# AXIS D6310 Air Quality Sensor

User manual

## Table of Contents

## Installation

Important

- Keep at least 1.5 meters (4.9 feet) away from areas with significant vents, or pollution sources. This includes air vents, doors, windows, cooking areas etc.
- Install the device in a location that allows free air flow.
- For effective vaping or smoking detection, install the device on the ceiling at a height of 2.4–2.7 meters (7.9–8.9 feet) from the floor.
- For effective air quality and environmental monitoring, install the device at a height of 0.9–1.8 meters (3.0–5.9 feet) from the floor.

For detailed installation instructions, see the installation guide.

# Get started

**⚠ WARNING**

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

## Find the device on the network

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

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

### Browser support

You can use the device with the following browsers:

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

✓: Recommended

*: Supported with limitations

## Open the device's web interface

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

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

## Create an administrator account

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

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

Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings, on page 31*.

## 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 31*.
   After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

## Place your device

Where you place your device will depend on your use case. Install your device as close to your area of interest as possible while taking the following aspects into consideration:

| Area of interest | Placement | Height | Things to avoid |
|---|---|---|---|
| **Vaping and cigarette smoke** | Ceiling | 2.4–2.7 m (7.9–8.9 ft) | Corners |
| **PM, VOC, $NO_x$, $CO_2$** | Wall | 0.9–1.8 m (3–6 ft) | Corners, heat sources |
| **Humidity** | Ceiling or wall | Any | Windows, ventilation, heat sources, corners |
| **Temperature** | Ceiling or wall | Any | Heating and cooling sources, corners |

### Sensor coverage area

The coverage area extends from the sensor in a cone shape. The detection radius is 2 m (6.5 ft), but the total coverage area shifts based on environmental factors, such as the airflow and the layout of the room.

The coverage area for a sensor used to detect smoking or vaping is 12.6 $m^2$ (135 $ft^2$).

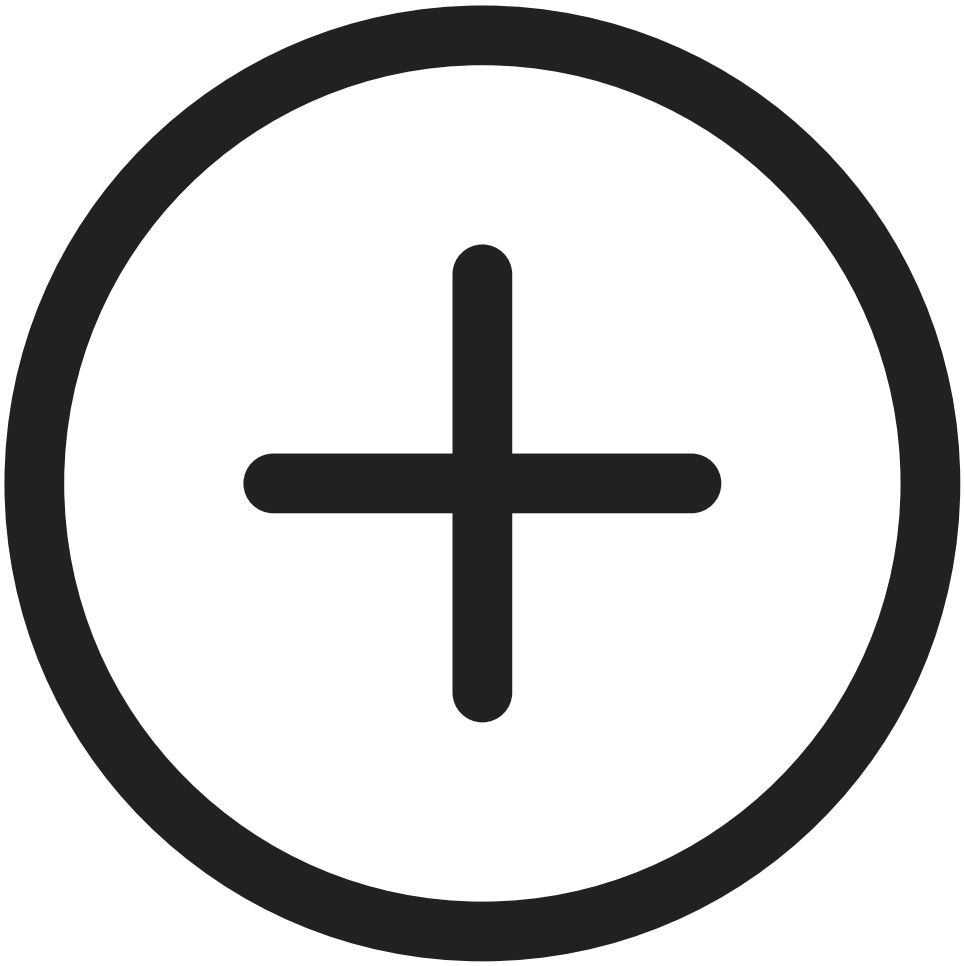
# Configure your device

## Configure air quality monitor

### Configure the dashboard of the air quality sensor

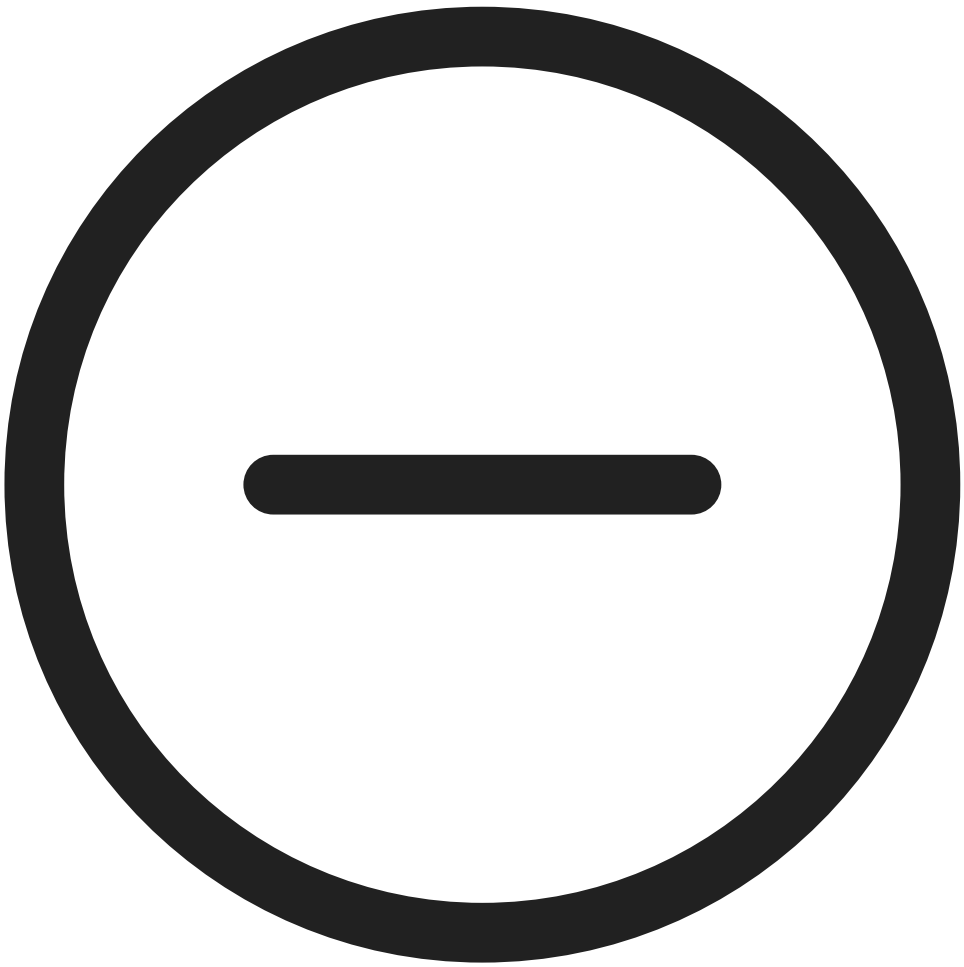
On the device webpage, go to **Air quality monitor** > **Dashboard**:

- To edit the name of the dashboard, click on the left.
- To show data on the dashboard, click **Edit** >



.

- To hide data on the dashboard, Click **Edit** >



.

Note

The dashboard only displays 12 variables at a time. If your dashboard is full, you need to hide an active variable before you can display a new one.

### Set the air quality sensor

On the device webpage, go to **Air quality sensor** > **Settings**.

- Set thresholds of temperature, humidity, CO2, NOx, PM1.0, PM2.5, PM4.0, PM10.0, VOC, AQI, humidex, and heat index. See *Settings*.
- Set vaping detect sensitivity, see *Settings*.
- Set storage retention time, see *Storage settings*.
- Set variable metadata frequency, see *Variable metadata*.
- Set the validation period, see *Validation period*.
- Enable Modbus, see *Modbus*.

### Download sensor data statistics

You can export up to 365 days of sensor statistics to a CSV file for use in applications such as Microsoft® Excel.

1. On the device webpage, go to **Air quality monitor** > **Statistics** > **Sensor Data Statistics**.
2. Choose a date range:
   - **Custom range**: In the **From** and **To** lists, select the start and end dates (up to 365 days).
   - **Predefined range**: In the **Predefined date range** list, select an available period.

   Note

   If both a custom and a predefined range are selected, the custom range takes precedence.

   Note

   The maximum download range is limited by the retention time configured in *Storage settings*.
3. In the **Source** list, select the desired source; to export data for all sources, click **Download all data**.
4. Click **Download data** to export the selected statistics.

Note

Click **Download all data** to export data for all sources within the chosen time span.

### Calibration for the first run of the device

Note

- Full CO2 accuracy takes 2 days the first time the device runs.
- The AQI (Air Quality Index) requires 12 hours to be functional the first time the device runs. The AQI will show **Calculating** until it has enough data. The calibration time is required whenever the device reboots.
- Full VOC accuracy is obtained after the device has been running for one hour. The calibration time is required whenever the device reboots.
- Full NOx accuracy is obtained after the device has been running for 6 hours. The calibration time is required whenever the device reboots.

### Publish MQTT data

Enable variable metadata:

1. Go to **Air quality monitor** > **Settings** > **Variable metadata**.
2. Enable **Variable metadata**.
3. Set your data transmission frequency.

Set up the MQTT broker:

1. Go to **System** > **MQTT**.
2. Enter the broker information:
   - **Host**: IP address
   - **Username** and **Password**
   - **Device topic prefix**: This is where the MQTT data will be published. The default topic will be `axis/MAC-address`.
3. Turn on the MQTT client. The text should change to **Status: Connected**.
4. Click **Save**.

Publish the MQTT data:

1. In the **MQTT publication** tab, click **Add condition**.
2. In the **Add condition** dialogue, enter:
   - **Condition**: Air quality cloud monitoring active

- **MQTT topic:** `axis/{serial}/event/tns:axis/AirQualityMonitor/VariableMetadata`
- **Payload topic:** `axis:AirQualityMonitor/VariableMetadata`

3. Click **Add**.

Note

If you can't see **Air quality cloud monitoring active**, you need to enable variable metadata in **Air quality monitor** > **Settings**.

The condition will publish all of the sensor parameters at the variable metadata interval you chose in a format like the following:


```
( "topic": "axis:AirQualityMonitor/Metadata", "timestamp": 1772553621219,
"message": { "source": { "sensor_name": "D6310" }, "key": {}, "data": { "NOx":
"4.000000", "Humidity": "21.290001", "Temperature": "26.430000", "PM10.0":
"5.200000", "AQI": "28", "PM4.0": "5.000000", "PM1.0": "3.800000", "CO2":
"580", "VOC": "180.000000", "PM2.5": "4.500000", "Humidex": "25", "Heat
index": "26",
```


The metadata fields that are generated will include:

| Field | Description |
|---|---|
| `topic` | The payload topic that produced the condition. |
| `timestamp` | Timestamp when the data was generated. |
| `serial` | MAC address of the device. The serial number is only displayed if you enable **Include serial number** in the **MQTT publication** tab. |
| `message` | A JSON object containing information about the condition. |
| `message.source` | N/A |
| `message.source.sensor_name` | Name of the device that produced the condition. |
| `message.key` | N/A |
| `message.data` | A JSON object containing the data information. |
| `message.data.NOx` | Real-time nitric oxide and nitrogen dioxide concentration. |
| `message.data.Humidity` | Real-time humidity from the air quality sensor. |
| `message.data.Temperature` | Real-time temperature from the air quality sensor in °C or °F. |
| `message.data.PM1.0` | Real-time particle matter 1.0 concentration. |
| `message.data.PM2.5` | Real-time particle matter 2.5 concentration. |
| `message.data.PM4.0` | Real-time particle matter 4.0 concentration. |
| `message.data.PM10.0` | Real-time particle matter 10.0 concentration. |
| `message.data.AQI` | Real-time air quality index based on air quality sensor data. |
| `message.data.CO2` | Real-time carbon dioxide concentration. |

| | |
|---|---|
| `message.data.VOC` | Real-time volatile organic compounds index. |
| `message.data.Humidex` | Real-time humidity index based on humidity and temperature data. |
| `message.data.Heat_index` | Real-time heat index based on humidity and temperature data. |

## 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**.

### Configure a profile with custom siren audio file

You can configure a profile with a custom audio file. You can save audio files up to 100 Mb in size on the device. For larger audio files, use an SD card, if the device is equipped with an SD card slot.

Upload an audio file:

1. Go to **Media** and click **Add**.
2. Browse to select the file from your computer.
3. Select **Storage location**.
4. Click **Save**.

To use the audio file in a profile:

1. Go to **Profiles** and create a profile. Fore more information, see *Configure a profile, on page 11*.
2. When configuring **Siren**, select the uploaded audio file as **Pattern**.

### 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 12* 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.

### Record video when detects vaping

The following example explains how to set up an air quality sensor to record video to the network storage when the air quality sensor detects vaping.

1. In the air quality sensor's webpage, go to **Settings > System > Storage** to check that the network storage is set.
2. Go to **Settings > System > Events** and add a rule. Enter the following information:
   - **Name**: Type a name for the rule.
   - **Condition**: **Air quality monitor > Vaping or smoking detected**.
   - **Action** : **Recordings > Record video**.
   - **Storage**: **Network storage**. Make sure the network storage is set.
   - **Camera**: Select a camera view area.
   - **Stream profile**: Select a stream profile or **Create a stream profile**.
   - **Prebuffer** and **Postbuffer**: Set the desired values.
3. Click **Save**.

### Play audio clip when CO2 is too high

This example explains how to play audio clip when CO2 is too high.

**Create a rule**

1. On the webpage, go to **Events** > **Rules** > **Add a rule** to create a rule.
2. Enter the following information:
   - **Name**: Type a name for the rule.
   - **Conditions**: **Air quality monitor** > **Air quality outside acceptable range**

- **Sensor**: **CO2**
- **Action**: **Play audio clip**
- **Clip**: select an audio clip.

3. Click **Save**.

**Set up the alarm range for CO2**

- In the webpage, go to **Air quality monitor** > **Settings** > **CO2**.
- Enter **MIN** and **MAX** data to set the CO2 range.

### Activate a light and siren profile via PIR sensor

This example explains how to activate a light and siren profile via PIR sensor. See *Product overview, on page 25* for the positions of the light (signaling LEDs) and siren.

Create a light and siren profile:

1. On the device webpage, go to **Profiles > Create**.
2. Enter the following information:
   - **Name**: Profile 1
   - **Description**: Add the profile description.
   - **Light** : Select **Pattern**, **Speed**, **Intensity**, **Color** and **Duration**.
   - **Siren**: Select **Pattern**, **Intensity** and **Duration**.

   Note

   Profiles with higher numbers have a higher priority.
   - **Priority**: Select **Light priority** and **Siren priority**.

Create an event :

1. Go to **System** > **Events** > **Rules** and add a rule.
2. Enter the following information:
   - **Name**: Activate signaling LEDs and siren
   - **Condition**: PIR sensor
   - **Action**: Run light and siren profile
   - **Profile**: Profile 1
   - **Action**: Start
3. Click **Save**.

### 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 light and siren profile through HTTP post when a camera detects motion

This example explains how to connect a camera to the air quality sensor, and activate a light and siren profile in the air quality sensor 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 air quality sensor.
- Create a profile in the air quality sensor called: "Light and 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**: air quality sensor
   - **Type**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/siren_and_light.cgi

Replace <IPaddress> with the address of the air quality sensor.

- The username and password of the newly created air quality sensor 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 air quality sensor with motion
   - **Condition**: **Applications > Motion Guard: Camera profile**
   - **Action**: **Notifications > Send notification through HTTP**
   - **Recipient: air quality sensor.**
     The information must be the same as you previously entered under **Events > Recipients > Name**.
   - **Method**: **Post**
   - **Body**:

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

Make sure to enter the same information under '**"profile" : <>**' as you did when you created the profile in the air quality sensor, in this case: "Light and siren profile".

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

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

Make sure to enter the same information under '**"profile" : <>**' as you did when you created the profile in the air quality sensor, in this case: "Light and siren profile".

5. Click **Save**.

### Activate a light and siren profile through virtual input when a camera detects motion

This example explains how to connect a camera to the air quality sensor, and activate a light and siren profile in the air quality sensor 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 air quality sensor.
- Create a profile in air quality sensor. See *Profiles*.
- 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 air quality sensor.
- The account and password of the newly created air quality sensor 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 air quality sensor.
   - The account and password of the newly created air quality sensor 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 air quality sensor:

1. In the air quality sensor 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 is active**
   - **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 light and siren profile over MQTT when a camera detects motion

This example explains how to connect a camera to the air quality sensor, and activate a light and siren profile in the air quality sensor whenever the camera detects motion.

Before you start:

- Create a profile in the air quality sensor.
- Set up an MQTT broker and get the broker's IP address, username and password.
- Make sure the motion detection application is configured and running in the camera.

Set up the MQTT client in the camera:

1. In the camera's web 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 air quality sensor:

1. In the air quality sensor web 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 air quality sensor 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**.

### 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 custom clip when an alarm is triggered

This example explains how to trigger a custom audio file when the digital input signal changes.

Upload an audio file:

1. Go to **Media** and click **Add**.
2. Click to browse and select the audio file from your computer.
3. Select **Storage location**.
4. Click **Save**.

Create a profile with the audio file:

1. Go to **Profiles** and click **Create**.
2. Enter **Name** and select light pattern for the profile.
3. In the siren section, select the uploaded audio file.
4. Select **Intensity** and **Duration**.
5. Click **Save**.

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. Enter 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 with the uploaded audio file.
7. 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:

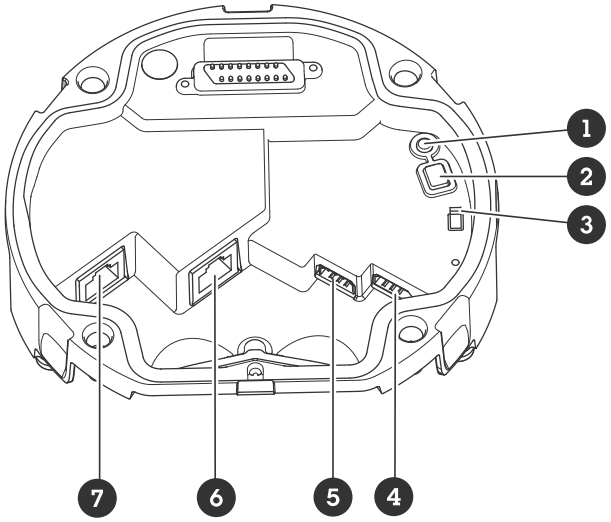
1. Go to **Settings > System > Events > Rules** and add a rule.
2. Type a name for the rule.
3. In the list of conditions, select **Audio clip playing**.
4. Check **Use this condition as a trigger.**
5. Check **Invert this condition.**
6. Click **+ Add a condition** to add a second condition to the event.
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**.

## The web interface

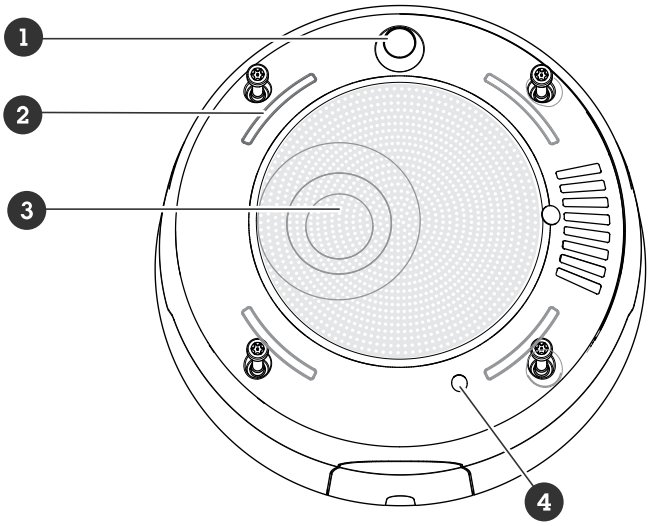
To read about all the features and settings available in the web interface of devices with AXIS OS, go to *AXIS OS web interface help*.

# Specifications

## Product overview




1 *Status LED indicator*
2 *Control button*
3 *Microphone switch*
4 *I/O connector*
5 *RS-485 connector*
6 *Network connector (PoE OUT)*
7 *Network connector (PoE IN)*




1 *PIR sensor*
2 *Signaling LEDs*
3 *Speaker*
4 *Internal microphone*

## Status LED

| 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. |

## Buttons

### Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 31*.

### Microphone switch

For location of the microphone switch, see *Product overview, on page 25*.

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

## Connectors

### Network connector

Input: RJ45 Ethernet connector with Power over Ethernet (PoE).

Output: RJ45 Ethernet connector with Power over Ethernet (PoE).

### I/O connector

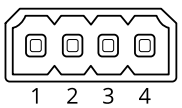
Use the I/O connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 VDC reference point and power (12 V DC output), the I/O connector provides the interface to:

**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.

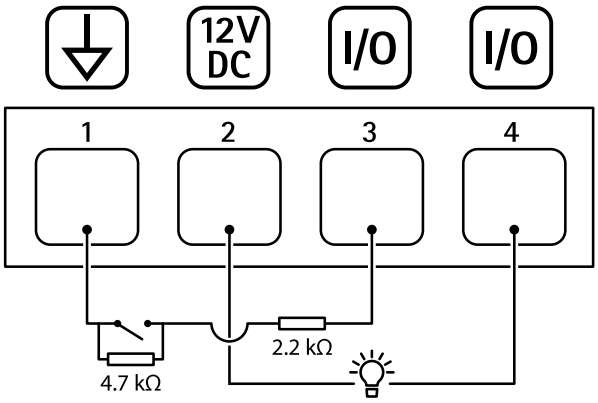
4-pin terminal block




| Function | Pin | Notes | Specifications |
|---|---|---|---|
| DC ground | 1 | | 0 VDC |

| | | | |
|---|---|---|---|
| DC output | 2 | ⚠<br>Can be used to power auxiliary equipment.<br>Note: This pin can only be used as power out. | 12 VDC<br>Max load = 25 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:**

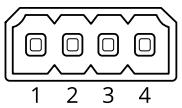



*1 DC ground*
*2 DC output 12 V, max 25 mA*
*3 I/O configured as supervised input*
*4 I/O configured as output*

## RS485/RS422 connector

Two 2-pin terminal blocks for RS485/RS422 serial interface. The serial port can be configured to support:

- Two-wire RS485 half duplex
- Four-wire RS485 full duplex
- Two-wire RS422 simplex
- Four-wire RS422 full duplex point to point communication




| Function | Pin | Notes |
|---|---|---|
| RS485/RS422 RX/TX A | 1 | (RX) For full duplex RS485/RS422<br>(RX/TX) For half duplex RS485 |
| RS485/RS422 RX/TX B | 2 | |
| RS485/RS422 TX A | 3 | (TX) For full duplex RS485/RS422 |
| RS485/RS422 TX B | 4 | |

## Light pattern names

| |
|---|
| Off |
| Steady |
| Alternate |
| Pulse |
| Escalate 3 steps |
| Blink |
| Blink 3x |
| Blink 4x |
| Blink 3x fade |
| Blink 4x fade |
| Flash 1x |
| Flash 3x |

## Siren pattern names

| |
|---|
| Off |
| 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.

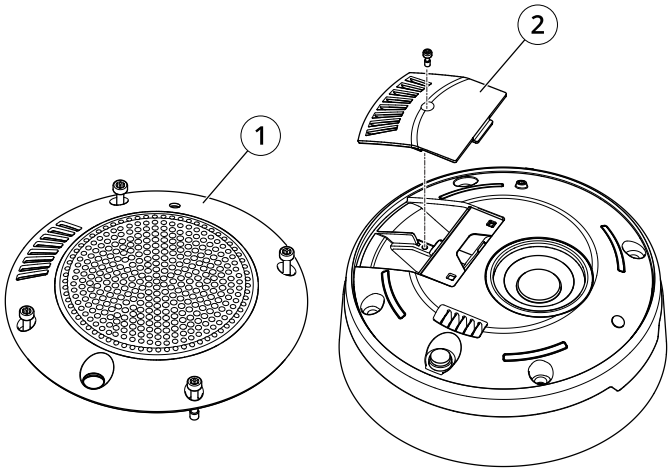
*NOTICE*

- Harsh chemicals can damage the device. Don't use chemicals such as window cleaner or acetone to clean your device.

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.
3. To avoid stains, dry the device with a clean, nonabrasive cloth.

Note

- Remove the cover (1) and the door (2).
- Use a brush to clean the dust.




*1 Cover*
*2 Door*

# 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:

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

## 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 AXIS OS** | |
|---|---|
| AXIS OS upgrade failure | 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** | |
|---|---|
| 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):<br>• 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.<br>• 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 can't be accessed from a browser** | |
|---|---|
| Can't 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.<br>If the password for the root account is lost, the device must be reset to the factory default settings. See *Reset to factory default settings, on page 31*. |

| | |
|---|---|
| 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).<br><br>If required, a static IP address can be assigned 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 device is accessible locally but not externally**

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

- AXIS Camera Station Edge: free of charge, ideal for small systems with basic surveillance needs.
- AXIS Camera Station 5: 30-day trial version free of charge, ideal for small to mid-size systems.
- 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*.

**Can't connect over port 8883 with MQTT over SSL**

| | |
|---|---|
| The firewall blocks traffic using port 8883 as it's deemed insecure. | In some cases the server/broker might not provide a specific port for MQTT communication. It may still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic.<br><br>• 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.<br>• 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. |

**The device doesn't start up after connecting it to another product**

| | |
|---|---|
| Wrong PoE class | Check that a PoE class 4 power supply is used, when the device is connected to another product. |

**The sensor data is not accurate**

| | |
|---|---|
| The sensor data inaccurate | The AQI (Air Quality Index), CO2, VOC and NOx take time to be functional. See *Calibration for the first run of the device, on page 9*. |

## 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.

T10222990

2026-07 (M6.2)