AXIS TP3604-E Cellular Back Box

User manual

Table of Contents

Installation

The video shows how to install the AXIS TP3604-E Cellular Back Box with AXIS P32 Dome Camera Series and AXIS P14 Bullet Camera Series.

For instructions that cover all installation scenarios as well as safety information, see the installation guide.

Get started

Find the device on the network

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

Browser support

You can use the device with the following browsers:

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

✓: Recommended

*: Supported with limitations

Open the device's web interface

1. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account, on page 4*.

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 4*.
3. Re-enter the password.
4. Accept the license agreement.
5. Click **Add account**.

Secure passwords

Important

Use HTTPS (which is enabled by default) to set your password or other sensitive configurations over the network. HTTPS enables secure and encrypted network connections, thereby protecting sensitive data, such as passwords.

The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

To protect your data we strongly recommend that you:

- Use a password with at least 8 characters, preferably created by a password generator.
- Don't expose the password.

- Change the password at a recurring interval, at least once a year.

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. Configure and install the device.

Configure your device

To configure your device, you need to go through the following steps:

1. *SIM management, on page 6*
2. If your network requires an explicit Access Point Name (APN), *Set APN, on page 6*
3. *Validate the signal strength and IP address, on page 6*
4. *Test the connectivity, on page 6*
5. *Check management ports, on page 6*
6. *Turn on forwarding to the camera, on page 6*

SIM management

SIM management is mandatory when the SIM PIN is enabled. If SIM PIN is disabled you can skip this step.

1. Insert the SIM card. Go to **Modem > SIM management > SIM status** to verify the modem/SIM detection.
2. If SIM PIN is locked, go to **Modem > SIM management > SIM PIN > Unlock** to unlock it with the correct PIN.

Set APN

Note

You only need to perform this step if your network requires an explicit APN (Access Point Name).

To set an explicit APN, go to **Modem > Cellular network > APN**.

Validate the signal strength and IP address

Note

This step requires access to the cellular network.

1. Check the signal strength in **System > Modem > Cellular network > Radio parameters > Signal strength index**. Three to four bars indicates a good signal quality.
2. In **System > Modem > Cellular network > User equipment IP address**, confirm that a cellular network IP address is received.

Test the connectivity

Note

This step requires access to the cellular network.

1. Go to **System > Modem > Cellular network > Test cellular connection**. Enter a hostname or an IP address.
2. Verify that the connection test is successful.

Check management ports

Before you turn on the final routing mode, verify the back box management ports.

1. Go to **Cellular routing > Back box management ports**.
2. Change any ports if the default values are not supported by the network.

Turn on forwarding to the camera

The final step is to turn on the forwarding to the camera.

1. Go to **Cellular routing > Main mode** and click **Enable forwarding to connected device**.

Once the forwarding is enabled, the normal service ports are forwarded to the camera, and the back box management remains available through the reserved management ports.

2. Test the access to the camera: In a web browser, enter the cellular IP address followed by the port number 80, `http://<cellular-ip-address>:80`.
3. Test the access to the back box: In a web browser, enter the cellular IP address followed by the port number 11080 (the default back box management port for HTTP), `http://<cellular-ip-address>:11080`.

Configure the IP ownership of the camera

Note

This step is optional and only required if you need to change from the default subnet behavior or tune the subnet behavior.

A cellular network hands out only a single IP address, and that IP is tied to the identity of the SIM card. A normal installation involves a back box and a connected camera. The DHCP mode decides which IP the camera gets to "own". This is the key decision behind choosing a DHCP server mode.

By default (Local mode), the cellular IP stays with the back box and the camera is assigned a private IP from the back box's local network. The camera is still fully reachable from the cellular network. For most deployments this is all that is needed and it keeps the camera safely isolated on a private network.

The difference becomes visible when a tool looks at the IP from the camera's own perspective. If a VMS reads the IP address reported by the camera, or if the camera is configured to burn its IP address into a video overlay, that IP will be the camera's private LAN IP, not the public cellular IP that the outside world uses to reach it. The two addresses don't match, because the cellular IP belongs to the SIM card identity held by the back box, not the camera.

Passthrough mode solves this by taking the single IP that the cellular network assigns to the back box and forwarding it to the camera. With Passthrough enabled, the camera owns the exact same IP that belongs to the cellular network, so the address the camera reports (and shows in a video overlay) is the same address used to reach it remotely. Because the camera now holds the cellular identity, this choice also changes how the camera can reach other user equipment (UEs) on the cellular network.

The rest of this section describes each mode in detail.

You can reach the camera that is connected to the back box over the cellular IP on the standard ports (`80/443/554/22`) and you can still reach the back box on the reserved management ports, (for example `11080/11443/11554/11022`).

The difference between Local and Passthrough mode:

Local mode

- The camera is assigned a private local subnet.
- The camera's internal IP address is different from the cellular reachable IP address.
- If you're in doubt, use the Local DHCP mode option.

Passthrough mode

- The camera is assigned the cellular IP address.

Local mode

Turn on Local mode

1. In **Cellular routing > Advanced DHCP configuration > DHCP server mode**, select **Local**.
2. Verify that the camera's local IP address doesn't conflict with any other reachable IP address in the network: **Cellular routing > Advanced DHCP configuration > Local private network configuration**

3. If needed, change the IP address in **Cellular routing > Advanced DHCP configuration > Local private network configuration**. Use the same value for **Starting IP address** and **Ending IP address**.
4. Click **Save**.

Passthrough mode

If UEs (User Equipment, i.e. cameras) doesn't communicate with each other, and traffic always comes from another VMS LAN toward the UEs, there is no UE-to-UE path for IP shadowing. In that case, Passthrough is considered safe from an IP shadowing perspective.

On a high level, this means that the cellular network is extended toward the camera side. This is useful when the camera should appear directly on the cellular-facing IP address.

Important risk: IP shadowing in Passthrough

This risk description applies to single-camera setups. Even with one camera, Passthrough still needs two IP addresses on the LAN-side subnet:

- One IP address for the camera.
- One IP for the back box DHCP server on the Ethernet side.

Scenario 1: Minimal subnet per UE `(/30)`

In this model, each UE has a small, separate subnet.

- A `(/30)` provides two usable host IP addresses.
- One IP address is used by the camera.

The spare IP is used internally by the back box DHCP server.

Recommendation for scenario 1:

- Keep each UE subnet separate.
- Make sure every UE subnet is unique. Don't let subnets overlap across UEs.

Scenario 2: Larger shared subnet with many UEs

Some deployments use one larger subnet shared by multiple UEs. Shadowing risk appears if the camera tries to reach another UE that uses the same IP as the back box DHCP server IP. In that case, traffic may resolve to the local back box-side address instead of the intended remote UE.

Recommendation for Scenario 2:

- Check the back box DHCP server IP address in the passthrough settings.
- Make sure that this IP address is not assigned to any other UE.
- Make sure that this IP address is not assigned to any SIM in the network service portal.

Turn on Passthrough mode

Note

Access to a cellular network is required.

1. In **Cellular routing > Advanced DHCP configuration > DHCP server mode** , select **Passthrough**.
2. In **Cellular routing > Advanced DHCP configuration > Local private network configuration > Server IP and prefix length**, validate that the automatically selected server IP and subnet prefix length doesn't conflict with other reachable IP addresses.
3. Click **Save**.

Set up rules for events

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

Trigger an action

1. Go to **System** > **Events** and click **+ 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.

Trigger a notification when the enclosure is opened

This example explains how to set up an email notification when the housing or casing of the device is opened.

Add an email recipient:

1. Go to **System > Events > Recipients** and click **Add recipient**.
2. Type a name for the recipient.
3. Select **Email** as the notification type.
4. Type the recipient's email address.
5. Type the email address that you want the camera to send notifications from.
6. Provide the login details for the sending email account, along with the SMTP hostname and port number.
7. To test your email setup, click **Test**.
8. Click **Save**.

Create a rule:

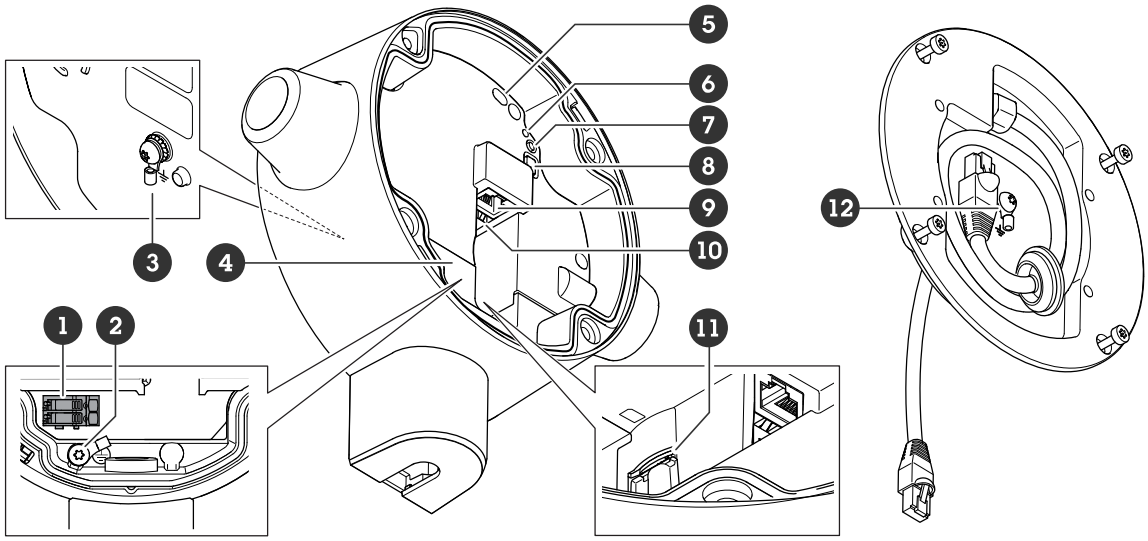
9. Go to **System > Events > Rules** and click **Add a rule**.
10. Type a name for the rule.
11. In the list of conditions, select **Casing open**.
12. In the list of actions, select **Send notification to email**.
13. Select a recipient from the list.
14. Type a subject line and message for the email.
15. 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 *AC connector*
2 *Protective grounding*
3 *Ground screw*
4 *Protective cover (AC)*
5 *Case open detector*
6 *Reset button*
7 *Status LED*
8 *Control button*
9 *PoE out (data)*
10 *PoE in*
11 *SIM card slot*
12 *Ground screw (camera)*

LED indicators

Status LED in setup mode

Status LED	Indication
Unlit	The casing detection IR is covered.
Green	Normal operation, the Ethernet interface is ready.
Amber	Steady during startup. Flashes during device software upgrade or reset to factory default.
Amber/Red	No Ethernet connection and the modem is being configured during startup.
Red	Device software upgrade failure.

Status LED in connected mode

Status LED	Indication
Unlit	The casing detection IR is covered.
Green	The modem is ready.
Amber	Steady during startup. Flashes during device software upgrade or reset to factory default.

Amber/Red	The modem is being configured during start up.
Red	Device software upgrade failure.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 14*.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and release the button, then wait for the status LED to flash green three times.

Connectors

PoE input connector (PoE in)

RJ45 Ethernet connector with Power over Ethernet (PoE) IEEE 802.3af/802.3at/802.3bt Type 3 Class 5.

Note

This connector is only used for power input, no network connection is available.

Note

- AC input is required for PoE IEEE 802.3at Type 2 Class 4 output.
- For PoE IEEE 802.3af Type 1 Class 3 output, IEEE 802.3at Type 2 Class 4 or higher is required.
- For PoE IEEE 802.3af Type 1 Class 3 input, the device is operational but does not output power.

Note

Maximum Ethernet cable length is 20 m.

Network connector (PoE out)

RJ45 Ethernet connector.

Note

- AC input is required for PoE IEEE 802.3at Type 2 Class 4 output.
- For PoE IEEE 802.3af Type 1 Class 3 output, IEEE 802.3at Type 2 Class 4 or higher is required.
- For PoE IEEE 802.3af Type 1 Class 3 input, the device is operational but does not output power.

Note

Maximum Ethernet cable length is 20 m.

Power connector

Terminal block for connecting AC power.

Note

AC input is required for PoE IEEE 802.3at Type 2 Class 4 output.

Clean your device

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

NOTICE

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

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

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

Troubleshooting

Reset to factory default settings

Important

Reset to factory default should be used with caution. A reset to factory default resets all settings, including the IP address, to the factory default values.

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See *Product overview, on page 11*.
3. Keep the control button pressed for 15–30 seconds until the status LED indicator flashes amber.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
   - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Use the installation and management software tools to assign an IP address, set the password, and access the device.
   The installation and management software tools are available from the support pages on *axis.com/support*.

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

AXIS OS options

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

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

Check the current AXIS OS version

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

To check the current AXIS OS version:

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

Upgrade AXIS OS

Important

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

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

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

Note

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

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

When the upgrade has finished, the product restarts automatically.

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

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

Problems after AXIS OS upgrade

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

Problems setting the IP address

Can't set the IP address

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

Problems accessing the device

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

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

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 14*.

The IP address has been changed by DHCP

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

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

Certificate error when using IEEE 802.1X

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

The browser isn't supported

For a list of recommended browsers, see *Browser support, on page 4*.

Can't access the device externally

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

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

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

Problems with MQTT

Can't connect over port 8883 with MQTT over SSL

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

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

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

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

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.

T10233346

2026-08 (M1.16)