AXIS S3008 Recorder

Help

AXIS S3008 Recorder help file

Browser support

You can use the device with these browsers:

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 User Manual available at *www.axis.com*.
If you want more information about recommended browsers, go to *www.axis.com/browser-support*.

Settings

Top menu

Use this to change the language.

Use this to change the display between light theme or dark theme.

Use this to see which user is logged in and the rights of the user.

Click here for the following:

- **About**: About this product and manufacturer.

- **Feedback**: Use this to share your experience.

Important

  If you have questions or need help with your Axis product, contact us at .

- **Legal**: Information about cookies and licenses.

- **Help**: Use the link to access the latest help about the product interface (internet connection required).

Side menu

Use this to open or close the side menu.

AXIS S3008 Recorder help file

Recorder status

This section provides an overview of the system.

Status

Allocated PoE: Shows how many watts (W) are currently allocated.
Total PoE consumption: Shows how many watts (W) are consumed.
Keep PoE active during recorder restart: Enable this to keep the power on during a product restart, if this is not enabled then PoE will not supply power to connected devices during a restart of the product.
Used space: Shows the percentage of space used.
Free space: Shows the percentage of space available for recordings.
Disk status: Shows the current status of the disk.
Disk temperature: Current running temperature.
Free space: Available disk space. Disk capacity is displayed in MB (megabytes), GB (gigabytes), or TB (terabytes).
Ports   Each port will have an individual number and settings information.   **PoE**: Enable or disable PoE for each port. When a device is connected the following information will be displayed.   **Allocated power**: Shows how many watts (W) are currently allocated.   **Mac**: The media access control address (MAC address) of the connected device.

Apps

About applications

AXIS Camera Application Platform (ACAP) is an open platform that enables third parties to develop analytics and other applications for Axis products. For information about available applications, downloads, trials, and licenses, go to *www.axis.com/applications*

Applications can be uploaded by product administrators.

Applications and licenses can be installed on multiple products at the same time using AXIS Camera Management, version 3.10 and later.

Note

- Several applications can run at the same time but some applications might not be compatible with each other. Certain combinations of applications might require too much processing power or memory resources when run in parallel. Verify that the applications work together before deployment.

- If you upgrade an application the settings, including the license, is removed. The license must be reinstalled and the application reconfigured.

Go to **Apps** for a list of applications that have already been installed on the product.

Application overview

Controls

- Status

    - **Running**: The application is up and running.

    - **Idle**: The application has been started, but no event trigger has been configured for the application. The Idle status is dependent on the type of application installed and is not used in all applications. You can find more information in the manual for the specific application.

    - **Stopped**: The application is not running.

- **Start and stop**: You can start or stop the application.

- **Delete**: If you delete the app, you remove it completely from the product.

- **Application log**: The application log generates a log of the application events. This log will be helpful when requesting support from the vendor of the application package.

Activate the license: Without an activated license, the product cannot run the application. To activate the license you need a license key.

Browse to the file and select **Activate**.

If you don't have a license key stored on the computer, go to *www.axis.com/applications*. You need the license code and the Axis product serial number to get a license key. Save the license file on the computer.

Deactivate the license: You can deactivate the license if you want to use it in another product. This means that if you deactivate the license, you also remove it from the product.

Settings: To set up the application, click **Open**. The available settings depend on the type of application. It's not available for all applications. See the manual for the specific application.

System

Date and time

The current device date and time is displayed.

📍 Select which time zone to use. This will automatically adjust for daylight saving time (alternating between summer time and winter time for applicable regions).

The settings can be automatically obtained or set manually by selecting the **Synchronization** method:

- **Automatic date and time (NTP server using DHCP)**
- **Automatic date and time (manual NTP server)**
    - **Primary and secondary NTP server configuration**: When you use both primary and secondary NTP servers the product syncs and adapts its time based on the input of both NTP servers. This means that the secondary NTP server is always used and not only when the primary NTP server isn't available.
- **Custom date and time**: Manually set the date and time or use **Get from system** to get a single update from the system date and time.

Note

Date and time settings are used in all recordings, logs and system settings.

Network

Select the Internet Protocol to be used. There are currently two IP versions: IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 addresses are most commonly used today.

IPv4

- **Automatic IP (DHCP)** and **DNS (DHCP)**: is used by default, this is the recommended setting for most networks.
- **Automatic IP (DHCP)** and **manual DNS**: Contact your network administrator to configure manually.
- **Manual IP (DHCP)** and **DNS**: Contact your network administrator to configure manually.

Automatic IP (DHCP) and **DNS (DHCP)**: Current settings are listed, all updated automatically.

Automatic IP (DHCP) and **manual DNS**: Current settings are listed, manual configure the following:

- **Hostname**: When using a hostname that is not fully qualified, enter here the domain(s) in which to search for the hostname used by the product.
- **Search domains**: When using a hostname that is not fully qualified, enter here the domain(s) in which to search for the hostname used by the product.

    Use the ✚ **Add search domain** to add more search domains.
- **DNS servers**: Enter the IP address of the primary DNS server.
  This provides the translation of hostnames to IP addresses on your network.

    Use the ✚ **Add DNS server** to add more DNS servers.

Manual IP and manual DNS: Contact your network administrator to configure manually.

- **IP address** : Specify a unique IP address for the product. Static IP addresses can be assigned at random within isolated networks, provided that each given address is unique..
  To avoid conflicts, we strongly recommend that you contact your network administrator prior to assigning a static IP address.
- **Subnet mask**: Adjust to the mask for the subnet the product is located on.
- **Router**: Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.
- **Hostname**: When using a hostname that is not fully qualified, enter here the domain(s) in which to search for the hostname used by the product.

- **Search domains**: When using a hostname that is not fully qualified, enter here the domain(s) in which to search for the hostname used by the product.

  Use the **+** **Add search domain** to add more search domains.
- **DNS servers**: Enter the IP address of the primary DNS server.
  This provides the translation of hostnames to IP addresses on your network.

  Use the **+** **Add DNS server** to add more DNS servers.

IPv6

Assign automatically (DHCP) is used by default.

HTTP and HTTPS

Allow access through

Select if a user is allowed to connect to the device through **HTTP**, **HTTPS**, or both.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that provides encryption for page requests from users and for the pages returned by the web server. The encrypted exchange of information is governed by the use of an HTTPS certificate, which guarantees the authenticity of the server.

The Secure Socket Layer (SSL) as used by HTTPS uses a 40-bit key size for encryption, a level considered adequate for most commercial exchanges.

To use HTTPS on the Axis product, an HTTPS certificate must be installed. Go to **System > Security** to create and install certificates.

Note

- HTTPS is not supported by all video management software.

- Viewing encrypted web pages via HTTPS may cause a slight drop in performance, especially when requesting a page for the first time.

Friendly name

Use **Bonjour**®: Allow automatic discovery on the network.

- **Bonjour name**: Type a friendly name to be visible on the network. The default name is Axis product name and MAC address.

Use **Use UPnP**®: Allow automatic discovery on the network.

- **UPnP name**: Type a friendly name to be visible on the network. The default name is Axis product name and MAC address.

One-Click Cloud Connect (O3C) in conjunction with an O3C service provides easy and secure Internet access to live and recorded video accessible from any location.

Allow O3C

- **One-click**: Enabled by default. Press and hold the control button to connect to an O3C service over the Internet. Once registered, Always is enabled and your Axis product stays connected to the O3C service. If you do not register your Axis product within 24 hours from when the control button was pressed, the Axis product disconnects from the O3C service.
- **Always**: The Axis product constantly attempts to connect to an O3C service over the Internet. Once registered the product stays connected to the O3C service. Use this option if the control button is out of reach.
- **No**: Select this option to disable the O3C services.

Proxy settings

- **Host**: If needed, enter the proxy settings and port number to connect to the HTTP server
    - **Port**: Enter the number of the port used for access.

- **Login** and **Password**: Write a username and password for the proxy server, if needed.
- **Authentication method**
  - **Basic**: The **Basic** authentication method is the most compatible authentication scheme for HTTP. It is however less secure as it sends the username and password unencrypted to the server.
  - **Digest**: The **Digest** authentication method is more secure than **Basic** as it always transfers the password across the network encrypted.
  - **Auto**: This option enables the Axis product to select the authentication method automatically depending on the methods supported. It prioritizes the **Digest** method over the **Basic** method.

Connected clients: Expand this section to see the current settings.

To refresh the list use the **Update** button.

Security

Certificates

Certificates are used to authenticate devices on a network. The Axis product can use two types of certificate: **Client certificates** and **CA certificates**.

Client Certificates

A Client certificate identifies the Axis product, 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.

Use ⎯ᴼ៦ to open the filter options to search for specific client certificates in the list.

To add a self-signed certificate, use ✚ **Add certificate** button
and chose to **Create a self-signed certificate and certificate signing request**. Provide the requested information and then click **Save**.

When the process is complete, you will see the PEM-formatted signing request, which you can copy and send to your preferred Certificate Authority (CA).

Alternatively, click ✚ and then select **Upload** to install a certificate that has already been signed by a CA. Select the type of signing method and also select the file(s) containing the required information.

To view the properties for an installed client certificate, select it and click ✚

To **remove** a certificate, select it and click ✚

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 Axis product connects to a network protected by IEEE 802.1X. The Axis product has several pre-installed CA certificates.

Additional certificates can be installed by clicking ✚

To view the information for an installed certificate, select the certificate and click ✚

To remove a certificate, select it and click ✚

Note

All certificates will be deleted if the product is reset to factory default, although any pre-installed CA certificates will be re-installed.

The following formats are supported:

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

Custom-signed firmware certificate

Custom-signed firmware certificate

Install and select the custom-signed firmware before you upgrade.

Signed firmware at Axis

Axis signed firmware is based on the industry-accepted RSA public-key encryption method. The private key is stored in a closely guarded location at Axis while the public key is embedded in Axis devices. The integrity of the entire firmware image is assured by a signature of the image content. A primary signature verifies a number of secondary signatures, being verified while the image is unpacked.

Secure boot and Custom firmware certificates

While secure boot makes the product safer, it does also reduce the flexibility with different firmware, making it more complicated to load any temporary firmware, such as test firmware or other custom firmware from Axis, into the product. However, Axis has implemented a mechanism that approves individual units to accept such non-production firmware. This firmware is signed in a different way, with approval by both the owner and Axis, and results in a Custom Firmware Certificate. When installed in the approved units, the certificate enables use of a custom firmware that can run only on the approved unit, based on its unique serial number and chip ID. Custom Firmware Certificates can be created only by Axis, since Axis holds the key to sign them.

Users

All users are administrators.

Viewers: These users have access to the live view only.

Operators: Can access all settings except:

- Uploading applications and language files
- The settings included under **System**.

Administrators: These users have unrestricted access to all settings, and can also create, edit and remove other users.

How to create a user

- Use the **+** **Add user** button to add a new user.

Username: Enter a unique username.

New password: Enter a password for the user.

Passwords can consist of 1 to 64 characters. Only printable ASCII characters (code 32 to 126), for example, letters, numbers, punctuation marks and some symbols are allowed in the password.

Repeat password: Enter the same password again.

Rold: Select user type from the list.

NOTICE

The maximum number of users is 100.

Storage

Onboard storage

Onboard storage means that the video is recorded and stored directly into the product.

Information on the storage device is displayed.

Safely remove the storage: Use **Unmount** to safely remove the onboard storage device..

⚠**WARNING**

Never remove the storage without first unmounting it and turning off the power, or recordings may be lost

- **Write-protect**: Check this option to stop writing to the SD card and protect recordings from being removed. A locked storage unit cannot be formatted.
- **Format new storage devices to ext4**: SD cards are normally pre-formatted with the file system vFAT. If you select Format new storage devices to ext4, the product checks the current file system and then formats the storage device into the ext4 file system if required. *We recommend using ext4 as it is a more reliable file system.*
- **Retention time**: This option can be used to limit the amount of old recordings in order to avoid filling the storage device and also to comply with regulations regarding data storage. Enter the length of time to keep the old recordings. Old recordings will be removed sooner if the storage device becomes full.

Tools: Select an action, and click to perform it.

- **Check**: Check for errors on the SD card. This only works for the ext4 file system.
- **Repair**: Repairs errors in the ext4 file system. To repair a vFAT formatted SD card, eject the SD card, insert it in a computer and perform a disk repair.
- **Format (erase all)**: Format the storage device, when you need to change the file system or to quickly erase all the data. VFAT and ext4 are the two available file system options. The recommended format is ext4, due to its resilience against data loss if the card is ejected, or if there is an abrupt power loss. However, a third-party ext4 driver or application will be needed to access the file system from Windows. Most devices are supplied pre-formatted with vFAT.
- **Encrypt**: Encrypts data that is stored.
- **Decrypt**: Decrypt data that is stored.
- **Passphrase**: A passphrase is required for **Encrypt** and **Decrypt**.

Note

Not all tools are available for all file formats.

Maintenance

Restart: Restart the product if it is not behaving as expected. This does not affect any of the current settings.

Note

- Running applications restart automatically.

Restore: When you restore the product it returns **most** settings to the factory default values. This means that you must re-configure the product, reinstall any applications (ACAP's) and recreate any event types and PTZ presets.

System

> **NOTICE**
>
> Uploaded applications remain unchanged, but need a restart.
>
> **The only settings saved are:**
>
> - Boot protocol (DHCP or static)
> - Static IP address
> - Default router
> - Subnet mask
> - 802.1X settings
> - O3C settings

Factory default: When you make a default reset, **all** settings return to the factory default values. This means that you need to reset the IP address to make the product accessible.

- It is also possible to make a default reset using the **Control button** located in the product casing.

Firmware upgrade: From time to time, Axis releases new firmware for your product. These new releases can contain improved functionality, bug fixes, and completely new features. We recommend that you always use the latest release, which can be obtained from the Axis support web at *www.axis.com/support*.

- So that you can be sure you are only installing verified firmware on your product, all Axis product firmware is now digitally signed. This further increases the overall minimum cybersecurity level of Axis products. For more information, please see the white paper at *www.axis.com*.
- Axis product firmware is digitally signed as of version 8.30.1. For backwards compatibility your product will also still accept **unsigned** firmware up until the release of version 9.20.1, After updating to 9.20.1, signed firmware is fully activated and your product will then only accept firmware that is digitally signed by AXIS. This means that it will no longer be possible to downgrade to a firmware version earlier than 8.30.1. For more information and support on this subject, please contact the Axis helpdesk at *www.axis.com/support*.

Firmware recovery: Use this feature to go back to the previously installed firmware version.

Reports

View the device server report: Use this setting 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: Use this setting to download the server report. Downloading the server report 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. The server report .zip file should always be included when contacting support.

Download the crash report: Use this setting 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 may contain sensitive information such as network traces. The report may take several minutes to generate.

Logs

View the system log: Use this setting to show information about system events such as product startup, warnings and critical messages

View the access log: Use this setting to show all failed attempts to access the product, for example when a wrong login password is used.

Analytics data

We at Axis are continually updating and improving our products, and gathering anonymous browser data is of great value to us in this respect. Note that no personal data is gathered.

Network trace

The network trace file helps you troubleshoot when there are problems with the device or the network. When contact support always include a copy of the network trace.

Trace time: Select how long a time period the trace should gather data for, the trace should include a time that includes what you need to troubleshoot.

SSH server

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