

AXIS A1210 Network Door Controller

AXIS A1210-B Network Door Controller

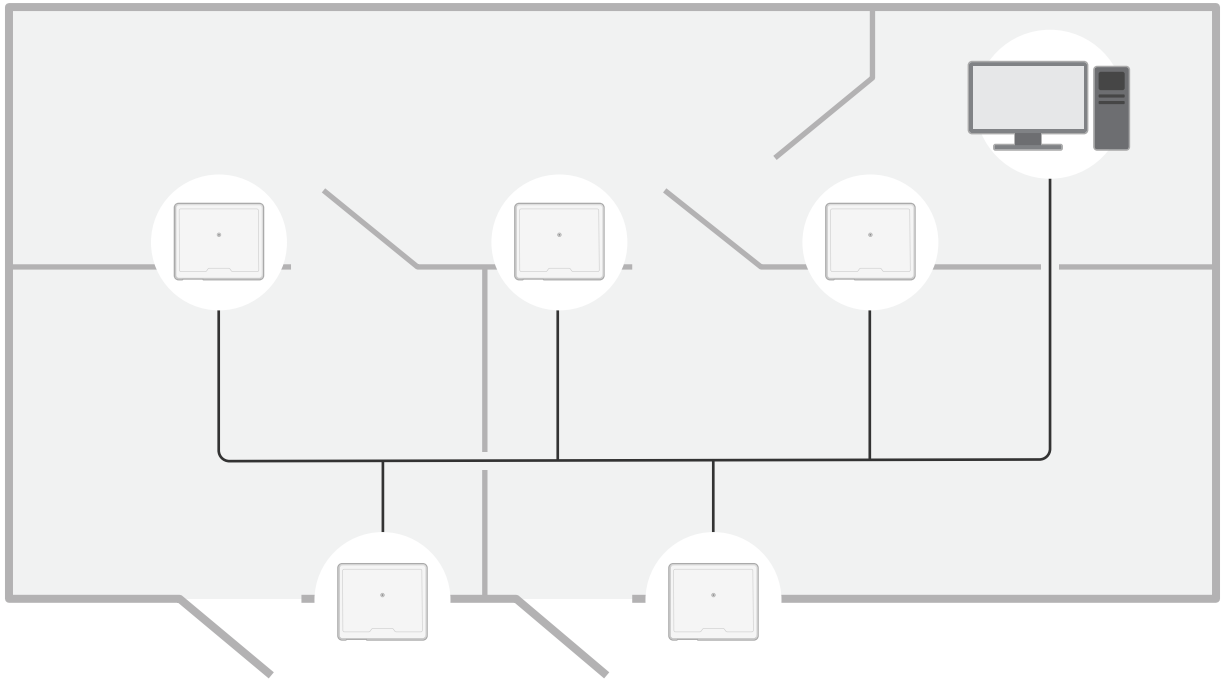
User manual

Table of Contents

| | |
|---|----|
| Solution overview | 3 |
| Installation | 5 |
| Get started | 6 |
| Find the device on the network | 6 |
| Open the device's web interface | 6 |
| Create an administrator account | 6 |
| Secure passwords | 6 |
| Verify that no one has tampered with the firmware | 7 |
| Web interface overview | 7 |
| Configure your device | 8 |
| The web interface | 9 |
| Status | 9 |
| Access control | 10 |
| System | 10 |
| Maintenance | 20 |
| Learn more | 21 |
| Cybersecurity | 21 |
| Specifications | 22 |
| Product overview | 22 |
| LED indicators | 22 |
| Buttons | 23 |
| Connectors | 23 |
| Troubleshooting | 29 |
| Reset to factory default settings | 29 |
| Firmware options | 29 |
| Check the current firmware version | 29 |
| Upgrade the firmware | 29 |
| Technical issues, clues, and solutions | 30 |
| Contact support | 31 |

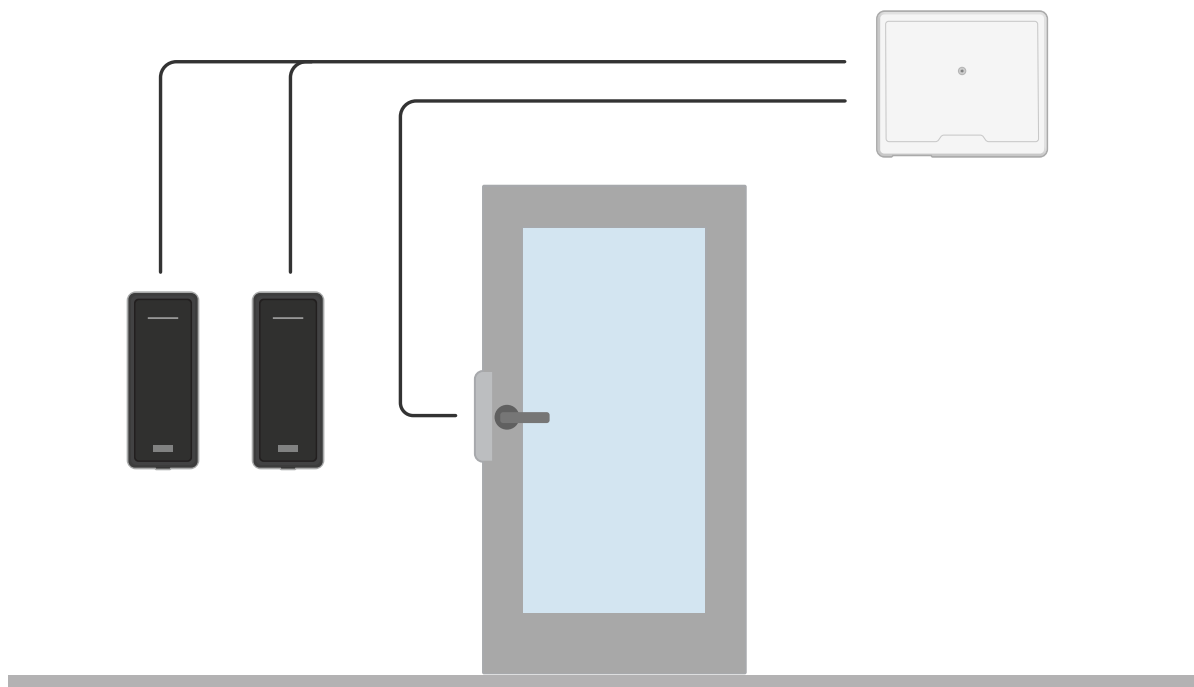
Solution overview

Solution overview



The network door controller can easily be connected to and powered by your existing IP network with no need for special cabling.

Solution overview



Each network door controller is an intelligent device that is easily mounted close to a door. It can power and control up to two readers.

Installation



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

help.axis.com/?etpiald=74266&tsection=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 browsers:

| | 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 *NSURLSession Websocket*.

If you need more information about recommended browsers, go to *AXIS OS Portal*.

Open the device's web interface

1. Open a browser and type 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. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account on page 6*.

Create an administrator account

The first time you log in to your device, you must create an administrator account.

1. Enter a username.
2. Enter a password. See *Secure passwords on page 6*.
3. Re-enter the password.
4. Click **Add user**.

Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings on page 29*.

Secure passwords

Important

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.

Verify that no one has tampered with the firmware

To make sure that the device has its original Axis firmware, or to take full control of the device after a security attack:

1. Reset to factory default settings. See *Reset to factory default settings on page 29*.

After the reset, secure boot guarantees the state of the device.

2. Configure and install the device.

Web interface overview

This video gives you an overview of the device's web interface.



To watch this video, go to the web version of this document.
help.axis.com/?&pid=74266§ion=web-interface-overview

Axis device web interface

Configure your device

Configure your device


For how to configure your device, see *AXIS Camera Station user manual* or third-party solutions.












The web interface

The web interface

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

Note

Support for the features and settings described in this section varies between devices. This icon  indicates that the feature or setting is only available in some devices.

-  Show or hide the main menu.
-  Access the release notes.
-  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 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 firmware version and serial number.
 - Legacy device interface**: Change the device's web interface to the legacy version.

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 **Date and time** page where you can change the NTP settings.

Device info

Shows the device information, including firmware version and serial number.

Upgrade firmware: Upgrade the firmware on your device. Takes you to the **Maintenance** page where you can do a firmware upgrade.

Access control

Alarms

Device motion: Turn on to trigger an alarm in your system when it detects a movement of the door controller.

Casing open: Turn on to trigger an alarm in your system when it detects an open door controller case. Turn off this setting for barebone door controllers..

External tamper: Turn on to trigger an alarm in your system when it detects an external tamper. For example, when someone opens or closes the external cabinet.

- **Supervised input:** Turn on to monitor the input state and configure the end-of-line resistors.
 - To use parallel first connection, select **Parallel first connection with a 22 K Ω parallel resistor and a 4.7 K Ω serial resistor.**
 - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.

Peripherals

Upgrade readers: Click to upgrade readers to a new firmware version. The feature can only upgrade supported readers when they are online.

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

Note

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

Network

IPv4

The web interface

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 -.

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.

HTTP and HTTPS

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.

The web interface

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

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. The device allows port 80 or any port in the range 1024-65535. 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. The device allows port 443 or any port in the range 1024-65535. 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.

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.

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

Proxy settings: If needed, enter the proxy settings to connect to the 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.
 - **Warm start:** Sends a trap message when you change an SNMP setting.
 - **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 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.

Connected clients

Shows the number of connections and connected clients.

View details: View and update the list of the connected clients. The list shows IP address, protocol, port, and PID/Process of each client.

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.

- More  : Show more fields to fill in or select.
- Secure keystore: Select to use **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/en-us/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  :

- **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.

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, you must install a signed client certificate 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 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.

Prevent brute-force attacks

The web interface

Blocking: Turn on to block brute-force attacks. A brute-force attack uses trial-and-error to guess login info or encryption keys.

Blocking period: Enter the number of seconds to block a brute-force attack.

Blocking conditions: Enter the number of authentication failures allowed per second before the block starts. You can set the number of failures allowed both on page level and device level.

IP address filter

Use filter: Select to filter which IP addresses are allowed to access the device.

Policy: Choose whether to **Allow** or **Deny** access for certain IP addresses.

Addresses: Enter the IP numbers that are either allowed or denied access to the device. You can also use the CIDR format.

Custom-signed firmware certificate

To install test firmware or other custom firmware from Axis on the device, you need a custom-signed firmware certificate. The certificate verifies that the firmware is approved by both the device owner and Axis. The firmware can only run on a specific device which is identified by its unique serial number and chip ID. Only Axis can create custom-signed firmware 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 firmware.

Accounts

Accounts



Add account: Click to add a new account. You can add up to 100 accounts.

Account: Enter a unique account name.

New password: Enter a password for the account. 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.

Privileges:

- **Administrator:** Has full access to all settings. Administrators can also add, update, and remove other accounts.
- **Operator:** Has access to all settings except:
 - All **System** settings.
 - Adding apps.
- **Viewer:** Doesn't have access to change any settings.



The context menu contains:

Update account: Edit the account properties.

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

MQTT

MQTT (Message Queuing Telemetry Transport) is a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth. The MQTT client in Axis device firmware can simplify integration of data and events produced in the device to systems which are not video management software (VMS).

Set up the device as an MQTT client. MQTT communication is based on two entities, the clients and the broker. The clients can send and receive messages. The broker is responsible for routing messages between clients.

You can learn more about MQTT in *AXIS OS Portal*.

ALPN

ALPN is a TLS/SSL extension that allows for the selection of an application protocol during the handshake phase of the connection between the client and server. This is used to enable MQTT traffic over the same port that is used for other protocols, such as HTTP. In some cases, there might not be a dedicated port open for MQTT communication. A solution in such cases is to use ALPN to negotiate the use of MQTT as the application protocol on a standard port, allowed by the firewalls.

MQTT client

Connect: Turn on or off the MQTT client.

Status: Shows the current status of the MQTT client.

Broker

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

Protocol: Select which protocol to use.

Port: Enter the port number.

- 1883 is the default value for **MQTT over TCP**
- 8883 is the default value for **MQTT over SSL**
- 80 is the default value for **MQTT over WebSocket**
- 443 is the default value for **MQTT over WebSocket Secure**

ALPN protocol: Enter the ALPN protocol name provided by your MQTT broker provider. This is only applicable with MQTT over SSL and MQTT over WebSocket Secure.

Username: Enter the username that the client will use to access the server.

Password: Enter a password for the username.

Client ID: Enter a client ID. The client identifier is sent to the server when the client connects to it.

Clean session: Controls the behavior at connection and disconnection time. When selected, the state information is discarded at connect and disconnect.

Keep alive interval: Enables the client to detect when the server is no longer available without having to wait for the long TCP/IP timeout.

Timeout: The time interval in seconds to allow a connect to complete. Default value: 60

Device topic prefix: Used in the default values for the topic in the connect message and LWT message on the **MQTT client** tab, and in the publication conditions on the **MQTT publication** tab.

Reconnect automatically: Specifies whether the client should reconnect automatically after a disconnect.

Connect message

Specifies if a message should be sent out when a connection is established.

The web interface

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this Topic

QoS: Change the QoS layer for the packet flow.

Last Will and Testament message

The Last Will Testament (LWT) lets a client provide a testament along with its credentials when connecting to the broker. If the client disconnects ungracefully at some point later (maybe because his power source died), it can let the broker deliver a message to other clients. This LWT message has the same form as an ordinary message and gets routed via the same mechanics.

Send message: Turn on to send messages.

Use default: Turn off to enter your own default message.

Topic: Enter the topic for the default message.

Payload: Enter the content for the default message.

Retain: Select to keep the state of client on this Topic

QoS: Change the QoS layer for the packet flow.

MQTT publication

Use default topic prefix: Select to use the default topic prefix, that is defined in the device topic prefix in the MQTT client tab.

Include topic name: Select to include the topic that describes the condition in the MQTT topic.

Include topic namespaces: Select to include ONVIF topic namespaces in the MQTT topic.

Include serial number: Select to include the device's serial number in the MQTT payload.



Add condition: Click to add a condition.

Retain: Defines which MQTT messages are sent as retained.

- **None:** Send all messages as non-retained.
- **Property:** Send only stateful messages as retained.
- **All:** Send both stateful and stateless messages as retained.

QoS: Select the desired level for the MQTT publication.

MQTT subscriptions

The web interface



Add subscription: Click to add a new MQTT subscription.

Subscription filter: Enter the MQTT topic that you want to subscribe to.

Use device topic prefix: Add the subscription filter as prefix to the MQTT topic.

Subscription type:

- **Stateless:** Select to convert MQTT messages into a stateless message.
- **Stateful:** Select to convert MQTT messages into a condition. The payload is used as the state.

QoS: Select the desired level for the MQTT subscription.

Accessories



I/O ports



Use digital input to connect external devices that can toggle between an open and closed circuit, for example, PIR sensors, door or window contacts, and glass break detectors.

Use digital output to connect external devices such as relays and LEDs. You can activate connected devices through the VAPIX® Application Programming Interface or the web interface.

Port

Name: Edit the text to rename the port.


Direction:  indicates that the port is an input port.  indicates that it's an output port. If the port is configurable, you can click the icons to change between input and output.

Normal state: Click  for open circuit, and  for closed circuit.

Current state: Shows the current state of the port. The input or output is activated when the current state is different from the normal state. An input on the device has an open circuit when it's disconnected or when there is a voltage above 1 V DC.

Note

During restart, the output circuit is open. When the restart is complete, the circuit goes back to the normal position. If you change any settings on this page, the output circuits go back to their normal positions regardless of any active triggers.

Supervised  : Turn on to make it possible to detect and trigger actions if someone tampers with the connection to digital I/O devices. In addition to detecting if an input is open or closed, you can also detect if someone has tampered with it (that is, cut or shorted). To supervise the connection requires additional hardware (end-of-line resistors) in the external I/O loop.

Logs

Reports and logs

The web interface

Reports

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

Logs

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

Network trace

Important

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

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

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

Remote system log

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



Server: Click to add a new server.

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

Format: Select which syslog message format to use.

- Axis
- RFC 3164
- RFC 5424

Protocol: Select the protocol and port to use:

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

Severity: Select which messages to send when triggered.

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

Maintenance

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

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

Important

The only settings saved after restore are:

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

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

Note

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

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

When you upgrade, you can choose between three options:

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

Firmware rollback: Revert to the previously installed firmware version.

Learn more

Cybersecurity

Signed firmware

Signed firmware is implemented by the software vendor signing the firmware image with a private key. When a firmware has this signature attached to it, a device will validate the firmware before accepting to install it. If the device detects that the firmware integrity is compromised, the firmware upgrade will be rejected.

Secure boot

Secure boot is a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on the use of signed firmware, secure boot ensures that a device can boot only with authorized firmware.

Axis Edge Vault

Axis Edge Vault provides a hardware-based cybersecurity platform that safeguards the Axis device. It offers features to guarantee the device's identity and integrity and to protect your sensitive information from unauthorized access. It builds on a strong foundation of cryptographic computing modules (secure element and TPM) and SoC security (TEE and secure boot), combined with expertise in edge device security.

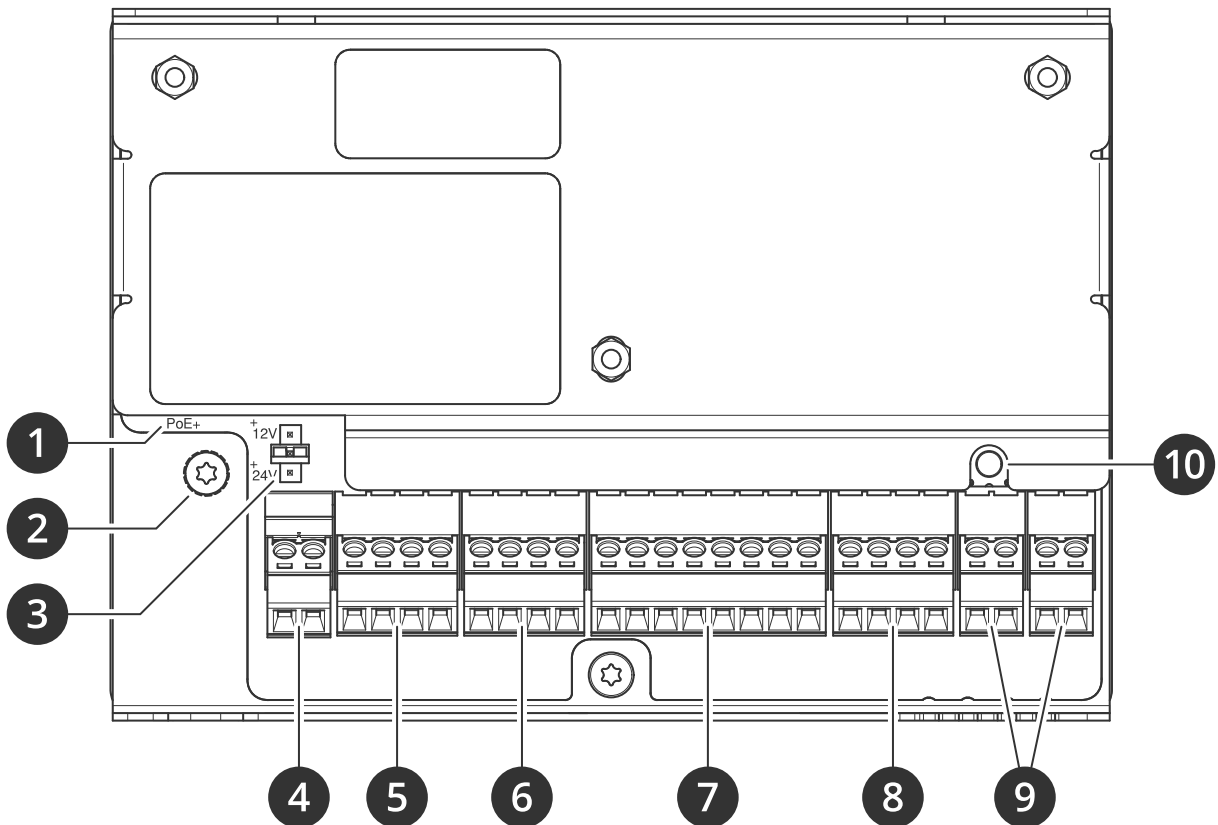
Axis device ID

Being able to verify the origin of the device is key to establishing trust in the device identity. During production, devices with Axis Edge Vault are assigned a unique, factory-provisioned, and IEEE 802.1AR-compliant Axis device ID certificate. This works like a passport to prove the origin of the device. The device ID is securely and permanently stored in the secure keystore as a certificate signed by Axis root certificate. The device ID can be leveraged by the customer's IT infrastructure for automated secure device onboarding and secure device identification

To learn more about Axis Edge Vault and cybersecurity features in Axis devices, go to axis.com/learning/white-papers and search for cybersecurity.

Specifications

Product overview



- 1 Network connector
- 2 Grounding position
- 3 Relay jumper
- 4 Power connector
- 5 Relay connector
- 6 Door connector
- 7 Reader connector
- 8 Auxiliary connector
- 9 External connectors
- 10 Control button

LED indicators

| LED | Color | Indication |
|---------|-------|--|
| Network | Green | Steady for connection to a 100 MBit/s network. Flashes for network activity. |
| | Amber | Steady for connection to a 10 MBit/s network. Flashes for network activity. |
| | Unlit | No network connection. |

| | | |
|--------|-------|--|
| Status | Green | Steady green for normal operation. |
| | Amber | Steady during startup and when restoring settings. |
| | Red | Slow flash for failed upgrade. |
| Power | Green | Normal operation. |
| | Amber | Flashes green/amber during firmware upgrade. |
| Relay | Green | Relay active. ¹ |
| | Unlit | Relay inactive. |

1. Relay is active when COM is connected to NO.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings* on page 29.

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet Plus (PoE+).

UL: Power over Ethernet (PoE) shall be over Ethernet IEEE 802.3af/802.3at Type 1 Class 3 or Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4 power limited injector that provides 44–57 V DC, 15.4 W / 30 W. Power over Ethernet (PoE) has been evaluated by UL with AXIS T8133 Midspan 30 W 1-port.

Power priority

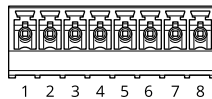
This device can be powered by either PoE or DC input. See *Network connector* on page 23 and *Power connector* on page 27.

- When PoE and DC are both connected before the device is powered, PoE is used for powering.
- PoE and DC are both connected and PoE is currently powering. When PoE is lost, the device uses DC for powering without restart.
- PoE and DC are both connected and DC is currently powering. When DC is lost, the device restarts and uses PoE for powering.
- When DC is used during startup and PoE is connected after the device has started, DC is used for powering.
- When PoE is used during startup and DC is connected after the device has started, PoE is used for powering.

Reader connector

One 8-pin terminal block supporting both OSDP and Wiegand protocols for communication with the reader.

It can connect up to two OSDP readers (multi-drop) or one Wiegand reader. 500 mA at 12 V DC is reserved for all readers connected to the door controller.



Specifications

Configured for one OSDP reader

| Function | Pin | Note | Specifications |
|-------------------|-----|---------------------------|---------------------|
| DC ground (GND) | 1 | | 0 V DC |
| DC output (+12 V) | 2 | Supplies power to reader. | 12 V DC, max 500 mA |
| A | 3 | Half duplex | |
| B | 4 | Half duplex | |

Configured for two OSDP readers (multi-drop)

| Function | Pin | Note | Specifications |
|-------------------|-----|---------------------------------|---|
| DC ground (GND) | 1 | | 0 V DC |
| DC output (+12 V) | 2 | Supplies power to both readers. | 12 V DC, max 500 mA combined for both readers |
| A | 3 | Half duplex | |
| B | 4 | Half duplex | |

Important

- When the reader is powered by the controller, the qualified cable length is up to 200 m (656 ft). Verified only for Axis readers.
- When the reader is not powered by the controller, the qualified cable length for reader data is up to 1000 m (3280,8 ft) if the following cable requirements are met: 1 twisted pair with shield, AWG 24, 120 ohm impedance. Verified only for Axis readers.

Configured for one Wiegand reader

| Function | Pin | Note | Specifications |
|-------------------|-----|---|--------------------------------------|
| DC ground (GND) | 1 | | 0 V DC |
| DC output (+12 V) | 2 | Supplies power to reader. | 12 V DC, max 500 mA |
| D0 | 3 | | |
| D1 | 4 | | |
| LED 1 | 5 | Red LED | |
| LED 2 | 6 | Green LED | |
| TAMPER | 7 | Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. | 0 to max 30 V DC |
| BUZZER | 8 | Digital output – If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients. | 0 to max 30 V DC, open drain, 100 mA |

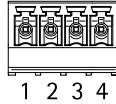
Important

- When the reader is powered by the controller, the qualified cable length is up to 150 m (500 ft).
- When the reader is not powered by the controller, the qualified cable length for reader data is up to 150 m (500 ft) if the following cable requirement is met: AWG 22.

Door connector

One 4-pin terminal block for door monitoring devices (digital input).

Door monitor supports supervision with end of line resistors. If the connection is interrupted, an alarm is triggered. To use supervised inputs, install end of line resistors. Use the connection diagram for supervised inputs. See *page 28*.



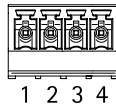
| Function | Pin | Notes | Specifications |
|-----------|------|--|------------------|
| DC ground | 1, 3 | | 0 V DC |
| Input | 2, 4 | For communicating with door monitor. Digital input or Supervised input – Connect to pin 1 or 3 respectively to activate, or leave floating (unconnected) to deactivate. | 0 to max 30 V DC |

Important

The qualified cable length is up to 200 m (656 ft) if the following cable requirement is met: AWG 24.

Relay connector

One 4-pin terminal block for form C relays that can be used, for example, to control a lock or an interface to a gate.



| Function | Pin | Notes | Specifications |
|-----------------|-----|--|--|
| DC ground (GND) | 1 | | 0 V DC |
| NO | 2 | Normally open. For connecting relay devices. Connect a fail-secure lock between NO and DC ground. The two relay pins are galvanically separated from the rest of the circuitry if the jumpers are not used. | Max current = 2 A Max voltage = 30 V DC |
| COM | 3 | Common | |
| NC | 4 | Normally closed. For connecting relay devices. Connect a fail-safe lock between NC and DC ground. The two relay pins are galvanically separated from the rest of the circuitry if the jumpers are not used. | |

Relay power jumper

When the relay power jumper is fitted, it connects 12 V DC or 24 V DC to the relay COM pin.

It can be used to connect a lock between the GND and NO, or GND and NC pins.

Specifications

| Power source | Max power at 12 V DC | Max power at 24 V DC |
|--------------|----------------------|----------------------|
| DC IN | 1 600 mA | 800 mA |
| PoE | 900 mA | 450 mA |

NOTICE

If the lock is non-polarized, we recommend you to add an external flyback diode.

Auxiliary connector

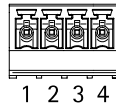
Use the auxiliary connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the auxiliary connector provides the interface to:

Digital input – For connecting devices that can toggle between an open and closed circuit, for example PIR sensors, door/window contacts, and glass break detectors.

Supervised input – Enables possibility to detect tampering on a digital input.

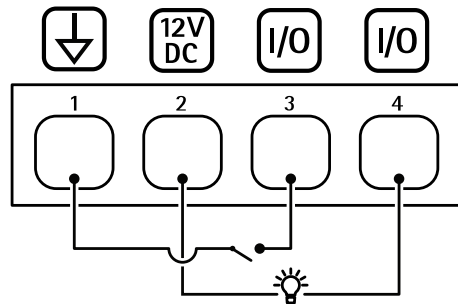
Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface or from the product's webpage.

4-pin terminal block



| Function | Pin | Notes | Specifications |
|-----------------------------------|-----|--|--------------------------------------|
| DC ground | 1 | | 0 V DC |
| DC output | 2 | Can be used to power auxiliary equipment. Note: This pin can only be used as power out. | 12 V DC Max load = 50 mA in total |
| Configurable (Input or Output) | 3-4 | Digital input or supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors. | 0 to max 30 V DC |
| | | Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients. Each I/O is capable of driving 12 V DC, 50 mA (max) external load, if internal 12 V DC output (pin 2) is used. In the case of using open drain connections in combination with an external power supply, then the I/Os can manage DC supply of 0-30 V DC, 100 mA. | 0 to max 30 V DC, open drain, 100 mA |

Specifications

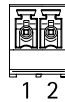


- 1 DC ground
- 2 DC output 12 V
- 3 I/O configured as input
- 4 I/O configured as output

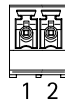
External connector

Two 2-pin terminal blocks for external devices, for example glass break or fire detectors.

UL: The connector has not been evaluated by UL for burglar or fire alarm use.



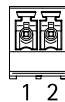
| Function | Pin | Notes | Specifications |
|-----------|-----|--|------------------|
| DC ground | 1 | | 0 V DC |
| TAMPER | 2 | Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. | 0 to max 30 V DC |



| Function | Pin | Notes | Specifications |
|-----------|-----|--|------------------|
| DC ground | 1 | | 0 V DC |
| ALARM | 2 | Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. | 0 to max 30 V DC |

Power connector

2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤ 100 W or a rated output current limited to ≤ 5 A.



Specifications

| Function | Pin | Notes | Specifications |
|-----------------|-----|---|-------------------|
| DC ground (GND) | 1 | | 0 V DC |
| DC input | 2 | For powering controller when not using Power over Ethernet. Note: This pin can only be used as power in. | 12 V DC, max 36 W |

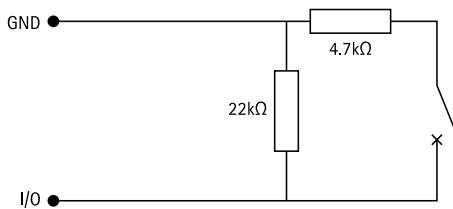
UL: DC power to be supplied by a UL 603 listed power supply, depending on application, with appropriate ratings.

Supervised inputs

To use supervised inputs, install end of line resistors according to the diagram below.

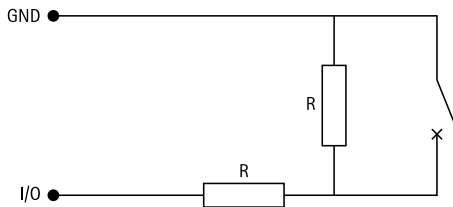
Parallel first connection

The resistor values must be $4.7\text{ k}\Omega$ and $22\text{ k}\Omega$.



Serial first connection

The resistor values must be the same and possible values are $1\text{ k}\Omega$, $2.2\text{ k}\Omega$, $4.7\text{ k}\Omega$ and $10\text{ k}\Omega$.



Note

It is recommended to use twisted and shielded cables. Connect shielding to 0 V DC.

Troubleshooting

Reset to factory default settings

Important

Reset to factory default should be used with caution. A reset to factory default resets all settings, including the IP address, to the factory default values.

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See *Product overview on page 22*.
3. Keep the control button pressed for 25 seconds until the status LED indicator turns amber for the second time.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90.
5. Use the installation and management software tools, assign an IP address, set the password, and access the product.

You can also reset parameters to factory default through the device's web interface. Go to **Maintenance > Factory default** and click **Default**.

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's web 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.
- 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.

Note

Because the database of users, groups, credentials, and other data are updated after a firmware upgrade, the first start-up could take a few minutes to complete. The time required is dependent on the amount of data.

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.

4. When the product has been restarted, clear the web browser's cache.

Technical issues, clues, and solutions

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

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 | 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): <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 | 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. If the password for the root account is lost, the device must be reset to the factory default settings. See <i>Reset to factory default settings</i> on page 29. |
|--------------|--|

Troubleshooting

| | |
|--|--|
| The IP address has been changed by DHCP | 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). If required, a static IP address can be assigned manually. For instructions, go to axis.com/support . |
| 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 device is accessible locally but not externally

To access the device externally, we recommend you to use one of the following applications for Windows®:

- AXIS Companion: free of charge, ideal for small systems with basic surveillance needs.
- AXIS Camera Station: 30-day trial version free of charge, ideal for small to mid-size systems.

For instructions and download, go to axis.com/vms.

Can't connect over port 8883 with MQTT over SSL

| | |
|--|---|
| The firewall blocks traffic using port 8883 as it's deemed insecure. | In some cases the server/broker might not provide a specific port for MQTT communication. It may still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic. <ul style="list-style-type: none">• If the server/broker supports WebSocket/WebSocket Secure (WS/WSS), typically on port 443, use this protocol instead. Check with the server/broker provider to see if WS/WSS is supported and which port and basepath to use.• If the server/broker supports ALPN, the use of MQTT can be negotiated over an open port, such as 443. Check with your server/broker provider to see if ALPN is supported and which ALPN protocol and port to use. |
|--|---|

Contact support

Contact support at axis.com/support.

