

## AXIS Camera Station User Manual

# AXIS Camera Station User Manual

## What's new?

---

### 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 User Manual

## AXIS Camera Station features

---

### AXIS Camera Station features

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

# AXIS Camera Station User Manual

## AXIS Camera Station tutorial videos

---

### AXIS Camera Station tutorial videos

For more information about the AXIS Camera Station tutorial videos, go to *AXIS Camera Station tutorial videos*.

# AXIS Camera Station User Manual

## Helpful links for an administrator

---

### Helpful links for an administrator

Here are some links you might be interested in. Enjoy the reading!

- *Log in to AXIS Camera Station server on page 13*
- *Configure devices on page 55*
- *Configure storage on page 82*
- *Configure recording and events on page 85*
- *Configure connected services on page 116*
- *Configure server on page 118*
- *Configure licenses on page 124*
- *Configure security on page 128*

# AXIS Camera Station User Manual

## Helpful links for an operator

---

### Helpful links for an operator

Here are some links you might be interested in. Enjoy the reading!

- *Log in to AXIS Camera Station server on page 13*
- *Configure client on page 113*
- *Live view on page 17*
- *Playback recordings on page 29*
- *Export recordings on page 31*

# AXIS Camera Station User Manual

## Quick start

---

### Quick start

This tutorial will walk you through the basic steps to make your system up and running.

Before you start, you may need to:

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

After necessary configurations, you can start to work with AXIS Camera Station.

For an administrator:

1. *Start AXIS Camera Station*
2. *Add devices*
3. *Configure recording method on page 7*

For an operator:

1. *Live view cameras on page 8*
2. *Playback recordings on page 8*
3. *Export recordings on page 8*
4. *Play and verify recordings in AXIS File Player on page 9*

## Start AXIS Camera Station

AXIS Camera Station Service Control automatically starts after the installation is complete.

Double-click the AXIS Camera Station client icon to start the AXIS Camera Station client. When starting the client for the first time, it automatically 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 first time you start your AXIS Camera Station, you are navigated to the Add devices page. AXIS Camera Station automatically searches the network for connected devices and displays a list of devices found. See *Add devices*.

1. Select the cameras to add from the list.  
If your camera is not listed, click **Manual search**.
2. Click **Add**.
3. Select **Quick configuration** or **Site Designer configuration**. Click **Next**. See *Import Site Designer projects on page 58*.
4. Use the default settings and ensure the recording method is set to **None**. Click **Install**.

## Configure recording method

1. Go to **Configuration > Recording and events > Recording method**.
2. If you want to enable motion detection recording:


# AXIS Camera Station User Manual

## Quick start


---

- 2.1 Select a camera.
- 2.2 Turn on **Motion detection**.
- 2.3 Click **Apply**.
3. If you want to enable continuous recording:
  - 3.1 Select a camera.
  - 3.2 Turn on **Continuous**.
  - 3.3 Click **Apply**.




## Live view cameras

1. Click the Live view tab to navigate to the camera live view.
2. Click a camera to navigate to the live view of that camera.  
A blue dot after the camera name shows that continuous recording is in progress. A red dot after the camera name shows that motion detection recording is in progress.
3. Click  to navigate from Live view to Recordings.  
A red line in the timeline shows that motion detection recording has been taken for that period. A blue line in the timeline shows that continuous recording is in progress.

## Playback recordings

1. Go to the Recording tab.
2. In the timeline of the camera, use the mouse wheel to zoom in and out and drag the timeline to make the marker pointing at your desired position.
3. To start playing the recording from the desired position, click  .

## Export recordings

1. Go to the Recording tab.
2. In the timeline of the camera, use the mouse wheel to zoom in and out.
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. In the Export tab, you can do the following if desired. See *Export recordings on page 31* in User Manual.
  - Click  to add a note for the recording.
  - Click **Browse** to select the location to export the recordings.
  - Select **Include Axis File Player**, **Include notes**, and **Add digital signature**.
7. Click **Export**.



# AXIS Camera Station User Manual

## Quick start

---

8. Select Use password and enter your password for the digital signature. Click OK.

### **Play and verify recordings in AXIS File Player**


1. Go to the folder that you have specified for the exported recordings.

# AXIS Camera Station User Manual

## Quick start

---

In this example, the exported files include the recordings in the .asf format, the notes in the .txt format, and AXIS File Player.

2. Double-click AXIS File Player. The exported recordings will be automatically played.
3. Click  to show the notes added to the recordings.
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 is displayed.

## Network configuration

When AXIS Camera Station client, AXIS Camera Station server, and the connected network devices are installed on different networks, you might need to configure proxy or firewall settings before using AXIS Camera Station.

### Client proxy settings

When the client and the server are separated by a proxy server, configure the client proxy settings.

1. Double-click the AXIS Camera Station client icon.
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 network devices and the server are separated by a proxy server, configure the server proxy settings.

1. Double-click the AXIS Service Control icon in Windows notification area.
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 the client and the server are separated by a NAT, firewall or similar, configure the NAT or firewall to ensure that the HTTP port, TCP port, and streaming port specified in AXIS Camera Station Service Control are allowed to pass through the firewall and/or NAT. For instructions how to configure the NAT or firewall, contact the network administrator.

## Server port configuration

The ports 55752 (HTTP), 55754 (TCP), 55756 (mobile communication), and 55757 (mobile streaming) are used on AXIS Camera Station server for communication between the server and the client. If required, the ports can be changed from 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).

# AXIS Camera Station User Manual

## Quick start

---

- Install AXIS Camera Station server, cameras, video encoders, and auxiliary devices on a secure network separated from the office network. AXIS Camera Station client can be installed on a computer on another network, for example a network with Internet access.
- Ensure all users have strong passwords. Using Windows Active Directory a high level of security can be implemented.

# AXIS Camera Station User Manual

## About AXIS Camera Station

---

### About AXIS Camera Station

AXIS Camera Station is a complete monitoring and recording system for small and midsize installations, such as retail shops, hotels, manufacturing sites and schools.

Optimized to take full advantage of Axis leading network cameras and video encoders, AXIS Camera Station combines easy installation and intuitive operation with powerful features for effective investigation and high definition identification.

AXIS Camera Station is comprised of

- **AXIS Camera Station server:** handles all communication with cameras, video encoders and auxiliary devices in the system. The number of cameras and encoders that each server can communicate with is limited by the total bandwidth available.
- **AXIS Camera Station client:** provides access to recordings, live video, logs and configuration. The client can be installed on any computer enabling remote viewing and control from anywhere on the Internet or corporate network.
- **AXIS mobile viewing app:** provides access to recordings and live video on multiple systems. The app can be installed 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 port and mobile streaming port 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.

# AXIS Camera Station User Manual

## Log in to AXIS Camera Station server

---

### Log in to AXIS Camera Station server

Through the AXIS Camera Station client, you can connect to a single server installed on the local computer or elsewhere on the network, or to multiple servers.

When trying to connect to a server for the first time, the client checks the server certificate ID. To ensure that you are connecting to the correct server, manually verify the certificate ID with the one displayed in AXIS Camera Station Service Control. See *General* on page 185.

When trying to connect to a server, the client will be upgraded automatically if the client version is not the same as the server version.

#### Note

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


Double-click the AXIS Camera Station icon to start the AXIS Camera Station client. You can connect to AXIS Camera Station servers in the following ways:

To connect to the servers used in the previous session, select **Last used servers**.

To connect to the server installed on the same computer as the client, select **This computer**.


- 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.
- Select **Log in as <username>** if you have your username and password remembered.

To connect to a remote server:

1. Select **Remote server**.
2. Select a server from the **Remote server** drop-down list or enter the IP or DNS address in the field. If the server is not 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.
  - Select **Log in as <username>** if you have your username and password remembered.

To sign in to AXIS Secure Remote Access:

1. Click the **Sign in to AXIS Secure Remote Access** link.
2. Enter your MyAxis account credentials. See *Axis Secure Remote Access*.
3. Click **Sign in** and **Grant** to grant access.

To connect to the servers from a server list, select a server list from the drop-down list of the **Server list** field. Click  to create or edit the server lists. See *Server lists*.

To import a server list file that has been exported from AXIS Camera Station, click **Import server list** at the bottom right and browse to a .msl file. See *Server lists*.

# AXIS Camera Station User Manual

## Log in to AXIS Camera Station server

---

To delete the usernames and passwords that have saved for all the connected servers, click **Delete saved passwords** at the bottom right.

To connect to a server, it may be necessary to change the client proxy settings, click **Change client proxy settings** at the bottom right. See *Client proxy settings*.

### 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 depending on your setup.

- **Direct connection:** Select this option if there is 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. Wildcards can be used 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 installed on the local computer. Local addresses are identified by the lack of a period (.) in the URI, as in `http://webserver/`, or access the local server, including `http://localhost`, `http://loopback`, or `http://127.0.0.1`

# AXIS Camera Station User Manual










## AXIS Camera Station client

---




### AXIS Camera Station client


When using AXIS Camera Station for the first time, you are navigated to the Add devices page in the Configuration tab automatically. See *Add devices*.

#### Tabs

-  Live view: Live video from connected cameras. See *Live view*.
-  Recordings: Search, play and export recordings. See *Recordings*.
-  Smart search 1: A motion search used to quickly locate important events in recorded video. See *Smart search 1*.
-  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*.
-  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*.
- Alarms and Tasks: The Alarms and Tasks tabs are displayed at the bottom of the client. See *Alarms and Tasks*.

#### Menus

- Click  to browse the main menu.
  - Select **Servers** to connect to a new AXIS Camera Station server, and view the server lists and the connection status for all servers. See *Configure server*.
  - Select **Actions** to start or stop a recording manually, and change the status of I/O ports. See *Record manually* and *Monitor I/O ports*.
  - Select **Help** to select the help related options.
  - Select **Log off** to disconnect from the server and log off from the AXIS Camera Station client.
  - Select **Exit** to exit and close the AXIS Camera Station client.
- Click  to enter the full screen mode. To return to normal mode, press ESC or click . You can configure a hotkey to toggle full screen mode. See *Hotkeys*.

In full screen mode, the top and bottom navigation panels are hidden during inactivity. Move the cursor to the top to show the tabs. Or move the cursor to the bottom to show the view or camera navigation panel.
- Click  or F1 to browse the built-in help.

#### Status bar

# AXIS Camera Station User Manual


## AXIS Camera Station client

---

The status bar can include the following information. Click the links for more information.

- An warning icon appears when there is a time mismatch between client and server. You must ensure 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 left or how much overage that 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. See *AXIS Camera Station update on page 118*.

### Client version

Go to  > Help > About to see the installed AXIS Camera Station client version.

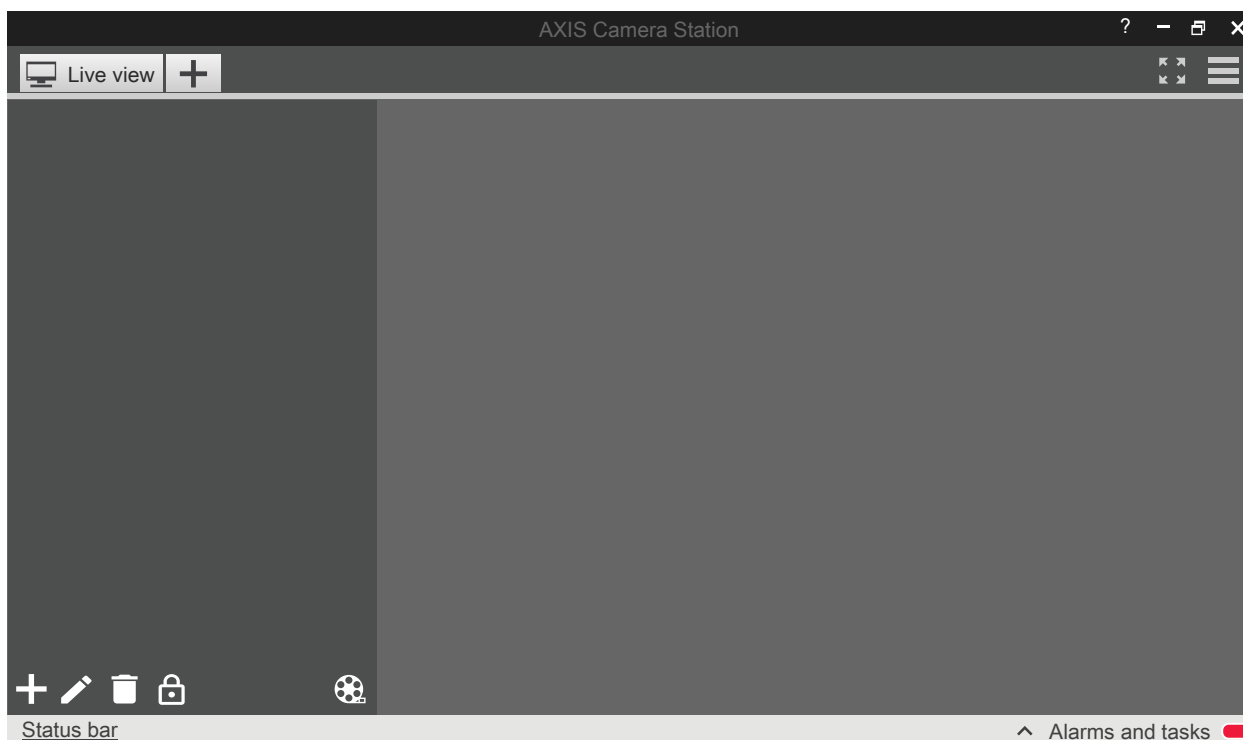


# AXIS Camera Station User Manual

## Live view

---

### Live view



The live view shows the views and cameras and live videos from the connected cameras. When connecting to multiple AXIS Camera Station servers, all the views and cameras of connected servers are displayed grouped by the server name.

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. When cameras and devices are added to or removed from AXIS Camera Station, the views are updated automatically. New cameras and devices are added as new views, and the number of views are optimized for the number of installed devices. Views can be accessed by all users. For information about user access rights, see *Configure user permissions*.

# AXIS Camera Station User Manual

## Live view

---

### Note

My Views (private views) that were created in earlier versions of Axis Camera Station are still available after an upgrade of Axis Camera Station, but can only be edited and removed.

### Find views or cameras

The views and cameras are displayed under **Views** and **Cameras**. Use the **Type to Search** field to find a specific view or camera in the list. Click the camera or view to show it in the live view.

### Tree view navigation for a large system

We recommend that you use tree view navigation for a large system. See *Client settings*. You can also assign a hotkey to toggle tree view navigation. See *Hotkeys*.

### Navigation path

If you enable **Show navigation path when navigating in view**, the navigation path is displayed on top of the view when navigating in a split view. Click the link in the navigation path to go to a specific view. Click **Home** to go to the view where you started.

## Multiple monitors


Right-click a view, camera, or sequence and select **Show on Screen** to show it on the specified monitor.


Select the cameras or views and drag and drop to a new tab in the main screen or monitor screen. A dynamic split view is displayed.

If you have added AXIS T8705 Video Decoder in AXIS Camera Station,

- Right-click a view, camera, or sequence and select **Show on AXIS T8705** to show it on the monitor that is connected to AXIS T8705 Video Decoder.
- Select multiple cameras or views, right-click and select **Show on AXIS T8705**. A symmetric split view with the selected cameras or views will be shown on the monitor that is connected to AXIS T8705 Video Decoder.

## Manage views in live view

Click  to add a new split view, sequence, camera view, map, webpage, or folder.

To edit a view, select the view under **Views** and click .

To edit a camera, select the camera under **Cameras** and click . You can only edit the camera name. To edit the camera settings, see *Edit camera settings*.

To remove a view, select the view under **Views** and click . You need to have permission to edit the view and all secondary views to remove it.

To remove a camera from AXIS Camera Station, see *Cameras on page 61*.

Administrators can select a view under **Views** and click  to lock the view and prevent operators or views from moving or editing the view.

## Image management in live view

- Right-click an image in a split view and select **Navigate** to go to the camera view.
- Right-click an image and select **Show on** to show the image on the specified screen if you have multiple screens.

# AXIS Camera Station User Manual

## Live view

---

- Right-click an image and select **Take snapshot** to take a snapshot. The snapshot is saved to the snapshot folder specified under **Configuration > Client > Settings**.
- Right-click an image and select **Add snapshot to export**. The snapshot is added to the export list in the Export tab.
- Right-click an image and select **Streaming profile** to set the streaming profile. See *Streaming profiles*.
- **Zoom:** Use the mouse wheel to zoom in and out. Alternatively, press CTRL + (+) to zoom in and CTRL + (-) to zoom out.
- **Mechanical PTZ:** Mechanical PTZ is available for PTZ cameras and for cameras where digital PTZ has been enabled in the camera's configuration page. 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, click the desired area and drag to draw a rectangle surrounding the area to be magnified. 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 a desired area in the image to pan or tilt to that area. 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.
- **Go to a preset position:** Right-click the image, select **Presets** and select the preset to go to. To create presets, see *PTZ presets*.
- **Add preset:** Drag the image view to the desired position, right-click and select **Presets > Add preset**.
- Right-click the image and select **Set focus** to adjust camera 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.
- Right-click the image, select **Focus recall zone** and then select to add or remove focus recall zone.
- Right-click the image, select **Autotracking on/off** and then select to turn on or turn off autotracking for an Axis PTZ camera with AXIS PTZ Autotracking configured.



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

[www.axis.com/products/online-manual/34074#t10162342](http://www.axis.com/products/online-manual/34074#t10162342)

*Add digital presets*

# AXIS Camera Station User Manual

## Live view

---



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


[www.axis.com/products/online-manual/34074#t10162342](http://www.axis.com/products/online-manual/34074#t10162342)

*PTZ control*

### Note


Administrators can disable mechanical PTZ for users. See *Configure user permissions*.

## Recording and instant replay in live view

Select a camera or a split view, and click  to go to the Recordings tab.

In the live view, an ongoing recording is indicated by a recording indicator in the lower part of the image:

- **Yellow:** Manual recording in progress.
- **Red:** Motion detection or event recording in progress.
- **Blue:** Continuous recording in progress.

To play an ongoing recording, hover the mouse pointer over the image and click  **Instant replay** at the top right. The Recordings tab will open and the last 5 seconds of the recording will be played.

To record manually from the live view, hover the mouse pointer over the image and click **REC**. Click **STOP** to stop recording.

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 disable manual recording for users. See *Configure user permissions*.

## Audio in live view

Audio is available if the camera has audio capabilities and audio has been enabled in the profile used for the live view.

Go to **Configuration > Devices > Streaming profiles** and configure audio for the camera. See *Streaming profiles on page 62*.

When you hover the mouse pointer over the image,

- The audio control button will be displayed. Use the slider to control audio volume. Click the button to mute audio in this view.
- The **Listen to this view only** button will be displayed. Click the button to mute other views and listen to this view only.
- The **Speak through the speaker** button will be displayed for full-duplex mode by default. Click the button to speak through the configured speaker.
- The **Push-to-talk** button will be displayed for simplex and half-duplex modes by default. Click and hold the button to speak through the configured speaker.

# AXIS Camera Station User Manual

## Live view

---


### Note

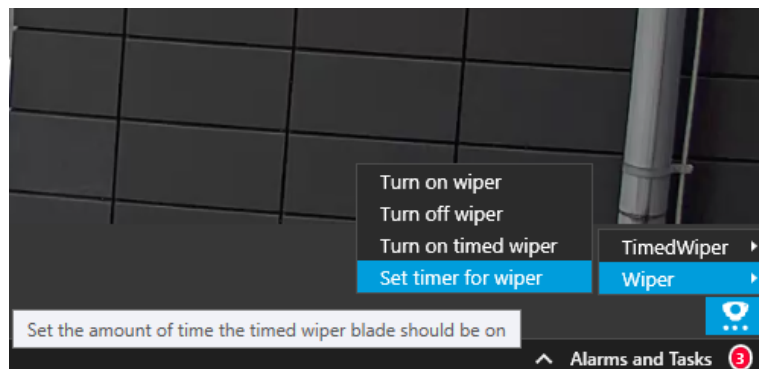
- Administrators can disable audio for users. See *Configure user permissions*.
- The **Push-to-talk** button will be displayed for all duplex modes if you turn on **Use push-to-talk for all duplex modes** under *Configuration > Client > Streaming > Audio*. See *Streaming on page 115*.

## Onscreen control in live view

### Note

Onscreen control requires firmware 7.40 or later.

In the live view, click  to access the available camera features.



## Split view


A split view displays 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.

One frame can be set as a hotspot that automatically loads the view from another frame when clicking in that frame. Hotspots are particularly useful for asymmetric split views with one large and several small frames. The largest frame is typically defined as the hotspot.

To add a split view:

1. In the Live view tab, click  .
2. Select **New Split View**. A new split view tab opens.
3. Enter a name for the split view.
4. Select a template you want to use from the **Template** drop-down list.
5. Add views or cameras. Use the **Type to search** field for find specific views or cameras.
  - Drag and drop a view or a camera to the desired slot in the grid view. If there is already a camera or view in that slot, the old one will be replaced.
  - Double-click a view or a camera to add it to the first available slot in the grid view.

# AXIS Camera Station User Manual

## Live view

---

- Select multiple views or cameras, and drag and drop to add them to the first available slots in the grid view.
  - Select multiple views or cameras, press ENTER to add them to the first available slots in the grid view.
6. Edit or remove views or cameras in the grid view.
    - Select a view or a camera in the grid view, and move the mouse to the borders or the right corner of the image to resize it.
    - Select a view or a camera in the grid view, and drag and drop it to the desired slot.
    - Select multiple views or cameras, and click **Remove view** or press DELETE to delete them from the grid view.
    - Right-click a camera in the grid view, select **Streaming profile** to set the streaming profile for the camera. See *Streaming profiles*.
  7. Select a frame in the split view and click **Set Hotspot** to set the frame as a hotspot. To remove a hotspot, select a hotspot and click **Remove Hotspot**.
  8. Click **Save view** and the split view is saved on the server you logged on.



*Add a split view*

To edit a split view, right-click a split view and select **Edit**.

To remove a split view, right-click a split view and select **Delete**.

## Door dashboard in split view


If you have configured a door under **Configuration > Access control > Doors and zones**, 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 139*.
2. Add the door dashboard to a view.
  - 2.1 In the Live view tab, click **+** and select **New split view**.
  - 2.2 Enter a name for the split view.
  - 2.3 Select a template you want to use from the **Template** drop-down list.
  - 2.4 Drag and drop a door to the desired slot in the grid view.
  - 2.5 Drag and drop a camera or a view to the desired slot in the grid view.
  - 2.6 Click **Save view**.
3. Under **Dashboard**,

# AXIS Camera Station User Manual

## Live view

---

- The door details, door status and lock status are displayed.
  - Click **Access**, **Lock**, **Unlock** or **Lockdown** to perform actions on the door.
  - An access control event is displayed with cardholder details including photo, for example, when the cardholder swipes the card. Other access control events related to the cardholder are also displayed.
- Click  to bookmark an event and make it available under **Transactions**.
- Alarms are displayed with alarm trigger information, for example, when a door is open too long.
  - The latest transaction is displayed.
4. Under **Transactions**, the recent transactions and saved transactions are displayed.



*Monitor and assist in door dashboard*


## Sequence

A sequence view automatically switches between included views. The dwell time, i.e. the number of seconds to show a view, before switching to the next, can be set individually for each view.

### 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**. A new sequence view tab opens.
3. Enter a name for the sequence.
4. Add views or cameras. The views or cameras added in the sequence are marked with a number to show its order in the sequence. Use the **Type to search** field for find specific views or cameras.
  - Drag and drop a view or a camera to the sequence. If there is already a camera or view in that position, the old one will be replaced.
  - Double-click a view or a camera to add it to the first available position in the sequence.
  - Select multiple views or cameras, and drag and drop to add them to the first available positions in the sequence.
  - Select multiple views or cameras, press ENTER to add them to the first available positions in the sequence.
5. Edit or remove views or cameras in the sequence.

# AXIS Camera Station User Manual

## Live view

---

- Select a view or a camera in the sequence, and drag and drop it to change its order in the sequence.
  - Select multiple views or cameras, select **Remove view** or press **DELETE** to delete them from the sequence.
  - Right-click a camera in the sequence, select **Streaming profile** to set the streaming profile for the camera. See *Streaming profiles*.
6. Select a view or a camera in the sequence, and set the dwell time in the **Dwell time** field. By default the dwell time is set to 5 seconds when a view or a camera is added.
  7. For cameras with PTZ capabilities, select a PTZ preset from the **PTZ preset** drop-down list. See *PTZ presets*.
  8. Click **Save view** and the sequence is saved on the server you logged on.



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

[www.axis.com/products/online-manual/34074#t10128940](http://www.axis.com/products/online-manual/34074#t10128940)

*Add a sequence*

To edit a sequence, right-click a sequence and select **Edit**.

To delete a sequence, right-click a sequence and select **Delete**.


## Camera view

A camera view displays live video from one camera. Camera views can be used in split views, sequences and maps.

### Note

When connecting to multiple AXIS Camera Station servers, all cameras from all connected servers are shown in the list.

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 list, and click **OK**.

To edit a camera view, right-click a camera view and select **Edit**.

To remove a camera view, right-click a camera view and select **Delete**.

## Map

A map is an imported image on which camera views, split views, sequences, webpages, other maps, and doors can be placed. The map gives a visual overview and makes it easy to quickly locate and access individual devices. You can place cameras on imported floor plans or create several maps and arrange them on an overview map for large installations.



# AXIS Camera Station User Manual

## Live view


---

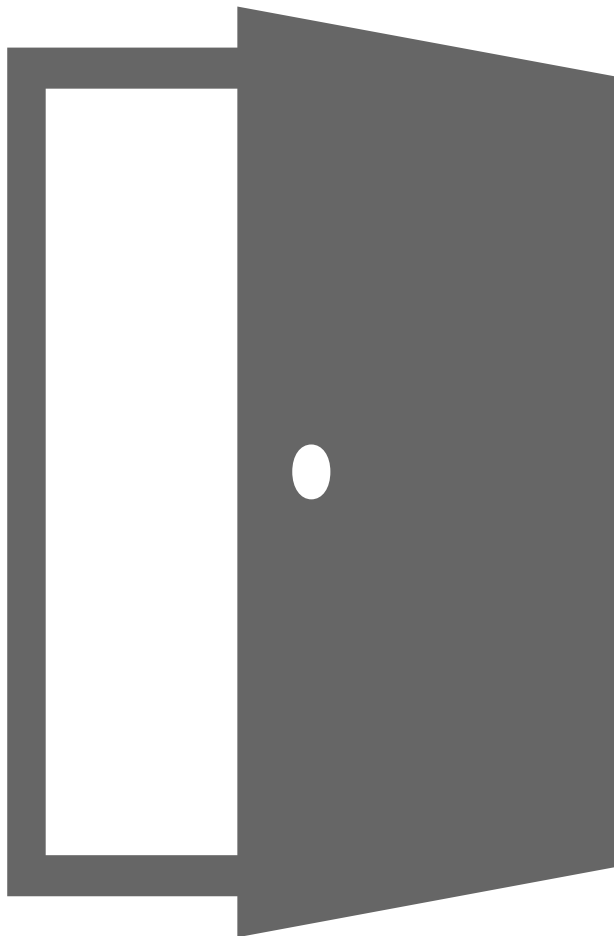
You can open a camera, device, view, or door dashboard from a map. The action buttons are also available from the map view if they are set with a map. See *Create action button triggers*.

### Note

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




### Add a map

1. In the Live view tab, click  .
2. Select **New map**. A new map view tab opens.
3. Enter a name for the map.
4. Click **Choose image** and navigate to 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 to the desired position on the map. You can use the **Type to search** field to find them. A door icon can be:



- : 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.
6. Click an icon on the map to edit the settings:
- **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.
7. To add a label to the map, click **Add label**, enter a label name, and set the size, rotation, style, and color of the label. Click and drag the label to the desired position on the map. Click  to remove the label.

# AXIS Camera Station User Manual

## Live view

---

### Note

Some settings can be edit for multiple icons and labels at the same time. To select multiple items on the map, keep CTRL pressed and click the items. To select all items on the map, press CTRL + A.

8. Click **Save view**. The map view is saved on the server selected in the main window.



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

[www.axis.com/products/online-manual/34074#t10128941](http://www.axis.com/products/online-manual/34074#t10128941)

*Add a map*



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

[www.axis.com/products/online-manual/34074#t10128941](http://www.axis.com/products/online-manual/34074#t10128941)

*Trigger audio from a map*

To edit a map, right-click a map and select **Edit**.

To remove a map, right-click a map and select **Delete**.

### Snapshot

When you take a snapshot of a map, the status of the devices on the map is also visible in the snapshot.

- To save a snapshot:
  1. Right-click a map and select **Take snapshot**.
  2. The snapshot is automatically saved to the folder that you have configured under **Configuration > Client > settings**.
- To export a snapshot:
  1. Right-click a map and select **Add snapshot to export**.
  2. The snapshot is added to the export list in the **Export** tab. Follow *Export recordings on page 31* to export your recordings with the snapshot of the map.

### Map zooming and navigation

# AXIS Camera Station User Manual

## Live view

---


- **Mouse:** Use the mouse wheel to zoom in and zoom out. When the map is zoomed in, drag the map to navigate to the desired position.
- **Keyboard:** Press CTRL + (+) to zoom in and CTRL + (-) to zoom out. Press CTRL and arrow keys to navigate to the desired position.
- **Joystick:** Twist the head of the joystick to zoom in and zoom out. Tilt the joystick to navigate to the desired position.

## Webpage

A webpage view displays a page from the Internet. The webpage can for example be shown in a split view or a sequence together with live video.



To add a webpage:

1. In the Live view tab, click  .
2. Select **New webpage**.
3. Enter a descriptive name for the webpage.
4. Enter the complete Internet address in the **Url** field. Both http and https protocols can be used. For example:  
`http://example.com/path.html`.
5. Click **OK**.


To edit a webpage, right-click a webpage and select **Edit**.

To delete a webpage, right-click a webpage and select **Delete**.

## Folders

Folders are used 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**.

To edit a folder, right-click a folder and select **Edit**.


To remove a folder, right-click a folder and select **Delete**.

# AXIS Camera Station User Manual

## Recordings



---

### Recordings

The Recordings tab handles recording search, playback and export. To access the Recordings tab, go to the tabs menu or click  in the Live view tab.

The left panel shows the views and cameras of connected servers grouped by the server name. You can find views or cameras, manage views, and use tree view navigation for a large system. See *Live view*.

The right panel shows the camera images, playback tools and recording timeline.

- Right-click an image:
  - Select **Navigate** to go to the camera Recordings tab if you start from the Recordings tab of a split view.
  - Select **Show on** to show it on the specified screen if you have multiple screens.
  - Select **Take snapshot** to take a snapshot. The snapshot is saved to the snapshot folder specified under **Configuration > Client > Settings**.
  - Select **Add snapshot to export**. The snapshot is added to the export list in the Export tab.
  - Select **Incident report** to create incident reports if you have the incident report enabled.
  - Select **Streaming profile** to set the streaming profile. See *Streaming profiles*
- Click  and select the date and time to navigate to a specific time in the timeline.
- Click  to configure the types of recordings shown in timeline.
- Click **Show all body worn metadata** to show all metadata of a body worn system. Notes and categories added in AXIS Body Worn Assistant are also displayed.
  - Type keywords in the **Type to search** field to find recordings.
  - Double-click a recording in the list and navigate to the recording in the timeline.
- *Playback recordings*
- *Bookmarks*
- *Export recordings*
- *Export incident reports on page 35*

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

#### Note

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

### Playback recordings

Recordings from multiple cameras can be played at the same time if the playback marker is positioned over several timeline recordings. To view recordings in cameras that are listed with timeline but not shown in the view, drag a camera from the timeline to a playback window in the view.

When using multiple monitors, live video can be displayed at the same time as recorded video.

Playback timeline

# AXIS Camera Station User Manual

## Recordings


---

The playback timeline represents the time period of the playback. You can zoom in, zoom out, and drag the timeline. If the marker points to recordings, when you drag the timeline you can have a quick overview of the recordings (scrubbing) and find a specific event in the recordings. The playback will be paused temporarily when you drag the timeline and will be resumed when you release the timeline.








The timeline below the playback window displays the search result. Recordings are color coded:

- **Red:** Motion detection or rule triggered recording
- **Yellow:** Manual recording
- **Blue:** Continuous recording
- **Dark grey:** Failover recording



### Navigate to recordings

- Click  and select the date and time to navigate to a specific time in the timeline. In the timeline, use the mouse wheel to zoom in and out and drag the timeline to make the marker pointing at your desired recording.
- Use the Smart search tab to navigate to the desired recording. See *Smart search 1*.
- Use the bookmarks to navigate to the desired recording with a bookmark. See *Bookmarks*.

### Playback recordings

1. Navigate to the recording that you want to playback.
2. In the Playback control panel:
  - Click  to start playing the recording.
  - Click  to pause the recording.
  - Click  to jump to the start of the ongoing or previous recording.
  - Click  to jump to the start of the next recording.
  - Click  to step to previous frame in the recording. The option is only available when paused. Right-click the icon the access optional amount of frames to skip (up to 20 frames).
  - Click  to step to next frame in the recording. The option is only available when paused. Right-click the icon the access optional amount of frames to skip (up to 20 frames).
  - Click  to mute audio. This icon is displayed when audio is included in the recording.
  - Move the audio slider to control the audio volume. This icon is displayed in the playback image when audio is included in the recording.
  - For panoramic cameras, click the image and scroll in and out with the mouse wheel to pan, tilt and zoom during playback. To zoom in on an area, place the cursor in the desired area and use the mouse wheel to zoom. Or use CTRL + (+) to zoom in and CTRL + (-) to zoom out.

## Bookmarks

In the Recordings tab, click  to show all bookmarks to the recordings.  indicates that the recording is locked.

# AXIS Camera Station User Manual




## Recordings

---


### Note

- A locked recording can't be deleted unless actively unlocked.
- Locked recordings will be deleted if the camera is removed from AXIS Camera Station.
- The lock interval for a locked recording is 5 minutes.

Use the **Type to search** field to find a particular bookmark. Select a bookmark:

- Right-click and select **Go to** to show the bookmarked recording in the timeline, and click  to play a recording from the bookmarked time.
- Click  to edit the bookmark name and description, and change whether to lock or unlock the recording:
  - Select **Prevent recording deletion** to lock the recording.
  - Clear **Prevent recording deletion** to unlock the recording.
- Click  to remove the bookmark. You can remove multiple bookmarks at the same time. To select multiple bookmarks, press SHIFT or CTRL while selecting the bookmarks.

### Add bookmarks

1. Navigate to the recording. See *Playback recordings*.
2. Select the position in the timeline and click .
3. Enter the bookmark name and description. You can use keywords in the description to make the bookmark easy to find and recognized.
4. Select **Prevent recording deletion** to lock the recording. The lock interval is 5 minutes. When the system deletes old recordings, the recordings within the lock interval will not be deleted.

### Note

A locked recording can't be deleted. To unlock the recording, clear the option or delete the bookmark.

5. Click OK.

## Export recordings

Recordings can be exported to a local storage or a network location that is accessible from the AXIS Camera Station client. Multiple recordings can be exported at the same time.

You can export your recordings to the .asf, .mp4, or .mkv format and they can be played by Windows Media Player or AXIS File 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.

Before you start, ensure you have permission for exporting. See *User permission for exporting on page 33*.






### Export recordings

1. In the Recordings tab, select a camera or a view.
2. Add the recordings to the export list. The recordings that are added to the export list are highlighted and the others are greyed out in the timeline.
  - Right-click a recording and select **Export > Add recordings**. The single selected recording is added to the export list.

# AXIS Camera Station User Manual

## Recordings

---

- Right-click outside of a recording and select **Export > Add recordings**. The recordings that include the marker are added to the export list.
  - Click  to display the selection markers. Move the selection markers to the desired times. Right-click a recording within the selection markers and select **Export > Add recordings** to add the single recording to the export list. Right-click outside of a recording and select **Export > Add recordings** to add all recordings within the selection markers to the export list.
3. If you want to remove any recordings from the export list:
- Right-click a recording and select **Export > Remove recordings**. The single selected recording is removed from the export list.
  - Right-click outside of a recording and select **Export > Remove recordings**. The recordings that include the marker are removed from the export list.
  - When the selection markers are displayed, right-click a recording within the selection markers and select **Export > Remove recordings** to remove the single recording from the export list. Right-click outside of a recording and select **Export > Remove recordings** to remove all recordings within the selection markers from the export list.
4. When a recording or a snapshot is added to the export list, the Export tab is displayed. If the Incident report tab is displayed, click **Switch to export** to navigate to the Export tab.
5. If you want to save the export list to a file, click **Save**.
6. If you want to include the export list that you have saved before, click **Load**.
7. In the export list, the information about the recordings is displayed including the start time, end time, duration, event, streaming profile, and whether it has been edited or contains notes or audio.
- Click one recording in the exported list to preview and play it. You can only preview multiple recordings if they are from one camera.
  - Click one recording and go to the timeline to adjust the recording start and end time. The timeline shows up to thirty minutes of recording around the selected recording.
  - Click one recording and drag the timeline to a specific location. Right-click the image and select **Add snapshot** to add snapshots.
  - Select the streaming profile in the **Preferred streaming profile** field.
  - If the recording contains audio, you can click  to mute audio.
  - To edit the recording, click . See *Edit recordings before exporting* on page 33.
  - To edit notes for the recording, click .
  - To remove the recording from the export list, click .
8. Click **Browse** to select the location to export the recordings to.
9. 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 to the recording in AXIS File Player.
10. Under **Advanced settings**:
- To ensure image authenticity and integrity by making image tampering impossible, select **Add digital signature**. This option is only available for recordings in the .asf format. See *Play and verify exported recordings* on page 35.
  - To include AXIS File Player with the exported recordings, select **Include AXIS File Player**.



# AXIS Camera Station User Manual

## Recordings

---

- 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.
- To export to a Zip file, select **Export to Zip file** and you can set password to the exported Zip file.
- From the **Export format** drop-down list, select a format you want to export your recordings to. If you select MP4, audio in G.711 or G.726 format will not be included in the exported recordings.
- If any recording has been edited, you can set the video encoding format to **Automatic**, **H.264**, or **M-JPEG** under **Edited video encoding**. **Automatic** means using M-JPEG for M-JPEG format and H.264 for other formats.

11. Click **Export**. The export recordings task is shown at the bottom right, and added to the Tasks tab.






*Export recordings*

The export folder includes:

- The recordings in one of the supported format.
- The notes in the .txt format if you have selected **Include notes**.
- AXIS File Player if you have selected **Include AXIS File Player**.
- The playlist in the .asx format if you have selected **Create playlist(.asx)**.

### User permission for exporting

The export permission can be configured in *Configure user permissions on page 128*.

- If you have the export permission disabled and the incident report permission disabled, you do not have permission to export recordings or generate incident reports.
- If you have the export permission disabled and the incident report permission enabled, you only have permission to generate incident reports. When you click  in the Recordings tab, the Incident report tab will open.
- If you have the export permission enabled and the incident report permission disabled, you only have permission to export recordings. When you click  in the Recordings tab, the Export tab will open.
- If you have the export permission and the incident report permission enabled, you have permission to export recordings and generate incident reports. When you click  in the Recordings tab, the Export tab will open by default. During one connection session, the tab that is recently used will open.


### Edit recordings before exporting

Blur a moving object

# AXIS Camera Station User Manual

## Recordings

---

1. In the Export tab or Incident report tab, select a recording and click .
2. Drag the timeline to the start point of the moving object.
3. Click **Add** under **Bounding boxes** to add a new bounding box. Or right-click the object and select **Add new bounding box**.
4. Go to **Bounding box options > Size** to adjust the size. Or drag the handles of the bounding box.
5. Drag the bounding box to cover the object.
6. Go to **Bounding box options > Fill** and set it to **Pixelated** or **Black**.
7. When playing the recording, drag and drop the bounding box to add a key frame. Or right-click the object and select **Add key frame**.
8. To add continuous key frames, keep dragging the bounding box to cover the object when playing the recording.
9. Drag the timeline and check the object is completely covered.
  - To remove a key frame, right-click the key frame and select **Remove key frame**.
  - To go to the specific location on timeline, right-click the key frame and select **Go to time position**.
10. Double-click the last key frame, click **Set end** under **Bounding box options** to set an end. Or right-click and select **Set end**. All the key frames after the end point will be removed.

### Note

You can add multiple bounding boxes in the video. If the bounding boxes overlap, the overlapped part will fill with color in the order of Black, Pixelated, and Clear.

### Show a moving object with blurred background


1. Follow the steps in the previous section to blur the moving object.
2. Go to **Bounding box options > Fill** and set it to **Clear**.
3. Go to **Video background** and set it to **Pixelated** or **Black**.

### Note

You can select multiple bounding boxes in the list, right-click and select **Pixelate all but this**. The selected bounding boxes will fill with **Clear** and the others will fill with **Pixelated**.

### Generate bounding boxes

If you have enabled the camera's analytic data under **Configuration > Devices > Streaming profiles**, you can generate bounding boxes from the analytic data for the recording.

1. In the Export tab or Incident report tab, click .
2. Click **Generate bounding boxes**.
3. Check and adjust the bounding boxes to cover the moving object.
4. Fill the bounding boxes or video background.

### Improve video editing with AXIS Video Content Stream

For cameras with firmware 5.50 and later, video editing can be improved by installing the application **AXIS Video Content Stream 1.0** on the camera.

# AXIS Camera Station User Manual

## Recordings

---

The application is automatically installed on new cameras added to AXIS Camera Station but can also be installed from the device management page, see *Install camera application*. The application enables AXIS Video Content Stream in the camera. The use of AXIS Video Content Stream is only permitted through AXIS Camera Station.




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

[www.axis.com/products/online-manual/34074#t10141635](http://www.axis.com/products/online-manual/34074#t10141635)

*Edit recordings before exporting*

### Play and verify exported recordings

To ensure image authenticity and integrity, a digital signature can be added to the exported recordings with or without password. The digital signature can be further verified in AXIS File Player to check whether the recording has been changed.

1. Go to the folder that you have specified for the exported recordings. If you have set password for the exported Zip file, you need to input your password to open the folder.
2. Double-click AXIS File Player. The exported recordings will be automatically played.
3. In AXIS File Player, click  to show the notes added to the recordings.
4. In AXIS File Player, verify the digital signature if you have selected **Add digital signature**.
  - 4.1 Go to **Tools > Verify digital signature**.
  - 4.2 Select **Validate with password** and enter your password if you have selected **Use password**.
  - 4.3 Click **Verify**. The verification result page is displayed.

### Export incident reports

You can export incident reports with recordings, snapshots, and notes on a storage or a network location that is accessible from the AXIS Camera Station server. In this way, the person who generates the incident reports do not have access to the exported materials.

You can export your recordings to the .asf, .mp4, or .mkv format and they can be played by Windows Media Player or AXIS File Player. AXIS File Player is a free software for video and audio playback. It is automatically included when you generate the incident reports. No installation is required. To play recordings, open AXIS File Player and select the recordings to play.

Before you start, ensure you have permission for exporting. See *User permission for exporting on page 33*.

# AXIS Camera Station User Manual

## Recordings

---




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

[www.axis.com/products/online-manual/34074#t10138955](http://www.axis.com/products/online-manual/34074#t10138955)

*Incident reporting*





### Generate incident reports

1. In the Recordings tab, select a camera or a view.
2. Add the recordings to the export list. The recordings that are added to the export list are highlighted and the others are greyed out in the timeline.
  - Right-click a recording and select **Export > Add recordings**. The single selected recording is added to the export list.
  - Right-click outside of a recording and select **Export > Add recordings**. The recordings that include the marker are added to the export list.
  - Click  to display the selection markers. Move the selection markers to the desired times. Right-click a recording within the selection markers and select **Export > Add recordings** to add the single recording to the export list. Right-click outside of a recording and select **Export > Add recordings** to add all recordings within the selection markers to the export list.
3. If you want to remove any recordings from the export list:
  - Right-click a recording and select **Export > Remove recordings**. The single selected recording is removed from the export list.
  - Right-click outside of a recording and select **Export > Remove recordings**. The recordings that include the marker are removed from the export list.
  - When the selection markers are displayed, right-click a recording within the selection markers and select **Export > Remove recordings** to remove the single recording from the export list. Right-click outside of a recording and select **Export > Remove recordings** to remove all recordings within the selection markers from the export list.
4. Add the snapshots to the export list. In the Recordings tab, drag the timeline to a specific location, right-click the image and select **Incident report > Add snapshot**.
5. When a recording or a snapshot is added to the export list, the Incident report tab is displayed. If the Export tab is displayed, click **Switch to incident report** to navigate to the Incident report tab.
6. If you want to save the export list to a file, click **Save**.
7. If you want to include the export list that you have saved before, click **Load**.
8. In the export list, the information about the recordings is displayed including the start time, end time, duration, event, streaming profile, and whether it has been edited or contains notes or audio.
  - Click one recording in the exported list to preview and play it. You can only preview multiple recordings if they are from one camera.
  - Click one recording and go to the timeline to adjust the recording start and end time. The timeline shows up to thirty minutes of recording around the selected recording.
  - Click one recording and drag the timeline to a specific location. Right-click the image and select **Add snapshot** to add snapshots.

# AXIS Camera Station User Manual

## Recordings

---

- Select the streaming profile in the **Preferred streaming profile** field.
  - If the recording contains audio, you can click  to mute audio.
  - To edit the recording, click . See *Edit recordings before exporting on page 33*.
  - To edit notes for the recording or snapshot, click .
  - To remove the recording or snapshot from the export list, click .
9. In the Incident report tab:
- The **Description** field is prefilled with what you have defined in the Description template. You can add the necessary information you want to include in the incident report.
  - In the **Category** field, select a category that the report belongs to.
  - In the **Reference ID** field, a reference id is automatically generated. You can manually change it. The reference id is unique to identify the incident report.
10. To include notes of the recordings and snapshots, select **Include notes**. The notes are available as a .txt file in the exported folder. The notes of the recordings are also displayed as a bookmark to the recording in AXIS File Player. The notes of the snapshots are included in the incident report.
11. If any recording has been edited, you can set the video encoding format to `Automatic`, `H.264`, or `M-JPEG` under **Edited video encoding**. `Automatic` means using `M-JPEG` for `M-JPEG` format and `H.264` for other formats.
12. Click **Create report**. The export incident report task is shown at the bottom right, and added to the Tasks tab.

The export folder includes:


- AXIS File Player
- The recordings in the .asf format
- The notes of the recordings and snapshots in the .txt format if applicable
- The incident report: Includes general information about the incident, recording summaries, and snapshot summaries
- The playlist if multiple recordings are exported

## Record manually

### Note

When connecting to multiple AXIS Camera Station servers, you can manually start and stop a recording on any connected server by selecting 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. Use the **Type to search** field to find cameras.
3. Click **Start** and the Status of the cameras changes from `Stopped` to `Recording`. Or click **Stop** and the Status of the cameras changes from `Recording` to `Stopped`.

To start and stop a manual recording from Live view:

1. Go to Live view.

# AXIS Camera Station User Manual

## Recordings

---

2. Move the mouse pointer to the camera's live view frame.
3. Click **REC** at the top right. A yellow indicator appears while the camera is recording.
4. Click **STOP** to stop the recording.

# AXIS Camera Station User Manual

## Smart search 1

---

### Smart search 1

#### Note

By default smart search 1 is shown. To hide this feature, turn off **Show smart search 1**. See *Client settings on page 114*.

Smart search 1 is a motion search used to quickly locate important events in recorded video. Instead of going through hours of recorded video manually, smart search 1 finds the points in time when there is movement in a selected area in the recorded video.

Smart search 1 will be faster if you enable analytics by selecting **Include analytics data for smart search** when configuring streaming profiles. See *Streaming profiles*.

#### Use smart search 1

1. Click **+** and select **Smart search 1** to display the Smart search 1 tab.
2. Select a camera that contains the recording that you want to search.
3. Adjust the area of interest in which moving objects are detected. The area is a polygon displayed on top of the recorded video. The polygon can have 3 to 20 corners.
  - Use the mouse to move and resize the area.
  - To add a new corner, click the line between two corners.
  - To remove a corner, right-click the corner.
4. In the Search tab, configure the ignore filters:
  - **Short-lived objects filter**: adjust the minimum time in the Time slider that objects must appear in the image.
  - **Small objects filter**: adjust the size of the ignored objects in the Width and Height sliders.
5. In the Search tab, select a date from the calendar and select the start time and end time from the drop-down lists. To select a range of dates, keep the SHIFT key pressed while selecting the dates.
6. Click **Search**.



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

[www.axis.com/products/online-manual/34074#t10129947](http://www.axis.com/products/online-manual/34074#t10129947)

*Smart search 1*

#### Manage search result

The search results are shown in the Results tab. Select **Show detection area** to see the area of interest used for the search.

- Double-click a search result to move the playback marker to the time when motion was detected.
- Right-click one or multiple search results and select **Export** to export the recordings. See *Export recordings*.

# AXIS Camera Station User Manual

## Smart search 1

---

- Right-click one or multiple search results, you can add the recordings to the export list and edit the export list.
- Right-click a search result, you can add a bookmark to the recording and edit the bookmark. See *Bookmarks*.
- Right-click one or multiple search result and select **Remove** to remove the recordings from the search result.

### Improve smart search 1 with AXIS Video Content Stream

For cameras with firmware 5.50 and later, smart search 1 can be improved by installing the application AXIS Video Content Stream 1.0 on the camera.

The application is automatically installed on new cameras added to AXIS Camera Station but can also be installed from the device management page, see *Install camera application*. The application enables AXIS Video Content Stream in the camera. The use of AXIS Video Content Stream is only permitted through AXIS Camera Station.



# AXIS Camera Station User Manual

## Smart search 2 <sup>BETA</sup>

---

### Smart search 2 <sup>BETA</sup>



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

[www.axis.com/products/online-manual/34074#t10171106](http://www.axis.com/products/online-manual/34074#t10171106)

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.

#### Note

- It requires streaming analytics metadata over RTSP.
  - For cameras with AXIS OS earlier than 9.60, it requires to install AXIS Video Content Stream on cameras. See *Install camera application on page 76*.
- It requires time synchronization between the AXIS Camera Station server and cameras.

### Limitations


- Metadata will only be recorded after enabling smart search 2. Hence historic data is not searchable.
- High or very variable network latency can cause time synchronization issue and affect classification of detections based on analytics metadata.
- Continuous recording is recommended. Using motion detection triggered recordings will result in detections without video recordings.
- Classification of object types and detection accuracy will be negatively affected by low image quality due to high compression levels, by weather conditions such as heavy rain or snow and for cameras with low resolution, heavy distortion, large field of view or excessive vibrations.
- Stationary objects are not detected.
- Small and distant objects may not be detected.
- Make sure that the lighting conditions are within the camera specification. Use additional lighting if needed. Color classification will not work in darkness or with IR illumination.
- Body worn cameras are not supported.
- Object classification is not supported for thermal cameras.
- Each time a PTZ preset position changes and for a short recalibration period after position change no moving objects will be detected.
- Line crossing and area filters do not follow PTZ position changes.

### Workflow

1. *Configure smart search 2 <sup>BETA</sup> on page 152*
2. Configure time synchronization between the AXIS Camera Station server and cameras.
  - Use an external NTP server.
    - 2.1 Synchronize the server to an NTP server.
    - 2.2 Synchronize the cameras to the same NTP server.
  - Use AXIS Camera Station as the NTP server.
    - 2.1 Go to **Configuration > Server > Settings > Time synchronization**.
    - 2.2 Select **Use this server as the NTP server for connected devices**.
    - 2.3 Restart the AXIS Camera Station service.
3. Create a filter or load an existing filter. See *Create a filter on page 42*.
4. Manage search results. See *Smart search results on page 49*.
  - Go to recording
  - Export recording
  - Generate detection report

### Create a filter

The cameras selected under **Configuration > Smart search 2 > Settings** are available and can be used for smart search.

1. Click  and select **Smart search 2 <sup>BETA</sup>** to display the Smart search 2 tab.
2. Click **Cameras** and select the cameras used for search.
3. Click **Search interval**, select a time range or click **Custom** to set a time range.
4. To detect persons, click **Person detection**. Select **Person** and select the clothing colors. You can select multiple colors.
5. To detect vehicles, click **Vehicle detection**. Select the vehicle types and colors. You can select multiple vehicle types and vehicle colors.
6. To filter by area:
  - 6.1 Click **Area**, select the camera and turn on **Filter by area**.
  - 6.2 Adjust the area of interest displayed on top of the recorded video.
    - Click and drag to move it.
    - Drag the anchor points to adjust the size and shape. It can have up to 25 anchor points.
    - To add a new anchor point, click the line between two anchor points.
    - To remove an anchor point, right-click it.
  - 6.5 Click **Reset** to reconfigure the area of interest.
7. To filter by line crossing:
  - 7.1 Click **Line crossing**, select the camera and turn on **Filter by line crossing**.

# AXIS Camera Station User Manual

## Smart search 2 BETA

---

- 7.2 Adjust the blue line displayed on top of the recorded video. You can add new anchor points and drag and drop the anchor points to adjust the line.
  - 7.3 Under **Direction**, select the line crossing direction to detect. The direction is displayed as red arrow on top of the recorded video.
  - 7.4 Click **Reset** to reconfigure the crossing line and the direction.
8. To filter by size and duration:
  - 8.1 Click **Size and duration**, select the camera and turn on **Filter by size and duration**.
  - 8.2 Adjust the minimum height as a percentage of the total image. Objects that are smaller than the specified height are ignored.
  - 8.3 Adjust the minimum width as a percentage of the total image. Objects that are smaller than the specified width are ignored.
  - 8.4 Adjust the minimum duration in seconds. Objects that appear a shorter time in the image than the specified duration are ignored.
  - 8.5 Click **Reset** to reconfigure the filters.
9. To include the detections that are classified as unknown, select **Unknown detections**.
10. Click **Search**. The progress bar is displayed with the number of detections remaining and estimated time left.

### Manage filters

#### Note

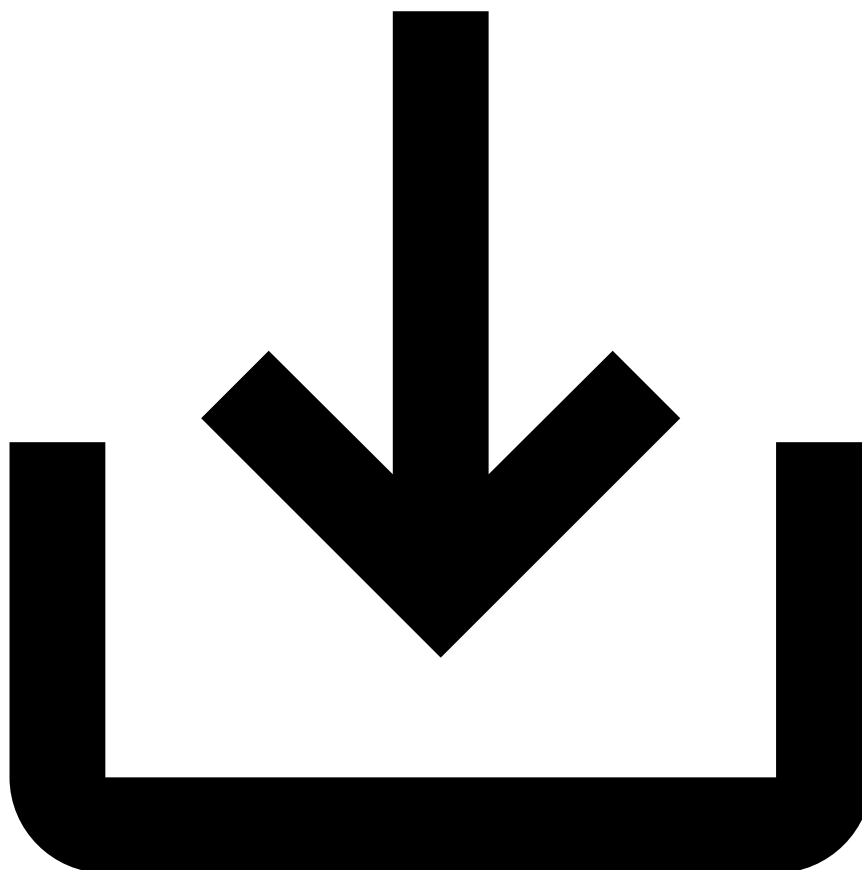
Only the user who created the filter can access and manage it.

# AXIS Camera Station User Manual

## Smart search 2 BETA

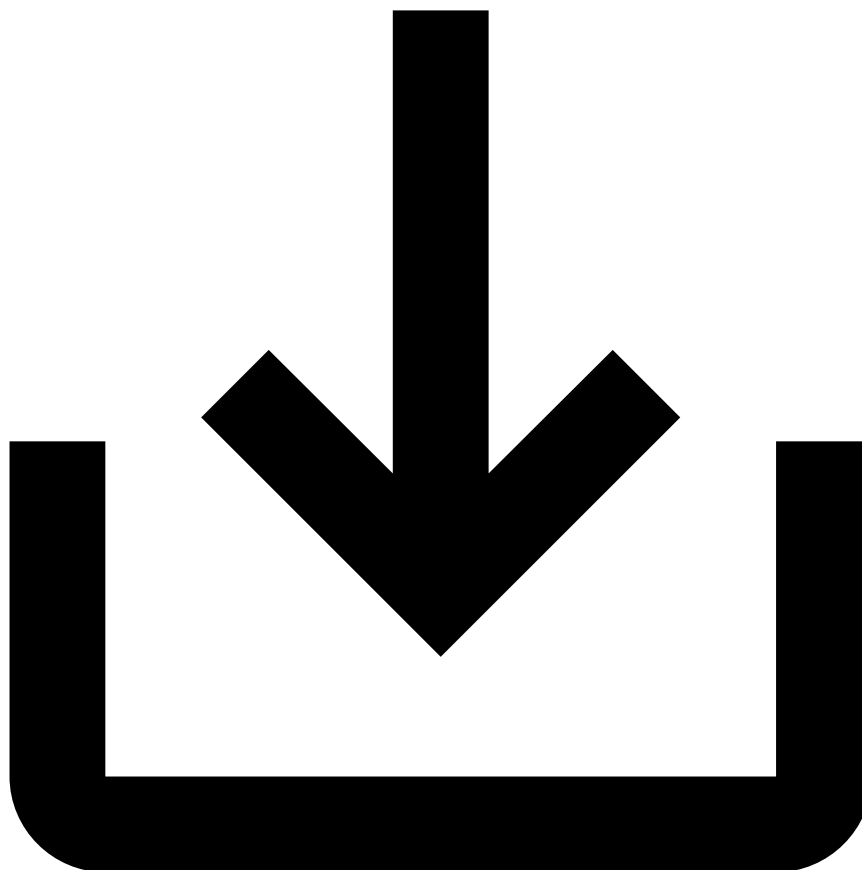
---

- To save a filter, click



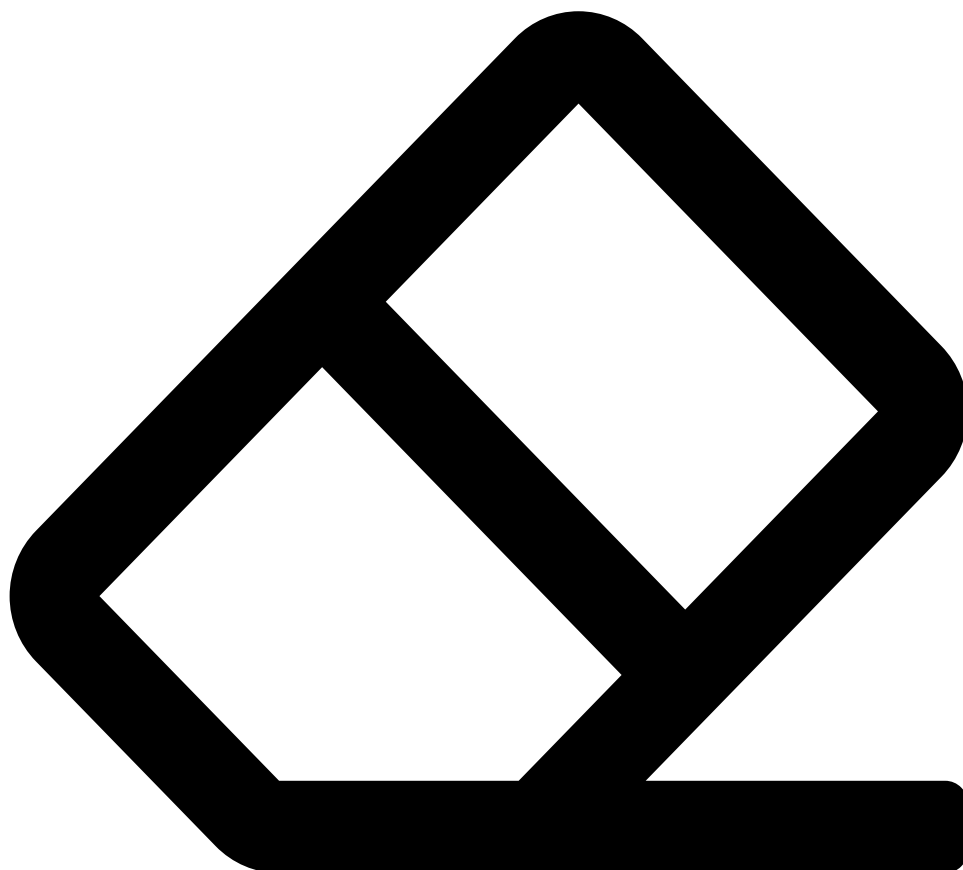
, type a filter name and click **Save**.

- To replace an existing filter, click



, select an existing filter and click **Replace**.

- To reset a filter, click



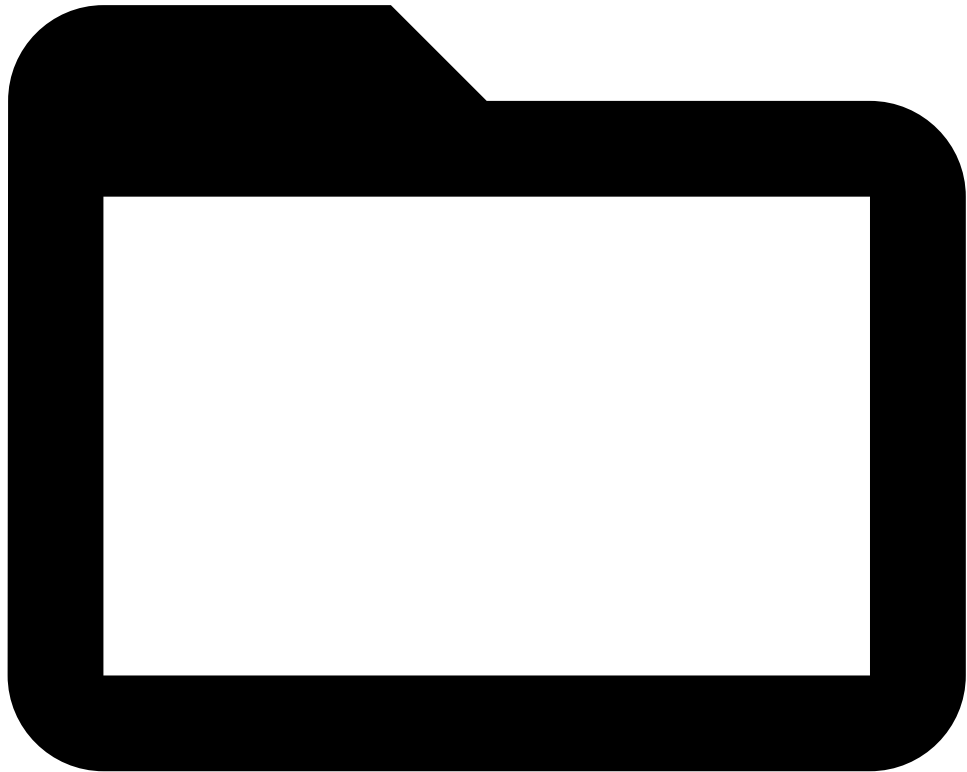
and click Reset.

# AXIS Camera Station User Manual

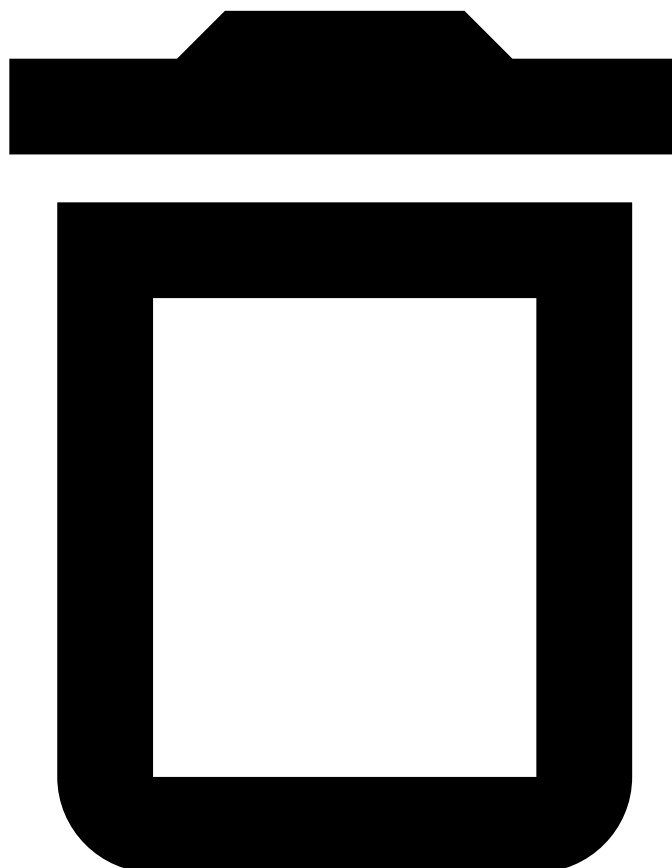
## Smart search 2 BETA

---

- To delete a filter, click

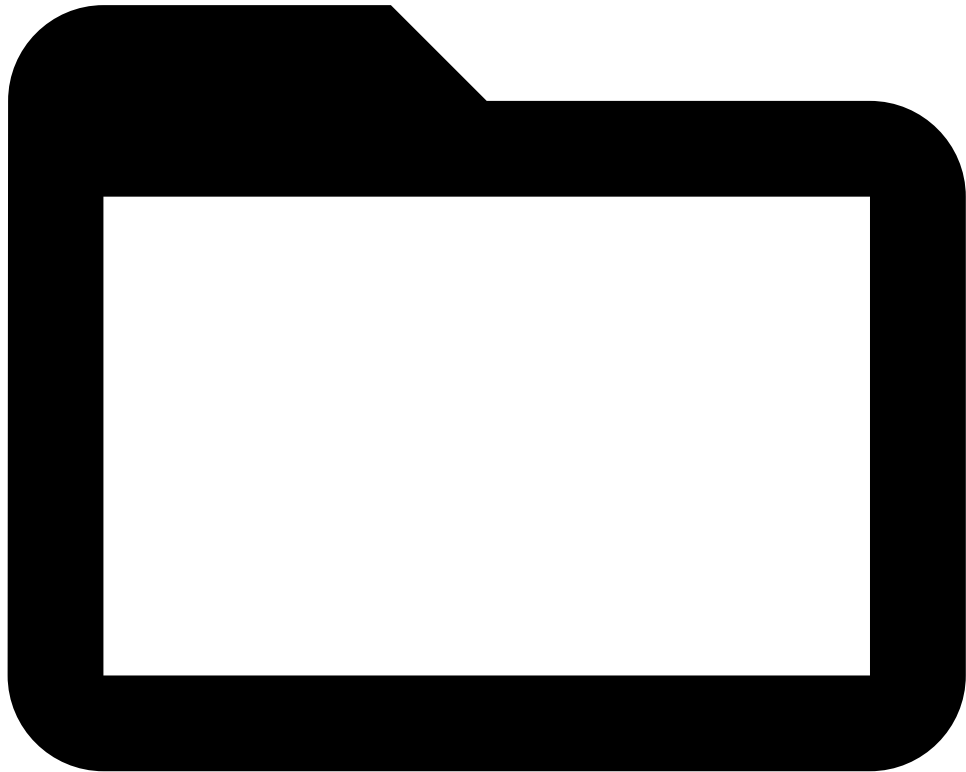


and click





- To load a filter, click



and click a filter.

### Smart search results

The search results are grouped by date. A search result includes:

- **Icon:** Show the classification and color of the detection. It can be an icon of person, vehicle or unknown.
- **Time:** The time when it was detected.
- **Image:** A snapshot of the detection with a red box showing the detected object.

To manage a search result:

- By default, the search results are displayed in descending order with the latest detections on top. Click **Earliest first** to show the oldest detections on top.

# AXIS Camera Station User Manual

## Smart search 2 BETA

---

- To further filter the search results, click **Confidence** and set the confidence level. High confidence ignores uncertain classifications.
- Click a search result to view more information and more options.
  - **General information:** The camera name and time of the detection.
  - **Recording:** The recording is played automatically with prebuffer and postbuffer if applicable. You can mute the recording and view it in full screen.
  - **Snapshot:** The snapshot of the detected object with the classification and detected color.
  - **Go to recording:** Click to open the Recordings tab of the camera and navigate to the recording in the timeline. See *Recordings on page 29*.
  - **Export recording:** Click to open the Export tab with the recording in the export list. To edit the recording before export, right-click and select **Edit recording and export**. See *Export recordings on page 31*.
  - **Classification details:** Click to view the classification details.
  - **Generate 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.

# AXIS Camera Station User Manual

## Data search

---


### Data search

You can search for data that originates from an external source or system and easily go to the recordings in AXIS Camera Station and track what happened at the time of each event. See *External data sources on page 81*.

Examples of possible data:

- Events generated by an access control system. For example: access granted, access denied, door opened, door locked, door open too long, and door forced open.
- License plates captured by a device with AXIS License Plate Verifier.

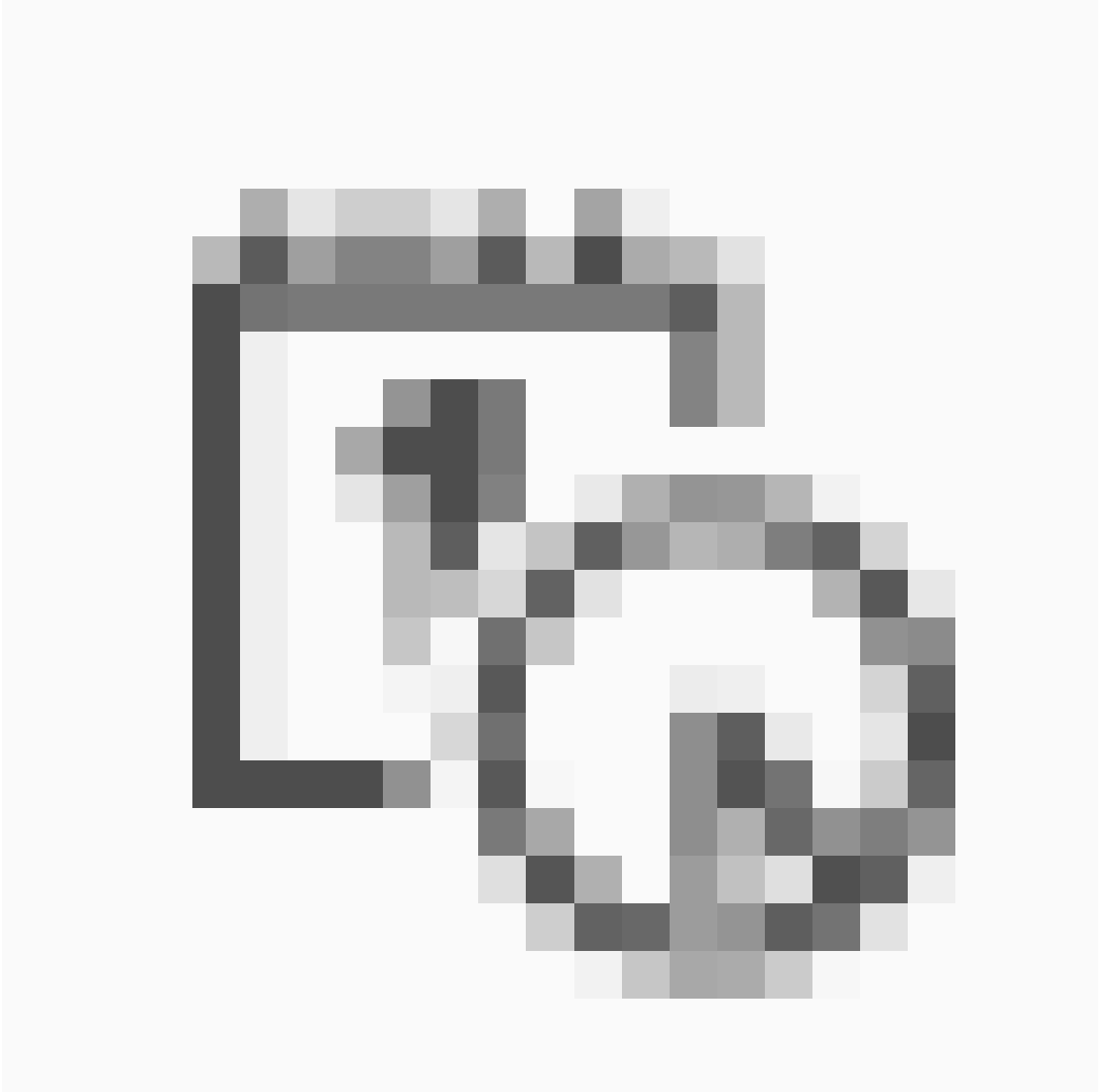
By default, you can search for data in last 90 days. To change the number of days to keep external data, go to **Configuration > Server > Settings > External data**.

1. Click  and select **Data search** to display the Data search tab.

## Data search

---

2. Select a search interval from the drop-down list beside





- Live: Select **Live** to search real-time data. The maximum amount of live data can be shown is 3000. In live mode, you can't use search operators.
  - Preconfigured time range: Select a time range to search. For example, Last hour, Last 12 hours, Last 30 days.
  - Custom: Select **Custom** and specify the start time and end time to search.
3. To specify the data source to search, select a data source from the **Source** drop-down list.
  4. To search for data with specific words, type the keywords in the search field. See *Optimize your search on page 53*.
  5. Click **Search**. A list of data is displayed with details including time, source and event specific information. Click a column heading to sort by the content of the column.
  6. If a source has been configured with a view:

# AXIS Camera Station User Manual

## Data search

---

- The data generated from the source is automatically bookmarked in the timeline of the view. Click the data in the list to go to the recording to track the event.
  - In live mode, click  to navigate between the recording timeline and live view.
7. Click  to export the search results to a .txt file. Only event information is exported. Recordings and images are not exported.

Item	Description
Time	The time when the event happened.
Source	The name of the source of the event.
Server	The server that the event data are sent to. Only available when connecting to multiple servers.
Typical items for access control events	
Cardholder	The cardholder who triggers the event.
Event	The description of the event. For example: door locked.
Location	The name of the door and the name of the door controller with IP address.
Photo	The cardholder photo. Hover the mouse pointer over it to view a larger image.
Typical items for AXIS License Plate Verifier events	
License plate	The license plate number captured by the device.



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

[www.axis.com/products/online-manual/34074#t10148979](http://www.axis.com/products/online-manual/34074#t10148979)

*Search for access control data*

## Optimize your search

You can use the following search operators to optimize your search and find the best matches:

- Use quotation marks " " to find exact matches for 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.

# AXIS Camera Station User Manual

## Data search

---


- 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"

# AXIS Camera Station User Manual

## Configuration

---

### Configuration

The Configuration tab is used to manage and maintain connected devices, as well as settings for the client and servers. Click  and select **Configuration** to display the Configuration tab in the AXIS Camera Station client.

### Configure devices

In AXIS Camera Station, a device refers to a network product with its own IP address. A camera refers to a video source which is 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, each video port is treated 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
- a door station

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 streaming profiles in regard to resolution, format and more. See *Streaming 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 81*.

### Add devices

#### Note

- When connecting to multiple AXIS Camera Station servers, you can add devices on any connected server by selecting the server from the **Selected server** drop-down list.
- View areas are considered as individual cameras. You must create view areas in the camera before using them. See *Use view areas*.
- We recommend not using 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 56*

# AXIS Camera Station User Manual

## Configuration

---

- *Find your video streams on page 57*
  - *Find prerecorded videos on page 58*
2. *Add devices, video streams or prerecorded videos on page 58*

### Device list

The device list includes the following information:

- **Name:** The name of the device. Click the name to change the name of the device.
- **IP address:** The IP address of the device. Only used when the hostname of the device is not available.
- **Hostname:** The hostname of the device. Used as the default communication address when it is available.
- **MAC address:** The MAC address of the device.
- **Status:** The status of the device.
  - **(empty):** Device can be added 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 does not 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, the username and password will be used 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. You can type your password or click **Generate** to automatically generate a password up to the length allowed by the device. You can select to use this password for all devices with the `Set password` status. We recommend that you show the automatically generated password and make a copy of it.
  - **Model not supported:** AXIS Camera Station does not support the device model.
  - **Obsolete firmware:** The camera's firmware is old and must be updated before the camera can be added to AXIS Camera Station.
  - **Faulty device:** The device parameters retrieved by AXIS Camera Station corrupt.
  - **Set tilt orientation:** Click the link to set the tilt orientation. Tilt orientation must be set before the camera can be added. Select tilt orientation Ceiling, Wall, or Desk depending on how the camera is mounted. Tilt orientation is a required setting for some camera models. Setting tilt orientation ensures that video from the camera is presented correctly and that pan, tilt and zoom tools work correctly.
  - **Unsupported third-party device:** AXIS Camera Station does not support this specific third-party device.
  - **Can only be used with AXIS Companion:** The device is designed to be used with AXIS Companion and can't be used with AXIS Camera Station.
- **Manufacturer:** The manufacturer of the device.
- **Model:** The model of the device.

### 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**.



# AXIS Camera Station User Manual

## Configuration

---

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**.

# AXIS Camera Station User Manual

## Configuration

---

### Find prerecorded videos

You can add prerecorded videos in the .mkv format to AXIS Camera Station and configure a .dewarp file to dewarp the video stream of the prerecorded video.

The .mkv files need to support the following:

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

The following is an example of a .dewarp file. For more information, see *Image configuration on page 66*.

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

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 video stream, add a .dewarp file with the same name as the .mkv file to the folder.
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. Go to **Configuration > Devices > Add devices**.
2. If you want to change the device's name, click the name in the list and enter a new name.
3. Select the devices, video streams or prerecorded videos. Click **Add**.
4. Choose whether to use hostnames instead of IP when possible for the devices.
5. Choose how to configure your devices.
  - Select **Quick configuration** and click **Next**. For devices with video capabilities, select the retention time, recording method, and where to store recordings. You can only configure continuous recording for video streams and prerecorded videos.
  - Select **Site Designer configuration** and click **Next**. Enter your access code or upload the Site Designer setup file and click **Import**. See *Import Site Designer projects*.
6. Click **Install**.

### Import Site Designer projects



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

[www.axis.com/products/online-manual/34074#t10129836](http://www.axis.com/products/online-manual/34074#t10129836)

# AXIS Camera Station User Manual

## Configuration

---

AXIS Site Designer is an online design tool that helps you to build a site with Axis products and accessories. With site templates you can customize your own surveillance solution.

If you have created a site design project in AXIS Site Designer, you can import the project to AXIS Camera Station. If you have previously used Site Designer to setup your devices, you have the option of accessing the design online by using an access code. Alternatively, you can select a downloaded Site Designer setup file.

You can only import the settings from a Site Designer project when adding an Axis device.

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** when your AXIS Camera Station server is connected to the Internet. Or click **Download settings file** when your AXIS Camera Station is not connected to the Internet.
2. From 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 navigate to the Site Designer setup file you have downloaded.
6. Click **Import**. The first device that matches the IP address as the one you are adding is selected automatically. If no IP address matches, the first device that matches the device name is selected. Otherwise, select one from the drop-down list.
7. Click **Install**.

### Settings imported from the Site Designer project

When importing a Site Designer project, the following settings are imported into AXIS Camera Station:

- Schedules with name and time slots.
- Maps with name, icon color, icon location, and item name.
- For encoders, video decoders, door controllers, radar detectors, and speakers:
  - Name
  - Description
- For cameras, door stations, and F/FA series:
  - 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

# AXIS Camera Station User Manual

## Configuration

---

### Note

- If only one of the recording profiles is defined or two identical recording profiles are defined in the Site Designer project, the profile is set to medium in AXIS Camera Station after importing the Site Designer project.
  - If both recording profiles are defined in the Site Designer project, the continuous recording profile is set to medium and the motion triggered recording is set to high in AXIS Camera Station after importing the Site Designer project.
  - The resolution is set with ideal aspect ratio according to AXIS Camera Station. After importing, the resolution might be different from the one defined in the Site Designer project.
- Zipstream strength
  - Audio settings for live view and recordings
  - Retention time for recordings

### Note

- The audio settings can only be set in AXIS Camera Station if the device has a built-in microphone or speaker. To use an external audio device, manually enable it after installing the device.
- The audio settings are not applied to door stations. Door stations always get audio enabled for Live view only even if the settings in Site Designer is different.

### Add third-party devices

Third-party devices can be added to AXIS Camera Station in the same way as adding Axis products. See *Add devices*.

### Note

You can also add third-party devices as video streams to AXIS Camera Station. See *Find your video streams on page 57*.

For detailed 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, nevertheless 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

# AXIS Camera Station User Manual

## Configuration

---

### Use view areas

View areas are supported by certain camera models. AXIS Camera Station lists view areas as individual cameras on the Add devices page. See *Add devices*.

All view areas in a network camera are counted as one camera in the total number of cameras allowed by the AXIS Camera Station license. The number of cameras that can be added depends on the installed license. Each AXIS Camera Station license allows a particular number of cameras.

To use view areas with AXIS Camera Station, view areas must first be enabled 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 sign in.
4. Click **Help** for instructions on where to find the setting because enabling view areas differ depending on camera model and firmware.

### Cameras

Go to **Configuration > Devices > Cameras** to view the list of all cameras that have been added to AXIS Camera Station. The information includes the camera's name, address, MAC address, manufacturer, model, video channel and server if connected to multiple AXIS Camera Station servers.

From this page, you can:

- Click the camera's address link to open the camera's configuration page.

#### Note

If the AXIS Camera Station client is running externally and the AXIS Camera Station server and cameras are behind a NAT, the configuration page will not open.

- Click **Edit** to edit the camera settings. See *Edit camera settings*.
- Click **Remove** to remove the selected cameras.

#### Note

This will delete all recordings, including recordings that have been locked.

- Use the **Type to search** field to find specific cameras.

### Using view areas

View areas are supported by certain camera models. Axis Camera Station lists view areas as individual cameras on the Add devices page. See *Add devices*.

#### Note

To use view areas with AXIS Camera Station, view areas must first be enabled in the camera's configuration page. Links to each installed camera can be found in **Configuration > Devices > Cameras**.

All view areas in a network camera are counted as one camera in the total number of cameras allowed by the AXIS Camera Station license. The number of cameras that can be added depends on the installed license. Each AXIS Camera Station license allows a particular number of cameras.

### Edit camera settings

To edit camera settings:

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

# AXIS Camera Station User Manual

## Configuration

---

2. Select a camera and click **Edit**.
3. In the Settings section:
  - **Enabled** is selected by default. If you clear **Enabled**, the video stream can neither be recorded nor viewed in Live view. Recordings and Live view can still be configured.
  - Enter a unique camera name and description.
  - Enter the camera's hostname or IP address, and port number if different from the default port 80.
  - When the **Channel** field is available for multiport video encoders, select the port number. When the **Channel** field is available for view areas, select the number corresponding to the view area.
4. In the Credentials section, enter a username and password for an administrator account on the camera. The password is used by AXIS Camera Station to communicate with the camera.

### Other devices

Go to **Configuration > Devices > Other devices**, a list of devices without video capabilities is displayed including door controllers, audio devices and IO modules.

For information about supported products, go to [www.axis.com](http://www.axis.com) See *Use audio from other devices*.

In this page, you can:

- Select the devices and click **Edit** to edit device settings such as device name, address and password.
- Select the devices and click **Remove** to remove the devices from AXIS Camera Station.
- Click the device's address link to open the device's configuration page.

#### Note

If there is a NAT or firewall between the AXIS Camera Station client and the device, the configuration page will not open.


### 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**.
3. In the Settings section:
  - Enter a unique name for the auxiliary device. This name is displayed in AXIS Camera Station.
  - Enter the auxiliary device's hostname or IP address, and port number if different from the default port 80.
4. In the Credentials section, enter a username and password for an administrator account on the device.

### Streaming profiles

Go to **Configuration > Devices > Streaming profiles** to open the Streaming profiles page. A list of all cameras is displayed. Use the **Type to search** field to find cameras in the list.

The microphone  indicates that the camera has an enabled microphone (built-in, line-in, auxiliary device). The microphone transmits audio from the camera to live view and recordings. Any built-in microphones or speakers can't be shared with other cameras.

The speaker  indicates that the camera has an enabled speaker (built-in or external auxiliary device). In the live view, use the **Speak** or **Push-to-talk** button to transmit spoken messages through the speaker.

# AXIS Camera Station User Manual

## Configuration

---

The following profiles can be used in Live view and recordings settings:

- **Video profiles:** Contains profile settings for resolution, video format, frame rate, and compression. Each camera displays settings for its video profiles. To enable profile settings in recordings, see *Action rules*.
  - **High:** Optimized for the highest quality and resolution.
  - **Medium:** Optimized to balance high quality with performance.
  - **Low:** Optimized for performance.

### Note

In Live view and recordings, the Streaming profile is set to **Automatic** by default. That means the streaming profile will be automatically changed to **High**, **Medium**, or **Low** depending on the available size for the video stream.

- **Audio:** Contains profile settings for microphone and speaker usage.

### Edit streaming profiles

1. Go to **Configuration > Devices > Streaming profiles**, and select the cameras.
2. Under **Video profiles**, configure the following for **High**, **Medium**, and **Low** profiles:
  - **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. H.264 is supported by most camera models and requires less bandwidth and storage space compared to, for example, M-JPEG.

### Note

Cameras can only have one video profile configured for 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:** Select the level of bitrate reduction to reduce the average bitrate in an H.264 or H.265 stream in real time. This option is only available for Axis devices that support Zipstream. Default means to use the Zipstream setting configured through the device's configuration page.

The strength parameter defines the effort level for Zipstream.

Strength	Effort level	Visible consequences
Off	Off	None
10	Low	No visible effect in most scenes
20	Medium	Visible effect in some scenes: less noise and slightly lower level of detail in regions of lower interest
30	High	Visible effect in many scenes: less noise and lower level of detail in regions of lower interest
40	Higher	Visible effect in even more scenes: less noise and lower level of detail in regions of lower interest
50	Extreme	Visible effect in most scenes: less noise and lower level of detail in regions of lower interest

3. Under **Audio**, configure the following:
  - **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*.

# AXIS Camera Station User Manual

## Configuration

---

- **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. Audio can be enabled for Live view and recordings, Live view only or Recordings only.
4. Under **Advanced**, configure the following settings:
    - To allow data to be gathered for smart search during video streaming, select **Include analytics data for Smart search**. This option is only available for Axis devices that support analytics data. Data gathering for *Smart search 1* can add latency in live video streaming.
    - To improve compatibility with third-party devices, select **Use FFmpeg** to enable FFmpeg streaming. This option is only available for third-party devices.
    - 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 only available for an Axis PTZ camera with AXIS PTZ Autotracking configured. For a complete workflow to set up AXIS PTZ Autotracking in AXIS Camera Station, see *Set up AXIS PTZ Autotracking*.
  5. Click **Apply**.

### Customize profile 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*.

### Optimize profile settings for low bandwidth

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 AXIS Camera Station server. See Bandwidth usage in *Streaming*.

### Use audio from other devices

Audio from other, non-camera or auxiliary, devices can be used together with video from a network camera or video encoder for live viewing or recording.

#### Note

External audio devices must first be added to AXIS Camera Station. To edit audio devices, see *Other devices*. To manage audio devices, see the Edit streaming profile section as described in *Streaming profiles*.

1. Add the non-camera device to AXIS Camera Station. See *Add devices*.
2. Configure the camera to use audio from the device. See *Streaming profiles*.
3. Enable audio for Live view or Recording. See *Streaming profiles*.

### Examples



# AXIS Camera Station User Manual

## Configuration

---



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

[www.axis.com/products/online-manual/34074#t10130014](http://www.axis.com/products/online-manual/34074#t10130014)

*Set up audio devices and make live announcements*



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

[www.axis.com/products/online-manual/34074#t10130014](http://www.axis.com/products/online-manual/34074#t10130014)

*Create an action button to manually play audio when motion is detected*



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

[www.axis.com/products/online-manual/34074#t10130014](http://www.axis.com/products/online-manual/34074#t10130014)

*Automatically play audio when motion is detected*



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

[www.axis.com/products/online-manual/34074#t10130014](http://www.axis.com/products/online-manual/34074#t10130014)

*Add an audio clip to speaker and AXIS Camera Station*

# AXIS Camera Station User Manual

## Configuration

---

### 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
```

# AXIS Camera Station User Manual

## Configuration

---

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

# AXIS Camera Station User Manual

## Configuration

---



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

[www.axis.com/products/online-manual/34074#t10128937](http://www.axis.com/products/online-manual/34074#t10128937)

*Upgrade firmware versions*

If you have set up automatic check for new software versions in *AXIS Camera Station update on page 118*, 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.

[www.axis.com/products/online-manual/34074#t10128937](http://www.axis.com/products/online-manual/34074#t10128937)

*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:** No connection with the device until a root user and password is set. Click the link to set the root user password. You can type your password or click **Generate** to automatically generate a password up to the length allowed by the device. You can select to use this password for all devices with the **Set password** status. We recommend that you show the automatically generated password and make a copy of it.

# AXIS Camera Station User Manual

## Configuration

---

- **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 <sup>BETA</sup> on page 81*.
- **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 <sup>BETA</sup> on page 81*.
- **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 77*.
- **IEEE 802.1X:** The IEEE 802.1X status of the device. See IEEE 802.1X status in *Security on page 77*.
- **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*.

# AXIS Camera Station User Manual

## Configuration


---

- 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 77*.
- Collect device data. See *Collect device data*.
- Select to use IP address or hostname. See *Connection on page 80*.
- 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 <sup>BETA</sup> on page 81*.

### 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.

# AXIS Camera Station User Manual

## Configuration

---

### 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 BETA* on page 81.

- 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 72*.
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 72*.
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**.

# AXIS Camera Station User Manual

## Configuration

---

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 72*.
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](http://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.



# AXIS Camera Station User Manual

## Configuration

---

- **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**.

# AXIS Camera Station User Manual

## Configuration

---

### 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.

[www.axis.com/products/online-manual/34074#t10129866](http://www.axis.com/products/online-manual/34074#t10129866)

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.

# AXIS Camera Station User Manual

## Configuration



---

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:

# AXIS Camera Station User Manual

## Configuration

---

- 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**.



*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](http://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](http://www.axis.com/se/sv/products/camera-applications/license-key-registration#/registration)

If an application can't be installed, go to [www.axis.com](http://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:

# AXIS Camera Station User Manual

## Configuration

---

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

AXIS Camera Station can automatically handle the client and server certificates by configuring a certificate authority (CA). If a CA is configured, any preinstalled certificates will be ignored when new certificates are installed using the CA. However, we recommend that you uninstall any preinstalled certificates. For more on how to configure certificates, see *Certificates on page 130*.

### View installed certificates

1. Go to **Configuration > Devices > Management**.
2. Right-click the devices, select **Security > Certificates > View installed certificates** to get an overview of the installed certificates and on which devices they are installed. A warning icon appears in the **Valid to** column if the certificate is approaching its expiration date.
3. To search for a specific certificate, use the **Type to search** field.
4. To view the certificate details, double-click the row that lists the certificate.

The installed certificates are grouped into:

- **Client certificates:** the certificates to be used as client certificates, for example the certificates used for IEEE 802.1X. It includes the client certificates that are both automatically installed and manually installed using AXIS Camera Station.
- **Server certificates:** the certificates to be used as server certificates, for example the certificates used for HTTPS. It includes the server certificates that are both automatically installed and manually installed using AXIS Camera Station.
- **Combined client/server certificates:** the certificates to be used as both client and server certificates, for example when it is intended to use a single certificate for both HTTPS and IEEE 802.1X instead of using two different certificates. It includes all client/server certificates that are manually installed using AXIS Camera Station.
- **Externally installed client/server certificates:** the certificates to be used as both client and server certificates, for example when it is intended to use a single certificate for both HTTPS and IEEE 802.1X instead of using two different certificates. It includes the combined client/server certificates that are installed not using AXIS Camera Station.
- **CA certificates:** the certificates to be used for verification.

# AXIS Camera Station User Manual

## Configuration

---

### Manage HTTPS or IEEE 802.1X certificates

#### Note

- When a certificate authority has not been configured in AXIS Camera Station, after enabling HTTPS, you may lose contact with your devices if the certificates on the devices can't be validated.
- Before enabling IEEE 802.1X, ensure 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 **Security > Certificates > Delete certificates** and select the certificate in the list to delete the selected certificates from the devices.

#### 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.

### Manually install certificates

If you use an existing CA and are not willing to allow AXIS Camera Station to sign the certificates on your behalf, you have to create the certificates outside of AXIS Camera Station and manually install them on devices.

#### Note

When manually installing certificates, all certificates in the batch must have the same passphrase.

1. Go to **Configuration > Devices > Management**.
  2. Right-click the devices:
    - Select **Security > Certificates > Install server certificates (HTTPS)** to manually install the server certificates on the devices.
    - Select **Security > Certificates > Install client certificates (IEEE 802.1X)** to manually install the client certificates on the devices.
    - Select **Security > Certificates > Install combined client/server certificates** to manually install the combined client/server certificates on the devices.
- If a single certificate is selected, it will be installed on all selected devices.
  - If multiple certificates are selected, AXIS Camera Station will try to match each certificate to a device based on the subject common name of each certificate. The installation will ignore the devices or certificates that can't be matched and continue installing the certificates that meet the following conditions on matched devices.
    - Part of a certificate's subject common name must contain the entire hostname, MAC, or IP address of a selected device. Otherwise, the certificate will be ignored.
    - A certificate must only match against a single selected device. Otherwise, the certificate will not be installed on any device.
    - A device must only have a single certificate that match against it. Otherwise, no certificate will be installed on that device.

# AXIS Camera Station User Manual

## Configuration

### Status of HTTPS and IEEE 802.1X

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

	Status	Description/Solution
HTTPS	Enabled	HTTPS is active on the device.
	Disabled	HTTPS is not active but ready to be activated on the device.
	Disabled (missing server certificate)	HTTPS is not active and can't be activated until a server certificate is installed on the device. Possible solution: <ul style="list-style-type: none"><li>• Configure the certificate authority. See <i>Certificates on page 130</i>.</li><li>• Manually install a server certificate. See <i>Manually install certificates in Security on page 77</i>.</li><li>• Manually install a combined client/server certificate. See <i>Manually install certificates in Security on page 77</i>.</li></ul>
	Disabled (multiple server certificates)	HTTPS is not active and can't be activated until there is only one server certificate on the device. Possible solution: <ul style="list-style-type: none"><li>• Delete the redundant server certificates. See <i>Delete certificates in Security on page 77</i>.</li></ul>
	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.
	Disabled (missing client certificate)	IEEE 802.1X is not active and can't be activated until a client certificate is installed on the device. Possible solution: <ul style="list-style-type: none"><li>• Configure the certificate authority. See <i>Certificates on page 130</i>.</li><li>• Manually install a client certificate. See <i>Manually install certificates in Security on page 77</i>.</li><li>• Manually install a combined client/server certificate. See <i>Manually install certificates in Security on page 77</i>.</li></ul>
	Disabled (multiple client certificates)	IEEE 802.1X is not active and can't be activated until there is only one client certificate on the device. Possible solution: <ul style="list-style-type: none"><li>• Delete the redundant client certificates. See <i>Delete certificates in Security on page 77</i>.</li></ul>
	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:

# AXIS Camera Station User Manual

## Configuration

---

- 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.



# AXIS Camera Station User Manual

## Configuration

---

- 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 <sup>BETA</sup>

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 51*.

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**.

# AXIS Camera Station User Manual

## Configuration

---

2. Select an external data source and click Edit.
3. Select a view from the View drop-down list.
4. Click OK.

### 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: <ul style="list-style-type: none"><li>• OK</li><li>• <b>Storage full:</b> The storage is full. The unlocked, oldest recordings will be overwritten.</li><li>• <b>Unavailable:</b> The storage information is currently unavailable. For example, if a network storage has been removed or disconnected.</li><li>• <b>Intruding data:</b> If the slider for Recordings limit moved from the Free green area to the red Other data area, the status shows Intruding data. More storage space than what is available is being allocated to recordings.</li><li>• <b>No permissions:</b> The user is not authorized to read or write to the storage.</li></ul>
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 <i>Manage storage on page 83</i> .
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.

# AXIS Camera Station User Manual

## Configuration

---

### 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 *Troubleshooting recording and playback*.
- 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

- 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.

# AXIS Camera Station User Manual

## Configuration

---

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 <i>Device configuration tab <sup>BETA</sup> on page 81</i> .
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.

# AXIS Camera Station User Manual

## Configuration

---

- 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

Motion recording or continuous recording is configured automatically when cameras are added to AXIS Camera Station.

To adjust recording settings, or to disable recording for some cameras, go to **Configuration > Recording and events > Recording method**.

AXIS Camera Station supports:

- *Motion recording on page 85*
- *Continuous and scheduled recording on page 86*
- *Manual recording on page 87*
- *Rule triggered recording on page 87*
- *Failover recording on page 87*
- *Fallback recording on page 88*

## Motion recording

Motion detection can be used with all Axis network cameras and video encoders. Recording only when motion is detected saves considerably on storage space compared to continuous recording.

To enable or disable motion recording, or to change settings:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera in the list.
3. Turn on **Motion detection** to enable motion recording. To disable, turn it off. If the settings are greyed out, the feature is unavailable on that model.
4. Under **Video settings**:
  - The **High** profile is selected by default. To change it, select another profile from the **Profile** drop-down list. To edit profile settings, see *Streaming profiles*.
  - Select the number of seconds to include in a recording before the motion is detected under **Prebuffer**.
  - Select the number of seconds to include in a recording when the motion is no longer detected under **Postbuffer**.
  - Select **Raise alarm** to raise an alarm when motion is detected.
5. Under **Schedule**, select a schedule or click **New** to create a new schedule.
6. Under **Advanced**, set an interval time between two successive triggers in the **Trigger period** field. 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.

# AXIS Camera Station User Manual

## Configuration

---

7. 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*.
8. Click **Apply**.



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

[www.axis.com/products/online-manual/34074#t10161010](http://www.axis.com/products/online-manual/34074#t10161010)

*Configure motion detection*

### Tips:

- If too many or too few moving objects are detected, see *Troubleshooting motion detection*.
- If the size of the recorded files is too large for the available storage space, try the following:
  - Select a profile with lower resolution, lower frame rate or increased compression. Video format H.264 results in smaller files than the other formats.
  - Use a schedule to only record during specific time periods.
  - Change **Motion Settings** to reduce the number of detected objects.

### Note

You can configure motion recording using Action rules. When using Action rules for motion recording, ensure to disable motion recording in Recording method.

## Continuous and scheduled recording

A continuous recording saves images continuously. This requires more storage space than the other recording options.

To enable or disable continuous recording, or to change settings:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera in the list.
3. Turn on **Continuous** to enable continuous recording.
4. Under **Video settings**:
  - The **Medium** profile is selected by default. To change it, select another profile from the **Profile** drop-down list. To edit profile settings, see *Streaming profiles*.
5. Under **Schedule**, select a schedule or click **New** to create a new schedule.
6. Under **Advanced**, turn on **Average bitrate** and set **Max storage**. The estimated average bitrate is displayed based on the specified max storage and the retention time. The maximum average bitrate is 50000 Kbit/s. See *Configure average bitrate on page 90*.
7. Click **Apply** to save settings.

**Tips:** If the size of the recorded files is too large for the available storage space, try the following:

# AXIS Camera Station User Manual

## Configuration

---

- Select a profile with lower resolution, lower frame rate or higher compression. Video format H.264 results in smaller files than the other formats.
- Use a schedule to only record during specific time periods.
- Consider using motion recording.

### Manual recording

For how to record manually, see *Record manually*.

To configure manual recording settings:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera in the list.
3. Under **Manual**, configure Video settings:
  - The **High** profile is selected by default. To change it, select another profile from the **Profile** drop-down list. To edit profile settings, see *Streaming profiles*.
  - Select the number of seconds to include in a recording before the motion is detected under **Prebuffer**.
  - Select the number of seconds to include in a recording when the motion is no longer detected under **Postbuffer**.
4. Click **Apply**.

### Rule triggered recording

A rule triggered recording is started and stopped according to a rule created in Action rules.

Rules can, for example, be used 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, go to **Configuration > Recording and events > Action rules**. See *Action rules*.

#### Note

If using a rule to configure motion recording, ensure to disable motion recording to avoid duplicate recordings. Go to **Configuration > Recording and events > Recording method**, select the camera and turn off **Motion detection**.

### Failover recording

Failover recording can be enabled on a camera with an SD card and firmware 5.20 or later. Failover recording will only affect H.264 recordings.

To enable failover recording:

1. Go to **Configuration > Storage > Selection**.
2. Select a camera and then select **Failover recording**.
3. Click **Apply** to save settings.

Once you have enabled failover recording, the camera automatically starts recording onto the SD card when the connection with AXIS Camera Station is lost and can't be reestablished within 10 seconds.

#### Note

Any restart of the AXIS Camera Station server will not trigger failover recordings. For example when you run Database maintainer, restart AXIS Camera Station Service Control, and restart the computer where the server is installed.

# AXIS Camera Station User Manual

## Configuration

---

When connection is restored, the failover recording is imported to AXIS Camera Station and marked with a dark grey color in the timeline. The camera will try to compensate for the 10 seconds delay before the failover recording is triggered by storing the last 10 seconds of a stream in its internal memory. Short gaps about 1 - 4 seconds might still appear.

When the recording method is set as:

- **Motion detection with prebuffer**

AXIS Camera Station continuously requests recording stream from the camera and processes it on the server side. In case of disconnection for more than 10 seconds, failover recording will be triggered and the camera will continuously record to the SD card until connection is restored or the SD card becomes full.

- **Motion detection without prebuffer**

- AXIS Camera Station requests recording stream from the camera only when motion is detected. In case of disconnection for more than 10 seconds when motion recording is not ongoing, failover recording will not be realized even if motion is detected afterwards when the camera is still disconnected.
- AXIS Camera Station requests recording stream from the camera only when motion is detected. In case of disconnection for more than 10 seconds when motion recording is ongoing, failover recording will be triggered and the camera will continuously record to the SD card until connection is restored or the SD card becomes full.

- **Continuous recording**

AXIS Camera Station continuously requests recording stream from the camera and processes it on the server side. In case of disconnection for more than 10 seconds, failover recording will be triggered and the camera will continuously record to the SD card until connection is restored or the SD card becomes full.



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

[www.axis.com/products/online-manual/34074#t10161014](http://www.axis.com/products/online-manual/34074#t10161014)

*Use SD card for failover recording*

### Fallback recording

You can turn on fallback recording on a device with AXIS S3008 Recorder as recording storage.

Once you have turned on fallback recording, the device automatically starts a continuous recording with medium streaming profile on the recorder when the connection between AXIS Camera Station and the recorder is lost.

**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 is triggered, another continuous recording will be started with medium streaming profile. Then the stream will be duplicated on the recorder.

To turn on fallback recording, make sure that AXIS S3008 Recorder and the devices have been added and the recorder has been configured as recording storage for the device. See *Set up AXIS S3008 Recorder*.

1. Go to **Configuration > Storage > Selection**.
2. Select the device and select **Fallback recording**.



## Configuration

---

3. Click **Apply**.

### Recording method

Motion recording or continuous recording is configured automatically when devices are added to AXIS Camera Station.

Go to **Configuration > Recording and events > Recording method** to open the Recording method page. A list of all devices is displayed. Use the **Type to search** field to find devices in the list. The check marks indicate the enabled recording method for the devices. For devices of the same model, multiple devices can be configured at the same time. To customize profile settings for video and audio, see *Streaming profiles*.

#### Note

View areas do not support motion detection.

### Configure settings for motion recording

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera in the list.
3. Turn on **Motion detection** to enable motion recording. To disable, turn it off. (If the settings are greyed out, the feature is unavailable on that model).
4. Under **Video settings**:
  - The **High** profile is selected by default. To change it, select another profile from the **Profile** drop-down list. To edit profile settings, see *Streaming profiles*.
  - Select the number of seconds to include in a recording before the motion is detected under **Prebuffer**.
  - Select the number of seconds to include in a recording when the motion is no longer detected under **Postbuffer**.
  - Select **Raise alarm** to raise an alarm when motion is detected.
5. Under **Schedule**, select a schedule or click **New** to create a new schedule.
6. Under **Advanced**, set an interval time between two successive triggers in the **Trigger period** field. 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.
7. 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*.
8. Click **Apply**.

### Configure settings for continuous recording

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera in the list.
3. Turn on **Continuous** to enable continuous recording.
4. Under **Video settings**:
  - The **Medium** profile is selected by default. To change it, select another profile from the **Profile** drop-down list. To edit profile settings, see *Streaming profiles*.
5. Under **Schedule**, select a schedule or click **New** to create a new schedule.
6. Under **Advanced**, turn on **Average bitrate** and set **Max storage**. The estimated average bitrate is displayed based on the specified max storage and the retention time. The maximum average bitrate is 50000 Kbit/s. See *Configure average bitrate on page 90*.

# AXIS Camera Station User Manual

## Configuration

---

7. Click **Apply** to save settings.

### Configure settings for manual recording

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera in the list.
3. Under **Manual**, configure Video settings:
  - The **High** profile is selected by default. To change it, select another profile from the **Profile** drop-down list. To edit profile settings, see *Streaming profiles*.
  - Select the number of seconds to include in a recording before the motion is detected under **Prebuffer**.
  - Select the number of seconds to include in a recording when the motion is no longer detected under **Postbuffer**.
4. Click **Apply**.

### Configure average bitrate

With average bitrate, the bitrate is automatically adjusted over a longer timescale. So 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 will affect the quality of the selected streaming 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 > Streaming profiles** and make sure you have set H.264 or H.265 as the format for the video profile to be used for the 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 have configured.
5. Under **Advanced**, turn on **Average bitrate** and set **Max storage**. The estimated average bitrate is displayed based on the specified max storage and the retention time. The maximum average bitrate is 50000 Kbit/s.

#### Note

The max storage means the maximum space for the recordings over the retention time. It only guarantees that the recordings will not exceed the specified space. It doesn't guarantee that there will be 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 that can be installed on products with support for AXIS Camera Application Platform. Motion detection 2 requires firmware 5.60 or later. 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 motion recording is selected when cameras are added to AXIS Camera Station, AXIS Video Motion Detection 2 and 4 will only be installed on cameras with the required firmware. Other cameras will use the built-in motion detection. You can install the application from the device management page. See *Install camera application*.

When AXIS Video Motion Detection 2 or 4 is installed on the camera, motion detection detects moving objects within an area of interest.

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

# AXIS Camera Station User Manual

## Configuration

---

- **Area of interest:** An area in which moving objects are detected. Objects outside the area of interest are always ignored. The area is the polygon displayed on top of the video image. The polygon can have 3 to 20 points (corners).
- **Area to exclude:** An area within the area of interest in which moving objects will be ignored.
- **Ignore filters:** Filters that are created to ignore the moving objects detected by the application. Use as few filters as possible and configure the filters with care to ensure that no important objects are ignored. Enable 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 quickly moving shadows. Set the minimum time objects must appear in the image to trigger an alarm. The time is counted from the moment the application detects the object. Alarms are not triggered until the specified time has passed, that is, all alarms are delayed by the specified time. If the object disappears from the image within the specified time, no alarm is generated.
  - **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. Objects that are smaller than the specified width and height are ignored and do not trigger alarms. To be ignored, objects must be smaller than both width and height values.
  - **Swaying objects:** This filter ignores objects that only move a short distance, for example swaying foliage, flags and their shadows. Set distance as a percentage of the total image. Objects moving a distance that is shorter than the distance from the center of the ellipse to one of the arrowheads are ignored. The ellipse is a measure of movement and will be applied to all movement in the image.

### Note

Settings made here will change settings in the camera.

To configure motion settings:

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.
  - To add a new point, click the line between two points.
  - To remove a point, right-click the point, or click the point and click **Remove Point**.
4. Edit the exclude area.
  - To create an exclude area, click **Add Exclude Area** and configure in the same way as the area of interest.
  - To remove an exclude area, click **Remove Exclude Area**.
5. Create ignore filters.
  - To enable an ignore filter for short-lived objects, select **Short lived objects filter** and adjust the minimum time in the Time slider that objects must appear in the image to trigger an alarm.
  - To enable an ignore filter for small objects, select **Small objects filter** and adjust the size of the ignored objects in the Width and Height sliders.
  - To enable an ignore filter for swaying objects, select **Swaying objects filter** and adjust the size of the ellipse in the Distance slider.
6. Click **Apply**.

### Edit built-in motion detection

When the camera uses built-in motion detection, motion is detected within one or more include windows. An Include window is an area in which motion should be detected. An Exclude window is an area within an Include window in which motion should be

# AXIS Camera Station User Manual

## Configuration

---

ignored. Motion in areas outside Include windows is automatically ignored. You can use multiple Include and Exclude windows. In the preview window, Exclude windows are shaded.

### Note

Settings made here will change settings in the camera.

To add and edit an Include window:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera with built-in motion detection, and click **Motion Settings**. The Edit Motion Detection page is displayed.
3. Click **Add** in the Window section, and select **Include** in the Settings section.
4. The window is displayed on top of the video image. Use the mouse to move and resize the window.
5. Show all windows is selected by default. To only see this window, select **Show selected window**.
6. In the Settings section:
  - **Object size:** Object size relative to the region size. At a high level only very large objects are detected. At a low level even very small objects are detected.
  - **History:** Object memory length defines how long an object needs to be in a region before it is considered to be non-moving. At a high level an object will trigger motion detection for a long period of time. At a low level an object will trigger motion detection for a short period of time.

### Note

If no objects should appear in the region, a very high history level can be selected. This will cause motion detection to trigger as long as the object is present in the region.

- **Sensitivity:** Difference in luminance between the background and the object. At a high level ordinary colored object on ordinary backgrounds will be detected. At a low level only very bright objects on a dark background will be detected.

### Note

To only detect flashing light, select a low sensitivity. In other cases, we recommend a high sensitivity level.

7. To use the predefined settings. In the predefined settings section, select **Low**, **Moderate**, **High**, or **Very High**. **Low** detects larger objects with a shorter history. **Very High** detects smaller objects with a longer history.
8. In the Activity section, review the detected motion in the Include window. Motion is indicated by red peaks. Use the Activity window when adjusting Object size, History and Sensitivity.
9. Click **OK**.

To add and edit an Exclude window:

1. In the Edit Motion Detection page, click **Add** in the Window section, and select **Exclude** in the Settings section.
2. The window is displayed on top of the video image. Use the mouse to move and resize the window.
3. Click **OK**.

To remove an Include or Exclude window:

1. In the Edit Motion Detection page, select the window to remove.
2. Click **Remove** in the Window section.
3. Click **OK**.

# AXIS Camera Station User Manual

## Configuration

---

### I/O ports

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

There are two types of I/O ports:

- **Input port:** Used 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:** Used to connect to devices such as relays, doors, locks and alarms. Devices connected to output ports can be controlled from AXIS Camera Station.

Go to **Configuration > Recording and events > I/O ports** to view a list of all available I/O ports that are added to AXIS Camera Station.

#### Note

- When connecting to multiple AXIS Camera Station servers, you can add and manage I/O ports on any connected server by selecting the server from the **Selected server** drop-down list.
- If I/O ports have been configured using the device's configuration page, click **Reload I/O Ports** to update the list.
- Administrators can disable I/O ports for users. See *Configure user permissions*.

Use the **Type to search** field to find ports and devices.

To edit a port, select the port and click **Edit**. In the pop-up dialog, update the port information and click **OK**.

To remove a port, select the port and click **Remove**.

I/O ports are used in Action rules. Input ports are used as triggers, for example, when AXIS Camera Station receives a signal from a device connected to an input port, specified actions will be performed. Output ports are used as actions, for example, when a rule is activated, 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 be configured to 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 that can be added.
3. If I/O ports have been configured using the device's configuration page, click **Reload I/O Ports** to update the list.
4. Select the ports and click **OK**.
5. In the Port info section, review the port type and the device's IP address or hostname.
6. In the Names section, enter a name for the port, active and inactive state. These names are displayed in Action rules, in Logs and in I/O Monitoring.
7. When adding an output port, you can set the initial state of the output port when AXIS Camera Station establishes connection with the device. In the Initial State section, select **On startup set to** and select the initial state from the **State** drop-down list.

### Monitor I/O ports

#### Note


When connecting to multiple AXIS Camera Station servers, you can monitor I/O ports on any connected server by selecting the server from the **Selected server** drop-down list.

# AXIS Camera Station User Manual

## Configuration

---

To control output ports manually:

1. Go to  > **Actions** > **I/O Monitoring**.
2. Select an output port, and 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. Action rules is powerful to reduce the number of recordings, to interact with devices connected to I/O ports and to alert operators about important events.

Go to **Configuration** > **Recording and events** > **Action rules** and a list of rules that have been added to AXIS Camera Station is displayed. Use the **Type to search** field to find a rule.

#### Note

- When connecting to multiple AXIS Camera Station servers, you can create and manage action rules on any connected server by selecting the server from the **Selected server** drop-down list.
- For third-party devices, available actions can depend on the selected device. Many of these actions can require additional configuration in the device.

To edit an existing rule, select the rule and click **Edit**.

To remove an existing rule, select the rule and click **Remove**.

#### Create a new rule

1. Go to **Configuration** > **Recording and events** > **Action rules** and click **New**.
2. Create triggers to define when a rule should be activated. When all triggers are added, click **Next**. See *Add triggers*.
3. Create actions to define the actions to perform when the rule is activated. When all actions are added, click **Next**. See *Add actions*.
4. Create schedules to reduce the number of alarms and recordings. When satisfied, click **Next**.
  - Select **Always** to enable the rule at all times.
  - Select **Custom schedule** and select a schedule from the drop-down list. You can create a new schedule or edit an existing schedule. See *Schedules*.
5. Review the information in the Details page. Enter a name for the rule in the **Name** field, and click **Finish** to enable the rule.

### Add triggers

Triggers define when a rule should be activated. A rule can have multiple triggers. The rule will be active as long as any of the specified triggers are active.

The following triggers are available:

- **Motion detection:** The motion detection trigger is activated when the camera detects motion within a defined area. Detection is performed by the camera which means that no processing load is added to the AXIS Camera Station server. To find out if motion recording is enabled, go to **Configuration** > **Action rules**. See *Create motion detection triggers*.

#### Note

Avoid using the motion detection trigger to start recordings if motion recording is enabled in the camera.

- **Active tampering alarm:** The tampering trigger is activated when the device is repositioned or when the lens is covered, sprayed or severely defocused. Tampering detection is performed by the device which means that no processing load is added to the AXIS Camera Station server. Active tampering alarm is available for devices with tampering support and with firmware 5.11 or later. See *Create active tampering alarm triggers*.

# AXIS Camera Station User Manual

## Configuration

---

- **AXIS Cross Line Detection:** AXIS Cross Line Detection is an application that can be installed on cameras and video encoders. The application detects moving objects that cross a virtual line and can, for example, be used to monitor entrance and exit points. Before using AXIS Cross Line Detection as a trigger, the application must be installed on the camera. Download the application from [www.axis.com](http://www.axis.com). Then go to the Device management page, select the camera, right-click and select Install camera application. See *Install camera application*. The trigger is activated when an application detects a moving object. Since detection is performed by the application on the camera, no processing load is added to the AXIS Camera Station server. AXIS Cross Line Detection can be installed on products with support for AXIS Camera Application platform. See *Create AXIS Cross Line Detection triggers*.
- **System event and error:** A system event and error trigger is activated when recording errors occur, a storage becomes full, a network storage can't be contacted, or connection to one or more devices is lost. See *Create system event and error triggers*.
- **Input/Output:** 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. Before using an I/O trigger, the I/O port must be added to AXIS Camera Station. Go to **Configuration > I/O ports**. See *Create input/output triggers*.
- **Device event:** This trigger uses events directly from the camera or auxiliary device and can be used if no suitable trigger is available in AXIS Camera Station. Available events depend on the device. Many of these events can require additional configuration in the device. See *Create device event triggers*.
- **Action button:** Action buttons are used to start and stop actions in Live view. Action buttons are displayed on top of the live view or in a map. When clicking the button, the action will be performed. The same button can be used in different rules, but each rule can only have one action button trigger. See *Create action button triggers*.
- **AXIS Entry Manager event:** This 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. See *Create AXIS Entry Manager event triggers on page 104*.
- **External HTTPS:** The external HTTPS trigger makes it possible for external applications to trigger events in AXIS Camera Station through HTTPS communication. This trigger can be used to integrate AXIS Camera Station with external applications. See *Create external HTTPS triggers on page 104*.

### Triggers

Trigger	Generated by	Log message	Description
Motion Detection	Device with AXIS Video Motion Detection configured	Motion detected on <camera name>.	Motion is detected on the camera.
		Motion detection off on <camera name>.	Motion is no longer detected on the camera.
Active Tampering Alarm	Device with the active tampering alarm configured	Tampering detected on <camera name>.	The active tampering alarm is raised on the camera.
		Tampering no longer detected on <camera name>.	The active tampering alarm is no longer raised on the camera.
AXIS Cross Line Detection	Device with AXIS Cross Line Detection configured	Motion detected by AXIS Cross Line on <camera name>.	Motion is detected on the camera by AXIS Camera Detection application.
		Motion no longer detected by AXIS Cross Line on <camera name>.	Motion is no longer detected on the camera by AXIS Camera Detection application.

# AXIS Camera Station User Manual

## Configuration

System Event and Error	AXIS Camera Station server	Lost connection to: <camera name>.	The server can't connect to the camera.
		Disk full.	The recording disk is full.
		Disk access denied.	The server can't access the recording disk.
		Recording directory <directory path> is not accessible.	The server can't access the recording directory.
		Recording directory <directory path> is accessible.	The server can access the recording directory again.
		Recording error on: <camera name>.	The server fails to record video from the camera.
		Recording audio error on: <camera name>.	The server fails to record video from the camera because of audio problems.
Input/Output	Device with Input/Output ports configured	Port: <port name> set to: <state>.	The I/O port changes its state.
Device Event	Device when device events occur. Device events are dynamic description and depend on what the device has for functionality.	Device event detected on: <device name>.	A device event from the device becomes active.
		Device event no longer detected on: <device name>.	A device event from the device becomes inactive.
Action Button	AXIS Camera Station client	Action Button <rule name> was triggered by button <button name>.	A user turns on the action button.
		Action Button <rule name> is no longer triggered by button <button name>.	A user turns off the action button.
AXIS Entry Manager Event	AXIS Entry Manager	Access control point event detected on <access point name> (in).	A person enters the access control point.
		Access control point event no longer detected on <access point name> (in).	A person no longer enters the access control point.
		Access control point event detected on <access point name> (out).	A person exits the access control point.
		Access control point event no longer detected on <access point name> (out).	A person no longer exits the access control point.
		Access control door event detected on <door name>.	An event from the access control door becomes active.
		Access control door event no longer detected on <door name>.	An event from the access control door becomes inactive.
External HTTPS	External applications through HTTPS communication	External HTTPS trigger on <trigger name> activated.	The server receives a signal to activate the trigger.
		External HTTPS trigger <trigger name> deactivated.	The server receives a signal to deactivate the trigger.

### Create motion detection triggers

The motion detection trigger is activated when the camera detects motion within a defined area. Detection is performed by the camera which means that no processing load is added to AXIS Camera Station server.



# AXIS Camera Station User Manual

## Configuration

---

### Note

Avoid using motion detection triggers to start recordings if motion recording is enabled in the camera. To find out if motion recording is enabled, go to **Configuration > Action rules**.

To create an motion detection trigger:

1. Go to **Configuration > Recording and events > Action rules**, and click **New**.
2. Click **Add** and select **Motion detection**. Click **OK**.
3. In the pop-up page:
  - In the **Trigger on** field, select the camera that will detect motion.
  - 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.
  - 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*.
4. 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](http://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.

# AXIS Camera Station User Manual

## Configuration

---

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.

# AXIS Camera Station User Manual

## Configuration

---

- 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](http://www.axis.com/partners) and [www.axis.com/vapix](http://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

# AXIS Camera Station User Manual

## Configuration

---

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	Heartbeat
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

# AXIS Camera Station User Manual

## Configuration

---

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 Camera Station User Manual

## Configuration

### 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 <b>Yes</b> 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: <ul style="list-style-type: none"> <li>• Device casing is opened or closed</li> <li>• Device motion</li> <li>• Connected reader is removed from wall</li> <li>• 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.</li> </ul>
	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 <b>Any</b> 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.

# AXIS Camera Station User Manual

## Configuration

---

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**.

# AXIS Camera Station User Manual

## Configuration

---

- 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**.



# AXIS Camera Station User Manual

## Configuration

---

2. Click **Add** and select **External HTTPS**. Click **OK**.
3. Enter the trigger name in the **Trigger name** field.
4. Click **Advanced** to set trigger period to handle fluctuating signals and to avoid starting multiple actions.
  - If a trigger is activated within the trigger period time, the rule system simply continues to run the ongoing action without activating any additional actions.
  - If automatic deactivation time is used in combination with the trigger period, the trigger deactivates after both the automatic deactivation time and the trigger period has passed.
5. 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.
6. 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 109*.
- **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 110*.
- **Access control:** This action includes door actions and zone actions in AXIS Camera Station Secure Entry. See *Create access control actions on page 110*.

# AXIS Camera Station User Manual

## Configuration

---

### 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 > Streaming 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**.

# AXIS Camera Station User Manual

## Configuration

---

### 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**.

# AXIS Camera Station User Manual

## Configuration

---

- 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.

# AXIS Camera Station User Manual

## Configuration

---

### 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.

# AXIS Camera Station User Manual

## Configuration

---

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*.

#### Note

It currently requires that both AXIS Camera Station server and AXIS Camera Station mobile app are connected over Secure Remote Access. See *Axis Secure Remote Access on page 117*.

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 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.

# AXIS Camera Station User Manual

## Configuration

---

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 **Override schedule** and select the days.
  - 5.2 In the timeline, select the time slots that the schedule should be on.
  - 5.3 To remove an override, click . To remove all overrides, click **Clear all**.
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:

# AXIS Camera Station User Manual

## Configuration

---

- Install AXIS A1601 Network Door Controller. See *Add devices on page 55*.
  - Configure the door controller. See *Configure access control on page 137*.
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 137* and *Access management on page 156*.



# AXIS Camera Station User Manual

## Configuration

---

- Install an Axis network audio device and associate the audio device with a camera. See *Streaming profiles* on page 62.
  - 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 93.
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 software settings like startup options. See *Client settings* on page 114.

# AXIS Camera Station User Manual

## Configuration

---

- Edit client specific streaming performance settings like video scaling and hardware decoding. See *Streaming* on page 115.

### Client settings

Go to **Configuration > 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.

**Show What's new after each update** is turned on by default to show the What's new tab after you start the client after each AXIS Camera Station update. See *What's new tab* on page 180.

#### 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 door station notification window** to display a notification window when the call button is pushed on the door station 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.

# AXIS Camera Station User Manual

## Configuration

---

### 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.

### Language

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

### Features

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

### 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**.

## 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.

### Mode

# AXIS Camera Station User Manual

## Configuration

---

- **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 streaming profile Low on this client**, and AXIS Camera Station will always use the Low streaming profile for Live view. See *Streaming profiles*.

### Note

This setting affects H.264 and M-JPEG video. MPEG-4 is not affected.

- Turn on **Suspend video streams for inactive tabs**, and video streams in the inactive tabs are suspended.
- Turn on **Suspend video streams in door station notification window**, and video streams in the door station 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 door stations** to be able to listen and speak to door stations even if there are no ongoing calls from door stations.

### 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.

# AXIS Camera Station User Manual

## Configuration

---

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](http://www.axis.com). By default, this option is pre-selected. To manually update firmware, see *Upgrade firmware on page 74*.

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.

[www.axis.com/products/online-manual/34074#t10129865](http://www.axis.com/products/online-manual/34074#t10129865)

*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 Camera Station User Manual

## Configuration

---

### 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.

### AXIS Camera Station update

AXIS Camera Station automatically checks for new versions of the client and server. When a new version is available, you will be prompted with a request to download the new software. Use the latest version of AXIS Camera Station to ensure the latest features and improvements to your Axis experience.

#### Note

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

1. Go to **Configuration > Connected services > AXIS Camera Station update**.
2. Check for updates automatically or manually.
  - Under **Automatic check for updates**, select **Every start-up** to check for new software versions on each startup.
  - Under **Automatic check for updates**, select **Never**. Click **Check for updates** to manually check for new software version.
3. When there is a new software version, it is listed under **Update status**. Click **View details** to see the release notes. Click **Download software** to download the new version of the software.

## Configure server

### 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**.

# AXIS Camera Station User Manual

## Configuration

---

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 Roles 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**.

## 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 35*.

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)\`

# AXIS Camera Station User Manual

## Configuration

---

- 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>

### 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 a list of SMTP servers that have been added. Use the arrows to change the order of the servers in the list.

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. The default port number is 25.
4. In the User section, enter the name to appear in the email and email address to use as sender.
5. In the Logon section:
  - Select **Use authentication** if a username and password are required for this server. Enter the username and password to access the server.



# AXIS Camera Station User Manual

## Configuration

---

- Select **Use TLS** if the SMTP server uses TLS.

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.
- **Unknown recipient:** The specified email address is incorrect. Try again with a new email address.
- **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.

### 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.

### Time synchronization

Windows NTP Server is automatically activated when installing AXIS Camera Station. If you want to use this NTP server to configure all devices connected to AXIS Camera Station, select **Use this server as the NTP server for connected devices**.

### 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 80*.

### 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

# AXIS Camera Station User Manual

## Configuration

---

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.

### 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.

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.	<ul style="list-style-type: none"><li>• Add the user in the user permission dialog.</li><li>• Verify the username and password.</li></ul>
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.

# AXIS Camera Station User Manual

## Configuration

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.	<ul style="list-style-type: none"><li>• Check that the network is working properly.</li><li>• Check that the server is started.</li></ul>
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.	<ul style="list-style-type: none"><li>• Check that the network is working properly.</li><li>• Check that the server is started.</li></ul>
Invalid hostname	The DNS was not able to translate the hostname into an IP address.	<ul style="list-style-type: none"><li>• Check that the spelling of the hostname is correct.</li><li>• Check that the DNS has the information it needs.</li></ul>
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.

[www.axis.com/products/online-manual/34074#t10129754](http://www.axis.com/products/online-manual/34074#t10129754)

*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.

# AXIS Camera Station User Manual

## Configuration

---

- 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.

[www.axis.com/products/online-manual/34074#t10129856](http://www.axis.com/products/online-manual/34074#t10129856)

*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](http://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.

# AXIS Camera Station User Manual

## Configuration

---

### 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](http://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 127*

### 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.

# AXIS Camera Station User Manual

## Configuration

---

- 1.3 Click **Go to AXIS License Portal**.
2. In the AXIS License Portal [www.axis.com/licenses](http://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.  
[www.axis.com/products/online-manual/34074#t10129696](http://www.axis.com/products/online-manual/34074#t10129696)

*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](http://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**.

# AXIS Camera Station User Manual

## Configuration

---



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

[www.axis.com/products/online-manual/34074#t10129682](http://www.axis.com/products/online-manual/34074#t10129682)


*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](http://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.

[www.axis.com/products/online-manual/34074#t10158330](http://www.axis.com/products/online-manual/34074#t10158330)

*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](http://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**.

# AXIS Camera Station User Manual

## Configuration

---

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



# AXIS Camera Station User Manual

## Configuration

---

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 *Troubleshooting user searches*.
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

# AXIS Camera Station User Manual

## Configuration

---

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 System Health Monitoring:** Allow accessing System Health Monitoring.

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.

## Certificates

To manage certificates between the AXIS Camera Station server and the devices,

1. Go to **Configuration > Security > Certificates** to configure and enable a certificate authority for automatic certificate management.
2. Go to **Configuration > Devices > Management > Security** to manage the HTTPS and IEEE 802.1X certificates for secure communication. See *Security on page 77*.

### 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 as a root CA

# AXIS Camera Station User Manual

## Configuration

---



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

[www.axis.com/products/online-manual/34074#t10172855](http://www.axis.com/products/online-manual/34074#t10172855)

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. AXIS Camera Station can generate a self-signed root certificate and private key which is protected by a passphrase of your choice. A CA certificate generated by AXIS Camera Station is valid for 10 years.

To generate a CA:

1. Go to **Configuration > Security > Certificates**.
2. In the Certificate authority section, click **Generate**.
3. Provide your passphrase and click **OK**.
4. When the self-signed root certificate is generated, it is displayed in the box next to the **Import** button.
  - Click **View** to view the details of the CA certificate.
  - Click **Export**.
  - Select **No** 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.
  - Select **Yes** to export the CA certificate and the private key of the CA in .pfx or .p12 formats. The backup data is protected by the passphrase used to generate the CA.
5. To enable automatic renewal of the client/server certificates on devices that have HTTPS or IEEE 802.1X enabled, select **Remember passphrase**. Provide your passphrase and click **OK**.
6. Select the number of valid days of the signed client/server certificates.

### AXIS Camera Station as an intermediate 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.

To import a CA:

1. Go to **Configuration > Security > Certificates**.
2. In the Certificate authority section, click **Import**.
3. Provide your passphrase and click **OK**.
4. When the certificate is imported, it is displayed in the box next to the **Import** button.
5. Select the number of valid days of the signed client/server certificates.

### AXIS Camera Station not used as CA

If a certificate authority is not configured, you have to create the client/server certificates outside of AXIS Camera Station. If you are not willing to allow AXIS Camera Station to sign the certificates on your behalf, you need to manually install the certificates on devices. See *Manually install certificates* in *Security on page 77*.

# AXIS Camera Station User Manual

## Configuration

---

### 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 accept any HTTPS certificate enabling 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.

#### 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.

# AXIS Camera Station User Manual

## Configuration

---

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

- 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 if you have selected **Remember passphrase**.
- 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 your passphrase

If you forget your passphrase of the certificate authority:

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. Remove the existing CA certificate in the Certificate authority section.
3. Click **Generate** and reset your passphrase.
4. Click **Export** and **No** to save the CA certificate locally.
5. Go to **Configuration > Devices > Management** and enable HTTPS on selected devices.
6. 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.

# AXIS Camera Station User Manual

## Configuration

---

To configure and enable HTTPS communication:

1. 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.

[www.axis.com/products/online-manual/34074#t10137842](http://www.axis.com/products/online-manual/34074#t10137842)

*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.
3. To enable automatic renewal of the server certificates on the devices, ensure **Remember passphrase** is selected. Provide your passphrase and click **OK**.

**Note**

For increased security, we recommend not selecting **Remember passphrase**.

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**.

# AXIS Camera Station User Manual

## Configuration

---

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, a 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 if you have selected **Remember passphrase**. 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. Select the certificate authority
2. Select the authentication CA certificate
3. Select the client certificate common name

# AXIS Camera Station User Manual

## Configuration

---

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.
4. To enable automatic renewal of the client certificate, select **Remember passphrase**. Provide your passphrase and click **OK**.

### Note

For increased security, we recommend not selecting **Remember passphrase**.

### 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, a 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 if you have selected **Remember passphrase**. 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.



# AXIS Camera Station User Manual

## Configuration

---

### 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 74*.
- Turn on time synchronization under **Configuration > Server > Settings**. See *Server settings on page 120*.
- Set date and time for the controller under **Configuration > Devices > Management**. See *Set date and time on page 75*.
- Enable HTTPS on the controller under **Configuration > Devices > Management**. See *Security on page 77*.

### Workflow to configure access control

1. To edit the predefined identification profiles or create a new identification profile, see *Identification profiles on page 147*.
2. To use a custom setup for card formats and PIN length, see *Card formats and PIN on page 148*.
3. Add a door and apply an identification profile to the door. See *Add a door on page 139*.
4. Configure the door.
  - *Add a door monitor on page 142*
  - *Add emergency input on page 143*
  - *Add a reader on page 143*
  - *Add a REX device on page 145*
5. Add a zone and add doors to the zone. See *Add a zone on page 145*.

### 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.
Door side A in zone	The zone that side A of the door is in.



# AXIS Camera Station User Manual

## Configuration

---

Door side B in zone	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. <ul style="list-style-type: none"><li>• <b>Online:</b> The door is online and works normally.</li><li>• <b>Reader offline:</b> The reader in the door configuration is offline.</li><li>• <b>Reader error:</b> The reader in the door configuration doesn't support secure channel or secure channel is not enabled for the reader.</li></ul>
<b>Zones</b>	
Name	The name of the zone.
Number of doors	The number of doors included in the zone.

In this page, you can:

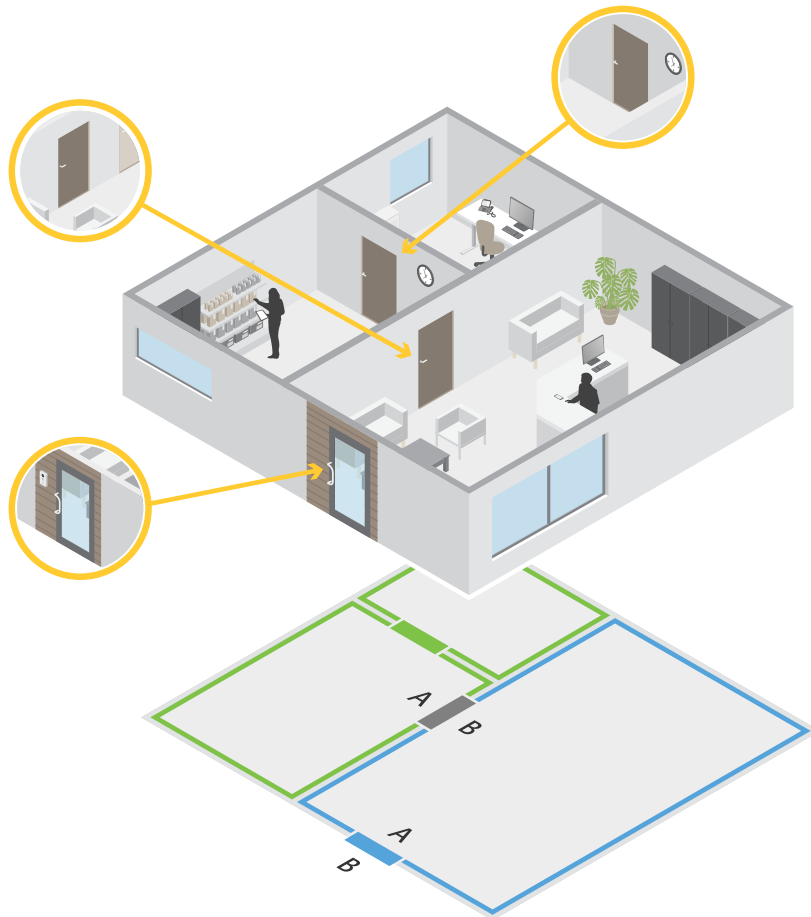
- Add, edit or remove a door. See *Add a door on page 139*.
- Add, edit or remove a zone. See *Add a zone on page 145*.
- Turn off OSDP Secure Channel for a specific reader.
  1. Select a door in the list.
  2. Click  and select **Turn off OSDP Secure Channel**.
  3. Click **Apply**.
- Turn on OSDP Secure 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**.

# AXIS Camera Station User Manual

## Configuration

---

### 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**.

# AXIS Camera Station User Manual

## Configuration


---

2. Type a door name.
3. Select a door controller from the **Connect to a door 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 first drop-down list under **Locks**.
6. To configure two locks on the door, select a relay port from the other drop-down list under **Locks**.
7. Configure the *Door settings on page 141*.
8. *Add a door monitor on page 142*
9. *Add emergency input on page 143*
10. *Add a reader on page 143*
11. *Add a REX device on page 145*


To add a door by copying an existing 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 **Connect to a door 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 **OK**.

To edit a door:

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

To remove a door:

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

# AXIS Camera Station User Manual

## Configuration

---



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

[www.axis.com/products/online-manual/34074#t10155962](http://www.axis.com/products/online-manual/34074#t10155962)

*Add and configure doors and zones*

### Door settings

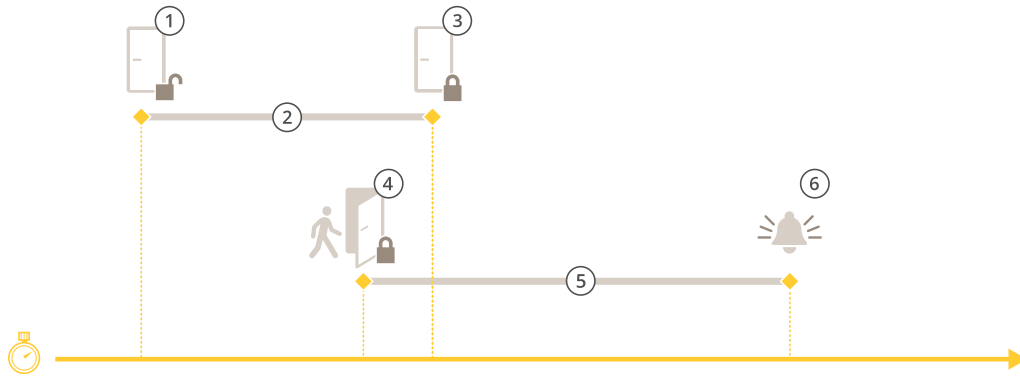
Go to the door configuration page and configure the door settings under **Door settings**.

- Under **General**, configure the following settings:
  - **Identification profile:** You must select an identification profile from a list of available identification profiles in the system.
  - **Access time:** 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:** 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.
- Under **Advanced**, configure the following settings:
  - **Long access time:** 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:** 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 after opening:** Only valid if a door monitor is configured. Set the number of milliseconds under **Relock delay time** that the door stays unlocked after the door is open for the lock.
  - **Relock after closing:** Only valid if a door monitor is configured. Set the number of milliseconds under **Relock delay time** that the door stays unlocked after the door is closed for the lock.

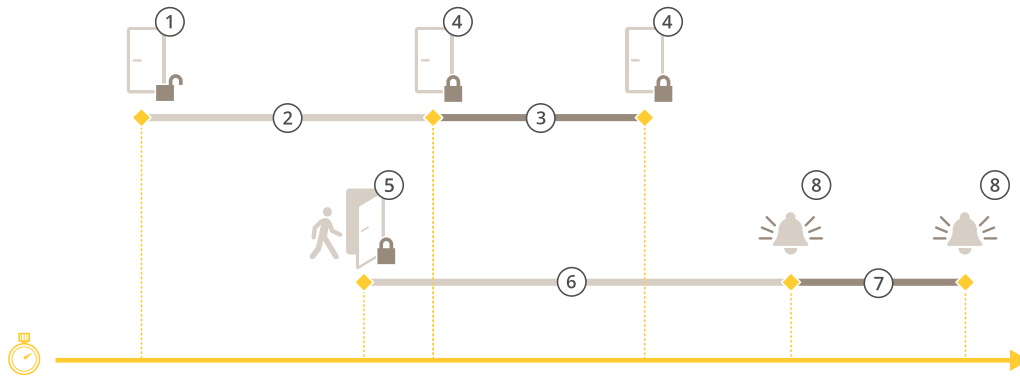
# AXIS Camera Station User Manual

## Configuration

### 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 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.

# AXIS Camera Station User Manual

## Configuration

---

1. Go to the door configuration page. See *Add a door on page 139*.
2. Click **Add door monitor**.
3. Select the I/O port that you want to configure the door monitor on.
4. Select how the door monitor circuits are connected.
  - **Open door = Open circuit:** 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.
  - **Open door = Closed circuit:** 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 146*.

### 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 139*.
2. Click **Add emergency input**.
3. Select how the circuits are connected.
  - **Emergency state = Open circuit:** Select if the emergency input circuit is normally closed. The emergency input gives the emergency state signal when the circuit is open.
  - **Emergency state = Closed circuit:** 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**.
5. Select what action is triggered when receiving the emergency state signal.
  - **Emergency action = Unlock door:** Select if you want to unlock the door when receiving the emergency state signal.
  - **Emergency action = 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 137*.

#### 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 AXIS A8207 is used as IP reader and you have 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 139*.

# AXIS Camera Station User Manual

## Configuration

---

2. Under one side of the door, click **Add reader**.
3. For RS485 readers, select **OSDP RS485** and select a reader port under **General**.
4. For readers that use Wiegand protocols, select **Wiegand** and select a reader port under **General**.
  - 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.
  - Select when the reader tamper input is in tamper.
  - **Tamper = Open circuit**: The reader gives the door the tamper signal when the circuit is open.
  - **Tamper = 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 146*.
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 144*.
6. To use **AXIS Barcode Reader**, select **AXIS Barcode Reader** and enter a name. See *Set up AXIS Barcode Reader*.
7. 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:
  - 7.1 Click **Advanced**.
  - 7.2 Turn on **Custom PIN length**.
  - 7.3 Set the **Min PIN length**, **Max PIN length**, and **End of PIN character**.
  - 7.4 Go to **Configuration > Doors and zones** and the **Card formats** column is marked as **Custom** for this door.
8. 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:
  - 8.1 Click **Advanced**.
  - 8.2 Turn on **Custom card formats**.
  - 8.3 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**.
  - 8.4 Go to **Configuration > Doors and zones** and the **Card formats** column is marked as **Custom** for this door.
9. To add a reader to the other side of the door, repeat the previous steps.

### 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 Camera Station User Manual

## Configuration

---

- 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

### 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 139*.
2. Under one side of the door, click **Add REX device**.
3. Select the I/O port that you want to configure the REX device on. If there is only one port available, it will be selected automatically.
4. Select what action is triggered when receiving the REX signal.
  - **Action = Unlock door:** Select if you want to unlock the door when receiving the REX signal.
  - **Action = None:** Select if you don't want to trigger any action when receiving the REX signal.
5. Select how the door monitor circuits are connected.
  - **REX activate = Open circuit:** Select if the REX circuit is normally closed. The REX device gives the signal when the circuit is open.
  - **REX activate = Closed circuit:** 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**.
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 146*.

### 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** and click **Add zone**.
2. Type a zone name.
3. Select the doors in the door list and click **Add**.
4. The door is set to be a perimeter door by default. To change it, select **Internal door** from the drop-down list.
5. For a perimeter door, it is set to use door side A to enter the zone by default. To change it, select **Leave zone** from the drop-down list. This option is only available for a perimeter door.
6. To remove a door from the zone, click  .


# AXIS Camera Station User Manual

## Configuration


---

7. Click **OK**.

To edit a zone:

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

To remove a zone:

1. Go to **Configuration > Access control > Doors and zones > Zones**.
2. Select a zone in the list.
3. Click  and select **Delete**.
4. Click **OK**.

### 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 142*.
- Connection between the door controller and the reader that uses Wiegand protocols. See *Add a reader on page 143*.
- Connection between the door controller and the REX device. See *Add a REX device on page 145*.

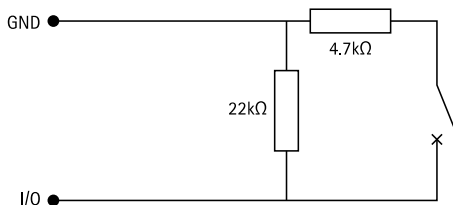
To use supervised inputs:

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 K $\Omega$  parallel resistor and a 4.7 K $\Omega$  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 k $\Omega$  and 22 k $\Omega$ .



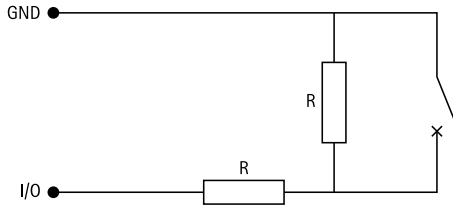
#### Serial first connection

The resistor values must be the same and within range 1-10 k $\Omega$ .

# AXIS Camera Station User Manual

## Configuration

---



### 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.

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 four 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.

*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.


# AXIS Camera Station User Manual

## Configuration

---

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.


[www.axis.com/products/online-manual/34074#t10155965](http://www.axis.com/products/online-manual/34074#t10155965)

*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:

# AXIS Camera Station User Manual

## Configuration

---

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:

# AXIS Camera Station User Manual

## Configuration

---

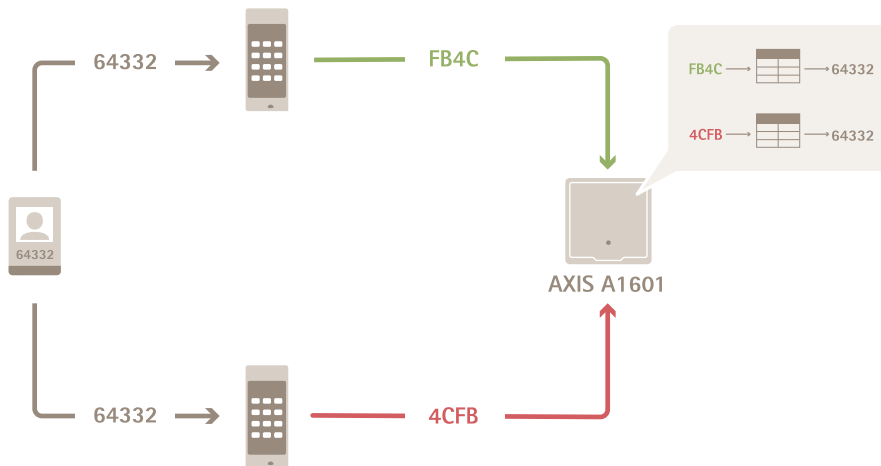
1. Go to Configuration > Access Control > Card formats and PIN.
2. Under PIN configuration, click .
3. Specify Min PIN length, Max PIN length, and End of PIN character.
4. Click OK.



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.

# AXIS Camera Station User Manual

## Configuration

---

### Invert bit order

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

64332 = 1111 1011 0100 1100  $\longrightarrow$  0011 0010 1101 1111 = 13023  
 $\longrightarrow$  Read from left      Read from right  $\longleftarrow$

### 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.

64 332 = 1111 1011 0100 1100  $\longrightarrow$  0100 1100 1111 1011 = 19707  
F B 4 C                      4 C F B

### 26-bit standard Wiegand card format

P FFFFFFF NNNNNNNNNNNNNNNN P  
①      ②                      ③                      ④



- 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 .

# AXIS Camera Station User Manual

## Configuration

---

- 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 **AXIS Barcode Reader**, 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.

### Configure smart search 2 **BETA**

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.

For requirements, limitations and how to use smart search 2, see *Smart search 2 **BETA** on page 41*.

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 postprocessing in the background for a camera, select **Active** under the **Background postprocessing** column. This increases the server load but improves the user experience.
3. Under **Storage**, select where you want to store the detections from cameras and click **Apply**.
4. Under **About smart search 2**, a list of details is displayed including the postprocessing queue length, processed and unprocessed detections.

### Configure System Health Monitoring (Preview)

#### 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.



# AXIS Camera Station User Manual

## Configuration

---

### General

To make a system visible in a multisystem setup:

1. Go to Configuration > System Health Monitoring (Preview) > General.
2. Turn on Allow System Health Monitoring through Windows Defender Firewall.

For how to set up multisystem, see *Multisystem* on page 154.

### Notifications



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

[www.axis.com/products/online-manual/34074#t10172919](http://www.axis.com/products/online-manual/34074#t10172919)

To send email notifications:

1. Configure an SMTP server and an email address to send the notifications. See *Configure an SMTP server* on page 153.
2. Configure the email addresses to receive the notifications. See *Configure email recipients* on page 153.
3. Configure the notification rules. See *Configure notification rules* on page 154.

#### Configure an SMTP server

1. Go to Configuration > System Health Monitoring (Preview) > Notifications > SMTP server.
2. Under **Server**, enter the address of the SMTP server and port to use.
3. Under **User**, enter the name to appear in the email and email address to use as sender.
4. Under **Login**:
  - Select **Use authentication** if a username and password are required for this server. Enter the username and password to access the server.
  - Select **Require TLS** if the SMTP server uses TLS. If not selected, TLS will also be used if supported.
5. Click **Save**.

#### Configure email recipients

1. Go to Configuration > System Health Monitoring (Preview) > Notifications.
2. Expand **Notifications**.
3. Under **Email recipients**, enter an email address and click **Save**. Repeat to add multiple email recipients.
4. To test the SMTP server, click **Send test email**. A message is displayed showing whether the test email was sent successfully.

# AXIS Camera Station User Manual

## Configuration

---

### 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 (Preview) > Notifications**.
2. Expand **Notifications**.
3. Under **Notification rules**, turn on or turn off the notification rules.
4. 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.

[www.axis.com/products/online-manual/34074#t10172920](http://www.axis.com/products/online-manual/34074#t10172920)

With System Health Monitoring, you can monitor the health data of several secondary systems from one main system.

1. In a secondary system, configure Windows Firewall under **Configuration > System Health Monitoring (Preview) > General**. See *General on page 153*.
2. In a secondary system, generate the system configuration to be accessed by the main system. See *Generate system configuration on page 154*.
3. Repeat the previous steps in other secondary systems.
4. In the main system, upload the system configurations. See *Retrieve data from other systems on page 155*.
5. Monitor the health data from multiple systems from the main system. See *System Health Monitoring (Preview) on page 166*.

### Generate system configuration

1. Go to **Configuration > System Health Monitoring (Preview) > Multisystem**.
2. Expand **Generate system configuration**.
3. Click **Generate**.
4. If you have not allowed System Health Monitoring through Windows Defender Firewall under **Configuration > System Health Monitoring (Preview) > General**, a dialog appears. Click **Generate**.
5. Click **Copy** to be able to upload it to the main system.
6. To view the system configuration details, click **Show details**.
7. To regenerate the system configuration, click **Delete** to delete the existing one first.

# AXIS Camera Station User Manual

## Configuration

---

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 (Preview) > Multisystem**.
2. Expand **Retrieve data from other systems**.
3. Click **Paste**. The information you have copied from the secondary system is automatically filled.
4. Check the host IP address and click **Add**. The secondary system is added and is displayed under **Available systems**.

# AXIS Camera Station User Manual

## Access management





---

### 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 137*.

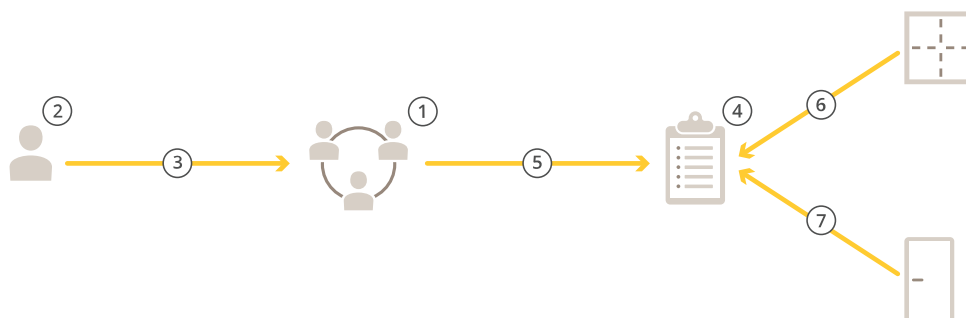
For a complete workflow to set up AXIS A1601 Network Door Controller in AXIS Camera Station, See *Set up AXIS A1601 Network Door Controller*.

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 164*.
-  **Settings:** Add custom fields to cardholder template and enable facility code in the system. See *Access management settings on page 164*.
-  **Import and export:** Import and export cardholder data. Reset the system to the state before the last import. See *Import and export on page 165*.

### 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 160*.
2. Add cardholders. See *Add a cardholder on page 157*.
3. Add cardholders to groups.
4. Add access rules. See *Add an access rule on page 160*.

# AXIS Camera Station User Manual




## Access management

---


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.

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.
8. *Add credentials on page 158.*
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:

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


# AXIS Camera Station User Manual

## Access management

---

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.

[www.axis.com/products/online-manual/34074#t10156251](http://www.axis.com/products/online-manual/34074#t10156251)



*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 157*

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 PIN credential:

1. Under **Credentials**, click  and .
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**.

# AXIS Camera Station User Manual

## Access management




---

5. Under **Expiration date**:



- 5.1 Under **Valid from**, click  and select a date.
- 5.2 Under **Valid to**, select an option from the drop-down list.
  - **No end date**: The credential will never expire.
  - **Date**: Select a specific date 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:

1. Under **Credentials**, click  and .
2. Enter a name.
3. Under **Expiration date**:
  - 3.1 Under **Valid from**, click  and select a date.
  - 3.2 Under **Valid to**, select an option from the drop-down list.
    - **No end date**: The credential will never expire.
    - **Date**: Select a specific date 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.
4. 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**.

# AXIS Camera Station User Manual

## Access management





---

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**.

### 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. To add cardholders to the group:
  - 4.1 Under **Cardholders**, click .
  - 4.2 Select a cardholder and click **Add**.
  - 4.3 Repeat to add multiple cardholders. Click  to exit.
5. 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:



# AXIS Camera Station User Manual


## Access management

---


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**.

# AXIS Camera Station User Manual

## Access management

---



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





[www.axis.com/products/online-manual/34074#t10156249](http://www.axis.com/products/online-manual/34074#t10156249)

*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**.

# AXIS Camera Station User Manual

## Access management

---



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

[www.axis.com/products/online-manual/34074#t10158421](http://www.axis.com/products/online-manual/34074#t10158421)

*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.

[www.axis.com/products/online-manual/34074#t10158421](http://www.axis.com/products/online-manual/34074#t10158421)

*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**.

# AXIS Camera Station User Manual

## Access management

---

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 147*.

To edit the email template:

# AXIS Camera Station User Manual

## Access management

---

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.

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.

1. Go to **Access management > Import and export**.
2. Select **Import** from the **Select action** drop-down list.
3. Select **New** 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.
  - 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 and exports the cardholder photos to `C:\Program Files\Axis Communications\AXIS Camera Station\Secure Entry\Cardholder photos`.

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

# AXIS Camera Station User Manual

## System Health Monitoring (Preview)

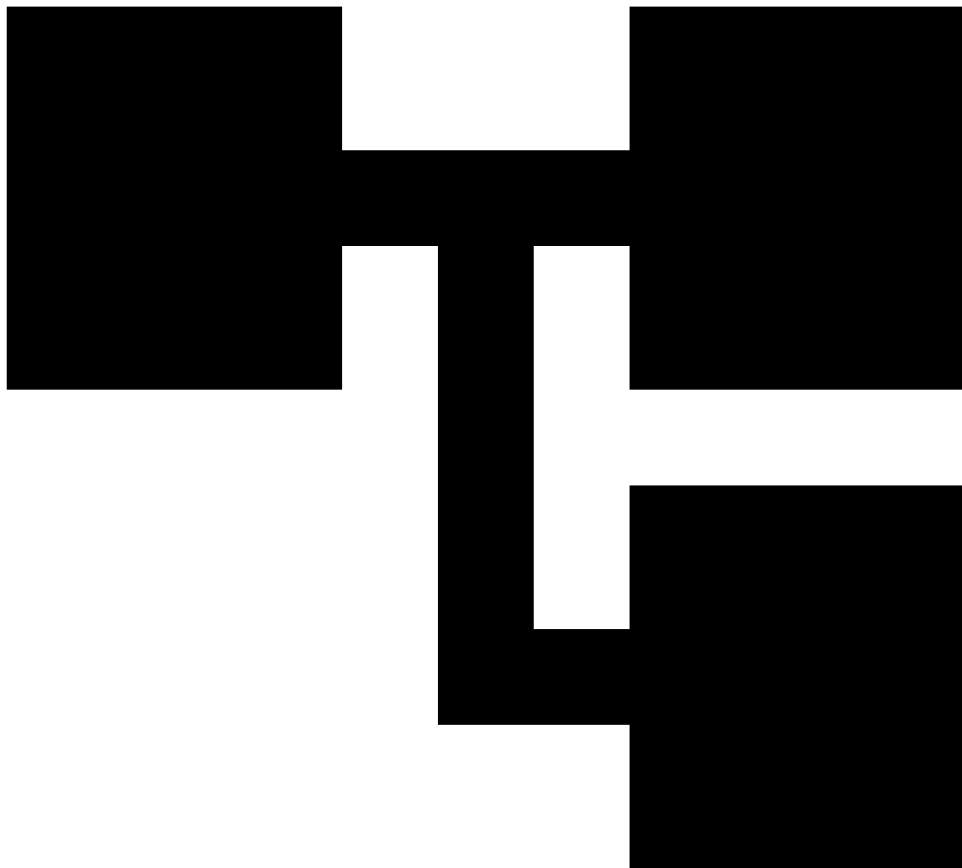
---

### System Health Monitoring (Preview)

Click **+** and select **System Health Monitoring (Preview)** 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.

It contains the following pages:

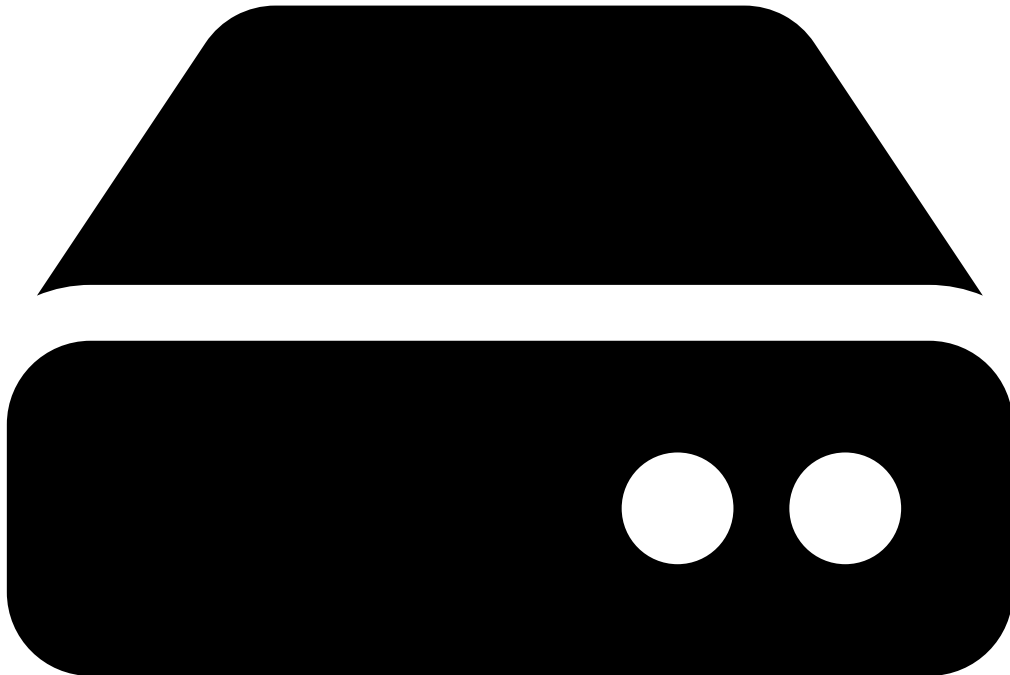



- Inventory: Shows a summary of the devices and systems that you have access to. See *Inventory on page 168*.

# AXIS Camera Station User Manual

## System Health Monitoring (Preview)

---



- Storage: Shows that storage summary and recording details of each camera from the monitored systems. See *Storage on page 168*.
-  Notifications: Shows the System Health Monitoring logs from the monitored systems. See *Notifications on page 169*.

### Limitations

- Monitoring of storage space for recordings done on AXIS S3008 Recorder is not yet supported.
- When retention time is not fulfilled, warnings are only presented for continuous recordings.
- Inactivated storage devices are still visible and gathered data are kept for up to two weeks.
- Notification settings only affect the local System Health Monitoring server.
- Accessing System Health Monitoring in AXIS Camera Station requires administrator privileges.
- Recordings except for continuous and motion triggered recordings are flagged with None as recording type.

# AXIS Camera Station User Manual

## System Health Monitoring (Preview)

---

### Workflow

1. *Configure System Health Monitoring (Preview) on page 152*
  - Set up notifications. See *Notifications on page 153*.
  - Set up multisystem. See *Multisystem on page 154*.
2. Monitor the health data from AXIS Camera Station systems.
  - *Inventory on page 168*
  - *Storage on page 168*
  - *Notifications on page 169*

### Access System Health Monitoring through web browser

1. To access a local System Health Monitoring system, go to `https://localhost:56256` in a web browser.
2. To access a remote System Health Monitoring system:
  - Turn on **Allow System Health Monitoring through Windows Defender Firewall** under **Configuration > System Health Monitoring > General**.
  - In a web browser, go to `https://<server_address>:56256`.
3. For first-time access, a security warning is displayed. Click **Advanced** and continue to access the page.
4. Log in using a credential with permission to access System Health Monitoring. See *User or group privileges on page 129*.

### Inventory

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

1. Go to **System Health Monitoring (Preview)**.
2. Click **Inventory**.
  - To view a summary of a system, expand the system and 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, expand the system and 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 generate AXIS Camera Station system report, click **☰** and select **AXIS Camera Station system report**. See *System report on page 178*.
  - To generate System Health Monitoring report:
    1. Click **☰** and select **System Health Monitoring report**.
    2. To include the database in the report, select **Include all databases** and click **Generate**.
    3. When the report is ready, click to save it.



# AXIS Camera Station User Manual

## System Health Monitoring (Preview)

### 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 (Preview)**.
2. Click **Storage**.
3. When monitoring multisystem health data, select a system from the **Systems** drop-down list.

Item	Description
<b>Storage summary</b>	
Status	The storage status. See <i>Configure storage on page 82</i> .
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.
<b>Recording details of each camera</b>	
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 <b>Configuration &gt; Storage &gt; Selection</b> .
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 (Preview)**.
2. Click **Notifications**.

Item	Description
Status	(empty): Normal status. Warning icon: An SMTP server has been configured but the notification email couldn't be sent.
Notification sent	The time when the notification was sent.

# AXIS Camera Station User Manual

## System Health Monitoring (Preview)

---


Item	The device name for notifications triggered by <code>device down</code> . Or <code>system</code> for notifications triggered by <code>system down</code> .
System	The name of the system on which the event occurs.
Rule	The rule that has triggered the notification. <code>System down</code> or <code>Device down</code>
Detected	The time when the issue was detected.
Resolved	The time when the issue was resolved.

# AXIS Camera Station User Manual

## Hotkeys

---

### 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

### AXIS T831x Video Surveillance Control Board

#### Note










Joystick buttons 7-10 are not supported by AXIS T8311 Video Surveillance Joystick. See *Input devices*.

Joystick	AXIS T8311 button
Button 1	J1
Button 2	J2

# AXIS Camera Station User Manual

## Hotkeys

---


Button 3	J3
Button 4	J4
Button 5	L
Button 6	R
Keypad	AXIS T8312 key
A	
B	
C	
D	
E	
Jog dial	AXIS T8313 button
Jog 1	L
Jog 2	
Jog 3	
Jog 4	
Jog 5	
Jog 6	R

# AXIS Camera Station User Manual

## Logs

---

### 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.
Plugin	The plugin 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.
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


# AXIS Camera Station User Manual

## Logs

---

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.

# AXIS Camera Station User Manual



## Alarms

---






### 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 192*.

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.
- **Plugin:** The plugin 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**.

# AXIS Camera Station User Manual

## Tasks

---

### 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: <ul style="list-style-type: none"><li>• <b>Canceling:</b> Cleaning up before canceling the task.</li><li>• <b>Canceled:</b> Cleaning is complete and the task is canceled.</li><li>• <b>Error:</b> Task completed with errors, that is, the task failed on one or more devices.</li><li>• <b>Finished:</b> Task completed.</li><li>• <b>Finished during lost connection:</b> Displayed if the task completed while the connection to the server was down. Task status could not be determined.</li><li>• <b>Lost connection:</b> Displayed if the client lost connection with the server while the task was running. Task status could not be determined.</li><li>• <b>Running:</b> Performing the task.</li><li>• <b>Pending:</b> Waiting for another task to be completed.</li></ul>
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.



# AXIS Camera Station User Manual

## 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: <ul style="list-style-type: none"><li>• <b>Finished:</b> The task was successfully completed.</li><li>• <b>Error:</b> The task was unable to complete on the device.</li><li>• <b>Canceled:</b> The task was canceled before completion.</li></ul>
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.


# AXIS Camera Station User Manual

## Generate reports


---

### 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.

[www.axis.com/products/online-manual/34074#t10133271](http://www.axis.com/products/online-manual/34074#t10133271)

*Generate a system report*

# AXIS Camera Station User Manual

## Generate reports

---

### 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 113*, 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**.

# AXIS Camera Station User Manual

## Generate reports

---

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 130*.

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.

[www.axis.com/products/online-manual/34074#t10151521](http://www.axis.com/products/online-manual/34074#t10151521)

*Set up an Axis body worn system*



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

[www.axis.com/products/online-manual/34074#t10151521](http://www.axis.com/products/online-manual/34074#t10151521)

*Playback and export Axis body worn camera recordings*

# AXIS Camera Station User Manual

## Generate reports


---

### What's new tab


**Note**

It is only available when the AXIS Camera Station client is online.

The What's new tab is shown automatically when you start the client after each AXIS Camera Station update. See *Client settings on page 114*.

To view the what's new tab manually, go to  > What's new.

### 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 User Manual

## Input devices

---

### Input devices

The following input devices can be used with AXIS Camera Station:

- AXIS T8311 Video Surveillance Joystick
- AXIS T8312 Video Surveillance Keypad
- AXIS T8313 Video Surveillance Joy Dial

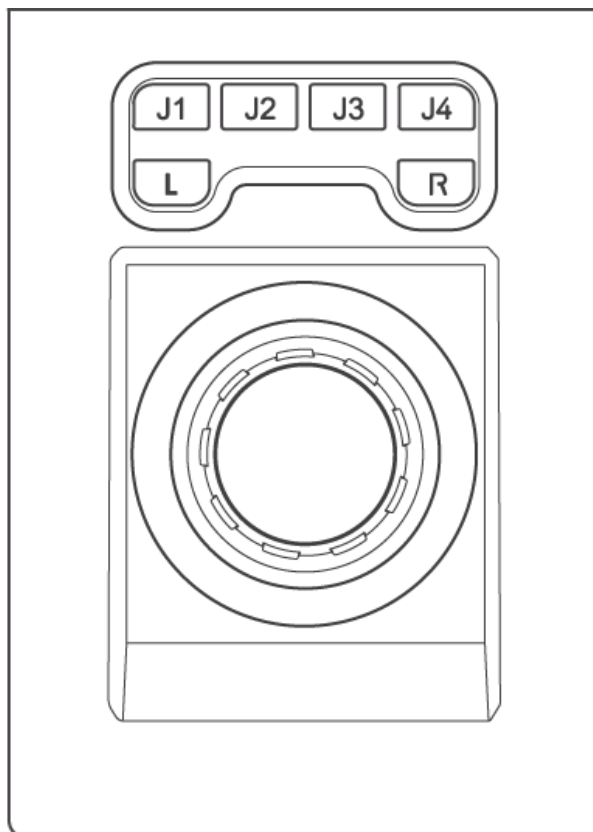
### AXIS T8311 Video Surveillance Joystick

AXIS T8311 Video Surveillance Joystick is a USB device that can be used as a computer mouse to pan, tilt and zoom in the camera view (cameras with mechanical PTZ only).

Connect the joystick before AXIS Camera Station is started. The joystick is detected and installed automatically.

#### Note

- If the joystick is connected after AXIS Camera Station has been started, the application must be restarted.
- The joystick can be configured to toggle between the PTZ and mouse modes. See *Hotkeys*.



- J1: Preset 1 from camera.
- J2: Preset 2 from camera.
- J3: Preset 3 from camera.

# AXIS Camera Station User Manual

## Input devices

---

- J4: Preset 4 from camera.
- L: Left mouse button.
- R: Right mouse button.

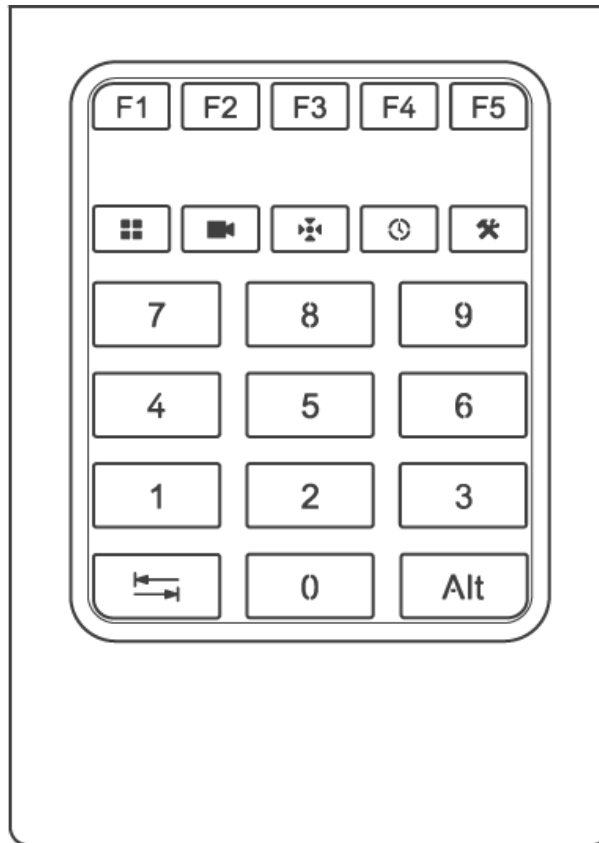
### AXIS T8312 Video Surveillance Keypad



AXIS T8312 Video Surveillance Keypad is a USB device used to quickly navigate between tabs, cameras, and views.

Connect the keypad before you start AXIS Camera Station. The keypad is detected and installed automatically.

**Note**

If the keypad is connected after AXIS Camera Station has been started, you must restart the application.



- F2: Go to Hotkeys.
- F4: Go to Logs.
- F5: Go to Configuration.
-  Tab: Go forward in a split view. Press ALT+  to go backward.

### AXIS T8313 Video Surveillance Jog Dial

AXIS T8313 Video Surveillance Jog Dial is a USB device used to jog and shuttle through recorded video.

# AXIS Camera Station User Manual

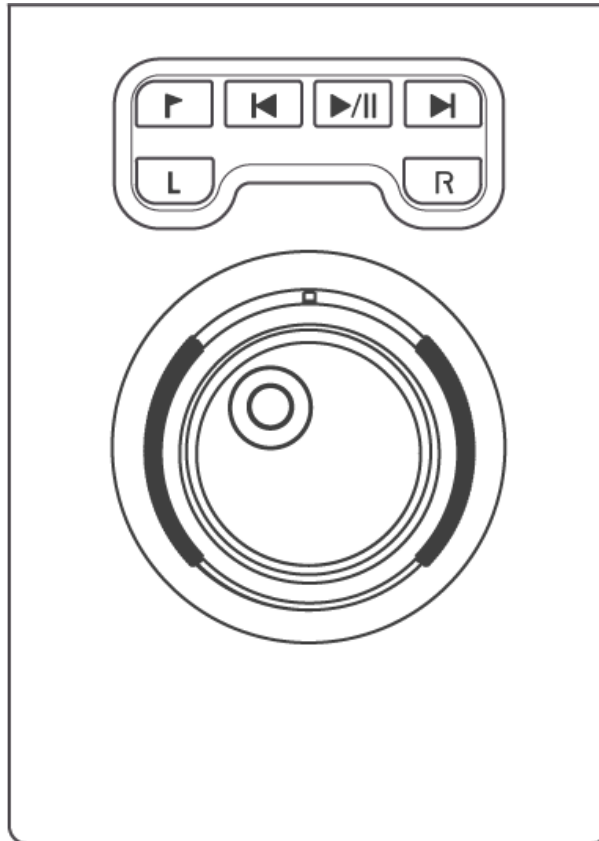
## Input devices





---

Connect the jog dial before you start AXIS Camera Station. The jog dial is detected and installed automatically.

**Note**

If the jog dial is connected after AXIS Camera Station has been started, you must restart the application.



-  **Bookmark:** Add a bookmark.
-  **Go to previous:** Go to the previous recording.
-  **Play/Pause:** Play and pause the recording.
-  **Go to next:** Go to the next recording.
- **L:** Show or hide Export markers.
- **R:** Switch between Live view and Recordings.
- **Jog clockwise:** Step forward in playback paused state.
- **Jog counterclockwise:** Step backward in playback paused state.
- **Shuttle clockwise:** Increase speed in playback state.
- **Shuttle counterclockwise:** Reduce speed in playback state.






# AXIS Camera Station User Manual

## AXIS Camera Station Service Control

---

### 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.

# AXIS Camera Station User Manual

## AXIS Camera Station Service Control

---

- **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.
- **Plugin communication port:** The port number used by the plugin 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 186*.

### 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

# AXIS Camera Station User Manual

## AXIS Camera Station Service Control

				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.

# AXIS Camera Station User Manual

## AXIS Camera Station Service Control

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 (RemoteFacadeBinder). 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 plugin	+7 offset from main HTTP port. Used for secure communication between plugin 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 User Manual

## 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 (AC-MSM)	Web server port	55766	HTTPS	Inbound	Client (Access management tab) and component	+14 offset from main HTTP port. Older installations used port 8081.

## 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.

# AXIS Camera Station User Manual

## AXIS Camera Station Service Control

---

- **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 189*.

A system backup includes both the core database files and the component database files. See *Database files on page 189*.

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**.
- **Plugins:** 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 file 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 189*.

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:

# AXIS Camera Station User Manual

## AXIS Camera Station Service Control

---


- 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 192*.
- Automatically by the scheduled database maintenance task configured in Windows Task Scheduler. See *Tools on page 192*.

### 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 190*.

#### 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 190*.
  - To restore from an automatic backup, go to the backup folder specified in *Database settings on page 189*, 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 **Plugins > ACMSM** to `C:\ProgramData\Axis Communications\AXIS Camera Station Secure Entry Service`.

# AXIS Camera Station User Manual

## AXIS Camera Station Service Control

---

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](http://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.



# AXIS Camera Station User Manual

## AXIS Camera Station Service Control

---

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.

### 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.

# AXIS Camera Station User Manual

## Troubleshooting

---


### Troubleshooting

#### More information


Visit [www.axis.com/products/cam\\_station\\_software](http://www.axis.com/products/cam_station_software) for

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

#### 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 [www.axis.com/support](http://www.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.

To create a screenshot:

1. Press ALT + PRT SCR.
2. Open Paint.
3. In Paint, select Edit > Paste.
4. Save file.

### Troubleshooting recording and playback

#### How do I play exported recordings?

Exported recordings can be played using Windows Media Player and AXIS File 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.

#### 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** 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.

#### Network storage is unavailable

# AXIS Camera Station User Manual

## Troubleshooting

---

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.

### Recordings are deleted

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. If so, 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 **Devices > Streaming profiles**.
- Use video format H.264 for recording. M-JPEG requires much more storage space.

## Troubleshooting motion detection

If motion detection detects too many or too few moving objects, try the following:

### Adjust motion settings

The area in which moving objects are detected can be adjusted by selecting Motion Settings. Follow these steps:

1. Go to **Configuration > Recording and events > Recording method**.
2. Select the camera and click **Motion Settings**.
3. Available motion settings are different for different cameras.
  - **AXIS Video Motion Detection 2 and 4:** The area of interest can be adjusted. See *Edit AXIS Video Motion Detection 2 and 4*.
  - **Built-in motion detection:** Include and exclude windows can be configured. See *Edit built-in motion detection*.

### 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**.

### Install AXIS Video Motion Detection 2 and 4

Axis network cameras and video encoders can detect motion using different methods:

# AXIS Camera Station User Manual

## Troubleshooting

---

- AXIS Video Motion Detection 2 and 4
- Built-in motion detection

AXIS Video Motion Detection 2 and 4 are camera applications that can be installed on products with support for AXIS Camera Application Platform. AXIS Video Motion Detection 2 requires firmware 5.60 or later. 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 motion recording is selected when cameras are added to AXIS Camera Station, AXIS Video Motion Detection 2 and 4 are installed automatically on all cameras that support the application. Other cameras will use the built-in motion detection.

To install AXIS Video Motion Detection 2 or 4 on a camera that uses the built-in motion detection, follow these steps:

1. Go to the *Device management* page.
2. If the camera does not have the required firmware, the firmware must first be upgraded. Select the camera, right-click and select **Upgrade firmware**.
3. Select the camera, right-click and select **Install camera application**.
4. Follow the on-screen instructions.

See also *Install camera application* and *Upgrade firmware*.

## Troubleshooting live view

### No video in Live view

If live view does not display video from a known-good camera, try to turn off hardware decoding. Hardware decoding is enabled by default, see *Hardware Decoding* as described in *Streaming*.

### Repeated error message "Media Failed"

A repeated error message "Media Failed" indicates that the CPU load is too high. To reduce the CPU load, try to optimize the profile settings for low bandwidth. See *Video and audio Settings* as described in *Streaming profiles*.

### Empty "ActiveMovie Window" popup

An empty "ActiveMovie Window" popup indicates problems with the graphics card's video memory and hardware acceleration.

Possible solutions:

- Install the latest graphics card driver, see *Troubleshooting graphics card*.
- Upgrade to a graphics card with more video memory and higher performance.
- Use the CPU for video rendering, see the *Use CPU for video rendering* section below.

### 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.
- Problems with the graphics card.

Possible solutions for graphics card problems:

- Install the latest graphics card driver, see *Troubleshooting graphics card*.
- Upgrade to a graphics card with more video memory and higher performance.
- Use the CPU for video rendering, see the *Use CPU for video rendering* section below.

# AXIS Camera Station User Manual

## Troubleshooting

---

- Change the video and audio settings, for example by optimizing profile settings for low bandwidth. See Video and audio Settings as described in *Streaming profiles*.

### Use CPU for video rendering

To use the CPU for video rendering:

1. Navigate to the AXIS Camera Station client installation folder. The default location is C:\Program Files\Axis Communications\AXIS Camera Station\Client (Current version)
2. Open the file "AcsClient.exe.config" in a text editor, for example Notepad.
3. Find this entry: `<setting name="ForceCompatibilityVideoMode" serializeAs="String">  
<value>False</value> </setting>`
4. Change the value from "False" to "True".
5. Save the file and restart AXIS Camera Station.

#### Note

Using the CPU for video rendering results in higher CPU usage.

## Troubleshooting graphics card

### Update graphics card driver

For AXIS Camera Station to run properly, the graphics card in the computer must use the latest driver. Update the graphics card driver if the graphics card is more than 12 months old. To find out what graphics card is installed in the computer, the diagnostic program dxdiag can be used.

1. Open dxdiag:
  - Windows 8: Go to the **Start** screen and type **dxdiag**.
  - Windows 7/Windows Vista/Windows Server 2008: Open the **Start** menu and type **dxdiag** in the search field.
2. If a prompt appears for the Diagnostic Tool, click **Yes**.
3. Select the **Display** tab. The name of the graphics card appears under **Device**.

To download the latest driver go to the graphics card manufacturer's website. Some of the more common ones are:

- nVidia: [www.nvidia.com](http://www.nvidia.com)
- ATI: [www.ati.com](http://www.ati.com)
- S3: [www.s3graphics.com](http://www.s3graphics.com)

To upgrade the graphics card driver:

1. Download the driver from the manufacturer's website.
2. Make sure that there are no other programs running on the computer.
3. Run the installer and follow the wizard to install necessary files.
4. Restart the computer.

## Troubleshooting PTZ

### Mechanical PTZ and presets

# AXIS Camera Station User Manual

## Troubleshooting

---

Mechanical PTZ and PTZ presets are available for PTZ cameras and for cameras where digital PTZ has been enabled in the camera's configuration page.

For information about how to enable digital PTZ, see the camera's User Manual.

Mechanical PTZ and PTZ presets are not available if the camera's control queue is enabled. The control queue can be disabled from the camera's configuration page. For more information about the control queue, see the camera's User Manual.

### Area zoom does not work

Area zoom is not supported by AXIS 209MFD and AXIS 212 PTZ.

## Troubleshooting 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).

To configure profiles for audio:

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

To 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

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

# AXIS Camera Station User Manual

## Troubleshooting

---

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 > Streaming 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.

## Troubleshooting login

Unable to log in or connect to server.

### Note

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*.

### 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 on Windows 8, Windows 7 and Windows Vista.
- For information about user access rights, see *Configure user permissions*.

# AXIS Camera Station User Manual

## Troubleshooting

---

### User is not authorized to log in to the server

The username is not authorized to use AXIS Camera Station on the specified server.

Possible solution: Add the user in the user permission dialog.

### Unable to verify message security. Please make sure server and client UTC times are reasonably synchronized.

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. Adjust the client and server time to be within 3 hours from each other.

### No contact with the server computer. Please make sure that the server computer is connected to the network.

The client was unable to establish any kind of connection to the server.

- 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. Please make sure that the server is running and accepting connections.

The client was able to contact the server computer but no AXIS Camera Station server was running. Make sure that you are connecting to the right computer and that the AXIS Camera Station server is running.

### Unable to connect to the server

An unknown error was encountered when connecting to the server. Make sure that your network is properly configured.

- 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*. The server status is displayed in the General tab. If status is "Stopped", click Start to start the Server.

### Unable to find the server. Please make sure that the address is correct.

The client was 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. Please upgrade the server to make sure the client and the server can communicate correctly. Client version (x) is not compatible with server version (y)

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. Please upgrade your client to make sure the client and the server can communicate correctly. Client version (x) is not compatible with server version (y)

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 was 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. Start the server or select a remote server to log in to.



# AXIS Camera Station User Manual

## Troubleshooting

---

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.

**AXIS Camera Station server is not installed on this computer. Select a remote server to log in to.**

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. Please select another server list.**

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.

### Troubleshooting licenses

#### License registration problems

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 Camera Station Portal*.

#### License registered too many times

If the initial installation and license registration was successful, but the computer or software needs to be reinstalled, ask Axis Customer Support to deactivate the license. Include the original license key and the name of the company and person the license is registered to.

### Troubleshooting installation failed

Installation failed is displayed if some cameras could not be added or configured. The page describes what has failed and how many cameras that are affected.

Error	Description
Continuous recording was not enabled	Continuous recording is not enabled for the listed cameras. To enable, go to <b>Configuration &gt; Recording and events &gt; Recording method</b> . Select the camera and turn on <b>Continuous</b> to enable continuous recording.
Could not contact the camera	AXIS Camera Station could not 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. Then go to <b>Configuration &gt; Add devices</b> and try to add the camera again.
Could not record on the specified drive	The recording storage (local storage or network storage) could not be configured. To use a different storage, go to <b>Configuration &gt; Storage &gt; management</b> . Add the storage and configure the storage settings for the cameras that should record to the storage.

# AXIS Camera Station User Manual

## Troubleshooting

Failed to install the AXIS Video Content Stream application	<p>AXIS Video Content Stream could not be installed. AXIS Video Content Stream is a camera application that improves smart search. Without the application, smart search can still be used but performance is reduced. AXIS Video Content Stream can be installed on cameras with support for AXIS Camera Application Platform and firmware 5.50 and later.</p> <p>This error message is displayed if the application could not be installed on a camera that supports AXIS Video Content Stream.</p> <p>To install the application manually, go to <b>Configuration &gt; Devices &gt; Management</b>, right-click the camera and select <b>Install camera application</b>.</p>
Failed to install the AXIS Video Motion Detection application	<p>AXIS Video Motion Detection 2 or 4 could not be installed. The built-in motion detection will be used for motion recording. AXIS Video Motion Detection 2 and 4 are camera applications used for motion detection. If motion recording is selected when cameras are added to AXIS Camera Station, the application is installed automatically on all cameras that support the application. If a camera does not support the application, the built-in motion detection will be used.</p> <p>AXIS Video Motion Detection 2 can be installed on cameras with support for AXIS Camera Application Platform and firmware 5.60 and later. AXIS Video Motion Detection 4 can be installed on cameras with support for AXIS Camera Application Platform and 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.</p> <p>This error message is displayed if the application could not be installed on a camera that supports AXIS Video Motion Detection 2 or 4. To install the application manually, see <i>Edit AXIS Video Motion Detection 2 and 4</i>.</p>
Failed to retrieve current Motion Detection	<p>AXIS Camera Station could not retrieve motion detection parameters from the camera.</p> <p>If this error message is displayed, the built-in motion detection will be used. To use AXIS Video Motion Detection 2, the application must be installed manually. See also "Failed to install the AXIS Video Motion Detection 2.1 application" above.</p>
Failed to set password on camera	<p>Password could not be set for the listed cameras.</p> <p>To set the password manually, go to <b>Configuration &gt; Devices &gt; Management</b>, right-click the camera and select <b>User Management &gt; Set password</b>.</p>
Installation was canceled	<p>Installation was canceled by the user. The listed cameras are not added. To add the cameras, go to <b>Configuration &gt; Add devices</b>.</p>
Motion detection not configured	<p>Motion detection could not be configured in the listed cameras.</p> <p>To configure motion detection manually, go to <b>Configuration &gt; Recording and events &gt; Recording method</b> and select the camera. Click <b>Motion settings</b> to configure motion detection.</p>
Motion detection was not enabled	<p>Motion recording is not enabled for the listed cameras.</p> <p>To enable, go to <b>Configuration &gt; Recording and events &gt; Recording method</b>. Select the camera and turn on <b>Motion detection</b> to enable motion detection recording.</p>

### Troubleshooting no devices found

AXIS Camera Station automatically searches the network for connected cameras and video encoders. If no cameras are found:

- Check that the camera is connected to the network and that power has been applied.
- If the client, server and/or cameras are located on different networks, then proxy and firewall settings might need to be configured.

# AXIS Camera Station User Manual

## Troubleshooting

---

- Change the client proxy settings if the client and the server are separated by a proxy server. See *Client proxy settings*.
  - Change the NAT or firewall if the client and the server are separated by a NAT or firewall. Ensure that the HTTP port, TCP port and streaming port specified in AXIS Camera Station Service Control are allowed to pass through the firewall and/or NAT.
  - Change the server proxy settings if the server and the devices are separated by a proxy server. See the Proxy settings section in *General* under AXIS Camera Station Service Control.
- To add cameras manually, see *Add devices*.

### Troubleshooting user searches

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.

### Troubleshooting 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 could 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.

