

AXIS Camera Station S2216 Mk II Appliance

Table of Contents

Get started.....	4
Install your device.....	5
.....	5
Setup examples.....	5
Setup in an independent surveillance network.....	5
Setup in an existing network	6
Connect the switch directly to the corporate network	7
Configure your device.....	9
Initial Axis recorder setup	9
Connect to a server	9
Connect to a remote server.....	10
Sign in to AXIS Secure Remote Access	10
Configure AXIS Camera Station Pro.....	10
Start the video management system	11
Add devices.....	11
Configure recording method	11
View live video	11
View recordings.....	11
Add bookmarks.....	12
Export recordings	12
Play and verify recordings in AXIS File Player.....	12
Network configuration	12
Server port configuration	13
Security considerations	13
License a system online.....	13
License a system that's offline	13
Manage local Windows® user accounts.....	15
Create a user account.....	15
Create an administrator account.....	15
Create a local user group	15
Delete a user account	15
Change a user account's password	15
Create a password reset disk for a user account.....	16
Manage AXIS Camera Station Pro user accounts	17
User permissions	17
Add users or groups.....	17
User or group privileges	18
Manage your device.....	21
Update Secure Boot certificates.....	21
Check your certificate status.....	21
Recommended actions	22
Update certificate through the BIOS.....	22
Update certificate through Windows Update	22
Check the current BIOS version.....	22
Update the BIOS	23
Update Windows®	23
Configure Windows® update settings	23
Add additional storage.....	24
Remove the bezel	24
Install the hard drive.....	24
Add a new recording storage	24
Create RAID volume.....	25
Initiate RAID volume in Microsoft Windows®	25

Manage the built-in switch.....	27
About the built-in switch.....	27
Log in to the switch's management page	27
Running configuration.....	27
Overview	27
Power management.....	28
Allocate power	28
Turn on and turn off PoE	30
Network overview	30
Lock and unlock ports	30
Settings	31
Configure network settings.....	31
Configure date and time.....	31
Configure DHCP server.....	31
Configure SNMP.....	31
Maintenance	32
Update firmware	32
Reboot the switch	32
Backup the switch's settings.....	32
Restore the switch's settings.....	32
Manage certificates.....	32
Change password	33
Configure web settings	33
Reset to factory default settings	33
Logs.....	33
Create switch reports.....	33
Specifications.....	34
Product overview	34
Front and rear.....	34
LED indicators.....	34
Troubleshooting.....	36
Reset your server.....	36
Perform a system recovery	36
.....	36
Troubleshoot AXIS Camera Station Pro	37
Need more help?.....	38
Useful links.....	38
Contact support.....	38

Get started

The standard workflow to configure an AXIS Camera Station Pro recording server is:

1. *Install your device.*
2. Initial Windows® setup: After installing your device, you are guided through a few steps to set up the region, language, keyboard layout, an administrator account and its password.
3. Initial Axis recorder setup: After the initial Windows® setup, AXIS Recorder Toolbox is opened and you are guided through a few steps to set up basic and necessary settings, for example, computer name, date and time, and network. See *Initial Axis recorder setup, on page 9*.
4. Configure Windows®. We recommend to:
 - Update Windows® to the latest version. See *Update Windows®, on page 23*.
 - Create a standard user account. See *Create a user account, on page 15*.
5. Update AXIS Camera Station Pro to the latest version.
 - If your system is online: open the AXIS Recorder Toolbox app and click **Update AXIS Camera Station Pro**.
 - If your system is offline: go to *axis.com* and download the latest version.
6. Start the AXIS Camera Station Pro client.
7. *Connect to AXIS Camera Station Pro server.*
8. *Configure AXIS Camera Station Pro, on page 10.*

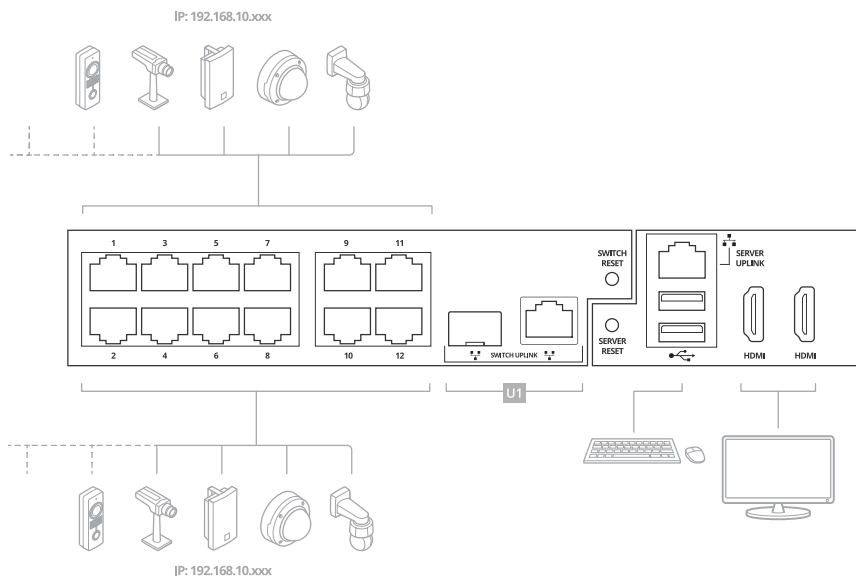
Install your device

For instructions on how to install the product, see the installation guide included in the box or on the product's support page on axis.com.

Setup examples

Setup in an independent surveillance network

You can create an independent surveillance network which has no interconnectivity to another external network. This setup is a basic plug and play installation. The built-in switch's DHCP server is enabled by default. As soon as you plug the cameras into the PoE ports, the cameras will power on and obtain an IP address and be accessible via AXIS Camera Station Pro.



Difficulty level	Basic
Benefits	Dedicated surveillance network with no interconnectivity to another external network Plug and play installation
Limitations	Bandwidth PoE budget No remote access
Actions needed	Change the default password for the built-in switch Register the AXIS Camera Station Pro license

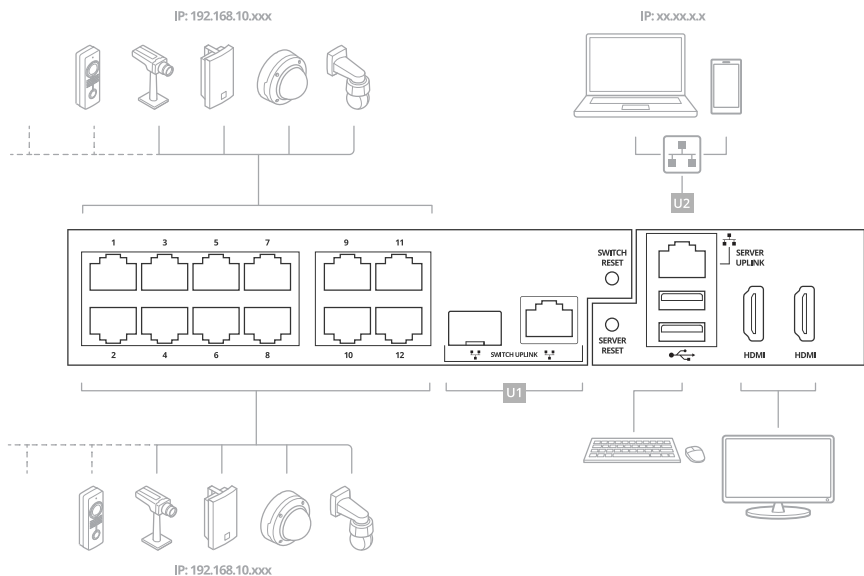
Connectors used	PoE Ethernet ports USB 2.0 ports (for keyboard and mouse) Displayport™ or HDMI connector
Connectors NOT used	Switch uplink port Server uplink port USB 3.2 port (front side) Universal audio jack (front side)

Setup in an existing network

You can create a surveillance network within an existing network. This means that the surveillance network is separated from the existing network.

Note

When you use an additional recorder, for example, the AXIS S30 Recorders, the appliance does not route network data from the surveillance network to the server network for recording. Make sure that the AXIS S30 Recorders are connected to the same network as the cameras.

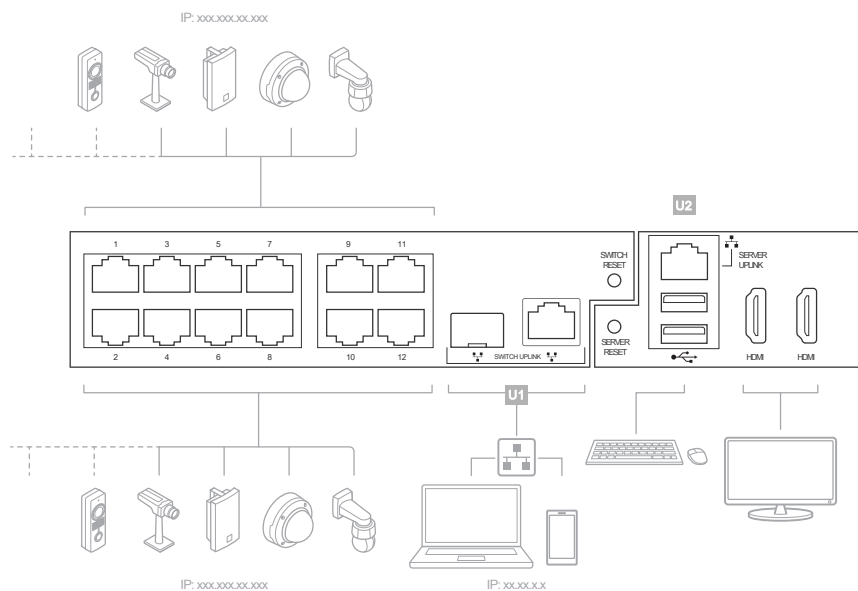


Difficulty level	Advanced
Benefits	Ability to use an AXIS Camera Station Pro client to connect to S22 series over the network. Network segregation
Limitations	May require you to follow corporate network policies
Actions needed	Change the default password for the built-in switch Register the AXIS Camera Station Pro license

Connectors used	PoE Ethernet ports Ethernet port — Server uplink for connection to network (Optional) USB 2.0 ports (for keyboard and mouse) (Optional) Displayport™ or HDMI connector
Connectors NOT used	Switch uplink port USB 3.2 port (front side) Universal audio jack (front side)

Connect the switch directly to the corporate network

This setup integrates the system directly into your existing corporate network, allowing cameras to be accessed and monitored from anywhere on the network.



Difficulty level	Advanced
Benefits	Cameras are accessible from the corporate network and can be monitored with an SNMP server.
Limitations	May require you to follow corporate network policies
Actions needed	Turn off DHCP on the switch Change the switch's IP address to a static one from the corporate network Set the PC's internal NIC to DHCP or a static IP on the corporate network Change the switch's default password. Configure and register AXIS Camera Station Pro

Connectors used	PoE Ethernet ports Switch uplink port (U1) (Optional) USB 2.0 ports (for keyboard and mouse) (Optional) Displayport™ or HDMI connector
Connectors NOT used	PC uplink port (U2) USB 3.2 port (front side) Universal audio jack (front side)

Configure your device

Initial Axis recorder setup

After you have configured Windows®, AXIS Recorder Toolbox is opened automatically and you are guided through the first-time configuration setup assistant. In this setup assistant, you can configure several basic and necessary settings before you manage your device in AXIS Recorder Toolbox.

Note

The settings are for the server. To change the switch's settings, go to the switch's management page. See *Settings, on page 31*.

1. Select **Light** or **Dark** theme and click **Next** (if it's available for your product).
2. Change the computer name if you want and click **Next**.
3. Under **Date and time**, configure the following settings and click **Next**.
 - Select a time zone.
 - To set up an NTP server, select **NTP server** and enter the NTP server address.
 - To set manually, select **Manual** and select a date and time.
4. Under **Network settings**, configure the following settings and click **Next**.
 - **Use automatic IP settings (DHCP)** and **Use automatic DNS settings** are turned on by default.
 - If your device is connected to a network with a DHCP server, the assigned IP address, subnet mask, gateway, and preferred DNS are automatically displayed.
 - If your device is not connected to a network or there is no DHCP server available, enter the IP address, subnet mask, gateway, and preferred DNS manually depending on the network requirements.
5. Click **Finish**. If you have changed the computer name, AXIS Recorder Toolbox will prompt you to restart the device.

Connect to a server

The AXIS Camera Station S2216 Mk II Appliance client lets you connect to a single server or multiple servers in different ways:

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

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

Remote server – See *Connect to a remote server, on page 10*.

Note

- The first time you connect to a server, the client checks the server certificate ID. To make sure you're connecting to the correct server, compare the certificate ID with the one displayed in AXIS Camera Station S2216 Mk II Appliance Service Control.

Server list	To connect to servers from a server list, select a one from the Server list drop-down menu. Click  to create or edit the server lists.
Import server list	To import a server list file exported from AXIS Camera Station, click Import server list and browse to an .msl file.

Delete saved passwords	To delete saved usernames and passwords for all connected servers, click Delete saved passwords .
Change client proxy settings	If you can't connect to a server, you might need to update your client proxy settings. Click Change client proxy settings .

Connect to a remote server

1. Select **Remote server**.
2. Select a server from the **Remote server** drop-down list or enter the IP or DNS address. If the server isn't listed, click  to refresh the list of all the available remote servers. If the server is configured to accept clients on a different port than the default port number 55754, enter the IP address followed by the port number, for example, 192.168.0.5:46001.
3. Do one of the following:
 - Select **Log in as current user** to log in as the current Windows® user.
 - Clear **Log in as current user** and click **Log in**. Select **Other user** and provide another username and password to log in with different credentials.

Sign in to AXIS Secure Remote Access

Important

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

What does this mean for your AXIS Camera Station S2216 Mk II Appliance system?

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

Note

- When trying to connect to a server using Axis Secure Remote Access, the server can't upgrade the client automatically.
 - If the proxy server is between the network device and the AXIS Camera Station S2216 Mk II Appliance server, you must configure the proxy settings in Windows on the AXIS Camera Station S2216 Mk II Appliance server to access the server using AXIS Secure Remote Access.
1. Click the **Sign in to AXIS Secure Remote Access** link.
 2. Enter your My Axis account credentials.
 3. Click **Sign in**.
 4. Click **Grant**.

Configure AXIS Camera Station Pro

Before you start:

- 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 Pro:

1. *Start the video management system*

2. *Add devices*
3. *Configure recording method, on page 11*
4. *View live video, on page 11*
5. *View recordings, on page 11*
6. *Add bookmarks, on page 12*
7. *Export recordings, on page 12*
8. *Play and verify recordings in AXIS File Player, on page 12*

Start the video management system

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

You can connect to multiple AXIS Camera Station Pro servers in different ways.

Add devices

The first time you start AXIS Camera Station S2216 Mk II Appliance, the **Add devices** page opens and searches the network for devices to add.

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

Configure recording method

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

View live video

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

View recordings

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

Add bookmarks

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

Note

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

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

Export recordings

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

Play and verify recordings in AXIS File Player

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

Note

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

Network configuration

Configure proxy or firewall settings before using AXIS Camera Station S2216 Mk II Appliance if the client, server, and connected network devices are on different networks.

Client proxy settings

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

Server proxy settings

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

NAT and Firewall

When a NAT or firewall separates the client and the server, configure it to ensure that the HTTP port, TCP port, and streaming port specified in AXIS Camera Station S2216 Mk II Appliance Service Control can pass through. Contact your network administrator for help.

Server port configuration

The AXIS Camera Station S2216 Mk II Appliance server uses ports 55752 (HTTP), 55754 (TCP), 55756 (mobile communication), and 55757 (mobile streaming) for communication between the server and the client. You can change the ports in AXIS Camera Station Service Control if required.

Security considerations

To prevent unauthorized access to cameras and recordings:

- Use strong passwords for all network devices (cameras, video encoders, and auxiliary devices).
- Install the AXIS Camera Station S2216 Mk II Appliance server, cameras, video encoders, and auxiliary devices on a secure network, separate from the office network. You can install the AXIS Camera Station S2216 Mk II Appliance client on a computer on another network, for example, a network with internet access.
- Make sure all users have strong passwords.

License a system online

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

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

License a system that's offline

To license your system manually:

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

Note

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

4. Open *AXIS License Manager*.
5. In AXIS License Manager:
 - 5.1. Select the correct organization, or create one if you haven't already. Read the *My Systems user manual on help.axis.com* for more information.
 - 5.2. Go to **System setup**.
 - 5.3. Click **Upload system file**.
 - 5.4. Click **Upload system file** and select your system file.

- 5.5. Click **Upload system file**.
- 5.6. Click **Download license file**.
6. Go back to the AXIS Camera Station S2216 Mk II Appliance client.
7. Click **Import license file...** and select your license file.
8. Click **Go to AXIS License Manager** to manage your licenses.

Manage local Windows® user accounts

Create a user account

To help keep your personal data and information more secure, we recommend that you add a password for each local account.

Important

Once you create a password for a local account, don't forget it. There's no way to recover a lost password for local accounts.

1. Go to **Settings > Accounts > Other users > Add other user** and click **Add account**.
2. Click **I don't have this person's sign-in information**.
3. Click **Add a user without a Microsoft account**.
4. Enter a user name, password and password hint.
5. Click **Next** and follow the instructions.

Create an administrator account

1. Go to **Settings > Accounts > Other people**.
2. Go to the account you want to change and click **Change account type**.
3. Go to **Account type** and select **Administrator**.
4. Click **OK**.
5. Restart your device and sign in with the new administrator account.

Create a local user group

1. Go to **Computer Management**.
2. Go to **Local Users and Groups > Group**.
3. Right-click **Group** and select **New Group**.
4. Enter a group name and a description.
5. Add group members:
 - 5.1. Click **Add**.
 - 5.2. Click **Advanced**.
 - 5.3. Find the user account(s) you want to add to the group and click **OK**.
 - 5.4. Click **OK** again.
6. Click **Create**.

Delete a user account

Important

When you delete an account you remove the user account from the login screen. You also remove all files, settings and program data stored on the user account.

1. Go to **Settings > Accounts > Other people**.
2. Go to the account you want to remove and click **Remove**.

Change a user account's password

1. Log in with an administrator account.
2. Go to **User Accounts > User Accounts > Manage another account** in sequence.

You'll see a list with all user accounts on the device.

3. Select the user account whose password you would like to change.
4. Click **Change the password**.
5. Enter the new password and click **Change password**.

Create a password reset disk for a user account

We recommend to create a password reset disk on a USB flash drive. With this, you can reset the password. Without a password reset disk, you can't reset the password.

Note

If you're using Windows® 10, or later, you can add security questions to your local account in case you forget your password, so you don't need to create a password reset disk. To do this, go to **Start** and click **Settings > Sign-in options > Update your security questions**.

1. Sign in to your device with a local user account. You can't create a password reset disk for a connected account.
2. Plug an empty USB flash drive into your device.
3. From the Windows® search field, go to **Create a password reset disk**.
4. In the **Forgotten Password** setup assistant, click **Next**.
5. Select your USB flash drive and click **Next**.
6. Type your current password and click **Next**.
7. Follow the onscreen instructions.
8. Remove the USB flash drive and keep it in a safe place. You don't have to create a new disk when you change your password even if you change it several times.

Manage AXIS Camera Station Pro user accounts

User permissions

Go to **Configuration > Security > User permissions** to see the users and groups in AXIS Camera Station S2216 Mk II Appliance.

Note

Administrators of the computer that runs the AXIS Camera Station S2216 Mk II Appliance server are automatically granted administrator privileges in AXIS Camera Station S2216 Mk II Appliance. You can't change or remove the Administrators group's privileges.

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

When a user belongs to a group, they receive the highest role permission assigned to them individually or to the group. For example, a user with access to camera X who also belongs to a group with access to cameras Y and Z has access to all three cameras.

	Indicates the entry is a single user.
	Indicates the entry is a group.
Name	Username as it appears in the local computer or Active Directory.
Domain	The domain that the user or group belongs to.
Role	The access role assigned to the user or group. Possible values: Administrator, Operator, and Viewer.
Details	Detailed user information as it appears on the local computer or in Active Directory.
Server	The server that the user or group belongs to.

Add users or groups

Microsoft Windows® and Active Directory users and groups can access AXIS Camera Station S2216 Mk II Appliance. To add a user to AXIS Camera Station S2216 Mk II Appliance, you must add users or a group to Windows®.

To add a user in Windows® 10 and 11:

- Press the Windows key + X and select **Computer Management**.
- In the **Computer Management** window, navigate to **Local Users and Groups > Users**.
- Right-click **Users** and select **New User**.
- In the popup dialog, enter the new user's details and clear **User must change password at next login**.
- Click **Create**.

If you use an Active Directory domain, consult your network administrator.

Add users or groups

1. Go to **Configuration > Security > User permissions**.
2. Click **Add**. The available users and groups appear in the list.
3. Under **Scope**, select where to search for users and groups.
4. Under **Show**, select to show users or groups. The search results may not appear if there are too many users or groups. Use the filter to narrow the results.

5. Select the users or groups and click **Add**.

Scope	
Server	Select to search for users or groups on the local computer.
Domain	Select to search for Active Directory users or groups.
Selected server	When connected to multiple AXIS Camera Station S2216 Mk II Appliance servers, select a server to search for users or groups on that server.

Configure a user or group

1. Select a user or group in the list.
2. Under **Role**, select **Administrator**, **Operator**, or **Viewer**.
3. If you selected **Operator** or **Viewer**, you can configure the user or group privileges. See *User or group privileges*.
4. Click **Save**.

Remove a user or group

1. Select the user or group.
2. Click **Remove**.
3. In the pop-up dialog, click **OK** to remove the user or group.

User or group privileges

There are three roles you can assign to a user or group. For how to define the role for a user or group, see *Add users or groups*.

Administrator – Full access to the entire system, including access to live and recorded video of all cameras, all I/O ports, and views. This role is required to access system configuration.

Operator – Select cameras, views, and I/O ports to get access to live and recorded video. An operator has full access to all functionality of AXIS Camera Station S2216 Mk II Appliance except system configuration.

Viewer – Access to live video of selected cameras, I/O ports, and views. A viewer doesn't have access to recorded video or system configuration.

Cameras

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

Access	Allow access to the camera and all camera features.
Video	Allow access to live video from the camera.
Audio listen	Allow access to listen from the camera.
Audio speak	Allow access to speak to the camera.
Manual Recording	Allow starting and stopping recordings manually.

Mechanical PTZ	Allow access to mechanical PTZ controls. Available only for cameras with mechanical PTZ.
PTZ priority	Set the PTZ priority. A lower number means a higher priority. No assigned priority is set to 0. An administrator has the highest priority. When a role with higher priority operates a PTZ camera, others can't operate the same camera for 10 seconds by default. Available only for cameras with mechanical PTZ that have Mechanical PTZ selected.

Views

The following access privileges are available for users or groups with the **Operator** or **Viewer** role. You can select multiple views and set the access privileges.

Access	Allow access to the views in AXIS Camera Station S2216 Mk II Appliance.
Edit	Allows editing of views in AXIS Camera Station S2216 Mk II Appliance.

I/O

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

Access	Allow full access to the I/O port.
Read	Allows viewing the state of the I/O port without changing it.
Write	Allows changing the state of the I/O port.

System

You can't configure grayed-out access privileges in the list. A check mark means the user or group has this privilege by default.

The following access privileges are available for users or groups with the **Operator** role. **Take snapshots** is also available for the **Viewer** role.

Take snapshots	Allows taking snapshots in live view and recording mode.
Export recordings	Allow exporting recordings.
Generate incident report	Allow generating incident reports.
Prevent access to recordings older than	Prevent access to recordings older than the specified number of minutes. Users can't find these recordings when they search.
Access alarms, tasks, and logs	Get alarm notifications and allow access to the Alarms and tasks bar and Logs tab.
Access data search	Allow searching for data to track what happened at the time of an event.

Add categories to events	Allow adding categories to events in the Recordings tab.
Remove categories from event	Allow removing categories from events in the Recordings tab.

Access control

The following access privileges are available for users or groups with the **Operator** role. **Access Management** is also available for the **Viewer** role.

Access control configuration	Allow configuration of doors and zones, identification profiles, card formats, and PIN, encrypted communication, and multi-server.
Access management	Allow access management and access to the Active Directory settings.

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

System health monitoring

The following access privileges are available for users or groups with the **Operator** role. **Access to system health monitoring** is also available for the **Viewer** role.

Configuration of system health monitoring	Allows configuration of system health monitoring.
Access to system health monitoring	Allows access to system health monitoring.

Manage your device

Update Secure Boot certificates

Microsoft is retiring the 2011 Secure Boot certificates in June 2026 and replacing them with new 2023 certificates. To keep your recorder safe, install the 2023 certificates before then.

Installing the 2023 certificates requires Windows 10 LTSC (Long-Term Servicing Channel) or Windows 11 LTSC. If your device is within warranty but is running Windows 10 SAC (Semi-Annual Channel) instead of an LTSC version, contact Axis Technical Support. They can tell you if you can upgrade to an LTSC version before you update the BIOS or change any certificates.

Note

After June 2026, devices without the 2023 certificates will keep working as normal, but won't receive new security protections for the early boot process, including Windows Boot Manager updates and revocation lists for new vulnerabilities.

Check your certificate status

To verify that the 2023 certificates are installed and that the Windows bootloader has been updated, use one of the following methods:

Method 1:

1. Open Registry Editor.
2. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing.
3. Check the UEFICA2023Status value. If the value says **Updated**, the 2023 certificate is installed.

 (Default)	REG_SZ	(value not set)
 BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
 ConfidenceLevel	REG_SZ	No Data Observed - Action Required
 ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
 LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
 UEFICA2023Status	REG_SZ	Updated
 WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

Method 2:

1. Open Windows Security.
2. Go to Device security.
3. Under Secure boot, check the status message. If the certificate is up to date, the card shows: "Secure Boot is on and all required certificate updates have been applied. No further certificate changes are needed."

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

Note

Windows Security only shows certificate status if your device has the April 14, 2026 cumulative update or later installed. If you don't see a certificate status message, install the latest Windows update or use Method 1 instead.

Recommended actions

A BIOS update stores the 2023 certificates permanently in the firmware. This is the most reliable method, and we recommend it even if you've already installed the certificates through Windows Update.

Important

If you only install the certificates through Windows Update and then reset the BIOS Secure Boot keys to factory defaults, the certificates will be lost and the device won't start with Secure Boot turned on. Update the BIOS to make the certificates permanent before you reset Secure Boot keys.

Update certificate through the BIOS

Install the BIOS version listed for your model, or a later version. You can download these from the product page on Axis.com:

Model	Minimum BIOS version
AXIS S2208	TBC
AXIS S2212	TBC
AXIS S2216	TBC
AXIS S2224	TBC
AXIS S2108	Z218-004
AXIS S2208 Mk II	Z670-005
AXIS S2212 Mk II	Z671-005
AXIS S2216 Mk II	Z672-005
AXIS S2224 Mk II	Z673-005

Update certificate through Windows Update

If a BIOS update isn't available yet for your model, you can get the 2023 certificates through Windows Update instead.

Important

Certificates installed this way are stored in the current Secure Boot database, not in the firmware. If you reset the BIOS Secure Boot keys to factory defaults, you'll lose the certificates and the device may not be able to start with Secure Boot turned on. Install a BIOS update as soon as one is available for your model, even if you've already used this method.

To use this path:

1. Make sure your device runs Windows 10 LTSC or Windows 11 LTSC.
2. Install all Windows updates released April 14, 2026 or later.
3. Go to **Windows Security > Device security > Secure Boot** to check your certificate status.
4. If the certificate doesn't update after installing the latest updates, check the **UEFICA2023Status** registry value. If your device remains ineligible for the automatic update, update the BIOS or contact Axis Technical Support.

Important

Don't manually revoke the 2011 certificate until you've confirmed that all recovery media, boot environments, and drivers in your environment are signed with the 2023 certificate. Revoking the 2011 certificate too early will leave your device unable to start with Secure Boot turned on.

Check the current BIOS version

To check the current BIOS:

1. Power on the device and repeatedly press **DEL** until the Axis logo appears.
2. The version number is shown as first entry under **Main**.

Update the BIOS

Follow the instructions included in the BIOS guide, available on the download page of the BIOS file.

Update Windows®

Windows® periodically checks for updates. When an update is available, your device automatically downloads the update but you've to install it manually.

Note

Recording will be interrupted during a scheduled system restart.

To manually check for updates:

1. Go to **Settings > Windows Update**.
2. Click **Check for updates**.

Configure Windows® update settings

It is possible to change how and when Windows® do its updates to suit your needs.

Note

All ongoing recordings stop during a scheduled system restart.

1. Open the Run app.
 - Go to **Windows System > Run**, or
2. Type `gpedit.msc` and click **OK**. The Local Group Policy Editor opens.
3. Go to **Computer Configuration > Administrative Templates > Windows Components > Windows Update**.
4. Configure the settings as required, see example.

Example:

To automatically download and install updates without any user interaction and have the device restart, if necessary, at out of office hours, use the following configuration:

1. Open **Always automatically restart at the scheduled time** and select:
 - 1.1. **Enabled**
 - 1.2. **The restart timer will give users this much time to save their work (minutes): 15.**
 - 1.3. **Click OK.**
2. Open **Configure Automatic Updates** and select:
 - 2.1. **Enabled**
 - 2.2. **Configure Automatic updates: Auto download and schedule the install**
 - 2.3. **Schedule Install day: Every Sunday**
 - 2.4. **Schedule Install time: 00:00**
 - 2.5. **Click OK.**
3. Open **Allow Automatic Updates immediate installation** and select:
 - 3.1. **Enabled**
 - 3.2. **Click OK.**

Add additional storage

The demand for storage can differ. Retention time of stored data or for storing high-resolution recordings often results in a need to install more storage. This section explains how to install an additional hard drive in your AXIS S22 series product.

Note

Follow the instructions below to add additional storage to applicable AXIS S22 products. These instructions are as-is, and Axis Communications AB takes no responsibility for loss of data or misconfiguration during these steps. The standard precautions should be taken to backup data that is business critical. The following procedure of expanding storage will not be supported by Axis Technical Support.

Note

To avoid electrostatic discharge, we recommend that you always use a static mat and static strap while working on internal system components.

Warranty

Detailed information about warranty is available at: www.axis.com/support/warranty.



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

Remove the bezel

1. Loosen the two thumbscrews located at each side of the bezel.
2. Remove the bezel.

Install the hard drive

⚠ CAUTION

- Use only hard drives that have been tested and approved for use with AXIS S22 series.
- When you install a hard drive, make sure that the hard drive carrier is pushed all the way in. You will hear a click when the drive carrier is locked.
- Before you install a hard drive, make sure the power cord is disconnected.
 1. Shut down the system and make sure the power is off.
 2. Disconnect the power cord.
 3. Press the release button on the front of the hard drive carrier and open the hard drive carrier handle.
 4. Pull out the hard drive carrier using the handle.
 5. Insert a hard drive in the hard drive carrier.
 6. Fasten the hard drive to the hard drive carrier with four screws.
 7. Insert the hard drive carrier into the hard drive slot until the carrier connects with the backplane.
 8. Close the hard drive carrier handle to lock the hard drive in place.
 9. Reattach the front bezel.
 10. Start the system.

Add a new recording storage

1. Create and format a new hard disk partition in Windows:

- 1.1. Right-click the **Start** menu and select **Disk Management**.
- 1.2. Click **OK** if the **Initialize Disk** popup appears. If it doesn't, right-click on the new hard drive and select **Initialize Disk**.
- 1.3. Right-click on an unallocated region on the newly initialized disk and select **New Simple Volume**.
- 1.4. Follow the wizard to set the volume size, assign a drive letter, and format the partition.
- 1.5. Complete the wizard to create the new simple volume.
2. Add a new recording storage in AXIS Camera Station Pro:
 - 2.1. Open AXIS Camera Station Pro.
 - 2.2. Go to **Storage > Management**.
 - 2.3. Click **Add...**
 - 2.4. Select the newly added drive and click **OK**.
 - 2.5. Go to **Storage > Selection**.
 - 2.6. Select which devices you want to transfer recording data to the new drive.
 - 2.7. In the **Store to** drop-down list, select the new drive and click **Apply**.

For more information about storage management, see *AXIS Camera Station Pro – User manual*.

Create RAID volume

1. Make sure that the disks to be used in the RAID volume are detected.
 - 1.1. Turn on your device and instantly press F12 until the Axis logo appears.
 - 1.2. In the UEFI boot menu, select **Device Configuration** and press Enter.
 - 1.3. In the Intel® Rapid Storage Technology menu, make sure that the disks are correctly displayed under **Non-RAID Physical Disks**.

Note

Only RAID 0 and RAID 1 are available on devices that have physical space for just an additional single drive.

2. In the Intel Rapid Storage Technology menu, select **Create RAID Volume** and press Enter.
3. Type a name for the volume.
4. Choose the RAID level.
 - 4.1. Select **RAID Level** and press Enter.
 - 4.2. In the popup dialog, select the RAID level you want to use and press enter.
5. Include the disks to be used in the volume.
 - 5.1. Select a disk and press enter.
 - 5.2. Select **X** to include this disk in the volume.
 - 5.3. Repeat until you have selected all the disks you want to use.
6. Leave **Stripe Size** and **Capacity** to the default values, unless specified.
7. Select **Create Volume** and press enter.
8. In the Intel Rapid Storage Technology menu, the newly created RAID volume appears under **RAID Volumes**.
9. Press Esc and then press Y to save and exit to the UEFI menu.
10. Press CTRL + ALT+ DELETE to restart your device.

Initiate RAID volume in Microsoft Windows®

To configure a new volume:

1. Right-click the **Start** menu and select **Disk Management**.
2. In the pop-up "Initialize Disk", select **GPT** and click **OK**.
3. Right-click the unallocated disk and select **New Simple Volume**.
 - Follow the instructions in the setup assistant.
4. When the setup assistant is finished, **Disk Management** shows the new volume. Close **Disk Management** for the system to use the new volume.

Manage the built-in switch

About the built-in switch

The AXIS Camera Station S22 Mk II Appliance Series comes with an integrated Power over Ethernet (PoE) switch. You can configure and manage the built-in switch.

The purpose of the switch is to segregate traffic on the network so that security cameras and related traffic managed by the switch (PoE and the switch uplink ports) are not shared with other networks.

The switch's power management follows these rules:

- Each port can reserve power according to the connected powered device's PoE class. You can also manually allocate power to a port.
- If the actual power consumption for a given port exceeds the reserved power for that port, it will shut down.
- Ports will shut down when the actual power consumption for all ports exceeds the total amount of power that the power supply can deliver. The ports are then shut down according to the ports priority where a lower port number means higher priority.

Log in to the switch's management page

1. Go to the menu bar.
 - From the web browser, enter the switch's IP address. By default: 192.168.10.1
 - From AXIS Recorder Toolbox, go to **Switch > Open the switch configuration**.
2. Log in with your username and password.
 - Your username is `admin`
 - Your password is located on a sticker that's placed on top of the unit or included in the box content as a self-adhesive sticker.

Log out from the menu bar to exit the switch's management page.

Running configuration

The running configuration is the set of settings that are currently active and operational on your network device. It reflects your device's current state and how it's functioning in real time. However, these changes aren't saved if your device reboots.

In contrast, the startup configuration is the set of settings that are saved on your device's non-volatile memory. This configuration is loaded and applied when your device starts up or restarts.

When you make changes in the web interface and click **Save**, those changes are applied to the running configuration.

To save your settings to the startup configuration, use the **Save** icon in the upper-right corner of the web interface.

If there are unsaved changes in the running configuration, the icon will flash yellow.

Overview

In the menu bar, click **Overview**.

General information

Category	Item	Description
Ports summary	Active ports	The number of ports in use.
	Ports using PoE	The number of PoE-enabled ports in use.

	Locked ports	The number of locked ports.
Power consumption	Current PoE usage	The PoE power in watts consumed by devices and the percentage of consumed PoE power out of the total dedicated PoE power.
	Power requested	The total power in watts and percentage allocated to devices.
Port status	Active	The port is in use.
	Inactive	The port is ready to be used.
	Blocked	The port is blocked.

Note

You can click on a port to view more information about it.

Power management

In the menu bar, click **Power management**.

Port list

Item	Description
Port	The port number that the device is connected to.
PoE	The PoE status. You can click the icon to turn on or turn off PoE on the port.
PoE class	The PoE class of the connected device.
Priority	The priority of power allocation to the connected device. By default, the priority is the port number.
Power consumption (W)	The power in watts consumed by the device connected to the port.
Power requested (W)	The power in watts requested by the device connected to the port.
Power allocated (W)	Manually adjust the power allocated to the port. Only available when you select Manual as the power allocation method.

Allocate power

PoE power can be allocated to the connected devices in the following ways:

- **PoE class:** The switch allocates PoE power based on the PoE class of the connected device.
- **Manual:** You can manually adjust PoE power allocated to the connected device.
- **LLDP-MED:** The switch communicates with the connected device and dynamically allocates PoE power as needed.

Note

The LLDP-MED power allocation method only works for cameras with AXIS OS 9.20 or later.

To change the power allocation method:

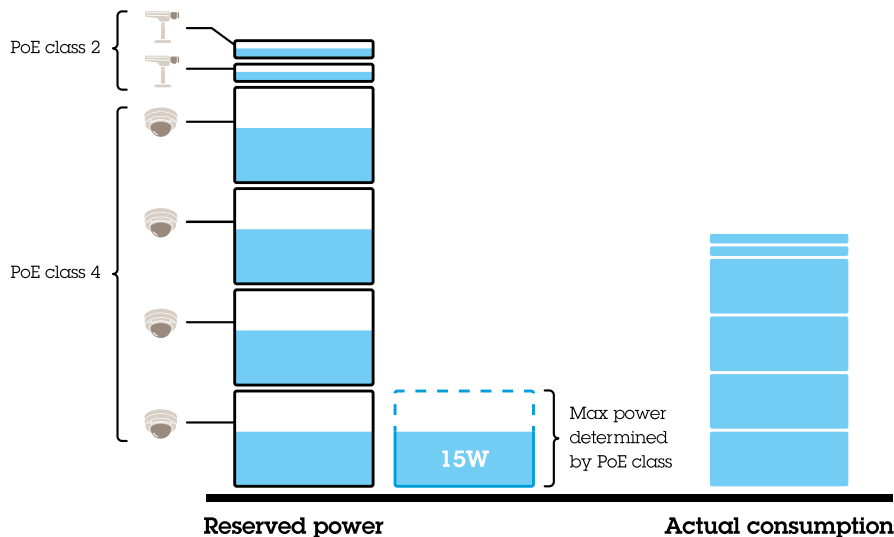
1. In the switch's power management page, go to **Power management**.
2. Select **PoE class**, **Manual**, or **LLDP-MED** under **Allocate power**

3. If you have selected **Manual**, you can change the power allocated to the connected device in the **Power allocated** column.
4. If you want to change the priority of the connected device, select a priority for that device. The priority of other devices will change automatically.

Example:

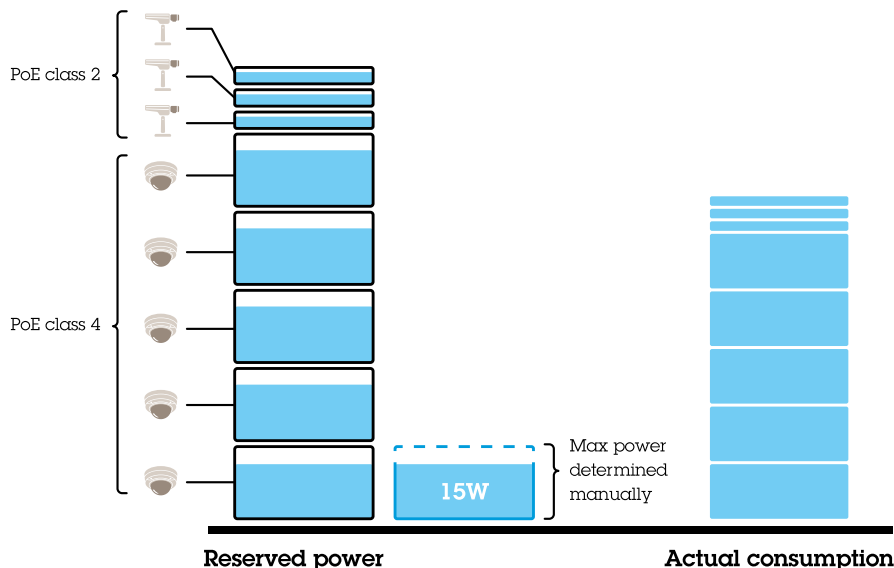
In this example, the switch has a total power budget of 135 W. A PoE class 4 device requests 30 W power but only consumes 15 W. A PoE class 2 device requests 7 W power but only consumes 5 W power.

Allocate power by PoE class



The power requested by each device is determined by the PoE class. The switch can power 4 PoE class 4 devices and 2 PoE class 2 devices. The total power requested is $(4 \times 30) + (2 \times 7) = 134$ W. The actual power consumed is $(4 \times 15) + (2 \times 5) = 70$ W. In this way, all connected devices are guaranteed enough power and the priority is less important.

Allocate power manually



The power requested is manually adjusted to 20 W for PoE class 4 devices. The switch can power 5 PoE class 4 devices and 3 PoE class 2 devices. The total power requested is $(5 \times 20) + (3 \times 7) = 121$ W. The actual power consumed is $(5 \times 15) + (3 \times 5) = 90$ W. In this way, all connected devices are guaranteed enough power and the priority is less important.

Turn on and turn off PoE

Turn on PoE on a port

1. In the menu bar, click **Overview**.
2. In the PoE column, click  to turn on PoE on the specific port.

Turn off PoE on a port

1. In the menu bar, click **Overview**.
2. In the PoE column, click  to turn off PoE on the specific port.

Turn on and turn off PoE on all ports

1. In the menu bar, click **Power management**.
2. To turn off PoE on all ports, go to the **PoE ports state** drop-down menu and select **Turn off all**.
3. To turn on PoE on all ports, go to the **PoE ports state** drop-down menu and select **Turn on all**.

Network overview

The network overview provides detailed information about the network traffic status of each port.

PoE ports

Item	Description
Port	The port number that the device is connected to.
Device	The name of the device connected to the port.
IP address	The IP address of the device connected to the port.
MAC address	The MAC address of the device connected to the port.
Receive	The current data rate in megabits per second for inbound data on the port.
Transmit	The current data rate in megabits per second for outbound data on the port.
Packet sent	The number of data packets that the switch has transmitted to the network.
Packet received	The number of data packets that the switch has received from the network.
Packet lost	The number and percentage of data packets that failed to reach their destination due to network issues.
Lock	Displays whether the port is locked. You can click the icon to lock or unlock the port.

Lock and unlock ports

You can lock a MAC address to a port so that only traffic coming from that MAC address will pass. This improves security and prevents unauthorized users from connecting a laptop or other devices to the security network.

Lock a MAC address to a port

1. In the menu bar, click **Network overview**.
2. In the Lock column, click  to lock the specific port.

Unlock a MAC address from a port

1. In the menu bar, click **Network overview**.

2. In the **Lock** column, click  to unlock the specific port.

Lock or unlock all ports

1. In the menu bar, click **Network overview**.
2. To lock all ports, go to the **Lock ports** drop-down menu and select **Lock all**.
3. To unlock all ports, go to the **Lock ports** drop-down menu and select **Unlock all**.

Settings

Configure network settings

You can change the switch's IP address. But for most camera installations, we recommend using the default settings. The reason for this is that a surveillance network is normally isolated from other networks, for example a corporate LAN. In this case, you would only use the surveillance network to manage and collect surveillance devices and data from the video management software installed on the server.

1. In the menu bar, go to **Settings > Network settings**.
2. Enter the connection type, IP address, subnet mask, gateway, primary DNS, secondary DNS, and hostname.

Note

The factory default settings are: a static IP connection with address 192.168.10.1 and a subnet mask with address 255.255.255.0.

3. Click **Save**.

Configure date and time

1. In the menu bar, go to **Settings > Date and time**.
2. Select the country and time zone.
3. To set the time manually, select **Manual** and manually adjust the time.
4. To set up an NTP server, select **NTP server** and enter the NTP server address.

Note

NTP only works when the switch is connected to a network and configured with Internet access.

5. Click **Save**.

Configure DHCP server

You can configure the switch to use its internal DHCP server for assigning IP addresses to connected devices. When you use the switch uplink connection to allow devices to access or be accessed by external applications, you must specify the gateway and DNS addresses.

1. In the menu bar, go to **Settings > DHCP server**.
2. Select **Enable DHCP server**.
3. Enter the start IP address, end IP address, subnet mask, gateway, primary DNS, secondary DNS, lease length, and domain name.
4. Click **Save**.

Configure SNMP

1. In the menu bar, go to **Settings > SNMP**.
2. Enter the server name, contact, and location used for the SNMP connection.
3. If you want to use SNMPV1 or SNMPV2c, select **SNMPV1 / SNMPV2c** and enter the read community.

4. If you want to use SNMPV3, select **SNMPV3 (MD5)** and enter the username and password.

Note

Currently we only support MD5 authentication used for SNMP.

5. Click **Save**.

Maintenance

Update firmware

1. In the menu bar, go to **Maintenance > Update firmware**.
2. Drag and drop the firmware file or click **Browse** and navigate to the firmware file.
3. Click **Upload**.
4. Once the firmware has been updated, reboot the switch.

Reboot the switch

Important

While the switch reboots, all connected devices will temporarily lose connection with the switch including PoE.

1. In the menu bar, go to **Maintenance > Reboot switch**.
2. Click **Reboot** and **Yes**.
3. When the switch reboots after a few minutes, enter your username and password to log in.

Backup the switch's settings

Note

The username and password are included in the backup file.

1. In the menu bar, go to **Maintenance > Backup and restore**.
2. Click **Create a backup file**. This creates a backup file in the .bin format and saves it in your **Downloads** folder.

Restore the switch's settings

Note

To restore the switch's settings, you must previously have created a backup file.

1. In the menu bar, go to **Maintenance > Backup and restore**.
2. Drag and drop the backup file or click **Browse** and navigate to the backup file.
3. Click **Upload**.

It can take a few minutes to restore the switch from the backup file. Once the settings are restored, the switch will automatically reboot, and you will need to log in again.

Manage certificates

1. In the menu bar, go to **Maintenance > Manage certificates**.
2. Click  and navigate to your private key file.
3. Click  and navigate to your certificate file.
4. Click  and navigate to your CA bundle file.
5. Click **Save**.

6. Reboot the switch.

Change password

You can change the switch's default password to a password you choose yourself.

Important

Make sure to select a password you can remember. If you forget the password, see *Reset to factory default settings, on page 33* to restore the factory default password.

1. In the menu bar, go to **Maintenance > Change password**.
2. Enter the current password and your new password as required.
3. Click **Save**.

Configure web settings

1. In the menu bar, go to **Maintenance > Web settings**.
2. Enter the port number.

Note

- If you decide to change the port number, make sure to write down the new port number. If you forget the new port number, see *Reset to factory default settings, on page 33* to restore the factory default port number.
- We recommend that you keep HTTPS enabled.

Reset to factory default settings

Hold down the reset button for five seconds to reset the switch to its factory default settings.

You can also reset the switch through the web interface:

1. In the menu bar, go to **Maintenance > Reset to factory default settings**.
2. Click **Reset** and **Yes**.

After the reset is done, the switch will reboot automatically.

Logs

In the menu bar, click **Logs** to see a list of logs. Click the column title to sort in alphabetical order.

Item	Description
Time	The date and time the log event occurred.
Level	The level of severity displayed as warning icons.
User	The user that initiated the log event.
IP address	The IP address of the user that initiated the log event.
Service	The service that the log event is related to. Possible values are desktop, network, network, system, ntpd, storage, dhcp, etc.
Event	A description of the log event.

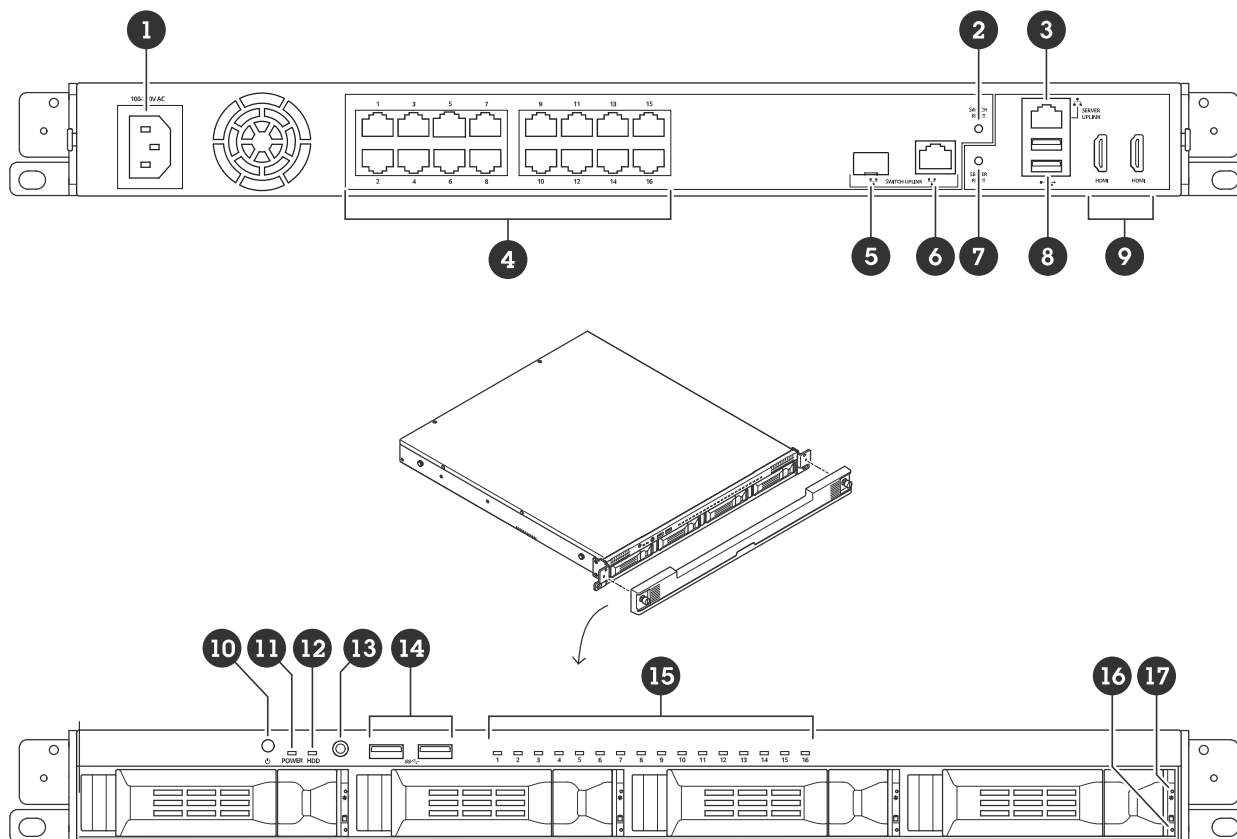
Create switch reports

In the log page, click **Export** to create a text file with switch information, including the log entries from the log page.

Specifications

Product overview

Front and rear



- 1 Power connector
- 2 Switch reset button
- 3 1 GbE Ethernet port – Server uplink
- 4 1 GbE PoE Ethernet ports
- 5 1 GbE Ethernet port – Switch uplink (SFP)
- 6 1 GbE Ethernet port – Switch uplink (RJ45)
- 7 Server reset button
- 8 USB 2.0 ports
- 9 HDMI ports
- 10 Power button
- 11 Power LED
- 12 Hard drive activity LED
- 13 Universal audio jack
- 14 USB 3.2 ports
- 15 PoE Ethernet ports status LED
- 16 Hard drive activity LED
- 17 Hard drive status LED

LED indicators

Front LEDs

Power button	Power LED	Indication
Not pressed	Off	PC and switch are off
	Amber	PC is on and switch is off
	Blinks amber	PC is on and switch is booting
	Green	PC is on and the switch has finished booting
Pressed	Up to 0 seconds	Powers on both the switch and PC if they are turned off
	Until it blinks amber (3 seconds)	Switch initiates graceful shutdown
	Until it blinks red (6 seconds)	PC and switch initiate graceful shutdown
	Until it turns solid red (9 seconds)	PC initiates ungraceful shutdown, switch initiates graceful shutdown

LED indicator	Color	Indication
Hard drive (HDD)	Blinks green	Hard drive activity
	Red	Possible hard drive failure
PoE Ethernet port status	Green	Link state
	Amber	Powered device, no link state
	Red	PoE budget exceeded
Hard drive status	Green	Hard drive present
	Red	Possible hard drive failure

Rear LEDs

Network speed and activity	Color	Indication
Right LED	Amber	10/100 Mbit/s
	Green	1000 Mbit/s
Left LED	Green	PoE connection OK
	Red	PoE budget exceeded

Troubleshooting

Reset your server

You can use the server reset button to reset your server. It will take more than one hour to reset your server.

1. Power off your device.
2. Press and hold the server reset button for 5 seconds. Windows® RE will be started.
3. Select Troubleshoot.
4. Select Reset your PC.
5. Select Keep my files or Remove everything. If you select Keep my files, you need to provide the administrator credentials.
6. Follow the instructions on the screen.
7. The server reboots and starts the procedure to restore Windows® to factory default settings.



Reset your server to factory default settings

Perform a system recovery

If the device has had a complete system failure, you must use a recovery image to recreate the Windows® system. To download the AXIS Network Video Recorder Recovery Kit, contact Axis technical support and supply the serial number of your device.

Note

The AXIS Network Video Recorder Recovery Kit comes in two variants:

- **sb11** – for devices still using the 2011 certificate.
- **sb23** – for devices that have moved to the 2023 certificate.

Check your certificate status before you download the Recovery Kit, and select the matching variant. If you select the wrong variant, the installation won't produce a bootable result, and you'll need to start over with the correct image. This won't damage your device.

If your device already has the 2023 certificate installed, the sb11 variant is still safe to use, as long as the 2011 certificate hasn't been manually revoked. Once it's revoked, only sb23 will work.

To recreate the system:

1. Download the AXIS Network Video Recorder Recovery Kit and AXIS Network Video Recorder Recovery: ISO to USB Tool.
2. Insert a USB drive into your computer.
 - Use a USB drive with a minimum of 16 GB.
 - The USB drive will be formatted, and all existing data will be erased.
3. Run the AXIS Network Video Recorder Recovery: ISO to USB Tool and follow the onscreen instructions. Writing data to the USB drive takes approximately 10 to 15 min. Don't remove the USB drive until the process is complete.
4. After the AXIS Network Video Recorder Recovery: ISO to USB Tool is complete, take the USB drive and plug it into your device.
5. Start your device.

6. When you see the Axis splash screen, press F12.
7. Click **UEFI: USB Drive**.
8. Navigate to your USB drive and press enter. The system boots into the AXIS Network Video Recorder Recovery Kit.
9. Click **Reinstall Operating System**.
The recovery takes roughly 10 to 15 min to complete. You find detailed instructions in the download for the recovery kit.

Troubleshoot AXIS Camera Station Pro

For information about how to troubleshoot AXIS Camera Station Pro, go to the *AXIS Camera Station Pro user manual*.

Need more help?

Useful links

- *AXIS Camera Station Pro user manual*
- *Sign in to AXIS Secure Remote Access*
- *Sign in to AXIS Secure Remote Access v2*
- *What to include in an Antivirus allow list for AXIS Camera Station*

Contact support

If you need more help, go to axis.com/support.

T10207038

2026-09 (M6.2)

© 2024 – 2026 Axis Communications AB