



# AXIS I8016-LVE Network Video Intercom User Manual

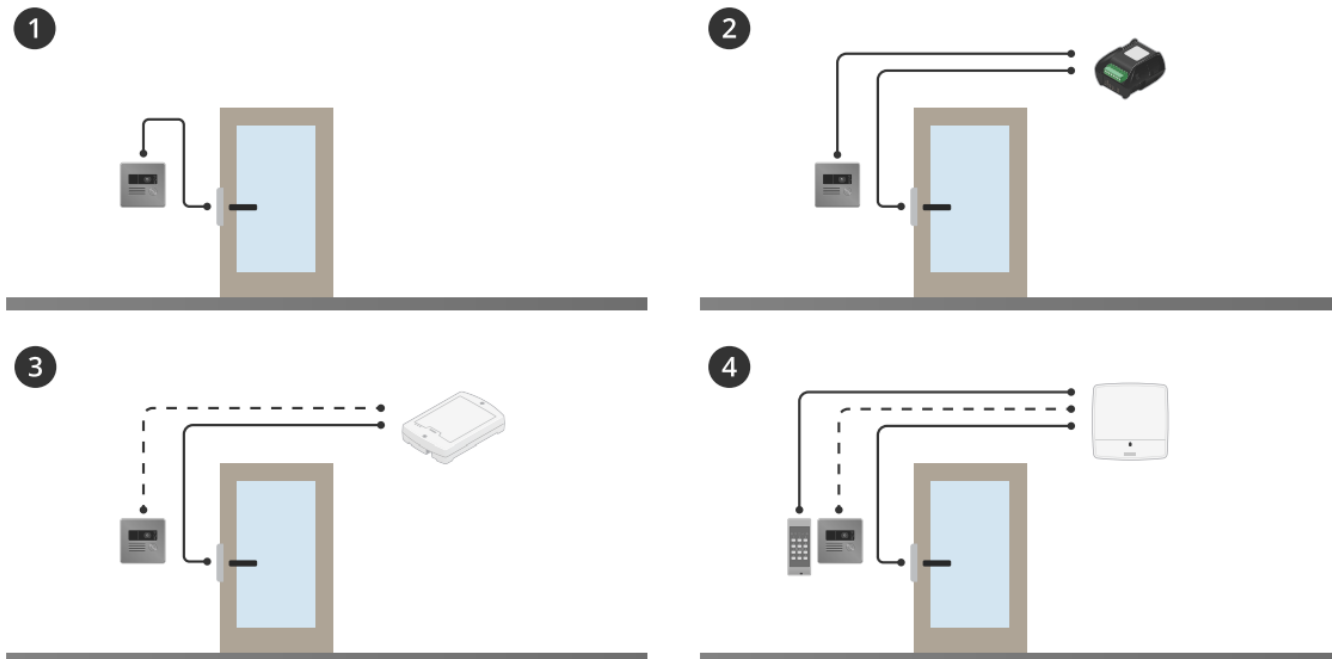
[Home](#) » [AXIS](#) » [AXIS I8016-LVE Network Video Intercom User Manual](#) 



## Contents

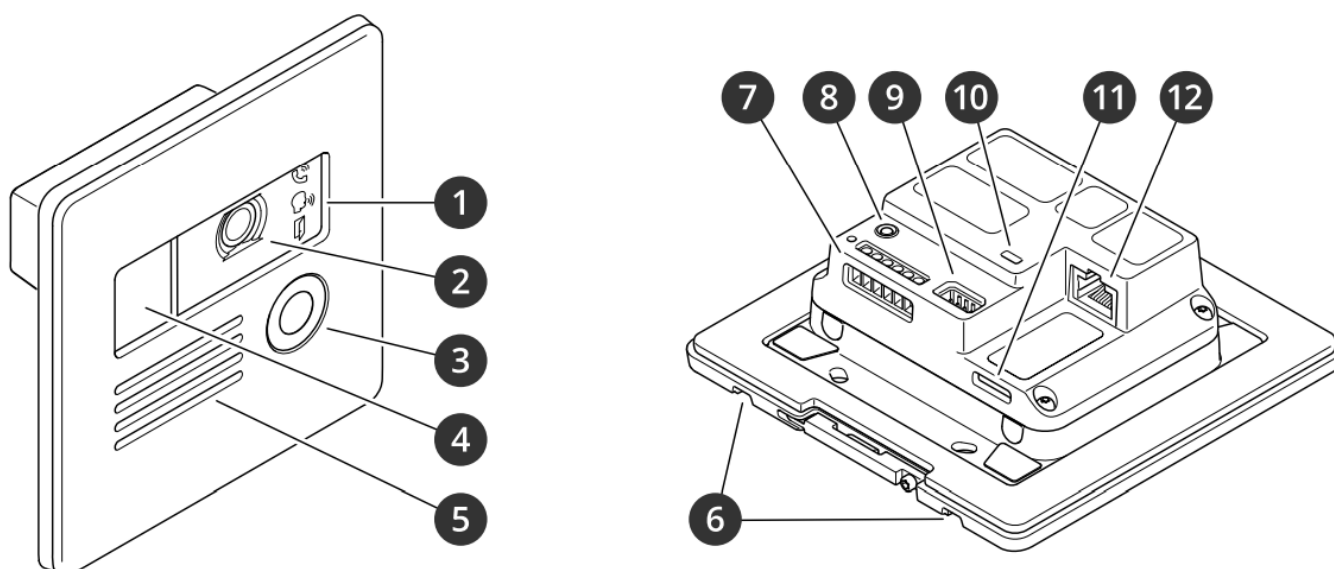
- [1 Setup overview](#)
- [2 Product overview](#)
- [3 Get started](#)
- [4 Configure your device](#)
- [5 Learn more](#)
- [6 Troubleshooting](#)
- [7 Connect equipment](#)
- [8 Specifications](#)
- [9 Safety information](#)
- [10 Documents / Resources](#)
  - [10.1 References](#)
- [11 Related Posts](#)

## 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, for example AXIS A1001 or AXIS A1601

## Product overview



1. Call indicator icons on page 20
2. Camera
3. Call button
4. IR illuminator
5. Speaker
6. Microphone
7. I/O connector on page 21

8. Control button on page 20
9. Audio connector on page 21
10. Status LED
11. SD card slot on page 20 (microSD/microSDHC/microSDXC)
12. Network connector on page 21

## 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](https://axis.com/support). For more information about how to find and assign IP addresses, go to How to assign an IP address and access your device.

### Browser support

You can use the device with the following browsers:

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

\*To use AXIS OS web interface with iOS 15 or iPadOS 15, go to Settings > Safari > Advanced > Experimental Features and disable NSURLSession Websocket.

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

### Open the device's webpage

1. Open a browser and enter the IP address or hostname of the Axis device.  
If you do not know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Enter the username and password. If you access the device for the first time, you must set the root password.  
See Set a new password for the root account on page 5.

### Verify that no one has tampered with the firmware

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

1. Reset to factory default settings. See Reset to factory default settings on page 14.  
After the reset, a secure boot guarantees the state of the device.
2. Configure and install the device.

### Set a new password for the root account

The default administrator username is root. There's no default password for the root account. You set a password for the first time you log in to the device.

1. Type a password. Follow the instructions about secure passwords. See Secure passwords on page 6.
2. Retype the password to confirm the spelling.
3. Click Add user.

### **Important**

If you lose the password for the root account, go to Reset to factory default settings on page 14 and follow the instructions.

## **Secure passwords**

### **Important**

Axis devices send the initially set password in clear text over the network. To protect your device after the first login, set up a secure and encrypted HTTPS connection and then change the password.

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

To protect your data we strongly recommend that you:

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

## **Configure your device**

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

### **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, see Voice over IP (VoIP) on page 11.

In this product, VoIP is enabled through the SIP protocol. For more information about SIP, see Session Initiation Protocol (SIP) on page 11

There are two types of setups for SIP. Peer-to-peer 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 11.

1. Go to System > SIP > 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 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. Signaling traffic through this port is non-encrypted. The default port number is 5060.
- TLS port – for SIPS and TLS-secured SIP sessions. Signaling traffic through this port is encrypted with Transport Layer Security (TLS). The default port number is 5061.
- RTP start port – Enter the port used for the first RTP media stream in a SIP call. The default start port for media transport is 4000. Some firewalls might block RTP traffic on certain port numbers. A 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 13.

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 11.

In this device, VoIP is enabled through the SIP protocol. For more information about SIP, see Session Initiation Protocol (SIP) on page 11

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 12.

1. Request the following information from your PBX provider:

- User ID
- Domain
- Password
- Authentication ID
- Caller ID
- Registrar
- RTP start port

2. Go to System > SIP > SIP accounts and click + 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.

### **Create a contact**

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

To create a new contact:

1. Go to a 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 11.

5. Select the SIP account to call from.
6. Choose the contact's Availability. If a call is attempted when the contact is not available, the call is canceled unless there's a fallback contact.

**Note**

Availability options are defined in System > Events > Schedules.

7. In Fallback, select None.

**Note**

A fallback is a contact, to whom the call is forwarded if the original contract does not reply.

8. Click Save.

### Configure the call button

By default, the call button is configured to make VMS (Video Management System) 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 the Call button.
2. Turn off Make calls in the video management system (VMS).
3. Under Recipients, select a 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 on the intercom's webpage.

Before you start

- Allow SIP calls from the device and set up a SIP account. See Set up direct SIP (P2P) on page 7 and Set up SIP through

a server (PBX) on page 7.

Define the DTMF signal in the intercom

1. Go to System > SIP > SIP accounts and locate the SIP account.



2. Click > Edit.

3. Click DTMF.

4. Click + DTMF sequence.
5. In the Sequence field, enter “1”.
6. In the Description field, enter “Unlock door”.
7. Click Save.

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

1. Follow the steps under Define the DTMF signal in the intercom
2. Go to System > Events > Rules and add a rule.
3. In the Name field, enter “DTMF unlock door”.
4. From the list of conditions, under Call, select DTMF and Unlock door.
5. From the list of actions, under I/O, select Toggle I/O once.
6. From the list of ports, select Relay 1.
7. Change Duration to 00:00:07, which means that the door is open for 7 seconds.
8. Click Save.

### **Benefit from IR light in low-light conditions by using night mode**

Your camera uses visible light to deliver color images during the day. But as the visible light diminishes, color images become less bright and clear. If you switch to night mode when this happens, the camera uses both visible and near-infrared light to deliver bright and detailed black-and-white images instead. You can set the camera to switch to night mode automatically.

1. Go to Video > Image > Day-night mode, and make sure that the IR-cut filter is set to Auto.
2. To set at what light level you want the camera to switch to night mode, move the Threshold slider toward Bright or Dark.

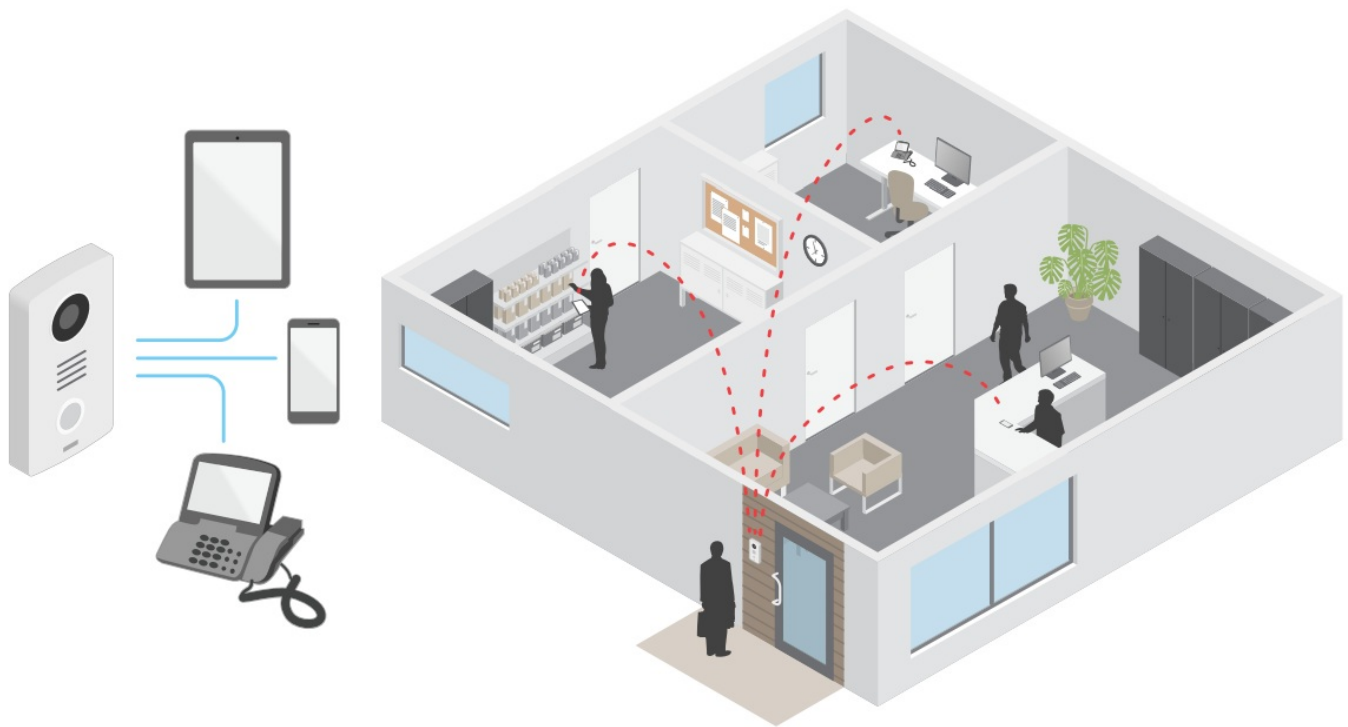
### **Learn more**

#### **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).

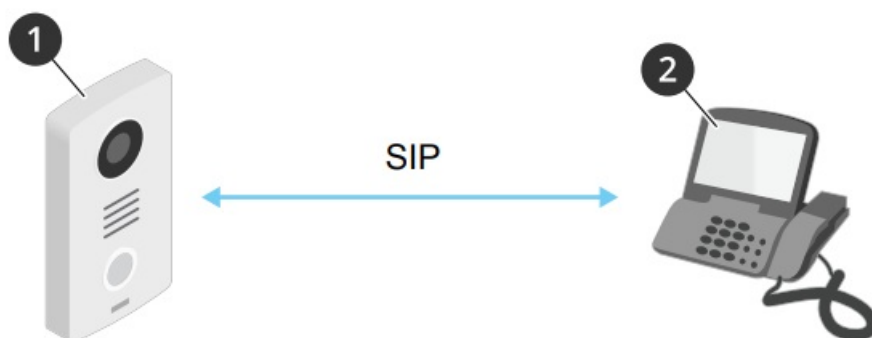
You can make calls on local networks using a peer-to-peer setup, or across networks using a PBX.

### **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.

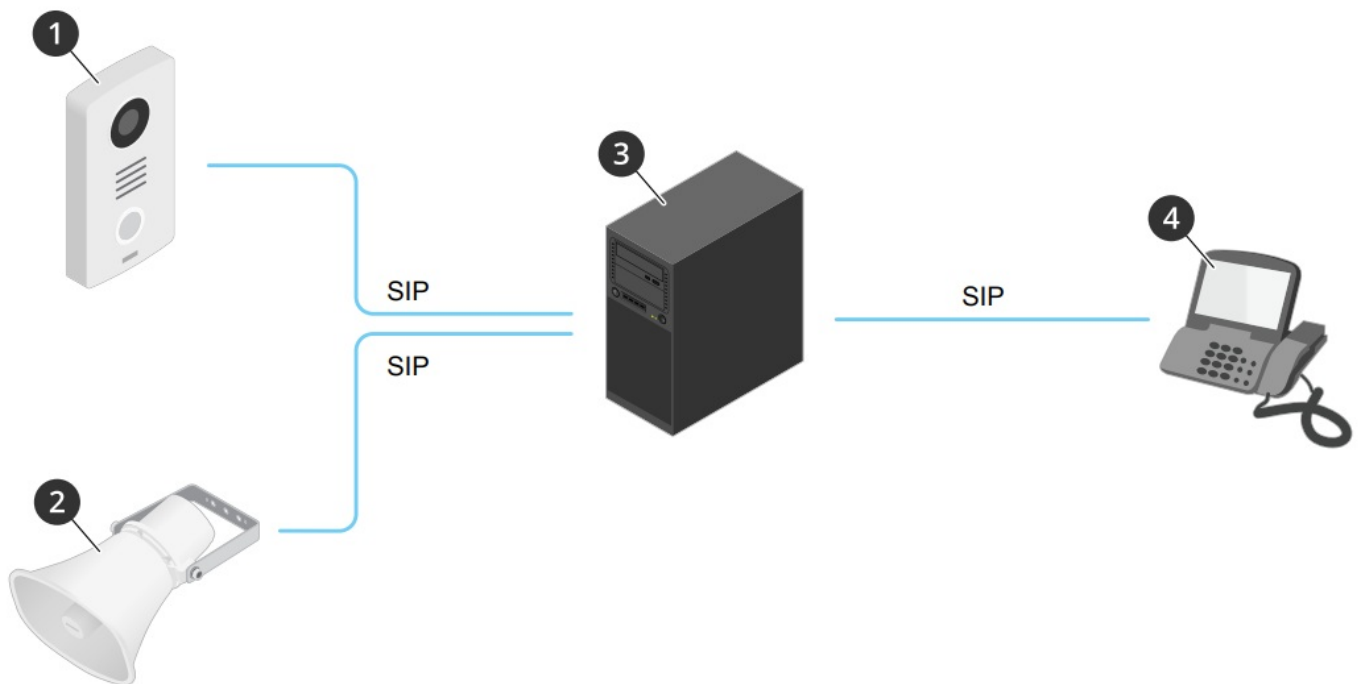


## Private Branch Exchange (PBX)

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. [sipmydoor@company.com](mailto:sipmydoor@company.com)
2. [sipmyspeaker@company.com](mailto:sipmyspeaker@company.com)
3. [PBXsip.company.com](mailto:PBXsip.company.com)
4. [sipoffice@company.com](mailto:sipoffice@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.

### 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, check out our guide [Get started with rules for events](#).

### NAT traversal

Use NAT (Network Address Translation) traversal when the Axis device is located on a 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.

## Applications

AXIS Camera Application Platform (ACAP) is an open platform that enables third parties to develop analytics and other applications for Axis products. To find out more about available applications, downloads, trials, and licenses, go to [axis.com/applications](https://axis.com/applications).

To find the user manuals for Axis applications, go to [help.axis.com](https://help.axis.com).

## 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 the Product overview on page 4.
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. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90.
5. Use the installation and management software tools 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](https://axis.com/support). You can also reset parameters to factory default through the device's webpage. Go to Maintenance > Factory default and click Default.

### Check the current firmware version

Firmware is the software that determines the functionality of network devices. When you troubleshoot a problem, we recommend you start by checking the current firmware version. The latest firmware version might contain a correction that fixes your particular problem.

To check the current firmware:

1. Go to the device interface > Status.

2. See the firmware version under Device info.

## **Upgrade the firmware**

### **Important**

Preconfigured and customized settings are saved when you upgrade the firmware (provided that the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.

### **Important**

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

### **Note**

When you upgrade the device with the latest firmware in the active track, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before you upgrade the firmware. To find the latest firmware and the release notes, go to [axis.com/support/firmware](https://axis.com/support/firmware).

1. Download the firmware file to your computer, available free of charge at [axis.com/support/firmware](https://axis.com/support/firmware).
2. Log in to the device as an administrator.
3. Go to Maintenance > Firmware upgrade and click Upgrade.

When the upgrade has finished, the product restarts automatically.

### **Technical issues, clues, and solutions**

If you can't find what you're looking for here, try the troubleshooting section at [axis.com/support](https://axis.com/support).

Problems upgrading the firmware

Firmware upgrade failure	If the firmware upgrade fails, the device reloads the previous firmware. The most common reason is that the wrong firmware file has been uploaded. Check that the name of the firmware file corresponds to your device and try again.
Problems after firmware upgrade	If you experience problems after a firmware upgrade, roll back to the previously installed version from the Maintenance page.
Problems setting the IP address	
The device is located on a different subnet	If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you cannot set the IP address. Contact your network administrator to obtain an IP address.
The IP address being used by another device	<p>Disconnect the Axis device from the network. Run the ping command (in a Command/DO S window, type ping and the IP address of the device):</p> <ul style="list-style-type: none"> <li>• If you receive: Reply from &lt;IP address&gt;: 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 device.</li> <li>• If you receive: A request timed out, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.</li> </ul>
Possible IP addresses conflict with another device on the same subnet	<p>The static IP address in the Axis device is used before the DHCP server sets a dynamic address.</p> <p>This means that if the same default static IP address is also used by another device, there may be problems accessing the device.</p>
The device can't be accessed from a browser	
Can't log in	<p>When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type http or https in the browser's address field. If the password for the user root is lost, the device must be reset to the factory default settings. See Reset to factory default settings on page 14.</p>
The IP address has been changed by DHCP	<p>IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).</p> <p>If required, a static IP address can be assigned manually. For instructions, go to <a href="https://axis.com/support">axis.com/support</a>.</p>
Certificate error when using IEEE 802.1X	For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to System > Date and time.

The device is accessible locally but not externally

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

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

For instructions and download, go to [axis.com/vms](https://axis.com/vms).

## Performance considerations

When setting up your system, it is important to consider how various settings and situations affect performance. Some factors affect the amount of bandwidth (the bitrate) required, others can affect the frame rate, and some affect both. If the load on the CPU reaches its maximum, this also affects the frame rate.

The following factors are the most important to consider:

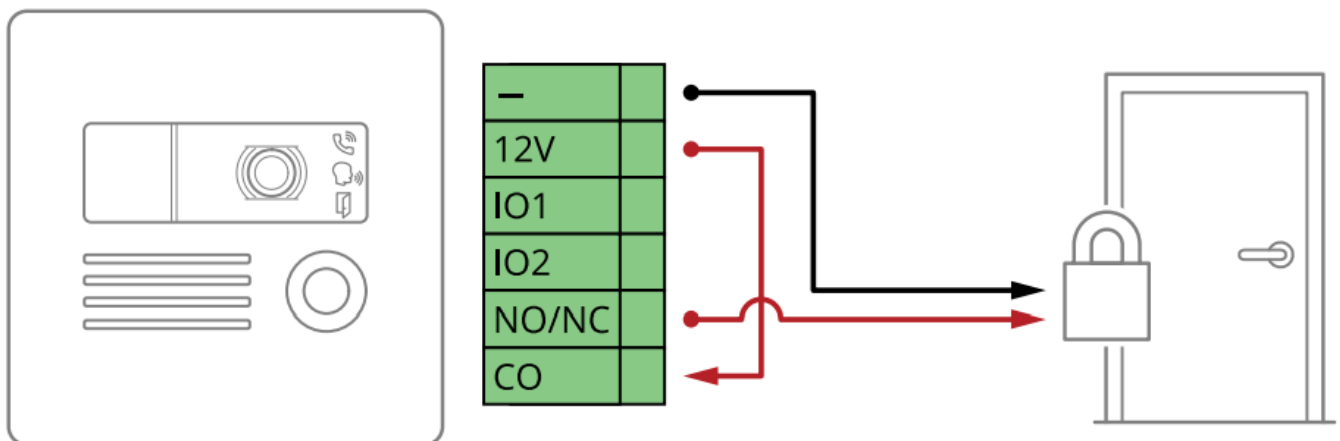
- High image resolution or lower compression levels result in images containing more data which in turn affects the bandwidth.
- Access by large numbers of Motion JPEG or unicast H.264 clients affects the bandwidth.
- Simultaneous viewing of different streams (resolution, compression) by different clients 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 Motion JPEG and H.264 video streams simultaneously affect both frame rate and bandwidth.
- Heavy usage of event settings affects the product's CPU load which in turn affects the frame rate.
- Using HTTPS may reduce the frame rate, in particular, if streaming Motion JPEG.
- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Viewing 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



Contact support at [axis.com/support](https://axis.com/support).

## Connect equipment

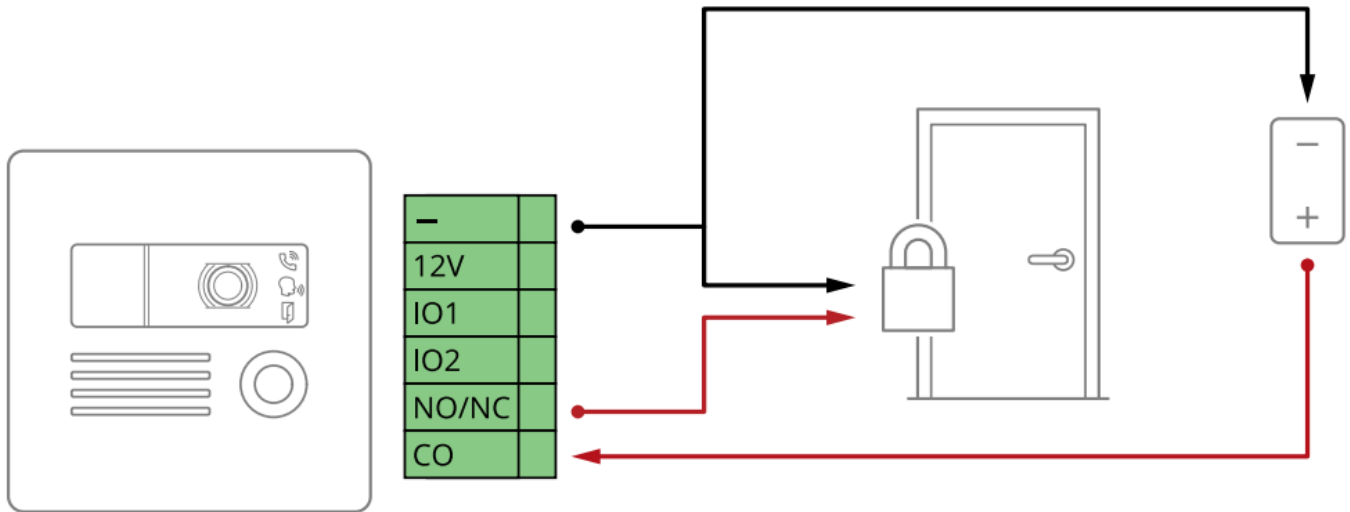
### Relay powered by PoE (12V)



1. To check the 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

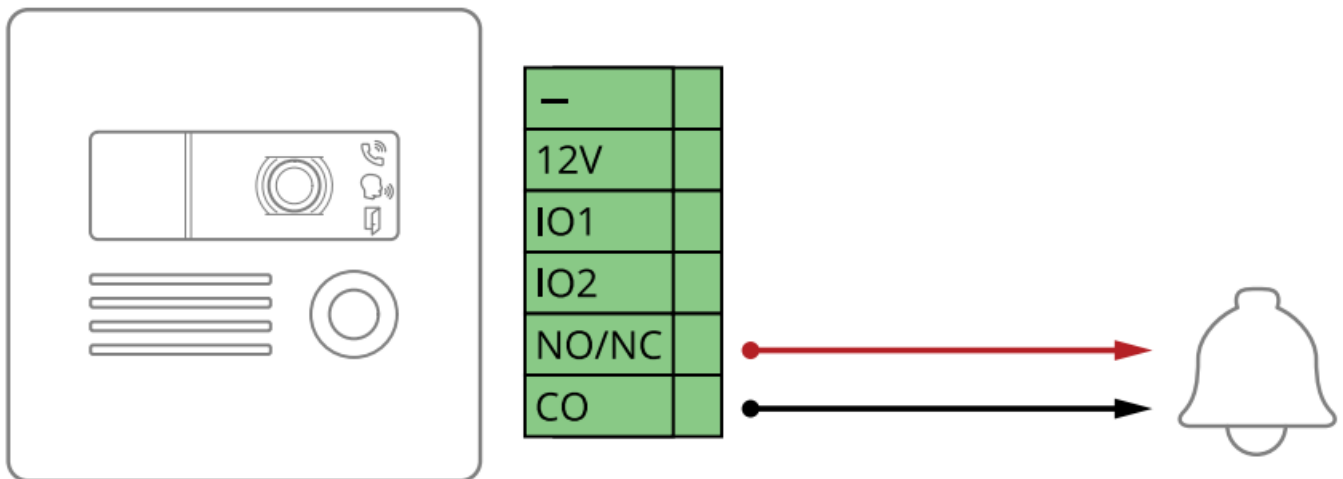


1. To check relay state, go to System > Accessories and find the relay port.

2. Set Normal state to:



-  for a fail-secure lock.
-  for a fail-safe lock.

## Potential-free relay

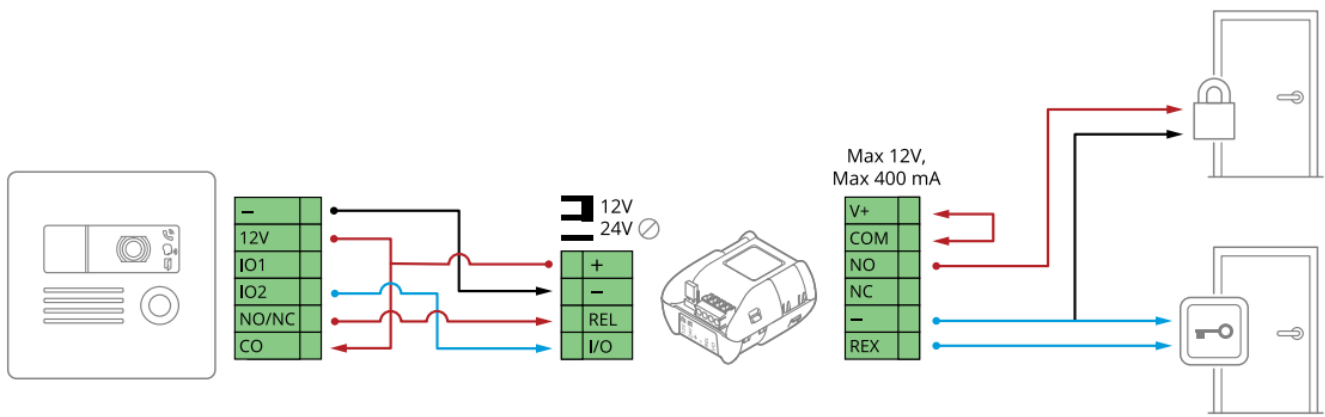


1. To check relay state, go to System > Accessories and find the relay port.

2. Set Normal state to:



-  for a fail-secure lock.
-  for a fail-safe lock.

## 12V Fail-secure lock powered by PoE from intercom

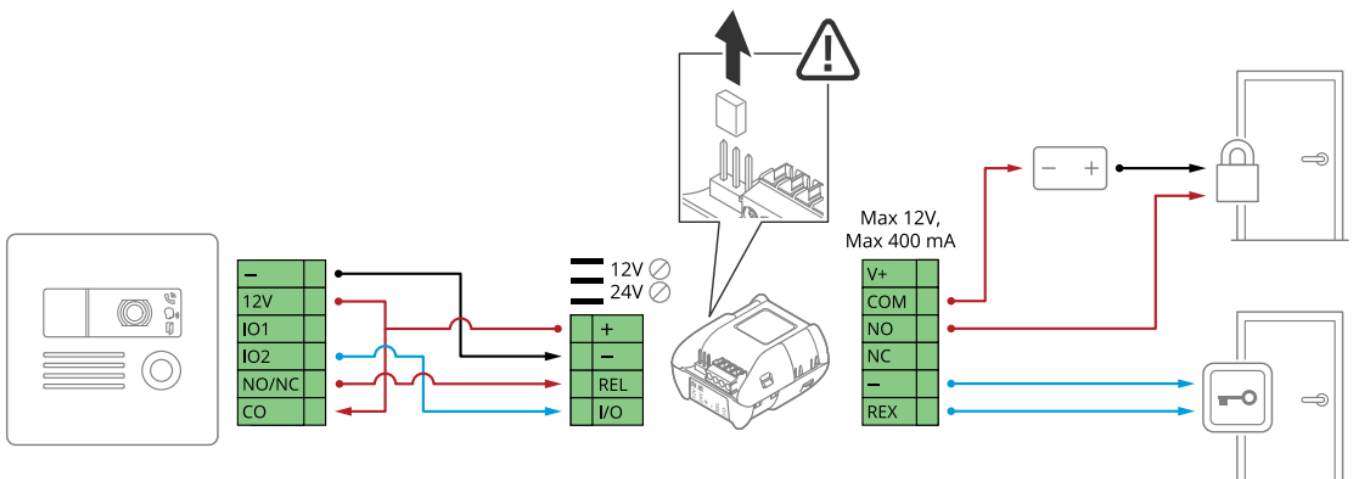


1. To check relay state, go to System > Accessories and find the relay port.

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.

## Specifications

### Front panel indicators and controls

When you connect the product to power, the indicator icons, and the indicator strip light up for a few seconds.

### Call indicator icons

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

## LED indicators

Status LED	Indication
Green	Steady green for normal operation.

## SD card slot

### NOTICE

- Risk of damage to SD card. Do not 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. Do not remove the SD card while the product is running. Unmount the SD card from the product's webpage before removal.

This product supports microSD/microSDHC/microSDXC cards.  
For SD card recommendations, see [axis.com](https://www.axis.com).



microSD, microSDHC, and microSDXC Logos are trademarks of SD-3C LLC. microSD, microSDHC, and 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 14.

## Connectors

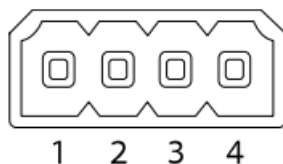
### Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

### Audio connector

4-pin terminal block for audio input and output.





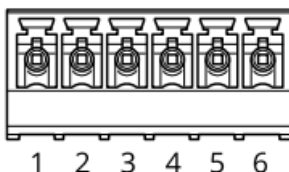
Function	Pin	Notes
Line in	1	Line in (mono)
GND	2	Audio ground
Line out	3	Line out (mono)
GND	4	Audio ground

### I/O connector

Use the 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 (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 product's webpage.



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

## 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

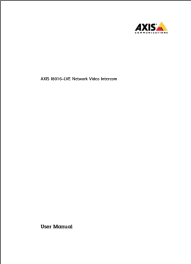
Indicates significant information which is essential for the product to function correctly.

### Note

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

**User Manual**  
**AXIS I8016-LVE Network Video Intercom**  
**© Axis Communications AB, 2020 – 2022**  
**Ver. M6.4**  
**Date: February 2022**  
**Part No. T10154915**

## Documents / Resources

	<p><a href="#">AXIS I8016-LVE Network Video Intercom</a> [pdf] User Manual I8016-LVE, Network Video Intercom, I8016-LVE Network Video Intercom</p>
--	--

## References

- [Axis Communications - Leader in network cameras and other IP networking solutions | Axis Communications](#)
- [AXIS GENERAL SOFTWARE LICENSE TERMS | Axis Communications](#)
- [Welcome to Axis support | Axis Communications](#)
- [Firmware | Axis Communications](#)
- [Video management software | Axis Communications](#)
- [Axis documentation](#)