Teledyne FLIR
Security Solutions

Installation and User Guide

FH-Series Cameras

427-0102-00-10 - Revision 130 - November 2023

This document does not contain any export-controlled information.

© 2023 Teledyne FLIR LLC All rights reserved worldwide. No parts of this manual, in whole or in part, may be copied, photocopied, translated, or transmitted to any electronic medium or machine readable form 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.

This product is protected by patents, design patents, patents pending, or design patents pending.

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.teledyneflir.com or write to Teledyne FLIR LLC

Teledyne FLIR LLC
6769 Hollister Avenue
Goleta, CA 93117

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.

Note 1: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the user's own expense.

Note 2: If this equipment came with shielded cables, it was tested for compliance with the FCC limits for a Class A digital device using shielded cables and therefore shielded cables must be used with the device.

Industry Canada Notice:
This Class A digital apparatus complies with Canadian ICES-003.

Avis d'Industrie Canada:
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

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	September 2021	Initial Teledyne FLIR release
110	November 2021	Thermal video analytics color palette; Vehicle Detection Filter; Differential analytics item; external illumination support; camera web page improvements; installation and cleaning instructions improvements;

Product Registration and Warranty Information

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

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

This document does not contain any export-controlled information.

Table of Contents

1. Camera Overview 1

1.1 Accessing Product Information from the Teledyne FLIR Website 2

1.2 Camera Dimensions 3

1.3 Camera Specifications 4

2. Installation 7

2.1 Supplied Components 8

2.2 Site Preparation 8

2.3 Supplying Power to the Camera 9

2.4 Additional Connections 10

2.5 Connect the Camera 11

2.6 Configure for Networking 14

2.7 Mount the Camera 16

2.8 Connect the Camera 17

2.9 Aim the Camera 18

2.10 Check the Boresight 18

2.11 Configure the Analytics 18

2.12 Additional Configuration 18

2.13 Attach the Camera to a Supported VMS 19

2.14 Pairing an FH-Series Camera with a FLIR Security PTZ Camera (Optional) 19

2.14.1 Pairing with a Quasar 4K IR-PTZ, DX-Series, or DM-Series Camera 20

2.14.2 Pairing with a PT-Series HD Camera 22

2.14.3 Confirming PTZ Camera Pairing Configuration 25

3. Operation 26

3.1 Accessing the Camera 26

3.2 View Settings Home Page 26

3.3 Making Changes to Settings 27

3.4 Video Page 29

3.5 Visible Page 31

3.6 Thermal Page 35

3.7 Illumination Page 38

3.8 I/O Page 38

3.9 Radiometry Page (R models) 39

3.10 Video Analytics Page 42

3.10.1 Check the Analytics Calibration 44

3.10.2 Create Analytics Regions 45

3.11 OSD Page 48

This document does not contain any export-controlled information.

Table of Contents

3.12 Geotracking Page 48
3.13 Georeference Page 51
4. Configuration 53
4.1 Network Page 53
4.1.1 Settings 54
4.1.2 SNMP 54
4.2 Date & Time Page 56
4.3 Users Page 56
4.4 Alarm Page 57
4.4.1 Modifying or Defining Rule Triggers 59
4.4.2 Modifying or Defining Rule Actions 60
4.5 Audio Page 61
4.6 I/O Devices Page 62
4.7 Messaging Page 63
4.8 Heaters & Fans Page 63
4.9 Cyber Page 64
4.9.1 Certificates 65
4.9.2 802.1X 66
4.9.3 TLS / HTTPS 66
4.9.4 Services 66
4.9.5 IP Filter 67
4.10 Media Browser Page 68
4.11 ONVIF Page 68
4.12 Map Page 69
4.13 Boresight Page 71
4.14 Scheduler Page 74
4.15 Recording Page 77
4.16 SD Card Page 78
4.17 Firmware & Info Page 79
5. Maintenance and Troubleshooting Tips 82
5.1 Cleaning 82
5.2 Troubleshooting 82
6. Appendix 85
6.1 Configuring ioi PTZ Tracker Hand-Off 85

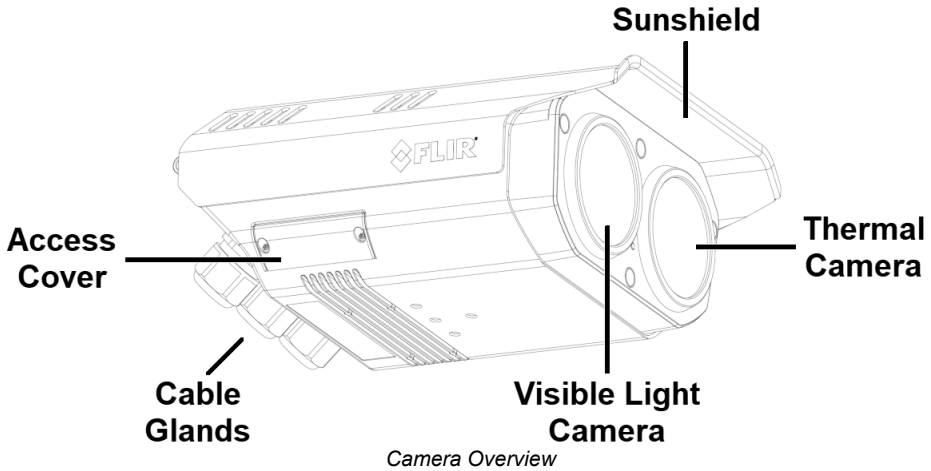
This document does not contain any export-controlled information.

1 Camera Overview

The FH-Series are ruggedized, multispectral fixed cameras that integrate industry-leading thermal imaging with 4K visible imaging to provide reliable intruder-detection capabilities for perimeter security. Built-in convolutional neural network (CNN) analytics accurately detect and classify human and vehicle threats moving at high or low speeds, minimizing false alarms and daily operations costs. Custom scheduling enables security operators to set intrusion analytics to run on visible streams during the day and on thermal streams throughout the night,establishing optimized coverage for any lighting condition.

FH-Series R models provide radiometry and can generate alarms determined by detected surface temperature. During critical alarm events, use the visible imager to immediately assess the alarms and save valuable seconds.

When the camera is connected to an IP network, it functions as a server, providing services such as camera control, video streaming, and network communications. The server uses an open, standards-based communication protocol to communicate with Teledyne FLIR and third-party video management system (VMS) clients, including systems that are compatible with ONVIF®. These clients can be used to control the camera and stream video during day-to-day operations. For a list of supported VMS clients, see the product page on the Teledyne FLIR website. The camera streams digital video from the camera over an IP network using H.265, H.264, and MJPEG encoding, and provides analog video output.



Camera Overview

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

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

Related Documentation

- *FH-Series Quick Install Guide*
- *FLIR Security Edge Devices Accessory Guide*
- *FH-Series Mounting Accessories*
- *FLIR CGI Interface Description 2.1*
- *NEXUS® CGI WebSockets Manual*
- *FLIR Sensors SDK Programmer's Guide*

This document does not contain any export-controlled information.

1.1 Accessing Product Information from the Teledyne FLIR Website

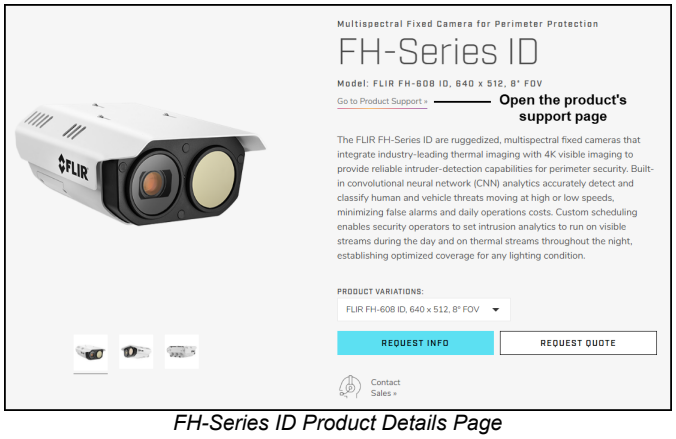
Up-to-date resources for the camera, including the FLIR Discovery Network Assistant (DNA) software tool and this installation and user guide, are available from the camera's pages on the Teledyne FLIR website.

To access product information from the Teledyne FLIR website:

1. Open https://www.teledyneflir.com/browse/security/thermal-security-cameras/.

Thermal Security Cameras Page on the Teledyne FLIR Website

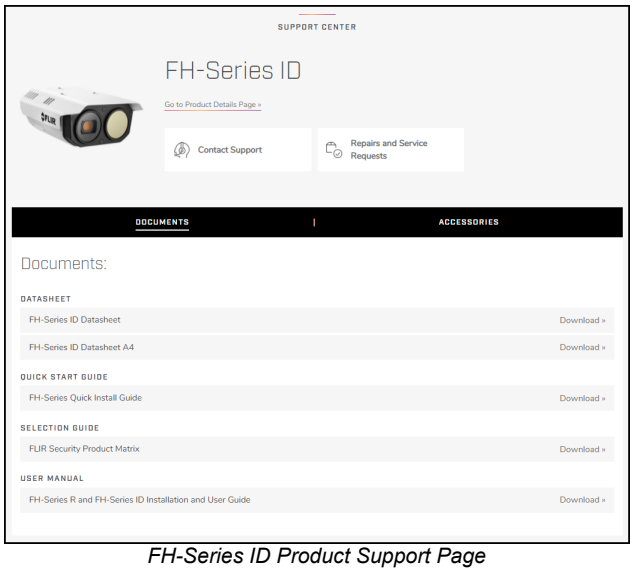
2. Find and click the appropriate model, FH-Series ID or R. The product details page appears.



FH-Series ID Product Details Page

3. To see specifications and other resources, scroll down.
4. Open the camera's support page. Click **Go to Product Support**.

This document does not contain any export-controlled information.

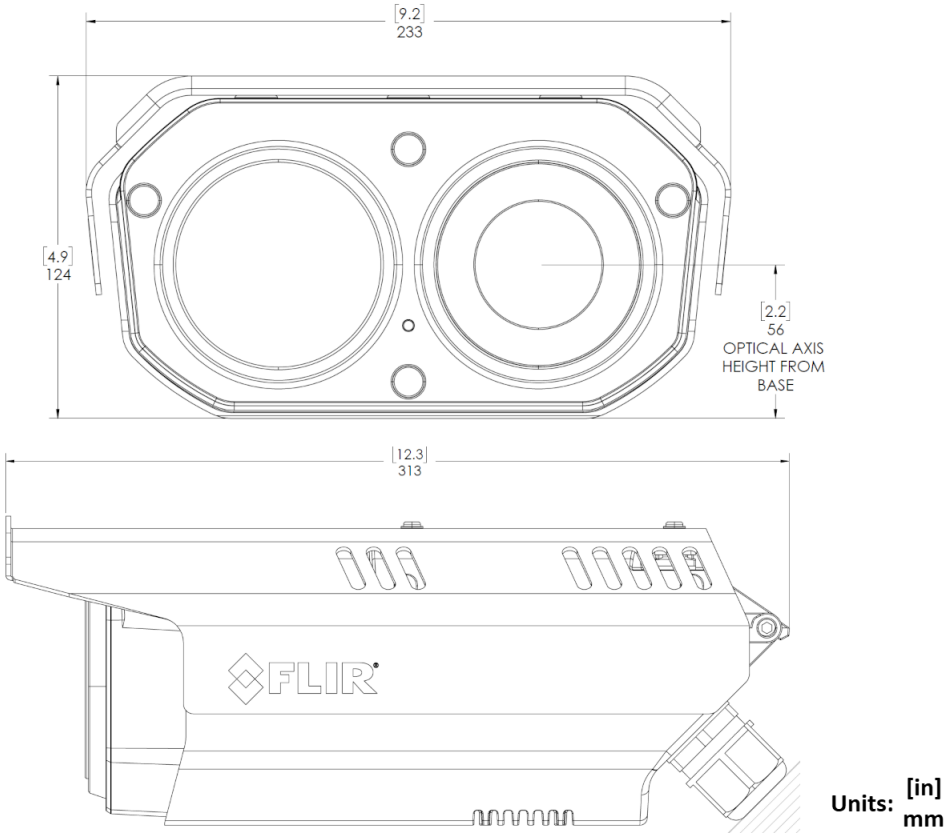


FH-Series ID Product Support Page

5. Select the relevant tab. For example, to download the DNA tool, open the Downloads tab.
6. To download the resource, click the corresponding **Download** link.

1.2 Camera Dimensions

With the sunshield attached, the FH-Series camera dimensions are:



This document does not contain any export-controlled information.

1.3 Camera Specifications

Thermal Sensor & Optics	Array Format (NTSC)	FH-3xx models: 320x256 FH-6xx models: 640x512			
	Detector Type	Long-life, uncooled VOx microbolometer			
	Pixel Pitch	17 µm			
	Thermal Frame Rate	NTSC: 30 Hz or PAL: 25 Hz - user switchable < 9 Hz available			
	Optical Characteristics	**Model**	**FOV**	**Focal Length**	**F/#**
		369 R	69° × 56°	9 mm	F1.4
		324 R	24° × 18°	13 mm	F1.0
		313 R	13° × 10°	25 mm	F1.1
		669 R / ID	69° × 56°	9 mm	F1.4
		644 R / ID	44° × 36°	13 mm	F1.0
		625 R / ID	25° × 18°	25 mm	F1.1
		617 R / ID	17° × 14°	35 mm	F1.1
		612 ID	12° × 10°	50 mm	F1.2
		610 ID	10° × 8.2°	60 mm	F1.2
		608 ID	8.6° × 6.6°	75 mm	F1.1
	Spectral Range	7.5 µm to 13.5 µm			
	Sensitivity (NEdT)	R models: <35mK @ 25°C (77°F) F1.0			
		ID models: <30mK @ 25°C (77°F) F1.0			
Visible Light Camera	Sensor Type	4K 2160p (3820 x 2160)			
	Optical Characteristics	**Model**	**Default FOV**	**Focal Length**	**F/#**
		369	98° × 55°	3.6-10mm	F1.5-2.8
		324	34° × 19°	9-22mm	F1.4-1.7
		313	18° × 10°	13-55 mm	F1.6-2.2
		669	98° × 55°	3.6-10mm	F1.5-2.8
		644	63° × 35°	3.6-10mm	F1.5-2.8
		625	36° × 20°	9-22mm	F1.4-1.7
		617	24° × 14°	13-55 mm	F1.6-2.2
		612	17°×10°	13-55 mm	F1.6-2.2
		610	14° × 8°	13-55 mm	F1.6-2.2
		608	11°× 6°	13-55 mm	F1.6-2.2

This document does not contain any export-controlled information.

Temperature Measurement (R models only)	Measurement Accuracy	Target below 100°C (212°F): ± 5°C (±9°F) accuracy Target below 150°C (302°F): ± 5% accuracy Target above 150°C (302°F): ± 15% accuracy Measured at 25°C ambient temperature. Inaccuracy can be greater at extreme temperatures.
	Object Temperature Range	High Gain Mode: 0°C to +160°C (32°F to 320°F) Low Gain Mode: 0°C to +380°C (32°F to 716°F)
Video	Video Type	IP or analog
	Sensitivity	Color: 0.25 Lux @ (f1.6 AGC On, 30FPS) B/W: 0.10 Lux @ (f1.6 AGC On, 30FPS)
	Visible Frame Rate	30Hz
	IP Video Compression	H.264 / H.265 / MJPEG Four independent streams; two visible and two thermal
	Streaming Resolutions	**Primary Stream**
		Thermal: VGA (640x512)
		Visible: 4K (3840x2160) except MJPEG, 1080p (1920x1080), 720p (1280x720), VGA 640x480
		Secondary Stream
		Thermal: VGA (640x512)
		Visible: 1080p (1920x1080), 720p (1280x720), VGA 640x480
	Thermal Image Settings	Auto AGC, Digital Detail Enhancement (DDE), brightness, contrast
	Thermal AGC Region of Interest (ROI)	Default, presets, and user-definable to ensure optimal image quality on subjects of interest
	Image Uniformity Optimization	Automatic flat-field correction (FFC) - thermal and temporal triggers
System Integration	Ethernet	100/1000 Mbps
	Network APIs	NEXUS SDK; NEXUS CGI; ONVIF Profiles S, G, T
	Digital I/O	Input: two dry alarm contacts Output: two relay contacts 1A max at 24 VAC / 30 VDC Configurable between normally open and normally closed
	Onboard Storage	microSD card slot: up to 512GB on a Class 10 microSD/microSDHC/ microSDXC card (minimum 8GB)
Network	Supported Protocols	IPv4, HTTP, HTTPS, UPnP, DNS, NTP, RTSP, TCP, UDP, ICMP, IGMP, DHCP, ARP, IEEE 802.1X
General	Input Voltage	12 VDC (±10%) 24 VDC (±10%) 24 VAC (±10%) 802.3bt
	Power Consumption	Nominal: 15W 12 VDC with heaters enabled: 48W All other input voltages with heaters enabled: 70W
	Weight	5.1 kg (11.3 lbs)
Environmental	IP Rating (Dust & Water Ingress)	IP66, IP67

This document does not contain any export-controlled information.

	Enclosure	NEMA 4X
	Operating Temperature Range	-40°C to 70°C (PoE 70W class 8 or 24V AC / DC) -20°C to 70°C (PoE 50W class 6 or 12 VDC)
	Storage Temperature Range	-55°C to 85°C
	Corrosion	MIL-STD 810G, 1000hr salt spray
	Humidity	0-95% relative
	Shock	IEC 60068-2-27
	Vibration	IEC 60068-2-64
	Vandalism	IK10 (except windows)
	Surge Immunity on AC Power Lines	EN 50130-4
	Surge Immunity on Signal Lines	EN 50130-4
	Surge / Lightning Protection	TVS 6000V lightning protection, surge protection, voltage transient protection
Compliance & Certifications	FCC Part 15 (Subpart B, class A) CE Marked RoHS WEEE IEC 62368 ONVIF Profile S, G, T	
Video Analytics	Region entrance / intrusion detection Tampering Loitering CNN classifier	
Cybersecurity	IEEE 802.1X TLS / HTTPS User authentication Access control via firewall User credentials with policy enforcement Digest authentication	

Specifications are subject to change without notice. For the most up-to-date specs, see the product's web page on the Teledyne FLIR website.

This document does not contain any export-controlled information.

2 Installation

Caution

A qualified service person should install the camera.
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.
Be careful not to leave fingerprints on the camera's infrared optics.
Operating the camera outside of the specified input voltage range or the specified operating temperature range can cause permanent damage.
At the mounting location, secure the camera before supplying power to it.

This chapter includes information about:

- Supplied Components
- Site Preparation
- Supplying Power to the Camera
- Additional Connections
- Pairing an FH-Series Camera with a FLIR Security PTZ Camera (Optional)

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

1. Connect the Camera
2. Configure for Networking
3. Mount the Camera
4. Connect the Camera
5. Aim the Camera
6. Check the Boresight
7. Configure the Analytics
8. Additional Configuration
9. Attach the Camera to a Supported VMS

However, circumstances can dictate adjusting the sequence of the steps. For example, you can mount the camera before configuring it for networking, or connect the camera before mounting it.

This document does not contain any export-controlled information.

2.1 Supplied Components

The FH-Series camera kit includes these items:

Camera Body with Sun Shield Attached

Teledyne FLIR ships the cameras with watertight cable glands and seal plugs attached to the rear cable ingress holes.

In addition, the camera kit includes a bag with the following parts:

- a T10 Torx wrench
- two 10-pin terminal block, for I/O connectors
- one three-pin terminal block, for 12 VDC input connector
- three two-pin terminal blocks, for 24 VAC output / input connectors

For information about the camera's connectors, see Connect the Camera.

2.2 Site Preparation

Select a suitable location to mount the camera.

FH-Series cameras are intended to be mounted on a medium-duty fixed pedestal mount or wall mount commonly used in the CCTV industry, at an installation height of at least 4 m (13 ft). Cables exit from the back of the camera housing. The mount must support up to 30 lbs (15 kg). For the full list of mounting and other accessories available for the camera from Teledyne FLIR, see the *FLIR Security Cameras - Accessory Guide*.

Mount the camera in a location that allows access for regular periodic cleaning (fresh water rinse), inspection of mounting integrity and mechanical soundness, and preventive maintenance. Ensure the camera and the camera mount are routinely inspected on a periodic basis.

If you are powering the camera with PoE 70W class 8 or 24V AC / DC, verify that the operating temperature is -40°C to 70°C (-40°F to 158°F) with cold start at -40°C (-40°F), 0-95% relative humidity. For other power sources, see Supplying Power to the Camera.

Consider cable lengths and cable routing. Make sure the cables are long enough, given the proposed mounting locations and cable routing requirements; do not exceed their specifications; adhere to all local and industry standards, codes, and best practices; have sufficient dimensions to ensure safety (for power cables); and adequate signal strength (for video and communications). Before you mount the camera and fit the mounting hardware, route the cables.

In addition, prior to installing the unit and for proper installation and operation, the following requirements need to be properly addressed:

This document does not contain any export-controlled information.

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

The physical installation of the unit is one 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. In addition to physical installation, installation also consists of setup and configuration.

2.3 Supplying Power to the Camera

The camera itself does not have an on/off switch. Generally, the FH-Series camera will be connected to a circuit breaker and the circuit breaker will be used to apply or remove power to the camera. If power is supplied to it, the camera will be in one of two modes: Booting Up or Powered On.

The power cable supplied by the installer must use wires that are sufficient size gauge (16 AWG recommended) for the supply voltage and length of the cable run, to ensure adequate current carrying capacity. Always follow local building codes.

Ensure the camera is properly grounded. Typical to good grounding practices, the camera chassis ground should be connected to the lowest resistance path possible. Anchor a grounding strap to the grounding lug inside the camera housing (see Connect the Camera) and connect it to the nearest earth-grounding point.

The camera can be powered by:

- 12 VDC (±10%)
- 24 VDC (±10%)
- 24 VAC (±10%)—for example, Teledyne FLIR part number 4124857
- PoE IEEE 802.3bt 50W class 6 or 70W class 8

This document does not contain any export-controlled information.

Teledyne FLIR recommends using PoE 70W class 8 or 24V AC / DC. Other power sources limit low-temperature operation:

	12V	24V	PoE 50W class 6	PoE 70W class 8
Lowest operating temperature	-20°C	-40°C	-20°C	-40°C
Cold start	•	•	•	•
De-icing		•		•
De-fogging		•	•	•
Fog prevention	•	•	•	•

If using PoE, make sure the PoE switch or injector is a Power Sourcing Equipment (PSE) device. If using an external AC or DC power supply, make sure to connect the power supply to the appropriate connector and connection. The AC / DC power connectors included in the camera kit accept 16 AWG maximum wire size.

Nominal power consumption is 15W; 48W on 12 VDC with heaters enabled; and 70W on all other input voltages with heaters enabled.

Warnings

- Make sure the camera's power cable is properly connected. All electrical work must be performed in accordance with local regulatory requirements.
- Use a UL Listed Power Adapter that meets LPS (Limited Power Source) requirements.

Heaters

Onboard heaters de-fog and de-ice the camera's lenses and other components in the event of, for example:

- A power interruption that disables the camera for an extended period
- Freezing rain that covers the lenses and obstructs the images

By default, the heaters automatically turn on and off at certain temperatures. Camera web page users assigned the role of admin or expert can change the temperature mode for these components, manually turn the heaters on and off, and monitor the temperature of the components on the Heaters & Fans Page.

2.4 Additional Connections

Ethernet Connection

The FH-Series camera produces digital (IP) and analog video output. An Ethernet connection is required for IP video streaming, configuration, and communication.

The camera's cable gland seals are designed for shielded Category 6 Ethernet cable.

FLIR IP cameras support FLIR UVMS video management systems, along with third-party VMSs. These systems tend to evolve and change over time. Therefore, for up-to-date information, contact the local Teledyne FLIR representative or Teledyne FLIR Support.

Analog Video Connections

There are two BNC connectors for analog video connections: one for thermal camera video and the other provides user-configurable analog visible or thermal video output. Analog video requires a connection to a video monitor or to an analog video matrix switch. To ensure a quality video signal, use cable rated RG59U or better.

The camera can output analog video in either NTSC or PAL.

This document does not contain any export-controlled information.

Alarm I/O Connections

The camera provides two alarm input connections and two sets of output connections. The output pins support a normally open or normally closed idle state; that is, when there is no alarm and when power is not being supplied to the camera.

Audio I/O Connections

The camera provides a line-level analog audio input, analog-to-digital encoding, and a digital audio output.

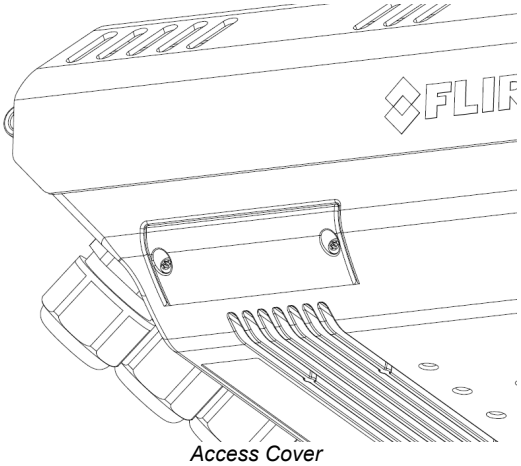
Power to External IR LED Illuminators

The camera provides two 24 VAC output connections for external IR LED illuminators. For information about the Raytec IR LED illuminators FH-Series cameras support, see the *FLIR Security - Accessory Guide*.

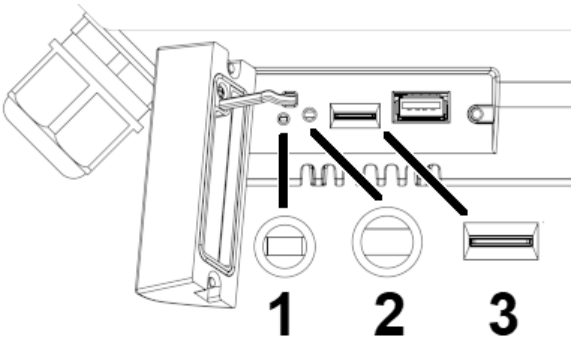
2.5 Connect the Camera

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

The camera's interfaces and connections are inside the camera body. A microSD card slot and reset / default button are located on a panel on the side of the camera. To access the side panel, loosen and remove the screws that attach the access cover to the camera. An anti-drop strap prevents the access cover from falling. Before closing and locking the access cover, make sure to store the anti-drop strap inside the camera to ensure that the camera remains waterproof.



Access Cover



Side Panel Interfaces

Side Panel		
1	**LED status indicator—**Solid green indicates the camera is powered and operating.	• To reboot and reset the camera to its previously saved settings, press the button for between 1-3 seconds. The LED flashes red and green, becomes solid red, and then becomes solid green. To make sure all of the camera's systems properly boot up, wait a couple of minutes before performing any other operation. • To reboot and reset the camera to its factory default settings, press the button for at least 10 seconds. While you are pressing the button, the LED flashes green and red. When the LED flashes only red, release the button and the camera reboots.
2	**Recessed Default / Reset button—**To press the button, Teledyne FLIR recommends using a cell phone SIM or memory card tray eject tool or something similar.	
3	**microSD card slot**	
The USB port is reserved for future use.		

This document does not contain any export-controlled information.

Important

Use a preformatted microSD card, or format it using the camera's web page or a PC; see SD Card Page.

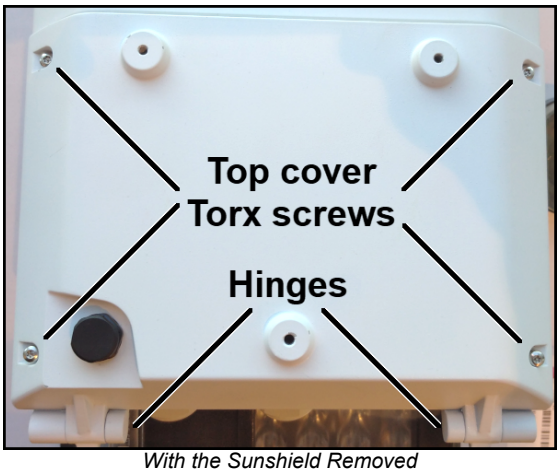
Tips

- Access the camera's web page, open the SD Card Page, and make sure the camera recognizes the microSD card.
- To configure local recording to the microSD card, use the Recording Page.
- You can also configure local recording or other storage on the edge (SoE) using FLIR UVMS, an approved third-party VMS, or another ONVIF-compliant client.

To open the camera's top cover:

1. Through slots in the sunshield, use the Torx wrench supplied with the camera to loosen and remove the two screws that secure the camera's top cover that are closest to the hinges. Then, loosen and remove the other two screws.

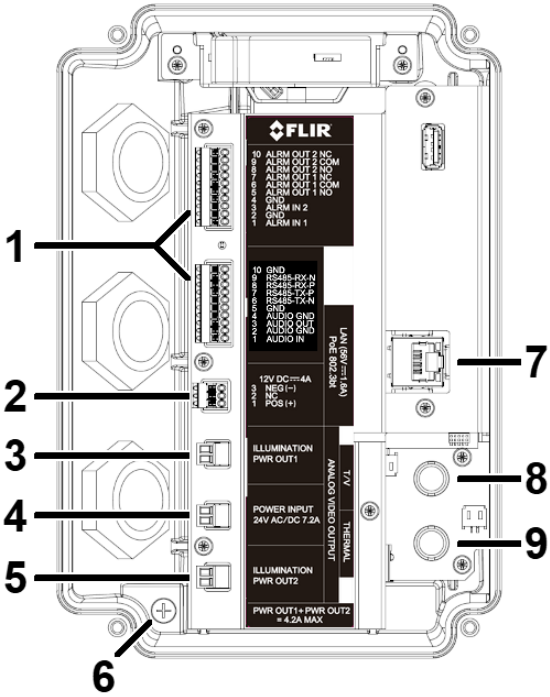
   You do not need to remove the sunshield to open the cover. Nonetheless, if you want to remove the sunshield, loosen and remove the screws that attach it to the camera body. Then, carefully remove the sunshield.



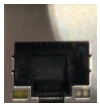
With the Sunshield Removed

This document does not contain any export-controlled information.

2. Open the camera cover to expose the inside of the camera body and the following connections.



Camera Connections

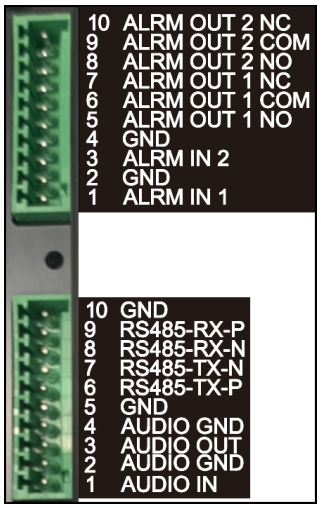
Connection			Description
1	10-pin terminal block x 2		Connect wires from an external power supply; alarm or audio I/O devices; or IR LED illuminators, to the appropriate pins on the appropriate connector. Then, insert the connectors into the terminal blocks. • Do not connect a 12V DC power supply to the 24V AC / DC power input connection. • Do not use the 12V DC and 24V AC / DC power input connections at the same time. • The ILLUMINATION POWER OUT 1 + 2 24V AC connections can supply a maximum 4.2A total to external illuminators. They must be connected to equipment with fireproof enclosures. FH-Series cameras support Raytec Long-Range Infra-Red illuminator models VAR2-i6-1, VAR2-i6-2, VAR2-i8-1, VAR2-i8-2, and VAR2-i16-1. For information about which Raytec illuminator each FH-Series model supports, see the *FLIR Security Edge Devices Accessory Guide*.
2	12V DC⎓4A (IN)		
3	ILLUMINATION POWER OUT 1 24V AC		
4	POWER INPUT 24V AC / DC 7.2A		
5	ILLUMINATION POWER OUT 2 24V AC		
6			Anchor a ground strap to this grounding lug and connect it to the nearest earth-grounding point. Make sure the camera is properly grounded. Failure to properly ground the camera can permanently damage the camera.
7	LAN (56V⎓1.6A) PoE 802.3bt		Attach a Cat 6 cable from the network switch to the RJ45 connection for a 100/1000 Mbps Ethernet and PoE connection. A solid green LED indicates an active connection. A flashing orange LED indicates data traffic between the camera and the network.

This document does not contain any export-controlled information.

Connection		Description	
8	BNC x 2	**T/V—**User-configurable analog visible or thermal video output; supports OSD	Attach analog video cables rated RG59U or higher to these connectors. You can enable on-screen display (OSD) on the OSD Page. Users assigned the role of admin or expert can specify the video format of the T/V connector on the Firmware & Info Page.
9		Analog thermal video output; no OSD	

12V DC Power Input Connector

10-Pin Terminal Blocks



To use the camera's external IR illumination feature to turn illuminators on and off, connect them to ALARM OUT 2.

2.6 Configure for Networking

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

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

Notes

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

This document does not contain any export-controlled information.

Notes (con't)

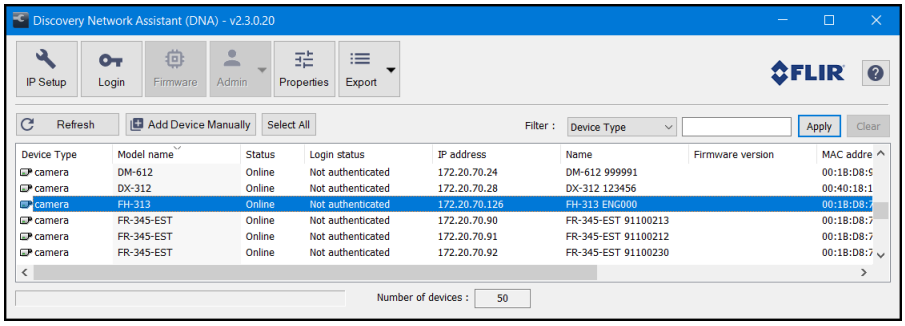
- For more information about using a supported VMS to configure one or more cameras at the same time, see the VMS documentation.

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

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

To configure the camera for networking using the DNA tool:

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

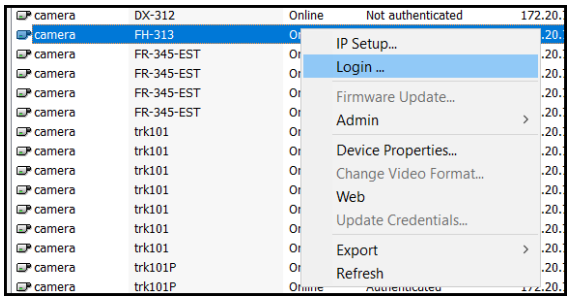


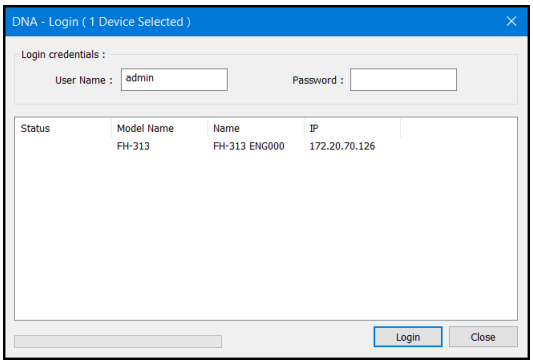
In the DNA Discover List, verify that the camera's status is *Online*.

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

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

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





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

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

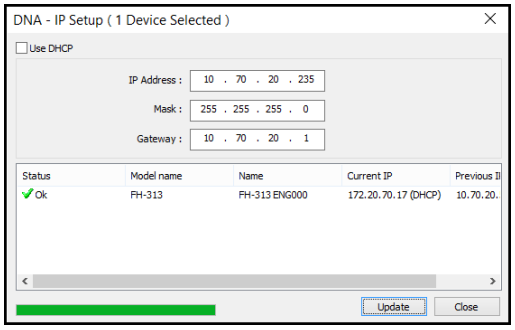
This document does not contain any export-controlled information.

2. Change the camera's IP address.

   Right-click the camera and select **IP Setup**.

   In the **DNA - IP Setup** window, clear *Use DHCP* and specify the camera's *IP address*. You can also specify the *Mask* (default: 255.255.255.0) and *Gateway*.

   Then, click **Update**, wait for ✔ Ok status to appear, and then click **Close**.



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

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

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

Close the Cover

Disconnect the camera.

To prevent damaging the camera's internal components while moving it from the bench or lab to its mounting location, securely close the camera cover. If you removed the sunshield, either re-attach it or bring it to the mounting location.

At the mounting location, to connect the camera, open the cover again. If necessary, remove the sunshield.

2.7 Mount the Camera

Teledyne FLIR offers the following accessories for mounting the camera and an external illuminator:

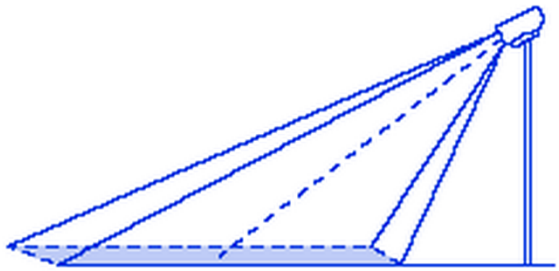
<table>
<tr><th>Mount</th><th>Wall</th><th>Large pole
⌀ 150-230 mm
(6-9")</th><th>Small pole
⌀ 65-110 mm
(2.6-4.3")</th><th>Corner</th><th>Pedestal</th></tr>
<tr><td rowspan="3">Accessories</td><td colspan="4">421-0087-00 Wall Mount Kit</td><td rowspan="2">500-1120-00
Pedestal Mount
Assembly</td></tr>
<tr><td></td><td>500-1116-00
Large Pole
Adapter
Assembly</td><td>500-1121-00
Small Pole
Adapter
Assembly</td><td>500-1119-00
Corner Mount
Assembly</td></tr>
<tr><td colspan="5">421-0086-00 Illuminator Bracket Kit</td></tr>
</table>

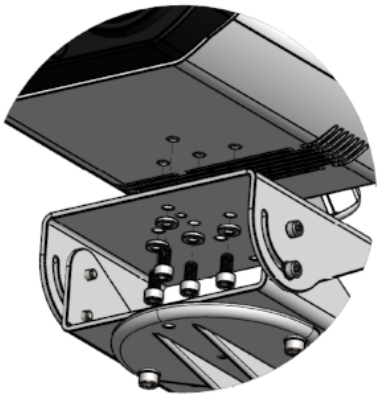
Be sure to have the required accessories and tools available.

Install the mounting hardware for the camera according to the instructions for the hardware. If relevant, route power, network, and other cables into the mounting hardware so that they are accessible when the camera is mounted.

Typically, point the camera towards the ground while ensuring that the field of view includes as little of the skyline as possible. Teledyne FLIR recommends mounting the camera with zero horizontal rotation; that is, a 0º installation roll angle. For accurate video analytics, you can mount the camera with an installation roll angle within ±5º.

This document does not contain any export-controlled information.





Attaching the Camera to the 421-0087-00 Wall Mount Kit

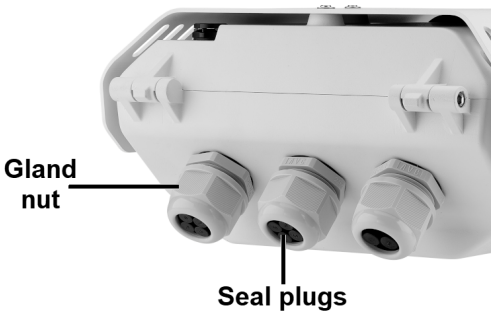
Attach the camera to the mounting surface using four 1/4"-20 UNC SUS 19mm screws, each with a metal flat washer, a spin washer, and a 1/4"-20 UNC nut. If you are mounting the camera using the FH-Series Wall Mount Kit (PN 421-0087-00), these items are supplied with the kit.

2.8 Connect the Camera

Caution

Carefully following these instructions makes sure water does not enter the camera and ensures its long-term reliability. Teledyne FLIR is not responsible for damage to the camera due to not adhering to these instructions.

Cables enter the camera body through liquid-tight 3/4" NPT compression glands, each with a gland seal insert and plugs for unused holes. To ensure watertight seals, the cable outer diameter must be between 0.23"-0.29". If you are using other, non-standard cable diameters, you might need to locate or fabricate an insert to fit the cable. Teledyne FLIR does not provide cable gland inserts other than those supplied with the camera.



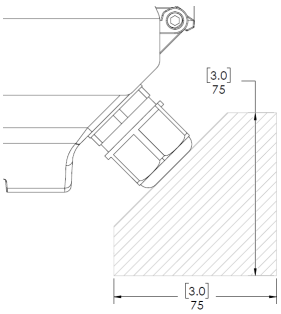
Cable Glands (Seal Inserts Not Shown)

Carefully loosen and remove the gland nuts.

Remove the appropriate number of cable gland seal plugs. However, make sure seal plugs are securely in place for all unused gland seal holes.

Route the cables through the gland seals before terminating and connecting them. In general, terminated connectors do not fit through the cable gland. If you need to route a terminated cable through the cable gland, make a clean, singular cut in the gland seal. Then, route the cable through it. Leave the gland nuts loose until you have finished routing and connecting all of the cables.

Allow enough space for cable egress through the gland. The typical cable bend radius is 50-75 mm (2-3 in). Observe the cable manufacturers' recommendations regarding bend radius.



Cable Egress Space (75 mm / 3 in Bend Radius)

According to the information in Connect the Camera, terminate the cables and then connect them.

To ensure a watertight seal, fully tighten the gland nuts.

Close and Secure the Cover

Using the Torx wrench, alternately tighten the four screws that secure the cover to the camera; torque to 8+0.5 kgf-cm.

This document does not contain any export-controlled information.

Caution

To ensure the camera's IP66 and IP67 dust and water ingress ratings, properly and securely close the camera cover and tighten the screws. Failure to do so can void the camera's warranty.

Re-attach the sunshield, if relevant.

2.9 Aim the Camera

The camera itself is stationary and does not provide physical aiming adjustment. For information about how to adjust mounting hardware to aim the camera, refer to the instructions for the mounting hardware.

Tips

- Aim the camera while you or someone else is monitoring the camera's live video on the camera web page or in a video stream.
- Aim the camera while supporting the camera's weight with your hand or with the help of someone else.

2.10 Check the Boresight

At the factory, the visible video image was aligned with the thermal video image. Users assigned the role of admin or expert can fine tune the camera's boresight to the scene using the camera's web page. For more information, see Boresight Page.

2.11 Configure the Analytics

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

2.12 Additional Configuration

Depending on how you are installing and using the FH-Series camera, and the network and VMS to which it is connected, initial configuration can also consist of enabling, disabling, or configuring the following settings using the camera's web page:

Settings	User Role
• Live video and video streams • Visible imager • Thermal imager • External IR illumination (when enabled) • Current and idle I/O states • Temperature measurement (R models) • On-screen display (OSD) • Geotracking • Georeference	Any user

This document does not contain any export-controlled information.

Settings	User Role
• Date and time • Alarms • Audio • Enabling and configuring external I/O devices • Notification emails • Onboard de-icing heaters and cooling fan • Cybersecurity • ONVIF auxiliary commands and output actions • Map • Boresight • Scheduled tasks • Recording • Format a microSD card • Firmware, factory defaults, external IR illumination, and other system settings	Default admin user / user assigned the admin or expert role
Users, roles, and passwords	User assigned the admin role
Pairing an FH-Series camera with a FLIR Security PTZ camera that supports geotracking	FH-Series camera: Any user PTZ camera: Default admin user / user assigned the admin or expert role
ioi PTZ Tracker hand-off	N/A

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

2.13 Attach the Camera to a Supported VMS

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

2.14 Pairing an FH-Series Camera with a FLIR Security PTZ Camera (Optional)

By default, FH-Series cameras support geotracking. You can pair a FH-Series camera with a FLIR Security PTZ camera that supports geotracking. The PTZ camera engages and tracks objects detected by the FH-Series camera.

Visible Cameras	Multispectral Cameras	Thermal Cameras
Quasar 4K 22x IR PTZ CP-6408-21-I	DM-Series	PT-Series HD
Quasar 4K 31x IR PTZ CP-6408-31-I	DX-Series	

Pairing does not require configuration on the FH-Series camera. However, geotracking does require accurate location information for both paired cameras. For the FH-Series camera, see Georeference Page.

If there are significant elevation differences in the coverage area, you might need to upload a digital elevation model (DEM) file to the PTZ camera. For information about creating and uploading the DEM file, see the PTZ camera's documentation.

This document does not contain any export-controlled information.

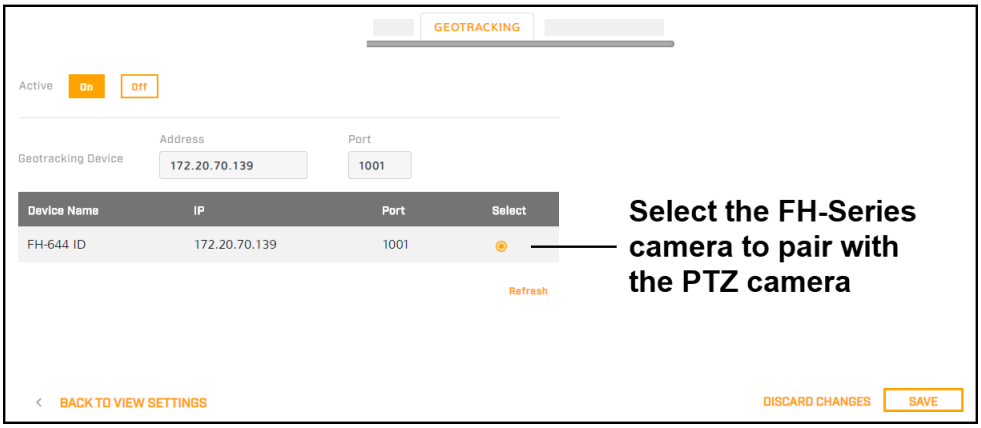
2.14.1 Pairing with a Quasar 4K IR-PTZ, DX-Series, or DM-Series Camera

To pair one of these PTZ cameras with an FH-Series camera, a PTZ camera user assigned the expert or admin role can enable and configure geotracking using *the PTZ camera's web page*. The PTZ camera requires firmware v1.6.0.31 or later.

To enable the pairing on the PTZ camera:

1. Access the PTZ camera and log in to its web page. For information about accessing the PTZ camera, see its installation and user guide.
2. Click **System Settings** and open the **Geotracking** tab.

   A list of supported geotracking devices on the same LAN segment as the PTZ camera appears.
3. Enable geotracking by clicking **On**.
4. From the list of supported geotracking devices, select the FH-Series camera to pair with the PTZ camera.



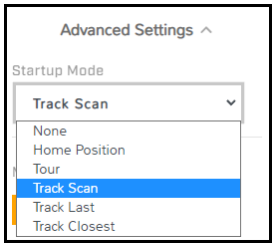
   If the FH-Series camera does not appear in the list, next to **Geotracking Device**, specify the FH-Series camera's IP address and port 1001. Click **Save**. The FH-Series camera appears in the list. Select it.

   Make sure the FH-Series camera's IP address and port appears next to Geotracking Device.
5. Click **Save**. The PTZ camera reboots.

   After the camera reboots, log back in to the camera's web page.

To enable and configure a geotracking mode on the PTZ camera:

1. From the View Settings menu, open the PTZ page.
2. Open **Advanced Settings**.

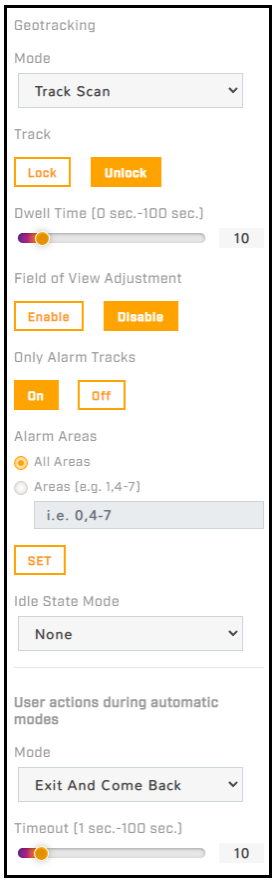


You can:

- Specify one of the following geotracking startup modes / modes:
  - **Track Scan—**The PTZ camera performs a tour scanning all active geotracks. It follows each geotrack for a specified dwell time.
  - **Track Last—**The PTZ camera follows the most recently detected geotrack.
  - **Track Closest—**The PTZ camera follows the geotrack closest to the PTZ camera.

  If the PTZ mode is Single Track, the PTZ camera is currently engaging a geotrack. Selecting another PTZ mode disengages the PTZ camera from the geotrack.

This document does not contain any export-controlled information.



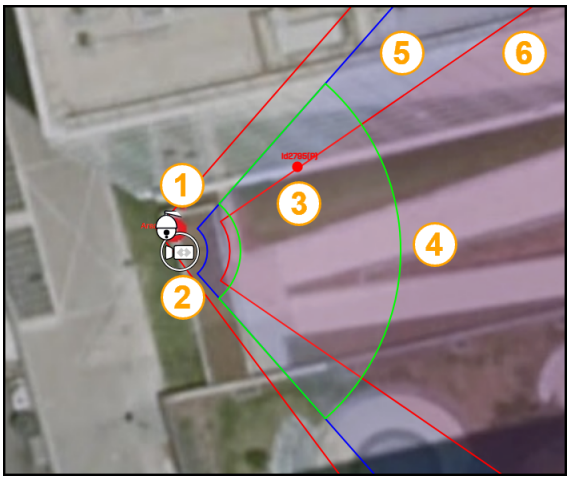
- Lock the PTZ camera onto a currently engaged track, regardless of the existing mode. Make sure the PTZ mode is not None or Single Track. Then, under Track, click **Lock**. As long as the FH-Series camera detects the object and provides the geotracking information, the PTZ camera follows the track. When the FH-Series camera no longer detects the object, the camera automatically changes Track to **Unlock**.
- Specify a Dwell Time, between 0-100 seconds. In Track Scan geotracking mode, the PTZ camera stays on each geotrack for the specified dwell time.
- Enable Field of View Adjustment. The distance from the FH-Series camera to a tracked object determines the PTZ camera's zoom. Specify the PTZ camera's field of view (FoV), between 1-100 meters.
- Enable Only Alarm Tracks. The PTZ camera only tracks objects detected by the FH-Series camera in an alarm region. Select:
  - **All Areas—**The PTZ camera tracks objects detected in all alarm regions.
  - **Areas—**The PTZ camera tracks objects detected in specified alarm regions. To specify specific regions and ranges of regions, you can use a comma. For example, you can specify 0, 4-7.

  Click **Set**.
- Specify the Idle State Mode, the behavior of the PTZ camera when it is in a geotracking mode and there is no track to engage:
  - **None—**PTZ camera stays at the current position.
  - **Home Position—**PTZ camera moves to its home position.
  - **Preset—**PTZ camera moves to the specified preset.
- Specify the behavior of the PTZ camera when it is in an automatic mode and a user performs a manual action such as moving, zooming, or focusing the camera:
  - **None—**PTZ camera does not allow manual commands and ignores them.
  - **Exit—**PTZ camera exits the automatic mode and performs the manual action.
  - **Exit and Come Back—**PTZ camera exits the automatic mode, performs the manual action, and then returns to the automatic mode after the specified Timeout, between 1-100 seconds.

The PTZ camera immediately applies and saves these settings. You do not have to click **Save**.

The image at right shows an example of an FH-Series camera's Geotracking Page display, with the following overlaid onto a map that has been uploaded and calibrated:

1. a supported FLIR Security PTZ camera
2. the FH-Series camera being accessed / configured (circled)
3. an object detected by the FH-Series camera inside a geotracking alarm region
4. FH-Series camera VA / geotracking range (green borders)
5. FH-Series camera visible sensor horizontal field of view (blue borders)



This document does not contain any export-controlled information.

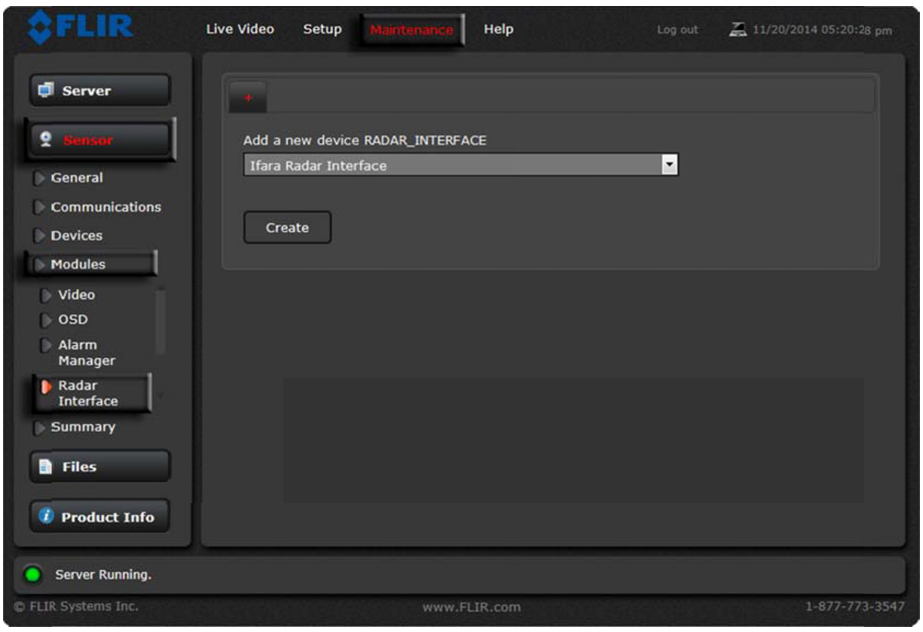
6. FH-Series camera thermal sensor horizontal field of view (red borders)

2.14.2 Pairing with a PT-Series HD Camera

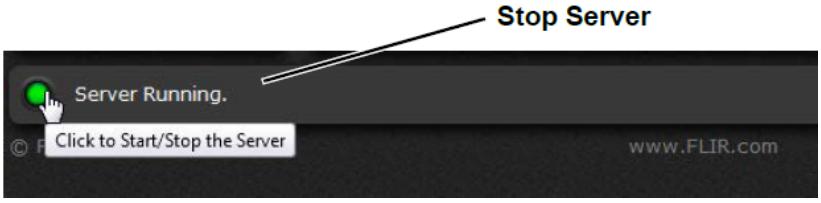
To pair a PT-Series HD camera with an FH-Series camera, a PT-Series HD camera user assigned the expert or admin role can enable and configure a geotracking radar interface using *the PT-Series HD camera's web page*. The PT-Series HD camera requires firmware v1.3.0.29 or later. For information about how to update the camera's firmware, see the *PT-Series HD Installation and User Guide*.

To enable a geotracking radar interface on a PT-Series HD camera:

1. Access the PT-Series HD camera and log in to its web page. For information about accessing a PT-Series HD camera, see the *PT-Series HD Installation and User Guide*.
2. Open the Maintenance menu and then open **Sensor > Modules > Radar Interface**.



3. Stop the camera's server.

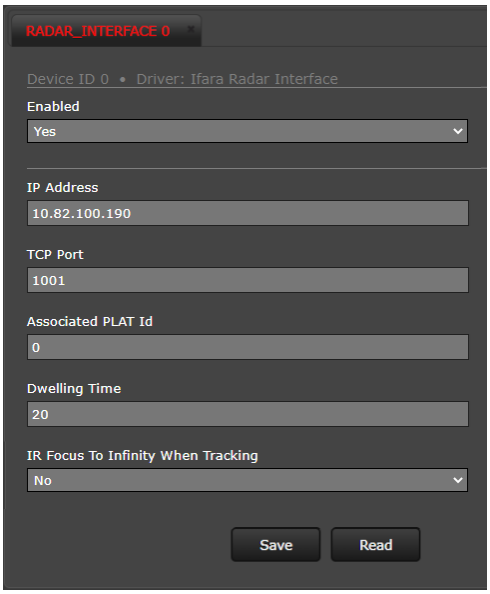


4. Under Add a new device RADAR_INTERFACE, select Ifara Radar Interface. Then, click **Create**.

   The camera creates the radar interface and the settings appear.

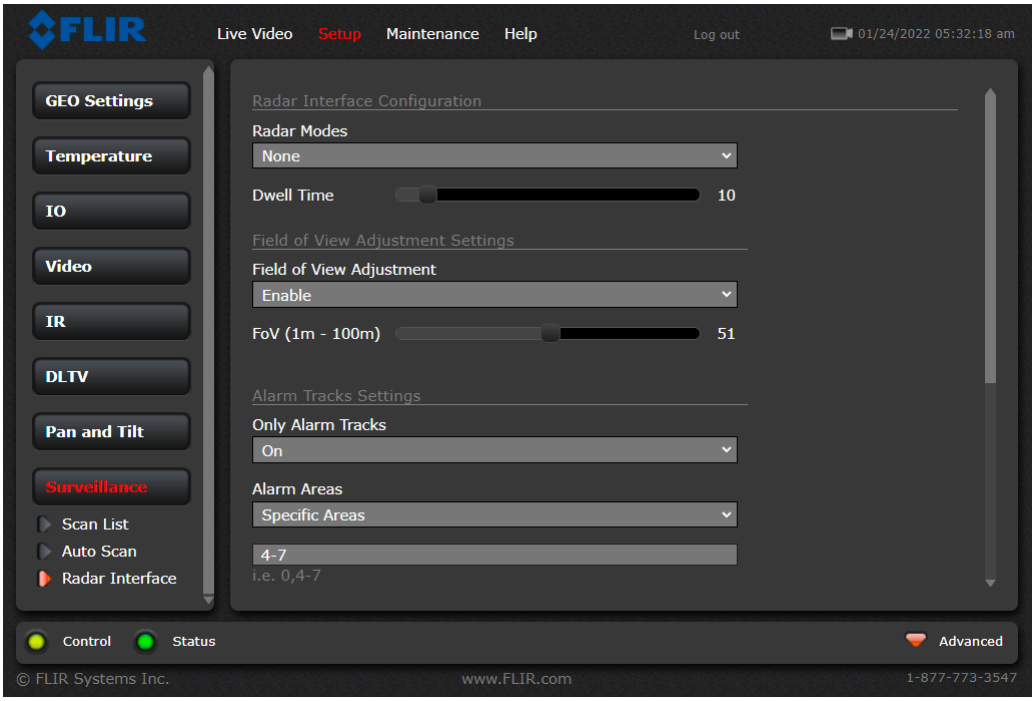
This document does not contain any export-controlled information.

5. Enable the interface.
6. Specify:
   - **IP Address—**The FH-Series camera's IP address.
   - **TCP Port—**The TCP port number the FH-Series camera's Nexus server uses (1001). This is not the port for the FH-Series camera nor for its web page.
   - **Associated PLAT Id—**Make sure it is 0 (zero).
   - **Dwelling Time—**The amount of time, in seconds, that elapses between the camera pointing at targets, when the camera is in Track Scan radar mode. It does not apply to any other camera modes.
   - **IR Focus To Infinity When Tracking—**Enable to set the camera's focus at infinity when it is engaged on a geotrack.
7. Click **Save**.



To configure the geotracking radar interface:

In the Setup menu, open **Surveillance > Radar Interface**.



You can:

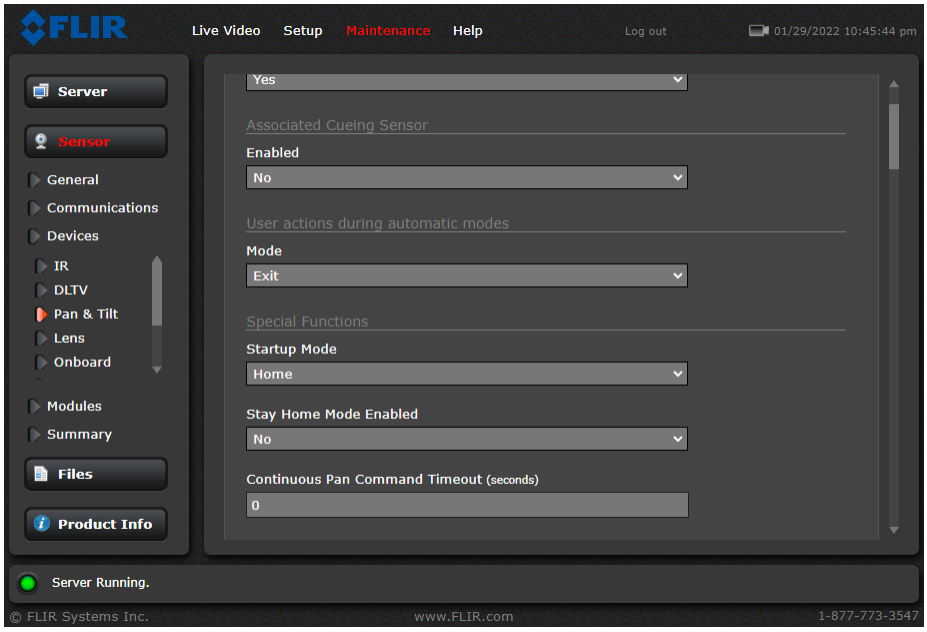
- Select a Radar Mode:
  - **Track Scan—**The PT-Series HD camera performs a tour scanning all active geotracks. It follows each geotrack for a specified dwell time.
  - **Engage Last—**The PT-Series HD camera follows the most recently detected geotrack.
  - **Engage Closest—**The PT-Series HD camera follows the geotrack closest to the PT-Series HD camera.

- Specify a Dwell Time between 0-100 seconds. In Track Scan mode, the camera stays on each geotrack for the specified dwell time.
- Enable Field of View Adjustment. The distance from the FH-Series camera to a tracked object determines the PT-Series HD camera's zoom. Specify the PT-Series HD camera's field of view (FoV), between 1-100 meters.
- Enable Only Alarm Tracks. The PT-Series HD camera only tracks objects detected by the FH-Series camera in an alarm region. Select:
  - **All Areas—**The PT-Series HD camera tracks objects detected in all alarm regions.
  - **Areas—**The PT-Series HD camera tracks objects detected in specified alarm regions. To specify specific regions and ranges of regions, you can use a comma. For example, you can specify 0, 4-7.

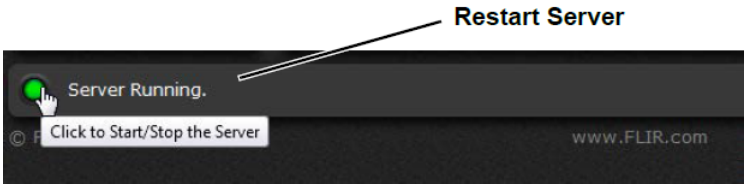
  Click **Set**.
- Specify the Idle State Mode, the behavior of the PT-Series HD camera when it is in a radar mode and there is no geotrack to engage:
  - **None—**PT-Series HD camera stays at the current position.
  - **P&T Home—**PT-Series HD camera moves to its home position.
  - **Go to Preset—**PT-Series HD camera moves to the specified preset.

To configure the PT-Series HD camera to start up in a geotracking radar mode:

1. In the Maintenance menu, open **Sensor > Devices > Pan & Tilt**.

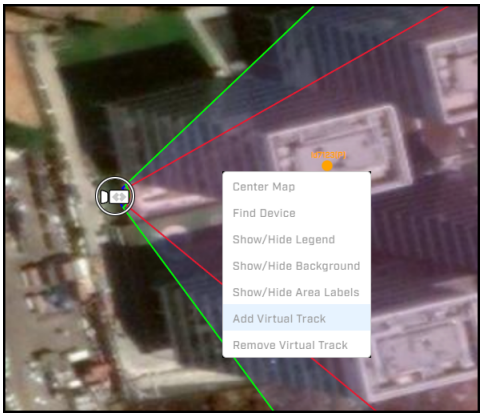


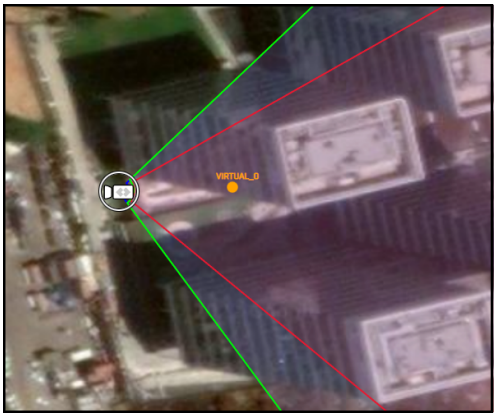
2. Under Special Functions, for Startup Mode, select one of the geotracking radar modes: Track Scan, Engage Last, or Engage Closest.
3. Scroll to the bottom of the page and click **Save**.
4. Restart the camera's server.



2.14.3 Confirming PTZ Camera Pairing Configuration

1. If you are not logged in to *the FH-Series camera's web page*, log in to it.
2. On the Geotracking page, right-click on the detection area display, within the camera's detection range, and select **Add Virtual Track**.





A virtual track appears at the right-click point, on the detection area display. The FH-Series camera communicates the virtual track to the PTZ camera, which points to the virtual track when pairing is properly configured. While the virtual track is enabled, the FH-Series camera ignores actual geotracks.

3. Make sure the PTZ camera is pointing at the virtual detected object.

   If it is not, right-click on the FH-Series camera detection area display and select **Remove Virtual Track**. Then, check and adjust the PTZ camera's and the FH-Series camera's georeference settings.

   Select **Add Virtual Track** and check again whether the PTZ camera is pointing at the virtual detected object.

This document does not contain any export-controlled information.

3 Operation

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

3.1 Accessing the Camera

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

To log in to the camera's web page:

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

     The DNA tool does not require a license to use and is a free download from Teledyne FLIR.

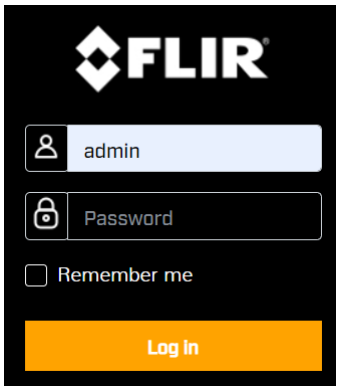
     Download the DNA tool; unzip the file; and then double-click to run the tool (DNA.exe). The Discover List appears, showing compatible devices on the VLAN.
   - Type the camera's IP address in a browser's address bar (when the PC and the camera are on the same network). If you do not know the camera's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

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

   User name—admin

   Password—admin

   If you do not know the user name or password, contact the person who configured the camera's users and passwords.



3. When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, specify a new password for the admin user and then log back in using the new password.

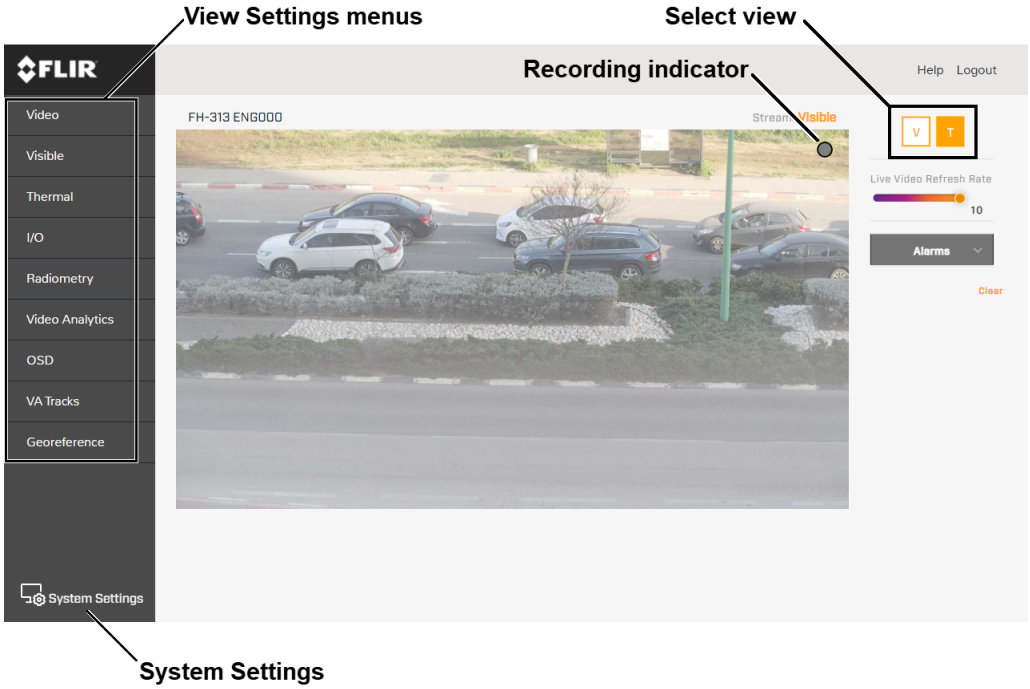
   Use a strong password consisting of at least 12 characters and at least one uppercase letter, one lowercase letter, and one number. Passwords can include the following special characters: | @#~!$&<>+_-.,*?= .

The camera's View Settings Home Page appears.

3.2 View Settings Home Page

The View Settings home page displays live video images of the selected view. When a user assigned the expert or admin role logs in to the camera's web page, the page also displays View Settings menus along the left side banner and other options.

This document does not contain any export-controlled information.



View Settings Home Page - FH-xxx R models - Users Assigned the Admin or Expert Role
Visible Video Images Selected - Default Settings

System Settings

Users assigned the admin or expert role can click **System Settings** to configure the camera. For more information, see Configuration.

Live Video

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

You can select to view visible (V) or thermal (T) live video images. The live video on the camera's web page is not the actual video stream. Changes to the video stream, analytics tracking overlay, or on-screen display (OSD) settings might not affect the live video.

You can also set the Live Video Refresh Rate between 1-10 image frames per second (FPS).

The view selected and the Live Video Refresh Rate setting only affect the live video; they do not affect the camera's video streams nor its analog video output.

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

Active Alarms

Other Options

Additional choices are for Help and Logout.

3.3 Making Changes to Settings

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

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

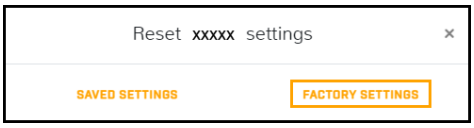
This document does not contain any export-controlled information.

Tip

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

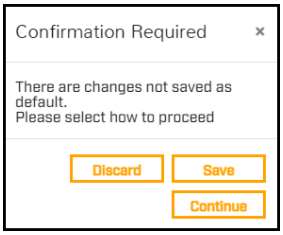
View Settings

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



Regardless of whether the camera has already applied changes, to save all changes since the last time these settings were saved, click **Save**. This can include earlier changes that were not saved.
To restore previously saved settings or the factory default settings, click **Reset**. To close the message and return to the page without restoring settings, click the close icon ✕.

Tip

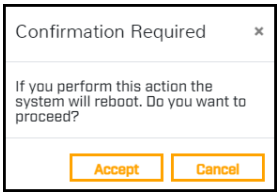


If you try to navigate to a different page before saving changes, a confirmation message appears. In most cases, you can click **Continue**, which allows you to navigate to other pages and test the setting changes. Then, you can return to the page and save the new settings. Or, you can: 1) discard the changes; 2) save them; or 3) close the confirmation message without discarding the changes or saving them by clicking the close icon ✕.

System Settings

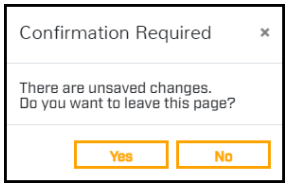
When you make a change to most System Settings, the **Discard Changes** link and the **Save** button become enabled. For some System Settings, the camera immediately applies the changes, but does not save them; for example, on the Alarm Page and on the Audio Page. For others, the camera does not apply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

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



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

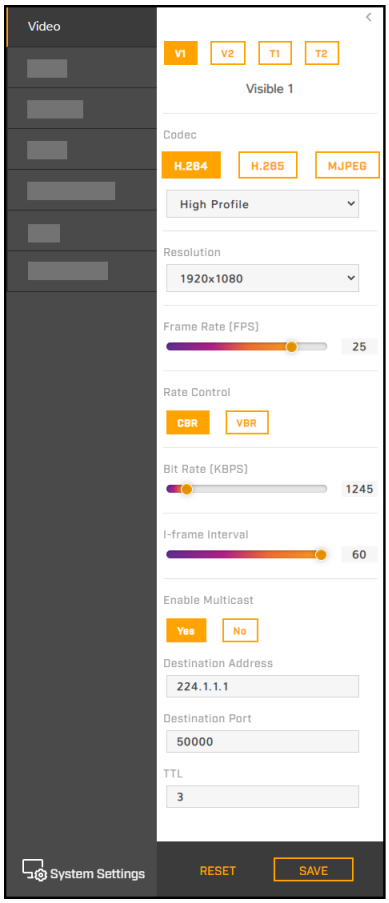
Tip



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

This document does not contain any export-controlled information.

3.4 Video Page



The camera provides four IP video streams: two visible streams (V1 and V2) and two thermal streams (T1 and T2). In general, modifying the default IP video settings is not necessary. In some cases, such as when a stream is sent over a wireless network, fine-tuning the streams can help reduce the bandwidth requirements.

To change the settings for a particular video stream, click the relevant button (V1, V2, T1, or T2).

V1 / V2

Codec options for the visible streams are H.264, H.265, or MJPEG.

Resolution options are 3840x2160 (4K), only available for V1 with H.264 or H.265; 1920x1080 (1080p); 1280x720 (720p); and 640x480 (480p). The Frame Rate range is 5-30 FPS (frames per second).

T1 / T2

Codec options are H.264 or MJPEG.

Thermal stream resolution is fixed at 640x512. In FH-3xx cameras, the native resolution of the thermal imager is 320x256. Therefore, FH-3xx cameras upscale thermal images to 640x512.

The Frame Rate range is 5-30 FPS.

Codecs, Quality, and Bandwidth

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

With the H.264 and H.265 codecs, you can set the:

- **Profile**:
  - **High Profile** (default for H.264 and the only profile available for H.265)—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.
- **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, you 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

This document does not contain any export-controlled information.

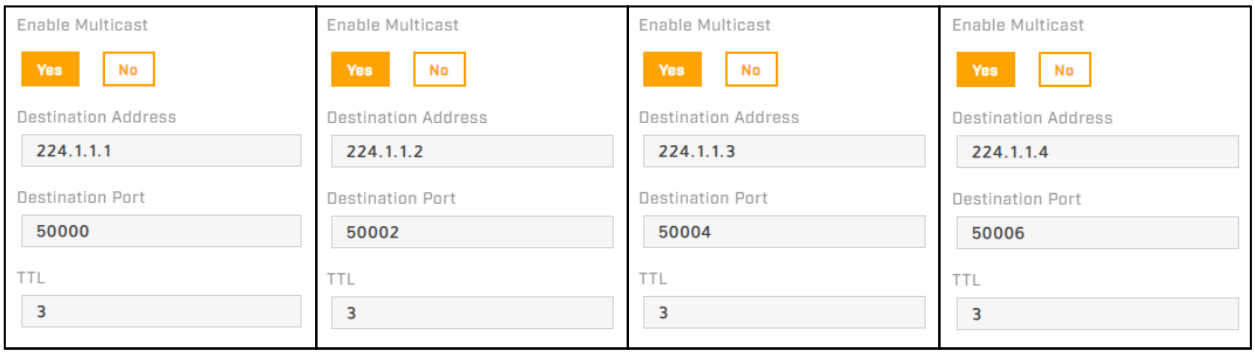
you experience video issues when using MJPEG and high-resolution video, try adjusting the Quality and the resolution settings.

Tips

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

Enable Multicast

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



Visible 1 *Visible 2* *Thermal 1* *Thermal 2*

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

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

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

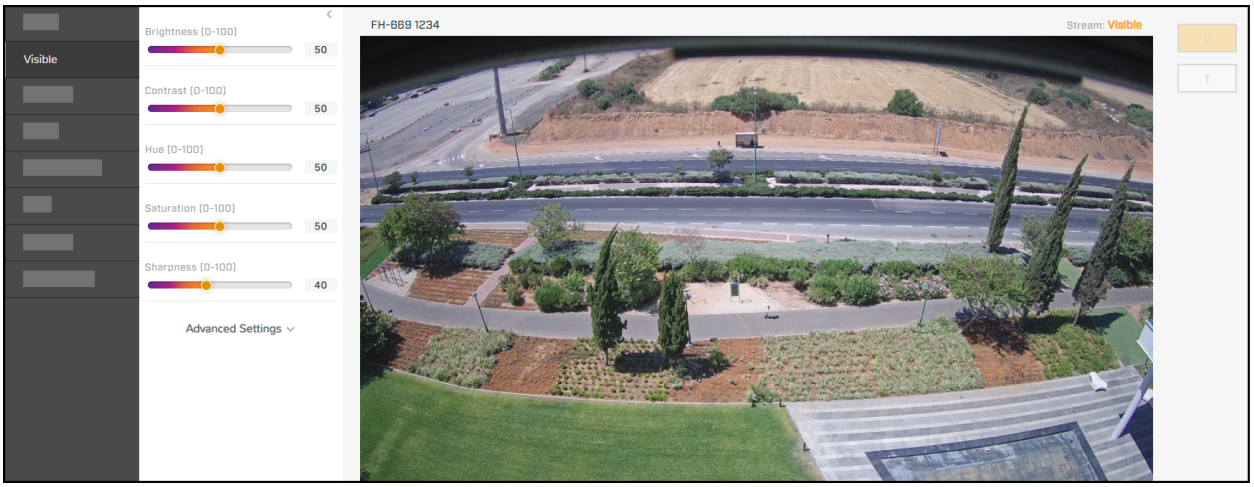
- **V1**—rtsp://192.168.0.250:554/stream1
- **V2**—rtsp://192.168.0.250:554/stream2
- **T1**—rtsp://192.168.0.250:554/stream3
- **T2**—rtsp://192.168.0.250:554/stream4

To maintain compatibility with legacy systems, the stream names are aliased as: ch0 = stream1, ch1 = stream2, ch2 = stream3; and ch3 = stream4.

By default, RTSP authentication is enabled. To access any of the camera's video streams, you can use the name and password for any of the camera's users. Users assigned the role of admin or expert can disable RTSP authentication on the Services.

This document does not contain any export-controlled information.

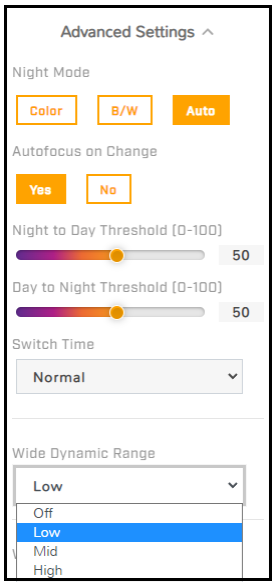
3.5 Visible Page



You can adjust the following visible video settings:

- **Brightness**
- **Contrast** (Max Gain)
- **Hue**
- **Saturation**
- **Sharpness**

Advanced Settings



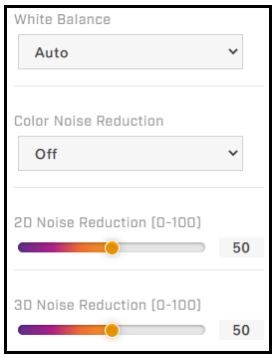
- **Night Mode**—Set the visible video to:
  - **Color** (day mode)
  - **B/W** (night mode)
  - **Auto** (default)—Automatically switches the visible video mode according to light level. When Night Mode is set to Auto, you can set the thresholds at which the visible video switches from black and white to color (Night to Day Threshold) and vice versa (Day to Night Threshold). Specify a value between 0-100, where 0 switches modes at a lower light level (darker) and 100 switches modes at a higher light level (brighter). You can also specify a Switch Time**,** the transition time between modes, to Slow, Normal, or Fast.
- **Autofocus on Change—**When the visible video mode switches from black and white to color, and vice versa, the visible camera lens performs a one-time autofocus. The default is No (disabled). Teledyne FLIR recommends enabling this only when external illumination is installed and active.
- **Wide Dynamic Range**

  Digital Wide Dynamic Range (dWDR) digitally enhances each video frame to improve image quality and increase the amount of detail in high contrast scenes. High contrast scenes consist of areas with different lighting conditions; some areas are bright and others are dark. WDR can produce more detail in both the dark and the bright areas of the image. Without WDR, either the bright areas would be overexposed (too bright) or the darker areas would be completely dark. As the scene contrast level

This document does not contain any export-controlled information.

increases, you can increase the dWDR level. Available when the Shutter WDR exposure mode is not enabled, select Off, Low, Mid, or High.

- **White Balance**—Set according to operating environment:



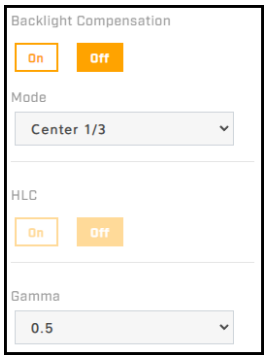
  - **Auto** (default)—Computes the white balance value output using color information from the entire screen. It is suitable for an environment with a light source color temperature in the range of approximately 2,700 ~ 7,500K.
  - **ATW** (Auto Tracking White Balance)—Automatically adjusts the white balance in a scene while temperature color is changing. It is suitable for an environment with a light source color temperature in the range of approximately 2,500 ~ 10,000K.
  - **Manual—**To activate the factory-optimized white balance setting, click One Push Trigger . Define the Rgain and Bgain between 0-100 to increase the red and blue luminance. This setting might not be ideal for every lighting environment.

- **Noise reduction (NR) settings**

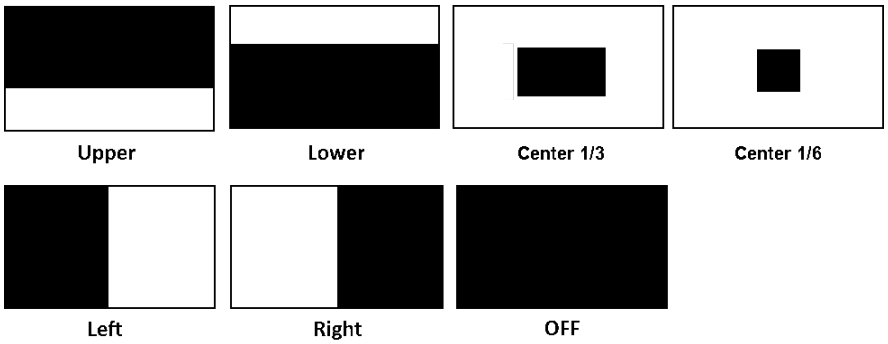
  NR reduces or eliminates artifacts that can limit the ability to positively identify an object. There are two types of noise: luminance noise and color (chroma) noise. 2D NR and 3D NR settings reduce luminance noise: dots of varying brightness levels (black, white, and gray). Teledyne FLIR recommends against completely eliminating luminance noise, because it can result in unnatural images. Teledyne FLIR also recommends configuring the Color Noise Reduction setting before configuring the 2D Noise Reduction and 3D Noise Reduction settings.

  - **Color Noise Reduction**—Controls the noise appearing as red, green and blue dots between light and dark areas. Four settings are available: Off, Low, Mid, High. High maximizes the blending of the color noise with the image, effectively removing the dots, while Low minimizes the blending.
  - **2D Noise Reduction**—Analyzes each individual frame pixel by pixel to eliminate environmental noise. 2D NR can produce superior images for moving objects. However, it is less precise than 3D NR and can cause blurring around the edges of objects. Specify a value between 0-100, where 0 provides no 2D NR and 100 provides the maximum level of 2D NR.
  - **3D Noise Reduction**—Provides superior noise reduction by analyzing adjacent frames to reduce image noise / snow in low-light conditions. However, 3D NR can create more motion blur on moving objects than 2D NR. When the camera's visible video is needed at night or other low-light conditions, use external IR illumination and 3D NR. Specify a value between 0-100, where 0 provides no 3D NR and 100 provides the maximum level of 3D NR.

- **Backlight Compensation** (BLC)— By default, BLC is disabled and the camera's auto exposure algorithm considers the entire image. For images with a bright light source that puts the subject of interest in shadow or silhouette, enabling BLC and selecting the region of interest (ROI) can improve the image. With BLC enabled, the auto exposure algorithm considers only the selected ROI. When the Shutter WDR exposure mode is not enabled, you can enable BLC and select Upper, Lower, Center 1/3, Center 1/6, Left, or Right.



This document does not contain any export-controlled information.



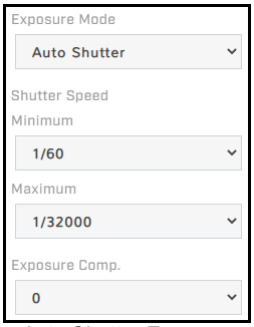
Backlight Compensation Modes

- **HLC** (Highlight Compensation)—Detects areas of the image overexposed by bright light sources such as headlights or spotlights and reduces image exposure only in these areas to enhance overall image quality. Available when the Shutter WDR exposure mode is not enabled and when dWDR is not enabled.

- **Gamma—**Ensures faithful reproduction of an image. Select 0.45 (default), 0.5, 0.6, 0.7, 0.8, 0.9, or 1. When set to 1, the image displayed on your screen is the same as the original image.

- **Exposure Mode**

  Each exposure mode has its own default settings for day / night mode, exposure compensation, backlight compensation, WDR level, and other features. When you change the exposure mode, the camera changes these other settings to the new exposure mode's default settings. To download the camera's current configuration, see the Firmware & Info Page.



Auto Shutter Exposure Mode Settings

  - **Auto Shutter—**A standard exposure mode that produces a natural image. Select a minimum and a maximum shutter speed.

    - **Minimum Shutter Speed**—Specify the slowest shutter speed based on the amount of light in the scene, speed of moving objects, and noise. If the scene includes fast-moving objects, Teledyne FLIR recommends specifying a minimum shutter speed faster than 1/25 or 1/30 seconds. The video format determines the minimum shutter speeds available, as shown, in fractions of a second:

Minimum Shutter Speed - Auto Shutter Mode					
NTSC			PAL		
1	1/200	1/4000	1	1/200	1/4000
1/2	1/250	1/5000	1/2	1/250	1/5000
1/4	1/400	1/8000	1/4	1/400	1/8000
1/7.5	1/500	1/10000	1/6.25	1/500	1/10000
1/15	1/800	1/12500	1/12.5	1/800	1/12500
1/30	1/1000	1/16000	1/25	1/1000	1/16000
1/60	1/2000	1/20000	1/50	1/2000	1/20000
1/120	1/2500	1/25000	1/100	1/2500	1/25000

    - **Maximum Shutter Speed**—Select the fastest shutter speed based on the amount of light in the scene. A faster shutter speed decreases the amount of light entering the sensor and results in a darker image.

This document does not contain any export-controlled information.

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

Maximum Shutter Speed - Auto Shutter Mode					
NTSC			PAL		
1/120	1/1000	1/10000	1/100	1/1000	1/10000
1/200	1/2000	1/12500	1/200	1/2000	1/12500
1/250	1/2500	1/16000	1/250	1/2500	1/16000
1/400	1/4000	1/20000	1/400	1/4000	1/20000
1/500	1/5000	1/25000	1/500	1/5000	1/25000
1/800	1/8000	1/32000	1/800	1/8000	1/32000

- **Shutter Priority**—Specify a fixed shutter speed.
- **Flickerless** (default)—Eliminates flicker caused by fluorescent lighting in the screening area. Specify the mode.
  - **Mode**—Specify the power used for lighting the scene, 50Hz or 60Hz.
- **Manual**—Specify a fixed shutter speed and the gain.
  - **Gain**—A higher value increases the sensitivity of the image sensor, which brightens the image and adds details, but also increases the noise level. Specify a value between 0-100.

Shutter Speed - Shutter Priority and Manual Exposure Modes					
NTSC			PAL		
1/7.5	1/500	1/10000	1	1/250	1/8000
1/15	1/800	1/12500	1/2	1/400	1/10000
1/30	1/1000	1/16000	1/4	1/500	1/12500
1/60	1/2000	1/20000	1/6.25	1/800	1/16000
1/120	1/2500	1/25000	1/12.5	1/1000	1/20000
1/200	1/4000	1/32000	1/25	1/2000	1/25000
1/250	1/5000		1/50	1/2500	1/32000
1/400	1/8000		1/100	1/4000	
			1/200	1/5000	

- **Shutter WDR**—Enables True WDR. The camera analyzes the exposure and level of detail in two consecutive frames taken at two exposure settings and shutter speeds; determines the optimal combination of regions within the scene; and generates a single, composite frame with wide dynamic range. When Shutter WDR is not enabled, the camera operates in linear mode; that is, the camera streams every visible frame it takes.

  When Shutter WDR is enabled, dWDR, BLC, and HLC are not available.

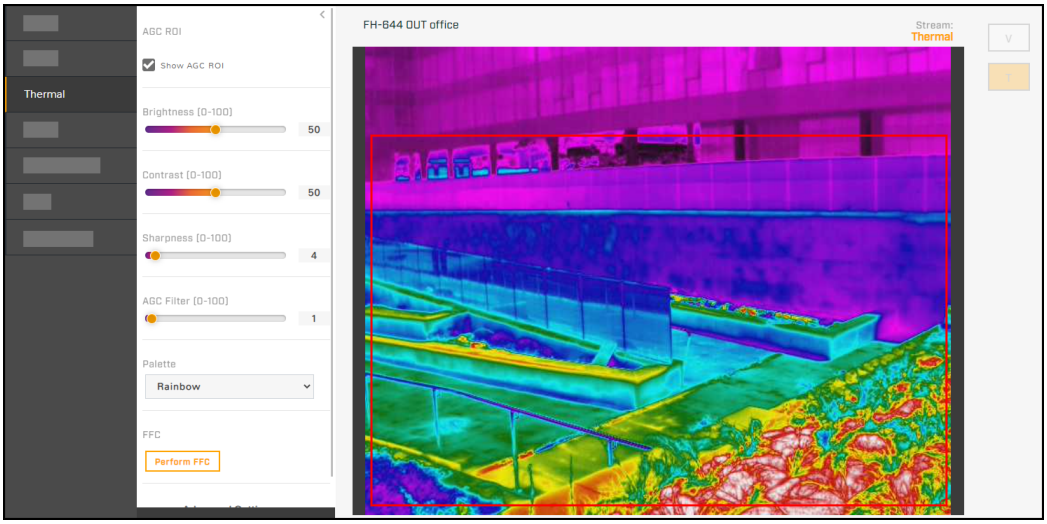
  When you change the Shutter Mode, the camera immediately applies the new setting. When you change the Shutter Mode to or from Shutter WDR, it can take a few seconds for the camera to apply the new setting.

This document does not contain any export-controlled information.

- **Exposure Comp.** (compensation; not available in Manual exposure mode)—0 (no compensation) by default. You can specify whether the camera's auto exposure algorithm produces a brighter or darker image by digitally adjusting the camera's F/# and shutter speed. You can specify a value between -2 (darkest) and +2 (brightest), in 1/3 increments.
- **Stabilization** (Electronic Image Stabilization)—Keeps the image steady and compensates for external vibration. To ensure calibration accuracy, after enabling stabilization, keep the camera still for three seconds. When Stabilization is On, the stabilization algorithm that processes the image slightly crops the video image. EIS is Off by default.

3.6 Thermal Page

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

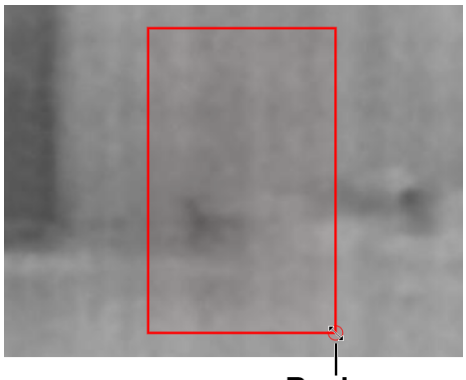


AGC ROI

By default, **Show AGC ROI** is selected. The AGC ROI (region of interest) overlay appears in the live video on the camera web page. In video streams, the overlay does not appear. By default, the ROI is full screen; the AGC algorithm considers the entire image. In some cases, defining an ROI that excludes a portion of the screen can improve the image. For example, you can define an AGC ROI that excludes the sky, which is cold and can strongly affect the overall image.

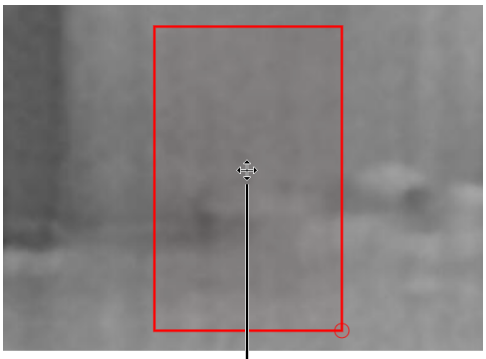
Defining a custom AGC ROI

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



Resize

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



Move

This document does not contain any export-controlled information.

Caution

The camera's thermal video analytics rely on accurate and useful AGC settings. Changes to the ROI can affect those analytics.

AGC Image Settings

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

- **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.

  Tip

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

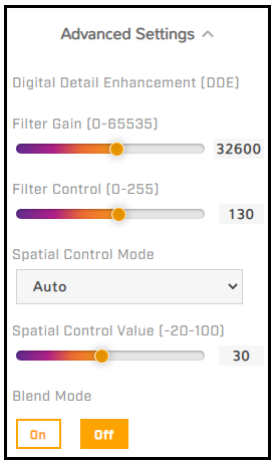
- **Sharpness** (DDE Gain)—Enhances details and/or suppresses fixed pattern noise. Range 0 to 100.
- **AGC Filter**—Determines how quickly a scene adjusts when a hot object appears (or disappears) within the AGC ROI. If set to a low value, when a hot object enters the ROI, the AGC will adjust more slowly to the hot object, resulting in a more gradual transition. Range 0 to 100.
- **Palette**—Select 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 video analytics are enabled for thermal video on the Video Analytics Page, the camera automatically uses the WhiteHot color palette.
- **FFC (Flat-Field Correction)**—To manually trigger FFC, click **Perform FFC**. 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. The thermal image momentarily freezes. At regular intervals or when the ambient temperature changes, the camera automatically performs FFC (also known as Non-Uniformity Correction or NUC).
- **Gain Mode** (available on R models)
  - **Auto—**Camera automatically switches between High Gain Mode and Low Gain Mode according to the maximum temperature detected in the radiometric items (see Radiometry Page (R models)). If no radiometric items have been configured, the camera remains in High Gain / Low Temperature mode. Teledyne FLIR recommends Auto Gain Mode.
  - **Low** (default)—Camera remains in Low Gain / High Temperature (up to 380°C) Mode. Because it allocates 256 shades over a wider temperature range than in High Gain / Low Temperature Mode, the image can appear to be washed out compared to High Gain Mode.
  - **High—**Camera remains in High Gain / Low Temperature (up to 150°C) Mode.

This document does not contain any export-controlled information.

Advanced Settings

Caution

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.



Digital Detail Enhancement (DDE)

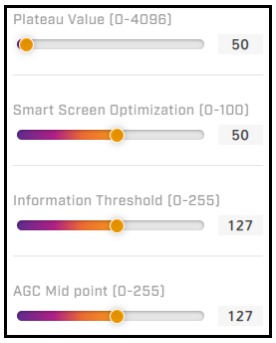
DDE is an advanced, nonlinear image processing algorithm that preserves detail in high dynamic range imagery. The camera enhances detail to match the total dynamic range of the original image, making details more visible. In a high-contrast scene, gain is higher than in a low-contrast scene, allowing faint details to be visible in high contrast scenes without increasing temporal and fixed pattern noise in low contrast scenes.

The DDE filter operates independently from the AGC and enhances edges without affecting brightness or contrast.

- **Filter Gain—**Amount of gain the algorithm applies to details in Manual Spatial Control Mode. Specify a value between 0-65535, with 0 (zero) meaning DDE is disabled. For any value other than zero, the algorithm attenuates or enhances details by a factor (Filter Gain Value / 2048). For example:
  - A value of 1 = 1 / 2048 attenuation of details.
  - A value of 8192 = 8192 / 2048 = 4x enhancement of details.

  The algorithm applies gain globally and locally to the low frequency portion of the image. Therefore, filter gain is relative.

  In Automatic Spatial Control Mode, the camera automatically sets the Filter Gain value.
- **Filter Control—**Also known as DDE Threshold, determines how much detail the algorithm enhances in Manual Spatial Control Mode. Specify a value between 0-255. The DDE algorithm does not enhance details above the specified value. specify a value between 0-255. In Automatic Spatial Control Mode, the camera automatically sets and adjusts the Filter Control value according to scene content.
- **Spatial Control Mode—**Automatic (default) or Manual. For all users and applications, Teledyne FLIR recommends Automatic, also known as Dynamic DDE. Teledyne FLIR strongly recommends not using Manual.
- **Spatial Control Value—**Controls the Automatic Spatial Control Mode. Range -20 to 100. 0 (zero) is neutral and the DDE filter has no effect. Decreasing the value below 0 softens the image, reducing sharp edges. Typical factory settings are between 10 and 30.



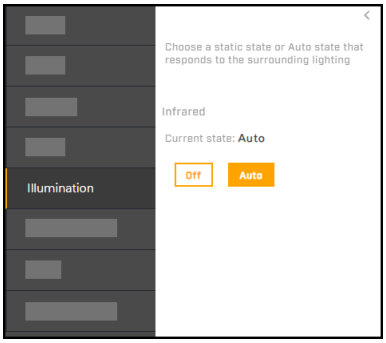
- **Blend Mode—?????**Determines whether the algorithm attempts to suppress detail sharpness halos.???????
- **Plateau Value—**The number of shades the AGC algorithm devotes to large areas of similar detected temperature in a given scene. Decreasing plateau value increases contrast and detail in the other areas of the scene; that is, decreasing the number of shades AGC allocates to those large areas increases the number of shades the algorithm allocates to other areas of the scene. Because AGC ROI has minimum size limitations that rely on plateau value, if you decrease the plateau value and have a very small AGC ROI, you might need to increase the AGC ROI to preserve proper AGC corrected video. Range 0 to 4095.
- **Smart Scene Optimization (SSO)—**Percentage of the AGC histogram allotted a linear mapping; helps provide the highest level of perceived contrast in every scene. Increasing SSO increases how well the

This document does not contain any export-controlled information.

radiometric aspects of an image are preserved; that is, the difference in shades between two objects is more representative of the difference in detected temperature. Range 0 to 100.

- **Information Threshold—**Defines the difference between neighboring pixels the AGC algorithm uses to determine whether the local area contains *information*. Decreasing the threshold increases the amount of information the algorithm determines to be present in the scene. Increasing the threshold decreases that amount and results in a more information-dependent image. Flat portions of the scene - for example, sky or sea - are given less contrast, and pixels exceeding the information threshold are given more contrast. Range 0 to 255.
- **AGC Mid point—**Determines the temperature represented by the middle of the 256 shades the AGC produces. Increasing the value increases detail in hotter scenes; decreasing the value increases detail in lower temperature scenes. Range 0 to 255.

3.7 Illumination Page



When the camera's visible video is needed at night or other low-light conditions, use external IR illumination.

When external illumination is enabled, the Illumination page is available. Users assigned the admin or expert role can enable external illumination on the Firmware & Info Page.

By default, infrared illumination is set to Auto; when the scene becomes dark enough, the visible camera video changes from day mode (color) to night mode (black and white) and turns on the external infrared illumination, using the ALARM OUT 2 connection (see Connect the Camera). Likewise, when the scene becomes light enough, the visible camera video changes from night mode to day mode and turns off the external infrared illumination. You can specify the visible camera's Night Mode setting and adjust the night-to-day and day-to-night thresholds on the Visible Page.

You can set the external infrared illumination to Off. Doing so does not affect the visible camera's Night Mode setting.

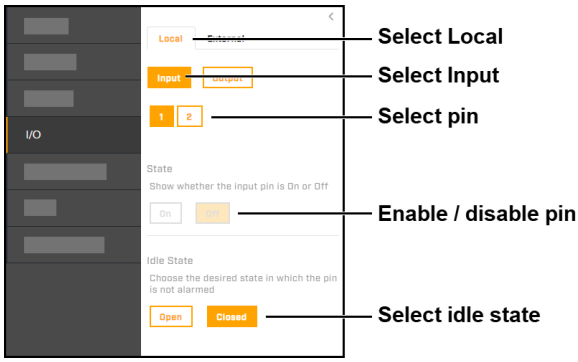
3.8 I/O Page

On the I/O (input / output) page, you can:

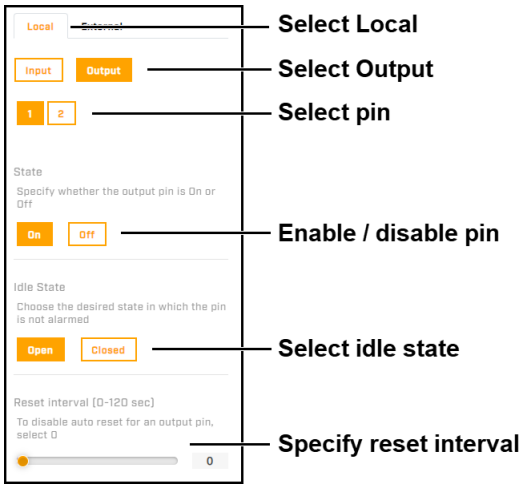
- Enable, disable, and configure the camera's local I/O pins.
- Enable and disable the camera's external I/O pins.

Local I/O pins

Input Pins



Output Pins



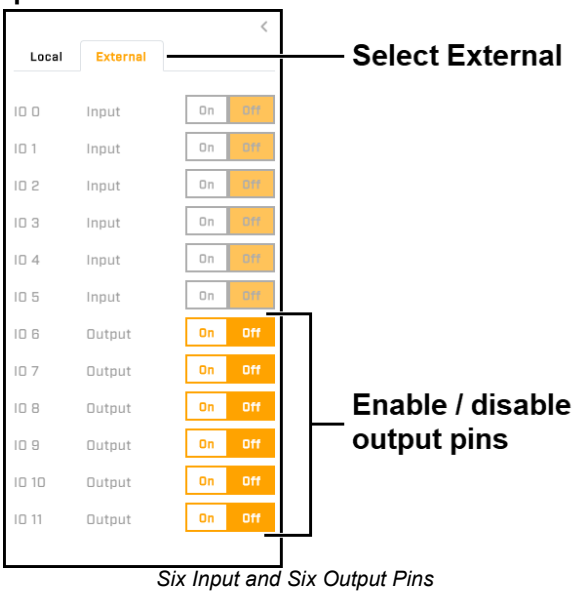
Keep in mind that, when enabled, the camera's external illumination setting controls output 2.

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

This document does not contain any export-controlled information.

External I/O pins

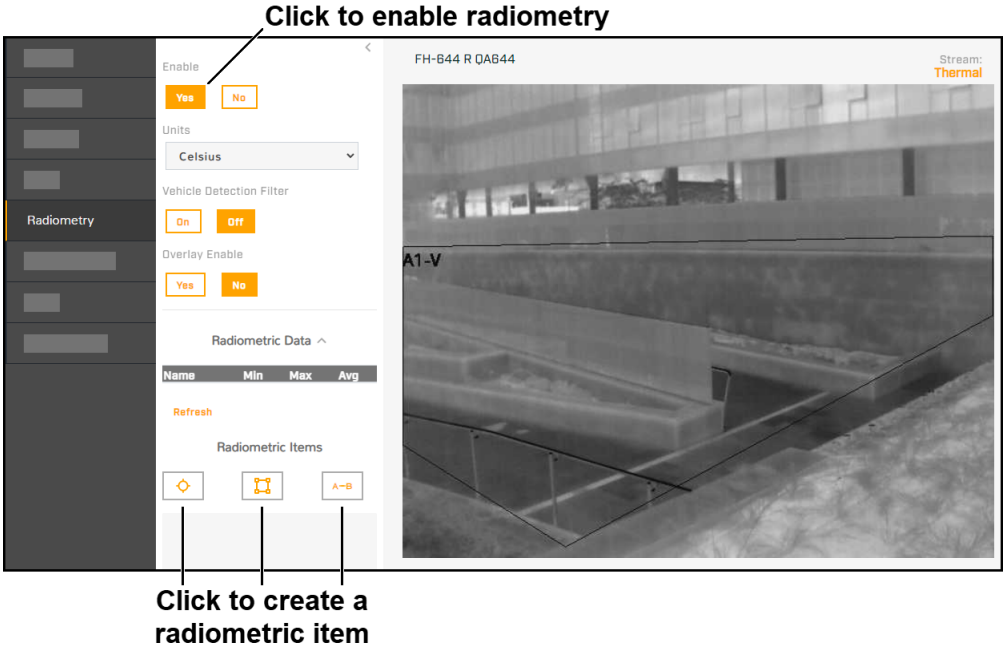
On the I/O Devices Page in System Settings, users assigned the admin or expert role can configure the camera's external I/O connections and the device managing those connections with the camera.



Six Input and Six Output Pins

3.9 Radiometry Page (R models)

FH-Series R models detect, measure, and monitor surface temperatures. Because using a thermal camera for reasonably accurate and precise temperature measurements requires at least a minimum level of expertise in thermography, Teledyne FLIR recommends training. The Infrared Training Center (http://www.infraredtraining.com/) offers training (including online training) and certification in all aspects of thermography.



On the Radiometry page, you can create up to four radiometric items. Each item can:

- detect the surface temperature in a specific spot in the camera's field of view
- detect temperatures over a defined area (box)
- detect the difference in temperatures between two spot or box items

This document does not contain any export-controlled information.

For each item, you can enable and disable temperature measurement and alarms, and specify the alarm condition and threshold. Users assigned the admin or expert role can create and configure alarm rules and actions triggered by these alarm conditions. For more information about creating and configuring alarms, see Alarm Page.

Enable the camera's radiometry features and then select the temperature units (Kelvin, Celsius, or Fahrenheit).

Vehicle Detection Filter

The vehicle detection filter helps prevent moving vehicles that have become stationary from triggering false radiometric alarms. Before enabling it, make sure:

- vehicle classification is enabled on one or more loitering regions on the thermal video
- the loitering regions match the radiometric boxes

After the video analytics detect and classify an object as a vehicle, and that vehicle stays in the loitering region for the specified loitering time, it does not trigger radiometric alarms.

Overlay Enable

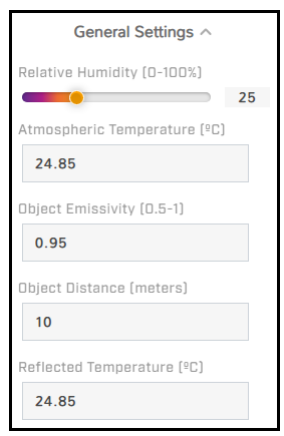
When enabled, an overlay with temperature data from defined radiometric items appears in the live thermal video on the camera web page and in the thermal video streams. You can specify the position of the overlay in the thermal video.

Radiometry overlay

General Settings

- **Relative Humidity (0-100%)—**Relative humidity where the camera is mounted.
- **Atmospheric Temperature—**Ambient temperature where the camera is mounted.

The camera can calculate detected surface temperatures of objects using general settings or values specified for a particular radiometric item (see **Local** below). Specify Object Emissivity, Object Distance, and Reflected Temperature.



This document does not contain any export-controlled information.

To create, enable, and configure radiometric items:

1. Under Radiometric Items, click the spot icon , the box icon , or the differential item icon A–B .

   The item appears in the Radiometric Items list. Spot and box items appear in the center of the live thermal video image.

2. Move spot and box items to the desired location. Hover over the item, and then click and drag it.

   To change the size or shape of a box, click one of the corners and then drag it.

3. For boxes, select the type of temperature measurement to compare (Minimum, Maximum, or Average), and then click **Save**. The differential item appears in the Radiometric Items list.

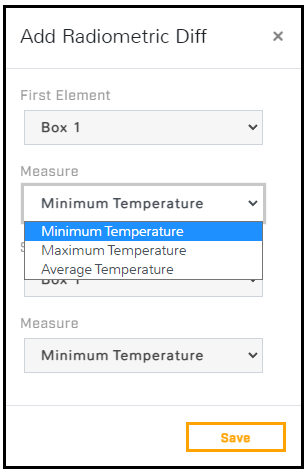
   For differential items, the Add Radiometric Diff screen appears. Select the spots or boxes to compare.

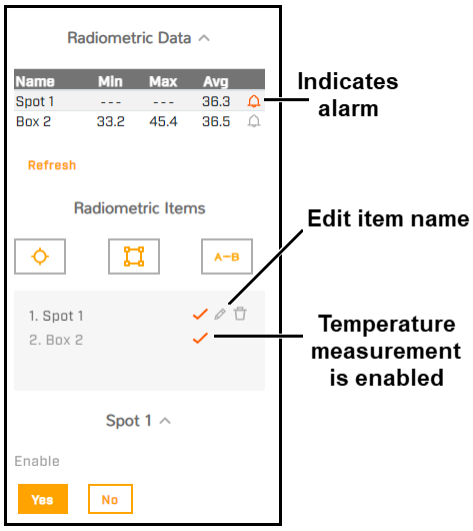
4. With the item selected, you can edit the name of the item, delete it, or configure it.

5. Enable temperature measurement for the item. Radiometric data appears.

   For spots, the surface temperature detected at the spot appears under Avg. For boxes, the minimum, maximum, and average temperatures detected in the box appear. For differential items, the difference in detected temperatures appears.

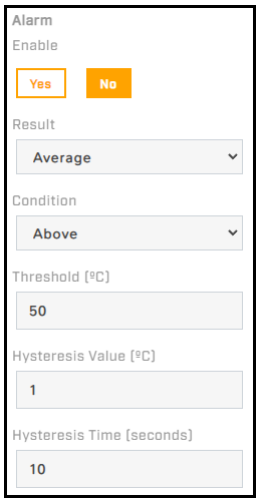
   In the Radiometric Items list, a red check icon indicates that temperature measurement is enabled for the item. To toggle temperature measurement for an item, click the check icon.





Alarm Settings

For each item, you can configure the following alarm settings:



- **Enable—**Enables alarms for the item.
- **Result—**Determines the data that triggers an alarm. For a spot, the alarm result is the Value of the temperature detected at the spot. For a box, select one of the following:
  - **Avg—**The average of the temperatures detected in the box.
  - **Min—**The minimum temperature detected in the box.
  - **Max—**The maximum temperature detected in the box.
- **Condition—**You can select whether a detected temperature Above, Below, or Matches the alarm threshold value triggers an alarm.
- **Threshold—**Specify a temperature value in degrees Kelvin, Celsius, or Fahrenheit, depending on the setting above.

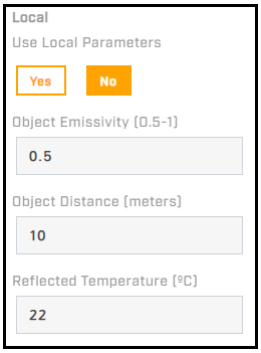
This document does not contain any export-controlled information.

- **Hysteresis—**Specify the number of degrees above or below the Threshold within which the camera does not clear the alarm. For example, the Condition is set to Above, the Threshold is set to 30°C, and the hysteresis is set at 2°C. When the detected temperature rises above 30°C, the camera triggers an alarm until the detected temperature drops below 28°C.

  Likewise, if the Condition is set to Below, the Threshold is set to 30°C, the hysteresis is set at 2°C, and the temperature drops below 30°C, the camera triggers an alarm until the detected temperature rises above 32°C.

- **Hysteresis Time—**Specify the amount of time in seconds that must pass before the camera triggers an alarm, after the alarm condition and threshold have been met. This can be a powerful tool for avoiding false alarms.

Local



Use Local Parameters—

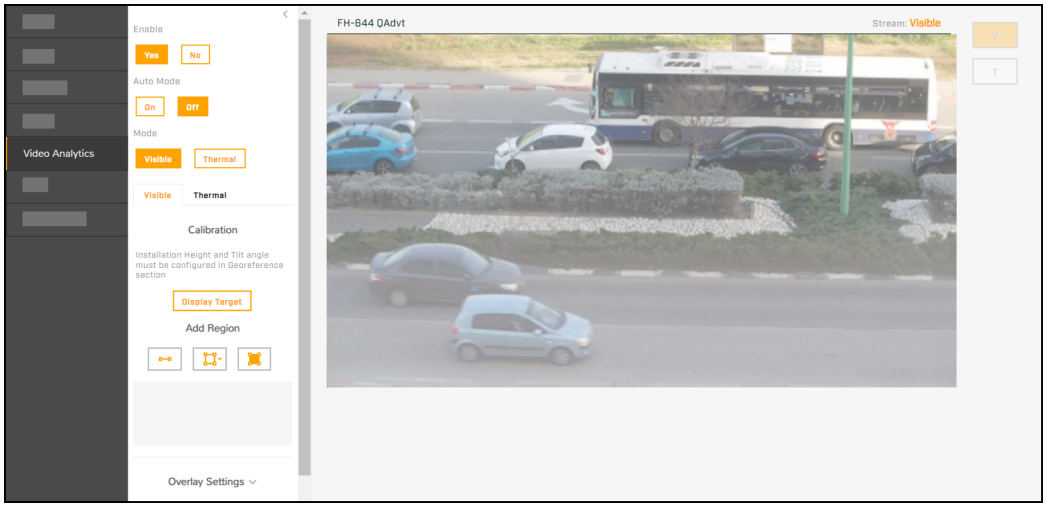
- **Yes**—Camera calculates detected temperatures of objects using values specified for the radiometric item.
- **No** (default)—Camera calculates detected temperatures of objects using General Settings values.

For the selected radiometric item, if the Object Emissivity, Object Distance, and Reflected Temperature are different than the general settings, click **Yes** and then specify those values.

3.10 Video Analytics Page

The camera's advanced onboard video analytics:

- Incorporate convolutional neural networks (CNN) technology
- Intrusion and loitering detection
- Classify detected objects as human or vehicle
- Can be configured separately for the visible video and for the thermal video



On the Video Analytics page, you can:

- Enable or disable the analytics—By default, analytics are disabled. When enabling video analytics for thermal video, use the WhiteHot color palette (see Thermal Page).

This document does not contain any export-controlled information.

- Turn the Auto mode on or off—When enabled, the camera's onboard analytics automatically switch between the visible video (day mode) and the thermal video (night mode), according to the amount of light in the field of view.
- Enable the video analytics on only the visible video or only on the thermal video.
- Check the analytics calibration on both the visible and the thermal video.
- For both the visible and thermal video, create and configure tripwires, intrusion detection or loitering regions, and masking regions. By default, tripwires or regions have not been defined, and alarm rules are disabled.
- Enable and configure the analytics tracking overlay.

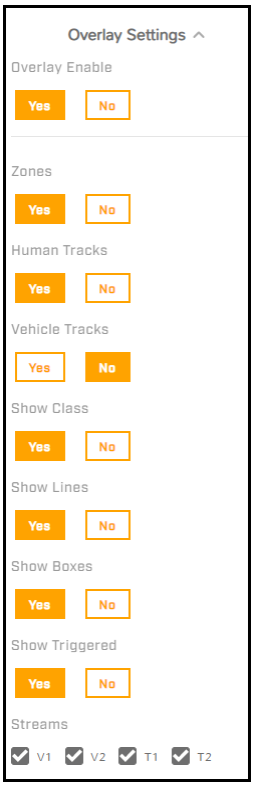
The camera immediately applies and saves changes to settings on the Video Analytics page, affecting the live video images, video streams, and analog video output.

Detection and Classification

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

Overlay Settings

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



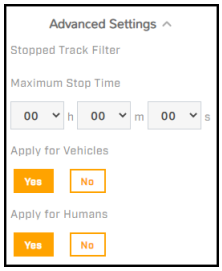
Setting	Description	Comments
Enable	Globally enable or disable the analytics overlay.	Enable one or more individual video streams.
Zones	Show intrusion regions, loitering regions, and tripwires.	
Human Tracks	Show detected objects classified as humans.	Enable Show Class, Show Lines, or Show Boxes.
Vehicle 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 tripwire, intrusion, or loitering alarm.	Enable Human Tracks or Vehicle Tracks. Enable Show Class, Show Lines, or Show Boxes.

This document does not contain any export-controlled information.

Streams ☑ V1 ☑ V2 ☑ T1 ☑ T2	Enable the analytics tracking overlay for individual video streams.	• Does not override the global analytics 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.

Advanced Settings

Stopped Track Filter



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

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

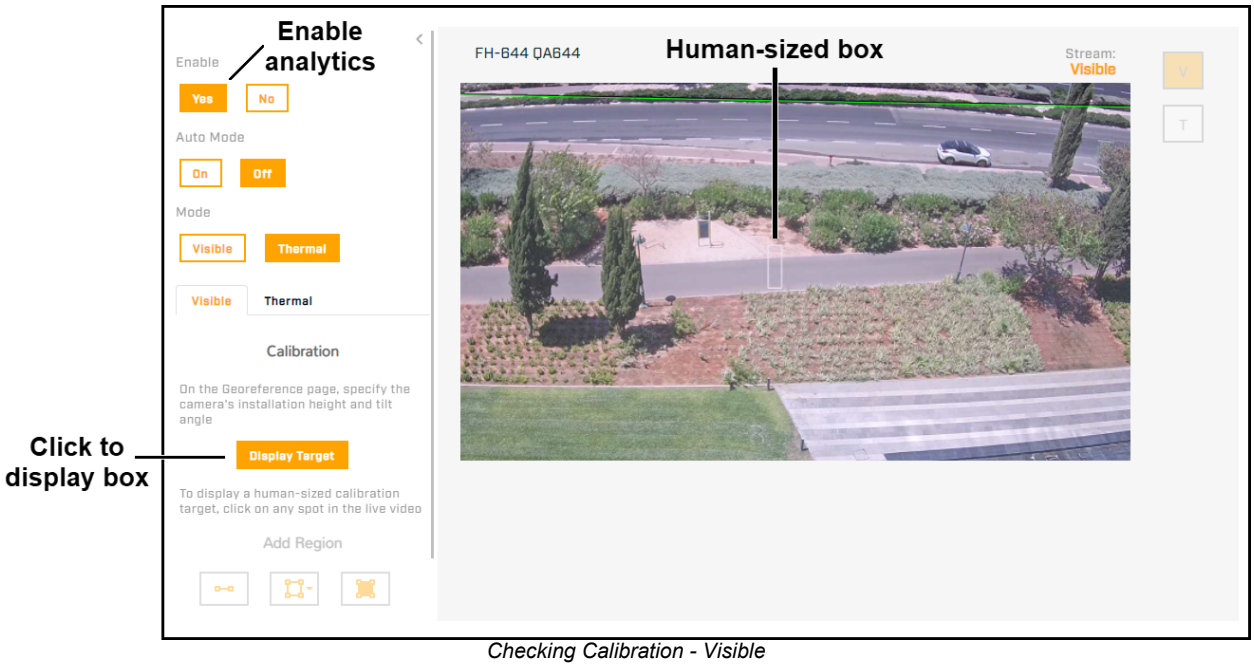
To configure the camera's video analytics:

1. Make sure the camera is mounted in its final location and properly aimed.
2. On the Georeference Page, specify the camera's installation height, tilt angle, and roll angle.
3. Enable the analytics overlay.
4. Check the Analytics Calibration.
5. Create Analytics Regions.

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

3.10.1 Check the Analytics Calibration

Before you can check the camera's video analytics calibration, you need to specify the camera's installation height, tilt angle, and roll angle on the Georeference Page.



Checking Calibration - Visible

1. Make sure that a person about 1.8m (5" 11') tall is in the camera's field of view.

This document does not contain any export-controlled information.

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

Tip

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

- On the Georeference Page, verify the camera's installation height, tilt angle, and roll angle.
- On the Boresight Page, verify the visible and thermal video vertical fields of view are properly aligned.

5. Open the Thermal tab, make sure the analytics are enabled, and repeat the previous steps.

3.10.2 Create Analytics Regions

Create separate analytics regions for the visible video and for the thermal video; for example, to define separate regions according to the time of day. You can also create a masking region; a region that does not generate intrusion alarms.

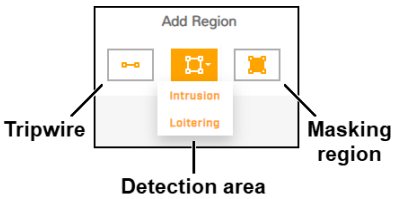
The mode and tab selected determine the tripwires, regions, and labels that appear in the live video. The tab selected determines the live video, the regions that you can create and modify, and the labels that appear in the live video (when the analytics overlay is enabled).

<table>
<tr><th rowspan="3">Mode</th><th rowspan="3">Tab & Live Video</th><th colspan="4">Tripwires and Regions</th></tr>
<tr><th colspan="2">Visible</th><th colspan="2">Thermal</th></tr>
<tr><th>Create / Modify</th><th>Labels</th><th>Create / Modify</th><th>Labels</th></tr>
<tr><td>Visible</td><td>Visible</td><td rowspan="2">Yes</td><td>Yes</td><td colspan="2">N/A</td></tr>
<tr><td>Thermal</td><td>Visible</td><td>No</td><td>No</td><td>Yes</td></tr>
<tr><td>Thermal</td><td>Thermal</td><td colspan="2">N/A</td><td rowspan="2">Yes</td><td>Yes</td></tr>
<tr><td>Visible</td><td>Thermal</td><td>No</td><td>Yes</td><td>No</td></tr>
</table>

When the analytics overlay is enabled for the Video Analytics page live video, tripwires and analytics regions are labeled according to analytics region type, T = Tripwire or A = Area (intrusion / loitering); unique region ID number; and video image type, T = thermal or V = visible. For example, T1-T = Tripwire 1 on the thermal video and A3-V = Area 3 on the visible video.

To create a region:

1. Select either the Visible or the Thermal tab.
2. Under Add Region, click the appropriate icon to create a tripwire; an intrusion or loitering detection area; or a masking region.

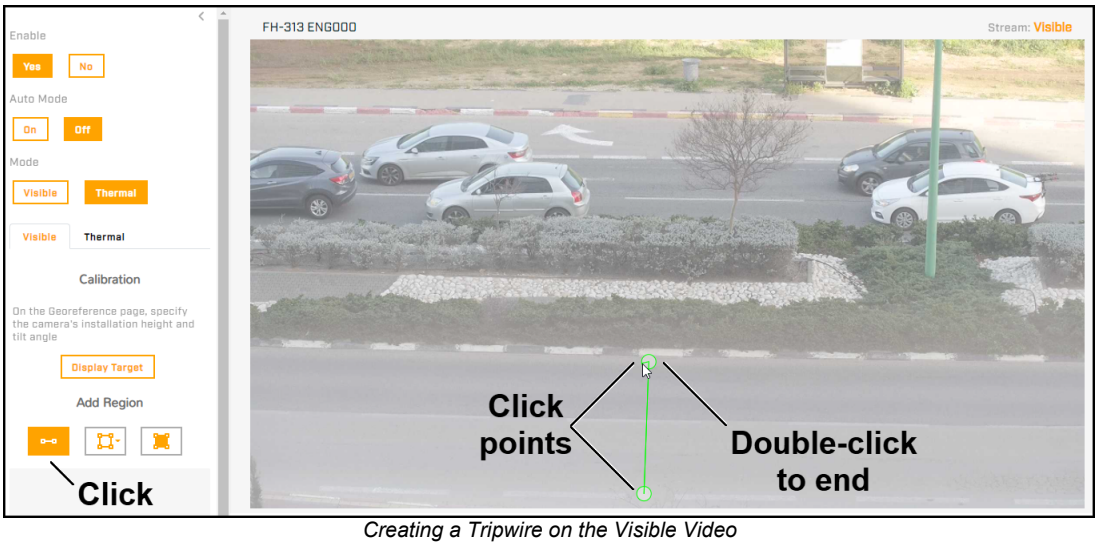


3. Specify each point of the region by clicking and releasing on the live video image. Do not click and drag. Also, do not draw one region line or border over another.

   For both the visible and thermal video, you can create up to two loitering detection areas and up to eight tripwires or intrusion detection areas. For each region, the maximum number of points is 16.

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

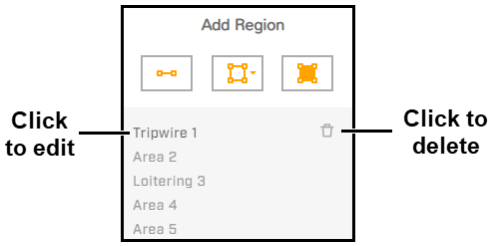
This document does not contain any export-controlled information.



Creating a Tripwire on the Visible Video

Tips

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



Masking regions—The region of the video image that does not generate alarms. For example, to eliminate alarms from trees or bushes moving in the wind. You can create a total of two masking regions for both the visible and thermal video; that is, you can create one masking region for each or two for either the visible or the thermal video.

Note

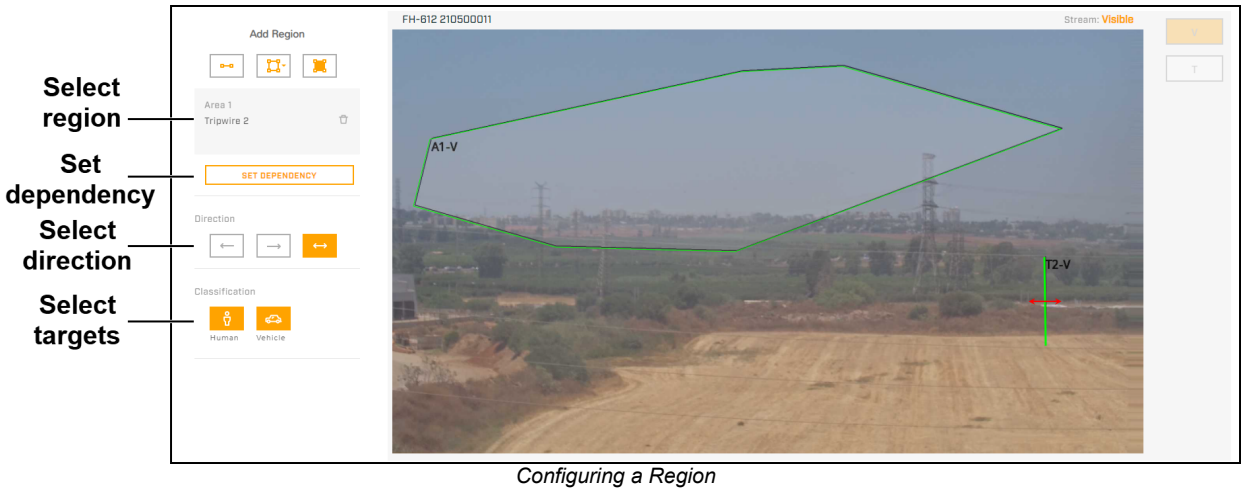
The camera provides intrusion detection masking, not privacy masking. Analytics are disabled for masking regions, and the camera does not generate alarms. However, the region itself appears in the video image.

After creating a region, you can configure the following:

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

For intrusion detection on thermal video, you can select DNN (default; also known as CNN) or Motion.

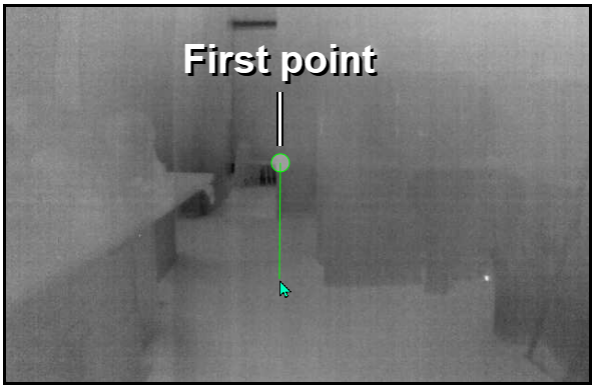
This document does not contain any export-controlled information.



Configuring a Region

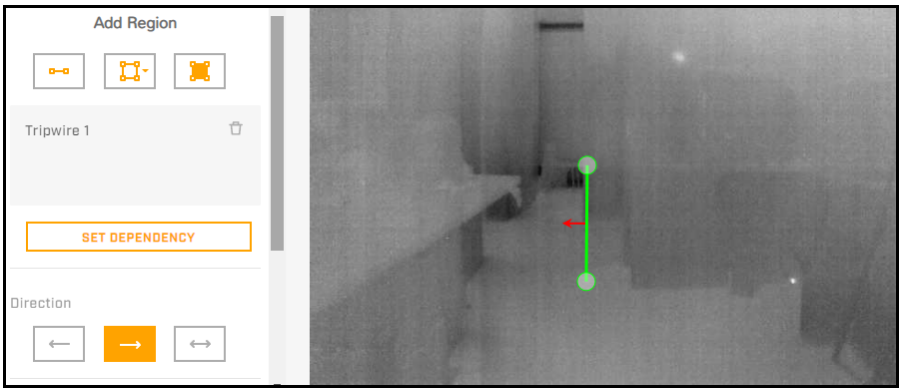
Tripwire Direction

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



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

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



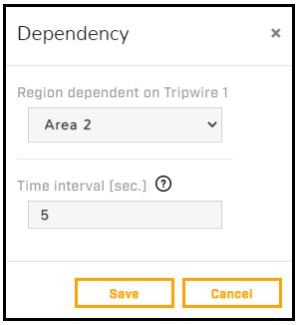
Dependency

After drawing at least two tripwires or detection areas for either the visible or the thermal video images, you can establish dependency between them.

This document does not contain any export-controlled information.

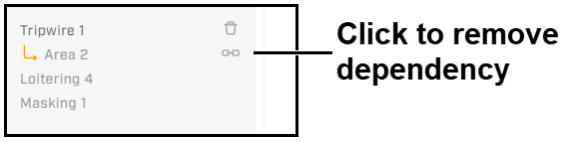
To establish dependency between two regions:

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



To remove a dependency:

Click the link icon corresponding to the dependent region.



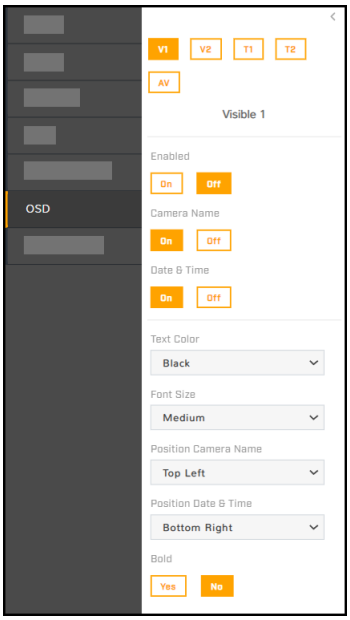
3.11 OSD Page

For each IP video stream (V1, V2, T1, and T2) and for the analog video output (AV), you can:

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

You can also specify:

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



When OSD is enabled for the V1 or T1 stream, the OSD appears in the live video on the camera web page. Enabling OSD on the V2 or T2 stream, or on the analog video, does not affect the live video on the camera web page.

3.12 Geotracking Page

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

You can pair this camera with a FLIR Security PTZ camera that supports geotracking so that the PTZ camera engages geotracks from this camera. For example, you can pair this camera with a:

- Quasar® 4K IR-PTZ camera (CP-6408-x1-I)
- DX-Series camera
- DM-Series camera

For information about how to pair this camera, including how to configure the PTZ camera when it is paired, see Pairing an FH-Series Camera with a FLIR Security PTZ Camera (Optional).

This document does not contain any export-controlled information.

Important

- Before enabling geotracking, make sure that the camera's video analytics are enabled on the Video Analytics Page. However, even though geotracking requires the camera's video analytics to be enabled, geotracking configuration is separate from the video analytics configuration. Configure geotracking alarm regions (area or tripwire) and exclusion regions separately from video analytics tripwires, intrusion / loitering regions, and masking regions.
- You can specify a video analytics tripwire or intrusion / loitering region as the trigger for a camera alarm. However, you cannot specify a geotracking alarm region as the trigger for a camera alarm. On the other hand, when an FH-Series camera is paired with a supported FLIR Security PTZ camera, you can specify an FH-Series camera's geotracking alarm region as the trigger for a PTZ camera alarm.

Detected Objects Tracked (Map Not Uploaded)

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

Icons and Descriptions			
	Fixed camera—a circle around this icon indicates the FH-Series camera you are currently configuring		Geotracking alarm region
	PTZ camera		Geotracking exclusion region
	Radar		Detected object
	Geotracking detection range of circled camera		Detected object in alarm region
	Visible camera detection range of circled camera		Object engaged by PTZ camera
	Thermal camera detection range of circled camera		

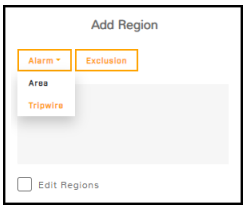
When a map has been uploaded and calibrated on the Map Page and the camera's georeference settings have been properly configured on the Georeference Page, the map appears in the display.

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

This document does not contain any export-controlled information.

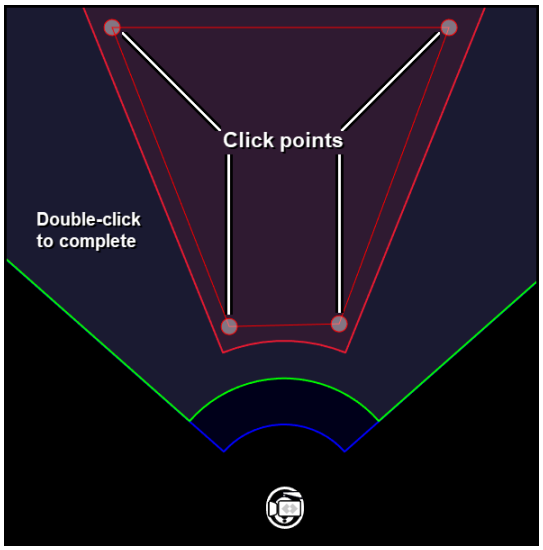
To add a geotracking region:

1. Click one of the Add Region options.



   Alarm (Areas or Tripwires)—Regions where the camera generates geotracking alarms. In the detection area display, the borders of these regions and detected objects appear in red. When an FH-Series camera is paired with a supported FLIR Security PTZ camera, you can specify whether the PTZ camera only tracks these alarms.

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



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

   To cancel creating a region, press **Esc**.

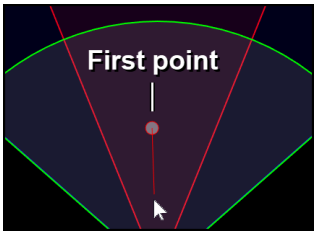
4. To define another region, repeat steps 1-4.

Managing Regions

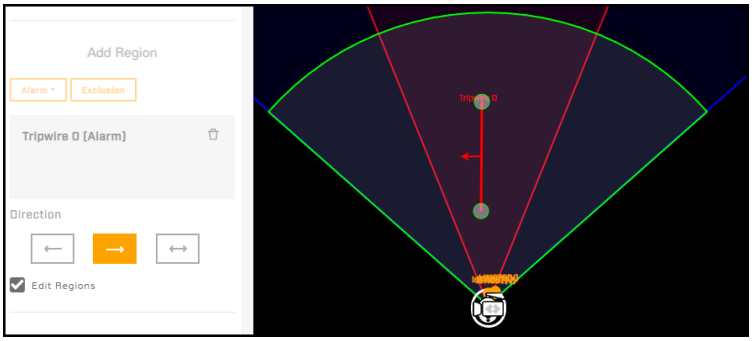
To edit an existing region, select **Edit Regions**, and click the region. You can:

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

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



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



This document does not contain any export-controlled information.

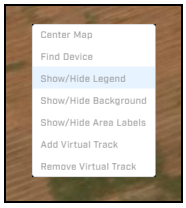
When Edit Regions is selected, it is not possible to add regions.

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

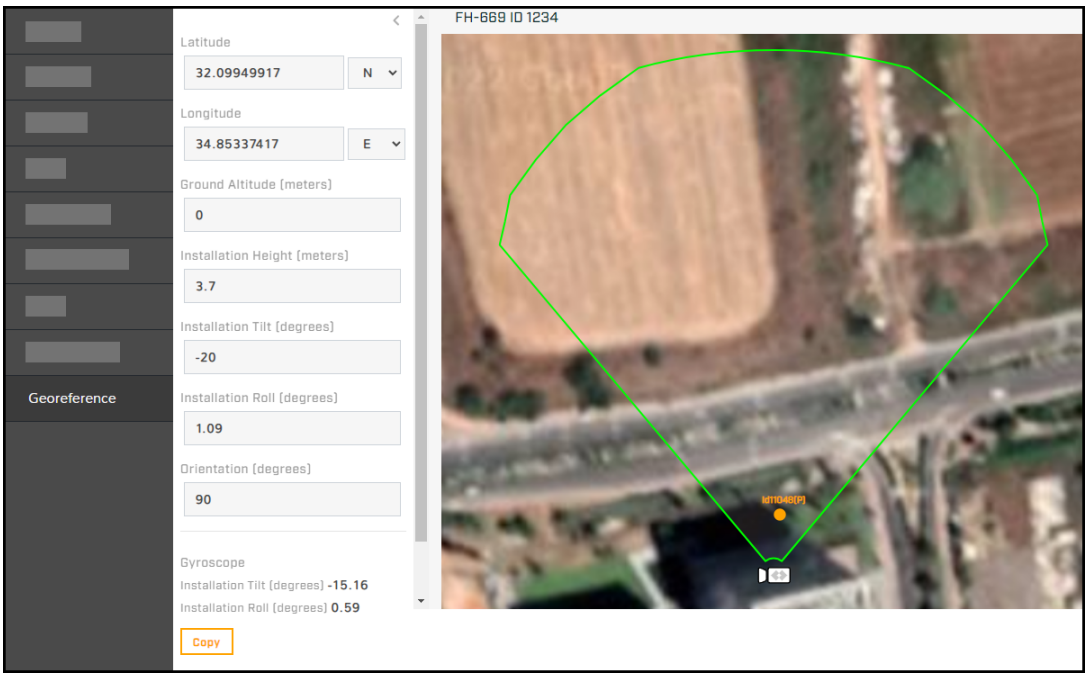
Tips

- To move the display, and to zoom in and out, you can use the mouse. To move the display, click on the display, hold, and drag. To zoom in or out, use the mouse scroll wheel.
- Right-click on the display to:
  - **Center Map—**If uploaded and calibrated, centers the map in the display.
  - **Find Device—**Centers the camera in the display. When the camera does not appear in the display window, select **Find Device**. For example, after you save the camera's coordinates or calibrate a map, the camera's position can be outside the display window.
  - **Show/Hide Legend—**Toggles the display legend.
  - **Show/Hide Background—**Toggles the map or other background image.
  - **Add/Remove Virtual Track—**Toggles a virtual geotrack that you can use to test features such as PTZ pairing and geotracking.

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



3.13 Georeference Page



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

Pairing this camera with a FLIR Security device that supports geotracking requires proper and accurate georeference configuration.

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

Retrieve the camera’s latitude and longitude coordinates by:

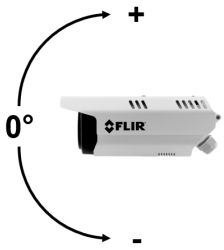
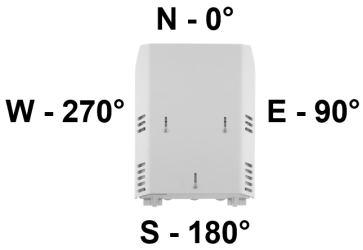
- Right-clicking on the display and then selecting **Georeference Sensor**.

- Manually specifying the coordinates, up to eight decimal places. To obtain the camera's latitude and longitude, you can use a map or a mobile GPS device.

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

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

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

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

Tips

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

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

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

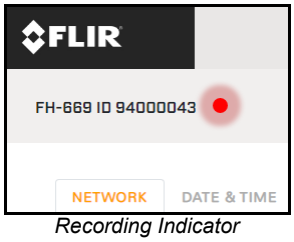
This document does not contain any export-controlled information.

4 Configuration

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

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

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



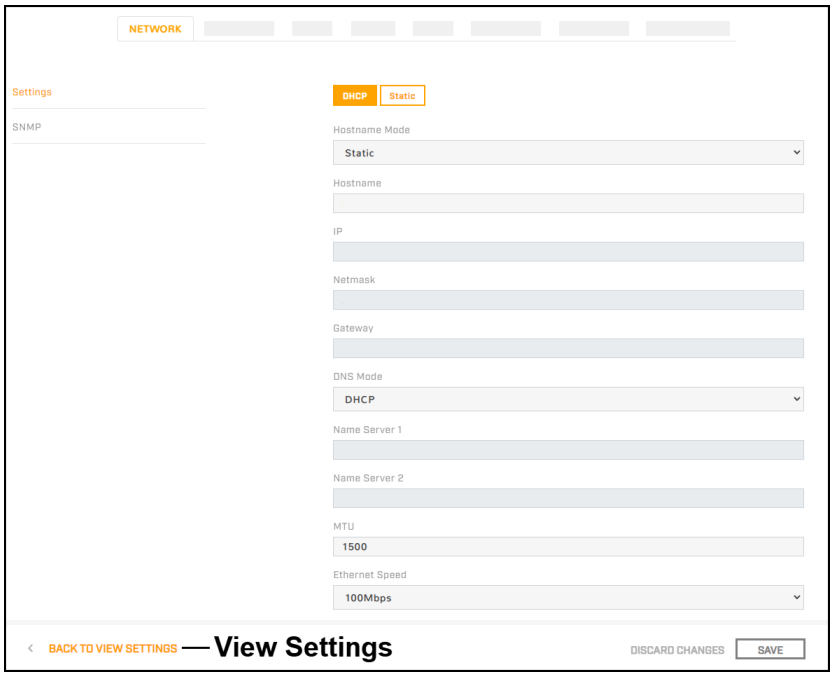
Recording Indicator

In addition, FH-Series cameras can hand-off detection events to a supported PTZ camera using an ioi PTZ Tracker (trk-101-P). For information about how to configure the PTZ Tracker for this hand-off, see Configuring ioi PTZ Tracker Hand-Off.

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

4.1 Network Page

The Network page provides networking and SNMP settings.



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

This document does not contain any export-controlled information.

4.1.1 Settings

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

In Static IP addressing mode, specify:

- **IP**—The camera's IP address.

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

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

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

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

  When the DNS Mode is set to Static, specify:

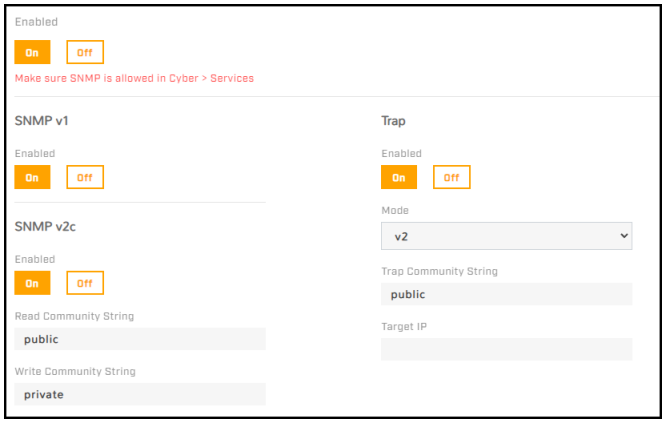
  - **Name Server 1**—The primary domain name server that translates host names into IP addresses.
  - **Name Server 2**—A secondary domain name server that backs up the primary DNS.

You can also specify the:

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

4.1.2 SNMP

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



This document does not contain any export-controlled information.

Important

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

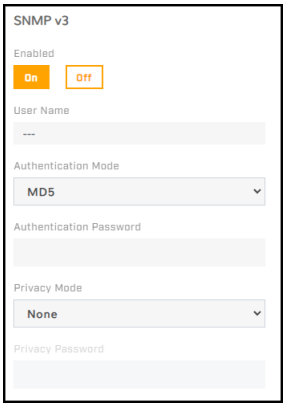
SNMP v1—Enable SNMP v1.

SNMP v2c

After enabling SNMP v2, specify:

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

SNMP v3



SNMP v3 provides security features including:

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

After enabling SNMP v3, specify:

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

Trap

The camera uses traps to send messages to the network management system for important events or status changes.

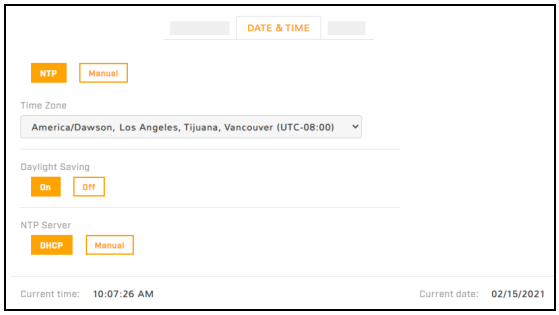
After enabling traps, specify:

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

This document does not contain any export-controlled information.

4.2 Date & Time Page

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

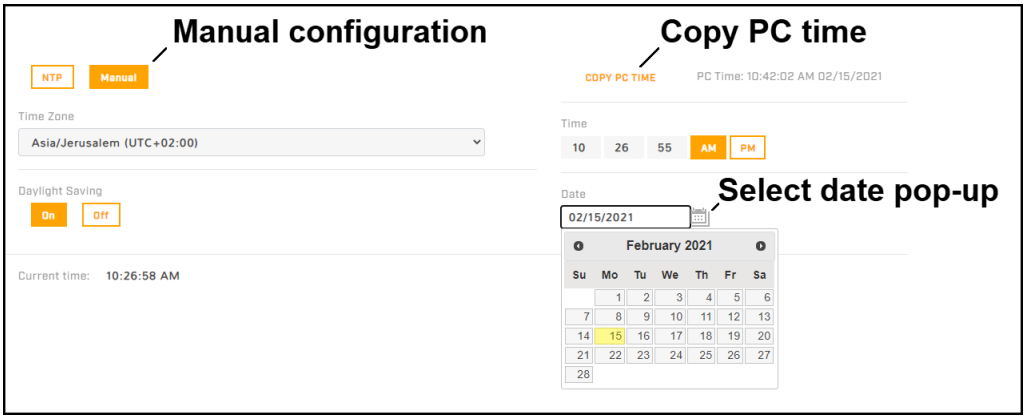


When DHCP IP addressing is enabled on the Settings, you can configure the camera to obtain the NTP server information from the DHCP server.

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

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

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



Tip

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

4.3 Users Page

Only users assigned the admin role can add users and change or set all passwords.

This document does not contain any export-controlled information.

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

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

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

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

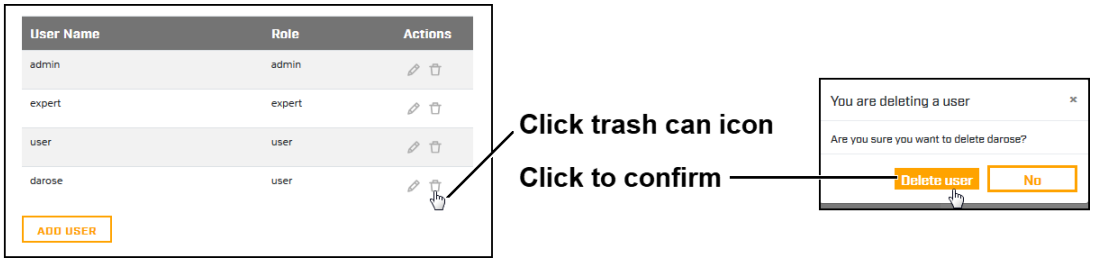
Role	user	expert	admin
Access	Can: • View live video • Switch between visible and thermal live video • View the Help page • Log out	Can access and use all View Settings and System Settings pages, menus, controls, and settings, except the Users page.	Can access and use all of the camera's web pages, including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

Add User

Edit User

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

Delete User



4.4 Alarm Page

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

- The camera's onboard video analytics
- The camera's radiometry (R models)

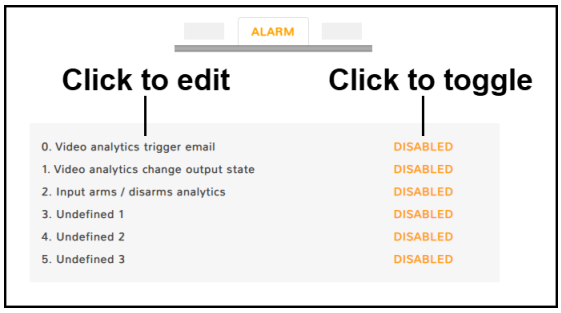
This document does not contain any export-controlled information.

- Video analytics from a supported remote camera or other device
- Radiometry from a supported remote camera or other device
- A supported geotracking device; for example, a radar
- Local or external I/O connections

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

- Record a snapshot image of live video
- Send a notification email
- Arm/disarm the camera's video analytics (available when Video Analytics are not the rule's trigger)
- Change the state of local or external I/O connections
- Enable/disable the camera's radiometry (R models; available when Radiometry is not the rule's trigger)

By default, the following rules are defined and disabled:



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

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

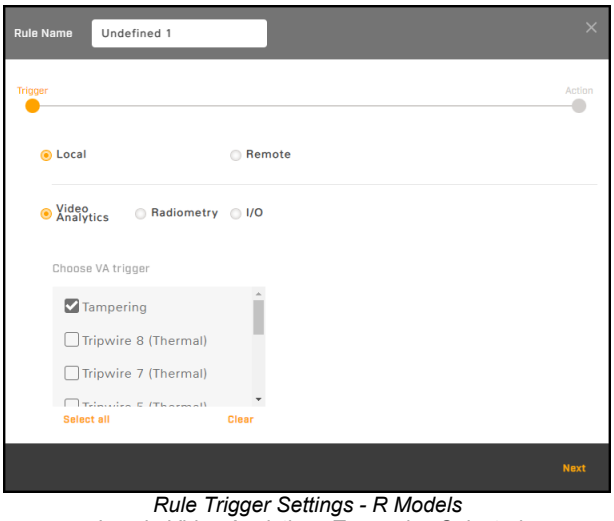
You can also define and enable three additional rules (**3. Undefined 1**, **4. Undefined 2**, and **5. Undefined 3**).

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

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

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

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



Rule Trigger Settings - R Models
Local - Video Analytics - Tampering Selected

This document does not contain any export-controlled information.

4.4.1 Modifying or Defining Rule Triggers

To modify or define alarm rule triggers:

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

Local Triggers		
Video Analytics	This FH-Series camera's onboard video analytics trigger this rule's action.	a. On the Video Analytics Page, make sure tripwires and intrusion detection / loitering regions have been defined. b. Select the tripwires and regions that trigger this rule's action. You 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.
Radiometry (R models)	This camera's radiometry triggers this rule's action.	a. On the Radiometry Page (R models), make sure at least one measurement item has been defined. b. Select one or more measurement items that trigger this rule's action.
I/O	**Local—**This camera's local I/O connections trigger this rule's action.	a. On the I/O Page, make sure local I/O connectors have been properly configured. b. Select one or more local I/O connections that trigger this rule's action. Keep in mind that, when enabled, the camera’s external illumination setting controls Out2.
	External—This camera's external I/O connections trigger this rule's action.	a. On the I/O Page and on the I/O Devices Page, make sure the external I/O connections and the device managing those connections with the camera have been properly configured. b. Select one or more external I/O connections that trigger this rule's action.

Tip

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

- For Video Analytics triggers, make sure video analytics are enabled.
- For Radiometry triggers, make sure radiometry is enabled, temperature measurement for the trigger is enabled, and that alarms for it are enabled.

Remote Triggers

Under Discovered Devices, select the remote camera, radar, geotracking device, or other device from the drop-down menu of supported devices on the same network as the camera; its IP address and port appear. You can also manually specify the remote device IP address and port, and then click **Refresh** to save it. Clicking **Refresh** also refreshes the drop-down menu of discovered devices. For example, if you just connected the remote device to the same network as the camera.

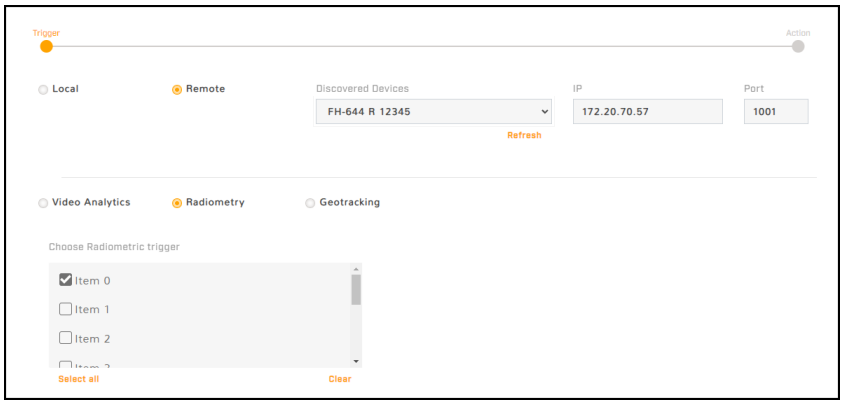
Note

The camera discovers supported devices on the same network as the camera. However, to be used as a trigger, the device must be on the same VLAN as the camera.

This document does not contain any export-controlled information.

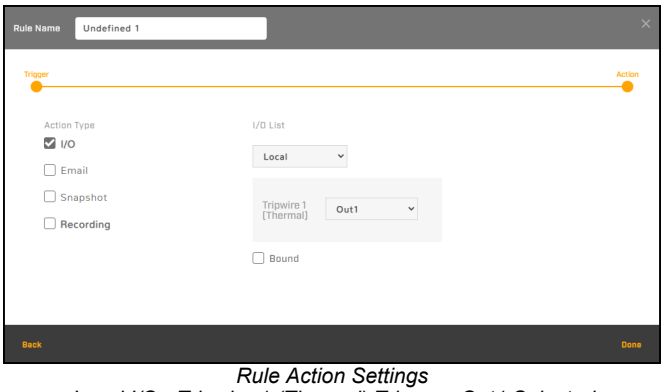
Remote Triggers		
Video Analytics	Video analytics from a supported remote camera or other device triggers an alarm.	a. On the remote camera or other device, make sure video analytics are enabled and that at least one tripwire, intrusion detection / loitering region, or another analytics item has been defined. b. Select one or more video analytics items that trigger this rule's action.
Radiometry	Radiometry from a supported remote camera or other device triggers an alarm.	a. On the remote camera or other device, make sure radiometry is enabled and that at least one radiometric item has been defined. a. Select one or more radiometric items that trigger this rule's action.
Geotracking	A remote geotracking device triggers an alarm.	a. On the remote geotracking device, make sure detection is enabled and that at least one alarm area, tripwire, or other area has been defined. b. Select one or more geotracking device areas that trigger this rule's action.

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



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

4.4.2 Modifying or Defining Rule Actions



Rule Action Settings
Local I/O - Tripwire 1 (Thermal) Trigger - Out1 Selected

To modify or define alarm rule actions:

1. For the alarm rule you are modifying or defining, select the checkbox for one or more action type.

This document does not contain any export-controlled information.

2. To configure an action type, click the selected action type. The selected action type appears in **bold**, and the relevant settings appear.

Action Type	
I/O	Under I/O List, select Local or External.
	Local—This rule changes the state of one or more local output pins. a. On the I/O Page, make sure local I/O connectors have been properly configured. b. For each trigger defined for the alarm rule, select the local output pin that changes. Keep in mind that, when external illumination is installed and enabled, the Illumination setting controls Out2.
	External—This rule changes the state of one or more local output pins. a. On the I/O Page and on the I/O Devices Page pages, make sure the external I/O connections and the device managing those connections with the camera have been properly configured. b. For every trigger defined for the alarm rule, select the external output pin that changes.
	Tip You can map individual local or remote triggers to specific local or external outputs.
	Bound—When selected, the camera changes the state of the output when the alarm is triggered and when it is cleared. When not selected, the camera changes the state of the output when the alarm is triggered. However, the output state remains changed until it is reset according to the configured Reset Interval or by a command from the network. You can configure the Reset Interval for the local outputs on the I/O Page and for the external outputs on the I/O Devices Page.
Arm/Disarm Analytics (not available when this rule's trigger is Video Analytics)**—**When triggered, this rule toggles the camera's onboard video analytics from enabled to disabled or vice versa.	
Email—When triggered, this rule sends a notification email according to the settings on the Messaging Page. Specify a subject for the email and whether the camera attaches a snapshot to the email. If you select Attach Snapshot, and if a thermal and a visible VA trigger are selected, the camera sends two emails: one with the snapshot from the thermal video and another with the snapshot from the visible video.	
Snapshot—When triggered, this rule records a snapshot image of live video.	
Radiometry (R models; not available when this rule's trigger is Radiometry)**—**When triggered, this rule toggles the camera's radiometry from enabled to disabled or vice versa.	

3. Click **Done**.

4.5 Audio Page

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

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

Audio In

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

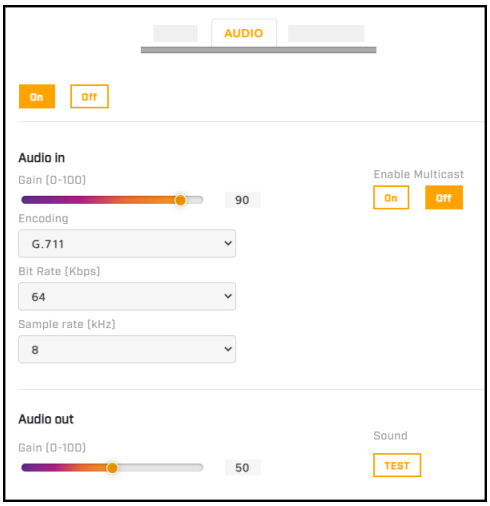
- **Gain**—You can adjust the audio input gain from 0-100 percent. The default is 90 percent.
- **Encoding**—G.711.

This document does not contain any export-controlled information.

- **Bit Rate**—The camera supports an audio input bit rate of 64 kilobits per second (kbps).
- **Sampling Rate**—The camera supports a sample rate of 8 kHz.
- **Enable Multicast**—Can be set to On or Off (default). When On, specify the destination address and port, and the time-to-live (TTL).

Audio Out

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



Tips

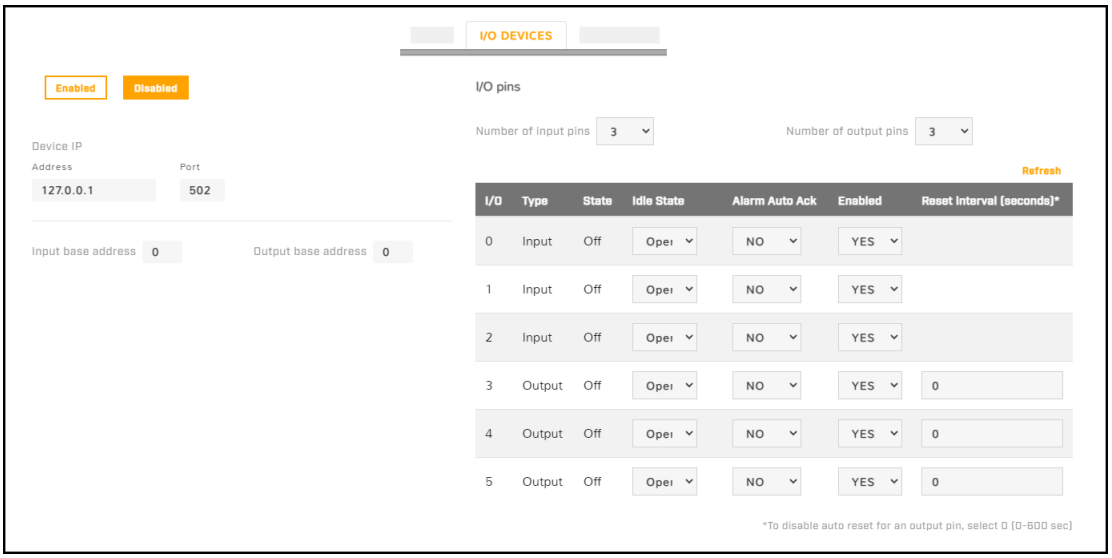
- Test whether the camera's audio output is functioning properly by clicking **Play**.
- If you are monitoring the audio IP output with a video stream and change any of the audio configuration settings except gain, restart the stream. For example, if you are monitoring a video stream and turn audio on,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

4.6 I/O Devices Page

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

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

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



This document does not contain any export-controlled information.

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

- **I/O pin number**
- **Type**—Input or Output
- **State**—the pin's current state: 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

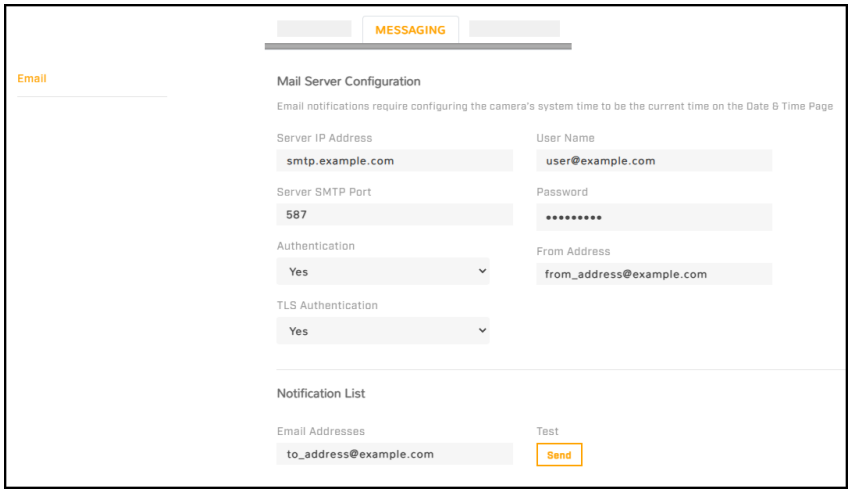
For more information about how to configure the device managing the external I/O connections, refer to the device's documentation.

4.7 Messaging Page

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

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

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



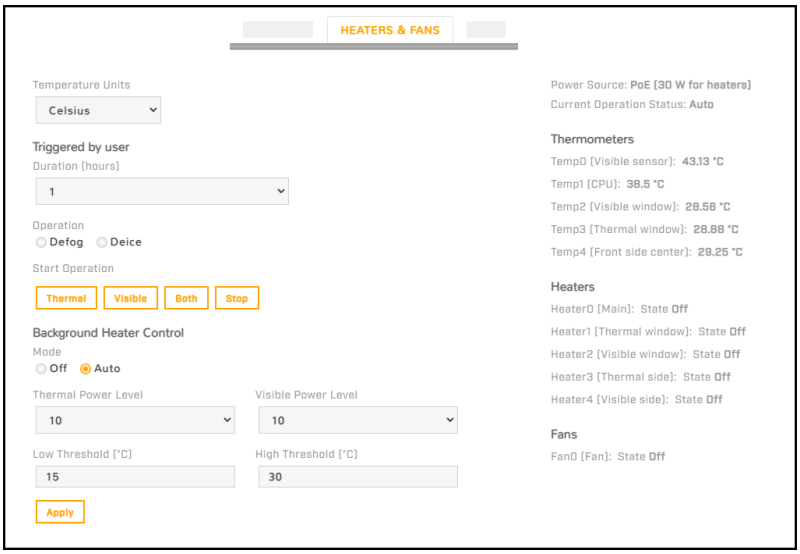
Tip

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

4.8 Heaters & Fans Page

The Heaters & Fans page provides configuration settings for the camera's defogging, deicing, and automatic background heating features; temperature information for camera components; and status information for the camera's onboard heaters and cooling fan.

This document does not contain any export-controlled information.



Select the units of temperature that appear on the page: Celsius, Fahrenheit, or Kelvin. On R models, note that this setting is independent of the Units setting on the Radiometry Page (R models).

To manually activate defogging or deicing on one of the camera's sensors or on both of them:

1. Under Triggered by user, select the Duration (0.5, 1, or 2 hours).
2. Select the Operation.
3. Click **Thermal**, **Visible**, or **Both**. The status of the heater(s) changes from Off to On.

To deactivate the operation, click **Stop**.

Background Heater Control

By default, background heater control is set to Auto. You can specify:

- Thermal and visible sensor heater power levels (0-15). Keep in mind the amount of power available to the heaters.
- Temperatures at which the heaters activate (Low Threshold) and deactivate (High Threshold).

Status Information

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

- **Power Source—**PoE, 12 VDC, 24 VDC, or 24 VAC (the amount of power available to the heaters)
- **Thermometers—**Temperatures for camera components
- **Heaters—**Status of the camera's heaters (On or Off)
- **Fans—**Status of the camera's cooling fan (On or Off)

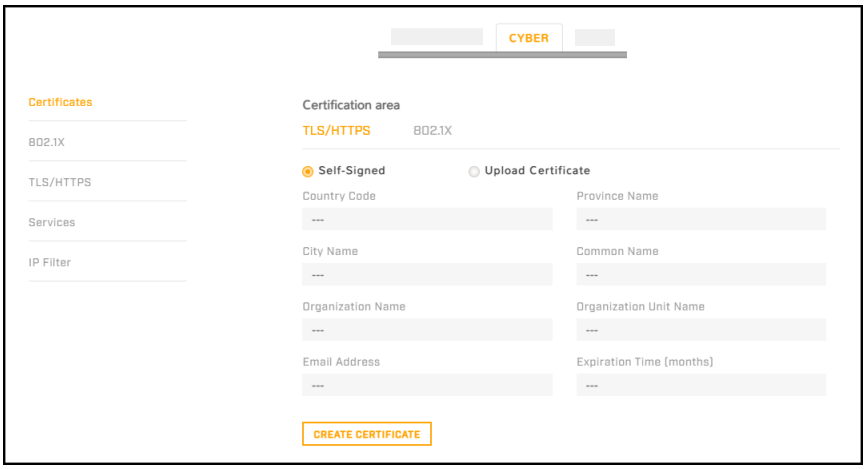
4.9 Cyber Page

The Cyber page provides security configuration settings for:

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

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

4.9.1 Certificates



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

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

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

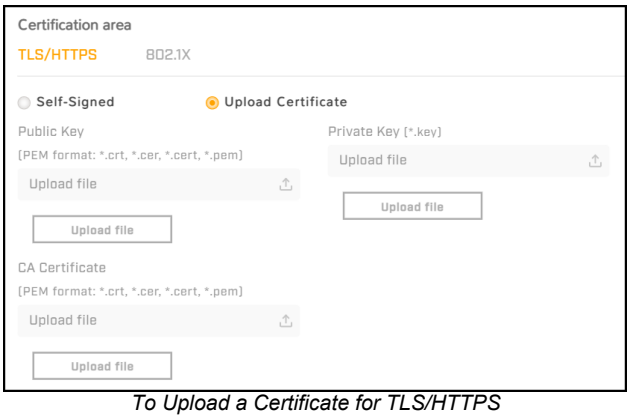
From the Certificates section of the Cyber page, you can download certificates and keys previously uploaded to or generated by the camera. If the certificate saved on the camera is self-signed, you can download the private and public key files. If the certificate was signed by a third-party CA, you can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

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

1. In the Certificates section and Certification area, select **TLS/HTTPS** and **Self-Signed**.
2. Enter information such as country code, city name, and organization name.
3. Click **Create Certificate**.
4. Allow 15 seconds for the camera to generate the certificate, at which point a confirmation appears.

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

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



To Upload a Certificate for TLS/HTTPS

To Upload a Certificate for 802.1X

This document does not contain any export-controlled information.

2. If you are uploading a self-signed certificate, under **Public Key** and then under **Private Key**:
   a. Click Upload file .
   b. Select the appropriate key file.
   c. Click Upload file .

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

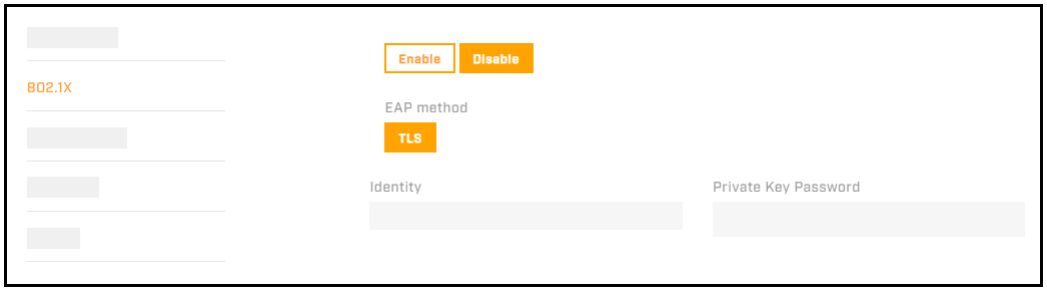
3. Verify that the camera certificate files are valid and make sure *Certificates are OK* appears under the certificate information, under Download certificate.

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

4.9.2 802.1X

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

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



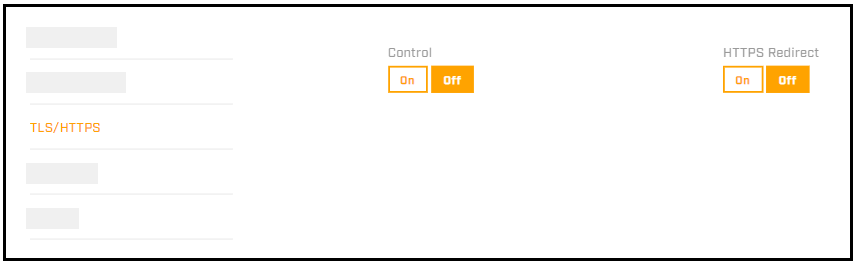
4.9.3 TLS / HTTPS

You can enable or disable:

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

For both, the default is disabled.

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



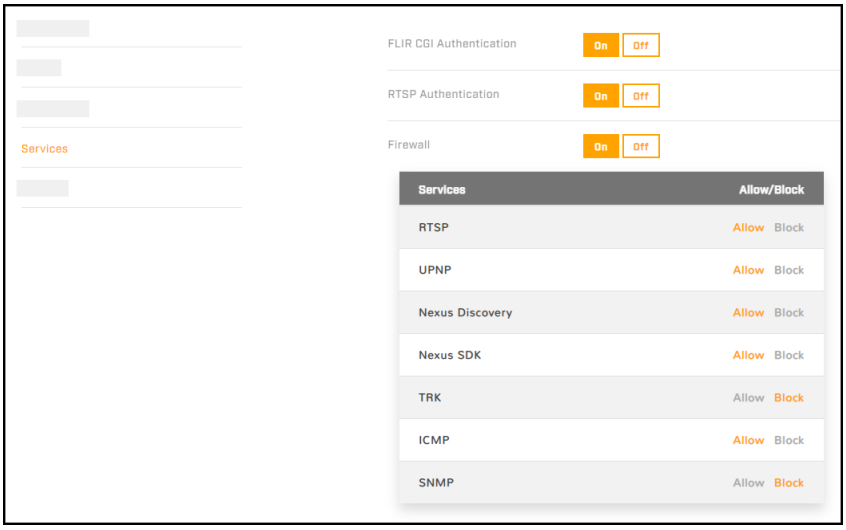
4.9.4 Services

You can enable or disable:

- Digest authentication for the FLIR CGI control interface.

- RTSP authentication. When disabled, accessing the camera's video streams does not require authentication.

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



Firewall Settings

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

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

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

Caution

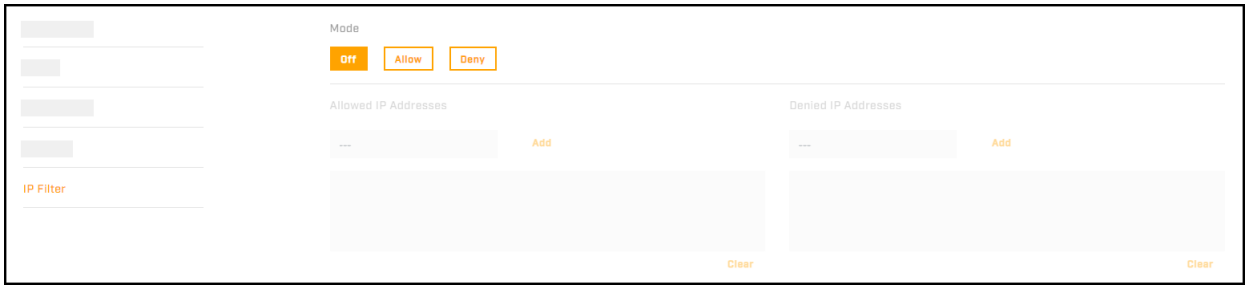
Disabling services and ports can affect product functionality.

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

4.9.5 IP Filter

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

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



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

This document does not contain any export-controlled information.

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

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

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

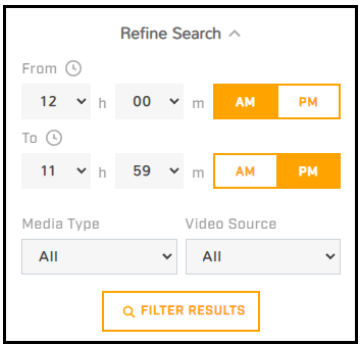
4.10 Media Browser Page

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

Date with Recorded Files Selected - File Selected

You can:

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



When you select a single file, a preview of the file appears.

After selecting one or more files, you can download or delete the file(s).

4.11 ONVIF Page

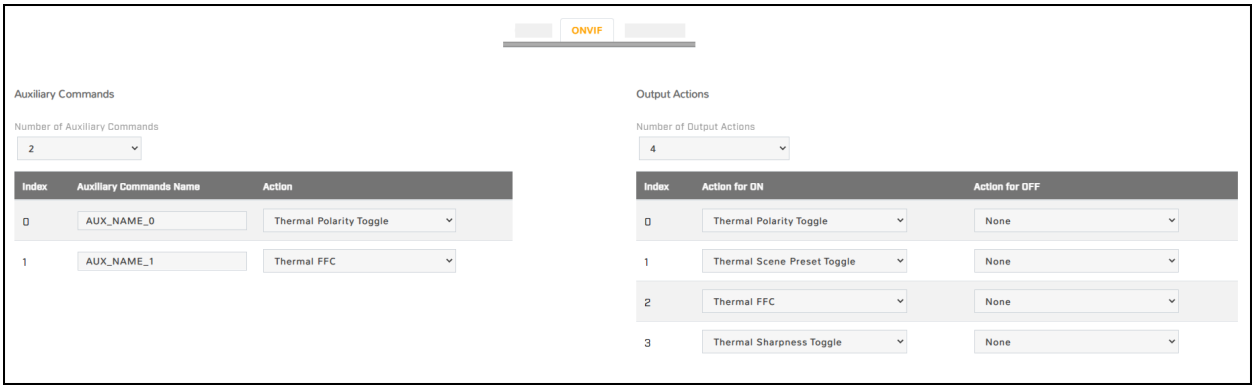
The ONVIF page provides settings for auxiliary commands and for output actions.

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.

This document does not contain any export-controlled information.

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 Page). For example, toggles the colorization from WhiteHot to BlackHot or vice versa; RedHot to RedHotInverse or vice versa; and so on.
   - **Thermal FFC**—Initiates flat-field correction on the thermal sensor.
   - **Thermal Palette Toggle**—Toggles through the thermal video colorization options.



Note

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

4.12 Map Page

On the Map page, you can upload and calibrate a reference map image upon which the camera overlays its detection area on the Geotracking Page.

Map Uploaded and Calibrated

To upload a reference map image and calibrate it:

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

   For example, if you use Google Maps or another online map, you can take a screenshot of a satellite view of the camera's detection range. In Windows 10, you can use the default keyboard shortcut

(Windows logo key + Shift + S) to take the screenshot, paste the screenshot into an image editor (for example, Paint), and then save the image in JPG or PNG format. The size of JPG files are optimized better.

Tips

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

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

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

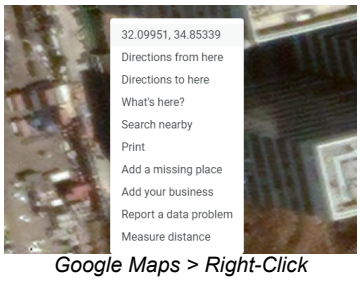
3. Under Map Display, click **Find file**, and then click **Upload**.

   If the map successfully uploads, a confirmation message appears.

4. Click **Accept**.

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

Right-Click on Map



Google Maps > Right-Click

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

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

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

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

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

8. Click **Save**.

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

This document does not contain any export-controlled information.

Tip

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

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

4.13 Boresight Page

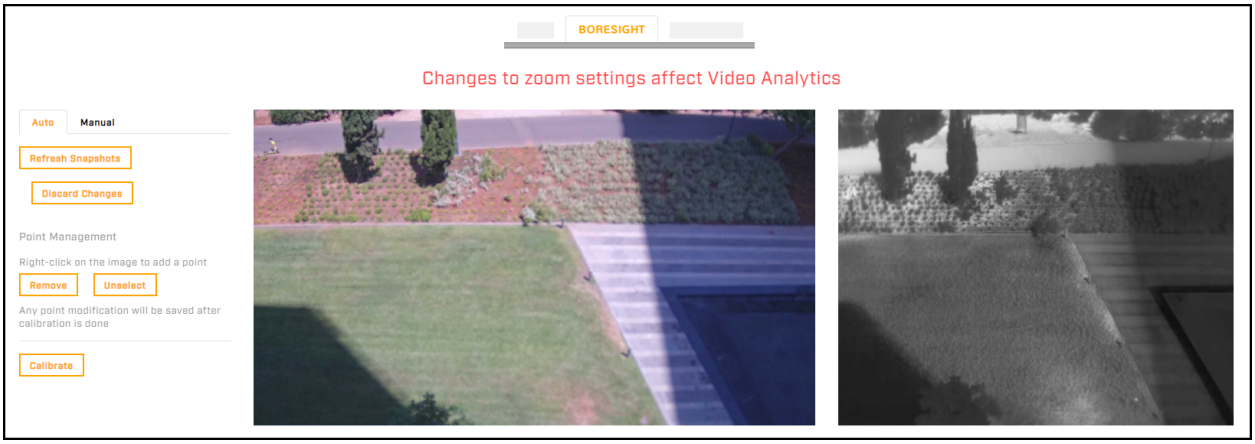
At the factory, the camera's visible video image was aligned with the thermal video image. On the Boresight page, you can fine tune the video image alignment to the scene using the Auto boresight feature or by manually adjusting it.

Caution

When adjusting the camera's boresight, exercise extreme caution.

Tips

- A minor image misalignment is normal. Fine-tuning the boresight settings enables drawing the analytics regions on thermal and visible images when analytics is enabled on only one of the image sources.
- With the lenses physically separated, even slightly, the most accurate alignment is at a specific distance from the camera. The alignment shifts slightly for objects closer or further away from that distance. When making the fine-tuning boresight adjustments, align the images on objects that are the same distance from the camera.
- On the Firmware & Info Page, resetting the camera to its factory settings resets the factory boresight settings. On the Firmware & Info Page, you can back up and restore the camera's configuration settings, including the customized boresight settings.



Before you boresight the camera, make sure video analytics and electronic image stabilization (EIS) are disabled.

To use Auto boresight:

1. Make sure the visible image is focused. Changes to the camera's focus slightly affect the FOV.
2. Select the Auto tab.

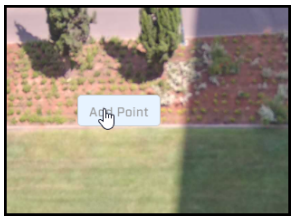
This document does not contain any export-controlled information.

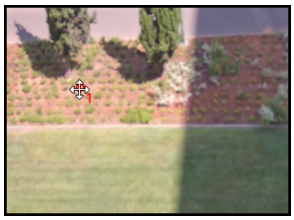
When using the Auto boresght feature, the images on the Boresight page are not live video images; they are snapshots. To monitor Auto boresight changes in real-time, view the live video streams on a FLIR UVMS, client program, or third-party ONVIF system.

3. Hover over a point in one of the images that you want in the field of view. Right-click, and then click **Add Point**.

   The calibration point appears in the image.

4. To move a point, hover over it, click it, and drag it.





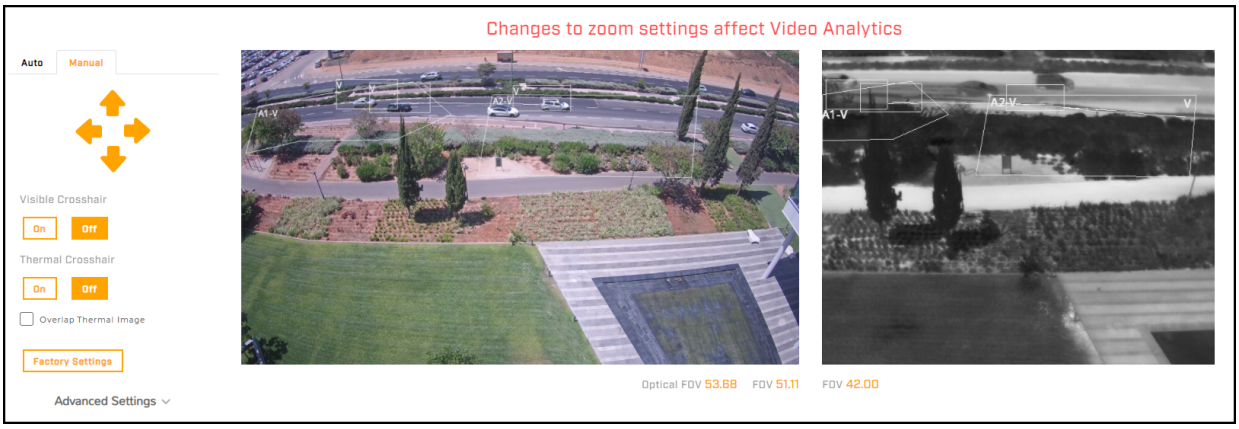
5. Hover over the same point in the other image, right-click, and then click **Add Point**.
6. Add at least two more pairs of calibration points by repeating the previous steps.
7. Click **Calibrate**. The camera aligns the images according to calibrations points by adjusting each imager's zoom, offsets, and so on.

   If the camera detects a significant error in the calibration points, a message appears. Re-configure the calibration points until the camera can align the images.

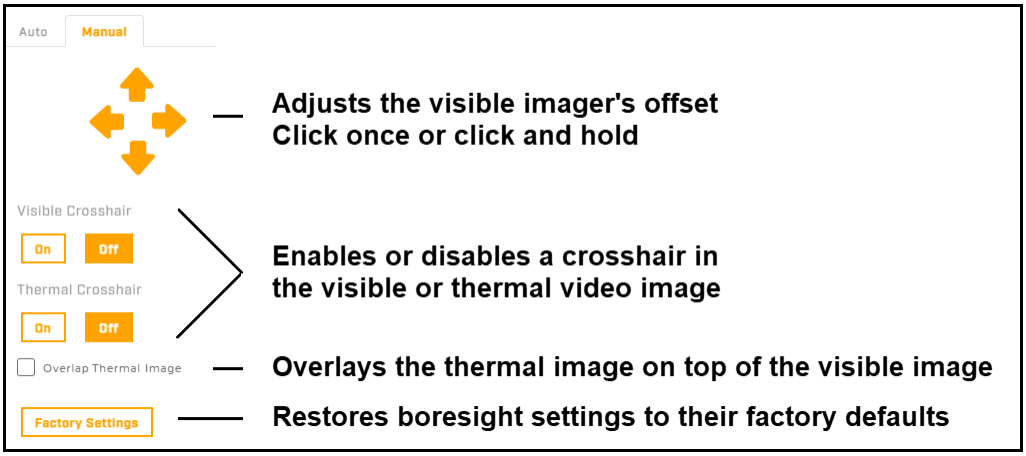
8. Click **Refresh Snapshots** and make sure the Auto boresight corrected the misalignment.

To manually boresight the camera:

1. Select the Manual tab.



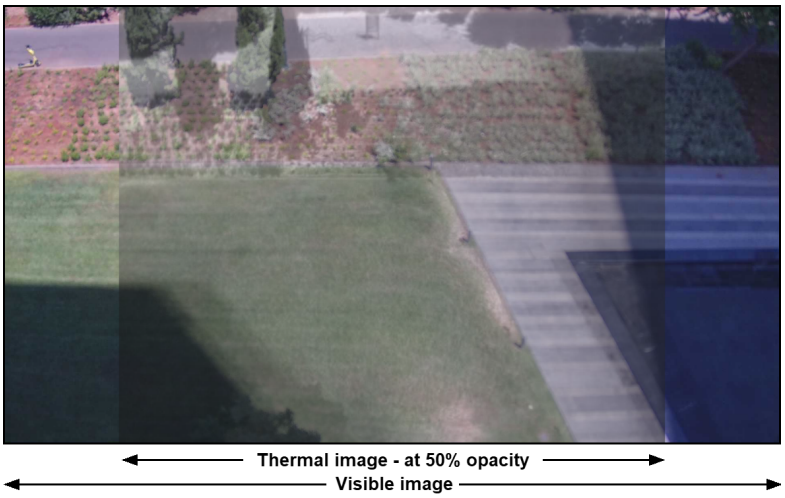
2. Use the controls and advanced settings on the Boresight page to align the visible and thermal video images and their fields of view.



This document does not contain any export-controlled information.

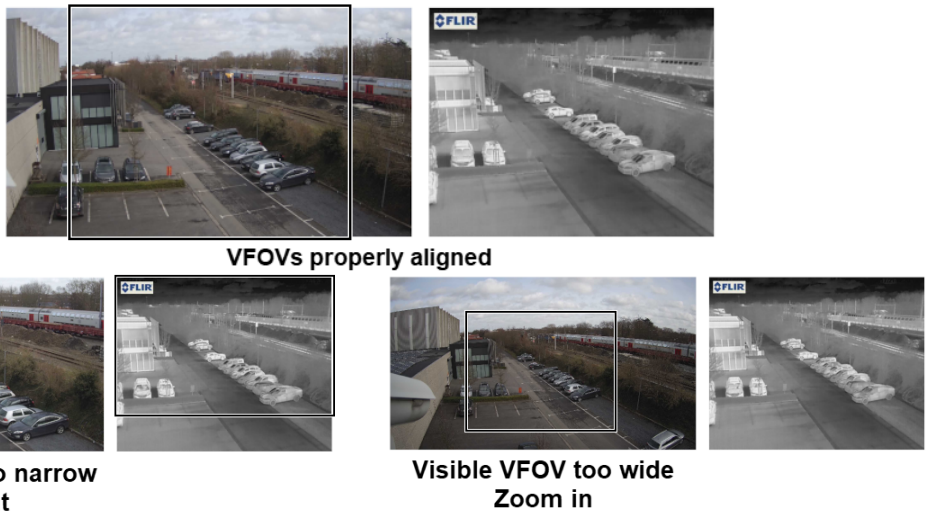
If the digital zoom magnification is 1x, you cannot adjust the visible imager's offset. To be able to adjust the offset, specify a magnification greater than 1x. Increasing the digital zoom increases the offset adjustment range.

If you select **Overlap Thermal Image**, you can specify the opacity of the thermal image over the visible image.



Important

For accurate video analytics, the VFOVs must be properly aligned. Teledyne FLIR recommends setting the vertical FOV of visible image slightly wider than the thermal image vertical FOV of thermal.



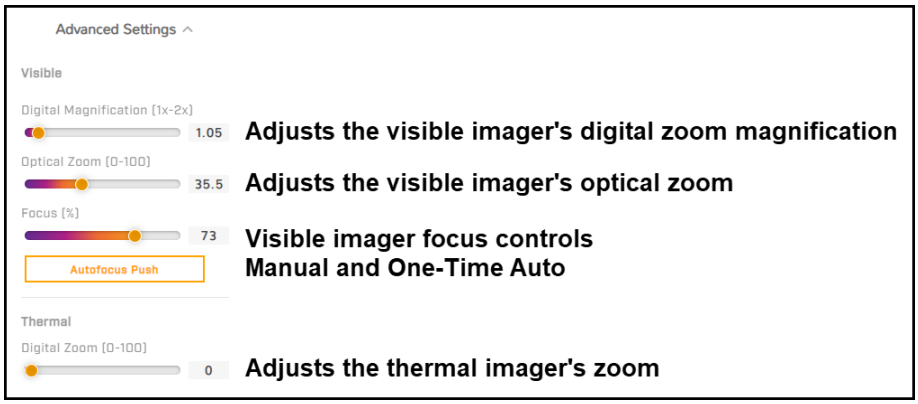
To restore the camera's boresight settings to their factory defaults, click **Factory Settings**.

Caution

After clicking **Factory Settings**, do not click on the camera web page until the camera finishes restore the boresight settings.

This document does not contain any export-controlled information.

Advanced Settings



Important

- Changes to zoom settings affect the camera's video analytics. If you have previously configured the video analytics, after changing the zoom settings, adjust the detection regions accordingly.
- On each FH-Series model, the visible imager lens has a different optical zoom range and default field of view. For information about your model's optical zoom range and default field of view, see Camera Specifications.

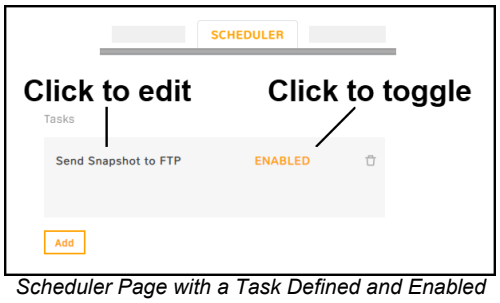
4.14 Scheduler Page

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



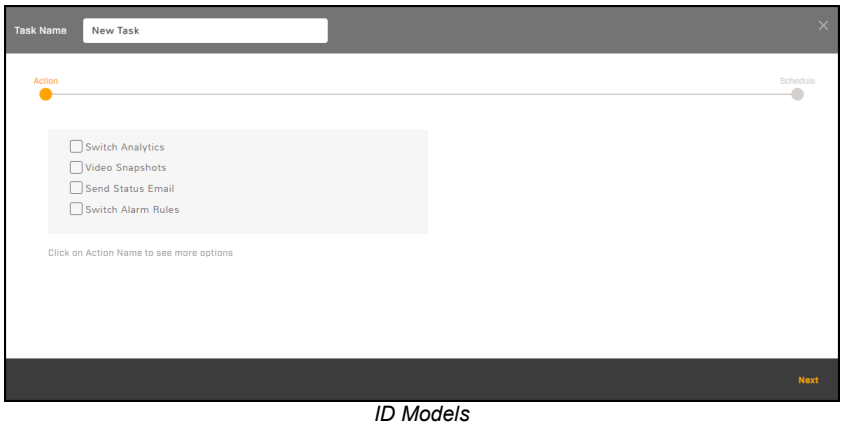
Scheduler Page with a Task Defined and Enabled

By default, no tasks are defined.

To define a task:

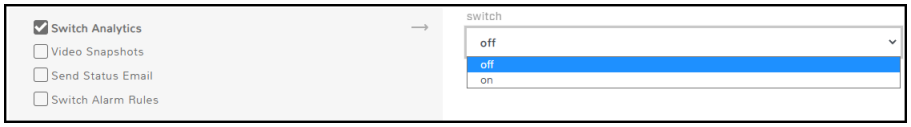
1. Click **Add**. A new task appears. By default, it is enabled.
2. Click **New Task**. The task action settings appear.

This document does not contain any export-controlled information.



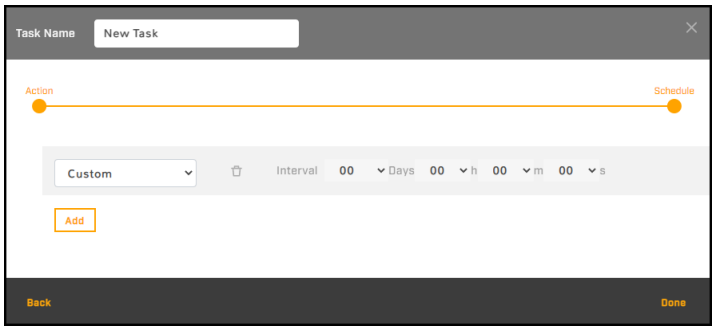
ID Models

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

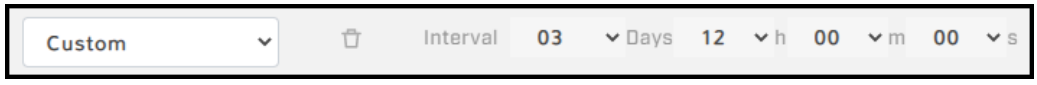
Predefined Actions	
Switch Analytics	Select whether the task disables the camera's onboard video analytics (off) or enables it (on). 
Video Snapshots	Records live video snapshots according to settings configured on the Recording Page, and, if supported, according to settings configured by using FLIR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

This document does not contain any export-controlled information.

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



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

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

Tip

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

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

8. Click **Done**.

Note

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

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

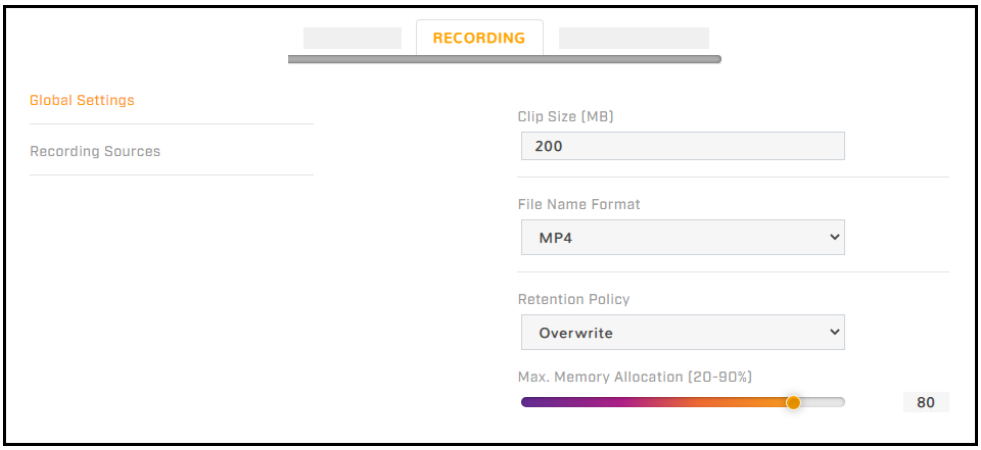
This document does not contain any export-controlled information.

4.15 Recording Page

On the Recording page, you can configure:

- Global video clip recording settings
- Recording sources

Global Settings



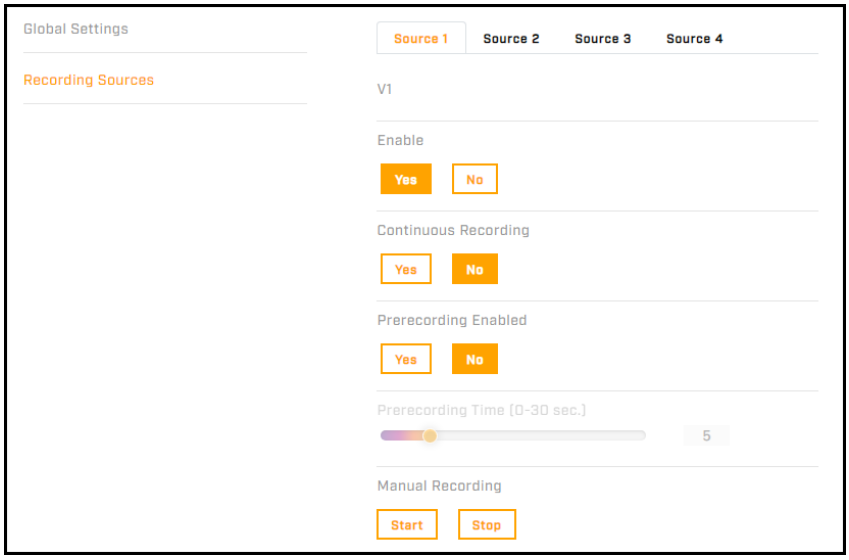
Clip Size—Specify in seconds the maximum allowed recording file size.

File Name Format—MP4.

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

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

Recording Sources



The camera has four recording sources: two visible video streams (V1 and V2) and two thermal video streams (T1 and T2). The camera can record up to two sources / streams at the same time.

This document does not contain any export-controlled information.

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

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

You can also manually start and stop recording the selected source / stream.

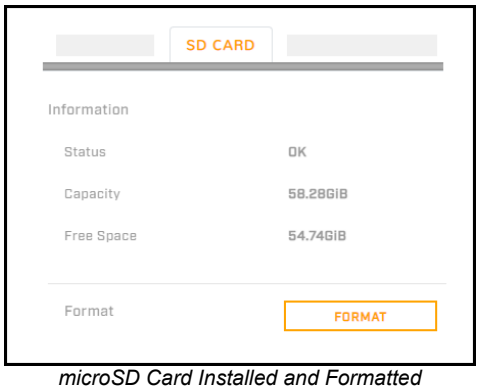
The current source and video stream settings appear to the right of the recording source settings.

Name	Associated Video	Associated Video Settings	Status
Source 1	Visible 1	H.264 3840 x 2160	Recording
Source 2	Visible 2	H.264 1920 x 1080	---
Source 3	Thermal 1	H.264 640 x 512	---
Source 4	Thermal 2	H.264 640 x 512	---

Example: Source 1 - Visible 1 is Currently Recording

4.16 SD Card Page

You can locally record up to 512GB on a Class 10 microSD/microSDHC/microSDXC card (minimum 8GB). For information about accessing the camera's microSD slot and inserting a card, see Connect the Camera.



microSD Card Installed and Formatted

The following information appears on the SD Card page:

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

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

This document does not contain any export-controlled information.

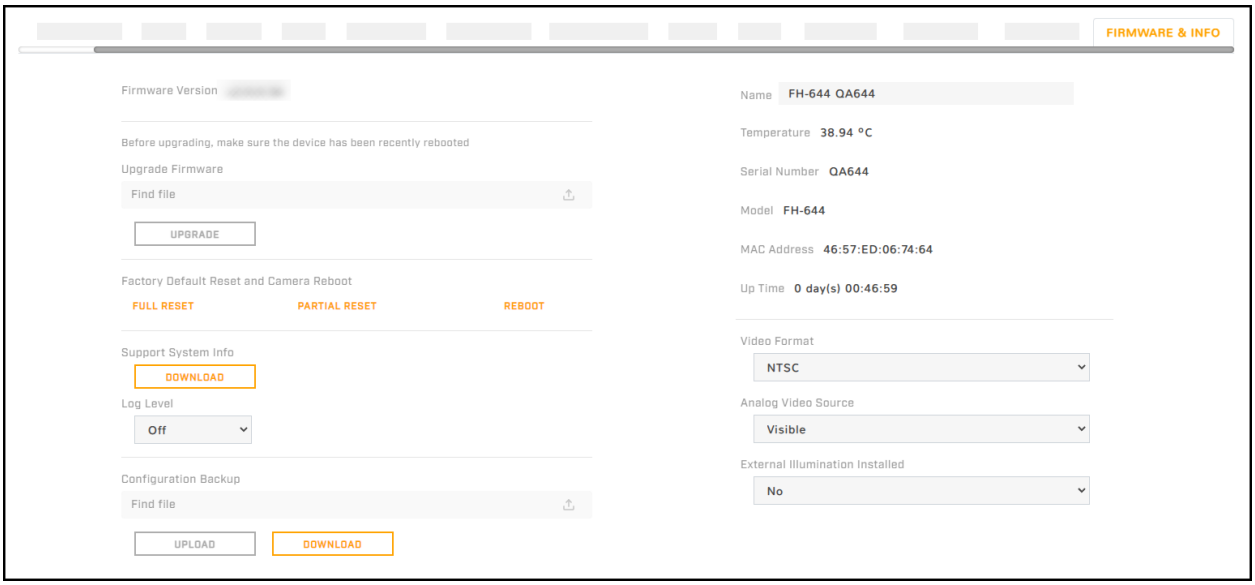
Caution

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

Notes

- Format the microSD card when using it for the first time, or when the card has been used with another camera or other device and transferred to this camera.
- The card must be preformatted as a single partition.

4.17 Firmware & Info Page



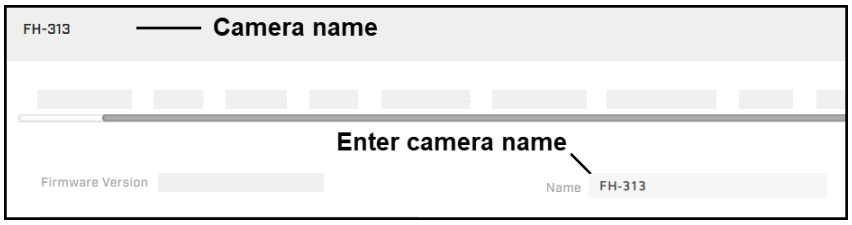
On the Firmware & Info page, you can:

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

Name

Specify a unique, friendly name for the camera, using only alphanumeric characters. The default name for the camera is the camera model followed by the camera’s serial number.

This document does not contain any export-controlled information.



To upgrade the camera's firmware:

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

   Caution

   Only upgrade with firmware developed for FH-Series cameras.

4. Click **Upgrade**.

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

Factory Defaults

Important

Before resetting or rebooting the camera, make sure DV8 - Dynamic Visual Optimization (available on ID models) is disabled on the View Settings Thermal Page.

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

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

Caution

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

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

Tips

- You can also reboot and reset the camera to its factory default settings by pressing the camera's physical Default / Reset button for at least 10 seconds; for example, if you are unable to access the camera via its web page or other communication method. The Default / Reset button is located on the camera's side panel.
- You can restore the camera's factory Boresight page settings on the Boresight Page.

This document does not contain any export-controlled information.

Support System Info

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

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

Configuration Backup

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

To upload a configuration backup file:

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

   Caution

   Make sure to upload a configuration backup file that was downloaded from another FH-Series camera that is the exact same model.

3. Click **Upload**.

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

To download the camera's saved settings:

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

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

Other Settings

Video Format—The visible imager shutter speed can be synchronized to the 50 Hz or 60 Hz power used for lighting the scene. If lighting is connected to 50 Hz power, the PAL setting might provide better video. Under 60 Hz lighting, NTSC might provide better video.

Analog Video Source—Specify the source for the camera's T/V analog video output:

- **None**—Disables the camera's T/V analog video output.
- **Visible**
- **Thermal**

External Illumination Setting—Enables the View Settings Illumination Page, where you can disable and enable automatic external IR illumination.

This document does not contain any export-controlled information.

5 Maintenance and Troubleshooting Tips

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/.

5.1 Cleaning

The camera's housing and lens windows are designed for harsh outdoor environments and the lens windows are coated for durability and anti-reflection. Nonetheless, they can require occasional cleaning.

Caution

- Use great care with your camera's optics. They are delicate and improper cleaning can damage them.
- Do not use abrasive materials, such as paper or scrub brushes, which can scratch and damage the lens windows.
- Only wipe a lens window clean when you can visually see contamination on the surface.

To clean the camera housing and lens windows:

1. Use a compressed air gun to remove dust, dirt, and other contaminants.
2. Check surfaces for any remaining contaminants.
3. If necessary, moisten a clean, soft cotton cloth with alcohol and wipe the surface clean.

5.2 Troubleshooting

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 Visible 1

rtsp://192.168.0.250:554/stream2 for Visible 2

rtsp://192.168.0.250:554/stream3 for Thermal 1

rtsp://192.168.0.250:554/stream4 for Thermal 2

This document does not contain any export-controlled information.

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 Page. Users assigned the role of admin or expert can disable RTSP authentication in the Services section of the Cyber page.

For more information on RTSP settings and stream names, see Video Page.

No IP or Analog Video

If the camera is not producing an image, check the connections at the camera and at the display. If the connections appear to be properly made but the camera still does not produce an image, ensure that power has been properly applied to the camera and the circuit breaker is set properly. 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.

Noisy Image

A noisy image is usually attributed to a cable problem (too long or inferior quality) or the cable is picking up electromagnetic interference (EMI) from another device. Although coax cable has built-in loss, the longer the cable, or the smaller the wire gauge, the more severe the loss becomes. Also, the higher the signal frequency, the more pronounced the loss. Unfortunately, this is one of the most common and unnecessary problems that plagues video systems in general.

A number of factors (core material, dielectric material, and shield construction, among others) determine cable characteristics. Carefully match cable to the specific application. Moreover, the physical environment through which the cable is run and the method of installation influences the transmission characteristics of the cable.

Check cable connector terminations. Inferior connections might use multiple adapters, which can cause unacceptable noise. When splitting the signal to multiple monitors, use a high-quality video distribution amplifier.

Thermal 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 of Thermal Imager 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.

Thermal 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.

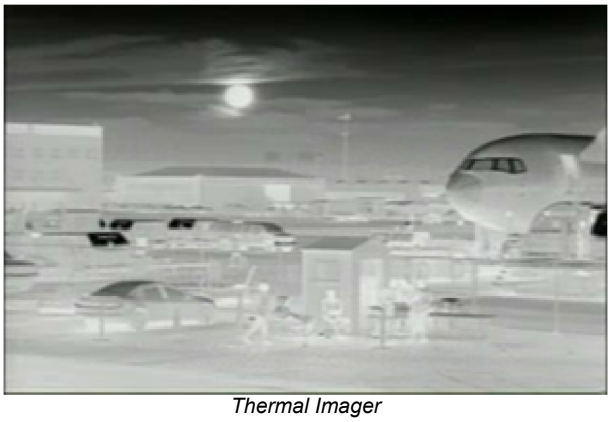
This document does not contain any export-controlled information.

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.

Camera Pointing the Sun

Visible Imager



Thermal Imager

This document does not contain any export-controlled information.

6 Appendix

6.1 Configuring ioi PTZ Tracker Hand-Off

FH-Series cameras can hand-off detection events to a supported PTZ camera using an ioi PTZ Tracker (trk-101-P). Hand-off requires using the PTZ Tracker's web page or FLIR UVMS to bind the FH-Series camera to the PTZ tracker. When the FH-Series camera detects an event, the camera communicates the object's location to the trk-101-P, which then controls and moves the PTZ camera to track and zoom in on the object.

An overview of using the PTZ Tracker's web page to bind the FH-Series camera to the PTZ tracker appears below. For the full procedure, see the *ioi HTML Edition Units User Guide*; you can download it from the product's web page on the Teledyne FLIR website.

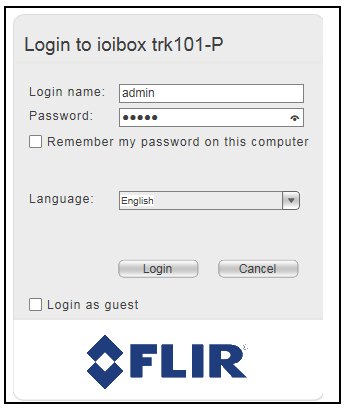
For information about using FLIR UVMS to bind the camera to the PTZ tracker, see the UVMS documentation.

Note

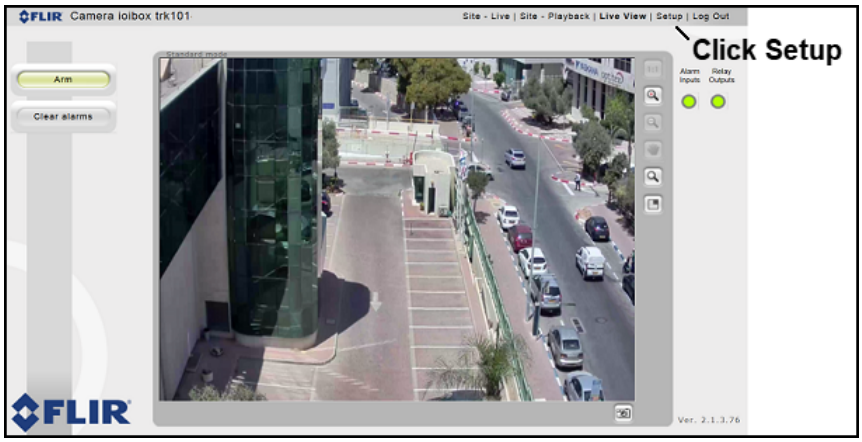
Using an ioi PTZ Tracker (trk-101-P) to hand-off detection events to a supported PTZ camera is separate from the PTZ pairing feature described elsewhere in this guide.

To configure PTZ hand-off using the tracker's web page:

1. Make sure the FH-Series camera's analytics have been calibrated and that analytics regions have been created on the Video Analytics Page.
2. Disable the FH-Series camera's analytics.
3. Log in to the PTZ tracker's web page.

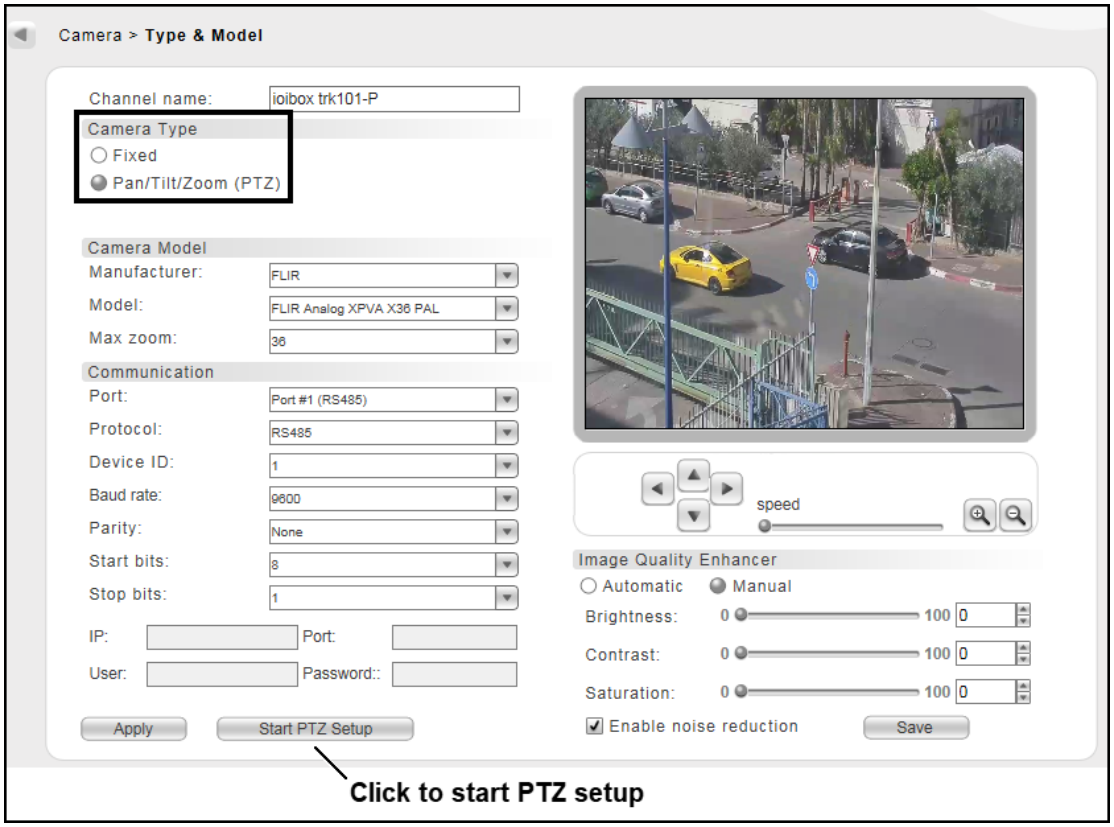


4. On the Live View screen (workspace), click **Setup**.



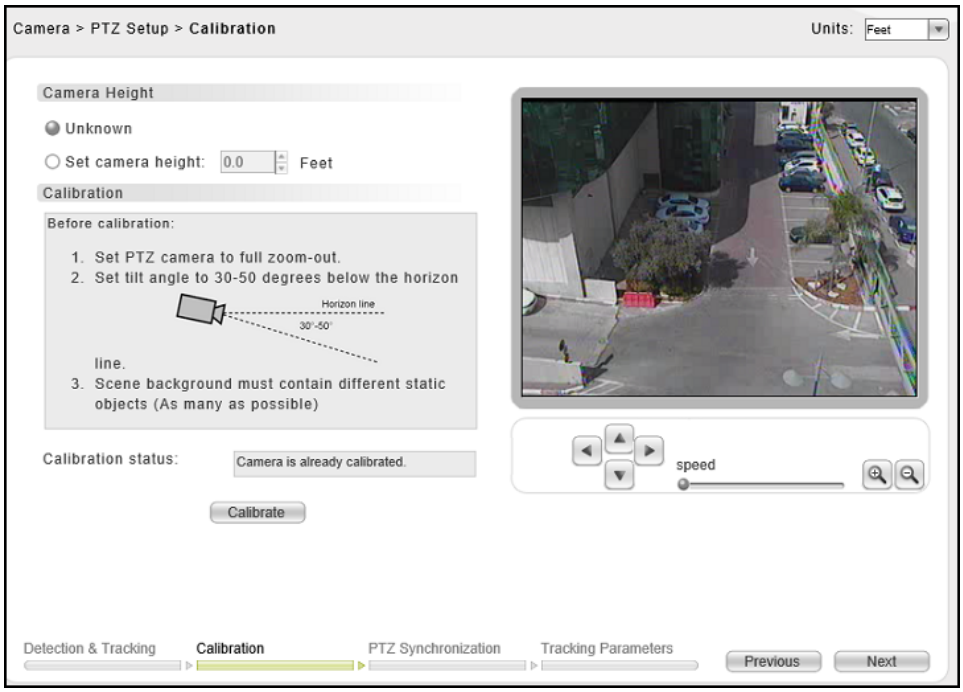
This document does not contain any export-controlled information.

1. On the Camera > Type & Model screen, make sure that the Camera Type selected is Pan/Tilt/Zoom (PTZ).

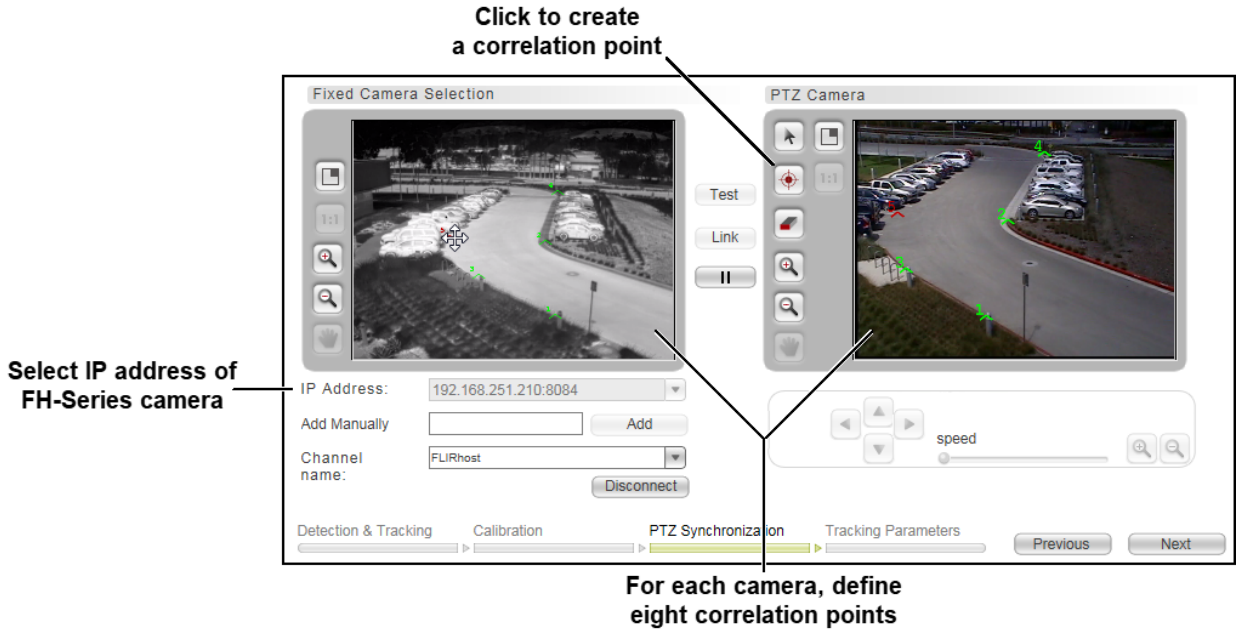


2. Click **Start PTZ Setup**. The Detection and Tracking screen appears.

3. Select Detection from another camera with Automatic PTZ tracking. Click **Next**. The Calibration screen appears.



4. Follow the on-screen instructions. When the PTZ camera has been calibrated, click **Next**. The PTZ Synchronization screen appears.



5. On the PTZ Synchronization screen, perform Step 3: PTZ Synchronization with Fixed Cameras of Using the PTZ Camera Definition Wizard in the *ioi HTML Edition Units User Guide*.

6. For each camera, create eight correlation points.

7. After defining all of the correlation points for both cameras, click **Test**. When the test succeeds, click **Link**.

For more information about defining correlation points, in the *ioi HTML Edition Units User Guide*, see To set correlation points in a preset.

8. Click **Next** and then click **Finish**.
9. Return to Live View and click **Arm**.
10. On the Video Analytics Page, enable the FH-Series camera's analytics.

This document does not contain any export-controlled information.

Americas
27700 SW Parkway Ave.
Wilsonville, OR 97070
USA

6769 Hollister Ave
Goleta, CA 93117
USA

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

Document:
427-0102-00-10
Revision: 130
Date: November 2023

This document does not contain any export-controlled information.