AXIS A8207-VE Network Video Door Station

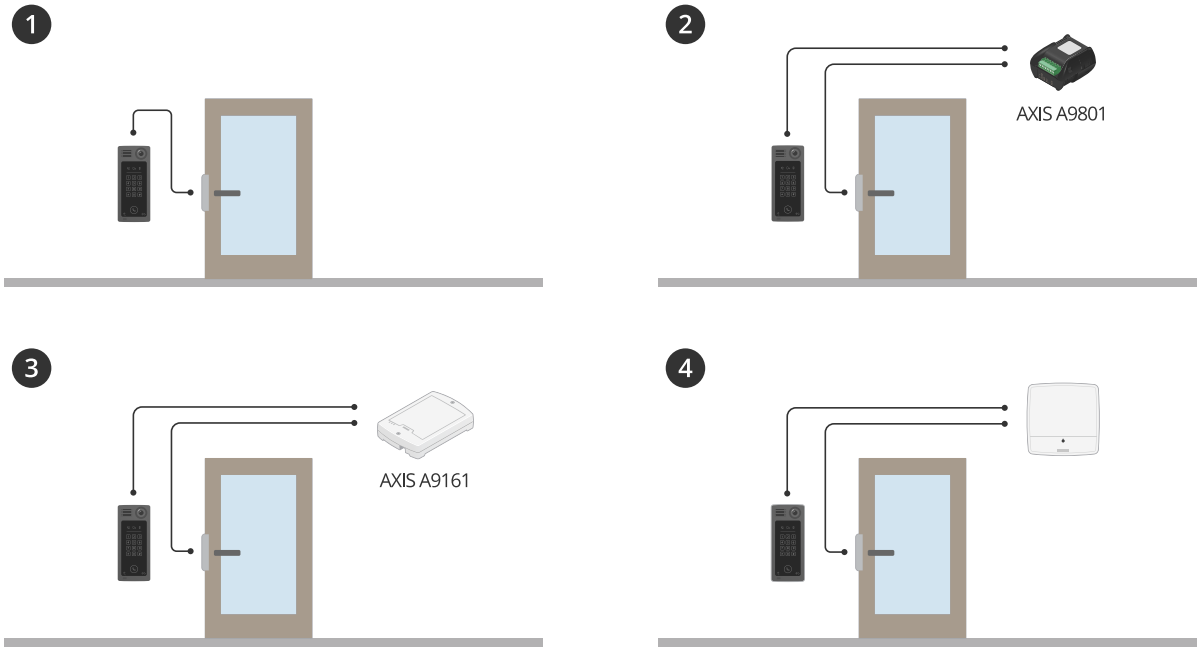
User manual

Table of Contents

Solution overview 4
Product overview 5
Installation 7
Get started 8
  Find the device on the network 8
    Browser support 8
  Open the device's web interface 8
  Create an administrator account 8
  Secure passwords 9
  Make sure that no one has tampered with the device software 9
  Web interface overview 9
Configure your device 10
  Change the root password 10
  Set up direct SIP (P2P) 10
  Set up SIP through a server (PBX) 11
  Create a contact 11
  Configure the call button 12
  Set up as reader 12
    Use Entry list to allow credential holders to open the door 12
    Set up as card reader using a door controller 13
  Use DTMF to unlock the door for a visitor 14
  Transmit live video to a monitor 14
The web interface 16
Learn more 17
  Voice over IP (VoIP) 17
    Session Initiation Protocol (SIP) 17
    Peer-to-peer SIP (P2PSIP) 17
    Private Branch Exchange (PBX) 18
  Set up rules for events 19
  Analytics and apps 19
    AXIS Client for Unified Communication Systems 19
Daily use 20
  Use the keypad 20
Troubleshooting 21
  Reset to factory default settings 21
  Check the current AXIS OS version 21
  Upgrade AXIS OS 21
  Technical issues, clues and solutions 22
  Performance considerations 23
Specifications 24
  Front panel indicators and controls 24
    Indicator icons 24
    Card reader indicator stripe 24
    Call button 24
  LED indicators 24
  SD card slot 24
  Buttons 24
    Control button 24
  Connectors 25
    HDMI connector 25
    Network connector 25
    Audio connector 25
    Relay connector 25

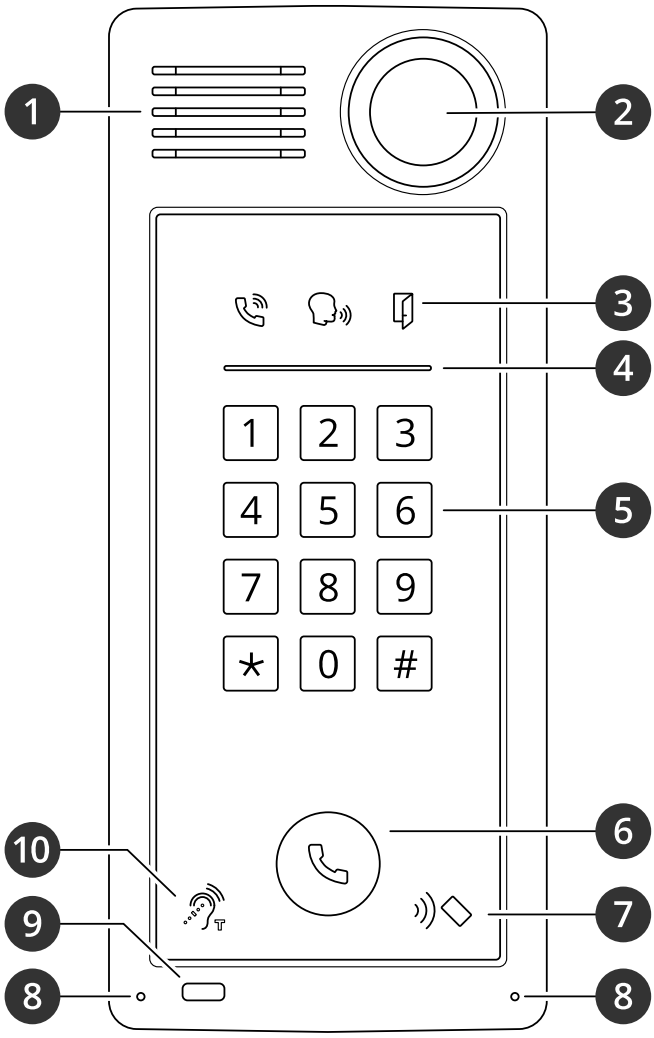
Reader connector 26
I/O connector 26
Power connector 27
Safety information 28
Hazard levels 28
Other message levels 28

Solution overview

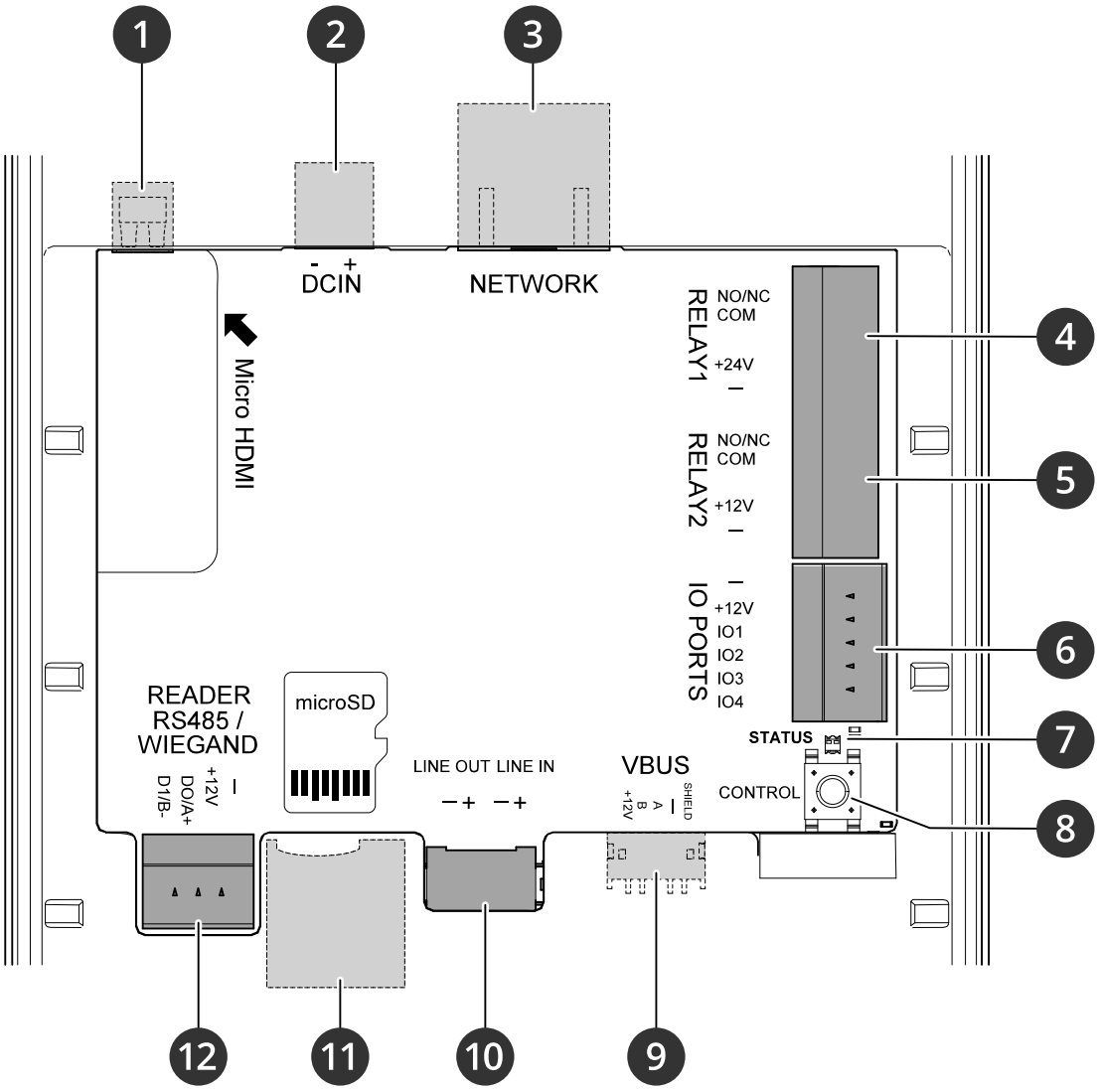


1 *Door station*
2 *Door station combined with AXIS A9801*
3 *Door station combined with AXIS A9161*
4 *Door station combined with an access control system, for example AXIS A1001 or AXIS A1601*

Product overview



1 *Speaker*
2 *Camera*
3 *Indicator icons, on page 24*
4 *Card reader indicator stripe, on page 24*
5 *Keypad*
6 *Call button, on page 24*
7 *Card reader icon*
8 *Microphone*
9 *PIR-sensor*
10 *T-coil icon*

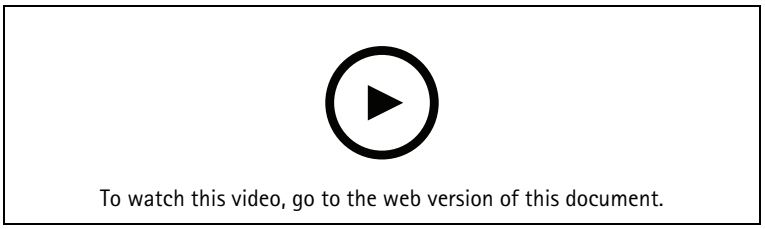


1 *HDMI connector, on page 25 (microHDMI)*
2 *Power connector, on page 27*
3 *Network connector, on page 25 (PoE+)*
4 *Relay connector, on page 25*
5 *Relay connector, on page 25*
6 *I/O connector, on page 26*
7 *Status LED*
8 *Control button, on page 24*
9 *2N VBUS (not used)*
10 *Audio connector, on page 25*
11 *SD card slot, on page 24 (microSD/microSDHC/microSDXC)*
12 *Reader connector, on page 26*

Installation



Installation video for A8207-VE reader.



Installation video for A8207-VE relay.

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 8*.

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 9*.
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 21*.

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 21*.
   After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

Web interface overview

This video gives you an overview of the device's web interface.



Axis device web interface

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.

Change the root password

1. Log in to the device interface and go to **System > Users**.
2. For the root user, click ⋮ **> Update user**.
3. Enter a new password and save.

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 17*.

In this device VoIP is enabled through the SIP protocol. For more information about SIP, see *Session Initiation Protocol (SIP), on page 17*

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 17*.

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 .

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 17*.

In this device, VoIP is enabled through the SIP protocol. For more information about SIP, see *Session Initiation Protocol (SIP), on page 17*

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 18*.

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 10*. 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 **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 17*.

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**.

Set up as reader

You can set up your door station as a reader to allow credential holders to open the door.

By using Entry list, the door station stores the credentials locally and can function as a standalone reader for up to fifty credential holders.

When connecting the door station to a door controller, the door station can still store up to fifty credentials, and if the requested credential is found in the Entry list, the door station manages the access permissions. If a requested credential is not found in the Entry list and the **Use connected door controller** option is enabled, the request is forwarded to the door controller, which then manages the access permissions.

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 as card reader using a door controller

Network connection

To use the door station as a card reader, you can connect it to a door controller. The door controller stores all credentials and keeps track of who is allowed through the door. In this example we connect the devices over the network. We also modify the allowed card types.

Important

The network connection only works with Axis door controllers. To connect to a non-Axis door controller, you need to physically connect the devices with wires. See *Wired connection, on page 13*.

Set up the door station as a card reader

1. Go to **Reader > Connection**.
2. Select the **VAPIX reader** protocol type.
3. Select the protocol for communicating with the door controller.

Note

We recommend turning on **Verify certificate** if you're using **HTTPS**.

4. Enter the IP address for the door controller.
5. Enter the credentials for the door controller.
6. Click **Connect**.
7. Select the entrance reader for the appropriate door.
8. Click **Save**.

Wired connection

To use the door station as a card reader, you can connect it to a door controller. The door controller stores all credentials and keeps track of who is allowed through the door. In this example, we connect the devices with wires, we use the Wiegand protocol, activate the beeper and use one I/O port for the LED. We also modify the allowed card types.

Important

Use I/O ports that are not already in use. If you use I/O ports already in use, any events created for these ports will stop working.

Before you start

- Connect the door station to a door controller.
  See the electrical wiring drawings, which you can download from *axis.com/products/axis-a8207-ve-mk-ii/support*.
- Configure the door controller's hardware, using the Wiegand protocol for the reader. See the door controller's user manual for instructions.

Set up the door station as a card reader

1. Go to **Reader > Connection**.
2. Select **Wiegand** as protocol type.
3. Turn on **Beeper**.
4. Under **Input for beeper**, select **I3**.

5. In **Input used for LED control**, select **1**.
6. Under **Input for LED1**, select **I1**.
7. Select what colors to use for each state.
8. Under **Keypress format**, select **FourBit**.
9. Click **Save**.
10. Go to **Reader > Chip types** and activate the chip types you want to use.

Note

You can keep the default set of chip types but we recommend that you modify the list according to your specific needs.

11. Click **Add data set** to specify the data sets for the different chip types.
12. Click **Save**.

Use DTMF to unlock the door for a visitor

When a visitor makes a call from the door station, 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 door station
- set up the door station to:
  - request the door controller to unlock the door, **or**
  - unlock the door using the internal relay.

You make all settings in the door station's webpage.

Before you start

- Allow SIP calls from the device and create a SIP account. See *Set up direct SIP (P2P), on page 10* and *Set up SIP through a server (PBX), on page 11*.

Define the DTMF signal in the door station

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 door station 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**.

Transmit live video to a monitor

Your device can transmit a live video stream to an HDMI monitor without a network connection. Use the monitor to see who is at the door.

1. Connect an external monitor to the HDMI connector.

2. Adjust the HDMI settings in **System > Video out**.

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*.

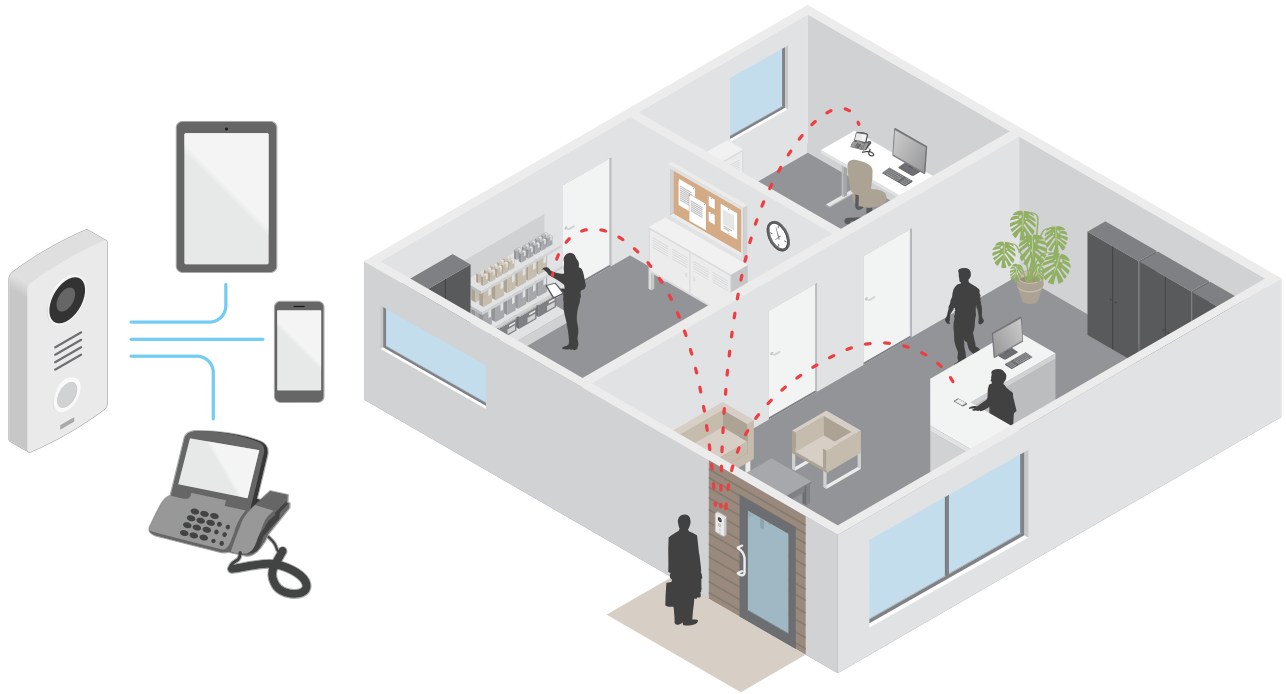
Learn more

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 door station, 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.

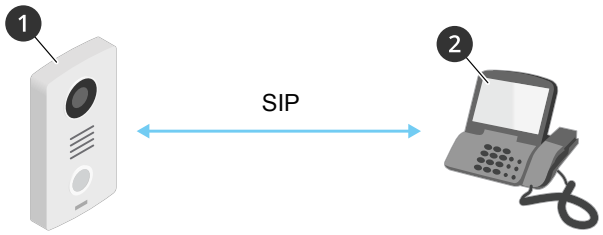
The actual audio or video is exchanged between the SIP user agents with a transport protocol, for example RTP (Real-Time Transport Protocol).

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 - door station. 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 door station to call for example a SIP-enabled phone on the same network using a peer-to-peer SIP setup.

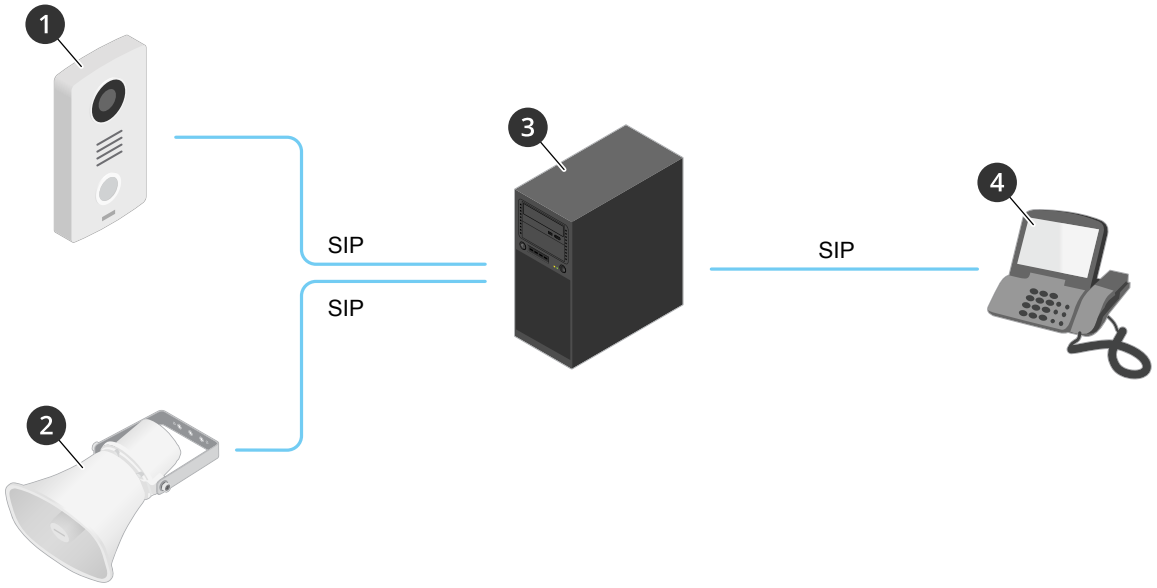
Private Branch Exchange (PBX)

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 door station, 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, see *Get started with rules for events*.

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*.

Daily use

Use the keypad

I want to...	Action
Call someone who can let me into the building.	Press .
Call a person in the building.	Enter the person's speed dial number and press .
Open the door with my card and PIN.	Tap the card and enter the PIN.
Open the door with my PIN.	Enter the PIN and press #.
Open the door with my card.	Tap the card.

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 5*.
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**.

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 Portal: 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 issues, clues and solutions

If you can't find what you're looking for here, try the troubleshooting section at *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 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 is being used by another device	Disconnect the Axis device from the network. Run the ping command (in a Command/DOS window, type `ping` and the IP address of the device): • 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 device. • 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.
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 may be problems accessing the device.

The device cannot be accessed from a browser	
Cannot log in	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 21*.
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 device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).

The device is accessible locally but not externally

To access the device externally, we recommend using 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*.

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.

Specifications

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

Card reader indicator stripe

The stripe indicates reader feedback.

Call button

You can use the built-in light around the call button to light up the faces of visitors.

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 21*.

Connectors

HDMI connector

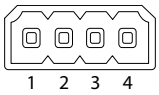
Use the microHDMI™ connector to connect a display or public view monitor.

Network connector

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

Audio connector

4-pin terminal block for audio input and output.

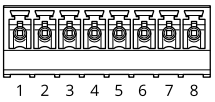


Function	Pin	Notes
Line in	1	Line in (mono)
GND	2	Audio ground
Line out	3	Line out
GND	4	Audio ground

Relay connector

8-pin terminal block for solid state relays that can be used in the following ways:

- 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.



Function	Pin	Notes	Specifications
NO/NC	1	Normally open/normally closed For connecting relay devices. The two relay pins are galvanically separated from the rest of the circuitry.	Max current 1 A Max voltage 30 V DC
COM	2	Common	
24 V DC	3	For powering auxiliary equipment. Note: This pin can only be used as power out.	Output voltage 24 V DC Max current 50 mA[1] Max current 350 mA[2]
DC ground	4		0 V DC
NO/NC	5	Normally open/normally closed For connecting relay devices.	Max current 1 A Max voltage 30 V DC

1. *When powered through Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3.*
2. *When powered through Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4 or DC power input.*

		The two relay pins are galvanically separated from the rest of the circuitry.	
COM	6	Common	
12 V DC	7	For powering auxiliary equipment. Note: This pin can only be used as power out.	Output voltage 12 V DC Max current 100 mA[3] Max current 700 mA[4]
DC ground	8		0 V DC

Reader connector

4–pin terminal block for connecting external reader.

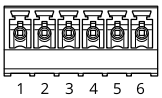
Function	Pin	Notes	Specifications
DC ground	1		0 V DC
12 V DC	2	For powering auxiliary equipment. Note: This pin can only be used as power out.	Output voltage 12 V DC
D0/A+	3	Wiegand: DATA0 output RS485: A+	
D1/B-	4	Wiegand: DATA1 output RS485: B-	

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 VDC 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's web interface.

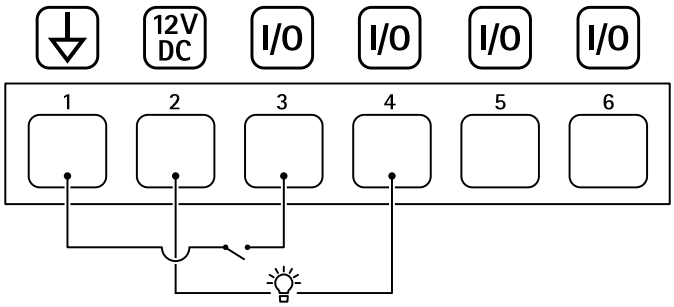


Function	Pin	Notes	Specifications
DC ground	1		0 VDC
DC output	2	⚠ Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 VDC Max load = 50 mA

3. When powered through Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3.
4. When powered through Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4 or DC power input.

Configurable (Input or Output)	3–6	Digital input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 VDC
		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.	0 to max 30 VDC, open drain, 100 mA

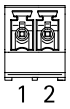
Example:



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

Power connector

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



Function	Pin	Notes	Specifications
DC ground	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 22 W Max load on outputs 9 W

Safety information

Hazard levels

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

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

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

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

Other message levels

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

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

T10121755

2026-02 (M23.2)

© 2019 – 2026 Axis Communications AB