AXIS D4100-VE Mk II Network Strobe Siren

User manual

Table of Contents

Installation

Get started

⚠ WARNING

Flashing or flickering lights can trigger seizures in persons with photosensitive epilepsy.

Find the device on the network

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. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account, on page 5*.

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

Create an administrator account

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

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

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.

Configure your device

Turn off maintenance mode after installing the siren

⚠ CAUTION

To protect the installer from hearing damage and from dazzling by bright light, it's recommended to have maintenance mode on when installing the device.

When you install the device for the first time, maintenance mode is on by default. When the device is in maintenance mode, the siren makes no sound and the light gives white pulsating light patterns.

Go to **Overview** > **Maintenance** to turn off **Maintenance mode**.

Turn on maintenance mode

To perform service of the device, go to **Overview** > **Maintenance** and turn on **Maintenance mode**. Ordinary light and siren activities are then paused.

Configure a profile

A profile is a collection of set configurations. You can have up to 30 profiles with different priorities and patterns.

To set a new profile:

1. Go to **Profiles** and click + **Create**.
2. Enter a **Name** and **Description**.
3. Select the **Light** and **Siren** settings that you want for your profile.
4. Set the light and siren **Priority** and click **Save**.

To edit a profile, click ⋮ and select **Edit**.

Import or export a profile

If you want to use a profile with predefined configurations, you can import it:

1. Go to **Profiles** and click + **Import**.
2. Browse to locate the file or drag and drop the file that you want to import.
3. Click **Save**.

To copy one or more profiles and save to other devices, you can export them:

1. Select the profiles.
2. Click **Export**.
3. Browse to locate the .json files.

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.

For more information about setting options, see *SIP*.

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*.

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.

For more information about setting options, see *SIP*.

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

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

Trigger an action

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

Start a profile when an alarm is triggered

This example explains how to trigger an alarm when the digital input signal is changed.

Set direction input for the port:

1. Go to **System** > **Accessories** > **I/O ports**.
2. Go to **Port 1** > **Normal state** and click **Circuit closed**.

Create a rule:

1. Go to **System** > **Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, select **I/O** > **Digital input is active**.
4. Select **Port 1**.
5. In the list of actions, select **Run light and siren profile while the rule is active**.
6. Select the profile you want to start.
7. Click **Save**.

Start a profile through SIP

This example explains how to trigger an alarm through SIP.

Activate SIP:

1. Go to **System** > **SIP** > **SIP settings**.
2. Select **Enable SIP** and **Allow incoming calls**.
3. Click **Save**.

Create a rule:

1. Go to **System** > **Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, select **Call** > **State**.
4. In the list of state, select **Active**.
5. In the list of actions, select **Run light and siren profile while the rule is active**.
6. Select the profile you want to start.

7. Click **Save**.

Control more than one profile through SIP extensions

Activate SIP:

1. Go to **System** > **SIP** > **SIP settings**.
2. Select **Enable SIP** and **Allow incoming calls**.
3. Click **Save**.

Create a rule to start a profile:

1. Go to **System** > **Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, select **Call** > **State change**.
4. In the list of reasons, select **Accepted by device**.
5. In **Call direction**, select **Incoming**.
6. In **Local SIP URI**, type **<sip:[Ext]@[IP address]>** where [Ext] is the extension used for the profile and [IP address] is the device address. For example **sip:1001@192.168.0.90**.
7. In the list of actions, select **Light and Siren** > **Run light and siren profile**.
8. Select the profile you want to start.
9. Select the action **Start**.
10. Click **Save**.

Create a rule to stop a profile:

1. Go to **System** > **Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, select **Call** > **State change**.
4. In the list of reasons, select **Terminated**.
5. In **Call direction**, select **Incoming**.
6. In **Local SIP URI**, type **sip:[Ext]@[IP address]** where [Ext] is the extension used for the profile and [IP address] is the device address. For example **sip:1001@192.168.0.90**.
7. In the list of actions, select **Light and Siren** > **Run light and siren profile**.
8. Select the profile you want to stop.
9. Select the action **Stop**.
10. Click **Save**.

Repeat the steps to create start and stop rules for each profile you want to control through SIP.

Run two profiles with different priorities

If you run two profiles with different priorities, the profile with a higher priority number will interrupt the profile with a lower priority number.

Note

If you run two profiles with the same priority, the most recent profile will cancel the previous one.

This example explains how to set the device to show one profile with priority 4 over another profile with priority 3 when triggered by the digital I/O port.

Create profiles:

1. Create a profile with priority 3.

2. Create another profile with priority 4.

Create a rule:

1. Go to **System** > **Events** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, select **I/O** > **Digital input is active**.
4. Select a port.
5. In the list of actions, select **Run light and siren profile while the rule is active**.
6. Select the profile that has the highest priority number.
7. Click **Save**.
8. Go to **Profiles** and start the profile with the lowest priority number.

Activate a strobe siren through virtual input when a camera detects motion

This example explains how to connect a camera to the strobe siren, and activate a profile in the strobe siren whenever the application AXIS Motion Guard, installed in the camera, detects motion.

Before you start:

- Create a new account with Operator or Administrator privileges in the strobe siren.
- Create a profile in the strobe siren.
- Set up AXIS Motion Guard in the camera and create a profile called "Camera profile".

Create two recipients in the camera:

1. In the camera's device interface, go to **System > Events > Recipients** and add a recipient.
2. Enter the following information:
   - **Name**: Activate virtual port
   - **Type**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     Replace <IPaddress> with the address of the strobe siren.
   - The account and password of the newly created strobe siren account.
3. Click **Test** to make sure all data is valid.
4. Click **Save**.
5. Add a second recipient with the following information:
   - **Name**: Deactivate virtual port
   - **Type**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
     Replace <IPaddress> with the address of the strobe siren.
   - The account and password of the newly created strobe siren account.
6. Click **Test** to make sure all data is valid.
7. Click **Save**.

Create two rules in the camera:

1. Go to **Rules** and add a rule.
2. Enter the following information:
   - **Name**: Activate virtual IO1
   - **Condition**: **Applications > Motion Guard: Camera profile**
   - **Action**: **Notifications > Send notification through HTTP**

- **Recipient**: **Activate virtual port**
- **Query string suffix**: schemaversion=1&port=1

3. Click **Save**.
4. Add another rule with the following information:
   - **Name**: Deactivate virtual IO1
   - **Condition**: **Applications > Motion Guard: Camera profile**
   - Select **Invert this condition**.
   - **Action**: **Notifications > Send notification through HTTP**
   - **Recipient**: **Deactivate virtual port**
   - **Query string suffix**: schemaversion=1&port=1
5. Click **Save**.

Create a rule in the strobe siren:

1. In the strobe siren's web interface, go to **System > Events** and add a rule.
2. Enter the following information:
   - **Name**: Trigger on virtual input 1
   - **Condition**: **I/O > Virtual input**
   - **Port**: **1**
   - **Action**: **Light and siren > Run light and siren profile while the rule is active**
   - **Profile**: select the newly created profile
3. Click **Save**.

Activate a strobe siren through HTTP post when a camera detects motion

This example explains how to connect a camera to the strobe siren, and activate a profile in the strobe siren whenever the application AXIS Motion Guard, installed in the camera, detects motion.

Before you start:

- Create a new user with the role Operator or Administrator in the strobe siren.
- Create a profile in the strobe siren called: "Strobe siren profile".
- Set up AXIS Motion Guard in the camera and create a profile called: "Camera profile".
- Make sure to use AXIS Device Assistant with firmware version 10.8.0 or later.

Create a recipient in the camera:

1. In the camera's device interface, go to **System > Events > Recipients** and add a recipient.
2. Enter the following information:
   - **Name**: Strobe siren
   - **Type**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/siren_and_light.cgi
     Replace <IPaddress> with the address of the strobe siren.
   - The username and password of the newly created strobe siren user.
3. Click **Test** to make sure all data is valid.
4. Click **Save**.

Create two rules in the camera:

1. Go to **Rules** and add a rule.

2. Enter the following information:
   - **Name**: Activate strobe siren with motion
   - **Condition**: **Applications > Motion Guard: Camera profile**
   - **Action**: **Notifications > Send notification through HTTP**
   - **Recipient**: **Strobe siren**.
     The information must be the same as you previously entered under **Events > Recipients > Name**.
   - **Method**: **Post**
   - **Body**:

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Strobe siren profile"  } }
```

Make sure to enter the same information under '**"profile" : <>**' as you did when you created the profile in the strobe siren, in this case: "Strobe siren profile".

3. Click **Save**.
4. Add another rule with the following information:
   - **Name**: Deactivate strobe siren with motion
   - **Condition**: **Applications > Motion Guard: Camera profile**
   - Select **Invert this condition**.
   - **Action**: **Notifications > Send notification through HTTP**
   - **Recipient**: **Strobe siren**
     The information must be the same as you previously entered under **Events > Recipients > Name**.
   - **Method**: **Post**
   - **Body**:

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Strobe siren
profile"  } }
```

Make sure to enter the same information under '**"profile" : <>**' as you did when you created the profile in the strobe siren, in this case: "Strobe siren profile".

5. Click **Save**.

Activate strobe siren over MQTT when camera detects motion

This example explains how connect a camera to the strobe siren over MQTT, and activate a profile in the strobe siren whenever the application AXIS Motion Guard, installed in the camera, detects motion.

Before you start:

- Create a profile in the strobe siren.
- Set up an MQTT broker and get the broker's IP address, username and password.
- Set up AXIS Motion Guard in the camera.

Set up the MQTT client in the camera:

1. In the camera's device interface, go to **System > MQTT > MQTT client > Broker** and enter the following information:
   - **Host**: Broker IP address
   - **Client ID**: For example Camera 1
   - **Protocol**: The protocol the broker is set to
   - **Port**: The port number used by the broker
   - The broker **Username** and **Password**
2. Click **Save** and **Connect**.

Create two rules in the camera for MQTT publishing:

1. Go to **System > Events > Rules** and add a rule.
2. Enter the following information:
   - **Name**: Motion detected
   - **Condition**: **Applications > Motion alarm**
   - **Action**: **MQTT > Send MQTT publish message**
   - **Topic**: Motion
   - **Payload**: On
   - **QoS**: 0, 1 or 2
3. Click **Save**.
4. Add another rule with the following information:
   - **Name**: No motion
   - **Condition**: **Applications > Motion alarm**
     - Select **Invert this condition**.
   - **Action**: **MQTT > Send MQTT publish message**
   - **Topic**: Motion
   - **Payload**: Off
   - **QoS**: 0, 1 or 2
5. Click **Save**.

Set up the MQTT client in the strobe siren:

1. In the strobe siren's device interface, go to **System > MQTT > MQTT client > Broker** and enter the following information:
   - **Host**: Broker IP address
   - **Client ID**: Siren 1
   - **Protocol**: The protocol the broker is set to
   - **Port**: The port number used by the broker
   - **Username** and **Password**
2. Click **Save** and **Connect**.
3. Go to **MQTT subscriptions** and add a subscription.
   Enter the following information:
   - **Subscription filter**: Motion
   - **Subscription type**: Stateful
   - **QoS**: 0, 1 or 2
4. Click **Save**.

Create a rule in the strobe siren for MQTT subscriptions:

1. Go to **System > Events > Rules** and add a rule.
2. Enter the following information:
   - **Name**: Motion detected
   - **Condition**: **MQTT > Stateful**
   - **Subscription filter**: **Motion**
   - **Payload**: On
   - **Action**: **Light and siren > Run light and siren profile while the rule is active**

- **Profile**: Select the profile you want to be active.

3. Click **Save**.

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

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>`.

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.

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

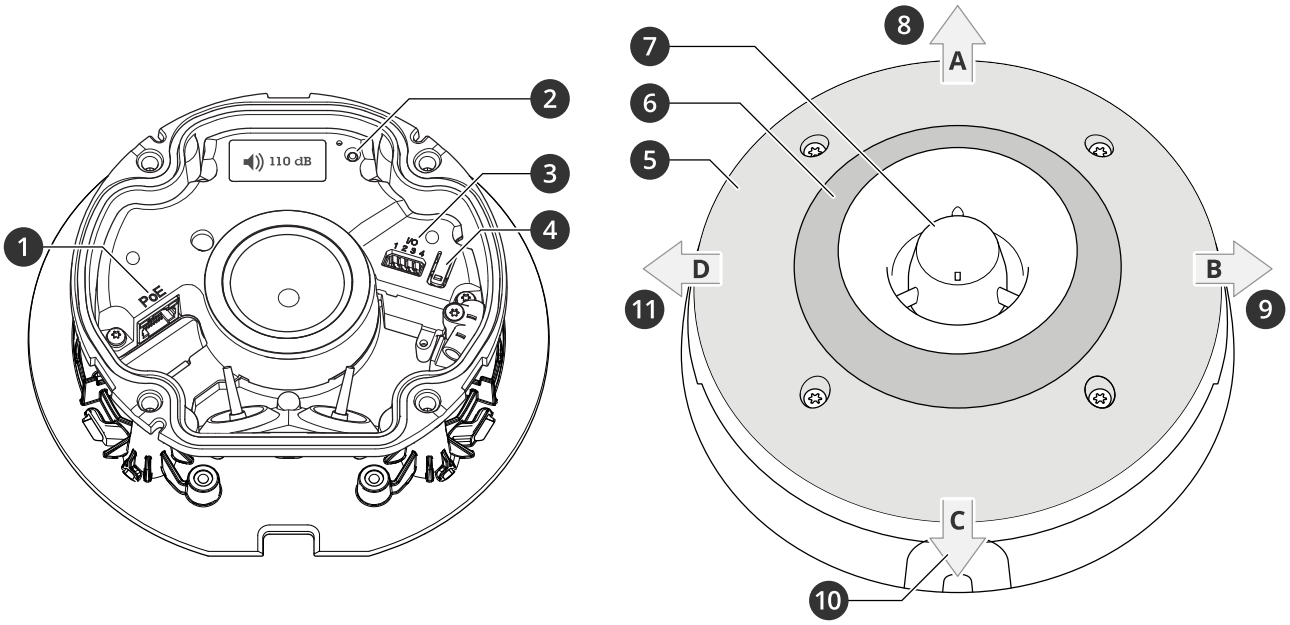
The router must support NAT traversal and UPnP®.

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.

Specifications

Product overview



1 *Network connector PoE*
2 *Status LED indicator*
3 *I/O connector*
4 *Control button*
5 *White LEDs*
6 *RGBA (red, blue, green, amber) LEDs*
7 *Siren*
8 *Light direction A*
9 *Light direction B*
10 *Light direction C*
11 *Light direction D*

LED indicators

Status LED	Indication
Green	Shows steady green for 10 seconds for normal operation after startup completed.
Amber	Steady during startup, during reset to factory default or when restoring settings.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 23*.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and release the button, then wait for the status LED to flash green three times.

Connectors

Network connector

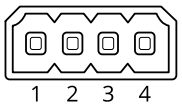
RJ45 Ethernet connector with Power over Ethernet (PoE).

I/O connector

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.

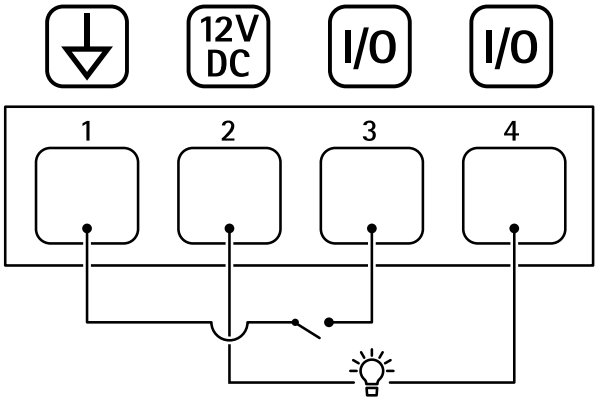
Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the device's web interface.

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 – 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 50mA
3 I/O configured as input
4 I/O configured as output

Light pattern names

Off
Steady
Steady white + flash color
Alternate

Pulse
Escalate 3 steps
Blink 3x
Blink 4x
Blink 3x fade
Blink 4x fade
Flash 1x
Flash 3x
Flash 1x white + steady color
Flash 3x white + steady color
Direction A + steady color
Direction B + steady color
Direction C + steady color
Direction D + steady color
Rotate white + steady color
Rotate tail white + steady color
Random white + steady color
Spin white + steady color
Steady white + steady color

Sound pattern names

Alarm: Alarm high pitch
Alarm: Alarm low pitch
Alarm: Bird
Alarm: Boat horn
Alarm: Car alarm
Alarm: Car alarm fast
Alarm: Classic clock
Alarm: First attender
Alarm: Horror
Alarm: Industrial
Alarm: Single beep
Alarm: Soft quad beep
Alarm: Soft triple beep
Alarm: Triple high pitch

Notification: Accepted
Notification: Calling
Notification: Denied
Notification: Done
Notification: Entry
Notification: Failed
Notification: Hurry
Notification: Message
Notification: Next
Notification: Open
Siren: Alternate
Siren: Bouncy
Siren: Evac
Siren: Falling pitch
Siren: Home soft

Clean your device

You can clean your device with lukewarm water and mild, nonabrasive soap.

NOTICE

- Harsh chemicals can damage the device. Don't use chemicals such as window cleaner or acetone to clean your device.
- Avoid cleaning in direct sunlight or elevated temperatures, since this can cause stains.

1. Use a can of compressed air to remove dust and loose dirt from the device.
2. If necessary, clean the device with a soft microfiber cloth dampened with lukewarm water and mild, nonabrasive soap.
3. To remove any residual cleaning agents, wipe the device with a soft microfiber cloth dampened with lukewarm water.
4. To avoid stains, dry the device with a clean, nonabrasive cloth.

For more information about cleaning of Axis devices, see the white paper *Chemical resistance to common cleaning agents*.

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 18*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
   - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.
   The installation and management software tools are available from the support pages on *axis.com/support*.

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

AXIS OS options

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

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

Upgrade AXIS OS

Important

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

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

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

Note

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

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

When the upgrade has finished, the product restarts automatically.

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

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

Problems after AXIS OS upgrade

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

Problems setting the IP address

Can't set the IP address

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

Problems accessing the device

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

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

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 23*.

The IP address has been changed by DHCP

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

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

Certificate error when using IEEE 802.1X

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

The browser isn't supported

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

Can't access the device externally

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

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

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

Problems with MQTT

Can't connect over port 8883 with MQTT over SSL

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

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

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

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

Problems with the sound	
The device is not as loud as expected	Check that the device is closed correctly and that there are no obstructions in the horn or on the speaker element.
The device makes no sound	Check if the device is in **Maintenance mode**. If it's in maintenance mode, turn it off.

Problems with the light	
The device is not as bright as expected	Check that a PoE class 4 power supply is used. Check the device's ambient temperature. If the device is installed in a high temperature environment, the lights will dim automatically.

Performance considerations

The most important factors to consider:

- Heavy network utilization due to poor infrastructure affects the bandwidth.

Contact support

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

Cybersecurity

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

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

Vulnerability management

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

Security notifications

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

Secure product lifecycle

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

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

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

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

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

T10223803

2026-07 (M6.2)