AXIS C1110-E Cabinet Speaker

User manual

Table of Contents

Solution overview

This manual describes how you make the device accessible to your audio system, and how to configure the device directly from its interface.

If you are using an audio or video management software, you can use that software for configuring the device. The following management software are available for controlling your audio system:

- **AXIS Audio Manager Edge** — Audio management software for small systems. Comes pre-installed on all audio devices with a firmware equal to or higher than 10.0.
    - *AXIS Audio Manager Edge user manual*
- **AXIS Audio Manager Pro** — Advanced audio management software for large systems.
    - *AXIS Audio Manager Pro user manual*
- **AXIS Camera Station Pro** — Advanced video management software for large systems.
    - *AXIS Camera Station Pro user manual*

For more information, see *Audio management software*.

To watch this video, go to the web version of this document.

An overview of how network audio works.

Installation

The following video shows an example of how you can install an AXIS C1110-E or C1111-E Cabinet Speaker.

For complete instructions on all installation scenarios as well as important safety information, see the installation guide on *axis.com/products/axis-c1110-e/support*.

To watch this video, go to the web version of this document.

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

Access the device

1. Open a browser and enter the IP address or host name of the Axis device.

2. Enter the username and password. If you access the device for the first time, you must set the root password. See *Set a new password for the root account, on page 5*.

Set a new password for the root account

Important
> The default administrator username is **root**. If the password for root is lost, reset the device to factory default settings. See *Reset to factory default settings, on page 16*

To watch this video, go to the web version of this document.

Support tip: Password security confirmation check

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 **Save**. The password has now been configured.

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.

Additional settings

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 19* to identify the control button.

Set up direct SIP (P2P)

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. To better understand how P2P works, see *Peer-to-peer SIP (P2PSIP), on page 12*.

For more information about setting options, see .

1. Go to **System** > **SIP** > **SIP settings** and select **Enable SIP**.

2. To allow the device to receive incoming calls, select **Allow incoming calls**.

3. Under **Call handling**, set the timeout and duration for the call.

4. Under **Ports**, enter the port numbers.
   - **SIP port** – The network port used for SIP communication. The signaling traffic through this port is non-encrypted. The default port number is 5060. Enter a different port number if required.

   - **TLS port** – The network port used for encrypted SIP communication. The signaling traffic through this port is encrypted with Transport Layer Security (TLS). The default port number is 5061. Enter a different port number if required.

   - **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.

5. Under **NAT traversal**, 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*.

6. Under **Audio**, select at least one audio codec with the desired audio quality for SIP calls. Drag-and-drop to change the priority.

7. Under **Additional**, select additional options.
   - **UDP-to-TCP switching** – Select to allow calls to switch transport protocols from UDP (User Datagram Protocol) to TCP (Transmission Control Protocol) temporarily. The reason for switching

is to avoid fragmentation, and the switch can take place if a request is within 200 bytes of the maximum transmission unit (MTU) or larger than 1300 bytes.

- **Allow via rewrite** – Select to send the local IP address instead of the router's public IP address.

- **Allow contact rewrite** – Select to send the local IP address instead of the router's public IP address.

- **Register with server every** – Set how often you want the device to register with the SIP server for the existing SIP accounts.

- **DTMF payload type** – Changes the default payload type for DTMF.

8. Click **Save**.

Set up SIP through a server (PBX)

Use a PBX-server when user agents will communicate within and outside the IP network. Additional features could be added to the setup depending on the PBX-provider. To better understand how P2P works, see *Private Branch Exchange (PBX), on page 12*.

For more information about setting options, see .

1. Request the following information from your PBX provider:

- User ID

- Domain

- Password

- Authentication ID

- Caller ID

- Registrar

- RTP start port

2. To add a new account, go to **System** > **SIP** > **SIP accounts** and click **+ Account**.

3. Enter the details you received from your PBX provider.

4. Select **Registered**.

5. Select a transport mode.

6. Click **Save**.

7. Set up the SIP settings the same way as for peer-to-peer. See *Set up direct SIP (P2P), on page 7* for more information.

Set up rules for events

You can create rules to make your device perform actions 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 play an audio clip according to a schedule or when it receives a call, or send an email if the device changes IP address.

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

Send an email if a speaker test fails

In this example the audio device is configured to send an email to a defined recipient when a speaker test fails. The speaker test is configured to be performed 18:00 every day.

1. Set up a schedule for the speaker test:
    1.1. Go to the device interface > **System** > **Events** > **Schedules**.
    1.2. Create a schedule that starts at 18:00 and ends at 18:01 every day. Name it "Daily at 6pm".

2. Create an email recipient:

    2.1.   Go to the device interface > **System** > **Events** > **Recipients**.

    2.2.   Click **Add recipient**.

    2.3.   Name the recipient "Speaker test recipients"

    2.4.   Under **Type**, select **Email**.

    2.5.   Under **Send email to**, enter the email addresses of the recipients. Use commas to separate multiple addresses.

    2.6.   Enter the details for the email account of the sender.

    2.7.   Click **Test** to send a test email.

Note

Some email providers have security filters that prevent users from receiving or viewing large attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid delivery problems and locked email accounts.

    2.8.   Click **Save**.

3.   Set up the automated speaker test:

    3.1.   Go to the device interface > **System** > **Events** > **Rules**.

    3.2.   Click **Add a rule**.

    3.3.   Enter a name for the rule.

    3.4.   Under **Condition**, select **Schedule** and select from the trigger list

    3.5.   Under **Schedule**, select your schedule ("Daily at 6pm").

    3.6.   Under **Action**, select **Run automatic speaker test**.

    3.7.   Click **Save**.

4.   Set up the condition for sending an email when the speaker test fails:

    4.1.   Go to the device interface > **System** > **Events** > **Rules**.

    4.2.   Click **Add a rule**.

    4.3.   Enter a name for the rule.

    4.4.   Under **Condition**, select **Speaker test result**.

    4.5.   Under **Speaker test status**, select **Didn't pass the test**.

    4.6.   Under **Action**, select **Send notification to email**.

    4.7.   Under **Recipient**, select your recipient ("Speaker test recipients")

    4.8.   Enter a subject and a message, and click **Save**.

Play audio when a camera detects motion

This example explains how to set up the audio device to play an audio clip when an Axis network camera detects motion.

Prerequisites
- The Axis audio device and Axis network camera are located on the same network.
- The motion detection application is configured and running in the camera.

1.   Prepare an audio clip link:

    1.1.   Go to **Audio** > **Audio clips**.

    1.2.   Click ⋮ > **Create link** for an audio clip.

    1.3.   Set the volume and number of times to repeat the clip.

    1.4.   Click the copy icon to copy the link.

2. Create an action rule:

    2.1.   Go to **System** > **Events** > **Recipients**.

    2.2.   Click **+ Add recipient**.

    2.3.   Type a name for the recipient, for example "Speaker".

    2.4.   Select **HTTP** from the **Type** drop-down list.

    2.5.   Paste the configured link from the audio device in the **URL** field.

    2.6.   Enter the user name and password of the audio device.

    2.7.   Click **Save**.

    2.8.   Go to **Rules** and click **+ Add a rule**.

    2.9.   Type a name for the action rule, for example "Play clip".

    2.10.   From the **Condition** list, select a video motion detection alternative under **Applications**.

> **Note**
>
> If there are no options for video motion detection, then go to **Apps**, click **AXIS Video Motion Detection** and turn on motion detection.

    2.11.   From the **Action** list, select **Send notification through HTTP**.

    2.12.   Under **Recipient**, select your recipient.

    2.13.   Click **Save**.

Stop audio with DTMF

This example explains how to:
- Configure DTMF on a device.

- Set up an event to stop the audio when a DTMF command is sent to the device.

1. Go to **System** > **SIP** > **SIP settings**.

2. Make sure **Enable SIP** is turned on.
   If you need to turn it on, remember to click **Save** afterwards.

3. Go to **SIP accounts**.

4. Next to the SIP account, click ⋮ > **Edit**.

5. Under **DTMF**, click **+ DTMF sequence**.

6. Under **Sequence**, enter "1".

7. Under **Description**, enter "stop audio".

8. Click **Save**.

9. Go to **System** > **Events** > **Rules** and click **+ Add a rule**.

10. Under **Name**, enter "DTMF stop audio".

11. Under **Condition**, select **DTMF**.

12. Under **DTMF Event ID**, select **stop audio**.

13. Under **Action**, select **Stop playing audio clip**.

14. Click **Save**.

Set up audio for incoming SIP calls

You can set up a rule that plays an audio clip when you receive a SIP call.

You can also set up an additional rule that answers the SIP call automatically after the audio clip has ended.
This can be useful in cases where an alarm operator wants to call the attention of someone near an audio device

and establish a line of communication. This is done by making a SIP call to the audio device, which will play an audio clip to alert the persons near the audio device. When the audio clip has stopped playing, the SIP call is automatically answered by the audio device and communication between the alarm operator and the persons near the audio device can take place.

Enable SIP settings:
1. Go to the device interface of the speaker, by entering its IP address in a web browser.

2. Go to **System** > **SIP** > **SIP settings** and select **Enable SIP**.

3. To allow the device to receive incoming calls, select **Allow incoming calls**.

4. Click **Save**.

5. Go to **SIP accounts**.

6. Next to the SIP account, click ⋮ > **Edit**.

7. Uncheck **Answer automatically**.

Play audio when a SIP call is received:
1. Go to **Settings > System > Events > Rules** and add a rule.

2. Type a name for the rule.

3. In the list of conditions, select **State**.

4. In the list of states, select **Ringing**.

5. In the list of actions, select **Play audio clip**.

6. In the list of clips, select the audio clip you want to play.

7. Select how many times to repeat the audio clip. 0 means "play once".

8. Click **Save**.

Answer the SIP call automatically after the audio clip has ended:
1. Go to **Settings > System > Events > Rules** and add a rule.

2. Type a name for the rule.

3. In the list of conditions, select **Audio clip playing**.

4. Check **Use this condition as a trigger.**

5. Check **Invert this condition.**

6. Click **+ Add a condition** to add a second condition to the event.

7. In the list of conditions, select **State**.

8. In the list of states, select **Ringing**.

9. In the list of actions, select **Answer call**.

10. Click **Save**.

Learn more

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:

sip:192.168.1.101   sip:192.168.1.100
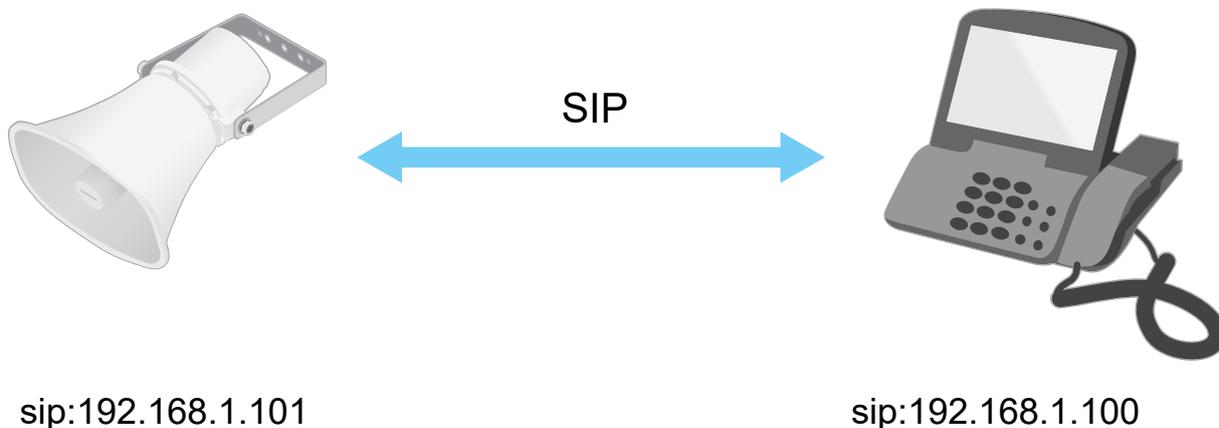
You can set up a SIP-enabled phone to call an audio device on the same network using a peer-to-peer SIP setup.

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:
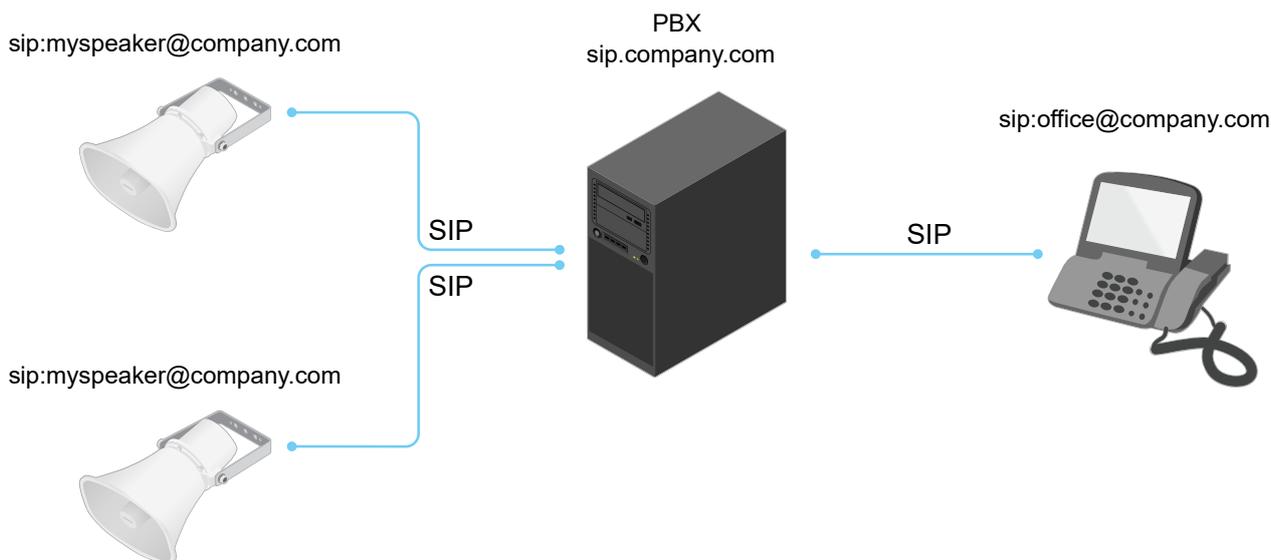
NAT traversal

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 Audio Analytics

AXIS Audio Analytics detects sudden increases in sound volume and specific types of sounds such as screams or shouts within range of the device it's installed on. These detections can be configured to trigger a response, such as recording video, playing an audio message, or alerting security staff. To find out more about how the application works, see *AXIS Audio Analytics user manual*.

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*.

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*.

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 19*.

3. Keep the control button pressed for 10 seconds until the status LED indicator turns amber for the second time.

4. Release the control button. The process is complete when the status LED indicator turns green. 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, assign an IP address, set the password, and access the product.

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 16.*
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).
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 **Settings > System > Date and time**.

The device is accessible locally but not externally

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

*   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*.

Problems with sound files

|	
Can't upload media clip	The following audio clip formats are supported: • au file format, encoded in μ-law and sampled with 8 or 16 kHz. • wav file format, encoded in PCM audio. It supports encoding as 8 or 16-bit mono or stereo and sample rate of 8 to 48 kHz. • mp3 file format, in mono or stereo with bitrate of 64 kbps to 320 kbps and sample rate of 8 to 48 kHz.
Media clips are played with different volumes	A sound file is recorded with a certain gain. If your audio clips have been created with different gains, they will be played with a different loudness. Make sure that you use clips that have the same gain.

Performance considerations

When you set up your system, it's important to consider how different settings and situations affect the required bandwidth (bitrate).

The most important factors to consider:

- Heavy network utilization due to poor infrastructure affects the bandwidth.
- Running multiple AXIS Camera Application Platform (ACAP) applications simultaneously may affect the general performance.

Specifications

Product overview
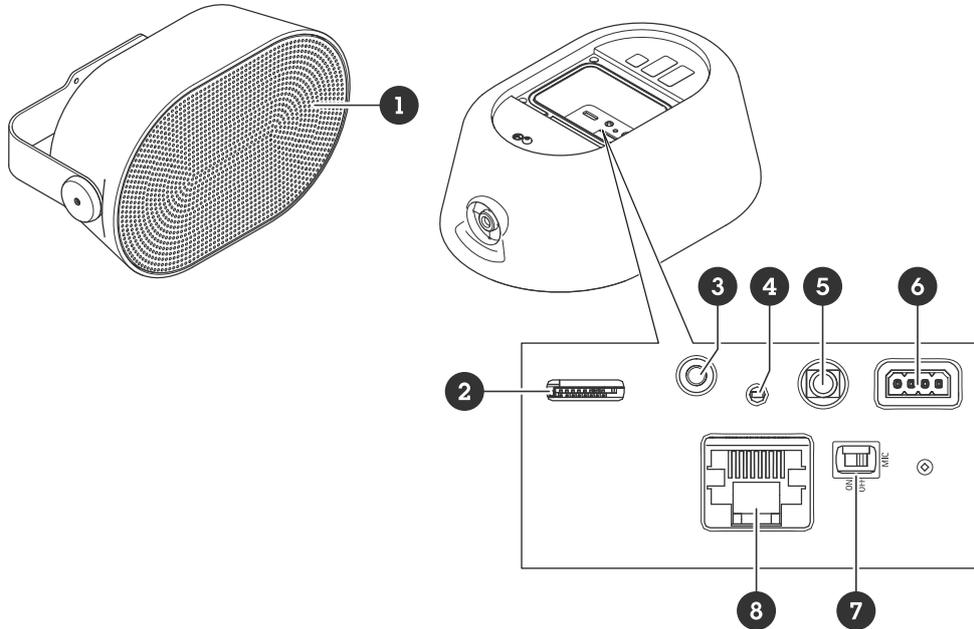
1 Mesh cover
2   SD card slot, on page 20
3   Control button, on page 20
4 Status LED, see
5   Audio connector, on page 20
6 I/O connector, on page 21
7 Microphone disable switch, on page 20
8 Network connector, on page 20

LED indicators

Status LED	Indication
Unlit	Unlit for normal operation.
Green	Steady for 10 seconds for normal operation after startup completed.
Amber	Steady during startup. Flashes during device software upgrade or reset to factory default.
Amber/Red	Flashes if network connection is unavailable or lost.
Red	Flashes slowly if upgrade failed.
Red/Green	Flashes fast when **Locate device** is selected.

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.

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

SD, SDHC, and SDXC Logos are trademarks of SD-3C LLC. SD, SDHC and SDXC 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:
- Calibrating the speaker test. Press and release the control button and a test tone is played.

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 16*.

Microphone disable switch

For location of the microphone disable switch, see *Product overview, on page 19*.

The microphone disable switch is used to mechanically turn the microphone **ON** or **OFF**. The factory default setting for this switch is **ON**.

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

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

Audio connector

- **Audio in** – 3.5 mm input for a stereo microphone, or a line-in stereo signal.

Audio input

1 Tip	2 Ring	3 Sleeve
Unbalanced microphone (with or without electret power) or line	Electret power if selected	Ground
Balanced microphone (with or without phantom power) or line, "hot" signal	Balanced microphone (with or without phantom power) or line, "cold" signal	Ground

Digital signal	Ring power if selected	Ground
Stereo unbalanced microphone (with or without electret power) or line, "left"	Stereo unbalanced microphone (with or without electret power) or line, "right"	Ground

Audio output

1 Tip	2 Ring	3 Sleeve
Channel 1, unbalanced line, mono	Channel 1, unbalanced line, mono	Ground
Balanced line, "hot" signal	Balanced line, "cold" signal	Ground
Stereo unbalanced line, "left"	Stereo unbalanced line, "right"	Ground
Channel 1, unbalanced line	Channel 2, unbalanced line	Ground

The internal microphone is used by default; the external microphone is used when connected.
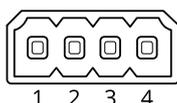
I/O connector

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.

Supervised input – Enables possibility to detect tampering on a digital input.

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.

4-pin terminal block

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
Configurable (Input or Output)	3–4	Digital input or Supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	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:
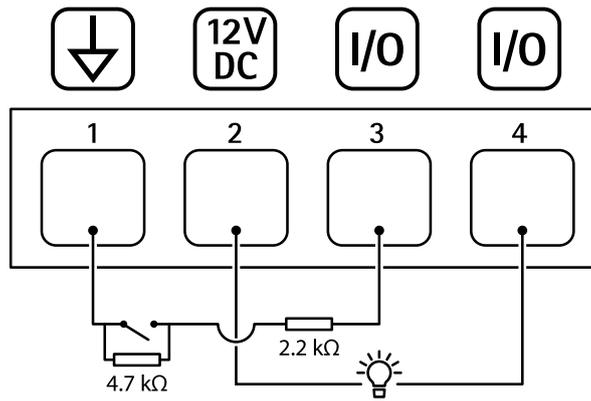
1 DC ground
2 DC output 12 V, max 50 mA
3 I/O configured as supervised input
4 I/O configured as output

API commands

VAPIX® is Axis' own open API (Application Programming Interface). You can control almost all functionality available in Axis devices through VAPIX®. To get access to the complete VAPIX® documentation, join Axis Developer Community at *axis.com/developer-community*

Enter the commands in a web browser, and replace `<deviceIP>` with the IP address or host name of your device.

Important
> The API commands execute immediately. If you restore or reset your device all settings will be lost. For example action rules.

Example: Request
Restart the device
Request
```
http://<deviceIP>/axis-cgi/restart.cgi
```

Example: Request
Restore the device. The request returns most settings to default values, but keeps the IP number.
Request
```
http://<deviceIP>/axis-cgi/factorydefault.cgi
```

Example: Request
Reset the device. The request returns all settings including IP number to default values.
Request
```
http://<deviceIP>/axis-cgi/hardfactorydefault.cgi
```

Example: Request
See a list of all device parameters.
Request
```
http://<deviceIP>/axis-cgi/param.cgi?action=list
```

Example: Request
Get a debug archive
Request
```
http://<deviceIP>/axis-cgi/debug/debug.tgz
```

Example: Request
Get a server report
Request
```
http://<deviceIP>/axis-cgi/serverreport.cgi
```

Example: Request
Capture a network trace of 300 seconds
Request
```
http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300
```

Example: Request
Enable FTP
Request
```
http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes
```

Example: Request
Disable FTP
Request
```
http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no
```

Example: Request
Enable SSH
Request
```
http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes
```

Example: Request
Disable SSH
Request
```
http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no
```