AXIS S3008 Recorder

User Manual

About your device

AXIS S3008 Recorder is a compact network video recorder with a built-in PoE switch for easy installation. The device features a surveillance-grade hard drive. It also includes a USB port for easy export of video footage. The recorder comes in three models – including a 2 TB, 4 TB or 8 TB hard drive.

How many cameras can I connect to the recorder?

Up to eight devices can be connected to the PoE switch of the recorder.

How much power can the recorder supply to the cameras?

These are the limitations for power over Ethernet (PoE):

- The recorder can supply up to eight devices with PoE.
- The total amount of power available:
  - 2 TB and 4 TB: 65 W
  - 8 TB: 60 W
- Each network port supports up to 15.4 W (PoE Class 3) at the PoE port (PSE) and 12.95 W on the camera side (PD).
- The switch allocates PoE power based on the PoE class of the connected device.

Browser support

Windows®

- Chrome™ (recommended)
- Firefox®
- Edge®

OS X®

- Chrome™ (recommended)
- Safari®

Other

- Chrome™
- Firefox®

To find out more about how to use the device, see the Manual available at *Documentation | Axis Communications*.
If you want more information about recommended browsers, go to *Axis OS browser support | Axis Communications*.

Get started

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

www.axis.com/products/online-manual/63362#t10153931

The AXIS S3008 Recorder is used with version 4 of the AXIS Companion video management software.

Get started with AXIS Companion

Note

Internet access is required during the system setup.

Installation overview:

1. *Register a MyAxis account on page 3*
2. *Install the hardware on page 4*
3. *Install the desktop app on page 4*
4. *Create a site on page 5*
5. *Install the mobile app on page 6*

Result of system installation:

- The **firmware** is upgraded on all Axis devices.
- A **password** is set for the devices.
- The **recordings** are enabled with default settings.
- The **remote access** is enabled.

Register a MyAxis account

Register a **MyAxis** account at *axis.com/my-axis/login*.

You can make your MyAxis account more secure by activating multi-factor authentication (MFA). MFA is a security system that adds another layer of verification to ensure the user's identity.

Activate MFA:

1. Go to *https://auth.axis.com/user-center/account/security-settings*.
2. Turn on **2–Step verification**.

You are redirected to a login page.

3. Log in with your **MyAxis** credentials.

MFA is now active.

Log in when MFA is active:

1. Log in to your **MyAxis** account.

An email is sent to you.

2. Open the email and click **Authenticate**.

If you didn't receive an email, then check if it's in your spam folder. If it's not there, then contact IT support.

Install the hardware

1. Install your camera hardware.
2. Connect the recorder to your network via the LAN port.

Note

If you have no recorder, then you need a camera with an SD card if you want to be able to record video.

3. Connect the cameras to the recorder's integrated PoE switch or an external PoE switch.
4. Connect the computer to the same network as the recorder.
5. Connect the power supply to the recorder.

Important

You must first connect the power cord to the recorder, and then connect the power cord to the power outlet.

6. Wait a few minutes for the recorder and cameras to boot up before proceeding.

⚠CAUTION

Keep the recorder in a well ventilated environment and with plenty of empty space around the recorder to avoid overheating.

Install the desktop app

1. Go to *axis.com/products/axis-companion* and click **Download** to download the AXIS Companion desktop app for Windows.
2. Sign in using your *MyAxis account*.
3. Read the license agreement, and select one of the alternatives to proceed.
4. Save the file to a location of your choice.
5. Open the file, and click **Run** to start the installation.
6. If you want to allow the app to make changes on your device, click **Yes**.
7. Select language and click **OK**.
8. Follow the setup wizard.

Get started

Create a site

With reservations for changes in the user interface.

A site is a single point of entry to a surveillance solution, for example all cameras in a store. You can keep track of several sites through a single MyAxis account.

Note

If you have used an earlier version of AXIS Companion, then you might have devices that are not supported in AXIS Companion version 4. Unsupported devices include third-party NAS devices and old Axis devices with a firmware that can't be updated to 5.50 or later. The wizard will inform you about any such issues and help you to address them.

Note

Sites that were created in an earlier version than AXIS Companion version 4, will not appear in the list of sites. You can read the Migration Guide (available on the support web page) for more information.

1. Start the AXIS Companion desktop app.
2. Sign in with your *MyAxis account*.
3. Click **Get started**.
4. Name your site and enter your company name.
5. Click **Next**.
6. Select the devices you want to add to your site.

   If any devices are password-protected, then you must enter the password for them before they can be selected.

Note

If you have devices that are not supported, then you can click **Read more** to find our why they are not supported.

7. Click **Next**.
8. Enter a password.

   This password is used for accessing the device webpages or offline mode in the AXIS Companion mobile app.
9. Click **Next**.
10. On the **Ready to install** page, there might be a list of cameras that need to be restored. If so, click the **Restore device** link to fix the issue on the device webpage.
11. Click **Finish** and wait while AXIS Companion configures the cameras.

Note

The configuration may take several minutes.

Get started

For getting-started video tutorials, see *AXIS Companion tutorials*.

Install the mobile app

You can use the AXIS Companion mobile app to set up your system and control it from anywhere. Real-time alert notifications keep you aware of any suspicious activity. You can also view and export video recordings.

1. Go to your App store or Google play.
2. Search for **AXIS Companion 4** and download the app.
3. Sign in to AXIS Companion with your *MyAxis account*.

To find out more on how to use the app, see *AXIS Companion tutorials*.

The device interface

The device interface

Show or hide the main menu.

Access the product help.

Change the language.

Set light theme or dark theme.

See information about the user who is logged in.

The context menu contains:

- **Analytics data**: Accept to share non-personal browser data.
- **Feedback**: Share any feedback to help us improve your user experience.
- **Legal**: View information about cookies and licenses.
- **About**: View device information, including firmware version and serial number.

Recorder status

Status

Allocated PoE: Number of watts (W) that are currently allocated.

Total PoE consumption: Number of watts (W) that are consumed.

Keep PoE active during recorder restart: Turn on to supply power to connected devices during a restart of the recorder.

Used space: Percentage of space used.

Free space: Percentage of space available for recordings.

Free space: Available disk space displayed in megabytes (MB), gigabytes (GB), or terabytes (TB).

Disk status: Current status of the disk.

Disk temperature: Current running temperature.

Ports

Each port has an individual number and individual settings.

PoE: Turn on or off PoE for each port. When a device is connected, you'll see the following information:

- **Allocated power**: Number of watts (W) that are currently allocated.
- **Mac**: The media access control address (MAC address) of the connected device.

Apps

Add app: Click to install a new app.

Find more apps: Click to go to an overview page of Axis apps.

The context menu contains:

- **App log**: Click to view a log of the app events. The log is helpful when you contact support.
- **Activate license with a key**: If the app requires a license, you need to activate it. Use this option if your device doesn't have internet access.
  If you don't have a license key, go to *axis.com/applications*. You need a license code and the Axis product serial number to generate a license key.
- **Activate license automatically**: If the app requires a license, you need to activate it. Use this option if your device has internet access. You need a license code to activate the license.
- **Deactivate the license**: Deactivate the license to use it in another device. If you deactivate the license, you also remove it from the device. To deactivate the license requires internet access.
- **Delete**: Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

Note

The device's performance might be affected if you run several apps at the same time.

Start: Start or stop the app.

Open: Click to access the app's settings. The available settings depend on the application. Some applications don't have any settings.

System

Date and time

The time format depends on the web browser's language settings.

Note

We recommend you to synchronize the device's date and time with an NTP server.

Synchronization: Select an option for synchronizing the device's date and time.

- **Automatic date and time (NTP server using DHCP)**: Synchronize with the NTP server connected to the DHCP server.
- **Automatic date and time (manual NTP server)**: Synchronize with NTP servers of your choice.
  - **Primary NTP server** and **Secondary NTP server**: Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
- **Custom date and time**: Manually set the date and time. Click **Get from system** to fetch the date and time settings once from your computer or mobile device.

Time zone: Select which time zone to use. Time will be automatically adjusted for daylight saving time and standard time.

Note

The system uses the date and time settings in all recordings, logs and system settings.

Network

IPv4 and IPv6

IPv4

- **Automatic IP (DHCP) and DNS (DHCP)**: The recommended setting for most networks. The current settings are updated automatically.
- **Automatic IP (DHCP) and manual DNS**: Contact your network administrator to configure the manual settings. The current automatic settings are updated automatically.
- **Manual IP and DNS**: Contact your network administrator to configure the settings.

IP address: Enter a unique IP address for the device. Static IP addresses can be assigned at random within isolated networks, provided that each address is unique. To avoid conflicts, we recommend you to contact your network administrator before you assign a static IP address.

Subnet mask: Enter the subnet mask.

Router: Enter the IP address of the default router (gateway) used to connect devices that are attached to different networks and network segments.

Hostname: Enter the hostname.

Search domains: When you use a hostname that is not fully qualified, click **Add search domain** and enter a domain in which to search for the hostname used by the device.

DNS servers: Click **Add DNS server** and enter the IP address of the primary DNS server. This provides the translation of hostnames to IP addresses on your network.

IPv6

Assign IPv6 automatically: Select to let the network router assign an IP address to the device automatically.

Friendly name

Bonjour®: Turn on to allow automatic discovery on the network.

Bonjour name: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

Use UPnP®: Turn on to allow automatic discovery on the network.

UPnP name: Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

One-click cloud connection

One-click cloud connection (O3C) together with an O3C service provides easy and secure internet access to live and recorded video from any location. For more information, see *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C:

- **One-click**: The default setting. Press and hold the control button on the device to connect to an O3C service over the internet. You need to register the device with the O3C service within 24 hours after you press the control button. Otherwise, the device disconnects from the O3C service. Once you have registered the device, **Always** is enabled and the device stays connected to the O3C service.
- **Always**: The device constantly attempts to connect to an O3C service over the internet. Once you have registered the device, it stays connected to the O3C service. Use this option if the control button on the device is out of reach.
- **No**: Disables the O3C service.

Proxy settings: If needed, enter the proxy settings to connect to the HTTP server.

Host: Enter the proxy server's address.

Port: Enter the port number used for access.

Login and **Password**: If needed, enter username and password for the proxy server.

Authentication method:

- **Basic**: This method is the most compatible authentication scheme for HTTP. It's less secure than the **Digest** method because it sends the username and password unencrypted to the server.
- **Digest**: This method is more secure because it always transfers the password encrypted across the network.
- **Auto**: This option lets the device select the authentication method depending on the supported methods. It prioritizes the **Digest** method over the **Basic** method.

Owner authentication key (OAK): Click **Get key** to fetch the owner authentication key. This is only possible if the device is connected to the internet without a firewall or proxy.

Connected clients

The list shows all clients that are connected to the device.

Update: Click to refresh the list.

Security

Certificates

Certificates are used to authenticate devices on a network. The device supports two types of certificates:

- **Client/server certificates**
  A client/server certificate validates the device's identity, and can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.
- **CA certificates**
  You can use a CA certificate to authenticate a peer certificate, for example to validate the identity of an authentication server when the device connects to a network protected by IEEE 802.1X. The device has several pre-installed CA certificates.

These formats are supported:

- Certificate formats: .PEM, .CER, and .PFX
- Private key formats: PKCS#1 and PKCS#12

Important

If you reset the device to factory default, all certificates are deleted. Any pre-installed CA certificates are reinstalled.


Filter the certificates in the list.


Add certificate : Click to add a certificate.

The context menu contains:

- **Certificate information**: View an installed certificate's properties.
- **Delete certificate**: Delete the certificate.
- **Create certificate signing request**: Create a certificate signing request to send to a registration authority to apply for a digital identity certificate.

IEEE 802.1x

IEEE 802.1x is an IEEE standard for port-based network admission control providing secure authentication of wired and wireless network devices. IEEE 802.1x is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1x, network devices must authenticate themselves. The authentication is performed by an authentication server, typically a RADIUS server (for example FreeRADIUS and Microsoft Internet Authentication Server).

Certificates

When configured without a CA certificate, server certificate validation is disabled and the device tries to authenticate itself regardless of what network it is connected to.

When using a certificate, in Axis' implementation, the device and the authentication server authenticate themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

To allow the device to access a network protected through certificates, a signed client certificate must be installed on the device.

Client certificate: Select a client certificate to use IEEE 802.1x. The authentication server uses the certificate to validate the client's identity.

CA certificate: Select a CA certificate to validate the authentication server's identity. When no certificate is selected, the device tries to authenticate itself regardless of what network it is connected to.

EAP identity: Enter the user identity associated with the client certificate.

EAPOL version: Select the EAPOL version that is used in the network switch.

Use IEEE 802.1x: Select to use the IEEE 802.1x protocol.

Custom-signed firmware certificate

To install test firmware or other custom firmware from Axis on the device, you need a custom-signed firmware certificate. The certificate verifies that the firmware is approved by both the device owner and Axis. The firmware can only run on a specific device which is identified by its unique serial number and chip ID. Custom-signed firmware certificates can only be created by Axis, since Axis holds the key to sign them.

Click **Install** to install the certificate. You need to install the certificate before you install the firmware.

Users

Add user: Click to add a new user. You can add up to 100 users.

Username: Enter a unique username.

New password: Enter a password for the user. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example letters, numbers, punctuation, and some symbols.

Repeat password: Enter the same password again.

Role:

- **Administrator**: Has full access to all settings. Administrators can also add, update, and remove other users.
- **Operator**: Has access to all settings except:
  - All **System** settings.
  - Adding apps.
- **Viewer**: Has access to:
  - Watch and take snapshots of a video stream.
  - Watch and export recordings.
  - With PTZ user access: pan, tilt, and zoom.

The context menu contains:

Update user: Edit the user's properties.

Delete user: Delete the user. You can't delete the root user.

Anonymous users

Allow anonymous viewers: Turn on to allow anyone to access the device as a viewer without having to log in with a user account.

Allow anonymous PTZ operators: Turn on to allow anonymous users to pan, tilt, and zoom the image.

Storage

Onboard storage

Hard drive

- **Free**: The amount of free disk space.
- **Status**: If the disk is mounted or not.
- **File system**: The file system that is used by the disk.
- **Encrypted**: If the disk is encrypted or not.
- **Temperature**: The current temperature of the hardware.
- **Overall heath test**: The result after checking the health of the disk.

Tools

- **Check**: Check the storage device for errors and tries to repair it automatically.
- **Repair**: Repair the storage device. Active recordings will pause during the repair. Repairing a storage device may result in lost data.
- **Format**: Erase all recordings and format the storage device. Choose a file system.
- **Encrypt**: Encrypt data that is stored.
- **Decrypt**: Decrypt data that is stored. All files on the storage device will be erased.
- **Change password**: Change the password for the disk encryption. Changing the password doesn't disrupt ongoing recordings.
- **Use tool**: Click to run the selected tool

Unmount: Click before you disconnect the device from the system. All ongoing recordings will be stopped.

Write protect: Turn on write protection to protect the storage device from being overwritten.

Auto format: The disk will be automatically formatted using the ext4 file system.

Logs

Reports and logs

Reports

- **View the device server report**: Click to show information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.
- **Download the device server report**: Click to download the server report. It creates a .zip file that contains a complete server report text file in UTF–8 format, as well as a snapshot of the current live view image. Always include the server report .zip file when you contact support.
- **Download the crash report**: Click to download an archive with detailed information about the server's status. The crash report contains information that is in the server report as well as detailed debug information. This report might contain sensitive information such as network traces. It can take several minutes to generate the report.

Logs

- **View the system log**: Click to show information about system events such as device startup, warnings and critical messages.
- **View the access log**: Click to show all failed attempts to access the device, for example when a wrong login password is used.

Network trace

Important

A network trace file might contain sensitive information, for example certificates or passwords.

A network trace file can help you troubleshoot problems by recording activity on the network. Select the duration of the trace in seconds or minutes, and click **Download**.

Remote system log

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, which indicates the software type generating the message, and assigned a severity level.

+ **Server**: Click to add a new server.

Host: Enter the hostname or IP address of the server.

Format: Select which syslog message format to use.

- RFC 3164
- RFC 5424

Protocol: Select the protocol and port to use:

- UDP (Default port is 514)
- TCP (Default port is 601)
- TLS (Default port is 6514)

Severity: Select which messages to send when triggered.

CA certificate set: See the current settings or add a certificate.

SSH server

Secure Shell (SSH): Turn on to allow a user to securely log on and perform shell and network services over the network.

Maintenance

Restart: Restart the device. This does not affect any of the current settings. Running applications restart automatically.

Restore: Return *most* settings to the factory default values. Afterwards you must reconfigure the device and apps, reinstall any apps that didn't come preinstalled, and recreate any events and PTZ presets.

Important

The only settings saved after restore are:

- Boot protocol (DHCP or static)
- Static IP address
- Default router
- Subnet mask
- 802.1X settings
- O3C settings

Factory default: Return *all* settings to the factory default values. Afterwards you must reset the IP address to make the device accessible.

Note

All Axis device firmware is digitally signed to ensure that you only install verified firmware on your device. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper "Signed firmware, secure boot, and security of private keys" at *axis.com*.

Firmware upgrade: Upgrade to a new firmware version. New firmware releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest release. To download the latest release, go to *axis.com/support*.

When you upgrade, you can choose between three options:

- **Standard upgrade**: Upgrade to the new firmware version.
- **Factory default**: Upgrade and return all settings to the factory default values. When you choose this option, you can't revert to the previous firmware version after the upgrade.
- **Autorollback**: Upgrade and confirm the upgrade within the set time. If you don't confirm, the device reverts to the previous firmware version.

Firmware rollback: Revert to the previously installed firmware version.

Additional settings

Allocate power

The recorder reserves a certain amount of power for each port. The total reserved power cannot exceed the total power budget. A port will not be powered up if the recorder tries to reserve more power than what is available. This makes sure that all of the connected devices will be powered.

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

- **PoE class** – Each port automatically determines the amount of power to reserve according to the PoE class of the connected device.
- **LLDP** – Each port determines the amount of power to reserve by exchanging PoE information using the LLDP protocol.

Note

Power allocation with LLDP only works for supported devices with firmware 9.80 or later, and for AXIS S3008 Recorder with firmware 10.2 or later.

LLDP is always active in AXIS S3008 Recorder but must be activated on the connected device. If LLDP is turned off or not supported in the connected device, then PoE class reservation will be used instead.

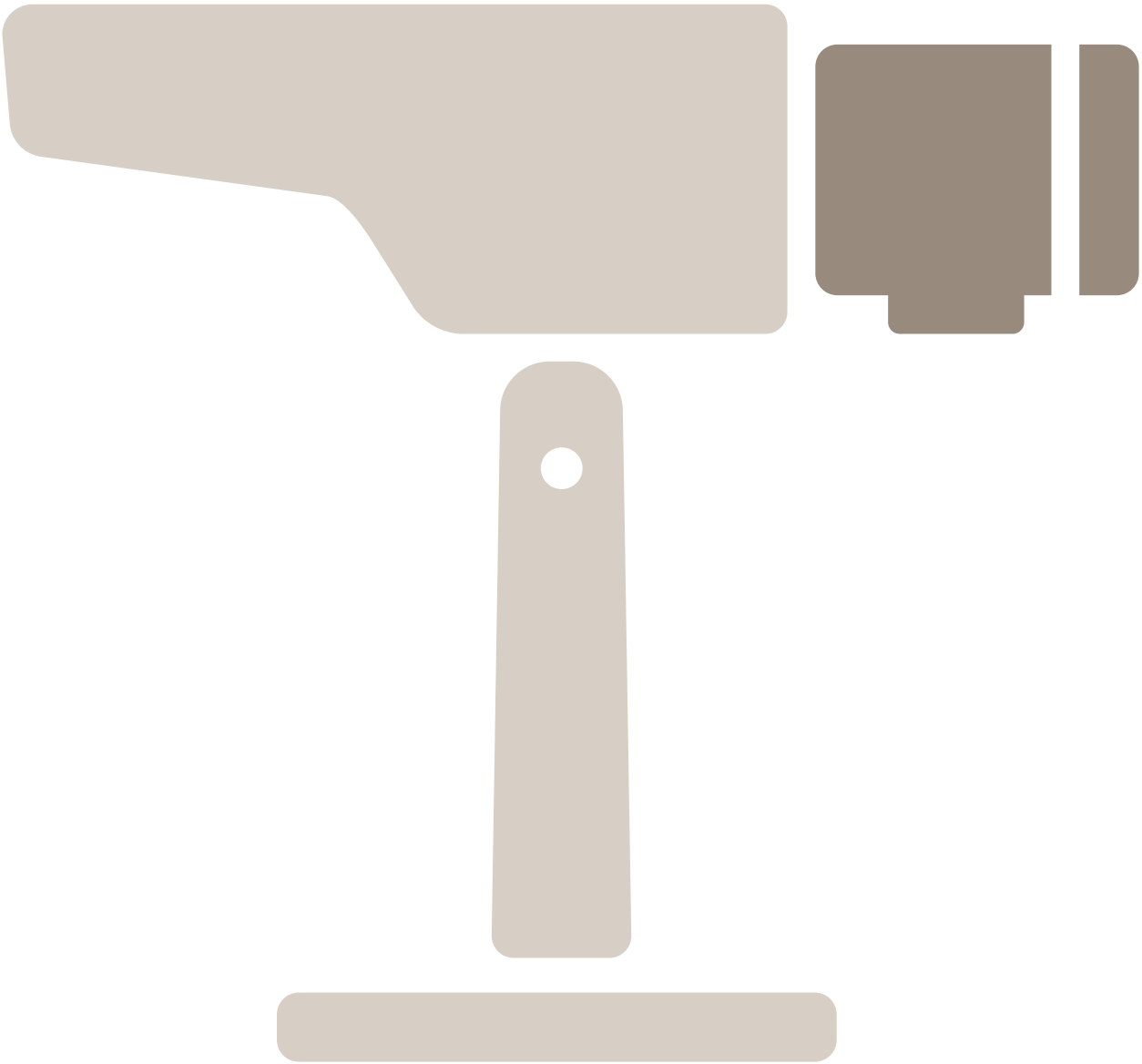
To turn on LLDP on your PoE device:

1. Open the device webpage.
2. Go to **Settings** > **System** > **Plain config** > **Network**.
3. Under **LLDP POE**, select the **LLDP Send Max PoE** checkbox.

Example

In this example, the AXIS S3008 Recorder has a total power budget of 65 W.

Additional settings

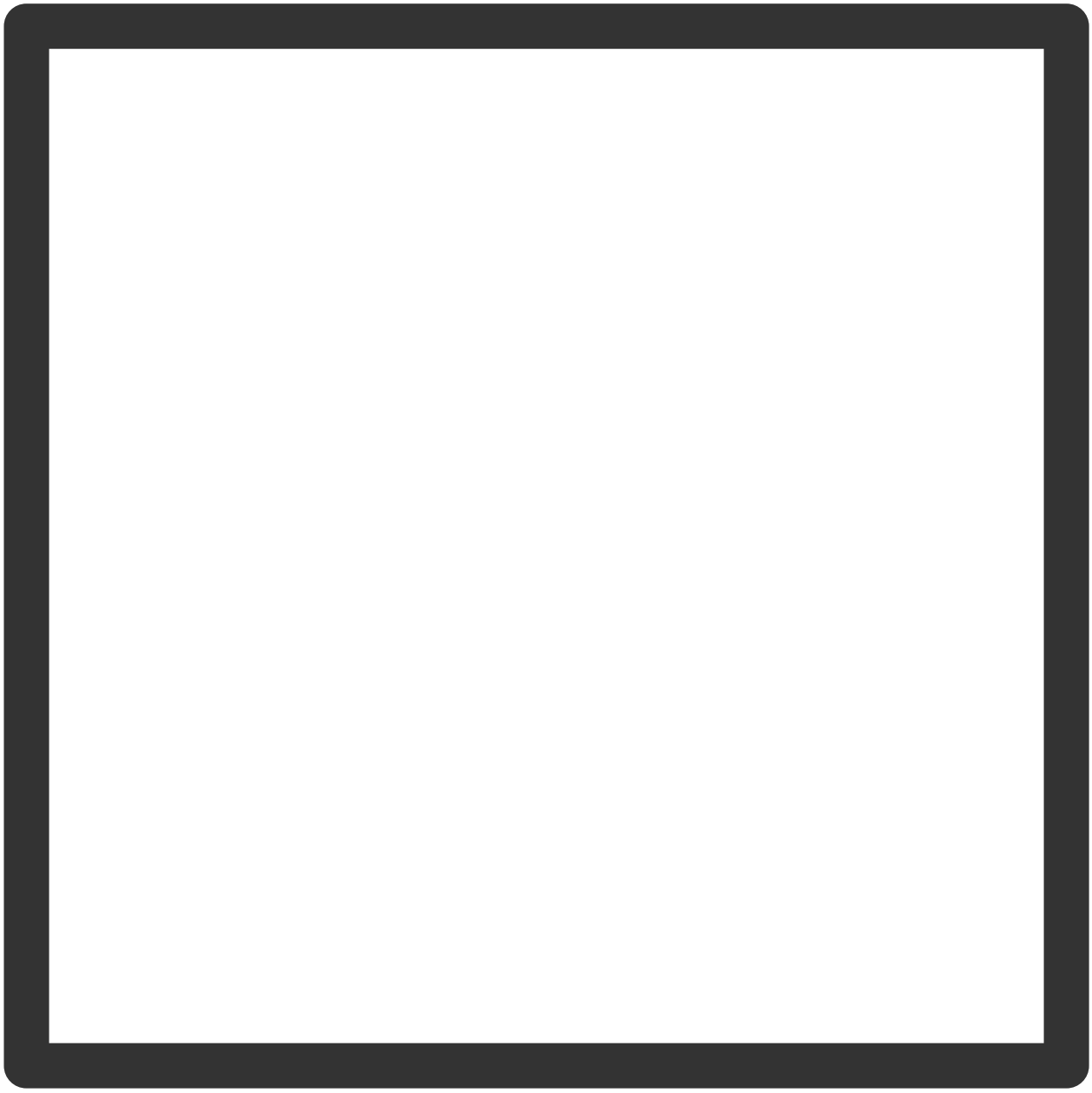


PoE class 2 device. Requests 7 W power but actually consumes 5 W power.

Additional settings

PoE class 3 device. Requests 15.5 W power but actually consumes 7.5 W power.

Additional settings



Reserved power.

Additional settings

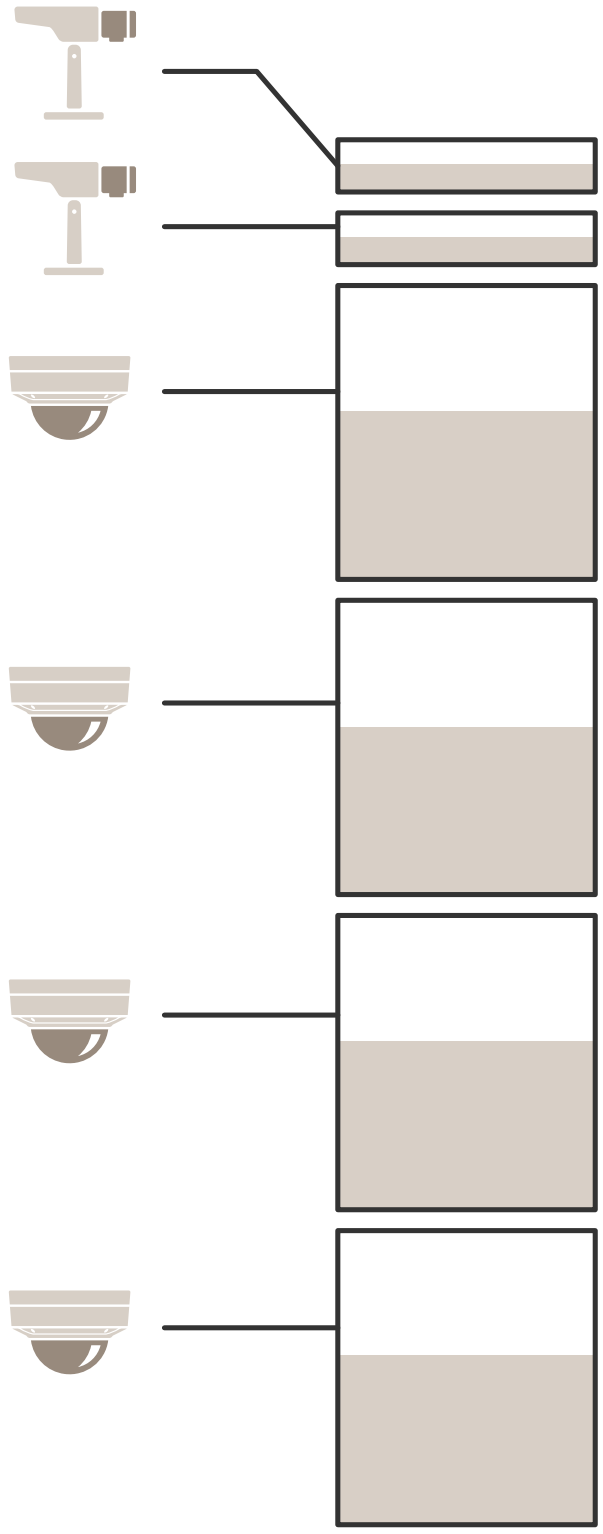
Actual power consumption.

Allocate power by PoE class

Additional settings

Reserved power

Actual power consumption



Additional settings

- Each port reserves the amount of power according to the device's PoE class.
- The recorder can power 2 PoE class 3 devices and 4 PoE class 2 devices.
- The total power reserved is (2 x 15.5) + (4 x 7) =59 W.
- The actual power consumed is (2 x 7.5) + (4 x 5) = 35 W.

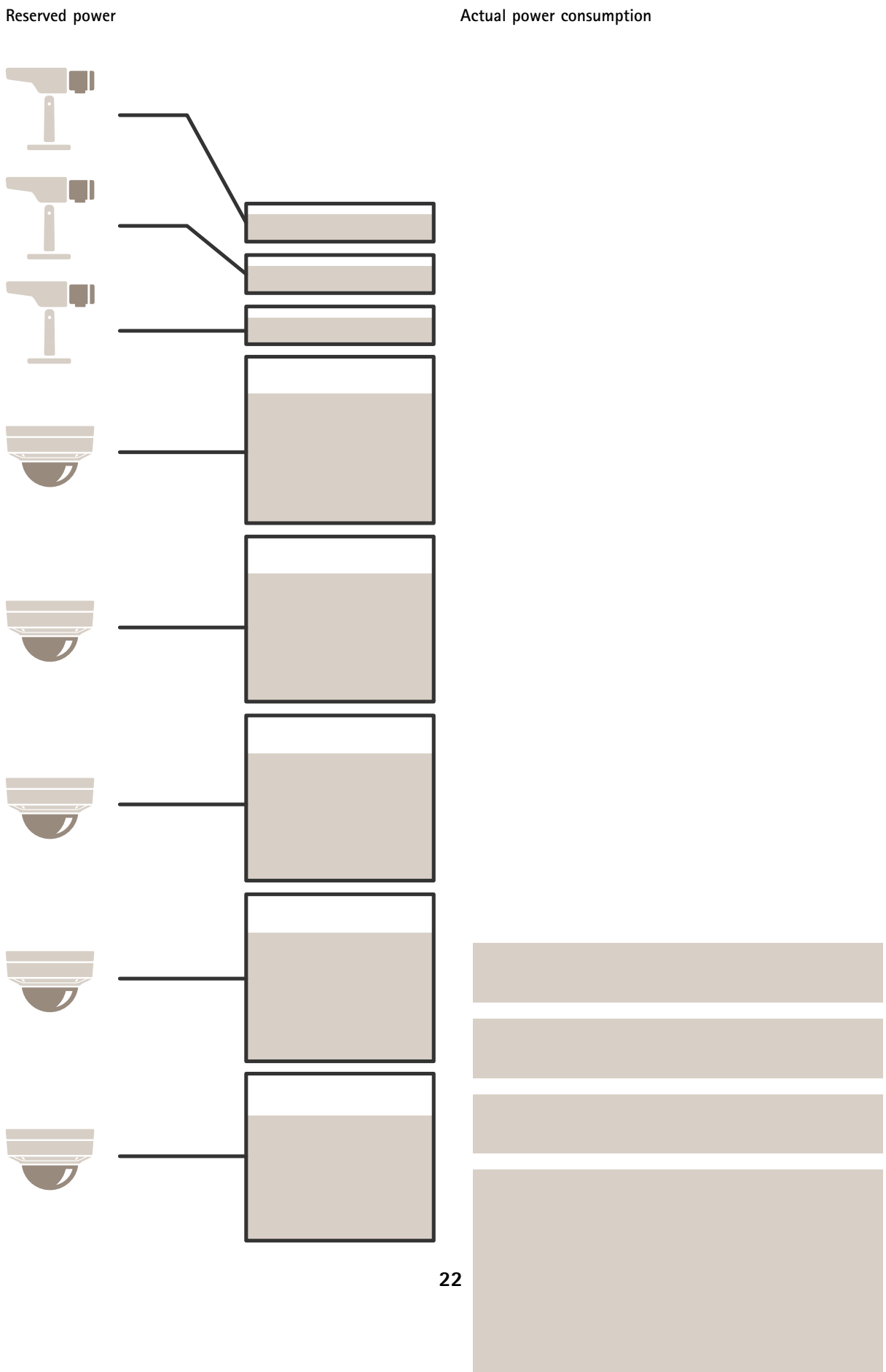
Allocate power by LLDP

Note

The power allocation via LLDP will over-provision for a worst-case power loss that will happen over the network cable.

PoE Class	1	2	3
Max power camera	3.84	6.49	12.95
Worst case power loss cable	0.14	0.41	1.92
Power needed at recorder	3.98	6.90	14.87
Max power for class	4.00	7.00	15.40
Power reserved at recorder	4 W	7 W	15.5 W

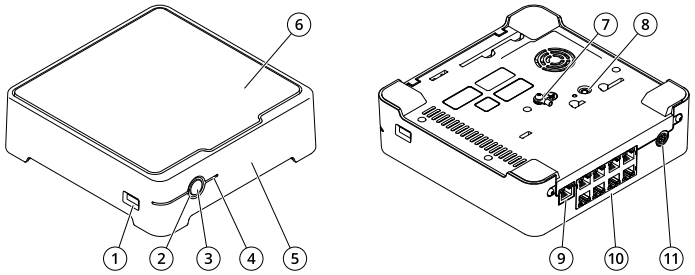
Additional settings



Additional settings

- Max power determined by the connected device.
- Each port reserves the amount of power according to the device's Max PoE power consumption.
- The recorder can power up to 8 devices, if their max power requirements remain within the limits.
- The total power reserved by 8 PoE class 3 devices with LLDP is (8 x 7.5) = 60 W.
- The actual power consumed by 8 PoE class 3 devices with LLDP is (8 x 7) = 56 W.
- In this way, a tighter PoE budget allocation allows for more connected devices.

Product overview



1 *USB port*
2 *Status LED*
3 *Power button*
4 *Hard drive LED*
5 *Alarm buzzer*
6 *Hard drive*
7 *Grounding*
8 *Control button*
9 *LAN port*
10 *PoE port (8x)*
11 *Power input*

Power button

- To shut down the recorder, long press the power button until the buzzer makes a brief sound.
- To silence the buzzer, short press the power button.

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Hard reset a recorder on page 26*.
- Connecting to an AXIS Video Hosting System service. To connect, press and hold the button for about 3 seconds until the status LED flashes green.

Troubleshooting

The status LED gives you the following information:

Status LED	Indication
Green	The recorder is on and the status is ok.
Orange	The recorder is starting up, or the firmware is upgrading. Wait until the LED turns green.
Red	This can mean that the PoE budget is exceeded. If you just connected a device to the recorder, try to remove it again. For more information about PoE limitations, see *How much power can the recorder supply to the cameras? on page 2* .

The hard drive LED gives you the following information:

Hard drive LED	Indication
Green	The LED is flashing green when data is written to the hard drive.
Red	A recording disruption has occurred. Go to **System** > **Storage** for more information.

The buzzer sounds for this reason:

- The PoE budget is exceeded. If you just connected a device to the recorder, try removing it again. For more information about PoE limitations, see *How much power can the recorder supply to the cameras? on page 2*

Note

You can stop the buzzer with a short press of the power button.

The recorder shuts down:

- The recorder is severely overheated.

Technical issues, clues and solutions

Issue	Solution
My recordings are not available.	Go to *Fix common issues on page 25*.
I cannot connect to my cameras.	Go to *Fix common issues on page 25*.
I receive error notification: "No contact".	Go to *Fix common issues on page 25*.
My sites do not appear in my mobile app.	Make sure you have version 4 of the AXIS Companion mobile app.

Fix common issues

Before you restart, configure or reset your devices, we recommend that you to save a system report.

See *Save a system report on page 27*.

1. Check that your cameras and recorder have power.

2. Check that you are connected to the internet.
3. Check that the network is working.
4. Check that the cameras are connected to the same network as the computer, unless you are remote.

Still not working?

5. Make sure that your cameras, recorder and AXIS Companion desktop app have the latest firmware and software updates.

   See *Upgrade firmware on page 26*.
6. Restart the AXIS Companion desktop app.
7. Restart you cameras and recorder.

Still not working?

8. Make a hard reset on the cameras and the recorder, to completely put them back to factory default settings.

   See *Hard reset a recorder on page 26*.
9. Add the reset cameras to your site again.

Still not working?

10. Update your graphics card with the latest drivers.

Still not working?

11. Save a system report and contact *Axis technical support*.

    See *Save a system report on page 27*.

Upgrade firmware

New firmware updates bring you to the latest and improved set of features, functions, and security enhancements.

1. Go to the leader device webpage.
2. Go to **System** > **Maintenance** and click **Upgrade** under **Firmware upgrade**.
3. Follow the instructions on the screen.

Hard reset a recorder

⚠WARNING

Move the recorder very gently while it is switched on. Sudden moves or shocks may damage the hard drive.

⚠WARNING

A hard reset will remove the saved encryption password for the hard drive. Failure to remember the encryption password for an encrypted hard drive will result in permanent loss of all recordings.

Note

A hard reset will reset all the settings, including the IP address.

1. Switch off the recorder:

   Press the power button on the front of the recorder for 4-5 seconds until you hear a beep.
2. Wait until the recorder is switched off, then turn it over to access the control button.

3. Press and hold the control button. Press and release the power button to start the recorder. Release the control button after 15-30 seconds when the LED indicator flashes amber.
4. Slowly put the recorder back in its place.
5. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is `192.168.0.90`
6. Reset your cameras connected to the recorder.
7. If your hard drive is encrypted, then it must be mounted manually after the recorder is reset:
   7.1 Go to the device webpage.
   7.2 Go to **System** > **Storage** and click **Mount**.
   7.3 Enter the encryption password used when encrypting the hard drive.

I can't log in to the product's webpage

If you set a password for the product during configuration, and later add that product to a site, you can no longer log in to the product's webpage with the password you've set. This is because AXIS Companion software changes the passwords of all devices in the site.

To log in to a device in your site, type the user name **root** and your site password.

How to erase all recordings

1. Go to the device webpage > **System** > **Storage**.
2. Select **Format** and click **Use tool**.

Note

This procedure erases all recordings from the hard drive, but the configuration of the recorder and the site doesn't change.

Save a system report

1. In AXIS Companion, go to  > **Save system report**.
2. When you register a new case at Axis Helpdesk, attach the system report.

Need more help?

Useful links

- *AXIS Companion user manual*

Contact support

Contact support at *axis.com/support*.

User Manual
AXIS S3008 Recorder

Ver. M14.2
Date: October 2021
Part No. T10152902