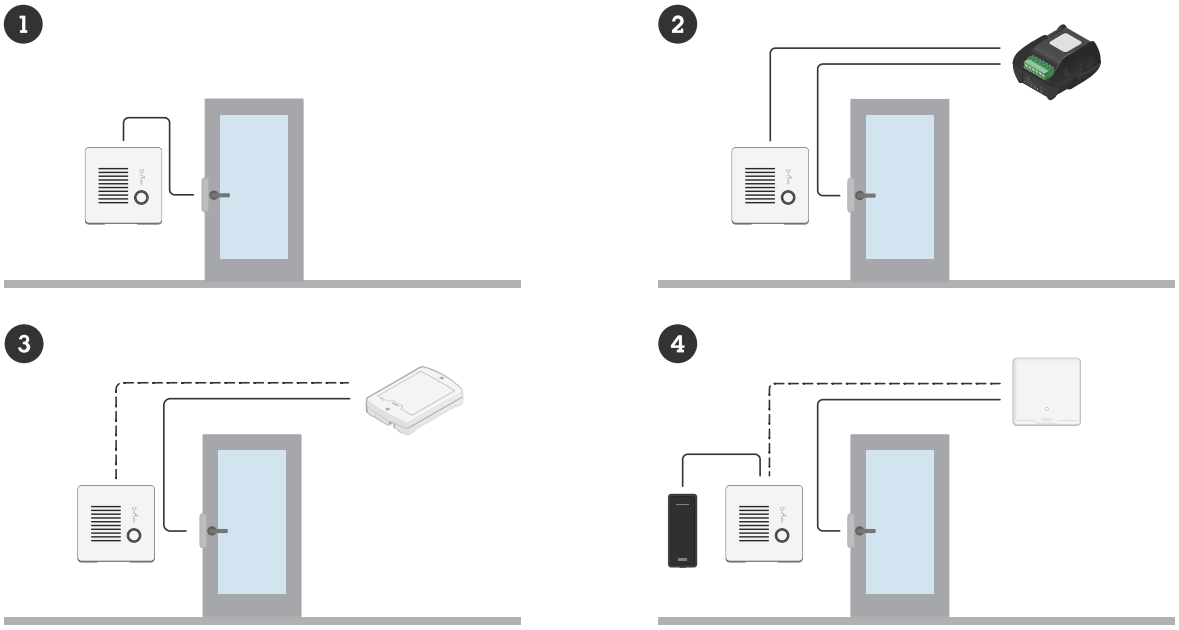
AXIS I7020 Network Intercom

User manual

Table of Contents

Setup overview



1 *Intercom*
2 *Intercom combined with AXIS A9801*
3 *Intercom combined with AXIS A9161*
4 *Intercom combined with a reader and an access control system*

Get started

Find the device on the network

To find Axis devices on the network and assign them IP addresses in Windows®, use AXIS IP Utility or AXIS Device Manager. Both applications are free and can be downloaded from *axis.com/support*.

For more information about how to find and assign IP addresses, go to *How to assign an IP address and access your device*.

Browser support

You can use the device with the following browsers:

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

✓: Recommended

*: Supported with limitations

Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device.
   If you don't know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account, on page 5*.

For descriptions of all features and settings in the web interface of devices with AXIS OS, see *AXIS OS web interface help*.

Create an administrator account

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

1. Enter a username.
2. Enter a password. See *Secure passwords, on page 6*.
3. Re-enter the password.
4. Accept the license agreement.
5. Click **Add account**.

Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings, on page 24*.

Secure passwords

Important

Use HTTPS (which is enabled by default) to set your password or other sensitive configurations over the network. HTTPS enables secure and encrypted network connections, thereby protecting sensitive data, such as passwords.

The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

To protect your data we strongly recommend that you:

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

Make sure that no one has tampered with the device software

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

1. Reset to factory default settings. See *Reset to factory default settings, on page 24*.
   After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

Configure your device

This section covers all the important configurations that an installer needs to do to get the product up and running after the hardware installation has been completed.

Calibrate and run a remote speaker test

You can run a speaker test to verify from a remote location that a speaker is working as intended. The speaker performs the test by playing a series of test tones that are registered by the built-in microphone. Every time you run the test, the registered values are compared with the values that were registered during the calibration.

Note

The test must be calibrated from its mounted position at the installation site. If the speaker is moved or if its local surroundings change, for instance if a wall is built or removed, the speaker should be re-calibrated

During calibration, it is recommended that someone is physically present at the installation site to listen to the test tones and ensure that the test tones are not muffled or blocked by any unintended obstructions in the speaker's acoustic path.

1. Go to the device interface > **Audio > Speaker test**.
2. To calibrate the audio device, click **Calibrate**.

Note

Once the Axis product is calibrated, the speaker test can be run at any time.

3. To run the speaker test, click **Run the test**.

Note

It is also possible to run the calibration by pressing the control button on the physical device. See *Product overview, on page 16* to identify the control button.

Set up direct SIP (P2P)

VoIP (Voice over IP) is a group of technologies that enables voice and multimedia communication over IP networks. For more information, see *Voice over IP (VoIP), on page 13*.

In this device VoIP is enabled through the SIP protocol. For more information about SIP, see *Session Initiation Protocol (SIP), on page 13*

There are two types of setups for SIP. Direct or peer-to-peer (P2P) is one of them. Use peer-to-peer when the communication is between a few user agents within the same IP network and there is no need for extra features that a PBX-server could provide. For information on how to set it up, see *Peer-to-peer SIP (P2PSIP), on page 13*.

1. Go to **Communication > SIP > Settings** and select **Enable SIP**.
2. To allow the device to receive incoming calls, select **Allow incoming calls**.

NOTICE

When you allow incoming calls, the device accepts calls from any device connected to the network. If the device is accessible from a public network or the internet, we recommend you not to allow incoming calls.

3. Click **Call handling**.
4. In **Calling timeout**, set the number of seconds that a call will last before it ends if there is no answer.
5. If you have allowed incoming calls, set the number of seconds before timeout for incoming calls in **Incoming call timeout**.
6. Click **Ports**.
7. Enter the **SIP port** number and **TLS port** number.

Note

- **SIP port** – for SIP sessions. Signalling traffic through this port is non-encrypted. The default port number is 5060.
- **TLS port** – for SIPS and TLS secured SIP sessions. Signalling traffic through this port is encrypted with Transport Layer Security (TLS). The default port number is 5061.
- **RTP start port** – the port used for the first RTP media stream in a SIP call. The default start port is 4000. Some firewalls can block RTP traffic on certain port numbers. The port number must be between 1024 and 65535.

8. Click **NAT traversal**.
9. Select the protocols you want to enable for NAT traversal.

Note

Use NAT traversal when the device is connected to the network from behind a NAT router or a firewall. For more information see *NAT traversal, on page 15*.

10. Click **Save**.

Set up SIP through a server (PBX)

VoIP (Voice over IP) is a group of technologies that enables voice and multimedia communication over IP networks. For more information, see *Voice over IP (VoIP), on page 13*.

In this device, VoIP is enabled through the SIP protocol. For more information about SIP, see *Session Initiation Protocol (SIP), on page 13*

There are two types of setups for SIP. A PBX server is one of them. Use a PBX server when the communication should be between an infinite number of user agents within and outside the IP network. Additional features could be added to the setup depending on the PBX provider. For more information, see *Private Branch Exchange (PBX), on page 14*.

1. Request the following information from your PBX provider:
   - User ID
   - Domain
   - Password
   - Authentication ID
   - Caller ID
   - Registrar
   - RTP start port
2. Go to **Communication > SIP > Accounts** and click **+ Add account**.
3. Enter a **Name** for the account.
4. Select **Registered**.
5. Select a transport mode.
6. Add the account information from the PBX provider.
7. Click **Save**.
8. Set up the SIP settings in the same way as for peer-to-peer, see *Set up direct SIP (P2P), on page 7*. Use the RTP start port from the PBX provider.

Include video stream from nearby camera in SIP call

If you have an Axis camera mounted close to the intercom, you can include the video stream from the camera in your intercom SIP and VMS calls.

Requirements

An Axis camera with H.264 and 1280x720, 800x800, or 640x480 resolution.

To connect the intercom to the camera:

1. Go to **System > Edge-to-edge > Pairing**.
2. Under **Camera pairing**, enter the address, username and password for the Axis camera.
3. Click **Connect**.

Create a contact

This example explains how to create a new contact in the contact list. Before you start, enable SIP in **Communication > SIP**.

To create a new contact:

1. Go to **Communication > Contact list**.
2. Click **+ Add contact**.
3. Enter the first and last name of the contact.
4. Enter the contact's SIP address.

Note

For information about SIP addresses, see *Session Initiation Protocol (SIP), on page 13*.

5. Select the SIP account to call from.

Note

Availability options are defined in **System** > **Events** > **Schedules**.

6. Choose the contact's **Availability**. If there's a call when the contact isn't available, the call gets canceled unless a there's a fallback contact.

Note

A fallback is a contact, to whom the call gets forwarded if the original contact doesn't reply or isn't available.

7. In **Fallback**, select **None**.
8. Click **Save**.

Configure the call button

By default, the call button is configured to make VMS (video management software) calls. If you want to keep this configuration, you just need to add the Axis intercom to the VMS.

This example explains how to set up the system to call a contact in the contact list when a visitor presses the call button.

1. Go to **Communication > Calls > Call button**.
2. Under **Recipients**, remove **VMS**.
3. Under **Recipients**, select an existing or create a new contact.

To disable the call button, turn off **Enable call button**.

Use DTMF to unlock the door for a visitor

When a visitor makes a call from the intercom, the person who answers can use the Dual-Tone Multi-Frequency signaling (DTMF) of his SIP device to unlock the door. The door controller unlocks and locks the door.

This example explains how to:

- define the DTMF signal in the intercom
- set up the intercom to:
  - request the door controller to unlock the door, **or**

– unlock the door using the internal relay.

You make all settings in the intercom's webpage.

Before you start

- Allow SIP calls from the device and create a SIP account. See *Set up direct SIP (P2P), on page 7* and *Set up SIP through a server (PBX), on page 8*.

Define the DTMF signal in the intercom

1. Go to **Communication > SIP > DTMF**.
2. Click **+ Add sequence**.
3. In **Sequence**, enter 1.
4. In **Description**, enter Unlock door.
5. In **Accounts**, select the SIP account.
6. Click **Save**.

Set up the intercom to unlock the door using the internal relay

7. Go to **System > Events > Rules** and add a rule.
8. In the **Name** field, enter DTMF unlock door.
9. From the list of conditions, under **Call**, select **DTMF** and **Unlock door**.
10. From the list of actions, under **I/O**, select **Toggle I/O once**.
11. From the list of ports, select **Relay 1**.
12. Change **Duration** to 00:00:07, which means that the door is open for 7 seconds.
13. Click **Save**.

Use Entry list to allow credential holders to open the door

With Entry list, you can make it possible for credential holders to use their credentials to trigger actions, such as opening a door. This example explains how to add a credential holder who can use their card to open the door 10 times.

Prerequisites

- Make sure the correct chip type is active in **Reader > Chip types**.

Turn on Entry list and add a credential holder:

1. Go to **Reader > Entry list**.
2. Turn on **Use Entry list**.
3. Click **+ Add credential holder**.
4. Enter the credential holder's first and last name. The first name must be unique.
5. Select **Card**.
6. Swipe the credential holder's card on the device and click **Get latest**.
7. Keep the event condition **Access granted**.
8. Under **Valid to**, select **Number of times**.
9. In **Number of times**, enter 10.
10. Click **Save**.

Create a rule:

1. Go to **System > Events**.
2. Under **Rules**, click **+ Add a rule**.
3. In **Name**, enter Open door.
4. In the list of conditions, select **Entry list > Access granted**.

5. In the list of actions, select **I/O > Toggle I/O once**.
6. In the list of ports, select **Door**.
7. Under **State**, select **Active**.
8. Set the duration to 00:00:07.
9. Click **Save**.

Set up rules for events

You can create rules to make your device perform an action when certain events occur. A rule consists of conditions and actions. The conditions can be used to trigger the actions. For example, the device can start a recording or send an email when it detects motion, or show an overlay text while the device is recording.

To learn more, see *Get started with rules for events*.

Trigger an action

1. Go to **System > Events** and add a rule. The rule defines when the device will perform certain actions. You can set up rules as scheduled, recurring, or manually triggered.
2. Enter a **Name**.
3. Select the **Condition** that must be met to trigger the action. If you specify more than one condition for the rule, all of the conditions must be met to trigger the action.
4. Select which **Action** to perform when the conditions are met.

The web interface

To read about all the features and settings available in the web interface of devices with AXIS OS, go to *AXIS OS web interface help*.

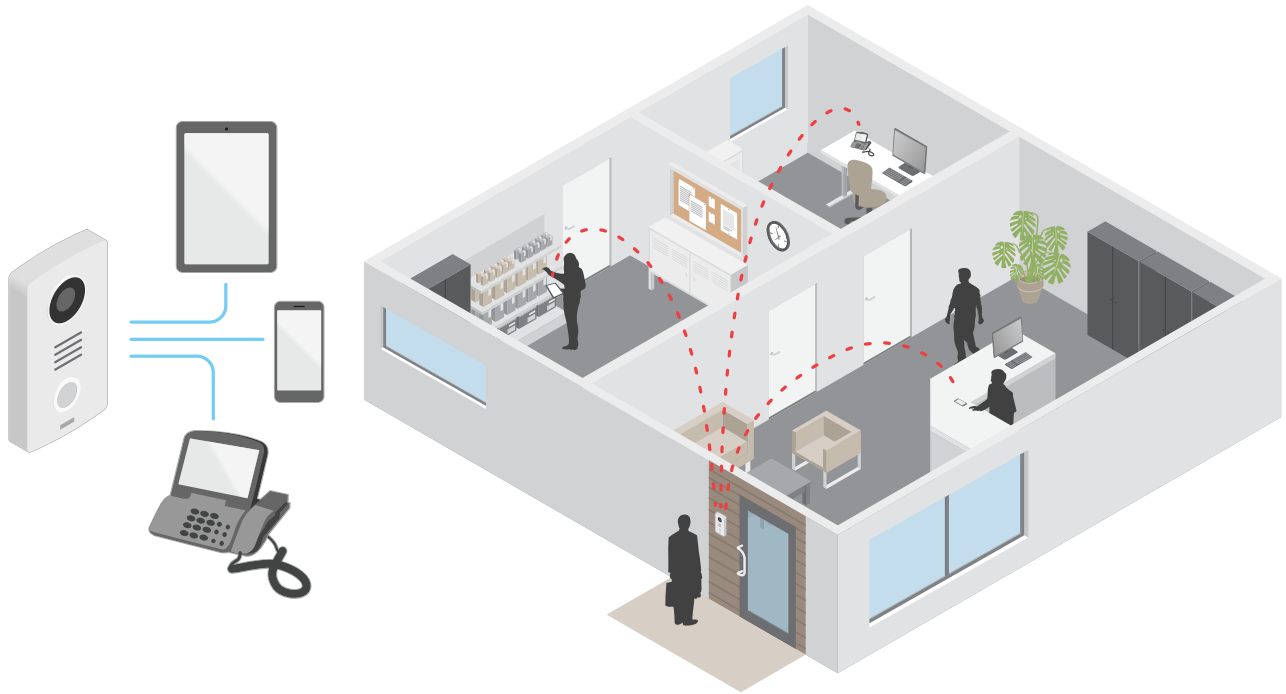
Learn more

Voice over IP (VoIP)

Voice over IP (VoIP) is a group of technologies that enables voice communication and multimedia sessions over IP networks, such as the internet. In traditional phone calls, analog signals are sent through circuit transmissions over the Public Switched Telephone Network (PSTN). In a VoIP call, analog signals are turned into digital signals to make it possible to send them in data packets across local IP networks or the internet.

In the Axis product, VoIP is enabled through the Session Initiation Protocol (SIP) and Dual-Tone Multi-Frequency (DTMF) signaling.

Example:



When you press the call button on an Axis intercom, a call is initiated to one or more predefined recipients. When a recipient replies, a call is established. The voice and video is transferred through VoIP technologies.

Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) is used to set up, maintain and terminate VoIP calls. You can make calls between two or more parties, called SIP user agents. To make a SIP call you can use, for example, SIP phones, softphones or SIP-enabled Axis devices.

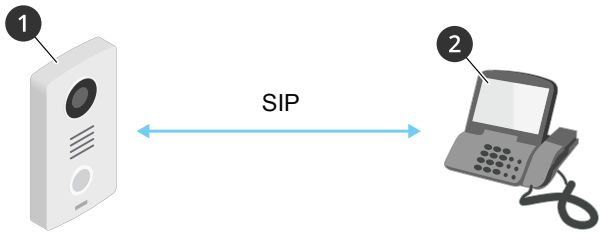
The actual audio or video is exchanged between the SIP user agents with a transport protocol, for example RTP (Real-Time Transport Protocol).

You can make calls on local networks using a peer-to-peer setup, or across networks using a PBX.

Peer-to-peer SIP (P2PSIP)

The most basic type of SIP communication takes place directly between two or more SIP user agents. This is called peer-to-peer SIP (P2PSIP). If it takes place on a local network, all that's needed are the SIP addresses of the user agents. A typical SIP address in this case would be `sip:<local-ip>`.

Example:



1 *User agent A - intercom. SIP address: sip:192.168.1.101*
2 *User agent B - SIP-enabled phone. SIP address: sip:192.168.1.100*

You can set up the Axis intercom to call for example a SIP-enabled phone on the same network using a peer-to-peer SIP setup.

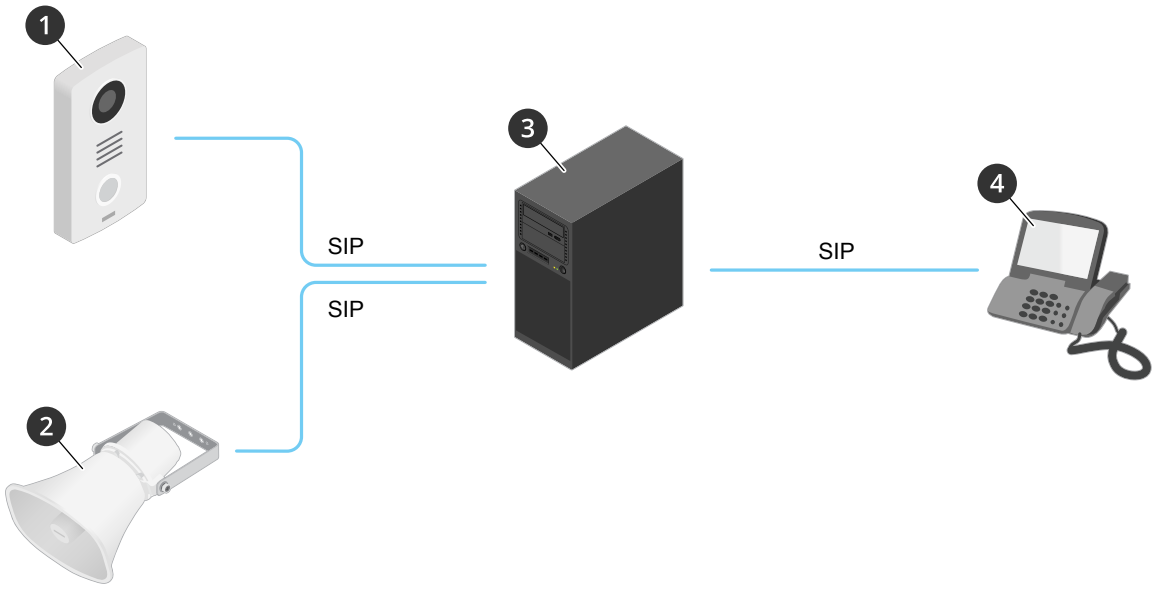
Private Branch Exchange (PBX)

When you make SIP calls outside your local IP network, a Private Branch Exchange (PBX) can act as a central hub. The main component of a PBX is a SIP server, which is also referred to as a SIP proxy or a registrar. A PBX works like a traditional switchboard, showing the client's current status and allowing for example call transfers, voicemail, and redirections.

The PBX SIP server can be set up as a local entity or offsite. It can be hosted on an intranet or by a third party provider. When you make SIP calls between networks, calls are routed through a set of PBXs, that query the location of the SIP address to be reached.

Each SIP user agent registers with the PBX, and can then reach the others by dialing the correct extension. A typical SIP address in this case would be `sip:<user>@<domain>` or `sip:<user>@<registrar-ip>`. The SIP address is independent of its IP address and the PBX makes the device accessible as long as it is registered to the PBX.

Example:



1 *sip:mydoor@company.com*
2 *sip:myspeaker@company.com*
3 ***PBX** sip.company.com*
4 *sip:office@company.com*

When you press the call button on an Axis intercom, the call is forwarded through one or more PBXs to a SIP address either on the local IP network or over the internet.

NAT traversal

Use NAT (Network Address Translation) traversal when the Axis device is located on an private network (LAN) and you want to access it from outside of that network.

Note

The router must support NAT traversal and UPnP®.

Each NAT traversal protocol can be used separately or in different combinations depending on the network environment.

- **ICE** The ICE Interactive Connectivity Establishment) protocol increases the chances of finding the most efficient path to successful communication between peer devices. If you also enable STUN and TURN, you improve the ICE protocol's chances.
- **STUN** - STUN (Session Traversal Utilities for NAT) is a client-server network protocol that lets the Axis device determine if it is located behind a NAT or firewall, and if so obtain the mapped public IP address and port number allocated for connections to remote hosts. Enter the STUN server address, for example, an IP address.
- **TURN** - TURN (Traversal Using Relays around NAT) is a protocol that lets a device behind a NAT router or firewall receive incoming data from other hosts over TCP or UDP. Enter TURN server address and the login information.

Analytics and apps

With analytics and apps you can get more out of your Axis device. AXIS Camera Application Platform (ACAP) is an open platform that makes it possible for third parties to develop analytics and other apps for Axis devices. Apps can be preinstalled on the device, available for download for free, or for a license fee.

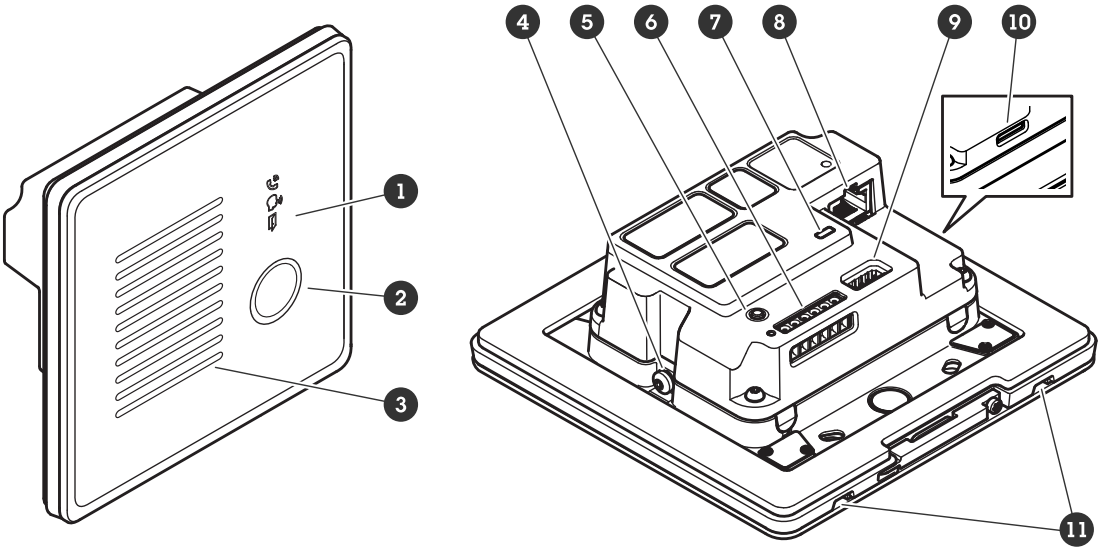
To find the user manuals for Axis analytics and apps, go to *help.axis.com*.

AXIS Client for Unified Communication Systems

With this application you can make calls between SIP-enabled Axis devices and linked Microsoft® Teams accounts. To find out more, see the *user manual for AXIS Client for Unified Communication Systems*.

Specifications

Product overview



1 *Indicator icons, on page 16*
2 *Call button*
3 *Speaker*
4 *Grounding screw*
5 *Control button, on page 17*
6 *I/O, reader, and relay connector, on page 17*
7 *Status LED*
8 *Network connector, on page 17*
9 *Audio connector, on page 17*
10 *SD card slot, on page 17 (microSD/microSDHC/microSDXC)*
11 *Microphone (2x)*

Front panel indicators and controls

When you connect the product to power, the front panel indicators light up for a few seconds.

Indicator icons

Icon	Indication
	Steady amber when outgoing call initiated. Flashes amber when incoming call initiated.
	Steady blue for ongoing call.
	Steady green when door is open.

LED indicators

Status LED	Indication
Green	Steady green for normal operation.

SD card slot

NOTICE

- Risk of damage to SD card. Don't use sharp tools, metal objects, or excessive force when inserting or removing the SD card. Use your fingers to insert and remove the card.
- Risk of data loss and corrupted recordings. Unmount the SD card from the device's web interface before removing it. Don't remove the SD card while the product is running.

This device supports microSD/microSDHC/microSDXC cards.

For SD card recommendations, see *axis.com*.

microSD, microSDHC, and microSDXC Logos are trademarks of SD-3C LLC. microSD, microSDHC, microSDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 24*.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and release the button, then wait for the status LED to flash green three times.

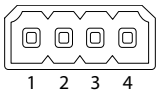
Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

Audio connector

4-pin terminal block for audio input and output.

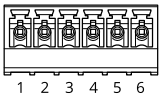


Function	Pin	Notes
Line in	1	Line in (mono)
GND	2	Audio ground
Line out	3	Line out (mono)
GND	4	Audio ground

I/O, reader, and relay connector

You can use this connector for I/O and relay, or for reader connectivity.

6-pin terminal block



1 -
2 *12V*

3 *A/IO1*
4 *B/IO2*
5 *COM*
6 *NO/NC*

Function	Pin	Notes	Specifications
DC ground	1		0 V DC
DC output	2	Can be used to power auxiliary equipment if the device is powered by PoE Class 4. Note: This pin can be used only as power out.	12 V DC **I/O** : Max load = 50 mA **Reader/relay** : Max load = 350 mA
I/O: Configurable (Input or Output) **Reader**: A	3	**I/O**: Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients. **Reader**: RS485 – A	**I/O** : input – 0 to max 30 V DC output – 0 to max 30 V DC, open drain, 100 mA
I/O: Configurable (Input or Output) **Reader**: B	4	**I/O**: same as pin 3 **Reader**: RS485 – B	**I/O**: same as pin 3
Relay: COM	5	Common	
Relay: NO/NC	6	Normally open/normally closed. For connecting relay devices. The two relay pins are galvanically separated from the rest of the circuitry.	Max current 700 mA, max voltage 30 V DC

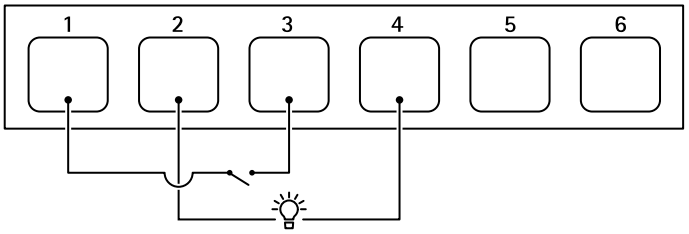
I/O connector

One option is to use the connector as an I/O connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (12 V DC output), the I/O connector provides the interface to:

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

Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the device interface.

Example:



1 *DC ground*
2 *DC output 12 V, max 50 mA*
3 *I/O configured as input*
4 *I/O configured as output*
5 *Relay only*

6 Relay only

Relay connector

In combination with I/O, you can use the connector as a relay connector to connect a solid state relay, and use it:

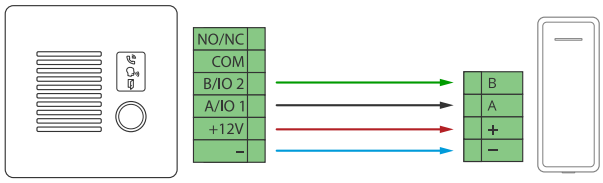
- as a standard relay that opens and closes auxiliary circuits,
- to control a lock directly,
- to control a lock through a safety relay. Using a safety relay on the secure side of the door prevents hotwiring.

Reader connector

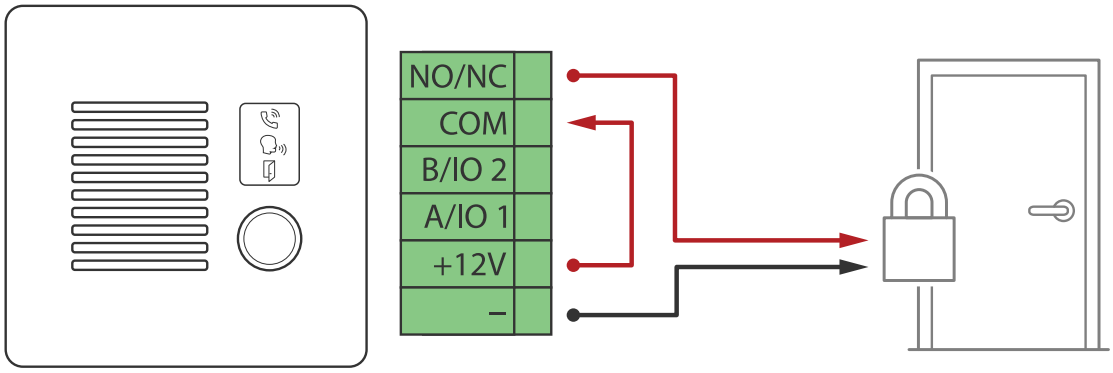
A third option is to use the connector as a reader connector to connect an external reader.

Connect equipment

Axis reader

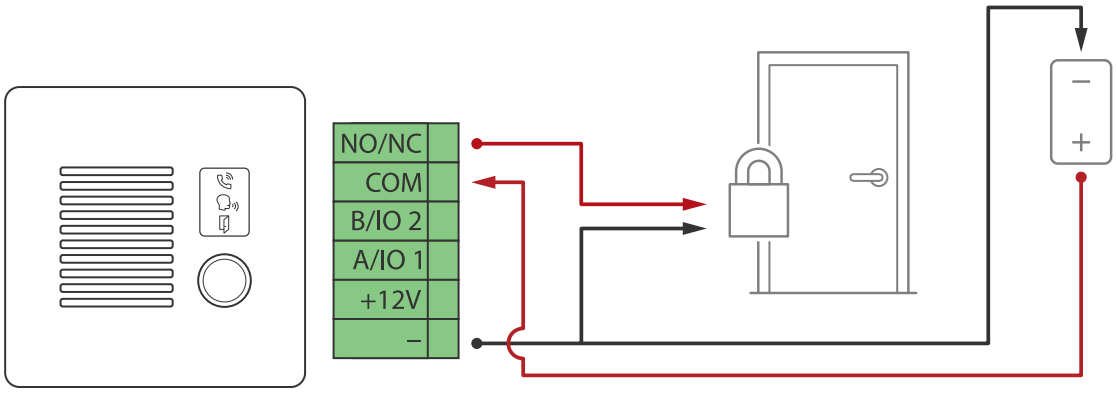


Relay powered by PoE (12V)



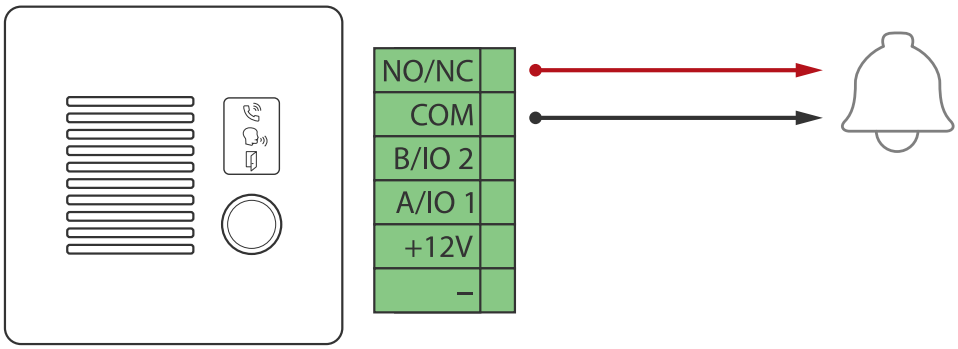
1. To check relay state, go to **System > Accessories** and find the relay port.
2. Set **Normal state** to:
   - for a fail-secure lock.
   - for a fail-safe lock.

Relay powered by separate power supply



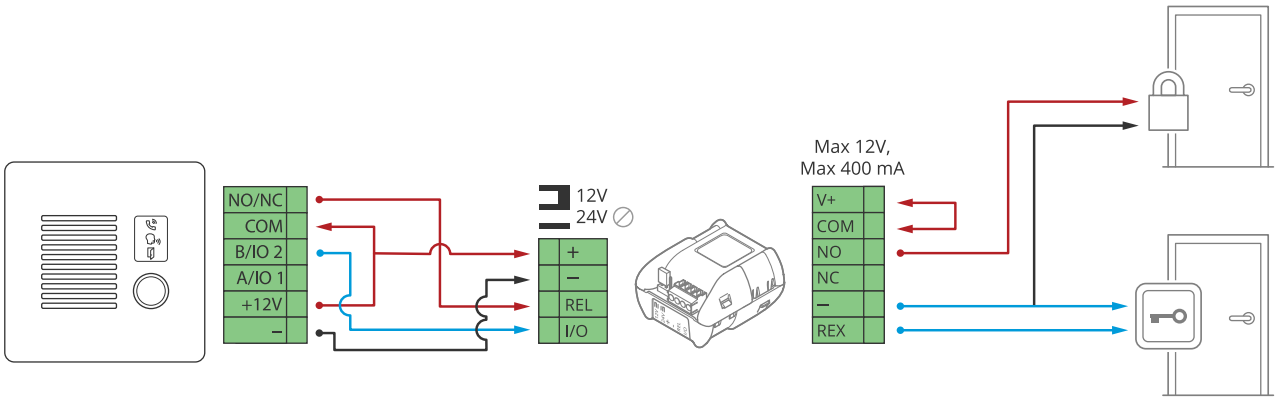
1. To check relay state, go to **System > Accessories** and find the relay port.
2. Set **Normal state** to:
   - for a fail-secure lock.
   - for a fail-safe lock.

Potential-free relay



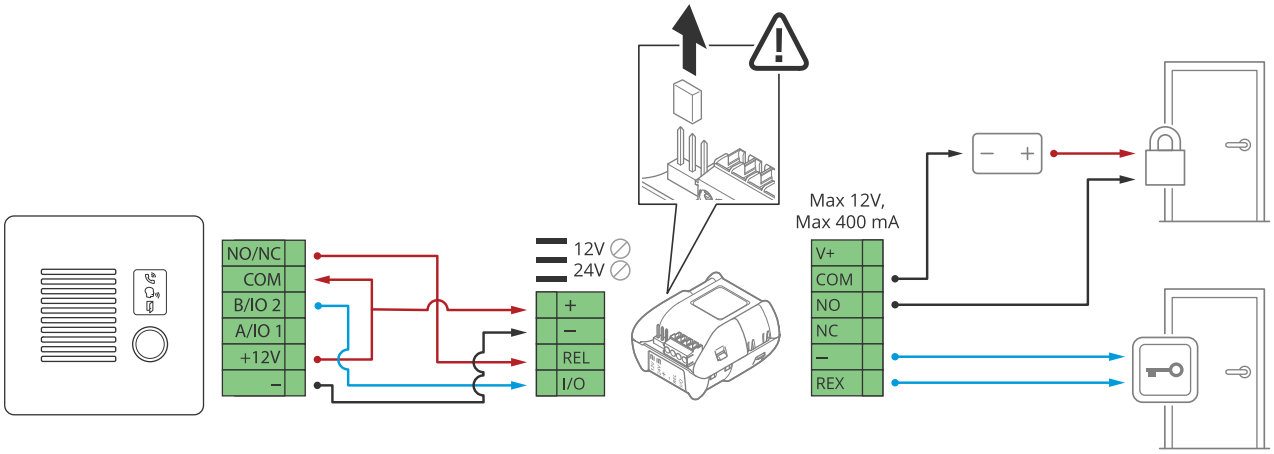
1. To check relay state, go to **System > Accessories** and find the relay port.
2. Set **Normal state** to:
   - for a fail-secure lock.
   - for a fail-safe lock.

12V Fail-secure lock powered by PoE from intercom



1. To check relay state, go to **System > Accessories** and find the relay port.
2. Set **Normal state** to:
   - for a fail-secure lock.
   - for a fail-safe lock.

12V Fail-secure lock powered by external power supply



1. To check relay state, go to **System > Accessories** and find the relay port.
2. Set **Normal state** to:
   -  for a fail-secure lock.
   -  for a fail-safe lock.

Cleaning recommendations

AXIS I7020 Network Intercom can withstand cleaning multiple times per day for at least five years with the chemicals listed above.

The front plate of the intercom withstands regular and frequent chemical wipedown with a soft cloth. There is no chemical reaction between the front plate material and the cleansers. Even with daily chemical wipedowns, the physical integrity of the intercom is maintained. You can clean your device with lukewarm water that contain any of the following chemicals:

- Isopropanol 70% (IPA)
- Hydrogen peroxide 3% (H_2O_2)
- Sodium hypochlorite <5% (NaClO) (Chloride-based bleach)
- Acetic acid (10%)
- Peracetic acid (0.12%)

⚠ CAUTION

Before you use a detergent, read and adhere to the safety data sheet (SDS) provided by the detergent manufacturer.

NOTICE

- Harsh chemicals can damage the device. Don't use chemicals such as acetone or gasoline to clean your device.
- Don't spray detergent directly on the device. Instead, spray detergent on a nonabrasive cloth and use that to clean the device.
- Avoid cleaning in direct sunlight or elevated temperatures, since this can cause stains.

1. Use a can of compressed air to remove dust and loose dirt from the device.
2. If necessary, clean the device with a soft microfiber cloth dampened with lukewarm water and detergent.
3. To avoid stains, dry the device with a clean, nonabrasive cloth.

Troubleshooting

Reset to factory default settings

Important

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

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See *Product overview, on page 16*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
   - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.
   The installation and management software tools are available from the support pages on *axis.com/support*.

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

AXIS OS options

Axis offers device software management according to either the active track or the long-term support (LTS) tracks. Being on the active track means continuously getting access to all the latest product features, while the LTS tracks provide a fixed platform with periodic releases focused mainly on bug fixes and security updates.

Using AXIS OS from the active track is recommended if you want to access the newest features, or if you use Axis end-to-end system offerings. The LTS tracks are recommended if you use third-party integrations, which are not continuously validated against the latest active track. With LTS, the products can maintain cybersecurity without introducing any significant functional changes or affecting any existing integrations. For more detailed information about Axis device software strategy, go to *axis.com/support/device-software*.

Check the current AXIS OS version

AXIS OS determines the functionality of our devices. When you troubleshoot a problem, we recommend that you to start by checking the current AXIS OS version. The latest version might contain a correction that fixes your particular problem.

To check the current AXIS OS version:

1. Go to the device's web interface > **Status**.
2. Under **Device info**, see the AXIS OS version.

Upgrade AXIS OS

Important

- When you upgrade the device software, your preconfigured and customized settings are saved. Axis Communications AB can't guarantee that the settings are saved, even if the features are available in the new AXIS OS version.
- Starting from AXIS OS 12.6, you must install every LTS version between your device's current version and the target version. For example, if the currently installed device software version is AXIS OS 11.2, you

have to install the LTS version AXIS OS 11.11 before you can upgrade the device to AXIS OS 12.6. For more information, see *AXIS OS Lifecycle guide: Upgrade path*.

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

Note

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

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

When the upgrade has finished, the product restarts automatically.

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

If the upgrade fails, the device reloads the previous version. The most common reason is that the wrong AXIS OS file has been uploaded. Check that the name of the AXIS OS file corresponds to your device and try again.

Problems after AXIS OS upgrade

If you experience problems after the upgrade, roll back to the previously installed version from the **Maintenance** page.

Problems setting the IP address

Can't set the IP address

- If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you can't set the IP address. Contact your network administrator to obtain an IP address.
- The IP address could be in use by another device. To check:
  1. Disconnect the Axis device from the network.
  2. In a Command/DOS window, type `ping` and the IP address of the device.
  3. If you receive: `Reply from <IP address>: bytes=32; time=10...` this means that the IP address might already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device.
  4. If you receive: `Request timed out`, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.
- There could be a possible IP address conflict with another device on the same subnet. The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there could be problems accessing the device.

Problems accessing the device

Can't log in when accessing the device from a browser

When HTTPS is enabled, make sure that you use the correct protocol (HTTP or HTTPS) when you try to log in. You might need to manually type `http` or `https` in the browser's address field.

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 24*.

The IP address has been changed by DHCP

IP addresses obtained from a DHCP server are dynamic and could change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).

If required, you can assign a static IP address manually. For instructions, go to *axis.com/support*.

Certificate error when using IEEE 802.1X

For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to **System > Date and time**.

The browser isn't supported

For a list of recommended browsers, see *Browser support, on page 5*.

Can't access the device externally

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

- AXIS Camera Station Edge: free of charge, ideal for small systems with basic surveillance needs.
- AXIS Camera Station Pro: 90-day trial version free of charge, ideal for small to mid-size systems.

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

Problems with MQTT

Can't connect over port 8883 with MQTT over SSL

The firewall blocks traffic that uses port 8883 since it's regarded insecure.

In some cases the server/broker might not provide a specific port for MQTT communication. It might still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic.

- If the server/broker supports WebSocket/WebSocket Secure (WS/WSS), typically on port 443, use this protocol instead. Check with the server/broker provider to see if WS/WSS is supported and which port and basepath to use.
- If the server/broker supports ALPN, the use of MQTT can be negotiated over an open port, such as 443. Check with your server/broker provider to see if ALPN is supported and which ALPN protocol and port to use.

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

Performance considerations

When you set up your system, it's important to consider how different settings and situations affect performance. Some factors affect bandwidth (bitrate), others affect frame rate, and some affect both.

The most important factors to consider:

- High image resolution or lower compression levels result in images containing more data which in turn affects the bandwidth.
- Access by large numbers of Motion JPEG clients or unicast H.264/H.265/AV1 clients affects the bandwidth.
- Simultaneous viewing of different streams (resolution, compression) by different clients affects both frame rate and bandwidth.
  Use identical streams wherever possible to maintain a high frame rate. Stream profiles can be used to ensure that streams are identical.
- Accessing video streams with different codecs simultaneously affects both frame rate and bandwidth. For optimal performance, use streams with the same codec.
- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.
- Using HTTPS may reduce frame rate, in particular if streaming Motion JPEG.
- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Viewing on poorly performing client computers lowers perceived performance and affects frame rate.
- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the frame rate and the general performance.

Contact support

If you need more help, go to *axis.com/support*.

Cybersecurity

Cybersecurity supports a successful product lifecycle with minimized risks. You can find in-depth information and documentation about our cybersecurity approach at *axis.com/about-axis/cybersecurity*. Follow the cybersecurity guidelines below to receive product security notifications from Axis and to configure your product for a secure lifecycle and decommissioning.

At *Axis Trust Center*, you can find information about how Axis implements security compliance, transparency, data protection, and privacy.

Vulnerability management

Axis is a *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. To minimize your risk of exposure, we follow industry standards when identifying and resolving vulnerabilities in our devices, software, and services. Refer to *axis.com/vulnerability-management* for information about our vulnerability management policy or to report a vulnerability.

Security notifications

Subscribe to Axis security notification emails at *axis.com/security-notification-service*. We will send you information about vulnerabilities, corresponding security advisories, and other security-related matters for your Axis product.

Secure product lifecycle

Axis minimizes risks throughout the lifetime of our products through secure lifecycle management. Use our hardening guides at *help.axis.com* to more securely configure and operate your Axis products and to find information about:

Secure first-use – Axis products are pre-configured with high default protection to allow for secure initialization and encrypted communication from the very start.

Intended use and common configuration mistakes – Our guides provide information about the intended usage of Axis products, including common security-relevant misuse and configuration mistakes that should be avoided.

Managing vulnerabilities and supply chain transparency – A Software Bill of Material (SBOM) is published with every software release on *axis.com* to disclose vulnerabilities and improve supply chain transparency.

Decommissioning and the secure erasure of data – To securely decommission a product when it reaches the end of its lifecycle, reset it to factory default settings. This erases your configurations, stored data, and sensitive 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.

T10213215

2026-07 (M14.2)