



AXIS T8705 Video Decoder User Manual

[Home](#) » [AXIS](#) » **AXIS T8705 Video Decoder User Manual** 

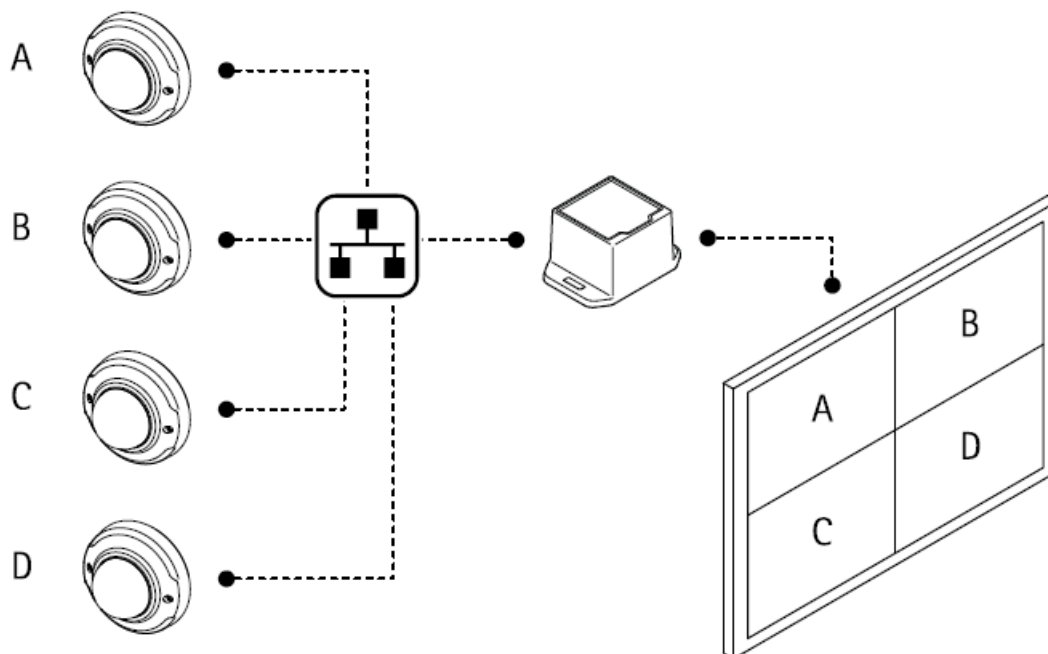
Contents

- [1 AXIS T8705 Video Decoder](#)
- [2 Solution overview](#)
- [3 Get started](#)
- [4 Webpage overview](#)
- [5 Configure your device](#)
- [6 The device interface](#)
- [7 Status](#)
- [8 Display](#)
- [9 System](#)
- [10 Network](#)
- [11 HTTP and HTTPS](#)
- [12 Security](#)
- [13 Logs](#)
- [14 Maintenance](#)
- [15 Streaming and storage](#)
- [16 Troubleshooting](#)
- [17 Firmware options](#)
- [18 Upgrade the firmware](#)
- [19 Specifications](#)
- [20 Buttons](#)
- [21 Documents / Resources](#)
 - [21.1 References](#)
- [22 Related Posts](#)





Solution overview



Get started

Find the device on the network

- To find Axis devices on the network and assign them IP addresses in Windows®, use AXIS IP Utility or AXIS Device Manager. Both applications are free and can be downloaded from axis.com/support.
- For more information about how to find and assign IP addresses, go to [How to assign an IP address and access your device](#).

Browser support

You can use the device with the following brows

	Chrome™	Firefox®	Edge™	Safari®
Windows®	recommended	recommended		
macOS®	recommended	recommended		
Linux®	recommended	recommended		
Other operating systems				*

To use AXIS OS web interface with iOS 15 or iPadOS 15, go to Settings > Safari > Advanced > Experimental Features and disable NSURLConnection Websocket.

Open the device's webpage

1. Open a browser and enter the IP address or host name of the Axis device. If you do not know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Enter the username and password. If you access the device for the first time, you must set the root password.
See Set a new password for the root account on page 4

Set a new password for the root account

The default administrator username is root. There's no default password for the root account. You set a password the first time you log in to the device.

1. Type a password. Follow the instructions about secure passwords. See Secure passwords on page 4 .
2. Retype the password to confirm the spelling.
3. Click Add user.

Important

If you lose the password for the root account, go to Reset to factory default settings on page 17 and follow the instructions.

Secure passwords

Axis devices send the initially set password in clear text over the network. To protect your device after the first login, set up a secure and encrypted HTTPS connection and then change the password. The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

To protect your data we strongly recommend that you

- Use a password with at least 8 characters, preferably created by a password generator.
- Don't expose the password.
- Change the password at a recurring interval, at least once a year.

Webpage overview

This video gives you an overview of the device interface

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

help.axis.com/?&piald=41938§ion=webpage-overview

Axis device web interface

Configure your device

Add multiple cameras

The camera wizard only works with Axis cameras. You must add cameras from other brands one by one, see Add a camera on page 6 .

1. Go to Video sources.
2. Click Add video sources and select the method Step-by-step.
3. Click Next.

The wizard searches the network for Axis cameras.

4. Click Add credentials and enter Name, Username and Password. Click Save.

The decoder needs usernames and passwords to the cameras to access the video streams. The decoder can have multiple credentials saved. It will try to access all cameras using all of the stored credentials.

5. Click Next.
6. Select the cameras you want to add and click Save.

The decoder will try to access the camera with all saved credentials. To access more settings for the cameras, see Advanced camera settings on page 7 .

Add a camera

1. Go to Video sources.
2. Click Add video sources and select the method Manual.
3. Click Next.
4. Select a video source type and click Next.
5. Enter the configuration details.
 1. For an Axis camera: Enter a name, IP address, username and password for the camera.
 2. For other brands: Enter a name, a URL that can be used to access the video stream, the camera's username and password, and the codec used for the stream.
6. Click Save.

To access more settings for the cameras

Configure a monitor


1. Go to Display.
2. Select one of these options under Multi mode:
 1. To show the video sources one at a time in sequence, select Sequencer, and set the interval that each

source is displayed.


2. To show multiple video sources at the same time, select Multiview, and select a layout.
3. Under Video output, select a resolution and refresh rate that works with your display. See the documentation for your display.

Advanced camera settings

After you've added a camera, you can access more camera settings from the Edit view.

1. Go to Video sources.
2. Select a video source.
3. Click  and then click Edit video source.

Remove a camera

1. Go to Video sources.
2. Find the camera you want to remove.
3. Click  and then click Delete video source.

Upgrade your device to firmware version 6.0.x

To upgrade your device to V6.0.x you must first upgrade it to V5.1.8.5. You need the following files:

- Firmware T8705_V5.1.8.5.bin (bridge firmware)
- Firmware T8705_V6.0.x.bin

Go to Maintenance > Firmware upgrade and click Upgrade. Follow the instructions.








- Un upgrade from V5.1.8.2 or V5.1.8.4 to V5.1.8.5 takes approximately 10 minutes.
- Un upgrade from V5.1.8.5 to V6.0.x takes approximately 15 minutes.

If the firmware upgrade failed

1. Send a report to axis.com/support. Include information about the device's MAC address in the report.
2. Unzip the included wic file (decoder-image-prod-6.0.x.wic.gz) and save it to an SD card.
3. Insert the SD card into an SD card reader. Open the file and follow the instructions to upgrade the firmware with the wic file.

The device interface

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

-  Show or hide the main menu.
-  Access the product help.
-  Change the language.
-  Set light theme or dark theme
-  The user menu contains:
 - Information about the user who is logged in.
 -  **Change user** : Log out the current user and log in a new user.
 -  **Log out** : Log out the current user.

The context menu contains

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

Status

- **RAM use**: Percentage of RAM that's used.
- **CPU use**: Percentage of CPU that's used.
- **GPU use**: Percentage of GPU that's used.
- **GPU bus use**: Percentage of GPU bus that's used.
- **Decoding process**: Current status of the decoding process, Running or Stopped.
- **IP address**: The device's IP address.
- **Date and time**: The device's date and time

The device interface Video sources

- **Name**: The video source's name.
- **Type**: The video source's type, Axis or Generic.
- **Add video sources**: Create a new video source. You can use two different methods:
- **Step-by-step**: Add an Axis device with help from a wizard.
- **Manual**: Add any device manually.



- The context menu contains:
 - **Edit video source**: Edit the properties of the video source
 - **Delete video source**: Delete the video source

Display



Click to configure the sequence order. With the sequence you can decide in which order you want to see the different views.

Click to add a new view. You can add as many views as you like.

Start sequence: Click to turn on the sequence.

View settings:

- **Name:** Enter a nice name of the view.
- **Duration:** Decide how long the view will be displayed in a sequence.
- **Layout:** Select a screen layout, then decide where each device should be displayed.

Resolution: Select which resolution you want to use for the view

Jobs

- Add job: Click to add a new job.
- Name: Enter a unique name for the job.
- Type: Select a type.
 - Restart decoding: Restarts the decoding at a certain time.
 - Reboot system: Reboots the system at a certain time.
 - NTP sync: Re-synchronize the NTP server at a certain time.
- **Recurrence:** Select when the system should run the job.
 - Minutely: The system runs the job at a certain interval, for example every 15th min.
 - Hourly: The system runs the job at a certain interval, for example every second hour and 15th min.
 - Daily: The system runs the job everyday at a certain interval.
 - Weekdays: The system runs the job a certain day at a certain interval.

The context menu contains:

- Delete the job.

System

Date and time

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

Note

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

- **Synchronization:** Select an option for synchronizing the device's date and time.
- **Automatic date and time (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.
- **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.
- **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.
- **Custom date and time:** Manually set the date and time. Click Get from system to fetch the date and time settings once from your computer or mobile device.
 - **Time zone:** Select which time zone to use. Time will be automatically adjusted for daylight saving time and standard time.

Note

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

Network

IPv4

- **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 to 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.

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 Hostname is used in the server report and in the system log. Allowed characters are A–Z, a–z, 0–9 and -.

DNS servers

- **Assign DNS automatically:** Select to let the network router 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 used by the device.
- **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

HTTP and HTTPS

- **Allow access through:** Select if a user is allowed to connect to the device through the HTTP, HTTPS, or both HTTP and HTTPS protocols.

HTTPS is a 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.

To use HTTPS on the device, you must install an HTTPS certificate. Go to System > Security to create and install certificates.

Note

If you view encrypted web pages through HTTPS, you might experience a drop in performance, especially when you request a page for the first time.

- **HTTP port:** Enter the HTTP port to use. Port 80 or any port in the range 1024-65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1-1023. If you use a port in this range, you get a warning.
- **HTTPS port:** Enter the HTTPS port to use. Port 443 or any port in the range 1024-65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1-1023. If you use a port in this range, you get a warning.
- **Certificate:** Select a certificate to enable HTTPS for the device.

Friendly name

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

- **Bonjour name:** Enter a friendly name to be visible on the network. The default name is the device name and MAC address.
- **Use UPnP®:** Turn on to allow automatic discovery on the network.
- **UPnP name:** Enter a friendly name to be visible on the network. The default name is the device name and MAC address

Security

Certificates

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




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

These formats are supported:

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

Important

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

-  Filter the certificates in the list.
-  Add certificate : Click to add a certificate.
-  The context menu contains:
 1. **Certificate information:** View an installed certificate's properties.
 - Delete certificate:** Delete the certificate.
 - Create certificate signing request:** Create a certificate signing request to send to a registration authority to apply for a digital identity certificate

IEEE 802.1x

- IEEE 802.1x is an IEEE standard for port-based network admission control providing secure authentication of wired and wireless network devices. IEEE 802.1x is based on EAP (Extensible Authentication Protocol).
- To access a network protected by IEEE 802.1x, network devices must authenticate themselves. The authentication is performed by an authentication server, typically a RADIUS server (for example FreeRADIUS

and Microsoft Internet Authentication Server).

Certificates

- When configured without a CA certificate, server certificate validation is disabled and the device tries to authenticate itself regardless of what network it is connected to.
- When using a certificate, in Axis' implementation, the device and the authentication server authenticate themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).
- To allow the device to access a network protected through certificates, a signed client certificate must be installed on the device
- **Client certificate:** Select a client certificate to use IEEE 802.1x. The authentication server uses the certificate to validate the client's identity.
CA certificate: Select a CA certificate to validate the authentication server's identity. When no certificate is selected, the device tries to authenticate itself regardless of what network it is connected to.
- **EAP identity:** Enter the user identity associated with the client certificate.
- **EAPOL version:** Select the EAPOL version that is used in the network switch.
- **Use IEEE 802.1x:** Select to use the IEEE 802.1x protocol

Users

- **Add user:** Click to add a new user. You can add up to 100 users.
- **Username:** Enter a unique username.
- **New password:** Enter a password for the user. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example letters, numbers, punctuation, and some symbols.
- **Repeat password:** Enter the same password again.

Role:

- **Administrator:** Has full access to all settings. Administrators can also add, update, and remove other users.
- **Operator:** Has access to all settings except:
 - All System settings.
- **Viewer:** Has access to:
 - Status
 - Display



The context menu contains:

- **Update user:** Edit the user's properties.
- **Delete user:** Delete the user. You can't delete the root user

Logs

Reports and logs

• Reports

- View the device server report: Click to show information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.
- Download the device server report: Click to download the server report. It creates a .zip file that contains a complete server report text file in UTF-8 format, as well as a snapshot of the current live view image. Always include the server report .zip file when you contact support.

• Logs

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

Plain config

Plain config is for advanced users with experience of Axis device configuration. Most parameters can be set and edited from this page.

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 recreate any events and PTZ presets.

Important

The only settings saved after restore are:

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

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

Note

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

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

When you upgrade, you can choose between three options:

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

Configuration

- **Download configuration file:** Select which settings you want to include in the configuration file. The file won't include certificates or private keys.
- **Upload configuration file:** The uploaded configuration file overwrites the existing configuration within the same area.
- **For example:** if your file only contains information about video, the system settings won't be affected. The configuration file doesn't include certificates or private keys. If you want other certificates than the default self-signed ones, you need to set them manually

Streaming and storage

Video compression formats

Decide which compression method to use based on your viewing requirements, and on the properties of your network. The available options are:

Motion JPEG

- Motion JPEG, or MJPEG, is a digital video sequence that is made up of a series of individual JPEG images. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion. For the viewer to perceive motion video the rate must be at least 16 image frames per second. Full motion video is perceived at 30 (NTSC) or 25 (PAL) frames per second.
- The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream.

H.264 or MPEG-4 Part 10/AVC

Note

- H.264 is a licensed technology. The Axis product includes one H.264 viewing client license. To install additional unlicensed copies of the client is prohibited.
- To purchase additional licenses, contact your Axis reseller.
- H.264 can, without compromising image quality, reduce the size of a digital video file by more than 80% compared to the Motion JPEG format and by as much as 50% compared to older MPEG formats.
- This means that less network bandwidth and storage space are required for a video file. Or seen another way, higher video quality can be achieved for a given bitrate

Troubleshooting

Reset to factory default settings

Use the reset to factory default function with caution. A reset to factory default resets all settings, including the IP address, to the factory default values.

1. Go to Maintenance > Factory default.
2. Click Default.
3. Click Restore all.

It is also possible to reset parameters to factory default with the restart button. With the device turned on, press and hold the restart button for 10 seconds.

Firmware options

- Axis offers product firmware management according to either the active track or the long-term support (LTS) tracks. Being on the active track means continuously getting access to all the latest product features, while the LTS tracks provide a fixed platform with periodic releases focused mainly on bug fixes and security updates.
- Using firmware from the active track is recommended if you want to access the newest features, or if you use Axis end-to-end system offerings. The LTS tracks are recommended if you use third-party integrations, which are not continuously validated against the latest active track. With LTS, the products can maintain cybersecurity without introducing any significant functional changes or affecting any existing integrations. For more detailed information about Axis product firmware strategy, go to axis.com/support/firmware.

Check the current firmware version

Firmware is the software that determines the functionality of network devices. When you troubleshoot a problem, we recommend you to start by checking the current firmware version. The latest firmware version might contain a correction that fixes your particular problem.

To check the current firmware:

1. Go to the device interface > Status.
2. See the firmware version under Device info

Upgrade the firmware

Important

Preconfigured and customized settings are saved when you upgrade the firmware (provided that the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.

Important

Make sure the device remains connected to the power source throughout the upgrade process.

Note

When you upgrade the device with the latest firmware in the active track, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before you upgrade the firmware. To find the latest firmware and the release notes, go to axis.com/support/firmware.

1. Download the firmware file to your computer, available free of charge at axis.com/support/firmware
2. Log in to the device as an administrator.
3. Go to Maintenance > Firmware upgrade and click Upgrade

When the upgrade has finished, the product restarts automatically.

You can use AXIS Device Manager to upgrade multiple devices at the same time. Find out more at axis.com/products/axis-device-manager.

Technical issues, clues, and solutions

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

Performance considerations

Problems upgrading the firmware

Firmware upgrade failure	If the firmware upgrade fails, the device reloads the previous firmware. The most common reason is that the wrong firmware file has been uploaded. Check that the name of the firmware file corresponds to your device and try again.
Problems after firmware upgrade	If you experience problems after a firmware upgrade, roll back to the previously installed version from the Maintenance page.

Problems setting the IP address

The device is located on a different subnet	If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you cannot set the IP address. Contact your network administrator to obtain an IP address.
The IP address is being used by another device	<p>Disconnect the Axis device from the network. Run the ping command (in a Command/DOS window, type <code>ping</code> and the IP address of the device):</p> <ul style="list-style-type: none"> • If you receive: <code>Reply from <IP address>: bytes=32; time=10...</code> this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device. • If you receive: <code>Request timed out</code>, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.
Possible IP address conflict with another device on the same subnet	The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the device.

The device can't be accessed from a browser

Can't log in	<p>When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type <code>http</code> or <code>https</code> in the browser's address field.</p> <p>If the password for the user root is lost, the device must be reset to the factory default settings. See <i>Reset to factory default settings on page 17</i>.</p>
The IP address has been changed by DHCP	<p>IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).</p> <p>If required, a static IP address can be assigned manually. For instructions, go to axis.com/support.</p>
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to System > Date and time .

The following factors are the most important to consider

- High image resolution or lower compression levels result in images containing more data which in turn affects the bandwidth.
- Access by large numbers of Motion JPEG or unicast H.264 clients affects the bandwidth.
- Simultaneous viewing of different streams (resolution, compression) by different clients affects both frame rate

and bandwidth.

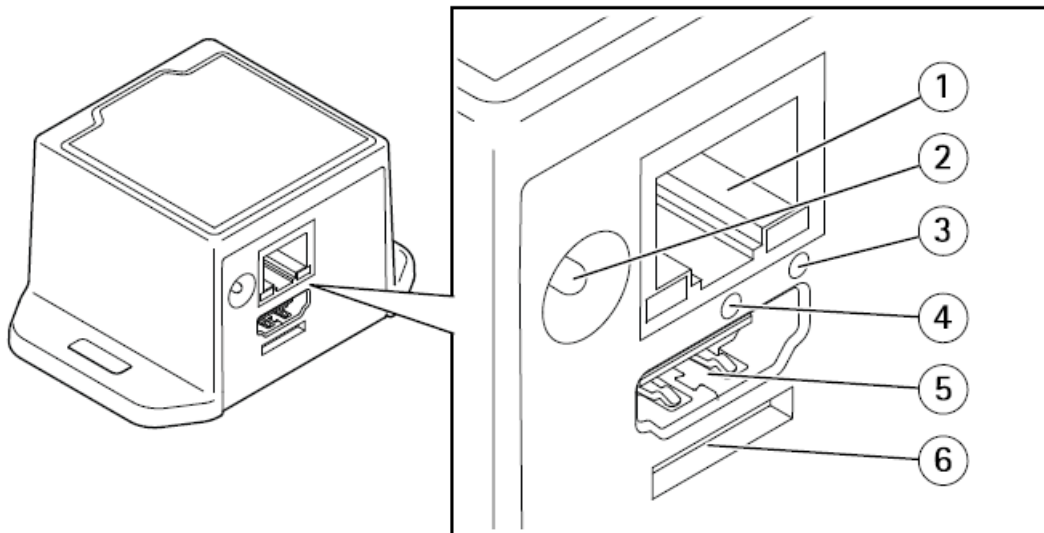
- Use identical streams wherever possible to maintain a high frame rate. Stream profiles can be used to ensure that streams are identical.
- Accessing Motion JPEG and H.264 video streams simultaneously affects both frame rate and bandwidth.
- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.
- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.
- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Viewing on poorly performing client computers lowers perceived performance and affects frame rate.

Contact support

- Contact support at axis.com/support.

Specifications

Product overview



1. Network connector
2. Power connector
3. Network LED
4. Restart button
5. HDMI connector
6. Reserved for operating system

LED

Network LED	Indication
Red	Flashes for network activity.
Unlit	No network connection.

Buttons

Control button

- **The control button is used for:**
 - Resetting the product to factory default settings. See Reset to factory default settings on page 17.

Connectors

- **HDMI connector**
 - Use the HDMI connector to connect a display or public view monitor.
- **Network connector**
 - RJ45 Ethernet connector
- **Power connector**
 - DC connector. Use the supplied adapter

User Manual Ver. M2.12

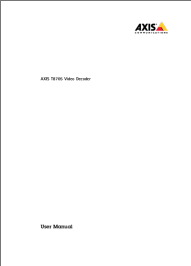
AXIS T8705 Video

Decoder Date: October 2022

© Axis Communications AB, 2017 – 2022

Part No. T10110349

Documents / Resources

	AXIS T8705 Video Decoder [pdf] User Manual T8705 Video Decoder, T8705, T8705 Decoder, Video Decoder, Decoder
---	---

References

- [Axis Communications - Leader in network cameras and other IP networking solutions | Axis Communications](#)
- [AXIS Device Manager | Axis Communications](#)
- [Welcome to Axis support | Axis Communications](#)
- [Firmware | Axis Communications](#)
- [AXIS T8705 Video Decoder User manual](#)