AXIS Camera Station 5

User manual

About AXIS Camera Station 5

AXIS Camera Station 5 is a complete monitoring and recording system for small and midsize installations.

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 5 release notes or the *AXIS OS Portal*. To check which products work with AXIS Camera Station 5, see *Compatible products*.

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

Access options

AXIS Camera Station 5 server – handles all communication with cameras, video encoders, and auxiliary devices in the system. The total bandwidth available limits the number of cameras and encoders each server can communicate with.

AXIS Camera Station 5 client – provides access to recordings, live video, logs, and configuration. You can install the client on any computer, enabling remote viewing and control from anywhere on the internet or corporate network.

AXIS mobile viewing 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. It uses HTTPS to communicate with the AXIS Camera Station 5 server. Configure the mobile communication and streaming ports as described in the Server settings section in *General*. For more information about how to use the app, see *AXIS Camera Station Mobile App user manual*.

Tutorial videos

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

System features

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

What's new?

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

Helpful links for an administrator

Here are some topics that might interest you:

- *Connect to a server, on page 8*
- *Configure devices, on page 37*
- *Configure storage, on page 61*
- *Configure recording and events, on page 66*
- *Configure connected services, on page 99*
- *Configure server, on page 102*
- *Configure licenses, on page 110*
- *Configure security, on page 112*

More manuals

- *AXIS Camera Station Integrator Guide*
- *What's new in AXIS Camera Station*
- *AXIS Camera Station Installation and Migration Guide*
- *AXIS Camera Station Mobile App*
- *AXIS Camera Station Feature Guide*
- *AXIS Camera Station tutorial videos*
- *AXIS Camera Station Troubleshooting Guide*
- *AXIS Camera Station System Hardening Guide*

Helpful links for an operator

Here are some topics that might interest you:

- *AXIS Camera Station getting started guide for operators*
- *Connect to a server, on page 8*
- *Configure client, on page 95*
- *Live view, on page 12*
- *Playback recordings, on page 21*
- *Export recordings, on page 23*
- *AXIS Camera Station cheat sheet - review and export*

Quick start

This tutorial walks you through the steps to get your system up and running.

Before you start:

- Configure the network depending on your installation. See *Network configuration*.
- Configure your server ports if needed. See *Server port configuration*.
- Consider security issues. See *Security considerations*.

For administrators:

1. *Start the video management system*
2. *Add devices*
3. *Configure recording method, on page 5*

For operators:

1. *View live video, on page 5*
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 5 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 5 server installed on the same computer as the client.

You can connect to multiple AXIS Camera Station 5 servers in different ways. See *Connect to a server*.

Add devices

The **Add devices** page opens the first time you start AXIS Camera Station 5. AXIS Camera Station 5 searches the network for connected devices and shows a list of devices found. See *Add devices*.

1. Select the cameras you want to add from the list. If you can't find your camera, click **Manual search**.
2. Click **Add**.
3. Select **Quick configuration** or **Site Designer configuration**. Click **Next**. See *Import Site Designer projects, on page 40*.
4. Use the default settings and ensure the recording method is **None**. Click **Install**.

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 21* 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 23* 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**. The verification result page appears.

Note

- Digital signature is different from Signed video. Signed video allows you to trace video back to the camera it came from, making it possible to verify that the recording 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 5 if the AXIS Camera Station 5 client, AXIS Camera Station 5 server, and the connected network devices are on different networks.

Client proxy settings

When a proxy server separates the client and the server, configure the client proxy settings.

1. Open the AXIS Camera Station 5 client.
2. Click **Change client proxy settings**.
3. Change the client proxy settings. See *Client proxy settings*.
4. Click **OK**.

Server proxy settings

When a proxy server separates the network devices and the server, configure the server proxy settings.

1. Open AXIS Camera Station 5 Service Control.
2. Select **Modify settings**.
3. In the Proxy settings section, use the default **System account internet option** or select **Use manual proxy settings**. See *General*.
4. Click **Save**.

NAT and Firewall

When a NAT, firewall, or similar separates the client and the server, configure the NAT or firewall to ensure that the HTTP port, TCP port, and streaming port specified in AXIS Camera Station 5 Service Control can pass through the firewall or NAT. Contact the network administrator for instructions on configuring the NAT or firewall.

See *Port list for AXIS Camera Station 5, on page 167* for more information.

Server port configuration

AXIS Camera Station server uses ports 55752 (HTTP), 55754 (TCP), 55756 (mobile communication), and 55757 (mobile streaming) for communication between the server and the client. You can change the ports in AXIS Camera Station Service Control if required.

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

Security considerations

To prevent unauthorized access to cameras and recordings, keep the following in mind:

- Use strong passwords for all network devices (cameras, video encoders, and auxiliary devices).
- Install AXIS Camera Station 5 server, cameras, video encoders, and auxiliary devices on a secure network separate from the office network. You can install the AXIS Camera Station 5 client on a computer on another network, for example, a network with internet access.
- Make sure all users have strong passwords. Windows® Active Directory provides a high level of security.

Connect to a server

Using the AXIS Camera Station 5 client, you can connect to multiple servers or a single server installed on the local computer or somewhere else on the network. You can connect to AXIS Camera Station 5 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 – See *Sign in to AXIS Secure Remote Access, on page 8*.

Note

When trying to connect to a server for the first time, the client checks the server certificate ID. To ensure that you're connecting to the correct server, manually verify the certificate ID with the one displayed in AXIS Camera Station 5 Service Control. See *General, on page 166*.

Server list	To connect to servers from a server list, select a 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 5, click **Import server list** and browse to an .msl file. See *Server lists*.
Delete saved passwords	To delete saved usernames and passwords all connected servers, click **Delete saved passwords**.
Change client proxy settings	You might need to change the client proxy settings to connect to a server, click **Change client proxy settings**. See *Client proxy settings*.

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 reload all the available remote servers. If the server is configured to accept clients on a different port than the default port number 55754, enter the IP address followed by the port number, for example, 192.168.0.5:46001.
3. You can:
   - 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

Important

To improve security and functionality, we're upgrading **Axis Secure Remote Access** (v1) to **Axis Secure Remote Access v2**. We're discontinuing the current version on December 1st, 2025, and we strongly recommend that you upgrade to Axis Secure Remote Access v2 before that.

What does this mean for your AXIS Camera Station 5 system?

- After December 1st, 2025, you will no longer be able to remotely access your system using **Axis Secure Remote Access** (v1).
- To use **Axis Secure Remote Access v2**, you must upgrade to AXIS Camera Station Pro version 6.8. This upgrade is currently free for all AXIS Camera Station 5 users until March 1st, 2026.

Note

- When trying to connect to a server using Axis Secure Remote Access, the server can't upgrade the client automatically.
- If the proxy server is between the network device and the AXIS Camera Station 5 server, you must configure the proxy settings in Windows on the AXIS Camera Station 5 server to access the server using AXIS Secure Remote Access.

1. Click the **Sign in to AXIS Secure Remote Access** link.
2. Enter your My Axis account credentials. See *Axis Secure Remote Access*.
3. Click **Sign in**.
4. Click **Grant**.

Client proxy settings

These settings apply to a proxy server that lies between the AXIS Camera Station 5 client and the AXIS Camera Station 5 server.

Note

Use AXIS Camera Station 5 Service Control to configure proxy settings for a proxy server that lies between an AXIS Camera Station 5 server and the network cameras. See *AXIS Camera Station 5 service control*.

Select the appropriate option for your setup.

- **Direct connection**: Select this option if there's no proxy server between the AXIS Camera Station 5 client and the AXIS Camera Station 5 server.
- **Use Internet Options settings** (default): Select this option to use the Windows settings.
- **Use manual proxy settings**: Select this option to configure the proxy settings manually. Provide the required information in the Manual settings section.
  - **Address**: Enter the address or hostname of the proxy server.
  - **Port**: Enter the port number of the proxy server.
  - **Do not use proxy server for addresses beginning with**: Enter the servers that you want to exclude from access by the proxy. Use semicolons to separate the entries. You can use wildcards in the addresses or hostnames, for example: "192.168.*" or "*.mydomain.com".
  - **Always bypass proxy server for local addresses**: Select this option to bypass the proxy when connecting to a server on the local computer. Local addresses don't have a domain name extension, for example, http://webserver/, http://localhost, http://loopback, or http://127.0.0.1.

AXIS Camera Station 5 client

The Add devices page on the Configuration tab opens when you're using AXIS Camera Station 5 for the first time. See *Add devices*.

Tabs

Live view	View live video from connected cameras. See *Live view*.
Recordings	Search, play and export recordings. See *Recordings*.
Smart search 1	Locate important 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 34*.
Configuration	Administration and maintenance of connected devices, as well as settings for the client and servers. See *Configuration*.
Hotkeys	A list of hotkeys for actions. 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 142*.
Smart search 2	Use advanced filters to find vehicles and persons based on characteristics. See *Smart search 2, on page 31*.
System health monitoring	Monitor the health data from a single or multiple AXIS Camera Station 5 systems. See *System Health Monitoring BETA, on page 150*.
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 5 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	Open help-related options. Go to **Help** > **About** to see which AXIS Camera Station 5 client version you're using.
Log out	Disconnect from the server and log off from the AXIS Camera Station 5 client.
Exit	Exit and close the AXIS Camera Station 5 client.

Title bar

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

Status bar

The status bar can include the following:

- A warning icon appears when there is a time mismatch between client and server. Always make sure that the time on the client is synchronized with the time on the server 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 .
- The secure remote access usage shows how much data is left or how much overage has been used this month for the included amount in your service level. See *Axis Secure Remote Access*.
- **AXIS Camera Station 5 update available** appears when there is a new version if you're logged in as administrator. See *Update AXIS Camera Station 5, on page 105*.

Alarms and Tasks

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

Live view

The live view shows the views and cameras and live videos from the connected cameras, and it displays all the views and cameras of connected servers grouped by the server name when connecting to multiple AXIS Camera Station 5 servers.

Views provide access to all the cameras and devices added to AXIS Camera Station 5. A view can consist of one or several cameras, a sequence of items, a map, or a webpage. The live view updates the views automatically when you add or remove devices from the system.

All users can access views. For information about user access rights, see *User permissions, on page 112*.

For help on how 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 cameras, views, or sequences 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

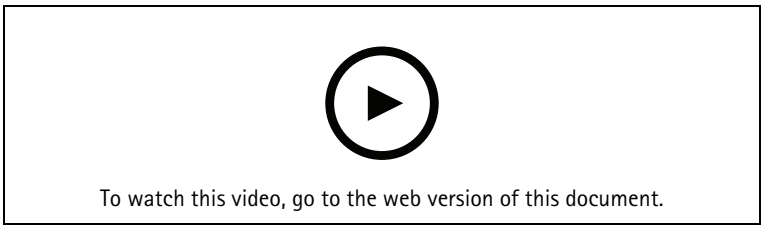
	Add a new split view, sequence, camera view, map, webpage, or folder.
	Edit a view or a camera name. For information on how to edit the camera settings, see *Edit camera settings*
	Remove a view. You need permissions to edit the view and all secondary views to remove it. For information on how to remove cameras from AXIS Camera Station 5, see *Cameras, on page 42*.
	As an administrator, you can lock the view and prevent operators or views from moving or editing the view.

Image management in live view

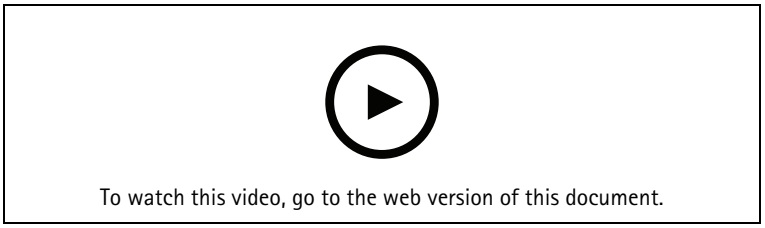
Navigate	To go to the camera view, right-click an image in a split view and select **Navigate**.
Take snapshot	To take a snapshot, right-click an image and select **Take snapshot**. The system saves the snapshot to the

	snapshot folder specified in **Configuration > Client > Settings**.
Add snapshot to Export	To add a snapshot to the export list in the Export tab, 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 where digital PTZ is enabled 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 in the image, 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 the image where you want to point the camera. To pan and tilt continuously in the live view image, move the cursor to the center of the image to show the navigation arrow. Then click and hold to pan in the direction of the navigation arrow. To pan and tilt the image at a higher pace, click and hold to make the navigation arrow longer.
Set focus	To adjust camera focus, right-click the image and select **Set focus**. Click **AF** to focus the camera automatically. To adjust focus manually, select the bars on the **Near** and **Far** sides. Use **Near** to focus on objects close to the camera. Use **Far** to focus on objects far away.
Focus recall zone	To add or remove focus recall zone, right-click the image, select **Focus recall zone**.
Autotracking on/off	To turn on or turn off autotracking for an Axis PTZ camera with AXIS PTZ Autotracking configured, right-click the image, 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 coordinates for repeatable positioning. 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 administrators 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 the cursor 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 the cursor 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

Administrators can turn off 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 43*.

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 98*.

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, webpages, maps and other split views in the split view.

Note

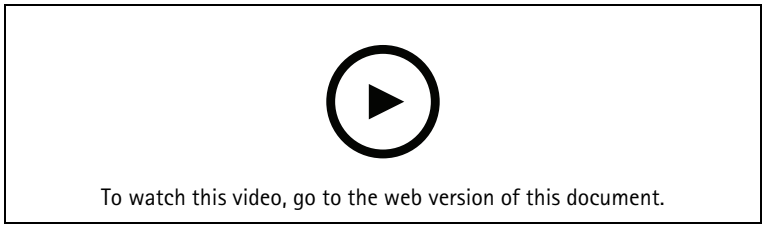
When connecting to multiple AXIS Camera Station 5 servers, you can add any view, camera, device, or audio zone from other servers to your split view.

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 template you want to use from the **Template** drop-down menu.
5. Drag and drop one or multiple views, audio zones, or cameras to the grid.
6. Click **Save view** to save the split view on the current server.

Set hotspot	To define a hotspot frame, right-click it and select **Set hotspot**. When you click another frame it opens in the hotspot. Hotspots are handy for asymmetric split views with one large and several small frames. The largest frame is typically the hotspot.
Stream profile	To set the stream profile for the camera, right-click a camera in the grid view and select **Stream profile** , See *Stream profiles*.



Add a split view

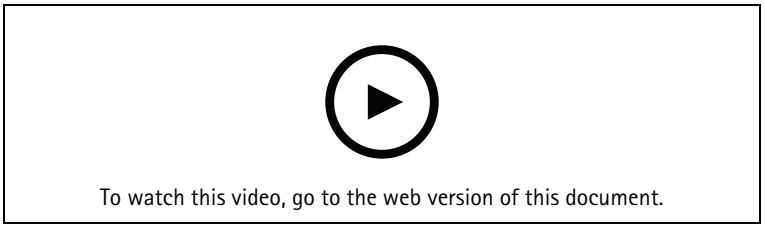
Door dashboard in split view

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

1. Add a door. See *Add a door, on page 122*.
2. Add the door dashboard to a split view, see *Split view, on page 15*.

Dashboard	To view door details, door status and lock status, open the **Dashboard** tab. The dashboard displays the following information: • Access control events with cardholder details, including photo, 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 in the same way it would if someone presented their credentials, which normally means it automatically locks 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

Sequence

A sequence switches between views.

Note

When connecting to multiple AXIS Camera Station 5 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 the sequence.
6. Optionally, set individual dwell times for each view.
7. For cameras with PTZ capabilities, select a PTZ preset from the **PTZ preset** drop-down list. See *PTZ presets*.
8. Click **Save view** to save the sequence on the current server.

Dwell time	Dwell time is the number of seconds to show a view, before switching to the next. You can set this individually for each view.



Add a sequence

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 5 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, sequences, webpages, 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.

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

Note

When connecting to multiple AXIS Camera Station 5 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 maximum size of the file is 20 MB, and BMP, JPG, PNG, GIF are supported.
5. Drag the views, cameras, other devices, and doors onto the map.
6. Click an icon on the map to edit the settings.
7. Click **Add label**, enter a label name, and set the size, rotation, style, and color of the label.

Note

You can edit some settings for multiple icons and labels at the same time.

8. Click **Save view** to save the map on the current server.

	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.
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.
Direction arrow	Shows arrows pointing in the direction of each camera's field of view. You can show arrows with or without coverage areas.

Coverage area	This option is only available for cameras and other 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** if you want the coverage area to flash when the camera is recording triggered by motion detection or other action rules. On the client settings page, you can turn off flashing coverage areas globally for all devices, see *Client settings, on page 95*.
Remove	Click to remove the icon from the map.



Add a map



Trigger audio from a map

Webpage

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

To add a webpage:

1. In the Live view tab, click .
2. Select **New webpage**.
3. Enter a name for the webpage.
4. Enter the webpage's full 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 can handle recording searches, playback, and export. The tab consists of a view of the recording and two panels where you can find views, images, playback tools, and cameras of the connected servers grouped by the server name, see *Live view*.

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

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

Note

You can't manually delete recordings from AXIS Camera Station 5. You must change the retention time under **Configuration > Storage > Selection** to delete the old recordings.

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

Use the timeline to navigate in the playback and find when a recording occurred. A red line in the timeline symbolizes a motion detection recording. A blue line in the timeline symbolizes a recording triggered by an action rule. 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. In a recording, move the timeline (scrubbing) to get an overview of the content and find specific occurrences.

Find recordings

	Click to select a date and time in the timeline.
	Use the filter to configure what type of recordings to show in the timeline.
	Use to find saved bookmarks, see *Bookmarks*.
Smart search 1	Use Smart search to search for recordings, 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 up or down to zoom in and out of the image and move the view to see other parts of the image. To zoom in on an area, place the cursor in the desired area and scroll to zoom.

Bookmarks

Note

- You can't delete a locked recording unless you manually unlock it.
- The system deletes locked recordings when you remove the camera from AXIS Camera Station 5.

	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, description, and unlock or lock the recording.
	Remove a bookmark. To remove multiple bookmarks, select multiple bookmarks and hold down CTRL or SHIFT to remove multiple bookmarks.
Prevent recording deletion	Select or clear to lock or unlock the recording.

Add bookmarks

1. Go to the recording.
2. In the timeline of the camera, 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 in the description to make the bookmark easy to find and recognize.
5. Select **Prevent recording deletion** to lock the recording.

Note

It's not possible to delete a locked recording. To unlock the recording, clear the option or delete the bookmark.

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

Export recordings

From the **Export** tab, you can export recordings to a local storage or network location. Here, you can also find information and a preview of the recording. It's possible to export multiple files at the same time, and you can select to export it to .asf, .mp4, and .mkv. 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 the .asf format.

Before you start, make sure you have permission to export. See *User permission for exporting, on page 25*.

Export recordings

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 recordings 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 file with a playlist 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 stop.
	To export recordings within the section markers, click .
Add recordings	To export 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 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 in the exported recording, deselect 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 (redaction) before exporting, on page 25*.
	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	To change to the **Export** tab if the **Incident report** tab is open, click **Switch to export**.
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 are from one camera.
Save	If you want to save the export list to a file, click **Save**.
Load	If you want to include a previously saved export list, click **Load**.
Include notes	To include notes of the recordings, select **Include notes**. The notes are available both as a .txt file in the exported folder and as a bookmark in the recording in AXIS File Player.

Export tab	
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 snapshots, drag the timeline in the preview to a specific location. Right-click the preview and select **Add snapshot**.

Advanced settings	
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 will 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 27*.
Export to Zip file	To export to a Zip file, select **Export to Zip file** and choose to enter a password for the exported Zip file.
Export format	From the **Export format** drop-down menu, select a format to export the recordings to. Exported recordings doesn'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**. Choose `Automatic` to use M-JPEG for M-JPEG format and H.264 for other formats.

User permission for exporting

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

To configure the permissions, go to *User permissions, on page 112*.

Edit recordings (redaction) 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** 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, 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 the bounding boxes overlap, the overlapped part fills in the order of Black, Pixelated, and 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 25*.
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 turns **Clear** and the not selected turns **Pixelated**.

Generate bounding boxes

To generate bounding boxes from the analytic data, turn on the camera's analytic data. See *Stream profiles, on page 43*.

1. In the **Export** tab or **Incident report** tab, click .
2. Click **Generate bounding boxes**.
3. Make sure that 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 5 starts the installation automatically when you add a camera to the system. See *Install camera application*.



Edit recordings before export

Play and verify exported recordings

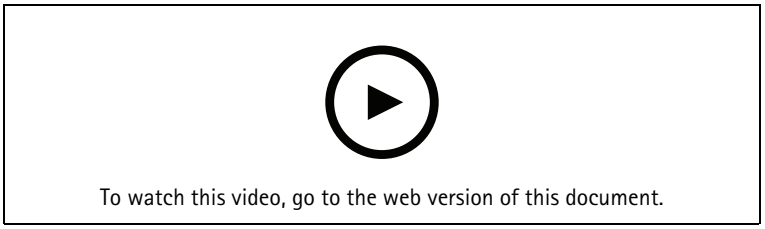
To prevent image tampering, you can add a digital signature to the exported recordings with or without password. Use AXIS File Player to verify the digital signature and to check for changes of the recording.

1. Go to the folder with the exported recordings. If the exported Zip file is password protected, input your password to open the folder.
2. Open AXIS File Player, the exported recordings automatically plays.
3. In AXIS File Player, click  to show the notes in the recordings.
4. In AXIS File Player, verify the digital signature for recordings 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 or network location. Here, 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 25*.



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 23*.
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 export incident report 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 in the exported recording, deselect 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 (redaction) before exporting, on page 25*.
	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 incident report	To change to the **Incident report** tab if the **Export** tab is open, click **Switch to incident report**.
Preferred stream profile	Select the stream profile in the **Preferred stream profile** dop-down.
Preview	To preview a recording, click the recording in the exported list and it starts to play. You can only preview multiple recordings if they are from one camera.
Save	If you want to save the incident report to a file, click **Save**.
Load	If you want to include 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 you want to include in the incident report.
Category	Select a category that the report belongs to.
Reference ID	A **Reference ID** is automatically generated, and you can manually change it if necessary. The reference id is unique and identifies the incident report.
Include notes	To include notes of the recordings and snapshots, select **Include notes**. The notes are available both as a .txt file in the exported folder and as a bookmark in the recording 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**. Choose `Automatic` to use M-JPEG for M-JPEG format and H.264 for 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 snapshots, 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 5 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. Move the mouse pointer to 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 the parts of a recording that have movement in a defined image area.

To increase search speed, select **Include analytics data** in stream profiles. 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 any unwanted results.
5. Select the start and end time, and date for the search. Use the SHIFT key to select a range of dates.
6. Click **Search**.

The search results appear on the **Results** tab. Here you can right-click one or many 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 the recordings.

When you turn on Smart search 2 for an Axis camera, AXIS Camera Station 5 starts recording metadata from that camera. Smart Search 2 uses the metadata to classify objects in the scene and lets you use filters to find things of interest.

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 application, on page 56*.
- Time synchronization between the AXIS Camera Station 5 server and cameras.

Note

General recommendations:

- We recommend using continuous recording. Using motion detection can result in detections without video.
- We recommend using the H.264 format if you want to preview recordings in the search result.
- Make sure that the lighting conditions are within the camera specification for optimal color classification. Use additional lighting if needed.

Workflow

1. *Configure smart search 2, on page 138*
2. Configure time synchronization between the AXIS Camera Station 5 server and cameras. See *Time synchronization, on page 60*.
3. Create a filter or load an existing filter. See *Search with filters, on page 31*.
4. Manage search results. See *Smart search results, on page 33*.

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 methods to speed it up:

- Turn on background server processing 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 at a given moment.
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 of 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 of you need to.
Size and duration	To filter by size and duration, click **Size and duration**, select the camera and turn on **Filter by size and duration on this camera**. Adjust the minimum width and height as a percentage of the total image. 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 that you want to include in the filter. Note The speed filter is available for products like radars 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**. 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 filter settings** and select a filter.
	To reset a filter, click and click **Reset**.

Smart search results

	To group detections that are likely to belong to the same event, you can group them in time intervals. Select an interval from the drop-down menu.
Latest first	Smart search 2 shows the 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. High confidence ignores 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 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 are not supported.
- Radar can only detect person and other vehicle. It's not possible to enable background server classification for radar.
- Object classification has unknown behavior for thermal cameras.
- Smart search 2 doesn't detect moving objects when a PTZ preset position changes and for a short recalibration period after the position change.
- 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 that you can use to find out more about what happened in an event. See *External data sources, on page 60* for more information. Here are a few examples:

- 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 the time AXIS Camera Station 5 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. The filters can vary depending on the data source type.
5. Enter any keywords in the search field. See *Optimize your search, on page 35*.
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	Access control is an example of a component that produces data. Use this option if you want to include data only from this specific component. Access control lets you filter on doors and zones, cardholders, and event types.
Third party	Use this option if you want 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. Here are a few examples:

Search results	
Server	The server that the event data are 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**. This feature only exports event information, not recordings or images.

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.

Configuration

On the Configuration tab, you can manage and maintain connected devices, as well as settings for the client and servers. Click + and select **Configuration** to open the Configuration tab.

Configure devices

In AXIS Camera Station 5, 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 5 only supports devices with IPv4 addresses.
- Some video encoders have one IP address for each video port. In this case, AXIS Camera Station 5 treats each video port as one device with one camera.

In AXIS Camera Station 5, 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

You can perform the following actions for devices:

- 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 in regard to 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 60*.

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 AXIS Camera Station 5 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 39*
   - *Find your video streams, on page 39*
   - *Find prerecorded videos, on page 39*
2. *Add devices, video streams or prerecorded videos, on page 40*

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 5.
Communicating	AXIS Camera Station 5 server is trying to access the device.
Device certificate not trusted	AXIS Camera Station 5 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 5 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 5 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 5 to trust the existing one.
Communication error	AXIS Camera Station 5 can't contact the device.
Enter password	AXIS Camera Station 5 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 5 will use this username and password for all devices on which the user exists.
Set password	The root account and password is not 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 that you show the generated password and make a copy of it. • Select to use this password for all devices with the `Set password` status.
Model not supported	AXIS Camera Station 5 doesn't support the device model.
Obsolete firmware	The device's firmware is old and you must update it before you can add the device.
Faulty device	The device parameters retrieved by AXIS Camera Station 5 are corrupt.
Set tilt orientation	Click the link to select tilt orientation Ceiling, Wall, or Desk, depending on how the camera is mounted. Tilt orientation is a required setting for some camera models.
Unsupported ONVIF device	AXIS Camera Station 5 doesn't support this third-party device.
Unsupported device	AXIS Camera Station 5 doesn't support this type of device.

Note

New HTTPS certificates are issued by AXIS Camera Station 5 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, type 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 the 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 the .mkv format to AXIS Camera Station 5.

.mkv file 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 47* 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. If you want to change the device's name, click the name in the list and enter a new name.
4. Select the devices, video streams, or prerecorded videos. Click **Add**.
5. Choose whether to use hostnames instead of IP when possible for the devices.
6. Choose **Quick configuration** if you just want to configure the basic settings.
   If you're importing a Site Designer project, see *Import Site Designer projects*.
7. Choose your **Retention time**, **Recording storage**, and **Recording method** preferences.

Note

If you choose the **Automatic** recording storage option, each camera will be assigned a storage with at least 32 GB capacity on a non-OS drive whenever possible. The system automatically selects storages with at least 15 GB available space, followed by storages with fewer cameras configured to record to them and any storages already installed in AXIS Camera Station 5.

8. Click **Install**. AXIS Camera Station 5 automatically enables HTTPS on the devices that support it.

Import 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 5. You can access the project using an access code or a downloaded Site Designer setup file.

To import a site designer project to AXIS Camera Station 5:

1. Generate an access code to the site designer project or download a project file.
   1.1. Sign in to *http://sitedesigner.axis.com* with your MyAxis 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 5 server has an internet connection. Or click **Download settings file** if your server doesn't have an internet connection.
2. In the AXIS Camera Station 5 client, go to **Configuration > Devices > Add devices**.
3. Select the cameras, and click **Add**.
4. Select **Site Designer configuration** and click **Next**.
5. Select **Access code** and enter the access code. Or select **Choose file** and find the downloaded Site Designer setup file.
6. Click **Import**. At import, AXIS Camera Station 5 tries to match the Site Designer project with the selected cameras by IP address or product name. You can select the correct camera from the drop-down menu if the match fails.

7. Click **Install**.

AXIS Camera Station 5 imports the following settings from the 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	✓	✓
Motion triggered recording: schedule and recording profile including frame rate, resolution, video encoding, and compression		✓
Continuous 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 just one of the recording profiles or if there are two identical recording profiles in the Site Designer project, AXIS Camera Station 5 sets the profile to medium.
- If you've defined both recording profiles in the Site Designer project, AXIS Camera Station 5 sets the continuous recording profile to medium and the motion-triggered recording to high.
- AXIS Camera Station 5 optimizes the aspect ratio, meaning the resolution can differ between the import and the Site Designer project.
- AXIS Camera Station 5 can set the audio settings if the device has a built-in microphone or speaker. To use an external audio device, you must manually enable it after installing it.
- AXIS Camera Station 5 doesn't apply audio settings to intercoms even if the settings in Site Designer differ. On intercoms, audio is always on in Live view only.



Add third-party devices

You can add third-party devices to AXIS Camera Station 5 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 5. See *Find your video streams, on page 39*.

For information about support for third-party devices, see the *latest technical paper*.

Note

You can download and run AXIS Camera Station Device Compatibility Tool to verify if your network video products are compatible with AXIS Camera Station 5 or later. The tool checks if the system can receive video streams from your network video products. See *AXIS Camera Station Device Compatibility Tool*.

AXIS Camera Station 5 is not ONVIF conformant, but it requires that third-party devices are ONVIF Profile S conformant and verified through AXIS Camera Station Device Compatibility Tool.

AXIS Camera Station 5 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 5)
- One video profile per camera
- Live view
- Continuous and Manual recordings
- Playback
- Recordings exports
- Device event triggers
- PTZ

Use view areas

Some camera models support view areas. AXIS Camera Station 5 lists view areas as individual cameras on the **Add devices** page. See *Add devices*.

Note

- All view areas in a network camera counts as one camera in the total number of cameras allowed by the AXIS Camera Station 5 license.
- The number of cameras you can add depends on the license.
- Each AXIS Camera Station 5 license allows a certain number of cameras.

To use view areas in AXIS Camera Station 5, you must first enable them 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, which differs depending on the camera model and firmware.

Cameras

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

On this page you can:

- Click a camera's address to open the its web interface. This requires that there's no NAT or firewall between the AXIS Camera Station 5 client and the device.
- Edit the camera settings. See *Edit camera settings*.

- Remove cameras. Doing this, AXIS Camera Station 5 deletes all recordings, including locked ones, associated with the deleted cameras.

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, deselect **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.
Username	Username for an administrator account on the camera.
Password	Password for an administrator account on the camera. AXIS Camera Station 5 uses the password to communicate with the camera.

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 5 client and the device.
- Edit the device settings, such as device name, address, and password.
- Remove devices.

Edit other device settings

To edit the settings for a non-camera device:

1. Go to **Configuration > Devices > Other devices**.
2. Select a device and click **Edit**.

Username	Username for an administrator account on the device.
Password	Password for an administrator account on the device. AXIS Camera Station 5 uses the password to communicate with 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 displays a list of all cameras.

The following profiles are available in Live view and recordings 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, meaning the stream profile changes automatically to **High**, **Medium**, or **Low** depending on the available size for the video stream.

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. This option is 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 toggleable overlays.
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 work 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. Optimize for storage uses more advanced compression tools to save additional storage compared to the default Zipstream setting. This profile 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:	Enable microphone audio for one or two streams. You can enable audio for Live view and recordings, Live view only, or Recordings only.

Advanced

Include analytics data	To allow data gathering for smart search during video streaming, select **Include analytics data**. This option is available only 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 enable FFmpeg streaming. This option is available only 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 up to 2000 milliseconds. This option is available only for an Axis PTZ camera with AXIS PTZ Autotracking. For a complete workflow to set up AXIS PTZ Autotracking in AXIS Camera Station 5, 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. Do not 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 5 client and AXIS Camera Station 5 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 5. See *Add devices*.

2. Configure the camera to use audio from the device. See *Stream profiles*.
3. Enable audio for Live view or Recording. See *Stream profiles*.

You can find the following examples in *AXIS Camera Station 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 5

Image configuration

You can configure the image settings for the cameras connected to AXIS Camera Station 5.

Note

The changes on image configuration are applied instantly.

To configure the image settings:

1. Go to **Configuration > Devices > Image configuration**, a list of all cameras added to AXIS Camera Station 5 is displayed.
2. Select the camera and the video feed is shown 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.

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 the same regardless of the color temperature of the light source. When selecting **Automatic** or **Auto**, the camera identifies the light source and compensates for its color automatically. If the result is not satisfactory, select an option corresponding to the type of light source. Available options depend on camera models.

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 spot of light, for example a light bulb, causes other areas in the image to appear too dark.

Dynamic contrast (wide dynamic range): Turn on to use wide dynamic range to improve the exposure when there is a considerable contrast between light and dark areas in the image. Use the slider to adjust dynamic contrast. Enable dynamic contrast in intense backlight conditions. Disable dynamic contrast 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.

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**, a list of cameras that can be used with PTZ is displayed. 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 where digital PTZ has been enabled
- ONVIF cameras that support PTZ presets.

Digital PTZ is enabled 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 5 and the camera's configuration page. We recommend that you configure PTZ presets in AXIS Camera Station 5.

- When a PTZ preset is configured in the camera's configuration page, you can only view the stream within the preset. The PTZ movements in live view can be seen and are recorded.
- When a PTZ preset is configured in AXIS Camera Station 5, you can view the complete stream of the camera. The PTZ movements in live view can't be seen and are not recorded.

Note

PTZ can't be used if the camera's control queue is enabled. For information about the control queue and how to enable and disable it, 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 the preset and click **Remove**. This will remove the preset from AXIS Camera Station 5 and from the camera.

Device management

Device management provides tools for administration and maintenance of devices connected to AXIS Camera Station 5.

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

If you have set up automatic check for new firmware versions in *Firmware upgrade settings, on page 99*, a link displays when there are new firmware versions available for devices. Click the link to upgrade the firmware versions. See *Upgrade firmware*.



Upgrade firmware versions

If you have set up automatic check for new software versions in *Update AXIS Camera Station 5, on page 105*, a link displays when there is a new AXIS Camera Station 5 version available. Click the link to install a new version of AXIS Camera Station 5.



Install a new version of AXIS Camera Station 5

A list of devices added to AXIS Camera Station 5 is displayed. 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 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 is not accessible.
  - **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:** No connection with the device 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 is not set up or the device still uses the default password. Click the link to set the root user password.
    - Type your password or click **Generate** to automatically generate a password up to the length allowed by the device. We recommend that you show the automatically generated password and make a copy of it.
    - Select to use this password for all devices with the `Set password` status.
    - Select **Enable HTTPS** to enable 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 5 does not 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 is some 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 is not trusted by AXIS Camera Station 5. 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 59*.
- **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 59*.
- **Manufacturer:** The manufacturer of the device.
- **Model:** The model of the device.
- **Firmware:** The version of firmware the device is currently using.
- **DHCP:** If the device is connected to the server using DHCP.
- **HTTPS:** The HTTPS status of the device. See HTTPS status in *Security, on page 57*.
- **IEEE 802.1X:** The IEEE 802.1X status of the device. See IEEE 802.1X status in *Security, on page 57*.
- **Server:** The AXIS Camera Station 5 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*.
- Set date and time on devices. See *Set date and time*.
- Restart devices.
- Restore devices to reset most settings, including the password, to their factory default values. The following settings are not reset: uploaded camera applications, boot protocol (DHCP or static), static IP address, default router, subnet mask, system time.

Note

- To prevent unauthorized access, we strongly recommend setting the 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 5server 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 application*.

- Reload devices when settings have been changed from the devices' configuration page.
- Configure devices. See *Configure devices*.
- User management. See *User management*.
- Manage certificates. See *Security, on page 57*.
- Collect device data. See *Collect device data*.
- Select to use IP address or hostname. See *Connection, on page 59*.
- Tag devices. See *Tags*.
- Enter device credentials. Right-click a device and select **Advanced > Enter device credentials** to enter password for the device.
- Go to the device's configuration tab and configure your device. See *Device configuration tab, on page 59*.

Assign IP address

AXIS Camera Station 5 can Assign IP address to multiple devices. New IP addresses can be obtained automatically from a DHCP server or assigned 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 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 5 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, subnet mask and default router are displayed in the Current IP address section.
   - 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 59*.

- For information about how to configure devices, see *Configuration methods*.
- For information about how to create a configuration file, see *Create configuration file*.
- For information about which settings can be copied, see *Configuration settings*.

Configuration methods

There are different methods to configure devices. AXIS Device management will attempt to configure 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 configuration of a single device by reusing some or all existing settings.

1. Go to **Configuration > Devices > Management**.
2. Right-click one device, select **Configure Devices > Configure**.
3. Select the settings to be applied. See *Configuration settings, on page 53*.
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, 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 to be applied. See *Configuration settings, on page 53*.
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 model or firmware even if some settings do not exist on all devices.

If some settings do not exist or can't be applied, the task status will show as Error in the Tasks tab at the bottom of the AXIS Camera Station 5 client. Right-click the task and select Show to display information about the settings that could not be applied.

Note

This method should only be used by experienced users.

1. Go to **Configuration > Devices > Management**.
2. Right-click the devices, select **Configure Devices > Configure**.
3. Click **Configuration File** to go to the configuration file. For how to create a configuration file, see *Create configuration file, on page 53*.
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. These settings can then be applied to other devices. For information on how to use the configuration file, see *Configuration methods*.

The displayed settings are the device settings that can be accessed using 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 device parameters that are used to 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.
- All device parameters are not accessible from AXIS Device management.

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

- **Insert device serial number variable:** This variable will be replaced with the serial number of the device that the configuration file is applied to.
- **Insert device name variable:** This variable will be 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:** This variable will be 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 5 Service Control.
- **Insert server time zone variable:** This variable will be replaced with the POSIX time zone of the server used when applying the configuration file. This can be used 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 pre-programmed Live view configuration profile for video encoding, image and audio settings. Stream profiles can be copied between devices.

- **Motion Detection Windows:** Motion detection windows are used to 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**, the Manage devices page is displayed for you to manage users of the devices.

When you set password or remove users for multiple devices, users that are not present on all devices are indicated with . Each user appears only once when the user is present on different devices with different roles.

Note

The accounts are device specific and not related to the user accounts of AXIS Camera Station 5.

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 that you set 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 5 are password protected.

The following characters can be used in passwords:

- letters A-Z, a-z
- numbers 0-9
- space, comma (,), period (.), colon (:), semicolon (;)
- !, ", #, $, %, &, ', (, +, *, -,), /, <, >, =, ?, [, \, ^, -, `, {, |, ~, @,], }

To set 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. Type your password or click **Generate** to generate a strong password.
5. Click **OK**.

Add user

To add local or Active Directory users to AXIS Camera Station 5:

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 drop-down list of the **Role** field:
   - **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 to be removed from the drop-down list of the **User** field.
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 the specific users in the list.

Upgrade firmware



Firmware is software that determines the functionality of the Axis product. Using the latest firmware ensures that your device will have the latest functionality and improvements.

New firmware can be downloaded using AXIS Camera Station 5 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 is not accessible during the process of upgrading firmware, click **Yes** to continue. If you have acknowledged this and do not want this to show again, select **Do not show this dialog again** and click **Yes**.
5. The Upgrade firmware dialogue 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 pre-selected when new firmware versions are available for download, and the latest firmware version is pre-selected 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*.

Set date and time

The date and time settings for your Axis devices can be synchronized with the server computer time, with an NTP server, or set manually.

To set date and time on devices:

1. Go to **Configuration > Devices > Management**.
2. Select the device and click or right-click it and select **Set date and time**.
3. **Device time** lists the current date and time for your Axis device. When selecting multiple devices, **Device time** is not available.
4. Select the time zone.
   - Select the time zone you want to use with your Axis product from the **Time zone** drop-down list.
   - Select **Automatically adjust for daylight saving time changes** if your product is located in an area that uses daylight saving time.

Note

Time zone can be set when selecting the **Synchronize with NTP server** or **Set manually** time mode.

5. In the Time mode section:
   - Select **Synchronize with server computer time** to synchronize the date and time of your product with the clock on the server computer, that is, the computer where the AXIS Camera Station 5 server is installed.
   - Select **Synchronize with NTP server** to synchronize the date and time of your product with an NTP server. Enter the IP address, DNS or hostname of the NTP server in the provided field.
   - Select **Set manually** to manually set the date and time.
6. Click **OK**.



Set date and time

Install camera application

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 5. 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, the license key file can be installed at the same time as the application or it can be installed later using the devices' 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 does not require any 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 does not require any license and can be installed on cameras with firmware 5.60 and later.

AXIS Video Content Stream – An application that enables Axis cameras to send motion object tracking data to AXIS Camera Station 5. It can be installed on cameras with firmware between 5.50 and 9.59. The use of AXIS Video Content Stream is only permitted when used in combination with AXIS Camera Station 5.

Other applications – Any application that 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 that you want to install the applications. Click  or right-click and select **Install camera application**.
3. Select the camera application that you want to install on the cameras. 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

Downgrade or overwrite the application resets the application 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 does not 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 5 certificate authority (CA) automatically signs and distributes client and server certificates to devices when you enable HTTPS or IEE 802.1X. The CA ignores preinstalled certificates. For more information on how to configure certificates, see *Certificates, on page 115*.

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 5.

1. Go to **Configuration > Devices > Management**.
2. Right-click the devices:
   - Select **Security > HTTPS > Enable/Update** to enable HTTPS or update the HTTPS settings for the devices.
   - Select **Security > IEEE 802.1X > Enable/Update** to enable IEEE 802.1X or update the IEEE 802.1X settings for the devices.
   - Select **Security > HTTPS > Disable** to disable HTTPS for the devices.
   - Select **Security > IEEE 802.1X > Disable** to disable 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 is only displayed as one item. Deleting the certificate will remove it from all of the devices on which it is installed.

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 5 uses HTTPS to connect to the device.
	Off	AXIS Camera Station 5 uses HTTP to connect to the device.
	Unknown	The device is unreachable.
	Unsupported firmware	HTTPS is not supported because the device firmware is too old.
	Unsupported device	HTTPS is not supported on this device model.
IEEE 802.1X	Enabled	IEEE 802.1X is active on the device.
	Disabled	IEEE 802.1X is not active but ready to be activated on the device.
	Unsupported firmware	IEEE 802.1X is not supported because the device firmware is too old.
	Unsupported device	IEEE 802.1X is not supported on this device model.

Collect device data

This option is typically used for troubleshooting purposes. Use this option 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 do not work on all devices. For example, PTZ status does not 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 by 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**.

Tags

Tags are used to organize devices in the Device management page. A device can have multiple tags.

Devices can for example be tagged according to model or location. For example, when devices are tagged according to 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 the tag.
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 the tag, and click All devices to display all devices connected to AXIS Camera Station 5.
   - 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 about how to configure your device, see the device's User Manual.
4. Close the tab and the device is reloaded to ensure the changes are implemented in AXIS Camera Station 5.

Limitations

- Auto authentication for third-party devices is not supported.
- General support for third-party devices cannot be guaranteed.
- The device configuration tab with active video streams increases the load and might impact the performance on 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 34*.

Go to **Configuration > Devices > External data sources** and a list of all external data sources is displayed. 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 5, 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 5, 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.

A list of devices added to AXIS Camera Station 5 is displayed. Right-click the header row and select which columns to show. Drag and drop the headers to display the columns in 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 59*.
- **MAC address:** The MAC address of the device.
- **Model:** The model of the device.
- **Enabled:** Shows if the time synchronization is enabled.
- **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:** Shows if the time synchronization settings are actually applied. This is only available for device 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 5 server. The following information is displayed:

- **Server:** The AXIS Camera Station 5 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 have selected **Static**, configure the primary and secondary NTP server.
5. Click **Apply**.

Send alarm when the time difference between server and device is larger than 2 seconds	Select this to receive an alarm if the time difference between server and device is more than 2 seconds.

Configure storage

Go to **Configuration > Storage > Management** to open the Manage storage page. In the Manage storage page, you get an overview of the local storage and network storage that exists in AXIS Camera Station 5.

List	
Location	The path and name of the storage.
Allocated	The maximum amount of storage allocated to recordings.

List	
Used	The amount of storage space currently used for recordings.
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 5. Or, there are recordings with no database connection, so-called non-indexed recordings, in the storage space allocated for AXIS Camera Station 5. • **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 5 considers too low. To prevent errors or corruption, AXIS Camera Station 5 performs a forced cleanup, regardless of the placement of the storage slider, to protect the drive. During the forced cleanup, AXIS Camera Station 5 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 5. AXIS OS Recorders supporting RAID can also have the following statuses: • **Online:** The RAID system works as it should. There is 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 is 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 synchronize. It's possible to record and play recordings from the storage, but there is 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 Collect non-indexed files in *Manage storage, on page 63*.
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.
Other data	Amount of storage space taken up by the files other than indexed recordings and therefore unknown to AXIS Camera Station 5. 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 5 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. On this page, you can specify the folder to store recordings. To prevent the storage from becoming full, set a maximum percentage of total capacity that AXIS Camera Station 5 can use. You can add additional local storage and network drives for security and more space.

Note

- When connected to multiple AXIS Camera Station 5 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 links 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 from the drop-down menu.
4. To add a shared network drive, select **Shared network drive** and enter the path to a shared network drive. 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 a local storage or shared network drive 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 5 can use.
4. Click **Apply**.

Note

- We recommend leaving at least 5% of the disk space free for optimal performance.
- The requirement for the minimum space of a storage added to AXIS Camera Station 5 is 32 GB with at least 15 GB of free space available.
- If there is less than 15 GB of free space available, AXIS Camera Station 5 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 collect and place 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 5 places the data in the folders after the order in which they were found, first by server then devices connected to that particular server.

You can choose to either look for a particular recording or log you have lost, or simply 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 initiate a task.
4. When the task finished, 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 features a list of all cameras in AXIS Camera Station 5 and you can specify the number of days to keep recordings for specific cameras. When selected, the storage information can be seen 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 59*.
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.
Failover recording	Shows if the camera uses failover recording.
Fallback recording	Shows if the camera uses fallback recording.
Server	The server where the local storage or network storage is.

The storage solution for every camera was configured when cameras were added to AXIS Camera Station 5. 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. Click **Apply**.

Recording storage	
Store to	Select the storage to save recordings to from the drop-down menu. Available options are the local storage and network storage that were created.
Failover recording	Select to store the recordings to the camera's SD card when AXIS Camera Station 5 and the camera loose connection. Once the connection is back, the failover recordings transfer to AXIS Camera Station 5. Note This feature is only available for cameras that have an SD card and firmware 5.20 or later.
Unlimited	Select retention time to keep recordings until the storage becomes full.

Recording storage	
Limited	Select to set the maximum number of days to keep recordings. Note If the amount of storage space reserved for AXIS Camera Station 5 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.

Configure recording and events

When you add cameras to AXIS Camera Station 5, it automatically configures motion recording or continuous recording. You can later change the recording method to suit your needs, go to *Recording method, on page 70*.

Motion recording

It's possible to use motion detection with all Axis network cameras and video encoders. To only record when a camera detects motion considerably saves storage space compared to 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 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** profile is default.
6. Select a schedule or click **New schedule...** to create a new custom schedule.
7. Set the time settings for pre- and postbuffer, as well as the trigger period.
8. Click **Apply**.

Note

You can use action rules to configure motion recording. Make sure to turn off **Motion detection** in **Recording method** before you use 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 happen. To lower the impact on your storage space, only record during specific time periods.
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	The time interval between two successive triggers to reduce the number of successive recordings. If an additional trigger occurs within this interval, the recording continues and the trigger period restarts.
Raise alarm	Raises an alarm when the camera detects motion.



Configure motion detection

Continuous and scheduled recording

Continuous recording saves images continuously and requires more storage space than other recording options. To reduce the file size, consider motion detection recording.

To use continuous recording:

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

Profile	Select a **Profile** in the drop-down menu.**High** profile is default. Use a lower resolution to reduce the recording size. To edit profile settings, see *Stream profiles*.
Schedule	Set the schedule for the recordings to happen. To lower the impact on your storage space, only record during specific time periods.
Average bitrate	Turn on 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. See *Configure average bitrate, on page 70*.

Manual recording

For more information on how to record manually, see *Record manually*.

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** in the drop-down menu, **High** profile is default. Use a lower resolution to reduce the recording size. To edit profile settings, see *Stream profiles*.
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	Select to add 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 off by default.
Maximum duration	Set the maximum length for each recording, not including prebuffer or postbuffer times. Set to 0 for unlimited duration.

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, tampering attempts, or AXIS Cross Line Detection. 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 make sure recordings are saved if the connection to AXIS Camera Station 5 is lost. When failover recording is enabled, the camera saves recordings to its SD card if the connection is down for more than 20 seconds. The camera must have an SD card installed and the function must be enabled. Failover recording only affects H.264 recordings.

To turn on failover recording:

1. Go to **Configuration > Storage > Selection**.
2. Select a camera that supports failover recording.
3. Select **Failover recording**.
4. Click **Apply**.

Note

- Restarting the AXIS Camera Station 5 server doesn't trigger failover recordings. For example, when you run Database maintainer, restart AXIS Camera Station 5 Service Control, or restart the computer where the server is installed.
- Enabling failover recording overwrites any existing failover configuration for that camera on other servers.
- Failover recording can only be active for one AXIS Camera Station 5 server at a time for each camera view.

When the connection is restored, AXIS Camera Station 5 automatically imports the failover recordings and marks them with a dark gray color in the timeline.

The camera uses a 20-second prebuffer and postbuffer to minimize recording gaps, but short gaps of about 1–4 seconds can still appear. The High streaming profile is always used for failover recordings. Audio is included if it's enabled on the camera and part of the stream before failover is turned on.

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.

Note

Devices running an AXIS OS version earlier than 11.11.42 use a legacy failover recording method. The main differences are:

- The camera starts failover recording after 10 seconds of lost connection.
- The camera uses a 10–second internal memory buffer instead of a 20–second pre-buffer and post-buffer.



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 you turn on fallback recording, the device automatically starts a continuous recording when you lose the connection between AXIS Camera Station 5 and the recorder. The device uses medium stream profile for fallback recording.

Note

- It requires AXIS Camera Station 5.36 or later, AXIS S3008 Recorder firmware 10.4 or later, Axis device firmware 5.50 or later.
- If there is 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 that you have added AXIS S3008 Recorder and the devices and selected the recorder as 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 5 automatically configures motion recording or continuous recording when you add devices.

A check mark in the list shows what 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 on or off a recording method.

Note

View areas don't support motion detection.

Configure average bitrate

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

Note

- This option is only available for continuous recording and 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 have 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 is enough space for the recordings.

7. Click **Apply**.

Edit AXIS Video Motion Detection 2 and 4

AXIS Video Motion Detection 2 and 4 are camera applications you can install on products with support for 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 5, 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 application*.

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**: This filter ignores objects that only appear a short time in the image. For example, light beams from a passing car and shadows that moves quickly. Set the minimum time that objects must appear in the image to trigger an alarm. The time starts from the moment that the application detects the object. The filter delays alarms and don't trigger them if the object disappears from the image within the specified time.
  - **Small objects**: This filter ignores objects that are small, for example small animals. Set the width and height as a percentage of the total image. The filter ignores objects that are smaller than the specified width and height and don't trigger alarms. The object must be smaller than both the width and height values for the filter to ignore it.
  - **Swaying objects**: This filter ignores objects that only move a short distance, for example swaying foliage, and flags and their shadows. Set 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

Settings made here changes the settings in 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 for 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 area and ignores all other motion. An include area is an area that detects motion. You can place an exclude area within an include area to ignore motion. It's possible to use multiple include and exclude areas.

To add and edit an include area:

Note

Settings made here changes settings in 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 only see the area you edit, 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 manually**.
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**.

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 5 can control devices connected to output ports.

Note

- When connected to multiple AXIS Camera Station 5 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 5 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 5 can activate or deactivate a device connected to an output port. See *Action rules*.

For information about how to connect devices and how to configure 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**. Change the information if necessary.
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 5 connects with 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 pop-up 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 5 servers, you can select any connected server in **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 5 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. Many of these actions can require additional configuration of the device.

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**. Increase the trigger period if you use this setting on pulse triggers. 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 75*.

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.

Active tampering alarm – The tampering trigger activates when you reposition the device, something covers the lens, or the lens is severely out of focus. See *Create active tampering alarm triggers, on page 75*.

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 .

AXIS Cross Line Detection – AXIS Cross Line Detection is an application for cameras and video encoders. The application detects moving objects that cross a virtual line, and you can, for example, use it to monitor entrance and exit points. See *Create AXIS Cross Line Detection triggers, on page 76*.

System event and error – A system event and error trigger activates when recording errors occur, a storage becomes full, contact with a network storage fails, or one or more devices loses connection. See *Create system event and error triggers, on page 76*.

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 77*. We recommend you use 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 5. See *Create device event triggers, on page 78*.

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 82*.

AXIS Entry Manager event – This trigger activates when AXIS Camera Station 5 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 83*.

External HTTPS – The external HTTPS trigger makes it possible for external applications to trigger events in AXIS Camera Station 5 through HTTPS communication. See *Create external HTTPS triggers, on page 84*.

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 5.

Note

Don't use motion detection triggers to start recordings together with motion recording 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 pop-up screen:
   5.1. Select the camera that should detect motion.
   5.2. Set a time interval between two successive to reduce the number of successive recordings. If an additional 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 active tampering alarm triggers

The active tampering alarm trigger activates when you reposition the camera, something covers the lens, or the lens is severely out of focus. Since the device processes the tampering detection, it doesn't add any processing load to AXIS Camera Station 5 server.

Active tampering alarm is available for cameras with support for camera tampering and with firmware 5.11 or later.

To create an active tampering alarm trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **Activate tampering alarm**.
4. Click **OK**.
5. In **Trigger on**, select the camera to use.
6. Click **OK**.

Create AXIS Cross Line Detection triggers

AXIS Cross Line Detection is an application for cameras and video encoders. The application detects moving objects that cross a virtual line and activates the trigger. You can also, for example, use it to monitor entrance and exit points. Since the camera processes the detection, it doesn't add any processing load to AXIS Camera Station 5 server.

You can only install the application on devices with support for AXIS Camera Application Platform. To use AXIS Cross Line Detection as a trigger, you have to download the application from *axis.com* and install it on the devices. See *Install camera application*.

To create an AXIS Cross Line Detection trigger:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and select **AXIS Cross Line Detection**.
4. Click **OK**.
5. Click **Refresh** to update the list.
6. Select the camera to use from the **Trigger on** drop-down menu.
   You can only select cameras with AXIS Cross Line Detection installed.
7. Set a time interval between two successive triggers in **Trigger period** to reduce the number of successive recordings.
   If an additional trigger occurs within this interval, the recording continues and the trigger period restarts.
8. Click **AXIS Cross Line Detection settings** to open the **Applications** page of the camera in a web browser. For information on available settings, see the documentation provided with AXIS Cross Line Detection.

Note

To configure AXIS Cross Line Detection, use Internet Explorer and set the browser to allow ActiveX controls. If asked, click **Yes** to install AXIS Media Control.

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, contact with a network storage fails, and one or more devices loses 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 is problem to access a network storage.
On lost connection to camera	Select **On lost connection to camera** to activate the trigger when there is problem to contact the cameras. • Select **All** to include all the cameras added to AXIS Camera Station 5. • Choose **Selected** and click **Cameras** to show a list of all cameras added to AXIS Camera Station 5. Use **Select all** to select all cameras or **Deselect all** to deselect 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 5 before you use an I/O trigger. See *I/O ports*.
- Use device event triggers instead of input/output triggers if possible. Device event triggers offer a better overall user experience. See *Create device event triggers, on page 78* 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 an interval time between two successive triggers in **Trigger period** to reduce the number of successive recordings. If an additional 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 is no suitable trigger available in AXIS Camera Station 5. The events differ between the cameras and have one or more filters that must be set. Filters are conditions that must be fulfilled 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 as a function of time. An event can be stateful or stateless. A step function represents the activity of a stateful event . A straight line with pulses from when the event was triggered represents the activity of 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 time interval between two successive triggers in **Trigger period** to reduce the number of successive recordings. If an additional 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	Heatbeat
MotionRegionDetector	Motion
Network	Network lost

	Only applicable for events used by the device, not applicable for events used by AXIS Camera Station 5.
	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.
Anti-passback detection	Someone used a credential belonging to a cardholder who entered a zone before them.
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 state ready. 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 state ready. Note that the rule can only trigger when all necessary services, such as event system, has 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 to turn on Supervised input and inspect 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 the requirement 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 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 events used by the device, not applicable for events used by AXIS Camera Station 5.
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, at weekends etc. 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 on 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 the action button.

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 – Use 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 it's also possible to 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 and the action button activates.

7. If you select **Use existing button**:
   7.1. Search for the button or click the button that you want to use.
   7.2. If you select to use 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 5 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 5.

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 makes it possible for external applications to trigger events in AXIS Camera Station 5 through HTTPS communication. This trigger only supports HTTPS communication and requires that you provide the valid AXIS Camera Station 5 username including domain name and password in the 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]:55756/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Deactivate the trigger with ID "trigger1": `https://[address]:55756/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Activate the trigger with ID "trigger1" and then automatically deactivate the trigger after 30 seconds: `https://[address]:55756/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]:55756/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 that uses the same server address as the client used when logging on. 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**.

Add actions

One rule can have multiple actions. The actions start when the rule becomes activate.

The following actions are available:

Record – This action starts a recording from the camera. See *Create record actions*.

Raise alarm – This action sends an alarm to all connected AXIS Camera Station 5 clients. See *Create raise alarm actions*.

Set output – This 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. See *Create output actions*.

Send email – This action sends an email to one or multiple recipients. See *Create send email actions*.

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

Siren and light – This action triggers a siren and light pattern on a compatible device according to a preconfigured profile. See *Create siren and light actions, on page 90*.

AXIS Entry Manager – This action can grant access, unlock, or lock a door connected to a door controller configured by AXIS Entry Manager. See *Create AXIS Entry Manager actions, on page 90*.

Send mobile app notification – The action sends a custom message to the AXIS Camera Station Mobile app. See *Create send mobile app notification actions, on page 90*.

Turn rules on or off – Use this action to turn other action rules on or off. See *Create an action that turns other action rules on or off, on page 91*.

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

Access control – This action includes door actions and zone actions in AXIS Camera Station Secure Entry. See *Create access control actions, on page 91*.

Create record actions

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

To create a record action:

1. Specify a location to save the recording to, 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. 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	Select 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 5 clients. The alarm appears in the **Alarms** tab and as a taskbar notification. It's possible to include instructions in form of a file with alarm procedures with the alarm. 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 create a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Raise alarm**.
5. Click **OK**.
6. Under **Alarm message**, configure title, description, and duration.
7. Under **Alarm procedure**.
   7.1. Select **On alarm show alarm procedure**.
   7.2. Click **Upload** and find the desired file.
   7.3. Click **Preview** to open the uploaded file in a preview window.
   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 time between 1 and 600 seconds for the pop-up alarms.

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 switch on a light or lock a door.

Note

Add the output port to AXIS Camera Station 5 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 create 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 how the port configuration.
8. Select **Pulse** to define how long the output port should remain 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 the second option and specify the number of seconds.

Create send email actions

The email action sends an email to one or multiple recipients. It's possible to attach snapshots from cameras with 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 create a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Send email**.
5. Click **OK**.
6. Add recipients under **Recipients**:
   6.1. Enter the email address in **New Recipient** and select **To**, **Cc**, or **Bcc**.
   6.2. Click **Add** to add the email address to **Recipients**.
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 in the email notification as attachments, select **Attach snapshots** and click **Cameras**. A list of all cameras added to AXIS Camera Station 5 appears. You can **Select all** to select all cameras or **Deselect all** to deselect all cameras.
Send one email for each event	To prevent sending multiple emails for the same event, select **Send one email for each event**.
Don't send another email for	To prevent sending emails too close in time. 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 the **Live view** tab with a specific camera, view, or preset position. The **Live view** tab opens in all connected AXIS Camera Station 5 clients. If the **Live view** tab shows a split view with a hotspot, the camera selected in the live view action loads 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 5 clients from the taskbar or bring the clients to the 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 create a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Live view**.
5. Click **OK**.
6. Under **Live view actions**, configure what should 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 5 clients from the taskbar or bring the clients to the front of other open applications when the live view action starts.
9. Click **OK**.

Live view actions	
View	To open a view, select **View** and select the view from the drop-down menu.
Camera	To open a camera view, select **Camera** and select the camera from the drop-down menu. If a camera has 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** to not open any 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 shows in the hotspot.

Example:
To open a **Live view** tab, go to the hotspot view and show a camera view in the hotspot, configure 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 show the camera view in the hotspot.
   2.1. Under **Live view actions**, select **Camera** and select 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. HTTP notifications can for example be used to turn on or off a feature 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, it can be necessary to adjust the AXIS Camera Station 5 server proxy settings. See *General*.

To create an HTTP notification action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and create 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. Click **Advanced** to display the advanced settings.
9. Click **OK**.

Advanced	
Method	Select 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. See below for more information.

Trigger data	
Type	The trigger that activated this action rule.
Source ID	The source ID is the ID of the source that triggered the action rule, and it often represents a camera or other type of device. Not all sources have a source ID.
Source Name	The source name is the name of the source that triggered the action rule, and it often represents a camera or other type of device. Not all sources have a source name.
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 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 create 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 can grant access, unlock, or lock 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 5.

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **AXIS Entry Manager**.
5. Click **OK**.
6. Select an action and door to perform the action.
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 click 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 create a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Send mobile app notification**.
5. Click **OK**.
6. In **Message**, enter your message that should show on the mobile app.
7. Under **Click notification and go to**, configure what should show when you click the notification.
8. Click **OK**.

Click notification and go to	
Camera	Select a camera view from the **Camera** drop-down menu that should show when you click the notification in the mobile app.
Default	Select **Default** to go to the mobile app start page when you click the notification in the mobile app.

Create an action that turns other action rules on or off

Use the turn rules on or off action, for example, if you want to turn off motion detection in an office when an employee swipes their access card.

To create a turn off rules on or off action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
4. Click **Add** and select **Turn rules on or off**.
5. Click **OK**.
6. Select one or multiple action rules.
7. Choose if you want to turn the selected action rules on or off.
8. Enter a delay if you want 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 selected action rule to stay changed when the trigger isn't active. In the example above, that means motion detection turns back on when the employee removes the access card from the reader.
10. Click **OK**.

Create access control actions

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

- **Door actions:** grant access, lock, unlock, or lockdown the selected doors.
- **Zone actions:** lock, unlock, or lockdown the selected doors in the selected zones.

Note

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

To create a access control action:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Click **Add** and create 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. Click **OK**.

Schedules

The Schedules page contains every schedule that you can apply to recording, action rules, and components such as AXIS Secure Entry. AXIS Site Designer creates some schedules during installation.

Schedules allow you to 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 if the schedule is a daily or weekly schedule.
- **In use**: Shows whether a component, recording rule, or an 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 they have been applied to.

Note

When connected to multiple AXIS Camera Station 5 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 is not in use before you attempt to delete 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 on the row.
- To edit a date range or time slot, left-click on 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 on the row.
- To edit a date range or time slot, left-click on it.
- Click **Apply** to save your changes.

Examples of action rules

Example: Door forced open

Door forced open

An example of how to set up an action rule in AXIS Camera Station 5 that triggers a recording and an alarm someone forces the entrance door open.

Before you start, you need to:

- Install an Axis network door controller. See *Add devices, on page 37*.
- Configure the door controller. See *Add a door, on page 122*.

Create the action rule:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Add the Door forced event 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**, make sure 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 the 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 setting	
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

An example of how to create an action rule in AXIS Camera Station 5 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 119* and *Access management, on page 142*.
- Install an Axis network audio device and associate the audio device with a camera. See *Stream profiles, on page 43*.
- 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 5. See *I/O ports, on page 73*.

Create the action rule:

1. Go to **Configuration > Recording and events > Action rules**.
2. Click **New**.
3. Add the device event 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**, make sure 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 60 seconds to keep the port in the state.
   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 card number of the important person.

Configure client

Go to **Configuration > Client** to:

- Edit client specific settings, like theme and language. See *Client settings, on page 95*.
- Edit user specific settings, like notifications and startup options. See *User settings, on page 96*.
- Edit client specific streaming performance settings like video scaling and hardware decoding. See *Streaming, on page 98*.

Client settings

These settings apply to all AXIS Camera Station 5 users on the computer. Go to **Configuration > Client > Client settings** to configure the AXIS Camera Station 5 client settings.

Theme	
System, Light, Dark	Select the theme for the client. **System** is the default theme for new installations. If you select **System**, the system uses the light or dark theme depending on the Windows system theme.

General	
Run application when Windows starts	Turn on if you want to run AXIS Camera Station 5 automatically every time Windows starts.

Live view	
Show camera names in live views	Show the name of the camera in live view.
	To indicate any type of recording, turn on **Show recording indicators in live views and maps**.
	To indicate motion detection recording or recordings started by an action rule, turn on **Show event indicators in live views and maps**.

Maps	
Allow flashing coverage areas for all maps	Use to globally prevent or allow flashing of all coverage areas using **Flash**. This global setting doesn't affect the local setting on the map level. See *Map, on page 18*.

Language
Change the language of AXIS Camera Station 5 client. The change is effective after you restart the client.

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 the option for the server, see *Server settings, on page 102*.

User settings

These settings apply to the signed in AXIS Camera Station 5 user. Go to **Configuration > Client > User settings** to configure the AXIS Camera Station 5 client user settings.

Navigation system	
Tree view navigation system	Turns on by default to enable tree view navigation pane with the views and cameras.
Show in navigation	Select to show views or cameras or both in the drop-down menu.
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 Windows taskbar when an alarm starts.
Show taskbar notification for tasks	Turn on to show a notification in Windows taskbar when someone adds a task or it finish.
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 pushes 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 folder to save snapshots in.

Startup	
Start in full screen	Turn on to start AXIS Camera Station 5 in full screen mode.
Remember last used tabs	Turn on to start AXIS Camera Station 5 with the same open tabs, views, and camera views from when AXIS Camera Station 5 closed last time.
Remember last used monitors	Turn on to start AXIS Camera Station 5 on the same monitor used when AXIS Camera Station 5 closed last time.

Note

- The system saves views and camera views per tab. The system remembers only when the client reconnects to the same server.
- Remember tabs in order to remember monitors, views and camera views.
- 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 if you don't want any sound with an alarm.
Beep	Select if you want a typical beep sound with an alarm.
Sound file	Select and click **Browse** to find a sound file if you want a customized sound with an alarm. Use any file format that Windows Media Player supports.
Play	Click to test the sound.

Sound on incoming call	
No sound	Select if you don't want any sound with an incoming call.
Beep	Select if you want a typical beep sound with an incoming call.
Sound file	Select and click **Browse** to find a sound file if you want a customized sound with an incoming call. Use any file format that Windows Media Player supports.
Play	Click to test the sound.

Features	
Show smart search 1	By default Smart search 1 shows. Turn off to hide this feature.

Show warning dialogs	
Invalid certificate warning	Turn on to show this warning when applicable.

Streaming

Go to **Configuration > Client > Streaming** to configure the AXIS Camera Station 5 client streaming options.

Video scaling	
Scale to best fit	Select to show video in the whole available space, and not lose the aspect ratio or crop the image.
Fill video area (may crop parts of the video)	Select to fit the video to the available space and preserve the aspect ratio. If the available space has a different aspect ratio than the video, the system crops the video.

Hardware decoding	
Mode	• **Automatic** Uses the graphics card (if supported) to decode streams with a resolution above 3840x2160p@25fps (also known as 4K or UHD). • **On** Uses the graphics card (if supported) to decode streams with a resolution above 1920x1080p@25fps (also known as 1080p or HD). • **Off** Hardware decoding is off and AXIS Camera Station 5 uses the CPU to decode video.
Graphics card	Select a graphics card from the drop-down menu.

Note

- Hardware decoding makes use of your graphics card to decode video. If you have a high performance graphics card, hardware decoding is a good way to improve performance and reduce CPU usage, especially when you stream high-resolution video. Hardware decoding supports M-JPEG and H.264.
- Cameras with a resolution below 1080p can't use hardware decoding, even if hardware decoding is **On**.
- If your graphics card doesn't support 4K decoding, hardware decoding only functions on 1080p streams, even if hardware decoding is **On**.

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 lowers the bandwidth consumption.
Suspend video streams for inactive tabs	Turn on to suspend video streams in the inactive tabs. This lowers the bandwidth consumption.

PTZ (Pan, Tilt, Zoom)	
Select view with first click instead of starting PTZ	Turn on to activate view selection when you click the first time in the view. All the following clicks in the view control PTZ.

Audio	
Push-to-talk release delay (ms)	Adjust how many milliseconds you want to keep audio transmitted from the microphone after you release the **Push-to-talk** button.
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 be able to listen and speak to intercoms even if there are no ongoing calls from them.

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

Firmware upgrade settings

Note

When connected to multiple AXIS Camera Station 5 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** from the drop-down menu to check for available firmware versions on the server on each startup. By default, AXIS Camera Station 5 is set **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

Important

To improve security and functionality, we're upgrading **Axis Secure Remote Access** (v1) to **Axis Secure Remote Access v2**. We're discontinuing the current version on December 1st, 2025, and we strongly recommend that you upgrade to Axis Secure Remote Access v2 before that.

What does this mean for your AXIS Camera Station 5 system?

- After December 1st, 2025, you will no longer be able to remotely access your system using **Axis Secure Remote Access** (v1).
- To use **Axis Secure Remote Access v2**, you must upgrade to AXIS Camera Station Pro version 6.8. This upgrade is currently free for all AXIS Camera Station 5 users until March 1st, 2026.

Axis Secure Remote Access allows you to connect to your AXIS Camera Station 5 server through a secure and encrypted internet connection. Axis Secure Remote Access doesn't rely on port forwarding in your router for camera access.

Note

- Axis Secure Remote Access is only available for AXIS Camera Station 5.12 or later.
- When connected to multiple AXIS Camera Station 5 servers, select any server from the **Selected server** drop-down menu to configure Axis Secure Remote Access.

Enable Axis Secure Remote Access

Axis Secure Remote Access is available if you sign in to your My Axis account. Axis Secure Remote Access must be turned on manually. This feature makes it possible to sign in to your server remotely, see *Connect to a server*.

1. Go to **Configuration > Connected services > Axis Secure Remote Access**.
2. Under My Axis account, enter your My Axis account credentials.
3. Click **Apply**.
4. In the Axis Secure Remote Access section, click **Enable** to turn on remote access.

Axis Secure Remote Access on mobile devices

To log in to your server using secure remote access on a mobile device (iOS and Android):

1. Using your mobile device, 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 with the same My Axis account used to activate remote access.
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.

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

Axis Secure Remote Access usage

The Axis Secure Remote Access usage appears in the status bar at the bottom of the AXIS Camera Station 5 client. Click the link to get an overview of how to use the secure remote connection.

Service level	Shows the service level of your Axis Secure Remote Access subscription.
Data used this month	Shows how much data you used the current month. The counter resets on the first every month by midnight.
Overage	Shows how much data you used the current month that surpasses the included amount in your service level. This is only available if you have Overage in your subscription.
Connections	Shows the servers connected through Secure Remote Access.

Setup AXIS System Health Monitoring Cloud Service

AXIS System Health Monitoring Cloud Service allows you to monitor health data from systems located on different networks. See *Organizations, on page 101* for more information.

You must create a My Axis account before you set up AXIS System Health Monitoring Cloud Service. See *my.axis.com*.

1. Go to **Configuration System Health Monitoring > Settings**.
2. Click **Manage**.
3. Sign in with your My Axis account and follow the on-screen instructions.

Organizations

The organization is at the center of your cloud services.

- It connects your AXIS Camera Station 5 system to the users of the different cloud services.
- It activates the cloud-based system health monitoring. For more information, see *Setup AXIS System Health Monitoring Cloud Service, on page 101*.
- It defines the different user roles, for example, service administrator and operator.
- You can structure an organization into folders that, for example, represent systems located on different sites. To create an organization, you need a My Axis account. See *my.axis.com*.

Disconnect a system from an organization

In some cases, it can be necessary to disconnect a system from its current organization. For example, when you move a system from an organization to another.

1. Go to **Configuration > Connected services > AXIS System Health Monitoring Cloud Service** .
2. Click **Disconnect**.

Invite a user to an organization

1. Go to **Configuration > System Health Monitoring > Settings**.
2. Click **Open AXIS System Health Monitoring Cloud Service**.
3. Select the organization you want to invite the user to.
4. Open the user settings and click **Manage organizations**.
5. Open the **Users** tab.
6. Click **Generate**.
7. Copy the invitation code and send it to the user you want to invite.

Note

When you share the invitation code with the user, include the name of the organization in the invite.

Join an organization

You receive an invitation code when someone wants you to join an organization. To join the organization:

1. Copy the invitation code.
2. Go to **Configuration > System Health Monitoring > Settings**.
3. Click **Open AXIS System Health Monitoring Cloud Service**.
4. Select the organization you want to invite the user to.
5. Open the user settings and click **Manage organizations**.
6. Open the **Users** tab.
7. Paste the invitation code.
8. Click **Join**.

Configure server

Server settings

Go to **Configuration > Server > Settings** to configure the AXIS Camera Station 5 server settings.

Note

When connected to multiple AXIS Camera Station 5 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 audits. Set a value between 7 and 1000 days.

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 event configuration rule activates.

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 that you want to show in the sender email.

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 a username and password are required for this server. Enter the username and password to access the server.

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 pop-up dialog, click **Yes** to remove the server.
Test all...	To test an SMTP server, select the server and click **Test all...**. In the pop-up 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 change the order of the servers in the list. The system uses the servers in the same order they're listed.

Server test results	
OK	Connection with the SMTP server was successful. Make sure that the recipients received the test email.
Unknown error	An unexpected error occurred when attempting to send the email. Check that the SMTP server is operating correctly.
No contact	AXIS Camera Station 5 can't access the SMTP server. Make sure the SMTP server works correctly and that all routers and proxy servers between AXIS Camera Station 5 and the SMTP server allow traffic.
Configuration error	TLS was requested but server doesn't support StartTLS, server doesn't support authentication, or no compatible authentication mechanism.
TLS/SSL handshake error	Error during TLS/SSL negotiations, such as invalid server certificate.

Server test results	
Authentication required	Server requires authentication to send email.
Authentication error	Credentials are wrong.
Connection dropped	Connection was established, but then lost.

System alarm

A system alarm occurs if a camera loses connection, access to a recording storage is denied, an unexpected server shutdown occurs, or if recording errors occur. It's possible to send email notifications on 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 activate system alarm email.
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 add the email address to the **Recipients** box.

Device connection	
Keep using the hostnames even if they become unreachable	Use the hostname to connect. To automatically switch to use the IP address to connect, clear the checkbox. You can manually select to use the hostname or IP address to connect to devices. See *Connection, on page 59*.

Language	
Change the language of the server	Changes the name of the AXIS Camera Station 5 Service Control and AXIS Camera Station Secure Entry. For example: system alarms, audit log messages, and external data in the **Data search** tab. The change is effective after you restart.

Body worn	
Disk **Folder**	Select the drive and folder where you want to receive 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.	This is the retention time for the rejected content.

Feedback	
Share anonymous server usage data with Axis Communications	Select this to help us improve the application and user experience. To change the options for the client, see *Client settings, on page 95*.

Advanced settings

You should change the settings only when instructed by Axis support. To change an advanced setting:

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

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

Update AXIS Camera Station 5

To get the latest version of AXIS Camera Station 5:

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

Note

- Once an update starts, whether manual or scheduled, there is no way to cancel it.
- Scheduled updates start automatically.
- The system doesn't update clients connected through secure remote access.
- In a multi-server system, always update the local server last.
- When you update the local server, the client and service control will close temporarily. You will not see a UI or progress indicator while it's updating. Keep the server computer turned on until both the client and server have restarted.
- This feature uses the Windows installer (msi) regardless of the type you currently use.

Incident report

If you turn on incident report permission, you can generate the incident reports including recordings, snapshots, and notes about the incidents. See *Export incident reports, on page 27*.

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 a format you want to export your recordings to.
4. Under **Categories**, add or remove the categories to group the incident reports. The categories can be the folder name in the export location if you configure the category as a variable in the server directory path.
   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: <Insert your name, mail, and phone number>.
6. Click **Apply**.

Location	
Server directory path	Select and enter the directory path to save the 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 5 server. See *Manage storage* for how to add storage to use for recordings.

Export format	
ASF	If selected , you can select **Add digital signature** to use a digital signature to make image tampering impossible. 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 export recordings.

At the selected time, an export of all recordings since the previous export starts. If the previous export is older than one week or if there is no previous export, the export only contains recordings less than one week old. To export older recordings, go to the **Recordings** tab and export them manually. See *Export recordings*.

Note

When connected to multiple AXIS Camera Station 5 servers, select any server from the **Selected server** drop-down menu to turn on and manage scheduled exports.

Export scheduled recordings

1. Under **Scheduled export**, select **Enable scheduled export** to use scheduled export.
2. Under **Cameras**, select the cameras to export recordings from. The system selects all listed cameras as 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 for when 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 5 server. See *Manage storage* for how to add storage to use for recordings.

Export	
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 you want to export your recordings to. **ASF** – Select **Add digital signature** to use a digital signature to make image tampering impossible. 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 2008 Server

To be able to export recordings from a server running Microsoft Windows 2008 Server, you must install Desktop Experience:

1. Click **Start > Administrative Tools > Server Manager** to open Server Manager.
2. Under **Features Summary**, click **Add features**.
3. Select **Desktop Experience**, click **Next**.
4. Click **Install**.

Microsoft Windows 2012 Server

To be able to export recordings from a server running Microsoft Windows 2012 Server, you must 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**.

New connection

Go to ☰ **> Servers > New connection** to connect to a AXIS Camera Station 5 server. See *Connect to a server*.

Connection status

Go to ☰ **> Servers > Connection status**, to show a list of the servers' connection status.

Use the slider in front of the server name to connect or disconnect to the server.

Status codes	Description	Possible solutions
Connecting	The client tries to connect to this server.	
Connected	The client uses TCP while connected to this server.	

Connected (using Secure Remote Access)	The client uses Secure Remote Access while connected to this server.	
Connected (using 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 disconnects from this server.	
Disconnected	There is no connection between the client and this server.	
Reconnecting	The client has lost connection to this server and tries to reconnect.	
Reconnection failed	The client fails to reconnect to this server. It finds the server but the user permissions or password can 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 fails. Make sure to synchronize the client and server computer UTC times.	
No contact with server computer	There was no response by the server computer on the used address.	• Check that the network works properly. • Check that the server runs.
No server running	The computer running the server is accessible, but the server doesn't run.	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 runs.
Invalid hostname	The DNS can't translate the hostname into an IP address.	• Check that the spelling of the hostname is correct. • Check that the DNS has the information it needs.
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 the expected one responds on this address.	Update the server list to connect to this server.

Client version (x) is not compatible with server version (y)	The client is too old or too new compared to the server.	Make sure to have the same version of AXIS Camera Station 5 installed on both the client and the server computer.
Server too busy	The server couldn't respond because of performance issues.	Make sure that the server computer and the network don't overload.



Multiple servers

Server lists

You can organize your AXIS Camera Station 5 servers in server lists. A server can belong to multiple server lists. It's possible to import, export, and use server lists in other AXIS Camera Station 5 clients.

Go to > **Servers** > **Server lists** to open the Server lists dialog.

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

	Select the server list and click .
+ New server list	Click to add a new server list and enter a name for the list.
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 the server list to log in 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 servers in a server list, select the servers and click **Remove**.
Rename a server	Double-click the list and enter a new name for the list.



Organize servers in server lists

Configure switch

If you have an AXIS Camera Station S22 Appliance series device, you have the option to configure the device from AXIS Camera Station 5. Go to **Configuration > Switch > Management** and enter your credentials to open the Switch management page in the AXIS Camera Station 5 client. For how to configure the switch, see your AXIS Camera Station S22 Appliance series User manual on *axis.com*.

Note

AXIS Camera Station 5 can only connect to https://192.168.0.1/ which is the default IP address of the switch.

Configure licenses

On the License page you can view the license keys and license status and manage the licenses of the connected devices.

Note

- When connected to multiple AXIS Camera Station servers, Station servers, select any server from the **Selected server** drop-down menu to manage licenses.
- We recommend that you write down the license keys or save them in a digital format on a USB flash drive for future reference. You can't retrieve lost license keys.
- When you register your Axis network video recorder in AXIS License Portal, you receive an NVR Core license. The NVR Core licenses are locked to the device's hardware and can't be moved. You can upgrade NVR Core to Universal in the same way as Core licenses. You can move and use the upgrade licenses for any system.

License management

Go to **Configuration > Licenses > Management** to get an overview of the number of unlicensed devices connected to the server. You can manage licenses online as well as offline. Remember to add licenses for all your devices before the end of the 30-day trial period. See *How to purchase licenses*. You can also click the license status link in the status bar to see the overview of your device licenses.

As license administrator, you can add multiple My Axis accounts to your AXIS Camera Station system.

Add a My Axis account to a system online

1. Go to **Configuration > Licenses > Management**.
2. Make sure **Manage licenses online** is on.
3. Click **Go to AXIS License Portal**.
4. In the AXIS License Portal, sign in with the new My Axis account that you want to add.
5. Go to **Edit license admins** and check that the account was added as license administrator.

Add a My Axis account to a system offline

1. Go to **Configuration > Licenses > Management**.
2. Turn off **Manage licenses online**.
3. Click **Export system file**.
4. Save your system file on a USB flash drive.
5. Go to the AXIS License Portal, *license-portal.lp.axis.com*.
6. Sign in with the new My Axis account that you want to add.
7. Upload your system file.
8. Go to **Edit license admins** and check that the account was added as license administrator.

There are different ways to license your system, depending on your internet connection.

- *License a system online*

- *License a system offline*
- *Move licenses between systems, on page 111*

Device status

Go to **Configuration > Licenses > Device status** to view a list of all connected devices and their license status.

Keys

Go to **Configuration > Licenses > Keys** to view a list of the keys necessary for each license of all connected devices.

License a system online

Both the AXIS Camera Station client and the server must have internet connection.

1. Go to **Configuration > Licenses > Management**.
2. Make sure **Manage licenses online** turns on.
3. Sign in with your My Axis account.
4. Under **Add license key**, enter your license key.
5. Click **Add**.
6. In AXIS Camera Station client, make sure your license keys appear under **Configuration > Licenses > Keys**.

License a system offline

1. Go to **Configuration > Licenses > Management**.
2. Turn off **Manage licenses online**.
3. Click **Export system file**.
4. Save your system file to a USB flash drive.
5. Go to the AXIS License Portal, *license-portal.lp.axis.com*.
6. Sign in with your My Axis account.
7. Click **Upload system file** to upload the system file from your USB flash drive.
8. Under **Add license key**, enter your license key.
9. Click **Add**.
10. Under **License keys**, click **Download license file** and save the file to a USB flash drive.
11. In AXIS Camera Station client, go to **Configuration > Licenses > Management**.
12. Click **Import license file** and select the license file on your USB flash drive.
13. Make sure your license keys appear under **Configuration > Licenses > Keys**.

Move licenses between systems

Note

You can't move NVR Core licenses since they are locked to the device's hardware.

To move licenses from one system to another system with the same My Axis account:

1. Go to the AXIS License Portal, *license-portal.lp.axis.com*.
2. Under **My systems**, click the system name that you want to move a license from.
3. Under **License keys**, find the license key that you want to move.

4. Click ⋮ and **Move**.
5. In the **To system** drop-down menu, select a system that you want to move the license to.
6. Click **Move license key** and click **Close**. You can find the action details under **History**.
7. Go to **My systems** and make sure that the licenses appear under the correct system.



Move licenses to another system

To release licenses from a system and add to another system with a different My Axis account:

1. Go to the AXIS License Portal, *license-portal.lp.axis.com*.
2. Under **My systems**, click the system name that you want to move a license from.
3. Under **License keys**, find the license key that you want to move.
4. Make a copy of the license key first.
5. Click ⋮ and **Release**.
6. Sign out and sign in with another My Axis account.
7. Under **My systems**, click the system that you want to license.
8. Under **Add license key**, enter the license key you released.
9. Click **Add**. You can find the action details under **History**.
10. Go to **My systems** and make sure that the licenses appear under the correct system.

Configure security

User permissions

Go to **Configuration > Security > User permissions** to view the users and groups that exists in AXIS Camera Station 5.

Note

Administrators of the computer that runs AXIS Camera Station 5 server are automatically given administrator privileges to AXIS Camera Station 5. You can't change or remove the Administrators group's privileges.

Before you can add a user or group, register the user or group on the local computer or make sure they have an Windows® Active Directory user account. To add users or groups, see *Add users or groups*.

When a user is part of a group, the user gets the highest role permission assigned to the individual or the group. The user also gets the access granted as an individual and receives the rights as part of a group. For example, a user has access to camera X as an individual. The user is also a member of a group that has access to cameras Y and Z. The user therefore has access to cameras X, Y, and Z.

	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 given to the user or group. Possible values: Administrator, Operator, and Viewer.
Details	Detailed user information as it appears in the local computer or 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 5. To add a user to AXIS Camera Station 5, 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 on **Users** and select **New User**.
- In the popup dialog, enter the new user's details and uncheck **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**.
   You can see the available users and groups 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 result doesn't display if there are too many users or groups. Use the filter function.
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 5 servers, select a server from the **Selected server** drop-down menu.

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 give 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 configure anything in the system.

Operator – Select cameras, views, and I/O ports to get access to live and recorded. An operator has full access to all functionality of AXIS Camera Station 5 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 to start and stop recordings manually.
Mechanical PTZ	Allow access to mechanical PTZ controls. Only available 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. Only available for cameras with mechanical PTZ and 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 5.
Edit	Allow to edit the views in AXIS Camera Station 5.

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	Allow to view the state of the I/O port. The user can't change the port state.
Write	Allow to change 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	Allow to take snapshots in the 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.

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	Allow configuration of the system health monitoring system.
Access to system health monitoring	Allow access to the system health monitoring system.

Certificates

To manage settings for certificates between the AXIS Camera Station 5 server and the 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 57* for more information.

AXIS Camera Station 5 can be used as:

- **Root certificate authority (CA):** If you use AXIS Camera Station 5 as a root CA it means AXIS Camera Station 5 uses its own root certificate to issue server certificates and there is no other root CA involved in the process.
- **Intermediate certificate authority:** In this scenario you need to import a CA certificate and its private key in AXIS Camera Station 5 to sign and issue server certificates for the Axis devices. This CA certificate can be a root certificate or an intermediate CA certificate.

Note

When you uninstall AXIS Camera Station 5, 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 5 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 5 as the root CA, or you can import a CA certificate and let AXIS Camera Station 5 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 5 stores its 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 all 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 5. • **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 5 server.
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). Note that the CA doesn't sign certificates that are valid beyond its own expiration date.

Generate a root CA

When AXIS Camera Station 5 starts, it looks for a CA. If missing, it generates a root CA automatically. It includes a self-signed root certificate and private key protected by a password. AXIS Camera Station 5 stores the password but doesn't make it visible. A CA certificate generated by AXIS Camera Station 5 is valid for 10 years.

To manually generate a new CA to replace the old one, see *Replace a CA, on page 117*.

If you upgrade from version 5.45 or earlier that uses a manually installed certificate on a device, AXIS Camera Station 5 automatically uses the existing root CA to install a new certificate when the manually installed certificate 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 5 as an intermediate CA. Import an existing CA consisting of a certificate and a private key to allow AXIS Camera Station 5 to sign certificates on the 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 be used within the its validity period. To import a CA to replace the existing one, see *Replace a CA, on page 117*.

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. You need to click **OK** to continue.
- When you import a CA certificate, it's added to Windows Trusted Root Certificates.
- After uninstalling AXIS Camera Station 5, 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**.

HTTPS

By default, AXIS Camera Station 5 validates the signature of the active HTTPS server certificate on each connected device and doesn't connect to a device without a validated certificate. The server certificate must be signed by the active CA in AXIS Camera Station 5 or validated through Windows Certificate Store. AXIS Camera Station 5 also validates if the address in the device HTTPS certificate matches the address used to communicate with the device if **Validate device address** is on.

Cameras with firmware 7.20 or later come with a self-signed certificate. These certificates are not trusted. Instead, generate or import a CA to let AXIS Camera Station 5 issue new certificates to the devices when you use HTTPS.

Temporarily ignore certificate validation	Turn on to let AXIS Camera Station 5 accept any HTTPS certificate and allow configuration of unsecure devices. Turn off so AXIS Camera Station 5 validates the device certificates. If it isn't trusted, a warning message appears under **Status** in **Device management** and the device isn't accessible.
Validate device address	Turn off for a stable behavior on DHCP networks without using hostnames. Turn on to require the addresses to match for additional security. We recommend that you only turn on this setting on networks where devices primarily use hostname to communicate, or devices have a static IP address.

Note

- When a secure connection (HTTPS) is unavailable, you can issue a new HTTPS certificate. See *Add devices, on page 37*
- To use HTTPS, firmware 5.70 or later, it requires 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 AXIS T85 PoE+ Network switch series.

IEEE 802.1X

For AXIS Camera Station 5 IEEE 802.1X authentication, the supplicant is an Axis network device that wishes to attach 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 sourced externally, for example from the IEEE 802.1X authentication server, or directly from AXIS Camera Station 5. This certificate installs on each Axis device and verifies the authentication server.

Note

To use IEEE 802.1X certificates, it requires firmware 5.50 or later 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 what version of Extensible Authentication Protocol (EAP) you want to use.
3. In the **EAP identity** drop-down menu, select to use either the device's MAC address, the device hostname, or custom text.
4. If you selected **Custom**, enter any text that functions as the EAP identity in **Custom**.
5. Click **Import** and select the IEEE 802.1X authentication CA certificate file.

6. In the **Common name** drop-down menu, select to use **Device IP address** or **Device EAP identity** as the common name in the individual certificates created for each device when AXIS Camera Station 5 acts as a certificate authority.
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 miss 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 5, the AXIS Camera Station 5 CA certificate, and 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 the expiration date you want AXIS Camera Station 5 to notify you.

Certificate renewal

Renew certificate between the server and devices

The device client or server certificates generated by AXIS Camera Station 5 automatically renew 7 days before the expiration warning appears. For this to be possible, you must have turned on HTTPS or IEEE 802.1X on the device. If you want to renew or update a certificate manually, see *Security, on page 57*.

Renew certificate between the server and the client

1. Go to **Configuration** > **Security** > **Certificates**.
2. Under **Certificate renewal**, click **Renew**.
3. Restart the server to apply the renewed certificate.

Reset the password

1. Go to **Configuration > Security > Certificates**.
2. Turn off **Validate device certificate** to make sure the devices that use CA certificates are 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 5, see *Set up an Axis network door controller*.

Note

Before you start, do the following:

- Upgrade the controller 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 identification profile, see *Identification profiles, on page 132*.
2. To use a custom setup for card formats and PIN length, see *Card formats and PIN, on page 133*.
3. Add a door and apply an identification profile to the door. See *Add a door, on page 122*.
4. Configure the door.
   - *Add a door monitor, on page 126*
   - *Add emergency input, on page 126*
   - *Add a reader, on page 127*
   - *Add a REX device, on page 129*
5. Add a zone and add doors to the zone. See *Add a zone, on page 129*.

Device software compatibility for door controllers

The table below shows the minimum and recommended AXIS OS version for each AXIS Camera Station 5 version:

AXIS Camera Station version	Recommended AXIS OS version
5.59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

Doors and zones

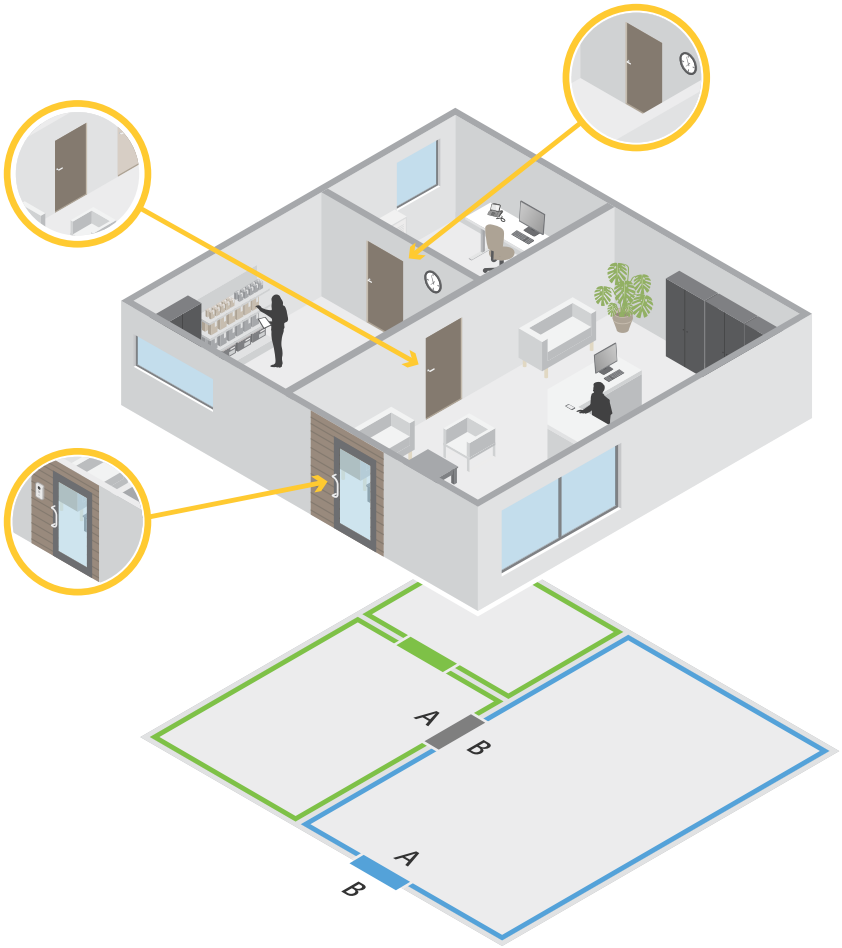
Go to **Configuration > Access control > Doors and zones** to get an overview and configure doors and zones.

Pin chart	View the controller pin chart associated with a door. If you want to print the pin chart, click **Print**.
Identification profile	Change identification profile on doors.
Secure Channel	Turn on or off OSDP Secure Channel for a specific reader.

Doors	
Name	The name of the door.
Door controller	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.
Card formats and PIN	Shows the type of card formats or PIN length.

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 in the door configuration doesn't support secure channel or secure channel is turned off for the reader.
Zones	
Name	The name of the zone.
Number of doors	The number of doors included in 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.

Create a new door configuration 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 125*.
Monitoring door	A door that can report whether it's open or closed. For more information, see .
Provisioned door	A door you can add as a placeholder in the system without the requirement of selecting the hardware for it.
Floor	A door type for elevator control that authenticates access to elevator floors using card readers. For more information, see .

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 active.
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 132*.
8. Configure the door settings. See *Door settings, on page 123*.
9. *Add a door monitor, on page 126*
10. *Add emergency input, on page 126*
11. *Add a reader, on page 127*
12. *Add a REX device, on page 129*
13. Click **Save**.

Copy an existing door configuration to add a door:

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**.

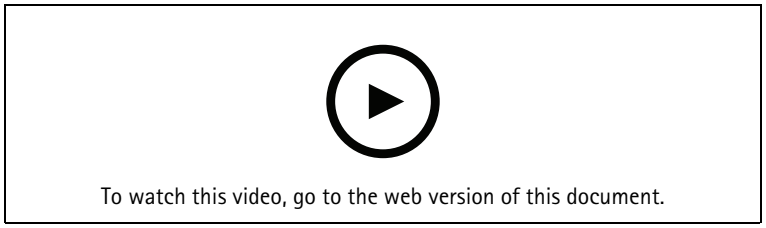
5. In the **Copy configuration** drop-down menu, select an existing door configuration. It shows the connected doors, and the controller grays out if it was configured with two doors or one door with two locks.
6. Change the settings if you want.
7. Click **Save**.

To edit a door:

1. Go to **Configuration > Access control > Doors and zones > Doors**.
2. Select a door in the list.
3. Click **Edit**.
4. Change the settings and click **Save**.

To remove a door:

1. Go to **Configuration > Access control > Doors and zones > Doors**.
2. Select a door in the list.
3. Click **Remove**.
4. Click **Yes**.



Add and configure doors and zones

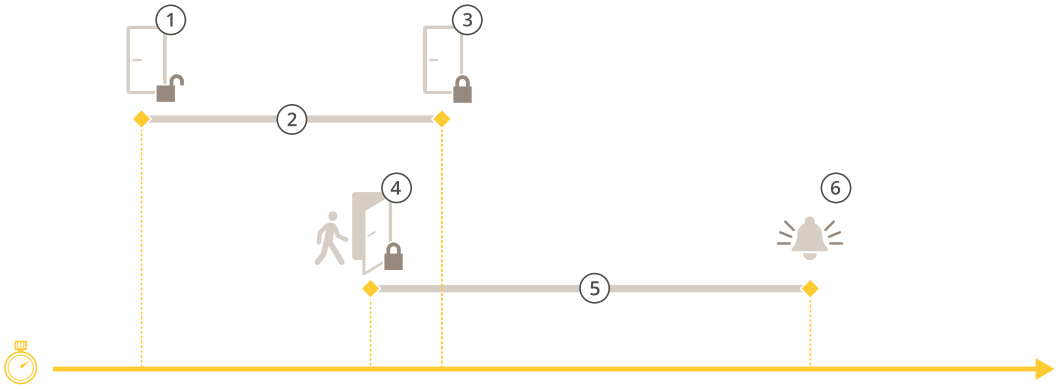
Door settings

1. Go to **Configuration > Access control > Door and Zones**.
2. Select the door you want to edit.
3. Click **Edit**.

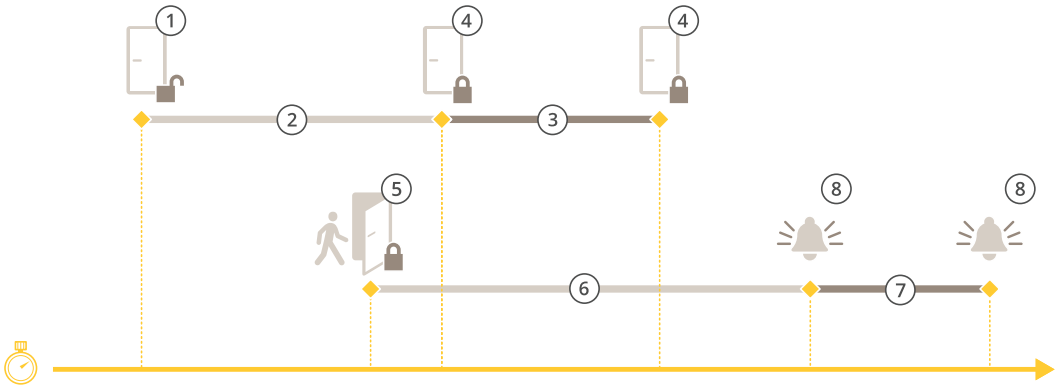
Access time (sec)	Set the number of seconds the door remains unlocked after access was granted. The door remains unlocked until the door opens or until the set time ends. The door locks when it closes even if there is access time left.
Open-too-long time (sec)	Only valid if you have configured a door monitor. Set the number of seconds the door stays open. If the door is open when the set time ends, it triggers the door open too long alarm. Set up an action rule to configure which action the open too long event triggers.
Long access time (sec)	Set the number of seconds the door remains unlocked after access was granted. Long access time overrides the access time for cardholders that has this setting turned on.
Long open-too-long time (sec)	Only valid if you have configured a door monitor. Set the number of seconds the door stays open. If the door is open when the set time ends, it triggers the

	door open-too-long event. Long open-too-long time overrides the already set open-too-long time for cardholders if you turn on the **Long access time** setting.
Relock delay time (ms)	Set the time, in milliseconds, that the door stays unlocked after the 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 an alarm when a door has been forced open.
Door open too long	Select whether you want the system to trigger an alarm when a door has been held open too long.

Time options



1 Access granted - lock unlocks
2 Access time
3 No action taken - lock locks
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 locks*
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 5 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.



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 Axis door controller and AXIS Camera Station 5 server must be synchronized.
- Before you start, use the Aperio application that ASSA ABLOY supports to pair the Aperio locks with the Aperio hub.
- Wireless locks will not 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 5, 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, 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 120*.

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 door position switch that monitors the physical state of a door. You can add a door monitor to your door and configure how to connect the door monitor.

1. Go to the door configuration page. See *Add a door, on page 122*.
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 an interruption in the connection between the door controller and the door monitor occurs, turn on **Supervised input**. See *Supervised inputs, on page 131*.

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 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 122*.
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 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, you can see it in **Card formats** under **Configuration > Access control > Doors and zones**. See *Doors and zones, on page 120*.

Note

- You can also add up to 16 Bluetooth readers to a door controller. For more information, see *Add a Bluetooth reader, on page 128*.
- If you use an Axis network intercom as 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 122*.
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 setup 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 displays 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, do this procedure again.

For information on how install an AXIS Barcode Reader, see .

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. For requirements and supported devices, see *IP reader, on page 128*.

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 when the reader tamper input is active. • **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 131*.

Add a Bluetooth reader

You can use the AXIS A4612 Network Bluetooth Reader to expand the wired door limits of Axis door controllers, which allow up to 16 of these readers to be assigned to their own door. Each reader can manage the door lock, Request-to-Exit (REX), and Door Position Switch (DPS).

Adding and using these readers does not 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 .
2. Go to the door configuration page. See *Add a door, on page 122*.
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 will be 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.

IP reader

It's possible to use Axis network intercoms as IP reader in AXIS Camera Station Secure Entry.

Note

- It requires AXIS Camera Station 5.38 or later and an Axis door controller with firmware 10.6.0.2 or later.
- It doesn't require special configuration to use the intercom as an IP reader.

Supported devices:

- AXIS A8207-VE Network Video Door Station with firmware 10.5.1 or later
- AXIS A8207-VE Mk II Network Video Door Station with firmware 10.5.1 or later
- AXIS I8116-E Network Video Intercom

Add a REX device

You can select to 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 122*.
2. Under one side of the door, click **Add**.
3. Select **REX device**.
4. Select the I/O port that you want to connect the REX device to. If there is only one port available, it will be 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 an interruption in the connection between the door controller and the REX device occurs, turn on **Supervised input**. See *Supervised inputs, on page 131*.

Action	
Unlock door	Select to unlock the door when it receives the REX signal.
None	Select if you don't want to trigger any 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.

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 entrance to 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. It enforces that a person must first exit the area before they can use 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 you can do it on 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 door.
6. Click **Apply**.

Anti-passback	
Log violation only (Soft)	Use this if you want to allow a second person to enter the door using the same credentials as the first person. This option only results in a system alarm.
Deny access (Hard)	Use this if you want to prevent the second user from entering the door 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** if you don't want timeout, meaning that the zone has anti-passback 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 is interruption in the connection to a door controller.

- Connection between the door controller and the door monitor. See *Add a door monitor, on page 126*.
- Connection between the door controller and the reader that uses Wiegand protocols. See *Add a reader, on page 127*.
- Connection between the door controller and the REX device. See *Add a REX device, on page 129*.

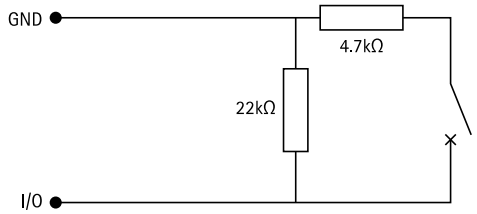
To use supervised inputs:

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.

Connection diagrams

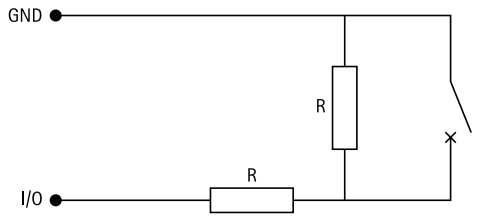
Parallel first connection

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.

Identification types are carriers of the credential information necessary to access a door. Common identification types are tokens, personal identification numbers (PINs), fingerprints, facial maps, and REX devices.
An identification type can carry one or more types of information.

Supported identification types: Card, PIN, REX, static QR, and dynamic QR.

Note

You must use dynamic QR and PIN together.

Go to **Configuration > Access control > Identification profiles** to create, edit, or remove identification profiles.

There are five default identification profiles available for you to use as they are or edit as required.

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.

QR Code is a registered trademark of Denso Wave Incorporated in Japan and other countries.

To create an identification profile:

1. Go to **Configuration > Access control > Identification profiles**.
2. Click **Create identification profile**.
3. Enter an identification profile name.
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. Configure the identification profile for one side of the door.
6. On the other side of the door, do the previous steps again.
7. Click **OK**.

To edit an identification profile:

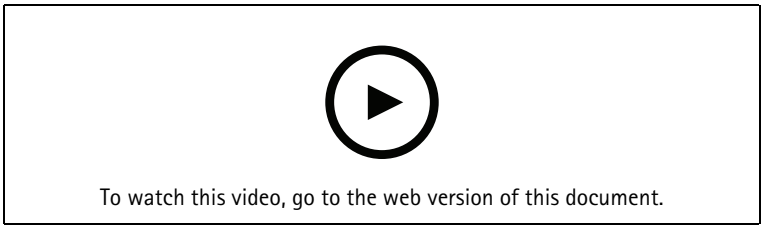
1. Go to **Configuration > Access control > Identification profiles**.
2. Select an identification profile and click .
3. To change the identification profile name, enter a new name.
4. Do your edits to the side of the door.
5. To edit the identification profile on the other side of the door, do the previous steps again.

6. Click **OK**.

To 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**.

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.



Set up identification profiles

Card formats and PIN

A card format defines how a card stores data. It's a translation table between the incoming data and the validated data in the system. Each card format has a different set of rules for how to organize the stored information. By defining a card format, you tell the system how to interpret the information that the controller gets from the card reader.

There are predefined commonly used card formats available for you to use as they are or edit as required. 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.

To 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.

ⓘ	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).

To 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**.

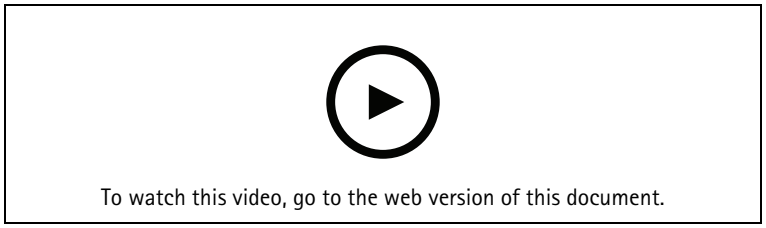
To reset a predefined card format:

1. Go to **Configuration > Access Control > Card formats and PIN**.

2. Click to reset a card format to the default field map.

To configure PIN length:

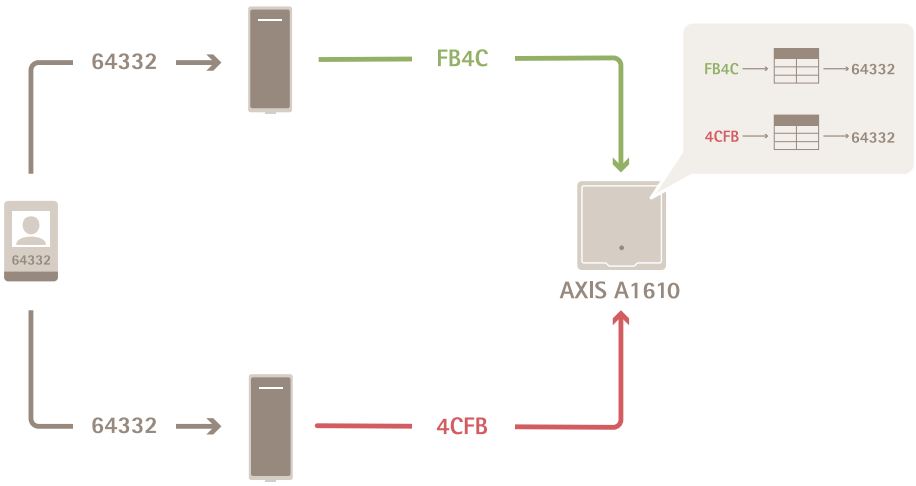
1. Go to **Configuration > Access Control > Card formats and PIN**.
2. Under **PIN configuration**, click .
3. Specify **Min PIN length**, **Max PIN length**, and **End of PIN character**.
4. Click **OK**.



Set up card formats

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 a 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.

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 166*.
- 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 137*.
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 137*.
3. Configure global cardholders and cardholder groups on the main server. See *Add a cardholder, on page 142* and *Add a group, on page 146*.
4. View and monitor global cardholders and cardholder groups from the sub server. See *Access management, on page 142*.

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 5. 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 5. See *Import active directory users, on page 138*.

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 5:

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 143*.

Configure smart search 2

With smart search 2, you can set several filters to easily find persons and vehicles of interest from the recordings generated from Axis cameras.



For requirements, limitations, and how to use smart search 2, see *Smart search 2, on page 31*.

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 amount 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.
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 that indicates that no metadata was recorded during a certain period.
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 less than 95% detections are classified.
	Server classification status from the last hour when the server classification is slow. Appears when less than 50% detections are classified.

Configure System Health Monitoring BETA

Note

- When connected to multiple AXIS Camera Station 5 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, AXIS System Health Monitoring Cloud Service provides the same functionality but through the cloud. See *Setup AXIS System Health Monitoring Cloud Service, on page 101* for more information.

Notifications

To send email notifications:

1. Configure an SMTP server and an email address to send the notifications. See *Server settings, on page 102*

2. Configure the email addresses to receive the notifications. See *Configure email recipients, on page 140*.
3. Configure the notification rules. See *Configure notification rules, on page 140*.

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 shows that the test email was sent.

Configure notification rules

There are two notification rules activated by default.

System down – Send a notification when the system in a single system setup or any system in a multisystem setup is down for 5 minutes.

Device down – Send a notification when a device listed in System Health Monitoring is down for 5 minutes.

1. Go to **Configuration > System Health Monitoring > Notifications**.
2. Under **Notification rules**, turn on or off the notification rules.
3. Under **Applied rules**, you can see a list of systems and devices including the applied notification rule.

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 140*.
2. In the main system, upload the system configuration. See *Retrieve data from other systems, on page 141*.
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 150*.

Generate system configuration

1. Go to **Configuration > System Health Monitoring > Multisystem**.
2. Click **Generate**.
3. Click **Copy** to be able to upload it to the main system.
4. To view the system configuration details, click **Show details**.
5. To regenerate the system configuration, click **Delete** to delete the existing one first.

After the upload of the system configuration to the main system, the main system information appears under **Systems with access**.

Retrieve data from other systems

After you have generated and copied 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 fill with the information you copied from the secondary system.
3. Check the host IP address and click **Add**.
   The secondary system appears under **Available systems**.

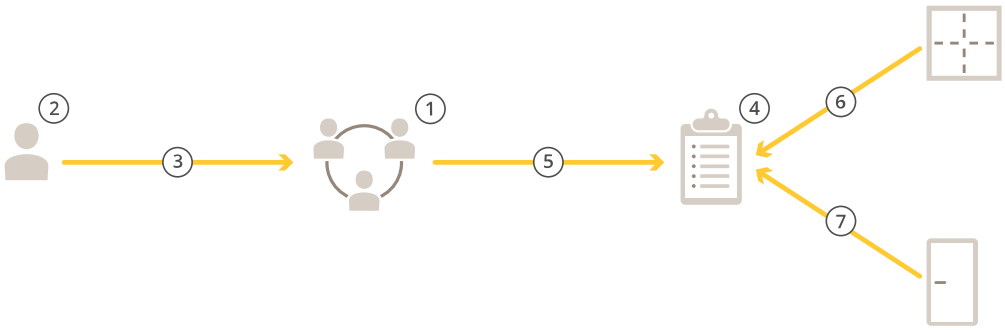
Access management

The Access management tab allows you 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 5, see *Set up an Axis network door controller*.

Workflow of access management

The access management structure is flexible, which allows you to develop a workflow that suits your needs. The following is a workflow example:



1. Add groups. See *Add a group, on page 146*.
2. Add cardholders. See *Add a cardholder, on page 142*.
3. Add cardholders to groups.
4. Add access rules. See *Add an access rule, on page 146*.
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 identifies the person and when and how to grant the person access to doors.

You can also choose to map users in an Active Directory database as cardholders, see *Active directory settings[BETA], on page 138*.

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 and click **Next**.
4. Optionally, click **Advanced** and select any options.
5. Add a credential to the cardholder. See *Add credentials, on page 143*
6. Click **Save**.
7. Add the cardholder to a group.
   7.1. Under **Groups**, select the group you want to add the cardholder to and click **Edit**.
   7.2. Click **+ Add** and select the cardholder you want to add to the group. You can select multiple cardholders.
   7.3. Click **Add**.

7.4. Click **Save**.

Advanced	
Long access time	Select to let the cardholder to have long access time and long open-too-long time when there is an installed door monitor.
Suspend cardholder	Select to suspend the cardholder.
Allow double swipe	Select to allow a cardholder to override the current state of a door. For example, they can use it to unlock a door outside the regular schedule.
Exempt from lockdown	Select to let the cardholder to have 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 137*.



Add cardholders and groups

Add credentials

You can add the following types of credentials to a cardholder:

- QR code
- PIN
- Card
- License plate

To add a QR credential to a cardholder:

Note

Using QR codes as credentials requires that the time on the system controller and the camera with AXIS Barcode Reader is synchronized. We recommend using the same time source for both devices for perfect time synchronization.

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 dynamic QR with PIN credential.
4. Set the start and end date for the credential.

5. To email QR code automatically after you save the cardholder, select **Send QR code to cardholder when credential is saved**.
6. Click **Add**.

To add a PIN credential to a cardholder:

1. Under **Credentials**, click **+ Add** and select **PIN**.
2. Enter a PIN.
3. To use a duress PIN to trigger a silent alarm, turn on **Duress PIN** and enter a duress PIN.
4. Set the **Valid from** and **Valid to** dates for the credential.
5. Click **Add**.

You can also configure a duress PIN that opens the door and triggers a silent alarm in the system.

Note

The cardholder must have an email address to receive the mobile credential.

To add a card credential to a cardholder:

1. Under **Credentials**, click **+ Add** and select **Card**.
2. To manually enter the card data, enter 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's not in the system.

3. To automatically get the card data of 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 reader(s)**.

Note

You can use 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 have enabled **Facility code** under **Access management > Settings**.
5. Set the start and end date for the credential.
6. Click **Add**.

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**.

See example in *Use license plate number as a credential, on page 145*.

Expiration date	
Valid from	Set a date and time for when the credential should be 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 expire. Select days, months, or years after the last use.

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 5. See *Add devices, on page 5*
2. Set date and time for the new devices with **Synchronize with server computer time**. See *Set date and time, on page 56*.
3. Upgrade the firmware on the new devices to the latest available version. See *Upgrade firmware, on page 55*.
4. Add a new door connected to your door controller. See *Add a door, on page 122*.
   4.1. Add a reader on **Side A**. See *Add a reader, on page 127*.
   4.2. Under **Door settings**, select **AXIS License Plate Verifier** as **Reader type** and enter a name for the reader.
   4.3. Optionally, add a reader or REX device on **Side B**.
   4.4. Click **Ok**.
5. Install and activate AXIS License Plate Verifier on your camera. See the *AXIS License Plate Verifier* user manual.
6. Start AXIS License Plate Verifier.
7. Configure AXIS License Plate Verifier.
   7.1. Go to **Configuration > Access control > Encrypted communication**.
   7.2. Under **External Peripheral Authentication Key**, click **Show authentication key** and **Copy key**.
   7.3. Open AXIS License Plate Verifier from the camera's web interface.
   7.4. Don't do the setup.
   7.5. Go to **Settings**.
   7.6. Under **Access control**, select **Secure Entry** as **Type**.
   7.7. In **IP address**, enter the IP address for the door controller.
   7.8. In **Authentication key**, paste the Authentication key that you copied earlier.
   7.9. Click **Connect**.
   7.10. Under **Door controller name**, select your door controller.
   7.11. Under **Reader name**, select the reader you added earlier.
   7.12. Turn on integration.
8. Add the cardholder that you want to give access to. See *Add a cardholder, on page 142*
9. Add license plate credentials to the new cardholder. See *Add credentials, on page 143*
10. Add an access rule. See *Add an access rule, on page 146*.

10.1. Add a schedule.

10.2. Add the cardholder that you want to give license plate access to.

10.3. Add the door with the AXIS License Plate Verifier reader.

Add a group

Groups allow you to manage cardholders and their access rules collectively and efficiently.

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 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 137*.
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**.

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**.
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.



Doors

For information about manual actions, like manually unlocking a door, see .

Zones

For information about manual actions, like manually unlocking a zone, see .

Export system configuration reports

You can export reports that contain different types of information about the system. AXIS Camera Station 5 exports the report as a comma-separated value (CSV) file and saves it 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.

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 132*.

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**.

Import and export

Import cardholders

This option imports cardholders, cardholder groups, credentials, and cardholder 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 one.

You can also choose to map users in an Active Directory database as cardholders, see *Active directory settings[BETA], on page 138*.

Import options	
New	This option removes existing cardholders and adds new cardholders.
Update	This option updates the existing cardholders and adds new cardholders.
Add	This option 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** and go to the CSV file. Click **Open**.
6. Enter a column delimiter and 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.

Import settings	
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. The Unique identifier prevents the import of duplicate personnel records.
Card number format	**Allow both hexadecimal and number** is selected 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 5 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 before the last cardholder import.

1. On the **Access management** tab, click **Import and export**.
2. Click **Undo import**.
3. Click **Yes**.

System Health Monitoring BETA

The System Health Monitoring tab allows you to monitor the health data from a single or multiple AXIS Camera Station 5 systems on the same network.

If you manage systems on different networks, AXIS System Health Monitoring Cloud Service provides the same functionality but through the cloud. See *Setup AXIS System Health Monitoring Cloud Service, on page 101* for more information.

	Shows a summary of the devices and systems that you have access to. See *Inventory, on page 150*.
	Shows a storage summary and recording details of each camera from the monitored systems. See *Storage, on page 151*.
	Shows the System Health Monitoring logs from the monitored systems. See *Notifications, on page 151*.

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 except for continuous and motion triggered recordings with **None** as recording type.

Workflow

1. *Configure System Health Monitoring BETA, on page 139*
   1.1. Set up notifications. See *Notifications, on page 139*.
   1.2. Set up multisytem. See *Multisystem, on page 140*.
2. Monitor the health data from AXIS Camera Station 5 systems.
   2.1. *Inventory, on page 150*
   2.2. *Storage, on page 151*
   2.3. *Notifications, on page 151*

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 information including 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 information including device details and storage information if it 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 161*.
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 the content of the 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 61*.
Location	The path and name of the storage.
Total	The total amount of storage space. This is the same amount as "Total size" shown in Windows properties for the storage location.
Allocated	The maximum amount of storage assigned to recordings.
Used	The amount of storage space being 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 that camera recordings from the camera have been in the storage.
Oldest recording	The time of the oldest recording from the camera kept in the storage.
Latest recording	The time of the latest recording from the camera kept 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 the content of the 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 on which the event occurs.
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 5.

- 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 have to 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 your mouse on 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 value to add the hotkey for this action. • 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 to the action.
Edit a hotkey	Click the keyboard value of an action, and edit the value.
Remove a hotkey	Click the keyboard value of an action, and remove the value.

	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 the live logs including 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	AXIS Camera Station 5 user that performs the action.
Computer	The computer (Windows domain name) on which AXIS Camera Station 5 is installed.
Window user	The Windows user that administers AXIS Camera Station 5.
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 5 searches the log list except for in **Time** and shows the search results that contain all the keywords. For supported search operators, see *Optimize your search, on page 35*.
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 alarms generated by rules and motion detection in a list. 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 ware taken care of.
	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, for example manual recordings, video streaming started or stopped, action rules, door created, and cardholder created. Select the audits and click  in the toolbar to export the audits as a text file.

Alarms

The Alarms tab is available at the bottom of AXIS Camera Station 5 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 176*.

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. AXIS Camera Station 5 server that sends the alarm.
Component	The component that triggers the alarm.
	Show an alarm procedure, only available when the alarm contains an alarm procedure.
	Go 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 the alarm before you remove it.

To deal with a specific alarm:

1. Click  **Alarms and Tasks** at the bottom of AXIS Camera Station 5 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 were taken care of, 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 AXIS Camera Station 5 client.

The following tasks are personal and are only visible for the administrators and the users who started it.

- 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 started by you. 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**: Task completed with errors, that is, the task failed on one or more devices. • **Finished**: Task completed. • **Finished during lost connection**: Displayed if the task completed while the server connection was down. Task status can't be determined. • **Lost connection**: Displayed if 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 5 server that performs the task.

To deal with one or more tasks:

1. Click **Alarms and Tasks** at the bottom of AXIS Camera Station 5 client, and click the **Tasks** tab.
2. Select the tasks and click on 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. All failed operations should be reviewed and configured 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 was successfully completed. • **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 a report in HTML format with an 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, cameras settings including action rules, schedules, recording storage, auxiliary devices, and licenses. This is useful for troubleshooting and when you contact support.

To view a report in HTML format with an overview of the server system configuration:

1. Go to **Configuration** > **Server** > **Diagnostics**.
2. Click **View server configuration sheet**.

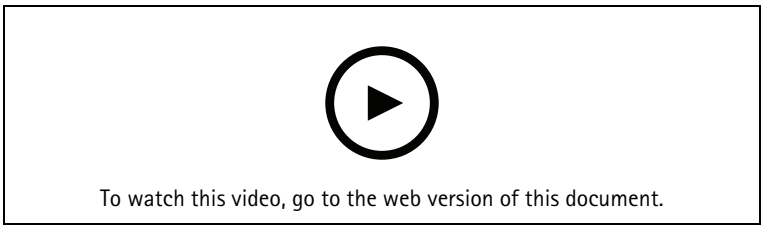
System report

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 the automatically generated file name.
4. Click **Browse** to select where to save the system report.
5. Choose your preferred settings:
   - **Automatically open folder when report is ready** to view it straight away.
   - **Include all databases** to add detailed information about recordings and system data.
   - **Include screenshots of all monitors** to simplify system report analysis.
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 data storage using the current system settings in AXIS Camera Station 5. Output: Passed or failed.
Low light conditions	Test of data streaming and data storage using settings optimized for typical low light conditions, for example gain settings. Output: Passed or failed.
Stress test	Test that increases data streaming and data storage step by step, until the system reaches its maximum limit. Output: Information about 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 5 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 view the report or click **Save report** to save it.

Feedback

You can choose to share anonymous client usage data automatically when you configure the client and manually send your feedback to help us improve AXIS Camera Station 5 and your user experience. See *Configure client, on page 95*.

Note

Don't use the feedback form to submit support requests.

1. Go to ☰ > **Help** > **Feedback**.
2. Choose a reaction and enter your feedback.
3. Click **Send**.

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 updates.

5. Click the link to go to the file location.

Body worn settings

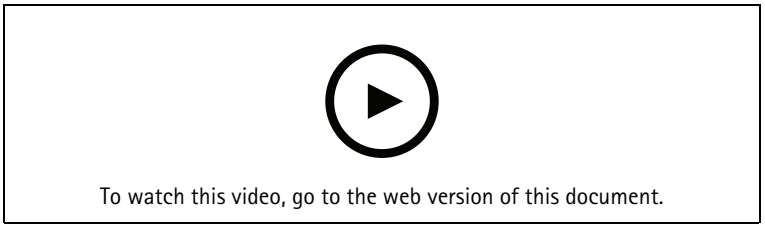
To connect with a body worn system, you must create a connection file. See *Set up an Axis body worn system.*

Note

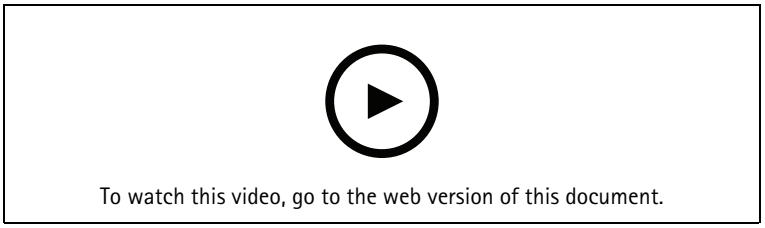
Before you create the connection file, renew the server certificate if the server IP address has changed, or AXIS Camera Station was upgraded from a version earlier than 5.33. For how to renew the certificate, see *Certificates, on page 115*.

To create a connection file:

1. Go to > **Other** > **Body worn settings**.
2. To change the default site name shown in your body worn system, enter a new name.
3. Click **Export**.
4. Under **Latest export**, a link to the file appears or updates.
5. Click the link to go to the file location.



Set up an Axis body worn system



Playback and export Axis body worn camera recordings

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 5 service control

The server uses AXIS Camera Station 5 service control to start and stop and to 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 be able 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 5 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 shows in the software client. The default server name is the computer name. The name doesn't change if you change the computer name.
Ports range	Specify the range of ports. The rest of the ports changes automatically.
Server HTTP port	The HTTP port number that the server uses to communicate with the client. The default port is 55752.
Server TCP port	The TCP port number that the server uses to communicate with the client. The default port is 55754. The port number is calculated by adding 2 to the server port number.
Mobile communication port	The mobile port number that the server uses to communicate with the client. The default port is 55756. The port number is calculated by adding 4 to the server port number.
Mobile streaming port	The mobile port number that the server uses for video streaming. The default port is 55757. The port number is calculated by adding 5 to the server port number.
Component communication port	The port number used by the component to communicate with network devices through the server. The default port is 55759. The port number is calculated by adding 7 to the server port number.
Ports used by AXIS Camera Station 5 components	After you specify the port range, the list shows the ports usable for the components. The default port range for AXIS Camera Station 5 components is 55760–55764.
Allow AXIS Camera Station 5 to add exceptions to the Windows Firewall	Select this option if you want to allow AXIS Camera Station 5 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.

Proxy settings	
Direct connection	Select this option if there isn't a proxy server between AXIS Camera Station 5 server and the cameras in the system.
System account Internet options / automatic	Default proxy settings. This option uses the current proxy settings in Internet Options for the system account.
Use manual proxy settings	Select this option if a proxy server separates the AXIS Camera Station 5 server and any cameras in the system. Enter the address and port number of the proxy server. This is usually the same address and port number under Internet Options in Windows Control Panel. • Specify to not use the proxy server with addresses beginning with certain characters. • Select **Always bypass proxy server for local addresses** and enter local addresses or hostnames of local cameras where communication doesn't need to pass through the proxy. You can use wildcards in the address or hostnames, for example: "192." or ".mydomain.com".

Port list for AXIS Camera Station 5

The following tables show which ports and protocols AXIS Camera Station 5 uses. You may need to allow these in your firewall for optimum performance and usability. We calculate port numbers based on the default HTTP main port 55752.

AXIS Camera Station 5 server sends data to devices on the following ports:

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.

AXIS Camera Station 5 server receives data from clients on the following ports:

Port	Number	Protocol	In/Out	Communication between	Description
Default SSDP port	1900	UDP	Multicast (Inbound + Outbound)	Server and client	Used to discover AXIS Camera Station 5 servers with SSDP (UPNP). Multicast 239.255.255.2-50.
Main HTTP port and HTTP streaming port	55752	TCP	Inbound	Server and client	Used for video, audio, metadata stream (AES encryption).
Main TCP port	55754	TCP	Inbound	Server and client	+2 offset from main HTTP port. Used for application data (TLS 1.2 encryption). For 5.15.007 or lower, TLS 1.1 encryption is used.
SSDP web server port	55755	TCP	Inbound	Server and client	+3 offset from main HTTP port. Used for AXIS Camera Station 5 server

					discovery with SSDP/UPNP.
API web server port	55756	TCP	Inbound	Server and mobile app	+4 offset from main HTTP port. Used for application data and video stream MP4 over HTTPS.
API media port	55757	TCP	Inbound	Server and mobile app	+5 offset from main HTTP port. Used for video stream RTSP over HTTP.
Local proxy HTTP port	55758	TCP	Inbound	Internal communication in server	+6 offset from main HTTP port. +2 offset from API web server port. Only accessible internally on AXIS Camera Station 5 server computer. Workaround port for unknown issue. Mobile apps makes 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	55759	TCP	Inbound	Server and component	+7 offset from main HTTP port. Used for secure communication between component and devices.

Reserved ports for components

Component	Listens on interface	Port	Number	Protocol	In/Out	Communication between	Description
Secure Entry	Localhost (127.0.0.1)	Web server port	55766	HTTPS	Inbound	Client (Access management tab) and component	+14 offset from main HTTP port. Older installations used port 8081.
Secure Entry	All (0.0.0.0/ INADDR_ ANY)	Web server port	55767	HTTPS	Inbound	Main server and sub servers	+15 offset from main HTTP port. Used for communication between main server and sub servers in multi-server setup.
System Health Monitoring	All (0.0.0.0/ INADDR_ ANY)	Web server port	55768	HTTPS	Inbound	Client (System Health Monitoring tab) and component	+16 offset from main HTTP port. Used to host System Health Monitoring web pages and for sharing data in multisystem setup.
System Health Monitoring Cloud Service	localhost	Web server port	55769	HTTPS	Inbound	AXIS Camera Station 5 (web page) and CloudService backend (plugin)	+17 offset from main HTTP port. Used for System Health Monitoring Cloud Service to enable System health monitoring.
Smart search 2	localhost	Web server port	55770	HTTPS	Inbound	Client (Smart search tab)	+18 offset from main HTTP port.

Compo-nent	Listens on interface	Port	Number	Protocol	In/Out	Communi-cation between	Description
						and component	Used to host Smart Search API and serve client web page.
			55771				Reserved for future use.
			55772				Reserved for future use.
			55773				Reserved for future use.
			55774				Reserved for future use.
			55775				Reserved for future use.
			55776				Reserved for future use.
			55777				Reserved for future use.
			55778				Reserved for future use.
			55779				Reserved for future use.
			55780				Reserved for future use-
			55781				Reserved for future use.
			55782				Reserved for future use.
			55783				Reserved for future use.

Compo-nent	Listens on interface	Port	Number	Protocol	In/Out	Communi-cation between	Description
Local-IAM (IDP)	0.0.0.0	IDP_OIDC (Public)	55784	HTTPS	Inbound	Reverse proxy and local-iam	+32 offset from main HTTP port. Public port.
Local-IAM (IDP)	0.0.0.0	MTLS (Admin)	55785	HTTPS	Inbound	Third party services	+33 offset from main HTTP port. Adminis-trator port.
Local-IAM (IDP)	127.0.0.1	TOKENIZER	55786	HTTPS	Inbound	Third party services	+34 offset from main HTTP port. Tokenizer port.
			55787				Reserved for future use.
Opentele-metry	127.0.0.1	gRPC port	55788	gRPC	Inbound	Third party services	+36 offset from main HTTP port.
Opentele-metry	127.0.0.1	HTTP port	55789	HTTPS	Inbound	Third party services	+37 offset from main HTTP port.
		Web server port	55790	HTTPS	Inbound	3rd party integration services and component	
			55791				Reserved for future use.
			55792				Reserved for future use.
			55793				Reserved for future use.
			55794				Reserved for future use.
			55795				Reserved for future use.

Compo-nent	Listens on interface	Port	Number	Protocol	In/Out	Communi-cation between	Description
NATS Broker	127.0.0.1	NATS	55796	NATS	Inbound	Between AXIS Camera Station 5 and compo-nents, and between compo-nents themselves	+44 offset from main HTTP port.
Opentele-metry	127.0.0.1	HTTP port	55797	HTTP	Inbound	Monitoring endpoint to fetch metrics from the open telemetry collector	+45 offset from main HTTP port.

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	55750	TCP	Inbound	Server and device	-2 offset from main HTTP port.
Upgrade status UDP port	15156	UDP	Inbound + Outbound	Server and service control	AXIS Camera Station 5 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 5 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 5 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`.

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 database creates a backup every night and before each system upgrade. In AXIS Camera Station 5 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 5 server to apply the change. If the backup folder path is incorrect or AXIS Camera Station 5 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. Any number between 1 and 30 can be used. 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 5 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, instead specify a location under **Configuration > Storage** to store them. Back up the recordings separately.
- Server settings, proxy settings, and database settings in AXIS Camera Station 5 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 174*. A system backup includes both the core database files and the component database files, see *Database files, on page 173*.

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. • **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 files includes more detailed information about the backup.

Maintenance backup

Specify the backup folder to store the maintenance backups in the **Database** tab, see *Database settings, on page 174*. 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 5.
- When you manually run database maintainer from AXIS Camera Station 5 service control. See *Database maintenance, on page 176*.
- Automatically by the scheduled database maintenance task configured in Windows Task Scheduler. See *Tools, on page 177*.

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 you can do a manual backup:

- Go to `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` and make a copy of the database files.
- Generate a system report with all databases included and copy the database backup files. Make sure to select **Include all databases**. See *System report, on page 161*.

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 174*.

Note

The database doesn't store the recordings, instead specify a location under **Configuration > Storage** to store them. Back up the recordings separately.

To restore the database:

1. Go to AXIS Camera Station 5 service control and click **Stop** to stop the service.
2. Go to the database backup files. See *Backup database, on page 174*.
3. Extract the files.
4. 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.
5. If you use AXIS Camera Station Secure Entry, copy **SecureEntry.db** from `Components > ACMSM` to `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db`.
6. If you use smart search, copy **smartSearch-backup-yyyyMMddHHmmssffff.sqlite3** from `smartsearch` to `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Smart Search\data` and rename it to **smartSearch.sqlite3**.
7. Go back to AXIS Camera Station 5 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 177*.

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 on the rare instance of forced shrinking.

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 since some antivirus software can corrupt the database. If you use an external backup system, don't back up the current and 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 5 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 look for errors in the RAM memory.

Tools

In AXIS Camera Station 5 service control, select **Modify settings** and click **Tools** to start database maintenance and create partial system reports.

Database maintainer

- Open AXIS Camera Station 5 service control.
- Click **Tools**.
- Under **Database maintainer**, click **Run**.
- The estimated downtime displays. Click **Yes** to continue. Once started the process can't be canceled.

Note

- AXIS Camera Station 5 server and all ongoing recordings stop during maintenance. After maintenance, the server starts automatically.
- Do not 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 5 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 5 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. AXIS Camera Station 5 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 start 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 5 and how to troubleshoot them. We have put the issues into a related topic to make it easier to find what you are looking for; a topic can be for example audio or live view. For every issue there is a solution described.

Learn more

Visit *axis.com/support* for

- Frequently Asked Questions
- Hardware requirements
- Software upgrades
- Tutorials, training material and other useful information

The AXIS Camera Station 5 service

The service restarts often

The server can be overloaded which causes a long task queue and can also corrupt the databases.

- In resource management of your system, verify if AXIS Camera Station 5 or any other application use a high number of resources.
- Run the database maintainer, go to *Database maintenance* in AXIS Camera Station 5 user manual.

If none of above helps, contact Axis Support. Go to *Escalation process, on page 193*.

Devices in the video management system

Common issues

Can't contact the camera	
The VMS can't contact the camera. The listed cameras weren't added.	1. Make sure the camera has a network connection, that there is power, and that the camera runs. 2. Go to **Configuration > Add devices** and try to add the camera again.

Installation was canceled	
The user canceled the installation. The listed cameras weren't added.	To add the cameras, go to **Configuration > Add devices**.

Fail to set password on camera	
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

If the device was used in a different system before you added it to AXIS Camera Station 5:

- Do a factory default of the device.

If the device still can't be added to the video management system, try to add the device to AXIS Device Manager.

You can add another device model than the one you want to add:

- If the device is a new product or has a newly released firmware, it can be a compatibility issue. Make sure to use the latest AXIS Camera Station 5 software version.

If it's not possible to add another device model:

- Troubleshoot the camera, go to *axis.com/support/troubleshooting*.

Can't update device firmware through AXIS Camera Station 5

It's not possible to upgrade the camera from its web interface:

- Troubleshoot the camera, go to *axis.com/support/troubleshooting*.

Firmware can't be upgraded for all devices:

- Make sure there is a network connection.
- If it's not a network related issue, contact Axis support. Go to *Escalation process, on page 193*.

Firmware can't be upgraded for specific models:

- It can be a compatibility issue, contact Axis support. Go to *Escalation process, on page 193*.

No devices found

The video management system automatically searches the network for connected cameras and video encoders but can't find any cameras.

- Make sure the camera has a network connection and that there is 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. Go to *Client proxy settings* in AXIS Camera Station 5 user manual.
  - Change the NAT or security system if a NAT or security system separates the client and the server. Make sure to 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 5*.
  - Change the server proxy settings if a proxy server separates the server and the devices. Go to the Proxy settings section in *Service control general* in AXIS Camera Station 5 user manual.
- Add cameras manually, go to *Add devices* in AXIS Camera Station 5 user manual.

Repeated message "Reconnecting to camera in 15 seconds"

Possible issues:

- An overloaded network.
- The camera isn't accessible. Make sure that the camera has a network connection and that there is power.
- 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.
- Change the video and audio settings, for example optimize the profile settings for low bandwidth.

Recordings

See *Live view, on page 183* for more information about possible performance issues influencing recordings and playback.

Common issues

Continuous recording isn't enabled	
The listed cameras don't have continuous recording 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	
The system can't configure the recording storage.	1. To use a different storage, go to **Configuration > Storage > management**. 2. Add the storage and configure the storage settings for the cameras.

Fail to install the AXIS Video Content Stream application	
This error message appears if the application can't be installed on a camera that supports AXIS Video Content Stream.	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 stop after a few seconds, it indicates that the disk is full or that there is too much intruding data.

- In the server configuration sheet, under **Recording Storage** control that there is free space and no intruding data.
- Increase the storage limit for the video management system.
- Assign more storage to the storage pool. Go to *Configure storage* in AXIS Camera Station 5 user manual.

Recording gaps during continuous recording

Along with gaps, alarms labeled **Recording errors**. The gaps can occur for several reasons, such as:

- Server overload
- Network issue
- Camera overload
- Disk overload

Control if the recording gaps occur on all the cameras. If it doesn't occur on all the cameras, it can be camera overload. Ask yourself these questions to find the reason:

- 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, confirm if the system uses one of the hardware resources more than normal. If the disk shows signs of overuse, add more disks and move several cameras to record to the new disks.
- Reduce the amount of data written on the disk (Video settings, ZIP stream, FPS, resolution). Keep in mind 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 183*.

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 exported recordings* in AXIS Camera Station 5 user manual.

Note

AXIS File Player automatically opens all recordings that are in the same folder as the player.

Recordings disappear

The system only saves recordings for a specified number of days. To change the number of days, go to **Configuration > Storage > Selection**.

If the storage becomes full, the system deletes recordings before the designated number of days.
To avoid a full storage, try the following:

- Add more storage. Go to **Configuration > Storage > Management**.
- Change the amount of storage space assigned to AXIS Camera Station 5. 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 H.264 video format for recording, M-JPEG format requires much more storage space.
  - Use Zipstream to additionally decrease the size of the recordings.

Failover recording issues

The failover recording doesn't record to the server after the connection was restored.

Cause	Solution
The bandwidth between the camera and the server is insufficient to transfer the recording.	Improve 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 synchronize the NTP for future recordings. • Synchronize the camera's time with the server or setup the same NTP server on the camera as on the server.

Failover recording in AXIS Camera Station 5 doesn't work in the following scenarios:

- Controlled server shutdowns.
- Short interruptions less than 10 seconds in the connection.

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 5 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	If you use an internal graphic card, we don't recommend more than two monitors per graphic card. 1. Open the DirectX Diagnostic Tool (search for dxdiag on the computer) 2. Make sure AXIS Camera Station 5 supports the dedicated graphic card, see *axis.com/products/axis-camera-station/hardware-guidelines*. Note You can't run the client on a virtual machine.

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 *axis.com/products/axis-camera-station/hardware-guidelines*.
The camera is connected to another video management system than AXIS Camera Station 5	Disconnect the camera from the other client and default the camera before you connect it to AXIS Camera Station 5.
One camera uses many different streams, especially high resolution	Could be a problem especially for some M-Line cameras. • Change the stream to the same streaming profile or lower resolution. See *Streaming profiles* in AXIS Camera Station 5 user manual.
Server overload	
Unusual CPU/RAM usage corresponding to the same time as the issue	Make sure no other CPU/RAM consuming application runs at the same time.
Network issue	
Unusual bandwidth usage corresponding to the same time as the issue	Make sure no other bandwidth consuming application 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 turns on by default, see Hardware decoding in *Streaming* in AXIS Camera Station 5 user manual.

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*.
- If there is an antivirus software installed, it might block live streams.
- Allow AXIS Camera Station 5 folders and processes, see *FAQ*.
- Make sure the firewall doesn't block connections on certain ports, see *Service control general* in AXIS Camera Station 5 user manual.
- Make sure the desktop experience was installed for supported Windows server OS versions. See *Scheduled export* in AXIS Camera Station 5 user manual.
- Make sure the lower resolution stream works.

If none of the above helps, contract Axis support, go to *Escalation process, on page 193*.

Storage

Network storage isn't accessible

If you use the local system account to log in to AXIS Camera Station 5 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 5 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

Fail to install the AXIS Video Motion Detection application	
Can't install AXIS Video Motion Detection 2 or 4. The camera uses the built-in motion detection for motion recording.	To install the application manually, go to *Install camera application* in AXIS Camera Station 5 user manual.

Fail to retrieve current Motion Detection	
The video management system can't retrieve motion detection parameters from the camera. The camera uses the built-in motion detection for motion recording.	To install the application manually, go to *Install camera application* in AXIS Camera Station 5 user manual.

Motion detection not configured	
Can't configure motion detection in the listed cameras.	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 is not enabled	
The listed cameras don't have motion recording 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 Video Motion Detection related recordings.

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* in AXIS Camera Station 5 user manual.
Built-in motion detection	You can configure the included and excluded windows. See *Edit built-in motion detection* in AXIS Camera Station 5 user manual.

Adjust trigger period

The trigger period is an interval time between two successive triggers, use this setting to reduce the number of successive recordings. The recording continues if an additional trigger occurs within this interval. If an additional trigger occurs, the trigger period starts over from that point in time.

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.

Audio

No audio in live view

If there is 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 5.

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* in AXIS Camera Station 5 user manual.

No audio in playback

Audio is available in playback if you enable 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 logged in to multiple servers the client starts, and you can see the connection status in the status bar. For more information about the connection status, see *Connection status* in AXIS Camera Station 5 user manual.

The username or password is incorrect	The username and password combination isn't valid to log in to the specified server.	• Review the spelling or use a different account. • Make sure that the user has access rights to AXIS Camera Station 5 server. • The clocks in AXIS Camera Station 5 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 on the server, must run the client as administrator. • For information about user access rights, see *Configure user permissions* in AXIS Camera Station 5 user manual.
User isn't authorized to log in to the server	The user can't use AXIS Camera Station 5 on the specified server.	Add the user in the user permission dialog.
Unable to verify message security	An error occurred when setting up the secure connection to the server, most likely caused by the client or server time being out of sync.	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	The client is unable to establish any kind of connection to the server.	• Make sure that the server computer can connect to the network. • Make sure the server computer is running. • Make sure the firewall was properly configured. • Check the spelling of the server address. • Check the client proxy settings.
No response from the server	The client can contact the server computer but no AXIS Camera Station 5 server is running.	Make sure that you connect to the right computer and that AXIS Camera Station 5 server is running.
Client can't connect to the server	The client can't connect to the server and an error message is appears.	Make sure that your network was properly configured: • Verify that the OS is supported. For a full list of the supported OS, go to *release note*

		• From service control, verify that AXIS Camera Station 5 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. • Investigate if there is a proxy server between the server and the client. – Configure the server proxy in service control. – Configure the client proxy setting at the log in page, select **Change proxy settings**. – Configure the client proxy settings in Windows Internet Options and select to use the default option in **Change Proxy settings**.
Unable to connect to the server	An unknown error was encountered when connecting to the server.	• Make sure that the address and port of AXIS Camera Station 5 server are correct. • Make sure that no NAT, firewall, or antivirus software block the connection to the server. See *Configure the firewall to allow access to AXIS Secure Remote Access* for more information. • Use AXIS Camera Station 5 service control to make sure that the server is running. – Open AXIS Camera Station 5 service control, see *AXIS Camera Station service control* in AXIS Camera Station 5 user manual. – View the server status in the **General** tab. If the status is **Stopped**, click **Start** to start the server.
Unable to find the server	The client can't resolve the address entered to an IP address.	• Make sure that the server computer can connect to the network. • Make sure that the address and port of AXIS Camera Station 5 server are correct. • Make sure that no NAT, firewall, or antivirus software block the connection to the server. See *Configure the firewall to allow access to AXIS Secure Remote Access* for more information.
The server and client version differs	The client runs a newer version of AXIS Camera Station 5 than the server.	Upgrade the server to run the same version as the client.
	The server runs a newer version of AXIS Camera Station 5 than the client.	Upgrade the client to run the same version as the server.

Unable to connect to server. Server is too busy.	The server can't respond because of performance issues.	Make sure that the server computer and the network isn't overloaded.
The local AXIS Camera Station 5 server doesn't run	You use **This computer** to connect, but the installed AXIS Camera Station 5 server doesn't run.	Use service control to start AXIS Camera Station 5 or select a remote server to log in to.
This computer doesn't have AXIS Camera Station 5 server installed	You use **This computer** to connect, but there is no server installed on this computer.	Install AXIS Camera Station 5 server or choose a different server.
The selected server list is empty	The selected server list for login was 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:

- Control that the license key was entered correctly.
- Change the client proxy settings to allow AXIS Camera Station 5 access the internet.
- Register your license offline, see *License a system offline* in AXIS Camera Station 5 user manual.
- Make a note of the Server ID and activate AXIS Camera Station 5 license from *license-portal.lp.axis.com*.
- Make sure that the server's time is up to date.

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 5 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 5 can't communicate with the device until you solve the certificate error.

Possible errors		
Certificate Not Found	If the device certificate was removed.	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	The device certificate was modified outside of AXIS Camera Station 5. This can indicate that an unauthorized person accessed and modified the device.	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 5 without a stored password, the alarm below 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 different 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 5 loses its connection to the devices, and some system components restart.

To let AXIS Camera Station 5 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 5 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 Windows Time service can't reach the NTP server.

- Make sure that the NTP server is online.
- Make sure that the firewall settings are correct.
- Make sure that 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 time stamped with the time when the server received it instead of the time of 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 that the device can reach the specified NTP server.
   2.3. Reload the device under **Configuration > Devices > Management**.
3. If the server time offset is smaller 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 disable alarms.

For assistance, contact Axis support.

Technical support

Technical support is available for customers with a licensed version of AXIS Camera Station 5. 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, see*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 happen.
- The time and the concerned camera's name or IP address where the issue happens.
- AXIS Camera Station 5 system report generated directly after the issue happens. The system report must be generated from the client or server where the issue was reproduced.
- Optional screenshots or recordings from all monitors that show the issue. Turn on the debug overlay function when you take screenshots or make the recording.
- If necessary, include the database files. Exclude these to make the upload go faster.

Some issues require additional information that the support team requests if necessary.

Note

If the file is larger than 100 MB, for example, network trace or database file, use a secure file sharing service that you trust to send the file.

Additional information	
Debug level logs	Sometimes we use debug level logging to collect more information. This is only done by request from an Axis support engineer. You can find Instructions on *Axis online helpdesk*.
Live view debug overlay	Sometimes it's beneficial to provide screenshots of the overlay information or a video that shows the change of values in the time that is of interest. To add overlay information do as follows: • Press Ctrl + i one time to display overlay information in the live view. • Press Ctrl + i two times to add debug information. • Press Ctrl + i three times to hide the overlay.
Network trace	If requested by the support engineer, generate network traces when you create the system report. Take the network traces during the time when the issue happens if it's reproducible. This includes: • A 60 sec Network trace taken on the camera (only applicable for firmware 5.20 and later) Use the following VAPIX command to change the login, IP address, and duration (in seconds) if necessary:

Additional information	
	`http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60` • A 10-30 sec Network trace taken on the server that shows communication between the server and the camera.
Database files	In cases where we have to examine or manually repair the database. Select **Include database in the report** before you generate the system report.
Screenshots	Use screenshots when it's a live view issue, related to UI. For example, when you want to show a timeline for recordings or when it's difficult to describe.
Screen recordings	Use screen recordings when it's difficult to describe the problem in words, for example when there are many UI interactions involved to reproduce the issue.

T10122292

2026-02 (M72.2)

© 2018 – 2026 Axis Communications AB