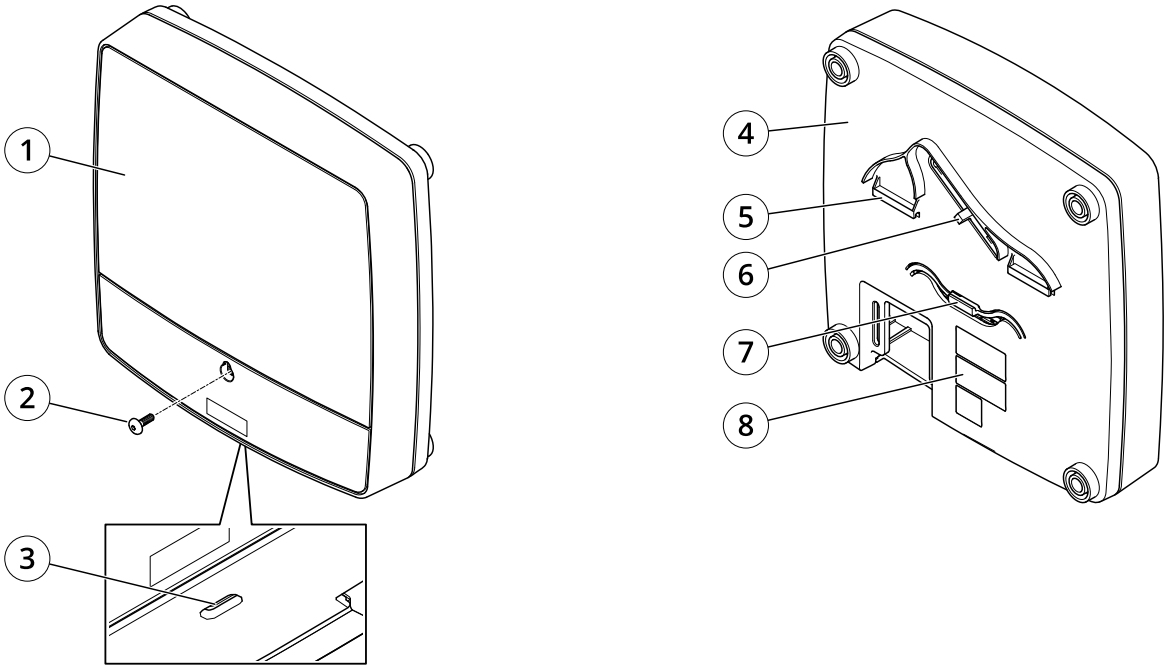
AXIS A1001 and AXIS Entry Manager

User manual

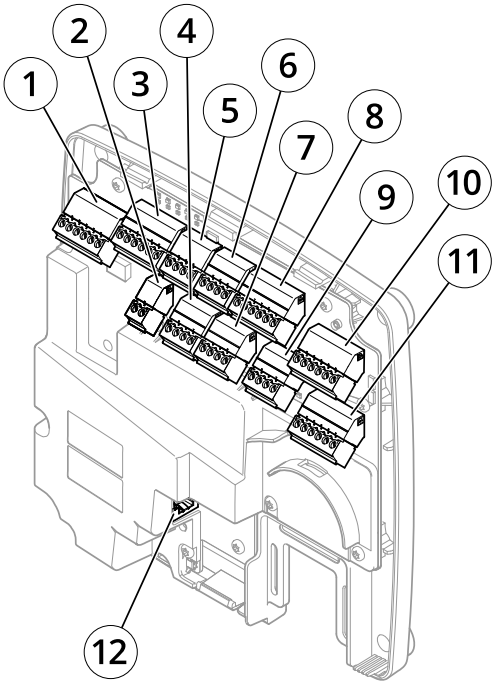
Table of Contents

Product overview



Front and back:

1 *Cover*
2 *Cover screw*
3 *Cover removal slot*
4 *Base*
5 *DIN clip – upper*
6 *Tampering alarm switch – back*
7 *DIN clip – lower*
8 *Part number (P/N) & Serial number (S/N)*



I/O interface:

1 *Reader data connector (READER DATA 1)*
2 *Reader data connector (READER DATA 2)*
3 *Reader I/O connector (READER I/O 1)*

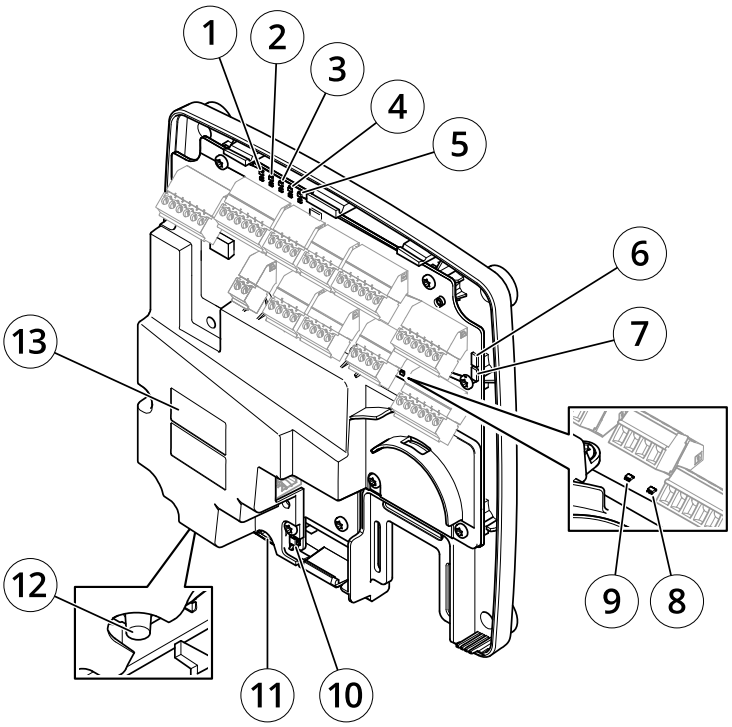
4 *Reader I/O connector (READER I/O 2)*
5 *Door connector (DOOR IN 1)*
6 *Door connector (DOOR IN 2)*
7 *Auxiliary connector (AUX)*
8 *Audio connector (AUDIO) (not used)*

External power inputs:

1 *Power connector (DC IN)*
2 *Network connector (PoE)*

Power outputs:

1 *Power lock connector (LOCK)*
2 *Power & Relay connector (PWR, RELAY)*



LED indicators, buttons and other hardware:

1 *Power LED indicator*
2 *Status LED indicator*
3 *Network LED indicator*
4 *Reader 2 LED indicator (not used)*
5 *Reader 1 LED indicator (not used)*
6 *Tampering alarm pin header – front (TF)*
7 *Tampering alarm pin header – back (TB)*
8 *Lock LED indicator*
9 *Lock LED indicator*
10 *Tampering alarm sensor – front*
11 *SD card slot (microSDHC) (not used)*
12 *Control button*
13 *Part number (P/N) & Serial number (S/N)*

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.
Lock	Green	Steady when not energized.
	Red	Steady when energized.
	Unlit	Floating.

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** .

Connectors and buttons

I/O Interface

Reader Data Connectors
Two 6-pin terminal blocks supporting RS485 and Wiegand protocols for communication with the reader. For specifications, see .

Reader I/O Connectors
Two 6-pin terminal blocks for reader input and output. In addition to the 0 V DC reference point and power (DC output), the reader I/O connector provides the interface to:

- Digital input – For connecting, for example, reader tampering alarms.
- Digital output – For connecting, for example, reader beepers and reader LEDs.

For specifications, see .

Door Connectors
Two 4-pin terminal blocks for connecting door monitoring devices and request to exit (REX) devices. For specifications, see .

Auxiliary Connector
4-pin configurable I/O terminal block. Use with external devices, in combination with, for example tampering alarms, 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 – An alarm input for connecting devices that can toggle between an open and closed circuit, for example PIR sensors or glass break detectors.
- Digital output – For connecting external devices such as burglar alarms, sirens or lights. Connected devices can be activated by the VAPIX® application programming interface or by an action rule.

For specifications, see .

External Power Inputs

NOTICE

The product shall be connected using a shielded network cable (STP). All cables connecting the product to the network shall be intended for their specific use. Make sure that the network devices are installed in accordance with the manufacturer's instructions. For information about regulatory requirements, see .

Power Connector

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

Network Connector
RJ45 Ethernet connector. Supports Power over Ethernet (PoE). For specifications, see .

Power Outputs

Power Lock Connector

4-pin terminal block for connecting one or two locks. The lock connector can also be used to power external devices. For specifications, see .

Power & Relay Connector

6-pin terminal block for connecting power and the door controller's relay to external devices such as locks and sensors. For specifications, see .

Buttons and Other Hardware

Tampering Alarm Pin Header
Two 2-pin headers for disconnecting the front and back tampering alarms. For specifications, see .

Control Button
The control button is used for:

- Resetting the product to factory default settings. See .
- Connecting to an AXIS Video Hosting System service. See . To connect, press and hold the button for about 1 second until the Status LED flashes green.
- Connecting to AXIS Internet Dynamic DNS Service. See . To connect, press and hold the button for about 3 seconds.

Installation

Installation video for the product.

How to access the product

To install the Axis product, see the Installation Guide supplied with the product.

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. AXIS Entry Manager opens in your browser. If you are using a computer, you will reach the Overview page. If you are using a mobile device, you will reach the mobile landing page.

About the mobile landing page

The mobile landing page shows the status of doors and locks connected to the door controller. You can test to lock and unlock. Refresh the page to see the result.

A link takes you to Axis Entry Manager.

Note

- Axis Entry Manager doesn't support mobile devices.
- If you continue to Axis Entry Manager, there is no link back to the mobile landing 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.

See also AXIS Internet Dynamic DNS Service at *www.axiscam.net*

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®.

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 AXIS Entry Manager 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 or in the system.

The first time you access the Axis product, the Overview page will prompt you to configure the hardware, to set date and time, to configure the network settings, and to configure the door controller as part of a system or as a standalone unit. 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 , , and .

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 AXIS Entry Manager 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 .
7. Configure the door controller system. See .

For information about how to configure and manage the system's doors, schedules, users and groups, see .

For information about maintenance recommendations, see .

Note

To add or remove door controllers, to add, remove, or edit users, or to configure the hardware, more than half of the door controllers in the system must be **online**. To check the door controller status, go to **Setup > Manage Network Door Controllers in System**.

Select a language

The default language of AXIS Entry Manager 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*

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, AXIS Entry Manager switches back to English.
- If you restore the product, AXIS Entry Manager will continue to use the selected language.
- If you restart the product, AXIS Entry Manager will continue to use the selected language.
- If you upgrade the firmware, AXIS Entry Manager will continue to use the selected language.

Set the Date and Time

If the door controller is part of a system, the date and time settings will be distributed to all the door controllers. This means that the settings are pushed to the other controllers in the system, regardless of whether you synchronize with an NTP server, set the date and time manually, or get the date and time from the computer. If you cannot see the changes, try refreshing the page in your browser. For more information about managing a system of door controllers, see .

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

Before you can manage the doors and floors, the hardware must be configured in the Hardware Configuration pages.

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.
- Motorized locks must be configured as secondary locks.

About door monitor and time options

The following door monitor options are available:

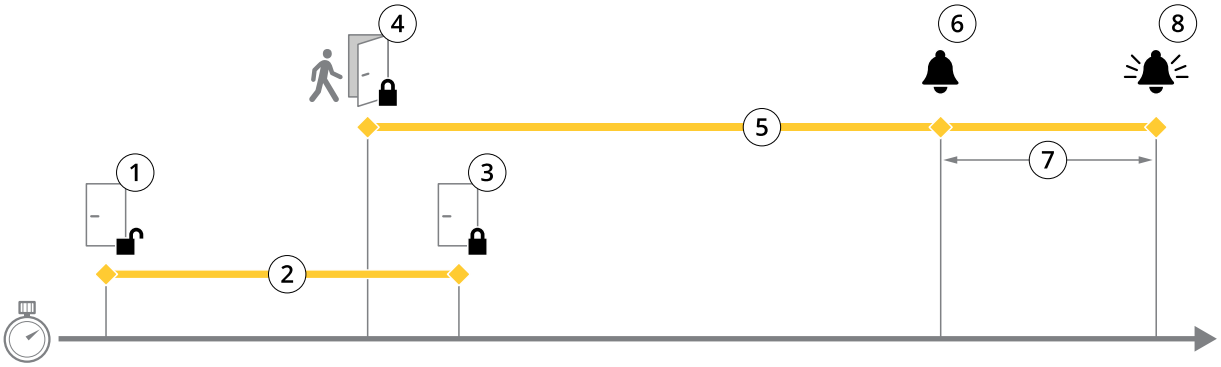
- **Door monitor** – Selected by default. Each door has its own door monitor that, for example, will signal when the door has been forced open or open too long. Deselect if no door monitor will be used.
  - **Open circuit = Closed door** – Select if the door monitor circuit is normally open. The door 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, see

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:

- 12 V

– **Fail-secure** – Select for locks that remain locked during power outages. When applying electric current, the lock will unlock.

– **Fail-safe** – Select for locks that unlock during power outages. When applying electric current, the lock will lock.

- **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.
  – **Relay open = Locked** – Select for locks that remain locked when the relay is open (fail-secure). When the relay closes, the lock will unlock.
  – **Relay open = Unlocked** – Select for locks that unlock during power outages (fail-safe). When the relay closes, the lock will lock.
- **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 readers, REX devices, and 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 connectors support supervised inputs:

- Reader I/O connector – tampering signal. See .
- Door connector. See .

Readers and switches that can be used with supervised inputs include:

- Readers and switches with internal 1 kΩ pull-up to 5 V.
- Readers and switches without internal pull-up.

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 A1001, 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 periphals 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 Periphals** 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 periphals 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 Periphals** 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**.

The floor is now visible in the **Floor** tab under **Access Management**.

Note

In AXIS Entry Manager you can add maximum 16 floors.

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:graphicB11ACA0E385B57DCF1D209C45A83E2AD″ 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:graphicBC6471AF6421E76E83F4F72C0A258C1D″

To delete a card format, click ,255mm,sfx)=″graphics:graphicBC6471AF6421E76E83F4F72C0A258C1D″.

Important

- All changes to card formats apply to the whole system of door controllers.
- You can only enable and disable card formats if at least one door controller in the system 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.

Preset facility code

Facility codes are sometimes used for verifying that the token matches the facility's access control system. Often all tokens issued for a single facility have the same facility code. Enter a preset facility code to allow easier manual registration of a batch of cards. The preset facility code is automatically filled in when adding users, see

To set a preset facility code:

1. Go to **Setup > Configure cards and formats**.
2. Under **Preset facility code**: Enter a facility code.
3. Click **Set facility code**.

Configure Services

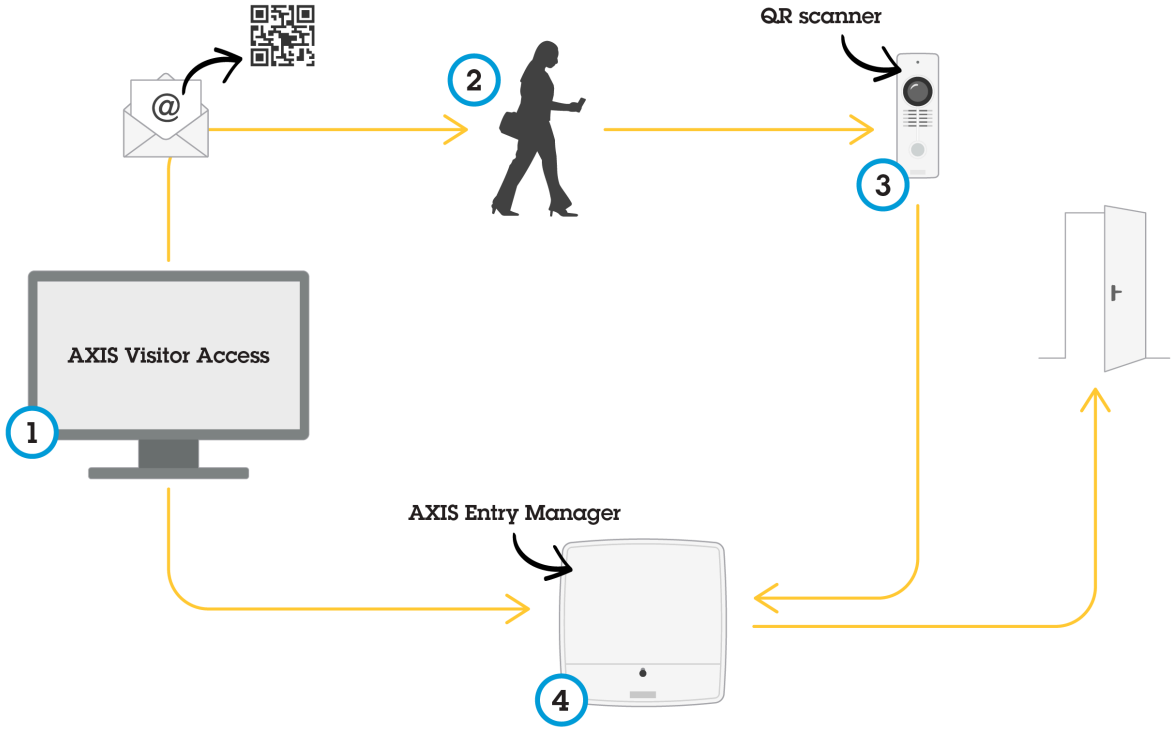
The Configure Services in the Setup page is used to access the set up for the external services that can be used with the door controller.

AXIS Visitor Access

With AXIS Visitor Access, temporary credentials can be created in the form of a QR code. An Axis network camera or door station connected to the access control system scans the QR code.

The service consists of:

- an Axis door controller with AXIS Entry Manager and firmware version 1.65.2 or higher
- an Axis network camera or door station, with the QR scanner application installed
- a Windows® PC with the AXIS Visitor Access application installed



Usage of AXIS Visitor Access service

The user creates an invitation in AXIS Visitor Access (1) and sends the invitation to the visitor's email address. At the same time the credentials to unlock the door are created and stored in the connected Axis door controller (4). The visitor shows the QR code included in the invitation at the network camera or door station (3), which asks the door controller (4) to unlock the door for the visitor.

QR Code is a registered trademark of Denso Wave, inc.

Prerequisites AXIS Visitor Access

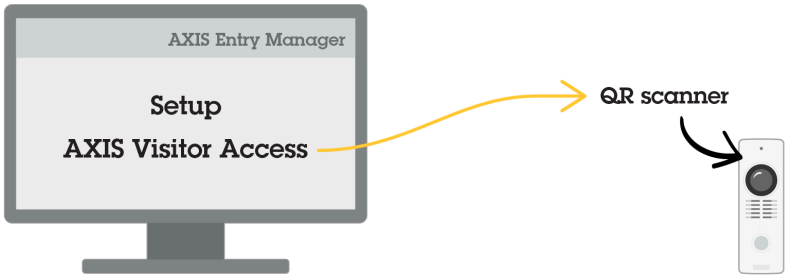
Before you can use the AXIS Visitor Access service, you need:

- to configure the door controller hardware
- an Axis network camera or door station connected to the same network as the door controller, and placed accessible to the visitor by the door
- the AXIS Visitor Access installation package. You can find it at *axis.com*
- two additional user accounts in the door controller, only to be used by the AXIS Visitor Access service. You need one for the AXIS Visitor Access application, and the other for the QR scanner application. To find out how to create user accounts, see

Important

- You can only connect the AXIS Visitor Access service to a single door controller in the entire system.
- With the AXIS Visitor Access service, you can only address doors that are controlled by the connected door controller. You cannot address other doors in the system.
- Use the AXIS Visitor Access application to modify and delete visitors. Do not use AXIS Entry Manager.
- If you change the password of the user account used for AXIS Visitor Access, you need to update it also in AXIS Visitor Access.
- If you change the password of the user account used for the QR scanner application, you need to set up the QR scanner again.

Set up AXIS Visitor Access



You install the QR scanner application on the Axis network camera or door station when you set up the AXIS Visitor Access service. You don't need to make any separate installation.

1. In the door controller's webpage, go to **Setup > Configure Services > Settings**.
2. Click **Start a new setup**.
3. Follow the instructions to finalize the setup.

Important

If you want to enforce HTTPS, make sure that the door controller communicates through HTTPS. Otherwise the application will not be able to communicate with the door controller.

4. On the computer that will be used for creating temporary credentials, install and set up the AXIS Visitor Access application.

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.

Manage Network Door Controllers

The Manage Network Door Controllers in System page shows information about the door controller, its system status, and which other door controllers are part of the system. It also enables the administrator to change the system setup by adding and removing door controllers.

Important

All door controllers in a system must be connected to the same network, and be setup for use at a single site.

To manage door controllers, go to **Setup > Manage Network Door Controllers in System**.

The Manage Network Door Controllers in System page includes the following panels:

- **System status of this controller** – Shows the door controller's system status and enables switching between system and standalone modes. For more information, see .
- **Network door controllers in system** – Shows information about the door controllers in the system and includes controls for adding and removing a controller from the system. For more information, see .

Door Controller System Status

If the door controller can be part of a system of door controllers depends on its system status. The door controller's system status is displayed in the **System status for this controller** panel.

If the door controller is not in standalone mode and you want to protect the door controller from being added to a system, click **Activate standalone mode** to enter standalone mode.

If the door controller is in standalone mode but you intend to add the door controller to a system, click **Deactivate standalone mode** to leave the standalone mode.

System Modes

- **This controller is not part of a system and not in standalone mode** – The door controller has not been configured as part of a system and it is not in standalone mode. This means that the door controller is open and can be added to a system by any other door controller within the same network. To protect the door controller from being added to a system, activate the standalone mode.
- **This controller is set to standalone mode** – The door controller is not part of a system. It cannot be added to a system by other door controllers in the network or add other door controllers itself.

Standalone mode is typically used in small setups with one door controller and one or two doors. To allow the door controller to be added into a system, deactivate the standalone mode.

- **This controller is part of a system** – The door controller is part of a distributed system. In the distributed system, users, groups, doors, and schedules are shared between the connected controllers.

Connected Door Controllers in the System

The **Network door controllers in system** panel provides controls for the following system changes:

- Add a door controller to a system, see .
- Remove a door controller from a system, see .

Connected Door Controllers List

The **Network door controllers in system** panel also includes a list that shows the following ID and status information about the connected door controllers in the system:

- **Name** – The user-defined name of the door controller. If the administrator has not set a name when configuring the hardware, the default name will be shown.
- **IP address**
- **MAC address**
- **Status** – The door controller from which you access the system will show status **This controller**. The other door controllers in the system will show status **Online**.
- **Firmware version**

To open the webpages of another door controller, click the controller's IP address.

To update the list, click **Refresh the list of controllers**.

Note

All controllers in a system always need to have the same firmware version. Use Axis Device Manager to do a parallel firmware upgrade on all controllers in the entire system.

Add Door Controllers to the System

Important

When pairing door controllers, all access management settings on the added door controller will be deleted and overwritten by the system's access management settings.

To add a door controller to the system from the list of door controllers:

1. Go to **Setup > Manage Network Door Controllers in System**.
2. Click **Add controllers to system from list**.
3. Select the door controller that you wish to add.
4. Click **Add**.
5. To add more door controllers, repeat the steps above.

To add a door controller to the system by its known IP address or MAC address:

1. Go to **Manage Devices**.
2. Click **Add controller to system by IP or MAC address**.
3. Enter the IP address or MAC address.
4. Click **Add**.
5. To add more door controllers, repeat the steps above.

When the pairing is completed, all users, doors, schedules, and groups are shared by all door controllers in the system.

To update the list, click **Refresh list of controllers**.

Remove Door Controllers from the System

Important

- Before removing a door controller from the system, reset its hardware configuration. If you skip this step, all doors related to the removed door controller will remain in the system and cannot be deleted.
- When removing a door controller from a two-controller system, both door controllers automatically switch to standalone mode.

To remove a door controller from the system:

1. Access the system through the door controller that you want to remove and go to **Setup > Hardware Configuration**.
2. Click **Reset hardware configuration**.
3. After the hardware configuration has been reset, go to **Setup > Manage Network Door Controllers in System**.
4. In the **Network door controllers in system** list, identify the door controller that you want to remove and click **Remove from system**.
5. A dialog opens reminding you to reset the door controller's hardware configuration. Click **Remove controller** to confirm.
6. A dialog opens prompting you to confirm that you want to remove the door controller. Click **OK** to confirm. The removed door controller is now in standalone mode.

Note

- When a door controller is removed from the system, all its access management settings are deleted.
- Only door controllers that are online can be removed.

Configuration mode

Configuration mode is the standard mode when you access the device for the first time. When configuration mode is disabled most of the configuration features for the device are hidden.

Important

To disable configuration mode should not be considered a security feature. It is intended to stop configuration mistakes and not to stop malicious users changing vital settings.

How to disable configuration mode

1. Go to **Setup** > **Disable Configuration Mode**.
2. Enter a PIN and select **OK**.

Note

PIN is not mandatory.

How to enable configuration mode

1. Go to **Setup** > **Enable Configuration Mode**.
2. Enter the PIN and select **OK**.

Note

If you don not remember your PIN you can enable configuration mode by entering `http://[IP-address]/webapp/pacs/index.shtml#resetConfigurationMode`.

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 .

- Make sure all access schedules, doors, groups, and users are up to date.
- If the door controller is not behaving as expected, see and for more information.

Access Management

About Users

In AXIS Entry Manager, users are people who have been registered as owners of one or more tokens (identification types). Each person must have a unique user profile to be granted access to doors in the access control system. The user profile consists of credentials that tell the system who the user is and when and how they are granted access to doors. For more information, see .

Users in this context should not be confused with administrators. Administrators have unrestricted access to all settings. And in the context of managing the access control system, the product's web pages (AXIS Entry Manager), administrators are also sometimes referred to as users. For more information, see .

The Access Management Page

The Access Management page allows you to configure and manage the system's users, groups, doors, and schedules. To open the Access Management page, click **Access Management**.

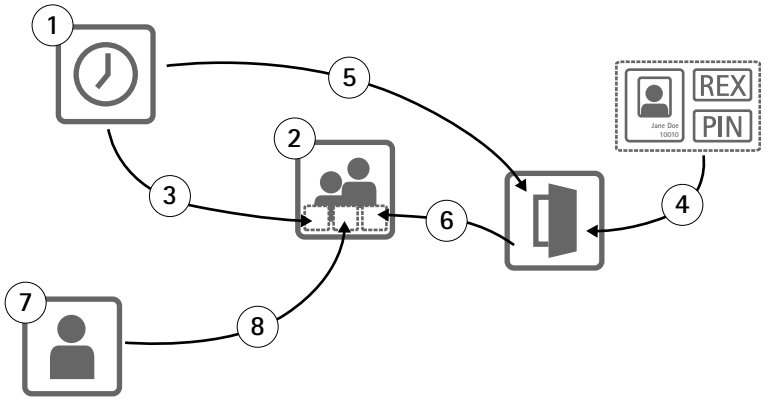
To add users to groups and apply access schedules and doors, drag the items to their respective destination in the **Groups** and **Doors** lists.

Note

Messages that require action are shown in red text.

Choose a Workflow

The access management structure is flexible, allowing you to develop a workflow that suits your needs. The following is a workflow example:



1. Create access schedules. See .
2. Create groups. See .
3. Apply access schedules to groups.
4. Add identification types to doors or floors. See and .
5. Apply access schedules to each identification type.
6. Apply doors or floors to groups.
7. Create users. See .
8. Add users to groups.

For applied examples of this workflow, see .

Create and Edit Access Schedules

Access schedules are used to define general rules for when doors can and cannot be accessed. They are also used to define rules for when groups can and cannot access the doors in the system. For more information, see .

To create a new access schedule:

1. Go to **Access Management**.
2. In the **Access Schedules** tab, click **Add new schedule**.
3. In the **Add access schedule** dialog, enter the schedule name.
4. To create a regular access schedule, select **Addition Schedule**.
   Or to create a subtraction schedule, select **Subtraction Schedule**.
   For more information, see .
5. Click **Save**.

To expand an item in the **Access Schedules** list, click . Addition schedules are shown in green text and subtraction schedules are shown in dark red text.

To view an access schedule's calendar, click .

To edit an access schedule's name or a schedule item, click ,255mm,sfx)=″graphics:graphicB11ACA0E385B57DCF1D209C45A83E2AD″ and make the changes. Then click **Save**.

To delete an access schedule, click ,255mm,sfx)=″graphics:graphicBC6471AF6421E76E83F4F72C0A258C1D″.

Note

The door controller has a few predefined commonly used access schedules that can be used as examples or modified as required. However, the predefined access schedule **Always** cannot be modified or deleted.

Access Schedule Types

There are two types of access schedules:

- **Addition schedule** – Regular access schedules that define when doors can be accessed. Typical addition schedules are office hours, business hours, after hours, or night time hours.
- **Subtraction schedule** – Exceptions to regular access schedules. They are generally used to restrict access during a specific time period that occurs within the time period of a regular schedule (addition schedule). For example, subtraction schedules can be used to deny users access to the building during public holidays that occur on weekdays.

Both types of access schedules can be used at two levels:

- **Identification type schedules** – Determine when and how readers grant users access to a door. Each identification type must be connected to an access schedule that tells the system when to grant users access with that particular identification type. Multiple addition schedules and subtraction schedules can be added to each identification type. For information about identification types, see .
- **Group schedules** – Determine when, but not how, members of a group are granted access to a door. Each group must be connected to one or more access schedules that tell the system when to grant its members access. Multiple addition schedules and subtraction schedules can be added to each group. For information about groups, see .

Group schedules can restrict entry access rights but not extend entry or exit access rights beyond what the identification type schedules allow. In other words, if an identification type schedule restricts entry or exit access at certain times, a group schedule cannot override that identification type schedule. However, if a group schedule is more restrictive about access than the identification type schedule, the group schedule overrides the identification type schedule.

Identification type schedules and group schedules can be combined in several ways to achieve different results. For example access schedule combinations, see .

Add Schedule Items

Both addition schedules and subtraction schedules can be one-time (single) events or recurring events.

To add a schedule item to an access schedule:

1. Expand the access schedule in the **Access Schedules** list.
2. Click **Add schedule item**.
3. Enter the name of the scheduled item.
4. Select **One time** or **Recurrence**.
5. Set the duration in the time fields. See .
6. For recurring schedule events, select the **Recurrence pattern** and **Range of recurrence** parameters. See and .
7. Click **Save**.

Time Options

The following time options are available:

- **All day** – Select for events that last for all 24 hours of the day. Then enter the desired **Start** date.
- **Start** – Click the time field and select the desired time. If required, click the date field and select the desired month, day, and year. You can also type the date directly in the field.
- **End** – Click the time field and select the desired time. If required, click the date field and select the desired month, day, and year. You can also type the date directly in the field.

Recurrence Pattern Options

The following recurrence pattern options are available:

- **Yearly** – Select to repeat every year.
- **Weekly** – Select to repeat every week.
- Recurs every week on **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, and **Sunday** – Select which days to repeat.

Range of Recurrence Options

The following range of recurrence options are available:

- **First occurrence** – Click the date field and select the desired month, day, and year. You can also type the date directly in the field.
- **No end date** – Select to repeat the occurrence indefinitely.
- **End by** – Click the date field and select the desired month, day, and year. You can also type the date directly in the field.

Create and Edit Groups

Groups allow you to manage users and their access rights collectively and efficiently. A group consists of credentials that tell the system which users the group consists of and when and how the group members are granted access to the doors.

Each user must belong to one or more groups. To add a user to a group, drag and drop the user to the desired group in the **Groups** list. For more information, see .

To create a new group:

1. Go to **Access Management**.
2. In the **Groups** tab, click **Add new group**.
3. In the **Add Group** dialog, enter the group's credentials. See .
4. Click **Save**.

To expand an item in the **Groups** list and view its members, door access rights and schedules, click ▶.

To edit a group's name or validity date, click ,255mm,sfx)=″graphics:graphicB11ACA0E385B57DCF1D209C45A83E2AD″ and make the changes. Then click **Save**.

To verify when and how a group can access certain doors, click  .

To delete a group or group members, doors or schedules from a group, click ,255mm,sfx)=″graphics:graphicBC6471AF6421E76E83F4F72C0A258C1D″.

Group Credentials

The following credentials are available for groups:

- **Name** (required)
- **Valid from** and **Valid to** – Enter the dates between which the group's credentials shall be valid. Click the date field and select the desired month, day, and year. You can also type the date directly in the field.
- **Whitelist** – Users in a whitelist group can always access the doors in the group, even in case of network or power failure. Since the users in the group always have access to the doors, schedules or valid to and valid from do not apply. Long access time is not supported for a user that opens a door in a whitelist group. Only doors with wireless locks that support whitelist functionality can be added to the group.

Note

- To be able to save the group, you must enter the group's **Name**.
- Valid to and valid from for a user do not apply when adding the user to whitelist group.
- To sync whitelisted credentials to a wireless lock takes some time and interferes with normal door opening procedures. Avoid adding or removing large numbers of credentials in a system during peak hours. When the sync of updated credentials to the lock is done, the event log will show `SyncOngoing: false` for the lock.

Manage Doors

The general rules for each door are managed in the **Doors** tab. The rules include adding identification types that determine how users will be granted access to the door and access schedules that determine when each identification type is valid. For more information, see and .

Before you can manage a door, you must add it to the access control system by completing the hardware configuration, see .

To manage a door:

1. Go to **Access Management** and select the **Doors** tab.
2. In the **Doors** list, click  next to the door you want to edit.
3. Drag the door to at least one group. If the **Groups** list is empty, create a new group. See .
4. Click **Add identification type** and select which credentials users need to present to the reader to be granted access to the door. See .
   Add at least one identification type to each door.
5. To add multiple identification types, repeat the previous step.
   If both identification types **Card number only** and **PIN only** are added, users can choose to either swipe their card or enter their pin to access the door. But if, instead, only the identification type **Card number and PIN** is added, users must both swipe their card and enter their PIN to access the door.
6. To define when the credentials are valid, drag a schedule to each identification type.

To manually unlock doors, lock doors, or grant temporary access, click one of the manual door actions as required. See .

Note

Controls to manually unlock doors, lock doors, or grant temporary access, are not available for wireless doors/devices.

To expand an item in the **Doors** list, click .

To edit a door or reader name, click ,255mm,sfx)="graphics:graphicB11ACA0E385B57DCF1D209C45A83E2AD" and make the changes. Then click **Save**.

To verify the reader, identification type, and access schedule combinations, click .

To verify the function of the locks connected to the doors, click the verification controls. See .

To delete identification types or access schedules, click ,255mm,sfx)="graphics:graphicBC6471AF6421E76E83F4F72C0A258C1D".

Identification Types

Identification types are portable credential storage devices, pieces of memorized information, or various combinations of the two that determine how users will be granted access to the door. Common identification types include tokens such as cards or key fobs, personal identification numbers (PINs), and request to exit (REX) devices.

For more information about credentials, see .

The following identification types are available:

- **Facility code only** – The user can access the door using a card or other token with the facility code accepted by the reader.
- **Card number only** – The user can access the door using only a card or other token accepted by the reader. The card number is a unique number that is usually printed on the card. See the card manufacturer's information about where to locate the card number. The card number can also be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**.
- **Card raw only** – The user can access the door using only a card or other token accepted by the reader. The information is stored as raw data on the card. The card raw data can be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**. Only use this identification type if a card number cannot be located.
- **PIN only** – The user can access the door using only a four-digit personal identification number (PIN).
- **Facility code and PIN** – The user needs both the card or other token with the facility code accepted by the reader, and a PIN to access the door. The user must present the credentials in the specified order (card first, then PIN).
- **Card number and PIN** – The user needs both the card, or other token accepted by the reader, and a PIN to access the door. The user must present the credentials in the specified order (card first, then PIN).
- **Card raw and PIN** – The user needs both the card, or other token accepted by the reader, and a PIN to access the door. Only use this identification type if a card number cannot be located. The user must present the credentials in the specified order (card first, then PIN).
- **REX** – The user can access the door by activating a request to exit (REX) device, such as a button, sensor, or push bar.
- **License plate only** – The user can access the door using only a license plate number for a vehicle.

Add Scheduled Unlock States

To automatically keep a door unlocked for a specific duration of time, you can add a **Scheduled unlock** state to a door and apply an access schedule to it.

For example, to keep a door unlocked during office hours:

1. Go to **Access Management** and select the **Doors** tab.
2. Click next to the **Doors** list item you want to edit.

3. Click **Add scheduled unlock**.
4. Select the **Unlock state** (**unlocked** or **unlock both locks** depending on whether the door has one or two locks).
5. Click **OK**.
6. Apply the predefined **Office hours** access schedule to the **Scheduled unlock** state.

To verify when the door is unlocked, click .

To delete a scheduled unlock state or access schedule, click ,255mm,sfx)=″graphics:graphicBC6471AF6421E76E83F4F72C0A258C1D″.

Use Manual Door Actions

Doors can be unlocked or locked and temporary access can be granted in the **Doors** tab through the **Manual door actions**. Which manual door actions are available for a specific door depends on how the door has been configured.

To use the manual door actions:

1. Go to **Access Management** and select the **Doors** tab.
2. In the **Doors** list, click next to the door that you want to control.
3. Click the required door action. See .

Note

To use the manual door actions, you need to open the Access Management page through the door controller the specific door is connected to. If you open the Access Management page through a different door controller, instead of the manual door actions there will be a link to the Overview page of the door controller the specific door is connected to. Click the link, go to **Access Management**, and select the **Doors** tab.

Manual Door Actions

The following manual door actions are available:

- **Get door status** – Verify the current state of the door monitor, door alarms, and locks.
- **Access** – Grant users access to the door. The given access time applies. See .
- **Unlock** (one lock) or **Unlock both locks** (two locks) – Unlock the door. The door remains unlocked until you press **Lock** or **Lock both locks**, a scheduled door state is activated, or the door controller is restarted.
- **Lock** (one lock) or **Lock both locks** (two locks) – Lock the door.
- **Unlock second lock and lock primary** – This option is only available if the door has been configured with a secondary lock. Unlock the door. The secondary lock remains unlocked until you press **Double lock** or a scheduled door state is activated.

Manage floors

If you have installed an AXIS 9188 Network I/O Relay Module to your system, floors can be managed in a similar way to managing doors.

Note

If you use an A1001 in cluster mode with global events enabled, make sure you use unique descriptive names for each floor. For example “Elevator A, Floor 1”.

Note

Max 2 AXIS 9188 Network I/O Relay Modules can be configured with each A1001 Network Door Controller.

The general rules for each floor are managed in the **Floors** tab. The rules include adding identification types that determine how users will be granted access to the floor and access schedules that determine when each identification type is valid. For more information, see and .

Before you can manage a floor, you must add it to the access control system by completing the hardware configuration, see .

To manage a floor:

1. Go to **Access Management** and select the **Floors** tab.
2. In the **Floors** list, click next to the floor you want to edit.
3. Drag the floor to at least one group. If the **Groups** list is empty, create a new group. See .
4. Click **Add identification type** and select which credentials users need to present to the reader to be granted access to the floor. See .
   Add at least one identification type to each floor.
5. To add multiple identification types, repeat the previous step.
   If both identification types **Card number only** and **PIN only** are added, users can choose to either swipe their card or enter their pin to access the door. But if, instead, only the identification type **Card number and PIN** is added, users must both swipe their card and enter their PIN to access the door.
6. To define when the credentials are valid, drag a schedule to each identification type.

To manually unlock floors, lock floors, or grant temporary access, click one of the manual door actions as required. See .

Note

Controls to manually unlock floors, lock floors, or grant temporary access, are not available for wireless doors/devices.

To expand an item in the **Floors** list, click .

To edit a floor or reader name, click ,255mm,sfx)=″graphics:graphicB11ACA0E385B57DCF1D209C45A83E2AD″ and make the changes. Then click **Save**.

To verify the reader, identification type, and access schedule combinations, click .

To verify the function of the locks connected to the floors, click the verification controls. See .

To delete identification types or access schedules, click ,255mm,sfx)=″graphics:graphicBC6471AF6421E76E83F4F72C0A258C1D″.

Identification Types Floors

Identification types are portable credential storage devices, pieces of memorized information, or various combinations of the two that determine how users will be granted access to the floor. Common identification types include tokens such as cards or key fobs, personal identification numbers (PINs), and request to exit (REX) devices.

For more information about credentials, see .

The following identification types are available:

- **Facility code only** – The user can access the floor using a card or other token with the facility code accepted by the reader.
- **Card number only** – The user can access the floor using only a card or other token accepted by the reader. The card number is a unique number that is usually printed on the card. See the card manufacturer's information about where to locate the card number. The card number can also be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**.
- **Card raw only** – The user can access the floor using only a card or other token accepted by the reader. The information is stored as raw data on the card. The card raw data can be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**. Only use this identification type if a card number cannot be located.

- **PIN only** – The user can access the floor using only a four-digit personal identification number (PIN).
- **Facility code and PIN** – The user needs both the card or other token with the facility code accepted by the reader, and a PIN to access the floor. The user must present the credentials in the specified order (card first, then PIN).
- **Card number and PIN** – The user needs both the card, or other token accepted by the reader, and a PIN to access the floor. The user must present the credentials in the specified order (card first, then PIN).
- **Card raw and PIN** – The user needs both the card, or other token accepted by the reader, and a PIN to access the floor. Only use this identification type if a card number cannot be located. The user must present the credentials in the specified order (card first, then PIN).
- **REX** – The user can access the floor by activating a request to exit (REX) device, such as a button, sensor, or push bar.

Add Scheduled Unlock States

To automatically keep a floor accessible for anyone for a specific duration of time, you can add a **Scheduled unlock** state to a floor and apply an access schedule to it.

For example, to keep a floor accessible for anyone during office hours:

1. Go to **Access Management** and select the **Floors** tab.
2. Click ▶ next to the **Floors** list item you want to edit.
3. Click **Add scheduled unlock**.
4. Select the **Unlock state** (**unlocked** or **unlock both locks** depending on whether the floor has one or two locks).
5. Click **OK**.
6. Apply the predefined **Office hours** access schedule to the **Scheduled unlock** state.

To verify when the floor is accessible, click .

To delete a scheduled unlock state or access schedule, click
,255mm,sfx)=″graphics:graphicBC6471AF6421E76E83F4F72C0A258C1D″.

Use Manual Floor Actions

Floors can have different accessibilities, restricted or accessible for everyone. Temporary access can be granted in the **Floors** tab through **Manual floor actions**. Which manual floor actions are available for a specific floor depends on how the floor has been configured.

To use the manual floor actions:

1. Go to **Access Management** and select the **Floors** tab.
2. In the **Floors** list, click ▶ next to the floor that you want to control.
3. Click the required floor action. See .

Note

To use the manual floor actions, you need to open the Access Management page through the floor controller the specific door is connected to. If you open the Access Management page through a different floor controller, instead of the manual floor actions there will be a link to the Overview page of the floor controller the specific floor is connected to. Click the link, go to **Access Management**, and select the **Floors** tab.

Manual Floor Actions

The following manual floor actions are available:

- **Get floor status** – Verify the current state of the relay connected to a floor.
- **Access** – Grant users access to the floor. The given access time applies. See .

- **Unlock** – The floor gets fully accessible for everyone until you press **Lock** , a scheduled floor state is activated, or the door controller is restarted.
- **Lock** – The floor gets inaccessible for everyone until you press **Unlock** , a scheduled floor state is activated, or the door controller is restarted.

Create and edit users

Each person must have a unique user profile to be granted access to doors in the access control system. The user profile consists of credentials that tell the system who the user is and when and how they are granted access to the doors.

To be able to manage the user access rights efficiently, each user must belong to one or more groups. For more information, see .

To create a new user profile:

1. Go to **Access Management**.
2. Select the **Users** tab and click **Add new user**.
3. In the **Add User** dialog, enter the user's credentials. See .
4. Click **Save**.
5. Drag the user to one or more groups in the **Groups** list. If the **Groups** list is empty, create a new group. See .

To expand an item in the **Users** list and view a user's credentials, click .

To find a specific user, enter a filter in the filter users field. To force exact matches, surround the filter text with double quotation marks, for example "John" or "potter, virginia".

To edit a user's credentials, click ,255mm,sfx)="graphics:graphicB11ACA0E385B57DCF1D209C45A83E2AD" and change the credentials as required. Then click **Save**.

To delete a user, click ,255mm,sfx)="graphics:graphicBC6471AF6421E76E83F4F72C0A258C1D".

Important

If a user was created through AXIS Visitor Manager, do not edit or delete it in AXIS Entry Manager. For more information about AXIS Visitor Manager and the QR code reader service, see .

User Credentials

The following credentials are available for users:

- **First name** (required)
- **Last name**
- **Valid from** and **Valid until** – Enter the dates between which the user's credentials shall be valid. Click the date field and select the desired month, day, and year. You can also type the date directly in the field.
- **Suspend credential** – Select to suspend the credential. When suspended, the user cannot access any doors in the system through this credential. Deselect to give the user access again. Suspension is intended to be temporary. If the user shall be denied access permanently, it is better to delete the user profile.
- **PIN** (required if no card number or card raw) – Enter the four-digit personal identification number (PIN) selected by or assigned to the user.
- **Facility code** – Enter a code to verify the facility's access control system. If a preset facility code is entered this field is filled in automatically, see
- **Card number** (required if no PIN or card raw) – Enter the card number. See the card manufacturer's information about where to locate the card number. The card number can also be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**.

- **Card raw** (required if no PIN or card number) – Enter the card raw data. The data can be retrieved by the system. Swipe the card on a connected reader, select the reader in the list, and click **Retrieve**. Only use this identification type if a card number cannot be located.
- **Long access time** – Select to override existing access time and allow the door to be open for the Long access time for the user, see
- **License plate** (this credential is not available in a default door controller installation) – When this credential is activated by partner software, enter the license plate number for the user's vehicle.

  This credential can only be used together with Axis partner software and a camera with license plate recognition software. For more information, contact your Axis partner or your local Axis sales representative.

Note

The **Retrieve** button is only available if the hardware configuration has been completed and one or more readers are connected to the controller.

Import Users

Users can be added to the system by importing a text file in comma-separated value (CSV) format. It is recommended to import users when you need to add many users at a time.

Before you can import users, you must create and save a file (*.csv or *.txt) in the correct CSV format. Separate values by commas, no spaces, and separate each user with a line break.

Example:

```
jane,doe,1234,12345678,abc123john,doe,5435,87654321,cde321
```

To import users:

1. Go to **Setup > Import Users**.
2. Locate and select the *.csv or *.txt file that holds the list of users.
3. Select the correct credential option for each column.
4. To import the users to the system, click **Import users**.
5. Verify that each column contains the correct type of credential.
6. If the columns are correct, click **Start importing users**. If the columns are incorrect, click **Cancel** and start over.
7. When the import is finished, click **OK**.

The following credential options are available:

- **First name**
- **Last name**
- **PIN code**
- **Card number**
- **License plate**
- **Unassigned** – Values that will not be imported. Select this option to skip a particular column.

For more information about credentials, see .

Export Users

The Export page shows a comma-separated value (CSV) list of all the users in the system. The list can be used to import the users to another system.

To export the user list:

1. Open a plain text editor and create a new document.
2. Go to **Setup > Export Users**

3. Select all the values on the page and copy them.
4. Paste the values into the text document.
5. Save the document as a comma-separated value file (*csv) or as a text (*.txt) file.

Example Access Schedule Combinations

Identification type schedules and group schedules can be combined in several ways to achieve different results. The examples below follow the workflow described on .

Example:
To create a schedule combination that

- grants guards access to a door at all times,
  - using their card during day shift hours (Monday–Friday, 6 a.m. to 4 p.m.), while
  - using their card and PIN before and after day shift hours, and that
- grants day shift personnel access to the same door,
  - using their card during day shift hours only:

1. Create an **Addition schedule** called **Day shift hours**. See .
2. Create a day shift hours **Schedule item** that recurs Monday–Friday, 06:00–16:00.
3. Create two groups, one **Group** called **Guards** and one **Group** called **Day shift personnel**. See .
4. Drag the predefined **Always** access schedule to the **Guards** group.
5. Drag the **Day shift hours** access schedule to the **Day shift personnel** group.
6. Add the **Card number and PIN** and **Card number only** identification types to the door's reader.
7. Drag the predefined **Always** access schedule to the **Card number and PIN** identification type.
8. Drag the **Day shift hours** access schedule to the **Card number only** identification type.
9. Drag the door to both groups. Then add users to the groups as required. See .

Example:
To create a schedule combination that

- grants guards access to a door at all times,
  - using their card during day shift hours (Monday–Friday, 6 a.m. to 4 p.m.), while
  - using their card and PIN before and after day shift hours, and that
- grants day shift personnel access to the same door every day between 6 a.m. and 4 p.m.,
  - using their card during day shift hours, while
  - using their card and PIN during nights and weekends:

1. Create an **Addition schedule** called **Day shift hours**. See .
2. Create a day shift hours **Schedule item** that recurs Monday–Friday, 06:00–16:00.
3. Create a **Subtraction schedule** called **Nights & weekends**.
4. Create a nights and weekends **Schedule item** that recurs Sunday–Saturday 16:00–06:00.
5. Drag the predefined **Always** schedule and the **Nights & weekends** access schedule to the **Day shift personnel** group.
6. Create two groups, one **Group** called **Guards** and one **Group** called **Day shift personnel**. See .
7. Drag the predefined **Always** access schedule to the **Guards** group and the **Day shift personnel** group.
8. Drag the **Nights & weekends** access schedule to the **Day shift personnel** group.
9. Add the **Card number and PIN** and **Card number only** identification types to the door's reader.
10. Drag the predefined **Always** access schedule to the **Card number and PIN** identification type.

11. Drag the **Day shift hours** access schedule to the **Card number only** identification type.
12. Drag the door to both groups. Then add users to the groups as required. See .

Alarm and 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. Logged events can be configured to trigger alarms and such alarms are logged in the alarm log.

- View the event log. See .
- Export the event log. See
- View the alarm log. See .
- Configure the event and alarm logs. See .

Alarms can also be configured to trigger actions such as email notifications. For more information, see .

View the event log

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

If global events is enabled, you can open the event log from any door controller in the system. For more information about global events, see .

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, and for which controllers. 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.
- Source – Filter on events from a selected controller. Available only in a controller cluster and when global events are enabled.
- Date and time – Filter the event log by a date and time span.

Export the Event Log

To export logged events, go to **Event Log**:

1. Click  .
2. Select export format from the pop up menu to start the export.

Note

CSV format is supported in all browsers, XLSX format is supported in Chrome™ and Internet Explorer®.

Note

After a completed export the export button changes from  to  . To initiate another export, refresh the webpage. The export button changes back to  .

View the Alarm Log

To view the triggered alarms, go to **Alarm Log**. If global events is enabled, you can open the alarm log from any door controller in the system. For more information about global events, see .

To expand an item in the alarm log and view the alarm details, for example door identity and state, click  .

To remove an alarm from the list after verifying the cause of the alarm, click **Acknowledge**. To remove all alarms click **Acknowledge all alarms**.

As an administrator, you might need some events to trigger alarms. Therefore, you can choose which events shall trigger alarms and for which controllers. For more information, see .

Configure the Event and Alarm Logs

The Configure Event and Alarm Logs page allows you to define which events shall be logged and trigger alarms.

To share events and alarms between all connected controllers, select **Global events**. When global events is enabled, you only need to open one Event Log page and one Alarm Log page to simultaneously manage the events and alarms of all door controllers in the system. Global events is enabled by default.

If you disable global events, you will have to open one Event Log page and one Alarm Log page for each individual door controller and manage their events and alarms separately.

Important

Each time that you enable or disable global events, the event log is cleared. This means that all events before that moment are removed and the event log starts over.

Alarms can also be configured to trigger actions such as email notifications. For more information, see .

Event log options

To define which events shall be included in the event log, go to **Setup > Configure Event and Alarm 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 in all door controllers. The event will be registered for all controllers and included in the event log.
- **Log for selected sources** – Enable event logging in selected door controllers. The event will be registered for all selected controllers and included in the event log. Select this option for events that will be combined with either the alarm log option **No alarms** or **Log alarm for selected controllers**.
  In the **Configure event logging** list, click **Select controllers** under the event log item you want to enable. The **Device Specific Event Logging** dialog opens. Under **Log event**, select the controllers that shall have alarm logging enabled and click **Save**.

Alarm log options

To define which events should trigger an alarm, go to **Setup > Configure Event and Alarm Logs**.

The following options for triggering and logging alarms are available:

- **No alarms** – Disable alarm logging. The event will not trigger any alarms or be included in the alarm log.
- **Log alarm for all sources** – Enable alarm logging in all door controllers. The event will trigger an alarm and be included in the alarm log.
- **Log alarm for selected sources** – Enable alarm logging in selected door controllers. The event will trigger an alarm and be included in the alarm log.
  In the **Configure alarm logging** list, click **Select sources** under the alarm log item you want to enable. The **Device Specific Alarm Triggering** dialog opens. Under **Trigger alarm**, select the door controllers that shall have alarm logging enabled and click **Save**.

How to set up action rules

The Event pages allow you to configure the Axis product to perform actions when different events occur. For example, the product can send an email notification or activate an output port when an alarm is triggered. 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 and .

This example describes how to set up an action rule to send an email notification when any alarm is triggered.

1. Configure the alarms. See .
2. Go to **Setup > Additional Controller Configuration > Events > Action Rules** and click **Add**.
3. Select **Enable rule** and enter a descriptive name for the rule.
4. Select **Event Logger** from the **Trigger** drop-down list.
5. Optionally, select a **Schedule** and **Additional conditions**. See below.
6. Under **Actions**, select **Send Notification** from the **Type** drop-down list.
7. Select an email recipient from the drop-down list. See .

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.

Triggers

Available action rule **triggers** and **conditions** include:

- **Access Point**

– **Access Point Enabled** – Triggers an action rule when an access point device such as a reader or REX device is configured, for example when the hardware configuration is completed or an identification type is added.

- **Configuration**

– **Access Point Changed** – Triggers an action rule when the configuration of an access point device such as a reader or REX device is changed, for example when hardware is configured or an identification type is edited, changing the ways through which a door can be accessed.

- **Access Point Removed** – Triggers an action rule when the hardware configuration of an access point device such as a reader or REX device is reset.
- **Area Changed** – Not supported by this version of AXIS Entry Manager. Must be configured by a client such as an access management system, through the VAPIX® application programming interface, that supports this feature and use devices that can provide the required signals. Triggers the action rule when an access area is changed.
- **Area Removed** – Not supported by this version of AXIS Entry Manager. Must be configured by a client such as an access management system, through the VAPIX® application programming interface, that supports this feature and use devices that can provide the required signals. Triggers the action rule when an access area is removed from the system.
- **Door Changed** – Triggers an action rule when the door configuration settings, for example door name, are changed or when a door is added to the system. This can for example be used to send a notification when a door is installed and configured.
- **Door Removed** – Triggers an action rule when a door is removed from the system. This can for example be used to send a notification when a door is removed from the system.

• **Door**

- **Battery Alarm** – Triggers an action rule when a wireless door battery is low and when it is flat.
- **Door Alarm** – Triggers an action rule when the door monitor indicates that the door has been forced open, the door is open too long, or if the door is faulty in any way. This can for example be used to send a notification when someone is forcing an entry.
- **Door Double-Lock Monitor** – Triggers an action rule only when the secondary lock changes state to either locked or unlocked.
- **Door Lock Monitor** – Triggers an action rule when the normal lock changes state to either locked or unlocked. For example, a fault is triggered when the door monitor detects that the door is open although the lock is locked.
- **Door Mode** – Triggers an action rule when the door changes states, for example, when the door has been accessed or blocked, or the door is in lockdown mode. For more detailed descriptions of these modes, see the online help.
- **Door Monitor** – Triggers an action rule when the door monitor state changes. This can for example be used to send a notification when a door monitor indicates that the door is opened or closed.
- **Door Tamper** – Triggers an action rule when the door monitor detects that the connection is interrupted, for example if someone cuts the wires to the door monitor. To use this trigger, make sure that **Enable supervised inputs** is selected and that end of line resistors are installed on the relevant door connector input ports. For more information, see .
- **Door Warning** – Triggers an action rule before the door open too long alarm goes off. This can be used to, for example, send a warning signal that the door controller will send the real alarm, the door open too long alarm, if the door is not closed within the specified door open too long time. For more information about door open too long time, see .
- **Lock Jammed** – Triggers an action rule when a wireless door lock is physically blocked.

• **Event Logger** – Keeps track of all events in the door controller, for example when a user swipes a card or opens a door. If **Global events** is enabled, the event logger keeps track of all the events in every controller in the system. To set which alarms and events that can trigger an action rule, go to **Setup > Configure Event and Alarm Logs**. The event logger is shared by the system and can store up to 30 000 events. When the limit is reached, the event logger uses the first in first out (FIFO) rule. This means that the first event is the first to be overwritten.

- **Alarm** – Triggers an action rule when one of the specified alarms has been triggered. The system administrator can configure which events are more important than others and select whether a particular event should trigger an alarm or not.
- **Dropped Alarms** – Triggers an action rule when new alarm records cannot be written to the alarm logs. For example if there are so many simultaneous alarms that the event logger cannot keep up. When an alarm is dropped, a notification can be sent to the operator.

- **Dropped Events** – Triggers an action rule when new event records cannot be written to the event logs. For example, if there are so many simultaneous events that the event logger cannot keep up. When an event is dropped, a notification can be sent to the operator.

  • **Hardware**

- **Network** – Triggers an action rule when the network connection is lost. Select **Yes** to trigger the action rule when the network connection is lost. Select **No** to trigger the action rule when the network connection is restored. Select **IPv4/v6 address removed** or **New IPv4/v6 address** to trigger an action when the IP address changes.
- **Peer Connection** – Triggers an action rule when the Axis product has established a connection with another door controller, if the network connection between the devices is lost, or if the pairing of door controllers has failed. This can for example be used to send a notification that a door controller has lost its network connection.

  • **Input Signal**

- **Digital Input Port** – Triggers an action rule when an I/O port receives a signal from a connected device. See .
- **Manual Trigger** – Triggers an action rule when the manual trigger is activated. It can be used by a client such as an access management system, through the VAPIX® application programming interface, to manually start or stop the action rule.
- **Virtual Inputs** – Triggers an action rule when one of the virtual inputs changes states. It can be used by a client such as an access management system, through the VAPIX® application programming interface, to trigger actions. Virtual inputs can, for example, be connected to buttons in the management system's user interface.

  • **Schedule**

- **Interval** – Triggers an action rule at the schedule's start time and remains active until the schedule's end time is reached.
- **Pulse** – Triggers an action rule when a one-time event occurs. That is, an event that happens at a specific time and has no duration.

  • **System**

- **System Ready** – Triggers an action rule when the system is in state ready. For example, the Axis product can detect the system state and send a notification when the system has started.
  Select **Yes** to trigger the action rule when the product is in state ready. Note that the rule will only trigger when all necessary services, such as the event system, has started.

  • **Time**

- **Recurrence** – Triggers an action rule by monitoring the recurrences that you have created. You can use this trigger to initiate recurring actions such as sending notifications every hour. Select a recurrence pattern or create a new one. For more information about setting up a recurrence pattern, see .
- **Use Schedule** – Triggers an action rule according to the selected schedule. See .

Actions

You can configure several actions:

- **Output Port** – Activate an I/O port to control an external device.
- **Send Notification** – Send a notification message to a recipient.
- **Status LED** – The status LED can be set to flash for the duration of the action rule or for a set number of seconds. The status LED can be used during installation and configuration to visually validate if the trigger settings, for example the door open too long trigger, work correctly. To set the status LED flash color, select an **LED Color** from the drop-down list.

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**.

Recipient types

The following recipient types are available:
HTTP
HTTPS
Email
TCP

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 > Additonal 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[1]	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

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.

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

Reports

The Reports page allows you to view, print, and export reports that contain different types of information about the system. For more information about which reports that are available, see .

View, Print, and Export Reports

To open the Reports page, click **Reports**.

To view a report, click **View and print**.

To print a report:

1. Click **View and print**.
2. Select the columns that shall be included in the report. All columns are selected by default.
3. If you want to narrow the scope of the report, enter a filter in the relevant filter field. For example, you can filter users by which group they belong to, doors by their schedules, or groups by the doors they have access to.
   To force exact matches, surround the filter text with double quotation marks, for example "John".
4. If you want to sort the report items in a different order, click ▲▼ in the relevant column. To change between standard and reverse order, toggle the sorting buttons.
   ▲ Shows the items in standard order (ascending).
   ▼ Shows the items in reverse order (descending).
5. Click **Print selected columns**.

To export a report, click **Export CSV file**.

The report is exported as a a comma-separated value (CSV) file and includes all possible columns and items for the report type. Unless otherwise specified, the exported file (*.csv) is saved in the default download folder. You can select a download folder in the web browser's user settings.

Note

Only users that have credentials are shown in reports.

Report Types

The following report types are available:

- Access schedules. For more information about access schedule types and options, see and .
- Groups. For more information about group credentials, see .
- Doors. For more information about doors and identification types, see and .
- Users. For more information about user credentials, see .
- Door controllers. For more information about connected controllers and their ID types, see . For more information about door monitor time options, see .

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*

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.

Date & Time

The Axis product's date and time settings are configured under **Setup > Additional Controller Configuration > System Options > Date & Time**.

Current Server Time displays the current date and time (24h clock).

To change the date and time settings, select the preferred **Time mode** under **New Server Time**:

- **Synchronize with computer time** – Sets date and time according to the computer's clock. With this option, date and time are set once and will not be updated automatically.
- **Synchronize with NTP Server** – Obtains date and time from an NTP server. With this option, date and time settings are updated continuously. For information on NTP settings, see .
  If using a host name for the NTP server, a DNS server must be configured. See .
- **Set manually** – Allows you to manually set date and time.

If using an NTP server, select your **Time zone** from the drop-down list. If required, check **Automatically adjust for daylight saving time changes**.

Network

Basic TCP/IP Settings

The Axis product supports IP version 4 (IPv4).

The Axis product can get an IPv4 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 .

ARP/Ping

The product's IP address can be assigned using ARP and Ping. For instructions, see .

The ARP/Ping service is enabled by default but is automatically disabled two minutes after the product is started, or as soon as an IP address is assigned. To re-assign IP address using ARP/Ping, the product must be restarted to enable ARP/Ping for an additional two minutes.

To disable the service, go to **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic** and clear the option **Enable ARP/Ping setting of IP address**.

Pinging the product is still possible when the service is disabled.

Assign an IP address using ARP/Ping

The device's IP address can be assigned using ARP/Ping. The command must be issued within 2 minutes of connecting power.

1. Acquire a free static IP address on the same network segment as the computer.
2. Locate the serial number (S/N) on the device label.
3. Open a command prompt and enter the following commands:
   Linux/Unix syntax
   `arp -s <IP address> <serial number> temp`

   `ping -s 408 <IP address>`
   Linux/Unix example
   `arp -s 192.168.0.125 00:40:8c:18:10:00 temp`

   `ping -s 408 192.168.0.125`
   Windows syntax (this may require that you run the command prompt as an administrator)
   `arp -s <IP address> <serial number>`

   `ping -l 408 -t <IP address>`
   Windows example (this may require that you run the command prompt as an administrator)
   `arp -s 192.168.0.125 00-40-8c-18-10-00`

   `ping -l 408 -t 192.168.0.125`
4. Restart the device by disconnecting and reconnecting the network connector.
5. Close the command prompt when the device responds with `Reply from 192.168.0.125:...` or similar.
6. Open a browser and type `http://<IP address>` in the address field.

For other methods of assigning the IP address, see the document How to assign an IP address and access your device at *www.axis.com/support*

Note

- To open a command prompt in Windows, open the **Start** menu and search for `cmd`.
- To use the ARP command in Windows 8/Windows 7/Windows Vista, right-click the command prompt icon and select **Run as administrator**.
- To open a command prompt in Mac OS X, open the **Terminal utility** from **Application > Utilities**.

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

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*

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 on the Axis product provides two configurable input and output ports for connection of external devices. For information about how to connect external devices, see the Installation Guide, available on *www.axis.com*

The I/O ports are configured under **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports**. Select the port direction (**Input** or **Output**). The ports can be given 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 .

Backup the application data

Go to **Setup > Create a backup** to create a backup of the application data. The data that is backed up includes users, credentials, groups, and schedules. When you create a backup, a file with the data is saved locally on your computer.

Go to **Setup > Upload a backup** to use a previously created backup file to restore the application data. Before you can upload the backup file, you have to reset the device to factory default settings. For instructions, 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*

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.

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**.

Troubleshooting

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.

Stand-alone door controllers:

1. Download the latest firmware file to your computer, available free of charge at *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.

Door controllers in a system:
You can use AXIS Device Manager or AXIS Camera Station to upgrade all door controllers in a system. See *www.axis.com* for more information.

Important

- Do not select sequential upgrade.

Note

- All controllers in a system must always be on the same firmware version.
- Upgrade all controllers in a system at the same time, using the parallel option in AXIS Device Manager or AXIS Camera Station.

Emergency Recovery Procedure

If power or network connection is lost during the upgrade, the process fails and the product may become unresponsive. Flashing red Status indicator indicates a failed upgrade. To recover the product, follow the steps below. The serial number is found on the product's label.

1. In **UNIX/Linux**, type the following from the command line:
   `arp -s <IP address> <serial number> temp`

   `ping -l 408 <IP address>`
   In **Windows**, type the following from a command/DOS prompt (this may require that you run the command prompt as an administrator):
   `arp -s <IP address> <serial number>`

   `ping -l 408 -t <IP address>`
2. If the product does not reply in 30 seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the product's IP address. In the page that opens, use the **Browse** button to select the upgrade file to use. Then click **Load** to restart the upgrade process.
4. After the upgrade is complete (1–10 minutes), the product automatically restarts and shows a steady green on the Status indicator.
5. Reinstall the product, referring to the Installation Guide.

If the emergency recovery procedure does not get the product up and running again, contact Axis support at *www.axis.com/support*

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 *axis.com*.
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	Disconnect the Axis product from the network. Run the Ping command (in a Command/DOS window, type `ping` and the IP address of the product): • If you receive: `Reply from <IP address>: bytes=32; time=10...` 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. • If you receive: `Request timed out`, this means that the IP address is available for use with the Axis product. Check all cabling and reinstall the product.
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	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 `http` or `https` in the browser's address field. If the password for the user root is lost, the product must be reset to the factory default settings. See .
The IP address has been changed by DHCP	IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the product on the network. Identify the product using its model or serial number, or by the DNS name (if the name has been configured). If required, a static IP address can be assigned manually. For instructions, see the document How to assign an IP address and access your device on the product page at *axis.com*
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 **Setup > Network Settings** or **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic**.

Status and Network indicator LEDs are flashing red rapidly

Hardware failure	Contact your Axis reseller.

Product does not start up

Product does not start up	If the product does not start up keep the network cable connected and re-insert the power cable to the midspan.

Specifications

Connectors

For information about the connectors' positions, see .

For connection diagrams and information about the hardware pin chart generated through the hardware configuration, see and .

The following section describes the connectors' technical specifications.

Reader Data Connector

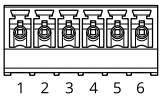
6-pin terminal block supporting RS485 and Wiegand protocols for communication with the reader.

The RS485 ports support:

- Two-wire RS485 half duplex
- Four-wire RS485 full duplex

The Wiegand ports support:

- Two-wire Wiegand



Function		Pin	Notes
RS485	A-	1	For full duplex RS485 For half duplex RS485
	B+	2	
RS485	A-	3	For full duplex RS485 For half duplex RS485
	B+	4	
Wiegand	D0 (Data 0)	5	For Wiegand
	D1 (Data 1)	6	

Important

The RS485 ports have a fixed baudrate of 9600 Bit/s.

Important

The recommended maximum cable length is 30 m (98.4 ft).

Important

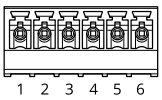
The output circuits in this section are Class 2 power limited.

Reader I/O Connector

6-pin terminal block for:

- Auxiliary power (DC output)
- Digital Input
- Digital Output
- 0 V DC (-)

Pin 3 on the reader I/O connectors can be supervised. If the connection is interrupted, an event is activated. To use supervised inputs, install end of line resistors. Use the connection diagram for supervised inputs. See .



Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC output	2	For powering auxiliary equipment. Note: This pin can only be used as power out.	12 V DC Max load = 300 mA
Configurable (Input or Output)	3–6	Digital input — Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 40 V DC
		Digital output — Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. If used with an inductive load, e.g. a relay, a diode must be connected in parallel with the load, for protection against voltage transients.	0 to max 40 V DC, open drain, 100 mA

Important

The recommended maximum cable length is 30 m (98.4 ft).

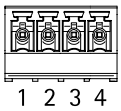
Important

The output circuits in this section are Class 2 power limited.

Door Connector

Two 4-pin terminal blocks for door monitoring devices (digital input).

All door input pins can be supervised. 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
0 V DC (-)	1, 3		0 V DC
Input	2, 4	For communicating with door monitor. Digital input — Connect to pin 1 or 3 respectively to activate, or leave floating (unconnected) to deactivate. Note: This pin can only be used for input.	0 to max 40 V DC

Important

The recommended maximum cable length is 30 m (98.4 ft).

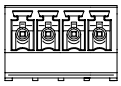
Auxiliary Connector

4-pin configurable I/O terminal block for:

- Auxiliary power (DC output)
- Digital Input
- Digital Output

- 0 V DC (-)

For an example connection diagram, see .



Function	Pin	Notes	Specifications
0 V DC (-)	1		0 V DC
DC output	2	For powering auxiliary equipment. Note: This pin can only be used as power out.	3.3 V DC Max load = 100 mA
Configurable (Input or Output)	3–4	Digital input — Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 40 V DC
		Digital output — Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. If used with an inductive load, e.g. a relay, a diode must be connected in parallel with the load, for protection against voltage transients.	0 to max 40 V DC, open drain, 100 mA

Important

The recommended maximum cable length is 30 m (98.4 ft).

Important

The output circuits in this section are Class 2 power limited.

Power connector

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

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.	10–28 V DC, max 36 W Max load on outputs = 14 W

Network Connector

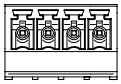
RJ45 Ethernet connector. Use Category 5e cables or higher.

Function	Specifications
Power and Ethernet	Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3, 44–57 V DC Max load on outputs = 7.5 W

Power lock connector

4-pin terminal block for powering one or two locks (DC output). The lock connector can also be used to power external devices.

Connect locks and loads to the pins according to the hardware pin chart generated through the hardware configuration.



Function	Pin	Notes	Specifications
0 V DC (-)	1, 3		0 V DC
0 V DC, floating, or 12 V DC	2, 4	For controlling up to two 12 V locks. Use the hardware pin chart. See .	12 V DC Max total load = 500 mA

NOTICE

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

Important

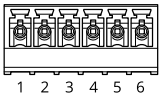
The output circuits in this section are Class 2 power limited.

Power & relay connector

6-pin terminal block with built-in relay for:

- External devices
- Auxiliary power (DC output)
- 0 V DC (-)

Connect locks and loads to the pins according to the hardware pin chart generated through the hardware configuration.



Function	Pin	Notes	Specifications
0 V DC (-)	1, 4		0 V DC
Relay	2–3	For connecting relay devices. Use the hardware pin chart. See . The two relay pins are galvanically separated from the rest of the circuitry.	Max current = 700 mA Max voltage = +30 V DC
12 V DC	5	For powering auxiliary equipment. Note: This pin can only be used as power out.	Max voltage = +12 V DC Max load = 500 mA
24 V DC	6	Not used	

NOTICE

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

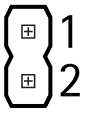
Important

The output circuits in this section are Class 2 power limited.

Tampering Alarm Pin Header

Two 2-pin headers for bypassing:

- Back tampering alarm (TB)
- Front tampering alarm (TF)



Function	Pin	Notes
Back tampering alarm	1–2	To bypass the front and back tampering alarm simultaneously, connect jumpers between TB 1, TB 2 and TF 1, TF 2 respectively. Bypassing the tampering alarms means that the system will not identify any tampering attempts.
Front tampering alarm	1–2	

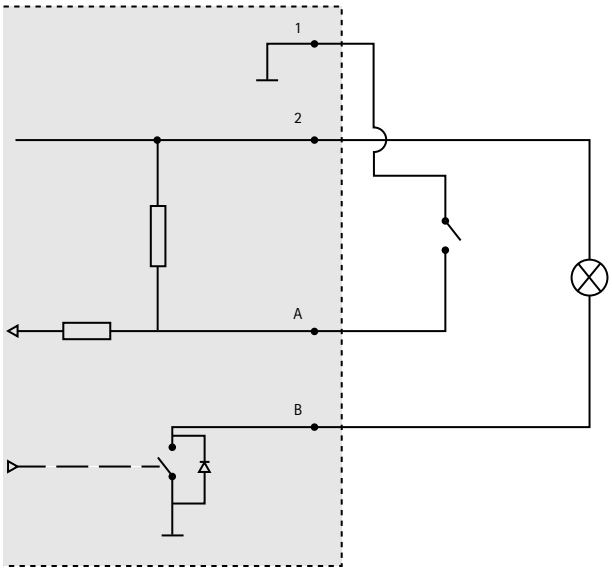
Note

Both the front and back tampering alarms are connected by default. The casing open trigger can be configured to perform an action if the door controller is opened or if the door controller is removed from the wall or ceiling. For information about how to configure alarms and events, see .

Connection Diagrams

Connect devices according to the hardware pin chart generated through the hardware configuration. For more information about hardware configuration and the hardware pin chart, see .

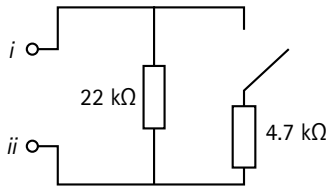
Auxiliary Connector



1 0 V DC (-)
2 DC output: 3.3 V, max 100 mA
3 I/O configured as input
4 I/O configured as output

Supervised inputs

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



i Input

ii 0 V DC (-)

Note

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

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.

T10010336

2025-11 (M26.2)