AXIS Camera Station User Manual

User manual

What's new?

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

AXIS Camera Station features

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

AXIS Camera Station tutorial videos

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

Helpful links for an administrator

Here are some topics that might interest you.

- *Log in to AXIS Camera Station server on page 11*
- *Configure devices on page 39*
- *Configure storage on page 64*
- *Configure recording and events on page 67*
- *Configure connected services on page 96*
- *Configure server on page 99*
- *Configure licenses on page 106*
- *Configure security on page 109*

More AXIS Camera Station 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.

- *Log in to AXIS Camera Station server on page 11*
- *Configure client on page 93*
- *Live view on page 15*
- *Playback recordings on page 24*
- *Export recordings on page 25*
- *AXIS Camera Station getting started guide for operators*
- *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 AXIS Camera Station*
2. *Add devices*
3. *Configure recording method on page 7*

For operators:

1. *View live video on page 7*
2. *View recordings on page 8*
3. *Export recordings on page 8*
4. *Play and verify recordings in AXIS File Player on page 8*

Start AXIS Camera Station

Double-click the AXIS Camera Station 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 server installed on the same computer as the client.

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

Add devices

The **Add devices** page opens the first time you start AXIS Camera Station. AXIS Camera Station 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 42*.
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 15* for more information.

View recordings

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

See *Recordings on page 24* for more information.

Export recordings

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

See *Export recordings on page 25* 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.

Network configuration

Configure proxy or firewall settings before using AXIS Camera Station if the AXIS Camera Station client, AXIS Camera Station 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 client.
2. Click **Change client proxy settings**.
3. Change the client proxy settings. See *Client proxy settings* in User Manual.
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 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* in AXIS Camera Station Service Control.
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 Service Control can pass through the firewall or NAT. Contact the network administrator for instructions on configuring the NAT or firewall.

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. See General in AXIS Camera Station Service Control.

See *General* in AXIS Camera Station Service Control.

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 server, cameras, video encoders, and auxiliary devices on a secure network separate from the office network. You can install the AXIS Camera Station 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.

About AXIS Camera Station

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

AXIS Camera Station 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 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 – 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 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*.

Multiple clients can connect to the same server, and each client can connect to multiple servers.

Log in to AXIS Camera Station server

Using the AXIS Camera Station 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 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 *Log in on a remote server on page 11*.

AXIS Secure Remote Access – See *Sign in to AXIS Secure Remote Access on page 11*.

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 Service Control. See *General on page 168*.

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, 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*.

Log in on 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 55752, 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 a different username and password.

Sign in to AXIS Secure Remote Access

Note

When trying to connect to a server using Axis Secure Remote Access, the server can't upgrade the client automatically.

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 client and the AXIS Camera Station server.

Note

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

The Add devices page on the Configuration tab opens when you're using AXIS Camera Station 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 37*.
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 141*.
Smart search 2	Use advanced filters to find vehicles and persons based on characteristics. See *Smart search 2 on page 34*.
System health monitoring	Monitor the health data from a single AXIS Camera Station system or multiple AXIS Camera Station systems. See *System Health Monitoring* ^{BETA} *on page 153*.
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 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 client version you're using.

Log out	Disconnect from the server and log off from the AXIS Camera Station client.
Exit	Exit and close the AXIS Camera Station 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 *Configure licenses*.
- 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 update available** appears when there is a new version if you're logged in as administrator. See *Update AXIS Camera Station on page 101*.

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 servers.

Views provide access to all the cameras and devices added to AXIS Camera Station. 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 *Configure user permissions on page 109*.

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 8 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, see *Cameras on page 44*.
🔒	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**.
Show on	To open a view on another screen, right-click the image and select **Show on**.

Live view

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**.
Stream profile	To set the stream profile, right-click an image and select **Stream profile**. See *Stream profiles*.
Zoom	Use the mouse wheel to zoom in and out. Alternatively, press CTRL + (+) to zoom in and CTRL + (-) to zoom out.
Use Mechanical PTZ	Mechanical PTZ is 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.
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.
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**.
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**.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=image-management-in-live-view

Add digital presets

▶

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=image-management-in-live-view

PTZ control

Note

As an administrators you can turn off mechanical PTZ for users. See *Configure 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 blue 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 *Configure 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 45*.

🔈 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 95*.

Note

As an administrator you can turn off audio for users. See *Configure 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 servers, you can add any view, camera or device 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 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*.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=split-view

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 18*.

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.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=door-dashboard-in-split-view

Monitor and assist in door dashboard

Sequence

A sequence switches between views.

Note

When connecting to multiple AXIS Camera Station 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.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=sequence

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 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 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. A door icon can be:
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.

Coverage area	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. This option is only available for cameras and other devices.
Remove	Click 🗑 to remove the icon from the map.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=map

Add a map

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=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**.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=webpage

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

The Recordings tab handles recording search, playback, and export. The tab contains of a view of the recording and two panels where you can find views, images, playback tools, and cameras of 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 15*.

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. You can 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 shows a motion detection recording. A blue line in the timeline shows a recording triggered by an action rule. When you hover over a recording in the timeline, the recording type and time is shown. 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

▶	Plays the recording.
⏸	Pauses the recording.
⏮	Jumps to the start of the ongoing or previous recording or event. Right-click to go to recordings, events, or both.
⏭	Jumps to the start of the next recording or event. Right-click to go to recordings, events, or both.
|◀	Goes 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).

⏭	Goes 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).
🔊	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	Shows the metadata for a body worn system. This also displays 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.

🔖	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 video 2.5 minutes before and after the bookmark.
✏	Edit the bookmark name, description, and unlock or lock the recording.
🗑	Remove a bookmark. 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 make the marker point 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 28*.

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)**.

▶

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=export-recordings

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	
🔊	To mute audio, select a recording with audio and click 🔊 .
🎨	To edit the recording, select a recording and click 🎨 . See *Edit recordings (redaction) before exporting on page 28*.
📄	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.
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 29*.
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 list, select a format to export the recordings to. If you select MP4, audio in G.711 or G.726 format won't be included in the exported recordings.
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 *Configure user permissions on page 109*.

Edit recordings (redaction) before exporting

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 when the recording plays.
9. Move the timeline and make sure that the bounding box covers the object is 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**.

1. Create a bounding box, see *Blur a moving object on page 28*.
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**.

To generate bounding boxes from the analytic data, turn on the camera's analytic data. See *Stream profiles on page 45*.

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.

To improve video editing, install the application AXIS Video Content Stream 1.0 on the camera. This is only valid for cameras with firmware 5.50 and later. The application installs automatically when you add a camera to AXIS Camera Station. See *Install camera application*.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=improve-video-editing-with-axis-video-content-stream

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. Tnd 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 28*.

▶

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=export-incident-reports

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 25*.
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.

🔊	To mute audio, select a recording with audio and click 🔊 .
✎	To edit the recording, select a recording and click ✎ . See *Edit recordings (redaction) before exporting on page 28*.
🗎	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 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.

▶

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=smart-search

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 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 58*.
- Time synchronization between the AXIS Camera Station 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 137*
2. Configure time synchronization between the AXIS Camera Station server and cameras. See *Time synchronization on page 63*.
3. Create a filter or load an existing filter. See *Search on page 34*.
4. Manage search results. See *Smart search results on page 36*.

Search

To create a filter:

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**.

⏲	For cameras with background server classification, ⏲ appears in the image, indicating the classification status in the last hour, when Smart search 2 has classified less than 95% detections.
⏲	For cameras with background server classification, ⏲ appears in the image, indicating the classification status in the last hour, when Smart search 2 has classified less than 50% detections.
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, or create a custom interval.
Person	To detect persons, click **Object characteristics**, select **Person** and the clothing colors. You can select multiple colors.
Vehicle	To detect vehicles, click **Object characteristics** and select the vehicle types and colors. You can select multiple vehicle types and vehicle colors.
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**.
🔍	For devices with deep learning capability, you can set the server classification strategy to decide how to use the classification on device and classification on server. To select server classification strategy, click 🔍 . Server classification gives you more detailed search results, including detections the device didn't classify. Not using server classification gives you faster search results.
📁	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 delete a filter, click 📂 and click 🗑 . To load a filter, click 📂 and click a filter.
◇	To reset a filter, click ◇ and click **Reset**.

Smart search results

Filter	To include recordings with no metadata in the search results, click **Filter** and select **Time periods without metadata**.
≋	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.
Detection report	To generate a detection report, expand the classification details and scroll down to the bottom. Click **Detection report** and choose a location to save the report. The detection report includes the recording, snapshots, tracking details, and logs.

Limitations

- 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, such as:

- 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 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 from the **Source** drop-down list.
4. Enter any keywords in the search field. See *Optimize your search on page 38*.
5. 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.

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.
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 62* for more information.
Download search result	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.

Depending on the data source you can get different items in your search result. Here are a few examples:

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.

Data search

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=data-search

Search for access control data

Optimize your search

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

Use quotation marks `"  "` for exact matches with keywords	• Search for `"door 1"` returns results containing "door 1". • Search for `door 1` returns results containing both "door" and "1".
Use `AND` to find matches containing all keywords.	• Search for `door AND 1` returns results containing both "door" and "1". • 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.	• Search for `"door 1" OR "door 2"` returns results containing "door 1" or "door 2". • Search for `door 1 OR door 2` returns results containing "door" or "1" or "2".
Use parentheses `(  )` together with `AND` or `OR`.	• 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" • 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.	• Search for `[Max speed] > 28` returns results containing a number greater than 28 in the Max speed column. • Search for `[Average speed] < = 28` returns results containing a number less than or equal to 28 in the Average speed 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, 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 only supports devices with IPv4 addresses.
- Some video encoders have one IP address for each video port. In this case, AXIS Camera Station treats each video port as one device with one camera.

In AXIS Camera Station, 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 62*.

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 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 40*
   - *Find your video streams on page 41*

  - *Find prerecorded videos on page 41*

2. *Add devices, video streams or prerecorded videos on page 42*

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.
Communicating	AXIS Camera Station server is trying to access the device.
HTTPS certificate not trusted	AXIS Camera Station can't verify that the HTTPS certificate on the device is signed by a trusted issuer.
Communication error	AXIS Camera Station can't contact the device.
Enter password	AXIS Camera Station 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 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 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 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 third-party device	AXIS Camera Station doesn't support this third-party device.
Can only be used with AXIS Companion	The device is designed for AXIS Companion only.

Find your devices

The devices in your network are displayed automatically. To find the devices that are not 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.

4.4 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.

4.3 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.

.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 48* 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. Click **Install**. AXIS Camera Station 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. 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:

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 server has an internet connection. Or click **Download settings file** if your AXIS Camera Station doesn't have an internet connection.
2. In the AXIS Camera Station 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 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 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 sets the profile to medium.
- If you've defined both recording profiles in the Site Designer project, AXIS Camera Station sets the continuous recording profile to medium and the motion-triggered recording to high.
- AXIS Camera Station optimizes the aspect ratio, meaning the resolution can differ between the import and the Site Designer project.
- AXIS Camera Station 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 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.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=import-site-designer-projects

Add third-party devices

You can add third-party devices to AXIS Camera Station 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. See *Find your video streams on page 41*.

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 AXIS Camera Station can receive video streams from your network video products. See *AXIS Camera Station Device Compatibility Tool*.

AXIS Camera Station 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 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)
- 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 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 license.
- The number of cameras you can add depends on the license.
- Each AXIS Camera Station license allows a certain number of cameras.

To use view areas in AXIS Camera Station, 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 client and the device.
- Edit the camera settings. See *Edit camera settings*.

- Remove cameras. Doing this, AXIS Camera Station 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 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 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 non-camera devices:

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 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 camera models support H.264, which requires less bandwidth and storage space compared to, for example, M-JPEG. Cameras can only have one video profile with MPEG-4 at a time.
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.

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

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, 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 client and AXIS Camera Station 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. 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

Image configuration

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

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 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

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

- 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, 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 and from the camera.

Device management

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

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 96*, a link displays when there are new firmware versions available for devices. Click the link to upgrade the firmware versions. See *Upgrade firmware*.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=device-management

Upgrade firmware versions

If you have set up automatic check for new software versions in *Update AXIS Camera Station on page 101*, a link displays when there is a new AXIS Camera Station version available. Click the link to install a new version of AXIS Camera Station.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=device-management

Install a new version of AXIS Camera Station

A list of devices added to AXIS Camera Station 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 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.
  - **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 62*.
- **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 62*.
- **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 60*.
- **IEEE 802.1X:** The IEEE 802.1X status of the device. See IEEE 802.1X status in *Security on page 60*.
- **Server:** The AXIS Camera Station 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.

- 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 60*.
- Collect device data. See *Collect device data*.
- Select to use IP address or hostname. See *Connection on page 61*.
- 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 62*.

Assign IP address

AXIS Camera Station 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 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 62*.

- 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 54*.
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 54*.
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 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 54*.
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 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.

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 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:

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

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=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 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 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**.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=set-date-and-time

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. 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. 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.

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 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 112*.

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.

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 uses HTTPS to connect to the device.
	Off	AXIS Camera Station 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.
- 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.

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 37*.

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 to set up AXIS A1601 Network Door Controller in AXIS Camera Station, see *Set up AXIS A1601 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, 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 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 62*.
- **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 server. The following information is displayed:

- **Server:** The AXIS Camera Station 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. To receive alarm for time difference larger than 2 seconds, select **Send alarm when the time difference between server and device is larger than 2 seconds**.

6. Click **Apply**.

Configure storage

Go to **Configuration** > **Storage** > **Management** to open the Manage storage page. A list of the local storage and network storage that have been added to AXIS Camera Station is displayed. This page contains the following information:

Item	Description
The list displays the following information.	
Location	The path and name of the storage.
Allocated	The maximum amount of storage delegated to recordings.
Used	The amount of storage space being currently used for recordings.
Status	The storage status. Possible values are: • **OK** • **Storage full:** The storage is full. The unlocked, oldest recordings will be overwritten. • **Unavailable:** The storage information is currently unavailable. For example, if a network storage has been removed or disconnected. • **Intruding data:** Data from other applications use storage space allocated for AXIS Camera Station. Or, there are recordings with no database connection, so-called non-indexed recordings, in the storage space allocated for AXIS Camera Station. • **No permissions:** The user is not authorized to read or write to the storage. • **Low space:** The drive has less than 15 GB of free space, which AXIS Camera Station considers too low. To prevent errors or corruption, AXIS Camera Station performs a forced cleanup, regardless of the placement of the storage slider, to protect the drive. During the forced cleanup, AXIS Camera Station prevents recording until more than 15 GB of storage is available. • **Insufficient capacity**: The total disk size is less than 32 GB, which is not enough for AXIS Camera Station. 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 have replaced a broken disk, the RAID status changes from Degraded to Syncing. • **Syncing:** The RAID disks are synchronizing. It's possible to record and play recordings from the storage, but there is no redundancy if a physical disk breaks down. Once the physical disks are 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 have replaced the broken physical disks.

Server	The server where the local storage or network storage is.
The Overview section displays the following information for a selected storage.	
Used	Amount of storage space currently used by recordings that is indexed in the database. If a file is in the recording directory but not indexed in the database, the file is not calculated in this category. See Collect non-indexed files in *Manage storage on page 65*.
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 that are not indexed recordings and therefore unknown to AXIS Camera Station. 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 is allowed to use for recordings. You can adjust the slider and click **Apply** to adjust the allocated space.
The Network storage section is only available for a selected 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. In this page, you can specify the folder to store recordings. To prevent the storage from becoming full, a maximum percentage of total capacity to be used by AXIS Camera Station should be set. Additional local storage and network drives can be added for security and more space.

Note

- When connecting to multiple AXIS Camera Station servers, you can add a local storage or shared network drive on any connected server by selecting the server from the **Selected server** drop-down list.
- When the Service is logged on using the System account, you can't add network drives linking to shared folders on other computers. See *Network storage is not accessible*.
- The local storage or network storage can't be removed 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** and click **Add**.
2. To add a local storage, select **Local storage** and select a storage from the drop-down list.
3. To add a shared network drive, select **Shared network drive** and enter the path to a shared network drive. For example: \\ip_address\share. Click **OK** and enter the username and password for the shared network drive.
4. 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**.

Add a folder for new recordings

1. Go to **Configuration** > **Storage** > **Management** and select a local storage or shared network drive from the storage list.
2. Enter a folder name in the **Folder for new recordings** field to change the location where recordings will be stored.
3. Click **Apply**.

Adjust storage capacity

1. Go to **Configuration > Storage > Management** and select a local storage or shared network drive from the storage list.
2. Move the slide bar to set the maximum space to be used by AXIS Camera Station in the Overview section.
3. 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 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 will automatically start deleting old recordings to free up space.

Collect non-indexed files

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

The collected files are not deleted, but collected and placed 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 that server.

The data in the folder is placed in the order of where it was found. That means the content is divided first by server and 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** and select a local storage or shared network drive from the storage list.
2. In the Collect non-indexed files section, click **Collect** to initiate a task.
3. When the task is done, go to the Tasks tab and double-click the task to view the result.

Select storage devices to connect

Go to **Configuration > Storage > Selection** to open the Select storage page. This page features a list of all cameras that have been added to AXIS Camera Station 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. Multiple cameras can be configured at the same time.

This page contains the following information:

Item	Description
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 62*.
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 being 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 failover recording is enabled for the camera.
Fallback recording	Shows if fallback recording is enabled for the camera.
Server	The server where the local storage or network storage is.

The storage solution for every camera is configured when cameras are added to AXIS Camera Station. To edit storage settings for a camera:

1. Go to **Configuration** > **Storage** > **Selection** and select the camera to edit the storage settings. Use the **Type to search** field to find specific cameras.
2. In the Recording storage section:
   - In the **Store to** field, select the storage to save recordings to from the drop-down list. Available options are the local storage and network storage that were created.
   - Select **Failover recording** to store the recordings to the camera's SD card when the connection between AXIS Camera Station and the camera is lost. Once the connection is restored, the failover recordings are transferred to AXIS Camera Station.

   Note

   This feature can only be used for cameras that have an SD card and firmware 5.20 or later.

   - Select **Unlimited** retention time to keep recordings until the storage becomes full. Otherwise, select **Limited** to set the maximum number of days to keep recordings.

   Note

   If the amount of storage space reserved for AXIS Camera Station becomes full, recordings may be deleted before the designated number of days.

   - Specify the number of days to keep your recordings.
3. Click **Apply**.

Configure recording and events

When you add cameras to AXIS Camera Station, 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. Turn on **Motion detection** to use motion recording.
4. Edit **Video settings**:

- Select a **Profile** in the drop-down menu, **High** profile is default. Use a lower resolution to decrease the recording size. To edit profile settings, see *Stream profiles*.
- **Prebuffer**: Set the number of seconds before the detected motion to include in a recording.
- **Postbuffer**: Set the number of seconds after the detected motion to include in a recording.
- Select **Raise alarm** to raise an alarm when the camera detects motion.

5. Select a schedule or click **New** to create a new schedule. To lower the impact on your storage space, only record during specific time periods.
6. 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.
7. 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*.
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.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=motion-recording

Configure motion detection

Continuous and scheduled recording

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

To configure continuous recording:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera.
3. Turn on **Continuous** to use continuous recording.
4. Select a **Profile** in the drop-down menu, **Medium** profile is default. Use a lower resolution to reduce the recording size. To edit profile settings, see *Stream profiles*.
5. Select a schedule or click **New** to create a new schedule. To lower the impact on your storage space, only record during specific time periods.
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. See *Configure average bitrate on page 71*.
7. Click **Apply**.

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. Under **Manual**, edit **Video settings**:
   - 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 the detected motion to include in a recording.
   - **Postbuffer**: Set the number of seconds after the detected motion to include in a recording.
3. Click **Apply**.

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 you can save recordings when you lose connection to AXIS Camera Station. The camera saves recordings to the SD card if the connection is down for more than 10 seconds. The camera must have an SD card and firmware 5.20 or later. 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

Restart of the AXIS Camera Station server doesn't trigger failover recordings. For example, when you run Database maintainer, restart AXIS Camera Station Service Control, or restart the computer where the server is installed.

When there is a connection again, AXIS Camera Station imports the failover recording and marks it with a dark grey color in the timeline. The camera stores the last 10 seconds of a stream in its internal memory to try to compensate for the 10 seconds delay before the failover recording triggers. Short gaps of about 1 - 4 seconds might still appear.

Failover recording works differently depending on the recording method:

- **Motion detection with prebuffer**

  In case of disconnection for more than 10 seconds, failover recording turns on. The camera continuously records to the SD card until the connection is back or the SD card becomes full.

- **Motion detection without prebuffer**

    - In case of disconnection for more than 10 seconds when motion recording is not ongoing, failover recording doesn't turn on even if motion is detected.
    - In case of disconnection for more than 10 seconds when motion recording is ongoing, failover recording turns on. The camera continuously records to the SD card until the connection is back or the SD card becomes full.

- **Continuous recording**

  In case of disconnection for more than 10 seconds, failover recording turns on. The camera continuously records to the SD card until the connection is back or the SD card becomes full.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=failover-recording

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 with medium stream profile when you lose the connection between AXIS Camera Station and the recorder.

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 triggers, a new continuous recording starts with medium stream profile. 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 set the recorder as recording storage for the device. See *Set up AXIS S3008 Recorder*.
2. Go to **Configuration > Storage > Selection**.
3. Select the device and select **Fallback recording**.
4. Click **Apply**.

Recording method

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

Go to **Configuration > Recording and events > Recording method** to open the **Recording method** screen and show a list of all the devices.

A check mark in the list show what recording method a device uses. For devices of the same model, you can configure multiple devices at the same time. To customize profile settings for video and audio, see *Stream profiles*.

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**, select the camera and turn on **Continuous**.
4. Under **Video settings**, select the video profile that you configured.
5. 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.

6. 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, 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 can control devices connected to output ports.

Note

- When connected to multiple AXIS Camera Station 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 *Configure user permissions*.

Action rules use I/O ports as triggers or actions. Triggers use input signals, for example, when AXIS Camera Station 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 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. Make sure the information in **Type** and **Device** is correct.
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 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 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

AXIS Camera Station uses rules to configure actions. A rule is a set of conditions that define how and when actions should be performed. With action rules you can reduce the number of recordings, interact with devices connected to I/O ports, and alert operators about important events.

Note

- When connected to multiple AXIS Camera Station servers, you can select any connected server in **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.

Create a new rule

1. Go to **Configuration** > **Recording and events** > **Action rules**.
2. Click **New**.
3. Create triggers to define when to activate a rule. See *Add triggers*.
4. Click **Next**.
5. Create actions to define what happens when the rule activates. See *Add actions*.
6. Click **Next**.
7. Create a schedule for when to use the action rule. This reduces the amount of events and recordings. See *Schedules*.
8. Click **Next**.
9. Review the information in the **Details** screen.
10. Enter a name for the rule, and click **Finish** to use the rule.

Edit	To edit an existing rule, select the rule and click **Edit**.
Copy	To copy an existing rule, select the rule and click **Copy**.
Remove	To remove an existing rule, select the rule and click **Remove**.
Always	Select **Always** to always have the rule active.
Custom schedule	Select **Custom schedule** and select a schedule from the drop-down menu. You can create a new schedule or edit an existing schedule.

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. Since the camera processes the detection, it doesn't add any processing load to AXIS Camera Station server. See *Create motion detection triggers on page 76*.

Active tampering alarm – The tampering trigger activates when you reposition the device, something covers the lens, or the lens severely defocus. Since the device processes the tampering detection, it doesn't add any processing load to AXIS Camera Station server. See *Create active tampering alarm triggers on page 76*.

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. You must install the application on the device before you use AXIS Cross Line Detection as a trigger. Since the camera processes the detection, it doesn't add any processing load to AXIS Camera Station server. See *Create AXIS Cross Line Detection triggers on page 77*.

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 77*.

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. You must add the I/O port before you use an I/O trigger. See *Create input/output triggers on page 78*.

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. Available events depend on the device. Many of these events can require additional configuration to the device. See *Create device event triggers on page 78*.

Action button – Action buttons displays on top of the live view or in a map. Use the buttons to start and stop actions from live view. You can use one button in different rules, but each rule can only have one action button trigger. See *Create action button triggers on page 82*.

AXIS Entry Manager event – This trigger activates when AXIS Camera Station 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 through HTTPS communication. You can use this trigger to integrate AXIS Camera Station with external applications. See *Create external HTTPS triggers on page 83*.

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 server.

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 an 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 is activated when the camera is repositioned or when the lens is covered, sprayed or severely defocused. Tampering detection is performed by the camera which means that no processing load is added to AXIS Camera Station 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**, and click **New**.
2. Click **Add** and select **Activate tampering alarm**. Click **OK**.

3. In the pop-up page:
   - In the **Trigger on** field, select the camera to use.
   - Click the **Tampering settings** link to open the camera tampering page in a web browser to configure tampering settings.
4. Click **OK**.

Create AXIS Cross Line Detection triggers

AXIS Cross Line Detection is an application that can be installed on cameras and video encoders with support for AXIS Camera Application Platform. The application detects moving objects that cross a virtual line and can, for example, be used to monitor entrance and exit points. The trigger is activated when an application detects a moving object that crosses a virtual line. Since detection is performed by the application on the camera, no processing load is added to AXIS Camera Station server.

To use AXIS Cross Line Detection as a trigger, you need to download the application from *www.axis.com* and install it on the cameras and video encoders. See *Install camera application*.

To create an AXIS Cross Line Detection trigger:

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and select **AXIS Cross Line Detection**. Click **OK**.
3. Click **Refresh** to update the list if AXIS Cross Line Detection has been installed on a new camera.
4. Select the camera to use from the **Trigger on** drop-down list. Only cameras with AXIS Cross Line Detection installed can be selected.
5. In **Trigger period**, set an interval time between two successive triggers. This setting is used to reduce the number of successive recordings. The recording will continue if an additional trigger occurs within this interval. If an additional trigger occurs, the trigger period starts over from that point in time.
6. Click the **AXIS Cross Line Detection settings** link 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 prompted, 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.

To create a system event and error trigger:

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and select **System event and error**. Click **OK**.
3. Select **On recording error** to activate the trigger when errors occur during recording, for example if a camera stops streaming.
4. Select **On full storage** to activate the trigger when a storage for recordings is full.
5. Select **On no contact with network storage** to activate the trigger when there is a problem accessing a network storage.
6. Select **On lost connection to camera** to activate the trigger when there is a problem contacting one or more cameras.
   - Select **All** to include all the cameras added to AXIS Camera Station.

- Choose **Selected** and click **Cameras**. A list of all cameras added to AXIS Camera Station is displayed. You can use the **Type to search** field to find a specific camera, **Select all** to select all cameras or **Deselect all** to deselect all cameras.

7. Click **OK**.

Create input/output triggers

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

Note

Before using an I/O trigger, the I/O port must be added to AXIS Camera Station. See *I/O ports*.

To create an input/output trigger:

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and select **Input/Output**. Click **OK**.
3. In the Trigger port and state section:
   - In the **I/O port** field, select the input or output port.
   - In the **Trigger state** field, select the I/O port state that will activate the trigger. Available states depend on how the port is configured.
   - In the **Trigger period** field, set an interval time between two successive triggers to reduce the number of successive recordings. If an additional trigger occurs within this interval, the recording will continue and the trigger period starts over from that point in time.
4. Click **OK**.

Create device event triggers

The device event trigger provides access to all events in the camera or auxiliary device. It can be used if no suitable trigger is available in AXIS Camera Station.

Most events have one or more filters that should be set. Filters are conditions that must be fulfilled for the device event trigger to be activated. For information about events and filters for Axis products, see the VAPIX® documentation available on *www.axis.com/partners* and *www.axis.com/vapix*

To create a device event trigger:

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and select **Device event**. Click **OK**.
3. In the Configure device event trigger section:
   - In the **Device** field, select the camera or auxiliary device.
   - In the **Event** field, select the event to use as trigger.

   Note

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

   - In the **Trigger period** field, set an interval time between two successive triggers to reduce the number of successive recordings. If an additional trigger occurs within this interval, the recording will continue and the trigger period starts over from that point in time.

4. In the Filters section, select the filters. Available filters depend on the selected event.

5. In the Activity section, review the current state of the device event trigger as a function of time. An event can be stateful or stateless. The activity of a stateful event is represented by a step function. The activity of a stateless event is represented by a straight line which is interrupted by pulses when the event is triggered.

6. Click **OK**.

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	Digital input port
	Manual trigger
	Virtual 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.
	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 A1601 Network Door Controller device events

Category	Device event	Trigger the action rule
Authorization	Access request granted	When access to a door has been granted to the cardholder who is identified by a specific PIN code, card number or access rule.
	Access request denied	When access to a door has been denied to the cardholder who is identified by a specific PIN code, card number or card UID.
Casing	Casing open	When the casing of the network door controller is removed or opened. Use, for example, to send a notification to the administrator if the casing has been opened for maintenance purposes or when someone has tampered with the casing.
Device status	System ready	When the system is in state ready. For example, the Axis product can detect the system state and send 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 will only trigger when all necessary services, such as event system, has started.
Door	Door forced	When the door is forced open.
	Door installation tampering detected	When the following is detected: • Device casing is opened or closed • Device motion • Connected reader is removed from wall • Tampering with connected door monitor, reader, or REX device. To use this trigger, make sure to turn on Supervised input and the end of line resistors are installed on the relevant door connector input ports.
	Door locked	When the door lock is locked.
	Door open too long	When the door is open too long.
	Door position	When the door monitor indicates that the door is open or closed.

	Door unlocked	When the door lock stays unlocked. For example, you can use this state when there are visitors who should be allowed to open the door without presenting their credentials.
Input ports	Virtual input	When one of the virtual inputs changes states. It can be used by a client such as a management software to initiate various actions. Select the input port that should trigger the action rule when it becomes active.
	Digital input port	When a digital input port changes state. You can 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 any of the input port becomes active.
	Manual trigger	When the manual trigger is activated. You can use this trigger to manually start or stop the action rule through the VAPIX API.
	External input	When the emergency input is active or inactive.
Network	Network lost	When the network connection is lost. Only applicable for events used by the device, not applicable for events used by AXIS Camera Station.
	AddressAdded	When a new IP address is added.
	AddressRemoved	When the IP address is removed.
Schedule	Scheduled event	When a predefined schedule changes state. It can be used to record video in specific time periods, for example during office hours, at weekends etc. Select a schedule in the Schedule drop-down list.
System message	Action failed	When an action rule fails and the action failed system message is triggered.
Trigger	DigitalInput	When a physical digital input port is active or inactive.

Create action button triggers

Action buttons are used to start and stop actions in Live view. Action buttons are displayed on the bottom of the live view or in a map. When clicking the button, the action will be performed. The same button can be used for multiple cameras and maps. There can be multiple action buttons used for a camera or a map. You can arrange the multiple buttons for a camera when you add or edit the action button. To arrange the multiple action buttons for a map, go to **Live View** and edit the map.

There are two types of action buttons:

- **Command buttons:** A command button is used to manually start an action. Use command buttons for actions that do not require a stop button.
  A command button has a button label and a tooltip. The button label is the text displayed on the button. The tooltip is displayed when hovering the mouse pointer over the button.
  For example: Activate an output for a predefined time (use output action with pulse set to the number of seconds the output should be active), raise an alarm, and send email.

- **Toggle buttons:** A toggle button is used to manually start and stop an action. The button has two states: toggle and untoggle. Clicking the button switches between the two states. By default, toggle buttons start the action when in the toggle state. To start the action in the untoggle state, select **Trigger on untoggle** when creating the button.
  A toggle button has a toggle label, an untoggle label and a tooltip. The toggle and untoggle labels are the texts displayed on the buttons in the toggle and untoggle states. The tooltip is displayed when hovering the mouse pointer over the button.
  For example: Open and Close Door (use output action with pulse set to "as long as any trigger is active").

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 is activated.

To create an action button trigger:

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

    4.1 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**.

    4.2 Click **Next**.

    4.3 Provide labels and tooltip for the button.

5. If you have selected **Use existing button**:

    5.1 Search and navigate to the button or directly click the button that you want to use.

    5.2 If you have selected to use an existing toggle button, you need to select **Trigger on toggle** or **Trigger on untoggle**.

    5.3 Click **Next**.

    5.4 Edit the labels and tooltip of the button.

6. Select the camera or map from the drop-down list. To add the button to multiple cameras or maps, click **Add to multiple cameras** or **Add to multiple maps**.
7. If a camera has multiple action buttons, click **Arrange** to change the order of the buttons. Click **OK**.
8. Click **Next**.

Create AXIS Entry Manager event triggers

The AXIS Entry Manager event trigger is activated when signals are received from doors configured in AXIS Entry Manager, for example if doors are forced open, doors are open too long or access is denied.

Note

> The AXIS Entry Manager event trigger is only available when AXIS A1001 Network Door Controller is added to AXIS Camera Station.

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

    Possible events are: Door accessed, Door forced open, Door open too long, and Access denied.

4. Click **OK**.

Create external HTTPS triggers

This trigger only supports HTTPS communication, and requires that you provide the valid AXIS Camera Station 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**, and click **New**.
2. Click **Add** and select **External HTTPS**. Click **OK**.
3. Enter the trigger name in the **Trigger name** field.
4. 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.
5. 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. When the rule is activated, all actions are performed.

The following actions are available:

- **Record:** This action starts a recording from the camera. The recording can be accessed and played from the Recordings tab. The recording is saved to the location specified in Recording storage via **Configuration > Storage > Selection**. See *Create record actions*.
- **Raise alarm:** This action sends an alarm to all connected AXIS Camera Station clients. The alarm appears in the Alarms tab and as a taskbar notification. Instructions in form of a file with alarm procedures can be included with the alarm. See *Create raise alarm actions*.
- **Set output:** This action sets the state of an output port to control the device connected to the output port, for example to turn on a light or lock a door. Before using the output action, an output port must be added to AXIS Camera Station via **Configuration > Recording and events > I/O ports**. See *Create output actions*.
- **Send email:** This action sends an email to one or multiple recipients. Snapshots from cameras can be sent as email attachments. To send emails, an SMTP server must first be configured. See *Create send email actions*.

- **Live view:** This action opens the live view of a specific camera, view or preset position in all connected AXIS Camera Station clients. If the live view shows a split view with a hotspot, the camera in the live view action is loaded in the hotspot. The live view action can also be used to restore open AXIS Camera Station clients from the taskbar or bring the clients to the front of other open applications. See *Create live view actions*.
- **Send HTTP notification:** This action sends an HTTP request to a camera, a door controller or an external web server. For example, HTTP notifications can be used to enable or disable a feature in the camera, or to open, close, lock or unlock a door connected to a door controller. See *Create HTTP notification actions*.
- **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 89*.
- **Send mobile app notification:** The action sends a custom message to the AXIS Camera Station mobile app. You can click the notification received on the mobile app and go to a specific camera view. See *Create send mobile app notification actions on page 89*.
- **Turn rules on or off:** Use this action to turn other action rules on or off. See .
- **Access control:** This action includes door actions and zone actions in AXIS Camera Station Secure Entry. See *Create access control actions on page 90*.

Create record actions

The record action starts a recording from the camera. The recording can be accessed and played from the **Recordings** tab. The recording is saved to the location specified via **Configuration > Storage > Selection**.

To create a record action:

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **Record**. Click **OK**.
4. In the **Camera** field, select the camera to record from.
5. In the Video setting section:
   - Select a profile from the **Profile** drop-down list. To create a new profile, go to **Configuration > Stream profiles**. A profile contains settings such as video format, resolution, compression, frame rate and if audio should be included.
   - Select the number of seconds to record before the action is triggered in the **Prebuffer** field.
   - Select the number of seconds to include in the recording when the action is no longer triggered in the **Prebuffer** field.
6. Click **OK**.

Create raise alarm actions

The raise alarm action sends an alarm to all connected AXIS Camera Station clients. The alarm will be displayed in the Alarms tab and as a taskbar notification. Instructions in form of a file with alarm procedures can be included with the alarm.

To create a raise alarm action:

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **Raise alarm**. Click **OK**.
4. Under **Alarm message**:

- Enter a title for the alarm. The title will be displayed in the Alarm field in the Alarms tab and in the taskbar notification.
- Enter a description of the alarm. The description will be displayed in the Description field in the Alarms tab and in the taskbar notification.
- Set the duration time between 1 and 600 seconds for the pop-up alarms.

5. Set alarm procedure under **Alarm procedure**. An alarm procedure is a file with instructions, for example for an operator. The alarm procedure is available from the **Alarms** and **Logs** tabs.

   5.1 Select **On alarm show alarm procedure**.

   5.2 Click **Upload** and browse to the desired file.

   5.3 Click **Preview** to open the uploaded file in a preview window.

   5.4 Click **OK**.

Create output actions

The output action sets the state of an output port. This is used to control the device connected to the output port, for example to switch on a light or lock a door.

Note

Before using an output action, the output port must be added to AXIS Camera Station. See *I/O ports*.

To create an output action:

1. Go to **Configuration** > **Recording and events** > **Action rules**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **Set output**. Click **OK**.
4. In the **Output port** field, select the output port.
5. In the **State on action** field, select the state to set the port to. Available options depend on how the port was configured.
6. Select **Pulse** to define how long the output port should remain in the new state.
   - 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**.
   - To keep the port in the new state for a fixed time, select the other option and specify the number of seconds.

Note

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

7. Click **OK**.

Create send email actions

The email action sends an email to one or multiple recipients. Snapshots from cameras can be sent as email attachments.

Note

To send emails, an SMTP server must first be configured. See *Server settings*.

To create a send email action:

1. Go to **Configuration** > **Recording and events** > **Action rules**, and click **New**.

2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **Send email**. Click **OK**.
4. In the Recipients section:
   - 4.1 Enter the email address in the **New Recipient** field and select **To**, **Cc** or **Bcc**.
   - 4.2 Click **Add** to add the email address to the **Recipients** field.
5. In the Contents section, enter the email subject and message.
6. In the Advanced section:
   - To attach snapshots in the form of jpg images 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 is displayed. You can use the **Type to search** field to find a specific camera, **Select all** to select all cameras or **Deselect all** to deselect all cameras.
   - To prevent sending multiple emails for the same event, select **Send one email for each event**.
   - 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 list.
7. Click **OK**.

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 will open in all connected AXIS Camera Station clients. If the Live view tab shows a split view with a hotspot, the camera selected in the live view action will be loaded in the hotspot. For more information about hotspots, see *Split view*.

The live view action can also be used to restore open AXIS Camera Station 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**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **Live view**. Click **OK**.
4. Under **Live view actions**, select the view to open in the Live view tab:
   - To open a view, select **View** and select the view from the drop-down list.
   - To open a camera view, select **Camera** and select the camera from the drop-down list. If a camera has PTZ preset, select Go to preset and select one area from the drop-down list to open a preset position.
   - Select **No action** and do not open any view.
5. Under **Shown in**:
   - Select **Live alert tab** to open the selected view or camera view in the live alert tab.
   - Select **Hotspot in view** and select a view with hotspot from the drop-down list. If the hotspot is visible in live view when the action is triggered, it will show the camera view in the hotspot.
6. In the Bring to front section, select **On trigger bring application to front** to restore open AXIS Camera Station clients from the taskbar or bring the clients to the front of other open applications when the live view action starts.
7. Click **OK**.

Example

To open a live view tab, navigate 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 to navigate to the view with hotspot in the live alert tab.
   1.1 Under **Live view actions**, select **View** and select the view with hotspot.
   1.2 Under **Show in**, select **Live alert tab**.
   1.3 Select **On trigger bring application to front**.
2. Create another live view action to navigate 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** and select the view with hotspot.

Create HTTP notification actions

The HTTP notification action sends an HTTP request to a recipient. The recipient can be a camera, a door controller, an external web server or any server that can receive HTTP requests. HTTP notifications can for example be used to enable or disable 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, the AXIS Camera Station server proxy settings might need to be adjusted. See *General*.

To create an HTTP notification action:

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **Send HTTP Notification**. Click **OK**.
4. In the **URL** field, enter the address to the recipient and the script that will handle the request. For example: http://192.168.254.10/cgi-bin/notify.cgi
5. Select **Authentication required** if the recipient requires authentication. Enter the username and password.
6. Click **Advanced** to display the advanced settings.
   - Select HTTP method GET, POST, or PUT from the **Method** drop-down list.
   - For POST and PUT methods, select the content type from the **Content type** drop-down list.
   - For POST and PUT methods, enter the request body in the **Body** field.
7. Click **OK**.

Create siren and light actions

The siren and light action triggers 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**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.

3. Click **Add** and select **Siren and light**. Click **OK**.
4. Select a device from the **Device** drop-down list.
5. Select a profile from the **Profile** drop-down list.
6. 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 added to AXIS Camera Station.

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **AXIS Entry Manager**. Click **OK**.
4. Select an action and door to perform the action.

   Possible actions are: Grant access, Unlock door, and Lock door.
5. 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 notification received on the mobile app and 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**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **Send mobile app notification**. Click **OK**.
4. In the **Message** field, enter your message that will be displayed on the mobile app.
5. Under **Click notification and go to**,
   - Select a camera view from the **Camera** drop-down list to go to the specific camera view when the notification is clicked on the mobile app.
   - Select **Default** to go to the mobile app start page when the notification is clicked on the mobile app.
6. Click **OK**.

Create an action that turns other action rules on or off

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

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **Turn rules on or off**. Click **OK**.

4. Select one or multiple action rules.
5. Choose if you want to turn the selected action rules on or off.
6. Enter a delay if you want some time between the trigger and the change of state.
7. 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 as soon as the employee removes the access card from the reader.
8. 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.

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and create a trigger. Click **Next**. See *Add triggers*.
3. Click **Add** and select **Access control**. Click **OK**.
4. To perform door actions:
   4.1 Under **Access control**, select **Door actions**.
   4.2 Under **Configure action**, select the doors and action.
5. To perform zone actions:
   5.1 Under **Access control**, select **Zone actions**.
   5.2 Under **Configure action**, select the zones, door types and action.
6. Click **OK**.

Schedules

Schedules can be used in Action rules. Once a schedule is created, it can be used as many times as needed.

Schedules can be overridden on specified days, for example during public holidays.

Note

When connecting to multiple AXIS Camera Station servers, you can add and manage schedules on any connected server by selecting the server from the **Selected server** drop-down list.

Go to **Configuration > Recording and events > Schedules**, a list of all schedules that have been created is displayed. The Used column indicates if the schedule is used.

Click a schedule, the details of the schedule is displayed.

To remove a schedule, select the schedule and click **Remove**. Schedules that are used can't be removed.

To add a schedule:

1. Go to **Configuration > Recording and events > Schedules** and click **New**.

2. Enter a name for the schedule.

3. In the timeline, select the time slots that the schedule should be on.

   - Click an empty time slot to set the schedule on.
   - Click a time slot with schedule on to set schedule off.
   - Click an empty time slot and drag to set the schedule on for selected time slots.
   - Click a time slot with schedule on and drag to set the schedule off for selected time slots.
   - Press CTRL to select five minute intervals.

4. To use the same schedule on another day, right-click a day and select **Copy schedule** and right-click another day and select **Paste schedule**.

5. To add exceptions to the schedule:

   5.1 Click **Add...** under **Schedule exceptions**.

   5.2 Select a start and end date for the exception.

   5.3 Mark the time interval in the timeline.

   5.4 Click OK.

   Note

   To remove an exception, click **Remove...**, select a time interval that includes the exception, and click OK.

6. Click **Apply**.

Examples of action rules

Example

This example shows how to set up an action rule in AXIS Camera Station to trigger a recording and an alarm when the entrance door is forced open.

Before you start, you need to:

- Install AXIS A1601 Network Door Controller. See *Add devices on page 39*.
- Configure the door controller. See *Configure access control on page 119*.

1. Go to **Configuration > Recording and events > Action rules** and click **New**.

2. Add the Door forced event trigger.

   2.1 Click **Add** and select **Device event**. Click **OK**.

   2.2 Under **Configure device event trigger**:

   - Select the AXIS A1601 Network Door Controller from the **Device** drop-down list.
   - Select **Door > Door forced** from the **Event** drop-down list.
   - Set 10 seconds as **Trigger period**.

   2.4 Under **Filters**:

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

2.3 Under **Activity**, check that the trigger is showing activity on the signal line.

2.4 Click **OK**.

3. Click **Next**.

4. Add a record action.

4.1 Click **Add** and select **Record**. Click **OK**.

4.2 Select a camera from the **Camera** drop-down list.

4.3 Under **Video setting**:

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

4.4 Click **OK**.

5. Add a raise alarm action.

5.1 Click **Add** and select **Raise alarm**. Click **OK**.

5.2 Under **Alarm message**, enter a title and description for the alarm. For example, The main entrance is forced open.

5.3 Click **OK**.

6. Click **Next** and select **Always** as the schedule.

7. Click **Finish**.

Example

This example shows how to set up an action rule in AXIS Camera Station to play a welcome message and call the elevator when an important person enters.

Before you start, you need to:

- Install and configure AXIS A1601 Network Door Controller and add cardholders. See *Configure access control on page 119* and *Access management on page 141*.
- Install an Axis network audio device and associate the audio device with a camera. See *Stream profiles on page 45*.
- 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. See *I/O ports on page 73*.

1. Go to **Configuration > Recording and events > Action rules** and click **New**.

2. Add the device event trigger.

2.1 Click **Add** and select **Device event**. Click **OK**.

2.2 Under **Configure device event trigger**:

- Select the AXIS A1601 Network Door Controller from the **Device** drop-down list.
- Select **Authorization > Access request granted** from the **Event** drop-down list.
- Set 10 seconds as **Trigger period**.

2.4 Under **Filters**:

- Select the door from the **Door name** drop-down list.

- Select the door side from the **Door side** drop-down list.
- Select **Card number** and type the card number of the important person.

2.4 Under **Activity**, check that the trigger is showing activity on the signal line.

2.5 Click **OK**.

3. Click **Next**.

4. Add a Send HTTP notification action to trigger a welcome message.

4.1 Click **Add** and select **Send HTTP notification**. Click **OK**.

4.2 In the **URL** field, enter the URL of the welcome message audio clip.

4.3 Select **Authentication required** and enter the username and password of the audio device.

4.4 Click **OK**.

5. Add a Set output action.

5.1 Click **Add** and select **Set output**. Click **OK**.

5.2 From the **Output port** drop-down list, select the output port of the I/O module which is connected to the elevator.

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

5.4 Select **Pulse** and set 60 seconds to keep the port in the state.

5.5 Click **OK**.

6. Click Next and select **Always** as the schedule.

7. Click **Finish**.

Configure client

Go to **Configuration** > **Client** to:

- Edit client specific settings, like theme and language. See *Client settings on page 93*.
- Edit user specific settings, like notifications and startup options. See *User settings on page 94*.
- Edit client specific streaming performance settings like video scaling and hardware decoding. See *Streaming on page 95*.

Client settings

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

Theme

Select the theme for the client. The changes are effective after you restart the application. Available themes are System, Light, Classic, and Dark. System is the default theme for new installations.

If you select System, the theme will be either Dark or Light depending on the Windows setting under **Settings** > **Personalization** > **Colors** > **Choose your default app mode**.

General

Turn on **Run application when Windows starts** if you would like to run Axis Camera Station automatically every time when Windows starts.

Live view

- Show camera names in live views
- To indicate any type of recording, turn on **Show recording indicators in live views and maps**. The recording indicator ● appears 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**. The motion detection indicator 🚶 appears in live views and maps.

Language

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

Feedback

Select to share anonymous client usage data with Axis Communications to help improve the application and user experience. To change the option for the server, go to **Configuration > Server > Settings**.

User settings

These settings apply to the current AXIS Camera Station user on the computer. Go to **Configuration > Client > User settings** to configure the AXIS Camera Station client user settings.

Navigation system

Tree view navigation system is turned on by default to enable tree view navigation pane with the views and cameras.

Select to show views or cameras or both in the **Show in navigation** drop-down list.

Turn on **Show navigation path when navigating in view** to display the navigation path on top of the view when navigating in a split view.

Notifications

- Turn on **Show taskbar notification on alarms** to display a notification in Windows taskbar when an alarm occurs.
- Turn on **Show taskbar notification for tasks** to display a notification in Windows taskbar when a task is added or finished.
- Turn on **Show notifications in Device management** to display notifications when new firmware is available for download.
- Turn on **Show intercom notification window** to display a notification window when the call button is pushed on the intercom system that has been installed in AXIS Camera Station.

Snapshot

- Turn on **When a snapshot is taken show a message** to show a message when a snapshot is taken.
- Turn on **When a snapshot is taken open the snapshot folder** to open the snapshot folder when a snapshot is taken. Click **Browse** to specify the folder to save snapshots.

Startup

- Turn on **Start in full screen** to start AXIS Camera Station in full screen mode.
- Turn on **Remember last used tabs** to start AXIS Camera Station with the tabs, views and camera views that were open when AXIS Camera Station was closed last time.
- Turn on **Remember last used monitors** to start AXIS Camera Station on the monitor when AXIS Camera Station was closed last time.

Note

- The views and camera views are saved per tab. They are remembered only when the client reconnects to the same server.
- Monitors, views and camera views are remembered only when tabs are remembered.
- Dynamic views that you drag and drop in the live view will never be remembered.
- When connecting to multiple servers, **Remember last used tabs** is not supported if different users are used for different servers.
- When connecting to multiple servers with the same user:
  - The last used tabs of the user who logs on to the first server will be remembered.
  - When a new server is connected, the last used tabs of the user who logs on to the new server will be remembered.

Sound on alarm

- Select **No sound** if you do not want any sound with an alarm.
- Select **Beep** if you want typical beep sound with an alarm. Click **Play** to test the sound.
- Select **Sound file** and click **Browse** to navigate to your sound file if you want a customized sound with an alarm. You can use a sound file with any format that is supported by Windows Media Player. Click **Play** to test the sound.

Sound on incoming call

- Select **No sound** if you do not want any sound with an incoming call.
- Select **Beep** if you want typical beep sound with an incoming call. Click **Play** to test the sound.
- Select **Sound file** and click **Browse** to navigate to your sound file if you want a customized sound with an incoming call. You can use a sound file with any format that is supported by Windows Media Player. Click **Play** to test the sound.

Features

By default smart search 1 is shown. Turn off **Show smart search 1** to hide this feature.

Streaming

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

Video scaling

- Select **Scale to best fit** to show video in the whole available space, without losing the aspect ratio or cropping the image.
- Select **Fill video area (may crop parts of the video)** to resize video to fit the available space. Aspect ratio will be preserved. If the available space has a different aspect ratio than the video, the video will be cropped.

Hardware decoding

Select the mode and graphic card from the drop-down list of the **Mode** and **Graphics card** fields. 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 streaming high-resolution video. Hardware decoding supports M-JPEG and H.264.

Mode

- **Automatic:** Streams with a resolution above 3840x2160p@25fps (also known as 4K or UHD) are decoded with hardware if the graphics card supports it.
- **On:** Streams with a resolution above 1920x1080p@25fps (also known as 1080p or HD) are decoded with hardware if the graphics card supports it.
- **Off:** Hardware decoding is turned off and AXIS Camera Station uses the CPU to decode video.

Graphics card: Lists your available graphics cards. If your system has multiple graphics card, AXIS Camera Station lists all the available graphics cards.

Note

- For cameras with a resolution below 1080p, hardware decoding is not used for these cameras, even if hardware decoding is turned On.
- For cameras with 4K streaming, if your graphics card does not support 4K decoding, hardware decoding is only used on 1080p streams and not for 4K streams, even if hardware decoding is turned On.

Bandwidth usage

The resolution and frame rate used in Live view can be limited to reduce bandwidth consumption, for example if a slow connection is used between the AXIS Camera Station client and the AXIS Camera Station server.

- Turn on **Always use the stream profile Low on this client**, and AXIS Camera Station will always use the Low stream profile for Live view. See *Stream profiles*.

Note

This setting affects H.264 and M-JPEG video.

- Turn on **Suspend video streams for inactive tabs**, and video streams in the inactive tabs are suspended.
- Turn on **Suspend video streams in intercom notification window**, and video streams in the intercom notification window are suspended.

PTZ (Pan, Tilt, Zoom)

Turn on **Select view with first click instead of starting PTZ** to enable view selection with the first click that you make in the view. All the following clicks in the view control PTZ.

Audio

- **Push-to-talk release delay (ms):** use the slider to adjust how many milliseconds you want to keep audio transmitted from the microphone after you release the **Push-to-talk** button.
- Turn on **Use push-to-talk for all duplex modes** to use push-to-talk for simplex, half-duplex, and full-duplex modes.
- Turn on **Always allow audio for intercoms** to be able to listen and speak to intercoms even if there are no ongoing calls from intercoms.

Instant replay

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 connecting to multiple AXIS Camera Station servers, you can configure firmware upgrade settings on any connected server by selecting the server from the **Selected server** drop-down list.

1. Go to **Configuration > Connected services > Firmware upgrade settings**.
2. In the Automatic check for updates section:
   - Select **Every start-up** from the **Check for updates** drop-down list to check for available firmware versions on the server on each startup. By default, AXIS Camera Station is set to never check for any firmware updates.
   - Click **Check now** to check for available firmware versions on the server.

- Select **Check axis.com for new available firmware** to automatically check for firmware updates published at www.axis.com. By default, this option is pre-selected. To manually update firmware, see *Upgrade firmware on page 57*.

In the Upgrade order section:

- Select **Parallel** to upgrade all devices at the same time. This option is quicker than **Sequential** but all devices will be offline at the same time.
- Select **Sequential** to upgrade devices one after the other. This option will take longer but the devices will not be offline at the same time. Select **Cancel remaining upgrades if one device fails** to abort a sequential upgrade when a problem occurs.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=firmware-upgrade-settings

Enable automatic firmware check

Axis Secure Remote Access

Axis Secure Remote Access allows you to connect to your AXIS Camera Station server through a secure and encrypted internet connection using a smart phone, tablet or computer. Axis Secure Remote Access does not 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 connecting to multiple AXIS Camera Station servers, you can configure Axis Secure Remote Access on any connected server by selecting the server from the **Selected server** drop-down list.

Enable Axis Secure Remote Access

Axis Secure Remote Access is available if you are signed in to your MyAxis account. Axis Secure Remote Access must be enabled manually.

1. Go to **Configuration > Connected services > Axis Secure Remote Access**.
2. In the MyAxis account section, enter your MyAxis account email address and password, and click **Apply**. We recommend using a strong password for your MyAxis account.
3. In the Axis Secure Remote Access section, click **Enable** to enable remote access.

When Axis Secure Remote Access is enabled you can log in to your server remotely. See *Log in to AXIS Camera Station server.*

Axis Secure Remote Access on mobile devices

For mobile devices (iOS and Android), download the *Axis Mobile viewing app.* In the Axis mobile viewing app, remote access needs to be activated first by signing in with the same MyAxis account as the one used to enable Axis Secure Remote Access on the remote server. When signed in, the total amount of relayed data used by the MyAxis account during the month will be shown.

Axis Secure Remote Access usage

The Axis Secure Remote Access usage is displayed on the status bar at the bottom of the AXIS Camera Station client. Click the link to get an overview of how the secure remote connection is used.

- **Service level:** Shows the service level of your Axis Secure Remote Access subscription.
- **Data used this month:** Shows how much data you have used this month. The counter will be reset on the first every month by midnight.
- **Overage:** Shows how much additional data you have used this month that surpasses the included amount in your service level. This is only available if you have Overage enabled in your subscription.
- **Connections:** Shows the servers you are connected to using 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. Since it's a cloud-based service it also provides added reliability, less maintenance, and the ability to monitor systems in different organizations. See *Organizations on page 98* for more information.

We recommend creating a *My Axis account* before you start setting up AXIS System Health Monitoring Cloud Service.

1. Go to **Connected services** > **AXIS System Health Monitoring Cloud Service**.
2. Click **Connect**.
3. Sign in using your My Axis account.
4. Select the organization that you want to connect the system to. See *Organizations on page 98* for more information.
5. Click **Next**.
6. Optionally, create **Folders** in the organization. Creating this structure can be useful for example if you have systems in your organization that are located on different sites.
7. Select the **Folder** that you want to connect the system to. You can also choose to connect the system directly to the organization.
8. Click **Next**.
9. Click **Save and exit**.
10. Wait until the connection is done.

Organizations

The organization is at the center of your cloud services.

- It connects your AXIS Camera Station system to the users of the different cloud services.
- In particular it enables the cloud based system health monitoring. See *Setup AXIS System Health Monitoring Cloud Service on page 98* for more information.
- It defines the different user roles, for example, service administrator, or operator.

An organization can be structured into folders that, for example, represent systems located on different sites. To create an organization, you need a *My Axis account*.

Manage organizations

To edit an organization:

1. Go to **System Health Monitoring** > **Settings**.
2. Click **Open AXIS System Health Monitoring Cloud Service**.

3. Open 👤 user settings and select the organization you want to edit.

4. Open 👤 user settings and click ⚙ **Manage organizations.**

In this view you can add or delete folders and sub-folders in an existing organization, as well as creating new organizations.

Disconnect a system from an organization

You may want to, for example, move a system from one organization to another. To do that you first need to disconnect the system from its current organization.

1. Go to **Connected services** > **AXIS System Health Monitoring Cloud Service**.

2. Click **Disconnect**.

Invite a user to an organization

1. Go to **System Health Monitoring** > **Settings**.

2. Click **Open AXIS System Health Monitoring Cloud Service**.

3. Open 👤 user settings and select the organization you want to invite the user to.

4. Open 👤 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, also provide the name of the organization for the invite.

Join an organization

When someone wants you to join an organization you will receive an invitation code. To join the organization:

1. Go to **System Health Monitoring** > **Settings**.

2. Click **Open AXIS System Health Monitoring Cloud Service**.

3. Open 👤 user settings and select the organization you want to join.

4. Open 👤 user settings and click ⚙ **Manage organizations.**

5. Open the **Users** tab.

6. Paste the invitation code.

7. Click **Join**.

Configure server

Server settings

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

Note

When connecting to multiple AXIS Camera Station servers, you can configure the server settings on any connected server by selecting the server from the **Selected server** drop-down list.

Export

To include audio when adding recording to the export list, select **Include audio when adding recordings to export**.

Logs

Specify the number of days to keep alarms, events and audits. Any value between 1 and 1000 days can be used.

External data

Specify the number of days to keep the external data. Any value between 1 and 1000 days can be used.

SMTP servers

SMTP servers must be added for AXIS Camera Station to send emails on system alarms or when an event configuration rule is activated.

This section lists added SMTP servers. Use the arrows to change the order of the servers in the list. The servers are used in the same order they're listed.

To add an SMTP server:

1. Go to **Configuration > Server > Settings**.
2. In the **SMTP servers** section, click **Add**.
3. In the **Server** section:
    - Enter the address of the SMTP server and port to use. 587 is the default port for SMTP TLS connections.
    - Select **Use authentication** if a username and password are required for this server. Enter the username and password to access the server.
    - Select **Use TLS** if the SMTP server uses TLS. TLS is the default protocol as it provides secure communications.
4. In the **Sender** section, enter the name that you want to display in the sender email and email address.

To edit an SMTP server, select the server and click **Edit**.

To remove an SMTP server, select the server and click **Remove**. In the pop-up dialog, click **Yes** to remove the server.

To test an SMTP server, select the server and click **Test all**. In the pop-up dialog, enter an email address in the **Recipient** field and click **OK** to send a test email.

SMTP server tests for a list of results and possible actions to take.

OK – Connection with the SMTP server was successful. Make sure that the recipients have 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 can't access the SMTP server. Make sure the SMTP server is working correctly and that all routers and proxy servers between AXIS Camera Station and the SMTP server are configured to 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.

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 connection to a camera is lost, access to a recording storage is denied, an unexpected server shutdown is detected or if recording errors occur. email notifications can be sent on system alarms.

Note

To send emails, an SMTP server must first be added.

To send email on system alarms:

1. Select **Send email on system alarm to the following recipients** to activate system alarm email.
2. In the Recipients section:
    2.1 Select if the address should be in the **To**, **Cc** or **Bcc** field of the email and enter the email address.
    2.2 Click **Add** to add the email address to the **Recipients** box.

Device connection

For devices that are connected by using the hostname, when the hostnames are unreachable:

- To keep connecting by using the hostname, select **Keep using the hostnames even if they become unreachable**.
- To automatically switch to connect by using the IP address, clear the checkbox.

You can manually select to use the hostname or IP address to connect to devices. See *Connection on page 61*.

Language

Change the language of

- AXIS Camera Station Service Control. The change is effective after you restart the Service Control.
- Data sent from AXIS Camera Station Secure Entry. For example: system alarms, audit log messages, external data in the Data search tab.

Feedback

Select to share anonymous server usage data with Axis Communications to help improve the application and user experience. To change the option for the client, go to **Configuration > Client > Settings**.

Advanced settings

You should change the settings only when you are instructed by Axis support.

1. Go to **Configuration > Server > Settings**.
2. To change a setting, type the setting and its value. Click **Add**.

To enable debug logging for troubleshooting purpose, select **Enable server side debug logging**. Enabling this setting will take up more space on your disk. This setting will be overridden by the `log4net.config` file in the **ProgramData** directory.

Update AXIS Camera Station

To get the latest version of AXIS Camera Station:

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

Here, you can also schedule updates, which start automatically on the given date if there's a newer version.

Note

- Once you have started an update, whether manual or scheduled, there is no way to cancel it.
- Scheduled updates start automatically.
- Clients connecting via secure remote access are not updated.
- In a multi-server system, always update the local server last.
- This feature uses the Windows installer (msi) regardless of the type you're currently using.

Incident report

If you have incident report permission enabled, you can generate the incident reports including recordings, snapshots, and notes about the incidents. See *Export incident reports on page 30*.

To configure the settings for incident reports:

1. Go to **Configuration > Server > Incident report**.
2. Under **Location**, select where to store the incident reports.
   - To save the incident reports to a folder on the computer, select **Server directory path**. Enter the directory path or right-click to insert the variables in the path field. You can define the server name, category, or the user name as variables. For example: `C:\Reports\$(Server Name)\$(Category)\$(User Name)\`
   - To save the incident reports to a folder on a network storage, select **Network directory path** and enter the directory path. You can select to use credentials for the network storage. The share must be reachable from the AXIS Camera Station server. See *Manage storage* for how to add storage to use for recordings.
3. From the **Export format** drop-down list, select a format you want to export your recordings to.
   - If you select ASF, you can select **Add digital signature** to use a digital signature to ensure image authenticity and integrity by making image tampering impossible. The digital signature can be verified in AXIS File Player. See the Digital signature section in *Export recordings*. You can also select **Use password** to use a password for the digital signature.
   - If you select MP4, audio in G.711 or G.726 format will not be included in the exported recordings.
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. Click **Add**.

   4.2 To remove a category, select it and click **Remove**.
5. Under **Description template**, define information to show in the Description field when generating your incident reports and click **Apply**. For example: Reported by: <Insert your name, mail, and phone number>

Scheduled export

Go to **Configuration > Server > Scheduled export** to export recordings from cameras on certain weekdays.

At the selected time, all recordings since the previous export will be exported. If the previous export is more than one week old (for example if scheduled export has been disabled for a while) or if there is no previous export, only recordings that are less than one week old will be exported. To export older recordings, go to the Recordings tab and export them manually. See *Export recordings*.

Note

When connecting to multiple AXIS Camera Station servers, you can enable and manage scheduled export on any connected server by selecting the server from the **Selected server** drop-down list.

Export scheduled recordings

1. Go to **Configuration > Server > Scheduled export**.

2. Under **Scheduled export**, select **Enable scheduled export** to enable scheduled export.
3. Under **Cameras**, select the cameras to export recordings from. By default, all listed cameras are selected. Clear **Use all cameras** and use the **Type to search** field to find and select the specific cameras in the list.
4. Under **Export**,
   - To save recordings to a folder on the computer, select **Server directory path** and enter the directory path.
   - To save recordings to a folder on a network storage, select **Network directory path** and enter the directory path. You can select to use credentials for the network storage. The share must be reachable from the AXIS Camera Station server. See *Manage storage* for how to add storage to use for recordings.
   - To create a playlist in the .asx format used by Windows Media Player, select **Create playlist**. The recordings will play in the order in which they were recorded.
   - From the **Export format** drop-down list, select a format you want to export your recordings to.

     If you select ASF, you can select **Add digital signature** to use a digital signature to ensure image authenticity and integrity by making image tampering impossible. The digital signature can be verified in AXIS File Player. See the Digital signature section in *Export recordings*. You can also select **Use password** to use a password for the digital signature.

     If you select MP4, audio in G.711 or G.726 format will not be included in the exported recordings.
5. Under **Weekly schedule**, select the time and the days on which recordings should be exported.
6. Click **Apply**.

Using Microsoft Windows 2008 Server

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

1. Click **Start** > **Administrative Tools** > **Server Manager** to open Server Manager.
2. In the Features Summary section, click **Add features**.
3. Select **Desktop Experience**, click **Next** and then click **Install**.

Using Microsoft Windows 2012 Server

To be able to export recordings from a server running on Microsoft Windows 2012 Server, Desktop Experience must be installed:

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. In the Features Summary section, select **User Interfaces and Infrastructure**.
4. Select **Desktop Experience**, click **Next** and then click **Install**.

New connection

Go to ☰ > **Servers** > **New connection** to connect to a new AXIS Camera Station server. See *Log in to AXIS Camera Station server.*

Connection status

Go to ☰ > **Servers** > **Connection status**, a list of the connection status for all servers is displayed.

Use the **Type to search** field to find a specific server.

Select the checkbox in front of the server name to connect to the server, or clear the checkbox to disconnect from the server.

Configuration

Status codes	Description	Possible solutions
Connecting	The client is trying to connect to this server.	
Connected	The client is connected to this server using TCP.	
Connected (using Secure Remote Access)	The client is connected to this server using Secure Remote Access.	
Connected (using HTTP)	The client is connected to this server using HTTP. This is less efficient than TCP and noticeable slower when connecting to multiple servers.	
Disconnecting	The client is disconnecting from this server.	
Disconnected	The client is not connected to this server.	
Reconnecting	The client has lost connection to this server and is trying to reconnect.	
Reconnection failed	The client failed to reconnect to this server. The server can be found but the user permissions or password may have changed.	• Add the user in the user permission dialog. • Verify the username and password.
Login canceled	The login was canceled by the user.	
Incorrect username or password	Click the link in the Action column and enter the correct credentials.	
User not authorized on the server	The user used to log in is not authorized by the server.	Add the user in the user permission dialog.
Security verification failed	A WCF related security check failed. Make sure that the client and server computer UTC times are reasonably synchronized.	
No contact with server computer	The was no response by the server computer on the address used.	• Check that the network is working properly. • Check that the server is started.
No server running	The computer running the server is accessible, but the server is not running.	Start the server.
Communication failure	Something went wrong when connecting to the server. Make sure the server computer is accessible.	• Check that the network is working properly. • Check that the server is started.
Invalid hostname	The DNS was not able to 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 responded 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 the same version of AXIS Camera Station is installed on both the client and the server computer.
Server too busy	The server was not able to respond because of performance issues.	Make sure that the server computer and the network is not overloaded.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=connection-status

Multiple servers

Server lists

AXIS Camera Station servers can be organized in server lists. A server can belong to multiple server lists. Server lists can be imported and exported and used in other AXIS Camera Station clients.

Go to ☰ > **Servers** > **Server lists** to open the Server lists page.

The default Recent connections list is displayed and contains the servers used in the previous session. Recent connections can't be removed.

Use the **Type to search** field to find the specific servers in a server list.

- To add a new server list, click **+ New server list** and enter a name for the list.
- To rename a server list, double-click the list and enter a new name for the list.
- To delete a server list, select the server list and click **Delete**.
- Click **Export lists** to export all server lists in a .msl file. You can import the server list to log in to the servers. See *Log in to AXIS Camera Station server.*
- To add servers to a server list:
  - Select a server list from the left panel. Click **Add** and enter the required information.
  - Select a server list and drag the servers in the server list to the appropriate server list.
- To edit a server in a server list, select a server in a server list and click **Edit**. You can only edit one server at a time.
- To remove servers in a server list, select the servers in a server list and click **Remove**.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=server-lists

Organize servers in server lists

Configure switch

If you have one Axis S22 series device, this option is available for you to configure your S22 series device from AXIS Camera Station. Go to **Configuration > Switch > Management** and enter your username and password to open the Switch management page in the AXIS Camera Station client. For how to configure the switch, see S22 series User Manual on *axis.com*.

Note

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

Configure licenses

You can view the license keys and license status, and manage the licenses of the connected devices.

Note

- When connecting to multiple AXIS Camera Station servers, you can manage licenses on any connected server by selecting the server from the **Selected server** drop-down list.
- We recommend that you write down the license keys, or save them in a digital format on a USB flash drive for future reference. Lost license keys can't be retrieved.
- When you register your Axis network video recorder in the AXIS License Portal, you receive a 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. The upgrade licenses can be moved and used for any system.

Device status

Go to **Configuration > Licenses > Device status** to view a list of all connected devices and their respective license status. This allows you to quickly see if the trial period for any device has expired and when to renew them. Use the **Type to search** field to find a specific device if you have a great number of connected devices.

Keys

Go to **Configuration > Licenses > Keys** to view a list of the keys necessary for each license of all connected devices. Use the **Type to search** field to find a specific key.

License management

Go to **Configuration > Licenses > Management** to get an overview of the number of unlicensed devices connected to the server. Manage licenses online as well as offline. Remember to add licenses for all your devices before they are disabled after a 30-day trial period. See *how to purchase licenses*. You can also see the overview of your device licenses by clicking the license status link in the status bar.

You can add multiple MyAxis accounts as license administrator to your AXIS Camera Station system.

Add a MyAxis account to a system online

1. In the AXIS Camera Station client,

    1.1 Go to **Configuration > Licenses > Management**.

1.2 **Manage licenses online** is turned on by default.

1.3 Click **Go to AXIS License Portal**.

2. In the AXIS License Portal,

2.1 Sign in with the new MyAxis account that you want to add.

2.2 Go to **Edit license admins** and check that the account is added as license administrator.

Add a MyAxis account to a system offline

1. In the AXIS Camera Station client,

1.1 Go to **Configuration > Licenses > Management**.

1.2 If AXIS Camera Station is online, turn off **Manage licenses online** and click **Export system file**.

1.3 If AXIS Camera Station is offline, click **Export system file**.

1.4 Save your system file on a USB flash drive.

2. In the AXIS License Portal *www.axis.com/licenses*,

2.1 Sign in with the new MyAxis account that you want to add and upload your system file.

2.2 Go to **Edit license admins** and check that the account is added as license administrator.

There are different ways to license your system, depending on how it is connected to the Internet.

- *License a system online*
- *License a system offline*
- *Move licenses between systems on page 108*

License a system online

Both the AXIS Camera Station client and the server must be connected to the internet.

1. In the AXIS Camera Station client,

1.1 Go to **Configuration > Licenses > Management**.

1.2 **Manage licenses online** is turned on by default.

1.3 Click **Go to AXIS License Portal**.

2. In the AXIS License Portal *www.axis.com/licenses*,

2.1 Sign in with your MyAxis account.

2.2 Under **Add license key**, enter your license key and click **Add**.

3. In the AXIS Camera Station client, check that your license keys are shown under **Configuration > Licenses > Keys**.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=license-a-system-with-internet-connection

AXIS Camera Station online license registration

License a system offline

1. In the AXIS Camera Station client, export the system file.
    1.1 Go to **Configuration > Licenses > Management**.
    1.2 If AXIS Camera Station is online, turn off **Manage licenses online** and click **Export system file**.
    1.3 If AXIS Camera Station is offline, click **Export system file**.
    1.4 Save your system file on a USB flash drive.
2. In the AXIS License Portal *www.axis.com/licenses*,
    2.1 Sign in with your MyAxis account.
    2.2 Click **Upload system file** to upload the system file that you exported to your USB flash drive.
    2.3 Under **Add license key**, enter your license key and click **Add**.
    2.4 Under **License keys**, click **Download license file** and save the file to a USB flash drive.
3. In the AXIS Camera Station client, import the license file.
    3.1 Go to **Configuration > Licenses > Management**.
    3.2 Click **Import license file** and select the license file on your USB flash drive.
    3.3 Check that your license keys are shown under **Configuration > Licenses > Keys**.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=license-a-system-without-internet-connection

AXIS Camera Station offline license registration

Move licenses between systems

Note

The NVR Core licenses are locked to the device's hardware and can't be moved.

To move licenses from a system to another system with the same MyAxis account:

1. Go to the AXIS License Portal *www.axis.com/licenses*.
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. Click ⋮ and **Move**.
4. In the **To system** drop-down list, select a system that you want to move the license to.
5. Click **Move license key** and click **Close**. You can find the action details under **History**.
6. Go back to **My systems** and check that the licenses have been successfully moved.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=move-licenses-between-systems

Move licenses to another system

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

1. Go to the AXIS License Portal *www.axis.com/licenses*.
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. Make a copy of the license key first and click ⋮ and **Release**.
4. Sign out and sign in with another MyAxis account.
5. Under **My systems**, click the system that you want to license with the released license key.
6. Under **Add license key**, enter the license key you have released and click **Add**. You can find the action details under **History**.
7. Go back to **My systems** and check that the licenses have been successfully added.

Configure security

Configure user permissions

Go to **Configuration** > **Security** > **User permissions** to view a list of the users and groups that have been added to AXIS Camera Station.

Note

> Administrators of the computer on which the AXIS Camera Station server is installed are automatically given administrator privileges to AXIS Camera Station. You can't change or remove the administrators group's privileges.

Before a user or group can be added, the user or group must be registered on the local computer or have an Windows Active Directory user account. Using Windows Active Directory, a high level of security can be implemented.

When a user is part of a group, the user gets the highest role permission that is assigned to the individual and the group.

When a user is part of a group, the user gets the access granted as an individual and also receives the rights as part of a group. For example, a user is given access to camera X as an individual. The user is also a member of a group. The group is given access to cameras Y and Z. The user then has access to cameras X, Y and Z.

If there are security concerns regarding the access to the computer by a designated AXIS Camera Station user, create a standard user account that you then use for access to Axis Camera Station. You can then elevate the account to administrator in **Configuration > Security > User permissions**.

The list consists of the following information:

Item	Description
Icon	Indicates the entry is a group or a single user.
Name	Username as it appears in the local computer or Active Directory.
Domain	Domain name where the user or group is registered.
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	Server name where the user or group is registered. Only available when connecting to multiple AXIS Camera Station servers.

To add users or groups, see *Add users or groups*.

To change user access rights for a user or group, click the user or group and make changes. Click **Apply**.

To remove a user or group, select the user or group and click **Remove**. In the pop-up dialog, click **OK** to remove the user or group.

Add users or groups

User accounts in Microsoft Windows and Active Directory users and groups can access AXIS Camera Station. To add a user to AXIS Camera Station, you have to add users or a group to Windows.

To add a user or group in Microsoft Windows: Adding a user in Windows may vary depending on which version of Windows you are running. Follow the instructions on *Microsoft's site*. If you are connected to an Active Directory domain network, consult your network administrator.

Add users or groups

1. Go to **Configuration > Security > User permissions** and click **Add**.
2. When connecting to multiple AXIS Camera Station servers, select a server from the **Selected server** drop-down list.
3. Select **Server** to search for users or groups on the local computer, or select **Domain** to search for Active Directory users or groups. When connecting to multiple AXIS Camera Station servers, you can select which server to search for.
4. Select **Users** or **Groups** to search for only users or groups.
5. The list of users or groups is displayed. Users and groups that have already been added to AXIS Camera Station are not listed.
   - If there are too many users or groups, the search result is not displayed. Use the **Type to search** field to refine the search and find a specific user or group.
   - If the domain user search fails, the Service logon account must be changed. See *Can't find domain users*.
6. Select the users or groups and click **Add**. The users or groups are added to the list and shown in italics.

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 have selected **Operator** or **Viewer**, you can configure the user or group privileges. See *User or group privileges*.
4. Click **Save**. The user or group in the list is not in italics and ready to be used.

User or group privileges

There are three roles that can be given to a user or group. For how to define access privileges 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, access to all I/O ports and views. Therefore, you do not need to specify any camera, I/O or view privileges for a user with this role. This role is required in order to configure anything in the system.
- **Operator:** Access to live and recorded video of selected cameras and access to selected I/O ports and views. An operator has full access to all functionality of AXIS Camera Station except system configuration.
- **Viewer:** Access to live video of selected cameras and access to selected I/O ports and views. A viewer does not 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. 0 means that no priority is assigned. 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 **Mechanical PTZ** is 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.
- **Edit:** Allow to edit the views in AXIS Camera Station.

I/O

The following access privileges are available for users or groups with the Operator or Viewer role. The I/O ports are listed by device.

- **Access:** Allow full access to the I/O port.
- **Read:** Allow to view the state of the I/O port. The user is not able to change the port state.
- **Write:** Allow to change the state of the I/O port.

System

The access privileges that can't be configured are greyed out and listed under **Role privileges**. The privileges with check mark means the user or group have this privilege by default.

The following access privileges are available for users or groups with the Operator role.

- **Take snapshots:** Allow taking snapshots in the live view and recordings modes.
- **Export recordings:** Allow exporting recordings.
- **Generate incident report:** Allow generating incident reports.
- **Prevent access to recordings older than:** Prevent accessing recordings older than the specified number of minutes. When using search, the user will not find recordings older than the specified time. Recordings and bookmarks older than the specified time can't be played.
- **Access alarms, tasks, and logs:** Get alarm notifications and allow access to the **Alarms and tasks** bar and the **Logs** tab.

The following access privileges are available for users or groups with the Viewer role.

- **Take snapshots:** Allow taking snapshots in the live view and recordings modes.

Access control

The following access privileges are available for users or groups with the Operator 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.

- **Access management:** Allow access management and access to the active directory settings.

System health monitoring

The following access privileges are available for users or groups with the Operator role.

- **Configuration of system health monitoring**
- **Access to system health monitoring**

The following access privileges are available for users or groups with the Viewer role.

- **Access to system health monitoring**

Certificates

To manage settings for certificates between the AXIS Camera Station server and the devices, go to **Configuration > Security > Certificates**.

To access and manage the HTTPS and IEEE 802.1X certificates:

1. Go to **Configuration > Devices > Management**
2. Right-click your selected devices and go to **Security**.

See *Security on page 60* for more information.

Certificate authority (CA)

A CA allows you to enable HTTPS and IEEE 802.1X on devices without any client/server certificates in place.

AXIS Camera Station automatically stores the passphrase of the certificate authority.

For an existing CA in AXIS Camera Station:

- Click **View** to view the details of the CA certificate.
- Click **Export** to export the CA certificate in .cer or .crt formats. The file does not contain the private key and therefore is not encrypted. The certificate can be installed in other systems that trusts the certificates signed by AXIS Camera Station.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=certificate-authority

Generate a root CA

When AXIS Camera Station starts, it will check if there is a CA configured. If not, it will generate a root CA automatically.

A root CA includes a self-signed root certificate and private key which is protected by an auto-generated passphrase. The auto-generated passphrased is stored in AXIS Camera Station and not visible. A CA certificate generated by AXIS Camera Station is valid for 10 years.

AXIS Camera Station can automatically create, sign, and install client/server certificates on devices when enabling HTTPS or IEEE 802.1X.

Note

- If you upgrade from version 5.45 or earlier that uses a manually installed certificate on a device, AXIS Camera Station will automatically install a new certificate using the existing root CA when the manually installed certificate expires.
- When you generate a CA certificate, it's added to Windows Trusted Root Certificates.
- When you uninstall AXIS Camera Station, it removes its CA certificates from Windows Trusted Root Certification Authorities.

To use a passphrase of your choice, see *Reset the passphrase on page 115*.

To manually generate a new CA to replace the old one, see *Replace a CA on page 114*.

Import a CA

If a certificate authority is configured, AXIS Camera Station can automatically create, sign, and install client/server certificates on devices when enabling HTTPS or IEEE 802.1X. If you are willing to allow AXIS Camera Station to sign the certificates on your behalf, you need to import the existing CA consisting of a certificate and a private key.

Note

- If the imported CA is not protected by a passphrase, a dialog appears asking for it each time a passphrase is required. For example, when you enable 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, you must manually remove imported CA certificates from Windows Trusted Root Certification Authorities.

To import a CA to replace the existing one, see *Replace a CA on page 114*.

Replace a CA

If the certificates signed by a CA is currently in use by devices for their HTTPS connection, to replace the CA:

1. Go to **Configuration** > **Security** > **Certificates** > **HTTPS** and turn on **Ignore certificate validation**.
2. Go to **Configuration** > **Security** > **Certificates** > **Certificate authority**:
    - Click **Generate** or **Import**.
    - Provide your passphrase and click **OK**.
    - Select the number of valid days of the signed client/server certificates.
3. Go to **Configuration** > **Devices** > **Management**. Right-click the devices and select **Security** > **HTTPS** > **Enable/Update**.
4. Go to **Configuration** > **Security** > **Certificates** > **HTTPS** and turn off **Ignore certificate validation**.

HTTPS

To enable HTTPS, a server certificate must be present on each device.

By default, AXIS Camera Station validates the signature of the active HTTPS server certificate on each connected device and will not connect to a device if its certificate is not validated. The server certificate needs to be signed by the active CA in AXIS Camera Station or validated through Windows Certificate Store.

- If you turn on **Ignore certificate validation**, AXIS Camera Station will not validate if the certificate sent by the device is trusted or not, and it will accept any HTTPS certificate and enable configuration of insecure devices.
- If you turn off **Ignore certificate validation** and AXIS Camera Station validates that the certificate sent by the device is not trusted, a warning message **HTTPS certificate not trusted** will appear in the Status column in Device management and the device is not accessible.

AXIS Camera Station can check if the address specified in the device HTTPS certificate matches the address used to communicate with the device. This option will be greyed out if you turn on **Ignore certificate validation**.

- **Validate device address** is turned off by default to ensure stable behavior on DHCP networks without using hostnames.
- Turn on **Validate device address** to require the addresses match for additional security. We recommend that you only turn on this setting on networks where devices primarily communicate using hostname, or devices have a static IP address.

Note

- When a secure connection (HTTPS) is unavailable, a connection can be made using HTTP to configure devices that are not yet secure.
- To use HTTPS, firmware 5.70 or later is required for video devices, and firmware 1.25 or later for access control and audio devices.
- Cameras with firmware 7.20 or later are preconfigured with a self-signed certificate. When enabling HTTPS with the self-signed certificate, it will fail because the self-signed certificate is not trusted. We recommend that you generate or import a CA so that AXIS Camera Station can issue new certificates to the devices when enabling HTTPS.

IEEE 802.1X

To enable IEEE 802.1X, a client certificate must be present on each device. In addition to the client certificate, an IEEE 802.1X authentication CA certificate has to be installed. The IEEE 802.1X authentication CA certificate will be installed when enabling or updating IEEE 802.1X.

Note

- To use IEEE 802.1X certificates, firmware 5.50 or later is required for video devices, and firmware 1.25 or later for access control and audio devices.
- Cameras with firmware 7.20 or later are preconfigured with a self-signed certificate. You need to delete the self-signed certificate before manually uploading your own client certificate because AXIS Camera Station only allows one client certificate per device, and the default self-signed certificate qualifies as both client and server certificates. If you encounter an error when deleting the self-signed certificate, disable HTTPS on the devices from AXIS Camera Station even if the HTTPS status is `Disabled`.

To configure IEEE 802.1X:

- In **EAPOL Version**, select what version of Extensible Authentication Protocol (EAP) you want to use.
- In **EAP identity**, select to use either the device's MAC address, the device hostname or custom text. If you have selected **Custom**, enter any text that will function as the EAP identity in the **Custom** field.
- Click **Import** and navigate to the IEEE 802.1X authentication CA certificate file which can either be sourced externally, for example from the IEEE 802.1X authentication server, or directly from AXIS Camera Station.
- Select to use either **Device IP address** or **Device EAP identity** as the common name in the individual certificates that are created for each device when AXIS Camera Station acts as a certificate authority.

Certificate expiration warning

A notification will be created if a client or server certificate is expired or is about to be expire. It applies to all certificates installed on connected devices, except CA certificates installed outside of AXIS Camera Station. A warning will appear as message **Certificate about to expire** or **Certificate has expired** in the Status column in the Device management page and as icon in the Installed certificates list.

If a CA certificate listed in **Configuration > Certificates** is about to expire, a warning will appear as icon in the Certificate page and a system alarm will be triggered.

In this section, specify how early you want AXIS Camera Station to notify you when certificates are approaching their expiration date.

Certificate renewal

Renew certificate between the server and devices

- The client or server certificates generated by AXIS Camera Station will automatically be renewed 7 days before the expiration warning is configured to appear.
- If you want to renew or update a certificate manually, follow the same steps as enabling HTTPS or IEEE 802.1X.

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 passphrase

To use a passphrase of your choice:

1. Go to **Configuration > Security > Certificates** and turn on **Ignore certificate validation** to ensure the devices that have been enabled with certificates are accessible during the resetting process.
2. Click **Generate** and enter your passphrase.
3. Click **Export** to save the CA certificate locally.

4. Go to **Configuration > Devices > Management** and enable HTTPS on selected devices.

5. Turn off **Ignore certificate validation** to ensure secure HTTPS communication.

Manage HTTPS certificates in AXIS Camera Station

HTTPS consists of communication over HTTP within a connection encrypted by Transport Layer Security (TLS). Network encryption protects the communication within the video management system. It prevents information being extracted by network traffic sniffing, and it prevents data being altered during transfer.

This section explains how to configure and enable HTTPS communication on Axis devices from AXIS Camera Station.

AXIS Camera Station can be used as:

- **Root certificate authority (CA):** Using AXIS Camera Station as a root CA simplifies the whole process of deploying and renewing certificates for the administrator. It means AXIS Camera Station will use its own root certificate to issue server certificates and there is no other root CA involved in the process.

- **Intermediate certificate authority:** Using AXIS Camera Station as an intermediate CA implies that you have an existing CA (root or intermediate CA) which can issue CA certificates to other intermediate CAs (e.g. AXIS Camera Station). In this scenario you need to import the CA certificate and its private key in AXIS Camera Station to sign and issue server certificates for the Axis devices. This CA certificate may be a root certificate or a subordinate CA certificate (intermediate certificate).

Note

- To use HTTPS, firmware 5.70 or later is required for video devices, and firmware 1.25 or later for access control and audio devices.
- Cameras with firmware 7.20 or later are preconfigured with a self-signed certificate. When enabling HTTPS with the self-signed certificate, it will fail because the self-signed certificate is not trusted. We recommend that you generate or import a CA so that AXIS Camera Station can issue new certificates to the devices when enabling HTTPS.

To configure and enable HTTPS communication:

1. Optional: Select the certificate authority

2. Enable HTTPS on devices

3. Optional: Add the CA certificate to the certificate store

4. Update or renew HTTPS certificates

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=manage-https-certificates-in-axis-camera-station

Manage HTTPS certificates in AXIS Camera Station

Select the certificate authority

1. Go to **Configuration > Security > Certificates**.

2. Under **Certificate authority**,

  - To use AXIS Camera Station as a root CA, click **Generate** and type your passphrase.
  - To use AXIS Camera Station as an intermediate CA, click **Import** and navigate to the file that contains the CA certificate and its private key.

Enable HTTPS on devices

1. Go to **Configuration > Devices > Management**.
2. Right-click the devices, select **Security > HTTPS > Enable/Update**. Ensure that HTTPS status changes to `Enabled`.
3. If you have selected multiple devices, double-click the task to check the result of each device.

Add the CA certificate to the certificate store

We recommend adding the CA certificate to your Windows certificate store so your web browser will not pop up a security warning regarding invalid security certificate and will not block the connection to the device. This will ensure a secure HTTPS connection to your devices. The following instructions are for Windows 10.

1. Go to the **Start** menu, type **mmc** and press ENTER.
2. In the console, go to **File > Add/Remove snap-in**.
3. Select **Certificates** in the left panel, and click **Add**. Select **Computer account** and configure the computer account and click **OK**.
4. In the left panel of the console, go to **Certificates (Local computer) > Trusted root certification authorities > Certificates**. Right-click and select **All Tasks > Import**, and click **Next**.
5. Click **Browse** and select the AXIS Camera Station root certificate saved on your computer or your own CA certificate, and click **Next**.
6. Select to place all certificates in the trusted root certification authorities. Click **Next** and **Finish**.

Update or renew HTTPS certificates

If a server certificate expired or is about to expire, an warning will appear:

- as message **Certificate about to expire** or **Certificate has expired** in the Status column in the Device management page.
- as icon in the installed certificates list.

How long time before expiration the warning should come is configured in **Configuration > Security > Certificates**.

If you have configured AXIS Camera Station as a certificate authority, the client or server certificates generated by AXIS Camera Station will automatically be renewed 7 days before the expiration warning is configured to appear. This task is done during the nightly jobs. If you want to renew or update a certificate manually, follow the same steps as enabling HTTPS.

Limitations

- Non-default ports (other than 443) are not supported.
- All certificates in an install batch must have same passphrase.
- Certificate operations over unencrypted channels, i.e. "Basic" are not supported. Devices should be set to "Encrypted & unencrypted" or "Encrypted only" to allow "Digest" communication.
- HTTPS can't be enabled on the AXIS T85 PoE+ Network switch series.

Manage IEEE 802.1X certificates in AXIS Camera Station

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN. IEEE 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. In our case, 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; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

This section explains how to manage IEEE 802.1X EAP-TLS certificates from AXIS Camera Station. AXIS Camera Station can help you to either import or generate, and then distribute client certificates and authentication certificates on the Axis network devices as well as enabling IEEE 802.1X EAP-TLS.

Note

- To use IEEE 802.1X certificates, firmware 5.50 or later is required for video devices, and firmware 1.25 or later for access control and audio devices.
- Cameras with firmware 7.20 or later are preconfigured with a self-signed certificate. You need to delete the self-signed certificate before manually uploading your own client certificate because AXIS Camera Station only allows one client certificate per device, and the default self-signed certificate qualifies as both client and server certificates. If you encounter an error when deleting the self-signed certificate, disable HTTPS on the devices from AXIS Camera Station even if the HTTPS status is `Disabled`.

To configure and enable IEEE 802.1X communication:

1. Optional: Select the certificate authority
2. Select the authentication CA certificate
3. Select the client certificate common name
4. Enable IEEE 802.1X to upload certificates
5. Update or renew IEEE 802.1X certificates

Select the certificate authority

1. Go to **Configuration > Security > Certificates**.
2. If you want to use AXIS Camera Station as a root CA:
   2.1 Click **Generate** and enter your passphrase.
   2.2 Once generated, click **Export** and **No** to export the certificate so that it can be provided to any third-party application to trust the camera certificate.
3. If you want to use AXIS Camera Station as an intermediate CA, click **Import** and navigate to the file that contains the CA certificate and its private key.

Select the authentication CA certificate

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. This certificate will be installed on each Axis device and used to verify the authentication server.

1. Go to **Configuration > Security > Certificates**.
2. In the IEEE 802.1X section, click **Import** and navigate to the IEEE 802.1X authentication CA certificate file. This certificate will be installed on each Axis device and used to verify the authentication server.

Select the client certificate common name

When AXIS Camera Station acts as a certificate authority, you can select the common name of the certificates on devices. The client certificates common name should be selected before enabling IEEE 802.1X on the devices.

1. Go to **Configuration > Security > Certificates**.
2. In the IEEE 802.1X section, select to use either **Device IP address** or **Device EAP identity** as the common name.

Enable IEEE 802.1X to upload certificates

1. Go to **Configuration > Devices > Management**.

2. Right-click the devices, select **Security > IEEE 802.1X > Enable/Update**. The IEEE 802.1X status should change to `Enabled` and the selected devices now support communication on the IEEE 802.1X network.

3. You can double-click the task to check the result of each device.

Update or renew IEEE 802.1X certificates

If a client certificate expired or is about to expire, an warning message will appear:

- as message **Certificate about to expire** or **Certificate has expired** in the Status column in the Device management page.

- as icon in the installed certificates list.

How long time before expiration the warning should come is configured in **Configuration > Security > Certificates**.

If you have configured AXIS Camera Station as a certificate authority, the client or server certificates generated by AXIS Camera Station will automatically be renewed 7 days before the expiration warning is configured to appear. This task is done during the nightly jobs. If you want to renew or update a certificate manually, follow the same steps as enabling IEEE 802.1X.

Limitations

- All client certificates in a single install batch must have same passphrase.

- For devices with several network adapters (such as wireless cameras), IEEE 802.1X can only be enabled for the first adapter, typically the wired connection.

- Devices missing parameter `Network.Interface.I0.dot1x.Enabled` are not supported. For example: AXIS P39 Series, T85 Series and T87 Video Decoder

- Certificate operations over unencrypted channels, i.e. "Basic" are not supported. Devices should be set to "Encrypted & unencrypted" or "Encrypted only" to allow "Digest" communication.

Configure access control

If you have added AXIS A1601 Network Door Controller to your system, you can configure the access control hardware in AXIS Camera Station version 5.35 or later.

For a complete workflow to set up AXIS A1601 Network Door Controller in AXIS Camera Station, See *Set up AXIS A1601 Network Door Controller.*

Note

Before you start, ensure the following:

- Upgrade the controller firmware under **Configuration > Devices > Management**. See *Upgrade firmware on page 57.*
- Set date and time for the controller under **Configuration > Devices > Management**. See *Set date and time on page 58.*
- Enable HTTPS on the controller under **Configuration > Devices > Management**. See *Security on page 60.*

Workflow to configure access control

1. To edit the predefined identification profiles or create a new identification profile, see *Identification profiles on page 130.*

2. To use a custom setup for card formats and PIN length, see *Card formats and PIN on page 132.*

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 128*

5. Add a zone and add doors to the zone. See *Add a zone on page 129*.

Doors and zones

Go to **Configuration > Access control > Doors and zones** and a list of doors and zones that have been configured is displayed.

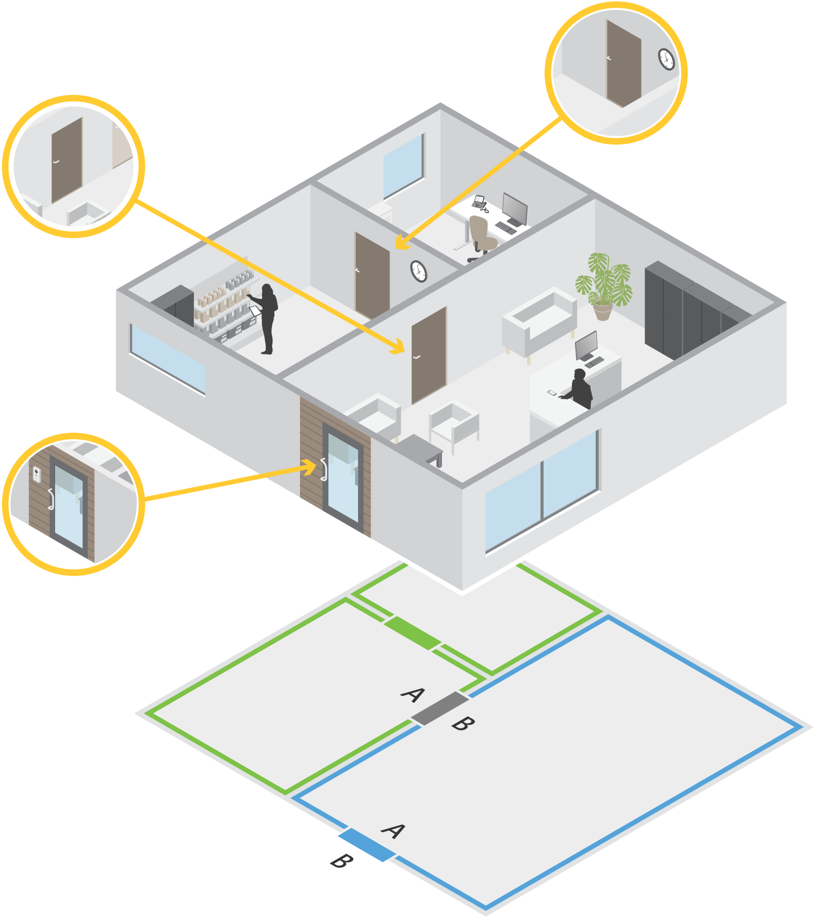
Item	Description
Doors	
Name	The name of the door.
Door controller	The door controller that the door is connected to.
Side A	The zone that side A of the door is in.
Side B	The zone that side B of the door is in.
Identification profile	The identification profile applied to the door.
Card formats and PIN	Shows the setup of card formats or PIN length applied to the door is a system setup or custom setup.
Status	The status of the door. • **Online:** The door is online and works normally. • **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 not enabled for the reader.
Zones	
Name	The name of the zone.
Number of doors	The number of doors included in the zone.

In this page, you can:

- Add, edit or remove a door. See *Add a door on page 122*.
- Add, edit or remove a zone. See *Add a zone on page 129*.
- Turn off OSDP Secure Channel for a specific reader.
  1. Select a door in the list.
  2. Click ⋮ and select **Turn off OSDP Secure Channel**.
  3. Click **Apply**.
- Turn on OSDP Secure Channel for a specific reader after it is turned off manually.
  1. Select a door in the list.
  2. Click ⋮ and select **Recreate OSDP Secure Channel**.
  3. Click **Apply**.
- View the controller pin chart associated with a door.
  1. Select a door in the list.
  2. Click **Pin chart**.
  3. If you want to print the pin chart, click **Print**.

- Change identification profile on doors.
  1. Press SHIFT or CTRL to select multiple doors in the list.
  2. Click **Select identification profile**.
  3. Select an identification profile and click **Apply**.

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

A door controller can be configured with one door with two locks, or two doors with one lock on each door.

To add a door by creating a new door configuration:

1. Go to **Configuration** > **Access control** > **Doors and zones** and click **Add door**.
2. Type a door name.
3. Select a door controller from the **Controller** drop-down list. It shows how many doors are connected to the controller and the controller is greyed out when there is no room for another door or when it is offline or HTTPS is not activated.
4. Click **Next** to go to the door configuration page.
5. Select a relay port from the **Primary lock** drop-down list.
6. To configure two locks on the door, select a relay port from the **Secondary lock** drop-down list.
7. Select an identification profile. See *Identification profiles on page 130*.
8. Configure the *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 128*
13. Click **Save**.

To add a door by copying an existing door configuration:

1. Go to **Configuration** > **Access control** > **Doors and zones** and click **Add door**.
2. Enter a door name.
3. Select a door controller from the **Controller** drop-down list.
4. Click **Next**.
5. Select an existing door configuration from the **Copy configuration** drop-down list. It shows how many doors are connected to the controller and the controller will be greyed out if it has been 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**.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=add-a-door

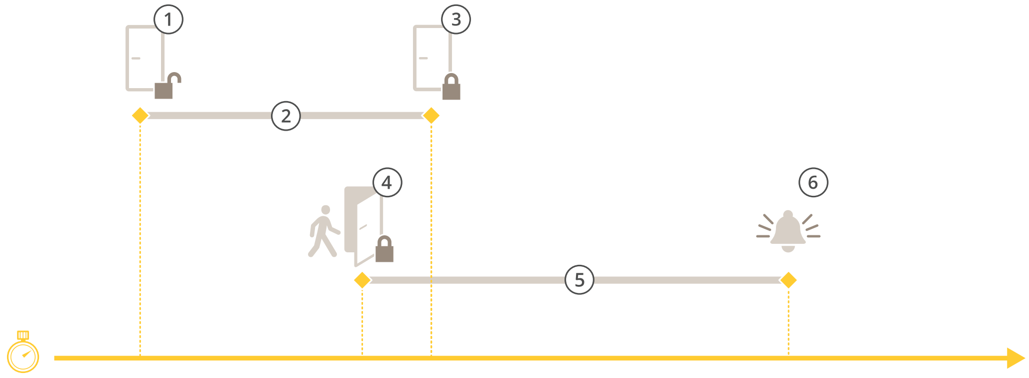
Add and configure doors and zones

Door settings

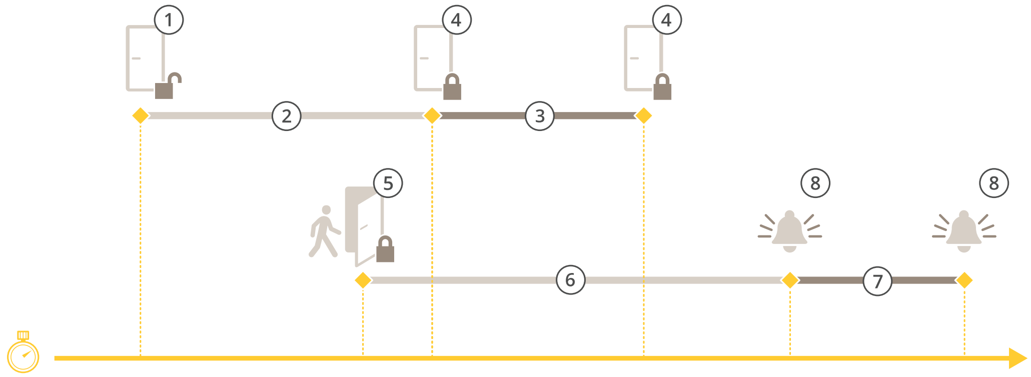
Go to the door configuration page and configure the door settings under **Door settings**.

- **Access time (sec):** Set the number of seconds the door should remain unlocked after access has been granted. The door remains unlocked until the door has been opened or until the set time has been reached. The door will lock when it closes regardless of whether the access time has expired or not if a door monitor is configured.
- **Open-too-long time (sec):** Only valid if a door monitor is configured. Set the number of seconds the door is allowed to stay open. If the door is still open when the set time has been reached, the door open too long alarm is triggered. Set up an action rule to configure which action the open too long event will trigger.
- **Long access time (sec):** Set the number of seconds the door should remain unlocked after access has been granted. Long access time overrides the already set access time for cardholders with this setting enabled.
- **Long open-too-long time (sec):** Only valid if a door monitor is configured. Set the number of seconds the door is allowed to stay open. If the door is still open when the set time has been reached, the door open-too-long event is triggered. Long open-too-long time overrides the already set open-too-long time for cardholders with this setting enabled.
- **Relock delay time (ms):** Set the time (milliseconds) that the door stays unlocked after the it's opened or closed.
- **Relock**
  - **After opening:** Only valid if a door monitor is configured.
  - **After closing:** Only valid if a door monitor is configured.

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 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 up to 16 wireless locks to a door controller.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=add-a-wireless-lock

Note

- The setup requires AXIS OS version 11.6.16.1 or later on the Axis door controller.
- The setup requires a valid AXIS Door controller Extension License.
- The Axis door controller time must be the same as the AXIS Camera Station server time.
- Before you start you must pair the Aperio locks with the Aperio hub using the Aperio programming application tool ASSA ABLOY supports.

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 the AXIS Door Controller Extension.

   2.1 In the door controller web interface, go to **Apps**.

   2.2 Open the 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 via the communication hub.

   3.1 In the door controller web interface, go to **Access control** > **Wireless locks**.

   3.2 Click **Connect 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're adding and click **Save**.

4. Add and configure the door with the wireless lock.

   4.1 In AXIS Camera Station, 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**, and click **Next**.

   4.4 Select your **Wireless lock**.

   4.5 Define the door sides A and B, and add any sensors. See *Doors and zones on page 120* for more information.

   4.6 Click **Save**.

Once you've connected the wireless lock you can see its battery level and status in the overview of doors.

Wireless lock battery level

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 may not work as intended.

Wireless lock status

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 select to add a door monitor to your door and configure how the door monitor circuits are connected.

1. Go to the door configuration page. See *Add a door on page 122*.
2. Under **Sensors**, click **Add** and select **Door monitor sensor**.
3. Select the I/O port that you want to connect the door monitor to.
4. Under **Door open if**, select how the door monitor circuits are connected.
   - **Circuit is open**: Select if the door monitor circuit is normally closed. The door monitor gives the door open signal when the circuit is open. The door monitor gives the door closed signal when the circuit is closed.
   - **Circuit is closed**: Select if the door monitor circuit is normally open. The door monitor gives the door open signal when the circuit is closed. The door monitor gives the door closed signal when the circuit is open.
5. To ignore the state changes of the digital input before it enters a new stable state, set a **Debounce time**.
6. To trigger an event when the connection between the door controller and the door monitor is interrupted, turn on **Supervised input**. See *Supervised inputs on page 129*.

Add emergency input

An emergency input can be configured to initiate an action to lock or unlock the door.

You can select to add emergency input to your door and configure how the circuits are connected.

1. Go to the door configuration page. See *Add a door on page 122*.
2. Under **Sensors**, click **Add** and select **Emergency input**.
3. Select how the circuits are connected.
   - **Circuit is open**: Select if the emergency input circuit is normally closed. The emergency input gives the emergency state signal when the circuit is open.
   - **Circuit is closed**: Select if the emergency input circuit is normally open. The emergency input gives the emergency state signal when the circuit is closed.

4. To ignore the state changes of the digital input before it enters a new stable state, set a **Debounce time (ms)**.

5. Select what **Emergency action** to trigger when receiving the emergency state signal.

   - **Unlock door**: Select if you want to unlock the door when receiving the emergency state signal.

   - **Lock door**: Select if you want to lock the door when receiving the emergency state signal.

Add a reader

A reader is a device that reads a cardholder's credentials from a card, key tag, or related item.

A door controller can be configured with two readers. You can select to add a reader on one side or both sides of a door.

If you apply a custom setup of card formats or PIN length to a reader, it is clearly displayed in the **Card formats** column under **Configuration > Access control > Doors and zones**. See *Doors and zones on page 120*.

Note

- For a reader, if you have configured a different end of PIN character in AXIS Camera Station Secure Entry and the device webpage, the configuration on the device webpage will be used.
- When using an Axis network intercom as IP reader and you've configured a different PIN length in AXIS Camera Station Secure Entry and the device webpage, the configuration on the device webpage will be used.

1. Go to the door configuration page. See *Add a door on page 122*.

2. Under one side of the door, click **Add** and select **Card reader**.

3. For RS485 readers, select **OSDP RS485 half duplex** and a reader port.

4. For readers that use Wiegand protocols, select **Wiegand** and a reader port.

   - Under **LED control**, select **Single wire** or **Dual wire (R/G)**. Readers with dual LED control use different wires for the red and green LEDs.

   - Under **Tamper alert**, select when the reader tamper input is active.

   - **Open circuit**: The reader gives the door the tamper signal when the circuit is open.

   - **Closed circuit**: The reader gives the door the tamper signal when the circuit is closed.

   - To ignore the state changes of the reader tamper input before it enters a new stable state, set a **Tamper debounce time**.

   - To trigger an event when the connection between the door controller and the reader is interrupted, turn on **Supervised input**. See *Supervised inputs on page 129*.

5. For IP readers, select **IP reader** and select a device from the drop-down list. For requirements and supported devices, see *IP reader on page 128*.

6. The PIN length is configured under **Configuration > Access control > Card formats and PIN**. To use a custom PIN length setup for this reader which is different from the system setup:

   6.1 Click **Advanced**.

   6.2 Turn on **Custom PIN length**.

   6.3 Set the **Min PIN length**, **Max PIN length**, and **End of PIN character**.

   6.4 Go to **Configuration > Doors and zones** and the **Card formats** column is marked as **Custom** for this door.

7. The card formats are configured under **Configuration > Access control > Card formats and PIN**. To use a custom card format setup for this reader which is different from the system setup:

   7.1 Click **Advanced**.

7.2 Turn on **Custom card formats**.

7.3 Change the card formats you want to use for the reader. If a card format with the same bit length is already in use, you need to deactivate it first.

A warning icon is displayed when the card format setup is different from the system setup configured under **Configuration > Access control > Card formats and PIN**.

7.4 Go to **Configuration > Doors and zones** and the **Card formats** column is marked as **Custom** for this door.

8. Click **Add**.

9. To add a reader to the other side of the door, repeat the previous steps.

For information on how to set up an AXIS Barcode Reader, see *Set up AXIS Barcode Reader*.

IP reader

Axis network intercoms can be used as IP reader in AXIS Camera Station Secure Entry.

Note

- It requires AXIS Camera Station 5.38 or later, AXIS A1601 Network Door Controller with firmware 10.6.0.2 or later.
- No special configuration is required in the intercom to use it as IP reader.

The following devices are supported:

- 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

A request to exit (REX) device is a device local to a door indicating that someone has requested to exit the door. A REX device can be a PIR sensor, REX button, or push bar.

You can select to add a REX device on one side or both sides of the door.

1. Go to the door configuration page. See *Add a door on page 122*.
2. Under one side of the door, click **Add** and select **REX device**.
3. 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.
4. Select the **Action** to trigger when receiving the REX signal.
   - **Unlock door**: Select if you want to unlock the door when receiving the REX signal.
   - **None**: Select if you don't want to trigger any action when receiving the REX signal.
5. Under **REX active**, select how the door monitor circuits are connected.
   - **Circuit is open**: Select if the REX circuit is normally closed. The REX device gives the signal when the circuit is open.
   - **Circuit is closed**: Select if the REX circuit is normally open. The REX device gives the signal when the circuit is closed.
6. To ignore the state changes of the digital input before it enters a new stable state, set a **Debounce time (ms)**.

7. To trigger an event when the connection between the door controller and the REX device is interrupted, turn on **Supervised input**. See *Supervised inputs on page 129*.

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. A door can be:

- **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**, select the doors you want to add to the zone, and click **Add**.
5. The door is set to be a perimeter door by default. To change it, select **Internal door** from the drop-down list.
6. For a perimeter door, it is set to use door side A to enter the zone by default. To change it, select **Leave** from the drop-down list. This option is only available for a perimeter door.
7. To remove a door from the zone, select it and click **Remove**.
8. 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**.

Supervised inputs

Supervised inputs can be used to trigger an event when the following connections are interrupted.

- 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 128*.

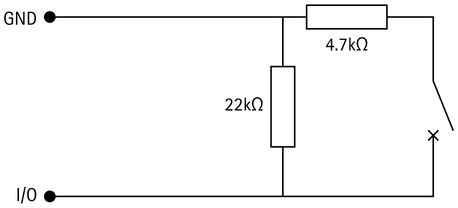
To use supervised inputs:

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, a door monitor, or a REX device, turn on **Supervised input**.
3. If you have 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 have followed the serial first connection diagram, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.

Connection diagram

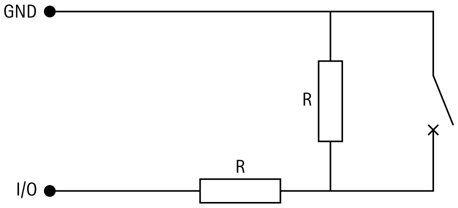
Parallel first connection

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 determine how and when a cardholder gets access to a door through a specific side of the door.

Identification types are carriers of the credential information that cardholders need to get access to a door. Common identification types are tokens, such as cards (card raw, card number) or key fobs, personal identification numbers (PINs), fingerprints, facial maps, and request to exit (REX) devices. And depending on the identification type, it can carry one or more types of information.

Supported identification types: Card, PIN, REX, Static QR, and Dynamic QR.

Note

Dynamic QR must be used with PIN together.

Go to **Configuration > Access control > Identification profiles** to create, edit, or remove identification profiles. Use the **Type to search** field to find a specific identification profile.

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

- **Card:** Cardholders need to swipe the card to access the door.
- **Card and PIN:** Cardholders need to swipe the card and enter the PIN to access the door.

- **PIN:** Cardholders need to enter the PIN to access the door.
- **Card or PIN:** Cardholders need to swipe the card or enter the PIN to access the door.
- **QR:** Cardholders need to show the QR Code® to camera to access the door. The QR identification profile is used for both static and dynamic QR.

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

To create an identification profile:

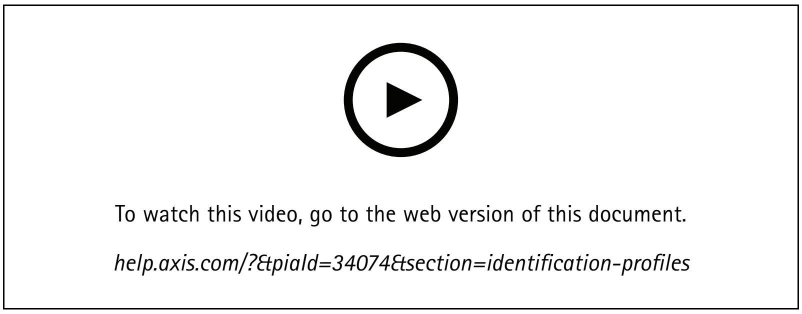
1. Go to **Configuration > Access control > Identification profiles** and click **Create identification profile**.
2. Type an identification profile name.
3. Select **Include facility code for card validation** to use facility code as one of the credential validation fields. This field is only available if you have enabled **Facility code** under **Access management > Settings**.
4. On a specific side of the door,
   4.1 Click **Add**.
   4.2 Select one or more types from the **Identification type** drop-down list.
   4.3 Select one or more schedules from the **Schedule** drop-down list.
5. On the other side of the door, repeat the previous steps.
6. 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, type a new name.
4. On a specific side of the door,
   - To change an identification type, select one or more types from the **Identification type** drop-down list.
   - To change a schedule, select one or more schedules from the **Schedule** drop-down list.
   - To remove an identification type and the related schedule, click ✕ .
   - To add an identification type and the related schedule, click **Add** and set the identification types and schedules.
5. To edit the identification profile on the other side of the door, repeat the previous steps.
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 has been applied to a door, select another identification profile for the door.
4. Click **OK**.



To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=identification-profiles

Set up identification profiles

Card formats and PIN

A card format defines how data is stored in a card. It is 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 the information stored on the card is organized. By defining a card format, you tell the system how to interpret the information that the controller gets from the card reader.

There are a few 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** and a list of card formats is displayed. You can create, edit, or activate card formats. You can also configure PIN. Use the **Type to search** field to find a specific card format. Click ⟲ to reset a card format to the default field map.

The custom card formats can contain the following data fields used for credential validation.

- **Card number:** A subset of the credential binary data that is encoded as decimal or hexadecimal numbers. Card number is used to identify a specific card or cardholder.
- **Facility code:** A subset of the credential binary data that is encoded as decimal or hexadecimal numbers. Facility code is used to identify a specific end customer or site.

To create a card format:

1. Go to **Configuration** > **Access Control** > **Card formats and PIN** and click **Add card format**.
2. Type a card format name.
3. In the **Bit length** field, type a bit length between 1 and 256.
4. Select **Invert bit order** if you want to invert the bit order of the data received from the card reader. Click ⓘ to see an example of the output after inverting bit order.
5. 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 can be divided by eight. Click ⓘ to see an example of the output after inverting byte order.
6. Choose 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.
   - **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.

     The decimal system, also known as base-10 positional numeral system, consists of the numbers 0–9.

     The hexadecimal system, 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 bit order means that the first bit is the smallest (least significant).

Big endian bit order means that the first bit is the biggest (most significant).

7. Click **OK**. The card format is added to the card format list.

8. 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, "Format A" and "Format B", and you have activated "Format A", you can't activate "Format B" without deactivating "Format A" first.
- You can only activate and deactivate card formats if the door controller has been configured with at least one reader.

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** if the bit length can be divided by eight.
4. If you edit a custom card format, you can edit all the fields.
5. 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 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**.

▶

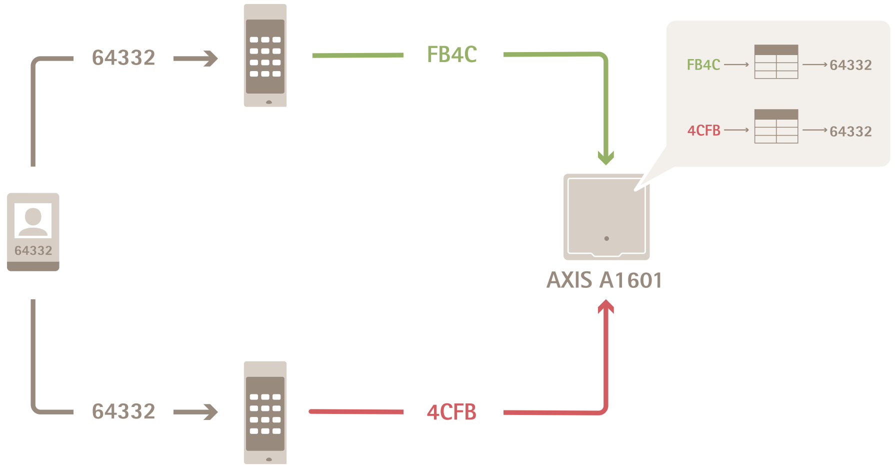
To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=card-formats-and-pin

Set up card formats

Card format settings

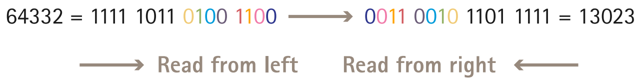
Overview



- 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 A1601 Network Door Controller receives FB4C and transfers it to decimal number 64332 according to the card format settings applied to the reader.
- AXIS A1601 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 applied to the reader.

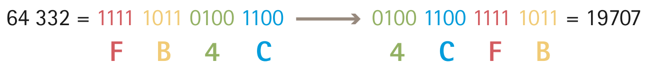
Invert bit order

After inverting bit order, the card data received from the reader is read from right to left bit by bit.

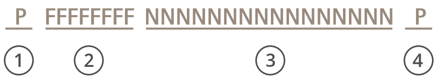


Invert byte order

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 enable line encryption between controller and Axis readers.

To turn on OSDP Secure Channel for entire system:

1. Go to **Configuration > Access control > Encrypted communication**.
2. Specify your main encryption key and click **OK**. To change the main encryption key, click ✎ .
3. Turn on **OSDP Secure Channel**. This option is only available after you have set the main encryption key.
4. By default, the OSDP Secure Channel key is generated by the main encryption 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 Type 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 can authenticate AXIS Barcode Reader by using the authentication key to grant access. For a complete workflow how to set up AXIS Barcode Reader, see *Set up AXIS Barcode Reader*.

To create a connection between a door controller and AXIS Barcode Reader:

1. In AXIS Camera Station:
   1.1 Go to **Configuration > Access control > Encrypted communication**.
   1.2 Under **External Peripheral Authentication Key**, click **Show authentication key** and **Copy key**.
2. In the device's webpage where AXIS Barcode Reader is running:
   2.1 Open the AXIS Barcode Reader application.
   2.2 If server certificate is not configured in AXIS Camera Station, turn on **Ignore server certificate validation**. See *Certificates* for more information.
   2.3 Turn on **AXIS Camera Station Secure Entry**.

2.4 Click **Add** and enter the IP address of the door controller and paste the authentication key.

2.5 Once the connection is created, view the information on the right panel. Select the reader to read barcodes from the door drop-down list.

Multi server BETA

With multi server, global cardholders and cardholder groups on the main server can be used from the connected sub servers.

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 168*.

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 136*.
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 136*.
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 141*.

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**. A configuration file in .json format is generated.
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 + and navigate to the configuration file that you have generated from the sub server.
4. Enter the server name, IP address, and port number of the sub server. Click **Import**.
5. The sub server is added to the list and the status shows `Connected`.

Revoke a sub server

You can only revoke a sub server before its configuration file is imported to a main server.

1. From the main server, go to **Configuration** > **Access control** > **Multi server**.
2. Click **Sub server** and click **Revoke server**.
3. 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, the sub server is connected to the main server.

To remove a sub server:

1. From the main server:
    1.1 Go to **Access management > Dashboard** and change the global cardholders and groups to local cardholders and groups.

    1.2 Go to **Configuration > Access control > Multi server** and click **Main server** to display the sub server list.

    1.3 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^{PREVIEW}

Note

User accounts in Microsoft Windows and Active Directory users and groups can access AXIS Camera Station. To add a user to AXIS Camera Station, you must add users or a group to Windows. How to add a user in Windows can vary depending on your version. Follow the *instructions on Microsoft's site*. Consult your network administrator if you're connected to 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. See *Import active directory users on page 137*.

After the initial configuration the page offers the following options.

- 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:

1. Go to **Configuration** > **Access control** > **Active directory settings**^{PREVIEW}.
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.

Configure smart search 2

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

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=smart-search-2-settings

For requirements, limitations and how to use smart search 2, see *Smart search 2 on page 34*.

1. Go to **Configuration** > **Smart search 2** > **Settings**.
2. Under **Cameras**,
   - 2.1 Select the cameras to send metadata to smart search 2.
   - 2.2 To allow server classification in the background for a camera, select **Allow** under the **Background server classification** column. This increases the server load but improves the user experience.
   - 2.3 For cameras with background server classification, an icon appears under the **Background server classification** column indicating the server classification status in the last hour when the server classification is slow.
     - appears when less than 95% detections are classified.
     - appears when less than 50% detections are classified.
   - 2.3 To limit the amount of detections saved on the server, under **Filter**, click ⚙ and create filters for **Size and duration**, and **Area**. You can use this for example to exclude small objects, or objects that only appear for a very short time. The filter applies to each individual camera.
3. Under **Storage**:
   - Select the drive and folder to store the detections and click **Apply**.
   - Set the storage size limit and click **Apply**. The oldest detections are removed when the storage limit is reached.

Configure System Health Monitoring BETA

Note

- When connecting to multiple AXIS Camera Station servers, you can configure System Health Monitoring on any connected server by selecting the server from the **Selected server** drop-down list.
- If you're managing systems located 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 98* 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 99*
2. Configure the email addresses to receive the notifications. See *Configure email recipients on page 139*.
3. Configure the notification rules. See *Configure notification rules on page 139*.

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 is displayed showing 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 turn off the notification rules.
3. Under **Applied rules**, a list of systems and devices including the applied notification rule is displayed.

Multisystem

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=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 to be accessed by the main system. See *Generate system configuration on page 139*.
2. Repeat the previous steps in other secondary systems.
3. In the main system, upload the system configurations. See *Retrieve data from other systems on page 140*.
4. Monitor the health data from multiple systems from the main system. See *System Health Monitoring ^{BETA} on page 153*.

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 system configuration is uploaded to the main system, the main system information is displayed 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**. The information you have copied from the secondary system is automatically filled.
3. Check the host IP address and click **Add**. The secondary system is added and is displayed under **Available systems**.

Access management

After you have configured access control, click + and select **Access management** to display the Access management tab in the AXIS Camera Station client. See *Configure access control on page 119*.

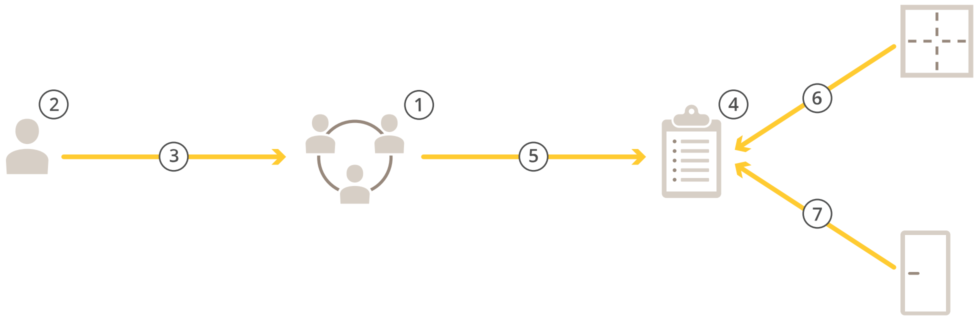
For a complete workflow to set up AXIS A1601 Network Door Controller in AXIS Camera Station, See *Set up AXIS A1601 Network Door Controller*.

The Access management tab allows you to configure and manage the system's cardholders, groups, doors, zones and access rules. It consists of the following views:

- Dashboard: Add cardholders, credentials, groups, access rules, and perform actions on doors and zones.
    - When the configuration of a cardholder, door or access rule is not complete, it is highlighted in yellow. For example, when a cardholder or door is not added to an access rule.
    - When something goes wrong with a cardholder configuration, it is highlighted in pink. For example, when a cardholder is expired or suspended.
- Reports: Export reports that contain different types of information about the system. See *Export reports on page 150*.
- Settings: Add custom fields to cardholder template and enable facility code in the system. See *Access management settings on page 151*.
- Import and export: Import and export cardholder data. You can also reset the system to the state before the last import. See *Import and export on page 151*.

Workflow of access management

The access management structure is flexible, allowing 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 147*.

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. A cardholder is configured with credentials that tell the system who the person is and when and how the person is granted access to doors.

You can also choose to map users in an Active Directory database as cardholders, see *Active directory settings*^{PREVIEW} *on page 137*.

1. Go to **Access management > Dashboard**.
2. Under **Cardholders**, click ⊕ and 👤 .
3. Enter the first name, last name, cardholder ID, and email address. The cardholder ID is a unique number that can always be used to identify a cardholder.
4. If you have configured custom fields under **Access management > Settings**, enter information for the custom fields too.
5. Add a cardholder image. Click **Add Image** and select **Upload image** or **Take a picture**.
6. Add groups that the cardholder belongs to.
   - 6.1 Expand **Groups** and click **Add**.
   - 6.2 Select a group and click **Add**.
   - 6.3 Repeat to add multiple groups. Click ✕ to exit.
7. Expand **More**:
   - Select **Suspend cardholder** if you want to suspend the cardholder.
   - Select **Long access time** if you want the cardholder to have long access time and long open-too-long time when a door monitor is configured.
   - Select **Exempt from lockdown** if you want the cardholder to have access during lockdown.
   - Select **Global cardholder** to make the cardholder can be viewed and monitored on the sub servers. This option is only available for cardholders created on the main server. See *Multi server*^{BETA} *on page 136*.
8. *Add credentials on page 143*.
9. Click **Add**.

To edit a cardholder:

1. Go to **Access management > Dashboard > Cardholders**.
2. Select a cardholder, click ⋮ and **Edit**.
3. Change the settings and click **Apply**. When you edit the cardholder, you can see recent transactions of the cardholder.

To suspend a cardholder:

1. Go to **Access management > Dashboard > Cardholders**.
2. Select a cardholder, click ⋮ and **Suspend**. A suspended cardholder is highlighted in pink.
3. To unsuspend a cardholder, select a suspended cardholder, click ⋮ and **Unsuspend**.

To send QR code to a cardholder:

For a complete workflow, see *Set up AXIS Barcode Reader*.

1. Go to **Access management** > **Dashboard** > **Cardholders**.
2. Select a cardholder, click ⋮ and **Send QR code**.
3. Click **OK**.

To delete a cardholder:

1. Go to **Access management** > **Dashboard** > **Cardholders**.
2. Select a cardholder, click ⋮ and **Delete**.
3. Click **Confirm**.

▶

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=add-a-cardholder

Add cardholders and groups

Add credentials

A credential is information that tells the system who the cardholder is. You can select to add a PIN and a card credential to a cardholder. See *Add a cardholder on page 142*

A PIN credential is always valid. You can also configure a duress PIN which allows to open the door but triggers a silent alarm in the system.

To add a license plate credential^PREVIEW^:

1. Under **Credentials**, click + and 🚗 .
2. Enter a name that describes the vehicle.
3. Enter the license plate number for the vehicle.
4. Under **Expiration date**:

   4.1 Under **Valid from**, set a date and time.

   4.2 Under **Valid to**, select an option from the drop-down list.

   - **No end date:** The credential will never expire.
   - **Date:** Set a date and time when the credential will expire.
   - **From first use:** Select how long will the credential expire after the first use. It can be a number of days, months, years or a number of times after the first use.

- **From last use:** Select how long will the credential expire after the last use. It can be a number of days, months or years after the last use.

5. Click **Add**.

To add a PIN credential:

1. Under **Credentials**, click + and PIN .
2. Enter a PIN.
3. To use a duress PIN to trigger silent alarm, turn on **Duress PIN** and enter a duress PIN.
4. Click **Add**.

To add a card credential:

1. Under **Credentials**, click + and ▭ .
2. To manually enter the card data, enter a card name, card number and bit length. Bit length is only configurable when you create a card format with a specific bit length that is not in the system.
3. To automatically get the card data of the last swiped card,
   3.1 Select a reader from the **Select reader** drop-down list.
   3.2 Swipe the card on the specified reader.
   3.3 Click **Get last swiped card data from the selected reader**.

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. Under **Expiration date**:
   5.1 Under **Valid from**, set a date and time.
   5.2 Under **Valid to**, select an option from the drop-down list.
   - **No end date:** The credential will never expire.
   - **Date:** Set a date and time when the credential will expire.
   - **From first use:** Select how long will the credential expire after the first use. It can be a number of days, months, years or a number of times after the first use.
   - **From last use:** Select how long will the credential expire after the last use. It can be a number of days, months or years after the last use.
6. Click **Add**.

To add a QR credential:

Note

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

1. Under **Credentials**, click + and ▦ .
2. Enter a name.

3. **Dynamic QR** is turned on by default. Dynamic QR must be used with PIN credential together.

4. Under **Expiration date**:

    4.1 Under **Valid from**, set a date and time.

    4.2 Under **Valid to**, select an option from the drop-down list.

    - **No end date:** The credential will never expire.

    - **Date:** Set a date and time when the credential will expire.

    - **From first use:** Select how long will the credential expire after the first use. It can be a number of days, months, years or a number of times after the first use.

    - **From last use:** Select how long will the credential expire after the last use. It can be a number of days, months or years after the last use.

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 edit a credential:

1. Go to **Access management** > **Dashboard** > **Cardholders**.

2. Select a cardholder, click ⋮ and **Edit**.

3. Under **Credentials**, select a credential. Click ⋮ and **Edit**.

4. Change the settings and click **Update** and **Apply**.

To suspend a credential:

1. Go to **Access management** > **Dashboard** > **Cardholders**.

2. Select a cardholder, click ⋮ and **Edit**.

3. Under **Credentials**, select a credential. Click ⋮ and **Suspend**.

4. To unsuspend a credential, select a suspended credential, click ⋮ and **Unsuspend**.

5. Click **Apply**.

To delete a credential:

1. Go to **Access management** > **Dashboard** > **Cardholders**.

2. Select a cardholder, click ⋮ and **Edit**.

3. Under **Credentials**, select a credential. Click ⋮ and **Delete**.

4. Click **Apply**.

Use license plate number as credentials$^{\text{PREVIEW}}$

This example shows you how to grant access using a vehicle's license plate number as credentials using a door controller and a camera with AXIS License Plate Verifier.

1. Add the door controller and the camera to AXIS Camera Station. See *Add devices on page 7*

2. Set date and time for the new devices using the **Synchronize with server computer time**. See *Set date and time on page 58*.

3. Upgrade the firmware on the new devices to the latest available version. See *Upgrade firmware on page 57*.

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 AXIS License Plate Verifier on your camera. See the *AXIS License Plate Verifier* user manual.

6. Activate the AXIS License Plate Verifier license. See the *AXIS License Plate Verifier* user manual.

7. Start AXIS License Plate Verifier.

8. Configure AXIS License Plate Verifier.

    8.1 Go to **Configuration > Access control > Encrypted communication**.

    8.2 Under **External Peripheral Authentication Key**, click **Show authentication key** and **Copy key**.

    8.3 Open AXIS License Plate Verifier from the camera's web interface.

    8.4 Skip the setup.

    8.5 Go to **Settings**.

    8.6 Under **Access control**, select **Secure Entry** as **Type**.

    8.7 In **IP address**, enter the IP address for the door controller.

    8.8 In **Authentication key**, paste the Authentication key that you copied earlier.

    8.9 Click **Connect**.

    8.10 Under **Door controller name**, select your door controller.

    8.11 Under **Reader name**, select the reader you added earlier.

    8.12 Turn on integration.

9. Add the cardholder that you want to give access to. See *Add a cardholder on page 142*

10. Add credentials to the new cardholder using the license plate option. See *Add credentials on page 143*

11. Create a new schedule. You will use this schedule to define the access rule in the next step. See .

12. Add an access rule. See *Add an access rule on page 147*.

    12.1 Add the schedule you created earlier.

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

    12.3 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. Go to **Access management** > **Dashboard** .

2. Under **Groups**, click ⊕ and 👥 .

3. Enter a name for the group.

4. Select **Global group** to make the cardholder group can be viewed and monitored on the sub servers. This option is only available for cardholder groups created on the main server. See *Multi server BETA on page 136*.
5. To add cardholders to the group:
   5.1 Under **Cardholders**, click ⊕ .
   5.2 Select a cardholder and click **Add**.
   5.3 Repeat to add multiple cardholders. Click ✕ to exit.
6. Click **Add**.

To edit a group:

1. Go to **Access management** > **Dashboard** > **Groups**.
2. Select a group, click ✎ .
3. Change the settings and click **Apply**.

To delete a group:

1. Go to **Access management** > **Dashboard** > **Groups**.
2. Select a group, click ✎ and **Delete**.
3. Click **Confirm**.

Add an access rule

An access rule defines the conditions that must be met to grant access. You can drag cardholders, groups, doors and zones to an access rule.

An access rule consists of:

- Cardholders and cardholder groups: who can be granted access.
- Schedules: when to grant access.
- Doors and zones: where the access applies to.

To add an access rule:

1. Go to **Access management** > **Dashboard** .
2. Under **Access rules**, click ⊕ .
3. Enter a name for the access rule.
4. Configure the schedules that apply to the access rule:
   4.1 Under **Schedules**, click ⊕ .
   4.2 Select a schedule and click **Add**.
   4.3 Repeat to add multiple schedules. Click ✕ to exit.
   4.4 To remove a schedule, select it and click ✕ .

5. Configure the cardholders and groups that apply to the access rule:

   5.1 Under **Cardholders** or **Groups**, click ⊕ .

   5.2 Select the cardholder or group and click **Add**.

   5.3 Repeat to add multiple cardholders and groups. Click ✕ to exit.

   5.4 Click a cardholder or group in the list to view the details.

   5.5 To remove a cardholder or a group, select it and click ✕ .

6. Configure the doors and zones that apply to the access rule:

   6.1 Under **Doors** or **Zones**, click + .

   6.2 Select the door or zone and click **Add**.

   6.3 Repeat to add multiple doors and zones. Click ✕ to exit.

   6.4 To remove a door or zone, select it and click ✕ .

7. Click **Add**.

All access rules are listed under **Access rules**. It shows the number of cardholders, groups, doors and zones in the access rule.

To edit an access rule:

1. Go to **Access management** > **Dashboard** > **Access rules**.
2. Select an access rule, click ✎ .
3. Change the settings and click **Apply**.

To delete an access rule:

1. Go to **Access management** > **Dashboard** > **Access rules**.
2. Select an access rule, click ✎ and **Delete**.
3. Click **OK**.

▶

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=add-an-access-rule

Add and configure access rules

Doors

Go to **Access management** > **Dashboard** > **Doors** to view a list of doors that have been added to the system including the door status, lock status and zones that the door is in. You can perform manual actions and configure unlock schedules on doors.

The possible actions you can perform on a door are:

- **Access:** Grant access to the door. This action is only available when a door monitor is configured.
- **Unlock:** Unlock the door.
- **Lock:** Lock the door.
- **Lockdown:** The door enters or exits a lockdown status.

To edit a door:

1. Click a door in the list and click ✎ .
2. To add unlock schedules:
   - 2.1 Under **Unlock schedules**, click ⊕ .
   - 2.2 Select a schedule and click **Add**.
   - 2.3 Repeat to add multiple unlock schedules. Click ✕ to exit.
   - 2.4 To remove an unlock schedule, select it and click ✕ .
3. You can turn on **First person in** so that the door will not unlock unless someone with access to the door has been granted access during the unlocking schedule.
4. Click **Apply**.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=doors

Turn on first-person-in rule

To perform an action on doors:

1. Select the doors in the list and click ••• .
2. Select an action to perform the action on the selected doors.

▶

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=doors

Set door state

Zones

Go to **Access management > Dashboard > Zones** to view a list of zones that have been added to the system and the zone status. You can perform manual actions and configure unlock schedules on zones.

The possible actions you can perform on a zone are:

- 🔓 **Unlock:** Unlock the door.
- 🔒 **Lock:** Lock the door.
- 🛡 **Lockdown:** The door enters a lockdown status.

To edit a zone:

1. Click a zone in the list and click ✎ .
2. To add unlock schedules:
    2.1 Under **Unlock schedules**, click ⊕ .
    2.2 Select a schedule and click **Add**.
    2.3 Repeat to add multiple schedules. Click ✕ to exit.
    2.4 Select the doors that an unlock schedule applies to. **Perimeter doors** or **Internal doors**.
3. Click **Apply**.

To perform an action on a zone:

1. Select a zone in the list and click ••• .
2. Select an action.
3. Choose to apply the action to all doors, perimeter doors or internal doors.

Export reports

You can export reports that contain different types of information about the system. The report is exported as a comma-separated value (CSV) file and saved in the default download folder.

1. Go to **Access management > Reports**.
2. Click an option, choose the export directory and click **Save**.

You can export the following reports:

- **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 that the cardholder is related to.
- **Cardholders group access report:** Includes the cardholder group name and information about the cardholders, access rules, doors and zones that the cardholder group is related to.
- **Access rule report:** Includes the access rule name and information about the cardholders, cardholder groups, doors and zones that the access rule is related to.
- **Door access report:** Includes the door name and information about the cardholders, cardholder groups, access rules and zones that the door is related to.
- **Zone access report:** Includes the zone name and information about the cardholders, cardholder groups, access rules and doors that the zone is related to.

Access management settings

To customize the cardholder fields used in the access management dashboard:

1. Go to **Access management > Settings**.
2. Click **Add custom field** and type a name. You can add at most 6 custom fields.
3. Click **Apply**.

To enable using facility code to verify your access control system:

1. Go to **Access management > Settings**.
2. Turn on **Facility code**.
3. Click **Apply**.

Note

> To use facility code for card validation, select **Include facility code for card validation** when you configure identification profiles. See *Identification profiles on page 130*.

To edit the email template:

1. Go to **Access management > Settings**.
2. Under **Email template**, change the subject and body text.
3. **Include visiting time in the email** is selected by default.
4. Click **Apply**.

Import and export

Import

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^{PREVIEW} on page 137*.

The following options are available when importing cardholder data:

- **New**: This option removes existing cardholders and adds new cardholders.
- **Add** : This option keeps existing cardholders and adds new cardholders.
  - If a cardholder ID already exists in the system, it is considered as an existing cardholder and will not be updated.
  - If a card number already exists in the system, the import will not succeed.
- **Update**: This option updates the existing cardholders and adds new cardholders.

1. Go to **Access management > Import and export**.
2. Select **Import** from the **Select action** drop-down list.
3. Select **New**, **Update**, or **Add** .
4. Configure the import settings:
   - Select **First row is header** if the CSV file contains a column header.
   - Enter a column delimiter that the CSV file is formatted with.
   - Under **Unique identifier**, **Cardholder ID** is used 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.
   - Under **Card number format**, **Allow both hexadecimal and number** is selected by default.
5. Click **Browse** and navigate to the CSV file. Click **Load**.
6. Under **Column mapping**, click ✎ and assign a heading to each column if **First row is header** is not selected.
7. If there are custom fields in the CSV file, the heading of the custom fields is shown as **Undefined**. Click ✎ and assign a heading.
8. Click **Import**.

Export

This option exports the cardholder data in the system to a CSV file.

1. Go to **Access management > Import and export**.
2. Select **Export** from the **Action** drop-down list.
3. Click **Export**.

AXIS Camera Station updates cardholder photos in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` whenever the configuration changes.

Reset

The system automatically saves its configuration when you import cardholders. The **Reset** option resets the cardholder data and all hardware configuration to the way it was before the last cardholder import.

1. Go to **Access management > Import and export**.
2. Select **Reset** from the **Action** drop-down list.
3. Click **Reset**.

System Health Monitoring BETA

Click + and select **System Health Monitoring** BETA to display the System Health Monitoring tab in the AXIS Camera Station client.

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

If you're managing systems located 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 98* for more information.

It contains the following pages:

- Inventory: Shows a summary of the devices and systems that you have access to. See *Inventory on page 153*.
- Storage: Shows that storage summary and recording details of each camera from the monitored systems. See *Storage on page 154*.
- Notifications: Shows the System Health Monitoring logs from the monitored systems. See *Notifications on page 155*.

Limitations

- Monitoring of storage space for recordings done on AXIS S3008 Recorder is not yet supported.
- Notification settings only affect the local System Health Monitoring server.
- Recordings except for continuous and motion triggered recordings are flagged with None as recording type.

Workflow

1. *Configure System Health Monitoring BETA on page 138*
   - Set up notifications. See *Notifications on page 138*.
   - Set up multisytem. See *Multisystem on page 139*.
2. Monitor the health data from AXIS Camera Station systems.
   - *Inventory on page 153*
   - *Storage on page 154*
   - *Notifications on page 155*

Inventory

The inventory page shows a summary of the devices and systems that you have access to.

1. Go to **System Health Monitoring** BETA.
2. Click **Inventory**.

- To view a summary of a system, click **AXIS Camera Station**.

  The information is displayed in the right panel including system and server details.
- To view a summary of a device in a system, click the device in the list.

The information is displayed in the right panel including device details and storage information if it contains a video source.

- To download AXIS Camera Station system report, select **AXIS Camera Station system report** from the **Create report** drop-down menu. See *System report on page 164*.
- To download System Health Monitoring report:
  1. Select **System Health Monitoring report** from the **Create report** drop-down menu.
  2. To include the database in the report, select **Include all databases** and click **Download**.
  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. Go to **System Health Monitoring** BETA.
2. Click **Storage**.
3. When monitoring multisystem health data, select a system from the drop-down list.

Item	Description
Storage summary	
Status	The storage status. See *Configure storage on page 64*.
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 delegated to recordings.
Used	The amount of storage space being currently used for recordings.
Last update	The time when the information was last updated.
Recording details of each camera	
Status	(empty): Normal status. Warning icon: Retention is not fulfilled. Info icon: Retention is not fulfilled because the camera has not recorded long enough.
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 recordings from the camera have been kept 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.

1. Go to **System Health Monitoring** BETA.
2. Click **Notifications**.

Item	**Description**
Notification sent	The time when the notification was sent.
Item	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 has 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

A hotkey gives quick access to commonly used actions. To show the Hotkeys tab, click + and select **Hotkeys** to display the Hotkeys tab in the AXIS Camera Station client. All available hotkeys are displayed and grouped into the following categories: Camera, Device management, Navigate to camera, Navigate to view, Navigation, PTZ presets, Recordings, Sequence, Tab, and Other.

No default hotkeys are assigned to the cameras and views in the Navigate to cameras and Navigate to views categories.

When a camera or view is deleted from a connected server, the associated hotkeys are also removed.

Note

- When you add or edit the hotkey of an action, if the assigned hotkey is already in use, 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 the hotkey of the conflict action is removed automatically.
- When connecting to multiple AXIS Camera Station servers, the cameras and views on the connected servers are also listed in the Navigate to cameras and Navigate to views categories.

In this tab, you can:

- **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 that is to be assigned 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.
- **Print:** Click 🖨 to print the hotkey table.
- **Reset:** Click ⟲ to reset all hotkeys to the original settings.
- **Search:** Enter the keywords in the **Type to search** field to find a hotkey or an action.

Hotkey devices

A hotkey can be:

- a keyboard combination
- a keypad combination
- a joystick button
- a jog dial button

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

Hotkey mapping - Joystick	Default action	AXIS TU9002	AXIS T8311
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/paus	⏯	-
Button 11	Jump to previous 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	📹	📹
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

Click + and select **Logs** to display the Logs tab in the AXIS Camera Station client. 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**.

Item	**Description**
Time	Date and time of the action.
Type	The type of the action: Alarm, Event, or Audit.
Category	The category of the action.
Message	A short description of the action.
User	The AXIS Camera Station user that performs the action.
Computer	The computer (Windows domain name) on which AXIS Camera Station is installed.
Window user	The Windows user that administers AXIS Camera Station.
Server	Only available when connecting to multiple AXIS Camera Station 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 will search in the log list except for the Time column and show the search results that contain all the keywords. For supported search operators, see *Optimize your search on page 38*.
3. Select the log types from **Alarms**, **Audits**, and **Events**.
4. Select a date or a range of dates from the calendar.
5. Select the start time and end time from the drop-down lists of the **Start time** and **End time** fields.
6. Click **Search**.

Alarms log

The Alarms log displays system alarms and alarms generated by rules and motion detection. Listed are the date and time of the alarm, alarm category and an alarm message. See *Alarms*.

Select an alarm and click:

- **Go to Recordings** to open the Recordings tab and start playback when the alarm contains a recording.
- **Show Alarm procedure** to open the alarm procedure when the alarm contains an alarm procedure.
- ✓ **Acknowledge Alarms** to notify other clients that the alarms have been taken care of.
- **Export log** 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. Listed are 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

The Audit log displays 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 the AXIS Camera Station client. It shows 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*.

The Alarms tab displays the following information:

- **Time:** The time the alarm occurred.
- **Category:** The category of the triggered alarm.
- **Description:** A brief description of the alarm.
- **Server:** Available when connecting to multiple AXIS Camera Station servers. The AXIS Camera Station server that sends the alarm.
- **Component:** The component that triggers the alarm.
- **Show alarm procedure:** Available when the alarm contains an alarm procedure.
- **Go to recordings:** Available when the alarm contains a recording.

To deal with a specific alarm:

1. Click **Alarms and Tasks** at the bottom of the AXIS Camera Station client, and click the Alarms tab.
2. For alarms with a recording, select the alarm and click **Go to Recordings** to navigate to the recording in the Recording alerts tab.
3. For alarms without a recording, double-click the alarm from a tab with camera view to navigate to the specified time in the Recording alerts tab with the camera view.
4. For alarms with an alarm procedure, select the alarm and click **Show alarm procedure** to open the alarm procedure.
5. To notify other clients that the alarms have been taken care of, select the alarms and click ✓ **Acknowledge selected alarms.**
6. To remove the alarms from the list, select the alarms and click **Clear selected alarm entries.**

Tasks

The Tasks tab is available at the bottom of the AXIS Camera Station 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 are not 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.

The Tasks tab displays the following information:

Item	Description
Name	The name of the task.
Start	The time when the task was started.
Message	Shows the status of the task or the information about the task. The possible status: • **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 connection to the server was down. Task status could not be determined. • **Lost connection:** Displayed if the client lost connection with the server while the task was running. Task status could not be determined. • **Running:** Performing the task. • **Pending:** Waiting for another task to be completed.
Owner	The user who initiated the task.
Progress	Shows how much of the task is left to be completed.
Server	Available when connecting to multiple AXIS Camera Station servers. The AXIS Camera Station server that performs the task.

To deal with one or more tasks:

1. Click ^ **Alarms and Tasks** at the bottom of the AXIS Camera Station client, and click the Tasks tab.
2. Select the tasks,

   - Click ◆ **Show** to display the Task result dialog.
   - Click ⊘ **Cancel** to cancel the task.

Tasks

- Click **Remove** to delete the tasks from the list.
- If the task fails when exporting recordings or creating incident report, click **Retry** 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 where the files are saved.

Item	Description
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 task performed, 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

Go to ≡ > **Help** > **Client configuration sheet** to compile a report in HTML format with an overview of the client system configuration. This is useful for troubleshooting and when contacting support.

Server configuration sheet

Go to ≡ > **Help** > **Server configuration sheet** and select a server to compile a report in HTML format with an overview of the server system configuration. The report includes information about general configuration, cameras settings including action rules, schedules, recording storage, auxiliary devices, and licenses. This is useful for troubleshooting and when contacting support.

System report

The system report is a .zip file containing parameters and log files that will help Axis Customer Support to analyze your system.

Always include a system report when contacting Customer Support.

1. Go to ≡ > **Help** > **System report** to generate the system report.
2. The file name is automatically generated. Edit the file name if you want to change.
3. Click **Browse** to select where to save the system report.
4. Select the following:
   - Select **Automatically open folder when report is ready** to automatically open the folder when the system report is ready.
   - Select **Include all databases** to include the database in the system report. The AXIS Camera Station database contains information about recordings and data that is needed for the system to work properly.
   - Select **Include screenshots of all monitors** to include screenshots in the system report. Screenshots of all the monitors can make it easier to analyze the system report.
5. Click **OK**.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=system-report

Generate a system report

AXIS Installation Verifier

AXIS Installation Verifier enables 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.

AXIS Installation Verifier tests:

- **Normal conditions:** Test of data streaming and data storage using the current system settings in AXIS Camera Station. 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

- Only devices that support AXIS Camera Application Platform 2 (ACAP 2) and later can be tested.
- During the test, AXIS Camera Station is placed in maintenance mode, and all surveillance activities are temporarily unavailable.

To enable the test:

1. Go to ≡ > **Help** > **Installation Verifier**.
2. Click **Start**.
3. When the test is completed, click **View report** to view the report or click **Save report** to save it.

Feedback

If you have selected to share anonymous client usage data when you *Configure client on page 93*, you can send your feedback to help us improve AXIS Camera Station and your user experience.

Note

The feedback form is not a form for submitting support requests.

1. Go to ≡ > **Help** > **Feedback**.
2. Choose a reaction and fill in your feedback.
3. Click **Send**.

Asset list

You can export a list of assets for your AXIS Camera Station 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 connecting 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. In the **Latest export** field, a link to the file is generated or updated. Click the link to go to the file location.

Body worn settings

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

Note

> Before you export the connection file, you must renew the server certificate first if the IP address of the server has changed or AXIS Camera Station is upgraded from a version earlier than 5.33. For how to renew the certificate, see *Certificates on page 112*.

To create a connection file,

1. Go to ≡ > **Other** > **Body worn settings**.

2. To change the default site name displayed in your body worn system, type a new name.

3. Click **Export**. A link is displayed under **Latest export**.

4. Click the link to navigate to the connection file folder.

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=body-worn-settings

Set up an Axis body worn system

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=34074&section=body-worn-settings

Playback and export Axis body worn camera recordings

Status of Axis services

1. Go to ≡ > **Help** > **Status of Axis services**.
2. The status of Axis services page is opened in a web browser. You can view the status of Axis online services.

AXIS Camera Station Service Control

AXIS Camera Station Service Control is used to start and stop the AXIS Camera Station server and to change server settings. It automatically starts after the installation is complete. If the server computer restarts, AXIS Camera Station Service Control will automatically restart in about 2 minutes.

An icon in Windows notification area shows if the service is running , is starting or has stopped .

Right-click the icon, and you can select **Open AXIS Camera Station Service Control**, **Start Service**, **Stop Service**, **Restart Service**, or **Exit**.

Open AXIS Camera Station Service Control

- Double-click the icon in Windows notification area.
- Right-click the icon in Windows notification area and select **Open AXIS Camera Station Service Control**.

Depending on the operating system, AXIS Camera Station Service Control can also be opened in the following ways:

- Go to the **Start** screen or **Start** menu and type "Service Control".
- Go to the **Start** menu and select **All Programs** > **AXIS Camera Station** > **AXIS Camera Station Tools** > **Service Control**.

Basic settings

In AXIS Camera Station Service Control:

- Select **Modify settings** to enable changing the server settings.
- Click **Restore Default Settings** to restore all settings to the original default settings.
- The Server status section shows the status of the server. Click **Start** or **Stop** to change the server status. Click **Restart** to restart the server.

General

In AXIS Camera Station Service Control, select **Modify settings** and click the General tab to change the general server settings.

Server certificate ID

The server certificate ID. It is used to manually verify that the client is connecting to the correct server.

Server settings

- **Server name:** The name of the server. The server name is displayed in the AXIS Camera Station client. The default server name is the computer name.

Note

When the computer name is changed, the server name will remain unchanged.

- **Ports range:** Specify the range of ports. The following ports will be changed 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 components: After you specify the port range, the ports that can be used by the components are listed. The default port range for AXIS Camera Station components is 55760 - 55764.
- To view the full port list, see *Port list on page 169*.

Note

- If there is a NAT, firewall or similar between the server and the client, the NAT and/or firewall must be configured to allow these ports to pass through.
- The port numbers must lie within the range 1024-65534.

Proxy settings

These settings apply to a proxy server between the AXIS Camera Station server and the cameras in the system.

- **Direct connection:** Select this option if there is no proxy server between the AXIS Camera Station 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 the AXIS Camera Station server and any cameras in the system are separated by a proxy server. 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 not to 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 does not need to pass through the proxy. Wildcards can be used in the address or hostnames, for example: "192." or ".mydomain.com".

Port list

The following tables identify ports and protocols used by AXIS Camera Station that you may need to enable on your firewall for optimum performance and usability. In the tables, we calculate port numbers based on the default HTTP main port 55752.

AXIS Camera Station 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 may be because it is being used by another application which refuses to share it. In that case a random port will be tried until a working one is found. When using a random port

				devices with link-local addresses will not be discoverable using Bonjour.
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 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 servers with SSDP (UPNP). Multicast 239.255.255.250.
Main HTTP port and HTTP streaming port	55752	TCP	Inbound	Server and client	Used for video, audio, metadata stream (AES encryption). If TCP fails on 55754, 55752 with HTTP is used for application data (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 server discovery with SSDP/UPNP.
API web server port	55756	TCP	Outbound	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	Outbound	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 (ServerPortParser). +2 offset from API web server port (RemoteFacade-Binder). Only accessible internally on the AXIS Camera Station 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.

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 Service Control listens on the port, and the server broadcasts the status of an ongoing upgrade.

Reserved ports for components

AXIS Camera Station Service Control

Component	Port	Number	Protocol	In/Out	Communication between	Description
System Health Monitoring	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.
Smart search 2	Web server port	55770	HTTPS	Inbound	Client (Smart search tab) and component	+18 offset from main HTTP port. Used to host Smart Search API and serve client web page.
Secure Entry	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	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.
		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
Local-IAM (IDP)	IDP_OIDC (Public)	55784	HTTPS	Inbound	Reverse proxy and local-iam	+32 offset from main Http port. Public port
Local-IAM (IDP)	MTLS (Admin)	55785	HTTPS	Inbound	Third party services	+33 offset from main Http port. Administrator port
Local-IAM (IDP)	TOKENIZER	55786	HTTPS	Inbound	Third party services	+34 offset from main Http port. Tokenizer port

Database

Database files

Core database files

The AXIS Camera Station core database files are located under `C:\ProgramData\AXIS Communication\AXIS Camera Station Server`.

- For versions earlier than 5.13, there is only one database file **ACS.FDB**.
- For 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**. This file is required by AXIS Camera Station to display the recordings in the timeline during playback.

Component database files

- **SecureEntry.db** - The AXIS Secure Entry database file contains all access control data except cardholder photos. It is located under `C:\ProgramData\Axis Communications\AXIS Camera Station Secure Entry Service`.
- **smartSearch.sqlite3** - The AXIS Camera Station smart search database file contains camera configuration and saved search filters. It is located under `C:\ProgramData\Axis Communications\AXIS Smart Search\data`.

Database settings

The database is backed up every night and before each system upgrade. In AXIS Camera Station Service Control, select **Modify settings** and click the Database tab to change the backup settings.

- **Backup folder:** Click **Browse** and select the folder to save the database backups. Restart the AXIS Camera Station server to apply the change.
  - If the backup folder path is incorrect, the backup will be saved to `C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup` by default.
  - If AXIS Camera Station has no access to the network share, the backup will be saved to `C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup` by default.

- **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 the events that happened since last restart of AXIS Camera Station Service Control.

Back up database

The database contains information about recordings and other metadata that is needed for the system to work properly.

Important

- Recordings are stored in the location specified under **Configuration > Storage** and not in the database. Recordings should be backed up separately.
- Server settings, proxy settings and database settings in AXIS Camera Station Service Control are not saved.

System backup

The system backups are triggered automatically and stored in the backup folder specified in the *Database settings on page 173*.

A system backup includes both the core database files and the component database files. See *Database files on page 173*.

The following backup files are available depending on the trigger:

- **System_YYYY-MM-DD-HH-mm-SSSS.zip**: The backup is triggered every night.
- **PreUpgrade_YYYY-MM-DD-HH-mm-SSSS.zip**: The backup is triggered before a database update.
- **User_YYYY-MM-DD-HH-mm-SSSS.zip**: The backup is triggered before a storage is removed.

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-yyyyMMddHH-mmssfff.sqlite3**.
- **Backup_Summary.txt**: This files includes more detailed information about the backup.

Maintenance backup

The maintenance backups are stored in the backup folder specified in the *Database settings on page 173*.

A maintenance backup includes only the core database files with each database file in a separate folder **PreMaintenance_YYYY-MM-DD-HH-mm-SSSS**.

It can be triggered:

- Automatically when you update your AXIS Camera Station.
- When you run database maintainer manually from AXIS Camera Station Service Control. See *Database maintenance on page 176*.
- Automatically by the scheduled database maintenance task configured in Windows Task Scheduler. See *Tools on page 176*.

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.

You can do a manual backup after some important changes in one of the following ways:

- Go to `C:\ProgramData\AXIS Communication\AXIS Camera Station Server` and make a copy of the database files.
- Generate a system report with all databases included.

    1. In the AXIS Camera Station client, go to ≡ > **Help** > **System report**.
    2. Enter the file name and select a folder.
    3. Select **Include all databases**.
    4. In the system report folder, go to the Server folder and find the database backup files.

Restore database

If the database is lost due to hardware failure or other problems, the database can be restored from one of the saved backups. By default, backup files are kept for 14 days. For more information about database backup, see *Back up database on page 174*.

Note

Recordings are stored in the location specified under **Configuration** > **Storage** and not in the database. Recordings should be backed up separately.

To restore the database:

1. Go to AXIS Camera Station Service Control and click **Stop** to stop the service.
2. Navigate to the database backup files. See *Back up database on page 174*.
    - To restore from an automatic backup, go to the backup folder specified in *Database settings on page 173*, select a timestamped zip file and extract it.
    - To restore from a manual backup, go to the folder where you put the copy of database files.
3. In the extracted folder, copy the following database files under `ACS` to `C:\ProgramData\AXIS Communication\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.
4. If you use AXIS Camera Station Secure Entry, copy **SecureEntry.db** from `Components > ACMSM` to `C:\ProgramData\Axis Communications\AXIS Camera Station Secure Entry Service`.
5. If you use smart search, copy **smartSearch-backup-yyyyMMddHHmmssfff.sqlite3** from `smartsearch` to `C:\ProgramData\Axis Communications\AXIS Smart Search\data` and rename it to **smartSearch.sqlite3**.
6. Go back to AXIS Camera Station Service Control and click **Start** to start the service.

Database maintenance

Database maintenance should be performed if the alarm `Database maintenance is required` is displayed or if the system was shut down unexpectedly, for example after a power outage.

To start database maintenance:

1. Open AXIS Camera Station Service Control.
2. Click the Tools tab.
3. Click **Run** under **Database maintainer**.
4. The estimated downtime will be displayed. Click **Yes** to continue. Once started, the process can't be canceled.

Note

- The AXIS Camera Station server and all ongoing recordings are stopped during maintenance. After maintenance, the server is started 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.

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 check for damaged sectors on the hard drive where the database is located. To start chkdsk, go to Windows Start screen (Windows 8) or Start menu and type "chkdsk" in the search field. Run chkdsk regularly.

Antivirus software and external backups – Exclude the database from virus scans because some antivirus software can corrupt the database. If you use an external backup system, do not back up the current and active database. Back up the files located 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 the AXIS Camera Station server on a dedicated computer with sufficient memory. For hardware requirements, see the Installation Guide or www.axis.com

Corrupted RAM memory – Run Windows Memory Diagnostic regularly to check for errors in the RAM memory.

Tools

In AXIS Camera Station Service Control, select **Modify settings** and click the Tools tab to start database maintenance and create partial system reports.

Database maintainer

Click **Run** to start database maintenance. Read the popup message and click **Yes** to start maintenance or click **No** to cancel. During maintenance, the AXIS Camera Station server and all ongoing recordings are stopped. The estimated downtime will be displayed before maintenance is started. After maintenance, the server will be restarted automatically.

Database maintenance should be performed if the alarm "Database maintenance is required" is displayed or if the system was shut down unexpectedly, for example after a power outage.

Database maintenance can also be scheduled to run automatically by enabling "AXIS Camera Station Database Maintenance Task" in Windows Task Scheduler. The task trigger can be edited to customize when and how often the database maintainer should be run.

AXIS Camera Station Service Control

Note

- Once started, maintenance can't be canceled.
- Do not turn off the computer during maintenance.

System report

The partial system report is a .zip file containing parameters and log files that helps Axis Customer Support to analyze your system. Always include a system report when contacting Customer Support.

To generate a partial system report:

1. Click **Run**.
2. In the popup dialog:
   - Enter a file name for the system report in the **File name** field.
   - Select where to save the system report in the **Folder** field.
   - Select **Automatically open folder when report is ready** to automatically open the folder when the system report is ready.
   - Select **Include database file in report** to include the database in the system report. The AXIS Camera Station database contains information about recordings and data that is needed for the system to work properly.
3. Click **Generate report**.

To generate a complete system report, go to ☰ **> Help > System report** in the AXIS Camera Station client.

Network logging

Click the link to download a network protocol analyzer application. Once installed, you can click **Start** to start the application directly.

Troubleshooting

About this guide

This guide is a collection of issues related to AXIS Camera Station and how to troubleshoot them. The issues are stored under 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. Troubleshooting can sometimes be to reproduce the problem in order to find your solution.

Learn more

Visit *axis.com/support* for

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

AXIS Camera Station user manual can be found here: *AXIS Camera Station user manual*

The AXIS Camera Station service

The AXIS Camera Station service restarts often

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

- Check the resource management of your system to verify if AXIS Camera Station or any other application is using a high number of resources.
- Run the database maintainer, go to *Tools* in the AXIS Camera Station user manual.
- If none of above helps, escalate the issue to Axis Support. Go to *Escalation process on page 191*.

Devices in AXIS Camera Station

Common issues

Can't contact the camera	
AXIS Camera Station can't contact the camera. The listed cameras are not added.	• Check that the camera is connected to the network, that power is connected, and that the camera is up and running. • Go to **Configuration > Add devices** and try to add the camera again.
Installation was canceled	
The installation was canceled by the user. The listed cameras are not 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.	• To set the password manually, go to **Configuration > Devices > Management**. • 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 being added to AXIS Camera Station, a factory default of the device might be required

- If the device still can't be added to AXIS Camera Station, try to add the device to AXIS Device Manager.

It's possible to add another device model.

- 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 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

If it's not possible to upgrade the camera from its webpage:

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

Firmware can't be upgraded for all devices:

- Check the network connection.
- If it's not a network related issue, escalate to AXIS Support. Go to *Escalation process on page 191*.

Firmware can't be upgraded for specific models:

- This can happen for new products and strange firmware.
- Escalate the issue to AXIS Support. Go to *Escalation process on page 191*.

No devices found

AXIS Camera Station automatically searches the network for connected cameras and video encoders but can't find any cameras.

- Check that the camera is connected to the network and that power is applied.
- If the client, server, or cameras are located on different networks, then proxy and firewall settings might need to be configured.
  - Change the client proxy settings if the client and the server are separated by a proxy server. Go to *Client proxy settings* in the AXIS Camera Station user manual.
  - Change the NAT or security system if the client and the server are separated by a NAT or security system. Ensure that the HTTP port, TCP (Transmission Control Protocol) port and streaming port specified in AXIS Camera Station Service Control are allowed to pass through the security system or NAT. To view the full port list, see *Port list* in the AXIS Camera Station user manual.
  - Change the server proxy settings if the server and the devices are separated by a proxy server. Go to the Proxy settings section in *Service control general* in the AXIS Camera Station user manual.
- To add cameras manually, go to *Add devices* in the AXIS Camera Station user manual.

Repeated message "Reconnecting to camera in 15 seconds"

This might indicate that:

- The network is overloaded.
- The camera is not accessible. Check that the camera is still connected to the network and that power is applied.
- 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 by optimizing profile settings for low bandwidth.

Recordings

See *Live view on page 182* for more information about possible performance issues influencing recordings and playback.

Common issues

Continuous recording is not enabled	
Continuous recording is not enabled for the listed cameras.	• To enable continuous recording, go to **Configuration > Recording and events > Recording method**. • Select the camera and turn on **Continuous**.

Can't record on the specified drive	
The recording storage (local storage or network storage) can't be configured.	• To use a different storage, go to **Configuration > Storage > management**. • Add the storage and configure the storage settings for the cameras that should record to the storage.

Fail to install the AXIS Video Content Stream application	
This error message is displayed if the application can't be installed on a camera that supports AXIS Video Content Stream.	• To install the application manually: • Go to **Configuration > Devices > Management**. • Right-click the camera and select **Install camera application**.

Recording doesn't start

Recordings don't start or stop after a few seconds.

It could be that the disk is full or that there is too much intruding data.

- Check the "Camera Recording Storage" in the Server Configuration Sheet to make sure there is free space and no intruding data.
- Increase the storage limit for AXIS Camera Station.
- Allocate more storage to the storage pool. Go to *Configure storage* in the AXIS Camera Station user manual.

Recording gaps during continuous recording

Along with gaps, AXIS Camera Station alarms show "Recording errors".

The gaps can occur for several reasons, such as:

- Server overload
- Network issue
- Camera overload

- Disk overload

Check if the recording gaps happen on all the cameras.

If it doesn't happen to all the cameras, check if the camera is overloaded. Questions that will help to sort things out:

- 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 happen?

Possible solutions:

- In the task manager or the resource manager of your server machine, you can confirm if one of the hardware resources is used more than normal. If the disk shows signs of overuse, we advise adding more disks and move several cameras to record on the new disks.
- You can also reduce the amount of data written on the disk (Video settings, ZIP stream, FPS, resolution). Keep in mind the throughput estimated by *axis.com/support/tools/axis-site-designer*.

For more information, see *Live view and playback performance on page 182*.

Can't play exported recordings

If Windows Media Player doesn't play your exported recordings, check the file format. Exported recordings can be played using Windows Media Player (.asf files) and AXIS File Player (.asf, .mp4, .mkv). For more information, see *Play and verify exported recordings* in the AXIS Camera Station user manual.

Note

The player will automatically open all recordings that are in the same folder as the player.

AXIS File Player is a free software for video and audio playback. You can select to include it with the exported recordings, no installation is required. To play recordings, open AXIS File Player and select the recordings to play.

Recordings disappear

Recordings are only saved for a specified number of days. To change the number of days, go to **Configuration > Storage > Selection**.

If the storage becomes full, recordings will be deleted 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 reserved for AXIS Camera Station. 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. Go to **Configuration > Devices > Stream profiles**.
  - Use Zipstream to additionally decrease the size of the recordings. Go to **Configuration > Devices > Stream profiles**.

Failover recording issues

The failover recording is not recording on the server after the connection is restored.

Possible causes:

- The bandwidth between the camera and the server is insufficient for the recording to be transferred.

- The camera was not recording to the SD card during the disconnection.
  - Check the camera's server report. See *axis.com/support/troubleshooting*.
  - Make sure that the SD card is working fine and there is recording on it.
- The camera time has changed or shifted since the disconnection.
  - Make sure that the NTP is synchronised correctly for future recordings.
  - Synchronize the camera's time with the server or setup the same NTP server on the camera as on the server.

The failover recording implementation in AXIS Camera Station is not designed to handle the following use cases:

- 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 client.

Client hardware	
Verify that the graphic card's or network adapter's driver is up to date	• Open the DirectX Diagnostic Tool (search for dxdiag on the computer) • Check on the manufacturer's website if the driver is the latest for this OS. • Check that the client and server are running on the same machine. • Try to run the client on a dedicated computer.
Verify the number of monitors	With an internal graphic card, no more than two monitors per graphic card is recommended. • Open the DirectX Diagnostic Tool (search for dxdiag on the computer) • Check if the dedicated graphic card is support, see *axis.com/products/axis-camera-station/hardware-guidelines*. • It is not supported for the client to use a virtual machine.

Connected devices	
Many clients connected at the same time	• Ask the customer for their typical use case. • Make sure the system meets the user's requirements and are according to the hardware guidelines. See *axis.com/products/axis-camera-station/hardware-guidelines*.
The camera is connected to another VMS than AXIS Camera Station	Disconnect the camera from the other client and restart it (sometimes defaulting off the camera is necessary).
Many different streams being used from the same camera, especially high resolution	• Could be a problem especially for some M-Line cameras. • Stream with same streaming profile or lower resolution. See *Streaming profiles* in the AXIS Camera Station user manual.

Server overload	
Abnormal CPU/RAM usage corresponding to the same time as the issue	Make sure no other CPU/RAM consuming application is running at the same time.

Network issue	
Abnormal bandwidth usage corresponding to the same time as the issue	Make sure no other bandwidth consuming application is running at the same time.
Enough bandwidth / Remote or local network	• Check network topology. • Health check on any network device (switch/router/network adapter/cable) in use between cameras, server and client.

No video in live view

Live view does not display video from a known, good camera.

- Try to turn off hardware decoding. Hardware decoding is enabled by default, go to Hardware decoding in *Streaming* in the AXIS Camera Station user manual.

Other possible solutions:

- Is it possible to see a live view stream through web interface of the camera? Is the camera's homepage working fine?
  - If not, troubleshoot the camera, go to *axis.com/support/troubleshooting*.
- Create a camera server report, go to *axis.com/support/troubleshooting*.
- Check if any antivirus software is installed, it might be blocking live streams.
- Allow AXIS Camera Station folders and processes, see *FAQ*.
- Make sure the firewall is not blocking connections on certain ports, see *FAQ*.
- Make sure the desktop experience is installed for supported Windows server OS versions. See *Scheduled export* in the AXIS Camera Station user manual.
- Check if the lower resolution stream works.

If none of the above helps

- Escalate the issue to AXIS support, go to *Escalation process on page 191*.

Storage

Network storage is not accessible

If the local system account is used to log in to AXIS Camera Station Service, you can't add network storage linking to shared folders on other computers.

To change the service logon account:

1. Open **Windows Control Panel**.
2. From the System & Security category, select **Administrative Tools > Services**.
3. Right-click AXIS Camera Station and select **Properties**.
4. Click the **Log on** tab.
5. Change from **Local System account** to **This account**.
6. Select a user with access to Windows Active Directory.

Network storage is unavailable

The computer that the AXIS Camera Station server is installed on should be 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 is 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. When your network storage is disconnected, 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	
AXIS Video Motion Detection 2 or 4 can't be installed. The built-in motion detection will be used for motion recording.	To install the application manually, go to *Install camera application* in the AXIS Camera Station user manual.

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

Motion detection not configured	
Motion detection can't be configured in the listed cameras.	• To configure motion detection manually, go to **Configuration > Recording and events > Recording method**. • Select the camera and click **Motion settings** to configure motion detection.

Motion detection is not enabled	
Motion recording is not enabled for the listed cameras.	• To enable, go to **Configuration > Recording and events > Recording method**. • Select the camera and turn on **Motion detection** to enable motion detection recording.

The motion detection detects too many or too few moving objects

This section describes possible solutions if you expected more or fewer detections in your Video Motion Detection related recordings.

Adjust motion settings

The area where moving objects are detected can be adjusted by selecting motion settings.

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: The area of interest can be adjusted. See *Edit AXIS Video Motion Detection 2 and 4* in the AXIS Camera Station user manual.
   - Built-in motion detection: Included and excluded windows can be configured. See *Edit built-in motion detection* in the AXIS Camera Station user manual.

Adjust trigger period

The trigger period is an interval time between two successive triggers, this setting is used to reduce the number of successive recordings. The recording will continue 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 and use the slider to adjust **Trigger period**.

Audio

No audio in live view

If there is no audio in live view, check the following:

- Check that the camera has audio capabilities.
- Check that the computer has an audio card and that the card is enabled.
- Check that the profile in use is configured for audio (see below).
- Make sure the user has access rights to audio (see below).

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. Select a microphone under **Microphone** in the audio settings.
5. Select when to enable audio under **Use microphone for** in the audio settings. Audio can be applied for **Live view and recording**, **Live view only**, or **Recording only**.
6. If applicable, select a speaker under **Speaker** in the audio settings.
7. Click **OK**.

Check and change user access rights

Note

To follow these steps you must have administrator rights to AXIS Camera Station.

1. Go to **Configuration > Security > User permissions**.
2. Select the User or Group and click **Edit**.

3. Click **Advanced**.
4. Select **Audio**.
5. Click **OK**.

No audio in sequences

Audio can be disabled in streaming profiles. For more information, see *Stream profiles* in the AXIS Camera Station user manual.

1. Go to **Configuration > Devices > Stream profiles**.
2. Select the camera.
3. Make sure that audio is enabled in the profile used for the first view in the sequence. This profile is used for all views in the sequence.

No audio in playback

Audio is available in playback if audio was enabled in the profile used for the recording.

Note

Audio can't be used with M-JPEG video. Select another video format.

To enable audio in recordings:

1. Ensure the video profile you want to use has been set with MPEG-4 or H.264 format.
   1.1 Go to **Configuration > Devices > Stream profiles**.
   1.2 Select the camera.
   1.3 For the video profile that you want to use, select **MPEG-4** or **H.264** from the **Format** drop-down list.
   1.4 Click **Apply**.
2. Go to **Configuration > Recording and events > Recording method**.
3. Select the camera.
4. Select the profile with MPEG-4 or H.264 from the **Profile** drop-down list.
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. In step Actions, select the Record action and click **Edit**.
4. Select a profile where audio is enabled.
5. Click **Finish** to save.

Login

Unable to log in or connect to server

This section describes login and connection problems that occur when connecting to a single server. When logging in to multiple servers the client will start and the connection status will be shown in the status bar. For more information about the connection status, see *Connection status* in the AXIS Camera Station user manual.

The username or password is incorrect	The username and password combination is not valid to log in to the specified server.	• Check the spelling or use a different account. • Check that the user has access rights to the AXIS Camera Station server. • Check that the clocks in the AXIS Camera Station server and client are synchronized. For domain users, also check that the domain server clock is synchronized with the server and client. • A user who has not been 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 the AXIS Camera Station user manual.
User is not authorized to log in to the server	The username is not authorized to use AXIS Camera Station 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.	Make sure server and client UTC times are 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 is connected to the network. • Make sure the server computer is running. • Make sure the firewall is properly configured. • Check the spelling of the server address. • Check the client proxy settings.
No response from the server	The client is able to contact the server computer but no AXIS Camera Station server is running.	Make sure that you are connecting to the right computer and that the AXIS Camera Station server is running.
Client can't connect to the server	The client is not able to connect to the server and an error message is displayed.	Make sure that your network is properly configured: • Verify that the OS is supported. - Check the AXIS Camera Station *release note* for a full list of supported OS. • Verify that AXIS Camera Station server is running. - Start the server from Service Control. • 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. • Check if there is a proxy server between the server and the client. - Configure the server proxy in Service Control. • Check if there is a proxy server between the server and the client. Configure the client proxy settings. - At the log in page, in the left lower corner, select **Change proxy settings**.

		- Or configure it in the 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.	• Check that the address and port of the AXIS Camera Station server are correct. • Check that there is no NAT, firewall or antivirus software blocking the connection to the server. • Use AXIS Camera Station Service Control to check that the server is running. - Open the Service Control by double-clicking the icon in Windows notification area. See *AXIS Camera Station Service Control* in the AXIS Camera Station user manual. - The server status is displayed in the General tab. If status is "Stopped", click **Start** to start the server.
Unable to find the server	The client is not able to resolve the address entered to an IP address.	• Check that the server computer is connected to the network. • Check that the address and port of the AXIS Camera Station server are correct. • Check that there is no NAT, firewall, or antivirus software blocking the connection to the server.
The server and client version differs	The client is running a newer version of AXIS Camera Station than the server.	Upgrade the server to run the same version as the client.
The server and client version differs	The server is running a newer version of AXIS Camera Station 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 is not able to respond because of performance issues.	Make sure that the server computer and the network is not overloaded.
The local AXIS Camera Station server is not started	You tried to connect using **This computer** but the installed AXIS Camera Station server is not running.	Start AXIS Camera Station using the Service Control in the system tray or select a remote server to log in to.
AXIS Camera Station server is not installed on this computer	You tried to connect using **This computer** but there is no server installed on this computer.	Install the AXIS Camera Station server or choose a different server.
The selected server list is empty	The server list selected for login was empty.	Add servers to the server list by clicking the **Edit** link next to the server list selection.

Licenses

License registration issues

If automatic registration fails, try the following:

- Check that the license key has been entered correctly.
- Change the client proxy settings to allow AXIS Camera Station to access the internet.
- Select the option **The server is not connected to the internet**.
- Make a note of the Server ID and activate AXIS Camera Station from *axis.com/licenses/systems*.
- Make sure that the server's time is up to date.

For more information, see *axis.com/products/axis-camera-station/license*.

Users

Can't find domain users

If the domain user search fails, change the Service logon account:

1. Open **Windows Control Panel**.
2. From the System & Security category, select **Administrative Tools** and then **Services**.
3. Right-click AXIS Camera Station and select **Properties**.
4. Click the **Log on** tab.
5. Change from **Local System account** to **This account**.
6. Select a user with access to Windows Active Directory.

Certificate errors

AXIS Camera Station can't communicate with the device until the certificate error is solved.

The certificate errors can be:

Certificate Not Found – if the device certificate has been removed. If you know why the certificate was removed, click **Repair** to repair the certificate. If you suspect unauthorized access, investigate the issue before clicking the button. Click **Advanced** to display certificate details. The certificate could have been removed because:

- The device was reset to factory default.
- Secure HTTPS communication has been disabled.
- An unauthorized person has accessed and modified the device.

Untrusted Certificate – if the device certificate has been modified outside of AXIS Camera Station. This can indicate that an unauthorized person has accessed and modified the device. If you know why the certificate was modified, click **Trust This Device**. If not, investigate the issue before clicking the button. Click **Advanced** to display certificate details.

Missing passphrase for certificate authority

If you have a certificate authority in AXIS Camera Station and no passphrase is stored with it, you will get an alarm:

You need to provide a passphrase for the Certificate Authority certificate. Read the AXIS Camera Station User Manual for more information.

You can resolve this issue in three different ways:

- Enable HTTPS on a device
- Import an existing certificate authority
- Let AXIS Camera Station generate a new certificate authority

To enable HTTPS on a device:

1. Open a **Configuration** tab.
2. Go to **Devices** > **Management**.

3. In the list, right-click and device and go to **Security** > **HTTPS** > **Enable/Update**.
4. Click **Yes** to confirm.
5. Enter the certificate authority passphrase. And click **OK**.

To import an existing certificate authority:

1. Open a **Configuration** tab.
2. Go to **Security** > **Certificates**.
3. Click **Import...**.
4. Click **OK** to confirm that you want to replace your existing certificate authority.

Note

AXIS Camera Station loses its connection to the devices, and some system components restart.

5. Locate and open your existing certificate authority.
6. Enter the certificate authority passphrase. And click **OK**.

To let AXIS Camera Station generate a new certificate authority:

1. Open a **Configuration** tab.
2. Go to **Security** > **Certificates**.
3. Click **Generate...**.
4. Click **OK** to confirm that you want to replace your existing certificate authority.

Note

AXIS Camera Station loses its connection to the devices, and some system components restart.

5. Create a new certificate authority passphrase. And click **OK**.

Time synchronization

Windows time service isn't running

The Windows Time service is not synchronized with the NTP server. This can be because it can't reach the NTP server. Make sure that:

- The NTP server is online.
- The firewall settings are correct.
- The device is on a network that can reach the NTP server.

For assistance, contact your system administrator.

Detected a time difference of {time} on {device}

The device is out of synchronization with the server time.

1. Go to **Configuration > Devices > Time synchronization** and check the server time offset of the device.
2. If the server time offset is more than 2 seconds:

   2.1 Make sure that **Enable time synchronization** is selected.

    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.

    3.2 The device is not properly synchronized with the server. The recording is time stamped with the time when the server received it instead of the time of when the device recorded it.

For assistance, contact Axis support.

Technical support

Technical support is available for customers with a licensed version of AXIS Camera Station. 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*. In order for the support to understand your issue and be able to solve it is necessary to include the following information:

- A clear description on how to reproduce the issue or under what circumstances does the issue happen.
- The TIME and the concerned camera's name or IP address when the issue happens.
- AXIS Camera Station system report generated directly after the issue happens.
- Make sure the system report is generated from the client or server where the issue has been reproduced.
- Live view related: Enable the **Include screenshots** option of all monitors in the **Generate System Report** dialog.
- Only include the database files if needed, excluding will speed up uploading.

Sometimes additional information is required and will be requested by the support team.
Supply the following information if requested:

Note

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

Debug logs – Sometimes we must turn on debug level logging to collect more information. This is only done by request from Axis Product Specialists. Instructions can be found in this *FAQ*.

Live view debug overlay – Sometimes it is beneficial to provide screenshots of the overlay information or a video showing 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 product specialist, the following information should be generated at the same time as when AXIS Camera Station system report is taken.
Issue isolated to a specific camera:

- It would be appreciated, if the camera's time is synchronized with the server's. This makes it easier for Axis Support to see the issue.
- Network traces taken over the time the issue happens if it's reproducible. This includes:
  - A 60 sec Network trace taken on the camera (only applicable to camera firmware 5.20 and above)

    Use the following VAPIX command: Change the login, IP address and duration (in seconds) if needed:

    ```
    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 showing communication between the server and the camera. *This document* contains detailed instructions which can be sent to customers directly.

Database files – In cases where we need to examine or manually repair the database. Select **Include database in the report** before the system report is generated.

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 is difficult to describe.

Screen recordings – Use screen recordings when it's difficult to describe the problem in words, for example when lots of UI interactions are involved to reproduce the issue.

Other resources

Besides this troubleshooting guide and the user manual, you can visit the YouTube channel for AXIS Camera Station There you can find technical support and feature videos. The videos are available on *youtube.com*.

User manual
AXIS Camera Station User Manual

Ver. M59.2
Date: December 2023
Part no. T10122292