Online help for product web interface EN

Web help

Online help for product web interface EN

Table of Contents

Browser support 3
Settings 4
. 4
Recorder status 5
. 5
Apps 6
About apps 6
System 7
Date and time 7
Network 7
Security 10
Users 11
Storage 11
Maintenance 12
SSH server 13

Online help for product web interface EN

Browser support

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/support/technical-notes/browser-support.*.

Online help for product web interface EN

Settings

Settings

Open or close the side menu.

Change the language.

Change the display between light theme or dark theme.

View which user is logged in and the rights of the user.

Click for the following:

- **About**: View information about this device and manufacturer.

Important

You will find the firmware version in use here.

- **Analytics data**: Share non-personal browser data with Axis Communications AB. This helps us improve the application and your user experience. This will download and run Google Analytics..
- **Feedback**: Help us to improve and share your experience.

Important

If you have questions or need help with your Axis device, contact us at *axis.com/support*.

- **Legal**: View information about cookies and licenses.
- **Help**: Access the latest help about the device interface (internet connection required).

Recorder status

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

Apps

Add app: Click to install a new app.

Status

- **Running**: The app is up and running.
- **Idle**: The app has been started, but no event trigger has been configured for the app. The Idle status is dependent on the type of app installed and is not used in all apps. You find more information in the manual for the specific app.
- **Stopped**: The app is not running.

Start and stop: Start or stop the app.

Delete: If you delete the app, you remove it completely from the device.

App log: The app log generates a log of the app events. This log is helpful when you contact support.

Activate the license: Without an activated license, the device can't run the app. 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 *axis.com/applications*. You need the license code and the Axis device 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 device. This means that if you deactivate the license, you also remove it from the device.

Settings: To configure the app, click **Open**. The available settings depend on the type of app. It's not available for all apps. For details, see the manual for the specific app.

About apps

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

To see a list of apps that are installed on your device, go to **Apps**.

You must be an administrator to install apps.

You can install apps and licenses on multiple devices at the same time using AXIS Camera Management, version 3.10 and later.

Note

- Several apps can run at the same time but some apps might not be compatible with each other. Certain combinations of apps might require too much processing power or memory resources when run in parallel. Before you deploy, verify that the apps work together.
- If you upgrade an app the settings, including the license, is removed. You must then reinstall the license and reconfigure the app.

Online help for product web interface EN

System

System

Date and time

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

Synchronization: Set which synchronization method to use, automatic or manual:

- **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 device 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. Use **Get from system** to get a single update from the system's date and time.

Note

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

Network

IPv4 and IPv6

There are currently two IP versions: IP version 4 (IPv4) and IP version 6 (IPv6).

Automatic IP (DHCP) and **DNS (DHCP)**: The default setting and the recommended setting for most networks. Current settings are listed, all update automatically.

Automatic IP (DHCP) and **manual DNS**: Contact your network administrator to configure manually. Current settings are listed, configure the following settings manually:

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

  Click + **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.

  Click + **Add DNS server** to add more DNS servers.

Manual IP (DHCP) and **DNS**: Contact your network administrator to configure manually.

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

  Click + **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.

  Click + **Add DNS server** to add more DNS servers.

Assign IPv6 automatically: By default, this setting is selected.

HTTP and HTTPS

Allow access through: Select if a user is allowed to connect to the device through:

- **HTTP**
- **HTTPS**
- **HTTP and HTTPS**

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 device, you must install an HTTPS certificate. 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.

Certificate: Select a certificate. The default setting is **Default (self-signed)**.

Friendly name

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

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

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

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

One-Click Cloud Connect

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**: The default setting. Press and hold the control button to connect to an O3C service over the Internet. Once registered, **Always** is enabled and your Axis device stays connected to the O3C service. If you don't register your Axis device within 24 hours from when the control button was pressed, the Axis device disconnects from the O3C service.
- **Always**: The Axis device constantly attempts to connect to an O3C service over the Internet. Once registered the device stays connected to the O3C service. Use this option if the control button is out of reach.
- **No**: Disables the O3C services.

Host and **Port**: If needed, enter the proxy settings and port number to connect to the HTTP server.

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 as it sends the username and password unencrypted to the server.

- **Digest**: This method is more secure than the **Basic** method since it always transfers the password across the network encrypted.
- **Auto**: This option enables the Axis device to select the authentication method automatically depending on the methods supported. It prioritizes the **Digest** method over the **Basic** method.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. An SNMP community is the group of devices and management station running SNMP. Community names are used to identify groups.

SNMP

Select the version of SNMP to use.

Read community: Specify the community name that has read-only access to all supported SNMP objects. The default value is **public**.

Write community: Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is **write**.

Activate traps: Select this to activate trap reporting.
Traps are used by the device to send messages to a management system for important events or status changes.
Trap settings are for use with SNMP v1/v2c and cannot be used when SNMP v3 is enabled. When using SNMP v3, set up traps through the SNMP v3 management application.

Trap address: Enter the IP address of the management server.

Trap community: Enter the community to use when sending a trap message to the management system.

Available traps

Cold start: Sends a trap message when SNMP has started, and when both the configuration and the MIB (Management Information Base) may have changed

Warm start: Sends a trap message when SNMP has started and the configuration file has changed, but not the MIB

Link up: Sends a trap message when a link changes from down to up

Authentication failed: Sends a trap message when an authentication attempt fails

Note

All AXIS Video MIB traps are enabled when enabling SNMP v1/v2c traps. For more information, see www.axis.com/techsup/.

SNMP v3

SNMP v3 is a more secure version, providing encryption and secure passwords. To use SNMP v3, it is recommended to activate HTTPS, as the password will then be sent via HTTPS. This also prevents unencrypted SNMP v1/v2c traps being accessed by unauthorized parties. SNMP v3 traps are set up through the SNMP management application.

Enable SNMP v3: Select this to activate SNMP v3. HTTPS should also be activated.

Traps will automatically be disabled when activating v3 or when turning off SNMP. No user action required.

SNMP v3 Initial user's password: Enter the SNMP password for the account named 'initial'. Although the password can be sent without enabling HTTPS, this is not recommended.

The SNMP v3 password can only be set once, and preferably only when HTTPS is enabled.

Once the password has been set, the password field will no longer be displayed. To set the password again, the product must be reset to the factory default settings.

Connected clients

System

Expand this section to see the current settings.

Update: Refresh the list.

Security

Certificates

Certificates are used to authenticate devices on a network. The Axis device can use two types of certificate:

- **Client certificates**
  A client certificate identifies the Axis device, 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 Axis device connects to a network protected by IEEE 802.1X. The Axis 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

Note

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

: Search for specific certificates in the list.

Add certificate : Click to add a certificate. You've several options:

- **Create a self-signed certificate and certificate signing request**
- **Upload a client-server certificate using a signing request**
- **Upload a client-server certificate using a private key (PKCS#12)**
- **Upload a client-server certificate using a separate private key**
- **Upload a CA certificate**

Provide the requested information and 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).

Certificate information: View an installed certificate's properties.

Delete certificate: Remove the certificate.

Create certificate signing request: TBA

Custom-signed firmware certificate

Online help for product web interface EN

System

Install: Click to install the custom-signed firmware. You should do this before you upgrade.

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.

While secure boot makes the product safer, it does also reduce the flexibility with different firmware. This makes it more complicated to load any temporary firmware, such as test firmware or other custom firmware from Axis, into the device. 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

+ **Add user**: Add a new user.

Update user: Select a user in the list to modify its properties.

Delete user: Select a user in the list to delete it.

Username: Enter a unique username.

New password: Enter a password for the user. Passwords can have 1 to 64 characters. 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: Select a user type.

- **Viewers**: Have access to the live view only.
- **Operators**: Have access to all settings except:
  - All **System** settings.
  - Upload apps and language files
- **Administrators**: Have unrestricted access to all settings. They can also create, edit and remove other users.

NOTICE

The maximum number of users is 100.

Storage

Onboard storage

Onboard storage means that the video is recorded and stored directly on the device.

⚠WARNING

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

Unmount: Click to safely remove the onboard storage device.

Write protect: Turn on to stop writing to the SD card and protect recordings from being removed. A locked storage unit can't be formatted.

Auto format: SD cards are normally pre-formatted with the file system vFAT. If you select **Auto format**, the device checks the current file system and then formats the storage device into the ext4 file system if required. We recommend to use ext4 as it is a more reliable file system.

Tools:

- **Check**: Check for errors on the SD card. This only works for the ext4 file system.
- **Repair**: Repair 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**: Format the storage device, for example when you need to change the file system or quickly erase all 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**: Encrypt data that is stored.
- **Decrypt**: Decrypt data that is stored.
- **Password**: A password is required for **Encrypt** and **Decrypt**.

Note

Not all tools are available for all file formats.

Maintenance

Restart: Restart the device. This does not affect any of the current settings.

Note

Running applications restart automatically.

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

NOTICE

Uploaded apps 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: Reset the device to factory default settings. When you make a factory default reset, *all* settings return to the factory default values. This means that you need to reset the IP address to make the device accessible. You can also make a default reset using the CONTROL BUTTON on the device casing.

Firmware upgrade: New firmware releases may contain improved functionality, bug fixes, and completely new features. We recommend that you always use the latest release. Go to *axis.com/support* to download the latest release.

- To be sure that you only install verified firmware on your device, all Axis device firmware is digitally signed. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper at *axis.com*.
- Axis device firmware is digitally signed as of version 8.30.1. For backwards compatibility your device 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 device will 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, contact Axis helpdesk at *axis.com/support*.

Firmware rollback: Revert back to the previously installed firmware version.

System

SSH server

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

Web help
Online help for product web interface EN

Ver. M5.2
Date: July 2020
Part No.