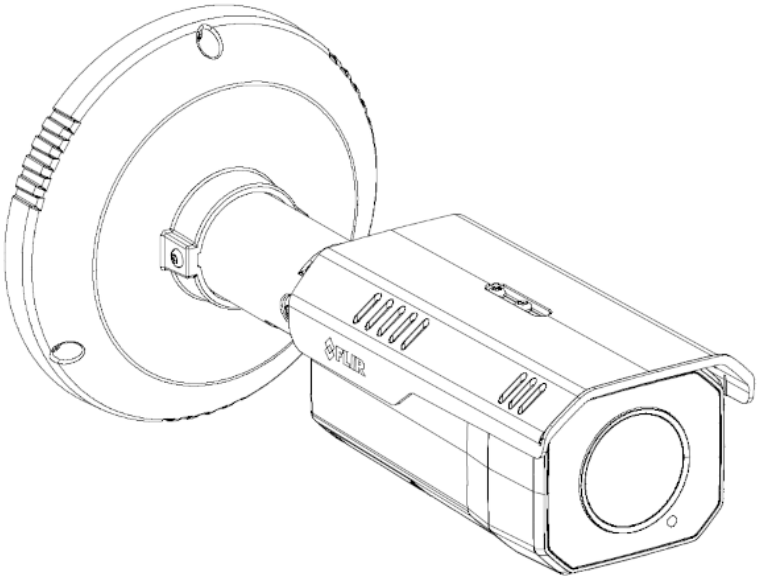
Quasar™ Premium Bullet Camera with FLIR Edge AI Video Analytics

Installation and User Guide



For additional information visit www.flir.com or write to:

Teledyne FLIR LLC
Antennvägen 6
PO Box 7376, SE-187
15 Täby
Stockholm County, 187 66
Sweden

Support: https://support.flir.com/

Important Instructions and Notices to the User:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modification of this device without the express authorization of Teledyne FLIR LLC may void the user's authority under FCC rules to operate this device.

Proper Disposal of Electrical and Electronic Equipment (EEE)

The European Union (EU) has enacted Waste Electrical and Electronic Equipment Directive 2012/19/EU (WEEE), which aims to prevent EEE waste from arising; to encourage reuse, recycling, and recovery of EEE waste; and to promote environmental responsibility.

In accordance with these regulations, all EEE products labeled with the "crossed out wheeled bin" either on the product itself or in the product literature must not be disposed of in regular rubbish bins, mixed with regular household or other commercial waste, or by other regular municipal waste collection means. Instead, and in order to prevent possible harm to the environment or human health, all EEE products (including any cables that came with the product) should be responsibly discarded or recycled.

To identify a responsible disposal method nearby, please contact the local waste collection or recycling service, the original place of purchase or product supplier, or the responsible government authority in the area. Business users should contact their supplier or refer to their purchase contract.

Document History

Revision	Date	Comment
100	December 2024	Initial Teledyne FLIR release

Product Registration and Warranty Information

Register your Product with Teledyne FLIR at https://customer.flir.com.

For warranty information, see https://www.teledyneflir.com/support-center/warranty/security/flir-security-product-warranties/.

Table of Contents

Table of Contents

1 Document Scope and Purpose

This document provides installation, operation, and configuration instructions for Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics (CB-650x).

Note
This document is intended for use by technical users who have a basic understanding of CCTV camera/video equipment and LAN/WAN network connections.

Warning
Installation must follow safety, standards, and electrical codes as well as the laws that apply where the units are being installed.

Disclaimer

Users of Teledyne FLIR products accept full responsibility for ensuring the suitability and considering the role of the product detection capabilities and their limitation as they apply to their unique site requirements.

Teledyne FLIR LLC and its agents make no guarantees or warranties to the suitability for the users' intended use. Teledyne FLIR LLC accepts no responsibility for improper use or incomplete security and safety measures.

Failure in part or in whole of the installer, owner, or user in any way to follow the prescribed procedures or to heed WARNINGS and CAUTIONS shall absolve Teledyne FLIR and its agents from any resulting liability.

Specifications and information in this guide are subject to change without notice.

Caution
- The unit's cover is an essential part of the product. Do not open or remove it.
- Never operate the unit without the cover in place. Operating the unit without the cover poses a risk of fire and shock hazards.
- Do not disassemble the unit or remove screws. There are no user serviceable parts inside the unit.
- Only qualified trained personnel should service and repair this equipment.
- Observe local codes and laws and ensure that installation and operation are in accordance with fire, security and safety standards.

A **Warning** is a precautionary message that indicates a procedure or condition where there are potential hazards of personal injury or death.

A **Caution** is a precautionary message that indicates a procedure or condition where there are potential hazards of permanent damage to the equipment and or loss of data.

A **Note** is useful information to prevent problems, help with successful installation, or to provide additional understanding of the products and installation.

A **Tip** is information and best practices that are useful or provide some benefit for installation and use of Teledyne FLIR products.

2 Camera Overview

Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics (CB-650x) provide 4K UHD (CB-6508) or 5MP (CB-6505) real-time video, up to 25 / 30 frames per second (fps). They feature Shutter (True) Wide Dynamic Range up to 130db; line-level audio in/out; and digital I/O. The camera features built-in artificial intelligence (AI)-optimized video analytics (VA) with deep neural network (DNN) technology that accurately detect and classify human and vehicle threats moving at high or low speeds, minimizing false alarms and daily operations costs. You can pair one or more Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics with a FLIR Security PTZ camera that supports geotracking.

When the camera is connected to an IP network, it functions as a server, providing services such as camera control, video streaming, and network communications. The camera supports up to three simultaneous video streams using H.265, H.264, or MJPEG compression, providing an ideal solution when differing levels of image quality are required. The camera can increase frame rate and level of detail when events are triggered. In addition, FLIR's adaptive streaming algorithms provide the highest image quality with the lowest bandwidth and storage requirements.

If help is needed during the installation process, contact the local Teledyne FLIR service representative or call the Support number that appears on the product's page at https://www.flir.com/support/. All installers and integrators are encouraged to take advantage of the training offered by Teledyne FLIR; visit https://www.flir.com/support-center/training/ for more information.

For safety, and to achieve the highest levels of performance from the camera system, always follow the warnings and cautions in this manual when handling and operating the camera.

Related Documentation

- *Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics Quick Install Guide*
- *FLIR Security Edge Devices Accessory Guide*
- *FLIR Security PTZ Pairing Configuration Guide*
- *DNA User Guide*

2.1 Features

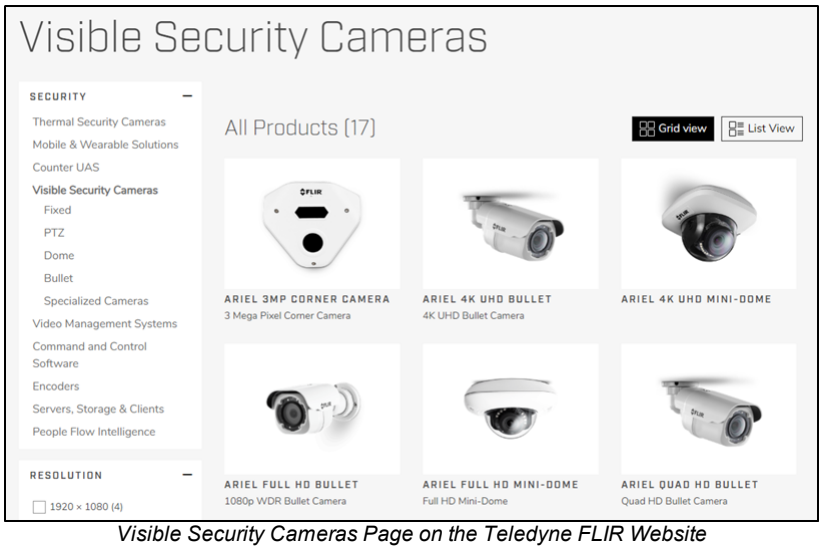
- CB-6508 models feature a 1 / 1.8" progressive CMOS sensor and up to 4K (3840 x 2160) resolution at 25 / 30fps
- CB-6505 models features a 1 / 2.8" progressive sensor and up to 5MP (2592 x 1944) resolution at 25 / 30fps
- 3DNR image noise reduction
- Configurable white balance
- Backlight compensation
- Audio line-in / line-out
- Built-in web server supports the latest version of Google Chrome® and other popular web browsers
- up to 20 users
- microSD card slot supports cards up to 1 TB
- Shutter (True) WDR
- ONVIF© Profile S / G / T
- 802.1X and SSL / TLS security protocols
- H.265, H.264, and MJPEG compression
- Alarm in / out
- Onboard VA event-driven alarms for:
  - Tripwires
  - Intrusion Detection
  - Loitering Detection
- Up to eight VA masking regions
- Powered by IEEE 802.3at, class 0 PoE; 24V AC; or 12V DC

2.2 Accessing Product Information from the Teledyne FLIR Website

Up-to-date resources for the camera, including the camera's specifications, the Teledyne FLIR Discovery Network Assistant (DNA) software tool, and this guide, are available on the Teledyne FLIR website.

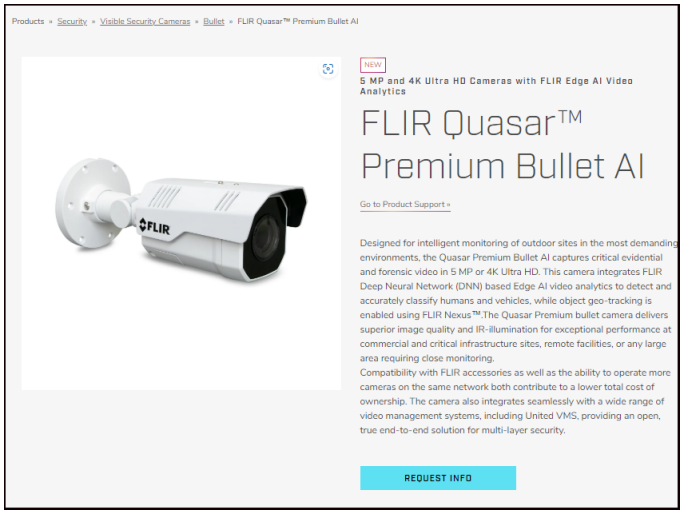
To access product information from the Teledyne FLIR website:

1. Open https://www.flir.com/browse/security/visible-security-cameras/.



Visible Security Cameras Page on the Teledyne FLIR Website

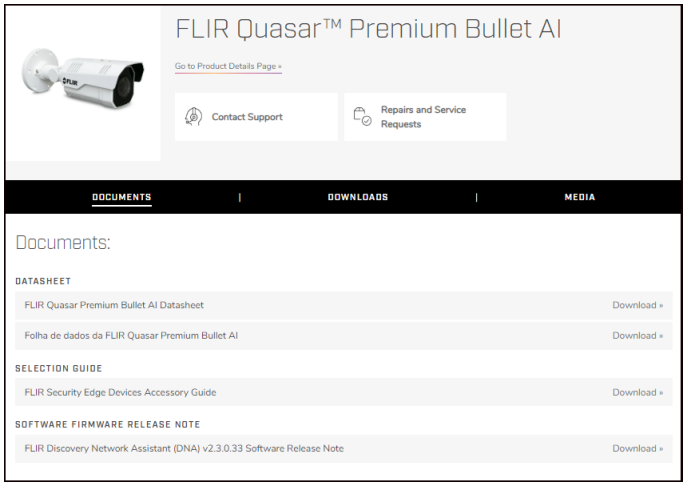
2. Find and click the camera. The camera's product details page appears.



Product Details Page (Example)

To see the camera's specifications and related content, scroll down.

3. Click **Go to Product Support**. The camera's support page appears.
4. Download product documentation from the Documents tab.

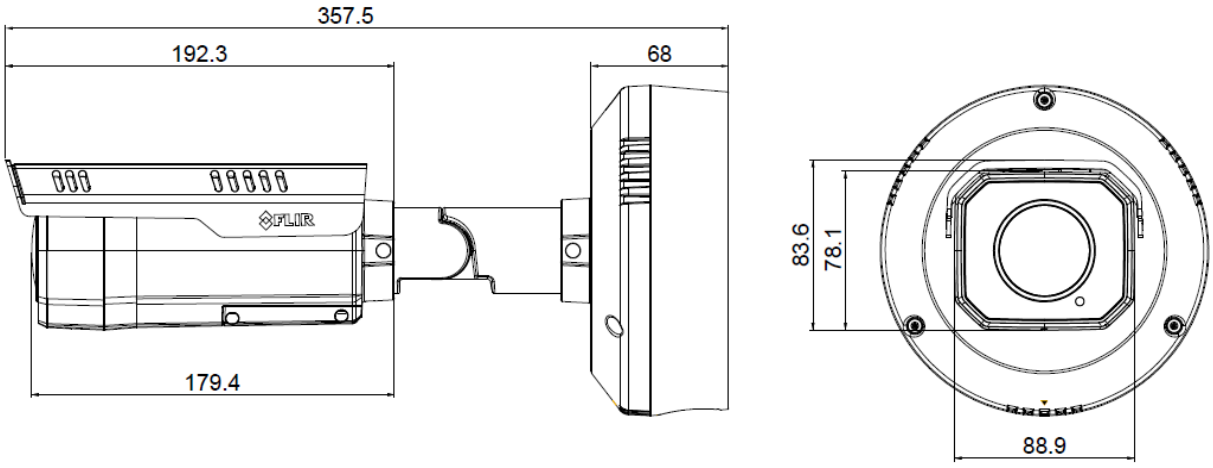


Product Support Page Documents Tab (Example)

5. Download the DNA tool from the Downloads tab.

2.3 Camera Dimensions (in mm)

With the sunshield attached, the Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics camera dimensions are:



3 Installation

Caution

- Except as described in this manual, do not open the camera for any reason. Damage to the camera can occur as the result of careless handling or electrostatic discharge (ESD). Always handle the camera with care to avoid damage to electrostatic-sensitive components.
- Prior to making any connections, ensure the power supply or circuit breaker is switched off.
- Operating the camera outside of the specified input voltage range or the specified operating temperature range can cause permanent damage.

This chapter includes information about:

To install the camera, Teledyne FLIR recommends connecting the camera on a bench or in a lab and configuring it for networking before mounting and aiming it:

However, circumstances can affect the sequence of the steps. For example, you can mount the camera before configuring it for networking.

3.1 Supplied Components

The Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics kit includes:

- two TP4x20 tapping screws for attaching the CB-650x back box to the mounting surface
- a T10 Torx Security wrench
- one two-pin connector for the 12 V DC / 24 V AC terminal block
- CB-650x Back Box with hole caps, plugs, and washers attached
- Multiple-cable rubber gland and seal
- one rubber single-cable gland
- two plastic screw anchors for attaching the CB-650x back box to the mounting surface
- a T20 Torx Security wrench
- two four-pin connectors for the alarm and audio I/O terminal blocks
- Mounting template sticker
- Printed installation guide

3.2 Site Preparation - General

There are several requirements that should be properly addressed prior to installation at the site.

The following specifications are requirements for proper installation and operation of the unit:

- **Ambient Environment Conditions:** Avoid positioning the unit near heaters or heating system outputs. Avoid exposure to direct sunlight. Use proper maintenance to ensure that the unit is free from dust, dirt, smoke, particles, chemicals, smoke, water or water condensation, and exposure to EMI.
- **Accessibility:** The location used should allow easy access to unit connections and cables.
- **Safety:** Cables and electrical cords should be routed in a manner that prevents safety hazards, such as from tripping, wire fraying, overheating, etc. Ensure that nothing rests on the unit's cables or power cords.
- **Ample Air Circulation:** Leave enough space around the unit to allow free air circulation.
- **Cabling Considerations:** Units should be placed in locations that are optimal for the type of video cabling used between the unit and the cameras and external devices. Using a cable longer than the manufacturer's specifications for optimal video signal may result in degradation of color and video parameters.
- **Physical Security:** The unit provides threat detection for physical security systems. In order to ensure that the unit cannot be disabled or tampered with, the system should be installed with security measures regarding physical access by trusted and un-trusted parties.
- **Network Security:** The unit transmits over IP to security personnel for video surveillance. Proper network security measures should be in place to assure networks remain operating and free from malicious interference. Install the unit on the backbone of a trusted network.
- **Electrostatic Safeguards:** The unit and other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc.) shall be properly grounded to prevent electrostatic discharge.

⚠ Warnings

- Before drilling into surfaces for camera mounting, verify that electrical or other utility service lines are not present. Serious injury or death may result from failure to heed this warning.
- Ensure the power supply or circuit breaker is off.

The physical installation of the unit is the first phase of making the unit operational in a security plan. The goal is to physically place the unit, connect it to other devices in the system, and to establish network connectivity. When finished with the physical installation, complete the second phase of installation, which is the setup and configuration of the unit.

3.3 Indoor Mounting

When installing the camera indoors:

- There must be a fuse or circuit breaker at the starting point of the electrical wiring infrastructure.
- The camera must be protected from hostile external elements such as: a corrosive environment, metallic dust, extreme temperatures, soot, over spray, and so on.
- Do not place the camera on or near radiators and heat sources.
- All electrical work must be performed in accordance with local regulatory requirements.

3.4 Outdoor Mounting

When installing the camera outdoors, consider the following:

- For outside wiring installation, always use weatherproof equipment, such as boxes, receptacles, connectors, and so on.
- For electrical wiring, use the properly rated sheathed cables for conditions to which the cable will be exposed; for example, moisture, heat, UV, physical requirements, and so on.
- Plan ahead to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.
- Use best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, and so on.
- All electrical work must be performed in accordance with local regulatory requirements.

3.5 Pre-Installation Checklist

Before installing the unit, make sure that:

- Instructions in the Document Scope and Purpose section are followed.
- All related equipment is powered off during the installation.
- Use best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, and so on.

Caution

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). The camera's operating temperature range is -40°C to 60°C (-40°F to 140°F) with IR off and -40°C to 50°C (-40°F to 122°F) with IR on; cold start -40°C (-40° F); and no more than 95% non-condensing humidity.

3.6 Supplying Power to the Camera

Warning

All electrical work must be performed by a qualified service person in accordance with local regulatory requirements.

The camera can be powered by 12V DC, 24V AC, or PoE+.

Maximum Power Consumption	12V DC	24V AC	PoE+
with IR (without heater)	16.6 W	14.6 W	15 W
without IR (with heater)	17.9 W	15.6 W	16.3 W

3.7 Connect the Camera

Connectors

Connector	Connection	
RJ-45 Two LEDs	Attach an Ethernet cable from the network switch to the RJ45 connector for a 10/100/1000 Mbps Ethernet and PoE+ (Power over Ethernet) IEEE 802.3at connection. Ethernet is required for streaming video and for configuring the camera. Green LED—10/100 Mbps connection. Orange LED—1000 Mbps connection. Steady LED—Active connection. Flashing LED—Network activity.	
POWER	DC12V - / AC24V ~	If using a 24V AC or 12V DC power supply, connect it to the power terminal block connector according to the pin assignment shown.
	DC12V + / AC24V ~	
AUDIO	AUDIO OUT - / +	Attach wires from external audio devices to the terminal block connector for audio in/out according to the pin assignment shown.
	AUDIO IN - / +	
ALARM	ALARM IN - / +	Attach wires from external devices to the terminal block connector for alarm in/out according to the pin assignment shown.
	ALARM COM / OUT	

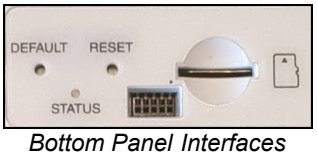
Warnings

- The power cord to the 12V DC or 24V AC power supply unit must be connected to a socket outlet with an earthing connector.
- The PoE unit and all interconnected equipment must be installed indoors within the same building, including all PoE-powered network connections, as described by Environment A of the IEEE 802.3at standard.
- All electrical work must be performed by a qualified service person in accordance with local regulatory requirements.

Bottom panel interfaces

To access the camera's default button, reset button, and microSD card slot, remove the access cover by loosening four screws.

Bottom of the Camera



Bottom Panel Interfaces

<table>
<tr><th>Interface</th><th>Description</th></tr>
<tr><td>DEFAULT (D)</td><td>To reset the camera to its factory defaults, press the button for at least 10 seconds.</td></tr>
<tr><td>RESET (R)</td><td>To reboot the camera, press the button for between 3-10 seconds.</td></tr>
<tr><td>STATUS</td><td>LED (green / red / amber) that indicates camera is booting up or firmware being upgraded.
<table>
<tr><th>Camera state</th><th colspan="2">LED state</th><th>Description</th></tr>
<tr><td rowspan="2">Booting up</td><td rowspan="2">Solid red for 2-3 seconds, then:</td><td>Green</td><td>Normal
After a successful boot, the LED turns off after three minutes.</td></tr>
<tr><td>Red</td><td>An error has occurred.</td></tr>
<tr><td>Firmware upgrade</td><td colspan="2">Flashing amber</td><td>During upgrade</td></tr>
</table></td></tr>
<tr><td>Console</td><td>For Support only.</td></tr>
<tr><td>microSD card slot</td><td>For video clip and snapshot recording and file storage, insert a microSDXC card in the card slot (maximum 2 TB SD Bus Mode UHS I). When the camera is powered on, do not remove the microSD card.</td></tr>
</table>

3.8 Configure for Networking

You can discover and configure the camera for networking using the FLIR Discovery Network Assistant (DNA) software tool; the camera's web page; or a supported VMS. Using the DNA tool or the camera's web page requires using the default admin user or any user assigned the admin or expert role.

Task	DNA Tool	Camera's Web Page
Discover camera IP address	•	
Configure IP address, mask, and gateway	•	•
Configure IP address, mask, and gateway for more than one camera at the same time	•	
Change user credentials	•	•
Configure DNS settings, MTU, and Ethernet speed		•

Notes

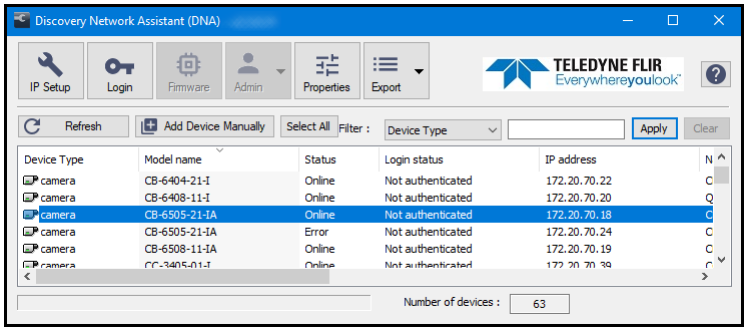
- Teledyne FLIR recommends using the DNA tool to discover the camera on the network. It does not require a license to use and is a free download from Teledyne FLIR. For more information about using the DNA tool, including how to configure more than one camera at the same time, see the *DNA User Guide*. While the software is open, click the Help icon.
- For more information about using a supported VMS to configure one or more cameras at the same time, see the VMS documentation.

By default, DHCP is enabled on the camera and a DHCP server on the network assigns the camera an IP address. If the camera cannot connect to a DHCP server, the camera's default IP address is 192.168.0.250.

- If the camera is managed by FLIR Horizon or Meridian VMS and the VMS is configured as a DHCP server, the VMS automatically assigns the camera an IP address.
- If the camera is managed by FLIR Latitude VMS or is on a network with static IP addressing, you can manually specify the camera's IP address using the DNA tool or the camera's web page.

To configure the camera for networking using the DNA tool:

1. Run the DNA tool (DNA.exe) by double-clicking . The Discover List appears, showing compatible devices on the VLAN and their current IP addresses.



2. In the DNA Discover List, verify that the camera's status is *Online*.

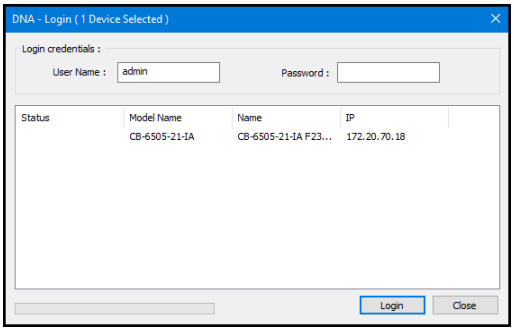
   If this is the first time you are configuring the camera or if it is the first time after resetting the camera to its factory defaults, DNA automatically authenticates the camera with the default password for the camera's admin user (*admin*).

   If the admin user password has been changed, you need to authenticate the camera.

   a. In the DNA Discover List, select the camera and click **Login** .

   b. In the **DNA - Login** window, type the password for the admin user. If you do not know the admin user password, contact the person who configured the camera's users and passwords.

   c. Click **Login**, wait for Ok status to appear, and then click **Close**.

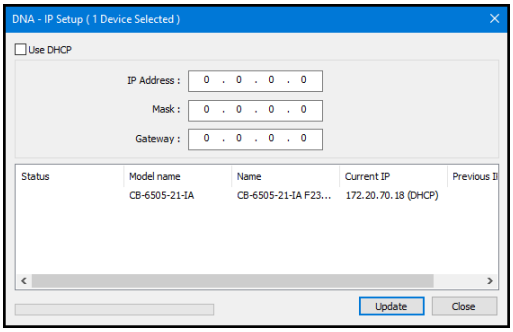


   In the DNA Discover List, verify that the camera's status is *Authenticated*.

3. Change the camera's IP address.

   Make sure the camera is selected in the Discover List, and then click **IP Setup** .

   In the **DNA - IP Setup** window, clear *Use DHCP* and specify the camera's *IP address*. You can also specify the *Mask* (default: 255.255.255.0) and *Gateway*. Then, click **Update**, wait for Ok status to appear, and then click **Close**.



To manually specify the camera's IP address using the camera's web page:

1. Access the camera's web page.

2. On the View Settings Home Page, click **System Settings**, and make sure the Settings appears.
4. Click **Static** IP addressing and then manually specify the camera's *Hostname*, *IP address*, *Netmask*, and *Gateway*.

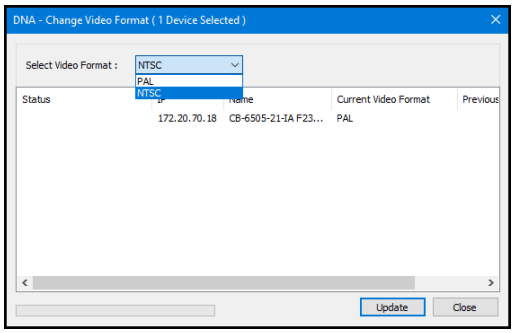
   You can also specify the *DNS Mode*, *Name Servers*, *MTU* (maximum transmission unit), and *Ethernet Speed*.
5. Click **Save**. Applying any changes on the Network page requires rebooting the camera.

3.9 Change Video Format (Optional)

By default, NTSC is the camera's video format. To change the format, you can use the DNA tool or the camera web page.

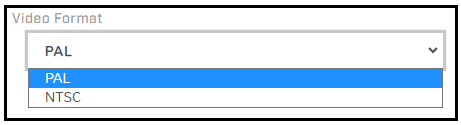
To change the camera's video format using the DNA tool:

1. In the DNA Discover List, right-click the camera and select **Change Video Format**.
2. In the **Change Video Format** window, select PAL.
3. Click **Update**, wait for ✔ Ok status to appear, and then click **Close**.



To change the camera's video format using the camera's web page:

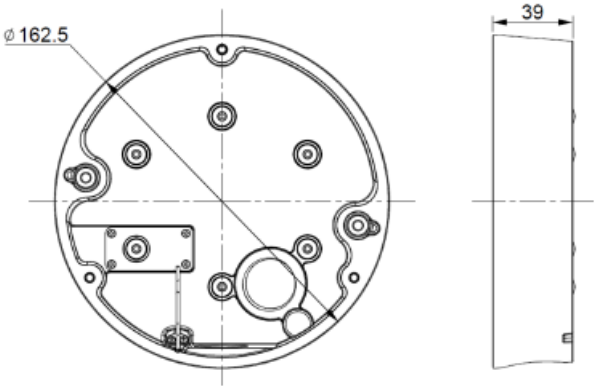
On the Firmware & Info Page, for Video Format, select another format.



To apply a video format change, the camera needs to reboot.

3.10 Install the Back Box

Dimensions (in mm)



The CB-650x Back Box provides a 3/4" side conduit hole for routing cables into the camera.

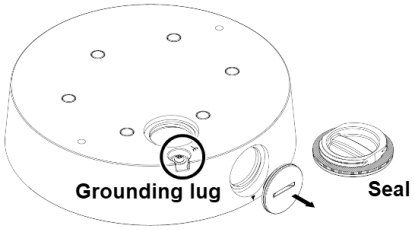
You can attach the CB-650x Back Box to a secure, flush, and vibration-free surface or to a standard single gang or double gang electrical box. You can route cables into the back box in two ways:

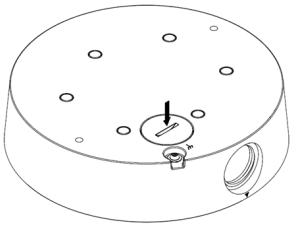
- Through the 3/4" side cable entry hole using a compression gland (not included).
- Through the 3/4" rear cable entry hole using the multiple-cable rubber gland and seal included in this kit.

The camera is shipped with a cap and rubber seal attached to the side cable entry hole. If you are routing cables through the side cable entry hole:

a. Use a coin to remove the cap and seal from the side cable entry hole.

b. Attach the cap and seal to the rear cable entry hole.





Make sure the cap is fully tightened.

Caution

Anchor a ground strap to the grounding lug on the back box and connect it to the nearest earth-grounding point. Failure to properly ground the camera can permanently damage it.

To help make sure the camera pans and tilts through its entire range; that is, to make sure the camera's mechanical stoppers do not interfere with aiming the camera, Teledyne FLIR recommends:

- **Wall mounting—**Attach the back box with the text facing up.
- **Ceiling mounting—**Attach the back box with the text facing away from the scene.

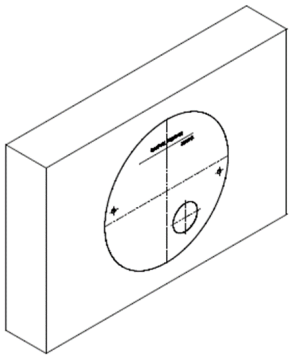
To attach the back box directly to a surface:

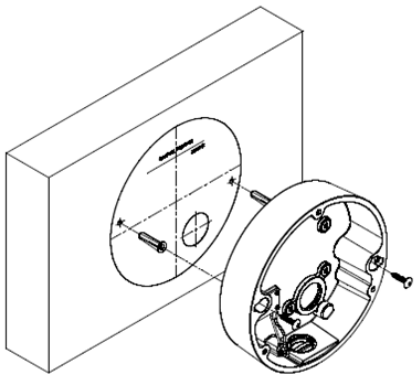
a. Using the mounting template sticker included in the kit, mark the surface and drill two anchor holes.

b. (Optional) If necessary, drill a hole for routing cables.

c. Hammer two plastic screw anchors into the drilled holes.

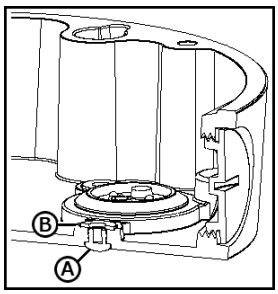
d. Insert the anchors and then attach the back box to the surface using two TP4x20mm tapping screws.

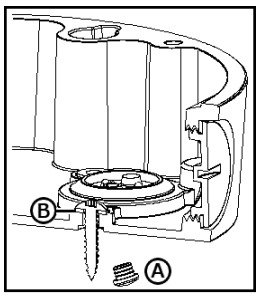




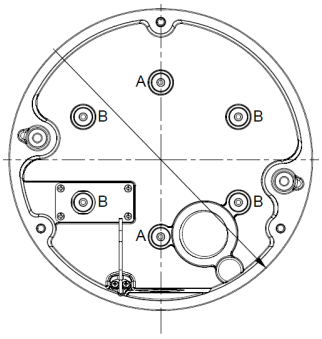
To attach the back box to a standard electrical box:

The back box is shipped with rubber seals and plugs attached to the electrical box mounting screw holes. For the holes you are not using, leave the seals and plugs in place. For the holes you are using, remove the rubber plug labeled A and leave the rubber seal labeled B in place to prevent water from entering the camera.





For example, if you are attaching the bracket to a single gang electrical box, remove the rubber plugs from the holes marked A on the back box. Leave the seals in place.



A: SINGLE GANG
B: DOUBLE GANG

Using truss head screws (not included), attach the back box to the electrical box.

3.11 Route the Cables

To route cables through the side conduit hole:

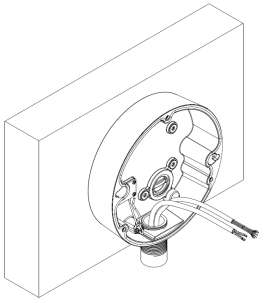
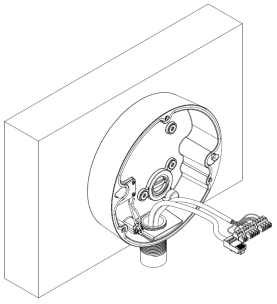
a. Attach a 3/4" PF thread or NPT thread compression gland (not included) to the side conduit hole.

PF thread	NPT thread
 For waterproofing, use a rubber seal.	 For improved waterproofing, use thread seal tape.

b. Make sure the seal is securely seated on the inside and outside of the cable entry hole. To seal any gaps, apply silicone sealant.

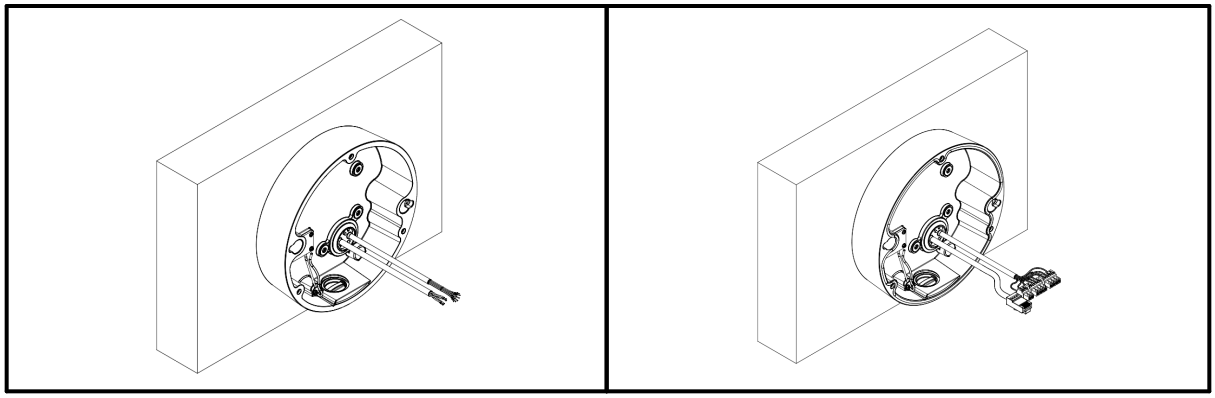
c. Route unterminated cables into the back box.

d. Terminate the cables. For the Ethernet cable, use an RJ45 connector and an RJ45 crimping tool. For other cables, use the connectors included in the camera kit. For more information, see the camera's documentation.

To route cables through the rear cable entry hole:

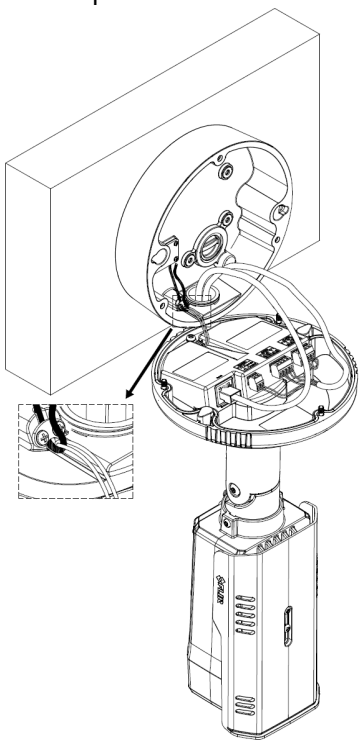
a. Route an unterminated Ethernet cable through a hole in the cable gland included in the CB-650x kit.
b. (Optional) Route an unterminated power, alarm, and audio cable through the other hole in the gland.
c. Terminate the cables. For the Ethernet cable, use an RJ45 connector and an RJ45 crimping tool. For other cables, use the connectors included in the camera kit. For more information, see the camera's documentation.
d. Attach the gland to the cable entry hole. Make sure that the side of the gland with the smaller diameter is inside the back box.



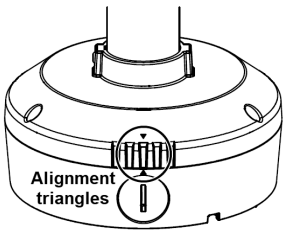
3.12 Connect and Mount the Camera

Make sure to attach the safety wire on the camera assembly to the clip on the back box.

The example at right shows the CB-650x Back Box attached to a wall, with an Ethernet cable and a power, alarm, and audio cable routed through the side cable entry hole and connected to the camera. The safety wire and clip is enlarged.



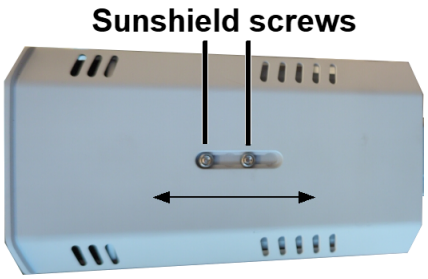
When attaching the camera assembly to the back box, align the triangle on the exterior of the camera assembly with the triangle on the back box. This makes sure the guide pins inside the camera assembly are aligned with the guide



Adjusting the sun shield

Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics are designed to operate in rugged environments. The sun shield is coated to prevent damage from sunlight or rain.

To adjust the sun shield, use the T20 Torx Security wrench to loosen the two screws on the shield hood, and move the shield forward or backward. Then, securely tighten the two screws.

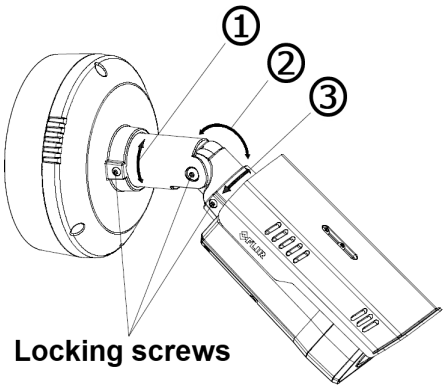


Caution	To avoid damaging the camera housing, do not adjust the sun shield beyond its limits.

Tip	Adjust the sun shield to avoid issues with shadows. Take into account the lens coverage.

3.13 Aim the Camera

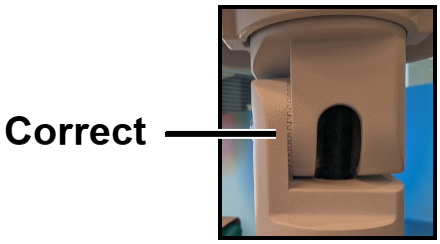
While supporting the camera with your hand, and using the T20 Torx Security wrench to loosen the locking screws, adjust the camera's pan, tilt, and rotation.



Aiming the Camera (Wall Mounting)

1. Retaining ring for pan adjustment (range 355°)
2. Bracket for tilt adjustment (range 90°)
3. Retaining ring for spin rotation (range 355°)

Adjust the pan position to make sure the camera tilts towards the scene and can be rotated to face upright towards the scene. For ceiling mounting, the proper pan position is 180° degrees from the proper pan position for wall mounting; to rotate the camera to face upright towards the scene, it needs to be tilting the opposite direction. An improper pan position prevents the camera from tilting towards the scene and a mechanical stopper prevents the camera body from being rotated so that it is upright facing the scene.



Make sure that toothed surfaces are properly aligned and meet evenly.

Then, use the T20 Torx Security wrench bit to securely tighten each locking screw.

3.14 Configure the Analytics

Using the Video Analytics Page, calibrate and then configure the camera's onboard VA.

3.15 Additional Configuration

Depending on how you are installing and using the Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics, and the network and VMS to which it is connected, initial configuration can also consist of enabling, disabling, or configuring the following settings using the camera's web page:

Settings	User Role
• Live video and video streams • Visible imager • Current and idle I/O states • On-screen display (OSD) • Geotracking • Georeference • Other networking settings • Date and time • Alarms • Audio • Enabling and configuring external I/O devices • Notification emails • Onboard heaters and fans • Cybersecurity • Map • Scheduled tasks • Recording • Format a microSD card • Firmware, factory defaults, and other system settings	Default admin user / any user assigned the admin or expert role
Users, roles, and passwords	Default admin user / any user assigned the admin role
Pairing one or more Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics with a FLIR Security PTZ camera that supports geotracking—see the corresponding pairing guide of the PTZ camera.	Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics: Default admin user / any user assigned the admin or expert role PTZ camera: Default admin user / user assigned the admin or expert role

Some of these configuration tasks can be performed before or after mounting the camera, but others can or should be performed only after mounting and connecting the camera.

3.16 Attach the Camera to a Supported VMS

After you have mounted the camera and discovered or defined its IP address, you can use VMS Discovery / Attach procedures to attach the camera to a supported VMS.

4 Operation

This chapter includes information about how to access the camera and how to operate it using the View Settings Home Page.

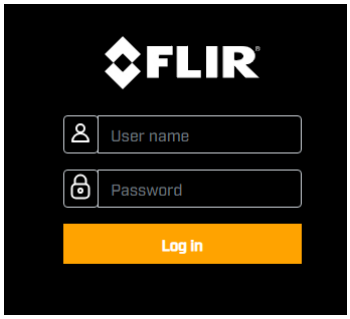
4.1 Accessing the Camera

To operate the camera, you first need to access it by logging in to the camera's web page. The camera's web page supports Google Chrome® and other popular web browsers. This guide supports and reflects Chrome.

To log in to the camera's web page:

1. Do one of the following:
   - In the FLIR Discovery Network Assistant (DNA) tool, double-click the camera in the Discover List.

     The DNA tool does not require a license to use and is a free download from Teledyne FLIR. Download the DNA tool; unzip the file; and then double-click to run the tool (DNA.exe). The Discover List appears, showing compatible devices on the VLAN.
   - Type the camera's IP address in a browser's address bar (when the PC and the camera are on the same network). If you do not know the camera's IP address, you can use the DNA tool to discover it.
2. On the login screen, type a user name and the password.

   When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, you need to log in with the camera's default credentials:

   User name—admin

   Password—admin

   If you do not know the user name or password, contact the person who configured the camera's users and passwords.
3. When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, specify a new password for the admin user and then log back in using the new password.

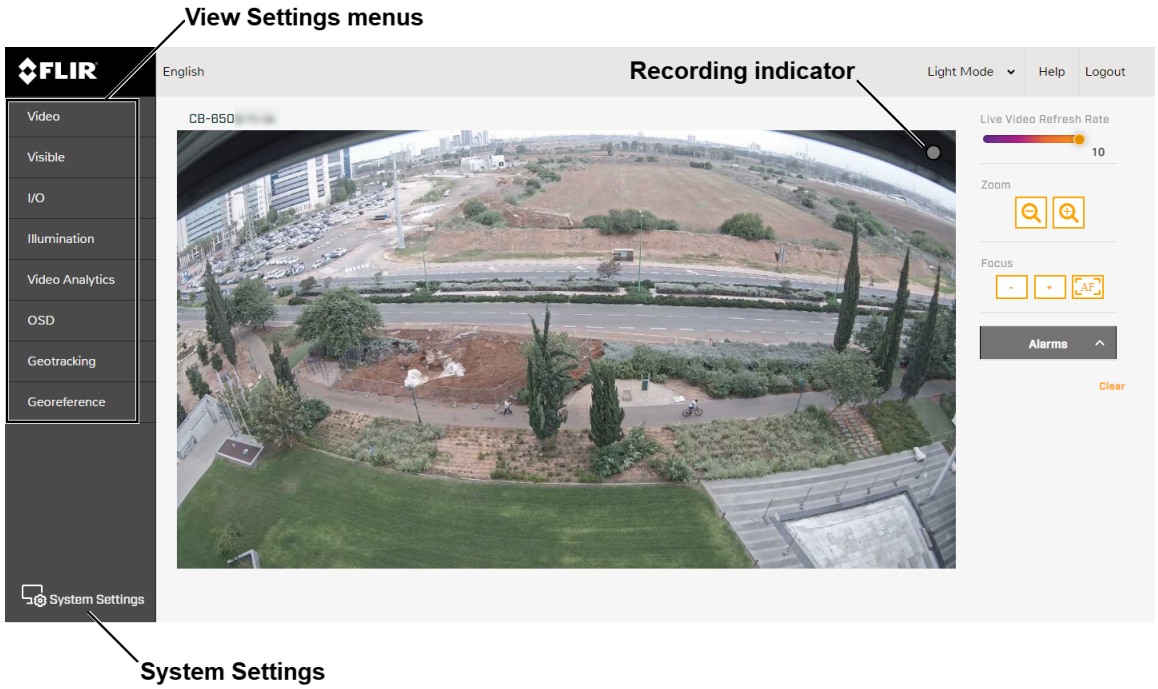
   Use a strong password consisting of at least 12 characters and at least one uppercase letter, one lowercase letter, and one number. Passwords can include the following special characters: | @#~!$&<>+_-.,*?= .

   In order to avoid cyber security vulnerabilities linked to passwords, any changes to the default password on the camera must be made within a closed and secure network or LAN . To change password over the web browser, HTTPS should be used to ensure security of the data.

The camera's View Settings Home Page appears.

4.2 View Settings Home Page

On the View Settings page, a navigation menu, live video images, and camera controls appear. Camera configuration and the role assigned to the user accessing the camera determines which settings and controls are available.



View Settings Home Page - Users Assigned the Admin or Expert Role

Above the live video, the following appear:

- **Languages—**The language for the camera's web page: Arabic, Simplified Chinese, Traditional Chinese, English (default), French, Portuguese, Russian, or Spanish.
- **Theme—**Dark Mode (default) or Light Mode.
- **Help—**Opens screen with a link to https://www.flir.com/ for support, along with system information.
- **Logout—**Logs out of the camera's web page.
- **Camera Name—**As specified on the Firmware & Info Page.

To the left of the live video, the View Settings menu appears:

- **Video—**Opens the Video page.
- **Visible—**Opens the Visible page.
- **I/O—**Opens the I/O page.
- **Illumination—**Opens the Illumination page.
- **Video Analytics—**Opens the Video Analytics (VA) page. If Video Analytics does not appear in the View Settings menu, contact FLIR Support.
- **OSD—**Opens the OSD (on-screen display) page.
- **Geotracking—**Opens the Geotracking page.
- **Georeference—**Opens the Georeference page.

Below the View Settings menu, users assigned the admin or expert role can click **System Settings** to access system settings pages and configure the camera. For more information, see Configuration.

Live Video

The recording indicator shows whether the camera is currently recording live video to the local microSD card.

The live video on the camera's web page is not the actual video stream. Changes to the video stream, analytics tracking overlay, or on-screen display (OSD) settings might not affect the live video.

Live Video Refresh Rate

Specify between 1-10 image frames per second (FPS). The Live Video Refresh Rate setting only affects the live video; it does not affect the camera's video streams.

Zoom & Focus

	Manual zoom out / in buttons.
	Manual focus out / in buttons.
	Triggers a one-time auto focus.

If the camera is currently detecting and classifying objects, and generating any alarms, they appear on the View Settings home page, as well.

4.3 Making Changes to Settings

The camera's configuration files store the following sets of settings:

- **Factory default settings—**The settings when you first connect the camera to power, and when resetting the camera to its factory default settings (see Firmware & Info Page). A partial factory reset restores all factory default settings except the settings on the Settings.
- **Saved settings—**The settings you save as you operate and configure the camera. When the camera reboots, it restores these settings. Changes made to any page since saving changes are lost.

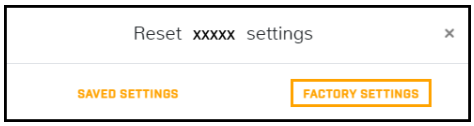
Tip

Whenever possible, Teledyne FLIR recommends testing new settings before saving them because saving changes overwrites the previously saved settings.

View Settings

When you make a change to most View Settings, the **Reset** and **Save** buttons become enabled. For some View Settings, the camera immediately applies the changes, but does not save them; for example, on the Visible Page. For others, the camera does not apply changes until you save them.

Regardless of whether the camera has already applied changes, to save all changes since the last time these settings were saved, click **Save**. This can include earlier changes that were not saved.

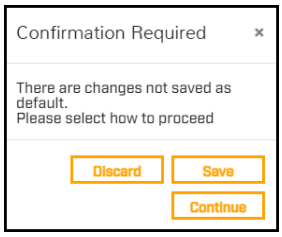


To restore previously saved settings or the factory default settings, click **Reset**. To close the message and return to the page without restoring settings, click the close icon ✖.

Tip

If you try to navigate to a different page before saving changes, a confirmation message appears. In most cases, you can click **Continue**, which allows you to navigate to other pages and test the setting changes. Then, you can return to the page and save the new settings. Or, you can:

1) discard the changes
2) save them
3) close the confirmation message without discarding the changes or saving them by clicking the close icon ✖.

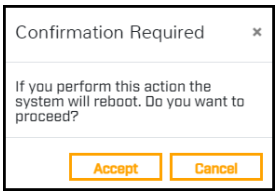


System Settings

When you make a change to most System Settings, the **Discard Changes** link and the **Save** button become enabled. For some System Settings, the camera immediately applies the changes, but does not save them; for example, on the Alarm Page and on the Audio Page. For others, the camera does not apply changes until you save them.

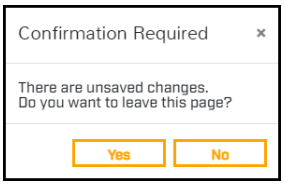
Regardless of whether the camera has already applied changes, to save changes, click **Save**. To discard changes and restore previously saved settings or the factory default settings, click **Discard Changes**.

Changes to some System Settings require the camera to reboot; for example, on the Settings and on the Date & Time Page. After clicking **Save**, a confirmation message appears. To save the changes, and reboot the camera with the changes applied, click **Accept**. To close the confirmation message and remain on the page — without discarding the changes or saving them — click **Cancel** or click the close icon ✖.



Tip

If you try to navigate away from the page before saving changes, a confirmation message appears. To leave the page, discard changes, and restore previously saved settings, click **Yes**. To close the confirmation message and remain on the page — without discarding the changes or saving them — click **No** or click the close icon ✖.



4.4 Video Page

The camera provides two IP video streams, Visible 1 / V1 and Visible 2 / V2. In general, modifying the default IP video settings is not necessary. In some cases, fine-tuning the streams can help reduce the bandwidth requirements; for example, when a stream is sent over a wireless network.

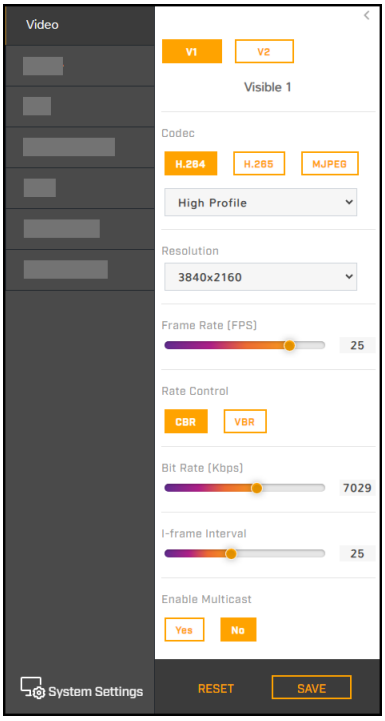
To change the settings for a particular video stream, click V1 or V2.

V1 / V2

You can specify:

- **Codec**—H.264, H.265, or MJPEG
- **Resolution**—
  - **3840x2160** (4K)—Available on CB-6508 models and only available for V1.
  - **2592x1944** (5MP)—Available on CB-6505 models and only available for V1.

- **1920x1080** (1080p)
- **1280x720** (720p)
- **640x480** (480p)



Frame Rate (FPS)—Between 5-30 / 25 frames per second (NTSC / PAL).

Codecs, Quality, and Bandwidth

The codec determines which settings are available. The values of those settings can have a significant impact on the quality and bandwidth requirements of the video stream.

With the H.264 codec, you can specify the following:

- **Profile:**
  - **High Profile** (default)—Designed for HD TV applications, provides the best trade-off between storage size and video latency. Compared to Main Profile, it requires 10-12% less storage, but can experience increased latency, depending on the stream structure.
  - **Main Profile**—Designed for SD TV applications, provides good picture quality over lower bandwidth.

With the H.265 codec, only Main Profile is available.

- **Rate Control**:
  - **CBR** (constant bit rate)—The Bit Rate parameter defines the target bit rate; the camera attempts to keep the video at or near the target bit rate.
  - **VBR** (variable bit rate)—The Bit Rate parameter defines the average bit rate.
- **I-frame Interval**—Controls the number of P-frames used between I-frames. I-frames are full frames of video and the P-frames contain the changes that occurred since the last I-frame. A smaller I-Frame Interval results in higher bandwidth (more full frames sent) and better video quality. A higher I-frame Interval means fewer I-frames are sent and therefore can result in lower bandwidth and possibly lower quality.

If you set the MJPEG resolution on V1 above 1080p, V2 will be displayed instead of V1 because the MJPEG resolution cannot exceed 1080p. In this case, the OSD on V2 needs to be enabled.

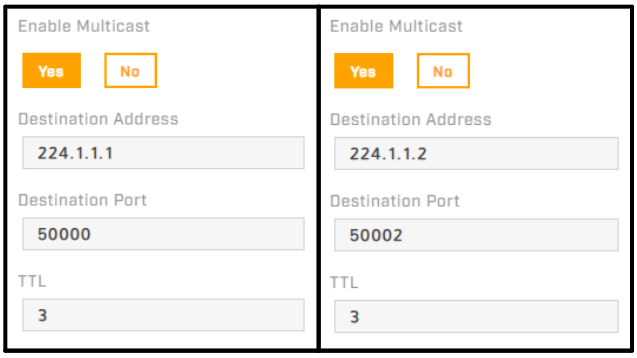
With the MJPEG codec, you can set the Quality between 0-100; 80 is the default. Setting a higher value can increase the video stream's bandwidth requirements. Teledyne FLIR recommends setting a value no higher than 80. If you experience video issues when using MJPEG and high-resolution video, try adjusting the Quality and the resolution settings.

Tips

- Use the default values initially. Then, incrementally modify and test individual parameters to determine when bandwidth and quality requirements are met.
- On the camera web page, the live video is not an actual video stream. Changes to stream settings might not affect the live video. Before saving changes, Teledyne FLIR recommends checking them using a FLIR UVMS, client program, or third-party ONVIF system.
- You can view a snapshot of live video using the following URL: http://<camera_IP_address>/images/snapshots/DLTVimage.jpeg.

Enable Multicast

By default, multicast is enabled. Multicast video packets are shared by streaming clients. Additional clients do not cause bandwidth to increase as dramatically as with unicast. Video stream requests for ch0/stream1 are unicast. Client-specific multicast requests vary according to the client.



V1 *V2*

If more than one camera is providing multicast streams on the network, make sure the Destination Network IP address is unique for each camera (the Destination Port can be reused). By default, the port assignment is unique per stream.

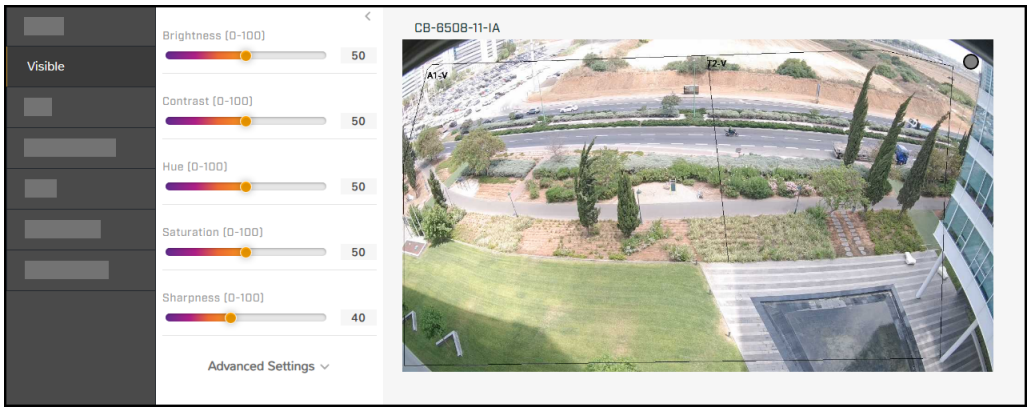
The time-to-live field controls the ability of IP packets to traverse network boundaries. A value of 1 restricts the stream to the same subnet. Greater values allow increasing access between networks.

The video streaming uses a protocol generally referred to as RTP, the real-time transport protocol, although there are actually a number of protocols involved, including the Real-Time Streaming Protocol (RTSP). The video stream URLs incorporate the IP address of the camera. Using the camera's default IP address, the complete URLs are:

- **V1**—rtsp://192.168.0.250:554/stream1
- **V2**—rtsp://192.168.0.250:554/stream2

To maintain compatibility with legacy systems, the stream names are aliased as ch0 = stream1 and ch1 = stream2.
By default, RTSP authentication is enabled. To access any of the camera's video streams, you can use the name and password for any of the camera's users. Users assigned the role of admin or expert can disable RTSP authentication on the Services.

4.5 Visible Page

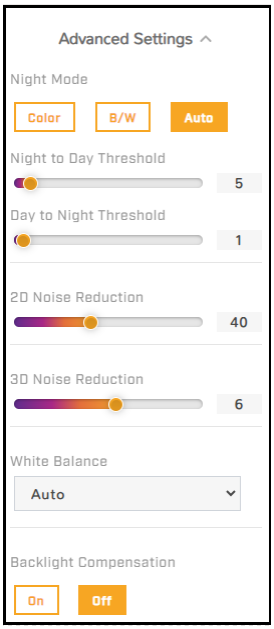


You can adjust the following image settings:

- **Brightness**
- **Saturation**

- **Contrast**
- **Hue**
- **Sharpness**

Advanced Settings—



- **Night Mode**
  - **Color** (day mode)
  - **B/W** (night mode)—Also turns the IR LED illuminator on, unless disabled on the Illumination Page.
  - **Auto** (default)—Automatically switches the video mode according to the light level detected by the camera's light sensor. When Night Mode is set to Auto, you can set the thresholds at which the video switches from black and white to color (Night to Day Threshold) and vice versa (Day to Night Threshold). Specify a value between 0-100, where 0 switches modes at a lower light level (darker) and 100 switches modes at a higher light level (brighter). These thresholds also determine when the camera turns the IR LED illuminator on and off.
- **2D / 3D Noise Reduction**—

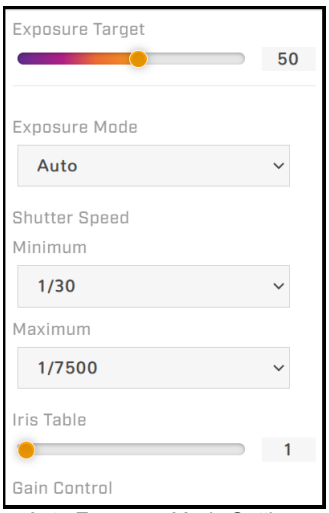
  Reduces or eliminates artifacts that can limit the ability to positively identify an object. There are two types of noise: luminance noise and color (chroma) noise. 2D NR and 3D NR settings reduce luminance noise: dots of varying brightness levels (black, white, and gray). Teledyne FLIR recommends against completely eliminating luminance noise, because it can result in unnatural images.
  - **2D Noise Reduction**—Analyzes each individual frame pixel by pixel to eliminate environmental noise. 2D NR can produce superior images for moving objects. However, it is less precise than 3D NR and can cause blurring around the edges of objects. Specify a value between 0-100, where 0 provides no 2D NR and 100 provides the maximum level of 2D NR.
  - **3D Noise Reduction**—Provides superior noise reduction by analyzing adjacent frames to reduce image noise / snow in low-light conditions. However, 3D NR can create more motion blur on moving objects than 2D NR. When the camera's visible video is needed at night or other low-light conditions, use external IR illumination and 3D NR. Specify a value between 0-100, where 0 provides no 3D NR and 100 provides the maximum level of 3D NR.
- **White Balance**—
  - **Auto (default)**
  - **Off**—Manually specify the Rgain (red level gain) and the Bgain (blue level gain), between 0-100. The default value for both is 100. To perform a one-time white balance, click **One Push Trigger**.
- **Backlight Compensation**—For images with a bright light source that puts the subject of interest in shadow or silhouette, enabling backlight compensation (BLC) can improve the image. By default, BLC is disabled.

Exposure Settings

Exposure is the amount of light reaching the image sensor. Exposure time (shutter speed), iris table (aperture size), and gain determine the exposure level. Increasing exposure produces a brighter video image and adds detail. Increasing gain increases the sensitivity of the sensor, which also produces a brighter image and adds detail. However, increasing gain can increase noise in the video image.

- **Exposure Target—**Specify the desired exposure level between 0-100. The default value is 50.

Exposure Mode—



Auto Exposure Mode Settings

- **Auto (default)—**Also known as Iris Priority. You can specify the maximum and minimum exposure times, the fixed iris table, and the gain control (maximum gain). To achieve the specified exposure target, the camera automatically adjusts the exposure time within the specified range, and the gain up to the specified maximum.
- **Lock—**Also known as Manual. You can specify the fixed gain and the fixed exposure time. The iris table is fixed and you cannot adjust it. Teledyne FLIR recommends Lock for scenes with fixed light levels and fixed lighting contrast such as indoor scenes; when a consistent, precise exposure level is required; or when other modes do not provide the desired exposure.
- **WDR 2x / WDR 3x—**Enables Shutter (True) WDR. The camera analyzes the exposure and level of detail in two / three consecutive frames taken at two / three exposure settings and shutter speeds; determines the optimal combination of regions within the scene; and generates a single, composite frame with wide dynamic range. When the camera is not in a WDR exposure mode, it operates in linear mode; that is, the camera streams every frame it takes.
- **Auto S—**Also known as Shutter Priority. You can specify the gain control and the fixed exposure time. To achieve the specified exposure target, the camera automatically adjusts the iris and the gain up to the specified maximum.
- **Auto Iris—**You can specify the maximum and minimum exposure times and the gain control. To achieve the specified exposure target, the camera automatically adjusts the iris, the exposure time within the specified range, and the gain up to the specified maximum.
- **50 Hz / 60 Hz—**Also known as Flickerless modes, they can eliminate flicker caused by fluorescent lighting. Select the power frequency used for lighting the scene.

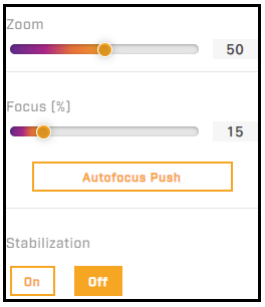
- **Minimum Shutter Speed**—Specify the slowest shutter speed based on the amount of light in the scene, speed of moving objects, and noise. If the scene includes fast-moving objects, Teledyne FLIR recommends specifying a minimum shutter speed faster than 1/25 or 1/30 seconds.
- **Maximum Shutter Speed**—Select the fastest shutter speed based on the amount of light in the scene. A faster shutter speed decreases the amount of light entering the sensor and results in a darker image.

The video format determines the shutter speeds available, as shown, in fractions of a second:

Supported Shutter Speed									
NTSC					PAL				
1/3	1/15	1/250	1/4000	1/15000	1/3	1/12	1/250	1/4000	1/15000
1/4	1/30	1/500	1/5000	1/20000	1/4	1/25	1/500	1/5000	1/20000
1/5	1/60	1/1000	1/7500		1/5	1/50	1/1000	1/7500	
1/7	1/120	1/2000	1/10000		1/6	1/100	1/2000	1/10000	

- **Iris Table**—Available in Auto exposure mode. Specify the fixed iris between 1-5, where 1 (default) is the largest aperture size and 5 is the smallest.
- **Gain—**Available in Lock exposure mode. Specify the fixed gain between 1-512. The default value is 1.
- **Gain Control—**Available in Auto, Auto S, and Auto Iris exposure modes. Specify the maximum gain – Off, Low (default), Medium, High.

Additional Settings



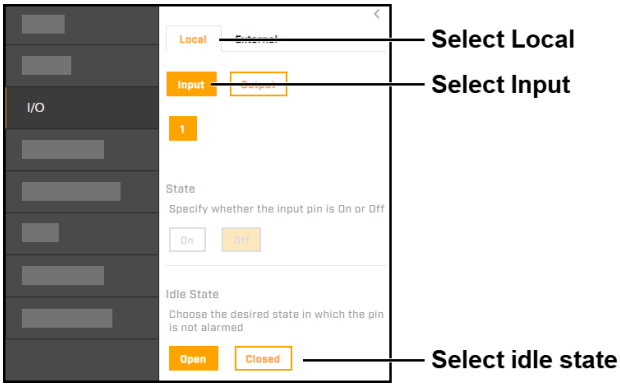
- **Zoom—**Manually adjust the zoom. Specify a value between 0-100.
- **Focus—**Manually adjust the focus. Specify a value between 0-100. To trigger a one-time auto focus, click **Autofocus Push**.
- **Stabilization** (Electronic Image Stabilization)—Keeps the image steady and compensates for external vibration. To ensure calibration accuracy, after enabling stabilization, keep the camera still for three seconds. When Stabilization is On, the stabilization algorithm that processes the image slightly crops the video image. Stabilization is Off by default, and cannot be enabled when the Exposure Mode is WDR 2x or WDR 3x.

4.6 I/O Page

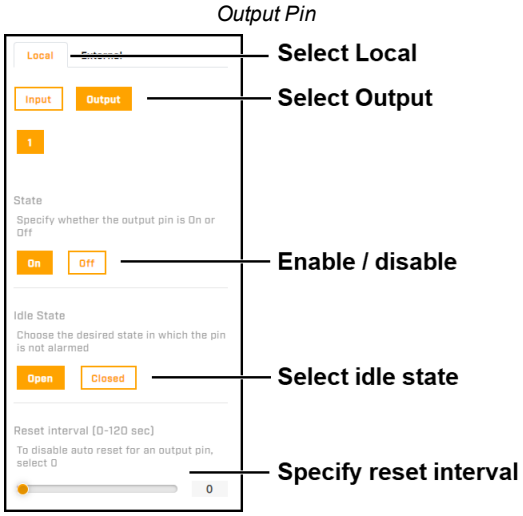
On the I/O (input / output) page, you can configure the camera's local and external I/O.

Local I/O

Input Pin



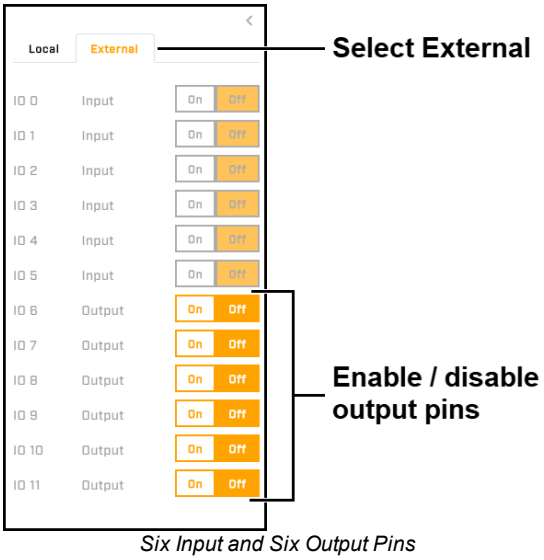
Output Pin



For information about the local I/O connector, see Connect the Camera.

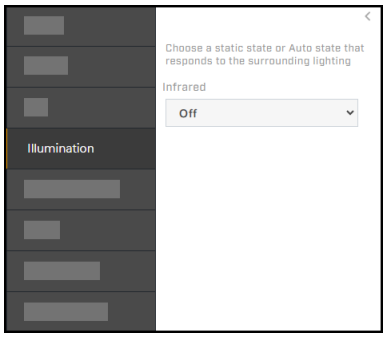
External I/O

On the I/O Devices Page in System Settings, users assigned the admin or expert role can configure the camera's external I/O connections and the device managing those connections with the camera.



Six Input and Six Output Pins

4.7 Illumination Page



By default, infrared (IR) illumination is set to Auto. On the Visible Page, when the Night Mode is also set to Auto, the camera's light sensor detects that the scene has become dark enough, the camera automatically turns the IR LED illuminator on and turns the IR Cut filter off. Likewise, when the scene becomes light enough, the camera turns the illuminator off and the IR Cut filter on. The camera's light sensor also determines the intensity of the IR illuminator.

Setting IR illumination to High, Medium, or Low specifies a fixed IR illumination intensity when the IR illuminator is on, as determined by the Night Mode settings on the Visible Page.

Setting IR illumination to Off disables the camera's IR illuminator, regardless of the Night Mode setting.

4.8 Video Analytics Page

The camera's advanced onboard VA:

- Incorporates deep neural networks (DNN) technology.
- Provides intrusion and loitering detection.
- Classifies detected objects as human or vehicle. Vehicle detection applies to cars, vans, small trucks and vehicles up to the size of 15m. Larger vehicles such as long trailers, forklifts, and heavy vehicles with special shapes, such as construction vehicles will not be detected nor filtered.

On the Video Analytics page, you can:

- Enable or disable the VA—By default, VA is disabled.
- Check the analytics calibration.
- Create and configure tripwires, intrusion detection or loitering regions, and masking regions. By default, tripwires or regions have not been defined, and alarm rules are disabled.
- Enable and configure the VA overlay.

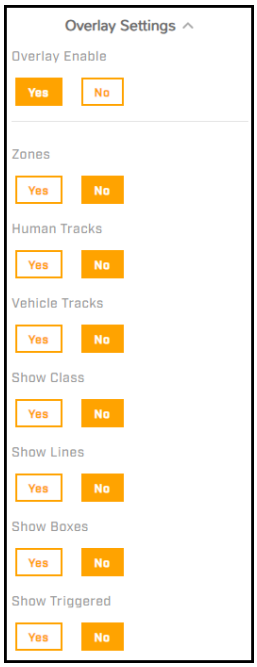
The camera immediately applies and saves changes to settings on the Video Analytics page, affecting the live video images and video streams.

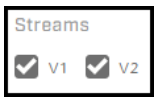
Detection and Classification

The camera's video analytics detect intrusion or loitering and classify detected objects separately for each region. In the analytics tracking overlay, H indicates a detected and classified human; V indicates a vehicle.

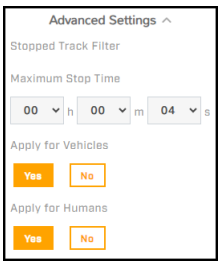
Overlay Settings

Enable and configure the VA overlay in the video streams. You can enable or disable the following:



Setting	Description	Comments
Enable	Globally enable or disable the VA overlay.	Enable one or more individual video streams.
Zones	Show analytics regions: tripwires, intrusion areas, and loitering areas.	When enabled, regions are labeled according to type and unique region ID number. T = tripwire and A = intrusion / loitering area. For example, A3 = Area 3.
Human Tracks	Show detected objects classified as humans.	Enable Show Class, Show Lines, or Show Boxes.
Vehicle Tracks	Show detected objects classified as vehicles.	
Show Class	When tracks are enabled, show the classification of the detected objects: human (H) or vehicle (V).	Enable Human Tracks or Vehicle Tracks.
Show Lines	When tracks are enabled, show the lines for the detected objects according to positions from prior frames; helps visually represent speed and direction.	
Show Boxes	When tracks are enabled, show a box around the track.	
Show Triggered	Show tracks only when they are triggering a tripwire, intrusion, or loitering alarm.	Enable Human Tracks or Vehicle Tracks. Enable Show Class, Show Lines, or Show Boxes.
	Enable the VA overlay for individual video streams.	• Does not override the global Overlay Enable setting above. For the overlay to appear in a stream, the global setting and the stream must be enabled. • The live video on the camera's web page is not the actual video stream. Therefore, enabling the VA overlay for a stream might not affect the live video.

Advanced Settings



Stopped Track Filter

Maximum Stop Time—Maximum amount of time, in hours (0-12), minutes (0-60), seconds (0-60), the camera shows the track of a detected object that has stopped moving.

You can apply the filter to detected objects classified as vehicles and to detected objects classified as humans.

To configure the camera's VA:

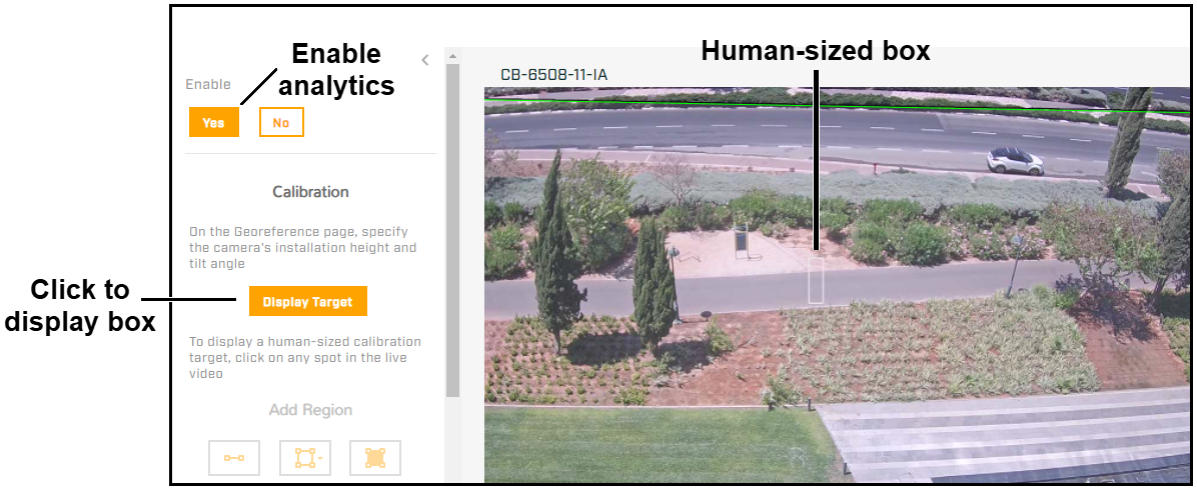
1. Make sure the camera is mounted in its final location and properly aimed.

2. On the Georeference Page, specify the camera's installation height, tilt angle, and roll angle.
3. Enable the VA overlay.
4. Check the VA Calibration.
5. Create VA Regions.

Users assigned the expert or admin role can enable, modify, or define alarm rules on the Alarm Page.

4.8.1 Check the VA Calibration

Before checking the camera's VA calibration, specify the camera's installation height, tilt angle, and roll angle on the Georeference Page.



1. Make sure that a person about 1.8m (5" 11') tall is in the camera's field of view.
2. On the Video Analytics page, make sure VA is enabled.
3. Expand Overlay Settings, and make sure Overlay Enable is **On**.
4. Click **Display Target**. A box simulating a 1.8m (5" 11') human appears in the live video for about 10 seconds and then automatically disappears. Make sure the height of the box corresponds to the size of the person standing in the camera's field of view.

Tip

If the height of the box does not correspond to the size of the person, on the Georeference Page, verify the camera's installation height, tilt angle, and roll angle.

4.8.2 Recommended Guidelines for Optimal Detection Results

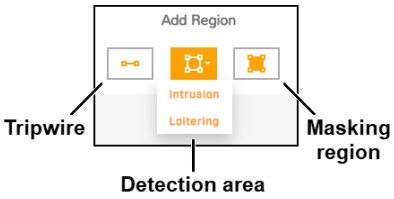
In order to achieve >95% detection accuracy, the following guidelines should be followed:

- Install the camera on a stable fixed pole, 6 meters high.
- Start the detection zone 3-5 meters from a fence line or boundary.
- Apply to flat surface terrains with no tall grass or slopes.

4.8.3 Create VA Regions

To create a VA region:

1. Under Add Region, click the appropriate icon to create a tripwire; an intrusion or loitering detection area; or a masking region.

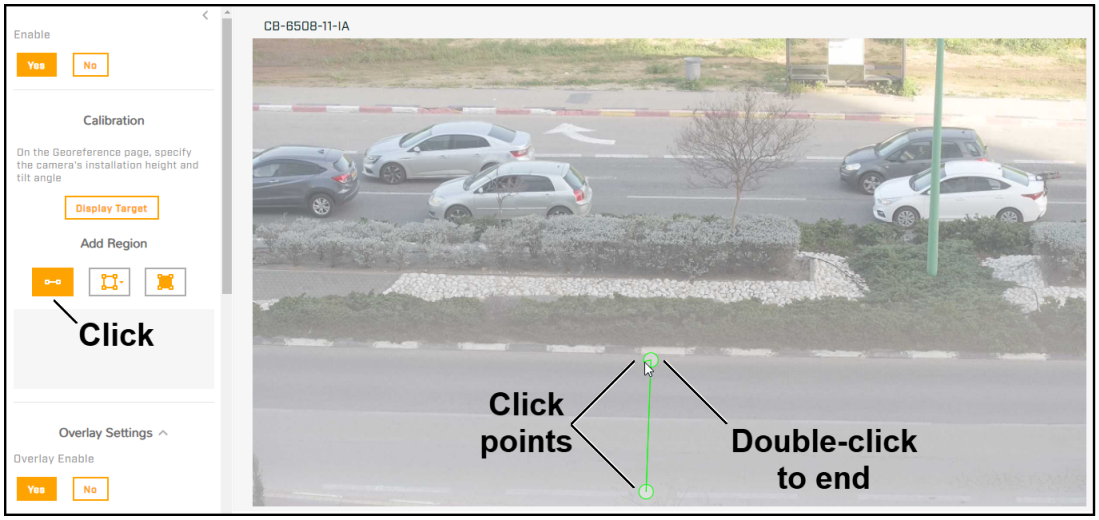


2. Specify each point of the region by clicking and releasing on the live video image. Do not click and drag. Also, do not draw one region line or border over another.

   You can create up to 8 masking regions.

   You can create up to two loitering detection areas and a total of eight tripwires and/or intrusion detection areas. For each region, the maximum number of points is 16.

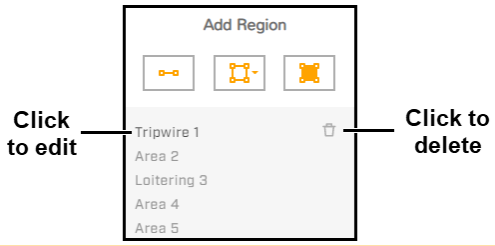
3. To finish creating the region, double-click on the last point.



Creating a Tripwire

Tips

- To cancel creating a region, press **Esc**.
- To modify the settings for an existing region or to delete one, click the region either in the region list or in the live video image.
  - To move or adjust the region points, tripwires, or an entire region, click on a point, line, or border, and drag.
  - To delete a region, click the trash icon .



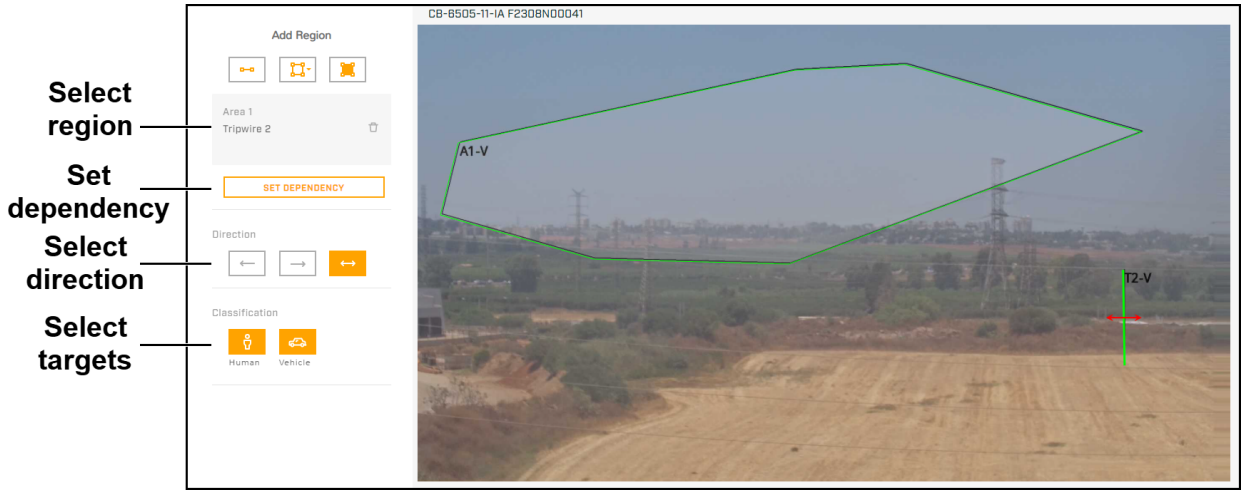
Masking regions—Regions of the video image in which the VA does not detect objects and does not generate alarms. For example, to eliminate alarms from trees or bushes moving in the wind.

Note

Masking regions provide VA detection masking, not privacy masking. VA is disabled in masking regions. However, the region itself appears in the video.

After creating a region, you can configure the following:

Region type	Direction	Human and Vehicle Classification	Loitering Time
Tripwires	•	•	
Intrusion		•	
Loitering		•	•
Masking	N/A		



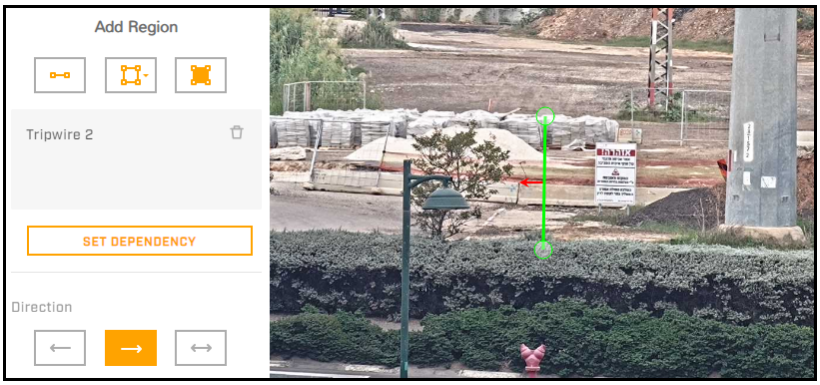
Configuring a Region

Tripwire Direction

By default, tripwires are bidirectional. However, you can configure them to be unidirectional. When configured as unidirectional, the direction selection arrows refer to the direction of movement over the tripwire *as seen from the first tripwire point created*.

At left, the first point of a tripwire has been defined and the tripwire is being drawn from top to bottom.

Below, the tripwire has been completed and the *left-to-right* direction button has been selected. Because detection direction relates to the first tripwire point created, the direction arrow in the video is *right to left* and the camera triggers events and alarms when it detects movement over the tripwire in that direction.

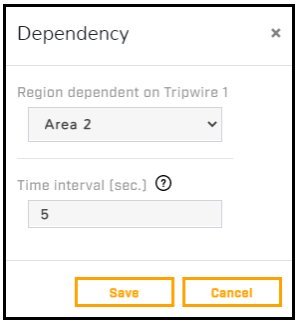


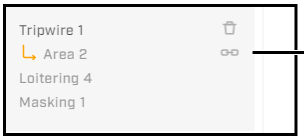
Dependency

After drawing at least two tripwires or detection areas, you can establish dependency between them.

To establish dependency between two regions:

1. Select a region and then click **Set Dependency**.
2. Select the region dependent on the previously selected region.
3. Define the Time interval (sec), the maximum amount of time during which the camera must continuously detect an object in both regions for it to trigger an event / alarm.
4. Click **Save**.





Click to remove dependency

To remove a dependency:

Click the link icon corresponding to the dependent region.

4.9 OSD Page

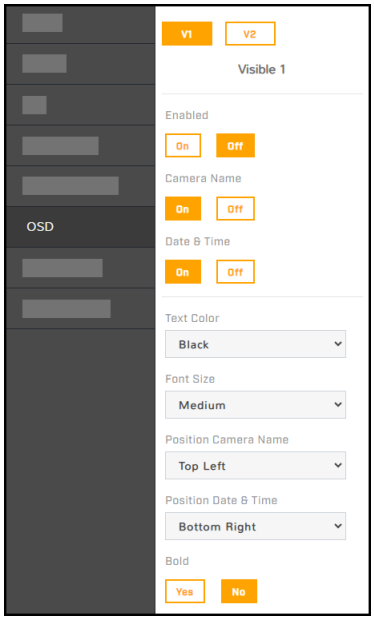
For each IP video stream (V1 or V2), you can:

- Enable or disable the camera's on-screen display (OSD)
- Enable or disable the camera name
- Enable or disable the date & time

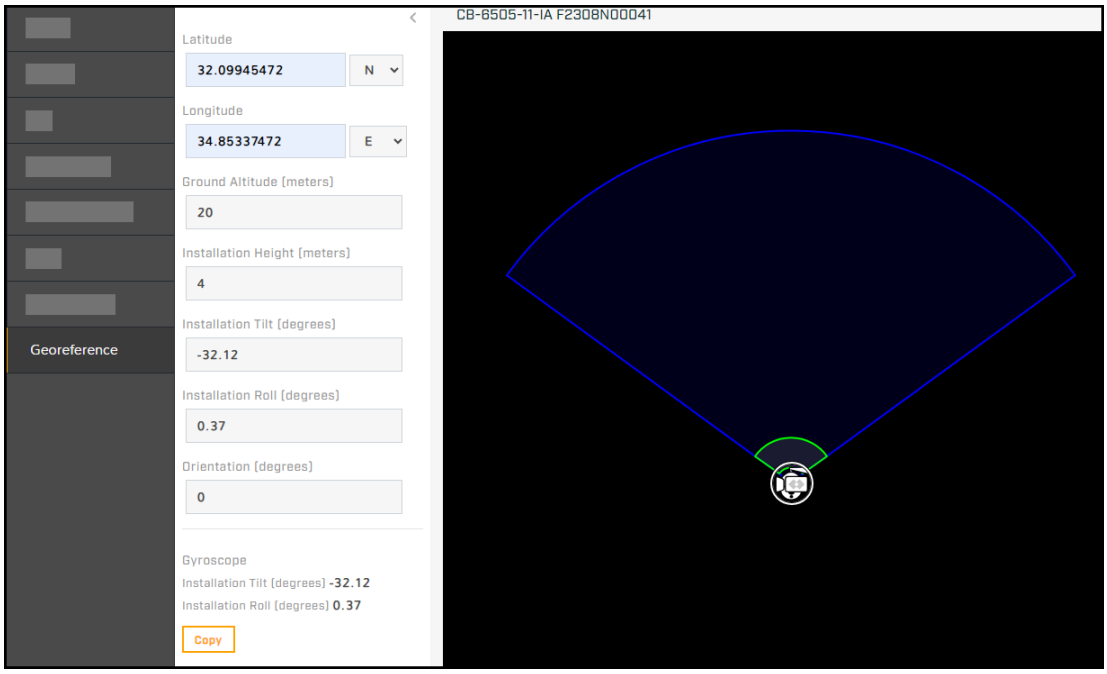
You can also specify:

- **Text Color**—Black or white, with or without a background
- **Font Size**—Small, medium, big, or giant
- **Position Camera Name**—Top or bottom; left, center, or right
- **Position Date & Time**—Top or bottom; left, center, or right
- **Bold text**

When OSD is enabled for the V1 or T1 stream, the OSD appears in the live video on the camera web page. Enabling OSD on the V2 stream does not affect the live video on the camera web page.



4.10 Georeference Page



On the Georeference page, you can specify the camera's geographical location and mounting information.

Pairing a Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics with a FLIR Security PTZ camera that supports geotracking requires proper and accurate georeference configuration. For more information about how to pair one or more Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics with a FLIR Security PTZ camera that supports geotracking, see the corresponding pairing guide of the PTZ camera.

- **Latitude**, in degrees North or South
- **Longitude**, in degrees East or West

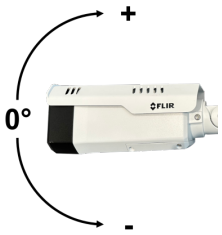
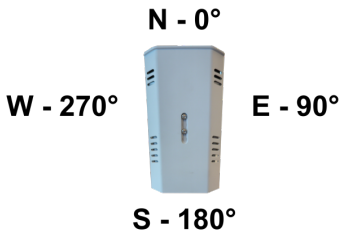
Retrieve the camera's latitude and longitude coordinates by:

- Right-clicking on the display and then selecting **Georeference Sensor**.
- Manually specifying the coordinates, up to eight decimal places. To obtain the camera's latitude and longitude, you can use a map or a mobile GPS device.

The camera immediately applies changes to the latitude and longitude settings. If a reference map has been uploaded and properly calibrated on the Map Page in System Settings, the camera icon moves accordingly. However, the camera does not automatically save these changes and does not move the detection range overlay. To save the changes, click **Save**. If you do not save changes within a few seconds, the camera restores the previous latitude and longitude settings, and moves the camera icon back.

- **Ground Altitude**, in meters above or below sea level, up to two decimal places.
- **Installation Height**, in meters above the ground, up to two decimal places (must be greater than zero).

You can copy the camera's installation tilt and installation roll angles from the camera's onboard gyroscope.

Installation Tilt	Installation Roll	Orientation
The vertical angle of the camera, up to three decimal places. When a camera is pointing down (below horizontal), the tilt angle is negative.	The horizontal rotation angle of the camera, up to three decimal places. Facing a camera leaning to the right, the roll angle is negative.	The direction the camera is pointing, between 0-360 degrees from North, up to two decimal places. For geotracking, this value must be accurate and precise.
		

Tips

- Teledyne FLIR recommends mounting the camera horizontally level; that is, with a 0º installation roll angle. For accurate video analytics, mount the camera with an installation roll angle within ±5º.
- The camera's configuration files do not store factory default Georeference settings. To restore Georeference settings to the camera's factory condition, manually change them to zero (0).

The camera can report georeference information via FLIR CGI or ONVIF, which:

- Allows the user or an application to show the camera on a map and the direction the camera is facing, along with the camera's detection range.
- Supports cueing or showing tracks and I/O alarms.

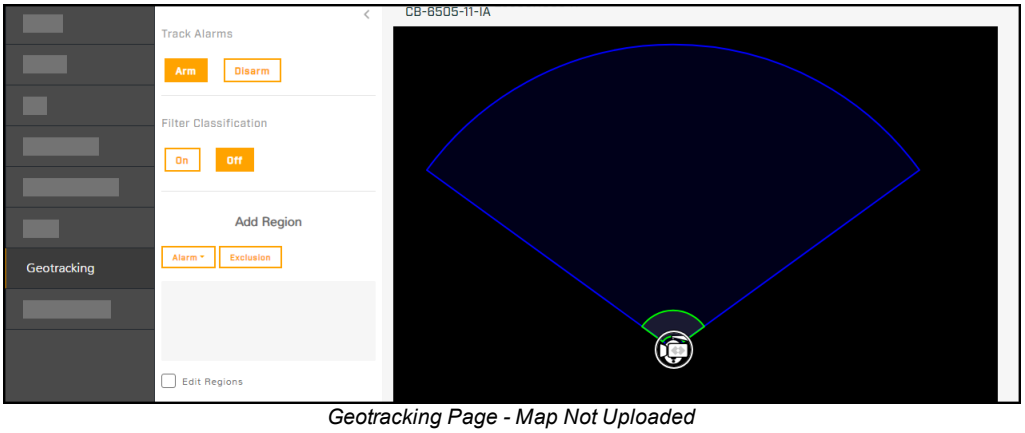
4.11 Geotracking Page

On the Geotracking page, you can enable (Arm), configure, and disable (Disarm) geotracking.

You can pair one or more Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics with a FLIR Security PTZ camera that supports geotracking. When the cameras are paired, the PTZ camera engages the geotracks from the Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics. For information about how to pair cameras, including how to configure the PTZ camera when it is paired, see the corresponding pairing guide of the PTZ camera.

Important

Before enabling geotracking, make sure that the camera's video analytics are enabled on the Video Analytics Page. However, even though geotracking requires the camera's video analytics to be enabled, geotracking configuration is separate from video analytics configuration.



Geotracking Page - Map Not Uploaded

The following appear in the Geotracking / Georeference Page page display, when present:

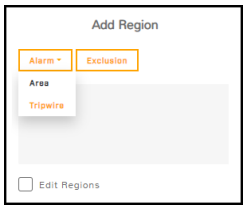
Icons and Descriptions			
	Fixed camera—The circle around this icon indicates the Quasar Premium BulletCamera with FLIR Edge AI Video Analytics you are currently configuring.		Geotracking alarm region
	PTZ camera		Geotracking exclusion region
	Radar		Detected object
	Geotracking range		Detected object in alarm region
	Video analytics detection range		Object engaged by PTZ camera

When a map has been uploaded and calibrated on the Map Page and the camera's georeference settings have been properly configured on the Georeference Page, the map appears in the display.

Filter Classification—When On, the camera generates geotrack information only for objects that the video analytics have classified as a person (P) or vehicle (V).

To add a geotracking region:

1. Click one of the Add Region options.

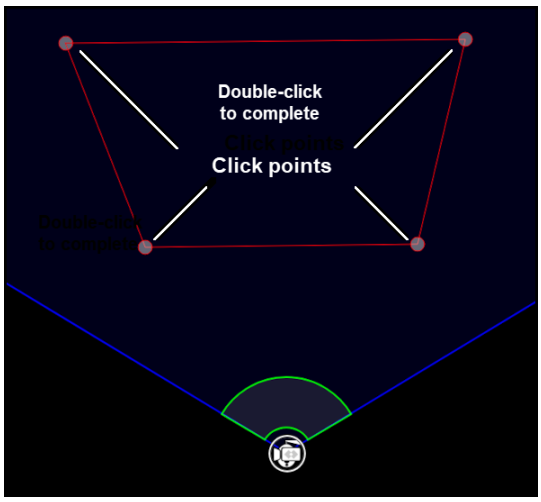


   Alarm (Areas or Tripwires)—Regions where the camera generates geotracking alarms. In the detection area display, the borders of these regions and detected objects appear in red. When a Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics is paired with a FLIR Security PTZ camera that supports geotracking, you can specify that the PTZ camera only engages geotracking alarm tracks.

   Exclusion—Regions where the camera's video analytics does not detect objects and does not generate geotracking alarms. In the detection area display, the borders of these regions appear in yellow. Exclusion regions can help eliminate alarms from a tree or bush moving in the wind, for example.

2. Create the first point of the region. Click and release on the detection area display.
3. Continue adding points (up to 25).
4. Complete the region. Double-click on the detection area display.

   To cancel creating a region, press **Esc**.
5. To define another region, repeat steps 1-4.

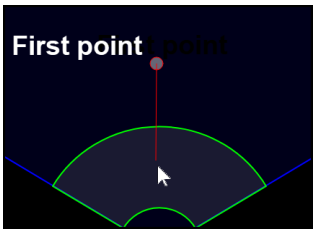


Managing Regions

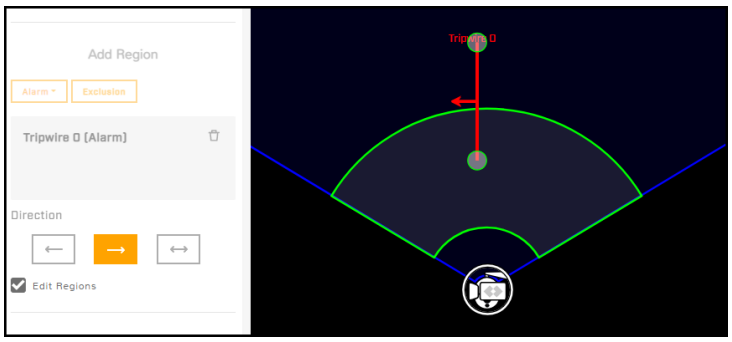
To edit an existing region, select **Edit Regions**, and click the region. You can:

- Move region points. Click on the point, hold, and drag.
- Define a tripwire's detection direction.

  By default, tripwires are bidirectional. However, you can configure them to be unidirectional. When configured as unidirectional, the direction selection arrows refer to the direction of movement over the tripwire *as seen from the first tripwire point created*.



At left, the first point of a tripwire has been defined and the tripwire is being drawn from top to bottom. Below, the tripwire has been completed and the left-to-right direction button has been selected. Because detection direction relates to the first tripwire point created, the direction arrow in the display is right to left and the camera triggers alarms when it detects movement over the tripwire in that direction.



When Edit Regions is selected, it is not possible to add regions.

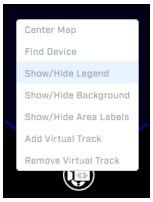
To delete a region, select the region and click the trash can icon next to it.

Tips

- To move the display, and to zoom in and out, you can use the mouse. To move the display, click on the display, hold, and drag. To zoom in or out, use the mouse scroll wheel.

Tips (continued)

- Right-click on the display to:
  - **Center Map—**If uploaded and calibrated, centers the map in the display.
  - **Find Device—**Centers the camera in the display. When the camera does not appear in the display window, select **Find Device**. For example, after you save the camera's coordinates or calibrate a map, the camera's position can be outside the display window.
  - **Show/Hide Legend—**Toggles the display legend.
  - **Show/Hide Background—**Toggles the map or other background image.
  - **Show/Hide Area Labels—**Toggles area labels in the display. For example, in the image above, the Tripwire 0 area label appears.
  - **Add/Remove Virtual Track—**Toggles a virtual geotrack that you can use to test features such as PTZ pairing and geotracking.



These right-click options are also available on the Georeference Page display.

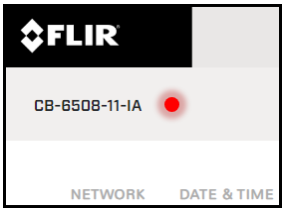
5 Configuration

Users assigned the admin or expert role can click **System Settings** on the View Settings Home Page to access the following configuration pages:

- Settings
- Date & Time Page
- Users Page
- Alarm Page
- Audio Page
- I/O Devices Page
- Messaging Page
- Heaters & Fans Page
- Cyber Page
- Media Browser Page
- Map Page
- Scheduler Page
- Recording Page
- SD Card Page
- Firmware & Info Page

In System Settings, a pulsating red button next to the camera name indicates the camera is currently recording live video to an installed and configured microSD card.

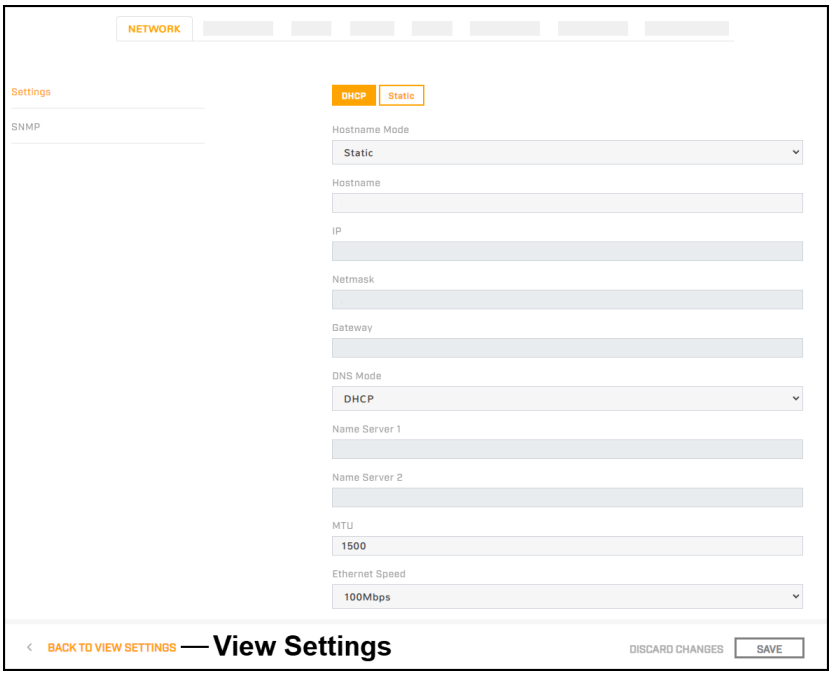
For information about making, apply, and saving changes on System Settings pages, see Making Changes to Settings.



Recording Indicator

5.1 Network Page

The Network page provides networking and SNMP settings.



View Settings

If you do not know how to configure these settings, contact your network administrator.

5.1.1 Settings

The DHCP (default) and Static buttons at the top of the page specify the IP addressing mode. If the IP addressing mode is set to DHCP but a DHCP server is not available on the network, the camera's IP address defaults to 192.168.0.250.

In Static IP addressing mode, specify:

- **IP**—The camera's IP address.

> **Caution**
>
> After changing the camera's IP address, the PC you are using to access the camera's web page might no longer be on the same network as the camera and can no longer access the camera's web page. To access the camera web page again, change the PC's IP address to be on the same network as the camera.

- **Netmask**—The default value is 255.255.255.0.
- **Gateway**

The Hostname Mode can be set to DHCP or Static (default); if set to Static, specify the hostname for the camera's server.

- **DNS Mode**—When the IP address mode is DHCP, you can set the DNS Mode to DHCP or Static. When the IP address mode is Static, the DNS Mode is also Static.

  When the DNS Mode is set to Static, specify:

  - **Name Server 1**—The primary domain name server that translates host names into IP addresses.
  - **Name Server 2**—A secondary domain name server that backs up the primary DNS.

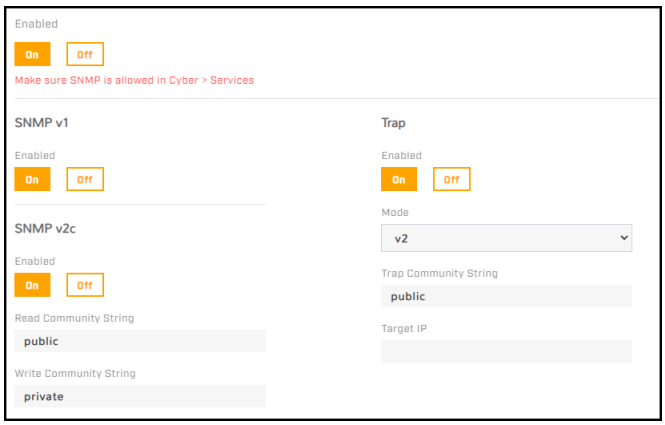
You can also specify the:

- **MTU**—Maximum transmission unit, the largest amount of data that can be transferred in one physical frame on the network. For Ethernet, the MTU is 1500 bytes (the default setting). For PPPoE, the MTU is 1492. Valid values are 1000-1500.
- **Ethernet Speed**—When set to 100Mbps (default), the camera supports 100 Mbps. When set to Auto, the camera supports 10/100/1000 Mbps. Teledyne FLIR recommends 100 Mbps.

5.1.2 SNMP

In the SNMP section, you can enable and configure SNMP (Simple Network Management Protocol). SNMP allows network management systems to monitor and to remotely manage the camera. By default, all SNMP features are disabled.

> **Important**
>
> - For cybersecurity reasons, change the default community strings.
> - If you are enabling SNMP, on the Cyber page, make sure SNMP is enabled.



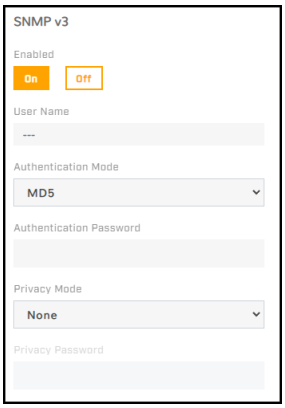
SNMP v1—Enable SNMP v1.

SNMP v2c

After enabling SNMP v2, specify:

- **Read Community String—**Name of community that has read-only access to all supported SNMP objects. The default value is *public*.
- **Write Community String—**Name of community that has read/write access to all supported SNMP objects (except read-only objects). The default value is *private*.

SNMP v3



SNMP v3 provides security features including:

- **Confidentiality—**Packet encryption prevents snooping by unauthorized sources.
- **Message Integrity—**Ensures that packets have not been tampered with in transit, including an optional packet replay protection mechanism.
- **Authentication—**Verifies the message is from a valid source.

After enabling SNMP v3, specify:

- **User Name—**Name of user on network management system using SNMP v3.
- **Authentication Mode—**Select None, MD5 (default), or SHA.
- **Authentication Password—**Password for authentication on network management system.
- **Privacy Mode—**Select None (default), DES, or AES.
- **Privacy Password—**Password for privacy on network management system.

Trap

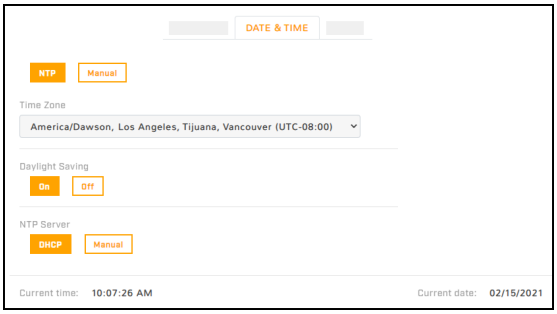
The camera uses traps to send messages to the network management system for important events or status changes. After enabling traps, specify:

- **Mode—**Specify v1, v2, or v3.
- **Trap Community String—**Name of community camera uses when sending traps to the network management system. The default value is *public*.
- **Target IP—**IP address of the network management system server.

5.2 Date & Time Page

By default, the camera synchronizes its date, time, and time zone with an NTP server.

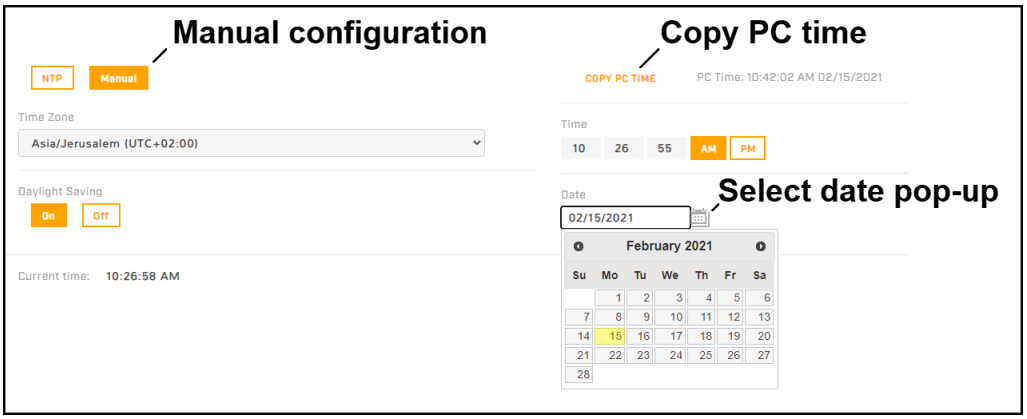
When DHCP IP addressing is enabled on the Settings, you can configure the camera to obtain the NTP server information from the DHCP server.



To manually specify one or more NTP server addresses, under NTP Server, click **Manual** and specify the address(es). Use a comma to separate addresses.

To manually configure the camera's time zone, time, and date:

1. At the top of the page, click **Manual**.
2. Specify the time zone and whether it is currently daylight saving time.
3. Copy the local PC's time or specify the hour, minute, second, AM or PM, and date.



Tip

Email notifications and other camera features require configuring the camera's system time to be the current time. You can configure email notifications on the Messaging Page.

5.3 Users Page

Only users assigned the admin role can add users and change or set passwords. It is not possible to change the role of the default admin user.

Users assigned the expert role only see the user currently logged in, and cannot add, edit, or delete a user.

To maintain security of the system, set up user names and passwords for each required login account.

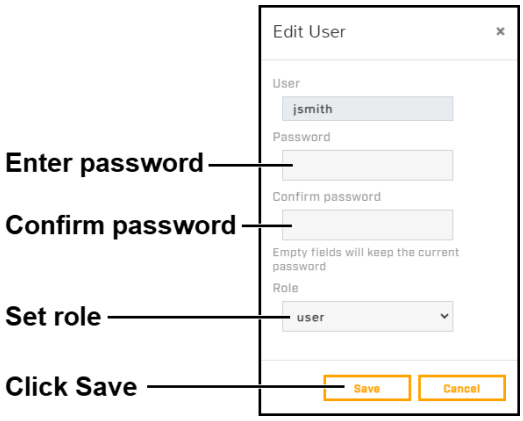
The camera limits user name length to 29 characters. Passwords must be at least 12 characters; must contain at least one number, one lowercase letter, and one uppercase letter; and can include the following special characters: |@#~!$&<>+_-.,*?= .

Assign one of the following roles, according to the level of access the user requires:

Role	user	expert	admin
Access	Can: • View live video • View the Help page • Log out	Can access and use all View Settings and System Settings pages, menus, controls, and settings, except the Users page.	Can access and use all of the camera's web pages, including the Users page (but cannot delete the default admin user).
	When the camera's video streams require RTSP authentication, accessing the camera's video streams requires the name and password for any camera user. All roles provide access to the camera's video streams.		

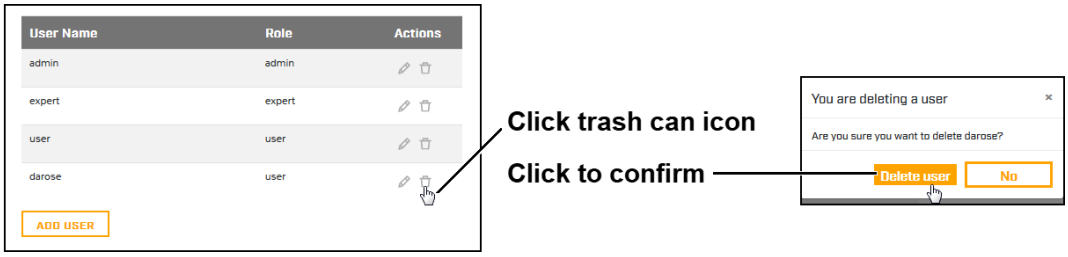
Add User

Edit User



To keep the existing password, leave the password fields empty.

Delete User



5.4 Alarm Page

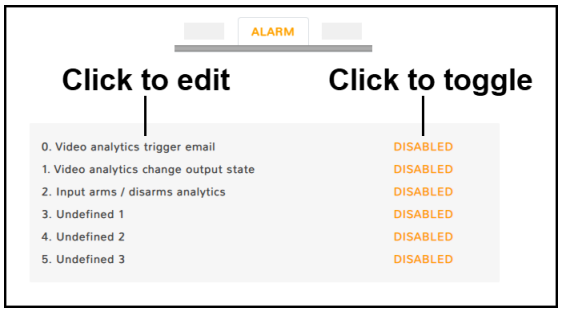
You can define camera alarms to be triggered by the following:

- The camera's onboard video analytics
- VA from a supported remote camera or other device
- Radiometry from a supported remote camera or other device
- A supported geotracking device; for example, a radar
- Local or external I/O connections

For each alarm, you can specify one or more of the following actions:

- Record a snapshot image of live video
- Send a notification email
- Arm/disarm the camera's VA (available when Video Analytics is not the rule's trigger)
- Change the state of local or external I/O connections

By default, the following rules are defined and disabled:



- **0. Video analytics trigger email**—The camera's VA triggers a notification email. Set up and configure the messaging settings on the Messaging Page.
- **1. Video analytics change output state**—The camera's VA triggers a change to the state of an local alarm output connector. If the idle state of the connector is Closed, the alarm changes the state to Open. Likewise, if the idle state is Open, the alarm changes the state to Closed. For information about configuring the idle state of the camera's local I/O connector pins, see I/O Page.
- **2. Input arms / disarms analytics**—Changes in the state of the local alarm input connector enable or disable the onboard VA.

You can modify the name, trigger, and action for the default rules. For example, you can modify the **Video analytics changes output state** rule so that it changes the state of an external output connected VMS system, instead of the state of an alarm out local I/O connector.

You can also define and enable three additional rules (**3. Undefined 1**, **4. Undefined 2**, and **5. Undefined 3**).

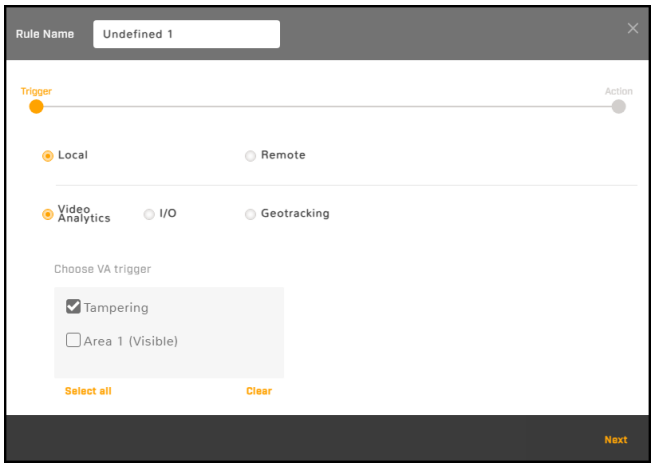
You can use the ID number identifying each rule (0-5) to schedule a task that switches alarm rules on or off. For more information, see Scheduler Page.

To modify an existing alarm rule or define an alarm rule:

1. Click the alarm name. The rule trigger settings appear.
2. Modifying or Defining Rule Triggers
3. Modifying or Defining Rule Actions

Enable or disable a rule by clicking **Enabled** or **Disabled**.

5.4.1 Modifying or Defining Rule Triggers



Rule Trigger Settings
Local - Video Analytics - Tampering Selected

To modify or define alarm rule triggers:

1. Modify or define the rule name.
2. Select whether the triggers are local (onboard the camera) or remote (external).

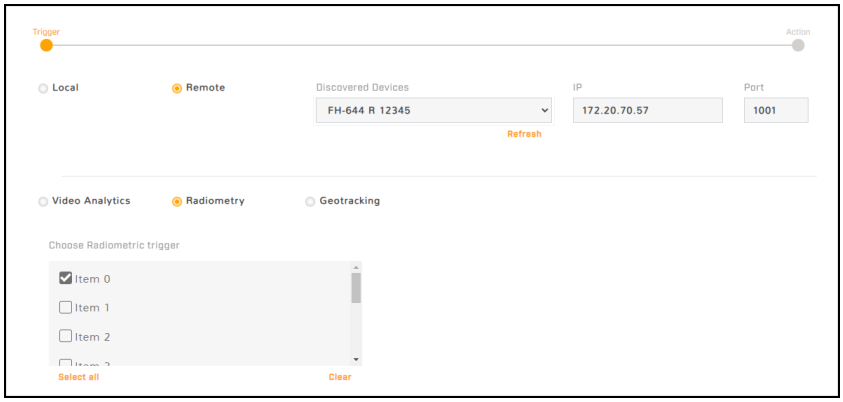
Local Triggers		
Video Analytics	This Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics onboard VA triggers this rule's action.	a. On the Video Analytics Page, make sure tripwires and intrusion detection / loitering regions have been defined. b. Select the tripwires and regions that trigger this rule's action. After the camera has been powered on for 24 hours, blocking the sensor of the camera for one minute triggers this rule's action.
I/O	**Local—**This camera's local I/O connections trigger this rule's action.	a. On the I/O Page, make sure local I/O connectors have been properly configured. b. Select one or more local I/O connections that trigger this rule's action.
	External—This camera's external I/O connections trigger this rule's action.	a. On the I/O Page and on the I/O Devices Page, make sure the external I/O connections and the device managing those connections with the camera have been properly configured. b. Select one or more external I/O connections that trigger this rule's action.

Tip

Specifying a trigger for an alarm rule and enabling the rule does *not* enable alarms for the trigger. Make sure VA has been enabled.

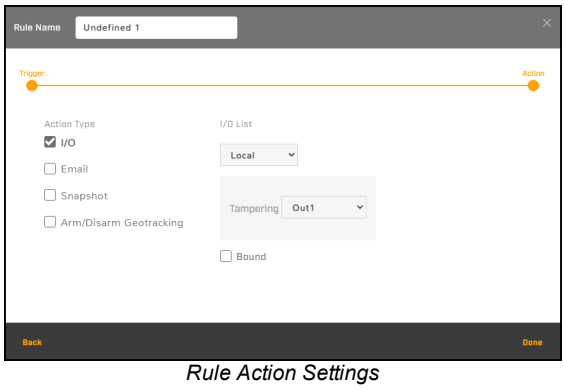
Remote Triggers		
Under Discovered Devices, select the remote camera, radar, geotracking device, or other device from the drop-down menu of supported devices on the same network as the camera; its IP address and port appear. You can also manually specify the remote device IP address and port, and then click **Refresh** to save it. Clicking **Refresh** also refreshes the drop-down menu of discovered devices. For example, if you just connected the remote device to the same network as the camera. **Note** The camera discovers supported devices on the same network as the camera. However, to be used as a trigger, the device must be on the same VLAN as the camera.		
Video Analytics	VA from a supported remote camera or other device triggers an alarm.	a. On the remote camera or other device, make sure VA is enabled and that at least one tripwire, intrusion detection / loitering region, or another VA item has been defined. b. Select one or more VA items that trigger this rule's action.
Radiometry	Radiometry from a supported remote camera or other device triggers an alarm.	a. On the remote camera or other device, make sure radiometry is enabled and that at least one radiometric item has been defined. a. Select one or more radiometric items that trigger this rule's action.
Geotracking	A remote geotracking device triggers an alarm.	a. On the remote geotracking device, make sure detection is enabled and that at least one alarm area, tripwire, or other area has been defined. b. Select one or more geotracking device areas that trigger this rule's action.

The following image shows a discovered FH-Series R camera selected as the remote device and its radiometric item 0 selected as the trigger.



3. Click **Next**. The rule action settings appear.
4. Continue with Modifying or Defining Rule Actions.

5.4.2 Modifying or Defining Rule Actions



Rule Action Settings
Tampering Trigger - Local I/O Out1 Selected

To modify or define alarm rule actions:

1. For the alarm rule you are modifying or defining, select the checkbox for one or more action type.
2. To configure an action type, click the selected action type. The selected action type appears in **bold**, and the relevant settings appear.

Action Type	
I/O	Under I/O List, select Local or External.
	Local—This rule changes the state of the local output (Out1). a. On the I/O Page, make sure local I/O connectors have been properly configured. b. For each trigger defined for the alarm rule, select Out1.
	External—This rule changes the state of one or more external output pins. a. On the I/O Page and on the I/O Devices Page pages, make sure the external I/O connections and the device managing those connections with the camera have been properly configured. b. For each trigger defined for the alarm rule, select an external output pin.
	Tip You can map individual local or remote triggers to specific local or external outputs.
	Bound—When selected, the camera changes the state of the output when the alarm is triggered and when it is cleared. When not selected, the camera changes the state of the output when the alarm is triggered. However, the output state remains changed until it is reset according to the configured Reset Interval or by a command from the network. You can configure the Reset Interval for the local output on the I/O Page and for the external output pins on the I/O Devices Page.
Arm/Disarm Analytics (not available when this rule's trigger is Video Analytics)**—**When triggered, this rule toggles the camera's onboard VA between enabled and disabled.	
Email—When triggered, this rule sends a notification email according to the settings on the Messaging Page. Specify a subject for the email and whether the camera attaches to the email a snapshot image of live video.	
Snapshot—When triggered, this rule records a snapshot image of live video.	
Arm/Disarm Geotracking (not available when this rule's trigger is Geotracking)**—**When triggered, this rule toggles the camera's geotracking between enabled and disabled.	

3. Click **Done**.

5.5 Audio Page

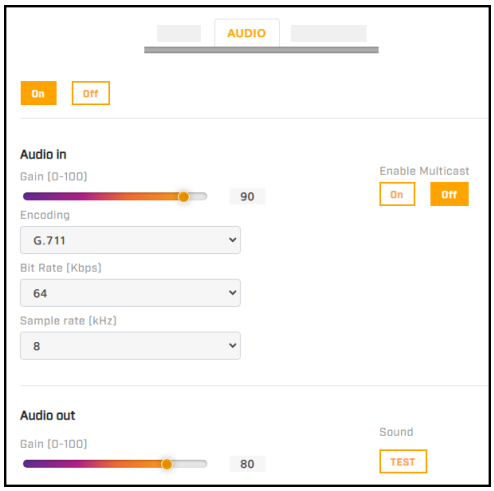
The Audio page provides configuration settings for and information about the camera's audio input and output features.

The On/Off buttons affect all audio input and output. For example, turning audio off immediately turns off all camera audio.

Audio In

When audio is On, the following audio input settings appear:

- **Gain**—You can adjust the audio input gain from 0-100 percent. The default is 90 percent.
- **Encoding**—G.711.
- **Bit Rate**—The camera supports an audio input bit rate of 64 kilobits per second (kbps).
- **Sampling Rate**—The camera supports a sample rate of 8 kHz.
- **Enable Multicast**—Can be set to On or Off (default). When On, specify the destination address and port, and the time-to-live (TTL).



Audio Out

When audio is On, you can adjust the audio line output gain from 0-100 percent. The default is 80 percent.

Tips

- Test whether the camera's audio output is functioning properly by clicking **Play**.
- If you are monitoring the audio IP output with a video stream and change any of the audio configuration settings except gain, restart the stream. For example, if you are monitoring a video stream and turn audio on, you need to restart the stream to hear the audio with the stream.

5.6 I/O Devices Page

On the I/O Devices page, you can configure the camera's external I/O connections and the device managing those connections with the camera.

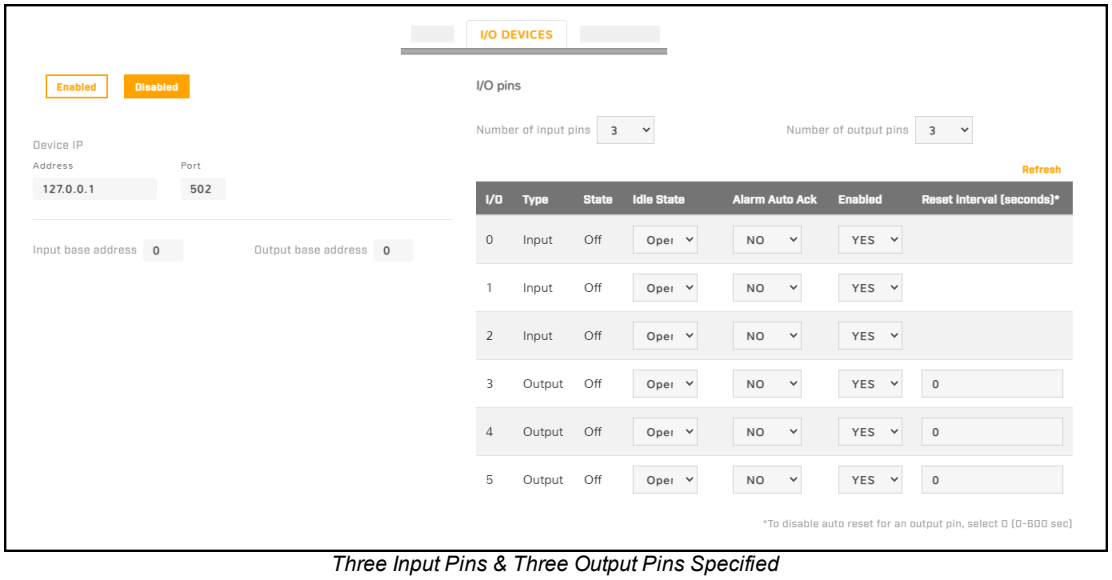
You can configure the following for the device managing the external I/O connections:

- **Enabled or Disabled**
- **Device IP address and port**
- **Input and output base addresses**
- **The number of input and output pins the device manages**

  By default, six input pins and six output pins are specified.

For each pin, the following information appears and you can confgure:

- **I/O pin number**
- **Type**—Input or Output
- **State**—the pin's current state: Off or On
- **Idle State**—Open or Closed
- **Alarm Auto Ack**—Yes or No
- **Enabled**—Yes or No
- **Reset Interval (for output pins only)**—between 0-600 seconds; to disable auto reset for an output pin, select 0



Three Input Pins & Three Output Pins Specified

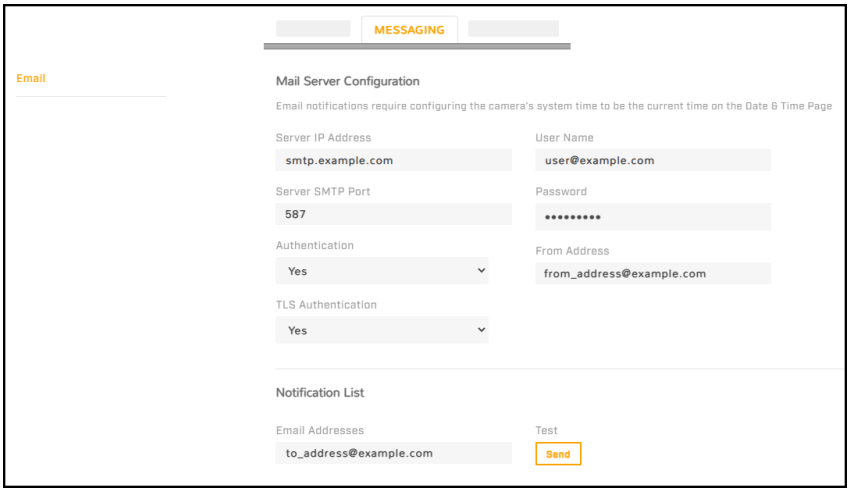
For more information about how to configure the device managing the external I/O connections, refer to the device's documentation.

5.7 Messaging Page

As an action for an alarm rule, the camera can send a notification email using the mail server settings you can configure on the Messaging page.

Specify the settings for the SMTP server in the appropriate fields. Settings include the SMTP server's IP address; port (the default port is 587); user name and password for the account on the mail server; whether the mail server requires authentication or TLS authentication; and the email address from which the camera sends the notification emails (also known as the reply-to address). If you do not know the mail server's settings, contact your mail server administrator.

Under Notification List, specify one or more email addresses, separated by commas, to receive the notifications.



Tip

For the camera to properly send email, the camera's date and time must be correctly configured on the Date & Time Page.

5.8 Heaters & Fans Page

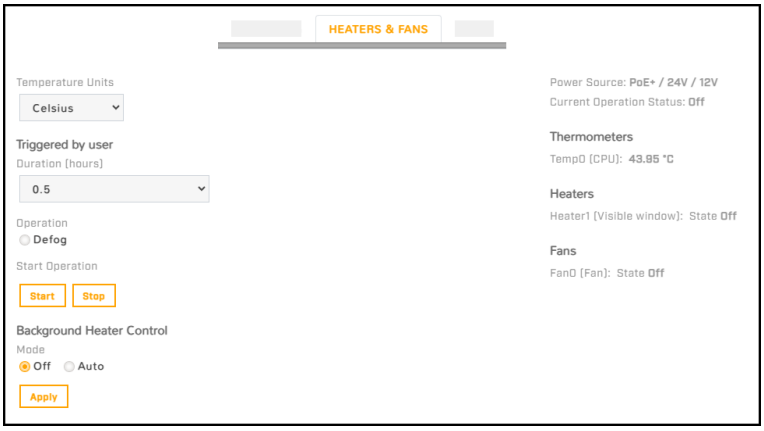
The Heaters & Fans page provides defogging and background heating controls, and information about the camera's CPU temperature, heater, and cooling fan.

Select the units of temperature that appear on the page: Celsius (default), Fahrenheit, or Kelvin.

To manually activate defogging:

1. Under Triggered by user, select the Duration (0.5, 1, or 2 hours).
2. Select **Defog**.
3. Click **Start**. The state of the heater changes from Off to On.

To deactivate defogging, click **Stop**.



Background Heater Control

By default, the background heater control is set to Off. Teledyne FLIR strongly recommends selecting Auto.

Status Information

Down the right side of the Heaters & Fans page, the following information appears:

- **Power Source—**PoE+ / 24V / 12 V.
- **Current Operation Status—**Current background heater control setting (Off or Auto).
- **Thermometers—**Temperature of the camera's CPU.
- **Heaters—**State of the camera's heater (On or Off).
- **Fans—**State of the camera's cooling fan (On or Off).

5.9 Cyber Page

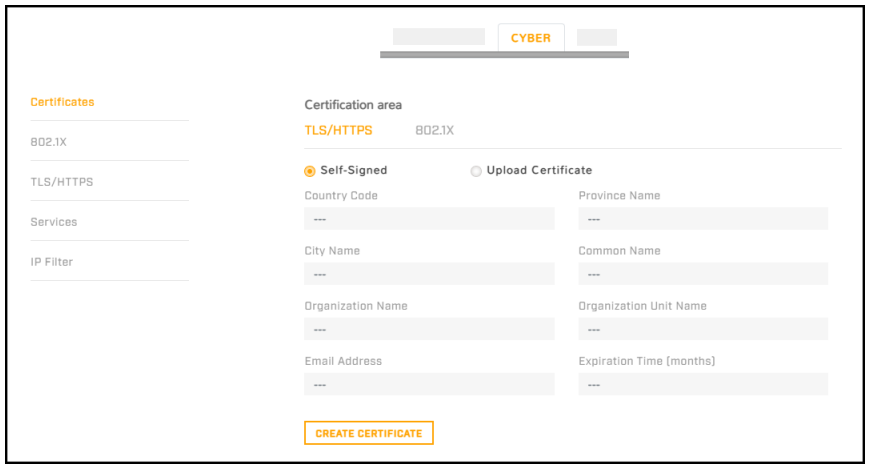
The Cyber page provides security configuration settings for:

- Certificates
- 802.1X
- TLS / HTTPS
- Services
- IP Filter

If you do not know how to configure these settings, contact your network administrator.

5.9.1 Certificates

Before you can enable TLS/HTTPS or 802.1X, you need to generate or upload a valid certificate. You can use the camera's web page to generate a self-signed certificate; upload a self-signed certificate; or upload a certificate signed by a third-party. If you do not know how to configure these settings, contact your network administrator.



Certificates and keys must be in PEM format. Common file extensions for TLS files in PEM format are:

- **For certificate and public key files:** *.crt, *.cer, *.cert, *.pem
- **For private key files:** *.key

From the Certificates section of the Cyber page, you can download certificates and keys previously uploaded to or generated by the camera. If the certificate saved on the camera is self-signed, you can download the private and public key files. If the certificate was signed by a third-party CA, you can download the CA Certificate and the private and public key files.

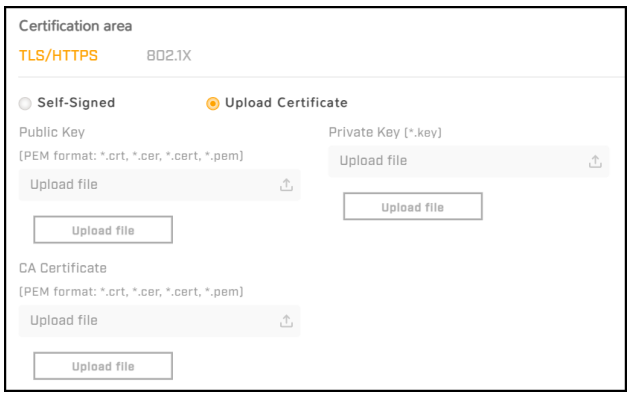
To generate and install a self-signed certificate for TLS/HTTPS:

1. In the Certificates section and Certification area, select **TLS/HTTPS** and **Self-Signed**.

2. Enter information such as country code, city name, and organization name.
3. Click **Create Certificate**.
4. Allow 15 seconds for the camera to generate the certificate, at which point a confirmation appears.

To upload a self-signed or third-party CA signed certificate for TLS/HTTPS or for 802.1X:

1. In the Certification area, click **TLS/HTTPS** and then select **Upload Certificates**, or click **802.1X**.



To Upload a Certificate for TLS/HTTPS

To Upload a Certificate for 802.1X

2. If you are uploading a self-signed certificate, under **Public Key** and then under **Private Key**:
   a. Click

.
   b. Select the appropriate key file.
   c. Click 

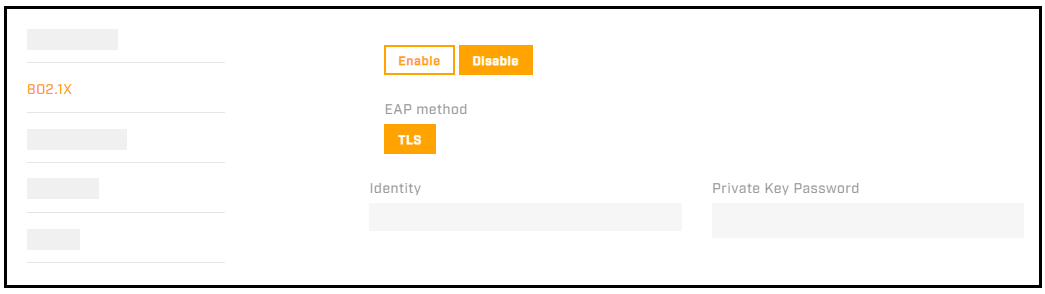
.
   If you are uploading a third-party CA signed certificate, select and upload the Public Key, Private Key, and CA Certificate.
3. Verify that the camera certificate files are valid and make sure *Certificates are OK* appears under the certificate information, under Download certificate.

Note that you can download keys and certificates from the camera.

5.9.2 802.1X

You can enable or disable IEEE 802.1X-compliant TLS communication provide the Identity and the Private Key Password. The default is disabled.

If you do not know how to configure these settings, contact your network administrator.



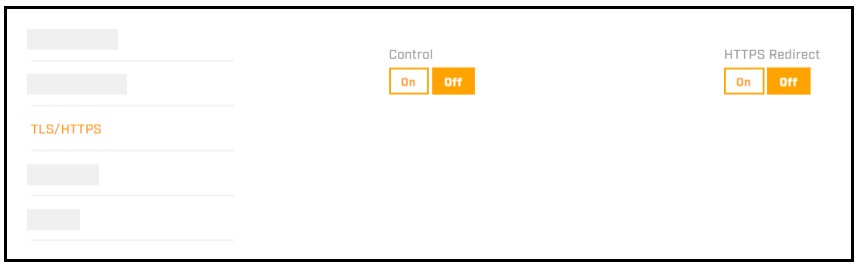
5.9.3 TLS / HTTPS

You can enable or disable:

- camera control using Transport Layer Security (TLS) / secure HTTP (HTTPS)
- HTTPS redirect

For both, the default is disabled.

If you do not know how to configure these settings, contact your network administrator.

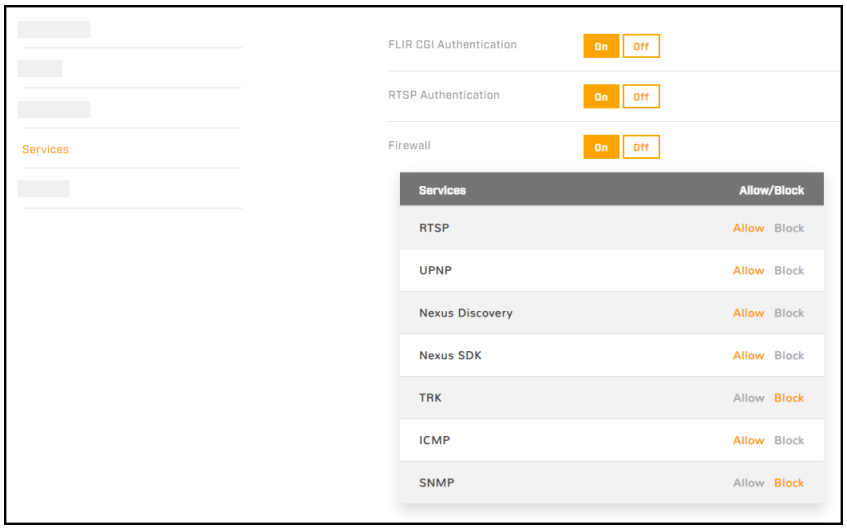


5.9.4 Services

You can enable or disable:

- Digest authentication for the FLIR CGI control interface.
- RTSP authentication. When disabled, accessing the camera's video streams does not require authentication.

The default setting for both settings is On (enabled).



Firewall Settings

For enhanced security, the camera has a firewall that is disabled by default. You can enable it by clicking **On**. By default, when you enable the firewall, the following services are set to **Allow**, which means they remain available and their default ports remain open:

- RTSP
- UPNP
- Nexus Discovery
- Nexus SDK
- TRK
- ICMP
- SNMP

To disable a service and its default port, click **Block**.

Caution

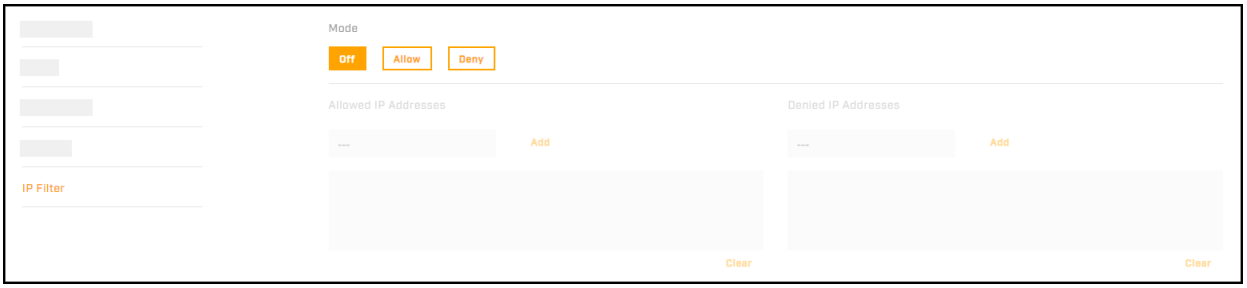
Disabling services and ports can affect product functionality.

If you do not know how to configure these settings, contact your network administrator.

5.9.5 IP Filter

The camera's IP filter can deny or allow access according to specific IPv4 addresses that you define.

By default, the IP filter is disabled (Off).



To define specific IP addresses that can access the camera, click **Allow**. The camera will deny access to all other IP addresses.

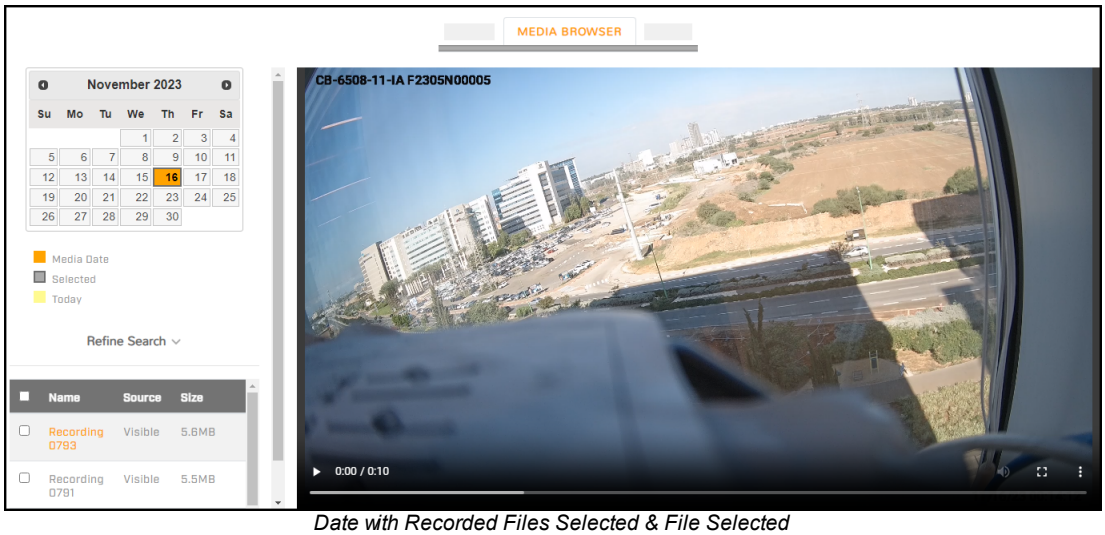
To define specific IP addresses that cannot access the camera, click **Deny**. The camera will allow access to all other IP addresses.

To add an IP address to a list, either under Allowed IP Addresses or under Denied IP Addresses, specify an IPv4 address and then click **Add**. You can specify up to 256 IP addresses.

To remove an IP address from a list, click the corresponding trash icon .

5.10 Media Browser Page

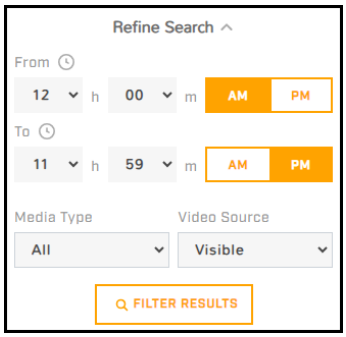
When recorded files exist on a properly installed and formatted microSD card, you can preview and access those files on the Media Browser page.



Date with Recorded Files Selected & File Selected

You can:

- view files by date—orange indicates recorded files exist for that date.
- filter the list by:
  - specific times
  - media type (Snapshot, Video, or All)



When you select a single file, a preview of the file appears, except for video files encoded using H.265.

Tip

Previews of video files do not appear at the full recorded frame rate. To see video files at the full frame rate, and to view video files encoded using H.265, download the files.

After selecting a file, you can download or delete the file. It is not possible to download more than one file at a time.

When you download a file, the default file name format is SOE1-<source>_VIDEO001_<source>_<start_time>_<end_time>_<x>_<yyyyy>.mp4, where:

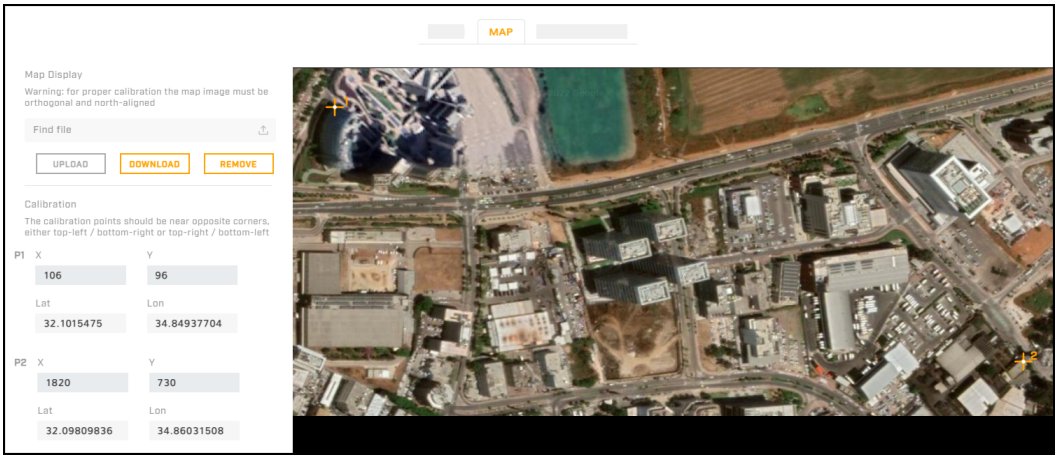
- <source> is the stream recorded—V1 / V2.
- <start_time> and <end_time> are Unix timestamps.

For example, SOE1-V1_VIDEO001_V1_1700982489_1700982789_3_22502.mp4.

5.11 Map Page

On the Map page, you can upload and calibrate a reference map image for geotracking. You can also:

- download a previously uploaded map and its calibration information as a zipped file
- upload a zipped map and calibration file
- remove a previously uploaded map



Map Uploaded and Calibrated

To upload a reference map image and calibrate it:

1. Using an online map or GPS service such as Google Maps, download a reference map image.

For example, if you use Google Maps or another online map, you can take a screenshot of a satellite view of the camera's detection range. In Windows 10, you can use the default keyboard shortcut (Windows logo key + Shift + S) to take the screenshot, paste the screenshot into an image editor (for example, Paint), and then save the image in JPG or PNG format. The size of JPG files are optimized better.

Tips

- When you take the screenshot, make sure that north is straight up in the map image and that the map is flat (2D).
- Use a large, high-resolution screen or display in its native resolution with no zoom. You might get better results taking the screenshot with the map source in full screen (in Google Chrome, press F11). Also, in Google Maps, for example, it might help to turn off labels.
- Keep in mind where the camera is or will be mounted and oriented, and take a screenshot that covers an area a little larger than the camera's maximum detection range.
- The quality and resolution of the map image should be high enough so that the reference map is useful when you zoom in on the detection area display.
- To move the map, and to zoom in and out, you can use the mouse. To move the map, click on it, hold, and drag. To zoom in or out, use the mouse scroll wheel.
- It might take a few attempts at different settings to achieve the best result.

2. Identify two calibration points for which you can obtain accurate and exact latitude and longitude coordinates. For example, intersections of two roads or highways.

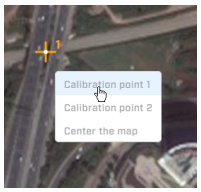
   For optimal calibration, the two calibration points should be as far apart as possible and on opposite sides of the map image. For example, at top-right and at lower-left.

3. Under Map Display, click **Find file**, and then click **Upload**.

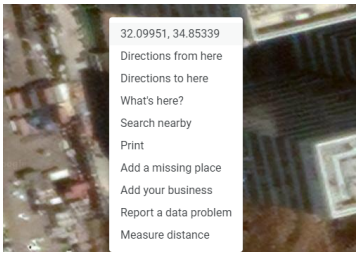
   If the map successfully uploads, a confirmation message appears.

4. Click **Accept**.

   If a map does not successfully upload, try again. Try changing the quality or compression of the map image. Higher quality or lower compression increases the map file size.



Right-Click on Map



Google Maps > Right-Click

5. Right-click on the first calibration point, and then select Calibration point 1.
6. Enter the latitude (Lat) and longitude (Lon) coordinates for the first calibration point (P1). You can obtain the coordinates from the online map or from a GPS service.

   For example, when using Google Maps, right-click on a point and select the coordinates. The point's latitude and longitude coordinates are copied to the clipboard. Paste the coordinates into the P1 **Lat** and **Lon** fields.

   The calibration point appears in the map as a crosshairs icon.

7. Repeat steps 4 and 5 for the second calibration point (P2).

8. Click **Save**.

   The camera calibrates the map. When a map is not calibrated, a message appears onscreen.

Tip

Even though it is not possible to delete an uploaded map image, you can upload a black image and replace the existing map. On the Geotracking Page and on the Georeference Page, information appears on the black image.

If you have not yet configured the camera's georeference settings, you can do so on the Georeference Page.

5.12 Scheduler Page

You can define one-time or recurring tasks, including their start and stop times. For example, you can:

- Enable the camera's onboard VA during certain times of the day.
- Schedule periodic uploads of snapshots of live video images to an FTP/SFTP server.

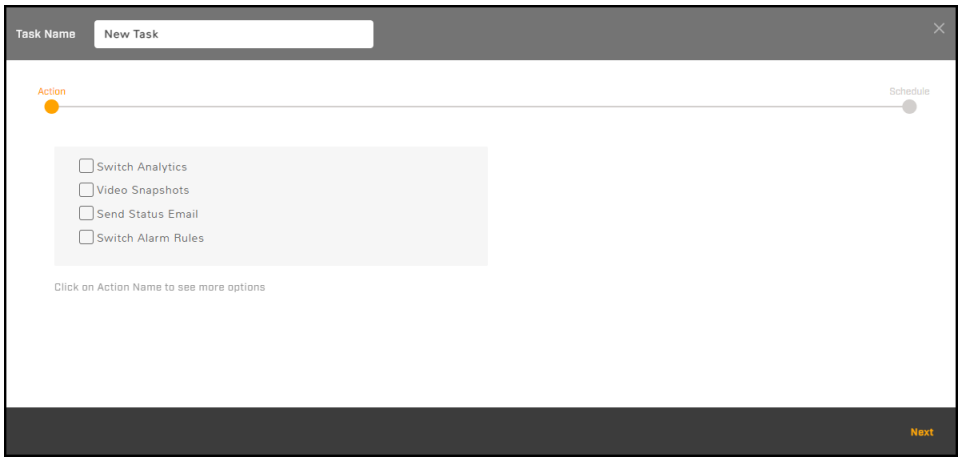
Note

You cannot use the scheduler to define a task that records live video.

By default, no tasks are defined.

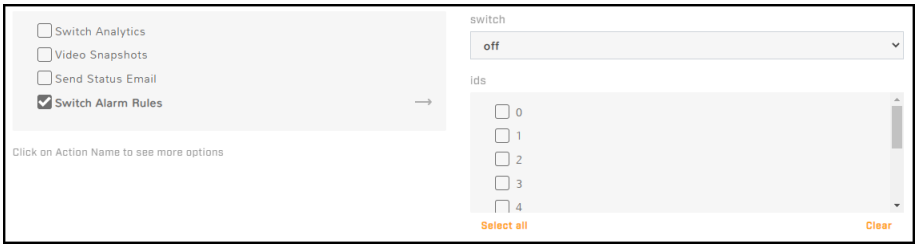
To define a task:

1. Click **Add**. A new task appears. By default, it is enabled.
2. Click **New Task**. The task action settings appear.

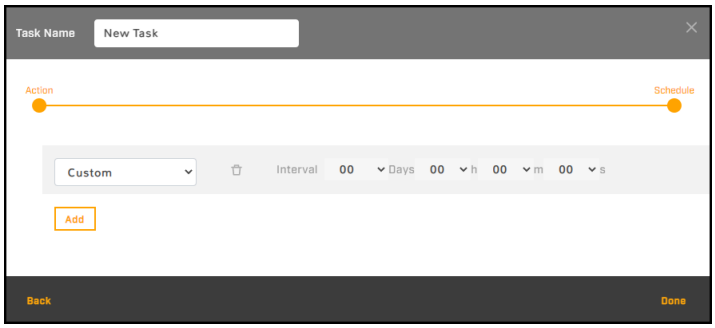


3. Define the task name.
4. Select the checkbox for one or more predefined actions.
5. To configure a predefined action, click the selected action. The selected action appears in **bold**, and the relevant settings appear.

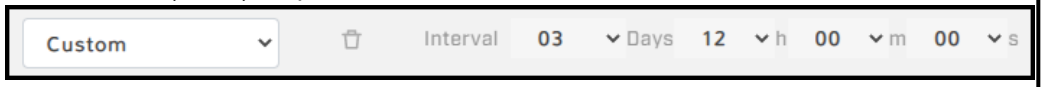
Predefined Actions	
Switch Analytics	Select whether the task disables the camera's onboard VA (off) or enables it (on).

Predefined Actions	
	
Video Snapshots	Records live video snapshots according to settings configured on the Recording Page, and, if supported, according to settings configured by using FLIR UVMS, an approved third-party VMS, or another ONVIF-compliant client.
Send Status Email	Sends an email with information about the camera's status, according to the settings on the Messaging Page.
Switch Alarm Rules	a. Select whether the task disables (off) or enables (on) alarm rules.  b. Select the alarm rules the task affects, according to rule ID number. To determine the rule ID, check the Alarm Page.

6. Click **Next**. The task schedule settings appear.



7. From the drop-down list, select the first schedule for the task.

Schedule	
Custom	Define the task interval in days, hours, minutes, and seconds. For example, to schedule a task to run every three and a half days, select 03 from the Days drop-down list and 12 from the h (hours) drop-down list: 
Hourly	Define the time, in minutes and seconds past the hour, for the task to run every hour. For example, to schedule a task to run at :15 every hour, select 15 from the h (hours) drop-down list.
Daily	Define the time of the day for the task to run. Define the hour according to the 24-hour clock, and the minute and second past the hour.
Weekly	1. Define the time of the day for the task to run. 2. Either select the day of the week for the task to run, or select All days.
Monthly	Define the day of the month and the time of day for the task to run.

Schedule	
Yearly	Define the month, day of the month, and time of day for the task to run.

Tip

You can define more than one schedule for a task. For example, if you want to schedule an action for every Monday at 08:00 and for midnight on the first of every month:

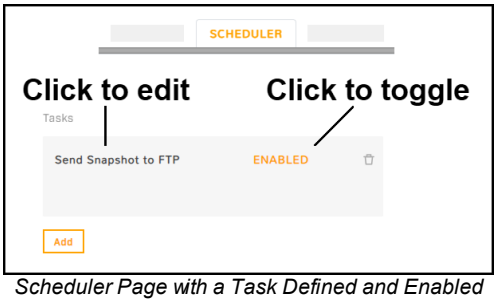
a. Define the 08:00 Mondays weekly schedule.
b. Click **Add**.
c. Define the first-of-every-month monthly schedule.

8. Click **Done**.

Note

When you click **Done**, new tasks and changes to tasks immediately take effect. Unless you have made other changes on the Alarm page, clicking **Save** is not necessary.

Enable or disable a task by clicking **Enabled** or **Disabled**. To delete a task, click the corresponding trash icon .

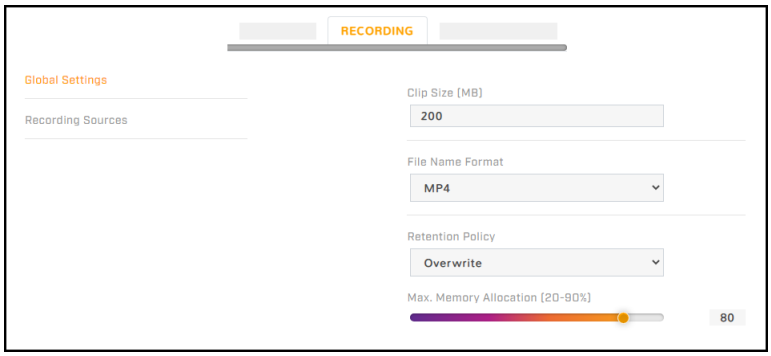


Scheduler Page with a Task Defined and Enabled

5.13 Recording Page

On the Recording page, you can configure:

- Global video clip recording settings
- Recording sources



Global Settings

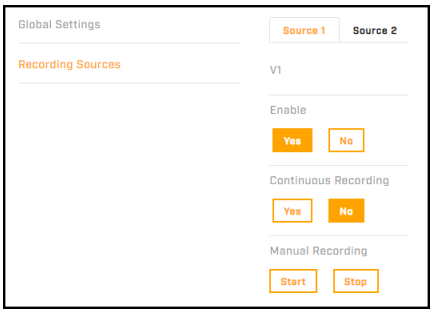
Clip Size—Specify in seconds the maximum allowed recording file size.

File Name Format—MP4.

Retention Policy—When the specified retention maximum memory percentage has been reached or exceeded, specify whether the camera stops recording (Stop) or deletes files to make space for new recordings (Overwrite; default).

Max. Memory Allocation—The percentage of space on the microSD card that triggers the specified retention policy. Range 20-90.

Recording Sources



The camera has two recording sources, the two video streams (V1 and V2). The camera can record both sources / streams at the same time.

For each recording source / video stream enabled on the Video Page, you can specify whether:

- recording is enabled for the stream
- the camera continuously records the stream

You can also manually start and stop recording the selected source / stream. However, manual recording of an H.265 source is not supported.

The current source and video stream settings appear to the right of the recording source settings.

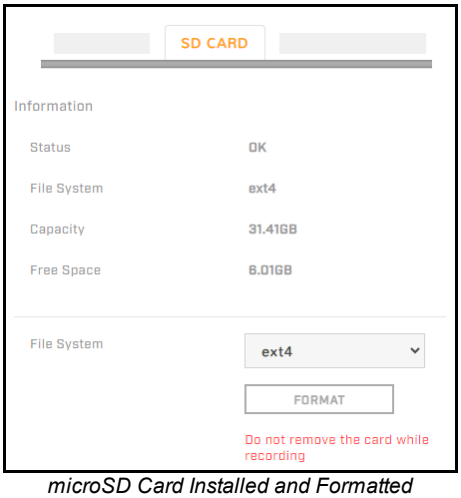
Name	Associated Video	Associated Video Settings	Status
Source 1	Visible 1	H.264 1920 x 1080	Recording
Source 2	Visible 2	H.264 1280 x 720	---

Example: Source 1 is Currently Recording

5.14 SD Card Page

You can locally record up to 512GB on a Class 10 microSD/microSDHC/microSDXC card (minimum 8GB).

The following information appears on the SD Card page:



microSD Card Installed and Formatted

- **Status**
  - OK—a microSD card has been properly installed and formatted
  - Error
  - Formatting
  - Done
  - No SD Card
- **Capacity—**The card's overall capacity, in GB.
- **Free Space—**How much free space is on it, in GB.

To format a microSD card before using it, click **Format**.

Caution

Formatting a microSD card deletes all data on the card, regardless of whether it has been encrypted.

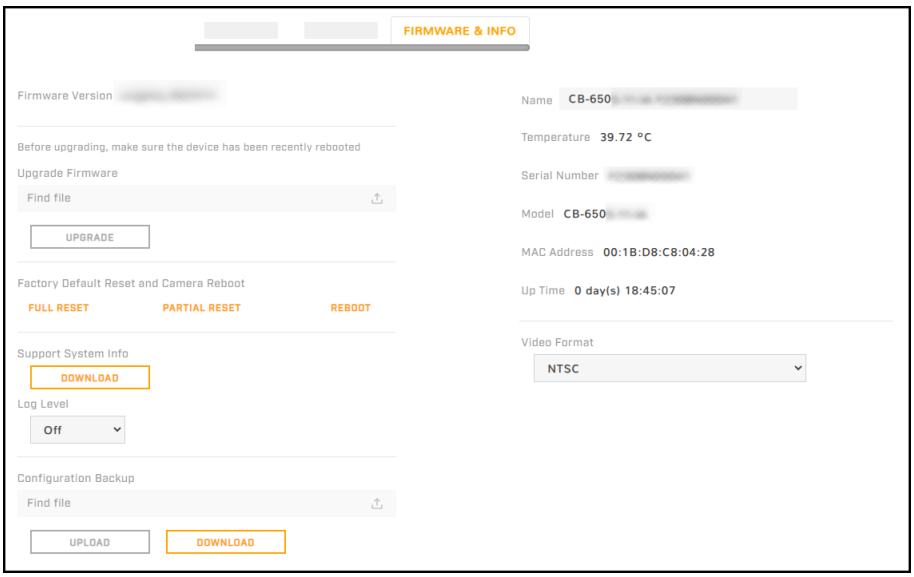
Notes

- Format the microSD card when using it for the first time, or when the card has been used with another camera or other device and transferred to this camera.
- The card must be preformatted as a single partition.
- For information about accessing the camera's microSD slot and inserting a card, see Connect the Camera.

5.15 Firmware & Info Page

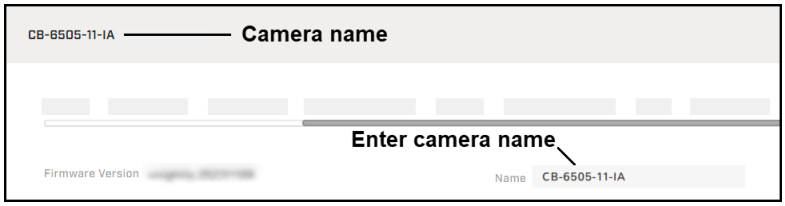
On the Firmware & Info page, you can:

- See the currently installed firmware version and other information about the camera
- Specify a unique name for the camera
- Upgrade the camera's firmware
- Reset the camera's settings to their factory defaults
- Reboot the camera
- Enable logs, define a log level, and download system information
- Download or upload a configuration backup file
- Configure the video format



Name

Specify a unique, friendly name for the camera, using only alphanumeric characters.



The default name for the camera is the camera model followed by the camera's serial number.

To upgrade the camera's firmware:

1. Make sure the camera has been recently rebooted.
2. Under Upgrade Firmware, click **Find file**.
3. On your computer or network, browse to and select the firmware file.

   Caution

   Only upgrade with firmware developed for Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics.

4. Click **Upgrade**.

   The camera uploads and installs the firmware, which takes a minute or two. After installing firmware, the camera requires a reboot. When prompted, confirm rebooting the camera.

Factory Defaults

To reset the camera to its factory default settings, click **Full Reset**, and then confirm. The camera reboots.

To reset the camera to its factory default settings but retain previously saved Network page and 802.1X settings, click **Partial Reset**, and then confirm. The camera reboots.

Caution

After confirming a reset, do not click on the camera web page until the camera reboots and the login screen appears. Then, according to the instructions in Accessing the Camera, log back in to the camera web page using the camera's default admin user.

To reboot the camera and reset the camera to previously saved settings, click **Reboot**, and then confirm. If you reboot the camera before saving changes on the Firmware & Info page or on any other page, the camera does not save those changes.

Tips

You can also:

- Reset the camera to its factory default settings by pressing the camera's physical default button for at least six seconds.
- Reboot the camera by pressing the camera's physical reset button for at least one second.

The default and reset buttons are located on the camera's bottom panel.
For example, if you are unable to access the camera via its web page or other communication method.

Support System Info

To retrieve the camera's log files, click **Download**.

Set the logging detail up to four levels; higher log levels increase the size of the log file.

Configuration Backup

You can back up the camera's saved settings or upload a configuration backup file; for example, when you replace a camera.

To upload a configuration backup file:

1. Click **Find file**.
2. On your computer or network, browse to and select the configuration backup file.

   Caution

   Make sure to upload a configuration backup file that was downloaded from a Quasar Premium BulletCamera with FLIR Edge AI Video Analytics that is the exact same model and with the same firmware version installed.

3. Click **Upload**.

   The camera uploads the backup file and requires a reboot. Confirm rebooting the camera.

To download the camera's saved settings:

1. Click **Download**.
2. On your computer or network, browse to and select the location where you want to save the backup file.

   backup.tar.gz is the default backup file name. You can change the backup file name, but do not change the **.tar.gz**.

Video Format

Select NTSC (default) or PAL. The video format determines the video stream frame rates available on the Video Page and the exposure times (shutter speeds) available on the Visible Page.

6 Appendices

6.1 Technical Specifications

Up-to-date resources for the camera, including the camera's specifications, are available from the camera's product information and support pages on the Teledyne FLIR website. See <%TARGETTITLE% >.

6.2 Install UPnP Components

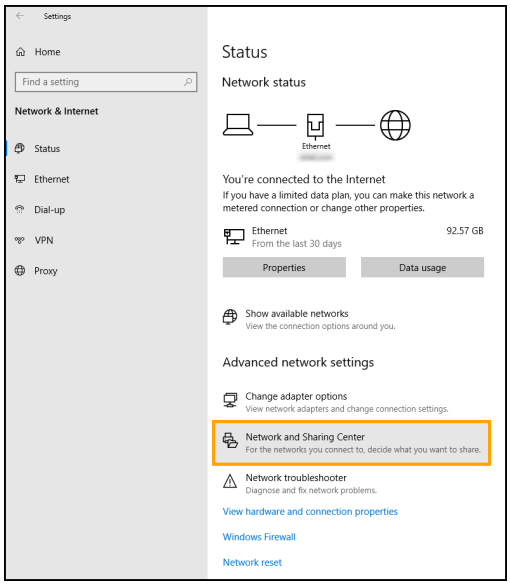
Windows PCs can discover the camera on the network when:

- network discovery is enabled
- the UPnP (Universal Plug and Play) Device Host service is running

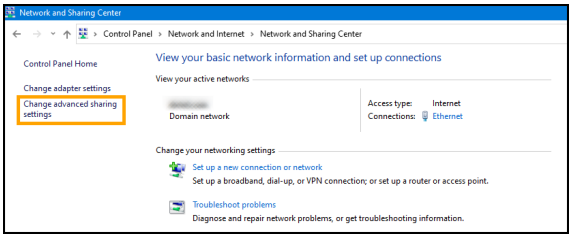
To enable network discovery:

1. Using an Administrator account, log in to Windows.
2. Open the Windows Network and Sharing Center.

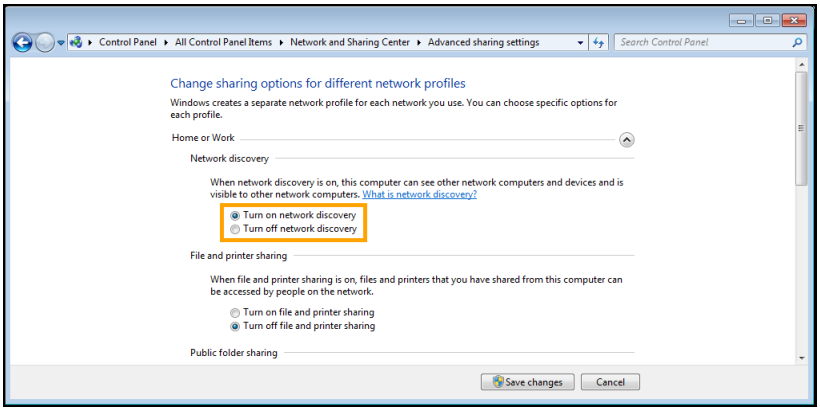
   In Windows 10, you can click **Start** > **Settings.** Then, click **Network & Internet**. In the Advanced network settings section, click **Network and Sharing Center**.



3. Click **Change advanced sharing settings**.



4. Expand the Home or Work section. Then, under **Network discovery**, select **Turn on network discovery**.



5. Click **Save Changes**.

Note

Network discovery requires that the DNS Client, Function Discovery Resource Publication, SSDP Discovery, and UPnP Device Host services are started, that network discovery is allowed to communicate through Windows Firewall, and that other firewalls are not interfering with network discovery.

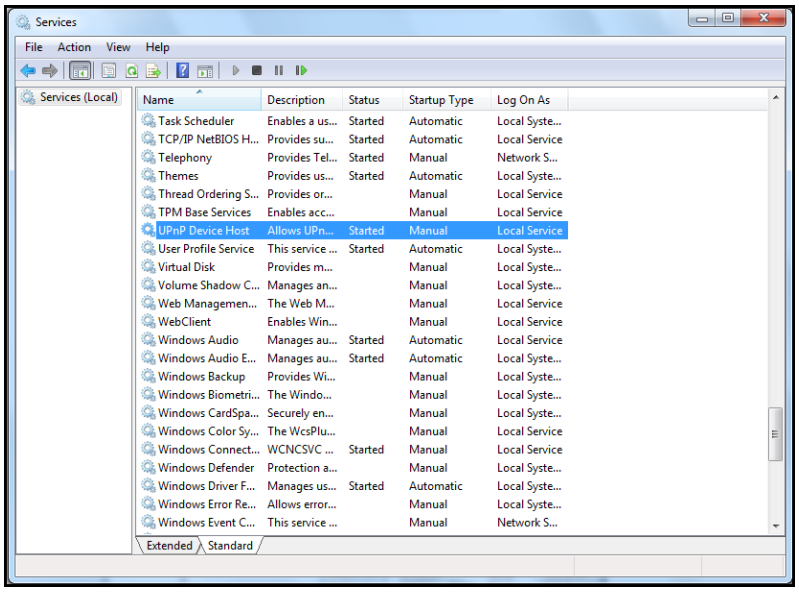
To check that the UPnP Device Host services are running:

1. Run the Windows *Services* app.

   In Windows 10, you can click **Start** ; search for *services*; and then click *Services* app 

.

2. Scroll down the list to *UPnP Device Host* and verify that the status is *Started*.



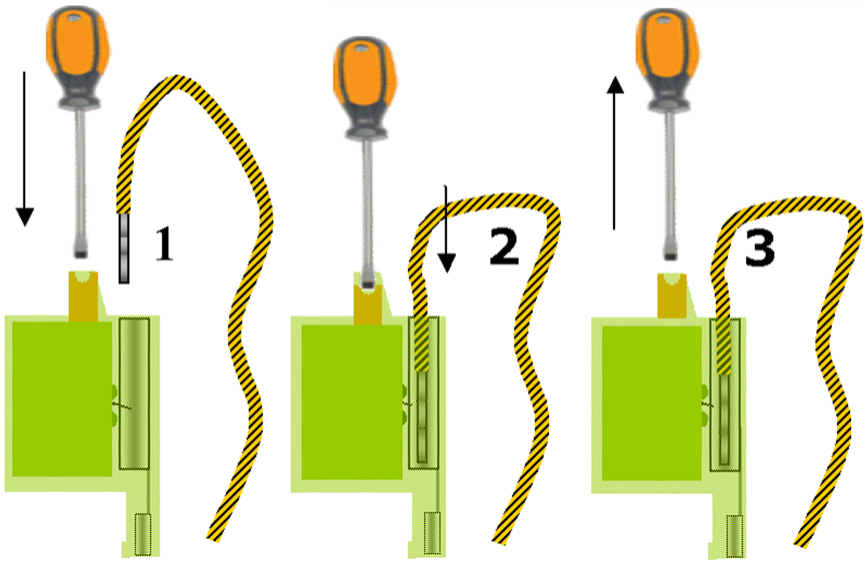
   If the status is not *Started*, right-click and select *Start*.

6.3 Connecting Leads to a Spring Clamp Connectors

The camera kit includes connectors with spring clamps for 24V AC or 12V DC power, alarm I/O, and audio I/O connections. Use the instructions below and the pin assignment information in Connect the Camera to attach wires to the appropriate connector. Then, attach the connector to the appropriate terminal block on the camera.

To connect a wire to the spring clamp connector:

1. Strip the insulation from the end of the wire. Approximately 1 cm (2.54”) of wire should be exposed.
2. With a small screwdriver, press in and hold the orange spring clamp button next to the female outlet where the wire will be inserted.
3. Insert the stripped end of the wire into the female outlet.
4. Release the orange spring clamp button.

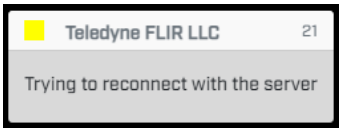
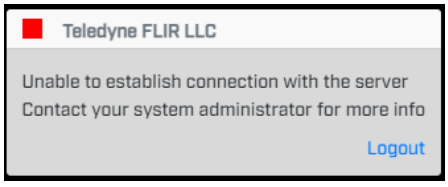
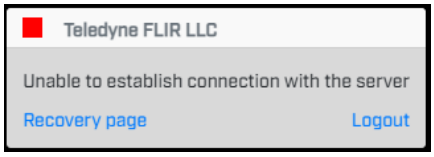


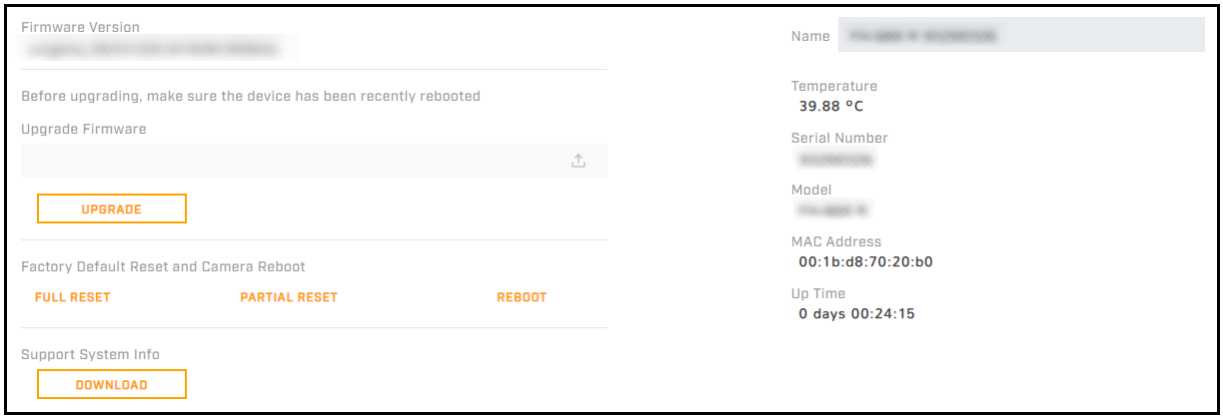
Connecting a Wire to a Terminal Block

6.4 Troubleshooting

Unable to Access the Camera

Under certain circumstances, after logging in to the camera's web page, the following messages appear:

	The camera's Nexus server might not be available, and the web page is attempting to re-establish the connection. The Nexus server provides the communication between the camera's web page and the camera's components.
	The camera's Nexus server is not available, and you logged in as a user assigned the expert or user role. For troubleshooting options, you need to log in as a user assigned the admin role. Click **Logout** and contact your system administrator.
	The camera's Nexus server is not available, and you logged in as a user assigned the admin role. You can click: • **Logout** • **Recovery page—**Opens a page similar to the Firmware & Info Page, on which you can see some system information and perform some system-related tasks. For example, you can reboot the camera.



Other Situations

Situation	Possible Solutions
No network connection	**Hardware issues:** • Check that the network is working and the unit is powered on. • Check that the network (Ethernet) cable is properly attached to the unit. • Confirm that the network cables are not damaged and replace if necessary.

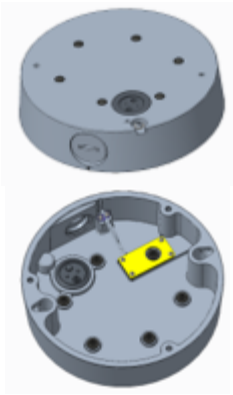
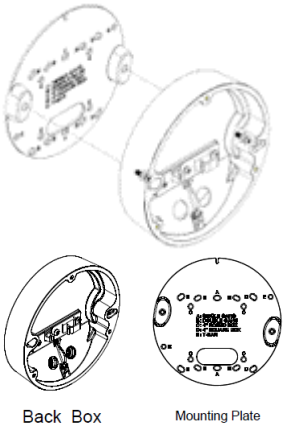
Situation	Possible Solutions
No network connection (continued)	**IP address issues:** • Change the default IP address/addresses of the unit. • From the PC running the web browser, ping the unit IP address and confirm that it can be reached. • Confirm that the network settings/firewalls are set according to the requirements. • The camera might be located on a different subnet. Contact your IT administrator to get the IP address of the camera.
How do I find the IP address of my unit?	• Check the network DHCP server IP address assignments and lease. • Alternatively, move the camera to an isolated network and make sure camera gets DHCP address and is accessible. Move the camera back to the network and test it. If you still have issues, reset the camera physically by pressing the reset button on the rear of the camera and test the camera again. This will ensure the camera releases the IP address.
The IP address responds to a ping on the network from the workstation but does not show in the Discovery List	• Disconnect the Ethernet cable from the camera's RJ-45 connector or turn the unit off. Then, ping the IP address again. If the IP address responds, there is another device using the IP address. Consult with your network administrator to resolve the conflict. • Check the network port and ensure that it is working OK. • Ensure that the switch ports provide the necessary power.
The unit IP address is in use by another computer (collision)	• Check the DHCP settings. Obtain a new IP address using DHCP. Ensure this is a unique IP address. • Alternatively, change the unit IP address after connecting to it directly (not through the system network).
Cannot log in to the camera	• Check the login user ID of the user or admin. • Check the login password of the user or admin.
No video image displayed on the camera's web page	• Reset the browser security settings to the default value. • Check that the correct port was configured. The default port is 554.
Poor video quality	• Check that the network cable is connected securely. • Check that the camera settings are correct on the camera and in the unit. • Check that the camera lens is clean and unobstructed. • Check that the cable length is within specification.

Situation	Possible Solutions
Streaming video image is hanging (stopped)	• Confirm the unit's video streaming settings. • Refresh your browser screen (F5). • Check that the bandwidth and bit rate settings of the network are set properly. • Check that other processes and applications are not causing undue latency. • Check that the firewall analysis or blocking is not interfering with the video stream and supports the required ports and communication protocols.
Bluish picture in an indoor scene (possibly mixing indoor and outdoor lighting)	Change the white balance setting to *Auto*. If the lighting in the scene is fixed, manually adjust the white balance to an acceptable image.
Reddish picture and incorrect colors in the image	Check the PoE power supply and associated network cables. Connect directly to the PoE and compare the images. If the problem persists, contact Support.
IR LEDs do not function	• Check the Night Mode settings and the IR Illumination setting. • If there is a light source close to the camera's ambient light sensor on the IR board, or if something is blocking the light sensor, resolve the issue and then reboot the camera.
Video Analytics does not appear in the View Settings menu	Contact FLIR Support.

6.5 Accessories

The following accessories are available from Teledyne FLIR for installing Quasar Premium Bullet Camera with FLIR Edge AI Video Analytics (CB-650x).

Part number / item code	Description	Images (not to scale)	CB-650x Bullet	CB-650x Bullet w/ NPT backbox
CM-SECA-W4	Side conduit adapter kit		compatible	N/A
421-0066-00 DH-CRNR-00	Corner mount kit		compatible	N/A * CB-650x's NPT back box does NOT have hole C: 4”Round box
421-0067-00 DH-POLE-00	Pole mount kit for pole diameter 150-230mm (6.0-9.0")		compatible	N/A * CB-650x's NPT back box does NOT have hole C: 4”Round box
421-0068-00 DH-PDST-00	Pendant mount kit		compatible	N/A * CB-650x's NPT back box does NOT have hole C: 4”Round box
421-0069-00	Pendant mount shroud kit		compatible	N/A * CB-650x's NPT back box does NOT have hole C: 4”Round box

Part number / item code	Description	Images (not to scale)	CB-650x Bullet	CB-650x Bullet w/ NPT backbox
CB-BKBX-65	Backbox with 3/4" NPT conduit holes		compatible	included (shipped attached)
CB-BKBX-65S	Backbox standard		included (shipped attached)	compatible
CM-CAPS-G3	Pendant capcap with 1.5" PF outer thread. To be used with CB-BKBX-65S. Can also be used with: Can use with ○ CX-ARMX-G3 wall mount bracket ○ CX-ELBX-G3 or CX-ELBX-G31 wall mount bracket with power box ○ CX-GSNK-G32 gooseneck pipe ○ CX-XTND-G3 extendable gooseneck mount			compatible

For more information about accessories, including specifications such as dimensions and weights, see the *FLIR Security Edge Devices Accessory Guide*, contact your Teledyne FLIR sales representative, or visit https://support.flir.com/ to request details on where to get the accessory.