

## **AXIS D4100-E Network Strobe Siren**

# AXIS D4100-E Network Strobe Siren

## Table of Contents

---

<b>Installation</b> .....	3
<b>Get started</b> .....	4
Find the device on the network .....	4
Open the device's webpage .....	4
Webpage overview .....	5
<b>Configure your device</b> .....	6
Turn off maintenance mode after installing the siren .....	6
Turn on maintenance mode .....	6
Configure a profile .....	6
Import or export a profile .....	6
Set up direct SIP (P2P) .....	6
Set up SIP through a server (PBX) .....	7
Set up rules for events .....	8
<b>Learn more</b> .....	15
Session Initiation Protocol (SIP) .....	15
Peer-to-peer SIP (P2PSIP) .....	15
Private Branch Exchange (PBX) .....	15
NAT traversal .....	15
<b>The device interface</b> .....	16
Status .....	16
Overview .....	16
Profiles .....	17
Apps .....	18
System .....	18
Maintenance .....	32
<b>Specifications</b> .....	33
Product overview .....	33
LED indicators .....	33
Buttons .....	33
Connectors .....	33
Light pattern names .....	34
Maximum sound pressure levels .....	35
<b>Cleaning recommendations</b> .....	37
<b>Troubleshooting</b> .....	38
Reset to factory default settings .....	38
Firmware options .....	38
Check the current firmware version .....	38
Upgrade the firmware .....	38
Technical issues, clues, and solutions .....	39
Performance considerations .....	40
Contact support .....	40

# AXIS D4100-E Network Strobe Siren

## Installation

---

### Installation



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

[www.axis.com/products/online-manual/62021#t10168836](http://www.axis.com/products/online-manual/62021#t10168836)

# AXIS D4100-E Network Strobe Siren

## Get started

---

### 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](https://axis.com/support).

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

### Browser support

You can use the device with the following browsers:

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

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

### Open the device's webpage

1. Open a browser and enter the IP address or host name of the Axis device.  
If you do not know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Enter the username and password. If you access the device for the first time, you must set the root password. See *Set a new password for the root account on page 4*.

### Set a new password for the root account

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

1. Type a password. Follow the instructions about secure passwords. See *Secure passwords on page 4*.
2. Retype the password to confirm the spelling.
3. Click **Add user**.

#### **Important**

If you lose the password for the root account, go to *Reset to factory default settings on page 38* and follow the instructions.

### Secure passwords

#### **Important**

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

# AXIS D4100-E Network Strobe Siren

## Get started

---

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.

## Webpage overview

This video gives you an overview of the device interface.



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

[www.axis.com/products/online-manual/62021#t10157625](http://www.axis.com/products/online-manual/62021#t10157625)

*Axis device web interface*

# AXIS D4100-E Network Strobe Siren

## Configure your device

---

### 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.

# AXIS D4100-E Network Strobe Siren

## Configure your device

---

### 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 15.

For more information about setting options, see *SIP* on page 28.

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 15.

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 the communication should be between an infinite number of user agents within and outside the IP network. Additional features could be added to the setup depending on the PBX-provider. To better understand how P2P works, see *Private Branch Exchange (PBX)* on page 15.

For more information about setting options, see *SIP* on page 28.

1. Request the following information from your PBX provider:

# AXIS D4100-E Network Strobe Siren

## Configure your device

---

- 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 6 for more information.

## Set up rules for events

To learn more, check out our guide *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** the device should perform when the conditions are met.

#### Note

If you make changes to an active rule, the rule must be turned on again for the changes to take effect.

## 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 position** 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**.



# AXIS D4100-E Network Strobe Siren

## Configure your device

---

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.

# AXIS D4100-E Network Strobe Siren

## Configure your device

---

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**.
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.

# AXIS D4100-E Network Strobe Siren

## Configure your device

---

### Activate strobe siren when camera detects motion

This example explains how 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.
- Set up AXIS Motion Guard in the camera and create a profile called "Profile A".

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 username and password of the newly created strobe siren user.
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 username and password of the newly created strobe siren user.
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: Profile A
  - **Action:** Notifications > Send notification through HTTP
  - **Recipient:** Activate virtual port
  - **Query string suffix:** schemaversion=1&port=1
3. Click **Save**.

# AXIS D4100-E Network Strobe Siren

## Configure your device

---

4. Add another rule with the following information:
  - **Name:** Deactivate virtual IO1
  - **Condition:** Applications > Motion Guard: Profile A
  - 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 device 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 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.

# AXIS D4100-E Network Strobe Siren

## Configure your device

---

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:

# AXIS D4100-E Network Strobe Siren

## Configure your device

---

- 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.

# AXIS D4100-E Network Strobe Siren

[Learn more](#)

---

[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.

# AXIS D4100-E Network Strobe Siren

## The device interface

---

### The device interface

-  Show or hide the main menu.
-  Access the product help.
-  Change the language.
-  Set light theme or dark theme.
-    The user menu contains:
  - Information about the user who is logged in.
  -  **Change user** : Log out the current user and log in a new user.
  -  **Log out** : Log out the current user.
-  The context menu contains:
  - Analytics data**: Accept to share non-personal browser data.
  - Feedback**: Share any feedback to help us improve your user experience.
  - Legal**: View information about cookies and licenses.
  - About**: View device information, including firmware version and serial number.
  - Legacy device interface**: Change the device interface to the legacy device interface.

### Status

#### NTP sync

Shows NTP synchronization information, including if the device is in sync with an NTP server and the time remaining until the next sync.

**NTP settings**: Click to go to the Date and time page where you can change the NTP settings.

#### Device info

Shows device information, including firmware version and serial number.

**Upgrade firmware**: Click to go to the Maintenance page where you can do a firmware upgrade.

### Overview

#### Light status

Shows the different light activities running on the device. You can have ten activities in the status list running at the same time. When two or more activities run at the same time, the one with the highest priority is played. That row is highlighted in green in the status list.

#### Siren status



# AXIS D4100-E Network Strobe Siren

## The device interface

---

Shows the different siren activities running on the device. You can have ten activities in the status list running at the same time. When two or more activities run at the same time, the one with the highest priority is played. That row is highlighted in green in the status list.

### Maintenance

**Maintenance mode:** Turn on to pause the ordinary light and siren activities during maintenance of the device. When maintenance mode is turned on, a pulsating light pattern is played and the siren is silent. To protect the installer from hearing damage and from dazzling by bright light, the siren makes no sound and the light gives white pulsating light in a triangle.

Maintenance has priority 11. Only system specific activities with higher priority can disrupt the maintenance mode.

Maintenance mode survives a reboot. For example, if you set the time to 2 hours, turn off the device and restart it one hour later, the device will be in maintenance mode for another hour.

When you do a default reset, the device returns to maintenance mode.

#### Duration

- **Continuous:** Select to let the device stay in maintenance mode until you turn it off.
- **Time:** Select to set a time when the maintenance mode will be turned off.

### Health check

**Check:** Click to do a health check of the device to make sure the light and siren are working. Each light section is turned on in turn and a test tone is played to test the functionality of the device. If the health check doesn't pass, go to the system logs for more information.

## Profiles

### Profiles

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



**Create:** Click to create a profile.

- **Name:** Enter a name of the profile.
- **Description:** Enter a description of the profile.
- **Light:** Select from the drop-down menu what kind of **pattern**, **speed**, **intensity** and **color** of the light you want.
- **Siren:** Select from the drop-down menu what kind of **pattern** and **intensity** of the siren you want.
- **Duration:** Set the duration of the activities.
  - **Continuous:** Once started, it runs until it's stopped.
  - **Time:** Set a specified time for how long the activity will last.
  - **Repetitions:** Set the activity to repeat the pattern X times.
- **Priority:** Set the priority of an activity from 1 to 10. Activities with priority numbers higher than 10 cannot be removed from the status list. There are three activities with higher priority than 10, **Maintenance** (11), **Identify** (12) and **Health check** (13).



**Import:** Click to add one or more profiles with predefined configurations.

- **Add:** Add new profiles.

#### Note

You can't have two profiles with the same name.

- **Delete and add:** The old profiles are deleted, and you can upload new profiles.
- **Overwrite:** Updated profiles overwrite the existing profiles.

To copy a profile and save it to other devices, select the profile and click **Export**. A .json file is exported.

# AXIS D4100-E Network Strobe Siren

## The device interface

---



: Click to start a profile. The profile and its activities appear in the status list.


## Apps

**Add app:** Click to install a new app.

**Find more apps:** Click to go to an overview page of Axis apps.



The context menu contains:

- **App log:** Click to view a log of the app events. The log is helpful when you contact support.
- **Activate license with a key:** If the app requires a license, you need to activate it. Use this option if your device doesn't have internet access.  
If you don't have a license key, go to [axis.com/applications](https://axis.com/applications). You need a license code and the Axis product serial number to generate a license key.
- **Activate license automatically:** If the app requires a license, you need to activate it. Use this option if your device has internet access. You need a license code to activate the license.
- **Deactivate the license:** Deactivate the license to use it in another device. If you deactivate the license, you also remove it from the device. To deactivate the license requires internet access.
- **Settings**  : Configure the parameters.
- **Delete:** Delete the app permanently from the device. If you don't deactivate the license first, it remains active.

### Note

The device's performance might be affected if you run several apps at the same time.

**Start:** Start or stop the app.

**Open:** Click to access the app's settings. The available settings depend on the application. Some applications don't have any settings.

## System

### Date and time

The time format depends on the web browser's language settings.

### Note

We recommend you to synchronize the device's date and time with an NTP server.

**Synchronization:** Select an option for synchronizing the device's date and time.

- **Automatic date and time (NTP server using DHCP):** Synchronize with the NTP server connected to the DHCP server.
- **Automatic date and time (manual NTP server):** Synchronize with NTP servers of your choice.
  - **Primary NTP server and Secondary NTP server:** Enter the IP address of one or two NTP servers. When you use two NTP servers, the device synchronizes and adapts its time based on input from both.
- **Custom date and time:** Manually set the date and time. Click **Get from system** to fetch the date and time settings once from your computer or mobile device.

**Time zone:** Select which time zone to use. Time will be automatically adjusted for daylight saving time and standard time.

### Note

The system uses the date and time settings in all recordings, logs and system settings.

# AXIS D4100-E Network Strobe Siren

## The device interface

---

### Network

#### IPv4 and IPv6

##### IPv4

- **Automatic IP (DHCP) and DNS (DHCP):** The recommended setting for most networks. The current settings are updated automatically.
- **Automatic IP (DHCP) and manual DNS:** Contact your network administrator to configure the manual settings. The current automatic settings are updated automatically.
- **Manual IP and DNS:** Contact your network administrator to configure the settings.

**IP address:** Enter a unique IP address for the device. Static IP addresses can be assigned at random within isolated networks, provided that each address is unique. To avoid conflicts, we recommend you to contact your network administrator before you assign a static IP address.

**Subnet mask:** Enter the subnet mask.

**Router:** Enter the IP address of the default router (gateway) used to connect devices that are attached to different networks and network segments.

**Hostname:** Enter the hostname.

**Search domains:** When you use a hostname that is not fully qualified, click **Add search domain** and enter a domain in which to search for the hostname used by the device.

**DNS servers:** Click **Add DNS server** and enter the IP address of the primary DNS server. This provides the translation of hostnames to IP addresses on your network.

##### IPv6

**Assign IPv6 automatically:** Select to let the network router assign an IP address to the device automatically.

#### HTTP and HTTPS

**Allow access through:** Select if a user is allowed to connect to the device through the HTTP, HTTPS, or both HTTP and HTTPS protocols.

HTTPS is a protocol that provides encryption for page requests from users and for the pages returned by the web server. The encrypted exchange of information is governed by the use of an HTTPS certificate, which guarantees the authenticity of the server.

To use HTTPS on the device, you must install an HTTPS certificate. Go to **System > Security** to create and install certificates.

##### Note

If you view encrypted web pages through HTTPS, you might experience a drop in performance, especially when you request a page for the first time.

**HTTP port:** Enter the HTTP port to use. Port 80 or any port in the range 1024–65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1–1023. If you use a port in this range, you get a warning.

**HTTPS port:** Enter the HTTPS port to use. Port 443 or any port in the range 1024–65535 are allowed. If you are logged in as an administrator, you can also enter any port in the range 1–1023. If you use a port in this range, you get a warning.

**Certificate:** Select a certificate to enable HTTPS for the device.

#### Friendly name

# AXIS D4100-E Network Strobe Siren

## The device interface

---

**Bonjour®:** Turn on to allow automatic discovery on the network.

**Bonjour name:** Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

**Use UPnP®:** Turn on to allow automatic discovery on the network.

**UPnP name:** Enter a friendly name to be visible on the network. The default name is the device name and MAC address.

### One-click cloud connection

One-click cloud connection (O3C) together with an O3C service provides easy and secure internet access to live and recorded video from any location. For more information, see [axis.com/end-to-end-solutions/hosted-services](http://axis.com/end-to-end-solutions/hosted-services).

#### Allow O3C:

- **One-click:** The default setting. Press and hold the control button on the device to connect to an O3C service over the internet. You need to register the device with the O3C service within 24 hours after you press the control button. Otherwise, the device disconnects from the O3C service. Once you have registered the device, **Always** is enabled and the device stays connected to the O3C service.
- **Always:** The device constantly attempts to connect to an O3C service over the internet. Once you have registered the device, it stays connected to the O3C service. Use this option if the control button on the device is out of reach.
- **No:** Disables the O3C service.

**Proxy settings:** If needed, enter the proxy settings to connect to the HTTP server.

**Host:** Enter the proxy server's address.

**Port:** Enter the port number used for access.

**Login and Password:** If needed, enter username and password for the proxy server.

#### Authentication method:

- **Basic:** This method is the most compatible authentication scheme for HTTP. It's less secure than the **Digest** method because it sends the username and password unencrypted to the server.
- **Digest:** This method is more secure because it always transfers the password encrypted across the network.
- **Auto:** This option lets the device select the authentication method depending on the supported methods. It prioritizes the **Digest** method over the **Basic** method.

**Owner authentication key (OAK):** Click **Get key** to fetch the owner authentication key. This is only possible if the device is connected to the internet without a firewall or proxy.

### SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices.

**SNMP:** Select the version of SNMP to use.

- **v1 and v2c:**
  - **Read community:** Enter the community name that has read-only access to all supported SNMP objects. The default value is **public**.
  - **Write community:** Enter the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is **write**.
  - **Activate traps:** Turn on to activate trap reporting. The device uses traps to send messages for important events or status changes to a management system. In the device interface, you can set up traps for SNMP v1 and v2c. Traps are automatically turned off if you change to SNMP v3 or turn off SNMP. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
  - **Trap address:** Enter the IP address or host name of the management server.
  - **Trap community:** Enter the community to use when the device sends a trap message to the management system.
  - **Traps:**
    - **Cold start:** Sends a trap message when the device starts.
    - **Warm start:** Sends a trap message when you change an SNMP setting.
    - **Link up:** Sends a trap message when a link changes from down to up.

# AXIS D4100-E Network Strobe Siren

## The device interface

### Note

- **Authentication failed:** Sends a trap message when an authentication attempt fails.

All Axis Video MIB traps are enabled when you turn on SNMP v1 and v2c traps. For more information, see *AXIS OS Portal > SNMP*.

- **v3:** SNMP v3 is a more secure version, which provides encryption and secure passwords. To use SNMP v3, we recommend you to activate HTTPS, as the password is then sent through HTTPS. This also prevents unauthorized parties to access unencrypted SNMP v1 and v2c traps. If you use SNMP v3, you can set up traps through the SNMP v3 management application.
  - **Password for the account "initial":** Enter the SNMP password for the account named "initial". Although the password can be sent without activating HTTPS, we don't recommend it. The SNMP v3 password can only be set once, and preferably only when HTTPS is enabled. Once the password is set, the password field is no longer displayed. To set the password again, you must reset the device to factory default settings.

### Connected clients

The list shows all clients that are connected to the device.

**Update:** Click to refresh the list.

## Security

### Certificates

Certificates are used to authenticate devices on a network. The device supports two types of certificates:

- **Client/server certificates**  
A client/server certificate validates the device's identity, and can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.
- **CA certificates**  
You can use a CA certificate to authenticate a peer certificate, for example to validate the identity of an authentication server when the device connects to a network protected by IEEE 802.1X. The device has several pre-installed CA certificates.

These formats are supported:

- Certificate formats: .PEM, .CER, and .PFX
- Private key formats: PKCS#1 and PKCS#12

### Important

If you reset the device to factory default, all certificates are deleted. Any pre-installed CA certificates are reinstalled.



Filter the certificates in the list.



**Add certificate** : Click to add a certificate.



The context menu contains:

- **Certificate information:** View an installed certificate's properties.
- **Delete certificate:** Delete the certificate.
- **Create certificate signing request:** Create a certificate signing request to send to a registration authority to apply for a digital identity certificate.

IEEE 802.1x

# AXIS D4100-E Network Strobe Siren

## The device interface

---

IEEE 802.1x is an IEEE standard for port-based network admission control providing secure authentication of wired and wireless network devices. IEEE 802.1x is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1x, network devices must authenticate themselves. The authentication is performed by an authentication server, typically a RADIUS server (for example FreeRADIUS and Microsoft Internet Authentication Server).

### Certificates

When configured without a CA certificate, server certificate validation is disabled and the device tries to authenticate itself regardless of what network it is connected to.

When using a certificate, in Axis' implementation, the device and the authentication server authenticate themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

To allow the device to access a network protected through certificates, a signed client certificate must be installed on the device.

**Client certificate:** Select a client certificate to use IEEE 802.1x. The authentication server uses the certificate to validate the client's identity.

**CA certificate:** Select a CA certificate to validate the authentication server's identity. When no certificate is selected, the device tries to authenticate itself regardless of what network it is connected to.

**EAP identity:** Enter the user identity associated with the client certificate.

**EAPOL version:** Select the EAPOL version that is used in the network switch.

**Use IEEE 802.1x:** Select to use the IEEE 802.1x protocol.

### Prevent brute-force attacks

**Blocking:** Turn on to block brute-force attacks. A brute-force attack uses trial-and-error to guess login info or encryption keys.

**Blocking period:** Enter the number of seconds to block a brute-force attack.

**Blocking conditions:** Enter the number of authentication failures allowed per second before the block starts. You can set the number of failures allowed both on page level and device level.

### IP address filter

**Use filter:** Select to filter which IP addresses that are allowed to access the device.

**Policy:** Choose whether to **Allow** access or **Deny** access for certain IP addresses.

**Addresses:** Enter the IP numbers that are either allowed or denied access to the device. You can also use the CIDR format.

### Custom-signed firmware certificate

To install test firmware or other custom firmware from Axis on the device, you need a custom-signed firmware certificate. The certificate verifies that the firmware is approved by both the device owner and Axis. The firmware can only run on a specific device which is identified by its unique serial number and chip ID. Custom-signed firmware certificates can only be created by Axis, since Axis holds the key to sign them.


Click **Install** to install the certificate. You need to install the certificate before you install the firmware.

# AXIS D4100-E Network Strobe Siren

## The device interface

---

### Users

 **Add user:** Click to add a new user. You can add up to 100 users.


**Username:** Enter a unique username.

**New password:** Enter a password for the user. Passwords must be 1 to 64 characters long. Only ASCII printable characters (code 32 to 126) are allowed in the password, for example letters, numbers, punctuation, and some symbols.

**Repeat password:** Enter the same password again.

**Role:**

- **Administrator:** Has full access to all settings. Administrators can also add, update, and remove other users.
- **Operator:** Has access to all settings except:
  - All **System** settings.
  - Adding apps.

 The context menu contains:

**Update user:** Edit the user's properties.

**Delete user:** Delete the user. You can't delete the root user.

### Anonymous users

**Allow anonymous viewers:** Turn on to allow anyone to access the device as a viewer without having to log in with a user account.

**Allow anonymous PTZ operators:** Turn on to allow anonymous users to pan, tilt, and zoom the image.


### Events

#### Rules

A rule defines the conditions that must be met for the product to perform an action. The list shows all the currently configured rules in the product.

**Note**

You can create up to 256 action rules.

 **Add a rule:** Click to create a rule.

**Name:** Enter a name for the rule.

**Wait between actions:** Enter the minimum time (hh:mm:ss) that must pass between rule activations. It is useful if the rule is activated by for example day-night mode conditions, to avoid that small light changes during sunrise and sunset activate the rule repeatedly.

**Condition:** Select a condition from the list. A condition must be met for the device to perform an action. If multiple conditions are defined, all of them must be met to trigger the action. For information about specific conditions, see *Get started with rules for events*.

**Use this condition as a trigger:** Select to make this first condition function only as a starting trigger. It means that once the rule is activated it remains active for as long as all the other conditions are met, no matter the state of the first condition. If you don't select this option, the rule will simply be active whenever all the conditions are met.

**Invert this condition:** Select if you want the condition to be the opposite of your selection.

# AXIS D4100-E Network Strobe Siren

## The device interface

---



**Add a condition:** Click to add an additional condition.

**Action:** Select an action from the list and enter its required information. For information about specific actions, see *Get started with rules for events*.

### Recipients

You can set up your device to notify recipients about events or send files. The list shows all the recipients currently configured in the product, along with information about their configuration.

#### Note

You can create up to 20 recipients.



**Add a recipient:** Click to add a recipient.

**Name:** Enter a name for the recipient.

**Type:** Select from the list:

- **FTP**
  - **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
  - **Port:** Enter the port number used by the FTP server. The default is 21.
  - **Folder:** Enter the path to the directory where you want to store files. If this directory doesn't already exist on the FTP server, you will get an error message when uploading files.
  - **Username:** Enter the username for the login.
  - **Password:** Enter the password for the login.
  - **Use temporary file name:** Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name, are correct.
  - **Use passive FTP:** Under normal circumstances the product simply requests the target FTP server to open the data connection. The device actively initiates both the FTP control and data connections to the target server. This is normally needed if there is a firewall between the device and the target FTP server.
- **HTTP**
  - **URL:** Enter the network address to the HTTP server and the script that will handle the request. For example: `http://192.168.254.10/cgi-bin/notify.cgi`.
  - **Username:** Enter the username for the login.
  - **Password:** Enter the password for the login.
  - **Proxy:** Turn on and enter the required information if a proxy server must be passed to connect to the HTTP server.
- **HTTPS**
  - **URL:** Enter the network address to the HTTPS server and the script that will handle the request. For example: `https://192.168.254.10/cgi-bin/notify.cgi`.
  - **Validate server certificate:** Select to validate the certificate that was created by HTTPS server.
  - **Username:** Enter the username for the login.
  - **Password:** Enter the password for the login.
  - **Proxy:** Turn on and enter the required information if a proxy server must be passed to connect to the HTTPS server.
- **Network storage**

You can add network storage such as a NAS (Network Attached Storage) and use it as a recipient to store files. The files are stored in the Matroska (MKV) file format.

  - **Host:** Enter the IP address or hostname for the network storage.
  - **Share:** Enter the name of the share on the host.
  - **Folder:** Enter the path to the directory where you want to store files.
  - **Username:** Enter the username for the login.
  - **Password:** Enter the password for the login.



# AXIS D4100-E Network Strobe Siren

## The device interface

- SFTP
  - **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
  - **Port:** Enter the port number used by the SFTP server. The default is 22.
  - **Folder:** Enter the path to the directory where you want to store files. If this directory doesn't already exist on the SFTP server, you will get an error message when uploading files.
  - **Username:** Enter the username for the login.
  - **Password:** Enter the password for the login.
  - **SSH host public key type (MD5):** Enter the fingerprint of the remote host's public key (a 32-digit hexadecimal string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
  - **SSH host public key type (SHA256):** Enter the fingerprint of the remote host's public key (a 43-digit Base64 encoded string). The SFTP client supports SFTP servers using SSH-2 with RSA, DSA, ECDSA, and ED25519 host key types. RSA is the preferred method during negotiation, followed by ECDSA, ED25519, and DSA. Make sure to enter the right MD5 host key that is used by your SFTP server. While the Axis device supports both MD5 and SHA-256 hash keys, we recommend using SHA-256 due to stronger security over MD5. For more information on how to configure an SFTP server with an Axis device, go to the *AXIS OS Portal*.
  - **Use temporary file name:** Select to upload files with temporary, automatically generated filenames. The files get renamed to the desired names when the upload completes. If the upload is aborted/interrupted, you don't get any corrupt files. However, you probably still get the temporary files. This way you know that all files that have the desired name, are correct.
- SIP
  - **From SIP account:** Select from the list.
  - **To SIP address:** Enter the SIP address.
- Email
  - **Send email to:** Enter the email address to send emails to. To enter multiple addresses, use commas to separate them.
  - **Send email from:** Enter the email address of the sending server.
  - **Username:** Enter the username for the mail server. Leave this field empty if the mail server does not require authentication.
  - **Password:** Enter the password for the mail server. Leave this field empty if the mail server does not require authentication.
  - **Email server (SMTP):** Enter the name of the SMTP server, for example smtp.gmail.com, smtp.mail.yahoo.com.
  - **Port:** Enter the port number for the SMTP server, using values in the range 0-65535. The default value is 587.
  - **Encryption:** To use encryption, select either SSL or TLS.
  - **Validate server certificate:** If you use encryption, select to validate the identity of the device. The certificate can be self-signed or issued by a Certificate Authority (CA).
  - **POP authentication:** Turn on to enter the name of the POP server, for example pop.gmail.com.

### Note

Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid your email account being locked or missing out on your expected emails.

- TCP
  - **Host:** Enter the server's IP address or hostname. If you enter a hostname, make sure that a DNS server is specified under **System > Network > IPv4 and IPv6**.
  - **Port:** Enter the port number used to access the server.

**Test:** Click to test the setup.



The context menu contains:

**View recipient:** Click to view all the recipient details.

**Copy recipient:** Click to copy a recipient. When you copy, you can make changes to the new recipient.

**Delete recipient:** Click to delete the recipient permanently.

# AXIS D4100-E Network Strobe Siren

## The device interface

---

### Schedules

Schedules and pulses can be used as conditions in rules. The list shows all the schedules and pulses currently configured in the product, along with information about their configuration.



Add schedule: Click to create a schedule or pulse.

### Manual trigger

The manual trigger is used to manually trigger a rule. The manual trigger can for example be used to validate actions during product installation and configuration.

### MQTT

MQTT (Message Queuing Telemetry Transport) is a standard messaging protocol for the Internet of Things (IoT). It was designed for simplified IoT integration and is used in a wide variety of industries to connect remote devices with a small code footprint and minimal network bandwidth. The MQTT client in Axis device firmware can simplify integration of data and events produced in the device to systems which are not video management systems (VMS).

Set up the device as an MQTT client. MQTT communication is based on two entities, the clients and the broker. The clients can send and receive messages. The broker is responsible for routing messages between clients.

You can learn more about MQTT in *AXIS OS Portal*.

### MQTT client

**Connect:** Turn on or off the MQTT client.

**Status:** Shows the current status of the MQTT client.

#### Broker

**Host:** Enter the hostname or IP address of the MQTT server.

**Protocol:** Select which protocol to use.

**Port:** Enter the port number.

- 1883 is the default value for **MQTT over TCP**
- 8883 is the default value for **MQTT over SSL**
- 80 is the default value for **MQTT over WebSocket**
- 443 is the default value for **MQTT over WebSocket Secure**

**Username:** Enter the username that the client will use to access the server.

**Password:** Enter a password for the username.

**Client ID:** Enter a client ID. The client identifier is sent to the server when the client connects to it.

**Clean session:** Controls the behavior at connection and disconnection time. When selected, the state information is discarded at connect and disconnect.

**Keep alive interval:** The keep alive interval enables the client to detect when the server is no longer available without having to wait for the long TCP/IP timeout.

**Timeout:** The time interval in seconds to allow a connect to complete. Default value: 60

**Device topic prefix:** Used in the default values for the topic in the connect message and LWT message on the **MQTT client** tab, and in the publication conditions on the **MQTT publication** tab.

**Reconnect automatically:** Specifies whether the client should reconnect automatically after a disconnect.

# AXIS D4100-E Network Strobe Siren

## The device interface

---

### Connect message

Specifies if a message should be sent out when a connection is established.

**Send message:** Turn on to send messages.

**Use default:** Turn off to enter your own default message.

**Topic:** Enter the topic for the default message.

**Payload:** Enter the content for the default message.

**Retain:** Select to keep the state of client on this Topic

**QoS:** Change the QoS layer for the packet flow.

### Last Will and Testament message

The Last Will Testament (LWT) lets a client provide a testament along with its credentials when connecting to the broker. If the client disconnects ungracefully at some point later (maybe because his power source died), it can let the broker deliver a message to other clients. This LWT message has the same form as an ordinary message and gets routed via the same mechanics.

**Send message:** Turn on to send messages.

**Use default:** Turn off to enter your own default message.

**Topic:** Enter the topic for the default message.

**Payload:** Enter the content for the default message.

**Retain:** Select to keep the state of client on this Topic

**QoS:** Change the QoS layer for the packet flow.

### MQTT publication

**Use default condition prefix:** Select to use the default condition prefix, that is defined using the device topic prefix in the MQTT client tab.

**Include condition name:** Select to include the topics that describe the condition in the MQTT topic.

**Include condition namespaces:** Select to include ONVIF topic namespaces in the MQTT topic.

**Include serial number:** Select to include the device's serial number in the MQTT payload.



**Add condition:** Click to add a condition.

**Retain:** Defines which MQTT messages are sent as retained.

- **None:** Send all messages as non-retained.
- **Property:** Send only stateful messages as retained.
- **All:** Send both stateful and stateless messages as retained.

**QoS:** Select the desired level for the MQTT publication.

### MQTT subscriptions

# AXIS D4100-E Network Strobe Siren

## The device interface

---



**Add subscription:** Click to add a new MQTT subscription.

**Subscription filter:** Enter the MQTT topic that you want to subscribe to.

**Use device topic prefix:** Add the subscription filter as prefix to the MQTT topic.

**Subscription type:**

- **Stateless:** Select to convert MQTT messages into a stateless message.
- **Stateful:** Select to convert MQTT messages into a condition. The payload is used as the state.

**QoS:** Select the desired level for the MQTT subscription.

## SIP

### SIP settings

Session Initiation Protocol (SIP) is used for interactive communication sessions between users. The sessions can include audio and video.

**Enable SIP:** Check this option to make it possible to initiate and receive SIP calls.

**Allow incoming calls:** Check this option to allow incoming calls from other SIP devices.

#### Call handling

- **Call timeout:** Set the maximum time a call can last before it ends if there is no answer (max 10 min).
- **Incoming call duration:** Set the maximum time an incoming call can last (max 10 min).
- **End calls after:** Set the maximum time that a call can last (max 60 min). Select **Infinite call duration** if you don't want to limit the length of a call.

#### Ports

A port number must be between 1024 and 65535.

- **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:** The network port used for the first RTP media stream in a SIP call. The default start port number is 4000. Some firewalls block RTP traffic on certain port numbers.

#### NAT traversal

Use NAT (Network Address Translation) traversal when the device is located on an private network (LAN) and you want to make it available from outside of that network.

#### Note

For NAT traversal to work, the router must support it. The router must also support 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 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 the TURN server address and the login information.

#### Audio

# AXIS D4100-E Network Strobe Siren

## The device interface

- **Audio codec priority:** Select at least one audio codec with the desired audio quality for SIP calls. Drag-and-drop to change the priority.

### Note

The selected codecs must match the call recipient codec, since the recipient codec is decisive when a call is made.

- **Audio direction:** Select allowed audio directions.

### Additional

- **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.

## SIP accounts

All current SIP accounts are listed under **SIP accounts**. For registered accounts, the colored circle lets you know the status.


- The account is successfully registered with the SIP server.
- There is a problem with the account. Possible reasons can be authorization failure, that the account credentials are wrong, or that the SIP server can't find the account.

The **peer to peer (default)** account is an automatically created account. You can delete it if you create at least one other account and set that account as default. The default account is always used when a VAPIX® Application Programming Interface (API) call is made without specifying which SIP account to call from.



**Account:** Click to create a new SIP account.

- **Active:** Select to be able to use the account.
- **Make default:** Select to make this the default account. There must be a default account, and there can only be one default account.
- **Name:** Enter a descriptive name. This can, for example, be a first and last name, a role, or a location. The name is not unique.
- **User ID:** Enter the unique extension or phone number assigned to the device.
- **Peer-to-peer:** Use for direct calls to another SIP device on the local network.
- **Registered:** Use for calls to SIP devices outside the local network, through a SIP server.
- **Domain:** If available, enter the public domain name. It will be shown as part of the SIP address when calling other accounts.
- **Password:** Enter the password associated with the SIP account for authenticating against the SIP server.
- **Authentication ID:** Enter the authentication ID used for authenticating against the SIP server. If it is the same as the user ID, you don't need to enter the authentication ID.
- **Caller ID:** The name which is presented to the recipient of calls from the device.
- **Registrar:** Enter the IP address for the registrar.
- **Transport mode:** Select the SIP transport mode for the account: UPD, TCP, or TLS. When you select TLS, you get the option to use media encryption.
- **Media encryption (only with transport mode TLS):** Select the type of encryption for media (audio and video) in SIP calls.
- **Certificate (only with transport mode TLS):** Select a certificate.
- **Verify server certificate (only with transport mode TLS):** Check to verify the server certificate.
- **Secondary SIP server:** Turn on if you want the device to try to register on a secondary SIP server if registration on the primary SIP server fails.
- **Answer automatically:** Select to automatically answer an incoming call.
- **SIP secure:** Select to use Secure Session Initiation Protocol (SIPS). SIPS uses the TLS transport mode to encrypt traffic.
- **Proxies**

-  **Proxy:** Click to add a proxy.


# AXIS D4100-E Network Strobe Siren

## The device interface

- **Prioritize:** If you have added two or more proxies, click to prioritize them.
- **Server address:** Enter the IP address of the SIP proxy server.
- **Username:** If required, enter the username for the SIP proxy server.
- **Password:** If required, enter the password for the SIP proxy server.
- **Video** ⓘ
  - **View area:** Select the view area to use for video calls. If you select none, the native view is used.
  - **Resolution:** Select the resolution to use for video calls. The resolution affects the required bandwidth.
  - **Frame rate:** Select the number of frames per second for video calls. The frame rate affects the required bandwidth.
- **DTMF**
  - **Use RTP (RFC2833):** Select to allow dual-tone multifrequency (DTMF) signaling, other tone signals and telephony events in RTP packets.
  - **Use SIP INFO (RFC2976):** Select to include the INFO method to the SIP protocol. The INFO method adds optional application layer information, generally related to the session.
  - **+ DTMF sequence:** Click to add an action rule triggered by touch-tone. You must activate the action rule in the Events tab.
  - **Sequence:** Enter the characters to trigger the action rule. Allowed characters: 0-9, A-D, #, and \*.
  - **Description:** Enter a description of the action to be triggered.

### SIP test call

**SIP account:** Select which account to make the test call from.

**SIP address:** Enter a SIP address and click  to make a test call and verify that the account works.

### Accessories



#### I/O ports



Use digital input to connect external devices that can toggle between an open and closed circuit, for example PIR sensors, door or window contacts, and glass break detectors.

Use digital output to connect external devices such as relays and LEDs. You can activate connected devices through the VAPIX® Application Programming Interface or in the device interface.

#### Port

**Name:** Edit the text to rename the port.

**Direction:**  indicates that the port is an input port.  indicates that it's an output port. If the port is configurable, you can click the icons to change between input and output.

**Normal state:** Click  open circuit, and  for closed circuit.

**Current state:** Shows the current state of the port. The input or output is activated when the current state is different from the normal state. An input on the device has an open circuit when it's disconnected or when there is a voltage above 1 V DC.

#### Note

During restart the output circuit is open. When the restart is complete, the circuit goes back to the normal position. If you change any settings on this page, the output circuits go back to their normal positions regardless of any active triggers.

**Supervised** ⓘ : Turn on to make it possible to detect and trigger actions if someone tampers with the connection to digital I/O devices. In addition to detecting if an input is open or closed, you can also detect if someone has tampered with it (that is, cut or shorted). To supervise the connection requires additional hardware (end-of-line resistors) in the external I/O loop.

# AXIS D4100-E Network Strobe Siren

## The device interface

---

### Logs

#### Reports and logs

##### Reports

- **View the device server report:** Click to show information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.
- **Download the device server report:** Click to download the server report. It creates a .zip file that contains a complete server report text file in UTF-8 format, as well as a snapshot of the current live view image. Always include the server report .zip file when you contact support.
- **Download the crash report:** Click to download an archive with detailed information about the server's status. The crash report contains information that is in the server report as well as detailed debug information. This report might contain sensitive information such as network traces. It can take several minutes to generate the report.

##### Logs

- **View the system log:** Click to show information about system events such as device startup, warnings and critical messages.
- **View the access log:** Click to show all failed attempts to access the device, for example when a wrong login password is used.

#### Network trace

##### Important

A network trace file might contain sensitive information, for example certificates or passwords.

A network trace file can help you troubleshoot problems by recording activity on the network. Select the duration of the trace in seconds or minutes, and click **Download**.

#### Remote system log

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, which indicates the software type generating the message, and assigned a severity level.



**Server:** Click to add a new server.

**Host:** Enter the hostname or IP address of the server.

**Format:** Select which syslog message format to use.

- RFC 3164
- RFC 5424

**Protocol:** Select the protocol and port to use:

- UDP (Default port is 514)
- TCP (Default port is 601)
- TLS (Default port is 6514)

**Severity:** Select which messages to send when triggered.

**CA certificate set:** See the current settings or add a certificate.

#### Plain config

Plain config is for advanced users with experience of Axis device configuration. Most parameters can be set and edited from this page.

# AXIS D4100-E Network Strobe Siren

## The device interface

---

### Maintenance

**Restart:** Restart the device. This does not affect any of the current settings. Running applications restart automatically.

**Restore:** Return *most* settings to the factory default values. Afterwards you must reconfigure the device and apps, reinstall any apps that didn't come preinstalled, and recreate any events and PTZ presets.

#### Important

The only settings saved after restore are:

- Boot protocol (DHCP or static)
- Static IP address
- Default router
- Subnet mask
- 802.1X settings
- O3C settings

**Factory default:** Return *all* settings to the factory default values. Afterwards you must reset the IP address to make the device accessible.

#### Note

All Axis device firmware is digitally signed to ensure that you only install verified firmware on your device. This further increases the overall minimum cybersecurity level of Axis devices. For more information, see the white paper "Signed firmware, secure boot, and security of private keys" at [axis.com](http://axis.com).

**Firmware upgrade:** Upgrade to a new firmware version. New firmware releases can contain improved functionality, bug fixes, and completely new features. We recommend you to always use the latest release. To download the latest release, go to [axis.com/support](http://axis.com/support).

When you upgrade, you can choose between three options:

- **Standard upgrade:** Upgrade to the new firmware version.
- **Factory default:** Upgrade and return all settings to the factory default values. When you choose this option, you can't revert to the previous firmware version after the upgrade.
- **Autorollback:** Upgrade and confirm the upgrade within the set time. If you don't confirm, the device reverts to the previous firmware version.

**Firmware rollback:** Revert to the previously installed firmware version.

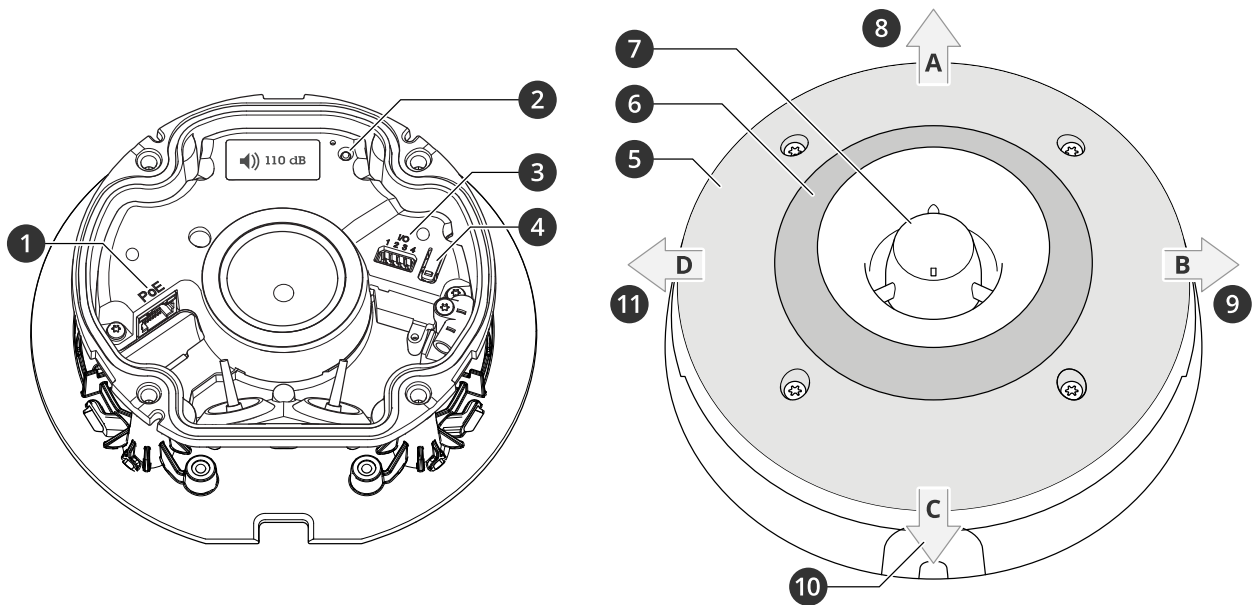


# AXIS D4100-E Network Strobe Siren

## Specifications

### 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 38.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and hold the button for about 3 seconds until the status LED flashes green.

# AXIS D4100-E Network Strobe Siren

## Specifications

### Connectors

#### Network connector

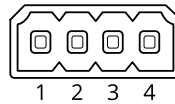
RJ45 Ethernet connector with Power over Ethernet (PoE).

#### 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.

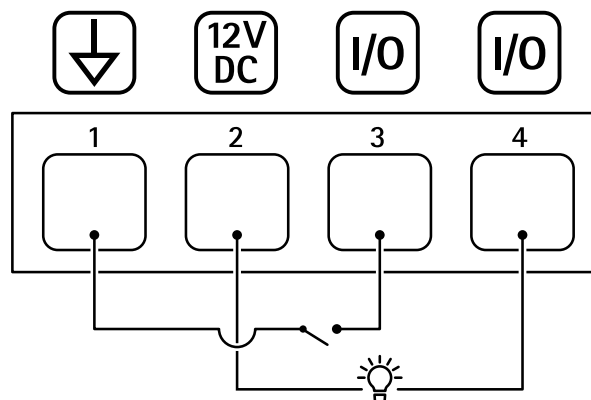
**Digital output** – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface, through an event or from the product's webpage.

4-pin terminal block



Function	Pin	Notes	Specifications
DC ground	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 V DC 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 V DC
		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 V DC, 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

# AXIS D4100-E Network Strobe Siren

## Specifications

---

### 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

### Maximum sound pressure levels

Sound pattern name	Sound pressure levels (dB)
	1
Alarm: Alarm high pitch	111
Alarm: Alarm low pitch	108
Alarm: Bird	112
Alarm: Boat horn	91
Alarm: Car alarm fast	107
Alarm: Car alarm slow	110
Alarm: Classic clock	96
Alarm: First attender	98
Alarm: Horror	109

# AXIS D4100-E Network Strobe Siren

## Specifications

---

Alarm: Industrial	103
Alarm: Single beep	98
Alarm: Soft quad beep	100
Alarm: Soft triple beep	103
Alarm: Triple high pitch	112
Notification: Accepted	83
Notification: Calling	92
Notification: Denied	89
Notification: Done	92
Notification: Entry	96
Notification: Failed	97
Notification: Hurry	88
Notification: Message	96
Notification: Next	85
Notification: Open	100
Siren: Alternate	110
Siren: Bouncy	112
Siren: Evac	102
Siren: Falling pitch	112
Siren: Home soft	111

1. Wall mounted at a distance of 1 meter on axis at volume setting 5.

# AXIS D4100-E Network Strobe Siren

## Cleaning recommendations

---

### Cleaning recommendations

If the device gets grease stains or becomes heavily soiled, you can clean it with mild, solvent-free soap or detergent.

**NOTICE**

Never use harsh detergent, for example gasoline, benzene, or acetone.

1. Use a can of compressed air to remove any dust or loose dirt from the device.
2. Clean the device with a soft cloth dampened with mild detergent and lukewarm water.
3. Wipe carefully with a dry cloth.

**Note**

Avoid cleaning in direct sunlight or at elevated temperatures, as this may cause stains when the water droplets dry.

# AXIS D4100-E Network Strobe Siren

## Troubleshooting

---

### 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 33*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90.
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.

The installation and management software tools are available from the support pages on [axis.com/support](https://axis.com/support).

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

#### Firmware options

Axis offers product firmware 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 firmware 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 product firmware strategy, go to [axis.com/support/firmware](https://axis.com/support/firmware).

#### Check the current firmware version

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

To check the current firmware:

1. Go to the device interface > **Status**.
2. See the firmware version under **Device info**.

#### Upgrade the firmware

##### Important

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

##### Important

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

# AXIS D4100-E Network Strobe Siren

## Troubleshooting

---

### Note

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

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

When the upgrade has finished, the product restarts automatically.

## Technical issues, clues, and solutions

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

### Problems upgrading the firmware

---

Firmware upgrade failure	If the firmware upgrade fails, the device reloads the previous firmware. The most common reason is that the wrong firmware file has been uploaded. Check that the name of the firmware file corresponds to your device and try again.
Problems after firmware upgrade	If you experience problems after a firmware upgrade, roll back to the previously installed version from the <b>Maintenance</b> 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 <code>ping</code> and the IP address of the device): <ul style="list-style-type: none"><li>• If you receive: <code>Reply from &lt;IP address&gt;: bytes=32; time=10...</code> this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device.</li><li>• If you receive: <code>Request timed out</code>, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.</li></ul>
Possible IP 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 <code>http</code> or <code>https</code> in the browser's address field.  If the password for the user <code>root</code> is lost, the device must be reset to the factory default settings. See <i>Reset to factory default settings on page 38</i> .
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 <b>AXIS IP Utility</b> or <b>AXIS Device Manager</b> 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, a static IP address can be assigned manually. For instructions, go to <a href="https://axis.com/support">axis.com/support</a> .
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 <b>System &gt; Date and time</b> .

# AXIS D4100-E Network Strobe Siren

## Troubleshooting

---

### The device is accessible locally but not externally

---

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

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

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

### 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 following factors are important to consider:

- Heavy network utilization due to poor infrastructure affects the bandwidth.
- For maximum light output, a PoE Class 4 power source is required.
- The light output can be reduced if the device is soiled, or at high ambient temperatures.
- In bright environments such as in direct sunlight, consider using the sunshield accessory to improve visibility.
- The sound output can be reduced if the siren is blocked or if the device is not correctly closed.
- The installation environment can affect the sound output. The sound volume can be higher if the device is installed on a wall or in an enclosed space, and lower if installed on a pole in an open space.

## Contact support

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



