

INSTALLATION & USER GUIDE



FCB-Series AI

FCB-334-AI FCB-350-AI FCB-618-AI

FCB-624-AI FCB-632-AI

© 2026 Teledyne FLIR LLC All rights reserved. No parts of this material may be copied, translated, or transmitted (in any medium) without the prior written permission of Teledyne FLIR LLC.

Names and marks appearing on the products herein are either registered trademarks or trademarks of Teledyne FLIR LLC and/or its subsidiaries. All other trademarks, trade names, or company names referenced herein are used for identification only and are the property of their respective owners.

Protected by one or more patents and patent applications. Learn more here: www.flir.com/patentnotice.

Photographs and images appearing in this manual may have been modified for illustrative purposes using commercial image editing software and may not always reflect an actual product configuration. The contents of this document are subject to change without notice.

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	January 2026	First release
101	January 2026	Minor fixes
102	January 2026	Minor formatting fixes
103	January 2026	Updated web related screenshots and minor updates and fixes
104	February 2026	Updated Product Specifications table
105	February 2026	Updated Video Analytics section

Contents

Document History	3
1. Product Registration and Warranty Information	7
1.1 Register Your Product with Teledyne FLIR	7
1.2 Warranty Information.....	7
2. Document Scope and Purpose.....	8
2.1 Disclaimer	8
3. Camera Overview	9
3.1 Related Documentation	9
4. Camera Dimensions.....	10
5. Camera Specifications.....	11
6. Models & Product Numbers.....	13
7. Product Information on the Teledyne FLIR Website	14
7.1 Accessing Product Information from the Teledyne FLIR Website:.....	14
8. Installing the Camera.....	15
8.1 Supplied Components.....	15
8.2 Site Preparation	15
8.3 Outdoor Mounting	16
8.4 Power Requirements	17
8.5 Installing the Back Box	17
Attaching the Back Box Directly to a Surface	18
Attaching the Back Box to a Standard Electrical Box.....	18
8.6 Routing the Cables	19
Routing Cables through the Side Conduit Hole	19
Routing Cables through the Rear Cable Entry Hole.....	20
8.7 Mounting the Camera.....	20
Adjusting the Sunshield	21
8.8 Connecting the Camera.....	21
8.9 Configuring Network Settings.....	22
Changing the IP Address Using FLIR DNA tool.....	23
Changing the IP Address Using the Camera's Web Interface.....	24
8.10 Aiming the Camera.....	25
8.11 Additional Configuration.....	26
8.12 Attach the Camera to a Supported Video Management System.....	27
9. Thermal Imaging Overview.....	28
10. Configuring the Camera Using the Web Interface	29
10.1 Accessing the Camera Web Interface.....	29
Logging in to the Camera's Web Interface	29

10.2	Web Interface Home Screen	30
	Top Navigation Bar.....	30
	Main Video Feed Area.....	30
	Left Sidebar - View Settings Menu	30
	Right Sidebar – Alarms Section.....	31
	Live Video Refresh Rate Slider.....	31
	Recording Indicator.....	31
10.3	Making Changes to Settings	31
	Camera Settings.....	31
	System Settings	32
10.4	Camera Settings	33
	Video	33
	Thermal	35
	I/O (Input/Output).....	37
	AI Video Analytics Capabilities	38
	OSD (On-Screen Display)	48
	Geotracking.....	49
	Georeference	52
11.	System Settings.....	54
11.1	Network.....	55
	Settings	55
	SNMP	56
11.2	Date & Time	57
	Manually Configuring the Camera's Time Zone, Time, and Date	57
11.3	Users	58
	Add User	58
	Edit User.....	59
	Delete User	59
11.4	Alarm	59
	Modify an Existing Alarm Rule or Define an Alarm Rule:	60
	Modify or Define Rule Triggers.....	60
	Modifying or Defining Rule Actions	63
11.5	Audio	64
	Audio In	64
	Audio Out	64
11.6	I/O Devices	65
11.7	Messaging	66
	Email.....	66
11.8	Heaters & Fans	67

11.9	Cyber.....	68
	Certificates.....	68
	802.1X.....	70
	TLS/HTTPS	70
	Services	70
	IP Filter	71
11.10	Media Browser.....	72
11.11	ONVIF	74
	To configure the ONVIF interface	74
11.12	Map.....	74
	Manually Uploading a Reference Map Image and Calibrating It.....	74
	Using Flir Raven Site Planning Tool to Download the Map and Calibration Data.....	76
11.13	Scheduler	80
	To Define a Task:	80
11.14	Recording	82
	Global Settings.....	82
	Recording Sources.....	83
11.15	SD Card	84
11.16	Firmware & Info	84
	Name.....	85
	Upgrading the Camera's Firmware:.....	85
	Factory Defaults.....	86
	Support System Info	86
	Configuration Backup	86
12.	Maintenance & Troubleshooting.....	88
12.1	Removing the Access Cover	88
12.2	Cleaning.....	88
12.3	Troubleshooting Tips	89
	Unable to Access the Camera.....	89
	Unable to Communicate over Ethernet.....	90
	Unable to View IP Video Stream.....	90
	No IP Video	90
	Image Freezes Momentarily	91
	Performance Varies with Time of Day	91
	Image Too Dark or Too Light.....	91
	Eastern or Western Exposure.....	91

1. Product Registration and Warranty Information

1.1 Register Your Product with Teledyne FLIR

Ensure you get the most out of your Teledyne FLIR product by registering it at <https://customer.flir.com>. By registering, you'll receive exclusive benefits, updates, and support tailored to your product.

1.2 Warranty Information

For comprehensive warranty details, visit <https://www.teledynelfir.com/support-center/warranty/security/flir-security-product-warranties/>. Here, you'll find all the information you need to understand the coverage and support available for your FLIR security products.

2. Document Scope and Purpose

This document provides installation, operation, and configuration instructions for FCB-Series AI cameras with FLIR Edge AI Video Analytics.

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.

2.1 Disclaimer

Users of Teledyne FLIR products accept full responsibility for ensuring their suitability and considering the role of the product detection capabilities and their limitations 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.



WARNING

- 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.** 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.

For installation support, visit <https://www.flir.com/support/> or contact your local Teledyne FLIR representative. Installers and integrators can also access Teledyne FLIR training at <https://www.flir.com/support-center/training/>.

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.

3. Camera Overview

The FB-Series AI cameras are advanced components within the FLIR perimeter security ecosystem. These cameras integrate robust deep neural network (DNN) video analytics to reliably detect and classify humans and vehicles with high accuracy. They are designed to minimize nuisance alarms by distinguishing genuine threats from environmental factors, even during attempts to deceive the system.

The camera supports multiple lens options, offering fields of view from 18° to 50°, and delivers VGA and QVGA resolutions for flexible deployment. With an industry-leading thermal sensitivity of ≤ 20 mK, the FB-Series AI ensures superior image quality and detection performance in challenging conditions. Ethernet connectivity enables seamless integration with external analytics platforms and video management systems, while supported protocols include IPv4, HTTP, HTTPS, and ONVIF profiles for interoperability.

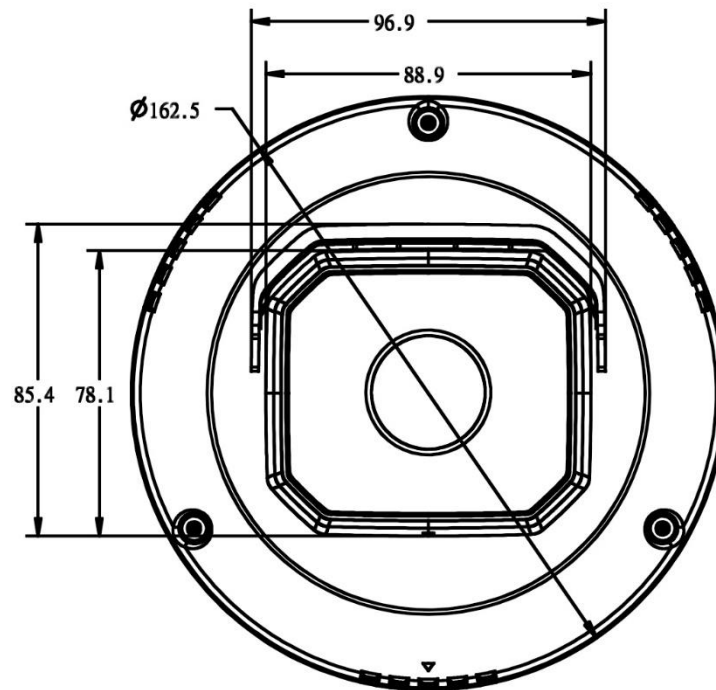
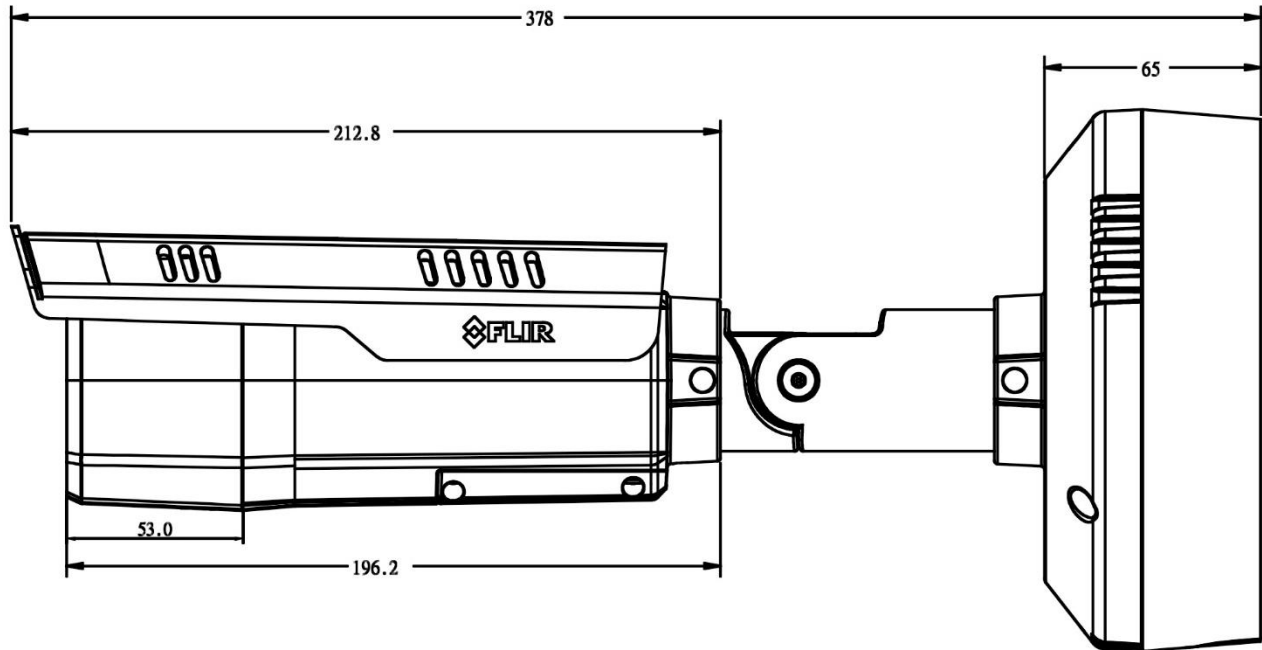
The FB-Series AI is ideal for perimeter protection, large and small area security, and remote site monitoring. Its advanced analytics, combined with precise geolocation and PTZ handoff capabilities, provide instant situational awareness and automated threat detection in a single, easy-to-use solution.

3.1 Related Documentation

- FCB-Series AI Quick Install Guide
- FLIR Security Edge Devices Accessory Guide
- FLIR Security PTZ Pairing Configuration Guide
- DNA User Guide

4. Camera Dimensions

The figures below show the dimensions in millimeters of the camera, from different perspectives.



5. Camera Specifications

Overview	
Array format	640 × 480 (FCB-618, -624, 632); 320 x 240 (FCB-334, -350).
Detector type	Long-life, uncooled, sun-safe VOx microbolometer.
Spectral range	8 μm to 14 μm.
Effective resolution	VGA: 327,680 pixels, QVGA: 81,920.
Pixel pitch	12 μm.
Thermal frame rate	30 Hz
Focus	Athermalized, focus-free.
Sensitivity	VGA: <20 mK; QVGA: <30 mK
Video & Audio	
Video	Two independent IP video streams.
Video compression	H.264, H.265 or MJPEG.
Streaming resolution	VGA: 640 × 512; QVGA: 320 x 256
Thermal Image Settings	Brightness, Contrast, Sharpness, Auto AGC, Digital Detail Enhancement (DDE), Gamma, Smart Screen Optimization.
Thermal AGC region of interest	Default, presets, and user-definable to ensure optimal image quality on subjects of interest.
Analytics management	Web-based configuration and management; masking of analytic detection areas; adjustable sensitivity; automatic responses; remote I/O control.
Analytics features	Region entrance/Intrusion detection; Crossover/fence trespassing; CNN classifier.
Image uniformity optimization	Automatic flat field correction (FFC); thermal and temporal triggers.
SD card Full SOE	Support up to 2 TB SD card (sold separately).
Audio	+1 x Line Input, G.711 a/μ-law AAC support +1 x Line Output.

System Integration				
Ethernet	10/100,1000 IEEE 802.3, auto sensing 1 x RJ45.			
External analytics compatible	Yes.			
Control input/output network	1x dry contact in; 1x relay out (rated load 0.025 A@ 5 VDC).			
APIs	NEXUS SDK, NEXUS CGI, ONVIF Profile S, G, T.			
Network				
Supported protocols	IPv4, HTTP, HTTPS, UPnP, DNS,NTP, RTSP, RTP, TCP, UDP, ICMP, IGMP, DHCP, ARP, IEEE 802.1X, ONVIF Profile G/T/S.			
General				
Weight with sunshield	2.34 Kg			
Dimensions	96.9 x 85.4 x 378 mm (3.8 x 3.4 x 14.9 in.).			
De-fog	Built-in heaters.			
Input Voltage	Source	PoE+ (802.3at)	12 VDC	24 VAC
	Heater off	6.8 W	7.2 W	7.0 W
	Heater On (100%)	13 W	12.4 W	12.5 W
Cybersecurity	Password protection, Password policy enforcement, IP filtering, IEEE 802.1X, Digest authentication, CA & self-signed certificates, Firewall.			
Environmental				
Enclosure	IP67, NEMA4X			
Operating temperature range	-40°C to 60°C/-40°F to 140°F (cold start)			
Storage temperature range	-50°C to 85°C (-58°F to 185°F)			
Humidity	0-95% relative humidity			
Shock & Vibration	ISTA 3A			
Vandalism protection	Yes (except window)			
Warranty & Regulatory				
Warranty	Camera: 3 years / Sensor: 10 years			
EMC	CE (EN 55032, EN 55035), EN 61000-6-3, EN 50130-4, AS/NZS CISPR 32, FCC Part 15 (Subpart B, Class A)			
International	RoHS, WEEE, UKCA, ICES-003, RCM			
Safety	CB Scheme IEC 62368-1 (2018, 2020+A112020), IEC 62471 CB (photo-biological safety for IR LEDs)			

6. Models & Product Numbers

The FCB-Series AI comprises the following camera models:

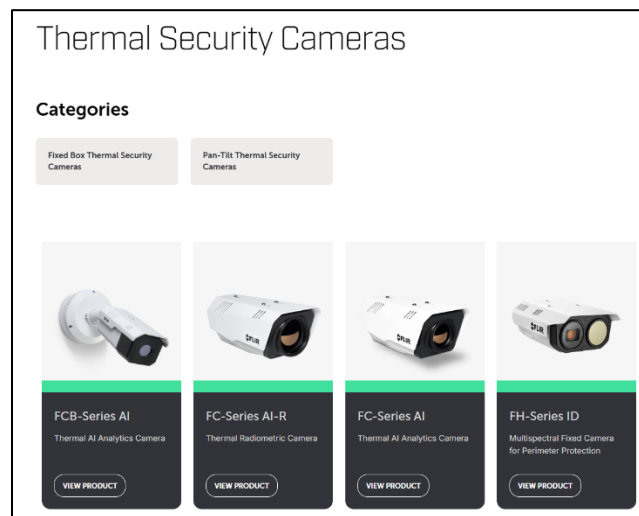
Model	Product Number	Focal Length	Sensor Resolution
FCB-334-AI	427-2064-30-00	6.3 mm	320 x 240
FCB-350-AI	427-2064-20-00	4.3 mm	320 x 240
FCB-618-AI	427-2064-90-00	24 mm	640 x 480
FCB-624-AI	427-2064-82-00	18 mm	640 x 480
FCB-632-AI	427-2064-81-00	14 mm	640 x 480

7. Product Information on the Teledyne FLIR Website

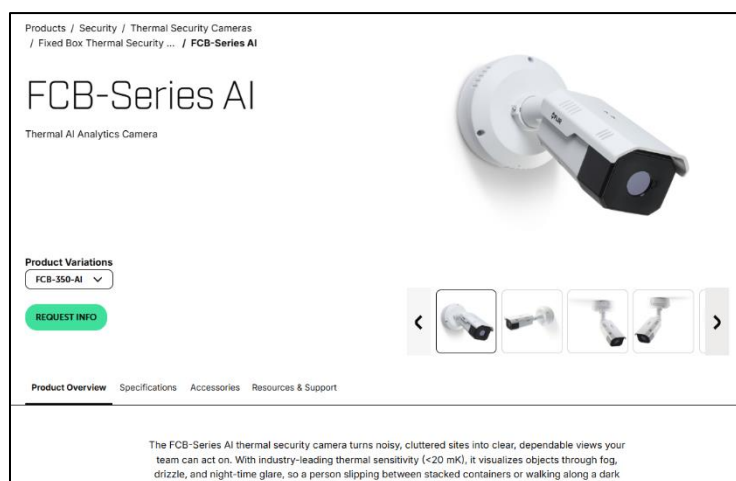
Up-to-date resources for the camera, including camera specifications, the Teledyne FLIR Discovery Network Assistant (DNA) software tool, and this guide, are available on the Teledyne FLIR website.

7.1 Accessing Product Information from the Teledyne FLIR Website:

1. Open [FLIR Security Thermal Cameras](#)



2. Find and click on the camera. The camera's product details page is displayed.



- To see the camera's specifications and related content, scroll down.
- To access the camera's support page, including documentation, select the **Resources & Support** tab.

3. **Download** the latest firmware and FLIR DNA application, if necessary.

8. Installing the Camera

The order of the installation steps described in this manual follow a standard procedure, but the order can be changed to accommodate the site or installation needs. For instance, before installing 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.



WARNING

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.

8.1 Supplied Components

The FCB-Series AI camera kit includes:

- One **FCB camera**.
- One **Back Box** (hole caps, plugs, and washers included).
- One **two-pin connector** for the 12 VDC/24 VAC terminal block.
- Two **four-pin connectors** for the Alarm and Audio terminal blocks.
- One **Mounting template sticker**.
- One **rubber multiple-cable gland**.
- Two **plastic screw anchors** for attaching the FCB back box to the mounting surface.
- Two **TP4x20 tapping screws** for attaching the FCB back box to the mounting surface.
- One **T10 Torx Security wrench**.
- One **T20 Torx Security wrench**.
- One **printed Quick Installation Guide**.

If any of these items are missing or damaged, contact your dealer or [Teledyne FLIR Support](#).

8.2 Site Preparation

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.

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. The camera must be protected from hostile external elements such as a corrosive environment, metallic dust, extreme temperatures, soot, over spray, etc.

- **Accessibility:** Camera placement 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 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:** All electrical work must be performed in accordance with local regulatory requirements. There must be a fuse or circuit breaker at the starting point of the electrical wiring infrastructure. Units should be placed in locations that are optimal for the type of video cabling used between the cameras and external devices.
- **Physical Security:** To prevent the unit from being disabled or tampered with, the system should incorporate security measures that address physical access by both trusted and untrusted individuals.
- **Network Security:** Proper network security measures should be in place to ensure networks remain operative and free from malicious interferences. 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.) should be properly grounded to prevent electrostatic discharge.



WARNING

- 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.

8.3 Outdoor Mounting

If the camera is to be installed outdoors, also consider the following:

- **For outside wiring installation, always use weatherproof equipment**, such as boxes, receptacles, connectors, etc.
- **For electrical wiring, use properly rated sheathed cables** for the conditions to which the cable will be exposed, for example, moisture, heat, UV, physical requirements, etc.
- **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, etc.
- 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); cold start -40 °C (-40 °F); and no more than 95% non-condensing humidity.
- **All electrical work must be performed in accordance with local regulatory requirements.**

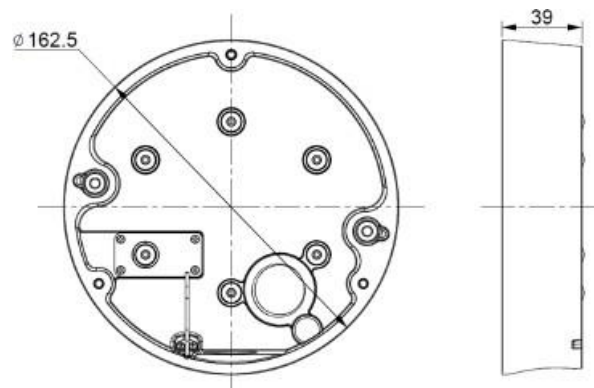
8.4 Power Requirements

The camera can be powered by 12 VDC, 24 VAC, or PoE+.

Maximum Power Consumption	12 VDC (1.25 A)	24 VAC (1.2 A)	PoE+ (0.3 A)
Heater OFF	7.2 W	7.0 W	6.8 W
Heater ON	12.4 W	12.5 W	13 W

8.5 Installing the Back Box

The diagram below shows the dimensions of the Back Box in millimeters.



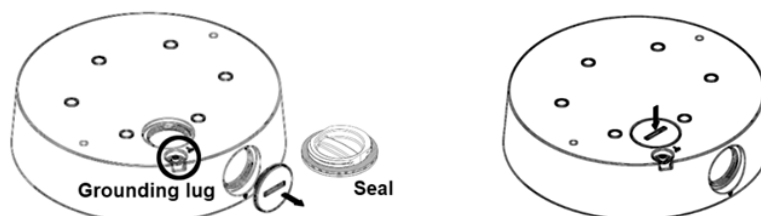
The FCB-Series AI Back Box provides a **3/4" side conduit hole** for routing cables into the camera.

Attach the Back Box to a **secure, flush, and vibration-free surface** or to a **standard single gang or double gang electrical box**. Cables can be routed 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 routing cables through the side cable entry hole:

1. **Use a coin** to remove the cap and seal from the side cable entry hole.
2. **Attach the cap and seal** to the rear cable entry hole.
3. Make sure the **cap is fully tightened**.





WARNING

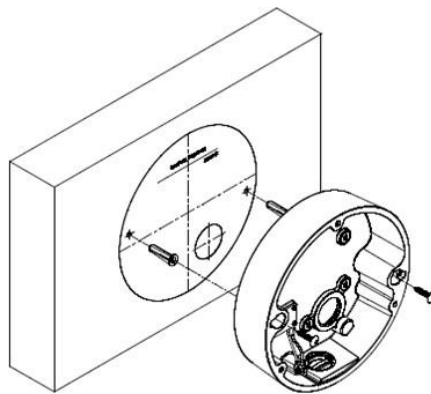
Anchor a ground strap to the grounding lug on the back box and **connect it to the nearest earth-grounding point**. Failure to properly ground the camera can permanently damage it.

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.

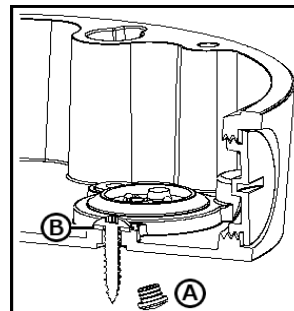
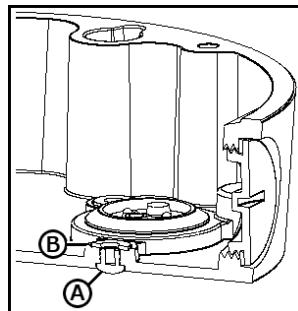
Attaching the Back Box Directly to a Surface

1. Using the mounting template sticker included in the kit, **mark the surface and drill two anchor holes**.
2. (Optional) If necessary, **drill a hole for routing cables**.
3. **Hammer two plastic screw anchors** into the drilled holes.
4. **Insert the anchors and then attach the back box** to the surface using two TP4x20 mm tapping screws.

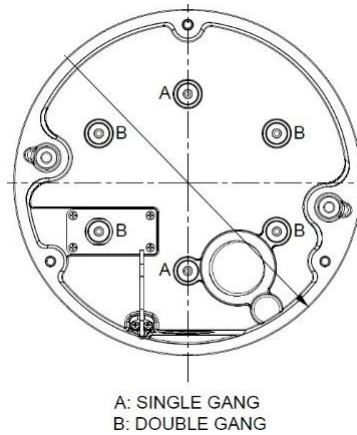


Attaching the Back Box to a Standard Electrical Box

The Back Box is shipped with rubber seals and plugs attached to the electrical box mounting screw holes. For the unused holes, leave the seals and plugs in place. For the holes in use, **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 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.



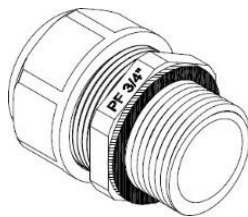
Using truss head screws (not included), **attach the back box to the electrical box.**

8.6 Routing the Cables

Routing Cables through the Side Conduit Hole

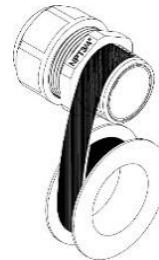
1. **Attach a 3/4" PF thread or NPT thread compression gland** (not included) to the side conduit hole.

PF thread



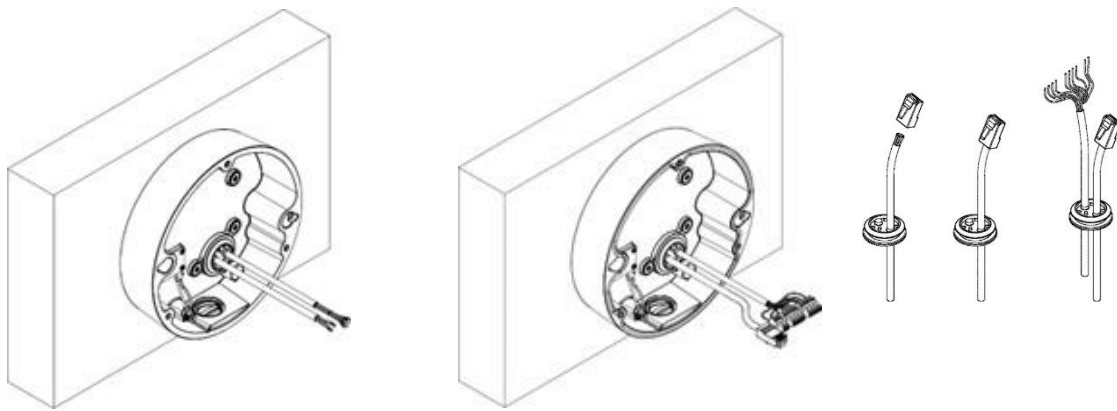
For waterproofing, use rubber gland

NPT thread



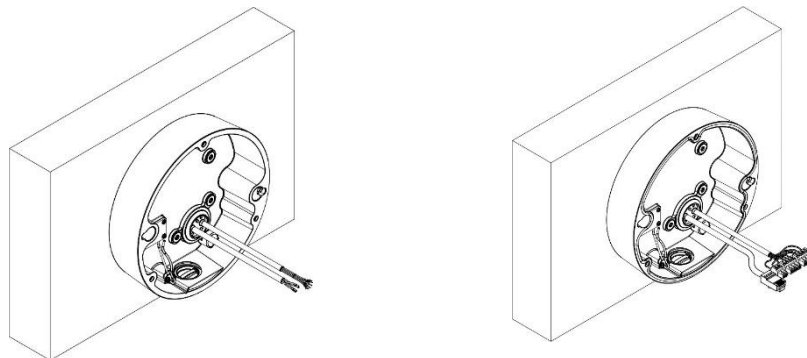
For improved waterproofing, use thread seal tape

2. Make sure the seal is **securely seated on the inside and outside** of the cable entry hole. To seal any gaps, apply silicone sealant.
3. **Route unterminated cables** into the back box.
4. **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.



Routing Cables through the Rear Cable Entry Hole

1. **Route an unterminated Ethernet cable** through a hole in the cable gland included in the camera kit.
2. (Optional) **Route an unterminated power, alarm, and audio cable** through the other hole in the gland.
3. **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.

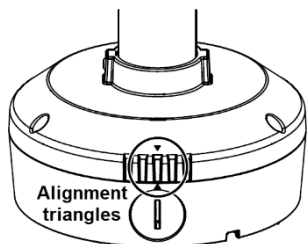


4. **Attach the gland to the cable entry hole.** Make sure that the side of the gland with the smaller diameter is inside the back box.

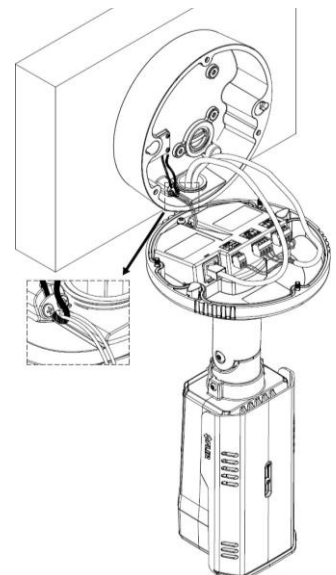
8.7 Mounting the Camera

The example on the right shows the 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 are enlarged.

To avoid accidentally dropping the camera, make sure to **attach the safety wire on the camera assembly to the clip on the back box.**



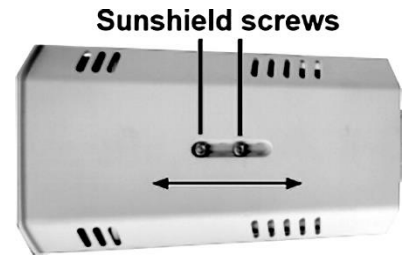
When attaching the camera assembly to the back box, **align the triangle on the exterior of the camera assembly with the triangle on the back box.** This makes sure the guide pins inside the camera assembly are aligned with the guide.



Adjusting the Sunshield

FCB-Series AI cameras are designed to operate in rugged environments. The sunshield 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. Adjust the sun shield to avoid issues with shadows, taking into account the lens coverage.



WARNING

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

8.8 Connecting the Camera



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 video streaming 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	12 VDC - / 24 VAC ~	When using a 24 VAC or 12 VDC power supply, connect it to the power terminal block connector according to the pin assignment shown.
	12 VDC + / 24 VAC ~	
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	



WARNING

- The power cord to the 12 VDC or 24 VAC 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.

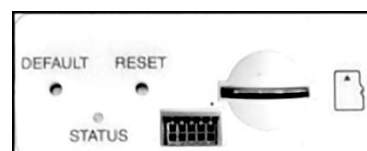
Bottom Panel Interfaces

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

Insert a microSDXC card in the card slot (maximum 2 TB SD Bus Mode UHS I) to store files, video recordings and snapshots. **Do not remove the microSD card while the camera is ON.**



Bottom of the camera.



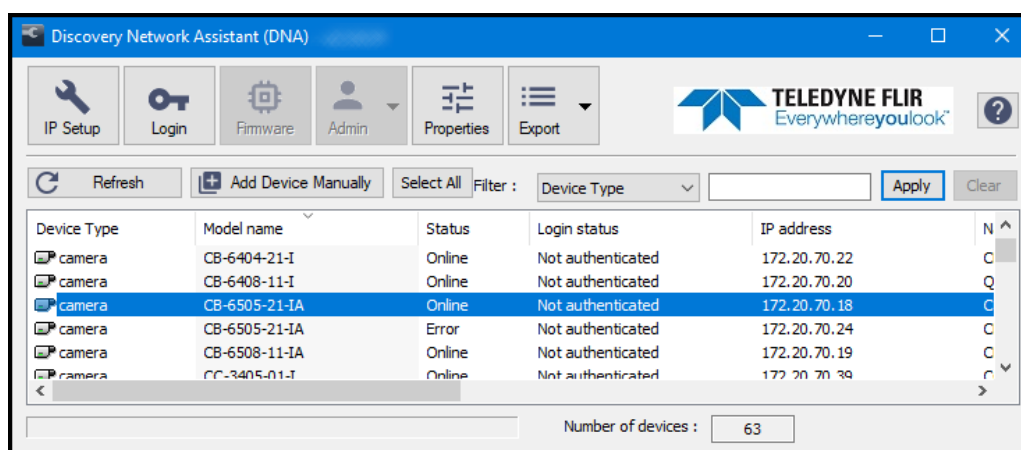
Bottom panel.

To learn how to use the controls in the bottom panel to troubleshoot your camera, please see [Maintenance & Troubleshooting](#).

8.9 Configuring Network Settings

The camera can be discovered and configured for networking using the **FLIR Discovery Network Assistant (DNA)** software tool; the **camera's web interface**; or a **supported VMS**. Using the DNA tool or the camera's web interface requires using the default admin user or any user assigned the admin or expert role. The table below indicates which tasks can be performed using each of these methods.

Task	DNA Tool	Camera's Web Interface
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		*

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* clicking on the Help icon  while the software is open.

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. For example, 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 cannot connect to a DHCP server, the camera's **default IP address is 192.168.0.250**.

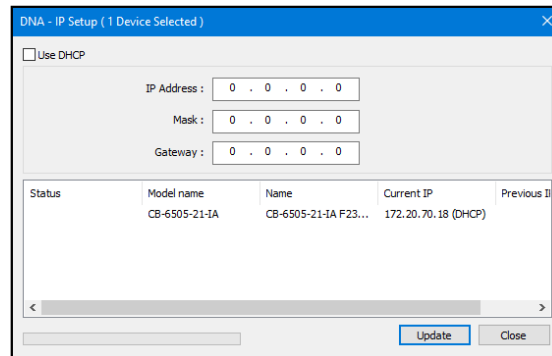
If the camera is managed by FLIR Latitude VMS or is on a network with static IP addressing, users can **manually specify the camera's IP address** using the DNA tool or the camera's web interface.

Changing the IP Address Using FLIR DNA tool

When the camera is connected to a network where several other cameras are connected, it is highly advisable to make sure that **all cameras have unique IP addresses**. To do so, the **DNA tool** can be used to manually set up each individual camera's address.

1. Make sure the camera and the PC are on the **same LAN segment**.
2. **Open the DNA tool** (DNA.exe). The Discover List is displayed, showing compatible devices on the LAN segment and their current IP addresses.
3. In the DNA Discover List, verify that the camera's **status is Online**. If this is the first time configuring the camera or if it is the first time after resetting the camera to its factory defaults, DNA automatically logs in to the camera using the **default username and password (admin)**.
4. Verify that the camera's Login **status is Authenticated**. If not, authenticate the camera using the custom username and password.

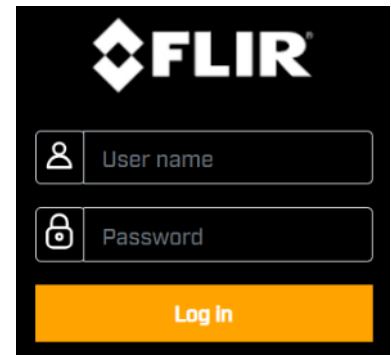
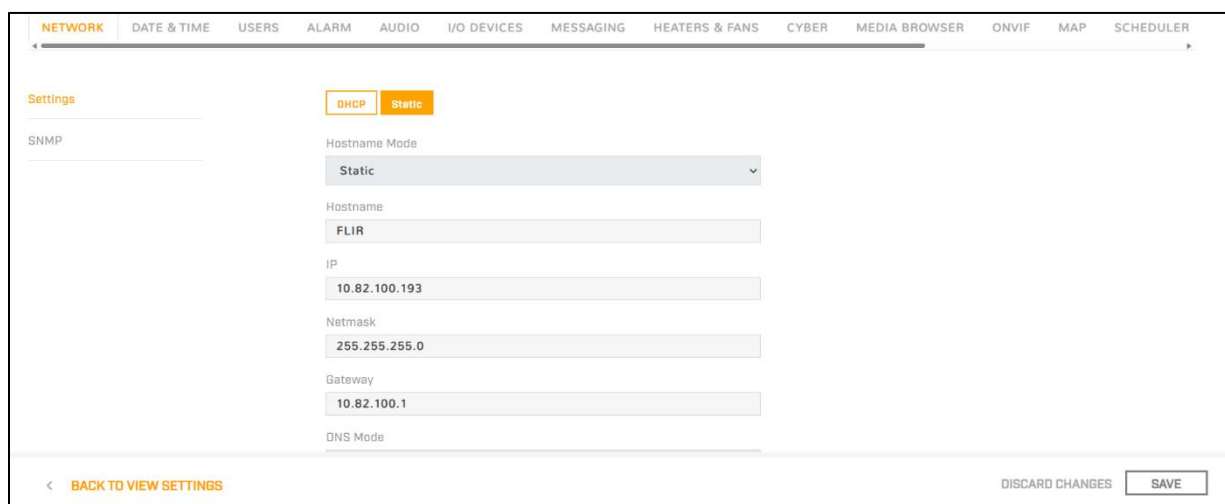
5. Select the camera from the Discover List, and then select **IP Setup**.



6. In IP Setup window, **uncheck the Use DHCP box and specify the new IP address**. It is also possible to specify the **Mask and Gateway**.
7. Finally, **select Update** and wait until OK is displayed in the status column, and select **Close**.

Changing the IP Address Using the Camera's Web Interface

1. **Access the camera's web interface** entering the camera's IP address on a modern browser such as Google Chrome, Microsoft Edge, or Mozilla Firefox, etc.
2. **Enter the username and password**. By default, these are both **"admin"**.
3. On the View Settings Home screen, click **System Settings** in the lower-left part of the screen.
4. By default, the **Network** tab is selected.
5. Click **Static IP addressing** and then manually specify the camera's *Hostname*, *IP address*, *Netmask*, and *Gateway*.
6. Users can also **specify the DNS Mode, Name Servers, MTU (maximum transmission unit), and Ethernet Speed**.

7. Click **Save**. Applying any changes on the Network screen **requires rebooting the camera**.

8.10 Aiming the Camera

To ensure optimal functionality, **the camera should be precisely positioned to cover the intended area**. This is especially relevant when using video analytics and georeferencing. To do so, 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**. Review the camera's video feed through the camera's web interface or a remote VMS client to ensure the image covers the intended area and satisfies georeferencing and video analytics requirements.

The following figure shows the screws used to aim the camera to accomplish the desired framing on the screen.

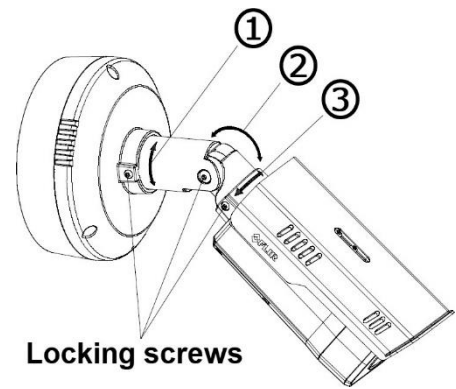
1. Retaining ring for **pan** adjustment (range 355°).
2. Bracket for **tilt** adjustment (range 90°).
3. Retaining ring for **spin** rotation (range 355°).

Adjust the **pan position (1)** to ensure that the camera tilts appropriately towards the scene and can be rotated to maintain an upright orientation facing the subject. 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 tilted in 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.

When adjusting the **Tilt bracket (2)**, make sure that toothed surfaces are properly aligned and meet evenly, as seen in the picture.

Adjust the spin of the camera, making sure the horizon is level and close to the top of the frame in order to properly use video analytics

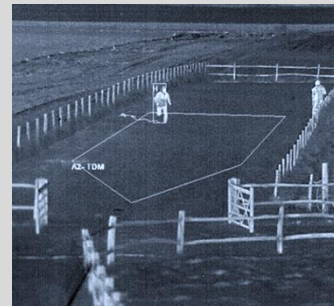
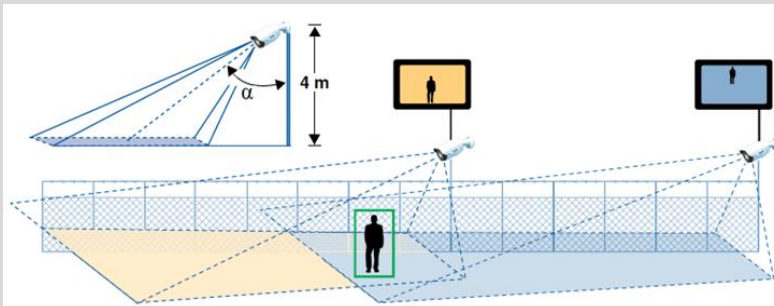
Then, use the T20 Torx Security wrench bit to **securely tighten each locking screw**.



TIPS

To fully utilize the camera's video analytics capabilities, ensure the following mounting requirements are met:

- The camera should be mounted at a **height of at least 4 meters**, with 6 meters being the ideal height.
- The **horizon line should be level and positioned near the top of the frame** for optimal performance.
- For installations with multiple cameras with on-board video analytics, the **fields of view of the cameras should overlap** in order to remove all dead zones in which a camera cannot see a target "head to toe". The camera's on-board analytics must be calibrated before it can detect targets.



8.11 Additional Configuration

When configuring the FCB-Series AI camera and integrating it with a network and VMS, the setup process may involve enabling, disabling, or adjusting various settings through the camera's web interface. **The available settings for configuration are determined by user roles**, each associated with specific permissions. The following table outlines which settings are accessible for each user group.

Settings	User Role
Other networking settings Date and time Alarms Audio Live video and video Enabling and configuring streamsexternal I/O devices Visible imager Notification emails Current and idle I/O states Onboard heaters and fans On-screen display (OSD) Cybersecurity Geotracking Map Georeference 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 FCB-Series AI with FLIR Edge AI Video Analytics with a FLIR Security PTZ camera that supports geotracking—see the corresponding pairing guide of the PTZ camera.	FCB-Series AI with FLIR Edge AI Video Analytics: Default admin user / any user assigned the admin or expert role

Certain configuration tasks may be completed either prior to or following camera installation; however, some tasks are best performed exclusively after the camera has been mounted and connected.

8.12 Attach the Camera to a Supported Video Management System

Once the camera has been mounted and its IP address identified or assigned, users can utilize the VMS Discovery and Attach procedures to connect the camera to a compatible Video Management System (VMS).

For more information, please refer to the VMS software documentation.

9. Thermal Imaging Overview

A thermal camera creates images by **detecting temperature differences** in its surroundings. Unlike visible light (daylight) cameras, which rely on photodetectors to capture reflected light from external sources such as sunlight or artificial illumination, **thermal cameras sense energy directly emitted by objects and surfaces**. This fundamental difference means that while visible light cameras—and even the human eye—depend on reflected light to reveal what’s present within a scene, **thermal cameras can visualize environments regardless of lighting conditions**.

Objects in everyday settings rarely emit visible light due to their relatively low temperatures, but **all objects continuously radiate infrared energy within the long-wave infrared spectrum (LWIR)**. Thermal cameras are specifically designed to detect this energy, enabling them to capture imagery even from extremely cold items like ice and snow. With time, users tend to find it more intuitive to interpret scenes containing familiar objects in thermal imagery.



The appearance of these thermal images is determined by palettes—color schemes that map different temperatures to specific shades. For example, using the standard WhiteHot palette displays warmer areas in white and cooler ones in black, as seen in the image above. The **Palette** option on the **Thermal** settings allows users to customize how temperatures are visually represented in the image.

Thermal cameras automatically adjust **image contrast** for most conditions, but **users can manually refine these settings for improved clarity**. Outdoor installation or exposure to sunlight may affect performance at different times of day. For instance, after sunset, surfaces warmed by the sun can retain heat and appear warm in thermal images, whereas those same objects might seem cooler than their surroundings before sunrise. Thus, **effective interpretation of thermal imagery involves noting subtle changes across the scene**, not just concentrating on the most prominent hot spots.

10. Configuring the Camera Using the Web Interface

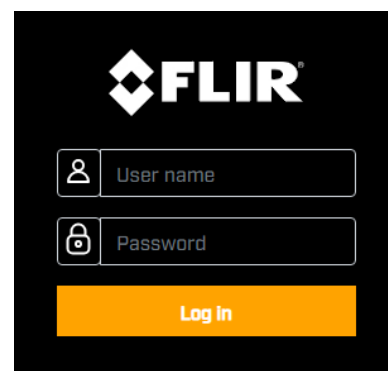
10.1 Accessing the Camera Web Interface

The camera can be configured and operated using the camera's web interface. The camera's web interface supports Google Chrome® and other popular web browsers. This guide uses Chrome as reference.

Logging in to the Camera's Web Interface

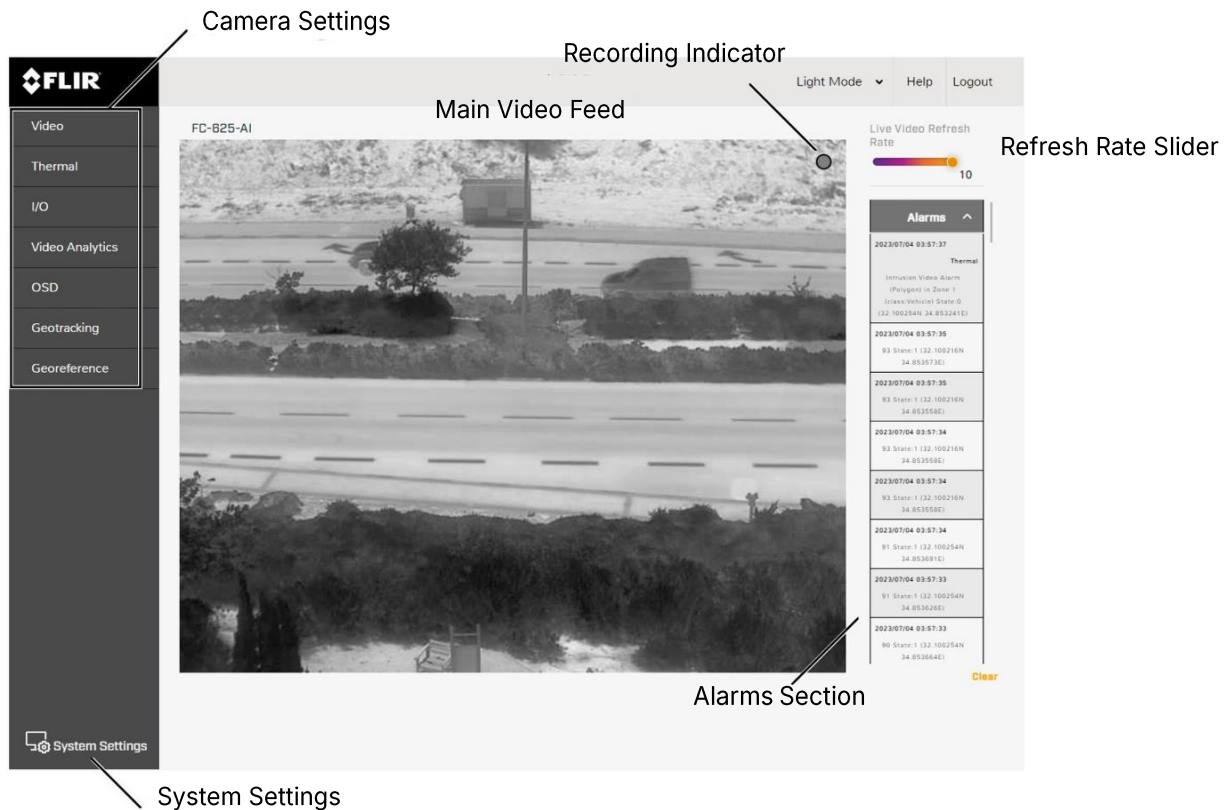
- Do one of the following:
 - In the [FLIR Discovery Network Assistant \(DNA\)](#) tool, **double-click the camera in the Discover List**.
 - The DNA tool does not require a license to use and is a free download from Teledyne FLIR. Download the DNA tool; unzip the file; and then double-click  to run 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.
- On the login screen, **enter your username and 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:
 - Username:** admin
 - Password:** admin
- 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.
 - Create a password consisting of:
 - At least 12 characters.
 - At least one uppercase letter.
 - At least one lowercase letter.
 - At least one number.
 - Can include the following special characters: |@#~!\$&<>+_-.,*?=-.
 - Log back in using the new password.**

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. When changing passwords via a web browser, it is essential to use HTTPS to safeguard the security of sensitive data.
- The camera web interface's **home screen** is displayed.



10.2 Web Interface Home Screen

The camera's web interface is organized to facilitate navigation and monitoring. The home screen is divided into sections that offer access to primary functionalities. The number of options displayed will depend on the user's role, for more information please see [Users](#) section.



Top Navigation Bar

Located in the upper-right corner, this bar features:

- **Light Mode:** Switches between light and dark display themes.
- **Help:** Provides access to assistance through official guides or comprehensive documentation.
- **Logout:** Exit the interface securely.

Main Video Feed Area

At the center of the window, a live video feed from the camera is displayed, providing up-to-the-minute surveillance visuals.

Left Sidebar - View Settings Menu

Available to Expert and Admin users only, this vertical menu provides quick access to core settings:

- **Video:** Configure the video stream, including codec, resolution, bitrate, etc.
- **Thermal:** Configure specific settings for the thermal video stream.
- **I/O:** Configure internal and external input/output settings.

- **Video Analytics:** Configure Video Analytics, including managing regions and calibration.
- **OSD (On-Screen Display):** Configure on-screen display elements, such as date and time and camera name.
- **Geotracking:** Configure the Geotracking functionality, including arming or disarming alarms and managing regions.
- **Georeference:** Enter the geographical camera information, including coordinates, height, tilt angle, etc.

Click the **System Settings** gear icon at the bottom of the sidebar to open the system configuration panel.

Right Sidebar – Alarms Section

This section lists recent alarms with detailed metadata:

- **Timestamp:** Date and time of the event.
- **Alarm Type:** e.g., Intrusion Video Alarm.
- **Zone Number:** Identifies the monitored area.
- **Coordinates:** Latitude and longitude of the detected event.

Live Video Refresh Rate Slider

The **Live Video Refresh Rate** slider, located above the Alarms section, adjusts the refresh rate for the Live video preview. It is important to note that this setting does not impact the video stream delivered by the camera via ethernet.

Recording Indicator

On the top-right corner, a circular icon indicates if the camera is recording its feed to the internal microSD card.

10.3 Making Changes to Settings

The camera's configuration files store two sets of settings:

- **Factory Default Settings:** The original settings provided on the camera when it leaves the manufacturer. A partial factory reset restores all factory default settings except those on the [System Settings](#).
- **Saved Settings:** These are the settings saved as the camera is configured and operated. When the camera reboots, it restores these settings, so changes made since the last save are lost.



TIP

Whenever possible, **test new settings before saving them**, since saving changes overwrites the previously saved settings.

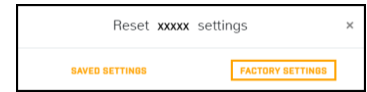
Camera Settings

Changing most View Settings activates the Reset and Save buttons. Some settings apply changes instantly without saving (like on the Thermal Page), while others require users to save before changes take effect. Select **Save** to keep all unsaved modifications since the last save.

RESET

SAVE

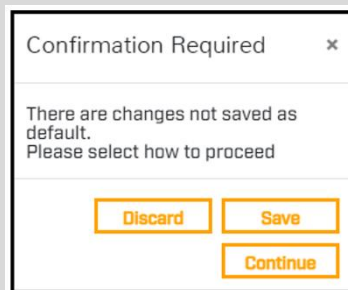
To restore previously saved settings or factory defaults, click **Reset**. The camera can be restored to the last saved settings or to the factory settings. To close the message without restoring settings, click the close icon on the top-right corner.



TIP

If you move to a different page before saving your changes, a confirmation message will appear. You can:

- Click **Continue** to navigate and test the changes, then return to save them.
- **Discard** the changes.
- **Save** the changes
- Close the confirmation message without discarding or saving by clicking the **Close** icon.



System Settings

When users adjust most System Settings, the **Discard Changes** and **Save** buttons become active. Some settings are applied immediately but not saved (such as on the Alarm Page), while others require users to save before changes take effect.



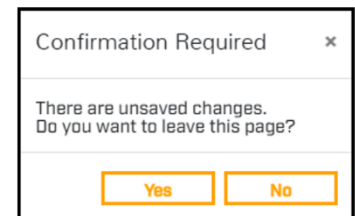
Click **Save** to keep changes, or **Discard Changes** to revert to the previous settings or factory defaults.

Some System Setting changes require the camera to reboot, such as those on the Settings and Date & Time page. After selecting **Save**, a confirmation message appears. To apply the changes and restart the camera, select **Accept**. To close the message without saving or discarding changes, select **Cancel** or the close icon.



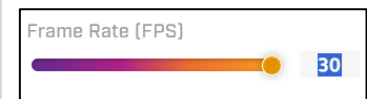
TIP

If you navigate away from a page before saving your changes, **a confirmation message will appear**. To leave the page and discard your changes, click **Yes**. To close the message without discarding or saving, click **No** or the close icon.



TIP

When adjusting sliders, you can either **slide the handle** left or right to change the value or **double click on the number and enter the desired value**, then pressing Enter to apply.



10.4 Camera Settings

Video

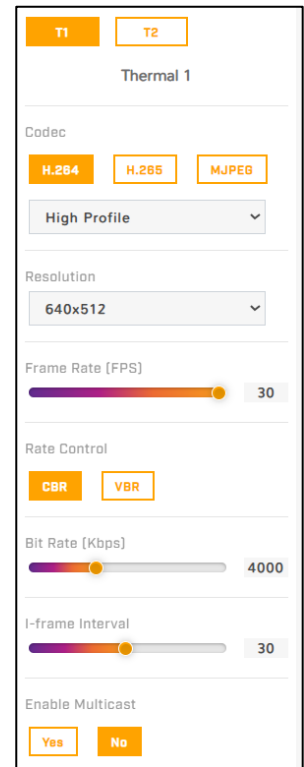
The camera delivers **two IP video streams** (Thermal 1 [T1] and Thermal 2 [T2]). Typically, it is not required to alter the default video configurations. However, in certain instances—such as transmitting a stream over a wireless network—adjusting the video stream parameters may be beneficial for reducing bandwidth consumption.

To change the settings for a particular video stream, click the relevant button (T1 or T2).

Codec options

Choosing the right codec is crucial for ensuring compatibility with the intended workflow. The selected codec can impact the quality, storage requirements, and accessibility of the video footage. The available options are:

- **H.264:** This codec is widely used in security cameras for its high compression efficiency, which means it can deliver good video quality at lower bitrates. This helps in saving storage space and bandwidth, making it suitable for continuous recording and remote streaming
- **H.265:** Also known as HEVC (High Efficiency Video Coding), this codec offers even better compression efficiency than H.264, providing higher quality video at lower bitrates. It's ideal for high-definition and 4K security cameras, as it allows for longer storage durations and smoother streaming without compromising on video quality
- **MJPEG:** Motion JPEG compresses each video frame as a separate JPEG image. While it doesn't offer the same compression efficiency as H.264 or H.265, it is simpler and can be useful for applications where individual frames need to be accessed quickly, such as in forensic analysis or video editing



Resolutions

This dropdown menu offers the different resolution options available for the video streams.

Frame Rate

The frame rate can be adjusted within a range of 5 to 30 frames per second.



TIP

To ensure optimal image quality and overall system performance, FLIR recommends configuring the camera to operate at a **frame rate of 30 fps**.

Codecs, Quality, and Bandwidth

The video 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** and **H.265** codecs, users can set the:

- **Profile:**
 - **High Profile** (only available for H.264): 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.
- **Bit 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.

With the **MJPEG** codec, users can set the:

- **Quality** between 0-100.
 - 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

1. **Initially use the default values.** Then, incrementally modify and test individual parameters to determine when bandwidth and quality requirements are met.
2. On the camera's web interface, **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.
3. You can **view a snapshot of live video** using the following URL:
http://<camera_IP_address>/images/snapshots/IRimage.jpeg.

Enable Multicast

By default, **multicast is enabled**. Multicast video packets are distributed among streaming clients. The addition of more clients does not significantly increase bandwidth usage compared to unicast. Requests for video streams from ch0/stream1 are handled using unicast, meaning each client receives an individual stream. The way multicast requests are processed may vary depending on the client's capabilities or settings, which can influence whether the client receives a dedicated multicast stream or connects differently

Enable Multicast

☒ Yes ☐ No

Destination Address

224.1.1.1

Destination Port

50000

TTL

3

Enable Multicast

☒ Yes ☐ No

Destination Address

224.1.1.2

Destination Port

50002

TTL

3

T1

T2

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.

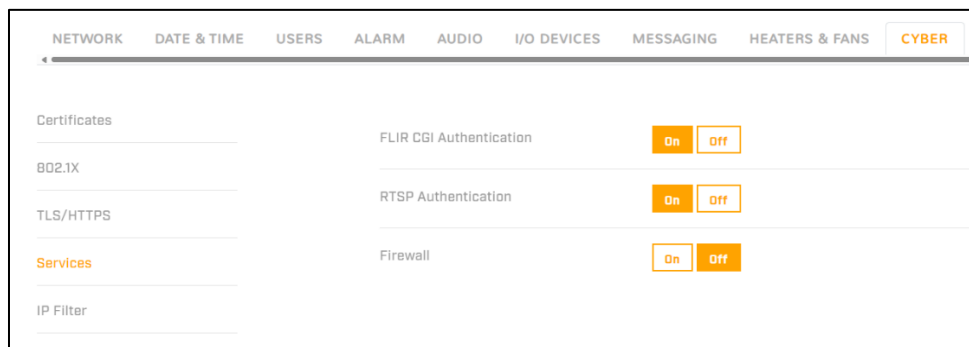
The **time-to-live** field controls the ability of IP packets to traverse network boundaries. A value of 1 restricts the stream to the same subnet. Greater values allow increasing access between networks.

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

- **T1:** rtsp://<camera_IP_address>:554/stream1
- **T2:** rtsp://<camera_IP_address>:554:554/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, use the name and password for any of the camera's users. Users assigned to the role of admin or expert can disable RTSP authentication on the **Services** section of the Cyber tab in the **System Settings**.



Thermal

In most installations, **changing the default settings of the thermal imager is not necessary**. However, in some situations and depending on the scene, modifying one or more parameters can improve the image. Be aware that, when conditions change, it might be necessary to adjust the parameters again. Teledyne FLIR recommends knowing how to restore the factory default settings (see [Firmware & Info](#)) before experimenting with the settings.

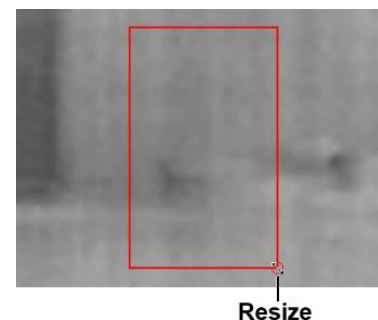
AGC ROI

By default, **Show AGC ROI** is enabled. The AGC ROI (Automatic Gain Control Region of Interest) overlay appears on the live video feed within the camera's web interface but is excluded from video streams. The default setting defines the ROI as the entire frame, allowing the AGC algorithm to evaluate the full image. In certain scenarios, **specifying an ROI that omits part of the scene may enhance image quality**. For instance, setting an AGC ROI that excludes colder regions such as the sky can help reduce their impact on the overall image.

Defining a Custom AGC ROI

To change the size of the ROI: Hover over the bottom-right corner of the ROI, and then click and drag it.

To move the entire ROI: Hover over the ROI, and then click and drag it.





WARNING

The camera's thermal Video Analytics rely on accurate and useful AGC settings. Changes to the ROI can affect VA.

AGC Image Settings

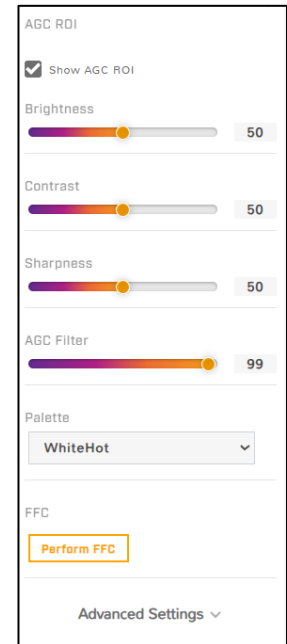
In some cases, changing the AGC image settings can provide a better image, depending on personal preferences, display devices, etc.

- **Brightness** (Gamma): Determines the allocation of the 256 shades produced by the AGC. Values above 50 allocate more shades to hotter objects, while values below 50 allocate more shades to lower temperature objects. Range: 0 to 100.
- **Contrast** (Max Gain): Increasing contrast can provide a better image, especially for scenes with little temperature variation. (It might also increase noise due to the increased gain.) Range: 0 to 100.



TIPS

Changes to the default contrast setting affect scenes with little temperature variation more than they affect scenes with greater temperature variation.



AGC ROI

☒ Show AGC ROI

Brightness 50

Contrast 50

Sharpness 50

AGC Filter 99

Palette
WhiteHot

FFC
[Perform FFC](#)

Advanced Settings ▾

- **Sharpness** (DDE Gain): Enhances details and/or suppresses fixed pattern noise. Range: 0 to 100.
- **AGC Filter**: Determines how quickly a scene adjusts when a hot object enters (or exits) the AGC ROI. If set to a low value, when a hot object enters the ROI, the AGC will adjust more slowly to the hot object, resulting in a more gradual transition. Range 0 to 100.
- **Palette**: Selects the color palette the camera uses to indicate detected levels of thermal energy. WhiteHot and BlackHot are gray-scale palettes; other palettes assign different colors to different temperatures. **When VA is enabled on the Video Analytics settings, the camera automatically uses the WhiteHot color palette.**
- **FFC (Flat-Field Correction)**: Click Perform FFC to manually initiate this process. During FFC, the thermal imager's shutter closes to provide a uniform temperature reference, which enables the device to **adjust for changes in ambient temperature and maintain accurate imaging**. The thermal image temporarily pauses during this adjustment. The camera also performs FFC automatically at set intervals or when it detects significant ambient temperature changes. This process is also referred to as Non-Uniformity Correction (NUC).

Advanced Settings

The **Equalization** menu provides tools to enhance image contrast and detail visibility by redistributing pixel intensity values. It offers two main equalization modes and several fine-tuning parameters:



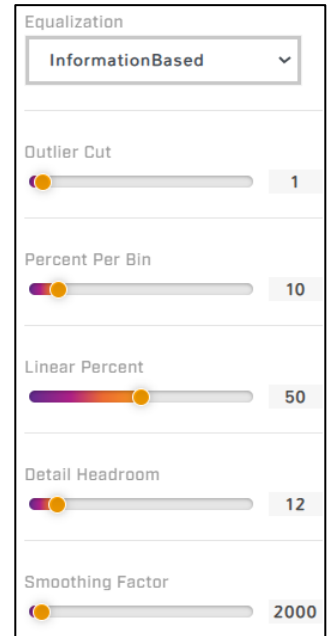
WARNING

Change the thermal sensor's advanced settings **only at the recommendation of Teledyne FLIR Support**. If not done properly, changing these settings can permanently damage the camera.

- **Plateau:** This mode limits the frequency of pixel intensity values to prevent over-enhancement of dominant tones. It helps maintain a balanced contrast by capping histogram peaks.
- **Information based:** This mode adjusts the image based on the distribution of information content, aiming to enhance areas with meaningful visual data while suppressing noise.

Each of these modes can be customized using the following parameters:

- **Outlier Cut:** Removes extreme pixel values to reduce noise and prevent distortion.
- **Percent Per Bin:** Controls the percentage of pixels allocated to each histogram bin, affecting contrast distribution
- **Linear Percent:** Determines the proportion of the image processed with linear scaling, balancing between linear and equalized output.
- **Detail Headroom:** Reserves intensity range for fine details, preventing them from being flattened during equalization.
- **Smoothing Factor:** Applies smoothing to the histogram to reduce abrupt transitions and artifacts.



Equalization

InformationBased

Outlier Cut

Percent Per Bin

Linear Percent

Detail Headroom

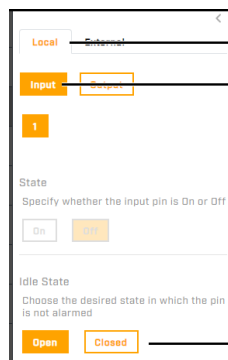
Smoothing Factor

I/O (Input/Output)

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

Local I/O

Input Pin

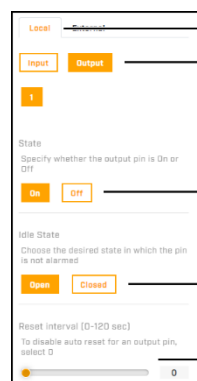


Select Local

Select Input

Select idle state

Output Pin



Select Local

Select Output

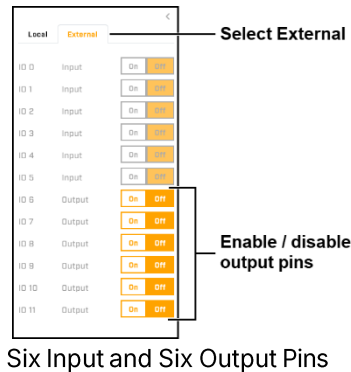
Enable / disable

Select idle state

Specify reset interval

For more information on the local I/O connector, see [Connecting the Camera](#).

External I/O



Six Input and Six Output Pins

In the [I/O Devices settings](#) in the [System Settings](#), Admin or expert users can configure the camera's external I/O connections and the device managing those connections with the camera.

AI Video Analytics Capabilities

The camera features advanced onboard AI Video Analytics, integrating an AI model that is **specifically optimized for 3D environments**. This model leverages deep neural networks along with sophisticated motion detection algorithms to deliver enhanced video analytics, particularly for **intrusion detection scenarios**.

Object Detection and Classification

The system is capable of **accurately classifying detected objects as either humans or vehicles**. Vehicle detection covers a range of types, including cars, vans, and small trucks, as well as vehicles up to 15 meters in length. However, larger vehicles, such as long trailers, forklifts, and heavy vehicles with unique shapes—such as construction vehicles—are not detected or filtered by the analytics system.

Configurable Detection Areas

The thermal video AI can be configured to **monitor specific zones for security events**. Users can define **tripwires, intrusion zones, and loitering detection areas**, allowing for flexible and targeted surveillance based on the needs of the installation site.

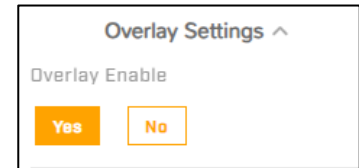


Configuring Video Analytics

1. Make sure the camera is **mounted in its final location and properly aimed**. Mounting orientation (tilt) should ideally be at a horizon level close to top of the scene.
2. On the Georeference settings, **specify the camera's installation height, tilt angle, and roll angle**.

3. Enable VA overlay:

- Click on **Overlay Settings**. The overlay menu opens.
- Under **Overlay Enable**, select **Yes**.



4. Enable VA:

- At the top of the page, under **Enable**, select **Yes**.
- By default, VA is disabled. When VA is enabled, **the camera automatically switches to the WhiteHot thermal color palette** (see [Thermal settings](#)).




WARNING

After enabling Video Analytics, changing the thermal palette to a different one is possible, but it is not recommended as it may affect the performance and accuracy of the video analytics.

5. Calibrate VA:

- See [VA Calibration](#) section.

6. Specify Motion Sensitivity Level:

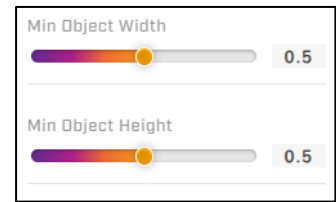
- In Advanced Settings, go to **Motion Sensitivity Level**.
- Click on the dropdown menu to choose the appropriate level.



Motion Sensitivity Level	Applicability
Low Motion Sensitivity	Enables detection of discreet human intrusions at very close range.
Medium Motion Sensitivity*	Enables detection of discreet human intrusions at an optimal range.
High Motion Sensitivity**	Increases maximum detection distance for upright and discreet human intrusions.
Ultra Motion Sensitivity***	Increases maximum detection distance for upright and discreet human intrusions.
* Can handle minor camera movements and vibration ** Requires the camera to withstand wind gusts *** Requires the camera to be stable, not move or vibrate	

8. Specify **Min Object Width/Height** (Fusion AI and DNN AI only):

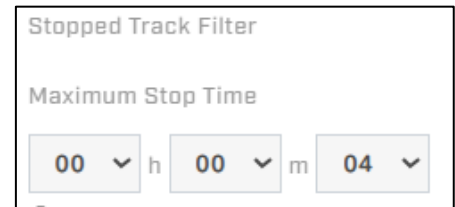
- In Advanced Settings go to **Min Object Width** and **Min Object Height**.
- **Enter the correct value:**
 - Use the Teledyne FLIR recommended minimum width and height of 0.3 meters to filter out small animals, such as birds, cats, or rabbits.
 - To filter out larger animals such as dogs, foxes, etc., specify a larger minimum, 0.5 meters width and 0.6 meters height, or larger if necessary.
 - The minimum object width should not exceed 0,5 meters to accurately detect human intruders and not small animals such as the rabbits seen in the picture. Users can reduce nuisance alarms from various animals by applying the recommended object size filter settings shown in the table:




Animal filter setting (Object size)	Width (meters)	Height (meters)
Bird, Rabbit, Small Cat (Default setting)	0.3	0.3
Large Birds (Stock, Swan), Hare, Dog, Wild Cat, Fox, Wolf	0.4	0.5
Large animals	0.5	0.7

9. Specify the **Maximum Stop Time** of a detected object:

- In Advanced Settings, go to **Stopped Track Filter**.
- Here users can specify the following:
 - **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.
 - **Apply for Vehicles:** Filters out vehicles that are stopped so that they do not trigger an alarm.

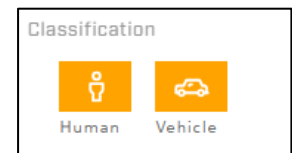


10. **Create VA Regions:**

- The camera's onboard VA detects intrusion or loitering and classifies detected objects separately for each region.

11. **Activate human and/or vehicle detection** in each region:

- **Click on the name of the region.**
- Under Classification, **click on the Human and/or Vehicle** icon to activate.
- In the VA tracking overlay, H indicates a detected and classified human; V indicates a vehicle.



12. **Configure the VA tracking overlay.**

- Expand the dropdown menu where users can enable or disable the following:

Setting		Comments
Enable	Globally enable or disable the VA overlay.	
Regions	Show intrusion regions, loitering regions, and trip wires.	
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 active; that is, when they are triggering a trip wire, intrusion, or loitering alarm.	Enable Human Tracks or Vehicle Tracks. Enable Show Class, Show Lines, or Show Boxes.
Streams	Enable the VA tracking overlay for individual video streams.	Does not override the global VA 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 tracking overlay for a stream might not affect the live video.



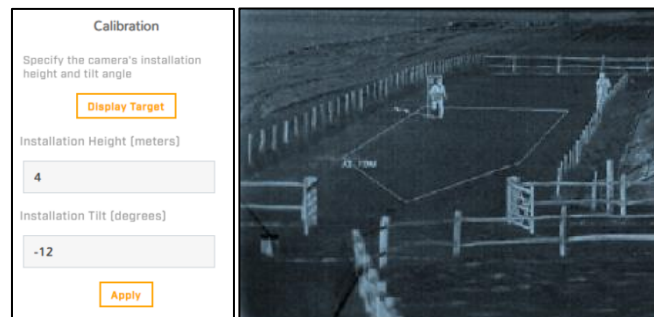
TIPS

For information regarding how to configure the VA for specific situations and optimal detection results, see [Recommended Guidelines](#).

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

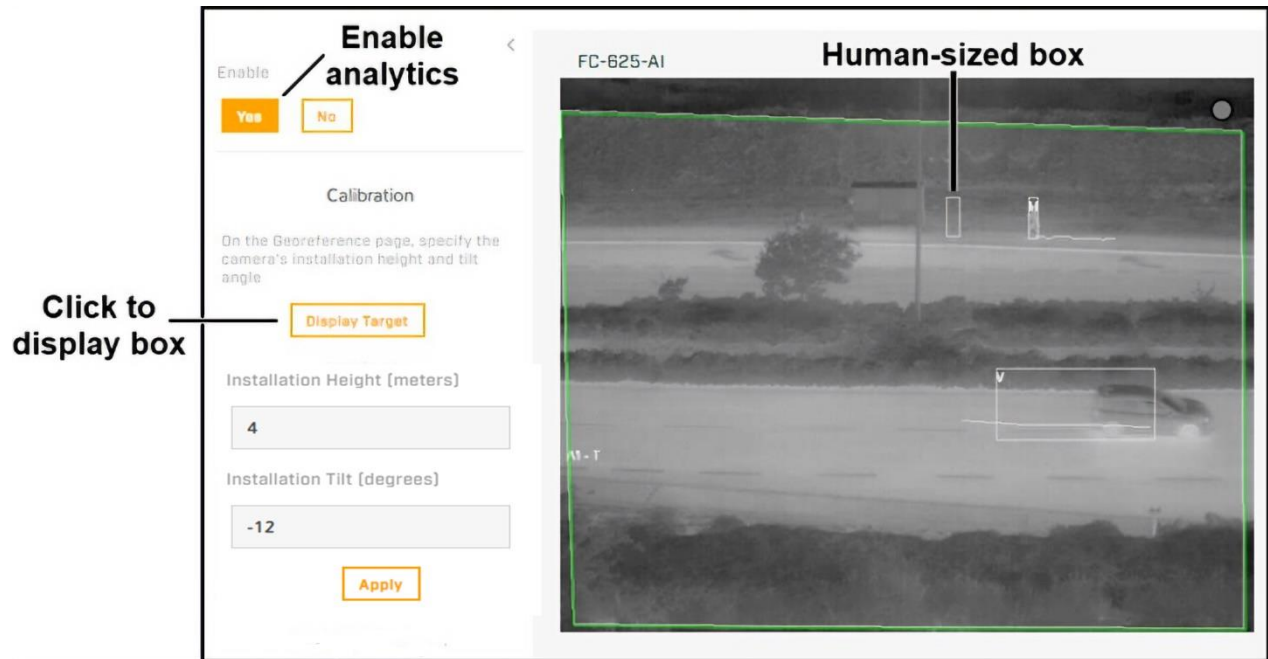
Video Analytics Calibration Check

Before users can check the camera's VA calibration, it is necessary to **specify the camera's installation height, tilt angle, and roll angle**. You will normally do this in the [Georeference settings](#), but the Height and Tilt values can be changed in the Video Analytics settings in order to facilitate fine tuning.



Verification of calibration is essential for accurately distinguishing between human and non-human intrusions. To perform this verification:

1. Select the **Display Target** button and **request a person in the field to move to different locations** within the camera's coverage area, including both the closest and farthest points from the camera.
2. When the person stops, **click on the corresponding position** on the screen to generate the **target box**. The detection human boxes indicate the standard height of a person (1.80 m/5'11"). If the **target box closely aligns with the actual size of the subject, the calibration is correct**.
3. Should the target box appear disproportionately large or small, please **recalibrate the camera** changing the height and tilt values, and try displaying the box again.



TIPS

1. Make sure that a person about **1.8 m (5' 11')** tall is in the camera's field of view.
2. On the Video Analytics page, make sure **analytics are enabled**.
3. Expand Overlay Settings and make sure **Overlay Enable is On**.

If the height of the box does not correspond to the size of the person:

1. On the Georeference settings, **verify the camera's installation height, tilt angle, and roll angle**. Mounting orientation (tilt) should ideally be at horizon level close to top of the scene.
2. When far away, if the **human box is too small**, the virtual horizon needs to be higher, so increase the tilt angle.
3. When far away, if the **human box is too large**, the virtual horizon needs to be lower, so decrease the tilt angle.

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, if possible.
- Start the detection zone **3-5 meters away from a fence line or boundary**.
- Apply to **flat surface terrains** with no tall grass or slopes.
- Use **Masking Level 2 or 3**.
- **Do not apply Fusion AI to road facing scenes** with dynamic activity, such as frequent vehicle traffic.

Types of Video Analytics Regions

There are two main types of regions in video surveillance systems: **Detection Regions** and **Masking Regions**.

Detection regions are user-defined areas within the video feed **where the system actively monitors and classifies objects**, such as humans or vehicles. These regions include **tripwires, intrusion detection areas, and loitering detection areas**, each serving a unique purpose in identifying and responding to potential security threats.

On the other hand, **masking regions** are areas **where video analytics are intentionally disabled** to prevent false alarms caused by non-threatening movements, such as swaying trees or moving shadows. By strategically configuring both detection and masking regions, users can ensure that their surveillance system is both efficient and accurate, focusing on relevant activities while minimizing unnecessary alerts.

Detection Regions:

Detection regions can classify objects as humans or vehicles. These regions include:

- **Tripwires:**

Tripwires may be configured as either bidirectional (the default setting) or unidirectional. This configuration allows the system to monitor movement in both directions or in a single direction, depending on operational requirements.

- **Intrusion detection areas:**

Intrusion detection zones may be configured to utilize either Deep Neural Network (DNN) detection, which is the default setting, or Motion detection. DNN detection employs sophisticated algorithms to accurately identify and categorize objects, whereas Motion detection relies on monitoring variations within the video stream.

- **Loitering detection areas:**

Loitering detection areas enable users to define a specific loitering time, representing the period during which an individual or vehicle must stay within the designated area before an event is activated. This functionality is valuable for monitoring and identifying potentially suspicious activities or unauthorized presence in particular zones.

Masking Regions:

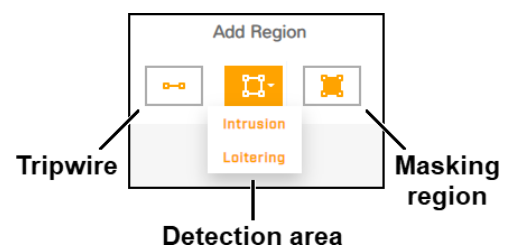
Masking regions are areas of the video image where Video Analytics (VA) are disabled, and no alarms are triggered. These regions are useful for preventing false alarms caused by non-threatening movements, such as trees or bushes swaying in the wind. Users can create up to eight masking regions.

Creating VA Regions

Adding Regions

To add a region, follow these steps:

1. **Tripwire:** Click the Tripwire icon to create a tripwire.
2. **Detection Area:** Click the Detection Area icon to create a detection area.
 - **Intrusion:** Select this option to create an intrusion detection area.
 - **Loitering:** Select this option to create a loitering detection area.
 - **Masking Region:** Click the Masking Region icon to create a masking region.



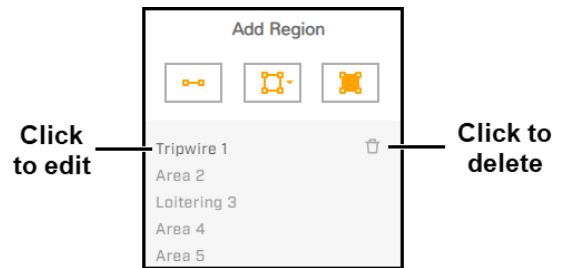
3. **Draw the region** by clicking on the video feed to add points to the polygon.
4. **Do not click and drag.**
5. Make sure the **regions do not overlap.**
6. To finish creating the region, **double-click on the last point** and a line will be drawn automatically closing the polygon.
7. To cancel creating a region, press **Esc.**



Editing VA Regions

To modify the settings for or to delete an existing region, **select the region either from the region list or in the live video image.**

- To **move or adjust**:
 - **Region points**: click and drag the points
 - **Tripwires**: click and drag the lines.
 - **Entire regions**: click and drag the border.
- To **delete a region**, click on the trash icon 🗑️ next to its name.



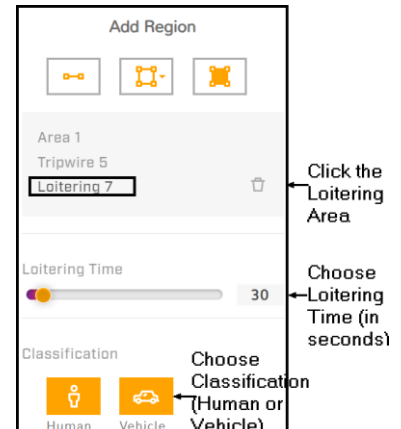
The specific configuration parameters vary depending on the region type, as seen in the table below:

Region type	Direction	Human and Vehicle Classification	Loitering Time	Intrusion Detection (DNN or Motion detection)	Advanced Settings Fuse DNN Area
Tripwires	*	*		*	*
Intrusion		*		*	*
Loitering		*	*	DNN Only	*
Masking	N/A			Level 2 enabled (DNN only)	Level 2 enabled

Configuring Loitering Detection Areas

To configure a Loitering Detection area:

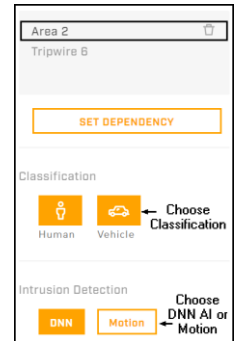
1. **Select the area from the list**: Options for Loitering Time and Classification are displayed.
2. **Choose loitering time** (0 - 600, in seconds).
3. **Choose Human and/or Vehicle Classification.**



Configuring Intrusion Detection Areas

To configure an Intrusion Detection area:

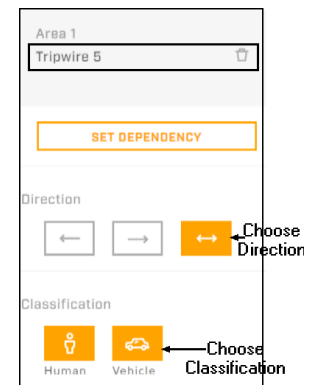
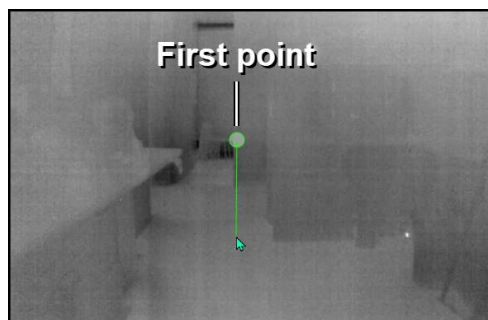
1. **Select the area from the list:** Options for classification are displayed.
2. Choose **Human and/or Vehicle** classification.
3. Choose **DNN** (default) or **Motion** detection.



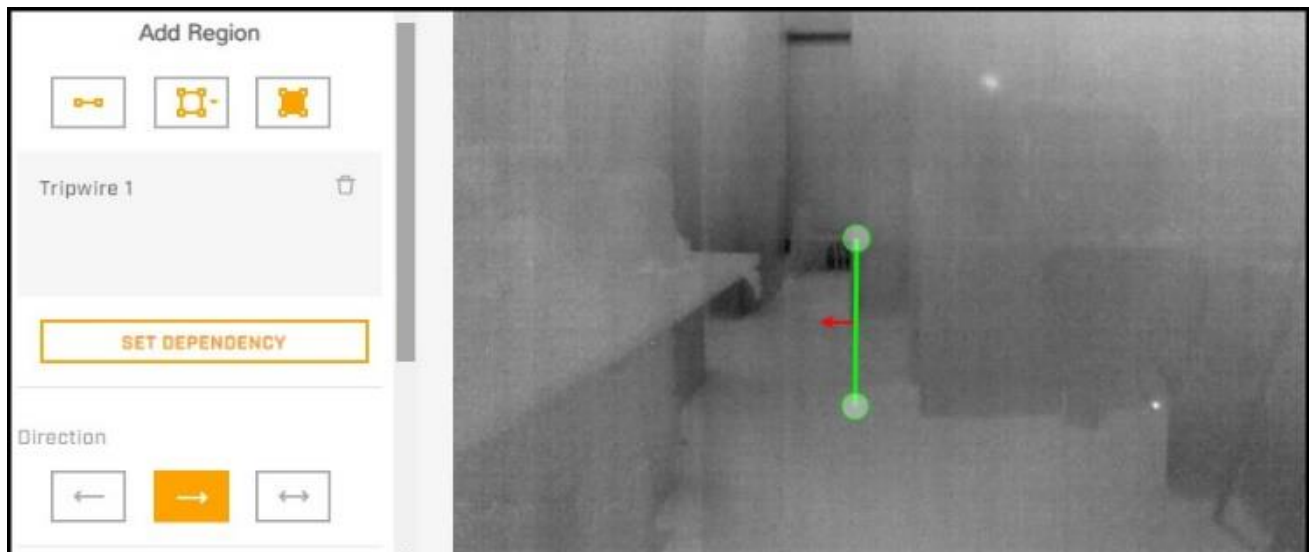
Configuring Tripwires

To configure a Tripwire:

1. **Select the tripwire from the list:** Options for Direction and Classification are displayed.
 2. **Choose bidirectional** (default) **or unidirectional** (left or right).
 3. The direction selection arrows refer to the **direction of movement** over the tripwire, as seen in the examples below.
- In the image below, the first point of a tripwire has been defined, and the tripwire is being drawn from top to bottom.



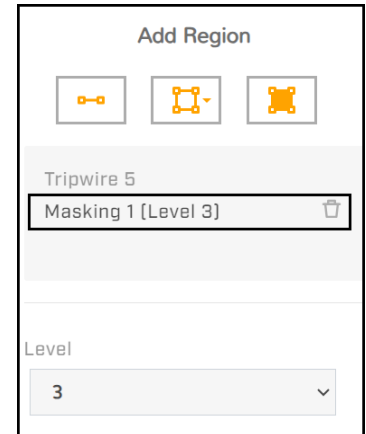
- In this image, the tripwire has been completed, and the *left-to-right* direction button has been selected. Because detection direction relates to the first tripwire point created, the direction arrow in the video is *right to left* and the camera triggers alarms when it detects movement over the tripwire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



Configuring Masking Regions

To configure a Masking region:

1. **Select the tripwire from the list.** Masking Level options are displayed.
2. For each masking region, **the level can be specified:**
3. **Level 3** (default): Completely blocks detection of all objects in the region.
4. **Level 2:** Apply for detecting normal upright and discrete human intrusions at 50% or above confidence level. Supported when DNN or Fuse DNN Area is enabled.



Display Region Labelling

When the VA overlay is enabled for the Video Analytics page live video, tripwires and VA regions are labeled according to:

1. **Region type:** T = tripwire, A = intrusion detection area, or L = loitering.
2. **Unique region ID number.**
3. **Video image type:** T=thermal video.
4. **VA type:** D=DNN, M=motion detection, DM=Fuse DNN Area enabled.

For example, A2-TDM= intrusion detection area 2 on the thermal video with Fuse DNN Area enabled.



Region Dependencies

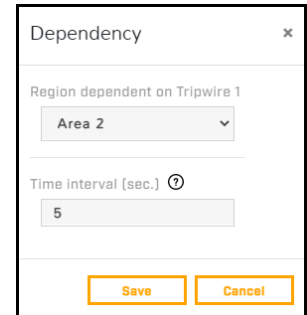
In order to make the most of the Video Analytics, it is possible to dependencies between two regions.



In the image above, Area 1 is dependent on Area 4. This means **that Area 1 will only trigger an alarm if Area 4 is triggered first.**

To **establish a 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 alarm.
4. Click **Save**.



Dependency

Region dependent on Tripwire 1

Area 2

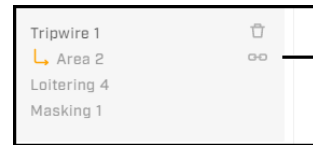
Time interval (sec.)

5

Save Cancel

To **remove a dependency**:

1. Click the link icon corresponding to the dependent region.



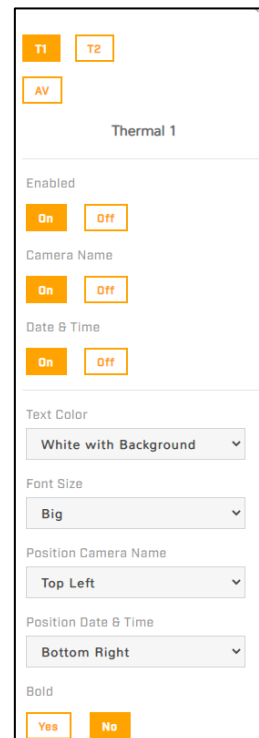
Click to remove dependency

OSD (On-Screen Display)

For each IP video stream (T1 and T2), users can:

1. Enable or disable the **camera's on-screen display** (OSD).
2. Enable or disable only the **camera name**.
3. Enable or disable only the **date & time**.
4. Users 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 T1 stream, the OSD appears in the live video on the camera's web interface. Enabling OSD on the T2 stream does not affect the live video on the camera's web interface.



T1 T2

AV

Thermal 1

Enabled

On Off

Camera Name

On Off

Date & Time

On Off

Text Color

White with Background

Font Size

Big

Position Camera Name

Top Left

Position Date & Time

Bottom Right

Bold

Yes No

Geotracking

The geotracking functionality **enables advanced spatial awareness and automated tracking capabilities** by integrating fixed cameras—such as the FCB-Series AI—with FLIR Security PTZ cameras that support geotracking. Once paired, **the PTZ camera dynamically engages geotracks generated by the fixed camera's video analytics**, allowing for real-time object tracking across defined alarm regions and exclusion zones. This system leverages georeferenced mapping, calibrated coordinates, and classification filters to ensure precise detection and engagement of targets classified as people or vehicles. Configuration is managed independently from video analytics, offering flexible control over detection thresholds, virtual tracks, and camera behavior within mapped environments.



IMPORTANT

Before enabling geotracking, make sure that the **camera's VA is enabled** on the [Video Analytics settings](#). However, even though geotracking requires the camera's VA to be enabled, geotracking configuration is separate from VA configuration.



NOTE

You can pair one or more FCB-Series AI with a FLIR Security PTZ camera that supports geotracking. When the cameras are paired, the PTZ camera engages the geotracks from the FC-Series AI cameras.



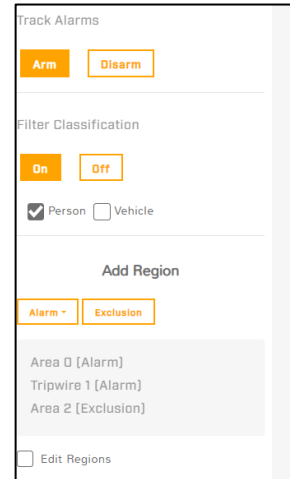
Detected intrusions tracked.

The following objects are recognized and displayed on the Geotracking and Georeference screens:			
	Fixed camera—The circle around this icon indicates the FC-Series AI camera you are currently configuring.		Geotracking alarm region
	PTZ camera		Geotracking exclusion region
	Radar		Detected object

	Geotracking range		Detected object in geotracking alarm region
	VA detection range		Object engaged by PTZ camera

The Geotracking menu includes the following options:

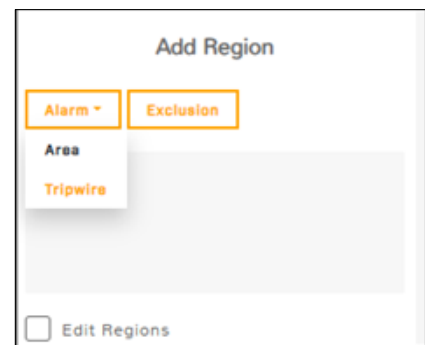
- **Track Alarms:** Allows users to activate or deactivate tracking using the "Arm" and "Disarm" buttons.
- **Filter Classification:** Enables filtering by object type including a toggle button ("On"/"Off") and checkboxes for "Person" (enabled) and "Vehicle" (disabled).
- **Add Region:** Lets users define new areas with options to add either "Alarm" (Areas or Tripwires) or "Exclusion" regions.
- **Regions List:** Displays existing regions and their types, such as "Area 0 (Alarm)", "Tripwire 1 (Alarm)", and "Area 2 (Exclusion)".
- **Edit Regions:** A button at the bottom which enables modifying the listed regions.



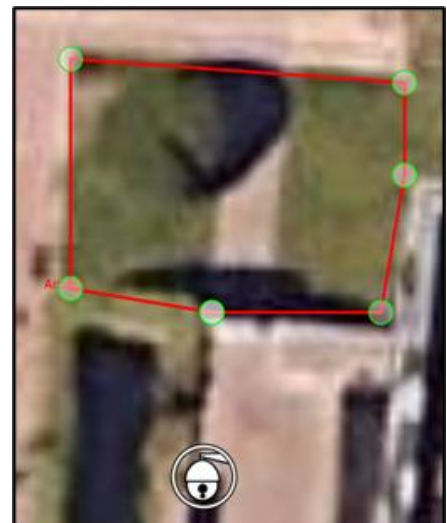
Adding a Geotracking Region

1. Select one of the Add Region options:

- **Alarm (Area or Tripwire):** Triggers geotracking alarms. In the detection area display, alarm areas and tripwires are displayed in red. Users can specify a geotracking alarm region as the trigger for a camera alarm. When a camera is paired with a FLIR Security PTZ camera that supports geotracking, it is possible to specify that the PTZ camera only engages geotracking alarm tracks.
- **Exclusion:** The camera does not detect objects and does not trigger geotracking alarms. In the detection area display, exclusion 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** by clicking on the map.
3. **Continue adding points** by clicking on the map (up to 25).
4. To complete the region, **double-click on the last point you want to add**, and a line will be automatically drawn, closing the polygon.
5. To cancel creating a region, press **Esc**.



Managing Geotracking Regions

Editing Regions

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

- **Move region points** by holding and dragging the point.
- **Define a tripwire's detection direction.**

By default, tripwires are bidirectional. However, users 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**.

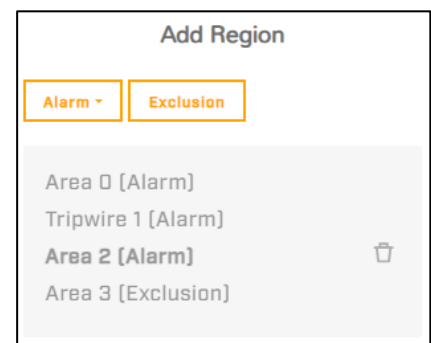


In the image above, the first point of a tripwire has been defined, and the tripwire is being drawn from top to bottom. Below, the tripwire has been completed, and the left-to-right direction button has been selected. Because detection direction relates to the first tripwire point created the direction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

Please note, **when Edit Regions is selected, it is not possible to add regions.**

Deleting Regions

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

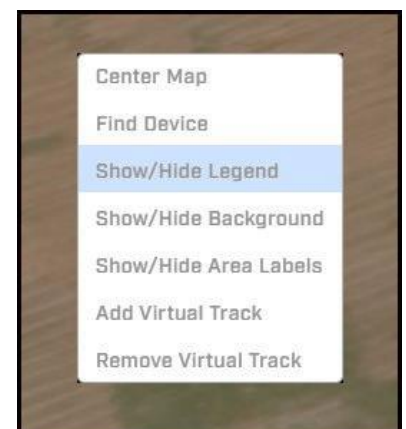


Navigating the Map

To move the map, click and drag with your mouse. Use the mouse scroll wheel to zoom in or out.

Right-click on the map 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 saving the camera's coordinates or calibrate a map, the camera's position can be outside the display window.
- **Show/Hide Legend:** Toggles legend display.
- **Show/Hide Background:** Toggles the map or background image.
- **Show/Hide Area Labels:** Toggles area labels in the display.
- **Add/Remove Virtual Track:** Toggles a virtual geotrack that can be used to test features such as PTZ pairing and geotracking.

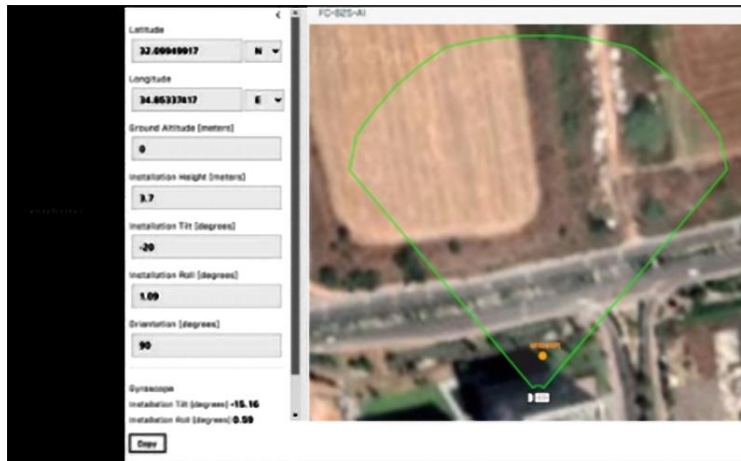


Please note that these right-click options are also available in the Georeference screen display.

Georeference

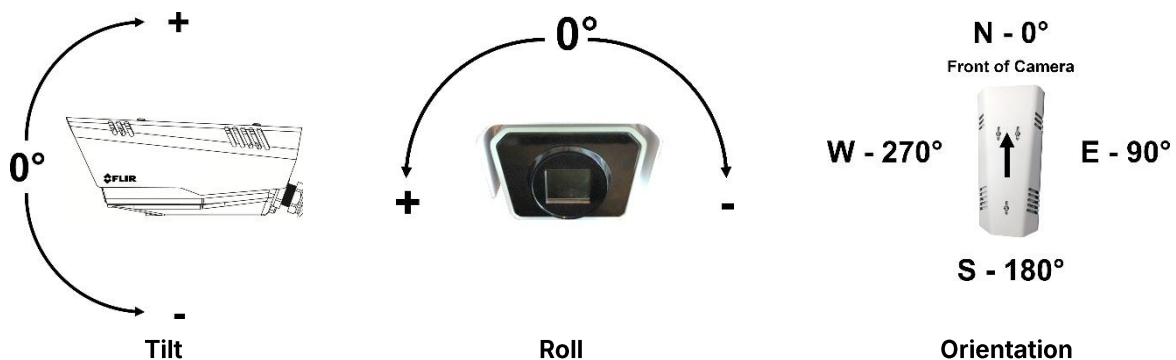
In the Georeference menu, users can enter the **camera's geographic coordinates and mounting details** required to calibrate geotracking and video analytics functions. For a smoother setup, **it's best to configure the [Map settings](#) in System Settings beforehand.**

1. Identify the camera's **geographical information**, which includes latitude (specified as degrees North or South) and longitude (specified as degrees East or West), accurate to eight decimal places. Coordinates may be obtained using a map, a GPS-enabled mobile device, or using the **Flir Raven site planning platform**.



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 users do not save changes within a few seconds, the camera restores the previous latitude and longitude settings and moves the camera icon back.

2. Enter the **mounting information**, including:
 - **Ground Altitude:** in meters above or below sea level, up to two decimals.
 - **Installation Height:** in meters above the ground, up to two decimals (must be greater than zero).
 - **Installation Tilt:** The vertical angle of the camera, up to three decimal places. When a camera is pointing down (below horizontal), the tilt angle is negative.
 - **Installation Roll:** The horizontal rotation angle of the camera, up to three decimal places. Facing a camera leaning to the right, the roll angle is negative.
 - **Orientation:** 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 0° installation roll angle. For accurate VA, mount the camera with an **installation roll angle within $\pm 5^\circ$** .
- 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 NEXUS® SDK, CGI, or ONVIF**, which:

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

11. System Settings

Users with the admin or expert role can select **System Settings** to open the related configuration pages.

- [Network](#)
- [Date & Time](#)
- [Users](#)
- [Alarm](#)
- [Audio](#)
- [I/O Devices](#)
- [Messaging](#)
- [Heaters & Fan](#)
- [Cyber](#)
- [Media Browser](#)
- [ONVIF](#)
- [Map](#)
- [Scheduler](#)
- [Recording](#)
- [SD Card](#)
- [Firmware & Info](#)



TIP

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.



IMPORTANT

Each time configuration settings are changed, you need to **wait 20 seconds before performing a reboot**. If you do not wait, the new settings will not be saved.

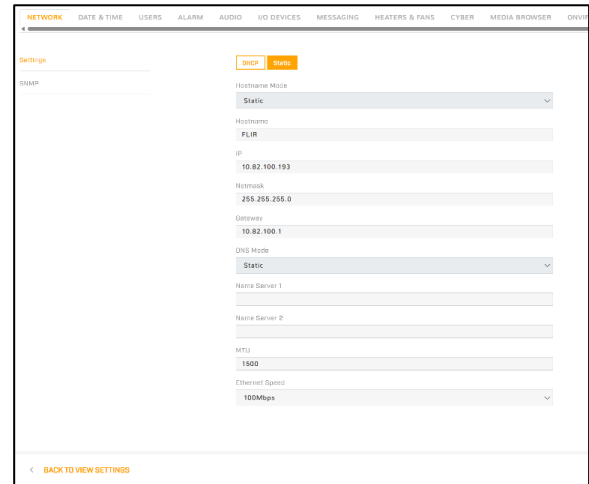
For information about making, applying, and saving changes on System Settings pages, see [Making Changes to Settings](#).

11.1 Network

The Network tab allows users to access and modify networking and SNMP (Simple Network Management Protocol) settings for system configuration. These settings are essential for ensuring proper device connectivity and communication within a networked environment.

If you are unsure about how to configure the networking or SNMP settings, it is recommended that you consult your network administrator for assistance. Proper configuration is important to maintain stable connectivity and optimal system performance.

The Network tab includes two different configuration panels: Settings and SNMP.



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 access the camera's web interface. To access the web interface again, change the PC's IP address to be on the same network as the camera.

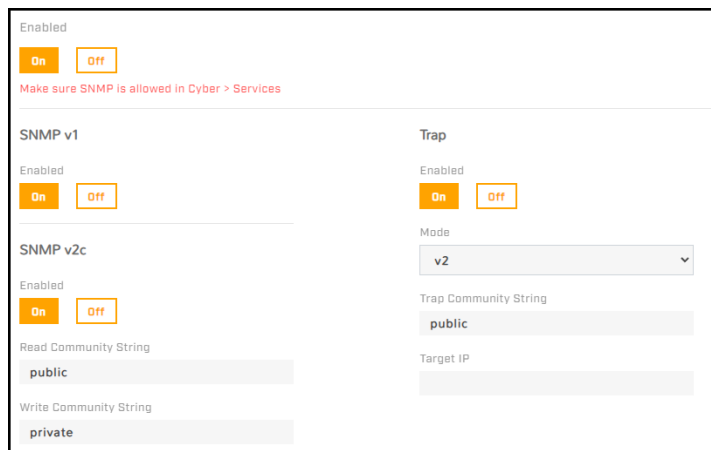
- **Netmask:** The default value is 255.255.255.0.
- **Gateway:** Specify the gateway address, which acts as an access point or IP router that the camera uses to communicate with devices outside its local network segment.
- **DNS Mode:** When the IP address mode is DHCP, users can set the DNS Mode to 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.
- **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 100Mbps. When set to Auto, the camera supports 10/100 Mbps.

SNMP

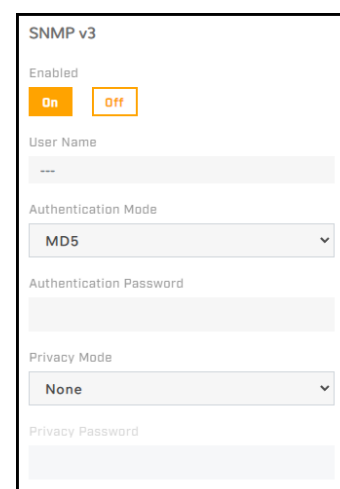
In the SNMP section, users can enable and configure SNMP (Simple Network Management Protocol). **SNMP allows network management systems to monitor and to remotely manage the camera.** By default, all SNMP features are disabled.




IMPORTANT

- For cybersecurity reasons, please **change the default community strings**.
- If you are enabling SNMP, on the [Cyber settings](#), 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** introduces robust security features designed to protect network communications. It ensures **confidentiality** by encrypting packets, thereby preventing unauthorized sources from snooping. It also provides **message integrity**, guaranteeing that packets remain unaltered during transit and optionally includes protection against packet replay attacks. Additionally, SNMP v3 supports **authentication**, verifying that each message originates from a legitimate 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 it, 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.

11.2 Date & Time

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

When DHCP IP addressing is enabled in the settings, users 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.

Manually Configuring 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

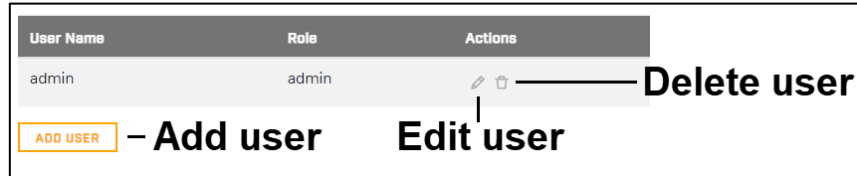
Email notifications and other camera features require configuring the camera's system time to be the current time. You can configure email notifications on the [Messaging settings](#).

11.3 Users

Only users assigned the **admin role** can add, edit and delete users and change or set all passwords.

Users assigned the **expert role** only see the user currently logged in, and cannot add, edit, or delete users. To maintain security of the system, set up usernames and passwords for each required login account.

The camera limits user name length to 29 characters. Passwords must have the following attributes:



- At least 12 characters
- Contain at least one number
- Contain at least one lowercase letter
- Contain at least one uppercase letter
- 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

- Open the **Add User** dialog box.
- Fill in the following fields:
 - **Username** (e.g., "darose").
 - **Password** and **Confirm Password**.
 - **Role** selection (e.g., "expert").
- To **retain the current password**, leave the password fields empty.
- Click **Save** to create the user or **Cancel** to discard changes.

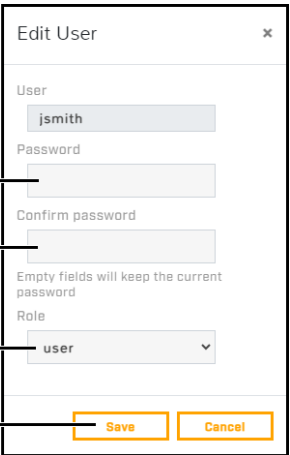


Edit User

- Access the **Edit User** dialog box.

The **User** field is pre-filled (e.g., "jsmith").

- Update the following as needed:
 - **Password** and **Confirm Password**
 - **Role selection** (e.g., "user")
- Click **Save** to apply changes or **Cancel** to exit without saving.



The **Edit User** dialog box contains the following fields and controls:

- User:** A text field with the value "jsmith".
- Password:** A text field.
- Confirm password:** A text field.
- Role:** A dropdown menu with the value "user".
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

Annotations with arrows point to the Password, Confirm password, Role, and Save buttons.

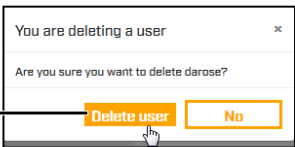
Delete User

User Name	Role	Actions
admin	admin	 
expert	expert	 
user	user	 
darose	user	 

ADD USER

Click trash can icon

Click to confirm



The confirmation dialog box contains the following text and controls:

- Title:** "You are deleting a user"
- Message:** "Are you sure you want to delete darose?"
- Buttons:** "Delete user" and "No" buttons.

1. **Locate the user in the list** (e.g., "darose").
 - Click the **trash can icon** under the Actions column.
2. A confirmation dialog will appear:
 - Click **Delete user** to confirm.
 - Click **No** to cancel the deletion.

11.4 Alarm

It is possible to define camera alarms to be triggered by:

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

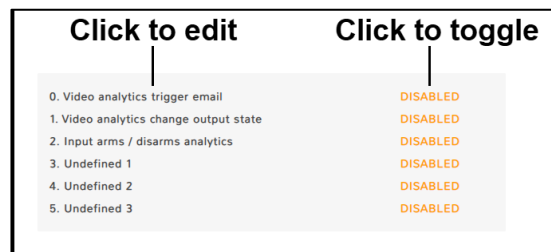
For each alarm, users can specify one or more of the following actions, such as:

- **Change the state** of local or external I/O connections, i.e. to turn on a light or play a prerecorded P.A. message.
- **Arm/disarm the camera's Video Analytics** (available when Video Analytics is not the rule's trigger).

- **Send a notification email.**
- **Save a snapshot image of the live video.**

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 settings](#).
- **1. Video analytics change output state:** The camera's VA triggers a change to the state of a 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 settings](#).
- **2. Input arms / disarms analytics:** A change in the state of the local alarm input connector enables or disables the onboard VA.

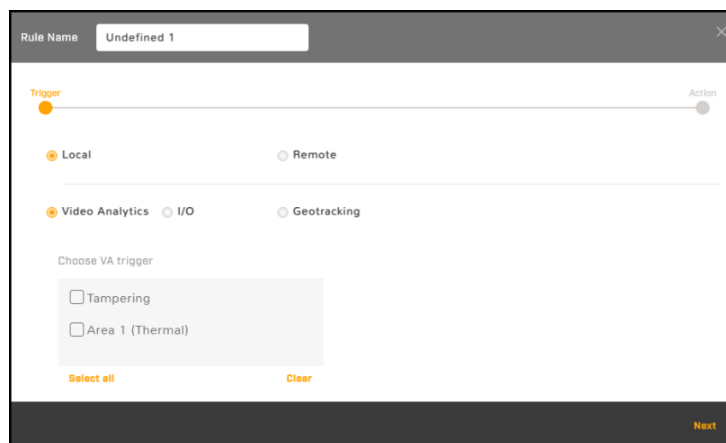


Users can modify the name, trigger, and action for the default rules. For example, users can modify the **Video Analytics changes output state** rule so that it changes the state of an external output connected VMS system, instead of the state of an alarm out local I/O connector.

Users can also define and enable three additional rules:

- 3. Undefined 1**
- 4. Undefined 2**
- 5. Undefined 3**

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 settings](#).



Modify an Existing Alarm Rule or Define an Alarm Rule:

1. **Click the alarm name.** The rule trigger settings appear.
2. Modify or Define the **Rule Triggers**, see section below.
3. Modify or Define the **Rule Actions**, see section below.
4. Enable or disable a rule by clicking **Enabled** or **Disabled**.

Modify or Define Rule Triggers

1. Modify or define the **rule name**.
2. Select whether the triggers are **local** (onboard the camera) or **remote** (external), see tables below.
3. Click **Next**. The rule action settings are displayed.
4. Continue with **Modifying or Defining Rule Actions**.

Local Triggers		
Video Analytics	The camera's onboard VA trigger this rule's action.	On the Video Analytics settings, make sure tripwires, intrusion detection and/or loitering regions have been defined. Select the tripwires and/or regions that trigger this rule's action. Users can also select tampering as a trigger. After the camera has been powered on for 24 hours, blocking the thermal sensor of the camera for one minute triggers this rule's action.
I/O	Local: The camera's local I/O connections trigger this rule's action.	On the I/O settings, make sure local I/O connectors have been properly configured. Select one or more local I/O connections that trigger this rule's action.
	External: The camera's external I/O connections trigger this rule's action.	On the I/O settings and on the I/O Devices settings, make sure the external I/O connections and the device managing those connections with the camera have been properly configured. Select one or more external I/O connections that trigger this rule's action.

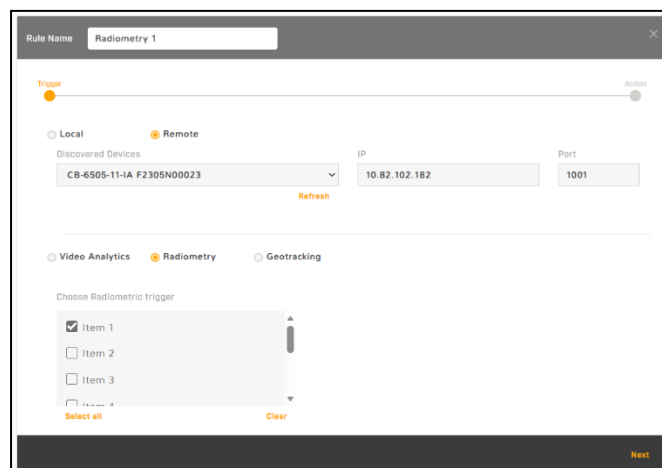


TIP

Specifying a trigger for an alarm rule and enabling the rule does not enable alarms for the trigger, make sure VA/geotracking is enabled.

Remote Triggers		
1. Select the triggering device from the Discovered Devices drop-down menu: The IP address and port are displayed. 2. Users can also manually specify the remote device IP address and port. 3. Click Refresh to save. The drop-down menu of discovered devices is also refreshed. Click Refresh once the remote device is connected to the same network as the camera. The camera discovers supported devices on the same network as the camera. However, only devices on the same VLAN as the camera can be used as a trigger.		
Video Analytics	VA from a supported remote camera or device trigger an alarm.	On the remote camera or other device, make sure VA is enabled and that at least one tripwire, intrusion detection/loitering region, or another analytics item has been defined. Select one or more VA items that trigger this rule's action.
Radiometry	Radiometry from a supported device triggers an alarm.	On the remote device, make sure radiometry detection is enabled and that at least one temperature threshold or region of interest has been defined. Select one or more radiometry conditions that trigger this rule's action.
Geotracking	A remote geotracking device triggers an alarm.	On the remote geotracking device, make sure detection is enabled and that at least one alarm area, tripwire, or other area has been defined. Select one or more geotracking device areas that trigger this rule's action.

The image below shows a discovered camera selected as the remote device and its radiometry item 0 selected as the trigger.



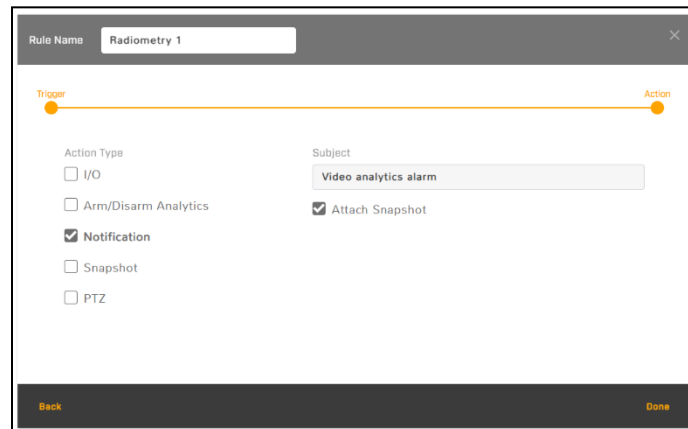
Modifying or Defining Rule Actions

1. For the alarm rule to be defined or modified, **select the checkbox for one or more action types**, see table below.
2. To configure an action type, **click the selected action type**. The selected action type is shown in bold, and the relevant settings are displayed.
3. Click **Done**.

Action Type	
I/O	Under I/O List, select Local or External: Local: This rule changes the state of one or more local output pins. On the I/O settings, make sure local I/O connectors have been properly configured. For each trigger defined for the alarm rule, select the local output pin that changes. External: This rule changes the state of one or more local output pins. On the I/O settings and on the I/O Devices settings, make sure the external I/O connections and the device managing those connections with the camera have been properly configured. For every trigger defined for the alarm rule, select the external output pin that changes. Users can map individual local or remote triggers to specific local or external output.
	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. Users can configure the Reset Interval for the local outputs on the I/O settings and for the external outputs on the I/O Devices settings.
Arm/Disarm Analytics (not available when this rule's trigger is Local > Video Analytics): When triggered, this rule toggles the camera's onboard VA from enabled to disabled or vice versa.	
Notification: When triggered, this rule sends notifications according to the settings on the Messaging settings. Specify a subject for the notifications. For email notifications, specify whether the camera attaches a snapshot. When notifications are enabled for an alarm rule, the camera sends all configured notifications. It is not possible to enable or disable individual notification types. Therefore, to differentiate between notifications triggered by the camera's onboard VA, Teledyne FLIR recommends configuring alarm rules for each type of VA region (tripwire, intrusion, and loitering). Then, specify different subjects for each rule's notifications.	
Snapshot: When triggered, this rule records a snapshot image of live video.	

Arm/Disarm Geotracking (not available when this rule's trigger is the camera's onboard geotracking): When triggered, this rule **toggles the camera's onboard geotracking alarms** from enabled to disabled or vice versa.

The image below shows that the previously configured rule triggers a notification, including a snapshot of the video. Sais notification is configured in the [Messaging](#) settings.



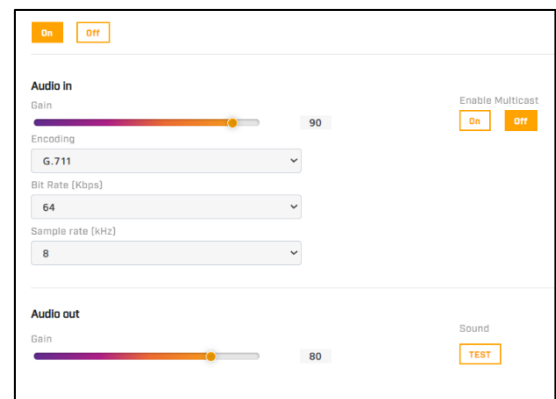
11.5 Audio

The Audio page provides configuration settings for and information about the camera's audio input and output features. The On/Off buttons control all audio; turning audio off instantly disables all camera sound.

Audio In

When audio is On, the following audio input settings are available:

- **Gain:** Users 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, users can adjust the audio line output gain from 0-100 percent. The default is 80 percent.

11.6 I/O Devices

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

Users 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.

For each pin, the following information is displayed, and users can configure:

- **I/O pin number**.
- **Type**: Input or Output.
- **State**: The pin's current state: Open or Closed.
- **Idle State**: Normally Open or Normally 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.

Additional details on configuring the device that manages external I/O connections can be found in the device's documentation.

Enabled Disabled

Device IP

Address

Port

127.0.0.1

502

Input base address

0

Output base address

0

I/O pins

Number of input pins

3

Number of output pins

3

Refresh

I/O	Type	State	Idle State	Alarm Auto Ack	Enabled	Reset Interval (seconds)*
0	Input	Off	Open	NO	YES	
1	Input	Off	Open	NO	YES	
2	Input	Off	Open	NO	YES	
3	Output	Off	Open	NO	YES	0
4	Output	Off	Open	NO	YES	0
5	Output	Off	Open	NO	YES	0

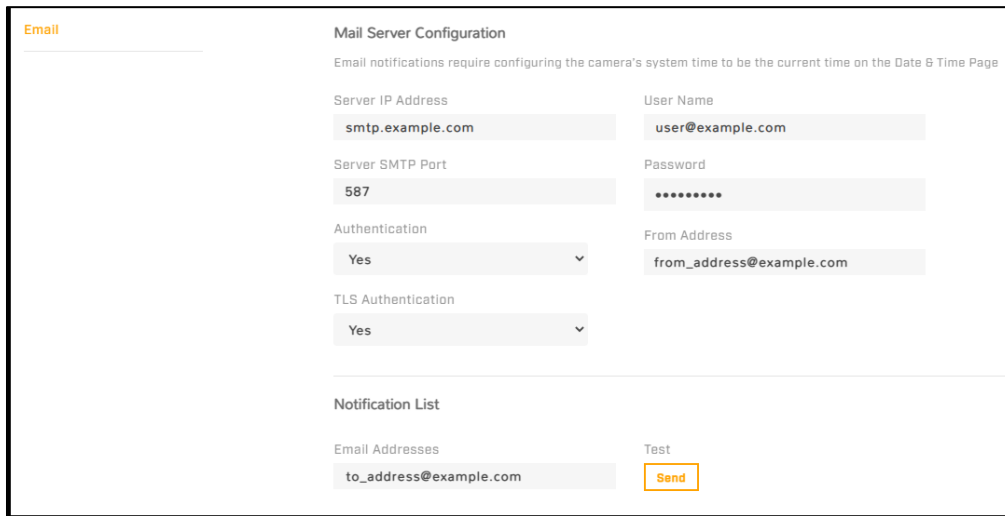
*To disable auto reset for an output pin, select 0 (0-600 sec)

11.7 Messaging

As an action for an alarm rule, the camera can **send notifications** according to the following on the Messaging settings:

- **Email.**
- **Generic XML.**
- **Milestone Generic Events.**
- **Custom Fixed Generic Events.**

Email



The screenshot shows the 'Email' configuration page. It has a left sidebar with 'Email' selected. The main area is titled 'Mail Server Configuration' and includes a note: 'Email notifications require configuring the camera's system time to be the current time on the Date & Time Page'. The configuration fields are as follows:

Field	Value
Server IP Address	smtp.example.com
User Name	user@example.com
Server SMTP Port	587
Password	
Authentication	Yes (dropdown)
From Address	from_address@example.com
TLS Authentication	Yes (dropdown)

Below the configuration fields is the 'Notification List' section, which includes an 'Email Addresses' field with the value 'to_address@example.com' and a 'Test' button labeled 'Send'.

- **Mail Server Configuration:**
Specify the settings for the SMTP server in the appropriate fields. Settings include:
 - 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**.
 - **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.
- **Notification List:**
Specify one or more email addresses, separated by commas, to receive the notifications. To test the mail server settings and the notification list, click **Send**.



TIP

For the camera to properly send email, the camera's **date and time must be correctly configured** on the [Date & Time settings](#).

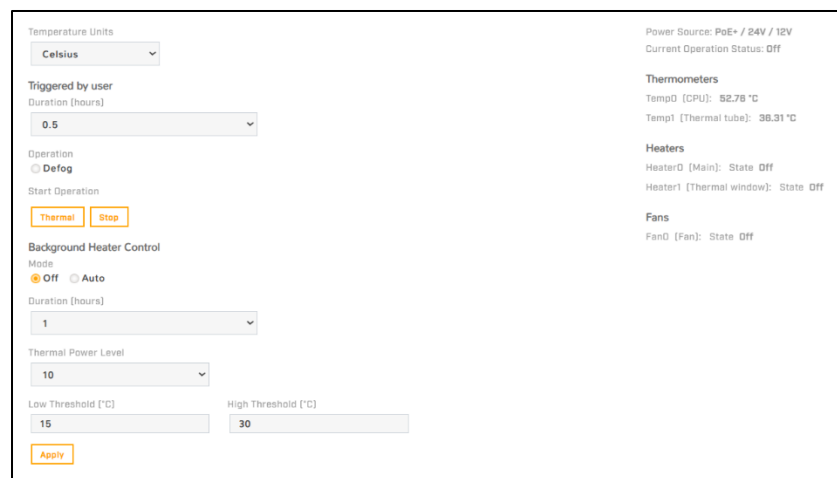
11.8 Heaters & Fans

The Heaters & Fans settings provide configuration for:

- **Defogging.**
- **Automatic background heating** features.
- **Temperature information** for camera components.
- **Status information** for the camera's onboard heaters and cooling fan.

By default, the **Background Heater Control is turned off**. When configuring the camera, it is recommended to turn on Auto Mode.

The thermometer readings, heaters, and fans will function **based on the user supplied settings** for the Background Heater Control.



It is also possible to select the unit of temperature: Celsius, 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 **Thermal**. The status of the thermal window heater changes from Off to On. To deactivate the operation, click **Stop**.

Background Heater Control

By default, background heater control is set to Off. If enabled, specify:

- **Thermal Power Level** (0-15): adjusts the **intensity or output of the heater** when it is active, being 0 the lowest setting and 15 the maximum.
- **Temperatures at which the heaters activate** (Low Threshold) and **deactivate** (High Threshold). It is recommended to set:
 - **Low Threshold:** 5 degrees below the ambient temperature.
 - **High Threshold:** 10 degrees above the ambient temperature.

Status Information

On the right side of the window, the following status information is displayed:

- **Power Source:** Indicates which power supplies are connected to the camera (PoE+ / DC / AC).
- **Thermometers:** Temperatures for camera components.
- **Heaters:** Status of the camera's heaters (On or Off).
- **Fans:** Status of the camera's fan.



IMPORTANT

If early condensation is seen on the window of the camera, you may need to increase settings for Low and High Threshold, and hours for Heater Control.

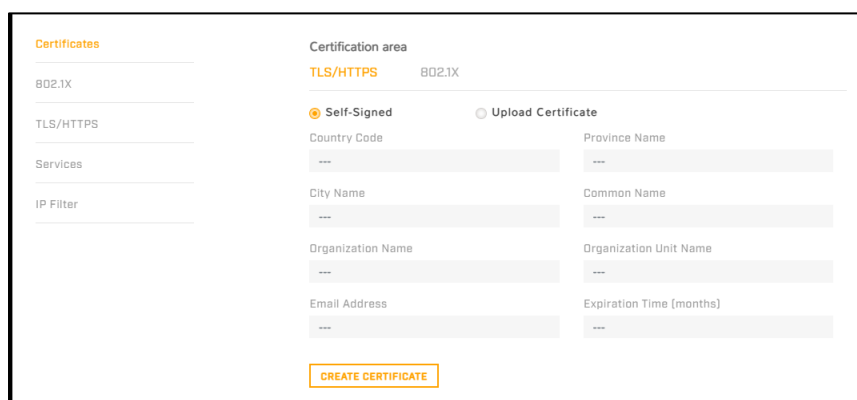
11.9 Cyber

The Cyber settings provide 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.

Certificates



Prior to enabling TLS/HTTPS or 802.1X, it is necessary to generate or upload a valid certificate. This can be accomplished using the camera's web interface to either create a self-signed certificate, upload an existing self-signed certificate, or upload a certificate issued by a trusted third party. If you require assistance with these configurations, please consult 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

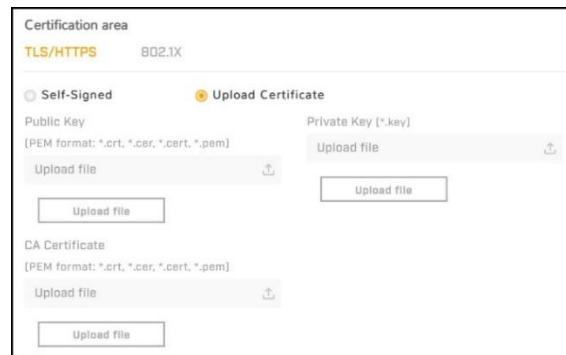
From the Certificates section of the Cyber page, you can download certificates and keys previously uploaded to or generated by the camera. If the certificate saved on the camera is self-signed, you can download the private and public key files. If the certificate was signed by a third-party CA, you can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

Generating and installing 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 is displayed.

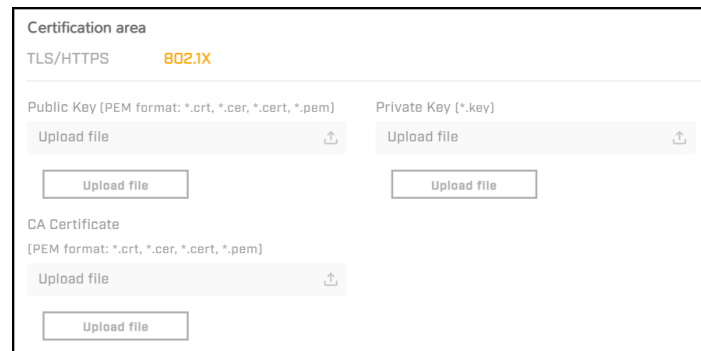
Uploading a self-signed or third-party CA signed certificate for TLS/HTTPS or for 802.1X

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



The screenshot shows the 'Certification area' with 'TLS/HTTPS' and '802.1X' tabs. The 'Upload Certificate' option is selected. It displays fields for 'Public Key' (format: *.crt, *.cer, *.cert, *.pem) and 'Private Key' (format: *.key), each with an 'Upload file' button. Below these is a 'CA Certificate' field (format: *.crt, *.cer, *.cert, *.pem) with an 'Upload file' button.

To Upload a Certificate for TLS/HTTPS



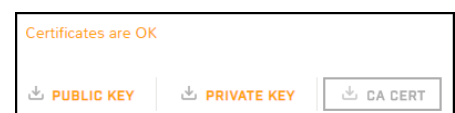
The screenshot shows the 'Certification area' with 'TLS/HTTPS' and '802.1X' tabs. The 'Upload Certificate' option is selected. It displays fields for 'Public Key' (format: *.crt, *.cer, *.cert, *.pem) and 'Private Key' (format: *.key), each with an 'Upload file' button. Below these is a 'CA Certificate' field (format: *.crt, *.cer, *.cert, *.pem) with an 'Upload file' button.

To Upload a Certificate for 802.1X

2. If uploading a self-signed certificate, under **Public Key** and then under **Private Key**:
 - **Select the Public Key file.**
 - **Click on Upload File.**
 - **Select the Private Key.**
 - **Click on Upload File.**

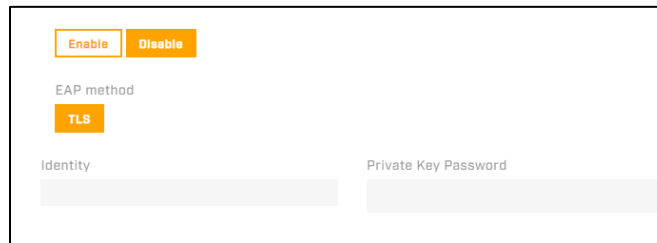
If uploading a **third-party CA signed certificate**, select and upload the Public Key, Private Key, and CA Certificate.

3. Verify that the camera certificate files are valid and make sure "Certificates are OK" is displayed above the certificate information, under Download certificate.



The screenshot shows a confirmation message 'Certificates are OK' in orange. Below it are three download buttons: 'PUBLIC KEY', 'PRIVATE KEY', and 'CA CERT', each with a download icon.

802.1X



Users can enable or disable **IEEE 802.1X-compliant TLS communication**. To configure it, provide the **Identity** and the **Private Key Password**. The default value is disabled.

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

TLS/HTTPS

Users can enable or disable the following security options for camera communication:

- Control:** Enabling **Transport Layer Security (TLS)** and **Secure HTTP (HTTPS)** ensures that all communication between the client and the camera is encrypted. This prevents sensitive data, such as login credentials or control commands, from being intercepted by unauthorized parties. TLS provides encryption and integrity checks, while HTTPS uses TLS to secure HTTP traffic.
- HTTPS redirect:** When this option is enabled, any attempt to access the camera using an unsecured HTTP connection will automatically be redirected to HTTPS. This guarantees that all sessions use a secure channel, reducing the risk of man-in-the-middle attacks or data exposure.



Both options are disabled by default. This means that, unless configured, the camera will accept unencrypted HTTP connections, which **could expose sensitive information on unsecured networks**.

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

Services

Users can enable or disable the following security and access control options for the camera:

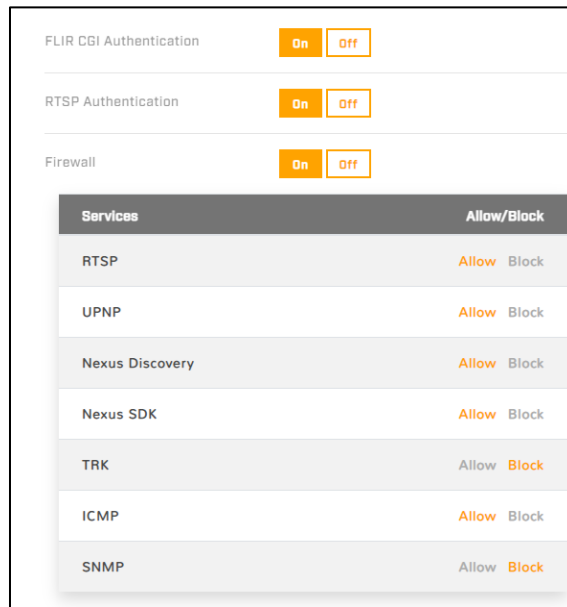
- FLIR CGI authentication:** Enables Digest authentication, which adds a layer of security when accessing the camera's CGI (Common Gateway Interface) control interface. Instead of sending credentials in plain text, it uses a challenge-response mechanism with hashing, which helps protect against credential theft during transmission. This is **especially important when managing cameras over unsecured networks**.
- RTSP authentication:** The Real-Time Streaming Protocol (RTSP) is used to deliver live video streams from the camera. When RTSP authentication is enabled, users must provide valid credentials before accessing the video stream. Disabling this option removes the authentication requirement, which can make the stream vulnerable to unauthorized access. For security reasons, it is **strongly recommended to keep RTSP authentication enabled**, particularly in production or public-facing environments.

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

- Firewall:** The built-in firewall enables users to manage which services can communicate with the camera. Users can **allow** or **block** specific protocols such as:
 - RTSP:** Controls video streaming access.

- **UpnP:** Universal Plug and Play for device discovery.
- **Nexus Discovery / Nexus SDK:** Used for integration with FLIR Nexus services.
- **TRK:** Tracking-related services.
- **ICMP:** Internet Control Message Protocol, often used for ping and diagnostics.
- **SNMP:** Simple Network Management Protocol for monitoring and management.

By selectively allowing or blocking these services, users can reduce the attack surface and prevent unauthorized access to unused or unnecessary protocols.



The screenshot shows a configuration interface with three toggle switches at the top: "FLIR CGI Authentication" (On), "RTSP Authentication" (On), and "Firewall" (On). Below these is a table for service settings.

Services	Allow/Block
RTSP	Allow Block
UPNP	Allow Block
Nexus Discovery	Allow Block
Nexus SDK	Allow Block
TRK	Allow Block
ICMP	Allow Block
SNMP	Allow Block



CAUTION

Disabling services and ports can affect product functionality.

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

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).

1. To define specific IP addresses that can access the camera, click **Allow**. The camera will deny access to all other IP addresses.
2. To define specific IP addresses that cannot access the camera, click **Deny**. The camera will allow access to all other IP addresses.
3. 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**. It is possible to specify up to 256 IP addresses.
4. To remove an IP address from a list, click the corresponding **trash icon**

11.10 Media Browser

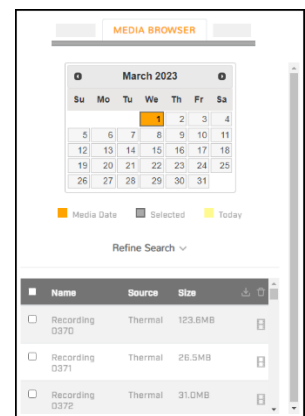


When recorded files exist on a properly installed and formatted microSD card, users can **preview and access** those files on the Media Browser tab.

Users can:

- **View files by clicking on the date:** orange indicates recorded files exist for that date.
- **Refine the search** filtering using:
 - Specific times.
 - Media type (Snapshot , Video , or All).
 - Video source: Visible or Thermal, if available.

When a single file is selected, a preview of the file is displayed, except for video files encoded using H.265.



**TIP**

Video file previews do not play back at the full recorded frame rate. To view the video in its original quality and to watch video files encoded with H.265, please download the files and use multimedia playing software, such as VLC.

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

When users download a file, the default file name format is:

SOE1-<source>_VIDEO001_<source>_<start_time>_<end_time>_<x>_<yyyy>.mp4, where:

- <source> is the stream recorded: T1 / T2.
- <start_time> and <end_time> are Unix timestamps.

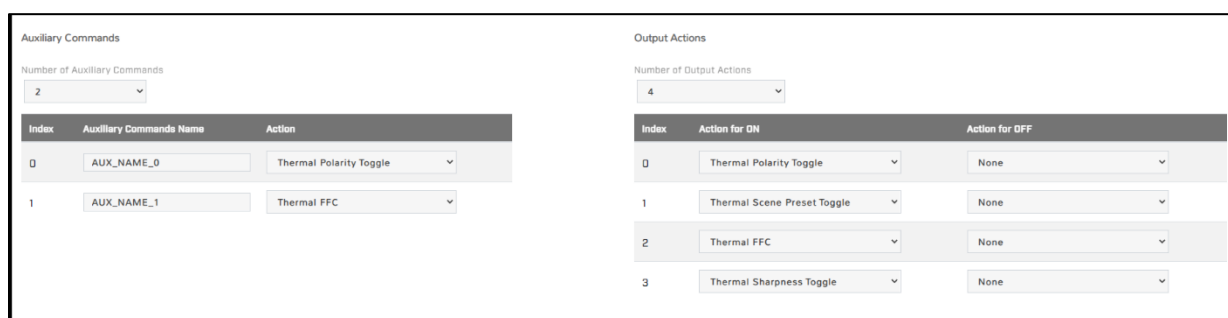
For example, SOE1-V1_VIDEO001_V1_1700982489_1700982789_3_22502.mp4.

11.11 ONVIF

ONVIF settings include options for **auxiliary commands** and **output actions**.

To configure the ONVIF interface:

1. Select the **number of auxiliary commands** (up to seven) and the **number of output actions** (also up to seven).
2. For each auxiliary command action, **specify the ONVIF command name**.
3. For each auxiliary command action, and separately for each ON and OFF output action, **select one of the following**:
 - **None**.
 - **Thermal Polarity Toggle**: Toggles the thermal video polarity (see [Thermal Settings](#)). For example, toggles the colorization from WhiteHot to BlackHot or vice versa; RedHot to RedHotInverse or vice versa; etc.
 - **Thermal FFC**: Initiates flat-field correction on the thermal sensor.
 - **Thermal Palette Toggle**: Toggles through the thermal video colorization options.



The screenshot displays two configuration panels. The 'Auxiliary Commands' panel on the left has a dropdown for 'Number of Auxiliary Commands' set to 2. Below it is a table with two rows. The first row has index 0, 'AUX_NAME_0', and 'Thermal Polarity Toggle'. The second row has index 1, 'AUX_NAME_1', and 'Thermal FFC'. The 'Output Actions' panel on the right has a dropdown for 'Number of Output Actions' set to 4. Below it is a table with four rows. The first row has index 0, 'Thermal Polarity Toggle' for ON, and 'None' for OFF. The second row has index 1, 'Thermal Scene Preset Toggle' for ON, and 'None' for OFF. The third row has index 2, 'Thermal FFC' for ON, and 'None' for OFF. The fourth row has index 3, 'Thermal Sharpness Toggle' for ON, and 'None' for OFF.

Auxiliary Commands		
Index	Auxiliary Commands Name	Action
0	AUX_NAME_0	Thermal Polarity Toggle
1	AUX_NAME_1	Thermal FFC

Output Actions		
Index	Action for ON	Action for OFF
0	Thermal Polarity Toggle	None
1	Thermal Scene Preset Toggle	None
2	Thermal FFC	None
3	Thermal Sharpness Toggle	None



TIP

Index numbering starts with 0 (zero). In the ONVIF Device Manager, index numbering starts with 1 (one).

11.12 Map

In order for the Geotracking functionality to work, users need to upload and calibrate a map of the area covered by the camera. This can be done in the Map tab using different methods:

- Users can upload their own map or blueprint and calibration coordinates.
- Users can log in to the Flir Raven site planning tool and download the map and calibration info for each of the installed cameras.

Manually Uploading a Reference Map Image and Calibrating It

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

For example, if using Google Maps or another online map, you can take a screenshot of a satellite view of the camera's detection range. In Windows 11, 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.

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.



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** set to its native resolution without zoom. For best results, take the screenshot in **full-screen mode** (press F11 in Google Chrome). If you're using Google Maps, consider turning off labels to improve clarity.
- **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 navigate the map, **click and drag** with your mouse. To zoom in or out, use the **scroll wheel**.
- **It might take a few attempts** at different settings to achieve the best result.

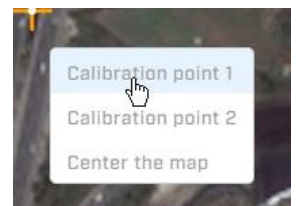
3. Under Map Display, click **Find file**, and then click **Upload**.

If the map successfully uploads, a confirmation message is displayed.

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.

5. **Right-click on the first calibration point**, and then select Calibration point 1.



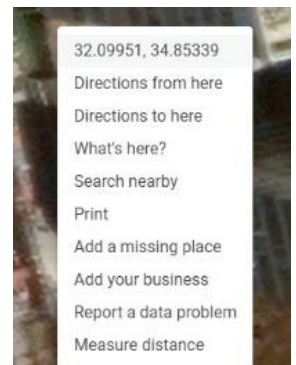
6. **Enter the latitude (Lat) and longitude (Lon) coordinates** for the first calibration point (P1). You can obtain the coordinates from the online map or from a GPS service.

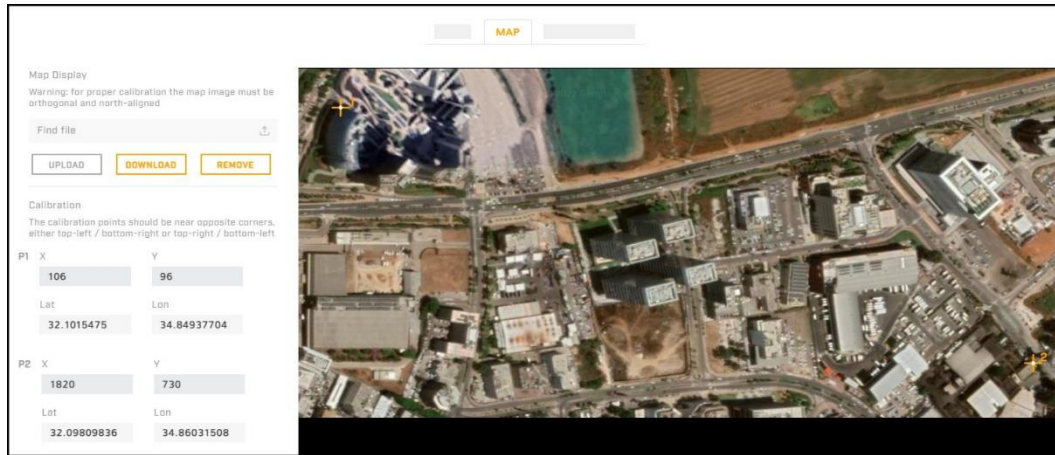
For example, when using Google Maps, right-click on a point and select the coordinates. The point's latitude and longitude coordinates are copied to the clipboard. Paste the coordinates into the **P1 Lat and Lon fields**.

The calibration point appears on the map as a crosshair 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 on the screen.





Uploaded and calibrated map.

If users have not yet set up the camera's georeference calibration, they need to do so on the [Georeference settings](#) page. **The web interface will continue to display a black map until the correct latitude and longitude for the camera are entered**, since the default coordinates do not match those of the actual map, resulting in an area without available map data.

Using Flir Raven Site Planning Tool to Download the Map and Calibration Data

The [FLIR Raven site planning tool](#) is designed to assist users in the **layout and optimization of thermal and visible camera deployments** for enhanced security across perimeters and designated areas. Through the use of detailed product information and simulation capabilities, the tool enables users to **visualize coverage and field of view**, ensuring effective placement of cameras and related devices.

Operators can input a specific address into the FLIR Raven site planning tool, which **automatically generates a map** of the selected area. Within this map interface, users have the option to **add a variety of FLIR Edge devices**, such as cameras and radars, tailoring the deployment to their security requirements.

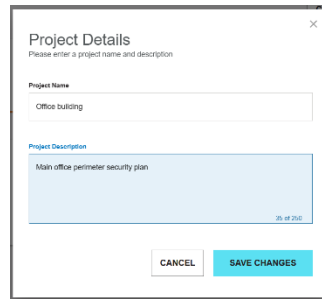
The tool allows precise **configuration of each device's position, height, and rotation**, supporting the design of a security system that meets all operational needs. This step-by-step simulation helps operators maximize coverage and optimize device placement for effective surveillance. Once a camera has been correctly positioned and configured on the map, **users can export the specific camera map, including calibration data, and the Digital Elevation Model, and import these files into the camera to streamline the set up process.**

Please note that in order to access and utilize the FLIR Raven site planning tool, users must create a **free Teledyne FLIR account**. Registration grants access to the full suite of planning features, enabling comprehensive site design and device management.

Follow these steps to create the map and calibration data for a camera using Raven:

1. Visit <https://flirraven.com/>.
2. Log in or create a new account.
3. Create a new project.

4. Enter a **project name** (required) and a **project description** (optional) and **save changes**.

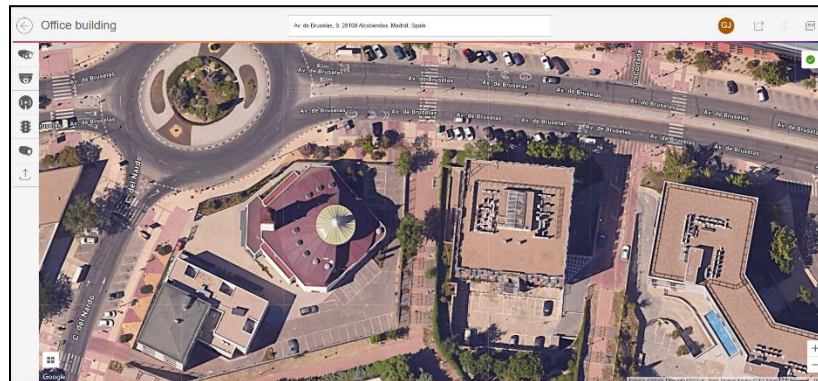


A dialog box titled "Project Details" with a close button (X) in the top right corner. Below the title is a prompt: "Please enter a project name and description". There are two input fields: "Project Name" with the text "Office building" and "Project Description" with the text "Main office perimeter security plan". At the bottom right of the description field, it says "36 of 200". At the bottom of the dialog are two buttons: "CANCEL" and "SAVE CHANGES".

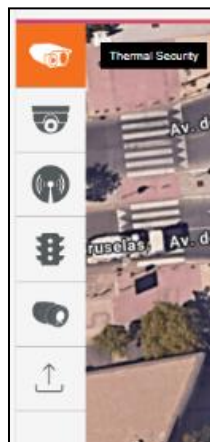
5. A new project is created, and the world map is displayed.
6. **Enter the site's address** in the address box at the top-center of the screen.



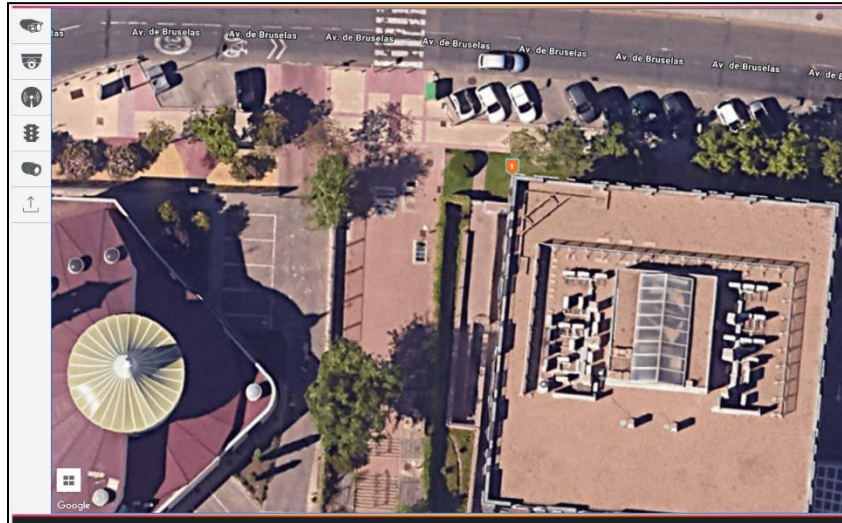
7. The map is updated to display the selected address.
8. Using the mouse, **pan and zoom the map** to maximize the area the cameras and devices are meant to cover.



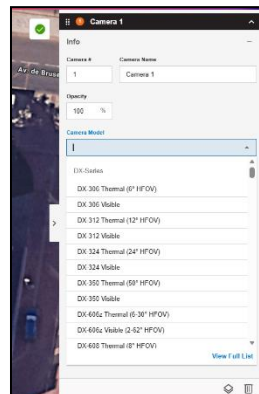
9. Using the toolbar on the left, **select the type of camera** to be added to the map.



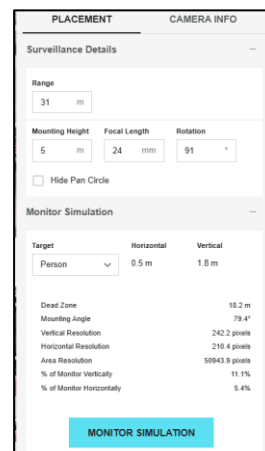
10. **Click on the map** to place the camera. Remember that you can use the mouse to pan and zoom the map as needed in order to place the camera with maximum precision.



11. A device panel is displayed on the right side of the screen where users need to **enter the camera's name** and **select the camera model**.



12. Using the **Placement tab** details and dragging the **person icon of the Field of View preview** on the map, configure the camera to cover the desired area.



13. Once the camera set up is complete, scroll down the device panel. Select **Download map** and choose the destination folder. If the camera supports Digital Elevation Maps, select **Download DEM file** and the destination folder. Leave this panel open to later copy the latitude and longitude of the camera.

Coordinates

Latitude 40.53139547362367
Longitude -3.6351783705369733

FLIR Nexus Tracking

DOWNLOAD MAP

DOWNLOAD DEM

14. Access the camera's web interface and **navigate to the Map tab in the System settings.**

Map Display

Warning: for proper calibration the map image must be orthogonal and north-aligned

Find file

UPLOAD

DOWNLOAD

REMOVE

15. On the **Map Display** pane, click on the **Find File** box and select the downloaded map file, then click **Upload**.

16. The map will be displayed on the main window, and the calibration data will be populated automatically.

17. To upload the Digital Elevation Model, click on the **Find File** box on the Digital Elevation Model pane, select the downloaded DEM file, and click **Upload**.

Digital Elevation Model

Find file

UPLOAD

DOWNLOAD

18. **Save the changes and exit** the System Settings and **open the Georeference panel.**

19. **Copy the latitude in Raven and paste it** into the corresponding field. **Do the same for Longitude.** You can fill out the rest of the fields and save the changes.

Latitude

40.53139547
N

Longitude

-3.63517837
W

Ground Altitude (meters)

45.12

Installation Height (meters)

45.12

Installation Tilt (degrees)

30.123

Installation Roll (degrees)

30.123

Orientation (degrees)

45.12

19. If you added several devices to the Raven project, once all the devices have been calibrated, **close the Raven project** by clicking on the arrow icon on the top-left corner of the screen. **Changes are automatically saved.**

11.13 Scheduler

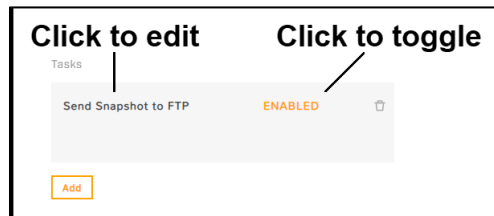
It is possible to define **one-time or recurring tasks**, including their start and stop times. For example, users can:

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



NOTE

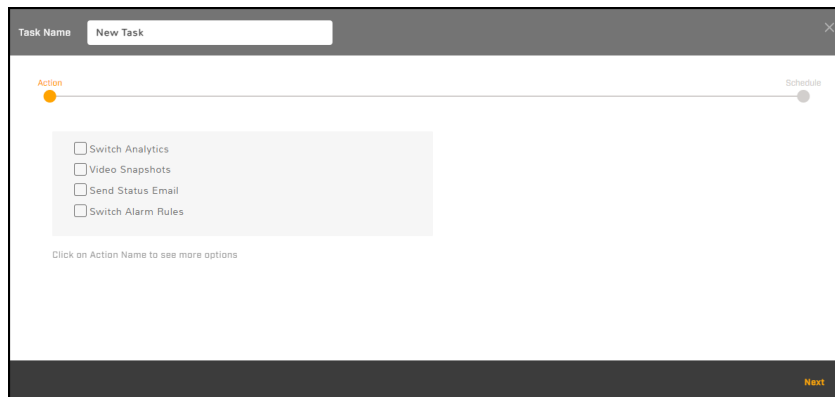
You cannot use the scheduler to define a task that records live video.



By default, no tasks are defined.

To Define a Task:

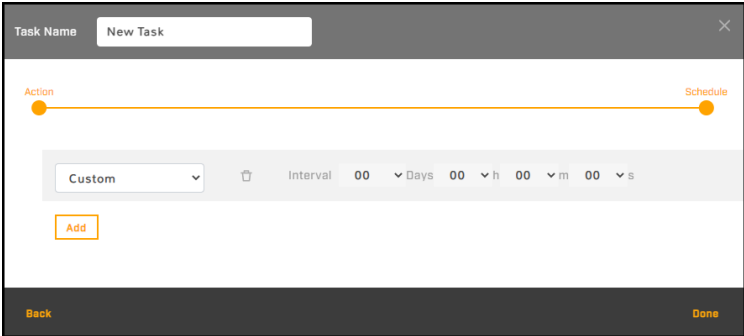
1. Select **Add**. A new task appears. By default, it is enabled.
2. Select **New Task**. The task action settings are displayed.



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 is shown in **bold**, and the relevant settings are displayed.

Predefined Actions	
Switch Analytics	Select whether the task disables the camera's onboard VA (off) or enables it (on). 
Video Snapshots	Records live video snapshots according to settings configured in the Recording settings, 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 settings.
Switch Alarm Rules	Select whether the task disables (off) or enables (on) alarm rules.  Select the rules affected by the task, according to rule ID number. To determine the rule ID, check the Alarm settings.

6. Click **Next**. The task schedule settings are displayed.



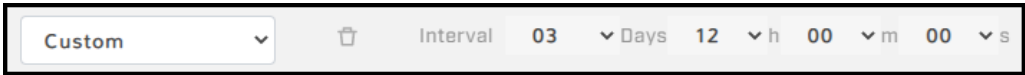
7. From the drop-down list, **select the first schedule** for the task.



TIPS

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:

- **Define the 08:00 Monday's weekly schedule.**
- Click **Add**.
- **Define the first-of-every-month monthly schedule.**

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

8. Click **Done**.

It is possible to enable or disable a task by selecting **Enabled** or **Disabled**. To **delete a task**, click on the corresponding trash icon .

11.14 Recording

On the Recording page, users can configure:

- **Global video clip recording settings.**
- **Recording sources.**

Global Settings

- **Clip Size:** Specify, in MB, the maximum allowed recording file size.
- **File Name Format:** MP4.
- **Retention Policy:** When the specified Maximum Memory Allocation percentage has been reached or exceeded, specify whether the camera stops recording (Stop) or deletes files to make space for new recordings (Overwrite; default).
- **Maximum Memory Allocation:** The percentage of space on the microSD card that triggers the specified retention policy. Range 20-90.

Global Settings

Recording Sources

Clip Size (MB)

200

File Name Format

MP4

Retention Policy

Overwrite

Max. Memory Allocation (20-90%)

80

Recording Sources

The camera **streams two thermal video streams** (T1 and T2) which can be recorded to the microSD card.

For each recording source/video stream enabled on the [Video Page](#), users can specify whether:

- **Recording is enabled** for the stream.
- The camera **continuously records the stream**.
- The camera **prerecords up to 30 seconds** prior to the scheduled start of recording or prior to an event that triggers recording.

Global Settings

Source 1Source 2

Recording Sources

T1

Enable

YesNo

Continuous Recording

YesNo

Prerecording Enabled

YesNo

Prerecording Time (0-30 sec.)

5

Manual Recording

StartStop

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

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

Name	Associated Video	Associated Video Settings	Status
Source 1	Thermal 1	H.264 640 x 512	Recording
Source 2	Thermal 2	H.264 640 x 512	---

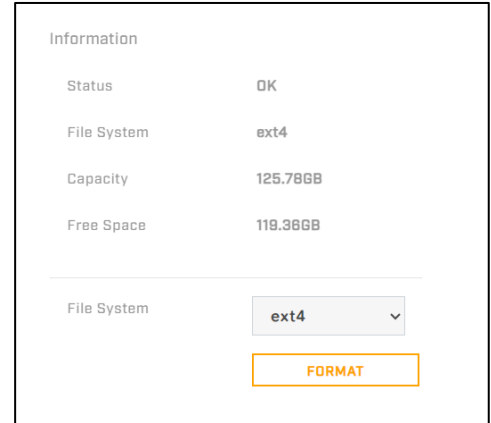
Example: Source 1 - Thermal 1 is Currently Recording

11.15 SD Card

It is possible to **locally record up to 512 GB on a microSD card**. For information on accessing the camera's microSD slot and inserting a card, see [Accessing the Bottom Panel](#).

The following information is displayed on the SD Card tab:

- **Status:**
 - **OK:** a microSD card has been properly installed and formatted.
 - **Error.**
 - **Formatting.**
 - **Done.**
 - **No SD Card.**
- **File System:** ext4.
- **Capacity:** The card's overall capacity, in GB.
- **Free Space:** How much free space is available, in GB.



Information	
Status	OK
File System	ext4
Capacity	125.78GB
Free Space	119.36GB

File System	ext4 ▼ FORMAT
-------------	-------------------------------------

To format a microSD card before using it, **select the file system**, and then click **Format**.



CAUTION

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



NOTES

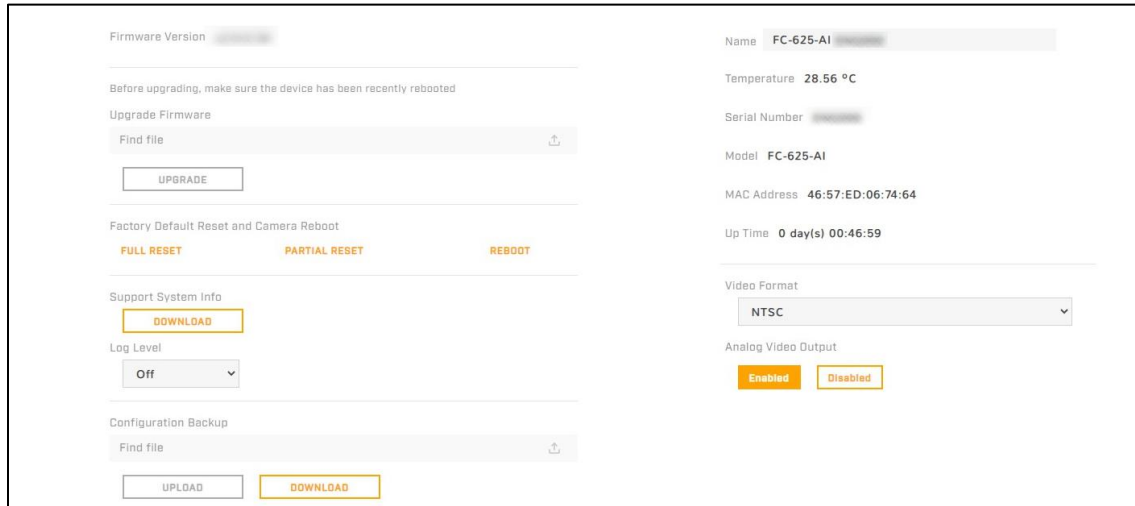
- **Format the microSD card when using it for the first time** or when **the card has been used with another camera** or other device and transferred to this camera.
- The card must be **formatted as a single partition**.
- Please note that the **ext4 format is not natively supported by Windows**, so third-party software (Ext2Fsd, Explore2fs, etc.) is needed to access the files in the card.

11.16 Firmware & Info

On the Firmware & Info tab, users 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.**

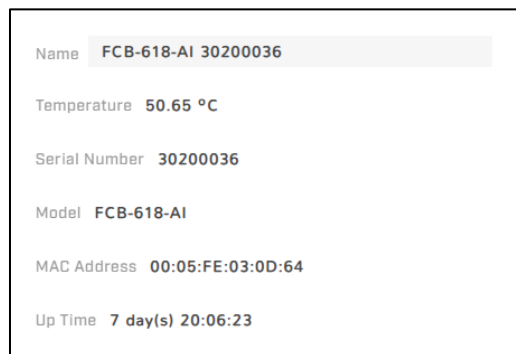
- Download or upload a configuration backup file.



The screenshot shows a web interface for configuring a FLIR camera. On the left, there are sections for 'Upgrade Firmware' (with a 'Find file' button and an 'UPGRADE' button), 'Factory Default Reset and Camera Reboot' (with 'FULL RESET', 'PARTIAL RESET', and 'REBOOT' buttons), 'Support System Info' (with a 'DOWNLOAD' button), 'Log Level' (set to 'Off'), and 'Configuration Backup' (with a 'Find file' button and 'UPLOAD'/'DOWNLOAD' buttons). On the right, there is a summary of camera information: Name (FC-625-AI), Temperature (28.56 °C), Serial Number, Model (FC-625-AI), MAC Address (46:57:ED:06:74:64), Up Time (0 day(s) 00:46:59), Video Format (NTSC), and Analog Video Output (Enabled/Disabled).

Name

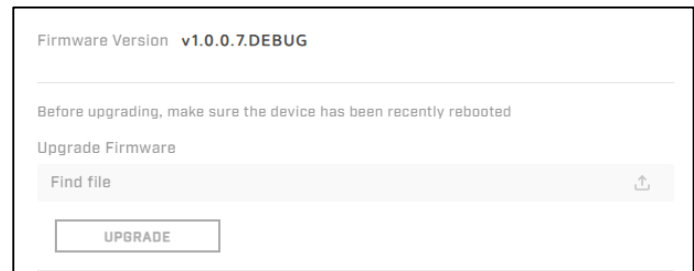
In the Name field, users can specify a **unique, friendly name** for the camera using **only alphanumeric characters**. The default name for the camera is the camera model followed by the camera's serial number.



This screenshot shows the 'Name' field in the configuration interface, which contains the text 'FCB-618-AI 30200036'. Below it, other camera details are listed: Temperature (50.65 °C), Serial Number (30200036), Model (FCB-618-AI), MAC Address (00:05:FE:03:0D:64), and Up Time (7 day(s) 20:06:23).

Upgrading 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**.
4. Click **Upgrade**.



This screenshot shows the 'Upgrade Firmware' section of the configuration interface. It includes the 'Firmware Version' (v1.0.0.7.DEBUG), a warning to 'Before upgrading, make sure the device has been recently rebooted', and the 'Upgrade Firmware' section with a 'Find file' button and an 'UPGRADE' button.



CAUTION

Please ensure that **only firmware specifically developed for FCB-Series AI cameras** is used for upgrades.

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.



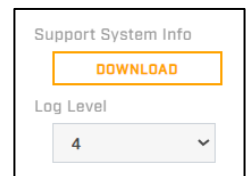
CAUTION

After confirming a reset, **do not click on the camera's web interface until the camera reboots** and the login screen appears. Then, according to the instructions in [Accessing the Camera](#), log back in to the camera's web interface 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.

Support System Info

1. To retrieve the camera's log files, click **Download**.
2. **Set Logging Detail** up to four levels; higher log levels increase the size of the log file.



Configuration Backup

Users can back up the camera's saved settings or upload a configuration backup file; for example, when a camera is replaced.



Uploading 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 FC-Series AI camera** 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**.

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

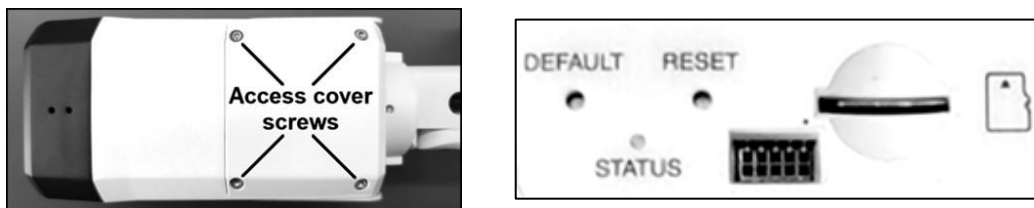
12. Maintenance & Troubleshooting

If help is needed during installation, operation, or configuration, **contact the local Teledyne FLIR representative, or visit the Teledyne FLIR Support Center** at: <https://support.flir.com/>. Teledyne FLIR LLC offers a comprehensive selection of training courses to help get the best performance and value from the thermal imaging camera.

Find out more at the Teledyne FLIR training web page: <https://www.teledyneflir.com/support-center/training/>.

12.1 Removing the Access Cover

To access the camera's **Default button**, **Reset button**, and **microSD card slot**, remove the access cover by loosening the four screws at the bottom of the camera.



- **DEFAULT:** Press this button for at least 10 seconds to restore the camera to its factory settings.
- **RESET:** Press this button for at least 10 seconds to restart the camera.
- **STATUS LED:**
 - **Green:** it turns off three minutes after a successful boot.
 - **Amber:** Flashes while a Firmware upgrade is in progress.
 - **Red:** Solid for the first 2-3 seconds at start up. If LED remains red, an error occurred. **Reset** or **Default** the camera to try again.
- **Console multipin connector:** To be used by maintenance personnel to diagnose and repair the camera.
- **MicroSD card slot:** Insert a microSDXC card in the card slot (maximum 2 TB SD Bus Mode UHS I) to store files, video recordings and snapshots. Do not remove the microSD card while the camera is ON.

If further assistance is needed, please visit: <https://support.flir.com/>.

12.2 Cleaning

It is essential to **exercise great caution when handling your camera's optical components**. These elements are sensitive and may be compromised by improper cleaning methods. The FCB-Series AI thermal camera lenses and windows are engineered for challenging outdoor conditions and feature coatings that enhance durability and minimize reflection. Nonetheless, **periodic cleaning may be necessary**. If there is a noticeable decline in image quality or visible accumulation of contaminants on the lens, Teledyne FLIR advises performing a lens cleaning.



TIP

While cleaning the camera, **do not disturb or move it**. The FCB-Series AI cameras are set and calibrated according to the exact position and camera angle. Inadvertent realignment can require relocation and recalibration of detection regions.

Rinse the camera housing and optics with low pressure fresh water to remove any salt deposits and to keep it clean. If water spots form on the front window of the camera, **wipe them off with a clean, soft cotton cloth dampened with fresh water.**

If further cleaning is needed, please use the following procedure and solvents, as required:

- **Acetone:** removes grease.
- **Ethanol:** removes fingerprints and other contaminants.
- **Alcohol:** final cleaning (before use).

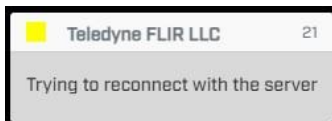
To clean the lens using the aforementioned products:

1. **Immerse lens tissue** (optical grade) in alcohol, acetone, or ethanol (reagent grade).
2. With a new tissue each time, **wipe the lens in an "S" motion** (so that each area of the lens will not be wiped more than once).
3. **Repeat** until the lens is clean. Use a new tissue each time.

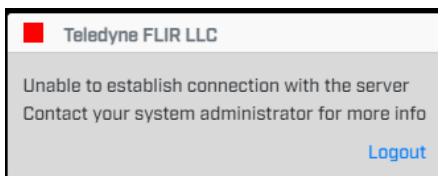
12.3 Troubleshooting Tips

Unable to Access the Camera

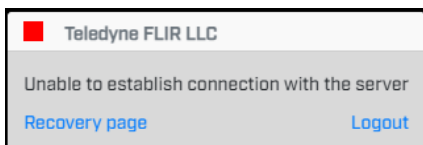
Under certain circumstances, after logging in to the camera's web interface, the following messages might be displayed.



The camera's **Nexus server might not be available**, and the web page is attempting to re-establish the connection. The Nexus server provides 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.

Firmware Version **v1.0.0.7.DEBUG**

Before upgrading, make sure the device has been recently rebooted

Upgrade Firmware

Find file 

UPGRADE

Factory Default Reset and Camera Reboot

FULL RESET PARTIAL RESET REBOOT

Support System Info

DOWNLOAD

Log Level

4

Name **FCB-618-AI 30200036**

Temperature **50.65 °C**

Serial Number **30200036**

Model **FCB-618-AI**

MAC Address **00:05:FE:03:0D:64**

Up Time **7 day(s) 20:06:23**

Unable to Communicate over Ethernet

First check to ensure the **physical connections are intact** and that the **camera is powered on**.

By default, the camera broadcasts a discovery packet twice per second. Use the [FLIR Discovery Network Assistant](#) (DNA) tool or a packet sniffer utility such as Wireshark and confirm the packets are being received by the PC from the camera.

Unable to View IP Video Stream

If the IP video stream from the camera is not displayed, the firewall might be blocking packets, or there could be a conflict with video codecs installed for other video programs.

When displaying video on a VMS for the first time, the Windows Personal Firewall might ask for permission to allow the video player to communicate on the network. Select the appropriate type of network(s) (domain, private, or public).

If necessary, **make sure the video from the camera can be viewed by a generic video player** such as VLC media player (<http://www.videolan.org/vlc/>). To view the video stream, specify RTSP port 554 and the appropriate stream name. For example, using the camera's default IP address when there is no DHCP server on the network (192.168.0.250):

- rtsp://192.168.0.250:554/stream1 for T1
- rtsp://192.168.0.250:554/stream2 for T2

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. See [Users settings](#). Users assigned the role of admin or expert can disable RTSP authentication in the [Services](#) section of the [Cyber settings](#).

For more information on RTSP settings and stream names, see [Video settings](#).

No IP Video

If the camera is not producing an image, **check the connections at the camera and at the display**. If all connections are confirmed to be correct and the camera continues to fail to produce an image, verify that **power is correctly supplied** to the camera and that the circuit breaker is appropriately set. If a fuse was used, be sure the fuse is not blown.

If the camera still does not produce an image, contact the Teledyne FLIR dealer or reseller who provided the camera, or contact Teledyne FLIR directly.

Image Freezes Momentarily

By design, the camera **image momentarily freezes during Flat-Field Correction** (FFC, and also known as Non-Uniformity Correction or NUC). At regular intervals or when the ambient temperature changes, the camera automatically performs FFC. You can also manually trigger FFC on the Thermal Page. The shutter for the thermal imager closes and provides a target of uniform temperature, allowing the thermal imager to correct for ambient temperature changes and provide the best possible image.

Performance Varies with Time of Day

The diurnal **cycle of the sun can cause difference thermal imager performance** at different times of the day. The thermal imager produces an image based on temperature differences. At certain times of the day, such as just before dawn, all of the objects in the scene could be the same temperature. Compare that type of scene to right after sunset, when objects in the scene might be radiating heat energy absorbed during the day. As temperature differences in the scene increase, the thermal imager can produce higher-contrast images.

When **objects in the scene are wet** rather than dry, performance also can be affected. For example, on a foggy day or early in the morning, when surfaces might be coated with dew. Under such conditions, the thermal imager might not be able to accurately detect the temperature of the object itself; instead, it detects the temperature of the surface water.

See also [Thermal Imaging Overview](#).

Image Too Dark or Too Light

By default, the camera's thermal imager uses an Automatic Gain Control (AGC) setting that has proven to be superior for most applications, and the camera automatically responds to varying conditions. Keep in mind that the sky is quite cold and can strongly affect the overall image. To avoid issues, it might be possible to slightly **move the camera up or down to include (or exclude) hot or cold areas** that influence the overall image. For example, a very cold background (such as the sky) can cause the camera to detect and display a wider temperature range than appropriate.

Eastern or Western Exposure

Once installed, the camera might point directly east or west, which can cause the sun to be in the field of view during certain portions of the day. Teledyne FLIR does **not recommend intentionally pointing the camera at the sun**. The sun can introduce image artifacts that the imager eventually corrects. However, recovery can take some time. The amount of time depends on how long the thermal imager was exposed to the sun. The longer the exposure, the longer the recovery time needed. Nonetheless, it does not permanently damage the imager. At the same time, in back-lit scenes, the thermal imager often provides a considerable advantage over a visible imager.



Images facing sun from visible light camera (left) and from thermal camera (right)