AXIS Camera Station S22 Appliance Series

AXIS Camera Station S2208 Appliance

AXIS Camera Station S2212 Appliance

AXIS Camera Station S2216 Appliance

AXIS Camera Station S2224 Appliance

User Manual

About your device

AXIS Camera Station S22 Appliance series is an all-in-one recording solution with integrated, manageable PoE switch designed to deliver reliable high-definition surveillance with up to 4K resolution. For quick and easy installation, the appliance series 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 3-year hardware warranty, the appliance series provides a reliable surveillance solution.

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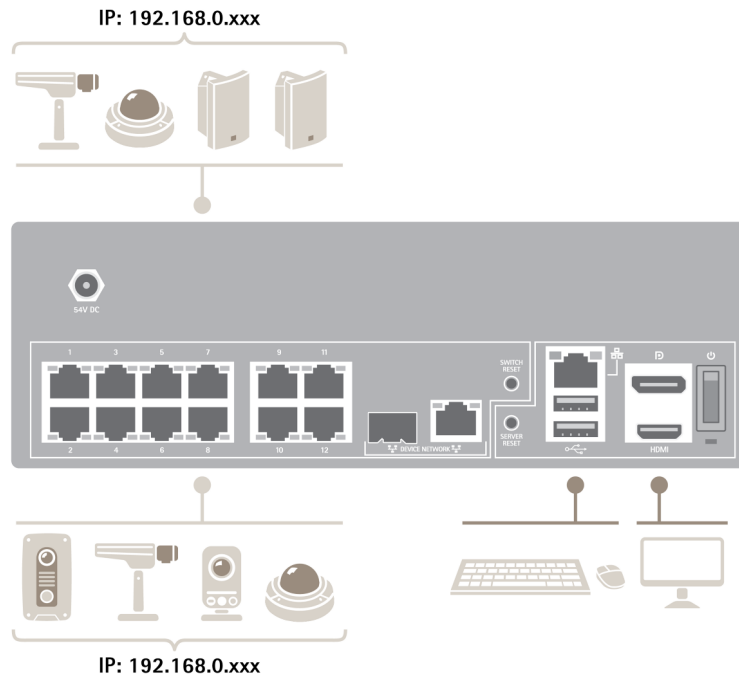
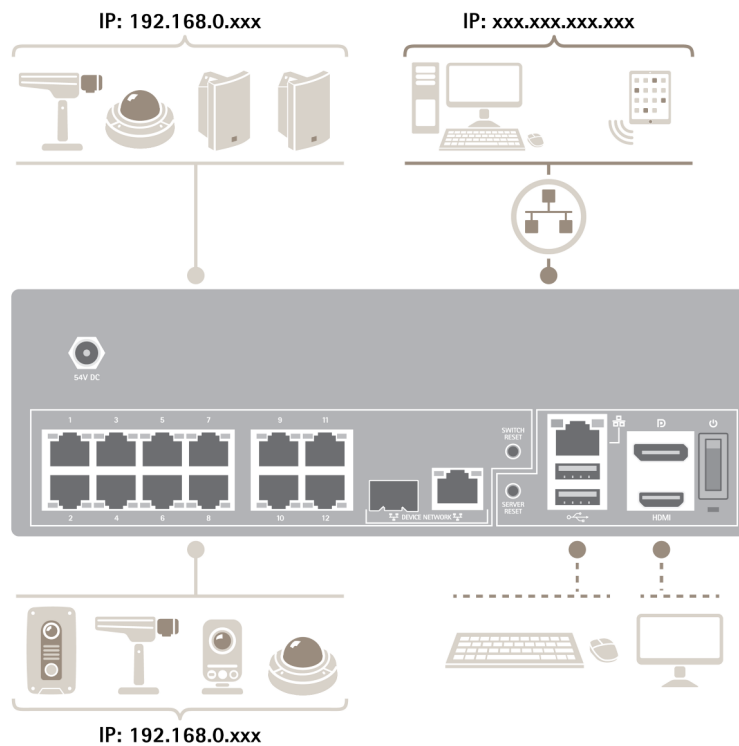| Difficulty level	Basic
Benefits	Dedicated surveillance network with no interconnectivity to another external network
	Plug and play installation
Limitations	Bandwidth
	PoE budget
	No remote access
Actions needed	Change the default password for the built-in switch
	Register the AXIS Camera Station license

Connectors used	PoE enabled network connectors, port 1-12
	USB 2.0 connector x2 (for keyboard and mouse)
	Displayport^{TM} or HDMI connector
Connectors NOT used	RJ45 switch uplink
	SFP switch uplink
	RJ45 server network
	USB 3.0 connector (front side)
	Audio line in (front side)
	Audio line out (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.

Difficulty level	Advanced
Benefits	Ability to use an AXIS Camera Station client to connect to S22 series over the network.
	Network segregation
Limitations	May require you to follow corporate network polices

AXIS Camera Station S22 Appliance Series

Setup examples

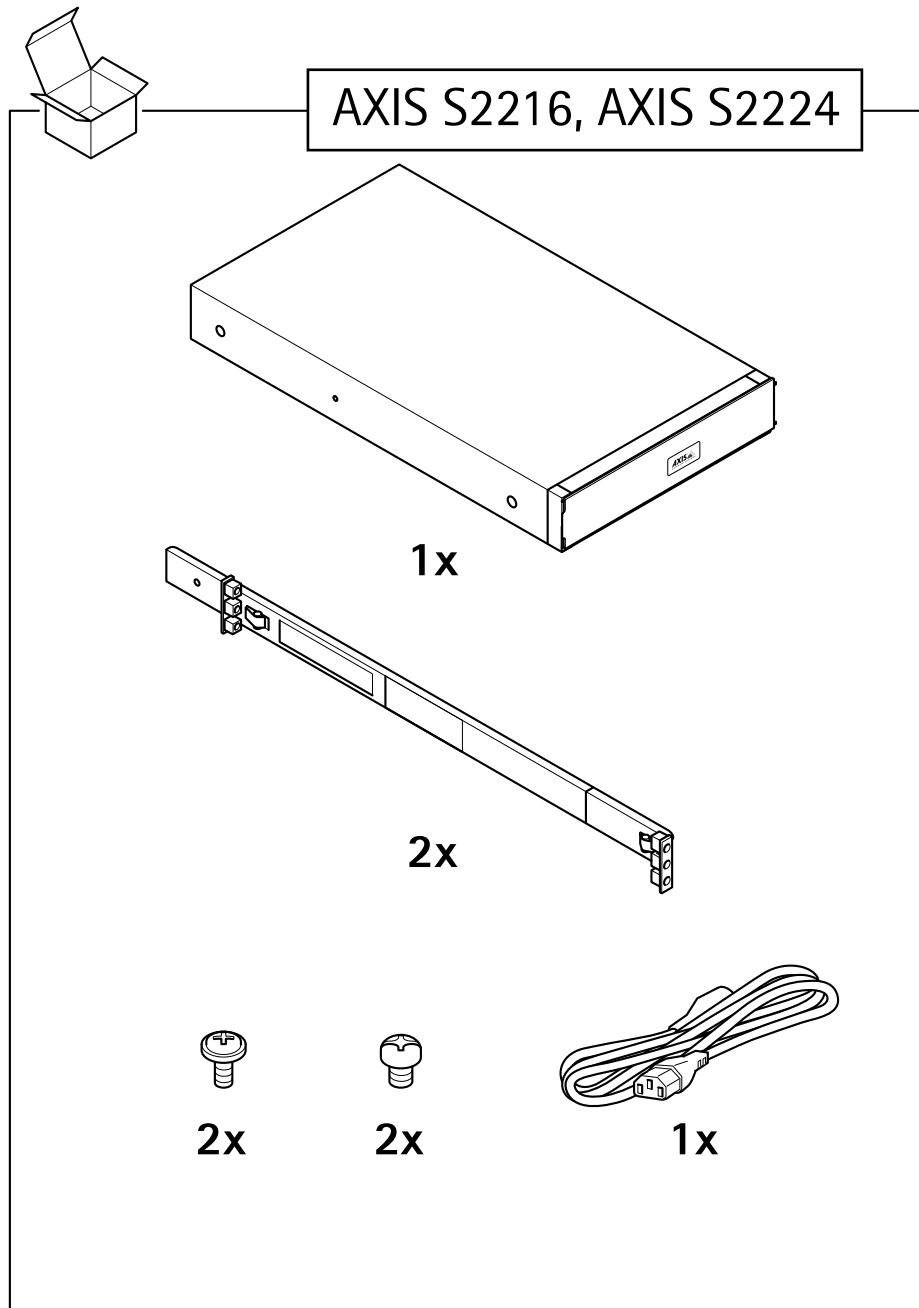|	
Actions needed	Change the default password for the built-in switch
	Register the AXIS Camera Station license
Connectors used	PoE enabled network connectors, port 1-12
	RJ 45 server network (for connection to network)
	(Optional) USB 2.0 connector x2 (for keyboard and mouse)
	(Optional) Displayport^{TM} or HDMI connector
Connectors NOT used	RJ 45 switch uplink
	SFP switch uplink
	USB 3.0 connector (front side)
	Audio line in (front side)
	Audio line out (front side)

Get started

The standard workflow to configure an AXIS Camera Station recorder is:

1. *Install your device*

2. 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.

3. Configure Windows®. We recommend to:

   - Update Windows® to the latest version. See *Update Windows® on page 29*

   - Create a standard user account. See *Create a user account on page 24*

4. *Configure AXIS Camera Station*

5. Register you AXIS Camera Station licenses.

   - *License a system with Internet connection on page 22*

   - *License a system without Internet connection on page 22*

6. Connect your system to the AXIS Camera Station mobile viewing app. See *Configure AXIS Secure Remote Access*
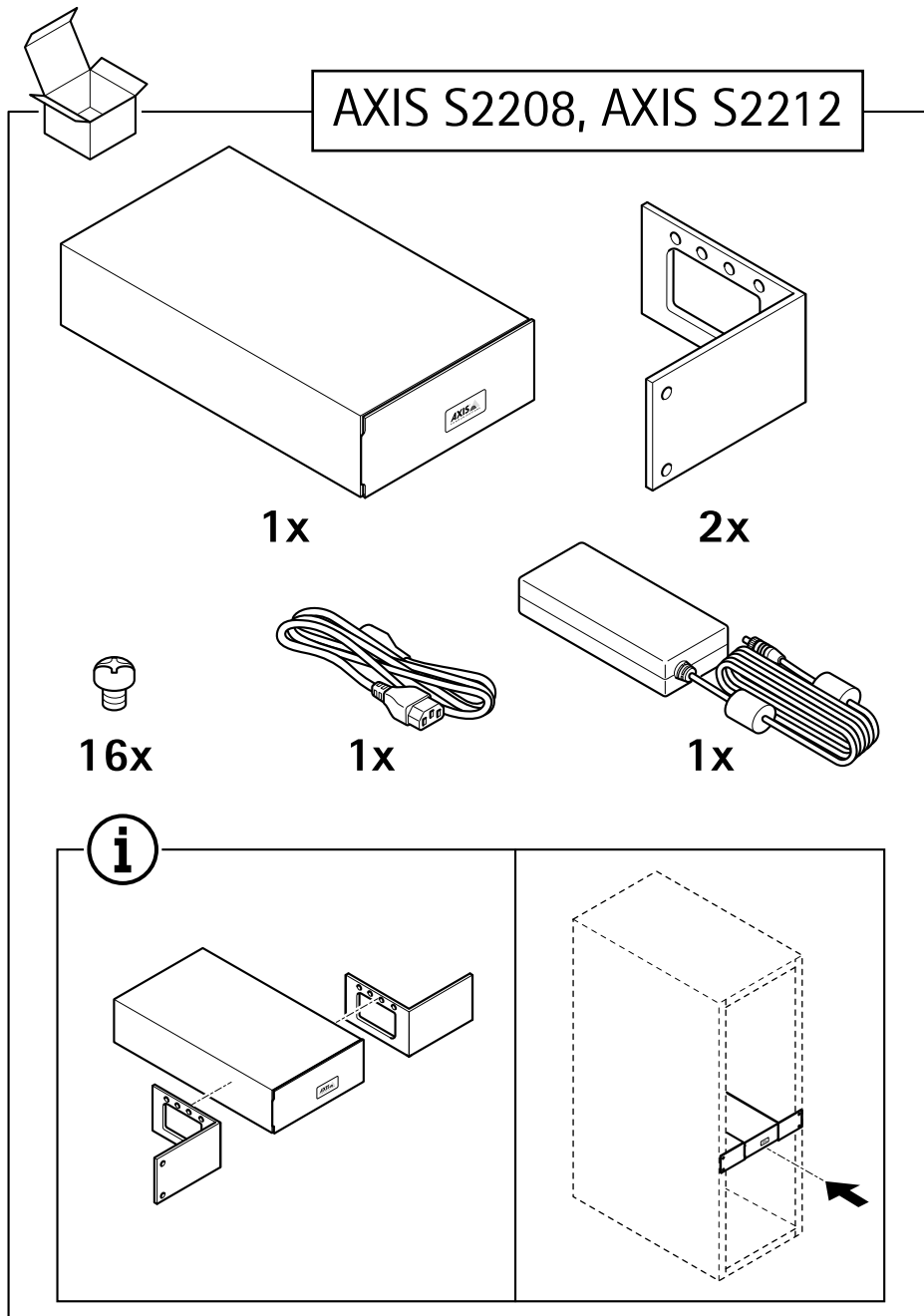
Install your device

AXIS S2216, AXIS S2224

1x

2x

2x   2x   1x

Install your device

AXIS S2208, AXIS S2212

1x

2x

16x

1x

1x

Install your device

Install your device

1.1

2x

2.1

1.2

PH3
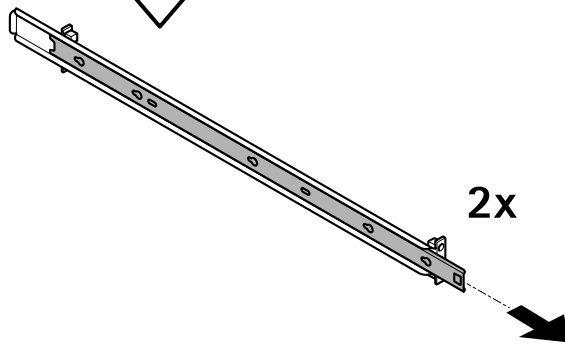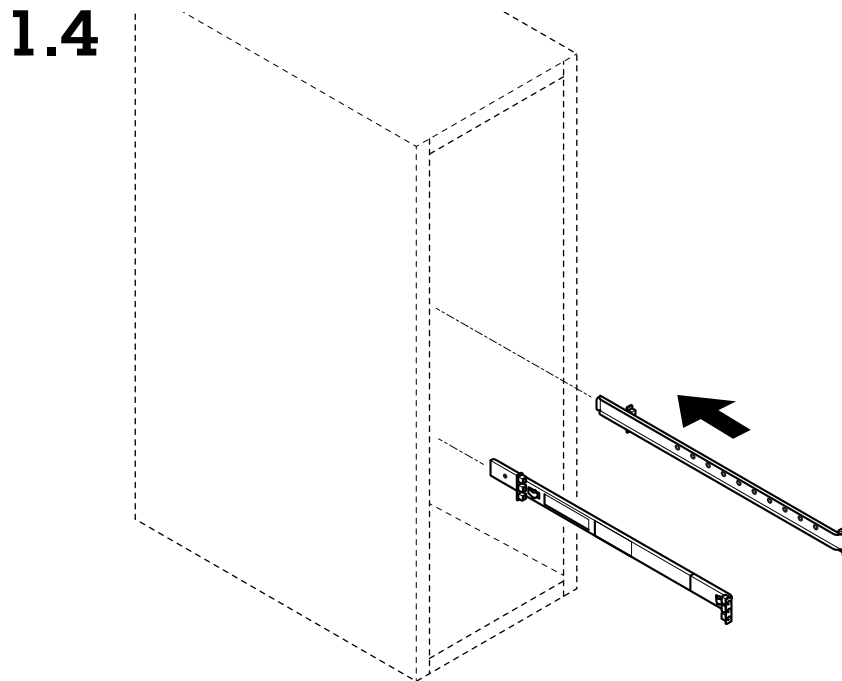
1.3

1.4

1.5

1.6

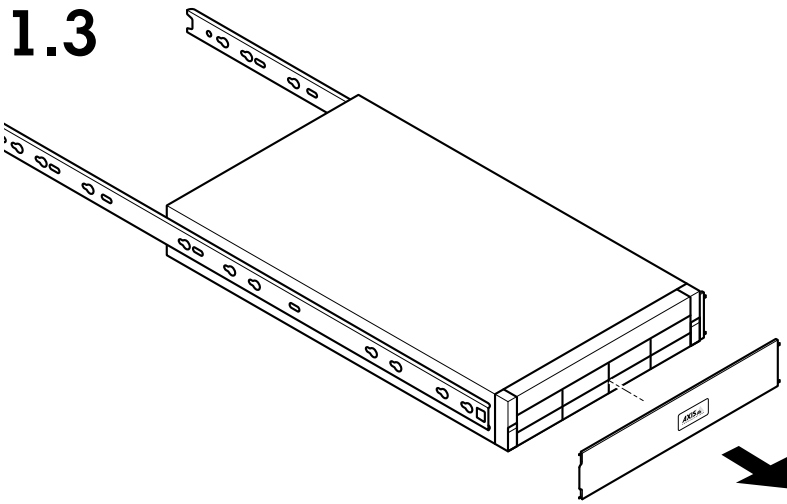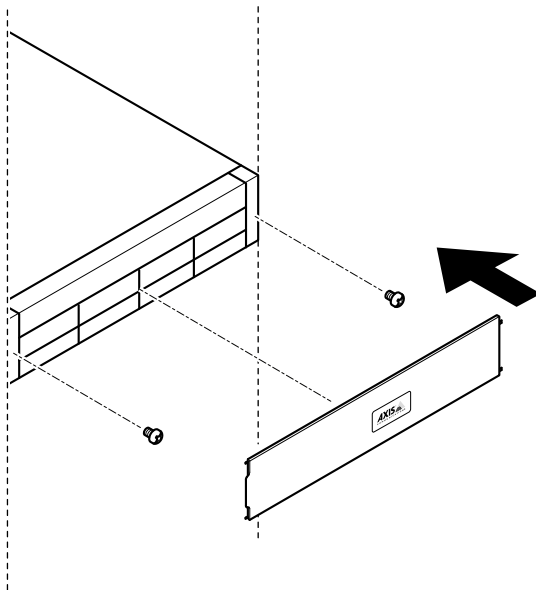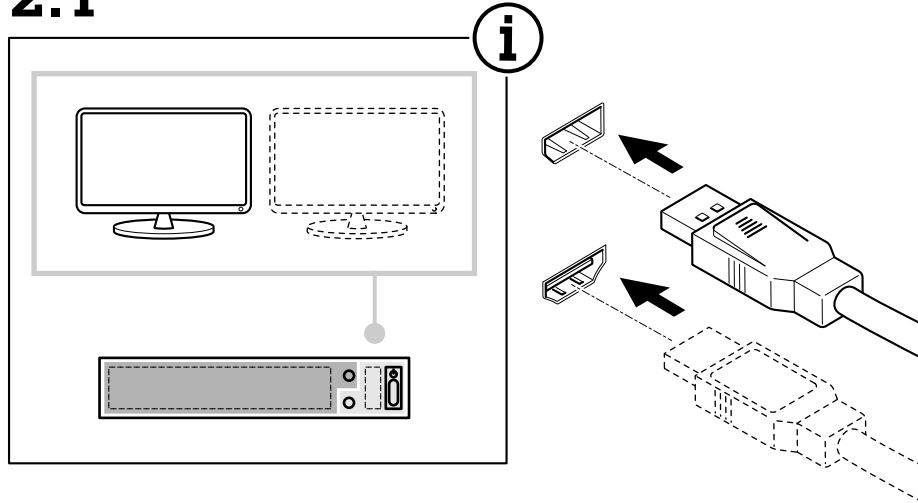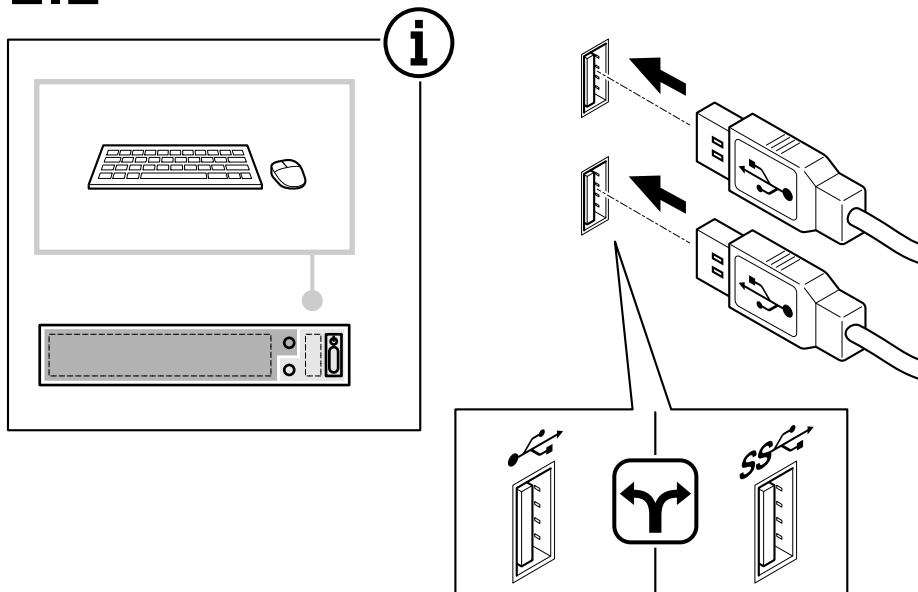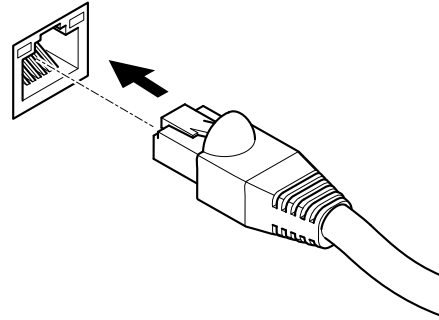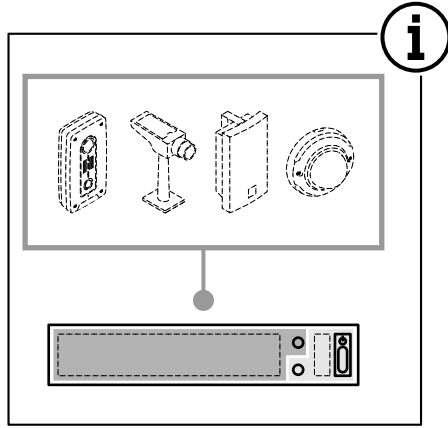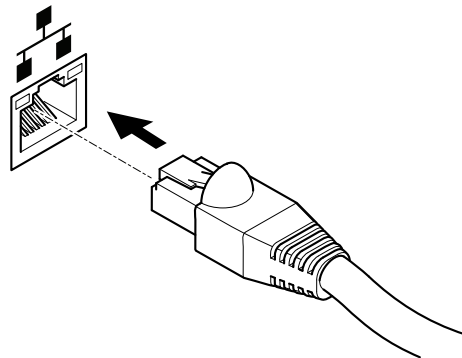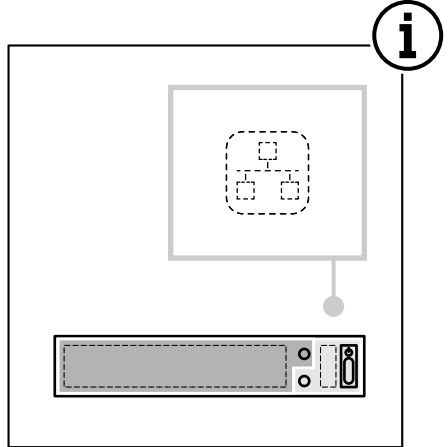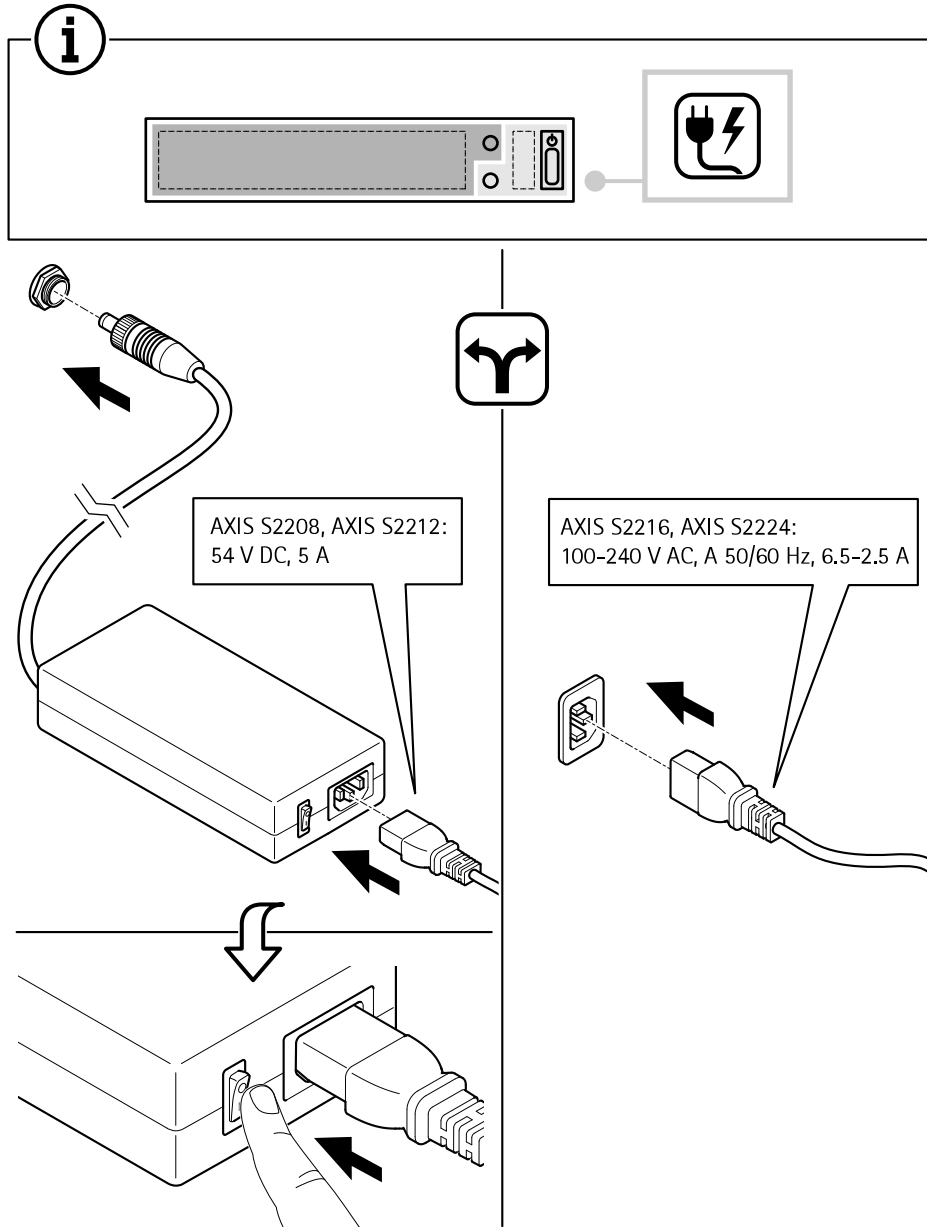# AXIS Camera Station S22 Appliance Series

Install your device

2.1

2.2

2.3

2.4

2.5

AXIS S2208, AXIS S2212:
54 V DC, 5 A

AXIS S2216, AXIS S2224:
100–240 V AC, A 50/60 Hz, 6.5–2.5 A

2.6

2.7
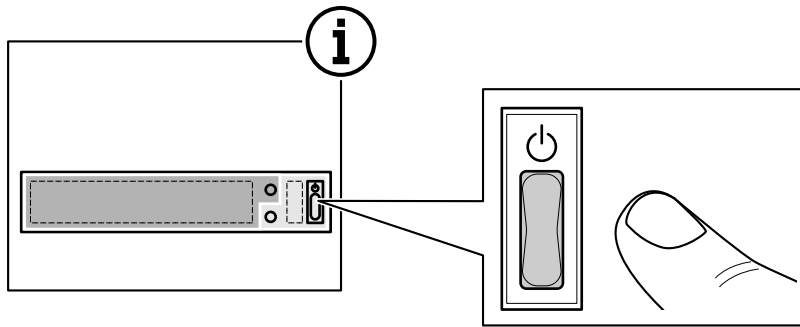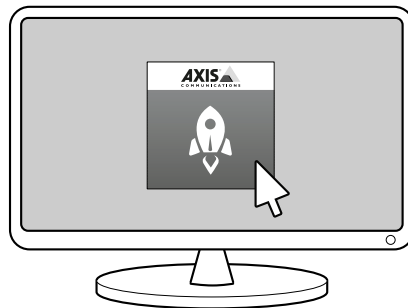
Configure your device

Log on to AXIS Camera Station server

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

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

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

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

- Select **Log on as current user** to log on as the current Windows user.

- Clear **Log on as current user** and click **Log on**. Select **Other user** and provide another username and password to log on with a different username and password.

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

To connect to a remote server:

1. Select **Remote server**.

2. Select a server from the **Remote server** drop-down list or enter the IP or DNS address in the field. If the server is not

   listed, click to reload all the available remote servers.
   If the server is configured to accept clients on a different port than the default port number 55752, enter the IP address followed by the port number, for example, 192.168.0.5:46001

3. You can:

   - Select **Log on as current user** to log on as the current Windows user.

   - Clear **Log on as current user** and click **Log on**. Select **Other user** and provide another username and password to log on with a different username and password.

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

To sign in to AXIS Secure Remote Access:

1. Click the **Sign in to AXIS Secure Remote Access** link.

2. Enter your MyAxis account credentials.

3. Click **Sign in** and **Grant** to grant access.

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

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

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

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

Configure AXIS Camera Station

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

Before you start, you may need to:

- Configure your network depending on your installation. See *Network configuration*.

- Configure your server ports if needed. See *Server port configuration*.

- Consider security issues. See *Security considerations*.

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

1. *Start AXIS Camera Station*

2. *Add devices*

3. *Configure recording method on page 18*

4. *Live view cameras on page 19*

5. *Replay recordings on page 19*

6. *Add bookmarks on page 19*

7. *Export recordings on page 19*

8. *Play and verify recordings in AXIS File Player on page 20*

Start AXIS Camera Station

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

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

1. Select the cameras to add from the list.
   If your camera is not listed, click **Find by address**, enter the camera address and click **OK**.

2. Click **Add**.

3. Select **Quick configuration** or **Site Designer configuration**. Click **Next**.

4. Use the default settings and ensure the recording method is set to None. Click **Install**.

Configure recording method

1. Go to **Configuration > Recording and events > Recording method**.

2. If you want to enable motion detection recording:

   2.1 Select a camera.

   2.2 Turn on **Motion detection**.

   2.3 Click **Apply**.

3. If you want to enable continuous recording:

   3.1 Select a camera.

   3.2 Turn on **Continuous**.

   3.3 Click **Apply**.

Live view cameras

1. Click the Live view tab to navigate to the camera live view.

2. Click a camera to navigate to the live view of that camera.
   A blue dot after the camera name shows that continuous recording is in progress. A red dot after the camera name shows that motion detection recording is in progress.

3. Click ⊕ to navigate from Live view to Recordings.
   A red line in the timeline shows that motion detection recording has been taken for that period. A blue line in the timeline shows that continuous recording is in progress.

Replay recordings

1. Go to the Recording tab.

2. In the timeline of the camera, use the mouse wheel to zoom in and out and drag the timeline to make the marker pointing at your desired position.

3. To start playing the recording from the desired position, click ▶ .

Add bookmarks

1. Go to the Recording tab.

2. In the timeline of the camera, use the mouse wheel to zoom in and out and drag the timeline to make the marker pointing at your desired position.

3. Click 🔖 .

4. Enter the bookmark name and description. Use keywords in the description to make the bookmark easy to find and recognized.

5. Select **Prevent recording deletion** to lock the recording. A locked recording cannot be deleted unless actively unlocked.

6. Click **OK**. A bookmark icon is displayed at your desired position in the timeline.

Export recordings

1. Go to the Recording tab.

2. In the timeline of the camera, use the mouse wheel to zoom in and out.

3. Click ⚑ to display the selection markers.

4. Drag the markers to include the recordings that you want to export.

5. Click ↗ to open the Export tab.

6. In the Export tab, you can do the following if desired.

19

- Click to add a note for the recording.

- Click **Browse** to select the location to export the recordings.

- Select **Include Axis File Player**, **Include notes**, and **Add digital signature**.

7. Click **Export**.

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

Play and verify recordings in AXIS File Player

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

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

2. Double-click AXIS File Player. The exported recordings will be automatically played.

3. Click ■ to show the notes added to the recordings.

4. To verify the digital signature:

    4.1 Go to **Tools > Verify digital signature**.

    4.2 Select **Validate with password** and enter your password.

    4.3 Click **Verify**. The verification result page is displayed.

Network configuration

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

Client proxy settings

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

1. Double-click the AXIS Camera Station Client icon.

2. On the Log on page, click **Change client proxy settings**.

3. Change the client proxy settings.

4. Click **OK**.

Server proxy settings

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

1. Double-click the AXIS Service Control icon in Windows notification area.

2. Select **Modify settings**.

3. In the Proxy settings section, use the default **System account internet option** or select **Use manual proxy settings**.

4. Click **Save**.

NAT and Firewall

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

Server port configuration

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

Security considerations

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

• Use strong passwords for all network devices (cameras, video encoders and auxiliary devices).

- Install AXIS Camera Station Server, cameras, video encoders, and auxiliary devices on a secure network separated from the office network. AXIS Camera Station Client can be installed on a computer on another network, for example a network with Internet access.

- Ensure all users have strong passwords. Using Windows Active Directory a high level of security can be implemented.

License a system with Internet connection

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

1. In the AXIS Camera Station client, go to **Configuration > Licenses > Management** and click **Go to AXIS Camera Station License Portal**.

2. In the AXIS Camera Station license portal, sign in with your MyAxis account.

3. Enter your license key, and click **Add licenses**.

Note

For AXIS Network Video Recorders, your license details are generated automatically and can be found under the License keys section. We recommend that you write them down, or save them in a digital format on a USB flash drive for future reference. Lost license keys cannot be retrieved.

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

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

www.axis.com/products/online-manual/

AXIS Camera Station online license registration

License a system without Internet connection

To license a system without Internet connection:

1. In the AXIS Camera Station client, export the system file.

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

   1.2 Click **Export system file**.

   1.3 Save your system file on a USB flash drive.

2. Go to the AXIS Camera Station license portal *www.axis.com/licenses*, sign in with your MyAxis account and upload your system file.

3. Enter your license key, and click **Add licenses**.

Configure your device

> **Note**
>
> For AXIS Network Video Recorders, your license details are generated automatically and can be found under the License keys section. We recommend that you write them down, or save them in a digital format on a USB flash drive for future reference. Lost license keys cannot be retrieved.

4. Click **Download license file** and save the file to a USB flash drive.

5. In the AXIS Camera Station client, import the license file.

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

    5.2 Click **Import license file**, and select the license file on your USB flash drive.

    5.3 Check that your license keys are shown in **Configuration > Licenses > Keys**.

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

www.axis.com/products/online-manual/

AXIS Camera Station offline license registration

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 using a USB flash drive. Then, if you forget your password, you can reset the password. Without a USB reset disk, you can't reset the password.

If you're using Windows 10, version 1803 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, got 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 a USB flash drive into your device.

3. If there's any data on the USB flash drive, back it up.

4. From the Windows® search field, go to **Create a password reset disk**.

5. In the Forgotten Password wizard, click **Next**.

6. Select your USB flash drive and click **Next**.

7. Type your current password and click **Next**.

8. Follow the onscreen instructions.

9. Remove the USB flash drive and keep it in a safe place where you'll remember it. 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

Configure user permissions

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

Note

- When connecting to multiple AXIS Camera Station servers, you can add and manage user permissions on any connected server by selecting the server from the **Selected server** drop-down list.
- Administrators of the computer on which the AXIS Camera Station server is installed are automatically given administrator privileges to AXIS Camera Station. You cannot change or remove the administrators group's privileges.

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

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

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

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

The list consists of the following information:

Item	Description
Name	Username as it appears in the local computer or Active Directory.
Type	Indicates the entry is a group or a single user.
Details	Detailed user information as it appears in the local computer or Active Directory.
Domain	Domain name where the user is registered.
Role	The access role given to the user or group. Possible values: - **Administrator:** Full access to all functionality and all cameras and devices. - **Operator:** Full access to all functionality except Configuration tab, Device management page, and Audit log. Full access to cameras and I/O ports. Access to playback and recording export can be restricted. - **Viewer:** Access to live video from cameras and access to I/O ports.

To add a user or group, see *Add users or groups*.

To change user access rights for a user or group, select the user or group and click **Edit**. You can edit multiple users or groups at the same time when they have the same role as Operator or Viewer.

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

Add users or groups

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

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

To add a user or a group in AXIS Camera Station:

1. Go to **Configuration > Security > User permissions** and click **Add**.

2. Select **Server** to search for users or groups on the local computer, or select **Domain** to search for Active Directory users or groups.

3. Select **Users** or **Groups** to search for only users or groups.

4. The list of users or groups is displayed. Users and groups that have already been added to AXIS Camera Station are not listed.

   - If there are too many users or groups, the search result is not displayed. Use the **Type to search** field to refine the search and find a specific user or group.

   - If the domain user search fails, the Service logon account must be changed.

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

6. Set the users or groups role to **Administrator**, **Operator**, or **Viewer**.

7. If you have selected the **Operator** or **Viewer** role, select the cameras, I/Os, or views to grant access to. Click **Advanced** to view all options for cameras and I/Os. See *User or group privileges*.

8. If you have selected **Operator** role, click **Playback** to restrict playback or recording export access. See *User or group privileges*.

9. Click **OK**.

User or group privileges

Users and groups with the Administrator role have full access to the entire system.

For users and groups with the Operator or Viewer role, you can grant different access privileges to the specific cameras, I/O ports, views, playback of recordings, and snapshots. For how to define access privileges for a user or group, see *Add users or groups*.

Cameras

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

- In the default **Simple** mode:

   - **Access:** Allow access to the camera and all camera features.

- In the **Advanced** mode:

   - **Access:** Allow access to the camera and all camera features.

   - **Video:** Allow access to live video from the camera.

   - **Audio:** Allow access to audio from the camera.

   - **Mechanical PTZ:** Allow access to mechanical PTZ controls.

   - **Manual Recording:** Allow to start and stop recordings manually.

I/O

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

- In the default **Simple** mode:

  - **Access:** Allow full access to the I/O port.

- In the **Advanced** mode:

  - **Access:** Allow full access to the I/O port.

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

  - **Write:** Allow to change the state of the I/O port.

Views

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

- **Access:** Allow access to the views in AXIS Camera Station.

- **Edit:** Allow to edit the views in AXIS Camera Station.

Playback

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

- **Export recordings:** Allow exporting recordings.

- **Generate incident report:** Allow generating incident reports.

- **Prevent access to recordings older than:** Prevent accessing recordings older than the specified number of minutes. When using search, the user will not find recordings older than the specified time. Recordings and bookmarks older than the specified time cannot be played.

Snapshots

The following access privilege is available for users or groups with the Operator or Viewer role.

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

Manage your device

Update Windows®

Windows® 10 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 > Update & Security > Windows Update**.

2. Click **Check for updates**.

Configure Windows update settings

Sometimes you might want to change how and when Windows® updates.

Note

All ongoing recordings stop during a scheduled system restart.

1. Open the Run app.

   - Go to **Windows System > Run**, or

   - press WIN and R.

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 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**.

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.

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

www.axis.com/products/online-manual/

Reset your server to factory default settings

Reset your switch

You can reset your switch to factory default settings by using one of the following ways:

*   The switch reset button. Before you start, ensure that the switch is on. Press and hold the switch reset button for about 5 seconds until the power button LED at the rear side of the device turns blue. It will take about 6 minutes.

*   The switch's management page. See *Reset to factory default settings on page 38*.

Manage the built-in switch

About the built-in switch

The AXIS Camera Station S22 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 ports and U1 network connections) are not shared with other networks.

The switch's power management follow these rules:

- Each port can reserve power according to the connected powered device's PoE class. Power can also be allocated manually.

- 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 switch's management page.

   - From the web browser, enter the switch's IP address. By default: 192.168.0.1

   - From AXIS Recorder Toolbox, go to **Switch > Open the switch configuration**.

   - From AXIS Camera Station Client, go to **Configuration > Switch > Management**. See *Configure switch*.

2. Log in with your credentials.

   - user name: `admin`

   - password: you can find the randomly generated password on a sticker underneath the product or a self-adhesive sticker in the box content.

To log out the switch's management page, go to ☰ > **Log out**.

Overview

In the switch's management page, click **Overview**.

General information

Category	Item	Description
Ports summary	Active ports	The number of ports that are in use.
	Ports using PoE	The number of ports with PoE enabled that are in use.
	Locked ports	The number of ports that are locked.
Current PoE usage		The total power in watts and percentage consumed by the PoE devices.
Port status		Click the port to see the details about the port.
	Active	The port is in use.
	Inactive	The port is ready to be used.
	Blocked	The port is blocked.

Manage the built-in switch

Port list

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.
PoE	Displays the PoE status. You can click the icon to turn on or turn off PoE on the port.
Power consumption (W)	The power in watts consumed by the device connected to the port.
Upstream (Mbit/s)	The average data rate in megabits per second for outbound data on the port.
Downstream (Mbit/s)	The average data rate in megabits per second for inbound data on the port.
MAC address	The MAC address of the device connected to the port.
Lock	Displays whether the port is locked. You can click the icon to lock or unlock the port.

Turn on and turn off PoE

Turn on PoE on a port

1. In the switch's management page, click **Overview**.

2. In the PoE column, click to turn on PoE on the specific port.

Turn on PoE on all ports

1. In the switch's management page, click **Overview**.

2. Click and select **Turn on PoE on all ports**.

Turn off PoE on a port

1. In the switch's management page, click **Overview**.

2. In the PoE column, click to turn off PoE on the specific port.

Turn off PoE on all ports

1. In the switch's management page, click **Overview**.

2. Click and select **Turn off PoE on all ports**.

Note

> You can also turn on and turn off PoE in the Power management page.

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 port

1. In the switch's management page, click **Overview**.

2. In the Lock column, click to lock the port.

Lock all ports

1. In the switch's management page, click **Overview**.

2. Click ⋮ and select **Lock all ports**.

Unlock a port

1. In the switch's management page, click **Overview**.

2. In the Lock column, click ⬤ to unlock the port.

Unlock all ports

1. In the switch's management page, click **Overview**.

2. Click ⋮ and select **Unlock all ports**.

Power management

In the switch's management page, click **Power management**.

General information

- Ports using PoE: the number of ports with PoE enabled that are in use.

- Current PoE usage: the PoE power in watts consumed by devices and the percentage of used PoE power out of the total dedicated PoE power.

- Power requested: the total power in watts and percentage allocated to devices.

Port list

Item	Description
Port	The port number that the device is connected to.
PoE	Displays 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 port.
Priority	The priority of power allocation of the port.
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 power allocation method LLDP-MED works only for cameras with firmware 9.20 or later.

Manage the built-in switch

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**, go to the Power allocated column and change the power allocated to the connected device.

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.

5. Click **Refresh**.

Example

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

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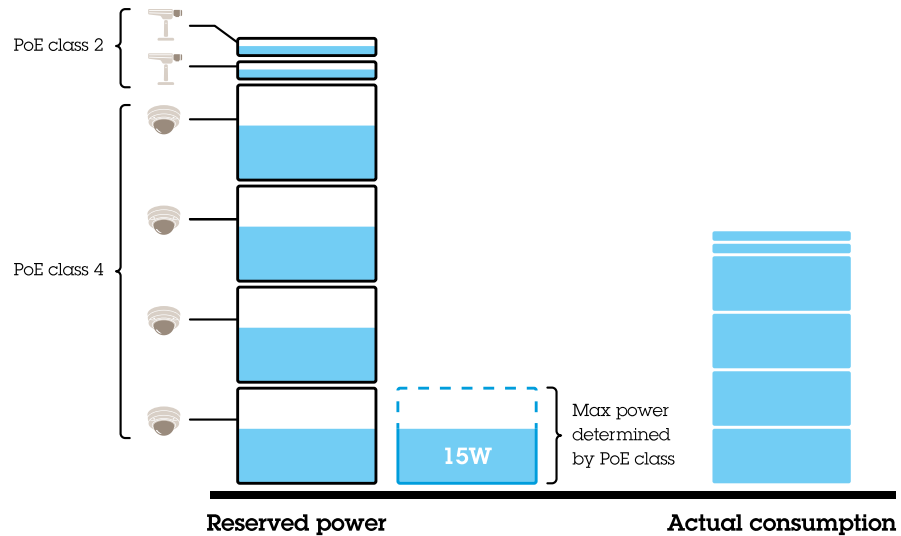
The power requested by each device is determined by the PoE class. The switch can power 4 PoE class 4 devices and 2 PoE class 2 devices. The total power requested is (4 x 30) + (2 x 7) =134 W. The actual power consumed is (4 x 15) + (2 x 5) = 70 W. In this way, all connected devices are guaranteed enough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

Allocate power manually

34

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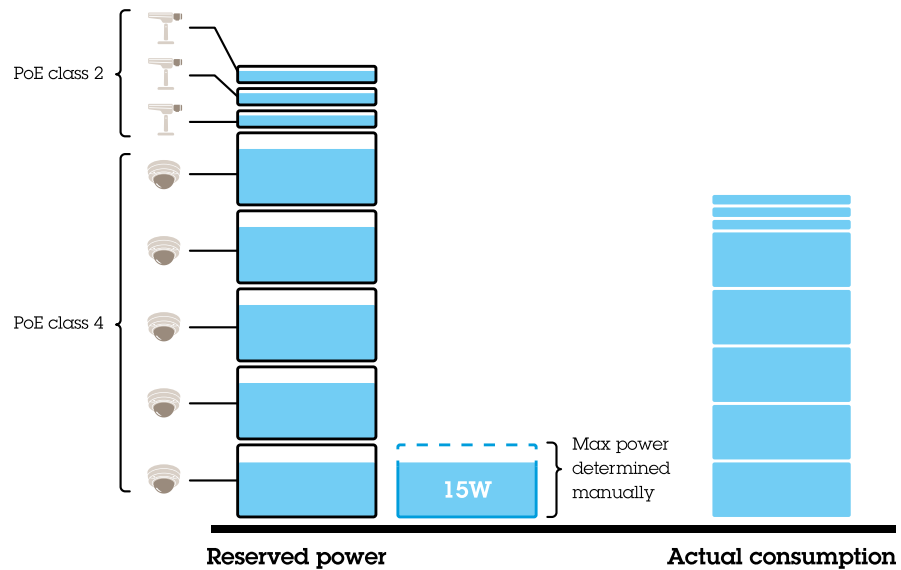
The power requested is manually adjusted to 20 W for PoE class 4 devices. The switch can power 5 PoE class 4 devices and 3 PoE class 2 devices. The total power requested is (5 x 20) + (3 x 7) = 121 W. The actual power consumed is (5 x 15) + (3 x 5) = 90 W. In this way, all connected devices are guaranteed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

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 switch's management page, go to **Settings > Network settings**.

2. Enter the connection type, IP address, subnet mask, gateway, DNS1, DNS2, and hostname.

Note

The factory default settings are: a static IP connection with address 192.168.0.1 and a subnet mask with address 255.255.255.0.

3. Click **Save**.

Configure date and time

1. In the switch's management page, 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

Important

If the switch's DHCP server is enabled and your AXIS Camera Station S22 Appliance is connected to an external network with its own DHCP server, you will have IP address conflicts. This might result in the corporate network not working.

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 being accessed by external application, you must specify the gateway and DNS addresses.

1. In the switch's management page, go to **Settings > DHCP server**.

2. Select **Use DHCP server**.

3. Enter the start IP address, end IP address, subnet mask, gateway, DNS 1, DNS 2, lease length, and domain name.

4. Click **Save**.

Configure SNMP

1. In the switch's management page, 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**.

Configure web settings

1. In the switch's management page, go to **Settings > Web settings**.

2. Enter the port number.

3. For more secure connection, select **Secure connection (HTTPS)** and enter the port number used for HTTPS connection.

4. Click **Save**.

Important

If you have changed the port number, ensure you record the new port number. If you've forgotten the new port number, contact Axis support.

Maintenance

Update firmware

1. In the switch's management page, 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. After the firmware updating is done, reboot the switch.

Manage the built-in switch

Reboot the switch

Important

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

1. In the switch's management page, 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 switch's management page, go to **Maintenance > Backup and restore**.

2. Click **Create a backup file**. The backup file in the .bin format is created in the **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 switch's management page, 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 could take a few minutes to restore the switch from the backup file. Once the settings are restored, the switch will automatically reboot and you need to log in again.

Manage certificates

1. In the switch's management page, 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

Ensure you select a password you remember. If you have forgotten the new password, contact Axis support.

1. In the switch's management page, go to **Maintenance > Change password**.

2. Enter the current password and your new password as required.

3. Click **Save**.

Reset to factory default settings

1. In the switch's management page, go to **Maintenance > Reset to factory default settings**.

2. Click **Reset** and **Yes**.

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

Log

In the switch's management page, click **Log** to see a list of logs. Click **Refresh** to refresh the list. Click the column title to sort in alphabetical order.

Item	Description
Time	The date and time when the log event happened.
Level	The serious level shown as warning icons.
User	The user that initiates the log event.
IP address	The IP address of the user that initiates the log event.
Service	The service that the log event is related to. Possible values are desktop, network, system, ntpd, storage, dhcp, etc.
Event	The description about the log event.

Create switch reports

1. In the switch's management page, click **Log**.
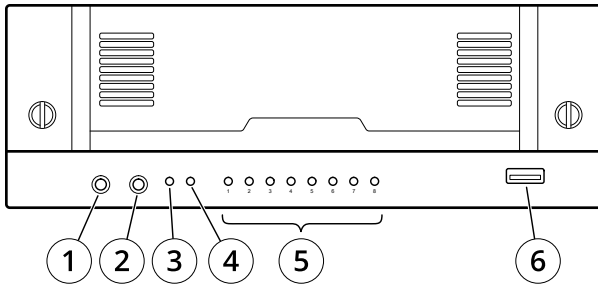
2. Click **Create switch report**.

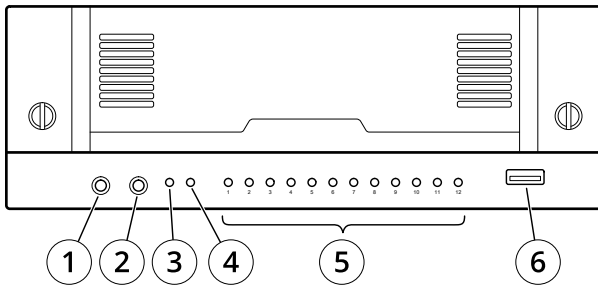# AXIS Camera Station S22 Appliance Series

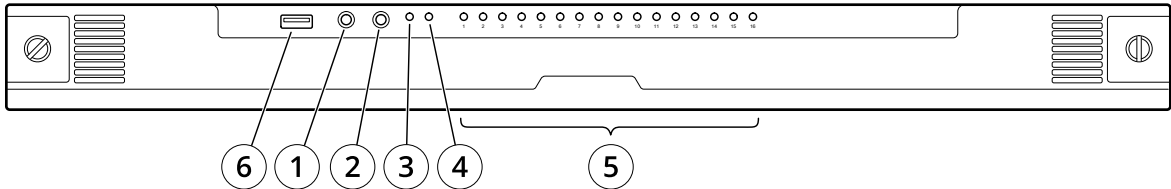## Product overview

Product overview

Front side

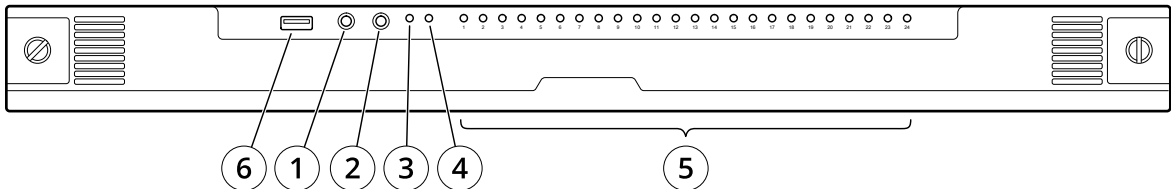**AXIS Camera Station S2208 Appliance**

AXIS Camera Station S2212 Appliance

AXIS Camera Station S2216 Appliance

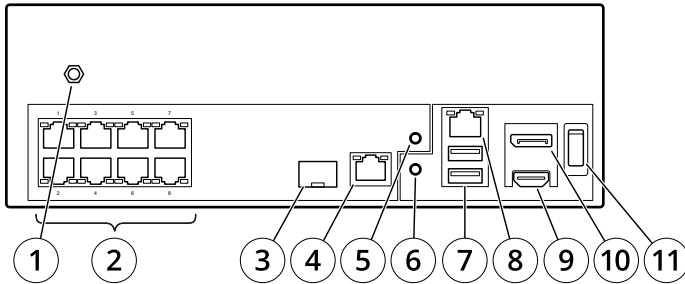**AXIS Camera Station S2224 Appliance**

1   Audio in
2   Audio out
3   System power LED
4   Disk activity LED
5   Status LEDs of PoE ports
6   USB 3.0
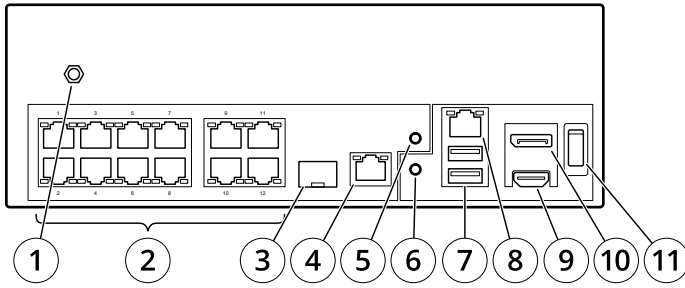
AXIS Camera Station S22 Appliance Series

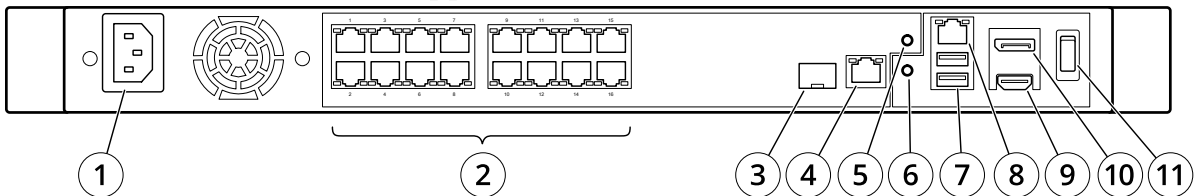## Product overview

Rear side

AXIS Camera Station S2208 Appliance

AXIS Camera Station S2212 Appliance

AXIS Camera Station S2216 Appliance

AXIS Camera Station S2224 Appliance
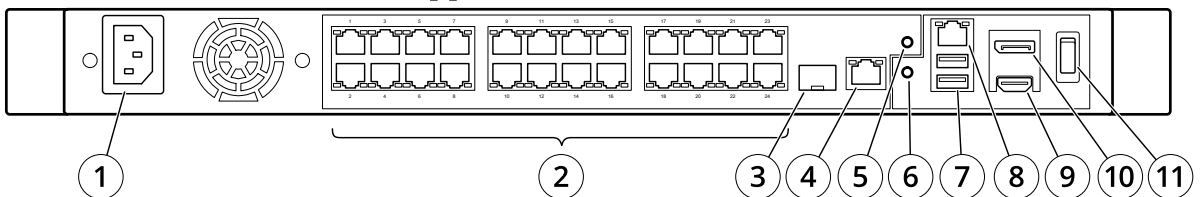
1	Power connector
2	PoE ports
3	Switch uplink, SFP
4	Switch uplink, RJ45
5	Switch reset button
6	Server reset button
7	USB 2.0 x2
8	Server network, RJ45
9	HDMI port
10	Displayport
11	Power button

AXIS Camera Station S22 Appliance Series

Product overview

Specifications

Front LEDs

LED indicator	Color	Indication
Power	Green	Server on
Network ports	Green	Link state
Hard drive	Blinks amber	Hard drive activity
	Blinks 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	Blinks green	Network activity

Power button	Color	Indication
When the power button is not pressed	Off	Switch and server off
	Blue	During switch boot
	Green	Switch boot completed
When the power button is pressed	Red (flashes once for 1s)	Power on
	>5s blinks green	Restarting server
	>10s steady blue	Power off switch
	>15s blinks blue	Power off switch and server

Troubleshooting

If you can't find what you're looking for here, try the troubleshooting section at *axis.com/support*.

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 Recovery Kit, contact AXIS Technical Support and supply the serial number of your device.

1. Download the AXIS Recovery Kit and AXIS ISO to USB Tool.

2. Insert a USB drive into your computer.

   - Use a USB drive with a minimum of 16 GB to 32 GB.

   - The USB drive will be formatted, and all existing data will be erased.

3. Run the AXIS 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 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 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*

- *Configure AXIS Secure Remote Access*

- *What to include in an Antivirus white list for AXIS Camera Station*

Contact support

Contact support at *axis.com/support.*