deletes recordings before the designated number of days.
Maximum days to keep recordings	Specify the number of days to keep your recordings.

SD card storage	
Playback SD card recordings	Turn on to play back recordings directly from the camera's SD card in AXIS Camera Station Pro, without copying them to the server. SD card recordings visible in the timeline can also be exported. This feature requires AXIS OS 5.60 or later.
Failover recording	Select to store recordings to the camera's SD card when the connection to AXIS Camera Station Pro is lost. Available for cameras that have an SD card and firmware 5.20 or later.
Copy SD card recordings to ACS server	Select to copy all recordings on the camera's SD card to the server. Use **Schedule** to set when recordings are copied. The default schedule is **Always**.

Configure recording and events

When you add cameras to AXIS Camera Station Pro, the system automatically configures motion recording or continuous recording. You can later change the recording method to suit your needs. See *Recording method, on page 77*.

Motion recording

You can use motion detection with all Axis network cameras and video encoders. Recording only when motion is detected saves considerably more storage space than continuous recording. In **Recording method**, you can turn on and configure **Motion detection**. You can, for example, configure the settings if the camera detects too many or too few moving objects, or if the size of the recorded files is too large for the available storage space.

To configure motion recording:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera.
3. Select the **Motion detection** checkbox.
4. Click **Motion settings** to configure the motion detection settings, such as number of detectable objects. Available settings are different for different cameras, see *Edit built-in motion detection* and *Edit AXIS Video Motion Detection 2 and 4*.
5. Select a **Profile** in the drop-down menu, **High** is the default profile.
6. Select a schedule or click **New schedule...** to create a new custom schedule.
7. Set the pre- and post-buffer times and the trigger period.
8. Click **Apply**.

Note

You can use action rules to configure motion recording. Make sure **Motion detection** is turned off in **Recording method** before using action rules.

Profile	Use a lower resolution to decrease the recording size. To edit profile settings, see *Stream profiles*.
Schedule	The schedule for the recordings. To lower the impact on your storage space, only record during specific time periods.
Event category	Which event category you want the recording to fall under, if any.

Prebuffer	The number of seconds before the detected motion to include in a recording.
Postbuffer	The number of seconds after the detected motion to include in a recording.
Trigger period	Sets the minimum time between two triggers to reduce the number of back-to-back recordings. If another trigger occurs within this interval, the recording continues and the interval restarts.
Notifications	A notification is sent when the camera detects motion. **Mobile app** sends a push notification to the AXIS Camera Station mobile app. **Server alarm** raises an alarm in AXIS Camera Station Pro.

Configure motion detection

Object detection

Object detection recording captures video when AXIS Object Analytics detects and classifies object types like people and vehicles. We recommend using it together with motion detection or continuous recording to ensure you don't miss events. AXIS Object Analytics supports up to 10 scenarios per camera.

Note

Your camera needs firmware version 12.4.26 or later, a single sensor, and AXIS Object Analytics ACAP installed to work with this feature.

To use object detection:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera.
3. Select the **Object detection** checkbox.
4. Configure your settings. See table below for more information.
5. Click **Apply**.

- Object detection events appear in pink on the timeline.

Object detection settings...	Click to open the AXIS Object Analytics web interface and configure which object types (Humans, Vehicles) trigger recordings, set minimum object size, define detection areas, and adjust time-in-area settings.
Profile	Select a **Profile** from the drop-down menu. **High** is the default profile. Use a lower resolution to reduce the recording size. To edit profile settings, see *Stream profiles*.
Schedule	Set the schedule for recordings. To lower the impact on your storage space, only record during specific time periods.

Event category	Select which event category you want the recording to fall under, if any. See *Event categories, on page 26* for more information.
Prebuffer	Set the number of seconds before the detected object to include in a recording.
Postbuffer	Set the number of seconds after the detected object to include in a recording.
Trigger period	Set a minimum time interval between triggers to reduce back-to-back recordings. If another trigger occurs within this interval, the recording continues and the trigger period restarts.
Notifications	Sends you a notification when AXIS Object Analytics detects an object. **Mobile app** sends a push notification to the AXIS Camera Station mobile app. **Server alarm** raises an alarm in AXIS Camera Station Pro.

Continuous and scheduled recording

Continuous recording saves images without interruption and requires more storage space than other recording options. To reduce the file size, consider using motion detection recording instead.

To use continuous recording:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera.
3. Select the **Continuous** checkbox.
4. Configure your settings. See table below for more information.
5. Click **Apply**.

Profile	Select a **Profile** from the drop-down menu. **High** is the default profile. Use a lower resolution to reduce the recording size. To edit profile settings, see *Stream profiles*.
Schedule	Set the schedule for recordings. To lower the impact on your storage space, only record during specific time periods.
Average bitrate	Turn on to set a maximum storage limit. The system shows the estimated average bitrate based on the specified max storage and retention time. The maximum average bitrate is 50000 Kbit/s. See *Configure average bitrate, on page 77*.

Manual recording

To configure manual recording settings:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera.
3. Select the **Manual** checkbox.
4. Configure your settings. See table below for more information.

5. Click **Apply**.

Profile	Select a **Profile** from the drop-down menu. **High** is the default profile. Use a lower resolution to reduce the recording size. To edit profile settings, see *Stream profiles*.
Event category	Select which event category you want the recording to fall under, if any.
Prebuffer	Set the number of seconds before you press record to include in the recording.
Postbuffer	Set the number of seconds after you stop recording to include in the recording.
Bookmark when recording	Adds bookmark details each time you start a manual recording. Bookmarks help you find and identify specific recordings later. This setting applies to operators and administrators only and is turned off by default.
Maximum duration	Set the maximum length for each recording, not including prebuffer or postbuffer times. Set to 0 for unlimited duration.

For more information on recording manually, see *Record manually*.

Rule-triggered recording

A rule triggered recording starts and stops according to a rule created in Action rules. You can use rules, for example, to generate recordings triggered by signals from I/O ports or device events. A rule can have several triggers.

To create rule-triggered recording, see *Action rules*.

Note

If you use a rule to configure motion recording, make sure to turn off motion recording to avoid duplicate recordings.

Failover recording

Use failover recording to save recordings to the camera's SD card when the connection to AXIS Camera Station Pro is lost.

AXIS Camera Station Pro automatically selects the failover method based on the camera's firmware version:

- **Firmware 11.11.42 or later:** Failover recording starts any time the camera loses contact with the server.
- **Earlier firmware:** Failover recording only starts on unexpected loss of connection. Planned server restarts don't trigger failover recording.

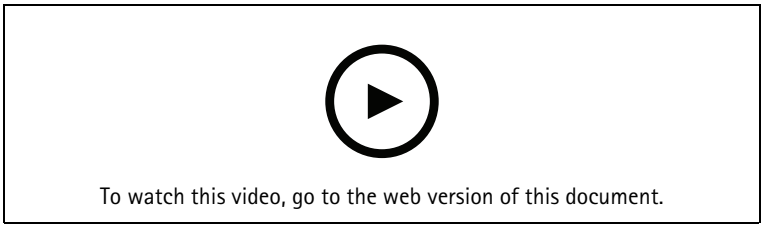
To configure failover recording, see *Select storage devices to connect, on page 70*.

Note

- When upgrading, if **Failover recording** was previously turned on, **Copy SD card recordings to ACS Pro server** is turned on automatically.
- Recordings on the SD card aren't deleted by AXIS Camera Station Pro. Their retention is controlled by the SD card retention time on the camera.
- Turning on failover recording overwrites any existing failover configuration for that camera on other servers.
- Failover recording can only be active for one AXIS Camera Station Pro server per camera view at a time.

When the connection is restored and **Copy SD card recordings to ACS Pro server** is turned on, the recordings are copied to the server and marked with a dark gray color in the timeline. The camera uses a 20-second prebuffer and postbuffer, though short gaps of 1–4 seconds can still appear.

Recording methods	
Motion detection with prebuffer	If the connection is lost for more than 20 seconds, the camera continuously records to the SD card until the connection is restored or the SD card becomes full.
Motion detection without prebuffer	• If the connection is lost for more than 20 seconds when motion recording is not ongoing, failover recording doesn't start. • If the connection is lost for more than 20 seconds when motion recording is ongoing, failover recording starts and continues until the connection is restored or the SD card becomes full.
Continuous recording	If the connection is lost for more than 20 seconds, the camera continuously records to the SD card until the connection is restored or the SD card becomes full.



Use SD card for failover recording

Fallback recording

You can turn on fallback recording on a device that uses AXIS S3008 Recorder as recording storage. Once turned on, the device automatically starts a continuous recording when the connection between AXIS Camera Station Pro and the recorder is lost. The device uses the medium stream profile for fallback recording.

Note

- This feature requires AXIS Camera Station 5.36 or later, AXIS S3008 Recorder firmware 10.4 or later, and Axis device firmware 5.50 or later.
- If there's an ongoing continuous recording when fallback recording starts, a new continuous recording starts. The system creates duplicates of the stream on the recorder.

To turn on fallback recording:

1. Make sure you've added AXIS S3008 Recorder and devices, and selected the recorder as the recording storage for the device. See *Set up AXIS OS Recorders*.
2. Go to **Configuration > Storage > Selection**.
3. Select the device and select **Fallback recording**.
4. Click **Apply**.

Recording method

AXIS Camera Station Pro automatically configures motion recording or continuous recording when you add devices.

A check mark indicates the recording method a device uses. To customize profile settings for video and audio, see *Stream profiles*.

To change the recording method:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select one or multiple devices.
   For devices of the same model, you can configure multiple devices at the same time.
3. In the **Recording method** screen, turn a recording method on or off.

Note

View areas don't support motion detection.

Configure average bitrate

With average bitrate, the bitrate automatically adjusts over a longer time. This lets you meet the target bitrate and provide good video quality based on the specified storage.

Note

- This option is only available for continuous recording. The cameras must support average bitrate and have firmware 9.40 or later.
- The average bitrate settings affect the quality of the selected stream profile.

1. Go to **Configuration > Storage > Selection** and make sure you've set a limited retention time for the camera.
2. Go to **Configuration > Devices > Stream profiles** and make sure you use H.264 or H.265 format for the profile used for continuous recording.
3. Go to **Configuration > Recording and events > Recording method**.
4. Select the camera and turn on **Continuous**.
5. Under **Video settings**, select the video profile that you configured.
6. Turn on **Average bitrate** and set **Max storage**. The system shows the estimated average bitrate based on the specified max storage and retention time. The maximum average bitrate is 50000 Kbit/s.

Note

Max storage means the maximum space for the recordings over the retention time. It only guarantees that the recordings don't exceed the specified space, it doesn't guarantee that there's enough space for the recordings.

7. Click **Apply**.

Edit motion settings

If your device uses AXIS Object Analytics, you can edit the settings for motion recording there.

Note

AXIS Object Analytics in AXIS Camera Station Pro requires AXIS OS 12.4.

1. Open a **Configuration** tab.
2. Go to **Recording and events** > **Recording method**.
3. Select the camera you want to configure.
4. Turn on **Motion detection**.
5. Click **Motion settings**.

Read the *AXIS Object Analytics user manual* for information on configuring AXIS Object Analytics on your device.

Edit AXIS Video Motion Detection 2 and 4

AXIS Video Motion Detection 2 and 4 are camera applications for products that support AXIS Camera Application Platform. When you install AXIS Video Motion Detection 2 or 4 on the camera, motion detection detects moving objects within an area of interest. Motion detection 2 requires firmware 5.60 or later, and AXIS Video Motion Detection 4 requires firmware 6.50 or later. You can also check the firmware release notes for your product to verify if it supports video motion detection 4.

If you select motion recording when you add cameras to AXIS Camera Station Pro, AXIS Video Motion Detection 2 and 4 installs on cameras with the required firmware. Cameras without the required firmware use the built-in motion detection. You can install the application manually from the device management page. See *Install camera applications*.

With AXIS Video Motion Detection 2 and 4, you can create:

- **Area of interest**: An area in a recording where the camera detects moving objects. The feature ignores objects outside the area of interest. The area displays on top of the video image in the form of a polygon. The area can have 3 to 20 points (corners).
- **Area to exclude**: An area within the area of interest that ignores moving objects.
- **Ignore filters**: Create filters to ignore the moving objects detected by the application. Use as few filters as possible and configure the filters with care to make sure not to ignore important objects. Use and configure one filter at a time.
  - **Short-lived objects filter**: This filter ignores objects that only appear a short time in the image. For example, light beams from a passing car and shadows that move quickly. Set the minimum time that objects must appear in the image to trigger an alarm. The time starts from the moment the application detects the object. The filter delays alarms and doesn't trigger them if the object disappears from the image within the specified time.
  - **Small objects filter**: This filter ignores small objects, such as animals. Set the width and height as a percentage of the total image. The filter ignores objects smaller than the specified width and height and doesn't trigger alarms. The object must be smaller than both the width and height values for the filter to ignore it.
  - **Swaying objects filter**: This filter ignores objects that only move a short distance, for example swaying foliage and flags and their shadows. Set the distance as a percentage of the total image. The filter ignores objects that move a shorter distance than the distance from the center of the ellipse to one of the arrowheads. The ellipse is a measure of movement and applies to all movement in the image.

To configure motion settings:

Note

These settings are applied directly to the camera.

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera with AXIS Video Motion Detection 2 or 4 and click **Motion Settings**.
3. Edit the area of interest.
4. Edit the exclude area.
5. Create ignore filters.

6. Click **Apply**.

Add a new point	To add a new point to your area of interest, click the line between two points.
Remove Point	To remove a point from your area of interest, click the point and click **Remove Point**.
Add Exclude Area	To create an exclude area, click **Add Exclude Area** and click the line between two points.
Remove Exclude Area	To remove an exclude area, click **Remove Exclude Area**.
Short lived objects filter	To use a short-lived objects filter, select **Short lived objects filter** and use the **Time** slider to adjust the minimum time that objects must appear in the image to trigger an alarm.
Small objects filter	To use a small objects filter, select **Small objects filter** and use the **Width** and **Height** sliders to adjust the size of the ignored objects.
Swaying objects filter	To use a swaying objects filter, select **Swaying objects filter** and use the **Distance** slider to adjust the size of the ellipse.

Edit built-in motion detection

With built-in motion detection, the camera detects motion within one or more include areas and ignores all other motion. An include area is an area that detects motion. You can use multiple include and exclude areas, and place an exclude area within an include area to ignore specific motion.

To add and edit an include area:

Note

These settings are applied directly to the camera.

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera with built-in motion detection, and click **Motion Settings**.
3. Click **Add** in the Window section.
4. Select **Include**.
5. To see only the area you're editing, select **Show selected window**.
6. Move and resize the shape in the video image. This is the include area.
7. Adjust **Object size**, **History**, and **Sensitivity**.
8. To use the predefined settings, select **Low**, **Moderate**, **High**, or **Very High**. **Low** detects larger objects with a shorter history. **Very High** detects smaller objects with a longer history.
9. In the **Activity** section, review the detected motion in the include area. Red peaks indicate motion. Use the **Activity** field when you adjust **Object size**, **History**, and **Sensitivity**.
10. Click **OK**.

Object size	Object size relative to the region size. The camera detects only very large objects at a high level. At a low level it detects even very small objects.
History	Object memory length defines how long an object needs to be in an area before it's considered to be non-moving. At a high level, an object triggers motion detection for a long period of time. At a low level, an object triggers motion detection for a short period of time. If no objects should appear in the area, select a very high history level. This triggers motion detection if the object is present in the area.
Sensitivity	Difference in luminance between the background and the object. With high sensitivity, the camera detects ordinary colored object on ordinary backgrounds. With low sensitivity, it detects only very bright objects on a dark background. To detect only flashing light, select a low sensitivity. In other cases, we recommend a high sensitivity level.

To add and edit an exclude area:

1. In the **Edit Motion Detection** screen, click **Add** in the **Window** section.
2. Select **Exclude**.
3. Move and resize the shaded shape in the video image.
4. Click **OK**.

To remove an include or exclude area:

1. In the **Edit Motion Detection** screen, select an area to remove.
2. Click **Remove**.
3. Click **OK**.

Configure event categories

Event categories make it easier to find recordings of a certain type. To create an event category:

1. Go to **Configuration** > **Recording and events** > **Event categories**.
2. Click **New**.
3. Enter a name for the event category.
4. Optionally, set an event category color and custom retention time for the event category.
5. Click **Apply**.

Name	We recommend using a name for the category that represents a type of event, like assault or traffic stop.
Retention time	You can set a custom retention time for each event category that overrides the camera's default retention time. The custom event category retention time applies only if it's longer than the default.

See *Event categories, on page 26* for more information.

I/O ports

Many cameras and video encoders have I/O ports for connection of external devices. Some auxiliary devices also have I/O ports.

There are two types of I/O ports:

Input port – Use to connect to devices that can toggle between an open and closed circuit. For example, door and window contacts, smoke detectors, glass break detectors, and PIRs (Passive Infrared Detector).

Output port – Use to connect to devices such as relays, doors, locks, and alarms. AXIS Camera Station Pro can control devices connected to output ports.

Note

- When connected to multiple AXIS Camera Station Pro servers, you can select any connected server from the **Selected server** drop-down menu to add and manage I/O ports.
- Administrators can turn off I/O ports for users. See *User permissions*.

Action rules use I/O ports as triggers or actions. Triggers use input signals, for example, when AXIS Camera Station Pro receives a signal from a device connected to an input port, it performs the specified actions. Actions use output ports, for example when a rule activates, AXIS Camera Station Pro can activate or deactivate a device connected to an output port. See *Action rules*.

For information on connecting devices and configuring I/O ports, see the Axis product's user manual or installation guide. Some products have ports that can act as input or output.

You can control output ports manually. See *Monitor I/O ports*.

Add I/O ports

To add I/O ports:

1. Go to **Configuration > Recording and events > I/O ports**.
2. Click **Add** to view a list of I/O ports you can add.
3. Select the port and click **OK**.
4. Review the information in **Type** and **Device**. Update if needed.
5. Enter a name in **Port**, **Active State**, and **Inactive State**. The names also show in Action rules, Logs, and I/O Monitoring.
6. For output ports, you can set the initial state for when AXIS Camera Station Pro connects to the device. Select **On startup set to** and select the initial state in the **State** drop-down menu.

Edit	To edit a port, select the port and click **Edit**. In the dialog, update the port information and click **OK**.
Remove	To remove a port, select the port and click **Remove**.
Reload I/O Ports	If you configure the I/O ports from the device configuration page, click **Reload I/O Ports** to update the list.

Monitor I/O ports

Note

When connected to multiple AXIS Camera Station Pro servers, you can select any connected server in the **Selected server** drop-down menu to monitor I/O ports.

To control output ports manually:

1. Go to ☰ **> Actions > I/O Monitoring**.

2. Select an output port.
3. Click **Change state**.

Action rules

Use action rules to automatically respond to events. For example, send an email when a camera detects motion outside office hours, interact with devices connected to I/O ports, and alert operators about important events.

Each rule has triggers (events that activate the rule), actions (what happens when triggered), and an optional schedule. When triggers activate, the rule carries out all actions.

Note

- When connected to multiple AXIS Camera Station Pro servers, you can select any connected server in the **Selected Server** drop-down menu to create and manage action rules.
- For third-party devices, the available actions can differ between devices. Some of these actions require additional device configuration.

Create a new action rule

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New...**.
3. Enter a name for the rule in the **Name** field.
4. Under **Schedule**, select **Always** or **Custom schedule** to choose a schedule from the drop-down menu. You can also create a new schedule or edit an existing one.
5. Under **Triggers**, click **Add...**, select the trigger type, configure it, and click **OK**. See *Add triggers* to learn more.
6. Under **Actions**, click **Add...**, select the action type, configure it, and click **OK**. See *Add actions* to learn more.
7. Click **Apply**.
   - The rule is automatically turned on when you save it.

Edit	To edit an existing rule, select the rule and click **Edit**.
Copy	To copy an existing rule, select the rule and click **Copy...**.
Remove	To remove a rule, select the rule and click **Remove**.

Configure multiple action rules

When you select multiple rules, only triggers and actions that are the same across all selected rules are shown. Any changes you make will apply to all selected rules.

- Go to **Configuration > Recording and events > Action rules.**
- Select multiple rules.
- Make your changes:
  - Add triggers or actions that will apply to all selected rules.
  - Remove common triggers or actions from all selected rules.
  - Change the schedule for all selected rules.
- Click **Apply**.

Note

You can't edit individual triggers or actions when multiple rules are selected. If your changes would make any rule invalid, you can't apply them.

Add triggers

Triggers activate rules, and a rule can have multiple triggers. As long as one of the triggers stays active, the rule stays active. If all triggers must be active for the rule to be active, select **All triggers must be active simultaneously to trigger the actions**. If you use this setting with pulse triggers, increase the trigger period. Pulse triggers are triggers that are active momentarily.

The following triggers are available:

Motion detection – Registered motion within a defined area activates the motion detection trigger. See *Create motion detection triggers, on page 83*.

Always active – This trigger is always on. For example, you can combine this trigger with a schedule that's always on and a recording action with a low profile to achieve a second continuous recording suitable for devices with limited performance.

Live view – The live view trigger occurs when a user opens a specific camera's video stream. You can use this, for example, to let people near a camera know that someone's watching them using the camera's LEDs. See *Create live view triggers, on page 84*.

System event and error – A system event and error trigger activates when recording errors occur, a storage becomes full, a network storage connection fails, or one or more devices loses connection. See *Create system event and error triggers, on page 84*.

Input/Output – The Input/Output (I/O) trigger activates when a device's I/O port receives a signal from, for example, a connected door, smoke detector, or switch. See *Create input/output triggers, on page 85*. We recommend using device event triggers instead of input/output triggers if possible.

Device event – This trigger uses events directly from the camera or auxiliary device. Use this if no suitable trigger is available in AXIS Camera Station Pro. See *Create device event triggers, on page 85*.

Action button – Use the action buttons to start and stop actions from live view. You can use one button in different rules. See *Create action button triggers, on page 90*.

AXIS Entry Manager event – This trigger activates when AXIS Camera Station Pro receives signals from doors configured in AXIS Entry Manager. For example, doors forced to open, open too long, or denied access. See *Create AXIS Entry Manager event triggers, on page 91*.

External HTTPS – The external HTTPS trigger lets external applications trigger events in AXIS Camera Station Pro through HTTPS communication. See *Create external HTTPS triggers, on page 91*.

Create motion detection triggers

The motion detection trigger activates when the camera detects motion within a defined area. Since the camera processes the detection, it doesn't add any processing load to AXIS Camera Station Pro.

Note

Don't use motion detection triggers to start recordings if motion recording is already turned on in the camera. Turn off motion recording before you use motion detection triggers. To turn off motion recording, go to **Configuration > Recording and events > Recording method**.

To create a motion detection trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **Motion detection**.
4. Click **OK**.
5. In the dialog:
   5.1. Select the camera that should detect motion.
   5.2. Set a minimum time interval between triggers to reduce back-to-back recordings. If another trigger occurs within this interval, the recording continues and the trigger period restarts.

5.3. Click **Motion settings** to configure motion detection settings. Available settings are different for different cameras. See *Edit built-in motion detection* and *Edit AXIS Video Motion Detection 2 and 4*.

6. Click **OK**.

Create live view triggers

The live view trigger occurs when a user opens a specific camera's video stream. You can use this, for example, to let people near a camera know that someone's watching them using the camera's LEDs.

To create a live view trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **Live view**.
4. Click **OK**.
5. Select the trigger camera.
6. Click **OK**.

Create system event and error triggers

Select one or more system events and errors to use as triggers. Examples of system events are recording errors, a full storage, a network storage connection fails, and one or more devices lose connection.

To create a system event and error trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **System event and error**.
4. Click **OK**.
5. Select a system event or error to create the trigger.
6. Click **OK**.

On recording error	Select **On recording error** to activate the trigger when errors occur during recording, for example if a camera stops streaming.
On full storage	Select **On full storage** to activate the trigger when a storage for recordings is full.
On no contact with network storage	Select **On no contact with network storage** to activate the trigger when there's a problem accessing s a network storage.
On lost connection to camera	Select **On lost connection to camera** to activate the trigger when there's problem contacting the cameras. • Select **All** to include all the cameras added to AXIS Camera Station Pro. • Choose **Selected** and click **Cameras** to show a list of all cameras added to AXIS Camera Station Pro. Use **Select all** or **Deselect all** to select or clear all cameras.

Create input/output triggers

The input/output (I/O) trigger activates when a device's I/O port receives a signal from, for example, a connected door, smoke detector, or switch.

Note

- Add the I/O port to AXIS Camera Station Pro before you use an I/O trigger. See *I/O ports*.
- We recommend using device event triggers instead of input/output triggers if possible. See *Create device event triggers, on page 85* for more information.

To create an input/output trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **Input/Output**.
4. Click **OK**.
5. Under **Trigger port and state**, configure the I/O port and trigger settings.
6. Click **OK**.

Trigger port and state	
I/O port	In **I/O port**, select the input or output port.
Trigger state	In **Trigger state**, select the I/O port state that should activate the trigger. Available states depend on the port's configuration.
Trigger period	Set a minimum interval between two successive triggers to reduce back-to-back recordings. If another trigger occurs within this interval, the recording continues and the trigger period restarts.

Create device event triggers

This trigger uses events directly from the camera or auxiliary device. Use this if there's no suitable trigger available in AXIS Camera Station Pro. The events differ between cameras and have one or more filters that must be set. Filters are conditions that must be met for the device event trigger to activate. For information about events and filters for Axis products, see the VAPIX® documentation on *axis.com/partners* and *axis.com/vapix*

To create a device event trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **Device event**.
4. Click **OK**.
5. Under **Configure device event trigger**, configure the event trigger.

Note

Available events depend on the selected device. For third-party devices, many of these events require additional configuration in the device.

6. Under **Filters**, select the filters.
7. Under **Activity**, review the current state of the device event trigger over time. An event can be stateful or stateless. A step function indicates a stateful event. A straight line with pulses indicates a stateless event.
8. Click **OK**.

Configure device event trigger	
Device	In **Device**, select the camera or auxiliary device.
Event	In **Event**, select the event to use as trigger.
Trigger period	Set a minimum interval between two successive triggers to reduce back-to-back recordings. If another trigger occurs within this interval, the recording continues and the trigger period restarts.

Examples of device events

Category	**Device event**
Amplifier	Amplifier overload
Audio Control	Digital signal status
AudioSource	Audio detection
Authorization	Access request granted
	Access request denied
Call	State
	State change
	Network quality
	SIP account status
	Incoming video
Casing	Casing open
Device	Ring power overcurrent protection
Device sensors	System ready
	PIR sensor
Device status	System ready
Door	Door forced
	Door installation tampering detected
	Door locked
	Door open too long
	Door position
	Door unlocked
Event buffer	Begin
Event logger	Dropped alarms
	Dropped events
	Alarm
Fan	Status

GlobalSceneChange	Image service
Hardware Failure	Storage failure
	Fan failure
Heater	Status
Input ports	Virtual input
	Digital input port
	Manual trigger
	Supervised input port
	Digital output port
	External input
Light	Status
LightStatusChanged	Status
Media	Profile changed
	Configuration changed
Monitor	Heartbeat
MotionRegionDetector	Motion
Network	Network lost Only applicable for events used by the device, not applicable for events used by AXIS Camera Station Pro.
	Address added
	Address removed
PTZ moving	PTZ movement on channel <channel name>
PTZ presets	PTZ preset reached on channel <channel name>
PTZController	Auto tracking
	PTZ control queue
	PTZ error
	PTZ ready
Recording Config	Create recording
	Delete recording
	Track configuration
	Recording configuration
	Recording job configuration
Remote camera	Vapix status
	PTZ position

Schedule	Pulse
	Interval
	Scheduled event
State	Active
Storage	Storage disruption
	Recording ongoing
System message	Action failed
Tampering	Tilt detected
	Shock detected
Temperature sensors	Above operating temperature
	Below operating temperature
	Within operating temperature
	Above or below operating temperature
Trigger	Relays and outputs
	Digital input
Video Motion Detection	VMD 4: profile <profile name>
	VMD 4: any profile
Video Motion Detection 3	VMD 3
Video source	Motion alarm
	Live stream accessed
	Day night vision
	Camera tampering
	Average bitrate degradation
	Video source connected

Axis network door controller device events

Device event	Trigger the action rule
Authorization	
Access request granted	The system granted access to a cardholder when they identified using their credentials.
Duress	Someone used their duress PIN. You can use this to, for example, trigger a silent alarm.
Access request denied	The system denied a cardholder access when they identified using their credentials.
Double-swipe	A cardholder swiped their card twice. The double-swipe allows a cardholder to override the current state of a door. For example, they can use it to unlock a door outside the regular schedule.

Anti-passback detection	Someone used a credential belonging to a cardholder who entered a zone before them.
Authorization with two-person rule	
Access request pending	The first out of two cardholders identified themselves using their credentials.
Access request granted	The system granted access to the last cardholder when they identified using their credentials.
Casing	
Casing open	Someone has opened or removed the casing of the network door controller. Use, for example, to send a notification to the administrator if the casing is open for maintenance purposes or if someone tampered with the casing.
Device status	
System ready	The system is in ready state. For example, the Axis product detects the system state and sends a notification to the administrator when the system has started. Select **Yes** to trigger the action rule when the product is in a ready state. The rule can only trigger when all necessary services, such as the event system, have started.
Door	
Door forced	The door is forced open.
Door installation tampering detected	When the system detects the following: • Device casing is open or closed. • Device motion. • Removal of the connected reader from wall. • Tampering with connected door monitor, reader, or REX device. To use this trigger, make sure you turn on **Supervised input** and check the installation of the end-of-line resistors on the relevant door connector input ports.
Door locked	The door lock is locked.
Door open too long	The door is open too long.
Door position	The door monitor indicates that the door is open or closed.
Door unlocked	The door lock stays unlocked. For example, you can use this state when there are visitors allowed to open the door without needing to present their credentials.
Input ports	
Virtual input	One of the virtual inputs changes states. A client, such as a management, can use it to initiate various actions. Select the input port that should trigger the action rule when it becomes active.
Digital input port	A digital input port changes state. Use this trigger to initiate various actions, for example, send a notification or flash the status LED. Select the input port that should trigger the action rule when it becomes active or select **Any** to trigger the action rule when one of the input port becomes active.
Manual trigger	Activates the manual trigger. Use this trigger to manually start or stop the action rule through the VAPIX API.

External input	The emergency input is active or inactive.
Network	
Network lost	The network loses connection. Only applicable for device events, not for events used by AXIS Camera Station Pro.
AddressAdded	A new IP address is added.
AddressRemoved	The IP address is removed.
Schedule	
Scheduled event	A predefined schedule changes state. Use it to record video in specific time periods, for example, during office hours or at weekends. Select a schedule in the **Schedule** drop-down menu.
System message	
Action failed	An action rule fails and triggers the action failed system message.
Trigger	
Digital Input	A physical digital input port is active or inactive.

Create action button triggers

Use action buttons to start and stop actions in live view. You can find the action buttons at the bottom of the live view or in a map. You can use one button for multiple cameras and maps, and there can be multiple action buttons for one camera or a map. You can arrange the buttons for a camera when you add or edit an action button for a camera.

There are two types of action buttons:

Command buttons – Used to manually start an action. Use command buttons for actions that don't require a stop button. A command button has a button label and a tooltip. The button label is the text shown on the button. Hover over the button with the mouse to show the tooltip.

Example: Create a button to activate an output for a predefined time, raise an alarm, and send email.

Toggle buttons – Used to manually start and stop an action. The button has two states: toggle and untoggle. Click the button to switch between the two states. By default, toggle buttons start the action when in the toggle state, but you can also start the action in the untoggle state.
A toggle button has a toggle label, an untoggle label, and a tooltip. The texts shown on the buttons in the toggle and untoggle states are the toggle and untoggle labels. Hover over the button with the mouse to show the tooltip.

Example: Create a button to open and close doors, use output action with pulse set to "as long as any trigger is active".

To create an action button trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **Action Button**.
4. Click **OK**.
5. Select **Create new button** or **Use existing button**. Click **Next**.
6. If you select **Create new button**:

6.1. Select **Command button** or **Toggle button**. If you want to use the toggle button to start the action in the untoggle state, select **Trigger on untoggle**.

6.2. Click **Next**.

6.3. Add labels and tooltip for the button.

Note

The letter or number after the first underscore in an action button label becomes the access key to the action button. Press Alt and the access key to activate the action button. For example, when you name an action button as A_BC, the action button name changes to ABC in live view. Press Alt + B to activate the action button.

7. If you select **Use existing button**:
   7.1. Search for the button or click the button you want to use.
   7.2. If you select an existing toggle button, you must select **Trigger on toggle** or **Trigger on untoggle**.
   7.3. Click **Next**.
   7.4. Edit the labels and tooltip of the button.
8. Select the camera or map from the drop-down menu.
9. To add the button to multiple cameras or maps, click **Add to multiple cameras** or **Add to multiple maps**.
10. If a camera has multiple action buttons, click **Arrange** to edit the order of the buttons. Click **OK**.
11. Click **Next**.

Create AXIS Entry Manager event triggers

AXIS Camera Station Pro activates the trigger when it receives signals from doors configured in AXIS Entry Manager. For example, doors forced to open, doors open too long, or denied access.

Note

AXIS Entry Manager event trigger is only available when you add AXIS A1001 Network Door Controller to AXIS Camera Station Pro.

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **AXIS Entry Manager event**.
4. Click **OK**.
5. Select an event and door to activate the trigger.
6. Click **OK**.

Create external HTTPS triggers

The external HTTPS trigger lets external applications trigger events in AXIS Camera Station Pro through HTTPS communication. This trigger only supports HTTPS communication and requires a valid AXIS Camera Station Pro username including domain name and password for HTTPS requests.

The following requests are supported with HTTP method GET*. You can also use POST with JSON data stated in the body of the request.

Note

- The external HTTPS trigger requests can only be tested in Google Chrome.
- The external HTTPS trigger uses the same ports as the mobile viewing app, see Mobile communication port and Mobile streaming port described in *General*.
- Activate the trigger with ID "trigger1": `https://[address]:29204/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`

- Deactivate the trigger with ID "trigger1": `https://[address]:29204/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Activate the trigger with ID "trigger1" and then automatically deactivate the trigger after 30 seconds: `https://[address]:29204/Acs/Api/TriggerFacade/ActivateDeactivateTrigger?{"triggerName":"trigger1","deactivateAfterSeconds":"30"}`

Note

The timer for automatic deactivation is canceled if any other command is issued to the same trigger.

- Pulse the trigger with ID "trigger1" (trigger activation followed by immediate deactivation): `https://[address]:29204/Acs/Api/TriggerFacade/PulseTrigger?{"triggerName":"trigger1"}`

To create an external HTTPS trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. click **New**.
3. Click **Add** and select **External HTTPS**.
4. Click **OK**.
5. Enter the trigger name in **Trigger name**.
6. Review the sample URL, which uses the same server address that the client used to log in. The URLs only work after the action rule is complete.
7. Click **OK**.

Suitable actions for external HTTPS triggers

- Requests to activate and deactivate the trigger are suitable for actions that start and stop recordings.
- Requests to pulse the trigger are suitable for actions such as **Raise Alarm** or **Send Email**.

Create smart search 2 triggers

To create a smart search 2 trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **Smart search 2**.
4. Click **OK**.
5. Select and configure the trigger:
   - To create a smart search filter to use as a trigger, see *Triggers, on page 155*.
   - Select **High processing delay** to activate the trigger whenever smart search 2 takes more than a minute to process detections.
6. Click **OK**.

Create AXIS Audio Manager triggers

To create an AXIS Audio Manager trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **Audio manager**.
4. Click **OK**.
5. Select and configure the trigger.
6. Click **OK**.

Device status changed	Select **Device status changed** to activate the trigger when the device status goes online or offline.
Playback status changed	Select **Playback status changed** to activate the trigger when playback starts or stops.
Target enabled or disabled	Select **Target enabled or disabled** to activate the trigger when the trigger target is turned on or off.
Volume controller volume changed	Select **Volume controller volume changed** to activate the trigger when the volume controller setting changes.

Add actions

One rule can have multiple actions. Actions start when the rule activates.

The following actions are available:

Record – Starts a recording from the camera. See *Create record actions*.

Raise alarm – Sends an alarm to all connected AXIS Camera Station Pro clients. See *Create raise alarm actions*.

Set output – Sets the state of an output port. Use this to control a device connected to the output port, for example, to turn on a light or lock a door. See *Create output actions*.

Send email – Sends an email to one or more recipients. See *Create send email actions*.

Live view – Opens the live view of a specific camera, view, or preset position in all connected AXIS Camera Station Pro clients. You can also use the live view action to restore open clients from the taskbar or bring them in front of other open applications. See *Create live view actions*.

Send HTTP notification – Sends an HTTP request to a camera, a door controller, or an external web server. See *Create HTTP notification actions*.

Siren and light – Triggers a siren and light pattern on a compatible device according to a preconfigured profile. See *Create siren and light actions, on page 98*.

Virtual I/O – Triggers a specific virtual input port on a device. See *Create virtual I/O actions, on page 98*

AXIS Entry Manager – Grants access, unlocks, or locks a door connected to a door controller configured by AXIS Entry Manager. See *Create AXIS Entry Manager actions, on page 99*.

Send mobile app notification – Sends a custom message to the AXIS Camera Station Mobile app. See *Create send mobile app notification actions, on page 99*.

Turn rules on or off – Turns other action rules on or off. See *Create an action that turns other action rules on or off, on page 99*.

Send to video decoder – Sends a view to a video decoder to display on a monitor for a specified amount of time. See *Create an action that sends a view to a video decoder, on page 100*

Access control – Includes door and zone actions in AXIS Camera Station Secure Entry. See *Create access control actions, on page 100*.

Create record actions

The record action starts a recording from the camera. Access and play recordings from the **Recordings** tab.

To create a record action:

1. Specify where to save the recording: go to **Configuration > Storage > Selection**.
2. Go to **Configuration > Recording and events > Action rules**.

3. Click **New**.
4. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
5. Click **Add** and select **Record**.
6. Click **OK**.
7. In **Camera**, select the camera to record from.
8. Under **Video setting**, configure profile, prebuffer, and postbuffer.
9. Under **Event setting**, select an event category for the recording, if applicable.
10. Click **OK**.

Video setting	
Profile	Select a profile from the **Profile** drop-down menu. To edit profile settings, see *Stream profiles*.
Prebuffer	Set the number of seconds before the detected motion to include in a recording.
Postbuffer	Set the number of seconds to include in the recording when the action is no longer ongoing.

Create raise alarm actions

The raise alarm action sends an alarm to all connected AXIS Camera Station Pro clients. The alarm appears in the **Alarms** tab and as a taskbar notification.You can attach a file with alarm procedures. The alarm procedure is available from the **Alarms** and **Logs** tabs.

To create a raise alarm action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Raise alarm**.
5. Click **OK**.
6. Under **Alarm message**, configure the title, description, and duration.
7. Configure the **Alarm procedure**.
   7.1. Select **On alarm show alarm procedure**.
   7.2. Click **Upload** and locate the file.
   7.3. Click **Preview** to preview the file.
   7.4. Click **OK**.

Alarm message	
Title	Enter a title for the alarm. The title appears in **Alarms** in the **Alarms** tab and in the taskbar notification.
Description	Enter a description of the alarm. The description appears in **Alarms > Description** in the **Alarms** tab and in the taskbar notification.
Duration (s)	Set the duration between 1 and 600 seconds for pop-up notifications.

Create output actions

The output action sets the state of an output port. Use this to control the device connected to the output port, for example, to turn on a light or lock a door.

Note

Add the output port to AXIS Camera Station Pro before you use an output action. See *I/O ports*.

To create an output action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Set output**.
5. Click **OK**.
6. In **Output port**, select the output port.
7. In **State on action**, select the state to set the port to. Available options depend on the port configuration.
8. Select **Pulse** to set how long the output port stays in the new state.

Note

To keep the port in the new state after the action, clear **Pulse**.

9. Click **OK**.

For as long as any trigger is active	To keep the port in the new state as long as all triggers in the rule are active, select **For as long as any trigger is active**.
Keep the state for a fixed time	To keep the port in the new state for a fixed time, select **Keep the state for a fixed time** and specify the number of seconds.

Create send email actions

The email action sends an email to one or more recipients. You can attach snapshots from cameras to the email.

Note

To send emails, you must first configure an SMTP server. See *Server settings*.

To create a send email action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Send email**.
5. Click **OK**.
6. Under **Recipients**, add email addresses:
   6.1. Enter the email address in **New Recipient** and select **To**, **Cc**, or **Bcc**.
   6.2. Click **Add**.
7. Under **Contents**, enter the email subject and message.
8. Under **Advanced**, configure attachments, number of emails, and intervals.
9. Click **OK**.

Advanced	
Attach snapshots	To attach .jpg snapshots from the cameras as attachments, select **Attach snapshots** and click **Cameras**. A list of all cameras added to AXIS Camera Station Pro appears. Click **Select all** to select all cameras or **Deselect all** to clear the selection.
Send one email for each event	To avoid sending multiple emails for the same event, select **Send one email for each event**.
Don't send another email for	To avoid sending emails too close together, select **Don't send another email for** and set the minimum time between emails from the drop-down menu.

Create live view actions

The live view action opens a specific camera, view, or preset position in the **Live view** tab across all connected AXIS Camera Station Pro clients. If the **Live view** tab shows a split view with a hotspot, the camera selected in the live view action appears in the hotspot. For more information about hotspots, see *Split view*.

You can also use the live view action to restore open AXIS Camera Station Pro clients from the taskbar or bring them in front of other open applications.

To create a live view action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Live view**.
5. Click **OK**.
6. Under **Live view actions**, configure what to show when the action is active.
7. Under **Shown in**, configure how to show the selected view.
8. Under **Bring to front**, select **On trigger bring application to front** to restore open AXIS Camera Station Pro clients from the taskbar or bring them in front of other open applications when the action starts.
9. Click **OK**.

Live view actions	
View	Select **View**, then select a view from the drop-down menu.
Camera	Select **Camera**, then select a camera from the drop-down menu. If the camera has a PTZ preset, select **Go to preset** and select an area from the drop-down menu to open a preset position.
No action	Select **No action** if you don't want to open a view.

Shown in	
Live alert tab	Select **Live alert tab** to open the selected view or camera view in the **Live alert** tab.
Hotspot in view	Select **Hotspot in view** and select a view with hotspot from the drop-down menu. If the hotspot is visible in live view when the action triggers, the camera view appears in the hotspot.

Example:
This example uses two live view actions in the same action rule.

1. Create a live view action that shows the hotspot view in the **Live alert** tab.
   1.1. Under **Live view actions**, select **View**.
   1.2. Select **Hotspot view**.
   1.3. Under **Show in**, select **Live alert tab**.
   1.4. Select **On trigger bring application to front**.
2. Create another live view action that goes to the hotspot view and shows the camera view in the hotspot.
   2.1. Under **Live view actions**, select **Camera** and then a camera view.
   2.2. Under **Show in**, select **Hotspot in view**.
   2.3. Select **Hotspot view**.

Create HTTP notification actions

The HTTP notification action sends an HTTP request to a recipient. The recipient can be a camera, door controller, external web server, or any server that can receive HTTP requests. For example, you can use HTTP notifications to turn a feature on or off in the camera, or to open, close, lock, or unlock a door connected to a door controller.

GET, POST, and PUT methods are supported.

Note

To send HTTP notifications to recipients outside the local network, you may need to adjust the AXIS Camera Station Pro server proxy settings. Contact Axis support for more information.

To create an HTTP notification action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Send HTTP Notification**.
5. Click **OK**.
6. In **URL**, enter the address to the recipient and the script that handles the request. For example: `https://192.168.254.10/cgi-bin/notify.cgi`.
7. Select **Authentication required** if the recipient requires authentication. Enter the username and password.
8. Select an authentication method.
9. Click **Advanced** to display the advanced settings.
10. Click **OK**.

Authentication method	
Digest	We recommend this option because it provides the best protection against eavesdropping.
Digest with basic as fallback	Use this option if you're unsure of which authentication method the device uses.

Advanced	
Method	Select an HTTP method from the **Method** drop-down menu.
Content type	For POST and PUT methods, select the content type from the **Content type** drop-down menu.
Body	For POST and PUT methods, enter the request body in **Body**.
Trigger data	You can also insert predefined trigger data from the drop-down menu.

Trigger data	
Type	The trigger that activated this action rule.
Source ID	Identifies the source that triggered the action rule. This is often a camera or other type of device. Not all sources have one.
Source Name	The name of the source that triggered the action rule. This is often a camera or other type of device. Not all sources have one.
Time (UTC)	The UTC date and time when the action rule was triggered.
Time (local)	The date and time of the server when the action rule was triggered.

Create virtual I/O actions

Use virtual I/O actions to activate a specific virtual input port on a device. You can use each port on a device for one action.

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Virtual I/O**.
5. Click **OK**.
6. Select the device and port you want to activate.
7. Click **OK**.

Create siren and light actions

The siren and light action activates a siren and light pattern on AXIS D4100-E Network Strobe Siren according to a configured profile.

Note

To use this action, a profile must be configured from the device's configuration page.

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Siren and light**.

5. Click **OK**.
6. Select a device from the **Device** drop-down menu.
7. Select a profile from the **Profile** drop-down menu.
8. Click **OK**.

Create AXIS Entry Manager actions

The AXIS Entry Manager action grants access, unlocks, or locks a door connected to a door controller configured by AXIS Entry Manager.

Note

The AXIS Entry Manager action is only available when AXIS A1001 Network Door Controller is available in AXIS Camera Station Pro.

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **AXIS Entry Manager**.
5. Click **OK**.
6. Select an action and the door to apply it to.
7. Click **OK**.

Create send mobile app notification actions

The send mobile app notification action sends a custom message to the AXIS Camera Station Mobile app. You can tap the received notification to go to a specific camera view. See *AXIS Camera Station Mobile app user manual*.

To create a send mobile app notification action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Send mobile app notification**.
5. Click **OK**.
6. In **Message**, enter the message to display in the mobile app.
7. Under **Click notification and go to**, configure what appears when you tap the notification.
8. Click **OK**.

Click notification and go to	
Camera	Select a camera view to show when you tap the notification.
Default	Select **Default** to go to the mobile app start page when you tap the notification.

Create an action that turns other action rules on or off

Use this action to, for example, turn off motion detection in an office when an employee swipes their access card.

To create a turn rules on or off action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Turn rules on or off**.
5. Click **OK**.
6. Select one or more action rules.
7. Choose whether you want to turn the selected action rules on or off.
8. Enter a delay to add time between the trigger and the change of state.
9. Select **Return to the previous state when the trigger is no longer active** if you don't want the action rule to stay changed when the trigger isn't active. In the example above, this means motion detection turns back on when the employee removes the access card from the reader.
10. Click **OK**.

Create a bookmark action

A bookmark action adds a bookmark to a recording at the moment the action rule triggers.

To create a bookmark action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Add bookmark**.
5. Click **OK**.
6. Configure the bookmark by entering a name and, optionally, a description.
7. Click **OK**.

Create an action that sends a view to a video decoder

Use this action to send a view to a video decoder to display on a monitor for a specified amount of time.

To create a send to video decoder action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Send to video decoder**.
5. Click **OK**.
6. In **Decoder**, select the video decoder to send the view to.
7. In **View**, select the camera or view to send.
8. In **Duration**, enter how long to display the view, in seconds.
9. Click **OK**.

Create access control actions

The access control action can perform the following actions in AXIS Camera Station Secure Entry:

- **Door actions:** grant access, lock, unlock, reset, or lockdown selected doors.
- **Zone actions:** lock, unlock, reset, or lockdown selected doors in selected zones.
- **Access rule actions:** turn access rules on or off.

Note

The access control action is only available for AXIS Camera Station Secure Entry.

To create an access control action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Access control**.
5. Click **OK**.
6. To perform door actions:
   6.1. Under **Access control**, select **Door actions**.
   6.2. Under **Configure action**, select the doors and action.
7. To perform zone actions:
   7.1. Under **Access control**, select **Zone actions**.
   7.2. Under **Configure action**, select the zones, door types, and action.
8. To turn access rules on or off:
   8.1. Under **Access control**, select **Action rule actions**.
   8.2. Under **Configure action**, select the access rule you want to turn on or off.
   8.3. Under **Action**, select **Enable** or **Disable**.
9. Click **OK**.

- To save a report as part of the action, select **Save report** and configure the report settings.

Create AXIS Audio Manager actions

The AXIS Audio Manager action controls audio playback and volume settings on connected audio devices.

To create an AXIS Audio Manager action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and configure a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Audio manager**.
5. Click **OK**.
6. Select and configure the action you want to trigger.
7. Click **OK**.

AXIS Audio Manager actions	
Play audio file	Select **Play audio file** to play a selected audio file. You can also configure playback parameters such as repeat count, priority, and visual profile.
Stop audio file	Select **Stop audio file** to stop audio playback.
Enable or disable target	Select **Enable or disable target** to turn devices on or off.
Mute volume	Select **Mute volume** to mute the volume controller.

AXIS Audio Manager actions	
Set volume	Select **Set volume** to set the volume of a volume controller. The value can be positive or negative.
Offset volume	Select **Offset volume** to adjust the volume relative to the current level. Enter a positive value to increase it, or a negative value to decrease it.

Schedules

The Schedules page contains all schedules that you can apply to recording, action rules, and components such as AXIS Secure Entry. Some schedules are created automatically during installation by AXIS Site Designer.

You can create and edit customized daily and weekly schedules, as well as override schedules. Override schedules are always daily, but you can apply them to both daily and weekly schedules on special dates such as public holidays.

The **Schedules** tab is the main view for managing all your daily and weekly schedules:

- **Name**: The schedule's name.
- **Type**: Indicates whether the schedule is a daily or weekly schedule.
- **In use**: Indicates whether a component, recording rule, or action rule is currently using the schedule.
- **Override schedules**: Lists which override schedules apply to this schedule.

The **Override schedules** tab is the main view for managing your override schedules, where you can see which daily and weekly schedules each override applies to.

Note

When connected to multiple AXIS Camera Station Pro servers, you can add and manage schedules on any connected server. Select the server from the **Selected server** drop-down menu to manage the schedules.

Manage daily and weekly schedules

To manage daily and weekly schedules, go to the **Schedules** tab.

To create a new daily or weekly schedule, click **New schedule**.

To delete a schedule, select it from the list and click **Delete**. Make sure the schedule isn't in use before deleting it.

Create or select a daily or weekly schedule to display its details.

- If it's a daily schedule, click **Add dates** to add a new date range to the schedule. You can add multiple date ranges to the same daily schedule.
- To add a time slot, either click **+** or double-click the row.
- To edit a date range or time slot, left-click it.
- To add an override schedule, select it from the drop-down menu and click **Add**. To remove an override schedule, select it from the list and click **Remove**.
- Click **Apply** to save your changes.

Manage override schedules

- To manage override schedules, go to the **Override schedules** tab.
- Click **Add dates** to add a new date range to the schedule. You can add multiple date ranges to the same override schedule.
- To add a time slot, either click **+** or double-click the row.
- To edit a date range or time slot, left-click it.

- Click **Apply** to save your changes.

Examples of action rules

Example: Door forced open

Door forced open

This example shows how to set up an action rule in AXIS Camera Station Pro that triggers a recording and an alarm when someone forces the entrance door open.

Before you start, you need to:

- Install an Axis network door controller. See *Add devices, on page 42*.
- Configure the door controller. See *Add a door, on page 133*.

Create the action rule:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Add the door forced event as the trigger:
   3.1. Click **Add** and select **Device event**.
   3.2. Click **OK**.
   3.3. Under **Configure device event trigger**, configure the trigger settings.
   3.4. Under **Filters**, configure the filter settings.
   3.5. Under **Activity**, verify that the trigger shows activity on the signal line.
   3.6. Click **OK**.
4. Click **Next**.
5. Add a record action:
   5.1. Click **Add** and select **Record**.
   5.2. Click **OK**.
   5.3. Select a camera from the **Camera** drop-down menu.
   5.4. Under **Video setting**, configure profile, prebuffer, and postbuffer.
   5.5. Click **OK**.
6. Add a raise alarm action:
   6.1. Click **Add** and select **Raise alarm**.
   6.2. Click **OK**.
   6.3. Under **Alarm message**, enter a title and description for the alarm. For example, "The main entrance is forced open".
   6.4. Click **OK**.
7. Click **Next** and select **Always** as the schedule.
8. Click **Finish**.

Configure device event trigger	
Device	Select an Axis network door controller from the **Device** drop-down menu.
Event	Select **Door > Door forced** from the **Event** drop-down menu.
Trigger period	Set 10 seconds as **Trigger period**.

Filters	
Door name	Select the door from the **Door name** drop-down menu.
Door status	Select **Forced** from the **Door status** drop-down menu.

Video settings	
Profile	Select **High** from the **Profile** drop-down menu.
Prebuffer	Set 3 seconds as **Prebuffer**.
Postbuffer	Set 5 seconds as **Postbuffer**.

Example: When an important person enters

When an important person enters

This example shows how to create an action rule in AXIS Camera Station Pro that plays a welcome message and calls the elevator when an important person enters.

Before you start, you have to:

- Install and configure an Axis network door controller, and add cardholders. See *Configure access control, on page 129* and *Access management, on page 163*.
- Install an Axis network audio device and associate it with a camera. See *Stream profiles, on page 49*.
- Install AXIS A9188 Network I/O Relay Module, connect the I/O to the elevator, and add the I/O ports of the network I/O relay module to AXIS Camera Station Pro. See *I/O ports, on page 81*.

Create the action rule:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Add the device event as the trigger:
   3.1. Click **Add** and select **Device event**.
   3.2. Click **OK**.
   3.3. Under **Configure device event trigger**, configure the event settings
   3.4. Under **Filters**, configure the filter settings.
   3.5. Under **Activity**, verify that the trigger shows activity on the signal line.
   3.6. Click **OK**.
4. Click **Next**.
5. Add a send HTTP notification action to play a welcome message:
   5.1. Click **Add** and select **Send HTTP notification**.
   5.2. Click **OK**.
   5.3. In **URL**, enter the URL of the welcome message audio clip.
   5.4. Select **Authentication required** and enter the username and password of the audio device.
   5.5. Click **OK**.
6. Add a set output action:
   6.1. Click **Add** and select **Set output**.
   6.2. Click **OK**.
   6.3. From the **Output port** drop-down menu, select the output port of the I/O module connected to the elevator.

6.4. From the **State on action** drop-down menu, select the state of the I/O module to call the elevator.

6.5. Select **Pulse** and set the duration to 60 seconds.

6.6. Click **OK**.

7. Click **Next** and select **Always** as the schedule.
8. Click **Finish**.

Configure device event trigger	
Device	Select an Axis network door controller from the **Device** drop-down menu.
Event	Select **Authorization > Access request granted** from the **Event** drop-down menu.
Trigger period	Set 10 seconds as **Trigger period**.

Filters	
Door name	Select the door from the **Door name** drop-down menu.
Door side	Select the door side from the **Door side** drop-down menu.
Card number	Select **Card number** and enter the person's card number.

Configure client

Go to **Configuration > Client** to:

- Edit client-specific settings, such as theme and language. See *Client settings, on page 105*.
- Edit user-specific settings, such as notifications and startup options. See *User settings, on page 106*.
- Edit client-specific streaming performance settings, such as video scaling and hardware decoding. See *Streaming, on page 108*.

Client settings

These settings apply to all AXIS Camera Station Pro users on the computer. Go to **Configuration > Client > Client settings**.

Theme	
System, Light, Dark	Select the theme for the client. **System** is the default for new installations. If you select **System**, the theme follows your Windows system theme.

General	
Run application when Windows starts	Turn on to run AXIS Camera Station Pro automatically when Windows starts.

Live view	
Show camera names in live views	Shows the camera names in live view.
	Turn on **Show recording indicators in live views and maps** to show an indicator for motion detection recordings or recordings started by an action rule.
	Turn on **Show event indicators in live views and maps** to show an indicator for motion detection recordings or recordings started by an action rule.

Maps	
Allow flashing coverage areas for all maps	Turn this setting on or off to control whether coverage areas flash on all maps. This global setting doesn't affect the local setting at the map level. See *Map, on page 20*.

Language
Change the language of the AXIS Camera Station Pro client. Restart the client for the change to take effect.

Feedback	
Share anonymous client usage data with Axis Communications to help improve the application and user experience	Share anonymous data with Axis to improve the user experience. To change this setting for the server, see *Server settings, on page 111*.

User settings

These settings apply to the signed-in AXIS Camera Station Pro user. Go to **Configuration > Client > User settings**.

Navigation system	
Tree view navigation system	On by default. Shows views, cameras, or both in the navigation pane.
Show in navigation	Select what to show in the drop-down menu: views, cameras, or both.
Show navigation path when navigating in view	Turn on to show the navigation path on top of the view when navigating in a split view.

Notifications	
Show taskbar notification on alarms	Turn on to show a notification in the Windows taskbar when an alarm starts.
Show taskbar notification for tasks	Turn on to show a notification in the Windows taskbar when a task is added or completed.
Show notifications in Device management	Turn on to show notifications when new firmware is available for download.
Show intercom notification window	Turn on to show a notification window when someone presses the call button on a connected intercom system.

Snapshot	
When a snapshot is taken show a message	Turn on to show a message when someone takes a snapshot.
When a snapshot is taken open the snapshot folder	Turn on to open the snapshot folder when someone takes a snapshot.
Browse	Click **Browse** to select the snapshot save folder.

Startup	
Start in full screen	Turn on to start AXIS Camera Station Pro in full screen mode.
Remember last used tabs	Turn on to start AXIS Camera Station Pro with the same open tabs, views, and camera views from when it closed last time.
Remember last used monitors	Turn on to start AXIS Camera Station Pro on the same monitor used when it closed last time.

Note

- The system saves views and camera views per tab. The system remembers them only when the client reconnects to the same server.
- The system never remember dynamic views that you drag and drop in the live view.
- When connected to multiple servers with different users, the system doesn't support **Remember last used tabs**.

Sound on alarm	
No sound	Select to play no sound when an alarm triggers.
Beep	Select to play a beep sound when an alarm triggers.
Sound file	Select and click **Browse** to use a custom sound file when an alarm triggers. Supports any file format compatible with Windows Media Player.
Play	Click to test the sound.

Sound on incoming call	
No sound	Select to play no sound when there's an incoming call.
Beep	Select to play a beep sound when there's an incoming call.
Sound file	Select and click **Browse** to use a custom sound file when there's an incoming call. Supports any file format compatible with Windows Media Player.
Play	Click to test the sound.

Features	
Show smart search 1	Shown by default. Turn off to hide Smart search 1.

Show warning dialogs	
Invalid certificate warning	Turn on to show a warning when an invalid certificate is detected.

Streaming

Go to **Configuration > Client > Streaming** to configure streaming options.

Video scaling	
Scale to best fit	Select to fit the video to the available space without cropping or changing the aspect ratio.
Fill video area (may crop parts of the video)	Select to fill the available space with video. If the aspect ratio of the available space differs from the video, the system crops the video to fit.

Hardware decoding	
Mode	• **Automatic:** Uses the graphics card to decode streams with a resolution above 3840x2160p@25fps (also known as 4K or UHD). • **On:** Uses the graphics card to decode streams with a resolution above 1920x1080p@25fps (also known as 1080p or HD). • **Off:** AXIS Camera Station Pro uses the CPU to decode video.
Graphics card	Select a graphics card from the drop-down menu.

Supported graphics cards	Decoder technology
NVIDIA	PureVideo
AMD	Unified Video Decoder (UVD)
Intel	Intel Quick Sync Video (QSV)

Note

- Hardware decoding uses your graphics card to decode video. With a high-performance graphics card, hardware decoding can improve performance and reduce CPU usage, especially when you stream high-resolution video. Hardware decoding supports H.264 and AV1 streams only.
- Cameras with a resolution below 1080p can't use hardware decoding, even if it's turned on.
- If your graphics card doesn't support 4K decoding, hardware decoding only functions on 1080p streams, even if it's turned on.
- Only one graphics card is used for hardware decoding, even on systems with multiple graphics cards.

Bandwidth usage	
Always use the stream profile Low on this client	Turn on to use the low stream profile for live view. See *Stream profiles*. This setting affects H.264 and M-JPEG video and reduces bandwidth usage.
Suspend video streams for inactive tabs	Turn on to suspend video streams in the inactive tabs. This reduces bandwidth usage.

PTZ (Pan, Tilt, Zoom)	
Select view with first click instead of starting PTZ	Turn on so that the first click in the view selects it. Subsequent clicks control PTZ.

Audio	
Push-to-talk release delay (ms)	Sets how long audio transmits from the microphone after you release the **Push-to-talk** button, in milliseconds.
Use push-to-talk for all duplex modes	Turn on to use push-to-talk for simplex, half-duplex, and full-duplex modes.
Always allow audio for intercoms	Turn on to listen and speak to intercoms even when there are no ongoing calls.

Instant replay	
Playback duration (s)	Set the playback duration time between 1 and 600 seconds to jump back in the timeline and replay the recording.

Configure connected services

Manage connected services

Connected services give you access to:

- Web client for AXIS Camera Station
- Device management
- Automatic license management
- System health monitoring

You must register your system and connect it to an organization to access these services. See *Register your system with an organization, on page 110* for more information.

Status	The status card shows the connection status between your server and the connected services, and the name of the organization you're registered with.
Disconnect	When you disconnect a server, it's still registered with the organization.

License management	Turn on **License management** to automatically synchronize your licenses. The system pushes license changes to AXIS License Manager and retrieves updated license status. Turn off **License management** to handle licenses manually, for example, if your system has no internet connection. See Manage licenses for more information. See *Manage licenses, on page 119* for more information.
Synchronize system	Turn on **Synchronize system** to automatically synchronize your devices and views with the Web client for AXIS Camera Station and AXIS Device Manager.

Register your system with an organization

To register the system:

1. Go to **Configuration** > **Connected services** > **Management**.
2. Click **Register** and follow the onscreen instructions.

For more information about registering your system, read the *AXIS Camera Station Pro Installation and migration guide*.

Firmware upgrade settings

Note

When connected to multiple AXIS Camera Station Pro servers, you can select any server from the **Selected server** drop-down menu to configure firmware upgrade settings.

1. Go to **Configuration > Connected services > Firmware upgrade settings**.
2. Under **Automatic check for updates**, configure how often and how to check for firmware updates.
3. Under **Upgrade order**, configure the order to update the devices.

Automatic check for updates	
Check for updates	Select **Every start-up** to check for available firmware versions each time the server starts. By default, AXIS Camera Station Pro is set to **Never**.
Check now	Click to check the server for available firmware versions.

Upgrade order	
Parallel	Select to upgrade all devices at the same time. This option is quicker than **Sequential** but all devices are offline at the same time.
Sequential	Select to upgrade devices one after the other. This option takes longer but the devices aren't offline at the same time. Select **Cancel remaining upgrades if one device fails** to stop the sequential upgrade.

Turn on automatic firmware check

Axis Secure Remote Access v2

Axis Secure Remote Access v2 lets you to connect to your AXIS Camera Station Pro server through an encrypted internet connection.

Note

Axis Secure Remote Access v2 is available for AXIS Camera Station Pro 6.8 or later.

To enable Axis Secure Remote Access v2:

1. Register your server with an organization. See *Register your system with an organization, on page 110*.
2. Sign in using Axis Secure Remote Access v2. See *Sign in to AXIS Secure Remote Access v2, on page 8*.

To limit access to AXIS Camera Station Pro servers only:

1. Go to **Organization > Users** in My Systems.
2. Select the user you want to configure.
3. Click **Roles and access.**
4. Assign the **ACS Pro Secure Remote Access** role. This role limits access to AXIS Camera Station Pro servers only, without access to other Axis My Systems features.

Once registered, you can manage access permissions by assigning organization user roles in Axis My Systems. For more information about AXIS Camera Station Pro user access rights, see *User permissions, on page 121*.

Cloud storage

AXIS Camera Station Cloud Storage is a licensed service for storing your recordings in the cloud. For more information, see *AXIS Camera Station Cloud Storage – User manual*.

Important

AXIS Camera Station Cloud Storage works only with AXIS Camera Station Pro version 6.18 or earlier. We recommend you export your recordings to local storage before upgrading. If you upgrade beyond version 6.18, your cloud storage service stops working, and you'll lose all data currently stored in the cloud. Security updates for version 6.18 will continue until cloud storage support is restored in a later version.

Before you can use the cloud storage service, you must register your system with connected services. After registering your system, you can manage cloud storage for your cameras in My Systems.

Configure server

Server settings

Go to **Configuration > Server > Settings**.

Note

When connected to multiple AXIS Camera Station Pro servers, select any server from the **Selected server** drop-down menu to configure the server settings.

Export	
Include audio when adding recordings to export	Select to include audio when adding recording to the export list.

Logs
Specify the number of days to keep alarms, events, and audit logs. Set a value between 7 and 1000 days. To continuously write logs to a file in real time for use with third-party systems such as Splunk, Elastic, or a SIEM tool, select **Write audit logs to file**, **Write event logs to file**, or both. The server writes log entries to `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Server\Logs`. The files are plain text and excluded from system reports.

File	Description
`AcsService.exe.audit.log.export`	Audit log entries
`AcsService.exe.event.log.export`	Event log entries

External data
Specify the number of days to keep the external data. Set a value between 1 and 1000 days.

SMTP servers

Add SMTP servers to send emails on system alarms or when an action rule triggers.

To add an SMTP server:

1. Under **SMTP servers**, click **Add**.
2. Under **Server**, configure the server address, port, authentication, and TLS protocol.
3. Under **Sender**, enter the email address and name to display as the sender.

Server	
Address	Enter the address of the SMTP server.
Port	Enter the port. 587 is the default port for SMTP TLS connections.
Use TLS	Select if the SMTP server uses TLS. TLS is the default protocol.
Use authentication	Select if the server requires a username and password, then enter your credentials.

Edit	To edit an SMTP server, select the server and click **Edit**.
Remove	To remove an SMTP server, select the server and click **Remove**. In the dialog, click **Yes** to remove the server.

Test all...	To test an SMTP server, select the server and click **Test all...**. In the dialog, enter an email address in **Recipient** and click **OK** to send a test email. The SMTP server tests for a list of results and possible actions to take.
Arrows	Select a server and use the arrows to set the order. The system contacts servers in the listed order.

Server test results	
OK	Connection to the SMTP server was successful. Verify that the recipients received the test email.
Unknown error	An unexpected error occurred while sending the email. Check that the SMTP server is operating correctly.
No contact	AXIS Camera Station Pro can't access the SMTP server. Verify that the SMTP server is working and that routers and proxy servers between AXIS Camera Station Pro and the SMTP server allow traffic.
Configuration error	TLS was requested but server doesn't support StartTLS, doesn't support authentication, or has no compatible authentication mechanism.
TLS/SSL handshake error	An error occurred during TLS/SSL negotiation, such as an invalid server certificate.
Authentication required	Server requires authentication to send email.
Authentication error	The credentials are incorrect.
Connection dropped	Connection was established, but then lost.

System alarm

A system alarm occurs when a camera loses connection, recording storage access is denied, the server shuts down unexpectedly, or recording errors occur. You can send email notifications for system alarms.

Note

To send emails, you must first add an SMTP server.

To send email on system alarms:

1. Select **Send email on system alarm to the following recipients** to set up system alarm email notifications.
2. Under **Recipients**:
   2.1. Select if the address should be in the **To**, **Cc** or **Bcc** field of the email.
   2.2. Enter the email address.
   2.3. Click **Add** to save the email address to the **Recipients** box.

Device connection	
Use hostnames instead of IP for newly added devices when possible	Use the hostname to connect to newly added devices when possible. If a hostname isn't available, the IP address is used instead.
Keep using the hostnames even if they become unreachable	Use the hostname to connect. To automatically switch to the IP address instead, clear the checkbox. You can manually select to use the hostname or IP address to connect to devices. See *Connection, on page 64*.

Language	
Change the language of the server	Changes the language of AXIS Camera Station Pro Service Control and AXIS Camera Station Secure Entry. For example, system alarms, audit log messages, and external data in the **Data search** tab. Restart the server for the change to take effect.

Body worn	
Disk **Folder**	Select the drive and folder to store rejected content from the body worn system. See *Transfer recordings to rejected content storage in the Axis body worn solution User manual* for more information.
Number of days to keep rejected content from the body worn system.	Sets the number of days to keep rejected content from the body worn system.

Feedback	
Share anonymous server usage data with Axis Communications	Select to share anonymous data with Axis to help improve the application and user experience. To change this setting for the client, see *Client settings, on page 105*.

Advanced settings

Only change these settings when instructed by Axis support. To change an advanced setting:

1. Enter the setting and its value.
2. Click **Add**.

To turn on debug logging for troubleshooting purposes, select **Enable server side debug logging**. This setting uses more disk space. The `log4net.config` file in the **ProgramData** directory overrides it.

See *Advanced server setting in the AXIS Camera Station Pro Troubleshooting guide* for more information.

Components

Components are software modules that add more capabilities to your system. The **Components** page lets you manage components and view their status.

To view the list of installed components:

1. Go to **Configuration > Server > Components**.
2. Turn on **Show components**.

Note

We consider components advanced settings. Show and manage components only after consulting Axis support.

Update AXIS Camera Station Pro

To update AXIS Camera Station Pro:

1. Go to **Configuration > Server > Update**.
2. Click **Download and install...**.

Note

- Once an update starts, whether manual or scheduled, it can't be cancelled.
- Scheduled updates start automatically.
- In a multi-server system, always update the local server last.
- When you update the local server, the client and service control close temporarily. You won't see a progress indicator while it's updating. Keep the server computer turned on until both the client and server have restarted.

Incident report

If you turn on incident report permissions, you can generate incident reports that include recordings, snapshots, and notes. See *Export incident reports, on page 30*.

To configure the settings for incident reports:

1. Go to **Configuration > Server > Incident report**.
2. Under **Location**, select where to store the incident reports.
3. From the **Export format** drop-down menu, select the format to export your recordings in.
4. Under **Categories**, add or remove the categories to group the incident reports. If configured as a variable in the server directory path, categories become folder names in the export location.
   4.1. Enter the category name in the box, for example, Accident or Theft.
   4.2. Click **Add**.
   4.3. To remove a category, select it and click **Remove**.
5. Under **Description template**, enter the information to show in **Description** when generating your incident reports. For example, "Reported by: [name, email, phone number]."
6. Click **Apply**.

Location	
Server directory path	Enter the directory path to save incident reports to a folder on the computer. You can use the server name, category, or the user name as variables. For example: `C:\Reports\$(Server Name)\$(Category)\$(User Name)\`.
Network directory path	Select to save the incident reports to a folder on a network storage. Enter the directory path or use credentials for the network storage. The share must be reachable from the AXIS Camera Station Pro server. See *Manage storage* for how to add storage to use for recordings.

Export format	
ASF	Select **Add digital signature** to help prevent image tampering. See the Digital signature section in *Export recordings*. You can also select **Use password** to use a password for the digital signature.
MP4	Exported recordings don't include audio in G.711 or G.726 format.

Scheduled export

Go to **Configuration > Server > Scheduled export** to create schedules for exporting recordings.

At the scheduled time, AXIS Camera Station Pro exports all recordings since the previous export. If the previous export is more than one week old, or if there's no previous export, only recordings from the past week are included. To export older recordings, go to the **Recordings** tab and export them manually. See *Export recordings*.

Note

When connected to multiple AXIS Camera Station Pro servers, select any server from the **Selected server** drop-down menu to manage scheduled exports.

Export scheduled recordings

1. Under **Scheduled export**, select **Enable scheduled export**.
2. Under **Cameras**, select the cameras to export recordings from. The system selects all listed cameras by default. Clear **Use all cameras** and select the specific cameras in the list.
3. Under **Export**, configure where to save the recordings, format, and creation of playlist.
4. Under **Weekly schedule**, select the time and the days to export recordings.
5. Click **Apply**.

Export	
Server directory path	Select and enter the directory path to save recordings to a folder on the computer.
Network directory path	Select to save the recordings to a folder on a network storage. Enter the directory path or use the credentials for the network storage. The share must be reachable from the AXIS Camera Station Pro server. See *Manage storage* for how to add storage to use for recordings.
Create playlist (.asx)	Select to create a playlist in the .asx format used by Windows Media Player. The recordings play in the order in which they were recorded.
Export format	Select a format to export your recordings in. **ASF** – Select **Add digital signature** to help prevent image tampering. See the Digital signature section in *Export recordings*. You can also select **Use password** to use a password for the digital signature. **MP4** – Exported recordings don't include audio in G.711 or G.726 format.

Microsoft Windows 2012 Server

To export recordings from a server running Microsoft Windows 2012 Server, install Desktop Experience:

1. Click **Start > Administrative Tools > Server Manager** to open Server Manager.
2. Select **Manage > Add Rules and Features** to start the Add Roles and Features Wizard.
3. Under **Features Summary**, select **User Interfaces and Infrastructure**.
4. Select **Desktop Experience**, click **Next**.
5. Click **Install**.

WebRTC settings

The Web client for AXIS Camera Station uses WebRTC to communicate with the server.

Enable TURN	Turns on a local TURN server on the AXIS Camera Station Pro server, allowing WebRTC communication to use a single port. This can simplify firewall configuration.
Prioritize TURN	Select to have WebRTC consider relay candidates only.

New connection

Go to ☰ > **Servers** > **New connection** to connect to an AXIS Camera Station Pro server. See *Connect to a server*.

Connection status

Go to ☰ > **Servers** > **Connection status**, to see the connection status of all servers.

Use the slider next to the server name to connect to or disconnect from the server.

Status code	Description	Possible solutions
Connecting	The client is trying to connect to this server.	
Connected	The client uses TCP while connected to this server. .	
Connected (Axis Secure Remote Access v2)	The client uses Axis Secure Remote Access v2 while connected to this server.	
Connected (HTTP)	The client uses HTTP while connected to this server. This is less efficient than TCP and slower when connected to multiple servers.	
Disconnecting	The client is disconnecting from this server. .	
Disconnected	The client isn't connected to this server.	

Reconnecting	The client lost connection to this server and is trying to reconnect.	
Reconnection failed	The server is found but the user permissions or password may have changed.	• Add the user in the **User permission** dialog. • Verify the username and password.
Login canceled	The user canceled the login.	
Incorrect username or password	Click the link in the **Action** column and enter the correct credentials.	
User not authorized on the server	The server doesn't authorize the user to log in.	Add the user in the **User permission** dialog.
Security verification failed	A WCF-related security check failed.	Synchronize the client and server computer UTC times.
No contact with server computer	The server computer didn't respond at the specified address.	• Check that the network is working properly. • Check that the server is running.
No server running	The computer running the server is accessible, but the server isn't running.	Start the server.
Communication failure	Connection to the server failed.	• Make sure the server computer is accessible. • Check that the network works properly. • Check that the server is running.
Invalid hostname	The DNS can't translate the hostname into an IP address.	• Verify that the hostname is spelled correctly. • Verify that the DNS can resolve the hostname.
Already connected to the same server	The client is already connected to this server.	Remove the duplicate server entry.
Not the expected server	A different server than expected responded at this address.	Update the server with the correct server.
Client version (x) is not compatible with server version (y)	The client is too old or too new compared to the server.	Install the same version of AXIS Camera Station Pro on both the client and the server computer.
Server too busy	The server couldn't respond because of performance issues.	Make sure the server computer and network aren't overloaded.

Multiple servers

Server lists

You can organize your AXIS Camera Station Pro servers in server lists. A server can belong to multiple server lists. You can import, export, and use server lists in other AXIS Camera Station Pro clients.

Go to ☰ > **Servers** > **Server lists**.

The default **Recent connections** list shows the servers used in the previous session. You can't remove **Recent connections**.

🗑	Select the server list and click 🗑 to delete it.
+ **New server list**	Click to add a new server list and give it a name.
Add	To add a server to a server list, select a server list and click **Add**. Enter the required information.
Export lists	Click to export all server lists in a .msl file. You can import server lists to connect to the servers. See *Connect to a server*.
Edit	To edit a server in a server list, select a server and click **Edit**. You can only edit one server at a time.
Remove	To remove a server from a server list, select it and click **Remove**.
Rename a list	Double-click the list and enter a new name.

Organize servers in server lists

Configure switch

If you have an AXIS Camera Station S22 Appliance series device, you can configure it from AXIS Camera Station Pro. Go to **Configuration > Switch > Management** and enter your credentials to open the switch management page.
To configure the switch, see the AXIS Camera Station S22 Appliance series user manual on *axis.com*.

Note

AXIS Camera Station Pro can only connect to https://192.168.0.1/, which is the default IP address of the switch.

Manage licenses

The Manage licenses page shows your current license status.

Trial	When you install AXIS Camera Station Pro you get a 90-day trial period. During this period, the system is fully functional. You can configure it and try out all the features before buying any licenses.
Check your licenses	If the system's license period expires without automatic renewal, AXIS License Manager provides a 30-day grace period.
Licensed	The system is fully licensed until the earliest expiration date.
Changes made in the system require a license synchronization	When you add devices to a licensed system, AXIS Camera Station Pro attempts to synchronize the changes with AXIS License Manager to update the system license status. If you're using automatic licensing, you might not notice this happening. If you use manual licensing and don't resynchronize within 60 days, the system becomes unlicensed.
Unlicensed	The system is operational but with limited functionality. Recording and action rules continue to work, and you won't lose any recordings. The following features won't work: • Live streams • Recordings playback • Instant playback • Snapshots • Recordings export

You can license your system in two ways:

Automatic licensing (online systems) – Your system automatically pushes changes that affect the number of licenses to AXIS License Manager and retrieves a new license status. This option requires an internet connection. See *License a system online, on page 120* for more information.

Manual licensing (offline systems) – With this option, you manually export your system file, upload it to AXIS License Manager, and import the new license. Every time you make changes to the system that affect the number of licenses, you must repeat this process. Choose this option if you prefer to handle the licenses manually, or if your system has no internet connection. See *License a system that's offline, on page 120* for more information.

License a system online

To use automatic licensing, you must register your system and connect it to an organization.

1. Go to **Configuration** > **Licenses** > **Management**.
2. Make sure **Automatic licensing** is on.
3. Click **Register...**.
4. Sign in using your My Axis account and follow the onscreen instructions.
5. Click **Go to AXIS License Manager** to manage your licenses. Read the *My Systems user manual on help.axis.com* for more information.

License a system that's offline

To license your system manually:

1. Go to **Configuration** > **Licenses** > **Management**.
2. Turn off **Automatic licensing**.
3. Click **Export system file...** and save the file to your computer.

Note

You must have an internet connection to access AXIS License Manager. If your client computer doesn't have internet, copy the system file to a computer that does.

4. Open *AXIS License Manager*.
5. In AXIS License Manager:
   5.1. Select the correct organization, or create one if you haven't already. Read the *My Systems user manual on help.axis.com* for more information.
   5.2. Go to **System setup**.
   5.3. Click **Upload system file**.
   5.4. Click **Upload system file** and select your system file.
   5.5. Click **Upload system file**.
   5.6. Click **Download license file**.
6. Go back to the AXIS Camera Station Pro client.
7. Click **Import license file...** and select your license file.
8. Click **Go to AXIS License Manager** to manage your licenses.

Configure security

User permissions

Go to **Configuration > Security > User permissions** to see the users and groups in AXIS Camera Station Pro.

Note

Administrators of the computer that runs the AXIS Camera Station Pro server are automatically granted administrator privileges in AXIS Camera Station Pro. You can't change or remove the Administrators group's privileges.

Before you can add a user or group, make sure they're registered on the local computer or have a Windows® Active Directory user account. To add users or groups, see *Add users or groups*.

When a user belongs to a group, they receivet the highest role permission assigned to them individually or to the group. For example, a user with access to camera X who also belongs to a group with access to cameras Y and Z has access to all three cameras.

	Indicates the entry is a single user.
	Indicates the entry is a group.
Name	Username as it appears in the local computer or Active Directory.
Domain	The domain that the user or group belongs to.
Role	The access role assigned to the user or group. Possible values: Administrator, Operator, and Viewer.
Details	Detailed user information as it appears on the local computer or in Active Directory.
Server	The server that the user or group belongs to.

Add users or groups

Microsoft Windows® and Active Directory users and groups can access AXIS Camera Station Pro. To add a user to AXIS Camera Station Pro, you must add users or a group to Windows®.

To add a user in Windows® 10 and 11:

- Press the Windows key + X and select **Computer Management**.
- In the **Computer Management** window, navigate to **Local Users and Groups** > **Users**.
- Right-click **Users** and select **New User**.
- In the popup dialog, enter the new user's details and clear **User must change password at next login**.
- Click **Create**.

If you use an Active Directory domain, consult your network administrator.

Add users or groups

1. Go to **Configuration > Security > User permissions**.
2. Click **Add**. The available users and groups appear in the list.
3. Under **Scope**, select where to search for users and groups.
4. Under **Show**, select to show users or groups. The search results may not appear if there are too many users or groups. Use the filter to narrow the results.
5. Select the users or groups and click **Add**.

Scope	
Server	Select to search for users or groups on the local computer.
Domain	Select to search for Active Directory users or groups.
Selected server	When connected to multiple AXIS Camera Station Pro servers, select a server to search for users or groups on that server.

Configure a user or group

1. Select a user or group in the list.
2. Under **Role**, select **Administrator**, **Operator**, or **Viewer**.
3. If you selected **Operator** or **Viewer**, you can configure the user or group privileges. See *User or group privileges*.
4. Click **Save**.

Remove a user or group

1. Select the user or group.
2. Click **Remove**.
3. In the pop-up dialog, click **OK** to remove the user or group.

User or group privileges

There are three roles you can assign to a user or group. For how to define the role for a user or group, see *Add users or groups*.

Administrator – Full access to the entire system, including access to live and recorded video of all cameras, all I/O ports, and views. This role is required to access system configuration.

Operator – Select cameras, views, and I/O ports to get access to live and recorded video. An operator has full access to all functionality of AXIS Camera Station Pro except system configuration.

Viewer – Access to live video of selected cameras, I/O ports, and views. A viewer doesn't have access to recorded video or system configuration.

Cameras

The following access privileges are available for users or groups with the **Operator** or **Viewer** role.

Access	Allow access to the camera and all camera features.
Video	Allow access to live video from the camera.
Audio listen	Allow access to listen from the camera.
Audio speak	Allow access to speak to the camera.
Manual Recording	Allow starting and stopping recordings manually.
Mechanical PTZ	Allow access to mechanical PTZ controls. Available only for cameras with mechanical PTZ.
PTZ priority	Set the PTZ priority. A lower number means a higher priority. No assigned priority is set to `0`. An administrator has the highest priority. When a role with higher priority operates a PTZ camera, others can't operate the same camera for 10 seconds by default. Available only for cameras with mechanical PTZ that have **Mechanical PTZ** selected.

Views

The following access privileges are available for users or groups with the **Operator** or **Viewer** role. You can select multiple views and set the access privileges.

Access	Allow access to the views in AXIS Camera Station Pro.
Edit	Allows editing of views in AXIS Camera Station Pro.

I/O

The following access privileges are available for users or groups with the **Operator** or **Viewer** role.

Access	Allow full access to the I/O port.
Read	Allows viewing the state of the I/O port without changing it.
Write	Allows changing the state of the I/O port.

System

You can't configure grayed-out access privileges in the list. A check mark means the user or group has this privilege by default.

The following access privileges are available for users or groups with the **Operator** role. **Take snapshots** is also available for the **Viewer** role.

Take snapshots	Allows taking snapshots in live view and recording mode.
Export recordings	Allow exporting recordings.

Generate incident report	Allow generating incident reports.
Prevent access to recordings older than	Prevent access to recordings older than the specified number of minutes. Users can't find these recordings when they search.
Access alarms, tasks, and logs	Get alarm notifications and allow access to the **Alarms and tasks** bar and **Logs** tab.
Access data search	Allow searching for data to track what happened at the time of an event.
Add categories to events	Allow adding categories to events in the **Recordings** tab.
Remove categories from event	Allow removing categories from events in the **Recordings** tab.

Access control

The following access privileges are available for users or groups with the **Operator** role. **Access Management** is also available for the **Viewer** role.

Access control configuration	Allow configuration of doors and zones, identification profiles, card formats, and PIN, encrypted communication, and multi-server.
Access management	Allow access management and access to the Active Directory settings.

AXIS Audio Manager Pro

The following access privileges are available for users or groups with the **Operator** or **Viewer** role.

Access to AXIS Audio Manager Pro component settings	Allows configuration of AXIS Audio Manager Pro in AXIS Camera Station Pro and access to the AXIS Audio Manager Pro server interface. Available for Operator only.
Access to AXIS Audio Manager Pro interface	Allows access to the AXIS Audio Manager Pro server interface. Available for Viewer only.

The following access privileges are available for users or groups with the **Viewer** role.

System health monitoring

The following access privileges are available for users or groups with the **Operator** role. **Access to system health monitoring** is also available for the **Viewer** role.

Configuration of system health monitoring	Allows configuration of system health monitoring.
Access to system health monitoring	Allows access to system health monitoring.

Certificates

To manage certificate settings for the AXIS Camera Station Pro server and connected devices, go to **Configuration > Security > Certificates**.

For information on how to turn on, delete, and view HTTPS and IEEE 802.1X certificates, see *Security, on page 63*.

AXIS Camera Station Pro can be used as:

- **Root certificate authority (CA):** AXIS Camera Station Pro uses its own root certificate to issue server certificates, with no other root CA involved.
- **Intermediate certificate authority:** Import a CA certificate and its private key into AXIS Camera Station Pro to sign and issue server certificates for Axis devices. This can be a root certificate or an intermediate CA certificate.

Note

When you uninstall AXIS Camera Station Pro, it removes its CA certificates from Windows Trusted Root Certification Authorities. It doesn't remove the imported CA certificates; these must be removed manually.

Certificate authority (CA)

A CA allows you to turn on HTTPS and IEEE 802.1X on devices without any client/server certificates in place. The AXIS Camera Station Pro CA certificate can automatically create, sign, and install client/server certificates on devices when you use HTTPS or IEEE 802.1X. You can use AXIS Camera Station Pro as the root CA, or you can import a CA certificate and let AXIS Camera Station Pro act as an intermediate CA. The system generates a root CA when you install the server.

Import	Click to import an existing CA certificate and its private key. AXIS Camera Station Pro stores the certificate password.
Generate	Click to generate a new public and private key and a self-signed CA certificate that is valid for 10 years. When you generate a new certificate authority, it replaces all component certificates and restarts the components.
View	Click to view the details of the CA certificate.
Export	Click to export the CA to a file. You can export it in two ways: • **Without the private key:** Saves the certificate in .cer or .crt format. Use this option if you only need to install the public certificate in other systems that should trust certificates signed by AXIS Camera Station Pro. • **With the private key:** Saves the CA in PKCS#12 format (.pfx or .p12). Use this option if you need to import the CA to another AXIS Camera Station Pro server. You can't import a .cer or .crt certificate into AXIS Camera Station Pro again.
Number of dates the signed client/server certificates will be valid for	Set the number of days that the automatically created client/server certificates are valid for. The maximum amount is 1095 days (three years). The CA doesn't sign certificates that are valid beyond its own expiration date.

Generate a root CA

When AXIS Camera Station Pro starts, it looks for a CA. If no CA is found, it generates a root CA automatically. It includes a self-signed root certificate and private key protected by a password. AXIS Camera Station Pro stores

the password but doesn't make it visible. A CA certificate generated by AXIS Camera Station Pro is valid for 10 years.

To manually generate a new CA to replace the old one, see *Replace a CA, on page 126*.

If you upgrade from version 5.45 or earlier with a manually installed certificate on a device, AXIS Camera Station Pro automatically uses the existing root CA to install a new certificate when the manual one expires.

Note

When you generate a CA certificate, it's added to Windows Trusted Root Certificates.

Import a CA

When you install a CA certificate from another CA, you can use AXIS Camera Station Pro as an intermediate CA. Import an existing CA consisting of a certificate and a private key to allow AXIS Camera Station Pro to sign certificates on behalf of that CA. The file must be a PKCS#12 file, the certificate must have a basic constraint (2.5.29.19) indicating that it's a CA certificate, and the certificate must be used within its validity period. To import a CA to replace the existing one, see *Replace a CA, on page 126*.

Note

- If the imported CA doesn't require a password, a dialog appears each time something requires a password. For example, when you use HTTPS or IEEE on a device, or add a device. Click **OK** to continue.
- When you import a CA certificate, it's added to Windows Trusted Root Certificates.
- When you import an intermediate CA certificate, the root certificate must already exist in the Windows certificate store. If the root certificate is missing, the import fails and an error message appears. AXIS Camera Station Pro continues to use the previous CA.
- After uninstalling AXIS Camera Station Pro, you must manually remove imported CA certificates from Windows Trusted Root Certification Authorities.

Replace a CA

To replace the CA that issues signed certificates used on devices with HTTPS connection:

1. Go to **Configuration > Security > Certificates > HTTPS**.
2. Turn off **Validate device certificate**.
3. Under **Certificate authority**, click **Generate** or **Import**.
4. Enter your password and click **OK**.
5. Select the number of valid days of the signed client/server certificates.
6. Go to **Configuration > Devices > Management**.
7. Right-click the devices and select **Security > HTTPS > Enable/Update**.
8. Go to **Configuration > Security > Certificates > HTTPS** and turn on **Validate device certificate**.

Issue custom certificate

You can create a custom certificate signed by the AXIS Camera Station Pro certificate authority. For example, you can use these certificates for external HTTPS endpoints. You must manually renew these certificates when they expire. To issue a custom certificate:

1. Go to **Configuration** > **Security** > **Certificates**.
2. Under **Issue custom certificate**, click **Issue certificate...**.
3. Enter the certificate details and click **OK**.

Issue certificate	
Common name (CN)	Identifies the certificate holder. The CN is usually the fully qualified domain name (FQDN) or IP address where you install the certificate.
Private key password	Password that protects the private key.
Duration (days)	The number of days the certificate is valid.
Server authentication	Select if you're using the certificate on a server to prove the server's identity. Typically, devices or other endpoints that AXIS Camera Station Pro connects to using HTTPS are considered server devices, and their certificates should use server authentication.
Client authentication	Select if you're using the certificate on a client to prove the client's identity before connecting to a server. For example, devices that want access to an IEEE 802.1X access-controlled network must use this certificate before entering.
Organization (O)	The certificate holder's organization.
Country code (C)	The certificate holder's country code.
DNS SAN	Dynamic name server subject alternative names. Alternative FQDNs for contacting the certificate holder. When issuing a certificate, the system automatically adds the CN as a DNS SAN. You can enter multiple addresses separated by commas, for example, address-1.com,address-2.com.
IP SAN	IP address subject alternative names. Alternative IP addresses for contacting the certificate holder. The system automatically adds the CN as an IP SAN if the CN is an IP address. You can enter multiple addresses separated by commas, for example, 192.168.1.1,192.168.1.2.

HTTPS

By default, AXIS Camera Station Pro validates the HTTPS server certificate on each connected device and won't connect to a device without a valid certificate. The server certificate must be signed by the active CA in AXIS Camera Station Pro or validated through Windows Certificate Store. AXIS Camera Station Pro also validates whether the address in the device HTTPS certificate matches the address used to communicate with the device when **Validate device address** is on.

Cameras with firmware 7.20 or later come with a self-signed certificate. These certificates aren't trusted. Instead, generate or import a CA to let AXIS Camera Station Pro issue new certificates to the devices when you use HTTPS.

Validate certificate	Turn on to connect only to devices with a valid certificate. Without certificate validation, devices with invalid certificates can connect.
Validate device address	Turn off for more stable behavior on DHCP networks that don't use hostnames. Turn on to require the addresses to match for additional security. We recommend turning on this setting only on networks where devices primarily use hostnames or have static IP addresses.

Note

- When a secure connection (HTTPS) is unavailable, you can issue a new HTTPS certificate. See *Add devices, on page 42*
- To use HTTPS, firmware 5.70 or later is required for video devices, and firmware 1.25 or later for access control and audio devices.

Limitations

- Non-default ports (other than 443) aren't supported.
- All certificates in an install batch must have same password.
- Certificate operations over unencrypted channels, such as **Basic** aren't supported. Set devices to **Encrypted & unencrypted** or **Encrypted only** to allow **Digest** communication.
- You can't turn on HTTPS on the AXIS T85 PoE+ Network switch series.

IEEE 802.1X

For AXIS Camera Station Pro IEEE 802.1X authentication, the supplicant is an Axis network device that wants to connect to the LAN. The authenticator is a network device, such as an Ethernet switch or wireless access point. The authentication server is typically a host running software that supports the RADIUS and EAP protocols.

You must import an IEEE 802.1X authentication CA certificate to turn on IEEE 802.1X. The IEEE 802.1X authentication CA certificate and IEEE 802.1X client certificate install when you turn on or update IEEE 802.1X. A certificate for the authentication can either be obtained externally, for example from the IEEE 802.1X authentication server, or generated directly in AXIS Camera Station Pro. This certificate is installed on each Axis device to verify the authentication server.

Note

To use IEEE 802.1X certificates, firmware 5.50 or later is required for video devices, and firmware 1.25 or later for access control and audio devices.

To configure IEEE 802.1X:

1. Go to **Configuration > Security > Certificates**.
2. In the **EAPOL Version** drop-down menu, select the version of Extensible Authentication Protocol (EAP) to use.
3. In the **EAP identity** drop-down menu, select the device's MAC address, the device hostname, or custom text.
4. If you selected **Custom**, enter the text to use as the EAP identity.
5. Click **Import** and select the IEEE 802.1X authentication CA certificate file.
6. In the **Common name** drop-down menu, select **Device IP address** or **Device EAP identity** as the common name in certificates created for each device.
7. Go to **Configuration > Devices > Management**.
8. Right-click the devices and select **Security > IEEE 802.1X > Enable/Update**.

Limitations

- For devices with several network adapters (such as wireless cameras), you can only turn on IEEE 802.1X for the first adapter, typically the wired connection.
- Devices that don't have the parameter `Network.Interface.I0.dot1x.Enabled` aren't supported. For example: AXIS P39 Series, AXIS T85 Series, and AXIS T87 Video Decoder
- Certificate operations over unencrypted channels, such as **Basic** aren't supported. Set devices to **Encrypted & unencrypted** or **Encrypted only** to allow **Digest** communication.

Certificate expiration warning

A warning appears when a client or server certificate has expired or is about to expire. The warning also triggers a system alarm for certain certificates. It applies to all client and server certificates, device CA certificates installed by AXIS Camera Station Pro, the AXIS Camera Station Pro CA certificate, and the IEEE 802.1X certificate. The warning appears as a message under **Status** on the **Device management** page and as an icon in the **Installed certificates** list.

Under **Certificate expiration warning**, specify how many days before expiration you want AXIS Camera Station Pro to notify you.

Certificate renewal

Renew certificate between the server and devices

Client and server certificates generated by AXIS Camera Station Pro automatically renew 7 days before the expiration warning appears. This requires HTTPS or IEEE 802.1X to be turned on for the device. To renew or update a certificate manually, see *Security, on page 63*.

Renew certificate between the server and the client

You can generate a new server certificate in the **Certificates** tab in AXIS Camera Station Pro Service Control. For instructions, see *Certificates, on page 205*.

Reset the password

1. Go to **Configuration > Security > Certificates**.
2. Turn off **Validate device certificate** so that devices using CA certificates remain accessible.
3. Under **Certificate authority**, click **Generate** and enter your password.
4. Under **Certificate authority**, click **Export** to save the CA certificate locally.
5. Go to **Configuration > Devices > Management** and turn on HTTPS on the selected devices.
6. Turn on **Validate device certificate**.

Configure access control

If you add an Axis network door controller to your system, you can configure the access control hardware in AXIS Camera Station version 6.x or later.

For a complete workflow to set up Axis network door controller in AXIS Camera Station Pro, see *Set up an Axis network door controller*.

Note

Before you start, do the following:

- Upgrade the controller's AXIS OS version under **Configuration > Devices > Management**.
- Set date and time for the controller under **Configuration > Devices > Management**.
- Turn on HTTPS on the controller under **Configuration > Devices > Management**.

Workflow to configure access control

1. To edit the predefined identification profiles or create a new one, see *Identification profiles, on page 146*.

2. To use a custom setup for card formats and PIN length, see *Card formats and PIN, on page 147*.
3. Add a door and apply an identification profile to the door. See *Add a door, on page 133*.
4. Configure the door:
   - *Add a door monitor, on page 138*
   - *Add emergency input, on page 140*
   - *Add a reader, on page 141*
   - *Add a REX device, on page 143*
5. Add a zone and add doors to the zone. See *Add a zone, on page 144*.

Device software compatibility for door controllers

Important

Keep the following in mind when you upgrade AXIS OS on your door controller:

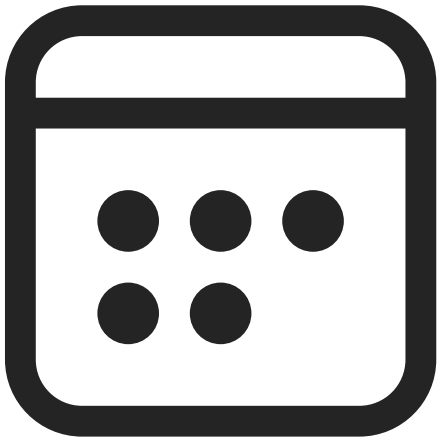
- **Supported AXIS OS versions:** The supported AXIS OS versions listed below only apply when upgrading from their original recommended AXIS Camera Station Pro version and when the system has a door configured. If the system doesn't meet these conditions, you must upgrade to the recommended AXIS OS version for the specific AXIS Camera Station Pro version.
- **Minimum supported AXIS OS version:** The oldest installed AXIS OS version in the system determines the minimum supported AXIS OS version, with a limit of two prior versions. Suppose you're using AXIS Camera Station Pro version 6.5 and upgrade all devices to the recommended AXIS OS version 12.0.86.2. Then, AXIS OS version 12.0.86.2 becomes the minimum supported version for your system moving forward.
- **Upgrading beyond recommended AXIS OS version:** Suppose you upgrade to an AXIS OS version above the recommended one for a particular AXIS Camera Station Pro version. Then, you can always downgrade back to the recommended AXIS OS version without any issues, as long as it's within the support limits set for the AXIS Camera Station Pro version.
- **Future AXIS OS recommendations:** Always follow the recommended AXIS OS version for the respective AXIS Camera Station Pro version to ensure system stability and full compatibility.
- **Track change:** Changing firmware tracks between 10.12.xx and 11.0.xx or higher requires a factory default reset.

The table below shows the minimum and recommended AXIS OS version for each AXIS Camera Station Pro version:

AXIS Camera Station version	Minimum AXIS OS version	Recommended AXIS OS version
Pro 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

Doors and zones

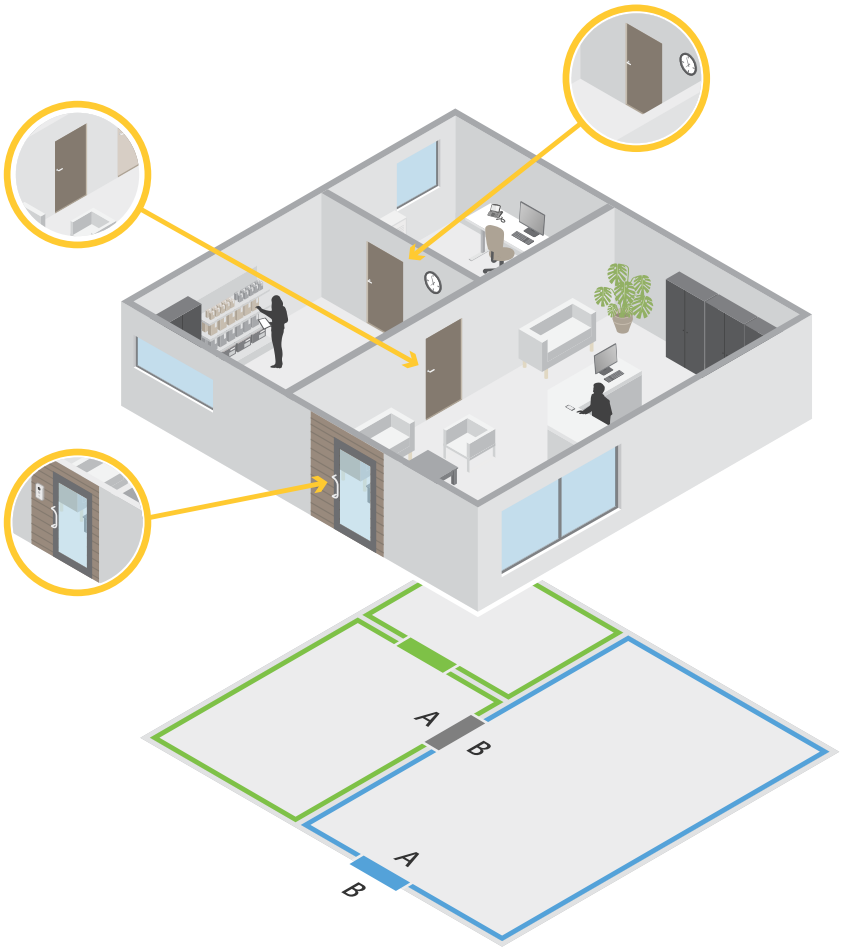
Go to **Configuration > Access control > Doors and zones** to get an overview and configure doors and zones.

 **Manual actions**	Manually set the state of a door. Select from the following options: **Reset** (follow system rules), **Grant access** (unlock door for 7 seconds), **Unlock** (keep the door unlocked), **Lock** (keep the door locked), or **Lockdown** (no one gets in or out).
 **Unlock schedules**	Set a schedule to automatically unlock doors at specific times. Doors stay locked at all other times. To require the first person to unlock the door manually before the schedule activates, turn on **First person in**.
Identification profile	Change identification profile on doors.
Pin chart	View the controller pin chart associated with a door. To print the pin chart, click **Print**.
Secure Channel	Turn on or off OSDP Secure Channel for a specific reader.

Doors	
Name	The name of the door.
Type	The type of door configuration.
Device	The device connected to the door.
IP address	The IP address of the door controller connected to the door.

Side A	The zone that side A of the door is in.
Side B	The zone that side B of the door is in.
Identification profile	The identification profile applied to the door.
Battery	The battery status of the door controller.
Status	The status of the door. • **Online:** The door is online and works correctly. • **Reader offline:** The reader in the door configuration is offline. • **Reader error:** The reader doesn't support secure channel, or it's turned off for the reader. • **Old firmware:** The device is running an outdated firmware version. Update the firmware for the best performance and security.
Zones	
Name	The name of the zone.
Number of doors	The number of doors included in the zone.
Security level	The security level applied to the zone.

Example of doors and zones



- There are two zones: green zone and blue zone.

- There are three doors: green door, blue door, and brown door.
- The green door is an internal door in the green zone.
- The blue door is a perimeter door for the blue zone only.
- The brown door is a perimeter door for both the green zone and blue zone.

Add a door

Note

- You can configure a door controller with one door that has two locks, or two doors that have one lock each. Multi-controllers support additional lock configurations.
- If a door controller has no doors and you're using a new version of AXIS Camera Station Pro with older firmware on the door controller, the system prevents you from adding a door. However, the system allows new doors on system controllers with older firmware if there's already an existing door.

To add a door:

1. Go to **Configuration > Access control > Doors and zones**.
2. Click + **Add door** and select a door type from the drop-down list.

Door types	
Door	A regular door with a door monitor that supports locks and readers. Requires a door controller.
Wireless door	A door you can configure with ASSA ABLOY Aperio® wireless locks and communication hubs. For more information, see *Add a wireless lock, on page 137*.
Monitoring door	A door that can report whether it's open or closed. For more information, see *Add a monitoring door, on page 139*.
Provisioned door	A door you can add as a placeholder in the system without selecting the hardware.
Floor	A door type for elevator control that authenticates access to elevator floors using card readers. For more information, see *Add a floor for elevator control BETA, on page 139*.

3. Enter a name for the door and select a door controller in the **Device** drop-down menu to associate with the door. The controller grays out when you can't add another door, when it's offline, or HTTPS isn't turned on.
4. Click **Next** to go to the door configuration page.
5. In the **Primary lock** drop-down menu, select a relay port.
6. To configure two locks on the door, select a relay port from the **Secondary lock** drop-down menu.
7. Select an identification profile. See *Identification profiles, on page 146*.
8. Configure the door settings. See *Door settings, on page 134*.
9. *Add a door monitor, on page 138*
10. *Add emergency input, on page 140*
11. *Add a reader, on page 141*
12. *Add a REX device, on page 143*
13. Configure the security level. See *Door security level, on page 135*.

14. Click **Save**.

Copy a door configuration:

1. Go to **Configuration > Access control > Doors and zones**.
2. Click **Add door**.
3. Enter a name for the door and select a door controller in the **Device** drop-down menu to associate with the door.
4. Click **Next**.
5. In the **Copy configuration** drop-down menu, select an existing door configuration. It shows the connected doors, and the controller grays out if it was configured with two doors or one door with two locks.
6. Change the settings if you want.
7. Click **Save**.

Add and configure doors and zones

Door settings

To edit a door:

1. Go to **Configuration > Access control > Door and Zones**.
2. Select the door you want to edit.
3. Click **Edit**.
4. Change the settings and click **Save**.

Access time (sec)	Set how many seconds the door stays unlocked after access is granted. The door locks again when it closes, even if time remains.
Open-too-long time (sec)	Only valid if you've configured a door monitor. Set how many seconds the door can stay open. If it's still open when the time runs out, the door-open-too-long alarm triggers. Set up an action rule to choose what happens when this event triggers.
Long access time (sec)	Set how many seconds the door stays unlocked after access is granted for cardholders with this setting enabled. This overrides the standard access time.
Long open-too-long time (sec)	Only valid if you've configured a door monitor. Set how many seconds the door can stay open for cardholders with **Long access time** enabled. Overrides the standard open-too-long time.
Relock delay time (ms)	Set how many milliseconds the door stays unlocked after it's opened or closed.
Relock	• **After opening:** Only valid if you added a door monitor.

	• **After closing:** Only valid if you added a door monitor.
Door forced	Select whether you want the system to trigger a system alarm when a door is forced open. Requires a door position sensor (DPS).
Door open too long	Select whether you want the system to trigger a system alarm when a door is held open too long.

To remove a door:

1. Go to **Configuration > Access control > Doors and zones > Doors**.
2. Select a door in the list.
3. Click **Remove** and confirm.

Manual actions

You can perform the following manual actions on doors and zones:

Reset – Returns to the configured system rules.

Grant access – Unlocks a door or zone for 7 seconds and then locks it again.

Unlock – Keeps the door unlocked until you reset.

Lock – Keeps the door locked until the system grants a cardholder access.

Lockdown – No one gets in or out until you reset or unlock.

To perform a manual action:

1. Go to **Configuration** > **Access control** > **Doors and zones**.
2. Select the door or zone.
3. Click any of the manual actions.

Door security level

You can add the following security features to the door:

Two-person rule – The two-person rule requires two people to use a valid credential to gain access.

Double-swipe – The double-swipe lets a cardholder override the current state of a door. For example, they can use it to lock or unlock a door outside the regular schedule, which is more convenient than unlocking the door through the system. Double-swipe doesn't affect an existing schedule. For example, if a door is scheduled to lock at closing time, and an employee leaves for lunch break, the door will still lock according to the schedule.

You can configure the security level while you're adding a new door, or apply it to an existing door.

To add **Two-person rule** to an existing door:

1. Go to **Configuration** > **Access control** > **Doors and zones**.
2. Select the door you want to configure a security level for.
3. Click **Edit**.
4. Click **Security level**.
5. Turn on **Two-person rule**.
6. Click **Apply**.

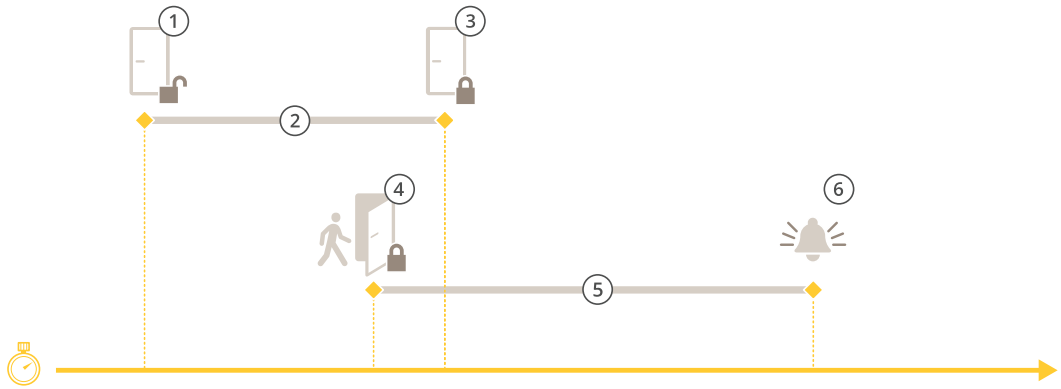
Two-person rule	
Side A and **Side B**	Select which sides of the door to use the rule on.
Schedules	Select when the rule is active.
Timeout (seconds)	Timeout is the maximum allowed time between card swipes or other types of valid credential.

To add **Double-swipe** to an existing door:

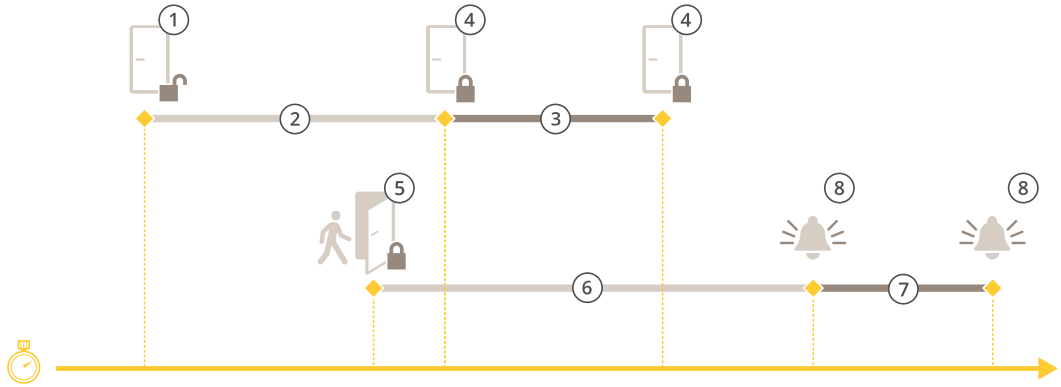
1. Go to **Configuration** > **Access control** > **Doors and zones**.
2. Select the door you want to configure a security level for.
3. Click **Edit**.
4. Click **Security level**.
5. Turn on **Double-swipe**.
6. Click **Apply**.
7. Apply **Double-swipe** to a cardholder.
   7.1. Open an **Access Management** tab.
   7.2. Click ⋮ on the cardholder you want to edit and click **Edit**.
   7.3. Click **More**.
   7.4. Select **Allow double-swipe**.
   7.5. Click **Apply**.

Double-swipe	
Timeout (seconds)	Timeout is the maximum allowed time between card swipes or other types of valid credential.

Time options



1 *Access granted - lock unlocks*
2 *Access time*
3 *No action taken - lock stays locked*
4 *Action taken (door opened) - lock locks or stays unlocked until door closes*
5 *Open-too-long time*
6 *Open-too-long alarm goes off*



1 *Access granted - lock unlocks*
2 *Access time*
3 *2+3: Long access time*
4 *No action taken - lock stays locked*
5 *Action taken (door opened) - lock locks or stays unlocked until door closes*
6 *Open-too-long time*
7 *6+7: Long open-too-long time*
8 *Open-too-long alarm goes off*

Add a wireless lock

AXIS Camera Station Pro supports the ASSA ABLOY Aperio® wireless locks and communication hubs. The wireless lock connects to the system via an Aperio communication hub connected to the door controller's RS485 connector. You can connect 16 wireless locks to one door controller.

To watch this video, go to the web version of this document.

Note

- The setup requires Axis door controller to have AXIS OS version 11.6.16.1 or later.
- The setup requires a valid license for AXIS Door Controller Extension.
- The time on the Axis door controller and the AXIS Camera Station Pro server must be synchronized.
- Before you start, use the Aperio application that ASSA ABLOY supports to pair the Aperio locks with the Aperio hub.
- You can only connect one Aperio communication hub per RS485 connector. Multi-drop isn't supported.
- Wireless locks won't follow unlock schedules when offline.

1. Access the door controller.
   1.1. Go to **Configuration > Devices > Other devices**.
   1.2. Open the web interface of the door controller connected to the Aperio communication hub.
2. Turn on AXIS Door Controller Extension.
   2.1. In the door controller web interface, go to **Apps**.
   2.2. Open AXIS Door Controller Extension context menu .
   2.3. Click **Activate license with a key** and select your license.

2.4. Turn on **AXIS Door Controller Extension**.

3. Connect the wireless lock to the door controller through the communication hub.
   3.1. In the door controller web interface, go to **Access control > Wireless locks**.
   3.2. Click **Connect communication hub**.
   3.3. Enter a name for the hub and click **Connect**.
   3.4. Click **Connect wireless lock**.
   3.5. Select the lock address and capabilities for the lock you want to add and click **Save**.
4. Add and configure the door with the wireless lock.
   4.1. In AXIS Camera Station Pro, go to **Configuration > Access control > Doors and zones**.
   4.2. Click + **Add door**.
   4.3. Select the door controller connected to the Aperio communication hub, and select **Wireless door** as **Door type**.
   4.4. Click **Next**.
   4.5. Select your **Wireless lock**.
   4.6. Define the door sides A and B, and add sensors. For more information, see *Doors and zones, on page 130*.
   4.7. Click **Save**.

Once you've connected the wireless lock, you can see its battery level and status in the overview of doors.

Battery level	Action
Good	None
Low	The lock works as intended, but you should replace the battery before the battery level becomes critical.
Critical	Replace the battery. The lock might not work as intended.

Lock status	Action
Online	None
Lock jam	Resolve any mechanical issues with the lock.

Add a door monitor

A door monitor is a position switch that tracks the physical state of a door. You can add a door monitor to your door and configure how to connect it.

1. Go to the door configuration page. See *Add a door, on page 133*.
2. Under **Sensors**, click **Add**.
3. Select **Door monitor sensor**.
4. Select the I/O port you want to connect the door monitor to.
5. Under **Door open if**, select how the door monitor circuits are connected.
6. To ignore the state changes of the digital input before it enters a new stable state, set a **Debounce time**.
7. To trigger an event when the connection between the door controller and the door monitor is interrupted, turn on **Supervised input**. See *Supervised inputs, on page 145*.

Door open if	
Circuit is open	The door monitor circuit is normally closed. The door monitor sends the door an open signal when the circuit is open. The door monitor sends the door a closed signal when the circuit is closed.
Circuit is closed	The door monitor circuit is normally open. The door monitor sends the door an open signal when the circuit is closed. The door monitor sends the door a closed signal when the circuit is open.

Add a monitoring door

A monitoring door is a door type that can show you if it's open or closed. For example, you can use this on a fire safety door that doesn't require a lock but where you need to know if the door is open.

A monitoring door is different from a regular door with a door monitor. A regular door with a door monitor supports locks and readers but requires a door controller. A monitoring door supports one door position sensor but only requires a network I/O relay module connected to a door controller. You can connect up to five door position sensors to one network I/O relay module.

Note

A monitoring door requires an AXIS A9210 Network I/O Relay Module with the latest firmware including the AXIS Monitoring Door ACAP application.

To set up a monitoring door:

1. Install your AXIS A9210 and upgrade it with the latest version of AXIS OS.
2. Install the door position sensors.
3. In AXIS Camera Station Pro, go to **Configuration** > **Access control** > **Doors and zones**.
4. Click **Add door**.
5. Enter a name.
6. Under **Type**, select **Monitoring door**.
7. Under **Device**, select your network I/O relay module.
8. Click **Next**.
9. Under **Sensors**, click + **Add** and select **Door position sensor**.
10. Select the I/O that's connected to the door position sensor.
11. Click **Add**.

Add a floor for elevator control BETA

A floor is a door type that you use to control access to elevator floors. When you add a floor, you create an elevator resource that groups all floors for that elevator. Each floor uses a card reader inside the elevator cab to authenticate users before allowing access to that floor.

Before you start, you need:

- A supported network door controller added to your system, such as *A1610*, *A1710-B*, or *A1810-B*.
- An *A9910 I/O Relay Expansion Module* for additional relays. To add your module to a controller, see .

Note

This feature is in Beta and currently supports up to 16 floors and card readers only.

To set up a floor:

1. Go to **Configuration > Access control > Doors and zones**.

2. Click **Add** and select **Floor** BETA.
3. Enter a name for the floor.
4. Select your controller.
5. Under **Elevator**, select an existing elevator or click **Create new elevator** to add a new one, then enter a name.
6. Under **Side A**, select **Card reader** and configure your reader. **Side B** can't be configured for safety reasons.
7. Click **Save and add new** to add more floors to the same elevator. The elevator and reader configuration remain filled in for the next floor. This option is only available if your controller has relays.
8. Click **Save** when you've added the floor. Floors appear as "Elevator name - Floor name", for example: "West Side - Floor 1"

Note

- Readers used on multiple floors can only be edited on the first floor they were added to.
- Elevators are automatically deleted when all related floors are deleted.

Add emergency input

You can add and configure an emergency input to initiate an action that locks or unlocks the door. You can also configure how to connect the circuit.

1. Go to the door configuration page. See *Add a door, on page 133*.
2. Under **Sensors**, click **Add**.
3. Select **Emergency input**.
4. Under **Emergency state**, select the circuit connection.
5. To ignore the state changes of the digital input before it enters a new stable state, set a **Debounce time (ms)**.
6. Select what **Emergency action** to trigger when the door receives the emergency state signal.

Emergency state	
Circuit is open	The emergency input circuit is normally closed. The emergency input sends an emergency state signal when the circuit is open.
Circuit is closed	The emergency input circuit is normally open. The emergency input sends an emergency state a signal when the circuit is closed.

Emergency action	
Unlock door	The door unlocks when it receives the emergency state signal.
Lock door	The door locks when it receives the emergency state signal.

Add an IP reader

You can use an Axis network intercom or other IP-enabled device as a reader. Before you can assign it to a door, you must add the device to AXIS Camera Station Pro.

Note

Make sure the IP reader is powered on and connected to the same network as AXIS Camera Station Pro before you start.

1. Go to **Configuration > Devices > Add devices**.
2. Select your IP reader from the list of discovered devices and click **Add**.
3. Enter the device credentials when prompted.

Once the device is added, you can assign it to a door. See *Add a reader, on page 141*.

Add a reader

You can configure a door controller to support multiple wired readers. Choose to add a reader on one side or both sides of a door.

If you apply a custom setup of card formats or PIN length to a reader, it appears in **Card formats** under **Configuration > Access control > Doors and zones**. See *Doors and zones, on page 130*.

Note

- You can also add up to 16 Bluetooth readers to a door controller. For more information, see *Add a Bluetooth reader, on page 142*.
- If you use an Axis network intercom as an IP reader, the system uses the PIN configuration set on the device webpage.

1. Go to the door configuration page. See *Add a door, on page 133*.
2. Under one side of the door, click **Add**.
3. Select **Card reader**.
4. Select the **Reader type**.
5. To use a custom PIN length for this reader.
   5.1. Click **Advanced**.
   5.2. Turn on **Custom PIN length**.
   5.3. Set the **Min PIN length**, **Max PIN length**, and **End of PIN character**.
6. To use a custom card format for this reader:
   6.1. Click **Advanced**.
   6.2. Turn on **Custom card formats**.
   6.3. Select the card formats you want to use for the reader. If a card format with the same bit length is already in use, you must deactivate it first. A warning icon appears in the client when the card format setup is different from the configured system setup.
7. Click **Add**.
8. To add a reader to the other side of the door, repeat this procedure.

For information on how install an AXIS Barcode Reader, see *Install AXIS Barcode Reader, on page 151*.

Reader type	
OSDP RS485 half duplex	For RS485 readers, select **OSDP RS485 half duplex** and a reader port.
Wiegand	For readers that use Wiegand protocols, select **Wiegand** and a reader port.
IP reader	For IP readers, select **IP reader** and select a device from the drop-down menu. You can use Axis network intercoms as an IP reader.

Wiegand	
LED control	Select **Single wire** or **Dual wire (R/G)**. Readers with dual LED control use different wires for the red and green LEDs.
Tamper alert	Select the circuit state that activates the reader tamper input. • **Open circuit**: The reader sends the door the tamper signal when the circuit is open. • **Closed circuit**: The reader sends the door the tamper signal when the circuit is closed.
Tamper debounce time	To ignore the state changes of the reader tamper input before it enters a new stable state, set a **Tamper debounce time**.
Supervised input	Turn on to trigger an event when there is interruption in the connection between the door controller and the reader. See *Supervised inputs, on page 145*.

Add a Bluetooth reader

You can use the AXIS A4612 Network Bluetooth Reader to expand the wired door limits of Axis door controllers. Up to 16 of these readers can be assigned per door controller. Each reader can manage the door lock, Request-to-Exit (REX), and Door Position Switch (DPS).

Adding and using these readers doesn't require any additional licensing.

To add an AXIS A4612 Network Bluetooth Reader to a door:

1. Make sure you have paired the AXIS A4612 with the door controller. See *Use AXIS Mobile Credential app as a Bluetooth credential, on page 142*.
2. Go to the door configuration page. See *Add a door, on page 133*.
3. Under one side of the door, click **Add**, then **Card reader**.
4. Select **IP reader** and choose the paired AXIS A4612 from the drop-down menu. If this reader is used for pairing credentials, mark it for pairing. Click **Add**.
5. In the **Overview** tab, change the identification profile. You can use the profiles **Tap in app** or **Touch reader** if you only have the AXIS A4612 attached to one side of the door and use a REX on the other.

Use AXIS Mobile Credential app as a Bluetooth credential

This example shows how to add an AXIS A4612 Bluetooth Reader to your system to allow cardholders to unlock doors using the AXIS Mobile Credential app.

1. Install the Bluetooth reader and connect it to a door controller.
2. Add the Bluetooth reader in the door controller's web interface.
   2.1. Access the door controller and go to **Peripherals** > **Readers**.
   2.2. Click **Add reader**.
   2.3. Enter the required information in the **Add Bluetooth reader** dialog.
   2.4. Click **Add**.
3. Add the Bluetooth reader to a door in AXIS Camera Station Pro.
   3.1. Go to **Configuration** > **Access control** > **Doors and zones**.
   3.2. Select the door you want to add the Bluetooth reader to and click **Edit**.

3.3. Click + **Add** on the side of the door where the Bluetooth reader is located.

3.4. Select **Card reader**.

3.5. Under **Add IP reader**, select **IP reader**.

3.6. Under **Select IP reader**, select your Bluetooth reader.

3.7. Click **Add**.

4. Select a Bluetooth reader for pairing. You must do this for at least one Bluetooth reader in your system.
   4.1. Select the Bluetooth reader you just added.
   4.2. Click **Edit**.
   4.3. Under **Edit bluetooth reader**, select **Use this reader for pairing**.
   4.4. Click **Apply**.
5. Choose the **Tap in app** or **Touch reader** identification profile. See *Identification profiles, on page 146* for more information.
6. Add the mobile credential to the cardholder. See *Add credentials, on page 164*.
7. Pair the mobile credential with the pairing reader:
   7.1. Bring the cardholder's mobile phone to the pairing-enabled Bluetooth reader.
   7.2. Follow the instructions provided in the email sent to the cardholder.

Add a REX device

You can add a request to exit (REX) device on one side or both sides of the door. A REX device can be a PIR sensor, REX button, or push bar.

1. Go to the door configuration page. See *Add a door, on page 133*.
2. Under one side of the door, click **Add**.
3. Select **REX device**.
4. Select the I/O port you want to connect the REX device to. If there's only one port available, it's selected automatically.
5. Select what **Action** to trigger when the door receives the REX signal.
6. Under **REX active**, select the door monitor circuit connection.
7. To ignore the state changes of the digital input before it enters a new stable state, set a **Debounce time (ms)**.
8. To trigger an event when the connection between the door controller and the REX device is interrupted, turn on **Supervised input**. See *Supervised inputs, on page 145*.

Action	
Unlock door	Select to unlock the door when it receives the REX signal.
None	Select to trigger no action when the door receives the REX signal.

REX active	
Circuit is open	Select if the REX circuit is normally closed. The REX device sends the signal when the circuit is open.
Circuit is closed	Select if the REX circuit is normally open. The REX device sends the signal when the circuit is closed.

Add a zone

A zone is a specific physical area with a group of doors. You can create zones and add doors to the zones. There are two types of doors:

- **Perimeter door:** Cardholders enter or leave the zone through this door.
- **Internal door:** An internal door within the zone.

Note

A perimeter door can belong to two zones. An internal door can only belong to one zone. See *Example of doors and zones, on page 132* for an overview.

1. Go to **Configuration > Access control > Doors and zones > Zones**.
2. Click **Add zone**.
3. Enter a zone name.
4. Click **Add door**.
5. Select the doors you want to add to the zone, and click **Add**.
6. The door is set as a perimeter door by default. To change it, select **Internal door** from the drop-down menu.
7. A perimeter door uses door side A as the entry side for the zone by default. To change it, select **Leave** from the drop-down menu.
8. To remove a door from the zone, select it and click **Remove**.
9. Click **Save**.

To edit a zone:

1. Go to **Configuration > Access control > Doors and zones > Zones**.
2. Select a zone in the list.
3. Click **Edit**.
4. Change the settings and click **Save**.

To remove a zone:

1. Go to **Configuration > Access control > Doors and zones > Zones**.
2. Select a zone in the list.
3. Click **Remove**.
4. Click **Yes**.

Zone security level

You can add the following security feature to a zone:

Anti-passback – Prevents people from using the same credentials as someone who entered an area before them. A person must exit the area before using their credentials again.

Note

- With anti-passback, all doors in the zone must have door position sensors so the system can register that a user opened the door after swiping their card.
- If a door controller goes offline, anti-passback works as long as all doors in the zone belong to the same door controller. However, if the doors in the zone belong to different door controllers that go offline, anti-passback stops working.

You can configure the security level while you add a new zone, or apply it to an existing zone. To add a security level to an existing zone:

1. Go to **Configuration** > **Access control** > **Doors and zones**.
2. Select the zone you want to configure a security level for.
3. Click **Edit**.
4. Click **Security level**.
5. Turn on the security features you want to add to the zone.
6. Click **Apply**.

Anti-passback	
Log violation only (Soft)	Select to allow a second person to enter using the same credentials as the first person. This option only results in a system alarm.
Deny access (Hard)	Select to prevent a second person from entering if they're using the same credentials as the first person. This option also results in a system alarm.
Timeout (seconds)	The amount of time until the system allows a user to re-enter. Enter 0 for no timeout, which means anti-passback applies until the user leaves the zone. Only use 0 timeout with **Deny access (Hard)** if all doors in the zone have readers on both sides.

Supervised inputs

Supervised inputs can trigger an event when there's an interruption in the connection to a door controller.

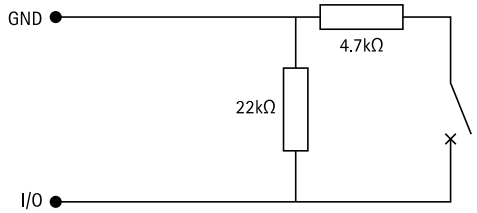
- Connection between the door controller and the door monitor. See *Add a door monitor, on page 138*.
- Connection between the door controller and the reader that uses Wiegand protocols. See *Add a reader, on page 141*.
- Connection between the door controller and the REX device. See *Add a REX device, on page 143*.

To use supervised inputs:

1. Install end of line resistors as close to the peripheral device as possible according to the connection diagram.
2. Go to the configuration page of a reader, door monitor, or REX device, turn on **Supervised input**.
3. If you followed the parallel first connection diagram, select **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor**.
4. If you followed the serial first connection diagram, select **Serial first connection**, and select a resistor value from the **Resistor values** drop-down menu.

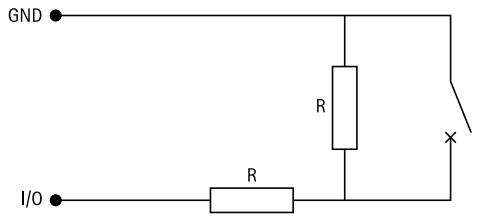
Parallel first connection

The resistor values must be 4.7 kΩ and 22 kΩ.



Serial first connection

The resistor values must be the same and within range 1-10 kΩ.



Identification profiles

An identification profile is a combination of identification types and schedules. You can apply an identification profile to one, or more, doors to set how and when a cardholder can access a door.

Note

You must use dynamic QR and PIN together.

Go to **Configuration > Access control > Identification profiles** to create, edit, or remove identification profiles.

The identification profiles available:

Card – Cardholders must swipe the card to access the door.

Card and PIN – Cardholders must swipe the card and enter the PIN to access the door.

PIN – Cardholders must enter the PIN to access the door.

Card or PIN – Cardholders must swipe the card or enter the PIN to access the door.

QR – Cardholders must show the QR Code® to camera to access the door. You can use the QR identification profile for both static and dynamic QR.

License plate – Cardholders must drive towards the camera in a vehicle with an approved license plate.

Tap in app – Cardholders must tap the credential in the AXIS Camera Station Mobile App while standing in range of the Bluetooth reader.

Touch reader – Cardholders must touch the Bluetooth reader while carrying a mobile phone with a mobile credential.

*QR Code is a registered trademark of Denso Wave Incorporated in Japan and other countries.

Create an identification profile

1. Go to **Configuration > Access control > Identification profiles**.
2. Click **Create identification profile**.
3. Enter a name for the identification profile.
4. Select **Include facility code for card validation** to use facility code as one of the credential validation fields. This field is only available if you turn on **Facility code** under **Access management > Settings**.
5. For Side A, click **Add**, select an identification type and a schedule.
   - To require cardholders to use more than one identification type, select multiple types in the same row.
   - To allow cardholders to use either type, click **Add** again and add another row.
6. For Side B, click **Add**, select an identification type and a schedule.
7. Click **OK**.

Set up identification profiles

Edit an identification profile

1. Go to **Configuration > Access control > Identification profiles**.
2. Select an identification profile and click .
3. To change the identification profile name, enter a new name.
4. Do your edits to the side of the door.
5. To edit the identification profile on the other side of the door, do the previous steps again.
6. Click **OK**.

Edit identification profile	
×	To remove an identification type and the related schedule.
Identification type	To change an identification type, select one, or more, types from the **Identification type** drop-down menu.
Schedule	To change a schedule, select one, or more, schedules from the **Schedule** drop-down menu.
+ **Add**	Add an identification type and the related schedule, click **Add** and set the identification types and schedules.

Remove an identification profile

1. Go to **Configuration > Access control > Identification profiles**.
2. Select an identification profile and click .
3. If the identification profile is used on a door, select another identification profile for the door.
4. Click **OK**.

Reset a predefined card format

1. Go to **Configuration > Access Control > Card formats and PIN**.
2. Click to reset a card format to the default field map.

Card formats and PIN

A card format defines how a card reader interprets data from a card. There are predefined card formats available to use or edit, and you can also create custom card formats

Go to **Configuration > Access Control > Card formats and PIN** to create, edit, or activate card formats. You can also configure PIN.

The custom card formats can contain the following data fields used for credential validation.

Card number – A subset of the credential binary data encoded as decimal or hexadecimal numbers. Use the card number to identify a specific card or cardholder.

Facility code – A subset of the credential binary data encoded as decimal or hexadecimal numbers. Use the facility code to identify a specific end customer or site.

PIN configuration

1. Go to **Configuration > Access Control > Card formats and PIN**.
2. Under **PIN configuration**, click .
3. Specify **Min PIN length**, **Max PIN length**, and **End of PIN character**.
4. Click **OK**.

Create a card format

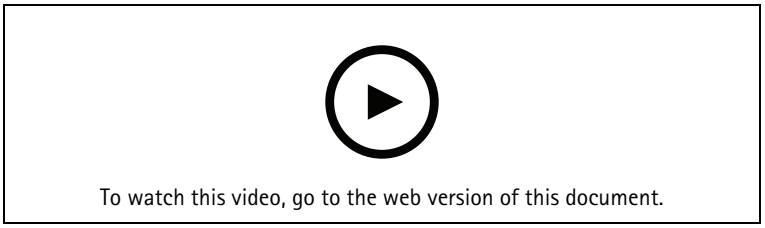
1. Go to **Configuration > Access Control > Card formats and PIN**.
2. Click **Add card format**.
3. Enter a card format name.
4. In the **Bit length** field, type a bit length between 1 and 256.
5. Select **Invert bit order** if you want to invert the bit order of the data received from the card reader.
6. Select **Invert byte order** if you want to invert the byte order of the data received from the card reader. This option is only available when you specify a bit length that you can divide by eight.
7. Select and configure the data fields to be active in the card format. Either **Card number** or **Facility code** must be active in the card format.
8. Click **OK**.
9. To activate the card format, select the checkbox in front of the card format name.

Note

- Two card formats with the same bit length can't be active at the same time. For example, if you have defined two 32-bit card formats, only one of these can be active. Deactivate the card format to active the other.
- You can only activate and deactivate card formats if the door controller has been configured with at least one reader.
- The predefined card formats can be edited but not deleted. To undo any changes to a predefined format, click the reset icon to restore it to its default settings. Card formats you've created can be deleted.

ⓘ	Click ⓘ to see an example of the output after inverting bit order.
Range	Set the bit range of the data for the data field. The range must be within what you have specified for **Bit length**.

Output format	Select the output format of the data for the data field. **Decimal**: Also known as base-10 positional numeral system, consists of the numbers 0–9. **Hexadecimal**: also known as base-16 positional numeral system, consists of 16 unique symbols: the numbers 0–9 and the letters a–f.
Bit order of subrange	Select the bit order. **Little endian**: The first bit is the smallest (least significant). **Big endian**: The first bit is the biggest (most significant).



Set up card formats

Edit a card format

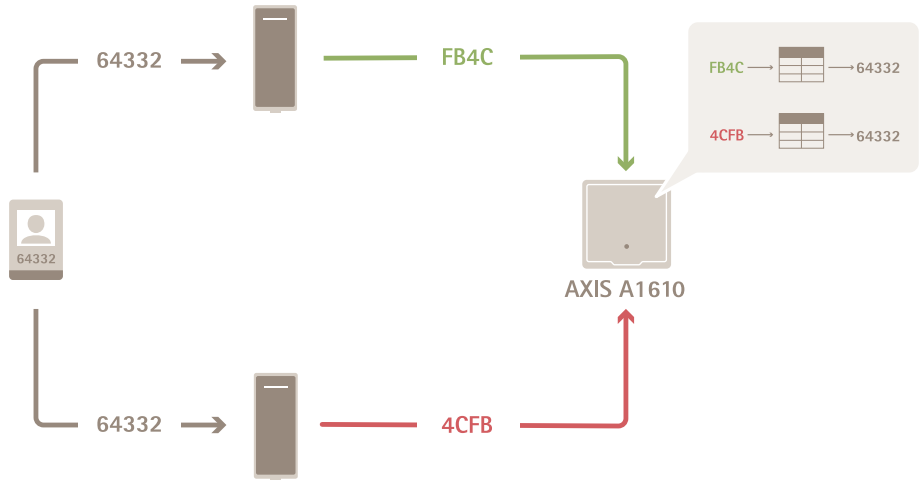
1. Go to **Configuration > Access Control > Card formats and PIN**.
2. Select a card format and click .
3. If you edit a predefined card format, you can only edit **Invert bit order** and **Invert byte order**.
4. Click **OK**.

You can only remove the custom card formats. To remove a custom card format:

1. Go to **Configuration > Access Control > Card formats and PIN**.
2. Select a custom card format, click and **Yes**.

Card format settings

Overview



- The card number in decimal is `64332`.
- One reader transfers the card number to hexadecimal number `FB4C`. The other reader transfers it to hexadecimal number `4CFB`.
- AXIS A1610 Network Door Controller receives `FB4C` and transfers it to decimal number `64332` according to the card format settings on the reader.
- AXIS A1610 Network Door Controller receives `4CFB`, changes it to `FB4C` by inverting byte order, and transfers it to decimal number `64332` according to the card format settings on the reader.

Invert bit order

After inverting bit order, the card data received from the reader is read from right to left bit by bit.

Invert byte order

A group of eight bits is a byte. After inverting byte order, the card data received from the reader is read from right to left byte by byte.

26-bit standard Wiegand card format

1 *Leading parity*
2 *Facility code*
3 *Card number*
4 *Trailing parity*

Encrypted communication

OSDP Secure Channel

AXIS Camera Station Secure Entry supports OSDP (Open Supervised Device Protocol) Secure Channel to active line encryption between controller and Axis readers.

To turn on OSDP Secure Channel for an entire system:

1. Go to **Configuration > Access control > Encrypted communication**.
2. Enter your main encryption key and click **OK**.
3. Turn on **OSDP Secure Channel**. This option is only available after you enter the main encryption key.
4. By default, the main encryption key generates an OSDP Secure Channel key. To manually set the OSDP Secure Channel key:
   4.1. Under **OSDP Secure Channel**, click .
   4.2. Clear **Use main encryption key to generate OSDP Secure Channel key**.
   4.3. Enter the OSDP Secure Channel key and click **OK**.

To turn on or turn off OSDP Secure Channel for a specific reader, see *Doors and zones*.

AXIS Barcode Reader

AXIS Barcode Reader is an application that can be installed on Axis cameras. Axis door controller uses the external peripheral authentication key to grant access and authenticate AXIS Barcode Reader and AXIS License Plate Verifier. For a complete workflow to set up AXIS License Plate Verifier in AXIS Camera Station Pro, see .

Install AXIS Barcode Reader

1. Download the application installation file from *axis.com*.
2. Go to the webpage of your Axis intercom or camera.
3. Install the application.
4. Activate the license.
5. Start the application.
6. We recommend changing the following camera setting for better QR accuracy.
   6.1. Go to camera settings.
   6.2. Under **Image > Exposure**, move the **Blur-noise trade-off** slider to the middle.

Configure AXIS Barcode Reader

1. To change the QR identification profile, go to **Configuration > Access control > Identification profiles** and click . See *Identification profiles*.
2. Add a door. See *Add a door*.
3. Select **QR** as the identification profile for this door. See *Door settings*.
4. Add a barcode reader. See *Add a reader*.
   4.1. Under one side of the door, click **Add reader**.
   4.2. Select **AXIS Barcode Reader** from the **Reader type** drop-down list. Enter a name and click **OK**.

1. To change the QR identification profile, go to **Configuration > Access control > Identification profiles** and click . See *Identification profiles*.
2. Add a door. See *Add a door*.

3. Select **QR** as the identification profile for this door. See *Door settings*.
4. Add a barcode reader. See *Add a reader*.
   4.1. Under one side of the door, click **Add reader**.
   4.2. Select **AXIS Barcode Reader** from the **Reader type** drop-down list. Enter a name and click **OK**.

Create a connection with door controller

1. In AXIS Camera Station Pro:
   1.1. Go to **Configuration > Access control > Encrypted communication**.
   1.2. Under **External Peripheral Authentication Key**, click **Show authentication key** and **Copy key**.
2. In the device web interface where AXIS Barcode Reader runs:
   2.1. Open AXIS Barcode Reader application.
   2.2. If the server certificate wasn't configured in AXIS Camera Station Pro, turn on **Ignore server certificate validation**. See *Certificates* for more information.
   2.3. If the server certificate wasn't configured in AXIS Camera Station Pro, turn on **Ignore server certificate validation**. See *Certificates* for more information.
   2.4. Turn on **AXIS Camera Station Secure Entry**.
   2.5. Click **Add** and enter the IP address of the door controller and paste the authentication key.
   2.6. Select the reader that reads barcodes from the door drop-down menu.

Multi server BETA

The connected sub servers can, with multi-server, use the global cardholders and cardholder groups from the main server.

Note

- One system can support up to 64 sub servers.
- It requires AXIS Camera Station 5.47 or later.
- It requires that the main server and sub servers are on the same network.
- On main server and sub servers, make sure to configure Windows Firewall to allow incoming TCP connections on the Secure Entry port. The default port is 55767. For customized port configuration, see *General, on page 191*.
- Connecting a sub server to a main server replaces its reader key, making any existing Bluetooth credentials invalid. To avoid this, create Bluetooth credentials on the main server instead of the sub server.

Workflow

1. Configure a server as a sub server and generate the configuration file. See *Generate the configuration file from the sub server, on page 152*.
2. Configure a server as a main server and import the configuration file of the sub servers. See *Import the configuration file to the main server, on page 153*.
3. Configure global cardholders and cardholder groups on the main server. See *Add a cardholder, on page 163* and *Add a group, on page 167*.
4. View and monitor global cardholders and cardholder groups from the sub server. See *Access management, on page 163*.

Generate the configuration file from the sub server

1. From the sub server, go to **Configuration > Access control > Multi server**.
2. Click **Sub server**.

3. Click **Generate**. It generates a configuration file in .json format.
4. Click **Download** and choose a location to save the file.

Import the configuration file to the main server

1. From the main server, go to **Configuration > Access control > Multi server**.
2. Click **Main server**.
3. Click + **Add** and go to the configuration file generated from the sub server.
4. Enter the server name, IP address, and port number of the sub server.
5. Click **Import** to add the sub server.
6. The status of the sub server shows `Connected`.

Revoke a sub server

You can only revoke a sub server before you import its configuration file to a main server.

1. From the main server, go to **Configuration > Access control > Multi server**.
2. Click **Sub server** and click **Revoke server**.
   Now you can configure this server as a main server or sub server.

Remove a sub server

After you import the configuration file of a sub server, it connects the sub server to the main server.

To remove a sub server:

1. From the main server:
   1.1. Go to **Access management > Dashboard**.
   1.2. Change the global cardholders and groups to local cardholders and groups.
   1.3. Go to **Configuration > Access control > Multi server**.
   1.4. Click **Main server** to show the sub server list.
   1.5. Select the sub server and click **Delete**.
2. From the sub server:
   - Go to **Configuration > Access control > Multi server**.
   - Click **Sub server** and **Revoke server**.

Active directory settings[BETA]

Note

User accounts in Microsoft Windows and Active Directory users and groups can access AXIS Camera Station Pro. The way you add users in Windows varies depending on your version. For more information, go to *support.microsoft.com*. Consult your network administrator if you use an Active Directory domain network.

The first time you open the Active Directory settings page you can import Microsoft Active Directory users to cardholders in AXIS Camera Station Pro. See *Import active directory users, on page 154*.

After the initial configuration, the following options appear on the Active directory settings page.

- Create and manage cardholder groups based on groups in Active Directory.
- Set up scheduled synchronization between Active Directory and the access management system.
- Manually synchronize to update all cardholders imported from Active Directory.
- Manage data mapping between user data from Active Directory and cardholder properties.

Import active directory users

To import Active Directory users to cardholders in AXIS Camera Station Pro:

1. Go to **Configuration** > **Access control** > **Active directory settings**[BETA].
2. Click **Set up import**.
3. Follow the on-screen instructions to complete these three main steps:
   3.1. Select a user from Active Directory to use as a template for data mapping.
   3.2. Map user data from the Active Directory database to cardholder properties.
   3.3. Create a new cardholder group in the access management system and select which Active Directory groups to import.

You can't change any of the imported user data, but you can add credentials to an imported cardholder, see *Add credentials, on page 164*.

Important

If you deactivate a user in Active Directory, AXIS Camera Station Pro permanently deletes the cardholder and all related data, including their history. This can't be undone. To block a cardholder's access without losing their data, suspend them in AXIS Camera Station Pro instead of deactivating them in Active Directory.

Configure AXIS Audio Manager Pro

You can connect to an AXIS Audio Manager Pro server and use its connected audio devices in AXIS Camera Station Pro.

This setup requires AXIS Camera Station Pro 6.12 or higher and AXIS Audio Manager Pro 5.0 or higher. Both servers must be set up, either on the same server or on different machines on the same network.

Important

If you have both AXIS Camera Station Pro and AXIS Audio Manager Pro running on the same server, both use port 443 by default. To prevent connection issues, configure one of them to use a different port.

You can change the port configuration in AXIS Camera Station Pro through *General, on page 191*. For information about how to change the port configuration in AXIS Audio Manager Pro, see *AXIS Audio Manager Pro — User manual*.

To get started with AXIS Audio Manager Pro in AXIS Camera Station Pro:

1. In AXIS Audio Manager Pro:
   1.1. Go to **System settings** > **API access**.
   1.2. Turn on the API and enter a username and password.
2. In AXIS Camera Station Pro:
   2.1. Go to **Configuration** > **AXIS Audio Manager Pro** and click **Connect** to set up a connection to your AXIS Audio Manager Pro server.
   2.2. In the popup dialog, enter the **Server URL**, **API username**, and **API password** of your AXIS Audio Manager Pro server and click **Connect**.

When the connection is established, you can:

- View the **Server status** of the AXIS Audio Manager Pro server and **Device status** of devices connected to that server.
- Open a new AXIS Audio Manager Pro tab to access the server's web interface.
- Use new audio-related features in AXIS Camera Station Pro.

For more information, see *AXIS Audio Manager Pro, on page 183*.

Note

To avoid certificate-related issues, we recommend that you create or obtain a certificate from a trusted Certificate Authority (CA), upload it to AXIS Audio Manager Pro, and add it to the AXIS Camera Station Pro server's trusted certificate list. For more information, see *AXIS Audio Manager Pro — User manual*.

Configure smart search 2

With smart search 2, you can set filters to find people and vehicles of interest in recordings from Axis cameras.

For requirements, limitations, and how to use smart search 2, see *Smart search 2, on page 34*.

1. Go to **Configuration > Smart search 2 > Settings**.
2. Under **Cameras**:
   2.1. Select the cameras that should send metadata to smart search 2.
   2.2. To allow server classification in the background for a camera, select **Allow** under **Background server classification**.
   This increases the server load but improves the user experience.
   2.3. To limit the number of detections saved on the server, under **Filter**, click ⚙ and create filters for **Area**, **Size and duration**, and **Swaying objects**.
   You can use these filters to exclude areas, small objects, or objects that only appear for a very short time, or swaying objects such as foliage.
   The smart search filters use any existing motion setting filters as a starting point.
3. Under **Storage**:
   – Select the drive and folder to store the detections and click **Apply**.
   – Set the storage size limit and click **Apply**. When the storage reaches its limit, it removes the oldest detections.
4. Select **Include periods with missing metadata** to display results where no metadata was recorded.
5. Select **Let the server classify detections when you start a search** to get more detailed search results, including detections the camera didn't classify. For faster search results, keep this option turned off.

Background server classification	
	Server classification status from the last hour when the server classification is slow. Appears when fewer than 95% of detections are classified.
	Server classification status from the last hour when the server classification is slow. Appears when fewer than 50% of detections are classified.

Triggers

You can configure smart search filters as triggers in action rules. To create a smart search trigger:

1. Go to **Configuration** > **Smart search 2** > **Triggers**.
2. Click **Create**.
3. Set up your filter. For more information about smart search filters, see *Search with filters, on page 34*.

4. Click **Next**.
5. Adjust the **Confidence** level of detections. A higher confidence level filters out uncertain classifications, reducing the number of detections.
6. Click **Next**.
7. Enter a name for your trigger and click **Save**.

Note

- Smart search 2 typically needs a few seconds after an object has left the camera's view to analyze the footage and verify the detection. For example, if you've set an action rule to trigger on the detection of a red car, the action only triggers a few seconds after the object leaves the camera's view.
- **Visual similarity** is not available as an option for smart search 2 triggers.
- Creating a trigger for a camera allows the server to process object detections even if **Enable background processing** is turned off for that camera.
- **Delayed detection periods** are periods with a high processing delay that cause action rules to trigger late. If this occurs frequently, you can reconfigure your trigger filter to have fewer cameras and use camera filters such as line crossing, area, size, and duration to reduce processing delays.

To use the smart search 2 trigger in an action rule, see *Create smart search 2 triggers, on page 92*.

Configure System Health Monitoring BETA

Note

- When connected to multiple AXIS Camera Station Pro servers, you can configure System Health Monitoring on any connected server. To do this, select the server from the **Selected server** drop-down menu.
- If you manage systems on different networks, Server monitoring in My Systems provides the same functionality but through the cloud.

Settings

Cloud connection	If you've registered your server with an organization, you can view your system health data from anywhere. If you're not yet connected, click **Manage** and follow the onscreen instructions.
Data retrieval frequency	Select a lower data frequency to resolve warnings about old data or general performance issues. In a multisystem setup, we recommend using the same setting or higher for a subsystem as for its parent system. • **Low** - For systems with over 100 devices. • **Medium** - For systems with 25–100 devices. • **High** - For systems with fewer than 25 devices.

Notifications

To send email notifications:

1. Configure an SMTP server and an email address to send the notifications. See *Server settings, on page 111*
2. Configure the email addresses to receive the notifications. See *Configure email recipients, on page 157*.
3. Configure the notification rules. See *Configure notification rules, on page 157*.

Configure email recipients

1. Go to **Configuration > System Health Monitoring > Notifications**.
2. Under **Email recipients**, enter an email address and click **Save**. Repeat to add multiple email recipients.
3. To test the SMTP server, click **Send test email**. A message confirms that the test email was sent.

Configure notification rules

There are two notification rules turned on by default.

System down – Send a notification when the system in a single system setup or any system in a multisystem setup is down longer than normal.

Device down – Send a notification when a device listed in System Health Monitoring is down longer than normal.

1. Go to **Configuration > System Health Monitoring > Notifications**.
2. Under **Notification rules**, turn the notification rules on or off.
3. Under **Applied rules**, you can see a list of systems and devices and the notification rules applied to them.

Multisystem

With System Health Monitoring, you can monitor the health data of several secondary systems from one main system.

1. In a secondary system, generate the system configuration. See *Generate system configuration, on page 157*.
2. In the main system, upload the system configuration. See *Retrieve data from other systems, on page 158*.
3. Repeat the previous steps in other secondary systems.
4. Monitor the health data from multiple systems from the main system. See *System Health Monitoring BETA, on page 174*.

Generate system configuration

1. Go to **Configuration > System Health Monitoring > Multisystem**.
2. Click **Generate**.
3. Click **Copy** to copy it for upload to the main system.
4. To view the system configuration details, click **Show details**.
5. To regenerate the system configuration, first click **Delete** to delete the existing one.

After uploading the system configuration to the main system, the main system information appears under **Systems with access**.

Retrieve data from other systems

After generating and copying the system configuration of a secondary system, you can upload it to the main system.

1. In the main system, go to **Configuration > System Health Monitoring > Multisystem**.
2. Click **Paste** to add the information you copied from the secondary system.
3. Check the host IP address and click **Add**.
   The secondary system appears under **Available systems**.

Configure analytics

AXIS Data Insights Dashboard

The AXIS Data Insights Dashboard presents the analytics data from your devices in graphs and charts. The configuration page for AXIS Data Insights Dashboard shows all supported applications and configured scenarios on the devices in your system. Go to **Analytics** > **Data Insights Dashboard** to:

- View a list of cameras and data sources running the supported applications.
- View a list of supported applications and scenarios for each device or data source. The following applications and scenarios are supported:
  - AXIS Object Analytics: Crossline counting and Occupancy in area
  - AXIS Audio Analytics
  - AXIS Image Health Analytics
  - AXIS People Counter
  - AXIS P8815-2 3D Counter
  - AXIS Air Quality Sensors (Air Quality Monitor)

  Note

  You can store a maximum of 100 MB of data, which limits storage time. For example, an air quality sensor monitoring all 12 data types results in around 430 days of retention time.
- Choose which scenarios to include in the dashboard.
- Tag scenarios to filter data in the dashboard, for example, to group cameras in the same location.

Note

To display AXIS Object Analytics crossline counting data in the **In and Out counting** dashboard, choose the scenario direction by selecting **In** or **Out** in the **Direction** field.

- View the status of scenarios.

Include	Turn on the switch in the **Include** column to show data from a scenario in a dashboard.
Tags	Select tags from the drop-down menu in the **Tags** column to add them to a scenario.

To add a new tag:

1. Open the **Tags** tab.
2. Enter a name for the tag.
3. Click the arrow.

Note

- AXIS Data Insights Dashboard requires TLS version 1.2 or higher for encrypted connections on your Windows server.
- AXIS Data Insights Dashboard overrides any existing MQTT settings on a camera if:
  - The camera doesn't have a configured MQTT client.
  - You manually turn on a scenario for a camera connected to another AXIS Camera Station Pro server.
- While connected to the AXIS Data Insights Dashboard, the MQTT client on the camera is dedicated to the Data Insights Dashboard.
- The cameras and the AXIS Camera Station Pro server must be on the same network.
- For optimal performance, we recommend a server with a minimum of 16 GB of RAM to run the AXIS Data Insights Dashboard in AXIS Camera Station Pro.
- You can store a maximum of 100 MB of data, resulting in a limited storage time. For example:
  - Estimation occupancy in a parking lot equipped with four cameras, each configured to detect five vehicle subclasses such as cars and bikes 24/7, results in 260 days of retention time.
  - People counting in a retail environment equipped with eight cameras where people flow continuously for 12 hours results in about 1270 days of retention time.
  - A camera running a crossline counting scenario with six classes where counting runs continuously for 24 hours results in around 860 days of retention time.

For information about adding a dashboard to a split view, see *AXIS Data Insights Dashboard in a split view, on page 18*.

How to enable the AXIS Data Insights Dashboard

License plate verifier

On the License plate verifier page, you can view the status of AXIS License Plate Verifier on your cameras and group cameras for easier list management.

The **Cameras** tab contains a list of all connected devices with AXIS License Plate Verifier installed:

- **Camera**: The camera's name.
- **Version**: Which version of AXIS License Plate Verifier is installed on the camera.
- **Status**: The current status of AXIS License Plate Verifier.
- **Latest event**: The time of the latest event captured by the camera.
- **Allowed**: The number of license plates included in the camera's 'Allowed' list.
- **Blocked**: The number of license plates included in the camera's 'Blocked' list.
- **Custom**: The amount of license plates included in the camera's 'Custom' list.
- **Group**: Which group the camera belongs to.

The **Groups** tab lists all your camera groups and the cameras in each group. In this tab, you can:

- Click **New...** to add a new group.
- Click **Delete** to delete an existing group.

- Rename a selected group in the **Group name** field
- Click **Add...** to add a camera in the selected group.
- Click **Remove** to remove a camera from a group.

You can create shared lists for grouped cameras. For more information, see *License plate management, on page 182*.

Configure body worn

Connect a body worn system

Connect your body worn system to AXIS Camera Station Pro to transfer recordings and metadata from body worn cameras.

1. Go to **Configuration > Body worn > Connect a body worn system**.
2. Under **Connection method**, select how you want to connect:
   - **Connect directly**: Enter the Body Worn Manager's IP address and credentials.
   - **Generate connection file**: Create a configuration file to upload to your Body Worn Manager.

Note

Before you create the connection file, renew the server certificate if the server IP address has changed, or AXIS Camera Station was upgraded from a version earlier than 5.33. For how to renew the certificate, see *Certificates, on page 124*.

If you selected **Connect directly:**

3. Under **Configure direct connection**, enter the **IP address**, **User name**, and **Password** for your Body Worn Manager.

1. Optionally, change the **AXIS Camera Station system name**. This name identifies the destination for copied and transferred recordings.
2. If you want to end all existing connections, select **End existing connections**. Upload the new connection file to each AXIS Body Worn System controller.
3. Click **Connect**.

If you selected **Generate connection file**:

4. Under **Generate connection file**, optionally change the **AXIS Camera Station system name**. This helps you identify where recordings are copied or transferred to.
   4.1. If you want to end all existing connections, select **End existing connections**. Upload the new connection file to each AXIS Body Worn System controller.
   4.2. Click **Export** and save the connection file.
   4.3. Upload the connection file to your Body Worn Manager.

To watch this video, go to the web version of this document.

Set up an Axis body worn system

To watch this video, go to the web version of this document.

Playback and export Axis body worn camera recordings

Snapshots

Export snapshots automatically from body worn bookmarks to a folder when recordings transfer to AXIS Camera Station Pro.

1. Go to **Configuration > Body worn > Snapshots**.
2. In **Storage location**, enter the folder path where you want to save snapshots.
3. Click **Apply**.
4. Turn on **Snapshot export**.

CAD integration

Integrate your Computer-aided Dispatch (CAD) system to automatically categorize body worn camera recordings based on dispatch data.

To set up the integration:

1. Go to **Configuration > Body worn > CAD integration**.
2. Click **Set up integration**.
3. Select your file format (CSV or XML) and click **Next**.
4. Turn on **Shared network drive** if your CAD file is on a shared network drive.
5. Enter the folder path of the CAD file, file name (CSV only), and column separator.
6. Click **Next**.
7. Map each field to the identifier as it appears in your CAD file:
   - **Officer name**: must match the virtual camera names in AXIS Camera Station Pro. If the name doesn't match, update it in Body Worn Manager, not in AXIS Camera Station Pro.
   - **Event ID**: unique dispatch identifier.
   - **Call category**: recording category. If it doesn't exist, it'll be created.
   - **Dispatch time**: start time in RFC 3339 format, for example., "2025-11-25T09:49:17+01:00".
   - **Clearance time**: end time in RFC 3339 format.
   - **Case number**: the case ID connected to the dispatch. The column must exist in the file, but the value can be left empty.
8. Click **Finish**, then **Apply**.
9. To review your recordings, click + and select **CAD recordings** to see all automatically categorized recordings. You can filter by time or officer name.

Note

If new categories are created automatically, you must manually set their retention times.

Limitations

Information might be lost if:

- AXIS Camera Station Pro or the component isn't running.
- Export files are larger than 1 GB.
- Network credentials need updating.

Body worn settings

Configure storage locations for body worn recordings.

Recording storage

Select a default storage location for body worn recordings for new system users:

1. Go to **Configuration > Body worn > Body worn settings**.
2. Under **Recording storage**, select a disk from the **Disk** drop-down.
3. Click **Save**.

Rejected recordings storage
Select where to store rejected content from the body worn system:

1. Under **Rejected recordings storage**, select a disk from the **Disk** drop-down and enter a **Folder** name.
2. Set the number of days to keep rejected content in **Number of days to keep rejected content from the body worn system**.
3. Click **Save**.

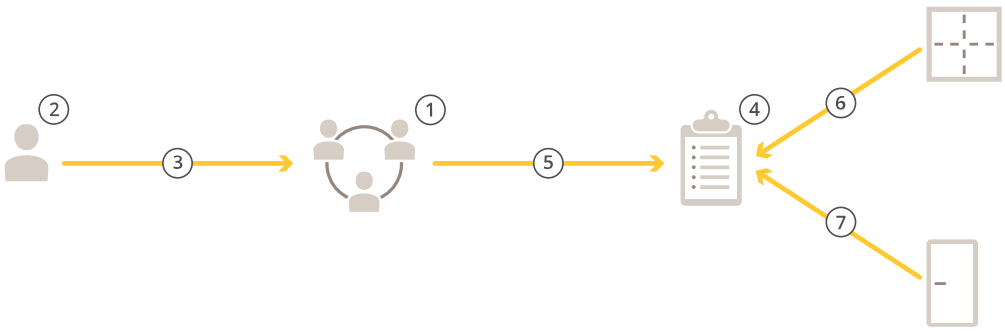
Access management

Use the **Access management** tab to configure and manage the system's cardholders, groups, and access rules.

For a complete workflow to set up Axis network door controller in AXIS Camera Station Pro, see *Set up an Axis network door controller*.

Workflow of access management

The access management structure is flexible, so you can develop a workflow that suits your needs. Example workflow:



1. *Add a group, on page 167*.
2. *Add a cardholder, on page 163*.
3. Add cardholders to groups.
4. *Add an access rule, on page 167*.
5. Apply groups to access rules.
6. Apply zones to access rules.
7. Apply doors to access rules.

Add a cardholder

A cardholder is a person with a unique ID registered in the system. Configure a cardholder with credentials that identify the person and define when and how they can access doors.

You can also map users in an Active Directory database as cardholders. See *Active directory settings*[BETA], *on page 153*.

1. Open an Access management tab.
2. Go to **Cardholder management** > **Cardholders** and click **Add**.
3. Enter the first and last name of the cardholder. Optionally, add more details to the cardholder:
   - In **Email**, enter the cardholder's email address.
   - Under **Groups**, select the groups you want to add the cardholder to.
   - Under **Access rules**, select the access rules you want to apply to the cardholder.
4. To add a photo, click **Cardholder picture** and select:
   - **Upload** to add an image from your device.
   - **Capture** to take a photo directly using your camera.

Note

The image must be a JPG, PNG, or GIF file. Images are automatically resized to a maximum of 700x700 pixels and converted to JPG.

5. Click **Advanced** to configure additional options.
6. Add a credential to the cardholder. See *Add credentials, on page 164*.
7. Click **Save**.
8. To print badges, select one or more cardholders and click **Print Badge**[BETA]. For more information, see *Print badge [BETA], on page 172*.

Use the search field to find a cardholder by first or last name. To filter by source, click **Filter** and select **Local**, **Global**, **AD**, or **Center**.

Advanced	
Long access time	Select to give the cardholder long access time and a long open-too-long time when there is an installed door monitor.
Suspend cardholder	Select to suspend the cardholder. This temporarily removes all access from the cardholder.
Allow double swipe	Select to allow a cardholder to override the current state of a door. For example, the cardholder can use this to unlock a door outside the regular schedule.
Exempt from lockdown	Select to give the cardholder access during lockdown.
Exempt from anti-passback	Select to give a cardholder an exemption from the anti-passback rule. Anti-passback prevents people from using the same credentials as someone who entered an area before them. The first person must first exit the area before their credentials can be used again.
Global cardholder	Select to make it possible to view and monitor the cardholder on the sub servers. This option is only available for cardholders created on the main server. See *Multi server [BETA], on page 152*.

Add cardholders and groups

Add credentials

You can add the following types of credentials to a cardholder:

- *QR-code credential, on page 165*
- *PIN credential, on page 165*
- *Mobile credential, on page 165*
- *Card credential, on page 166*
- *License plate credential, on page 166*

Expiration date	
Valid from	Set a date and time for the credential to become valid.
Valid to	Select an option from the drop-down menu.

Valid to	
No end date	The credential never expires.
Date	Set a date and time when the credential expires.
From first use	Select how long after the first use the credential expires. Select days, months, years, or number of times after the first use.
From last use	Select how long after the last use the credential expires. Select days, months, or years after the last use.

QR-code credential

Note

Using QR codes as credentials requires that the time on the system controller and the camera with AXIS Barcode Reader are synchronized. We recommend using the same time source for both devices to keep the time synchronized.

To add a QR-code credential to a cardholder:

1. Under **Credentials**, click + **Add** and select **QR-code**.
2. Enter a name for the credential.
3. Dynamic QR is on by default. You must use it with a PIN credential.
4. Set the start and end date for the credential.
5. To email the QR-code automatically after you save the cardholder, select **Send QR-code to cardholder when credential is saved**.
6. Click **Add**.

PIN credential

To add a PIN credential to a cardholder:

1. Under **Credentials**, click + **Add** and select **PIN**.
2. Enter a PIN.
3. Optionally, to trigger a silent alarm with a separate PIN, turn on **Duress PIN** and enter a duress PIN.
4. Set the **Valid from** and **Valid to** dates for the credential.
5. Click **Add**.

Mobile credential

Note

The cardholder must have an email address to receive the mobile credential.

To add a mobile credential to a cardholder:

1. Under **Credentials**, click + **Add** and select **Mobile credential**.
2. Enter a name for the credential.

3. Set the start and end date for the credential.
4. Select **Send the mobile credential to the cardholder after saving**. The cardholder receives an email with instructions for pairing.
5. Click **Add**.

For an example, see *Use AXIS Mobile Credential app as a Bluetooth credential, on page 142*.

Card credential

To add a card credential to a cardholder:

1. Under **Credentials**, click **Add** and select **Card**.
2. To manually enter the card data, provide a card name, card number, and bit length.

Note

Bit length is configurable only when you create a card format with a specific bit length that isn't already defined in the system.

3. To automatically get the card data for the last swiped card:
   3.1. Select a door from the **Select reader** drop-down menu.
   3.2. Swipe the card on the reader connected to that door.
   3.3. Click **Get last swiped card data from the door's readers**.

Note

You can use a 2N desktop USB card reader to get the card data. For more information, see *Set up 2N desktop USB card reader*.

4. Enter a facility code. This field is only available if you've turned on **Facility code** under **Access management > Settings**.
5. Set the start and end date for the credential.
6. Click **Add**.

License plate credential

To add a license plate credential to a cardholder:

1. Under **Credentials**, click **Add** and select **License plate**.
2. Enter a credential name that describes the vehicle.
3. Enter the license plate number for the vehicle.
4. Set the start and end date for the credential.
5. Click **Add**.

Use license plate number as a credential

This example shows you how to use a door controller, a camera with AXIS License Plate Verifier, and a vehicle's license plate number as credentials to grant access.

1. Add the door controller and the camera to AXIS Camera Station Pro. See *Add devices, on page 5*.
2. Upgrade the firmware on the new devices to the latest available version. See *Upgrade firmware, on page 61*.
3. Add a new door connected to your door controller. See *Add a door, on page 133*.
   3.1. Add a reader on **Side A**. See *Add a reader, on page 141*.
   3.2. Under **Door settings**, select **AXIS License Plate Verifier** as **Reader type** and enter a name for the reader.
   3.3. Optionally, add a reader or REX device on **Side B**.

3.4. Click **Ok**.

4. Install and activate AXIS License Plate Verifier on your camera. See the *AXIS License Plate Verifier* user manual.
5. Start AXIS License Plate Verifier.
6. Configure AXIS License Plate Verifier.
   6.1. Go to **Configuration > Access control > Encrypted communication**.
   6.2. Under **External Peripheral Authentication Key**, click **Show authentication key** and **Copy key**.
   6.3. Open AXIS License Plate Verifier from the camera's web interface.
   6.4. Skip the setup wizard.
   6.5. Go to **Settings**.
   6.6. Under **Access control**, select **Secure Entry** as **Type**.
   6.7. In **IP address**, enter the IP address for the door controller.
   6.8. In **Authentication key**, paste the authentication key that you copied earlier.
   6.9. Click **Connect**.
   6.10. Under **Door controller name**, select your door controller.
   6.11. Under **Reader name**, select the reader you added earlier.
   6.12. Turn on integration.
7. Add the cardholder you want to grant access. See *Add a cardholder, on page 163*
8. Add license plate credentials to the new cardholder. See *Add credentials, on page 164*
9. Add an access rule. See *Add an access rule, on page 167*.
   9.1. Add a schedule.
   9.2. Add the cardholder you want to grant license plate access.
   9.3. Add the door with the AXIS License Plate Verifier reader.

Add a group

Groups let you manage cardholders and their access rules together.

1. Open an Access management tab.
2. Go to **Cardholder management** > **Groups** and click **Add**.
3. Enter a name and optionally initials for the group.
4. Select **Global group** to view and monitor cardholders on the sub-servers. This option is only available for cardholders created on the main server. See *Multi server BETA, on page 152*.
5. Add cardholders to the group:
   5.1. Click **Add**.
   5.2. Select the cardholders you want to add and click **Add**.
6. Click **Save**.
7. To print badges for all cardholders in a group, select the group and click **Print Badge**BETA. For more information, see *Print badge BETA, on page 172*.

Add an access rule

An access rule defines the conditions that must be met to grant access.

An access rule consists of:

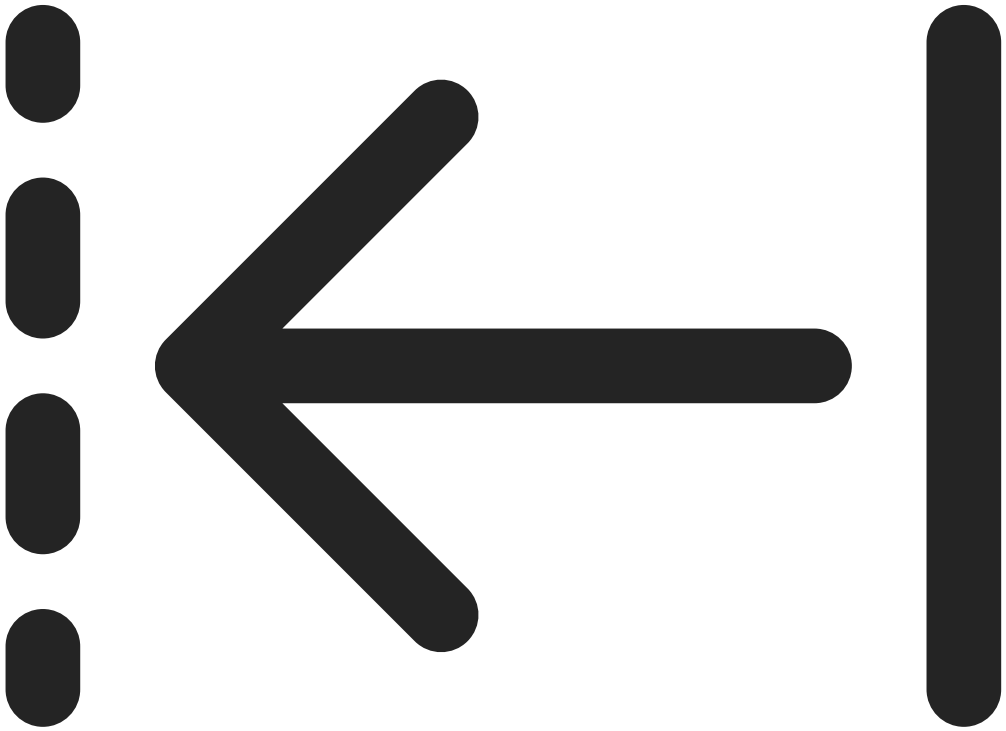
Cardholders and cardholder groups – who to grant access.

Doors and zones – where the access applies.

Schedules – when to grant access.

To add an access rule:

1. Open an Access management tab.
2. Go to **Cardholder management**.
3. Under **Access rules**



, click **Add**.

4. Enter a name for the access rule and click **Next**.
5. Configure the cardholders and groups:
   5.1. Under **Cardholders** or **Groups**, click **Add**.
   5.2. Select the cardholders or groups and click **Add**.
   5.3. You can also drag and drop a cardholder or group directly onto an access rule to apply it. When dragging, the access rules you can drop onto are highlighted. If you drag multiple cardholders or groups at once, a count shows how many you're moving.

6. Configure the doors and zones:
   6.1. Under **Doors** or **Zones**, click **Add**.
   6.2. Select the doors or zones and click **Add**.
7. Configure the schedules:
   7.1. Under **Schedules**, click **Add**.
   7.2. Select one or more schedules and click **Add**.
8. Click **Save**.

An access rule that's missing one or more of the components described above is incomplete. You can view all incomplete access rules in the **Incomplete** tab.

Export system configuration reports

You can export reports that contain different types of information about the system. AXIS Camera Station Pro exports reports as a comma-separated value (CSV) file and saves them in the default download folder. To export a report:

1. Open an Access management tab.
2. Go to **Reports** > **System configuration**.
3. Select the reports you want to export and click **Download**.

Cardholders details report	Includes information about the cardholders, credentials, card validation, and last transaction.
Cardholders access report	Includes the cardholder information and information about the cardholder groups, access rules, doors, and zones related to the cardholder.
Cardholders group access report	Includes the cardholder group name and information about the cardholders, access rules, doors, and zones related to the cardholder group.
Access rule report	Includes the access rule name and information about the cardholders, cardholder groups, doors, and zones related to the access rule.
Door access report	Includes the door name and information about the cardholders, cardholder groups, access rules, and zones related to the door.
Zone access report	Includes the zone name and information about the cardholders, cardholder groups, access rules, and doors related to the zone.

Create cardholder activity reports

A roll call report lists cardholders within a specified zone, helping identify who's present at a given moment.

A mustering report lists cardholders within a specified zone, helping identify who's safe and missing during emergencies. It helps building managers locate staff and visitors after evacuations. A muster point is a designated reader where personnel report during emergencies. The system generates a report of people on and off-site. The system marks cardholders as missing until they check in at a muster point or until someone manually marks them as safe.

Both roll call and mustering reports require zones to track cardholders.

To create and run a roll call or mustering report:

1. Open an Access management tab.
2. Go to **Reports** > **Cardholder activity**.
3. Click **Add** and select **Roll call / Mustering**.
4. Enter a name for the report.
5. Select which zones to include in the report.
6. Select any groups you want to include in the report.
7. If you want a mustering report, select **Mustering point** and a reader.
8. Select a time frame for the report.
9. Click **Save**.
10. Select the report and click **Run**.

Roll call report status	Description
Present	The cardholder entered the specified zone and didn't exit before you ran the report.
Not present	The cardholder exited the specified zone and didn't enter again before you ran the report.

Mustering report status	Description
Safe	The cardholder swiped their card at the mustering point.
Missing	The cardholder didn't swipe their card at the mustering point.

Import and export

Import cardholders

This option imports cardholders, groups, credentials, and photos from a CSV file. To import cardholder photos, make sure that the server has access to the photos.

When you import cardholders, the access management system automatically saves the system configuration, including all hardware configuration, and deletes any previously saved configuration.

You can also map users in an Active Directory database as cardholders. See *Active directory settings[BETA], on page 153*.

Import options	
New	Removes existing cardholders and adds new cardholders.
Update	Updates the existing cardholders and adds new cardholders.
Add	Keeps existing cardholders and adds new cardholders. Card numbers and cardholder IDs are unique and can only be used once.

1. On the **Access management** tab, click **Import and export**.
2. Click **Import cardholders**.
3. Select **New**, **Update**, or **Add**.
4. Click **Next**.
5. Click **Choose a file**, locate the CSV file, and click **Open**.
6. Enter a column delimiter, select a unique identifier, and click **Next**.
7. Assign a heading to each column.
8. Click **Import**.

Import settings	
First row is header	Select if the CSV file contains a column header.
Column delimiter	Enter a column delimiter format for the CSV file.
Unique identifier	The system uses **Cardholder ID** to identify a cardholder by default. You can also use first and last name, or the email address. Use this to prevent importing duplicate personnel records.
Card number format	**Allow both hexadecimal and number** is on by default.

Export cardholders

This option exports the cardholder data in the system to a CSV file.

1. On the **Access management** tab, click **Import and export**.
2. Click **Export cardholders**.
3. Choose a download location and click **Save**.

AXIS Camera Station Pro updates cardholder photos in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` whenever the configuration changes.

Undo import

The system automatically saves its configuration when you import cardholders. The **Undo import** option resets the cardholder data and all hardware configuration to the state it was before the last import.

1. On the **Access management** tab, click **Import and export**.
2. Click **Undo import**.
3. Click **Yes**.

Access management settings

To customize the cardholder fields used in the access management dashboard:

1. On the **Access management** tab, click **Settings** > **Custom cardholder fields**.
2. Click **Add** and enter a name. You can add up to 6 custom fields.
3. Click **Add**.

To use facility code to verify your access control system:

1. On the **Access management** tab, click **Settings** > **Facility code**.
2. Select **Facility code on**.

Note

You must also select **Include facility code for card validation** when you configure identification profiles. See *Identification profiles, on page 146*.

To edit an email template for sending a QR or mobile credential:

1. On the **Access management** tab, click **Settings** > **Email templates**.
2. Edit your template and click **Update**.

Badge templates BETA

You can customize badge templates with cardholder information, photos, logos, and custom branding. To create a new template:

1. Go to **Access management > Settings > Badge templates** BETA.
2. Click **Create new template**.
3. Enter a name in the **Template name** field.
4. Select **Use as default template for printing** to make this the default template.
5. Customize the badge design:
   - Select up to five text fields to display on the front side, including any custom fields you've created. When printing, only filled-out fields appear on the badge.
   - Choose the font and color for the text.
   - Add a background color or image.
   - Upload a logo for your organization.
   - For the back side, add either a background color or image.
6. Click **Save** to save your changes, or **Save as** to create a new template.

Note

Once a template is created, it can't be edited, only renamed.

Print badge BETA

You can print identification badges for cardholders using your configured badge templates. Card encoding isn't currently supported. Before you start:

- Make sure the cardholder has at least one card credential. You can't print badges for cardholders without credentials.
- You need a printer that supports CR80 card size and compatible printing material, such as thick card stock.
- Configure your browser's print settings:
  1. Set page size to CR80 or custom size matching your card dimensions.

2. Set orientation to portrait.
3. Turn off margins or set them to minimum.

Important

Secure Entry works with printers that have Windows drivers. HID Fargo printer series are verified to work. If you need a driver for your printer, contact your printer supplier.

To print badges:

1. Go to **Access management > Cardholder management > Cardholders**.
2. Select one or more cardholders.
3. Click **Print badge** BETA.
4. Click **Select template** and from the **Template** drop-down, select the badge template you want to use.
5. If the cardholder has multiple card credentials, select one from the **Card** drop-down.
6. Click **Print**.

Note

If your printer doesn't support duplex printing, print all front pages first, then flip the stack of cards and load them into the tray again to print the back pages.

System Health Monitoring BETA

Use the System Health Monitoring tab to monitor health data from one or more AXIS Camera Station Pro systems on the same network.

If you manage systems on different networks, Server monitoring in My Systems provides the same functionality but through the cloud.

	Shows a summary of the devices and systems that you have access to. See *Inventory, on page 174*.
	Shows a storage summary and recording details of each camera from the monitored systems. See *Storage, on page 175*.
	Shows the System Health Monitoring logs from the monitored systems. See *Notifications, on page 175*.

Limitations

- You can't monitor storage space for recordings on AXIS S3008 Recorder.
- Notification settings only affect the local System Health Monitoring server.
- The system flags recordings with **None** as the recording type, except for continuous and motion-triggered recordings.

Workflow

1. *Configure System Health Monitoring BETA, on page 156*
   1.1. Set up notifications. See *Notifications, on page 156*.
   1.2. Set up multisytem. See *Multisytem, on page 157*.
2. Monitor the health data from AXIS Camera Station Pro systems.
   2.1. *Inventory, on page 174*
   2.2. *Storage, on page 175*
   2.3. *Notifications, on page 175*

Inventory

The inventory page shows a summary of the devices and systems that you have access to.

1. In the **System Health Monitoring** BETA tab, click  .
2. To view a summary of a system, click **AXIS Camera Station**.
   The right panel shows system and server details.
3. To view a summary of a device in a system, click the device in the list.
   The right panel shows device and storage information, if the device contains a video source.
4. To download the system report, select **AXIS Camera Station system report** from the **Create report** drop-down menu. See *System report, on page 187*.
5. To download System Health Monitoring report:
   5.1. From the **Create report** drop-down menu, select **System Health Monitoring report**.
   5.2. To include the database in the report, select **Include all databases** and click **Download**.
   5.3. When the report is ready, click to save it.

Storage

The storage page shows the storage summary and recording details of each camera from the monitored systems. Click a column heading to sort by that column.

1. In the **System Health Monitoring** BETA tab, click .
2. When you monitor multisystem health data, select a system from the drop-down menu.

Summary	
Status	The storage status. See *Configure storage, on page 67*.
Location	The path and name of the storage.
Total	The total amount of storage space. Matches "Total size" shown in Windows properties for the storage location.
Allocated	The maximum amount of storage assigned to recordings.
Used	The storage space currently used for recordings.
Last update	The time when the information was last updated.

Camera	
Status	(empty): Normal status. Warning icon: Retention isn't fulfilled. Info icon: Retention isn't fulfilled because the camera recordings are too short.
Name	The camera name.
Recording type	The recording types applied to the camera.
Set retention	The retention time configured for the camera under **Configuration > Storage > Selection**.
Current retention	The number of days the recordings have been in storage.
Oldest recording	The time of the oldest recording from the camera in the storage.
Latest recording	The time of the latest recording from the camera in the storage.
Location	The storage location used by the camera.
Used storage	The amount of storage used by this camera for recordings.
Last update	The time when the information was last updated.

Notifications

The notifications page shows the System Health Monitoring logs from the monitored systems. Click a column heading to sort by that column.

In the **System Health Monitoring** BETA tab, click .

History	
Notification sent	The time when the notification was sent.
Item	Shows the device name for notifications triggered by `device down` or `system` for notifications triggered by `system down`.
System	The name of the system where the event occurred.
Rule	The rule that triggered the notification: `System down` or `Device down`
Detected	The time when the issue was detected.
Resolved	The time when the issue was resolved.

Hotkeys

The Hotkeys tab shows available hotkeys. The type of hotkey depends on what you use to control AXIS Camera Station Pro.

- A keyboard combination
- A keypad combination
- A joystick button
- A jog dial button

When you remove a camera or view from a connected server, the associated hotkeys are also removed.

The system groups the hotkeys into the following categories:

- Camera
- Device management
- Navigate to camera
- Navigate to view
- Navigation
- PTZ presets
- Recordings
- Sequences
- Split view
- Tab
- Other

You must manually assign to the actions in the Navigate to cameras and Navigate to views categories.

Note

- When you add or edit a hotkey, and the hotkey is already in use for another action, a warning icon appears. Hover over the warning icon to see the conflict action. Press ESC to cancel. Press ENTER to use the hotkey and automatically remove the conflicting hotkey.
- When connected to multiple servers, the Navigate to cameras and Navigate to views categories also list the cameras and views on the connected servers.

Assign a hotkey	If the keyboard value of an action is empty, click the empty field to add a hotkey for this. • To add a hotkey with the keyboard, press Ctrl and at least one another key or a function key F2-F12. • To add a hotkey with a keypad, press a numeric key combination or press one of the function keys F1-F5. • To add a hotkey with a joystick or jog dial, press the joystick or jog dial button to assign it.
Edit a hotkey	Click the keyboard value of an action to edit it.
Remove a hotkey	Click the keyboard value of an action to remove it.

	Click to print the hotkey table.
	Click to reset all hotkeys to the original settings.

Video surveillance control board keys

Hotkey mapping - Joystick	Default action	AXIS TU9002	AXIS T8311
Button 1	Go to preset 1	J1	J1
Button 2	Go to preset 2	J2	J2
Button 3	Go to preset 3	J3	J3
Button 4	Go to preset 4	J4	J4
Button 5	Simulate left mouse button	J5	L
Button 6	Simulate left right button	J6	R
Button 7	Select previous cell in split view	Top left	-
Button 8	Select next cell in split view	Top right	-
Button 9	Jump to previous recording		-
Button 10	Play/pause		-
Button 11	Jump to next recording		-
Button 12	Add bookmark		-
Button 13	Toggle zoom ring function between digital zoom and playback speed	M1	-
Button 14	Switch between live/ recordings	M2	-
Button 15	Frame step backward	Top left toggled	-
Button 16	Frame step forward	Top right toggled	-

Hotkey mapping - Keypad	Default action	AXIS TU9003	AXIS T8312
A	Open views		
B	Navigate to next camera or view		
ALT+B	Navigate to previous camera or view	Alt+	-
TAB	Navigate to the next tab		-

Hotkey mapping - Keypad	Default action	AXIS TU9003	AXIS T8312
ALT+TAB	Navigate to the previous tab	Alt+	-
C	-	-	
D	-	-	
E	-	-	
PLUS	Focus farther	+	-
MINUS	Focus nearer	-	-
F2	Open hotkeys	F2	F2
F4	Open logs	F4	F4
F5	Open configuration	F5	F5
F10	Auto focus	F10	-

Hotkey mapping - Jog	Default action	AXIS T8313
Jog 1	Show or hide export marker	L
Jog 2	Add bookmark	
Jog 3	Jump to previous recording	
Jog 4	Play/Pause	
Jog 5	Jump to next recording	
Jog 6	Switch between live/recordings	R

Note

AXIS T8311 Video Surveillance Joystick doesn't support joystick buttons 7–10.

Logs

By default, the **Logs** tab shows live alarms, events, and audit logs. You can search for previous logs as well. You can configure the number of days to keep logs under **Configuration > Server > Settings**.

Time	Date and time of the action.
Type	The type of the action: Alarm, Event, or Audit.
Category	The category of the action.
Message	A short description of the action.
User	The AXIS Camera Station Pro user who performs the action.
Computer	The computer (Windows domain name) on which AXIS Camera Station Pro is installed. This value is provided by the client and can't be independently verified by the server.
Windows user	The Windows user who administers AXIS Camera Station Pro. This value is provided by the client and can't be independently verified by the server. The User column shows the authenticated user.
Server	Only available when connecting to multiple servers. The server on which the action occurs.
Component	The component that the log is generated from.

Search logs

1. In the **Logs** tab, click **Search** under **Log search**.
2. In the filter box, type the keywords. AXIS Camera Station Pro searches the log list, excluding **Time**, and shows results that contain all the keywords. For supported search operators, see *Optimize your search, on page 40*.
3. Select **Alarms**, **Audits**, or **Events** under **Filter**.
4. Select a date or a range of dates from the calendar.
5. Select **Start time** and **End time** from the drop-down menus.
6. Click **Search**.

Alarms log

The **Alarms** log displays system alarms and those generated by rules and motion detection. The list includes the date and time of the alarm, alarm category, and an alarm message. See *Alarms*.

	Click an alarm and to open the **Recordings** tab and start playback when the alarm contains a recording.
	Click an alarm and to open the alarm procedure when the alarm contains an alarm procedure.
	Click an alarm and to notify other clients that the alarms have been acknowledged.
	Click an alarm and to export the log to a text file.

Events log

The **Events** log displays camera and server events, for example recordings, triggers, alarms, errors, and system messages, in a list. The list includes the date and time of the event, event category, and an event message.

Select the events and click  in the toolbar to export the events as a text file.

Audit log

In the **Audit** log, you can view all user actions, such as manual recordings, video streaming started or stopped, action rules, door created, and cardholder created. Select the audits and click  in the toolbar to export them as a text file.

License plate management

To manage license plate lists in AXIS Camera Station Pro, open the **License plate management** tab.

On this tab, you can edit three license plate lists for individual cameras or groups of cameras:

1. Select a group or camera from the **Groups** and **Cameras** lists.
2. Select which list to edit. By default, the three lists you can edit are named **Allow list**, **Block list**, or **Custom list**.
3. Make changes to the list:
   - To edit the list name, click **Edit list name**.
   - To add a new license plate, enter the license plate in the License plate column and optionally a description in the Description column. Click **Add**.
   - To edit or remove an existing license plate, select it and click **Edit** or **Remove**.
   - To import a license plate list from a CSV file, click **Import** and select the file. This overwrites your current list, so export it first if you want to keep a copy.
   - To export a license plate list to a CSV file, click **Export**.
4. Click **Apply** to save your changes.

Note

Once you apply changes, AXIS Camera Station Pro takes over managing the license plate lists for that group or camera. Every night, we update the camera to match the lists saved in AXIS Camera Station Pro, which overwrites any license plates stored directly on the camera.

AXIS Audio Manager Pro

Use the **AXIS Audio Manager Pro** tab to access the AXIS Audio Manager Pro server interface directly from AXIS Camera Station Pro. For more information about the server interface, see *AXIS Audio Manager Pro – User manual.*

The tab only appears after you've connected to an AXIS Audio Manager Pro server in AXIS Camera Station Pro. For more information, see *Configure AXIS Audio Manager Pro, on page 154*.

Important

You can'tt access the AXIS Audio Manager Pro server interface with Secure Remote Access v2.

The integration also lets you:

- *Create AXIS Audio Manager triggers, on page 92*
- *Create AXIS Audio Manager actions, on page 101*
- Add audio zones to maps. See *Map, on page 20*.
- *Use paging interfaces in split views, on page 19*
- Set AXIS Audio Manager Pro-related user privileges in AXIS Camera Station Pro. See *User or group privileges, on page 122*.
- Select audio devices from the AXIS Audio Manager Pro server as the associated audio device for a camera. See *Edit stream profiles, on page 49*.

Alarms

The Alarms tab is available at the bottom of the AXIS Camera Station Pro client and displays triggered events and system alarms. For information about how to create alarms, see *Action rules*. For information about the alarm "Database maintenance is required", see *Database maintenance, on page 204*.

Time	The time the alarm occurred.
Category	The category of the triggered alarm.
Description	A brief description of the alarm.
Server	Available when connected to multiple servers. The AXIS Camera Station Pro server that sends the alarm.
Component	The component that triggers the alarm.
	Shows an alarm procedure. Only available when the alarm contains an alarm procedure.
	Goes to recordings. Only available when the alarm contains a recording.
	Acknowledge the selected alarm
	Remove the alarm. The alarm is only temporarily removed if you don't acknowledge it first.

To deal with a specific alarm:

1. Click **Alarms and Tasks** at the bottom of the AXIS Camera Station Pro client, and open the **Alarms** tab.
2. For alarms with a recording, select the alarm and click to go to the recording in the **Recording alerts** tab.
3. For alarms without a recording, open a tab with live view and double-click the alarm to show the recording for the time of the alarm in the **Recording alerts** tab.
4. For alarms with an alarm procedure, select the alarm and click to open the alarm procedure.
5. To notify other clients that the alarms have been acknowledged, select the alarms and click .
6. To remove the alarms from the list, select the alarms and click .

Tasks

The Tasks tab is available at the bottom of the AXIS Camera Station Pro client.

The following tasks are personal and are only visible for the administrators and the users who started them:

- System report
- Create incident report
- Export recordings

If you are an administrator, you can view and operate all tasks started by any user, including the personal tasks.

If you are an operator or viewer, you can:

- View all tasks started by you and the tasks started by other users that aren't personal.
- Cancel or retry the tasks you started. You can only retry the incident report and export recordings tasks.
- View the result of all tasks in the list.
- Remove any finished tasks in the list. This only affects the local client.

Name	The name of the task.
Start	The time when the task started.
Message	Shows the status or information about the task. The possible statuses: • **Canceling**: Cleaning up before canceling the task. • **Canceled**: Cleaning is complete and the task is canceled. • **Error**: The task failed on one or more devices. • **Finished**: Task completed. • **Finished during lost connection**: The task completed while the server connection was down. Task status can't be determined. • **Lost connection**: The client lost connection with the server while the task ran. Task status can't be determined. • **Running**: Performing the task. • **Pending**: Waiting for another task to complete.
Owner	The user who initiated the task.
Progress	Shows the progress of the task.
Server	Available when connected to multiple servers. Shows AXIS Camera Station Pro server that performs the task.

To deal with one or more tasks:

1. Click **Alarms and Tasks** at the bottom of AXIS Camera Station Pro client, and click the **Tasks** tab.
2. Select the tasks and click one of the actions

	Click to display the Task result dialog.
	Click to cancel the task.

	Click to delete the tasks from the list.
	If the task fails when you export recordings or create incident reports, click to retry the failed task.

Task result

If a task was performed on multiple devices, the dialog shows the results for each device. Review and configure all failed operations manually.

For most tasks, the following details are listed. For tasks such as **Export recordings** and **System report**, double-click the task to open the folder with the saved files.

MAC address	The MAC address of the updated device.
Address	The IP address of the updated device.
Message	Information about how the task was executed: • **Finished**: The task completed successfully. • **Error**: The task was unable to complete on the device. • **Canceled**: The task was canceled before completion.
Description	Information about the task.

Depending on the type of performed task, the following details are listed:

New address	The newly assigned IP address of the device.
Action rules	The firmware version and the product name of the device.
Details	The serial number and IP address of a replaced device and the serial number and IP address of the new device.
Reference ID	The reference ID of the incident report.

Generate reports

Client configuration sheet

The client configuration sheet is useful for troubleshooting and when you contact support.

To view an HTML overview of the client system configuration:

1. Go to **Configuration** > **Server** > **Diagnostics**.
2. Click **View client configuration sheet**.

Server configuration sheet

The Server configuration sheet includes information about general configuration, camera settings including action rules, schedules, recording storage, auxiliary devices, and licenses. This is useful for troubleshooting and when you contact support.

To view an HTML overview of the server system configuration:

1. Go to **Configuration** > **Server** > **Diagnostics**.
2. Click **View server configuration sheet**.

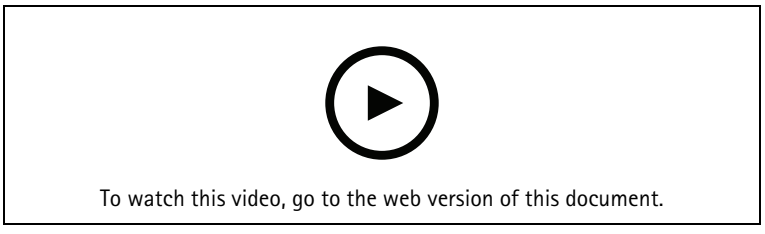
System report

The system report is a .zip file that contains parameters and log files that help Axis Customer Support to analyze your system.

Always include a system report when you contact Customer Support.

To generate the system report:

1. Go to the menu in the top right corner.
2. Click **Help** > **System report**.
3. Edit the file name if you want to change it from the automatically generated one.
4. Click **Browse** to select where to save the system report.
5. Choose your preferred settings:
   - **Automatically open folder when report is ready** to open it immediately.
   - **Include all databases** to add detailed information about recordings and system data.
   - **Include screenshots of all monitors** to help analyze the system report.
6. Click **OK**.



Generate a system report

AXIS Installation Verifier

AXIS Installation Verifier starts a performance test after installation to verify that all the devices in a system are fully operational. The test takes about 20 minutes to run.

Tests	
Normal conditions	Test of data streaming and storage using the current system settings in AXIS Camera Station Pro. Results show as passed or failed.
Low light conditions	Test of data streaming and storage using settings optimized for typical low light conditions. Results show as passed or failed.
Stress test	Tests that incrementally increase data streaming and storage until the system reaches its maximum limit. Results show the maximum system performance.

Note

- You can only test devices that support AXIS Camera Application Platform 2 (ACAP 2) and later.
- During the test, AXIS Camera Station Pro goes into maintenance mode, and all surveillance activities are temporarily unavailable.

To start the test:

1. Go to **Configuration** > **Server** > **Diagnostics**.
2. Click **Open AXIS installation verifier...**.
3. Click **Start**.
4. When the test finishes, click **View report** to open it **Save report** to save it.

Asset list

You can export a list of assets for your video management system. The asset list includes the name, type, model, status, and serial number of the following:

- All connected servers
- All connected devices
- The client terminal from which you export the asset list when connected to multiple terminals

To export an asset list:

1. Go to ☰ > **Other** > **Asset list**.
2. Click **Export**.
3. Select the file location and click **Save**.
4. Under **Latest export**, a link to the file appears or is updated.
5. Click the link to go to the file location.

Status of Axis services

To view the status of Axis online services:

1. Go to **Configuration** > **Server** > **Diagnostics**.
2. Click **View status of Axis services**.

AXIS Camera Station Pro service control

The server uses AXIS Camera Station Pro service control to start, stop, and change its settings. It automatically starts after the installation is complete. If the server computer restarts, service control automatically restart in about 2 minutes. An icon in Windows notification area shows the status of the service.

Right-click the icon, and select **Open AXIS Camera Station Service Control**, **Start Service**, **Stop Service**, **Restart Service**, or **Exit**.

To open service control from the start menu:

Go to the **Start** menu and select **All Programs > Tools > Service Control**.

	Running
	Starting
	Stopped

Modify Settings	Select to change the server settings.
Restore Default Settings	Click to restore all settings to the original default settings.
Start	Click to change the server status.
Stop	
Restart	Click to restart the server.

General

In AXIS Camera Station Pro service control, select **Modify settings** and click **General** to change the general server settings.

Server settings	
Server name	The name of the server. The server name appears in the software client. The default server name is the computer name. The name doesn't change if you change the computer name.
Web client port	The Web client for AXIS Camera Station uses this port.
Ports range	Specify the range of ports. The rest of the ports change automatically.
Allow AXIS Camera Station Pro to add exceptions to the Windows Firewall	Select to allow AXIS Camera Station Pro to automatically add exceptions to the Windows Firewall when a user changes the port range.

Note

- If there is a NAT, firewall, or similar between the server and the client, configure the NAT or firewall to allow these ports to pass through.
- The port numbers must be within the range 1024-65534.

Port list for AXIS Camera Station Pro

The following tables show which ports and protocols AXIS Camera Station Pro uses. You may need to allow these in your firewall for optimal performance and usability. Port numbers are calculated based on the HTTP main port 29200.

Server to devices

Port	Number	Protocol	In/Out	Description
Main HTTP and HTTPS ports	80 & 443	TCP	Outbound	Used for video streams and device data.
Default bonjour port	5353	UDP	Multicast (Inbound + Outbound)	Used to discover devices with mDNS Discovery (Bonjour). Multicast 224.0.0.251.

				If unable to bind to the default port it can be because another application uses it and refuses to share it. In that case a random port is used. Bonjour doesn't discover devices with link-local addresses when you use a random port.
Default SSDP port	1900	UDP	Multicast (Inbound + Outbound)	Used to discover devices with SSDP (UPNP). Multicast 239.255.255.250.
Default WS-Discovery port	3702	UDP	Multicast (Inbound + Outbound)	WS-Discovery webservices discovery used to discover Onvif devices. Multicast 239.255.255.250.

Client to server

Port	Number	Protocol	In/Out	Communication between	Description
HTTP streaming port	29200	TCP	Inbound	Server and client	Used for video, audio, metadata stream (AES encryption).
Main TCP port	29202	TCP	Inbound	Server and client	+2 offset from HTTP streaming port. Used for client switch.
API web server port	29204	TCP	Inbound	Server, client, and mobile app	+4 offset from HTTP streaming port. Used for application data and video stream MP4 over HTTPS.

Local proxy HTTP port	29206	TCP	Inbound	Internal communication in server	Mobile apps make calls to the SRA module, which receives HTTPS, converts it to HTTP and resends it to the local proxy HTTP port and the API media port.
Web proxy endpoint port	29207	TCP	Inbound	Server and component	+7 offset from HTTP streaming port. Used for secure communication between component and devices.

Domains and ports for Secure Remote Access v2

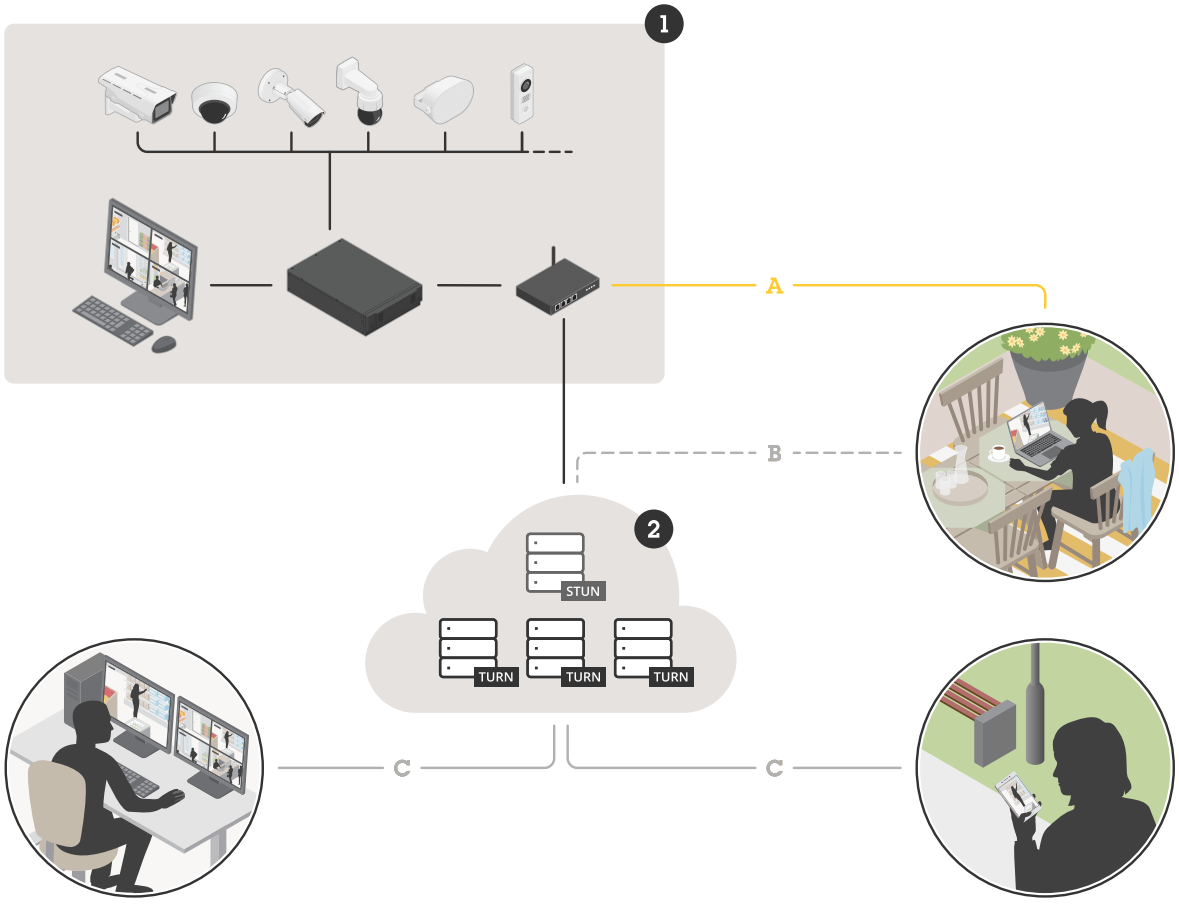


Image: Solution overview of Axis Secure Remote Access v2 in AXIS Camera Station Pro

1. Monitored site on local network with local viewing client
   - A – Remote (peer-to-peer) connection
   - B – Temporary STUN/TURN connection to Axis Cloud Connected Services

Name or type	Address	Port number	Protocol	Direction
SRA v2 - MyAxis Sign in	https://eu.login.connect.axis.com	443	TCP	Inbound and outbound
SRA v2 - Cloud Service communication	https://eu.cs.connect.axis.com	443	TCP	Inbound and outbound
SRA v2 - Cloud service API communication	https://api.vms.axis.cloud	443	TCP	Inbound and outbound
EdgeHost component	75.2.119.140	443, 8443	-	Inbound and outbound
EdgeHost component	99.83.133.42	443, 8443	-	Inbound and outbound
EdgeHost component	cep.connect.axis.com	443, 8443	-	Inbound and outbound

2. Axis Cloud Connected Services
   - C – Remote TURN connection to Axis Cloud Connected Services

Name or type	Address	Port number	Protocol	Direction
P2P proxy and WebRTC component communication	wss://signaling.prod.webrtc.connect.axis.com	443	TCP	Inbound and outbound
P2P proxy and WebRTC component communication	https://*.turn.prod.webrtc.connect.axis.com	443, 3478, 5349, 49152-65535	TCP	Inbound and outbound

Reserved for components

Component	Listens on interface	Port	Number	Protocol	In/Out	Communication between	Description
Secure Entry	Localhost (127.0.0.1)	Web server port	29214	HTTPS	Inbound	Client (Access management tab) and component	+14 offset from HTTP streaming port. Older installations used port 8081
Secure Entry	All (0.0.0.0/INADDR_ANY)	Web server port	29215	HTTPS	Inbound	Main server and sub servers	+15 offset from HTTP streaming port. Used for communication between main server

Compo-nent	Listens on interface	Port	Number	Protocol	In/Out	Communi-cation between	Description
							and sub servers in multi-server setup
System Health Monitoring	All (0.0.0.0/ INADDR_ ANY)	Web server port	29216	HTTPS	Inbound	Client (System Health Monitoring tab) and component	+16 offset from HTTP streaming port. Used to host System Health Monitoring web pages and for sharing data in multisys-tem setup
System Health Monitoring Cloud Service	localhost	Web server port	29217	HTTPS	Inbound	AXIS Camera Station Pro (web page) and CloudSer-vice backend (plugin)	+17 offset from HTTP streaming port. Used for System Health Monitoring Cloud Service to enable System health monitoring
Smart search 2	localhost	Web server port	29218	HTTPS	Inbound	Client (Smart search tab) and component	+18 offset from HTTP streaming port. Used to host Smart Search API and serve client web page
VMS API core	127.0.0.1, ::1	GraphQL API	29219	GraphQL	Inbound	VMS API and GraphQL clients	+19 offset from HTTP streaming port. Used to expose the

Compo-nent	Listens on interface	Port	Number	Protocol	In/Out	Communi-cation between	Description
							ACS as a GraphQL API to a client
			29222				Reserved for future use
Web Client	localhost	Web server port	29223	HTTPS	Inbound	WebClient to VMS API/ Embedda-ble Client	+23 offset from HTTP streaming port. Backend act as proxy in front of VMS API Configura-ble
Embedda-ble Client	localhost	Web server port	29224	HTTPS	Inbound	Embedda-ble Client to VMS API/ WebRTC Streamer/ Signaling Server	+24 offset from HTTP streaming port. Backend act as proxy in front of VMS API
Web Client configura-tion	localhost	Web server port	29225	HTTPS	Inbound	AXIS Camera Station Pro client (web page)	+25 offset from HTTP streaming port. Used to host Web Client configura-tion web page and backend
Embedda-ble Client configura-tion	localhost	Web server port	29226	HTTPS	Inbound	AXIS Camera Station Pro client (web page)	+26 offset from HTTP streaming port. Used to host Embedda-ble Client configura-tion web page and backend

Compo-nent	Listens on interface	Port	Number	Protocol	In/Out	Communi-cation between	Description
			29227				Reserved for future use
Local ICE config generator	localhost	Web server port	29228	HTTPS	Inbound	Signaling server to ICE config generator	+28 offset from HTTP streaming port. Part of WebRTC component on prem
Local WebRTC configura-tion	localhost	Web server port	29229	HTTPS	Inbound	AXIS Camera Station Pro client (web page)	+29 offset from HTTP streaming port. Used to host WebRTC configura-tion web page and backend. Part of WebRTC component on prem
Local TURN server	localhost	coturn server port	29230	UDP	Inbound/ Outbound	Embedda-ble Client/ WebClient ↔ TURN server	+30 offset from HTTP streaming port. Used for "single port WebRTC" on ACS onprem
			29231				Reserved for future use
Local-IAM (IDP)	0.0.0.0	IDP_OIDC (Public)	29232	HTTPS	Inbound	Reverse proxy and local-iam	+32 offset from HTTP streaming port. Public port
Local-IAM (IDP)	0.0.0.0	MTLS (Admin)	29233	HTTPS	Inbound	Third party services	+33 offset from HTTP streaming port.

Compo-nent	Listens on interface	Port	Number	Protocol	In/Out	Communi-cation between	Description
							Administra-tor port
Local-IAM (IDP)	127.0.0.1	TOKENIZER	29234	HTTPS	Inbound	Third party services	+34 offset from HTTP streaming port. Tokenizer port
WebRTC	localhost	Onboarding API	29235	HTTPS	Inbound	Cloud component	+35 offset from HTTP streaming port. Used by the onboarding to configure webrtc cloud connection. Part of WebRTC component
Opentele-metry	127.0.0.1	gRPC port	29236	gRPC	Inbound	Third party services	+36 offset from HTTP streaming port
Opentele-metry	127.0.0.1	HTTP port	29237	HTTPS	Inbound	Third party services	+37 offset from HTTP streaming port
Audio Manager Pro		Web server port	29238	HTTPS	Inbound	3rd party integration services and component	+38 offset from HTTP streaming port
			29239				Reserved for future use
			29240				Reserved for future use
Data Insights Dashboard	localhost	2dpc/3dpc push Receiver	29241	HTTPS	Inbound (External)	Receiver of Push (post) messages containing counting data from	+41 offset from HTTP streaming port

Compo-nent	Listens on interface	Port	Number	Protocol	In/Out	Communi-cation between	Description
						2dpc and 3dpc. Internally: database, Mosquitto broker	
Data Insights Dashboard	0.0.0.0	Mosquitto broker	29242	MQTTS	Inbound (External) Outbound (External)	Receiver of camera event messages. Bridging of MQTT brokers possible if needed. (Many to one for example using topic. Database "duplica-tion" and load balancing available for pro services when setting up a site) Internally: Receiver	+42 offset from HTTP streaming port
			29243				Reserved for future use
NATS Broker	127.0.0.1	NATS	29244	NATS	Inbound	Between AXIS Camera Station Pro and compo-nents, and between compo-nents themselves	+44 offset from HTTP streaming port
Opentele-metry	127.0.0.1	HTTP port	29245	HTTP	Inbound	Monitoring endpoint to fetch metrics from the open	+45 offset from HTTP streaming port

Compo-nent	Listens on interface	Port	Number	Protocol	In/Out	Communi-cation between	Description
						telemetry collector	
API Gateway	All (0.0.0.0/ INADDR_ ANY)	Reverse proxy fallback port used by edge host	29248	HTTPS	Inbound	Edge host and reverse proxy	+48 offset from HTTP streaming port
API Gateway	All (0.0.0.0/ INADDR_ ANY)	Fallback port hosted with ACS Server certificates, used as fallback communi-cation for ACS Windows Client	29250	HTTPS	Inbound	ACS Client and API Gateway	+50 offset from HTTP streaming port
System Health Monitoring	127.0.0.1	Health data opentele-metry gRPC receiver	29251	gRPC	Inbound	ACS Server and possibly other compo-nents towards SHM collector	+51 offset from HTTP streaming port. Used by health data producers to transfer data to SHM collector
System Health Monitoring	127.0.0.1	Health data opentele-metry http receiver	29252	HTTPS	Inbound	ACS Server and possibly other compo-nents towards SHM collector	+52 offset from HTTP streaming port. Used by health data producers to transfer data to SHM collector

Other ports

Port	Number	Protocol	In/Out	Communication between	Description
Internet HTTPS	80 & 443	TCP	Outbound	Client and server to internet	Used for license activation, download

					firmware, connected services etc.
Server TCP streaming port	29198	TCP	Inbound	Server and device	-2 offset from HTTP streaming port.
Upgrade status UDP port	15156	UDP	Inbound + Outbound	Server and service control	AXIS Camera Station Pro service control listens on the port, and the server broadcasts the status of an ongoing upgrade.

Database

Database files

Core database files

AXIS Camera Station Pro stores the core database files under `C:\ProgramData\AXIS Communications\AXIS Camera Station Server`.

For AXIS Camera Station versions earlier than 5.13, there is only one database file: **ACS.FDB**.

For AXIS Camera Station version 5.13 or later, there are three database files:

- **ACS.FDB**: This main database file contains the system configuration such as devices, views, permissions, events, and stream profiles.
- **ACS_LOGS.FDB**: This logs database file contains references to the logs.
- **ACS_RECORDINGS.FDB**: This recordings database file contains the metadata and references to the recordings stored in the location specified under **Configuration > Storage**. AXIS Camera Station Pro requires this file to display the recordings in the timeline during playback.

Component database files

SecureEntry.db – AXIS Secure Entry database file contains all access control data except cardholder photos. It's saved under `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\INTERNAL\main_db`.

smartSearch.sqlite3 – The smart search database file contains camera configuration and saved search filters. It's saved under `C:\ProgramData\Axis Communications\AXIS Smart Search\data`.

Database settings

The system backs up the database every night and before each upgrade. In AXIS Camera Station Pro service control, select **Modify settings** and click **Database** to change the backup settings.

Backup folder	Click **Browse** and select where to save the database backups. Restart AXIS Camera Station Pro server to apply the change. If the backup folder path is incorrect or AXIS Camera Station Pro doesn't have access to the network share, the backup is saved to`C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup`.
Days to keep backups	Specify the number of days to keep backups. You can set any number between 1 and 30. Default is 14 days.
Upgrade progress	Click **View details** to view the details about the latest database upgrade. It includes events that happened since last restart of AXIS Camera Station Pro service control.

Backup database

The database contains information about recordings and other metadata necessary for the system to work properly.

Important

- The database doesn't store the recordings. Specify a storage location under **Configuration > Storage** and back up the recordings separately.
- Server and database settings in AXIS Camera Station Pro service control aren't saved.

System backup

The system automatically saves the system backup in the folder specified on the **Database** tab. See *Database settings, on page 201*. A system backup includes both the core database files and the component database files. See *Database files, on page 201*.

Backup files	
`System_YYYY-MM-DD-HH-mm-SSSS.zip`	A nightly triggered backup.
`PreUpgrade_YYYY-MM-DD-HH-mm-SSSS.zip`	A backup triggered before a database update.
`User_YYYY-MM-DD-HH-mm-SSSS.zip`	A backup triggered before the removal of a storage.

In the .zip file, you can find the following files:

ACS	This folder includes the core database files `ACS.FDB`, `ACS_LOGS.FDB`, and `ACS_RECORDINGS.FDB`.
Components	This folder is only available if you use a component, for example, AXIS Camera Station Secure Entry or smart search. • **webrtc**: This folder contains WebRTC configuration files. • **ACMSM**: This folder includes AXIS Camera Station Secure Entry database file `SecureEntry.db` and cardholder photos.

	• **smartsearch**: This folder includes smart search database file `smartSearch-backup-yyyyMMddHHmmssfff.sqlite3`.
`backup_summary.json`	This file includes more detailed information about the backup.
`_cluster_yyyyMMddHHmmssfff.dbcbackup`	This file contains a logical backup of the PostgreSQL database cluster, which includes cluster-wide data such as roles and tablespaces.

Maintenance backup

Specify the backup folder to store the maintenance backups in the **Database** tab. See *Database settings, on page 201*. A maintenance backup includes the core database files with each database file in a separate folder `PreMaintenance_YYYY-MM-DD-HH-mm-SSSS`.

It can be triggered in different ways:

- Automatically when you update AXIS Camera Station Pro.
- When you manually run **Database maintainer** from AXIS Camera Station Pro service control. See *Database maintenance, on page 204*.
- Automatically by the scheduled database maintenance task configured in Windows Task Scheduler. See *Tools, on page 206*.

Manual backup

Note

A manual backup can only back up the core database files. It doesn't back up the component database files, for example, smart search database file.

There are two ways to perform a manual backup:

- **Option 1:** Go to `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` and make a copy of the database files. Then, back up the PostgreSQL database cluster:
  1. Open a terminal as Administrator in the directory where you want to save the backup.
  2. Run `"C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" backup -cluster`
  3. The backup is saved in a folder named **yyyyMMddHHmmssfff** in the directory where you opened the terminal.
- **Option 2:** Generate a system report and select **Include all databases** to include the database backup files. See *System report, on page 187*.

Restore database

If you lose the database due to hardware failure or other problems, you can restore the database from one of the saved backups. By default, the system keeps the backup files for 14 days. For more information about database backup, see *Backup database, on page 202*.

Note

The database doesn't store the recordings. Specify a storage location under **Configuration > Storage** and back up the recordings separately.

To restore the database:

1. Go to AXIS Camera Station Pro service control and click **Stop** to stop the service.
2. Go to the database backup files. See *Backup database, on page 202*.

3. Extract the files.
4. Restore the PostgreSQL database cluster:
   4.1. Open a terminal as Administrator in the extracted folder.
   4.2. Run `"C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" restore -backup-file _cluster_yyyyMMddHHmmssfff.dbcbackup`
   4.3. Click **y** when prompted to confirm that you trust the source of the backup file.
5. In the extracted folder, copy the following database files under **ACS** to `C:\ProgramData\AXIS Communications\AXIS Camera Station Server\`.
   - **ACS.FDB** - You must copy this file to restore the database.
   - **ACS_LOGS.FDB** - Copy this file if you want to restore logs.
   - **ACS_RECORDINGS.FDB** - Copy this file if you want to restore recordings.
6. If you use AXIS Camera Station Secure Entry, follow the instructions in `RESTORE_INSTRUCTIONS.txt` located in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db`.
7. If you use smart search, copy **smartSearch-backup-yyyyMMddHHmmssfff.sqlite3** from `smartsearch` to `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Smart Search\data` and rename it to **smartSearch.sqlite3**.
8. If you use the VMS web client, copy all the files from `webrtc` to `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\WebRTC`.
9. Go back to AXIS Camera Station Pro service control and click **Start** to start the service.

Database maintenance

Perform database maintenance if the alarm `Database maintenance is required` appears or if the system shuts down unexpectedly, for example after a power outage.

To start database maintenance, see *Tools, on page 206*.

Note

AXIS Camera Station Secure Entry uses DB Janitor to monitor and shrink the database files if necessary. The access control system becomes temporarily unavailable when forced shrinking occurs.

Database best practice

To avoid problems, keep the following in mind:

Check for disk errors – Disk errors can cause database corruption. Use a tool such as chkdsk (Check disk also known as Error checking) to look for damaged sectors on the hard drive used for the database. Run chkdsk regularly.

Antivirus software and external backups – Don't run virus scans on the database because some antivirus software can corrupt it. If you use an external backup system, don't back up the active database. Create a backup from the files in the backup folder instead.

Power failure – An unexpected shutdown, for example due to power failure, can corrupt the database. Use a UPS (Uninterruptible Power Supply) for critical installations.

Out of space – The database can become corrupted if the hard drive runs out of space. To avoid this, install AXIS Camera Station Pro server on a computer with sufficient memory. For hardware requirements, see *axis.com/products/axis-camera-station/hardware-guidelines*.

Corrupted RAM memory – Run Windows Memory Diagnostic regularly to check for RAM errors.

Certificates

Use the **Certificates** tab to manage server certificates for AXIS Camera Station Pro. You can view information about the current server certificate, see when it expires, generate and import new server certificates, or export the current one. Server certificates are stored in C:\ProgramData\Axis Communications\AXIS Camera Station Server\certs.

Server certificate

Generate	Create a new self-signed server certificate. This replaces the previous certificate used by the server and requires a server restart to take effect.
Import...	Import a server certificate from a file. The supported file formats are PEM and PFX/PKCS12. Only RSA keys with at least 2048 bits are supported.

Note

When importing a certificate with intermediate certificates in the PEM format, all intermediate certificates must be in the .cer file. If you're creating your own certificates, see *Prepare intermediate certificates for import, on page 205*.

Current certificate

Shows information about the current server certificate. Use this to manually verify that the client has connected to the correct server.

View	View more details about the server certificate.
Export...	Export the server certificate as a PFX file.

Generate a new server certificate

- Press the Windows key + S to search for and open AXIS Camera Station Pro service control.
- In the **Certificates** tab, click **Generate** to generate a new server certificate.
- Restart the server to apply the new server certificate.

Prepare intermediate certificates for import

To import a certificate with intermediate certificates into AXIS Camera Station Pro, combine the server certificate and intermediate certificate into one file:

1. Open one of the server certificates and the intermediate certificate in Notepad. The contents will be structured as follows:
   ```
   cert.cer
   ——BEGIN CERTIFICATE——
   MIIFTDCCB....
   ——END CERTIFICATE——
   ```
2. Copy and paste the contents from one certificate over to the other and change the first line to combined_cert.cer:
   ```
   combined_cert.cer
   ——BEGIN CERTIFICATE——
   MIIFTDCCB....
   ——END CERTIFICATE——
   ——BEGIN CERTIFICATE——
   MIIE+zCCA+OgA.....
   ——END CERTIFICATE——
   ```
3. Save the file.

Tools

In AXIS Camera Station Pro service control, select **Modify settings** and click **Tools** to start database maintenance and create partial system reports.

Database maintainer

- Open AXIS Camera Station Pro service control.
- Click **Tools**.
- Under **Database maintainer**, click **Run**.
- The estimated downtime appears. Click **Yes** to continue. Once started, the process can't be canceled.

Note

- AXIS Camera Station Pro server and all ongoing recordings stop during maintenance. After maintenance, the server starts automatically.
- Don't turn off the computer during maintenance.
- Database maintenance requires administrator rights on the Windows computer.
- If database maintenance can't recover the database, contact Axis technical support.

Make sure to run database maintenance if the alarm "Database maintenance is required" appears or if the system shuts down unexpectedly, for example after a power outage.

Database maintenance can also be scheduled to run automatically if you turn on " AXIS Camera Station Pro Database Maintenance Task" in Windows Task Scheduler. You can edit the trigger to customize when and how often to run the Database maintainer.

System report

The partial system report is a .zip file that contains parameters and log files that help Axis customer support to analyze your system. Always include a system report when you contact customer support. To generate a complete system report, go to  **> Help > System report** in AXIS Camera Station Pro client.

To generate a partial system report:

1. Click **Run**.
2. Select and enter the requested information in the dialog.
3. Click **Generate report**.

System Report Tool	
File name	Enter a file name for the system report.
Folder	Select where to save the system report.
Automatically open folder when report is ready	Select to automatically open the folder when the system report is ready.
Include database file in report	Select to include the database in the system report. The AXIS Camera Station Pro database contains information about recordings and data necessary for the system to work properly.

Network logging

- Click the link to download a network protocol analyzer application.
- Once installed, click **Start** to run the application.

Reset certificate authority

- Click **Reset** to generate a new certificate authority and restart the service.
- Once the service restarts, you'll be able to log in and import a custom certificate authority if needed.

Troubleshooting

About this guide

This guide is a collection of issues related to AXIS Camera Station Pro and how to troubleshoot them. Issues are grouped by topic to make them easier to find. A topic can be, for example, audio or live view. Every issue includes a suggested solution.

For more resources including hardware requirements, software upgrades, and tutorials, visit *axis.com/support*.

If you experience general issues, try restarting the AXIS Camera Station Pro server service before troubleshooting further:

1. Go to **Configuration** > **Server** > **Diagnostics**.
2. Click **Restart AXIS Camera Station server service...**.

Note

Restarting the server service can take a while, and there's no way to cancel the restart. The server is unavailable, and all connected devices lose connection while it restarts.

The AXIS Camera Station Pro service

The service restarts often

The server can be overloaded, which causes a long task queue and can also corrupt the databases.

- Check whether AXIS Camera Station Pro or any other application is using a high number of resources.
- Run the Database maintainer. See *Database maintenance, on page 204*.

If none of the above helps, contact Axis Support. Go to *Escalation process, on page 222*.

Devices in the video management system

Common issues

The listed cameras weren't added because the VMS can't contact the camera	1. Make sure the camera has a network connection, that there's power, and that the camera is running. 2. Go to **Configuration > Add devices** and try to add the camera again.
The listed cameras weren't added because the user canceled the installation	To add the cameras, go to **Configuration > Add devices**.
Password can't be set for the listed cameras	1. To set the password manually, go to **Configuration > Devices > Management**. 2. Right-click the camera and select **User Management > Set password**.

Device can't be added

The device was used in a different system before it was added to AXIS Camera Station Pro	• Perform a factory reset on the device. • Try adding the device to AXIS Device Manager.
A different device model is added instead of the one you want	This may be a compatibility issue. Use the latest AXIS Camera Station Pro version.
Not possible to add another device model	Troubleshoot the camera at *axis.com/support/troubleshooting*.

Can't upgrade device firmware through AXIS Camera Station Pro

The camera's firmware can't be upgraded from its web interface	Troubleshoot the camera at *axis.com/support/troubleshooting*.
Firmware can't be upgraded on all devices	• Make sure there's a network connection. • If it's not a network-related issue, contact Axis support. Go to *Escalation process, on page 222*.
Firmware can't be upgraded for specific models	This may be a compatibility issue. Contact Axis support. Go to *Escalation process, on page 222*.

No devices found

The video management system automatically searches the network for connected cameras and video encoders but hasn't found any.

- Make sure the camera has a network connection and that there's power.
- If the client, server, or cameras are located on different networks, configure the proxy and firewall settings.
  - Change the client proxy settings if a proxy server separates the client and the server.
  - Change the NAT or security system if a NAT or security system separates the client and the server. Allow the HTTP port, TCP (Transmission Control Protocol) port, and streaming port specified in AXIS Camera Station service control to pass through the security system or NAT. To view the full port list, see *Port list for AXIS Camera Station Pro, on page 191*.
- Add cameras manually. Go to *Add devices, on page 5*.

Repeated message "Reconnecting to camera in 15 seconds"

Possible issues:

- An overloaded network.
- The camera isn't accessible. Check that the camera has a network connection.
- There are problems with the graphics card.

Possible solutions for graphics card problems:

- Install the latest graphics card driver.
- Upgrade to a graphics card with more video memory and higher performance.
- Use the CPU for video rendering. Select it under **Graphics card** in **Hardware decoding**. You can find this setting under **Configuration > Client > Streaming**.
- Adjust the video and audio settings. For example, optimize the profile settings for low bandwidth.

Recordings

Common issues

Continuous recording isn't turned on	1. To turn on continuous recording, go to **Configuration > Recording and events > Recording method**. 2. Select the camera and turn on **Continuous**.
Can't record on the specified drive	1. To use a different storage, go to **Configuration > Storage > management**. 2. Add the storage and configure the storage settings for the cameras.
Can't install the AXIS Video Content Stream application	1. To install the application manually, go to **Configuration > Devices > Management**. 2. Select a camera and click  .

Recording doesn't start

If recordings don't start, or if they stop after a few seconds, the disk is full or there's too much intruding data.

- In the server configuration sheet, under **Recording Storage** check that there's free space and no intruding data.
- Increase the storage limit for the video management system.
- Assign more storage to the storage pool. See *Configure storage, on page 67*.

Recording gaps during continuous recording

Gaps trigger alarms labeled **Recording errors**. The gaps can occur for several reasons, such as:

- Server overload
- Network issue
- Camera overload
- Disk overload

Check whether the recording gaps occur on all cameras. If they don't occur on all cameras, it may indicate camera overload. Use these questions to help identify the cause:

- How often does the gap occur – every hour or every day?
- How long is the gap – seconds or hours?
- At what time does the gap occur?

Possible solutions:

- In the server task manager, check whether any hardware resource is being used more than normal. If the disk shows signs of overuse, add more disks and move some cameras to record to the new disks.
- Reduce the volume of data written to the disk (video settings, Zipstream, frame rate, resolution). Consider the throughput estimated by AXIS Site Designer, see *axis.com/support/tools/axis-site-designer*.

For more information, see *Live view and playback performance, on page 211*.

Can't play exported recordings

If Windows Media Player doesn't play your exported recordings, check the file format. To play your exported recordings, use Windows Media Player (.asf) or AXIS File Player (.asf, .mp4, .mkv).

For more information, see *Play and verify recordings in AXIS File Player, on page 6*.

Note

AXIS File Player automatically opens all recordings that are in the same folder as the player.

Recordings disappear

The system saves recordings only for a specified number of days. To change the number of days, go to **Configuration > Storage > Selection**.

If storage is full, the system may delete recordings before the retention period ends. To avoid full storage, try the following:

- Add more storage. Go to **Configuration > Storage > Management**.
- Change the amount of storage space assigned to AXIS Camera Station Pro. Go to **Configuration > Storage > Management**.
- Reduce the size of recorded files by changing, for example, resolution or frame rate. Go to **Configuration > Devices > Stream profiles**.
  - Use the H.264 video format for recording. The M-JPEG format requires much more storage space.
  - Use Zipstream to further reduce the size of the recordings.

Failover recording issues

The bandwidth between the camera and the server is insufficient to transfer the recording	Increase the bandwidth.
The camera didn't record to the SD card during the disconnection	• Do a check of the camera's server report. See *axis.com/support/troubleshooting*. • Make sure that the SD card works and there are recordings on it.
The camera time changed or shifted since the disconnection	• Make sure to set up NTP for future recordings. • Synchronize the camera's time with the server, or use the same NTP server on the camera as on the server.

Note

Failover recording doesn't work during controlled server shutdowns or connection interruptions shorter than 10 seconds.

Live view

Live view and playback performance

This section describes possible solutions if you experience either frame loss or graphical issues within your AXIS Camera Station Pro client.

Client hardware	
Verify that the graphic card's or network adapter's driver is up to date	1. Open the DirectX Diagnostic Tool (search for dxdiag on the computer). 2. Go to the manufacturer's website to make sure the driver is the latest for this OS. 3. Check that the client and server run on the same machine. 4. Try to run the client on a dedicated computer.
Verify the number of monitors	We don't recommend more than two monitors per graphics card. Note We don't support running the client on a virtual machine.
The graphics card doesn't support the encoding format configured under **Configuration > Devices > Stream Profiles**	• Make sure the graphics card supports the encoding format of your streams. • Try using different encoding formats. • If a supported encoding format doesn't work as expected on multiple cameras, make sure your graphics card drivers are up to date.

Connected devices	
Many clients connected at the same time	Based on your typical use case, make sure the system meets the requirements and follow the hardware guidelines. See *Server requirements in the AXIS Camera Station Pro Installation and migration guide*.
The camera is connected to another video management system than AXIS Camera Station Pro	Disconnect the camera from the other client and default the camera before you connect it to AXIS Camera Station Pro.
One camera uses many different streams, especially high resolution	This could be a problem especially for some M-Line cameras or multi-sensor cameras. • Change the stream to the same streaming profile or lower resolution. See *Stream profiles, on page 49*.

Server overload	
Unusual CPU or RAM usage corresponding to the same time as the issue	Make sure no other application that consumes CPU or RAM runs at the same time.

Network issue	
Unusual bandwidth usage corresponding to the same time as the issue	Make sure no other application that uses a lot of bandwidth runs at the same time.
Enough bandwidth, remote or local network	• Look over your network topology. • Do a health check on any network device, such as switch, router, network adapter, and cable, in use between cameras, server and client.

No video in live view

Live view doesn't display video from a known camera.

- Turn off hardware decoding. Hardware decoding is set to **Auto** by default. See Hardware decoding in *Streaming, on page 108*.
- If you have an antivirus software installed, it might block live streams or AXIS Camera Station Pro folders and processes. See the *FAQ*.

Other possible solutions:

- If you can't see the live view through the web interface, or if the web interface doesn't work, troubleshoot the camera. Go to *axis.com/support/troubleshooting*.
- Create a camera server report. Go to *axis.com/support/troubleshooting*.
- Make sure the firewall doesn't block connections on certain ports, see *General, on page 191*.
- Make sure the Desktop Experience was installed for supported Windows server OS versions. See *Scheduled export, on page 116*.
- Verify that the lower resolution stream works correctly.

If none of the above helps, go to *Escalation process, on page 222*.

Hardware decoding performance

Use this troubleshooting guide if you experience lagging, jerky, or choppy video, high CPU usage during live view, or frequent "Reconnecting to camera" messages.

1. Update your graphics card drivers. Outdated drivers are the most common cause of hardware acceleration problems. Go to the manufacturer's website (NVIDIA, AMD, or Intel) and download the latest driver for your GPU model.
2. Adjust the hardware decoding mode. Go to **Configuration > Client > Streaming** :
   - If the mode is **Automatic** or **On** and you're seeing issues, set it to **Off**. If performance improves, your GPU may not have enough capacity for the current stream load. See step 6.
   - If the mode is **Off** and CPU usage is high, try **Automatic** or **On**, provided you have a capable GPU.
3. Monitor system resources. Open Windows Task Manager (Ctrl + Shift + Esc) and go to the **Performance** tab:
   - CPU usage consistently above ~80% without hardware decoding suggests the system may be underpowered for the number or resolution of streams.
   - GPU dedicated memory near capacity with hardware decoding on indicates a GPU bottleneck.
4. Reduce the number of cameras displayed at the same time, or switch cameras to lower-resolution stream profiles to reduce the load on your system.
5. Make sure your cameras are streaming in H.264 or AV1. Other codecs don't use hardware decoding.
6. Evaluate GPU capabilities. Even a GPU that supports hardware decoding may have limits on resolution or frame rate. For setups with many high-resolution streams, check the *AXIS Camera Station Pro client requirements* and consider upgrading to a GPU with more VRAM and higher decode throughput.
7. If none of the above helps, contact *Axis support* and have the following ready:
   - System hardware (CPU, GPU, RAM).
   - Operating system version.
   - Graphics driver version.
   - AXIS Camera Station Pro version.
   - Specific symptoms and reproduction steps.

Storage

Network storage isn't accessible

If you use the local system account to log in to AXIS Camera Station Pro service control, you can't add network storage that links to shared folders on other computers.

To change the service logon account:

1. Open **Windows Control Panel**.
2. Search for "Services".
3. Click **View local services**.
4. Right-click AXIS Camera Station Pro and select **Properties**.
5. Go to the **Log on** tab.
6. Change from **Local System account** to **This account**.
7. Select a user with access to Windows Active Directory.

Network storage is unavailable

Make sure the computer and server that run the video management software are part of the same domain as the network storage.

Can't reconnect to a network storage with new username and password

If your network storage requires authentication, it's important to disconnect the network storage from all ongoing connections before you change your username and password.

To change the username and password for a network storage and reconnect:

1. Disconnect your network storage from all ongoing connections.
2. Change the username and password.
3. Go to **Configuration > Storage > Management** and reconnect your network storage with your new username and password.

Motion detection

Common issues

Can't install the AXIS Video Motion Detection application	To install the application manually, go to *Install camera applications, on page 62*.
Can't retrieve current motion detection	Restore the camera to factory settings: 1. Go to **Configuration > Devices > Management**. 2. Right-click the problem camera and click **Restore the camera to factory settings**. The camera is unavailable during the reset. IP and HTTPS settings aren't affected. When the reset is done, the status column shows **Set password**. Click **Set password** to reconnect the camera to the server.

Motion detection not configured	1. To configure motion detection manually, go to **Configuration > Recording and events > Recording method**. 2. Select the camera and click **Motion settings** to configure motion detection.
Motion detection isn't turned on	1. Go to **Configuration > Recording and events > Recording method**. 2. Select the camera and turn on **Motion detection** to turn on motion detection recording.

The motion detection detects too many or too few moving objects

This section describes possible solutions if you have more or fewer detections in your recordings related to Video Motion Detection.

Adjust motion settings

You can select motion settings to adjust the area that detects moving objects.

1. Go to **Configuration > Recording and events > Recording method**.
2. Select the camera and click **Motion Settings**.
3. Choose settings according to the camera firmware.

AXIS Video Motion Detection 2 and 4	You can configure the area of interest. See *Edit AXIS Video Motion Detection 2 and 4, on page 78*.
Built-in motion detection	You can configure the included and excluded windows. See *Edit built-in motion detection, on page 79*.

Adjust trigger period

The trigger period is the interval between two successive triggers. Use this setting to reduce the number of successive recordings. If an additional trigger occurs within the interval, the recording continues and the trigger period starts over.

To change the trigger period:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select the camera.
3. Under **Advanced** adjust **Trigger period** in seconds.

Action rules

Unexpected I/O trigger events

If you get unexpected input/output events around 1:15 am, replace your existing I/O triggers with device event triggers.

Audio

No audio in live view

If there's no audio in live view, do the following:

- Make sure that the camera has audio capabilities.
- Make sure that the computer has an audio card and that the card is in use.
- Make sure that the profile in use was configured for audio.
- Make sure the user has access rights to audio.

Configure profiles for audio

1. Go to **Configuration > Devices > Stream profiles**.
2. Select the camera.
3. Select **MPEG-4** or **H.264** under **Format** in the video profile settings.
4. Under **Audio**, select a microphone in the **Microphone** drop-down menu.
5. Select when to use audio in the **Use microphone for** drop-down menu.
6. If applicable, select a speaker in the **Speaker** drop-down menu.
7. Click **OK**.

Check and change user access rights

Note

To follow these steps, you must have administrator rights to AXIS Camera Station Pro.

1. Go to **Configuration > Security > User permissions**.
2. Select the user or group.
3. Select **Audio listen** or **Audio speak** for a specific device.
4. Click **Apply**.

No audio in sequences

You can turn on or off audio in stream profiles. For more information, see *Stream profiles, on page 49*.

No audio in playback

Audio is available in playback if you turn on audio in the profile used for the recording.

Note

You can't use audio with M-JPEG video. Select another video format.

To use audio in recordings:

1. Go to **Configuration > Devices > Stream profiles** to set the video format for the video profile you want to use.
2. Go to **Configuration > Recording and events > Recording method**.
3. Select the camera.
4. Select the profile you configured from the **Profile** drop-down menu.
5. Click **Apply**.

Rule-triggered recordings

To enable audio in an existing rule:

1. Go to **Configuration > Recording and events > Action rules**.
2. Select the rule and click **Edit**.
3. Click **Next** to go to **Actions**.

4. Select the **Record** action and click **Edit**.
5. Select a profile that uses audio.
6. Click **Finish** to save.

Login

Unable to log in or connect to server

This section describes login and connection problems that occur when connected to a single server. When you're logged in to multiple servers, the client starts and shows the connection status in the status bar. For more information about the connection status, see *Connection status, on page 117*.

The username or password is incorrect	• Review the spelling or use a different account. • Make sure the user has access rights to AXIS Camera Station Pro server. • The clocks in AXIS Camera Station Pro server and client must be synchronized. For domain users, the domain server clock must be synchronized with the server and client. • A user that wasn't added to the server but is a member of the local administrators group must run the client as administrator. • For information about user access rights, see *User permissions, on page 121*.
A user isn't authorized to log in to the server	Add the user in the **User permissions** dialog.
Unable to verify message security	The server and client UTC times must be reasonably synchronized. Adjust the client and server time to be within 3 hours from each other.
No contact with the server	• Make sure the server computer can connect to the network. • Make sure the server computer is running. • Make sure the firewall is properly configured. • Check the spelling of the server address. • Check the client proxy settings.
No response from the server	Make sure that you connect to the right computer and that AXIS Camera Station Pro server is running.
Client can't connect to the server	Make sure that your network is properly configured: • Verify that the OS is supported. For a full list of the supported OS, go to *release notes*. • From Service Control, verify that the AXIS Camera Station Pro server is running, or start the server if necessary. • Verify that the client and the server are connected to the same network. If not, the client should use the server's external IP address. • On the server machine, configure the server proxy settings in Windows Internet Options. • Configure the client proxy setting at the login page, select **Change proxy settings**. • On the client machine, configure the client proxy settings in Windows Internet Options.

Unable to connect to the server	• Make sure the AXIS Camera Station Pro server's address and port are correct. Verify the port range is set correctly in Service Control. • Make sure that no NAT, firewall, or antivirus software blocks the connection to the server. See *Domains and ports for Secure Remote Access v2, on page 193* for more information. • Use AXIS Camera Station Pro service control to make sure that the server is running. – Open AXIS Camera Station Pro service control, see *AXIS Camera Station Pro service control, on page 189*. – View the server status in the **General** tab. If the status is **Stopped**, click **Start** to start the server.
Unable to find the server	• Make sure that the server computer can connect to the network. • Make sure the AXIS Camera Station Pro server's address and port are correct. • Make sure that no NAT, firewall, or antivirus software blocks the connection to the server. • Verify your client DNS settings are correct. • Verify your DNS server has an entry for the server hostname and IP address.
Unable to connect to server	Make sure the server computer and the network aren't overloaded.
The server and client version differs	Upgrade the server to run the same version as the client.
The local AXIS Camera Station Pro server doesn't run	Use service control to start AXIS Camera Station Pro, or select a remote server to log in to.
This computer doesn't have the AXIS Camera Station Pro server installet	Install the AXIS Camera Station Pro server or choose a different server.
The selected server list is empty	To add servers to the server list, click **Edit** next to the server list selection.

Licenses

License registration issues

If automatic registration fails, try the following:

- Make sure that the system is registered to an organization.
- Go to **Configuration** and make sure that **Automatic licensing** is turned on. See *Manage licenses, on page 119*.
- Make sure the server's time is up to date.

For more information, see *AXIS Camera Station Pro Installation and migration guide*.

Users

Can't find domain users

If the domain user search fails, change the service logon account:

1. Open **Windows Control Panel**.

2. Search for "Services".
3. Click **View local services**.
4. Right-click AXIS Camera Station Pro and select **Properties**.
5. Click the **Log on** tab.
6. Change from **Local System account** to **This account**.
7. Select a user with access to Windows Active Directory.

Certificate errors

AXIS Camera Station Pro can't communicate with the device until you solve the certificate error.

Possible errors	
Certificate Not Found	If you know the reason, click **Repair**. If you suspect unauthorized access, investigate the issue before you restore the certificate. Click **Advanced** to view the certificate details. Possible reasons for removing the certificate: • The device was reset to factory default. • Secure HTTPS communication was disabled. • An unauthorized person accessed and modified the device.
Untrusted Certificate	If you know the reason, click **Trust This Device**. If not, investigate the issue before you trust the certificate. Click **Advanced** to view the certificate details.

Missing password for certificate authority

If you have a certificate authority in AXIS Camera Station Pro without a stored password, the following alarm appears:

You need to provide a password for the Certificate Authority certificate. Read the user manual for more information.

You can resolve this issue in three ways:

- Turn on HTTPS on a device
- Import an existing certificate authority
- Generate a new certificate authority

To turn on HTTPS on a device:

1. Go to **Configuration > Devices > Management**.
2. In the list, right-click a device and select **Security > HTTPS > Enable/Update**.
3. Click **Yes** to confirm.
4. Enter the certificate authority password.
5. Click **OK**.

To import an existing certificate authority:

1. Go to **Configuration > Security > Certificates > Devices**.
2. Under HTTPS, turn off **Validate device certificate**.

3. Under **Certificate authority**, click **Import**.
4. Enter your password and click **OK**.
5. Select the number of valid days of the signed client/server certificates.
6. Go to **Configuration > Devices > Management**.
7. Right-click the devices and select **Security > HTTPS > Enable/Update**.
8. Go to **Configuration > Security > Certificates > Devices** and turn on **Validate device certificate**.

Note

AXIS Camera Station Pro loses its connection to the devices, and some system components restart.

To let AXIS Camera Station Pro generate a new certificate authority:

1. Go to **Configuration > Security > Certificates > Devices**.
2. Under HTTPS, turn off **Validate device certificate**.
3. Under **Certificate authority**, click **Generate**.
4. Enter your password and click **OK**.
5. Select the number of valid days of the signed client/server certificates.
6. Go to **Configuration > Devices > Management**.
7. Right-click the devices and select **Security > HTTPS > Enable/Update**.
8. Go to **Configuration > Security > Certificates > Devices** and turn on **Validate device certificate**.

Note

AXIS Camera Station Pro loses its connection to the devices, and some system components restart.

Time synchronization

Windows time service isn't running

The Windows Time service and the NTP server are out of sync. This can be because the Windows Time service can't reach the NTP server.

- Make sure the NTP server is online.
- Make sure the firewall settings are correct.
- Make sure the device is on a network that can reach the NTP server.

For assistance, contact your system administrator.

Detected time difference on a device

The device is out of sync with the server time. The recording is timestamped with the time when the server received it, instead of the time when the device recorded it.

1. Go to **Configuration > Devices > Time synchronization** and review the server time offset.
2. If the server time offset is more than 2 seconds:
   2.1. Select **Enable time synchronization**.
   2.2. Make sure the device can reach the specified NTP server.
   2.3. Reload the device under **Configuration > Devices > Management**.
3. If the server time offset is less than 2 seconds, the device might not send sufficient data for time synchronization.
   3.1. Clear **Send alarm when the time difference between server and device is larger than 2 seconds** to turn off alarms.

For assistance, contact Axis support.

Secure Remote Access v2

Unable to connect to cloud services locally

To resolve connectivity issues with cloud services:

1. Open AXIS Camera Station Pro and go to **Configuration** > **Connected services** > **Management**.
2. Verify that **Status** is green. If it's not, check your internet connection.
3. If the issue persists, contact Axis support for assistance.

Unable to connect to cloud services remotely

In AXIS Camera Station Pro:

1. Go to **Menu** > **Help** and click on **Status of Axis services**. This will open the status page of *https://status.axis.com*, where you can check for maintenance notifications or scheduled downtime.
2. In the Axis Camera Station Pro section, expand the drop-down list to check whether cloud services are accessible.
3. Verify that your My Axis account is invited to the correct organization.

In AXIS Camera Station Pro Mobile App:

1. Go to **More** > **Help section** and click on **Status of Axis services**. This will open the status page of *https://status.axis.com*, where you can check for maintenance notifications or scheduled downtime.
2. Ensure you have a stable internet connection. Try testing with a different mobile device to help identify the cause of the issue.
3. Verify that your My Axis account is invited to the correct organization.

If the issue persists, contact Axis support for assistance.

General issues with packet loss, latency, or incorrect routing

1. Ensure that you have internet access. The main ports used are 80 and 443 and should also be open for outbound traffic.
2. Depending on your router, you may need to open the following extra domains with ports:
   - https://eu.login.connect.axis.com with port 433
   - https://eu.cs.connect.axis.com with port 433
   - https://api.vms.axis.cloud with port 433
   - wss://signaling.prod.webrtc.connect.axis.com with port 433
   - https://*.turn.prod.webrtc.connect.axis.com with ports 443, 3478, 5349 and 49152-65535

   Note

   The asterisk " * " is dynamic and consists of a combination of region and a non-static server ID's.)

For further assistance, contact Axis support.

Technical support

Technical support is available for customers with a licensed version of AXIS Camera Station Pro. To contact technical support, go to ☰ > **Help** > **Online Support** or *axis.com/support*.

We recommend that you attach the system report and screenshots to the support case.

Go to ☰ > **Help** > **System report** to create a system report.

Escalation process

When you have issues that can't be solved using this guide, escalate the issue to *Axis online helpdesk*. For our support team to understand your issue and be able to solve it, you must include the following information:

- A clear description on how to reproduce the issue, or under what circumstances the issue happens.
- The time the issue occurred, and, if applicable, the name or IP address of the affected camera.
- AXIS Camera Station Pro system report generated directly after the issue happens. The system report must be generated from the client or server where the issue was reproduced. If the issue reoccurs in a predictable way, enable debug logging for both the server and the client to capture the issue more completely. Remember to disable debug logging when done.

For some issues, the support team may request additional information.

Note

If the file is larger than 1 GB, for example, a network trace or database file, use a secure file sharing service that you trust to send the file.

Additional information	
Debug-level logs	Debug-level logs are disabled by default because the logfile size is limited. If you enable debug level logging, remember to disable it once you have generated the system report. Server: **Configuration > Server > Settings > Enable debug logging** Client: **Configuration > Client > Settings > Enable debug logging**
Live view and playback debug overlay	When you encounter an issue with live view or playback, it's helpful to have a screen recording of the debug overlay. This recording should capture the entire screen, including the system clock so we can trace the problem in the logs. • Press Ctrl + I one time to display overlay information in the live view. • Press Ctrl + I twice to add debug information. • Press Ctrl + I three times to hide the overlay.
Database files	Use this in cases where we have to examine or manually repair the database. Select **Include database in the report** before you generate the system report. Include this any time there's an issue with starting the AXIS Camera Station Service.
Screenshots	When adding screenshots, capture the entire screen to increase the context. If you believe that it's ambiguous with a fullscreen screenshot, point to the focus area with arrows.

Additional information	
Screen recordings	Use screen recordings when the problem is difficult to describe in words, for example when reproducing the issue involves many interactions in the user interface.
Recording files	Support may ask for you to provide examples of the .acsm and .acsi files that AXIS Camera Station uses to store recordings. This applies when there's an issue with playback or export of recordings, or if there are issues with AXIS File Player. You can find these files in the storage location you selected for each camera.

T10196821

2026-06 (M32.2)