

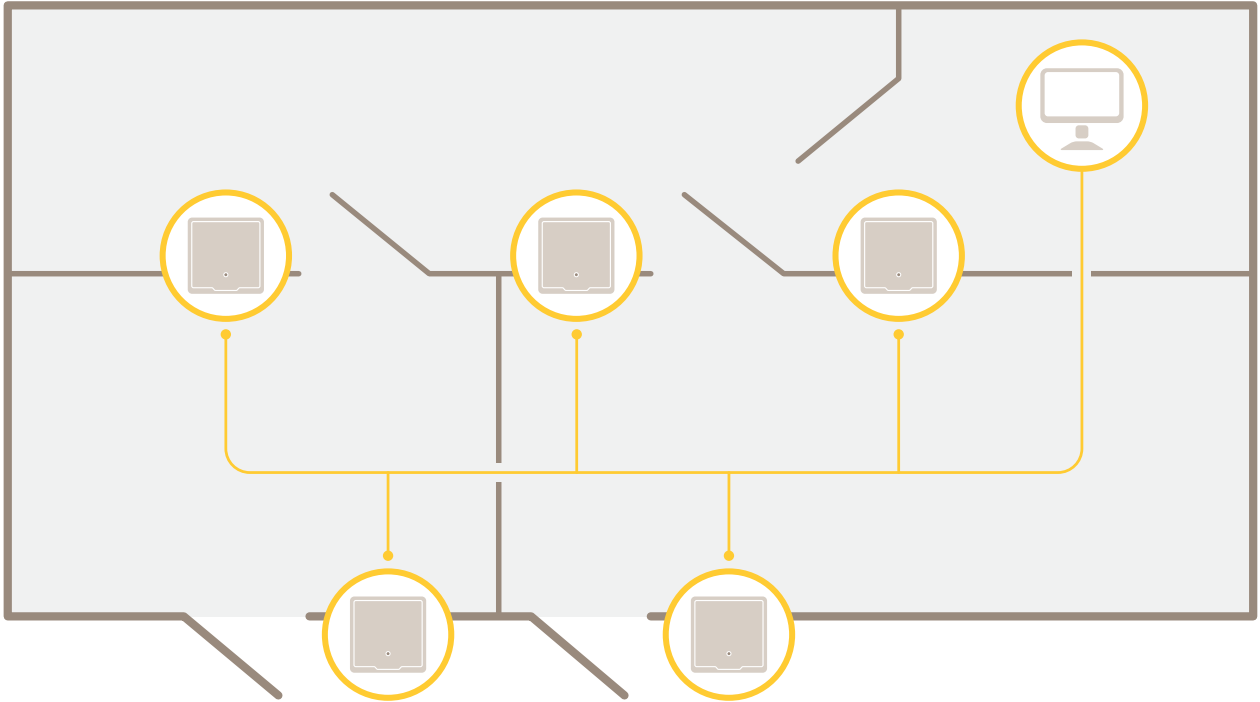
# **AXIS A1601 Network Door Controller**

## Table of Contents

Solution overview .....	4
Product overview .....	5
Find the device on the network .....	6
Access the device .....	6
How to access the product from the internet .....	6
Secure passwords.....	6
How to set the root password .....	7
The Overview page .....	7
System configuration .....	8
Configuration – step by step.....	8
Select a language.....	8
Set the Date and Time .....	8
Get the Date and Time from a Network Time Protocol (NTP) Server .....	8
Set the Date and Time Manually.....	9
Get the Date and Time from the Computer .....	9
Configure the Network Settings.....	9
Configure the hardware .....	9
How to import a hardware configuration file.....	10
Create a new hardware configuration .....	10
How to create a new hardware configuration without peripherals .....	10
How to create a new hardware configuration for wireless locks.....	13
How to create a new hardware configuration with elevator control (AXIS A9188) .....	14
How to add and setup network peripherals .....	14
Verify the Hardware Connections.....	15
Verification Controls Doors.....	15
Verification Controls Floors.....	15
Configure cards and formats .....	16
Card format descriptions .....	16
Field maps .....	16
Configure Services.....	17
SmartIntego.....	17
Maintenance Instructions .....	18
Event configuration.....	20
View the event log .....	20
Event Log Filters.....	20
Configure the event log .....	20
Event log options.....	20
How to set up action rules .....	20
How to add recipients.....	21
How to create schedules .....	22
How to set up recurrences.....	22
Reader feedback.....	22
System options.....	24
Security .....	24
Users.....	24
ONVIF.....	24
IP Address Filter.....	24
HTTPS.....	24
IEEE 802.1X.....	25
Certificates.....	25
Network.....	26
Basic TCP/IP settings.....	26
Advanced TCP/IP Settings.....	27

SOCKS.....	29
QoS (Quality of Service) .....	29
SNMP.....	29
UPnP.....	30
Bonjour .....	30
Ports & Devices.....	30
I/O ports.....	30
Port Status.....	30
Maintenance .....	30
Support.....	31
Support Overview .....	31
System Overview .....	31
Logs & Reports .....	31
Advanced .....	31
Scripting.....	31
File Upload.....	32
Troubleshooting.....	33
Reset to factory default settings.....	33
How to check the current firmware.....	33
How to upgrade the firmware.....	33
Symptoms, possible causes and remedial actions.....	34
Specifications.....	36
.....	36
LED indicators.....	36
Buttons.....	36
Control button .....	36
Connectors.....	36
Network connector .....	36
Reader connector .....	37
Door connector .....	38
Relay connector .....	39
Auxiliary connector.....	39
External connector .....	40
Power connector .....	41
Backup battery input connector .....	41
Safety information.....	42
Hazard levels .....	42
Other message levels .....	42
The web interface .....	43
.....	43
Status.....	43
Device.....	44
Alarms.....	44
Peripherals .....	44
Readers .....	44
System .....	44
Time and location .....	44
Network .....	45
Security.....	49
Accounts .....	53
MQTT .....	53
Accessories .....	56
Logs.....	57
Maintenance .....	59

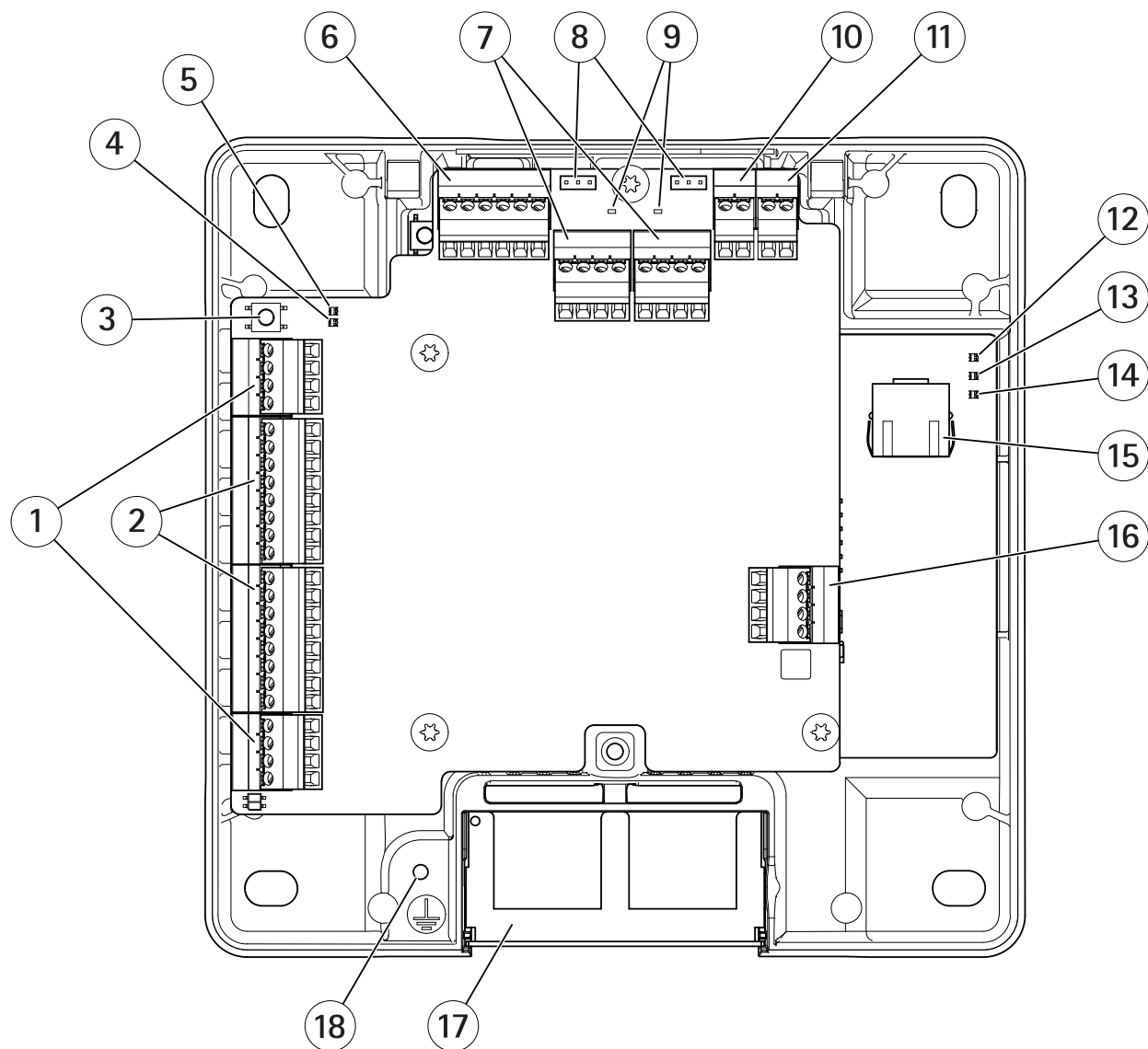
## Solution overview



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

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

## Product overview



- 1 (2x)
- 2 (2x)
- 3
- 4 Reader overcurrent LED
- 5 Relay overcurrent LED
- 6
- 7 (2x)
- 8 Relay jumper (2x)
- 9 Relay LED (2x)
- 10
- 11
- 12 Power LED
- 13 Status LED
- 14 Network LED
- 15
- 16
- 17 Reversible cable cover
- 18 Grounding position

### 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](https://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*.

### Access the device

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 .
3. The device's webpage opens in your browser. The start page is called the Overview page.

### How to access the product from the internet

A network router allows products on a private network (LAN) to share a single connection to the internet. This is done by forwarding network traffic from the private network to the internet.

Most routers are pre-configured to stop attempts to access the private network (LAN) from the public network (internet).

If the Axis product is located on an intranet (LAN) and you want to make it available from the other (WAN) side of a NAT (Network Address Translator) router, turn on **NAT traversal**. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the product.

#### How to turn on the NAT-traversal feature

- Go to **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.
- Click **Enable**.
- Manually configure your NAT router to allow access from the internet.

#### Note

- In this context, a "router" refers to any network routing device such as a NAT router, network router, internet gateway, broadband router, broadband sharing device, or a software such as a firewall.
- For NAT traversal to work, NAT traversal must be supported by the router. The router must also support UPnP®.

### 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.

### **How to set the root password**

To access the Axis product, you must set the password for the default administrator user **root**. This is done in the **Configure Root Password** dialog, which opens when the product is accessed for the first time.

To prevent network eavesdropping, the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate. HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt traffic between web browsers and servers. The HTTPS certificate ensures encrypted exchange of information. See .

The default administrator user name **root** is permanent and cannot be deleted. If the password for root is lost, the product must be reset to the factory default settings. See .

To set the password, enter it directly in the dialog.

### **The Overview page**

The Overview page in the product's web page shows information about the door controller's name, MAC address, IP address, and firmware version. It also enables you to identify the door controller on the network.

The first time you access the Axis product, the Overview page will prompt you to configure the hardware, to set date and time, and to configure the network settings. For more information about configuring the system, see .

To return to the Overview page from the product's other webpages, click **Overview** in the menu bar.

## System configuration

To open the product's setup pages, click **Setup** in the top right-hand corner of the Overview page.

The Axis product can be configured by administrators. For more information about users and administrators, see .

### Configuration – step by step

Before you start using the access control system, you should complete the following setup steps:

1. If English is not your first language, you may want the product's web page to use a different language. See .
2. Set the date and time. See .
3. Configure the network settings. See .
4. Configure the door controller and connected devices such as readers, locks and request to exit (REX) devices. See .
5. Verify the Hardware Connections. See .
6. Configure cards and formats. See .

For information about maintenance recommendations, see .

### Select a language

The default language of the product's web page is English, but you can switch to any of the languages that are included in the product's firmware. For information about the latest available firmware, see [www.axis.com](http://www.axis.com)

You can switch languages in any of the product's web pages.

To switch languages, click the language drop-down list  and select a language. All the product's web pages and help pages are displayed in the selected language.

#### Note

- When you switch languages, the date format also changes to a format commonly used in the selected language. The correct format is displayed in the data fields.
- If you reset the product to factory default settings, the product's web page switches back to English.
- If you restore or restart the product, or upgrade the firmware, the product's web page will continue to use the selected language.

### Set the Date and Time

To set the date and time of the Axis product, go to **Setup > Date & Time**.

You can set the date and time in the following ways:

- Get the date and time from a network time protocol (NTP) server. See .
- Set the date and time manually. See .
- Get the date and time from the computer. See .

Current controller time displays the door controller's current date and time (24h clock).

The same options for date and time are also available in the System Options pages. Go to **Setup > Additional Controller Configuration > System Options > Date & Time**.

### Get the Date and Time from a Network Time Protocol (NTP) Server

1. Go to **Setup > Date & Time**.
2. Select your Timezone from the drop-down list.



3. If daylight saving time is used in your region, select **Adjust for daylight saving** .
4. Select **Synchronize with NTP**.
5. Select the default DHCP address or enter the address of a NTP server.
6. Click **Save**.

When synchronizing with an NTP server, date and time are updated continuously because the data is pushed from the NTP server. For information about NTP settings, see .

If you use a host name for the NTP server, a DNS server must be configured. See .

### Set the Date and Time Manually

1. Go to **Setup > Date & Time**.
2. If daylight saving time is used in your region, select **Adjust for daylight saving** .
3. Select **Set date & time manually**.
4. Enter the desired date and time.
5. Click **Save**.

When setting the date & time manually, date and time are set once and will not be updated automatically. This means that if the date or time needs to be updated, the changes must be made manually because there is no connection to an external NTP server.

### Get the Date and Time from the Computer

1. Go to **Setup > Date & Time**.
2. If daylight saving time is used in your region, select **Adjust for daylight saving** .
3. Select **Set date & time manually**.
4. Click **Sync now and save**.

When using the computer time, date and time are synchronized with the computer time once and will not be updated automatically. This means that if you change the date or time on the computer you use to manage the system, you should synchronize again.

### Configure the Network Settings

To configure the basic network settings, go to **Setup > Network Settings** or to **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic**.

For more information about network settings, see .

### Configure the hardware

You can connect readers, locks and other devices to the Axis product before you complete the hardware configuration. However, it will be easier to connect devices if you complete the hardware configuration first. This is because a hardware pin chart will be available when the configuration is complete. The hardware pin chart is a guide on how to connect devices to the pins and can be used as a reference sheet for maintenance. For maintenance instructions, see .

If configuring the hardware for the first time, select one of the following methods:

- Import a hardware configuration file. See .
- Create a new hardware configuration. See .

#### Note

If the product's hardware has not been configured before or has been deleted, **Hardware Configuration** will be available in the notification panel in the Overview page.

### How to import a hardware configuration file

The hardware configuration of the Axis product can be completed faster by importing a hardware configuration file.

By exporting the file from one product and importing it to others, you can make multiple copies of the same hardware setup without having to repeat the same steps over and over again. You can also store exported files as backups and use them to restore previous hardware configurations. For more information, see .

To import a hardware configuration file:

1. Go to **Setup > Hardware Configuration**.
2. Click **Import hardware configuration** or, if a hardware configuration already exists, **Reset and import hardware configuration**.
3. In the file browser dialog that appears, locate and select the hardware configuration file (\*.json) on your computer.
4. Click **OK**.

### How to export a hardware configuration file

The hardware configuration of the Axis product can be exported to make multiple copies of the same hardware setup. You can also store exported files as backups and use them to restore previous hardware configurations.

#### Note

The hardware configuration of floors is not possible to export.

Wireless lock settings are not included in the hardware configuration export.

To export a hardware configuration file:

1. Go to **Setup > Hardware Configuration**.
2. Click **Export hardware configuration**.
3. Depending on the browser, you may need to go through a dialog to complete the export. Unless otherwise specified, the exported file (\*.json) is saved in the default download folder. You can select a download folder in the web browser's user settings.

### Create a new hardware configuration

Follow the instructions according to your requirements:

- 
- 
- 

### How to create a new hardware configuration without peripherals

1. Go to **Setup > Hardware Configuration** and click **Start new hardware configuration**.
2. Enter a name for the Axis product.
3. Select the number of connected doors and click **Next**.
4. Configure the door monitors (door position sensors) and locks according to your requirements and click **Next**. For more information about the available options, see .
5. Configure the readers and REX devices that will be used and click **Finish**. For more information about the available options, see .
6. Click **Close** or click the link to view the hardware pin chart.

## How to configure door monitors and locks

When you have selected a door option in the new hardware configuration, you can configure the door monitors and locks.

1. If a door monitor will be used, select **Door monitor** and then select the option that matches how the door monitor circuits will be connected.
2. If the door lock shall lock immediately after the door has been opened, select **Cancel access time once door is opened**.  
If you want to delay the relock, set the time of the delay in milliseconds in **Relock time**.
3. Specify the door monitor time options or, if no door monitor will be used, the lock time options.
4. Select the options that match how the lock circuits will be connected.
5. If a lock monitor will be used, select **Lock monitor** and then select the options that match how the lock monitor circuits will be connected.
6. If the input connections from readers, REX devices, and door monitors shall be supervised, select **Enable supervised inputs**.  
For more information, see .

### Note

- Most lock, door monitor, and reader options can be changed without resetting and starting a new hardware configuration. Go to **Setup > Hardware Reconfiguration**.
- You can connect one lock monitor per door controller. So if you use double-lock doors, only one of the locks can have a lock monitor. If two doors are connected to the same door controller, lock monitors cannot be used.

## About door monitor and time options

The following door monitor options are available:

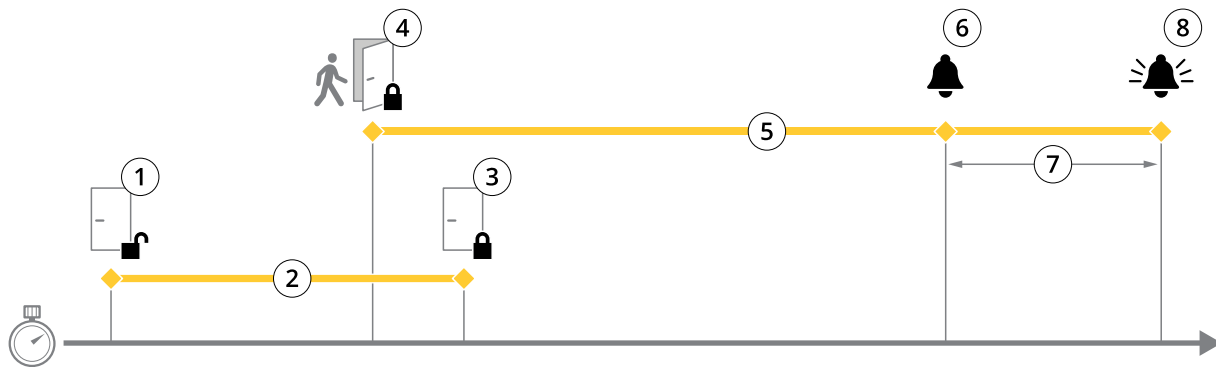
- **Door monitor** – Selected by default. Each door has its own door monitor that, for example, will signal when the door has been forced open or open too long. Deselect if no door monitor will be used.
- **Open circuit = Closed door** – Select if the door monitor circuit is normally open. The door monitor gives the door open signal when the circuit is closed. The door monitor gives the door closed signal when the circuit is open.
- **Open circuit = Open door** – Select if the door monitor circuit is normally closed. The door monitor gives the door open signal when the circuit is open. The door monitor gives the door closed signal when the circuit is closed.
- **Cancel access time once door is opened** – Select to prevent tailgating. The lock will be locked as soon as the door monitor indicates that the door has been opened.

The following door time options are always available:

- **Access time** – Set the number of seconds the door shall remain unlocked after access has been granted. The door remains unlocked until the door has been opened or until the set time has been reached. The door will lock when it closes regardless of whether the access time has expired or not.
- **Long access time** – Set the number of seconds the door shall remain unlocked after access has been granted. Long access time overrides the already set access time and will be enabled for users with long access time selected.

Select **Door monitor** to make the following door time options available:

- **Open too long time** – Set the number of seconds the door is allowed to stay open. If the door is still open when the set time has been reached, the door open too long alarm is triggered. Set up an action rule to configure which action the open too long event shall trigger.
- **Pre-alarm time** – A pre-alarm is a warning signal that is triggered before the open too long time has been reached. It informs the administrator and warns, depending on how the action rule has been set up, the person entering the door that the door needs to be closed to avoid the door open too long alarm to go off. Set the number of seconds before the door open too long alarm is triggered the system shall give the pre-alarm warning signal. To disable the pre-alarm, set the pre-alarm time to 0.



- 1 Access granted – lock unlocks
- 2 Access time
- 3 No action taken – lock locks
- 4 Action taken (door opened) – lock locks or stays unlocked until door closes
- 5 Open too long time
- 6 Pre-alarm goes off
- 7 Pre-alarm time
- 8 Open too long-alarm goes off

For information about how to set up an action rule, see .

## About lock options

The following lock circuit options are available:

- **Relay** – Can only be used on one lock per door controller. If two doors are connected to the door controller, a relay can only be used on the lock of the second door.
- **None** – Only available for Lock 2. Select if only one lock will be used.

The following lock monitor options are available for single-door configurations:

- **Lock monitor** – Select to make the lock monitor controls available. Then select the lock that shall be monitored. A lock monitor can only be used on double-lock doors and cannot be used if two doors are connected to the door controller.
- **Open circuit = Locked** – Select if the lock monitor circuit is normally closed. The lock monitor gives the door unlocked signal when the circuit is closed. The lock monitor gives the door locked signal when the circuit is open.
- **Open circuit = Unlocked** – Select if the lock monitor circuit is normally open. The lock monitor gives the door unlocked signal when the circuit is open. The lock monitor gives the door locked signal when the circuit is closed.

## How to configure readers and REX devices

When you have configured the door monitors and locks in the new hardware configuration, you can configure the readers and request to exit (REX) devices.

1. If a reader will be used, select the checkbox and then select the options that match the reader's communication protocol.
2. If a REX device such as a button, sensor, or push bar will be used, select the checkbox and then select the option that matches how the REX device's circuits will be connected.  
If the REX signal does not influence door opening (for example for doors with mechanical handles or push bars), select **REX does not unlock door**.
3. If connecting more than one reader or REX device to the door controller, do the previous two steps again until each reader or REX device has the correct settings.

## About reader and REX device options

The following reader options are available:

- **Wiegand** – Select for readers that use Wiegand protocols. Then select the LED control that is supported by the reader. Readers with single LED control usually toggle between red and green. Readers with dual LED control use different wires for the red and green LEDs. This means that the LEDs are controlled independently of each other. When both LEDs are on, the light appears to be amber. See the manufacturer's information about which LED control the reader supports.
- **OSDP, RS485 half duplex** – Select for RS485 readers with half duplex support. See the manufacturer's information about which protocol the reader supports.

The following REX device options are available:

- **Active low** – Select if activating the REX device closes the circuit.
- **Active high** – Select if activating the REX device opens the circuit.
- **REX does not unlock door** – Select if the REX signal does not influence door opening (for example for doors with mechanical handles or push bars). The door forced open alarm will not be triggered as long as the user opens the door within the access time. Deselect if the door shall unlock automatically when the user activates the REX device.

### Note

Most lock, door monitor, and reader options can be changed without resetting and starting a new hardware configuration. Go to **Setup > Hardware Reconfiguration**.

### How to use supervised inputs

Supervised inputs report on the status of the connection between the door controller and the door monitors. If the connection is interrupted, an event is activated.

To use supervised inputs:

1. Install end of line resistors on all the used supervised inputs. See the connection diagram on .
2. Go to **Setup > Hardware Reconfiguration** and select **Enable supervised inputs**. You can also enable supervised inputs during the hardware configuration.

### About supervised input compatibility

The following function supports supervised inputs:

- Door monitor. See .

### How to create a new hardware configuration for wireless locks

1. Go to **Setup > Hardware Configuration** and click **Start new hardware configuration**.
2. Enter a name for the Axis product.
3. In the list of peripherals, select a manufacturer for a wireless gateway.
4. If you want to connect a wired door, select the **1 Door** checkbox and click **Next**. If no door is included, click **Finish**.
5. Depending on what lock manufacturer you got, proceed according to one of the bullets:
  - **ASSA Aperio**: Click the link to view the hardware pin chart or click **Close** and go to **Setup > Hardware Reconfiguration** to complete the configuration, see
  - **SmartIntego**: Click the link to view the hardware pin chart or click **Click here to select wireless gateway and configure doors** to complete the configuration, see .

### Add Assa Aperio™ doors and devices

Before adding a wireless door to the system it needs to be paired with the connected Assa Aperio communication hub, using Aperio PAP (Aperio programming application tool).

To add a wireless door:

1. Go to **Setup > Hardware Reconfiguration**.
2. Under **Wireless Doors and Devices** click **Add door**.

3. In the **Door name** field: Enter a descriptive name.
4. In the **ID** field under **Lock**: Enter the six-character-long address of the device that you want to add. The device address is printed on the product label.
5. Optionally, under **Door position sensor**: Choose **Built in door position sensor** or **External door position sensor**.

### Note

If using an external door position sensor (DPS), make sure that the Aperio lock device has support for door handle state detection before configuring it.

6. Optionally, in the **ID** field under **Door position sensor**: Enter the six-character-long address of the device that you want to add. The device address is printed on the product label.
7. Click **Add**.

## How to create a new hardware configuration with elevator control (AXIS A9188)

### Important

Before creating a HW configuration you need to add a user in AXIS A9188 Network I/O Relay Module. Go to the A9188 web interface > **Preferences** > **Additional device configuration** > **Basic setup** > **Users** > **Add** > **User setup**.

### Note

Max 2 AXIS 9188 Network I/O Relay Modules can be configured with each Axis Network Door Controller

1. In the door controller's web page, go to **Setup** > **Hardware Configuration** and click **Start new hardware configuration**.
2. Enter a name for the Axis product.
3. In the list of peripherals, select **Elevator control** to include an AXIS A9188 Network I/O Relay Module and click **Next**.
4. Enter a name for the connected reader.
5. Select the reader protocol that will be used and click **Finish**.
6. Click **Network Peripherals** to complete the configuration see or click the link to go to the hardware pin chart.

## How to add and setup network peripherals

### Important

- Before you set up the network peripherals you need to add a user in AXIS A9188 Network I/O Relay Module. Go to the AXIS A9188 web interface > **Preferences** > **Additional device configuration** > **Basic setup** > **Users** > **Add** > **User setup**.
  - Don't add another AXIS A1001 Network Door Controller as a network peripheral.
1. Go to **Setup** > **Network Peripherals** to add a device
  2. Find your device(s) under **Discovered devices**.
  3. Click **Add this device**
  4. Enter a name for the device
  5. Enter the AXIS A9188 username and password
  6. Click **Add**.

### Note

You can manually add network peripherals by entering MAC address or IP address in the **Manually add device** dialog.

### Important

If you want to delete a schedule, first make sure it's not used by the network I/O relay module.

### How to setup I/Os and relays in network peripherals

#### Important

Before setting up the network peripherals you need to add a user in AXIS A9188 Network I/O Relay Module. Go to the AXIS A9188 web interface > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup.**

1. Go to **Setup > Network Peripherals** and click on the **Added devices** row.
2. Choose which I/Os and relays to set as floor.
3. Click **Set as floor** and enter a name.
4. Click **Add**.

### Verify the Hardware Connections

When the hardware installation and configuration is complete, and anytime during the door controller's lifetime, you can verify the function of the connected door monitors, Network I/O Relay Modules, locks and readers.

To verify the configuration and access the verification controls, go to **Setup > Hardware Connection Verification**.

#### Verification Controls Doors

- **Door state** – Verify the current state of the door monitor, door alarms and locks. Click **Get current state**.
- **Lock** – Manually trigger the lock. Both primary locks and secondary locks if there are any will be affected. Click **Lock** or **Unlock**.
- **Lock** – Manually trigger the lock to grant access. Only primary locks will be affected. Click **Access**.
- **Reader: Feedback** – Verify the reader feedback, for example sounds and LED signals, for different commands. Select the command and click **Test**. Which types of feedback that are available depends on the reader. For more information, see . See also the manufacturer's instructions.
- **Reader: Tampering** – Get information about the last tampering attempt. The first tampering attempt will be registered when the reader is installed. Click **Get last tampering**.
- **Reader: Card swipe** – Get information about the last swiped card or other type of user token accepted by the reader. Click **Get last credential**.
- **REX** – Get information about the last time the request to exit (REX) device was pressed. Click **Get last REX**.

#### Verification Controls Floors

- **Floor state** – Verify the current state of the floor access. Click **Get current state**.
- **Floor lock & unlock** – Manually trigger the floor access. Both primary locks and secondary locks if there are any will be affected. Click **Lock** or **Unlock**.
- **Floor access** – Manually grant temporary access to the floor. Only primary locks will be affected. Click **Access**.
- **Elevator Reader: Feedback** – Verify the reader feedback, for example sounds and LED signals, for different commands. Select the command and click **Test**. Which types of feedback that are available depends on the reader. For more information, see . See also the manufacturer's instructions.
- **Elevator Reader: Tampering** – Get information about the last tampering attempt. The first tampering attempt will be registered when the reader is installed. Click **Get last tampering**.
- **Elevator Reader: Card swipe** – Get information about the last swiped card or other type of user token accepted by the reader. Click **Get last credential**.
- **REX** – Get information about the last time the request to exit (REX) device was pressed. Click **Get last REX**.

## Configure cards and formats


The door controller has a few predefined commonly used card formats that you can use as they are or modify as required. You can also create custom card formats. Each card format has a different set of rules, field maps, for how the information stored on the card is organized. By defining a card format you tell the system how to interpret the information that the controller gets from the reader. For information about which card formats the reader supports, see the manufacturer's instructions.

To enable card formats:

1. Go to **Setup > Configure cards and formats**.
2. Select one or more card formats that match the card format used by the connected readers.

To create new card formats:

1. Go to **Setup > Configure cards and formats**.
2. Click **Add card format**.
3. In the **Add card format** dialog, enter a name, a description, and the bit length of the card format. See .
4. Click **Add field map** and enter the required information in the fields. See .
5. To add multiple field maps, repeat the previous step.

To expand an item in the **Card formats** list and view the card format descriptions and field maps, click .

To edit a card format, click ,255mm,sfx)="graphics:graphic21CC0221EE011FBA8A175057AB780214" and change the card format descriptions and field maps as required. Then click **Save**.

To delete a field map in the **Edit card format** or **Add card format** dialog, click ,255mm,sfx)="graphics:graphicF2CA0D5AAAD670C758A916091B751B79"

To delete a card format, click ,255mm,sfx)="graphics:graphicF2CA0D5AAAD670C758A916091B751B79".

### Important

- You can only enable and disable card formats if the door controller has been configured with at least one reader. See and .
- Two card formats with the same bit length cannot be active the same time. For example, if you have defined two 32-bit card formats, "Format A" and "Format B", and you have enabled "Format A", you cannot enable "Format B" without disabling "Format A" first.
- If no card formats have been enabled, you can use the **Card raw only** and **Card raw and PIN** identification types to identify a card and grant access to users. However, we do not recommend this since different reader manufacturers or reader settings can generate different card raw data.

## Card format descriptions

- **Name (required)** – Enter a descriptive name.
- **Description** – Enter additional information as desired. This information is only visible in the **Edit card format** and **Add card format** dialogs.
- **Bit length (required)** – Enter the bit length of the card format. This has to be a number between 1 and 1000000000.

## Field maps

- **Name (required)** – Enter the field map name unspaced, for example `OddParity`. Examples of common field maps include:
  - `Parity` – Parity bits are used for error detection. Parity bits are usually added to the beginning or end of a binary code string and indicate if the number of bits is even or odd.
  - `EvenParity` – Even parity bits make sure that there is an even number of bits in the string. The bits that have the value 1 are counted. If the count is already even, the parity bit value is set



to 0. If the count is odd, the even parity bit value is set to 1, making the total count an even number.

- **OddParity** – Odd parity bits make sure that there is an odd number of bits in the string. The bits that have the value 1 are counted. If the count is already odd, the odd parity bit value is set to 0. If the count is even, the parity bit value is set to 1, making the total count an odd number.
- **FacilityCode** – Facility codes are sometimes used for verifying that the token matches the ordered end user credential batch. In legacy access control systems, the facility code was used for a degraded validation, allowing entry to every employee in the credential batch that had been encoded with a matching site code. This field map name, which is case sensitive, is required for the product to validate on facility code.
- **CardNr** – The card number or user ID is what is most commonly validated in access control systems. This field map name, which is case sensitive, is required for the product to validate on card number.
- **CardNrHex** – The card number binary data is encoded as hex-lowercase numbers in the product. It is primarily used for troubleshooting why you are not getting the expected card number from the reader.
- **Range (required)** – Enter the bit range of the field map, for example 1, 2–17, 18–33, and 34.
- **Encoding (required)** – Select the encoding type of each field map.
  - **BinLE2Int** – Binary data is encoded as integer numbers in little endian bit order. Integer means that it needs to be a whole number (no decimals). Little endian bit order means that the first bit is the smallest (least significant).
  - **BinBE2Int** – Binary data is encoded as integer numbers in big endian bit order. Integer means that it needs to be a whole number (no decimals). Big endian bit order means that the first bit is the biggest (most significant).
  - **BinLE2Hex** – Binary data is encoded as hex-lowercase numbers in little endian bit order. The hexadecimal system, also known as the base-16 number system, consists of 16 unique symbols: the numbers 0–9 and the letters a–f. Little endian bit order means that the first bit is the smallest (least significant).
  - **BinBE2Hex** – Binary data is encoded as hex-lowercase numbers in big endian bit order. The hexadecimal system, also known as the base-16 number system, consists of 16 unique symbols: the numbers 0–9 and the letters a–f. Big endian bit order means that the first bit is the biggest (most significant).
  - **BinLEIBO2Int** – Binary data is encoded in the same way as for BinLE2Int, but the card raw data is read with inverted byte order in a multiple-byte sequence before field maps are taken out to be encoded.
  - **BinBEIBO2Int** – Binary data is encoded like for BinBE2Int, but the card raw data is read with inverted byte order in a multiple-byte sequence before the field maps are taken out to be encoded.

For information about which field maps your card format uses, see the manufacturer's instructions.

## Configure Services

The Configure Services in the Setup page is used to access the set up for the external services that can be used with the door controller.

## SmartIntego

SmartIntego is a wireless solution that increases the number of doors a door controller can handle.

### Prerequisites SmartIntego

The following prerequisites needs to be met before proceeding with the SmartIntego configuration:

- A csv-file needs to be created. The csv-file contains information about what GatewayNode and doors that are used in your SmartIntego solution. The file is created in a standalone software provided by a SimonsVoss partner.
- The Hardware Configuration of SmartIntego has been done, see .

### Note

- SmartIntego Configuration tool must be version 2.1.6452.23485, build 2.1.6452.23485 (8/31/2017 1:02:50 PM) or later.
- The Advanced Encryption Standard (AES) is not supported for SmartIntego, and must therefore be disabled in the SmartIntego Configuration tool.

## How To Configure SmartIntego

### Note

- Make sure that prerequisites listed have been met.
  - For increased visibility of the battery status, go to **Setup > Configure event and alarms logs**, and add either **Door — Battery alarm** or **IdPoint — Battery alarm** as an alarm.
  - The door monitor settings come from the imported CSV file. You shouldn't need to change this setting in a normal installation.
1. Click **Browse...**, select the csv-file and click **Upload file**.
  2. Select a GatewayNode and click **Next**.
  3. A preview of the new configuration is shown. Disable the door monitors if needed.
  4. Click **Configure**.
  5. An overview of the doors included in the configuration is shown. Click **Settings** to configure each door individually.

## How to re-configure SmartIntego

1. Click **Setup** in the top menu.
2. Click **Configure Services > Settings**.
3. Click **Re-configure**.
4. Click **Browse...**, select the csv-file and click **Upload file**.
5. Select a GatewayNode and click **Next**.
6. A preview of the new configuration is shown. Disable the door monitors if needed.

### Note

The door monitor settings come from the imported CSV file. You shouldn't need to change this setting in a normal installation.

7. Click **Configure**.
8. An overview of the doors included in the configuration is shown. Click **Settings** to configure each door individually.

## Maintenance Instructions

To keep the access control system running smoothly, Axis recommends regular maintenance of the access control system, including door controllers and connected devices.

Do maintenance at least once a year. The suggested maintenance procedure includes, but is not limited to, the following steps:

- Make sure all the connections between the door controller and the external devices are secure.
- Verify all the hardware connections. See .
- Verify that the system, including the connected external devices, functions correctly.

- Swipe a card and test the readers, doors, and locks.
- If the system includes REX devices, sensors or other devices, test them as well.
- If activated, test the tampering alarms.

If the results from any of the steps above indicate faults or unexpected behavior:

- Test the signals of the wires using appropriate equipment and check if the wires or cables are damaged in any way.
- Replace all damaged or faulty cables and wires.
- Once the cables and wires have been replaced, verify all the hardware connections again. See .
  - If the door controller is not behaving as expected, see and for more information.


## Event configuration

Events that occur in the system, for example when a user swipes a card or a REX device is activated, are logged in the event log.

- View the event log. See .
- Export the event log. See .
- Configure the event log. See .

### View the event log

To view logged events, go to **Event Log**.

To expand an item in the event log and view the event details, click .

Applying filters to the event log makes it easier to find specific events. To filter the list, select one or several event log filters and click **Apply filters**. For more information, see .

As an administrator, you might have more interest in some events than others. Therefore, you can choose which events that shall be logged. For more information, see .

### Event Log Filters

You can narrow the scope of the event log by selecting one or several of the following filters:

- User – Filter on events that relates to a selected user.
- Door & floor – Filter on events that relates to a specific door or floor.
- Topic – Filter on event type.
- Date and time – Filter the event log by a date and time span.

### Configure the event log

The Configure event log page allows you to define which events shall be logged.

#### Event log options

To define which events shall be included in the event log, go to **Setup > Configure Event Logs**.

The following options for logging events are available:

- **No logging** – Disable event logging. The event will not be registered or included in the event log.
- **Log for all sources** – Enable event logging. The event will be registered and included in the event log.

### How to set up action rules

The Event pages allow you to configure the Axis product to perform actions when different events occur. The set of conditions that defines how and when the action is triggered is called an action rule. If multiple conditions are defined, all of them must be met to trigger the action.

For more information about available triggers and actions, see the product's built-in help.

This example describes how to set up an action rule to activate an output port when the door is forced open.

1. Go to **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports**.
2. Select **Output** from the desired **I/O Port Type** drop-down list and enter a **Name**.
3. Select the I/O port's **Normal state** and click **Save**.
4. Go to **Events > Action Rules** and click **Add**.
5. Select **Door** from the **Trigger** drop-down list.

6. Select **Door Alarm** from the drop-down list.
7. Select the desired door from the drop-down list.
8. Select **DoorForcedOpen** from the drop-down list.
9. Optionally, select a **Schedule** and **Additional conditions**. See below.
10. Under **Actions**, select **Output Port** from the **Type** drop-down list.
11. Select the desired output port from the **Port** drop-down list.
12. Set state **Active**.
13. Select **Duration** and **Go to opposite state after**. Then enter the desired duration of the action.
14. Click **OK**.

To use more than one trigger for the action rule, select **Additional conditions** and click **Add** to add additional triggers. When using additional conditions, all conditions must be met to trigger the action.

To prevent an action from being triggered repeatedly, a **Wait at least** time can be set. Enter the time in hours, minutes and seconds, during which the trigger should be ignored before the action rule can be activated again.

For more information, see the product's built-in help.

### How to add recipients

The product can send messages to notify recipients about events and alarms. But before the product can send notification messages, you must define one or more recipients. For information about available options, see .

To add a recipient:

1. Go to **Setup > Additional Controller Configuration > Events > Recipients** and click **Add**.
2. Enter a descriptive name.
3. Select a recipient **Type**.
4. Enter the information needed for the recipient type.
5. Click **Test** to test the connection to the recipient.
6. Click **OK**.

### How to set up email recipients

Email recipients can be configured by selecting one of the listed email providers, or by specifying the SMTP server, port and authentication used by, for example, a corporate email server.

#### Note

Some email providers have security filters that prevent users from receiving or viewing large attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid delivery problems and locked email accounts.

To set up an email recipient using one of the listed providers:

1. Go to **Events > Recipients** and click **Add**.
2. Enter a **Name** and select **Email** from the **Type** list.
3. Enter the email addresses to send emails to in the **To** field. Use commas to separate multiple addresses.
4. Select the email provider from the **Provider** list.
5. Enter the user ID and password for the email account.
6. Click **Test** to send a test email.

To set up an email recipient using for example a corporate email server, follow the instructions above but select **User defined as Provider**. Enter the email address to appear as sender in the **From** field. Select **Advanced settings** and specify the SMTP server address, port and authentication method. Optionally, select **Use encryption**

to send emails over an encrypted connection. The server certificate can be validated using the certificates available in the Axis product. For information on how to upload certificates, see .

### How to create schedules

Schedules can be used as action rule triggers or as additional conditions. Use one of the predefined schedules or create a new schedule as described below.

To create a new schedule:

1. Go to **Setup > Additional Controller Configuration > Events > Schedules** and click **Add**.
2. Enter a descriptive name and the information needed for a daily, weekly, monthly or yearly schedule.
3. Click **OK**.

To use the schedule in an action rule, select the schedule from the **Schedule** drop-down list in the Action Rule Setup page.

### How to set up recurrences

Recurrences are used to trigger action rules repeatedly, for example every 5 minutes or every hour.

To set up a recurrence:

1. Go to **Setup > Additional Controller Configuration > Events > Recurrences** and click **Add**.
2. Enter a descriptive name and recurrence pattern.
3. Click **OK**.

To use the recurrence in an action rule, first select **Time** from the **Trigger** drop-down list in the Action Rule Setup page and then select the recurrence from the second drop-down list.

To modify or remove recurrences, select the recurrence in the **Recurrences List** and click **Modify** or **Remove**.

### Reader feedback

Readers use LEDs and beepers to send feedback messages to the user (the person accessing or trying to access the door). The door controller can trigger a number of feedback messages, some of which are preconfigured in the door controller and supported by most readers.

Readers have different LED behaviors, but typically they use different sequences of steady lights and flashing lights in red, green, and amber.

Readers can also use one-pitch beepers to send messages, using different sequences of short and long beeper signals.

The table below shows the events that are preconfigured in the door controller to trigger reader feedback and their typical reader feedback signals. Feedback signals for AXIS readers are presented in the Installation Guide supplied with the AXIS reader.

Event	Wiegand dual LED	Wiegand single LED	OSDP	Beeper pattern	State
Idle <sup>1</sup>	Off	Red	Red	Silent	Normal
RequirePIN	Flashing red/green	Flashing red/green	Flashing red/green	Two short beeps	PIN required
AccessGranted	Green	Green	Green	Beep	Access granted
AccessDenied	Red	Red	Red	Beep	Access denied

1. Idle state is entered when the door is closed and the lock is locked.

Feedback messages other than the above must be configured by a client such as an access management system, through the VAPIX® application programming interface, that supports this feature and use readers that can provide the required signals. For more information, see the user information supplied by the access management system developer and reader manufacturer.

## System options

### Security

#### Users

User access control is enabled by default and can be configured under **Setup > Additional Controller Configuration > System Options > Security > Users**. An administrator can set up other users by giving them user names and passwords.

The user list displays authorized users and user groups (access levels):

- **Administrators** have unrestricted access to all settings. The administrator can add, modify and remove other users.

#### Note

Note that when the option **Encrypted & unencrypted** is selected, the webserver will encrypt the password. This is the default option for a new unit or a unit reset to factory default settings.

Under **HTTP/RTSP Password Settings**, select the type of password to allow. You may need to allow unencrypted passwords if there are viewing clients that do not support encryption, or if you upgraded the firmware and existing clients support encryption but need to log in again and be configured to use this functionality.

### ONVIF

ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products.

By creating a user you automatically enable ONVIF communication. Use the user name and password with all ONVIF communication with the product. For more information see [www.onvif.org](http://www.onvif.org)

### IP Address Filter

IP address filtering is enabled on the **Setup > Additional Controller Configuration > System Options > Security > IP Address Filter** page. Once enabled, the listed IP address are allowed or denied access to the Axis product. Select **Allow** or **Deny** from the list and click **Apply** to enable IP address filtering.

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses).

### HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol providing encrypted browsing. HTTPS can also be used by users and clients to verify that the correct device is being accessed. The security level provided by HTTPS is considered adequate for most commercial exchanges.

The Axis product can be configured to require HTTPS when administrators log in.

To use HTTPS, an HTTPS certificate must first be installed. Go to **Setup > Additional Controller Configuration > System Options > Security > Certificates** to install and manage certificates. See .

To enable HTTPS on the Axis product:

1. Go to **Setup > Additional Controller Configuration > System Options > Security > HTTPS**
2. Select an HTTPS certificate from the list of installed certificates.
3. Optionally, click **Ciphers** and select the encryption algorithms to use for SSL.
4. Set the **HTTPS Connection Policy** for the different user groups.
5. Click **Save** to enable the settings.

To access the Axis product via the desired protocol, in the address field in a browser, enter `https://` for the HTTPS protocol and `http://` for the HTTP protocol.



The HTTPS port can be changed on the **System Options > Network > TCP/IP > Advanced** page.

### IEEE 802.1X

IEEE 802.1X is a 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, devices must be authenticated. The authentication is performed by an authentication server, typically a **RADIUS server**, examples of which are FreeRADIUS and Microsoft Internet Authentication Service.

In Axis implementation, the Axis product and the authentication server identify themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). The certificates are provided by a **Certification Authority (CA)**. You need:

- a CA certificate to authenticate the authentication server.
- a CA-signed client certificate to authenticate the Axis product.

To create and install certificates, go to **Setup > Additional Controller Configuration > System Options > Security > Certificates**. See .

To allow the product to access a network protected by IEEE 802.1X:

1. Go to **Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X**.
2. Select a **CA Certificate** and a **Client Certificate** from the lists of installed certificates.
3. Under **Settings**, select the EAPOL version and provide the EAP identity associated with the client certificate.
4. Check the box to enable IEEE 802.1X and click **Save**.

#### Note

For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See .

### Certificates

Certificates are used to authenticate devices on a network. Typical applications include encrypted web browsing (HTTPS), network protection via IEEE 802.1X and notification messages for example via email. Two types of certificates can be used with the Axis product:

**Server/Client certificates** – To authenticate the Axis product. A **Server/Client** certificate 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** – To authenticate peer certificates, for example the certificate of an authentication server in case the Axis product is connected to an IEEE 802.1X protected network. The Axis product is shipped with several preinstalled CA certificates.

#### Note

- If the product is reset to factory default, all certificates, except preinstalled CA certificates, will be deleted.
- If the product is reset to factory default, all preinstalled CA certificates that have been deleted will be reinstalled.

### How to create a self-signed certificate

1. Go to **Setup > Additional Controller Configuration > System Options > Security > Certificates**.
2. Click **Create self-signed certificate** and provide the requested information.

### How to create and install a CA-signed certificate

1. Create a self-signed certificate, see .
2. Go to **Setup > Additional Controller Configuration > System Options > Security > Certificates**.
3. Click **Create certificate signing request** and provide the requested information.
4. Copy the PEM-formatted request and send to the CA of your choice.
5. When the signed certificate is returned, click **Install certificate** and upload the certificate.

### How to install additional CA certificates

1. Go to **Setup > Additional Controller Configuration > System Options > Security > Certificates**.
2. Click **Install certificate** and upload the certificate.

## Network

### Basic TCP/IP settings

The Axis product supports IP version 4 (IPv4) and IP version 6 (IPv6).

The Axis product can get an IP address in the following ways:

- **Dynamic IP address – Obtain IP address via DHCP** is selected by default. This means that the Axis product is set to get the IP address automatically via Dynamic Host Configuration Protocol (DHCP). DHCP allows network administrators to centrally manage and automate the assignment of IP addresses.
- **Static IP address** – To use a static IP address, select **Use the following IP address** and specify the IP address, subnet mask and default router. Then click **Save**.

DHCP should only be enabled when using dynamic IP address notification, or if the DHCP can update a DNS server that makes it possible to access the Axis product by name (host name).

If DHCP is enabled and the product cannot be accessed, run AXIS IP Utility to search the network for connected Axis products, or reset the product to the factory default settings and then perform the installation again. For information about how to reset to factory default, see .

### AXIS Video Hosting System (AVHS)

AVHS used in conjunction with an AVHS service, provides easy and secure Internet access to controller management and logs accessible from any location. For more information and help to find a local AVHS Service Provider go to [www.axis.com/hosting](http://www.axis.com/hosting)

The AVHS settings are configured under **Setup > Additional Controller Configuration > System Options > Network > TCP IP > Basic**. The possibility to connect to an AVHS service is enabled by default. To disable, clear the **Enable AVHS** box.

**One-click enabled** – Press and hold the product's control button (see ) for about 3 seconds to connect to an AVHS service over the Internet. Once registered, **Always** will be enabled and the Axis product stays connected to the AVHS service. If the product is not registered within 24 hours from when the button is pressed, the product will disconnect from the AVHS service.

**Always** – The Axis product will constantly attempt to connect to the AVHS service over the Internet. Once registered, the product will stay connected to the service. This option can be used when the product is already installed and it is not convenient or possible to use the one-click installation.

#### Note

AVHS support is dependent on the availability of subscriptions from service providers.

### AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Service assigns a host name for easy access to the product. For more information, see [www.axiscam.net](http://www.axiscam.net)

To register the Axis product with AXIS Internet Dynamic DNS Service, go to **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic**. Under **Services**, click the **AXIS Internet Dynamic DNS Service Settings** button (requires access to the Internet). The domain name currently registered at AXIS Internet Dynamic DNS service for the product can at any time be removed.

### Note

AXIS Internet Dynamic DNS Service requires IPv4.

## Advanced TCP/IP Settings

### DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses. The DNS settings are configured under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

Select **Obtain DNS server address via DHCP** to use the DNS settings provided by the DHCP server.

To make manual settings, select **Use the following DNS server address** and specify the following:

**Domain name** – Enter the domain(s) to search for the host name used by the Axis product. Multiple domains can be separated by semicolons. The host name is always the first part of a fully qualified domain name, for example, `myserver` is the host name in the fully qualified domain name `myserver.mycompany.com` where `mycompany.com` is the domain name.

**Primary/Secondary DNS server** – Enter the IP addresses of the primary and secondary DNS servers. The secondary DNS server is optional and will be used if the primary is unavailable.

### NTP Configuration

NTP (Network Time Protocol) is used to synchronize the clock times of devices in a network. The NTP settings are configured under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

Select **Obtain NTP server address via DHCP** to use the NTP settings provided by the DHCP server.

To make manual settings, select **Use the following NTP server address** and enter the host name or IP address of the NTP server.

### Host Name Configuration

The Axis product can be accessed using a host name instead of an IP address. The host name is usually the same as the assigned DNS name. The host name is configured under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

Select **Obtain host name via IPv4 DHCP** to use host name provided by the DHCP server running on IPv4.

Select **Use the host name** to set the host name manually.

Select **Enable dynamic DNS updates** to dynamically update local DNS servers whenever the Axis product's IP address changes. For more information, see the online help.

### Link-Local IPv4 Address

**Link-Local Address** is enabled by default and assigns the Axis product an additional IP address which can be used to access the product from other hosts on the same segment on the local network. The product can have a Link-Local IP and a static or DHCP-supplied IP address at the same time.

This function can be disabled under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

## HTTP

The HTTP port used by the Axis product can be changed under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**. In addition to the default setting, which is 80, any port in the range 1024–65535 can be used.

## HTTPS

The HTTPS port used by the Axis product can be changed under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**. In addition to the default setting, which is 443, any port in the range 1024–65535 can be used.

To enable HTTPS, go to **Setup > Additional Controller Configuration > System Options > Security > HTTPS**. For more information, see .

## NAT traversal (port mapping) for IPv4

A network router allows devices on a private network (LAN) to share a single connection to the internet. This is done by forwarding network traffic from the private network to the "outside", that is, the internet. Security on the private network (LAN) is increased since most routers are pre-configured to stop attempts to access the private network (LAN) from the public network (internet).

Use **NAT traversal** when the Axis product is located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the product.

NAT traversal is configured under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

### Note

- For NAT traversal to work, this must be supported by the router. The router must also support UPnP®.
- In this context, router refers to any network routing device such as a NAT router, Network router, Internet Gateway, Broadband router, Broadband sharing device, or a software such as a firewall.

**Enable/Disable** – When enabled, the Axis product attempts to configure port mapping in a NAT router on your network, using UPnP. Note that UPnP must be enabled in the product (see **Setup > Additional Controller Configuration > System Options > Network > UPnP**).

**Use manually selected NAT router** – Select this option to manually select a NAT router and enter the IP address for the router in the field. If no router is specified, the product automatically searches for NAT routers on your network. If more than one router is found, the default router is selected.

**Alternative HTTP port** – Select this option to manually define an external HTTP port. Enter a port in the range 1024–65535. If the port field is empty or contains the default setting, which is 0, a port number is automatically selected when enabling NAT traversal.

### Note

- An alternative HTTP port can be used or be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.
- If you attempt to manually enter a port that is already in use, another available port is automatically selected.
- When the port is selected automatically it is displayed in this field. To change this, enter a new port number and click **Save**.

## FTP

The FTP server running in the Axis product enables upload of new firmware, user applications, etc. The FTP server can be disabled under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**.

### RTSP

The RTSP server running in the Axis product allows a connecting client to start an event stream. The RTSP port number can be changed under **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced**. The default port is 554.

#### Note

Event streams will not be available if the RTSP server is disabled.

### SOCKS

SOCKS is a networking proxy protocol. The Axis product can be configured to use a SOCKS server to reach networks on the other side of a firewall or proxy server. This functionality is useful if the Axis product is located on a local network behind a firewall, and notifications, uploads, alarms, etc need to be sent to a destination outside the local network (for example the Internet).

SOCKS is configured under **Setup > Additional Controller Configuration > System Options > Network > SOCKS**. For more information, see the online help.

### QoS (Quality of Service)

QoS (Quality of Service) guarantees a certain level of a specified resource to selected traffic on a network. A QoS-aware network prioritizes network traffic and provides a greater network reliability by controlling the amount of bandwidth an application may use.

The QoS settings are configured under **Setup > Additional Controller Configuration > System Options > Network > QoS**. Using DSCP (Differentiated Services Codepoint) values, the Axis product can mark event/alarm traffic and management traffic.

### 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.

To enable and configure SNMP in the Axis product, go to the **Setup > Additional Controller Configuration > System Options > Network > SNMP** page.

Depending on the level of security required, select the version on SNMP to use.

Traps are used by the Axis product to send messages to a management system on important events and status changes. Check **Enable traps** and enter the IP address where the trap message should be sent and the **Trap community** that should receive the message.

#### Note

If HTTPS is enabled, SNMP v1 and SNMP v2c should be disabled.

**Traps for SNMP v1/v2** are used by the Axis product to send messages to a management system on important events and status changes. Check **Enable traps** and enter the IP address where the trap message should be sent and the **Trap community** that should receive the message.

The following traps are available:

- Cold start
- Warm start
- Link up
- Authentication failed

**SNMP v3** provides encryption and secure passwords. To use traps with SNMP v3, an SNMP v3 management application is required.

To use SNMP v3, HTTPS must be enabled, see . To enable SNMP v3, check the box and provide the initial user password.

### Note

The initial password can only be set once. If the password is lost, the Axis product must be reset to factory default, see .

## UPnP

The Axis product includes support for UPnP®. UPnP is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

UPnP can be disabled under **Setup > Additional Controller Configuration > System Options > Network > UPnP**.

## Bonjour

The Axis product includes support for Bonjour. Bonjour is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

Bonjour can be disabled under **Setup > Additional Controller Configuration > System Options > Network > Bonjour**.

## Ports & Devices

### I/O ports

The auxiliary connector provides four configurable input and output ports for connection of external devices.

The external connector provides two configurable input and output ports for connection of external devices.

You can configure the I/O ports under **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports**. Select the port direction (**Input** or **Output**). You can give the ports descriptive names and their **Normal** states can be configured as **Open circuit** or **Grounded circuit**.

### Port Status

The list on the **System Options > Ports & Devices > Port Status** page shows the status of the product's input and output ports.

## Maintenance

The Axis product provides several maintenance functions. These are available under **Setup > Additional Controller Configuration > System Options > Maintenance**.

Click **Restart** to perform a correct restart if the Axis product is not behaving as expected. This will not affect any of the current settings.

### Note

A restart clears all entries in the Server Report.

Click **Restore** to reset most settings to the factory default values. The following settings are not affected:

- the boot protocol (DHCP or static)
- the static IP address
- the default router
- the subnet mask
- the system time
- the IEEE 802.1X settings

Click **Default** to reset all settings, including the IP address, to the factory default values. This button should be used with caution. The Axis product can also be reset to factory default using the control button, see .

For information about firmware upgrade, see .

## Support

### Support Overview

The **Setup > Additional Controller Configuration > System Options > Support > Support Overview** page provides information on troubleshooting and contact information, should you require technical assistance.

See also .

### System Overview

To get an overview of the Axis product's status and settings, go to **Setup > Additional Controller Configuration > System Options > Support > System Overview**. Information that can be found here includes firmware version, IP address, network and security settings, event settings, and recent log items.

### Logs & Reports

The **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports** page generates logs and reports useful for system analysis and troubleshooting. If contacting Axis Support, please provide a server report with your query.

**System Log** – Provides information about system events.

**Access Log** – Lists all failed attempts to access the product. The access log can also be configured to list all connections to the product (see below).

**View Server Report** – Provides information about the product status in a pop-up window. The access log is automatically included in the server report.

**Download Server Report** – Creates a .zip file that contains a complete server report text file in UTF-8 format. Select the **Include snapshot from Live View** option to include a snapshot of the product's Live View. The .zip file should always be included when contacting support.

**Parameter List** – Shows the product's parameters and their current settings. This may prove useful when troubleshooting or when contacting Axis Support.

**Connection List** – Lists all clients that are currently accessing media streams.

**Crash Report** – Generates an archive with debugging information. The report takes several minutes to generate.

The log levels for the system and access logs are set under **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration**. The access log can be configured to list all connections to the product (select Critical, Warnings & Info).

## Advanced

### Scripting

Scripting allows experienced users to customize and use their own scripts.

#### **NOTICE**

Improper use may cause unexpected behavior and loss of contact with the Axis product.

Axis strongly recommends that you do not use this function unless you understand the consequences. Axis Support does not provide assistance for problems with customized scripts.

To open the Script Editor, go to **Setup > Additional Controller Configuration > System Options > Advanced > Scripting**. If a script causes problems, reset the product to its factory default settings, see .

For more information, see [www.axis.com/developer](http://www.axis.com/developer)

### File Upload

Files, for example webpages and images, can be uploaded to the Axis product and used as custom settings. To upload a file, go to **Setup > Additional Controller Configuration > System Options > Advanced > File Upload**.

Uploaded files are accessed through `http://<ip address>/local/<user>/<file name>` where `<user>` is the selected user group (administrator) for the uploaded file.



## 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 .
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.

It is also possible to reset parameters to factory default through the web interface. Go to **Setup > Additional Controller Configuration > Setup > System Options > Maintenance** and click **Default**.

### How to check the current firmware

Firmware is software that determines the functionality of network devices. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem.

The current firmware version in the Axis product is displayed in the Overview page.

### How to upgrade the firmware

#### Important

- Your dealer reserves the right to charge for any repair attributable to faulty upgrade by the user.
- Preconfigured and customized settings are saved when the firmware is upgraded (providing the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.
- If you install a previous firmware version, you need to restore the product to factory default settings afterwards.

#### Note

- After the upgrade process has completed, the product restarts automatically. If you restart the product manually after the upgrade, wait 5 minutes even if you suspect that the upgrade has failed.
  - 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.
  - When you upgrade the Axis product with the latest firmware, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before upgrading the firmware.
1. Download the latest firmware file to your computer, available free of charge at [www.axis.com/support](http://www.axis.com/support)
  2. Go to **Setup > Additional Controller Configuration > System Options > Maintenance** in the product's webpages.
  3. Under **Upgrade Server**, click **Choose file** and locate the file on your computer.
  4. If you want the product to automatically restore to factory default settings after the upgrade, check the **Default** checkbox.

5. Click **Upgrade**.
6. Wait approximately 5 minutes while the product is being upgraded and restarted. Then clear the web browser's cache.
7. Access the product.

### Symptoms, possible causes and remedial actions

#### Problems upgrading the firmware

---

Firmware upgrade failure	If the firmware upgrade fails, the product reloads the previous firmware. Check the firmware file and try again.
--------------------------	--

#### Problems setting the IP address

---

When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the product. Make sure the Ping length is set to 408. For instructions, see Installation Guide on the product page at <a href="http://axis.com">axis.com</a> .
The product is located on a different subnet	If the IP address intended for the product and the IP address of the computer used to access the product are located on different subnets, you will not be able to 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 product from the network. Run the Ping command (in a Command/DOS window, type <code>ping</code> and the IP address of the product):</p> <ul style="list-style-type: none"> <li>• If you receive: <code>Reply from &lt;IP address&gt;: 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 product.</li> <li>• If you receive: <code>Request timed out</code>, this means that the IP address is available for use with the Axis product. Check all cabling and reinstall the product.</li> </ul>
Possible IP address conflict with another device on the same subnet	The static IP address in the Axis product 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 product.

#### The product cannot be accessed from a browser

---

Cannot log in	<p>When HTTPS is enabled, make sure 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 product must be reset to the factory default settings. See .</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 product on the network. Identify the product 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, see the document How to assign an IP address and access your device on the product page at <a href="http://axis.com">axis.com</a></p>
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See .

### **The product is accessible locally but not externally**

---

Router configuration	To configure your router to allow incoming data traffic to the Axis product, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the Axis product, see . The router must support UPnP®.
Firewall protection	Check the Internet firewall with your network administrator.
Default routers required	Check if you need to configure the router settings from <b>Setup &gt; Network Settings</b> or <b>Setup &gt; Additional Controller Configuration &gt; System Options &gt; Network &gt; TCP/IP &gt; Basic</b> .

## Specifications

Text marked with **UL** is only valid for UL 293 or UL 294 installations.

### 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 overcurrent	Red	Steady when short circuited or if overcurrent has been detected.
	Unlit	Normal operation.
Reader overcurrent	Red	Steady when short circuited or if overcurrent has been detected.
	Unlit	Normal operation.
Relay	Green	Relay active. <sup>2</sup>
	Unlit	Relay inactive.

#### Note

- The Status LED can be configured to flash while an event is active.
- The Status LED can be configured to flash for identifying the unit. Go to **Setup > Additional Controller Configuration > System Options > Maintenance**.

### Buttons

#### Control button

The control button is used for:

- Resetting the product to factory default settings. See .

### Connectors

#### Network connector

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

**UL:** Power over Ethernet (PoE) shall be supplied by a UL 294 listed Power 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.

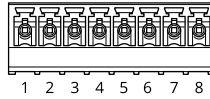
<sup>2</sup>. Relay is active when COM is connected to NO.

## Reader connector

Two 8-pin terminal blocks supporting both RS485 and Wiegand protocols for communication with the reader.

The specified power output values are shared between the two reader ports. It means that 486 mA at 12 V DC is reserved for all readers connected to the door controller.

Select which protocol to use in the product's web page.



### Configured for RS485

Function	Pin	Note	Specifications
DC ground (GND)	1		0 V DC
DC output (+12 V)	2	Supplies power to reader.	12 V DC, max 486 mA combined for both readers
RX/TX	3–4	Full duplex: RX. Half duplex: RX/TX.	
TX	5–6	Full duplex: TX.	
Configurable (Input or Output)	7–8	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
		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 200 m (656 ft).
- 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.

### Configured for Wiegand

Function	Pin	Note	Specifications
DC ground (GND)	1		0 V DC
DC output (+12 V)	2	Supplies power to reader.	12 V DC, max 486 mA combined for both readers
D0	3		
D1	4		
0	5–6	Digital output, open drain	

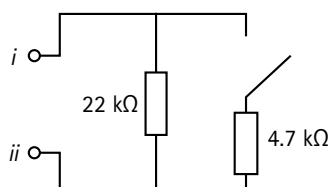
Configurable (Input or Output)	7–8	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
		Digital output – If used with an inductive load, e. g., a relay, connect a diode in parallel with the load, to protect against voltage transients.	0 to max 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.

**Supervised inputs**

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



i Input

ii 0 V DC (-)

UL: Supervised inputs were not evaluated by UL for burglary use. Only door monitor and REX support supervision with end of line resistors.

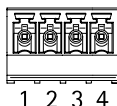
**Note**

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

**Door connector**

Two 4-pin terminal blocks 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 .



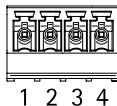
Function	Pin	Notes	Specifications
DC ground	1, 3		0 V DC
Input	2, 4	For communicating with door monitor. Digital input or Supervised input – Connect to pin 1 or 3 respectively to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC

**Important**

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

## Relay connector

Two 4-pin terminal blocks 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 per relay 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.

Power source	Max power at 12 V DC <sup>3</sup>	Max power at 24 V DC <sup>3</sup>
DC IN	1 600 mA	800 mA
PoE	800 mA	400 mA

**NOTICE**

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

## Auxiliary connector

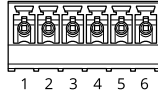
Use the auxiliary connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the auxiliary connector provides the interface to:

**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.

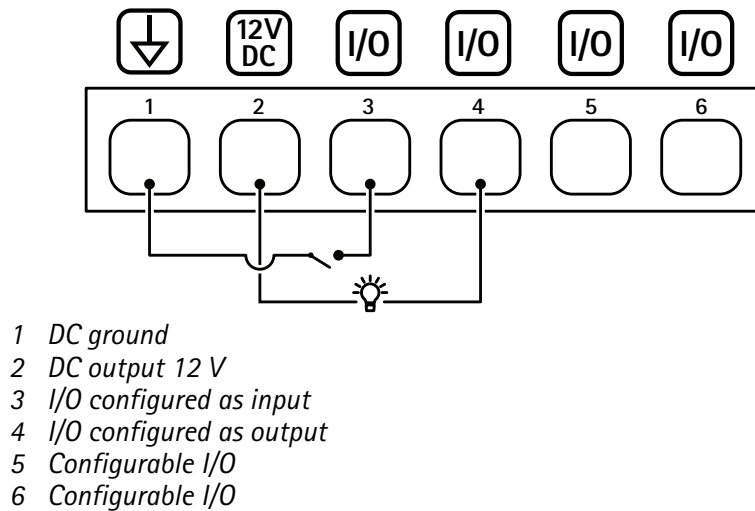
**Digital output** – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface or from the product's webpage.

3. The power is shared between the two relays and AUX I/O 12 V DC.

**6-pin terminal block**



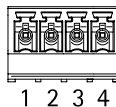
Function	Pin	Notes	Specifications
DC ground	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 V DC Max load = 50 mA for each I/O
Configurable (Input or Output)	3–6	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	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



**External connector**

4-pin terminal block for external devices, for example glass break or fire detectors.

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



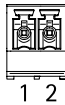
Function	Pin	Notes	Specifications
DC ground	1, 3		0 V DC



Configurable (Input or Output)	2, 4	Digital input – Connect to pin 1 or 3 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
		Digital output – Connect to pin 1 or 3 to activate, or leave floating (unconnected) to deactivate. 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

### 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  $\leq 100$  W or a rated output current limited to  $\leq 5$  A.



Function	Pin	Notes	Specifications
0 V DC (-)	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.	10.5–28 V DC, max 36 W

**UL:** DC power to be supplied by a UL 294, UL 293 or UL 603 listed power supply, depending on application, with appropriate ratings.

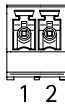
### Backup battery input connector

For a backup solution using a battery with built-in charger. 12 V DC input.

**UL:** The connector has not been evaluated by UL.

#### Important

When the battery input is used, an external 3 A slow blow fuse must be connected in series.



Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
Battery input	2	For powering the door controller when other power sources are unavailable. Note: This pin can only be used as battery power in. For connection to UPS only.	11– 13.7 V DC, max 36 W

## Safety information

### Hazard levels

#### **▲ DANGER**

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

#### **▲ WARNING**

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

#### **▲ CAUTION**

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

#### **NOTICE**

Indicates a situation which, if not avoided, could result in damage to property.

### Other message levels

#### **Important**

Indicates significant information which is essential for the product to function correctly.

#### **Note**









Indicates useful information which helps in getting the most out of the product.

## The web interface

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

### Note

This section is only valid for AXIS A1601 Network Door Controller with AXIS Camera Station Secure Entry firmware.

-  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 AXIS OS version and serial number.

## Status

### Time sync status

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

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

### Device info


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


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


## Device

### Alarms

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

**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 $\Omega$  parallel resistor and a 4.7 K $\Omega$  serial resistor**.
  - To use serial first connection, select **Serial first connection** and select a resistor value from the **Resistor values** drop-down list.

## Peripherals

### Readers

 **Add reader:** Click to add a new reader.

**Name:** Enter a name for the reader.

**Reader:** Select a reader from the drop-down list.

**IP address:** Enter the IP address of the reader manually.

**Username:** Enter the username of the reader.

**Password:** Enter the password of the reader.

**Ignore server certificate verification:** Turn on to ignore verification.

## System

### Time and location

#### Date and time

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

#### Note

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

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

- **Automatic date and time (manual NTS KE servers):** Synchronize with the secure NTP key establishment servers connected to the DHCP server.
  - **Manual NTS KE servers:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
  - **Max NTP poll time:** Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
  - **Min NTP poll time:** Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
- **Automatic date and time (NTP servers using DHCP):** Synchronize with the NTP servers connected to the DHCP server.
  - **Fallback NTP servers:** Enter the IP address of one or two fallback servers.
  - **Max NTP poll time:** Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
  - **Min NTP poll time:** Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
- **Automatic date and time (manual NTP servers):** Synchronize with NTP servers of your choice.
  - **Manual NTP servers:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
  - **Max NTP poll time:** Select the maximum amount of time the device should wait before it polls the NTP server to get an updated time.
  - **Min NTP poll time:** Select the minimum amount of time the device should wait before it polls the NTP server to get an updated time.
- **Custom date and time:** Manually set the date and time. Click **Get from system** to fetch the date and time settings once from your computer or mobile device.

**Time zone:** Select which time zone to use. Time will automatically adjust to daylight saving time and standard time.

- **DHCP:** Adopts the time zone of the DHCP server. The device must be connected to a DHCP server before you can select this option.
- **Manual:** Select a time zone from the drop-down list.

**Note**

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

## Network

### IPv4

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

**IP address:** Enter a unique IP address for the device. Static IP addresses can be assigned at random within isolated networks, provided that each address is unique. To avoid conflicts, we recommend you contact your network administrator before you assign a static IP address.

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

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

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

### Note

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

## IPv6

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

## Hostname

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

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

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

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

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

## DNS servers

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

**Search domains:** When you use a hostname that is not fully qualified, click **Add search domain** and enter a domain in which to search for the hostname the device uses.

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

## 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.

**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.

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

### 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](https://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.
    - **Link up:** Sends a trap message when a link changes from down to up.
    - **Link down:** Sends a trap message when a link changes from up to down.
    - **Authentication failed:** Sends a trap message when an authentication attempt fails.

**Note**

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

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

## Connected clients

Shows the number of connections and connected clients.

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

## Security

### Certificates

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

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

These formats are supported:


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

#### Important

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



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

- **More**  : Show more fields to fill in or select.
- **Secure keystore**: Select to use **Trusted Execution Environment (SoC TEE)**, **Secure element** or **Trusted Platform Module 2.0** to securely store the private key. For more information on which secure keystore to select, go to [help.axis.com/en-us/axis-os#cryptographic-support](http://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**  :

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

## Network access control and encryption

## IEEE 802.1x

IEEE 802.1x is an IEEE standard for port-based network admission control providing secure authentication of wired and wireless network devices. IEEE 802.1x is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1x, network devices must authenticate themselves. The authentication is performed by an authentication server, typically a RADIUS server (for example, FreeRADIUS and Microsoft Internet Authentication Server).

## IEEE 802.1AE MACsec

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

## Certificates

When configured without a CA certificate, server certificate validation is disabled and the device tries to authenticate itself regardless of what network it is connected to.

When using a certificate, in Axis' implementation, the device and the authentication server authenticate themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

To allow the device to access a network protected through certificates, you must install a signed client certificate on the device.

**Authentication method:** Select an EAP type used for authentication.

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

**CA certificates:** Select CA certificates to validate the authentication server's identity. When no certificate is selected, the device tries to authenticate itself regardless of what network it is connected to.

**EAP identity:** Enter the user identity associated with the client certificate.

**EAPOL version:** Select the EAPOL version that is used in the network switch.

**Use IEEE 802.1x:** Select to use the IEEE 802.1x protocol.

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

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

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

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

## Prevent brute-force attacks

**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.

### Firewall

**Activate:** Turn on the firewall.

**Default Policy:** Select the default state for the firewall.

- **Allow:** Allows all connections to the device. This option is set by default.
- **Deny:** Denies all connections to the device.

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

- **Address:** Enter an address in IPv4/IPv6 or CIDR format that you want to allow or deny access to.
- **Protocol:** Select a protocol that you want to allow or deny access to.
- **Port:** Enter a port number that you want to allow or deny access to. You can add a port number between 1 and 65535.
- **Policy:** Select the policy of the rule.



: Click to create another rule.

**Add rules:** Click to add the rules that you have defined.

- **Time in seconds:** Set a time limit for testing the rules. The default time limit is set to 300 seconds. To activate the rules straight away, set the time to 0 seconds.
- **Confirm rules:** Confirm the rules and their time limit. If you have set a time limit of more than 1 second, the rules will be active during this time. If you have set the time to 0, the rules will be active straight away.

**Pending rules:** An overview of the latest tested rules that you are yet to confirm.

#### Note

The rules that have a time limit appear under **Active rules** until the displayed timer runs out, or until you confirm them. If you don't confirm them, they will appear under **Pending rules** once the timer runs out, and the firewall will revert to the previously defined settings. If you confirm them, they will replace the current active rules.

**Confirm rules:** Click to activate the pending rules.

**Active rules:** An overview of the rules you are currently running on the device.



: Click to delete an active rule.



: Click to delete all rules, both pending and active.

### Custom signed AXIS OS certificate

To install test software or other custom software from Axis on the device, you need a custom signed AXIS OS certificate. The certificate verifies that the software is approved by both the device owner and Axis. The software can only run on a specific device which is identified by its unique serial number and chip ID. Only Axis can create custom signed AXIS OS certificates, since Axis holds the key to sign them.

**Install:** Click to install the certificate. You need to install the certificate before you install the software.



The context menu contains:

- **Delete certificate:** Delete the certificate.

## Accounts

### 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.
- **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 software 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 Knowledge base*.

## 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.

**HTTP proxy:** A URL with a maximum length of 255 bytes. You can leave the field empty if you don't want to use an HTTP proxy.

**HTTPS proxy:** A URL with a maximum length of 255 bytes. You can leave the field empty if you don't want to use an HTTPS proxy.

**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.

**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



**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 VDC.

### 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

#### 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 to use:

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

**Port:** Edit the port number to use a different port.

**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 presets.

### Important

The only settings saved after restore are:

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

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

### Note

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

**AXIS OS upgrade:** Upgrade to a new AXIS OS version. New releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest AXIS OS release. To download the latest release, go to [axis.com/support](https://axis.com/support).

When you upgrade, you can choose between three options:

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

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

T10125657

2025-04 (M13.2)

© 2018 – 2025 Axis Communications AB