AXIS S3008 Mk II Recorder

User manual

About your device

AXIS S3008 Mk II 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 is 124 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.*

Installation

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

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

Get started

Internet access is required during the system setup.

1.

2.

3.

4.

5.

When the installation is done:

- All Axis devices in the system have the latest firmware.

- All devices have a password.

- Recording using the default settings is active.

- You can use remote access.

Register a My Axis account

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

To make your My Axis account more secure, activate multi-factor authentication (MFA). MFA is a security system that adds another layer of verification to ensure the user's identity.

To activate MFA:
1. Go to *axis.com/my-axis/login*.

2. Log in with your **My Axis** credentials.

3. Go to ⊚ and select **Account settings**.

4. Click **Security settings**

5. Click **Handle your 2-factor authentication**.

6. Enter your **My Axis** credentials.

7. Choose one of the authentication methods **Authenticator App (TOTP)** or **Email** and follow the on-screen instructions.

Install the hardware

1. Install your camera hardware.

2. Connect the recorder to your network via the LAN port.

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-camera-station-edge* and click **Download** to download AXIS S3008 Mk II Recorder for Windows.

2. Open the setup file and follow the setup assistant.

3. Sign in with your *My Axis account.*

Create a site

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 My Axis account.

1. Start the AXIS S3008 Mk II Recorder desktop app.

2. Sign in with your *My Axis account.*

3. Click **Create new site** and give the site a name.

4. Click **Next.**

5. Select the devices you want to add to your site.

6. Click **Next.**

7. Select storage.

8. Click **Next.**

9. On the **Ready to install page**, **Offline mode** and **Upgrade firmware** are turned on by default. You can turn them off if you don't want to access offline mode or upgrade your devices to the latest firmware version.

10. Click **Install** and wait while AXIS S3008 Mk II Recorder configures the devices. The configuration can take several minutes.

Install the mobile app

With AXIS S3008 Mk II Recorder mobile app, you can access your devices and recordings from anywhere. You can also get notifications when events occur, or when someone calls from an intercom.
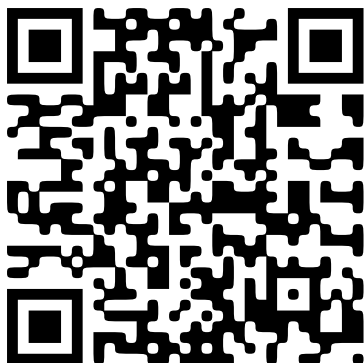
For Android

Click *Download* or scan the following QR Code®.
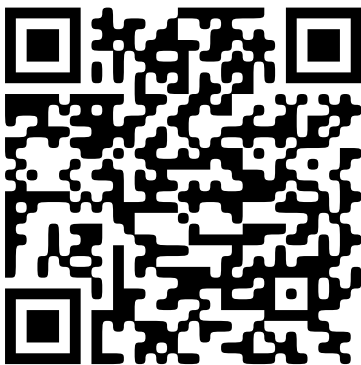
For iOS

Click *Download* or scan the following QR Code.

Open the AXIS S3008 Mk II Recorder mobile app and log in with your Axis credentials.

If you don't have a My Axis account, you can go to *axis.com/my-axis* to register a new account.

QR Code is a registered trademark of Denso Wave Incorporated in Japan and other countries.

The web interface

To reach the device's web interface, type the device's IP address in a web browser.

≡> Show or hide the main menu.

⊘ Access the release notes.

⑦ Access the product help.

A̅⃗ Change the language.

◑ Set light theme or dark theme.

⊙ ⊖ The user menu contains:

- Information about the user who is logged in.

- ⇄ **Change account** : Log out from the current account and log in to a new account.

- ⤓ **Log out** : Log out from the current account.

⋮ 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 AXIS OS version and serial number.

Status

Time sync status

Shows NTP synchronization information, including if the device is in sync with an NTP server and the time remaining until the next sync.

NTP settings: View and update the NTP settings. Takes you to the **Time and location** page where you can change the NTP settings.

Ongoing recordings

Shows ongoing recordings and their designated storage space.

Recordings: View ongoing and filtered recordings and their source. For more information, see

▯ ⊏⊐ Shows the storage space where the recording is saved.

Device info

Shows the device information, including AXIS OS version and serial number.

> **Upgrade AXIS OS**: Upgrade the software on your device. Takes you to the Maintenance page where you can do the upgrade.

Connected clients

Shows the number of connections and connected clients.

> **View details**: View and update the list of connected clients. The list shows IP address, protocol, port, state, and PID/process of each connection.

Apps

> ╋ **Add app**: Install a new app.
>
> **Find more apps**: Find more apps to install. You will be taken to an overview page of Axis apps.
>
> **Allow unsigned apps** ⓘ : Turn on to allow installation of unsigned apps.
>
> 🔔 View the security updates in AXIS OS and ACAP apps.
>
> | Note |
> |---|
>
> The device's performance might be affected if you run several apps at the same time.
>
> Use the switch next to the app name to start or stop the app.
>
> **Open**: Access the app's settings. The available settings depend on the application. Some applications don't have any settings.
>
> ⋮ The context menu can contain one or more of the following options:
>
> - **Open-source license**: View information about open-source licenses used in the app.
> - **App log**: 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/products/analytics*. 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 replace it with another license, for example, when you change from a trial license to a full license. If you deactivate the license, you also remove it from the device.
> - **Settings**: Configure the parameters.
> - **Delete**: Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

System

Time and location

Date and time

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

Note

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

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

- **Automatic date and time (manual NTS KE servers)**: Synchronize with the secure NTP key establishment servers connected to the DHCP server.
  - **Manual NTS KE servers**: 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.
  - **Max NTP poll time**: Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
  - **Min NTP poll time**: Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.

- **Automatic date and time (NTP servers using DHCP)**: Synchronize with the NTP servers connected to the DHCP server.
  - **Fallback NTP servers**: Enter the IP address of one or two fallback servers.
  - **Max NTP poll time**: Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
  - **Min NTP poll time**: Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.

- **Automatic date and time (manual NTP servers)**: Synchronize with NTP servers of your choice.
  - **Manual NTP servers**: 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.
  - **Max NTP poll time**: Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
  - **Min NTP poll time**: Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.

- **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 automatically adjust to daylight saving time and standard time.

- **DHCP**: Adopts the time zone of the DHCP server. The device must connected to a DHCP server before you can select this option.

- **Manual**: Select a time zone from the drop-down list.

Note

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

Network

IPv4

Assign IPv4 automatically: Select to let the network router assign an IP address to the device automatically. We recommend automatic IP (DHCP) for most networks.

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 contact your network administrator before you assign a static IP address.

Subnet mask: Enter the subnet mask to define what addresses are inside the local area network. Any address outside the local area network goes through the router.

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

Fallback to static IP address if DHCP isn't available: Select if you want to add a static IP address to use as fallback if DHCP is unavailable and can't assign an IP address automatically.

Note

If DHCP isn't available and the device uses a static address fallback, the static address is configured with a limited scope.

IPv6

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

Hostname

Assign hostname automatically: Select to let the network router assign a hostname to the device automatically.

Hostname: Enter the hostname manually to use as an alternative way of accessing the device. The server report and system log use the hostname. Allowed characters are A–Z, a–z, 0–9 and -.

Enable dynamic DNS updates: Allow your device to automatically update its domain name server records whenever its IP address changes.

Register DNS name: Enter a unique domain name that points to your device's IP address. Allowed characters are A–Z, a–z, 0–9 and -.

TTL: Time to Live (TTL) sets how long a DNS record stays valid before it needs to be updated.

DNS servers

Assign DNS automatically: Select to let the DHCP server assign search domains and DNS server addresses to the device automatically. We recommend automatic DNS (DHCP) for most networks.

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 the device uses.

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

Network discovery protocols

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.

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.

WS-Discovery: Turn on to allow automatic discovery on the network.

LLDP and CDP: Turn on to allow automatic discovery on the network. Turning LLDP and CDP off can impact the PoE power negotiation. To resolve any issues with the PoE power negotiation, configure the PoE switch for hardware PoE power negotiation only.

Global proxies

Http proxy: Specify a global proxy host or IP address according to the allowed format.

Https proxy: Specify a global proxy host or IP address according to the allowed format.

Allowed formats for http and https proxies:
- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

Note

Restart the device to apply the global proxy settings.

No proxy: Use **No proxy** to bypass global proxies. Enter one of the options in the list, or enter several separated by a comma:
- Leave empty
- Specify an IP address
- Specify an IP address in CIDR format
- Specify a domain name, for example: www.<domain name>.com
- Specify all subdomains in a specific domain, for example .<domain name>.com

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**: This is the default option. To connect to O3C, press the control button on the device. Depending on the device model, either press and release or press and hold, until the status LED flashes. Register the device with the O3C service within 24 hours to enable **Always** and stay connected. If you don't register, the device will disconnect from O3C.

- **Always**: The device continuously attempts to connect to an O3C service over the internet. Once you register the device, it stays connected. Use this option if the control button is out of reach.

- **No**: Disconnects the O3C service.

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

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices.

SNMP: Select the version of SNMP to use.

- **v1 and v2c**:
    - **Read community**: Enter the community name that has read-only access to all supported SNMP objects. The default value is **public**.
    - **Write community**: Enter the community name that has read or write access to all supported SNMP objects (except read-only objects). The default value is **write**.
    - **Activate traps**: Turn on to activate trap reporting. The device uses traps to send messages for important events or status changes to a management system. In the web interface, you can set up traps for SNMP v1 and v2c. Traps are automatically turned off if you change to SNMP v3 or turn off SNMP. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
    - **Trap address**: Enter the IP address or host name of the management server.
    - **Trap community**: Enter the community to use when the device sends a trap message to the management system.
    - **Traps**:
        - **Cold start**: Sends a trap message when the device starts.
        - **Link up**: Sends a trap message when a link changes from down to up.
        - **Link down**: Sends a trap message when a link changes from up to down.
        - **Authentication failed**: Sends a trap message when an authentication attempt fails.

Note

All Axis Video MIB traps are enabled when you turn on SNMP v1 and v2c traps. For more information, see *AXIS OS Portal > SNMP*.

- **v3**: SNMP v3 is a more secure version, which provides encryption and secure passwords. To use SNMP v3, we recommend you to activate HTTPS, as the password is then sent through HTTPS. This also prevents unauthorized parties' access to unencrypted SNMP v1 and v2c traps. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
    - **Password for the account "initial"**: Enter the SNMP password for the account named "initial". Although the password can be sent without activating HTTPS, we don't recommend it. The SNMP v3 password can only be set once, and preferably only when HTTPS is enabled. Once the password is set, the password field is no longer displayed. To set the password again, you must reset the device to factory default settings.

Network ports

Power over Ethernet

- **Allocated power**: 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.

$=$ Click to show or hide the ports image.

- Click a port in the image to see the port details in the port list.

Port list

- **Port**: The port number.

- **PoE**: Turn on or off PoE for the port.

- **Network**: Turn on or off network for the port.

- **Status**: Shows if there is device connected to this port.

- **Friendly name**: The friendly name is set in **Network settings**. The default name is a combination of the model and the media access control address (MAC address) of the connected device.

- **Power consumption**: Number of watts (W) that are currently consumed and allocated by the connected device.

Power over Ethernet

Allocated power: 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.

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

- **Friendly name**: The friendly name is set in **Network settings**. The default name is a combination of the model and the media access control address (MAC address) of the connected device.

- **Power consumption**: Number of watts (W) that are currently consumed and allocated.

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.

Add certificate : Click to add a certificate. A step-by-step guide opens up.

- **More** ⌄ : Show more fields to fill in or select.
- **Secure keystore**: Select to use **Trusted Execution Environment (SoC TEE)**, **Secure element** or **Trusted Platform Module 2.0** to securely store the private key. For more information on which secure keystore to select, go to *help.axis.com/axis-os#cryptographic-support*.
- **Key type**: Select the default or a different encryption algorithm from the drop-down list to protect the 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.

Secure keystore ⓘ :

- **Trusted Execution Environment (SoC TEE)**: Select to use SoC TEE for secure keystore.
- **Secure element (CC EAL6+)**: Select to use secure element for secure keystore.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)**: Select to use TPM 2.0 for secure keystore.

Network access control and encryption

15

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).

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec is an IEEE standard for media access control (MAC) security that defines connectionless data confidentiality and integrity for media access independent protocols.

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, you must install a signed client certificate on the device.

Authentication method: Select an EAP type used for authentication.

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

CA certificates: Select CA certificates 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.

These settings are only available if you use **IEEE 802.1x PEAP-MSCHAPv2** as the authentication method:

- **Password**: Enter the password for your user identity.
- **Peap version**: Select the Peap version that is used in the network switch.
- **Label**: Select 1 to use client EAP encryption; select 2 to use client PEAP encryption. Select the Label that the network switch uses when using Peap version 1.

These settings are only available if you use **IEEE 802.1ae MACsec (Static CAK/Pre-Shared Key)** as the authentication method:

- **Key agreement connectivity association key name**: Enter the connectivity association name (CKN). It must be 2 to 64 (divisible by 2) hexadecimal characters. The CKN must be manually configured in the connectivity association and must match on both ends of the link to initially enable MACsec.
- **Key agreement connectivity association key**: Enter the connectivity association key (CAK). It should be either 32 or 64 hexadecimal characters long. The CAK must be manually configured in the connectivity association and must match on both ends of the link to initially enable MACsec.

Firewall

Firewall: Turn on to activate the firewall.

Default Policy: Select how you want the firewall to handle connection requests not covered by rules.
- **ACCEPT:** Allows all connections to the device. This option is set by default.

- **DROP:** Blocks all connections to the device.

To make exceptions to the default policy, you can create rules that allows or blocks connections to the device from specific addresses, protocols, and ports.

+ New rule: Click to create a rule.

Rule type:
- **FILTER**: Select to either allow or block connections from devices that match the criteria defined in the rule.
    - **Policy**: Select **Accept** or **Drop** for the firewall rule.

    - **IP range**: Select to specify a range of addresses to allow or block. Use IPv4/IPv6 in **Start** and **End**.

    - **IP address**: Enter an address that you want to allow or block. Use IPv4/IPv6 or CIDR format.

    - **Protocol**: Select a network protocol (TCP, UDP, or Both) to allow or block. If you select a protocol, you must also specify a port.

    - **MAC**: Enter the MAC address of a device that you want to allow or block.

    - **Port range**: Select to specify the range of ports to allow or block. Add them in **Start** and **End**.

    - **Port**: Enter a port number that you want to allow or block. Port numbers must be between 1 and 65535.

    - **Traffic type**: Select a traffic type that you want to allow or block.
        - **UNICAST**: Traffic from a single sender to a single recipient.

        - **BROADCAST**: Traffic from a single sender to all devices on the network.

        - **MULTICAST**: Traffic from one or more senders to one or more recipient.

- **LIMIT**: Select to accept connections from devices that match the criteria defined in the rule but apply limits to reduce excessive traffic.
    - **IP range**: Select to specify a range of addresses to allow or block. Use IPv4/IPv6 in **Start** and **End**.

    - **IP address**: Enter an address that you want to allow or block. Use IPv4/IPv6 or CIDR format.

    - **Protocol**: Select a network protocol (TCP, UDP, or Both) to allow or block. If you select a protocol, you must also specify a port.

    - **MAC**: Enter the MAC address of a device that you want to allow or block.

    - **Port range**: Select to specify the range of ports to allow or block. Add them in **Start** and **End**.

    - **Port**: Enter a port number that you want to allow or block. Port numbers must be between 1 and 65535.

    - **Unit**: Select the type of connections to allow or block.

    - **Period**: Select the time period related to **Amount**.

    - **Amount**: Set the maximum number of times a device is allowed to connect within the set **Period**. The maximum amount is 65535.

    - **Burst**: Enter the number of connections allowed to exceed the set **Amount** once during the set **Period**. Once the number has been reached, only the set amount during the set period is allowed.

    - **Traffic type**: Select a traffic type that you want to allow or block.
        - **UNICAST**: Traffic from a single sender to a single recipient.

        - **BROADCAST**: Traffic from a single sender to all devices on the network.

> – MULTICAST: Traffic from one or more senders to one or more recipient.
>
> **Test rules**: Click to test the rules that you have defined.
>
> - **Test time in seconds**: Set a time limit for testing the rules.
> - **Roll back**: Click to roll back the firewall to its previous state, before you have tested the rules.
> - **Apply rules**: Click to activate the rules without testing. We don't recommend that you do this.

Custom signed AXIS OS certificate

> To install test software or other custom software from Axis on the device, you need a custom signed AXIS OS certificate. The certificate verifies that the software is approved by both the device owner and Axis. The software can only run on a specific device which is identified by its unique serial number and chip ID. Only Axis can create custom signed AXIS OS certificates, since Axis holds the key to sign them.
>
> **Install**: Click to install the certificate. You need to install the certificate before you install the software.
>
> ⋮ The context menu contains:
>
> - **Delete certificate**: Delete the certificate.

Accounts

Virtual host

> ╋ **Add virtual host**: Click to add a new virtual host.
>
> **Enabled**: Select to use this virtual host.
>
> **Server name**: Enter the name of the server. Only use numbers 0–9, letters A–Z, and hyphen (–).
>
> **Port**: Enter the port the server is connected to.
>
> **Type**: Select the type of authentication to use. Select between **Basic**, **Digest**, and **Open ID**.
>
> ⋮ The context menu contains:
>
> - **Update**: Update the virtual host.
> - **Delete**: Delete the virtual host.
>
> **Disabled**: The server is disabled.

Client Credentials Grant Configuration

> **Admin claim**: Enter a value for the admin role.
>
> **Verification URI**: Enter the web link for the API endpoint authentication.
>
> **Operator claim**: Enter a value for the operator role.
>
> **Require claim**: Enter the data that should be in the token.
>
> **Viewer claim**: Enter the value for the viewer role.
>
> **Save**: Click to save the values.

Events

Rules

A rule defines the conditions that triggers the product to perform an action. The list shows all the currently configured rules in the product.

Note

> You can create up to 256 action rules.

┼ **Add a rule**: Create a rule.

Name: Enter a name for the rule.

Wait between actions: Enter the minimum time (hh:mm:ss) that must pass between rule activations. It is useful if the rule is activated by, for example, day-night mode conditions, to avoid that small light changes during sunrise and sunset activate the rule repeatedly.

Condition: Select a condition from the list. A condition must be met for the device to perform an action. If multiple conditions are defined, all of them must be met to trigger the action. For information about specific conditions, see *Get started with rules for events*.

Use this condition as a trigger: Select to make this first condition function only as a starting trigger. It means that once the rule is activated, it remains active for as long as all the other conditions are met, no matter the state of the first condition. If you don't select this option, the rule will simply be active whenever all the conditions are met.

Invert this condition: Select if you want the condition to be the opposite of your selection.

┼ **Add a condition**: Click to add an additional condition.

Action: Select an action from the list and enter its required information. For information about specific actions, see *Get started with rules for events*.

Recipients

You can set up your device to notify recipients about events or send files.

Note

> If you set up your device to use FTP or SFTP, don't change or remove the unique sequence number that's added to the file names. If you do that, only one image per event can be sent.

The list shows all the recipients currently configured in the product, along with information about their configuration.

Note

> You can create up to 20 recipients.

 Add a recipient: Click to add a recipient.

Name: Enter a name for the recipient.

Type: Select from the list:

- FTP
    - Host: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
    - Port: Enter the port number used by the FTP server. The default is 21.
    - Folder: Enter the path to the directory where you want to store files. If this directory doesn't already exist on the FTP server, you will get an error message when uploading files.
    - Username: Enter the username for the login.
    - Password: Enter the password for the login.
    - Use temporary file name: Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name are correct.
    - Use passive FTP: Under normal circumstances, the product simply requests the target FTP server to open the data connection. The device actively initiates both the FTP control and data connections to the target server. This is normally needed if there is a firewall between the device and the target FTP server.

- HTTP
    - URL: Enter the network address to the HTTP server and the script that will handle the request. For example, http://192.168.254.10/cgi-bin/notify.cgi.
    - Username: Enter the username for the login.
    - Password: Enter the password for the login.
    - Proxy: Turn on and enter the required information if a proxy server must be passed to connect to the HTTP server.

- HTTPS
    - URL: Enter the network address to the HTTPS server and the script that will handle the request. For example, https://192.168.254.10/cgi-bin/notify.cgi.
    - Validate server certificate: Select to validate the certificate that was created by HTTPS server.
    - Username: Enter the username for the login.
    - Password: Enter the password for the login.
    - Proxy: Turn on and enter the required information if a proxy server must be passed to connect to the HTTPS server.

- Network storage
  You can add network storage such as NAS (network-attached storage) and use it as a recipient to store files. The files are stored in the Matroska (MKV) file format.
    - Host: Enter the IP address or hostname for the network storage.
    - Share: Enter the name of the share on the host.
    - Folder: Enter the path to the directory where you want to store files.
    - Username: Enter the username for the login.
    - Password: Enter the password for the login.

- SFTP ⓘ
    - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
    - **Port**: Enter the port number used by the SFTP server. The default is 22.
    - **Folder**: Enter the path to the directory where you want to store files. If this directory doesn't already exist on the SFTP server, you will get an error message when uploading files.
    - **Username**: Enter the username for the login.
    - **Password**: Enter the password for the login.
    - **SSH host public key type (MD5)**: Enter the fingerprint of the remote host's public key (a 32-digit hexadecimal string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
    - **SSH host public key type (SHA256)**: Enter the fingerprint of the remote host's public key (a 43-digit Base64 encoded string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
    - **Use temporary file name**: Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted or interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way, you know that all files that have the desired name are correct.

- SIP or VMS ⓘ :
  SIP: Select to make a SIP call.
  VMS: Select to make a VMS call.
    - **From SIP account**: Select from the list.
    - **To SIP address**: Enter the SIP address.
    - **Test**: Click to test that your call settings works.

- Email
    - **Send email to**: Enter the email address to send emails to. To enter multiple addresses, use commas to separate them.
    - **Send email from**: Enter the email address of the sending server.
    - **Username**: Enter the username for the mail server. Leave this field empty if the mail server does not require authentication.
    - **Password**: Enter the password for the mail server. Leave this field empty if the mail server does not require authentication.
    - **Email server (SMTP)**: Enter the name of the SMTP server, for example, smtp.gmail.com, smtp.mail.yahoo.com.
    - **Port**: Enter the port number for the SMTP server, using values in the range 0-65535. The default value is 587.
    - **Encryption**: To use encryption, select either SSL or TLS.
    - **Validate server certificate**: If you use encryption, select to validate the identity of the device. The certificate can be self-signed or issued by a Certificate Authority (CA).

- **POP authentication**: Turn on to enter the name of the POP server, for example, pop.gmail. com.

Note

Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid your email account being locked or missing out on your expected emails.

- TCP
  - **Host**: Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
  - **Port**: Enter the port number used to access the server.

Test: Click to test the setup.

⋮ The context menu contains:

View recipient: Click to view all the recipient details.

Copy recipient: Click to copy a recipient. When you copy, you can make changes to the new recipient.

Delete recipient: Click to delete the recipient permanently.

Schedules

Schedules and pulses can be used as conditions in rules. The list shows all the schedules and pulses currently configured in the product, along with information about their configuration.

╋ **Add schedule**: Click to create a schedule or pulse.

Manual triggers

You can use the manual trigger to manually trigger a rule. The manual trigger can, for example, be used to validate actions during product installation and configuration.

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 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 stored data.
- **Decrypt**: Decrypt stored data. The system will erase all files on the storage device.
- **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. This will stop all ongoing recordings.

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

Autoformat 🛈 : The disk will automatically format using the ext4 file system.

Logs

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

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 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

- DNS server IP address

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 software is digitally signed to ensure that you only install verified software on your device. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper "Axis Edge Vault" at *axis.com*.

AXIS OS upgrade: Upgrade to a new AXIS OS version. New releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest AXIS OS 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 AXIS OS 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 AXIS OS 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 AXIS OS version.

AXIS OS rollback: Revert to the previously installed AXIS OS version.

Troubleshoot

Reset PTR 🛈 : Reset PTR if for some reason the **Pan**, **Tilt**, or **Roll** settings aren't working as expected. The PTR motors are always calibrated in a new camera. But calibration can be lost, for example, if the camera loses power or if the motors are moved by hand. When you reset PTR, the camera is re-calibrated and returns to its factory default position.

Calibration 🛈 : Click **Calibrate** to recalibrate the pan, tilt, and roll motors to their default positions.

Ping: To check if the device can reach a specific address, enter the hostname or IP address of the host you want to ping and click **Start**.

Port check: To verify connectivity from the device to a specific IP address and TCP/UDP port, enter the hostname or IP address and port number you want to check and click **Start**.
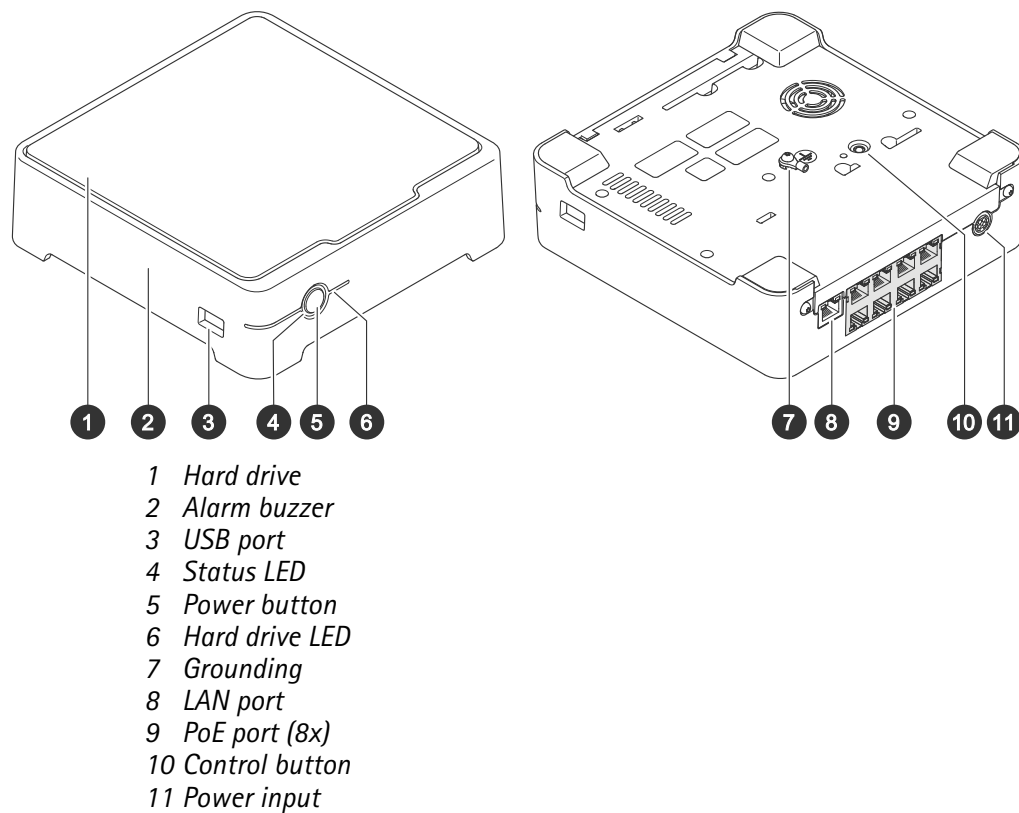
Network trace

Important

A network trace file might contain sensitive information such as certificates or passwords.

A network trace file can help you troubleshoot problems by recording activity on the network.

Trace time: Select the duration of the trace in seconds or minutes and click **Download**.

25

Product overview

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

- Connecting to a one-click cloud connection (O3C) service over the internet. 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 .

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

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 .
I cannot connect to my cameras.	Go to .
I receive error notification: "No contact".	Go to .
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 .

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 .

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 .

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 .

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's web interface.

2.   Go to **Maintenance > Firmware upgrade** and click **Upgrade**.

3.   Follow the instructions on the screen.

Hard reset a recorder

Important
    Move the recorder carefully while it's switched on. Sudden moves or shocks may damage the hard drive.

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

- A hard reset will not remove your recordings.

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.   Carefully 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 device IP address will default to one of the following:
    –   **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)

    –   **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24

6.   Reset your devices connected to the recorder.

7.   If your hard drive is encrypted, it must be mounted manually after the recorder is reset:
    7.1.   Go to the device's web interface.

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 web interface

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 web interface 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 username **root** and your site password.

How to erase all recordings

1.   In the device's web interface, go to **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 S3008 Mk II Recorder, 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

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