

AXIS A9188 Network I/O Relay Module

AXIS A9188 Network I/O Relay Module

Table of Contents

Safety information	3
Hazard levels	3
Other message levels	3
Hardware overview	4
LED indicators	5
How to access the product	7
Access the device	7
How to access the product from the internet	7
How to set the root password	7
The Dashboard Page	7
System configuration	9
Configuration – Step by Step	9
Select a Language	9
Configure the Hardware	9
Set the Date and Time	10
Configure the Network Settings	11
Maintenance Instructions	12
Schedule configuration	13
Event Configuration	14
View the Event Log	14
Set Up Action Rules	14
System options	17
Security	17
Date & Time	19
Network	19
Maintenance	24
Support	24
Advanced	25
Reset to factory default settings	25
Troubleshooting	26
How to check the current firmware	26
How to upgrade the firmware	26
Emergency Recovery Procedure	26
Symptoms, possible causes and remedial actions	26
Specifications	28
Connectors	28
Buttons	31
Connection Diagrams	31

AXIS A9188 Network I/O Relay Module

Safety information

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.

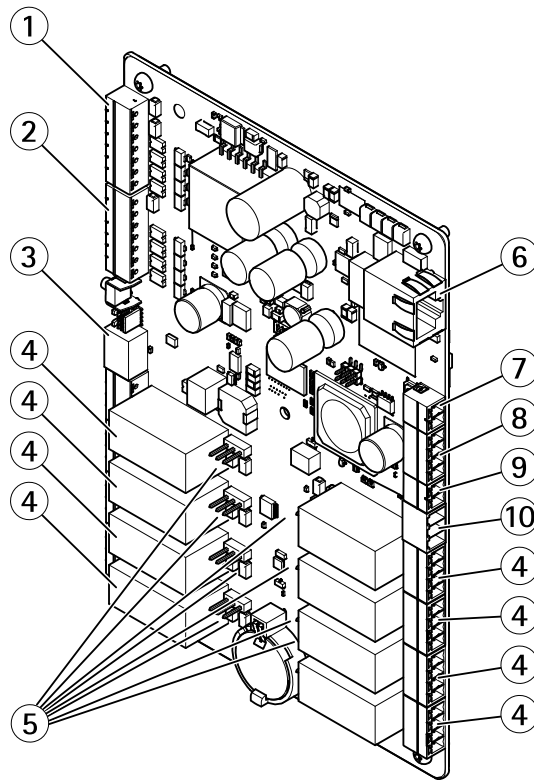
Note

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

AXIS A9188 Network I/O Relay Module

Hardware overview

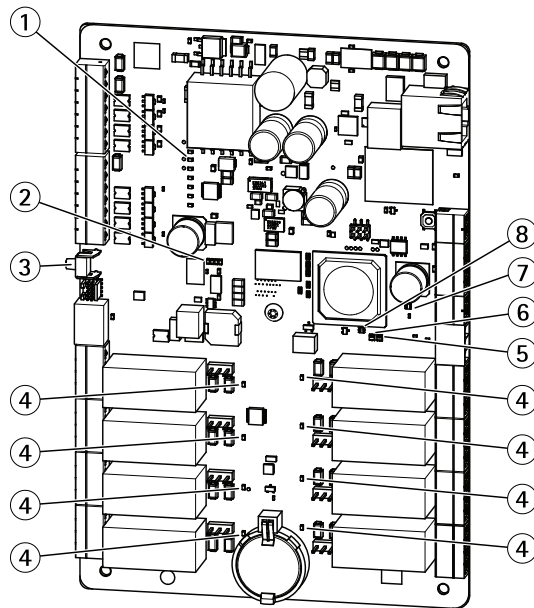
Hardware overview



- 1 Supervised I/O and power connector (DC OUT) port 1–4
- 2 Supervised I/O and power connector (DC OUT) port 5–8
- 3 12/24 V power connector (DC OUT)
- 4 Relay connector (8x)
- 5 Relay jumper (8x)
- 6 Network connector (PoE)
- 7 Power connector (DC IN)
- 8 RS-485 connector (not used)
- 9 Tampering alarm input
- 10 12/24 V power connector (DC OUT)

AXIS A9188 Network I/O Relay Module

Hardware overview



LED indicators, buttons

- 1 I/O LED indicators (8x)
- 2 I/O overcurrent LED indicator
- 3 Control button
- 4 Relay LED indicators (8x)
- 5 Status LED indicator
- 6 Network LED indicator
- 7 I/O overcurrent LED indicator
- 8 Power LED indicator

LED indicators

LED	Color	Indication
Network	Green	Steady for connection to a 100 MBit/s network. Flashes for network activity.
	Amber	Steady for connection to a 10 MBit/s network. Flashes for network activity.
	Unlit	No network connection.
Status	Green	Steady green for normal operation.
	Amber	Steady during startup and when restoring settings.
	Red	Slow flash for failed upgrade.
Power	Green	Normal operation.
	Amber	Flashes green/amber during firmware upgrade.
Relay	Green	Relay coil is energized
	Unlit	Relay coil is unenergized
I/O	Green	I/O is grounded
	Unlit	I/O is floating
	Blinking	Tamper error (wire cut or open)

AXIS A9188 Network I/O Relay Module

Hardware overview

RS485 (not used)	Red	Overcurrent
	Unlit	Normal state
I/O voltage	Red	Overcurrent
	Unlit	Normal state

AXIS A9188 Network I/O Relay Module

How to access 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.
2. Enter the username and password. If you access the device for the first time, you must set the root password. See *How to set the root password on page 7*.
3. AXIS I/O Manager opens in your browser. The start page is called the Dashboard.

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 **Preferences > Additional Device 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 *HTTPS on page 17*.

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 *Reset to factory default settings on page 25*.

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

The Dashboard Page

The dashboard page in AXIS Network IO module is the start screen that shows information about the IOs and relays. Click on each IO or relay row to expand for more settings. From this page you can navigate to **Schedules, Event log and Preferences**.

AXIS A9188 Network I/O Relay Module

How to access the product

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

AXIS A9188 Network I/O Relay Module

System configuration

System configuration

To open the product's Setup pages, click **Preferences > Additional device configuration** in the Dashboard page.

The Axis product can be configured by administrators. For more information about users and administrators, see [page 17](#).

Configuration – Step by Step

Before you start using your AXIS Network IO Relay Module, you should complete the following setup steps:


1. If English is not your first language, you may want AXIS Network IO Relay Module to use a different language. See [page 9](#).
2. Configure the module and connected devices. See [page 9](#).
3. Set the date and time. See [page 10](#).
4. Configure the network settings. See [page 11](#).

For information about maintenance recommendations, see [page 12](#).

Select a Language

The default language of AXIS Network IO Relay Module 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 webpages.

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

Note

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

Configure the Hardware

Before you can manage the connected devices, the hardware must be configured in the Dashboard page.

Devices can be connected to the Axis product before completing the hardware configuration. However, the connection of devices will be easier if you complete the hardware configuration first. This is because the hardware pin chart will be available when the configuration is complete. The hardware pin chart is a guide on how to wire the hardware and can be used as a reference sheet for maintenance. For maintenance instructions, see [page 12](#)

Configure the IOs

In the **Dashboard** page you can make various changes and settings for the IOs.

- Click on an IO row to expand and make the option available.
- Click **Change state** to set the IO **Active** or **Inactive** (for output only)
- Click **Settings** to change name, type, active state and schedule for the IOs.

AXIS A9188 Network I/O Relay Module

System configuration

- Choose **Digital output** or **Digital input** depending on your system setup.
- Choose **Supervised input** to report on the status of the connection between the network IO manager connected devices. If the connection is interrupted, an event is activated. Using supervised input requires external circuitry, see *Connection Diagrams on page 31*.
- Choose Active state **Grounded circuit** or **Open circuit** depending on your system setup.
- Select a schedule to use when Digital Output is chosen.

Note

You can make the schedule a fallback schedule. If the product normally uses another schedule through its connection to another device (for example, AXIS A1001) but that connection is lost, the product will use the fallback schedule instead.

- Click **Save** or **Cancel** to finish.

Configure the Relays

In the **Dashboard** page you can make various changes and settings for the relays

- Click on an Relay row to expand and make the options available.
- Click **Change state** to set the relay **Active** or **Inactive**
- Click **Settings** to change name and schedule for the relay.
 - Select a schedule to use.

Note

You can make the schedule a fallback schedule. If the product normally uses another schedule through its connection to another device (for example, AXIS A1001) but that connection is lost, the product will use the fallback schedule instead.

- Click **Save** or **Cancel** to finish.

How to use supervised inputs

Choose supervised input to monitor status of the cable connections, switches and other devices. 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 *page 31*.
2. Go to **Dashboard > IOs > Settings** and select **Supervised inputs**.

Set the Date and Time

To set the date and time of the Axis product, from the Dashboard go to **Preferences > Additional device configuration > System Options > 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 *page 11*
- Set the date and time manually. See *page 11*.
- Get the date and time from the computer. See *page 11*.

AXIS A9188 Network I/O Relay Module

System configuration

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

1. Go to Preferences > Additional device configuration > System Options > 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 *NTP Configuration on page 21*.

If you use a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 21*.

Set the Date and Time Manually

1. Go to Preferences > Additional device configuration > System Options > 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 Preferences > Additional device configuration > Basic 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 Preferences > Additional device configuration > System Options > System Options > Network > TCP/IP > Basic.

For more information about network settings, see *Network on page 19*.

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).

AXIS A9188 Network I/O Relay Module

System configuration

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 *page 25*.

Maintenance Instructions

To keep the network I/O module running smoothly, Axis recommends regular maintenance of the network I/O module 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 network I/O module and the external devices are secure.
- Verify all the hardware connections. This requires access to the product's webpages.

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. This requires access to the product's webpages.

For information about maintenance of the battery, see Installation Guide.

AXIS A9188 Network I/O Relay Module

Schedule configuration

Schedule configuration

Use schedules to control the active times for the relays and digital output ports. Go to **Schedules** to view and edit existing schedules and create new ones.

View predefined schedules listed in the drop down menu:

- Always
- Office hours
- Weekends
- After hours

To edit the name of the viewed schedule click **Edit schedule**

To edit the start and end times click on the calendar. Choose if you want weekly recurrence

To create a new schedule click **New schedule**

- Enter a name and click **Save**
- Click, hold and drag in the calendar to choose active start and end times.

Important

If you want to delete a schedule that's in use and was created in AXIS A1001 Network Door Controller, make sure you delete it from this device before you delete it in the door controller.

AXIS A9188 Network I/O Relay Module

Event Configuration

Event Configuration

Events that occur in the system, for example when an IO port or relay is activated, are logged in the event log. Events can be configured to trigger alarms.

- View the event log. See *page 14*.

View the Event Log

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

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 use the two drop down menus.

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

- Relay output port – Filter on events that relates to the relay port. Choose a specific relay with the secondary drop down menu.
- Schedule was triggered – Filter on schedules. Choose a specific schedule with the secondary drop down menu.
- Recurring UserAlarm was triggered.
- Port – Filter on events that relates to the IO port. Choose a specific IO port with the secondary drop down menu.
- Digital input port.
- System ready.
- Virtual port.
- Virtual input port.
- Device lost network.
- Device casing opened.
- Period heartbeat from controller.

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 *Actions on page 15*.

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

1. Go to **Preferences > Additional device configuration > Events > Action Rules**.
2. Select **Add** and enter a descriptive name for the rule.
3. Select **Event Logger** from the **Trigger** drop-down list.
4. Optionally, select a **Schedule** and **Additional conditions**. See below.
5. Under **Actions**, select **Send Notification** from the **Type** drop-down list.
6. Select an email recipient from the drop-down list. See *How to add recipients on page 15*.

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

AXIS A9188 Network I/O Relay Module

Event Configuration

For more information, see the online help [?](#).

Triggers

Available action rule triggers and conditions include:

- Event logger
- Hardware
- Input signal
- Schedule
- System
- Time

For more information, see the online help [?](#).

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.

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 *Recipient types on page 15*.

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

AXIS A9188 Network I/O Relay Module

Event Configuration

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 *Certificates on page 18*.

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 **Preferences > Additional Device 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**.

AXIS A9188 Network I/O Relay Module

System options

System options

Security

Users

User access control is enabled by default and can be configured under **Preferences > Additional Device 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 **Preferences > Additional Device 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.

To use HTTPS, an HTTPS certificate must first be installed. Go to **Preferences > Additional Device Configuration > System Options > Security > Certificates** to install and manage certificates. See *Certificates on page 18*.

To enable HTTPS on the Axis product:

1. Go to **Preferences > Additional Device 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.

AXIS A9188 Network I/O Relay Module

System options

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 **Preferences > Additional Device Configuration > System Options > Security > Certificates**. See *Certificates on page 18*.

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

1. Go to **Preferences > Additional Device 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 *Date & Time on page 19*.

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 **Preferences > Additional Device 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 *How to create a self-signed certificate on page 18*.

AXIS A9188 Network I/O Relay Module

System options

2. Go to Preferences > Additional Device 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 Preferences > Additional Device 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 **System Options > Date & Time**.

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 *NTP Configuration on page 21*.
If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 21*.
- **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 *page 25*.

ARP/Ping

The product's IP address can be assigned using ARP and Ping. For instructions, see *Assign an IP address using ARP/Ping on page 20*.

AXIS A9188 Network I/O Relay Module

System options

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 **Preferences > Additional Device 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.

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)

The AVHS settings are configured under **Preferences > Additional Device 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.

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.

AXIS A9188 Network I/O Relay Module

System options

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 **Preferences > Additional Device 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 **Preferences > Additional Device 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 **Preferences > Additional Device 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 **Preferences > Additional Device 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 **Preferences > Additional Device Configuration > System Options > Network > TCP/IP > Advanced**.

AXIS A9188 Network I/O Relay Module

System options

HTTP

The HTTP port used by the Axis product can be changed under **Preferences > Additional Device 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 **Preferences > Additional Device 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 **Preferences > Additional Device Configuration > System Options > Security > HTTPS**. For more information, see *HTTPS on page 17*.

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 **Preferences > Additional Device 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 **Preferences > Additional Device 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 **Preferences > Additional Device Configuration > System Options > Network > TCP/IP > Advanced**.

AXIS A9188 Network I/O Relay Module

System options

RTSP

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 **Preferences > Additional Device 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.

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 **Preferences > Additional Device 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 *HTTPS on page 17*. 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 *Reset to factory default settings on page 25*.

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 **Preferences > Additional Device Configuration > System Options > Network > UPnP**.

AXIS A9188 Network I/O Relay Module

System options

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 **Preferences > Additional Device Configuration > System Options > Network > Bonjour**.

Maintenance

The Axis product provides several maintenance functions. These are available under **Preferences > Additional Device 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 *Reset to factory default settings on page 25*.

For information about firmware upgrade, see *How to upgrade the firmware on page 26*.

Support

Support Overview

The **Preferences > Additional device configuration > System Options > Support > Support Overview** page provides information on troubleshooting and contact information, should you require technical assistance.

See also *Troubleshooting on page 26*.

System Overview

Logs & Reports

The **Preferences > Additional Device 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.

AXIS A9188 Network I/O Relay Module

System options

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 . 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 **Preferences > Additional Device Configuration > System Options > Advanced > Scripting**. If a script causes problems, reset the product to its factory default settings, see *page 25*.

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 **Preferences > Additional Device Configuration > System Options > Advanced > File Upload**.

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 and reconnect power.
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. Using 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 via the web interface. Go to **Preferences > Additional Device Configuration > System Options > Maintenance** and click **Default**.

AXIS A9188 Network I/O Relay Module

Troubleshooting

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.

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.

Note

- 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.

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.
--------------------------	--

AXIS A9188 Network I/O Relay Module

Troubleshooting

Problems setting the IP address

When using ARP/Ping

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 *Reset to factory default settings on page 25*.

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 *Date & Time on page 19*.

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 *NAT traversal (port mapping) for IPv4 on page 22*. The router must support UPnP®.

Firewall protection Check the Internet firewall with your network administrator.

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.

AXIS A9188 Network I/O Relay Module

Specifications

Specifications

Connectors

For information about the connectors' positions, see *Hardware overview on page 4*.

For connection diagrams and information about the hardware pin chart generated through the hardware configuration, see *Connection Diagrams on page 31*.

The following section describes the connectors' technical specifications.

Network Connector

NOTICE

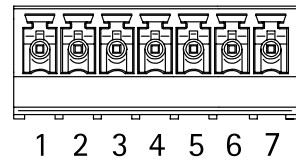
The product shall be connected using a shielded network cable (STP). All cables connecting the product to the network shall be intended for their specific use. Make sure that the network devices are installed in accordance with the manufacturer's instructions. For information about regulatory requirements,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

Function	Specifications
Power and Ethernet	Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4, 44–57 V DC

Supervised I/O and Power Connector

7-pin configurable I/O terminal block for:

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



For an example connection diagram, see *Connection Diagrams on page 31*.

Function	Pin	Notes	Specifications
0 V REF	1		0 V REF
12 V DC output	2	For powering auxiliary equipment. Note: This pin can only be used as power out.	See <i>Specifications on page 28</i>
24 V DC output	3	For powering auxiliary equipment. Note: This pin can only be used as power out.	See <i>Specifications on page 28</i>
Configurable (Input or Output)	4–7	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 40 V DC
		Digital output – Connect the load between DC out or external source and the output pin. If used with an inductive load, e.g. a relay, a diode must be connected in parallel with the load, for protections against transients.	0 to max 40 V DC, open drain, 100 mA

AXIS A9188 Network I/O Relay Module

Specifications

Important

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

Important

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

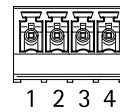
Important

The total power from all DC outputs are 12 W (PoE Type 2 Class 4) or 3.6 W (PoE Type 2 Class 3).

Relay Connector

4-pin relay terminal block for:

- 0 V REF
- NO
- COM
- NC



Function	Pin	Notes	Specifications
0 V REF	1		0 V REF
NO	2	For connecting auxiliary equipment.	0 to max 30 V AC/DC 1 A When PoE powered, relay output is only rated 12 V AC/DC (1 A) or 24 V AC/DC (500 mA).
COM	3	For connecting auxiliary equipment.	
NC	4	For connecting auxiliary equipment.	

⚠WARNING

Maximum connected load on the relay is 30 V AC/DC, 1 A

Relay Jumper

3-pin relay jumper for enabling power to auxiliary equipment via the Relay connector. Inserting the jumper between 12 V or 24 V to COM causes the internal voltage to be connected to the COM terminal of the relay.

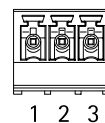
- +12 V
- Relay COM
- +24 V

Function	Pin	Notes	Specifications
+12 V	+12 V	Use jumper to connect power out to Relay COM	+12 V DC
Relay COM	COM	Output power to auxiliary equipment when jumper is used	
+24 V	+24 V	Use jumper to connect power out to Relay COM	+24 V DC

12/24 V DC Out Power Connector

3-pin terminal block for:

- 0 V REF
- 12 V DC OUT
- 24 V DC OUT



AXIS A9188 Network I/O Relay Module

Specifications

Function	Pin	Notes	Specifications
0 V REF	1		0 V DC
12 V DC OUT	2	For powering auxiliary equipment.	See <i>Specifications on page 28</i>
24 V DC OUT	3	For powering auxiliary equipment.	See <i>Specifications on page 28</i>

Important

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

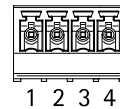
Important

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

RS-485 connector (not used)

4-pin RS-485/RS-422 half duplex serial port:

- +12 V DC
- 0 V REF
- A
- B



Function	Pin	Notes	Specifications
+12 V DC	1		12 V DC Max load = 350 mA
0 V REF	2		0 V DC
A	3		
B	4		

Important

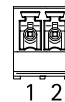
The recommended maximum cable length is 30 m (98.4 ft).

Important

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

Tampering Alarm Input Connector

2-pin terminal block for tampering alarm input.



Function	Pin	Notes	Specifications
0 V REF	1		0 V DC
IN	2	Tampering alarm input. When opened the alarm will trigger.	

AXIS A9188 Network I/O Relay Module

Specifications

DC In Power Connector

2-pin terminal block for DC power input. Use a Class 1 electrical energy source (ES1) or 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 at ≤ 100 W.



Function	Pin	Notes	Specifications
0 V REF	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.	8–28 V DC, max 26 W

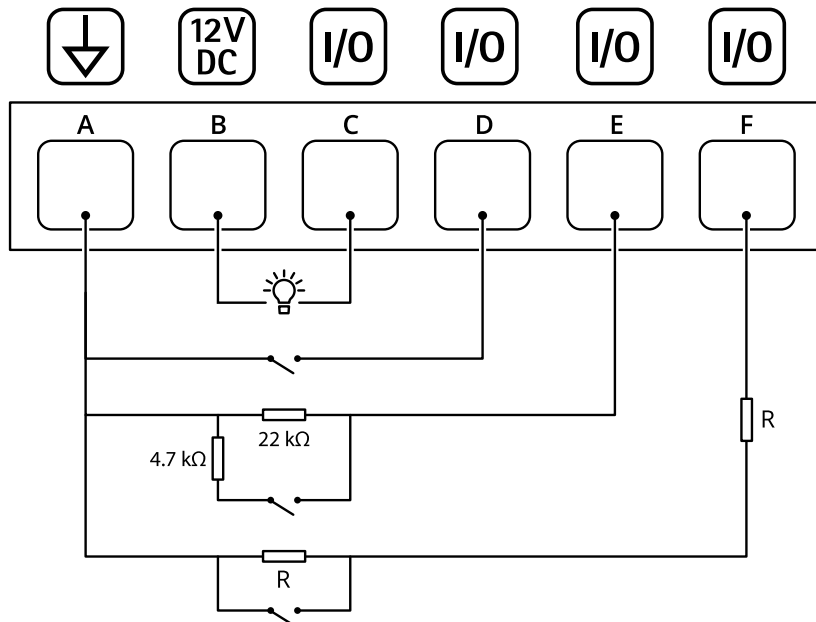
Buttons

The control button is used for:

- Resetting the product to factory default settings, *page 25*.
- Connecting to AXIS Internet Dynamic DNS Service. See www.axis.com

Connection Diagrams

IO connector



- A DC ground
- B DC output
- C I/O configured as output
- D I/O configured as input
- E I/O configured as supervised input with parallel resistor configuration
- F I/O configured as supervised input with serial resistor configuration ($R = 1-10$ k Ω)

