

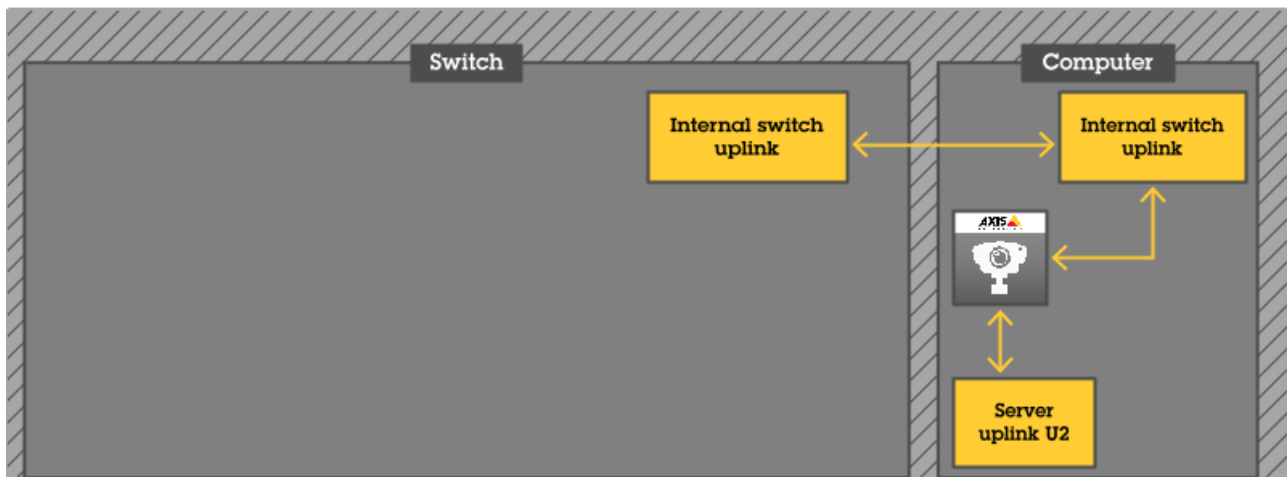
AXIS Camera Station S2108 Appliance

About your device

AXIS Camera Station S2108 Appliance is an all-in-one recording solution with integrated PoE switch designed to deliver reliable high-definition surveillance, supporting cameras up to 4K resolution. For quick and easy installation, the appliance is preconfigured and preloaded with AXIS Camera Station video management software including licenses plus all necessary system software. AXIS Camera Station offers an intuitive user interface that allows users to take full advantage of Axis wide range of video surveillance cameras and other IP products. With the operating system stored on a solid-state drive (SSD) and 5-year hardware warranty, the appliance provides a reliable surveillance solution.

AXIS Camera Station S2108 Appliance consists of two parts:

- **Switch:** Built-in Power over Ethernet (PoE) switch.
- **Computer:** Preloaded with all necessary software you need to create a surveillance solution including the video management software AXIS Camera Station.

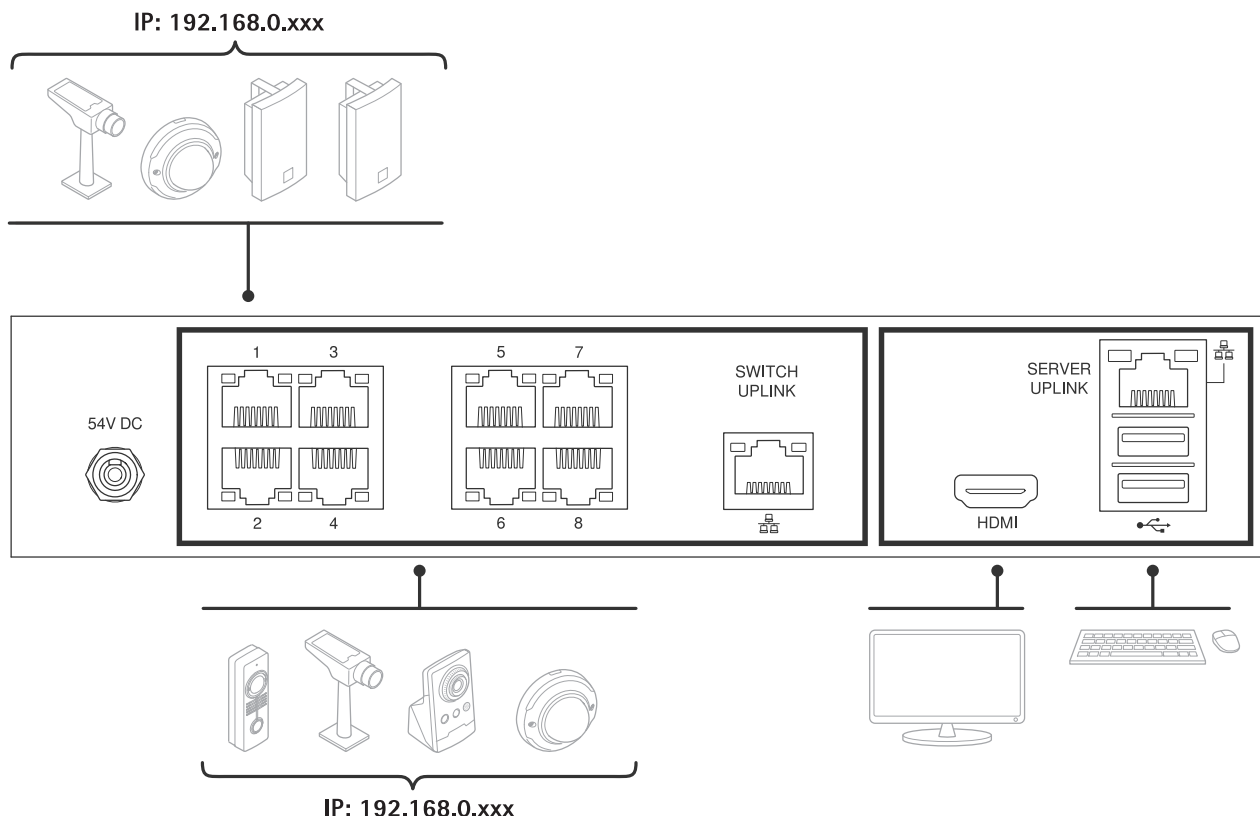


- The switch and computer are two separate parts.
- The switch and computer communicate through the internal uplink connectors: one is located on the switch Power Circuit Board and the other is located on the computer motherboard.
- The server uplink is an external network interface that can connect to an existing network.
- Devices connected to server uplink can not communicate with devices connected to the switch directly.
- Devices connected to server uplink can communicate with devices connected to the switch through AXIS Camera Station.

Setup examples

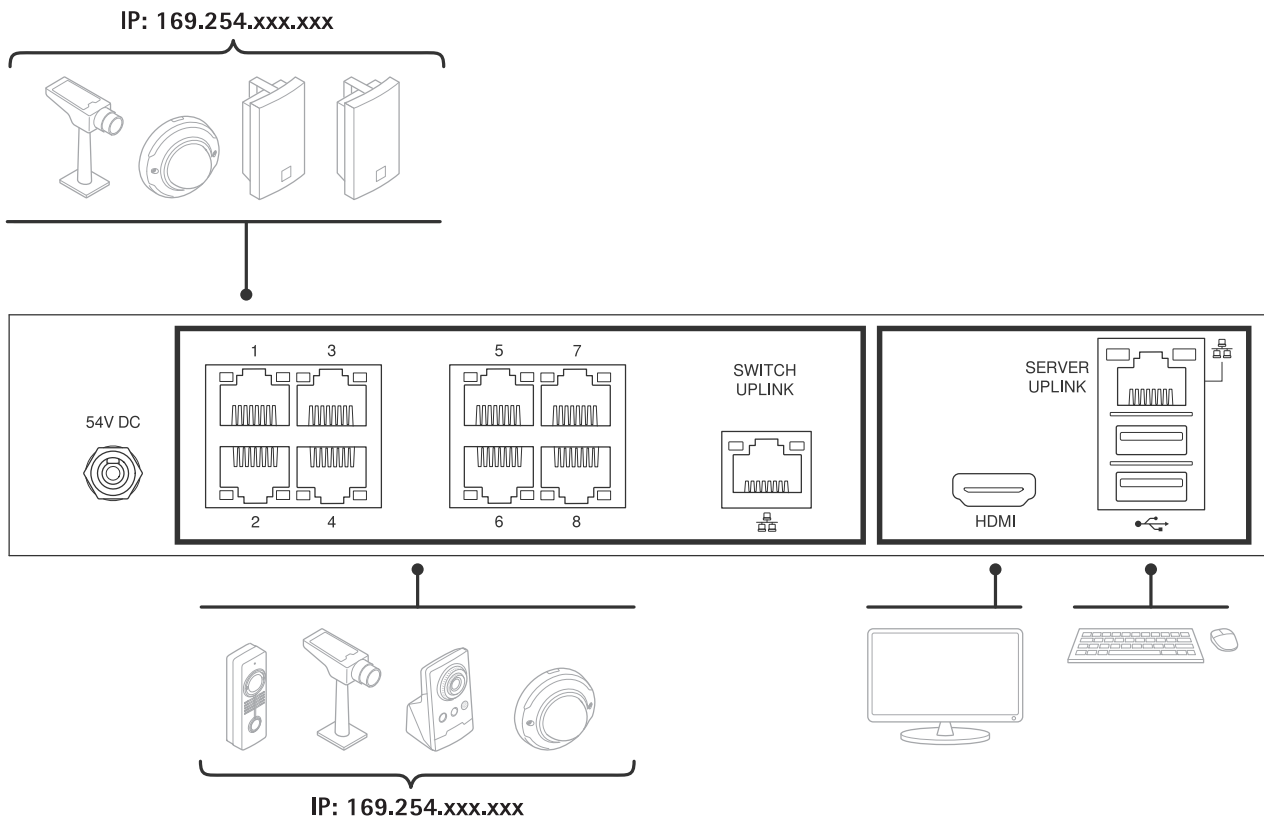
Assign static address to each device

You can create an independent network by assigning static IP address to each device and the AXIS S2108 Appliance. This network will have no interconnectivity to another external network unless parameters match between the networks. The computer can still get internet connectivity through the server uplink port. As soon as the devices are plugged into the powered PoE ports, they will take the link-local address and will need a fixed IP set, matching the AXIS S2108 Appliance.



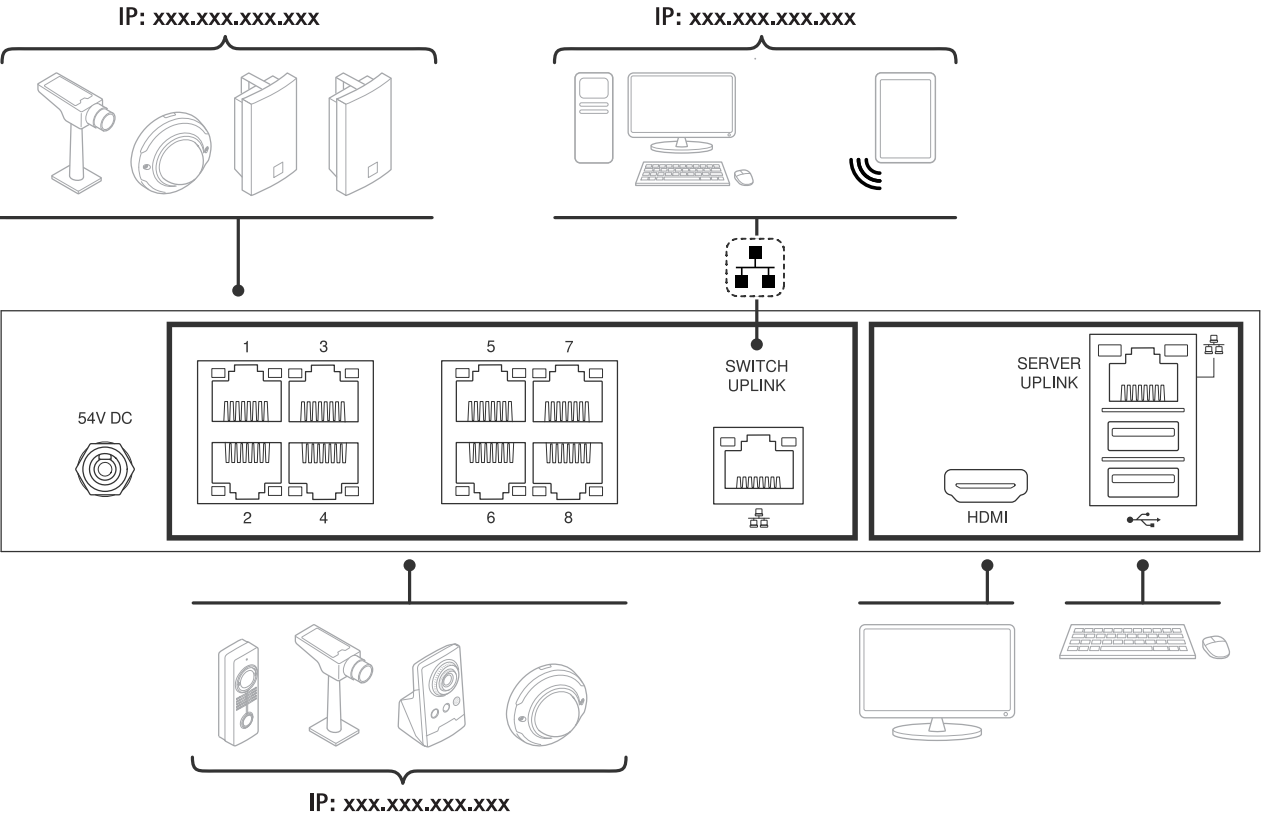
Use local address

You can create an independent network by using link-local address on each device and the AXIS S2108 Appliance. This network will have no interconnectivity to another external network. The computer can still get internet connectivity through the server uplink port. As soon as the devices are plugged into the powered PoE ports, they will take the link-local address and can be found by AXIS Camera Station on the AXIS S2108 Appliance.



Use a DHCP server from another network

You can join the AXIS S2108 Appliance and connected devices by having an existing network and DHCP server plugged in the switch uplink. This will make all connected devices to have an IP address from the DHCP server's range. If internet connectivity is available on that network, it will be available to the AXIS S2108 Appliance too. Otherwise, the computer can still get internet connectivity independently through the server uplink port. When the devices are plugged into the powered PoE ports, they will take the DHCP address if the DHCP server is active.



Get started

The standard workflow to configure an AXIS Camera Station 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 15*.
4. Configure Windows®. We recommend to:
 - Update Windows® to the latest version. See .
 - Create a standard user account. See *Create a user account, on page 20*.
5. Update AXIS Camera Station to the latest version.
 - If your system is online: open the AXIS Recorder Toolbox app and click **Update AXIS Camera Station**.
 - If your system is offline: go to *axis.com* and download the latest version.
6. Start the AXIS Camera Station client.
7. *Connect to AXIS Camera Station server*
8. *Configure AXIS Camera Station, on page 16*

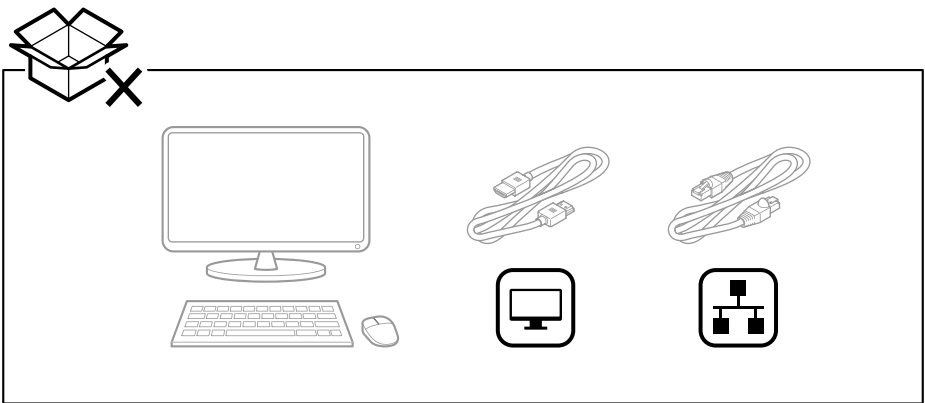
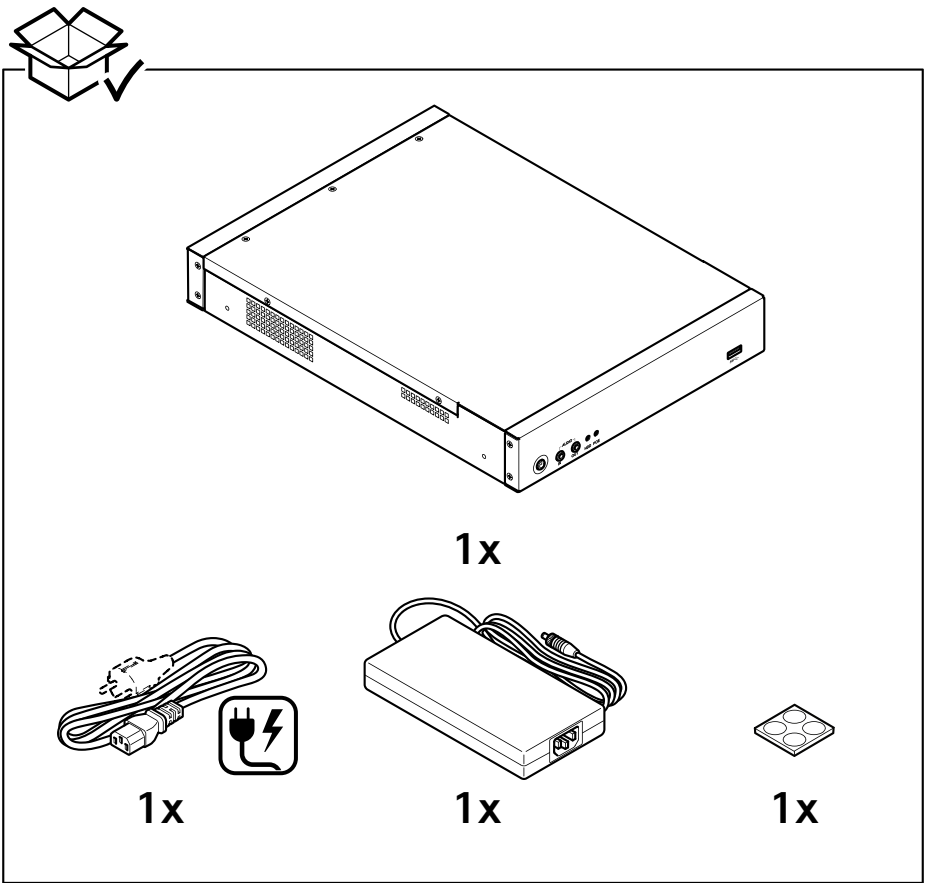
Install your device

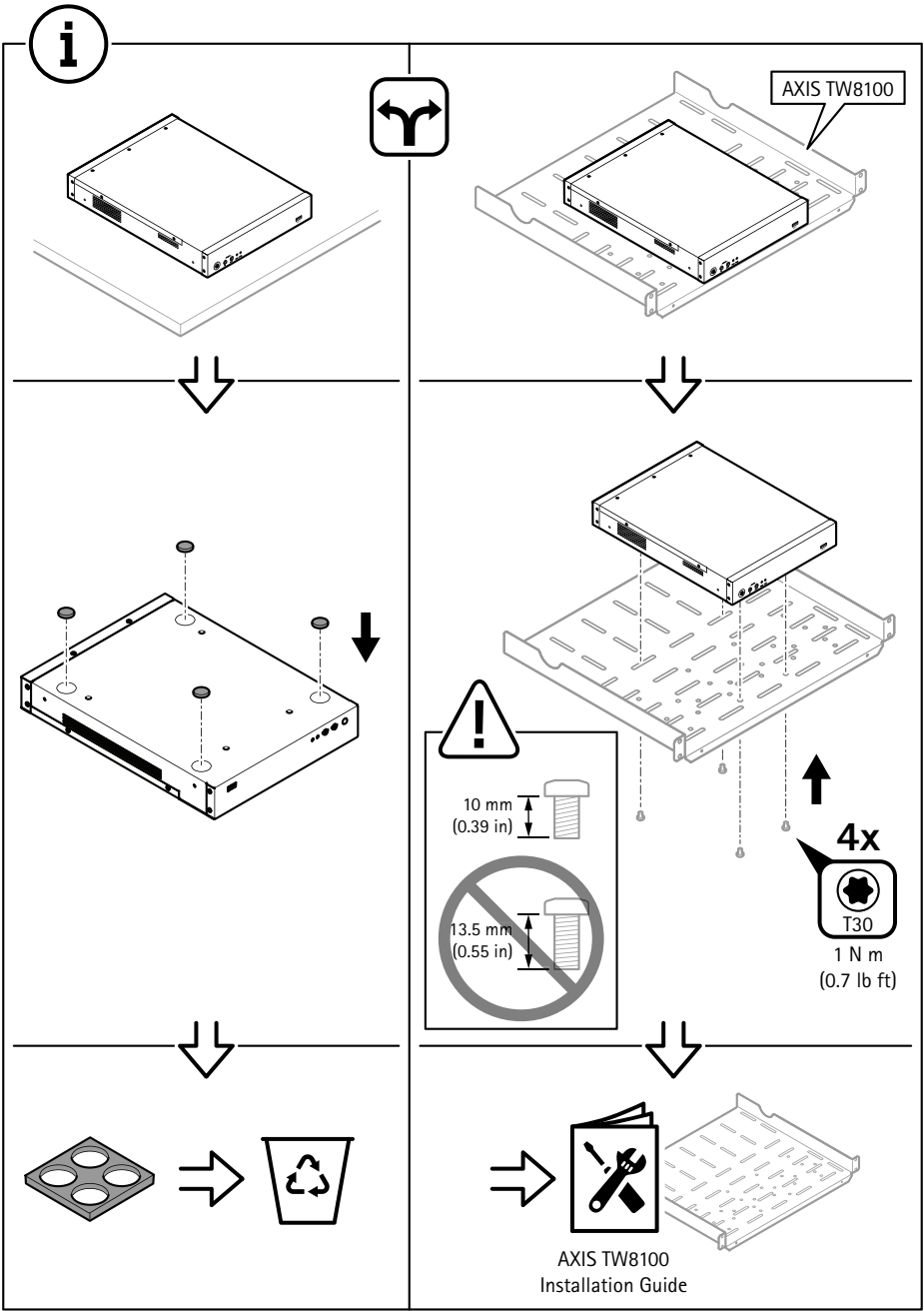
Before installation

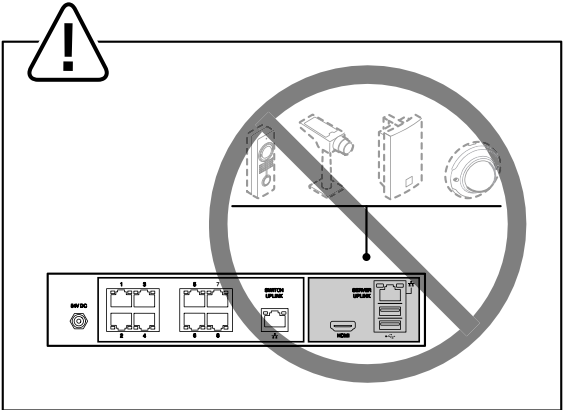
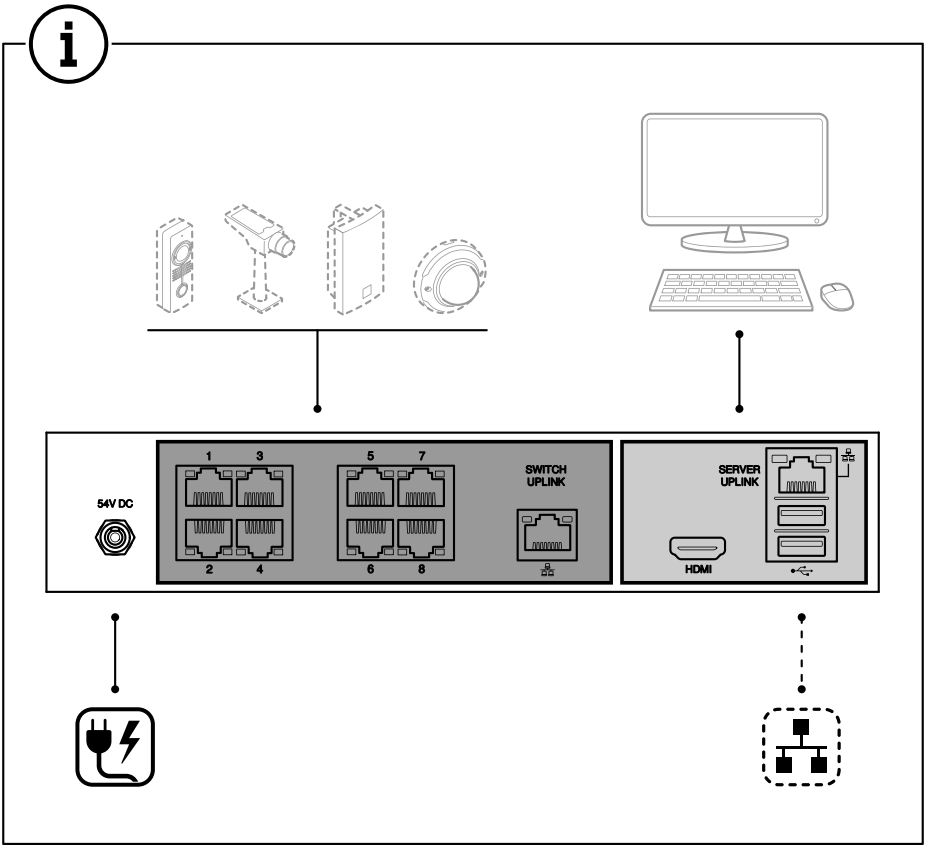
- Prepare additional accessories used for installation: monitor, mouse, keyboard and network cable.
- Understand the usage of different user accounts.

The following table lists the user accounts that can be used for installation, configuration and operation of your Axis system.

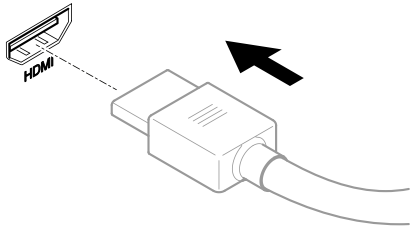
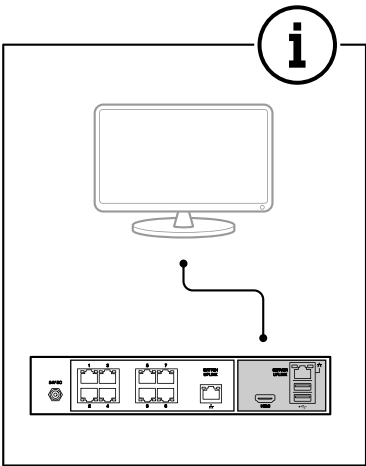
User account	Description	Note
MyAxis	Used to download the latest software, access the license system, Axis Secure Remote Access, and System Health Monitoring.	Registered from <i>my.axis.com</i> .
Windows®		
Windows® administrator	Administrator privileges in Windows®. We recommend you do not use it as AXIS Camera Station administrator.	Created during initial Windows® setup.
Windows® user with AXIS Camera Station administrator privileges	A Windows® user granted with administrator privileges in AXIS Camera Station to be used by system integrator or system administrator for configuration or troubleshooting.	Created in Windows® settings.
Windows® user with AXIS Camera Station operator or viewer privileges	A Windows® user granted with operator or viewer privileges in AXIS Camera Station.	Created in Windows® settings.
Device		
Device administrator	Used by the administrator to access the camera from the video management system or device webpage.	Created from the device webpage or when you add the device to AXIS Camera Station.



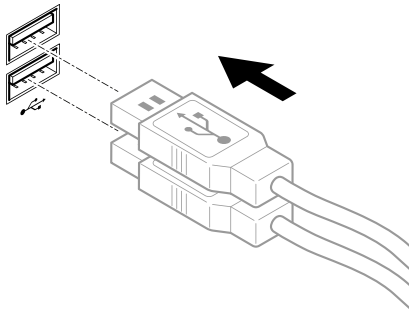
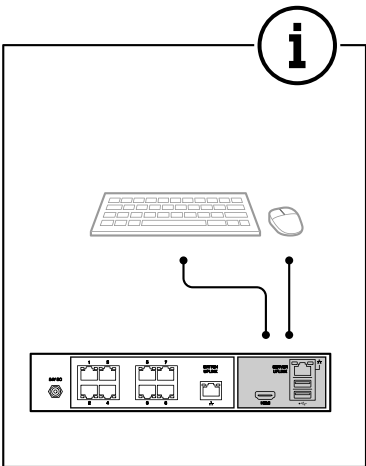




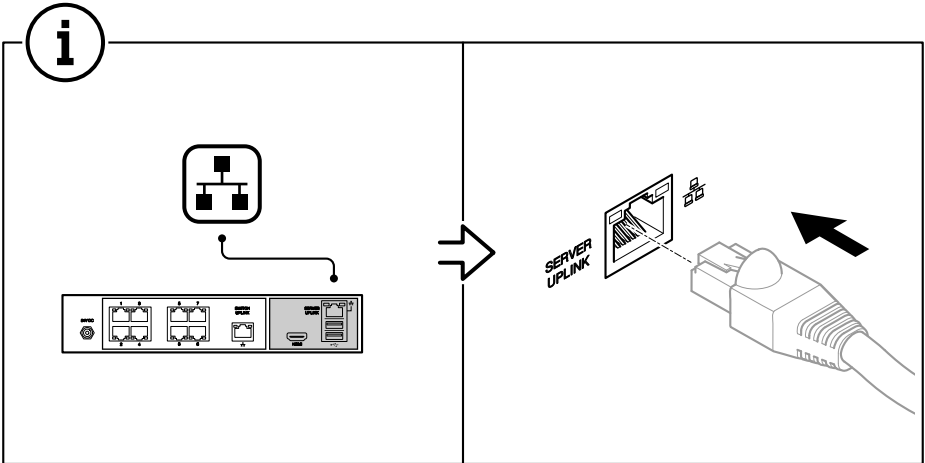
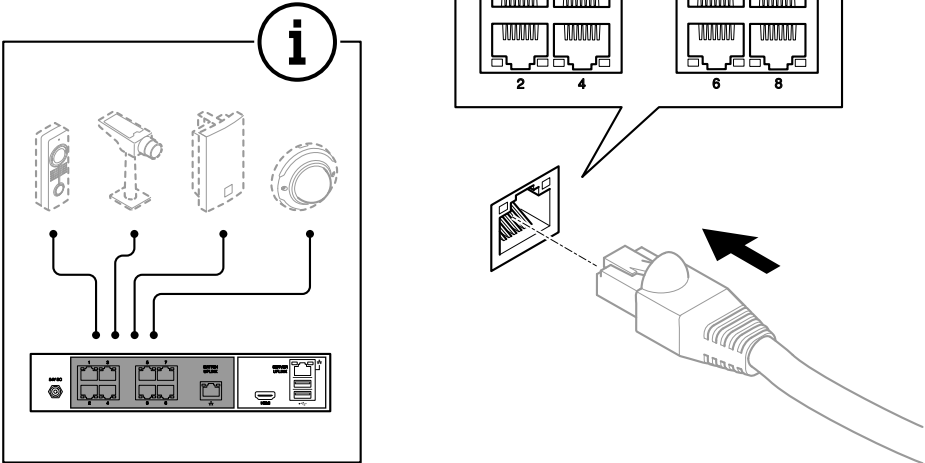
1.1



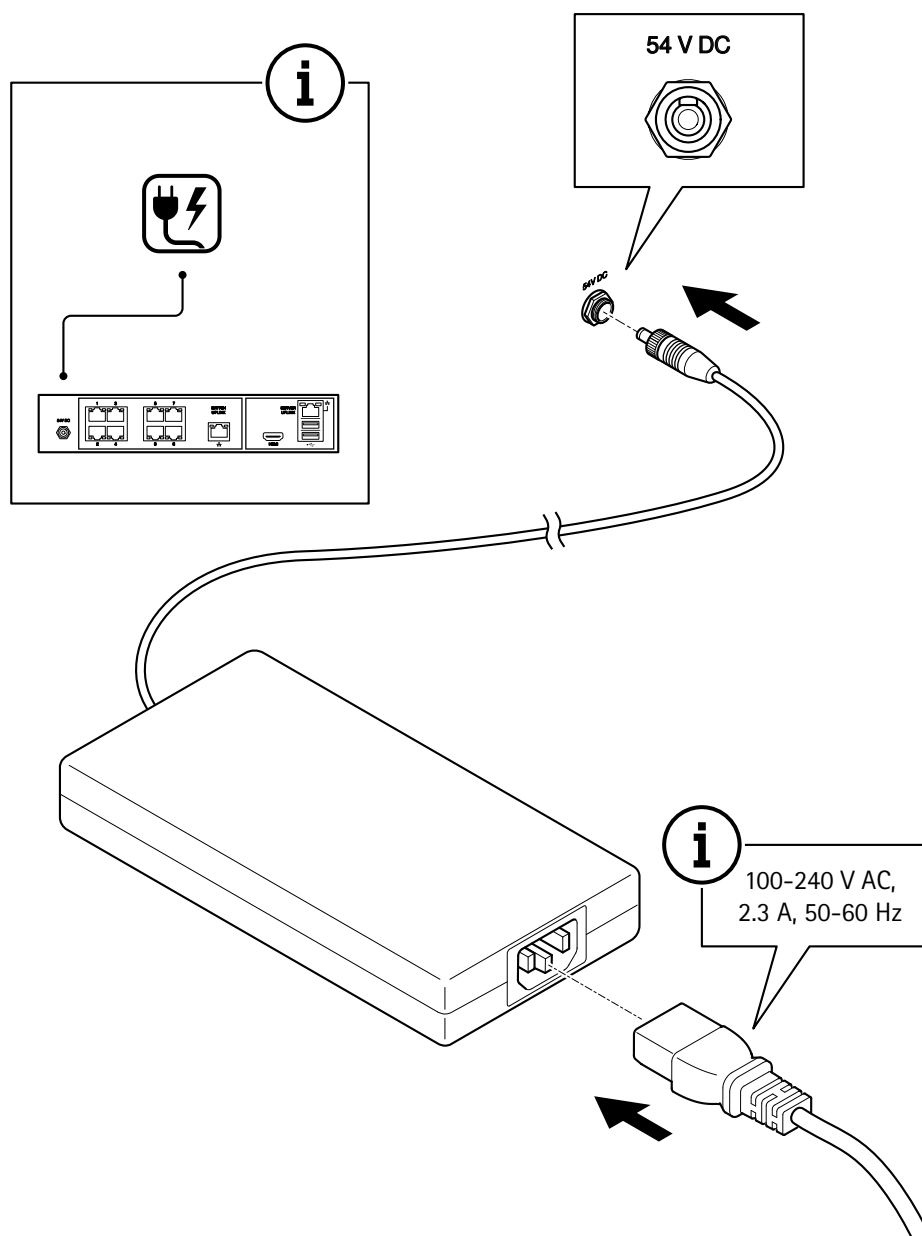
1.2



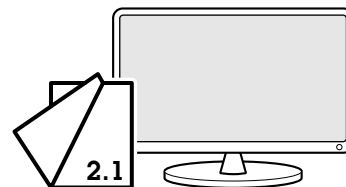
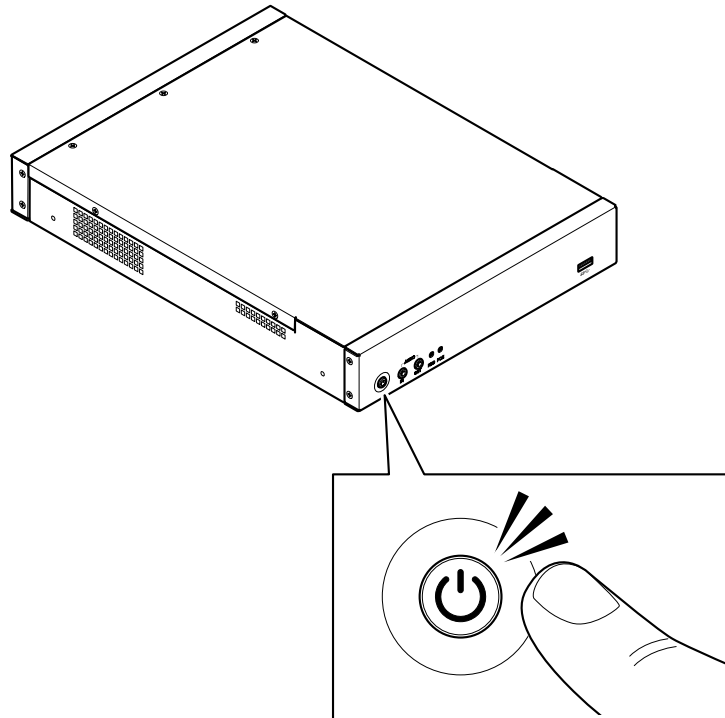
1.3



1.4



1.5



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.

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.

Log in to the server

Using the AXIS Camera Station client, you can connect to multiple servers or a single server installed on the local computer or somewhere else on the network. You can connect to AXIS Camera Station servers in different ways:

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

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

Remote server – See *Connect to a remote server, on page 16*.

AXIS Secure Remote Access – See *Sign in to AXIS Secure Remote Access, on page 16*.

Note

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

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 all connected servers, click Delete saved passwords .
Change client proxy settings	You might need to change the client proxy settings to connect to a server, click Change client proxy settings .

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 S2108 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 S2108 Appliance server, you must configure the proxy settings in Windows on the AXIS Camera Station S2108 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

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

Before you start:

- Configure your network depending on your installation. See *Network configuration, on page 18*.
- Configure your server ports if needed. See *Server port configuration, on page 19*.
- Consider security issues. See *Security considerations*.

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

1. *Start the video management system, on page 17*
2. *Add devices, on page 17*
3. *Configure recording method, on page 17*
4. *View live video, on page 17*
5. *View recordings, on page 17*

6. *Add bookmarks, on page 17*
7. *Export recordings, on page 18*
8. *Play and verify recordings in AXIS File Player, on page 18*

Start the video management system

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

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

Add devices

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

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

Configure recording method

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

View live video

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

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 if the AXIS Camera Station client, AXIS Camera Station server, and the connected network devices are on different networks.

Client proxy settings

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

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

Server proxy settings

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

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

NAT and Firewall

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

Server port configuration

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

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 S2108 Appliance server, cameras, video encoders, and auxiliary devices on a secure network, separate from the office network. You can install the AXIS Camera Station S2108 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

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

1. Go to **Configuration > Licenses > Management**.
2. Make sure **Manage licenses online** turns on.
3. Sign in with your My Axis account.
4. The license key automatically generates and appears under **License keys**.
5. If you purchased license keys separately, enter your license key under **Add license key**.
6. Click **Add**.
7. In AXIS Camera Station client, make sure your license keys appear under **Configuration > Licenses > Keys**.

License a system offline

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

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 people > Add someone else to this PC**.
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 user accounts

User permissions

Go to **Configuration > Security > User permissions** to see the users and groups in AXIS Camera Station S2108 Appliance.

Note

Administrators of the computer that runs the AXIS Camera Station S2108 Appliance server are automatically granted administrator privileges in AXIS Camera Station S2108 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 S2108 Appliance. To add a user to AXIS Camera Station S2108 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 S2108 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 S2108 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 S2108 Appliance.
Edit	Allows editing of views in AXIS Camera Station S2108 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\Service.
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
<i>AXIS S2108</i>	Z218-004
<i>AXIS S2208 Mk II</i>	Z670-005
<i>AXIS S2212 Mk II</i>	Z671-005
<i>AXIS S2216 Mk II</i>	Z672-005
<i>AXIS S2224 Mk II</i>	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**.

Power management

The switch has a total power budget of 105 W. This is the maximum power output to all connected devices.

In most cases, the connected devices consume less power than requested. To optimize the power usage, the PoE controller allows connected devices to request up to 125 W and limits the actual power usage to 105 W at the same time.

For example, the switch can power 8 PoE class 3 devices.

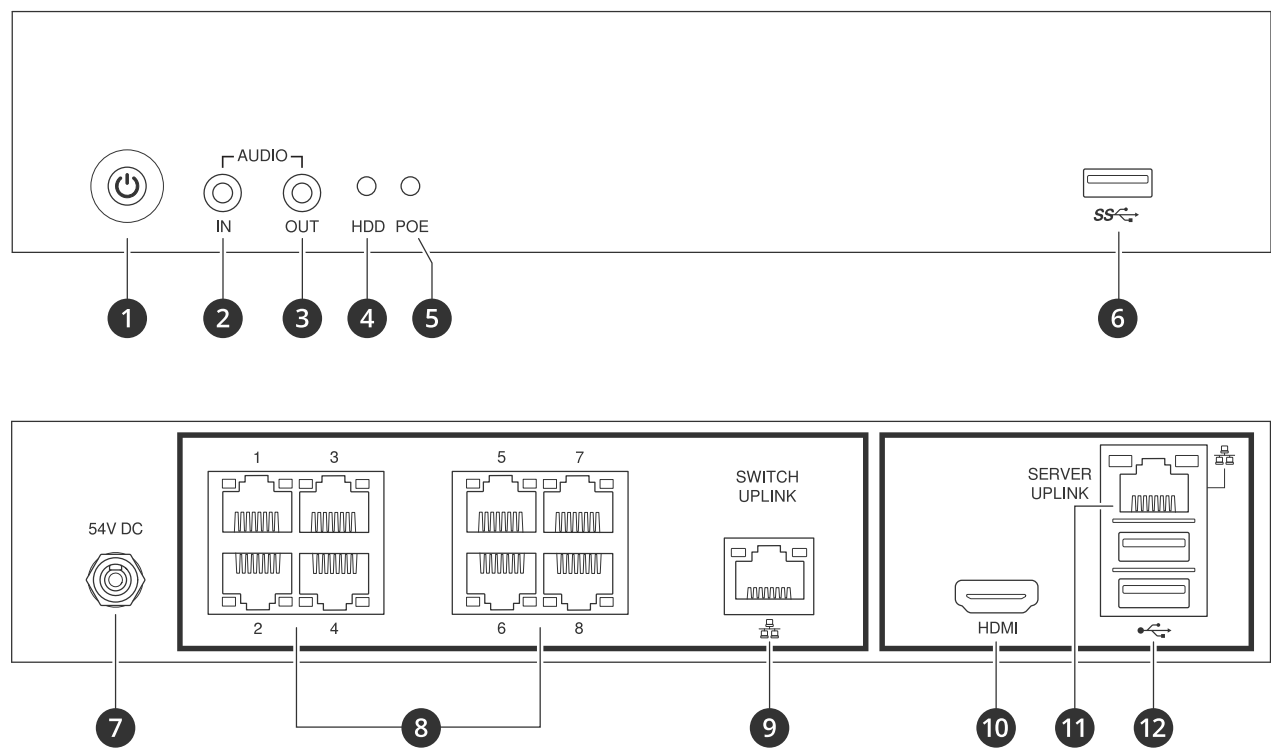
- 1 PoE class 3 device requests 15.4 W power.
- 8 PoE class 3 devices request $(8 \times 15.4) = 123.2$ W power. This is within the 125 W limit allowed by the PoE controller.
- 1 PoE class 3 device usually consumes 10–12 W power.
- 8 PoE class 3 devices usually consume 80–96 W power. This is within the 105 W limit of the total power budget.

⚠ WARNING

- When the connected devices request power more than 125 W:
 - The last plugged device will not start.
 - The PoE overload LED will turn on solid red until you unplug the last connected device, or free up enough PoE budget by removing other devices.
- When the connected devices actually consume power more than 105 W:
 - The last device powered on will shut down and try to restart.
 - The PoE overload LED will not turn on.

Product overview

Front and rear sides



- 1 Power button/power LED
- 2 Audio in
- 3 Audio out
- 4 Hard drive activity LED
- 5 Status LED of PoE ports
- 6 USB 3.0 port
- 7 Power connector
- 8 PoE ports
- 9 RJ45 switch uplink port
- 10 HDMI port
- 11 RJ45 server uplink port
- 12 USB 2.0 ports

Specifications

Front LEDs

LED indicator	Color	Indication
Power	Green	Server on
Hard drive	Blinks amber	Hard drive activity
	Blinks red	Possible hard drive failure
PoE overload	Red	Over PoE budget
	Off	OK

Rear LEDs

Network speed and activity	Color	Indication
Right LED	Amber	10/100 Mbit/s
	Green ¹	1000 Mbit/s
Left LED	Blinks green	Network activity

1. This is only valid for Switch uplink and Server uplink.

Troubleshooting

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

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

Need more help?

Useful links

- *AXIS Camera Station user manual*
- *Sign in to AXIS Secure Remote Access*
- *What to include in an Antivirus allowlist for AXIS Camera Station*

Contact support

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

T10181903

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB