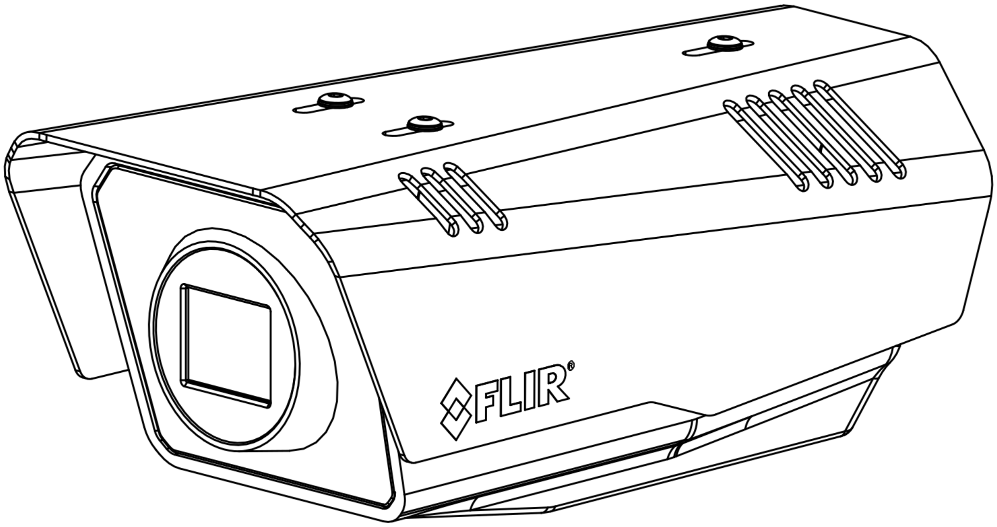
TELEDYNE | Teledyne FLIR
Security Solutions

User Guide

FC-Series AI



FC-Series AI User Guide - Revision 100 - September 2023

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.

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 2023	Initial Teledyne FLIR release

Product Registration and Warranty Information

Register your Product with Teledyne FLIR

Table of Contents

Table of Contents

1 Camera Overview

The FC-Series AI camera provides reliable intruder-detection capabilities for perimeter security. Built-in convolutional / deep neural network (CNN / DNN) analytics accurately detect and classify human and vehicle threats moving at high or low speeds, minimizing false alarms and daily operations costs. R models provide radiometry and can generate alarms determined by detected surface temperature.

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. 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.

This guide describes how to use the FC-Series AI web page to operate and configure the camera. For information about mounting and connecting the camera, including its dimensions and other specifications, see the *FC-Series AI Installation Guide*, which is available from the product page on the Teledyne FLIR website.

Related Documentation

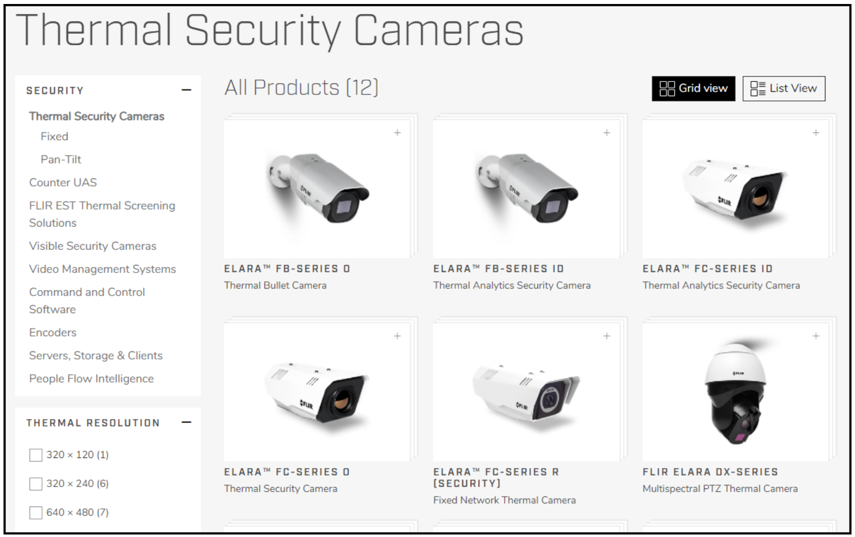
- *FC-Series AI Quick Connect Guide*
- *FLIR Security Edge Devices Accessory Guide*
- *FLIR CGI Interface Description 2.1*
- *NEXUS® CGI WebSockets Manual*
- *FLIR Sensors SDK Programmer's Guide*

2 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 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 h



Thermal Security Cameras

SECURITY –

Thermal Security Cameras

Fixed

Pan-Tilt

Counter UAS

FLIR EST Thermal Screening Solutions

Visible Security Cameras

Video Management Systems

Command and Control Software

Encoders

Servers, Storage & Clients

People Flow Intelligence

THERMAL RESOLUTION –

□ 320 × 120 (1)

□ 320 × 240 (6)

□ 640 × 480 (7)

All Products (12)

Grid view | List View

ELARA™ FB-SERIES O
Thermal Bullet Camera

ELARA™ FB-SERIES ID
Thermal Analytics Security Camera

ELARA™ FC-SERIES ID
Thermal Analytics Security Camera

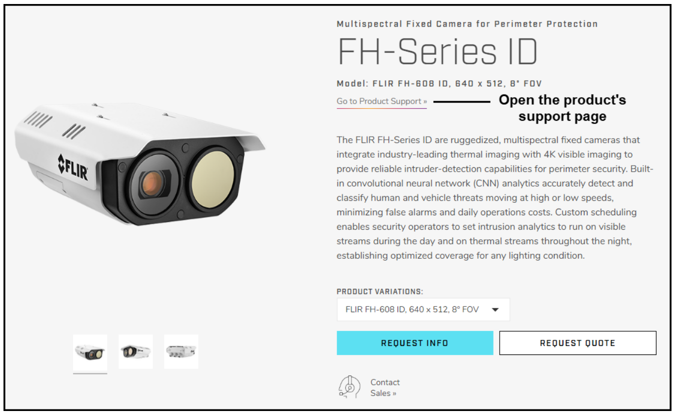
ELARA™ FC-SERIES O
Thermal Security Camera

ELARA™ FC-SERIES R [SECURITY]
Fixed Network Thermal Camera

FLIR ELARA DX-SERIES
Multispectral PTZ Thermal Camera

Thermal Security Cameras Page on the Teledyne FLIR Website

2. Find and click FC-Series AI or FC-Series AI - R. The product details page appears.



Multispectral Fixed Camera for Perimeter Protection

FH-Series ID

Model: FLIR FH-608 ID, 640 x 512, 8° FOV

Go to Product Support » — **Open the product's support page**

The FLIR FH-Series ID 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.

PRODUCT VARIATIONS:

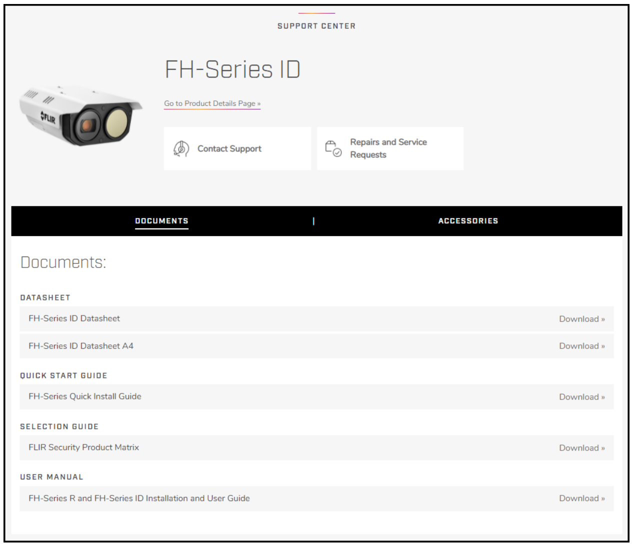
FLIR FH-608 ID, 640 x 512, 8° FOV ▾

REQUEST INFO | REQUEST QUOTE

Contact Sales »

Product Details Page (Example)

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



FH-Series ID

Documents:

DATASHEET

FH-Series ID Datasheet	Download »
FH-Series ID Datasheet A4	Download »

QUICK START GUIDE

FH-Series Quick Install Guide	Download »

SELECTION GUIDE

FLIR Security Product Matrix	Download »

USER MANUAL

FH-Series R and FH-Series ID Installation and User Guide	Download »

Product Support Page (Example)

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.

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.

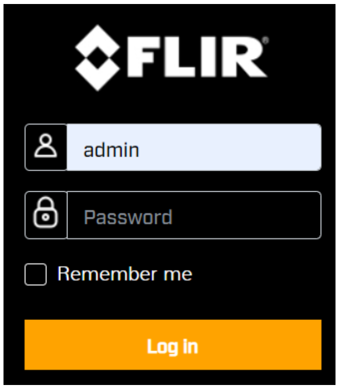
     Download the DNA tool; unzip the file; and then double-click to run the tool (DNA.exe). The Discover List appears, showing compatible devices on the VLAN.
   - ○ Type the camera’s IP address in a browser’s address bar (when the PC and the camera are on the same network). If you do not know the camera's 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.



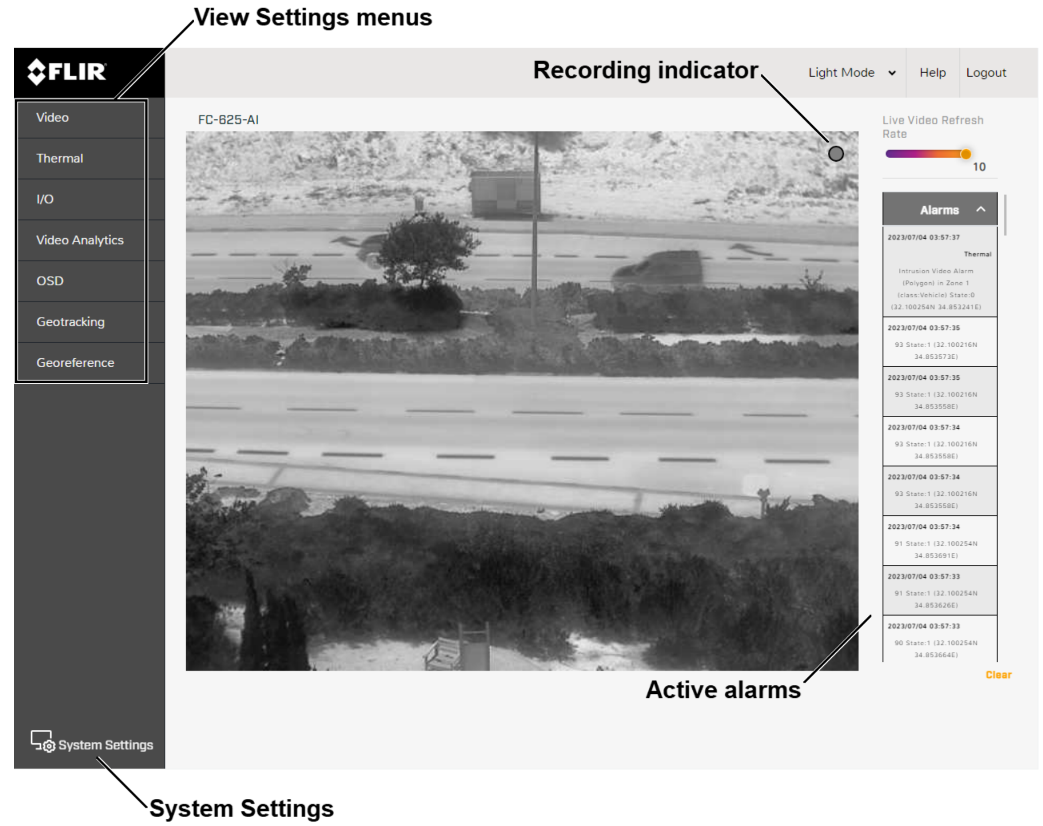
3. When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, specify a new password for the admin user and then log back in using the new password.

   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. 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.



2023/07/04 03:57:37
Thermal
Intrusion Video Alarm (Polygon) in Zone 1 (class:Vehicle) State:0 (32.100254N 34.853241E)

2023/07/04 03:57:35
93 State:1 (32.100216N 34.853573E)

2023/07/04 03:57:35
93 State:1 (32.100216N 34.853558E)

2023/07/04 03:57:34
93 State:1 (32.100216N 34.853558E)

2023/07/04 03:57:34
93 State:1 (32.100216N 34.853558E)

2023/07/04 03:57:34
91 State:1 (32.100254N 34.853691E)

2023/07/04 03:57:33
91 State:1 (32.100254N 34.853626E)

2023/07/04 03:57:33
90 State:1 (32.100254N 34.853664E)

View Settings Home Page (AI Models) - Users Assigned the Admin or Expert Role

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.

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.

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.

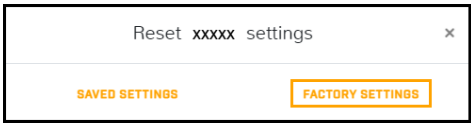
Tip

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 Thermal Page. For others, the camera does not apply changes until you save them.

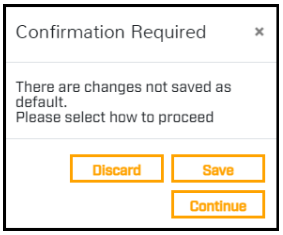
Regardless of whether the camera has already applied changes, to save all changes since the last time these settings were saved, click **Save**. This can include earlier changes that were not saved.


Reset xxxxx settings

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 ✖.


Confirmation Required

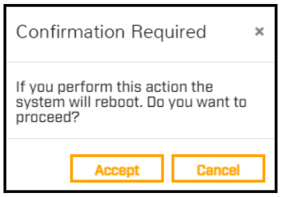
There are changes not saved as default.
Please select how to proceed

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**.

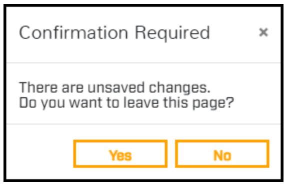
Changes to some System Settings require the camera to reboot; for example, on the Settings and on the Date & Time Page. After clicking **Save**, a confirmation message appears. To save the changes, and reboot the camera with the changes applied, click **Accept**. To close the confirmation message and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


Confirmation Required

If you perform this action the system will reboot. Do you want to proceed?

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 ✖.

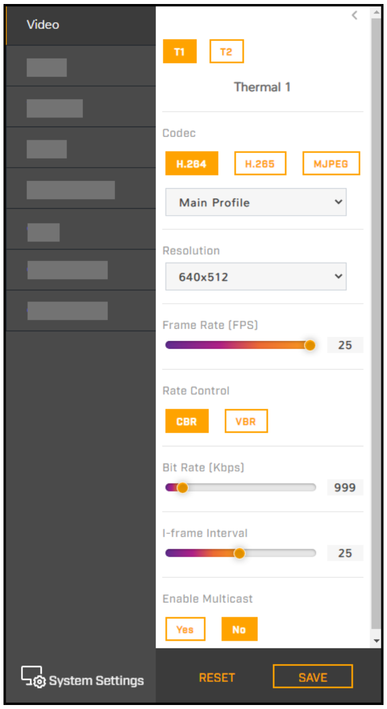


Confirmation Required

There are unsaved changes.
Do you want to leave this page?

3.4 Video Page

The camera provides two IP video streams (Thermal 1 / T1 and Thermal 2 / 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.



Video

T1 T2

Thermal 1

Codec: H.264 H.265 MJPEG

Main Profile

Resolution: 640x512

Frame Rate (FPS): 25

Rate Control: CBR VBR

Bit Rate (Kbps): 999

I-frame Interval: 25

Enable Multicast: Yes No

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

Codec options are H.264, H.265, or MJPEG.

Resolution is fixed at 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.

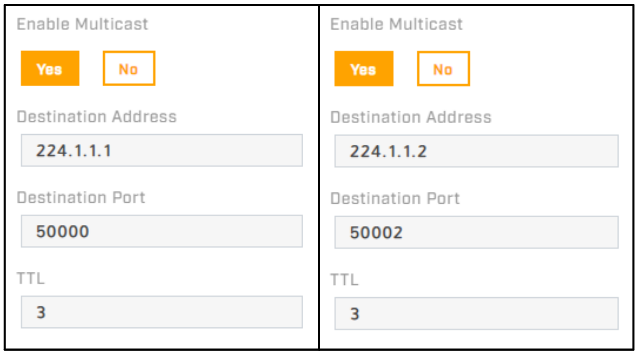
With the MJPEG codec, you can set the Quality between 0-100. Setting a higher value can increase the video stream's bandwidth requirements. Teledyne FLIR recommends setting a value no higher than 80. If you experience video issues when using MJPEG and high-resolution video, try adjusting the Quality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

Tips

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



Enable Multicast

[✓ Yes] No

Destination Address

224.1.1.1

Destination Port

50000

TTL

3

T1

Enable Multicast

[✓ Yes] No

Destination Address

224.1.1.2

Destination Port

50002

TTL

3

T2

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

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

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:

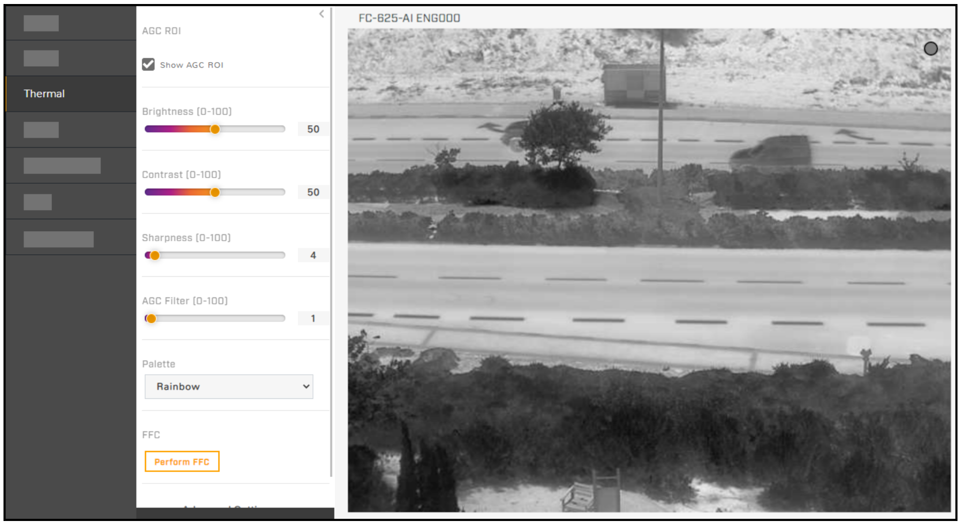
- **T1**—rtsp://192.168.0.250:554/stream1
- **T2**—rtsp://192.168.0.250:554/stream2

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

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

3.5 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

☑ Show AGC ROI

Brightness (0-100) 50

Contrast (0-100) 50

Sharpness (0-100) 4

AGC Filter (0-100) 1

Palette: Rainbow

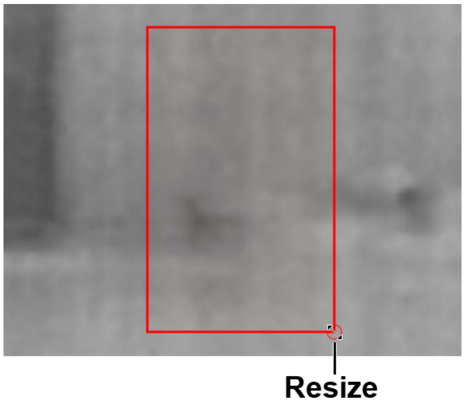
FFC

AGC ROI

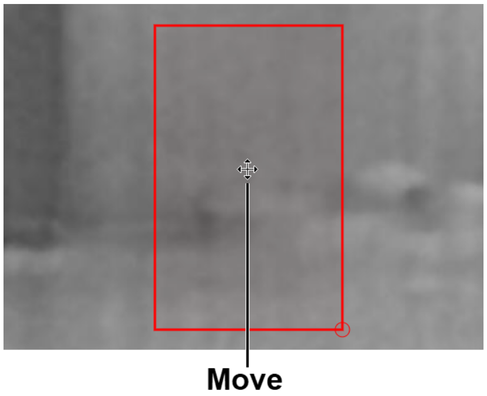
By default, **Show AGC ROI** is selected. The AGC ROI (region of interest) overlay appears in the live video on the camera web page. In video streams, the overlay does not appear. By default, the ROI is full screen; the AGC algorithm considers the entire image. In some cases, defining an ROI that excludes 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.



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



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.

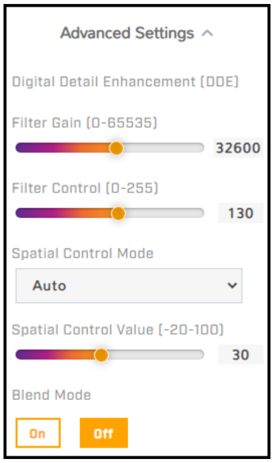
- **Contrast** (Max Gain)—Increasing contrast can provide a better image, especially for scenes with little temperature variation. (It might also increase noise due to the increased gain.) Range 0 to 100.

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).

Advanced Settings



Advanced Settings

Digital Detail Enhancement (DDE)

Filter Gain (0-65535) 32600

Filter Control (0-255) 130

Spatial Control Mode: Auto

Spatial Control Value (-20-100) 30

Blend Mode: On Off

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.

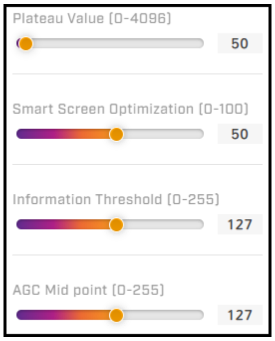
- **Filter Gain—**Amount of gain the algorithm applies to details in Manual Spatial Control Mode. Specify a value between 0-65535, with 0 (zero) meaning DDE is disabled. For any value other than zero, the algorithm attenuates or enhances details by a factor (Filter Gain Value / 2048). For example:
 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



Plateau Value (0-4096) 50

Smart Screen Optimization (0-100) 50

Information Threshold (0-255) 127

AGC Mid point (0-255) 127

- **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 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.

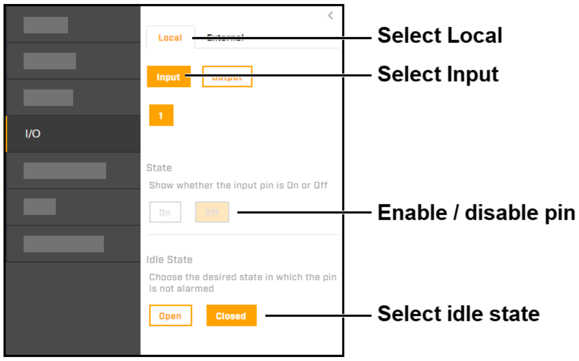
3.6 I/O Page

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

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

Local I/O pins

Input Pins



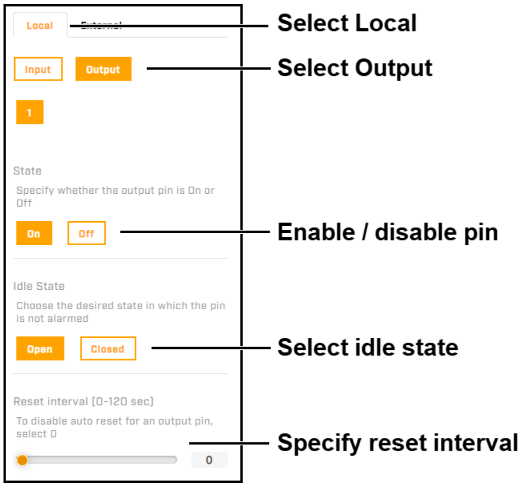
State

Show whether the input pin is On or Off

Idle State

Choose the desired state in which the pin is not alarmed

Output Pins



State

Specify whether the output pin is On or Off

Idle State

Choose the desired state in which the pin is not alarmed

Reset interval (0-120 sec)

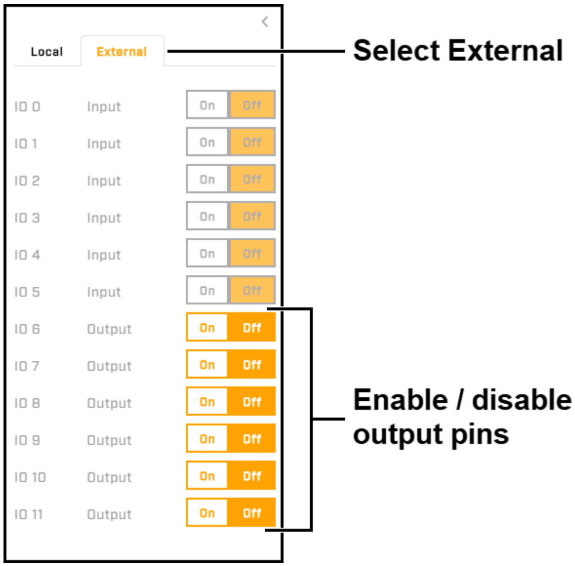
To disable auto reset for an output pin, select 0

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

For information about the local I/O connector, see the installation guide.

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.



IO 0	Input	On	Off
IO 1	Input	On	Off
IO 2	Input	On	Off
IO 3	Input	On	Off
IO 4	Input	On	Off
IO 5	Input	On	Off
IO 6	Output	On	Off
IO 7	Output	On	Off
IO 8	Output	On	Off
IO 9	Output	On	Off
IO 10	Output	On	Off
IO 11	Output	On	Off

Six Input and Six Output Pins

3.7 Radiometry Page (R models)

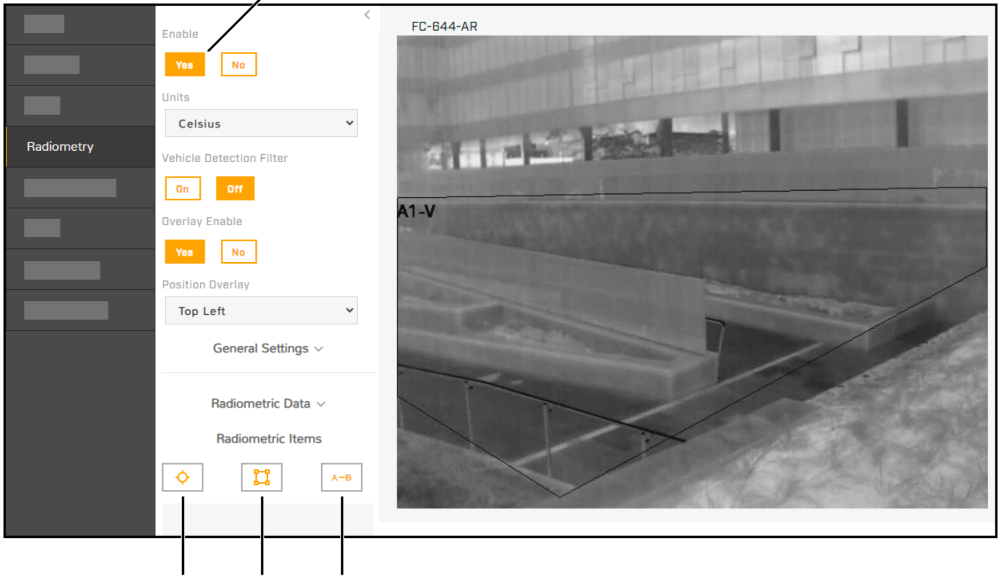
FC-Series AI R models detect, measure, and monitor surface temperatures. Using a thermal camera for reasonably accurate and precise temperature measurements requires at least a minimum level of expertise in thermography; Teledyne FLIR recommends training. The Infrared Training Center offers training (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

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.

Click to enable radiometry



Enable

Yes No

Units

Celsius

Vehicle Detection Filter

On Off

Overlay Enable

Yes No

Position Overlay

Top Left

Click to create a radiometric item

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:

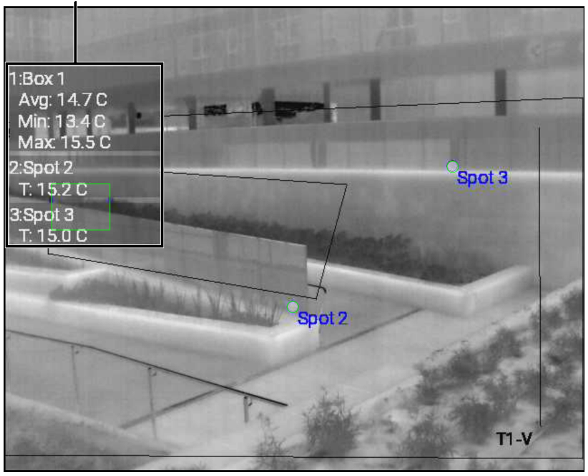
- vehicle classification is enabled on one or more loitering regions on the thermal video
- the loitering regions match the radiometric boxes

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

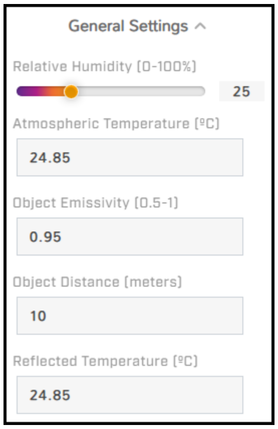


```
1:Box 1
  Avg: 14.7 C
  Min: 13.4 C
  Max: 15.5 C
2:Spot 2
  T: 15.2 C
3:Spot 3
  T: 15.0 C
```

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.



General Settings ^

Relative Humidity (0-100%) 25

Atmospheric Temperature (ºC) 24.85

Object Emissivity (0.5-1) 0.95

Object Distance (meters) 10

Reflected Temperature (ºC) 24.85

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 .

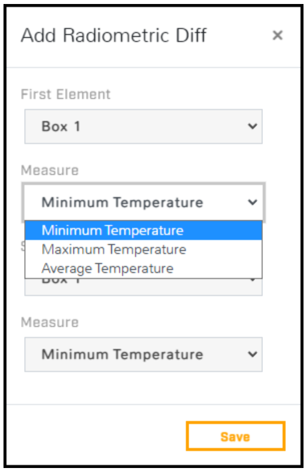
   The item appears in the Radiometric Items list. Spot and box items appear in the center of the live thermal video image.

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.



Add Radiometric Diff ×

First Element: Box 1

Measure: Minimum Temperature

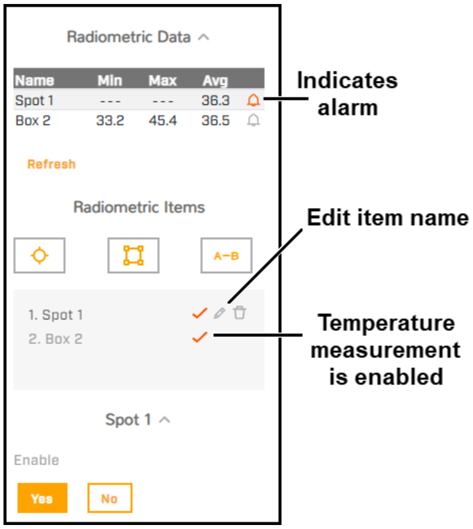
Measure: Minimum Temperature

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.



Radiometric Data ^

Name	Min	Max	Avg
Spot 1	---	---	36.3
Box 2	33.2	45.4	36.5

Radiometric Items

1. Spot 1 ✓
2. Box 2 ✓

Spot 1 ^

Enable:

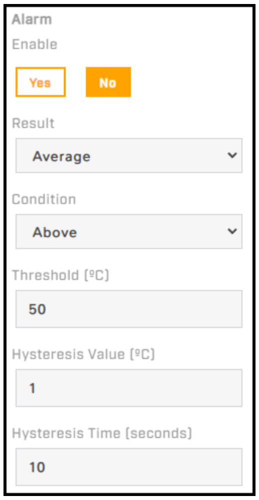
Indicates alarm

Edit item name

Temperature measurement is enabled

Alarm Settings

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



Alarm

Enable

Yes No

Result

Average

Condition

Above

Threshold (ºC)

50

Hysteresis Value (ºC)

1

Hysteresis Time (seconds)

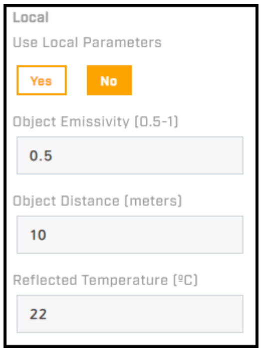
10

- **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.
- **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—



Local

Use Local Parameters

Yes No

Object Emissivity (0.5-1)

0.5

Object Distance (meters)

10

Reflected Temperature (ºC)

22

- **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.

3.8 Video Analytics Page

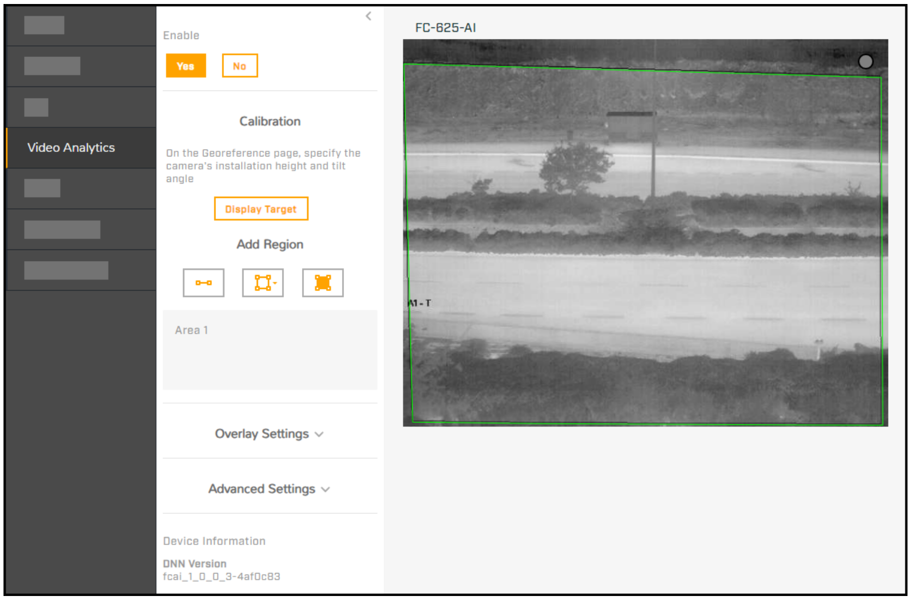
The camera's advanced onboard video analytics:

- Incorporate convolutional neural networks (CNN) technology
- Intrusion and loitering detection
- Classify detected objects as human or vehicle

On the Video Analytics page, you can:

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

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



Enable

[✓ Yes] No

Calibration

On the Georeference page, specify the camera's installation height and tilt angle

Display Target

Add Region

Area 1

Overlay Settings

Advanced Settings

Device Information

DNN Version
fcai_1_0_0_3-4af0c83

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.

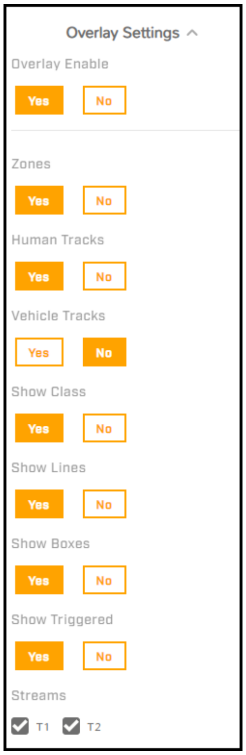
Detection and Classification

The camera's video analytics detect and classify 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.

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.



Overlay Settings

Overlay Enable
[✓ Yes] No

Zones
[✓ Yes] No

Human Tracks
[✓ Yes] No

Vehicle Tracks
Yes [✓ No]

Show Class
[✓ Yes] No

Show Lines
[✓ Yes] No

Show Boxes
[✓ Yes] No

Show Triggered
[✓ Yes] No

Streams
☑ T1 ☑ T2

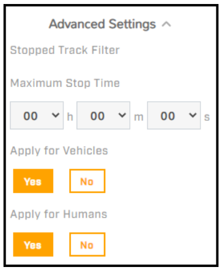
Setting	Description	Comments
Show Lines	When tracks are enabled, show the lines for the detected objects according to positions from prior frames; helps visually represent speed and direction.	Enable Human Tracks or Vehicle Tracks.
Show Boxes	When tracks are enabled, show a box around the track.	
Show 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.
Streams	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.



Advanced Settings

Stopped Track Filter

Maximum Stop Time

00 h 00 m 00 s

Apply for Vehicles

[✓ Yes] No

Apply for Humans

[✓ Yes] No

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.

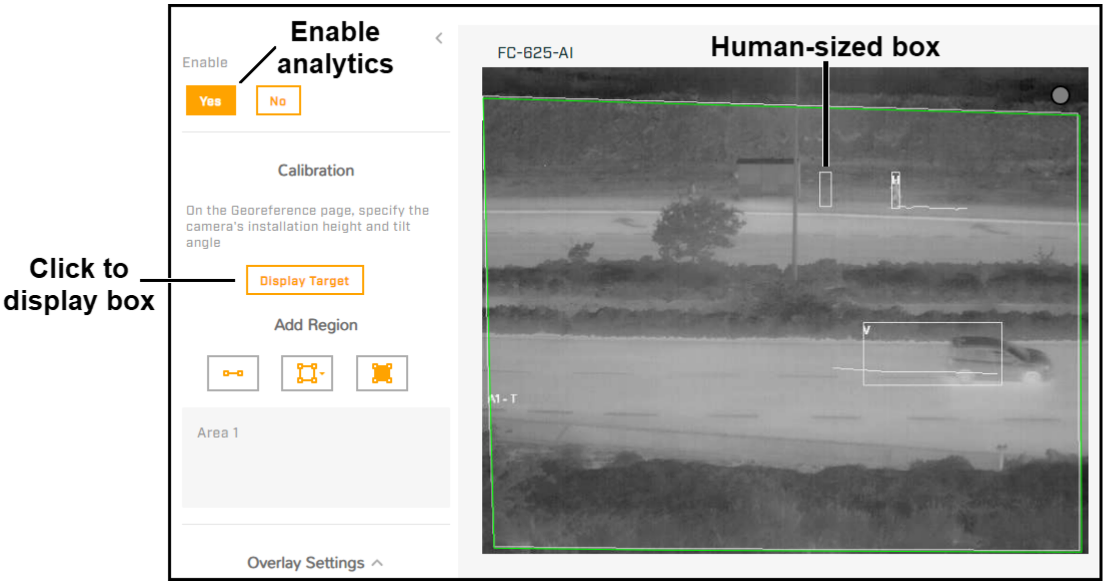
Users assigned the expert or admin role can enable, modify, or define alarm rules on the Alarm Page.

3.8.1 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.

1. Make sure that a person about 1.8m (5" 11') tall is in the camera's field of view.
2. On the Video Analytics page, make sure 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.

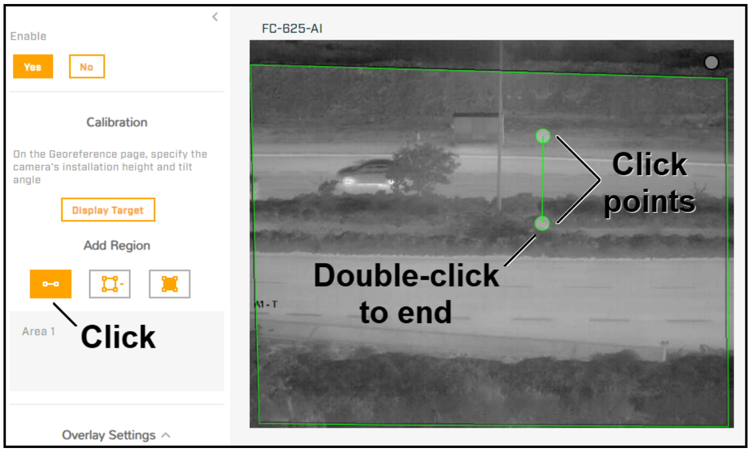


On the Georeference page, specify the camera's installation height and tilt angle

Checking Calibration

3.8.2 Create Analytics Regions

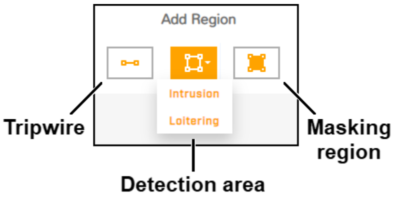
When the analytics overlay is enabled for the Video Analytics page live video, tripwires and analytics regions are labeled according to analytics region type, T = Tripwire or A = Area (intrusion / loitering), and unique region ID number.



On the Georeference page, specify the camera's installation height and tilt angle

Creating a Tripwire

To create a region:



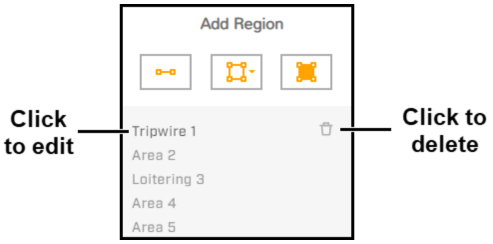
1. Under Add Region, click the appropriate icon to create a tripwire; an intrusion or loitering detection area; or a masking region.
2. Specify each point of the region by clicking and releasing on the live video image. Do not click and drag. Also, do not draw one region line or border over another.

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

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

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 🗑.



Click to edit

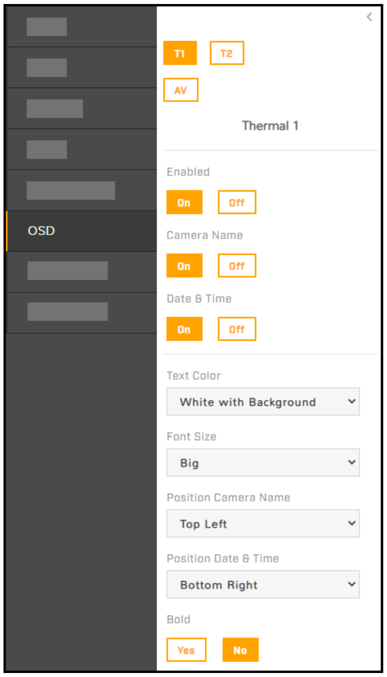
Click to delete

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 two masking regions.

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.

3.9 OSD Page



Enabled: On
Camera Name: On
Date & Time: On
Text Color: White with Background
Font Size: Big
Position Camera Name: Top Left
Position Date & Time: Bottom Right
Bold: No

For each IP video stream (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**

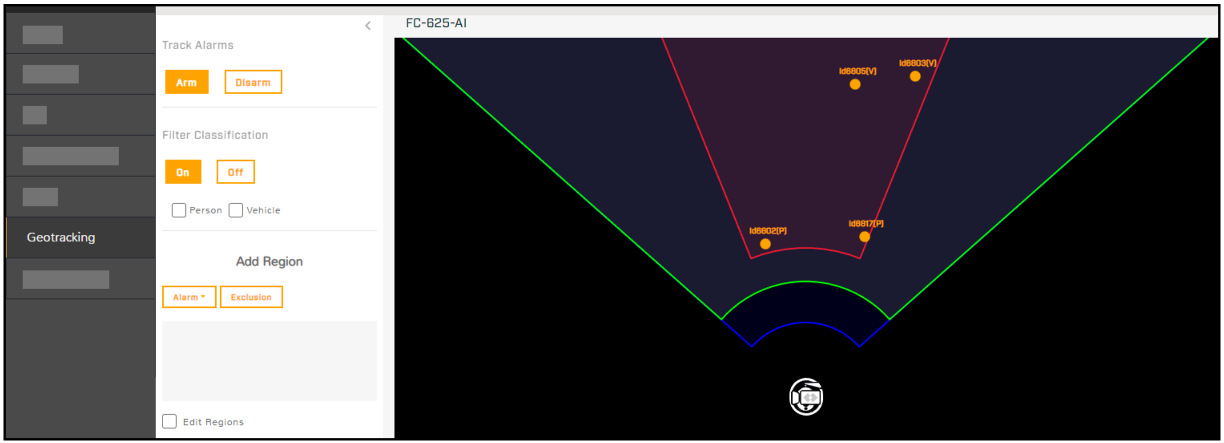
When OSD is enabled for the T1 stream, the OSD appears in the live video on the camera web page. Enabling OSD on the T2 stream, or on the analog video, does not affect the live video on the camera web page.

3.10 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, a Quasar® 4K IR PTZ camera (CP-6408-x1-I). For information about how to pair this camera, including how to configure the PTZ camera when it is paired, see Pairing an FH-Series AI Camera with a FLIR Security PTZ Camera.

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



Detected Objects Tracked (Map Not Uploaded)

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

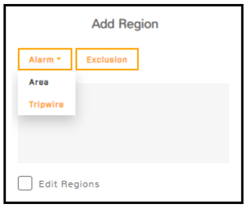
Icons and Descriptions			
📷	Fixed camera—a circle around this icon indicates the FC-Series AI camera you are currently configuring	▱	Geotracking alarm region
📹	PTZ camera	▱	Geotracking exclusion region
📡	Radar	🟠	Detected object
▽	Geotracking detection range of circled camera	🔴	Detected object in alarm region
▽	Visible camera detection range	▣	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).

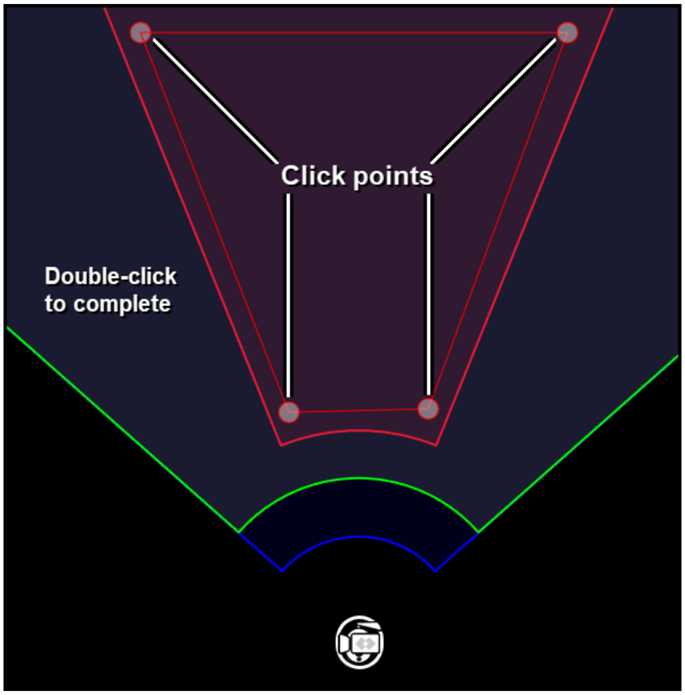
To add a geotracking region:

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. You can specify a geotracking alarm region as the trigger for a camera alarm. When an FC-Series AI 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.

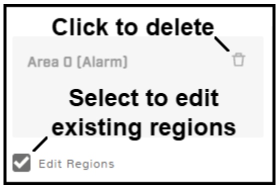


1. Create the first point of the region. Click and release on the detection area display.
2. Continue adding points (up to 25).
3. Complete the region. Double-click on the detection area display.

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

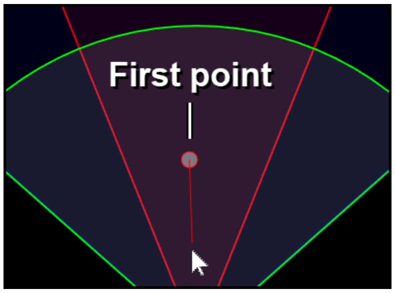
Managing Regions

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

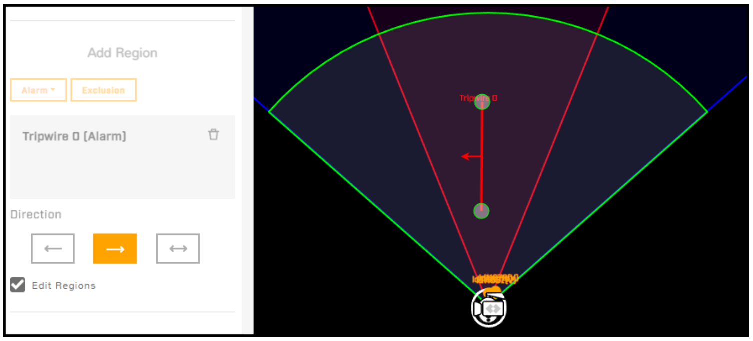


- Move region points. Click on the point, hold, and drag.
- Define a tripwire’s detection direction.

  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.

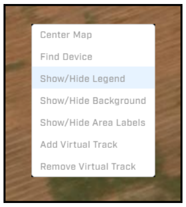


When Edit Regions is selected, it is not possible to add regions.

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.



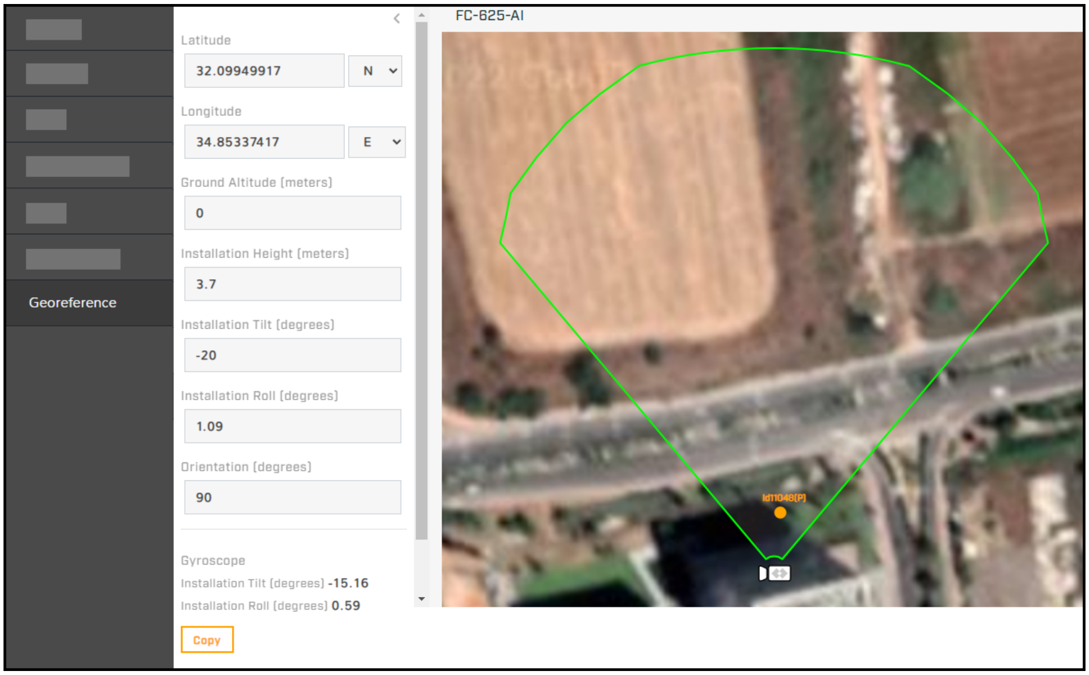
These right-click options are also available on the Georeference Page display.

3.11 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.

Specify the camera's Latitude in degrees North or South, and its Longitude in degrees East or West, up to eight decimal places. To obtain the camera's coordinates, you can use a map or a mobile GPS device.



FC-625-AI

Georeference

Latitude

32.09949917 N

Longitude

34.85337417 E

Ground Altitude (meters)

0

Installation Height (meters)

3.7

Installation Tilt (degrees)

-20

Installation Roll (degrees)

1.09

Orientation (degrees)

90

Gyroscope

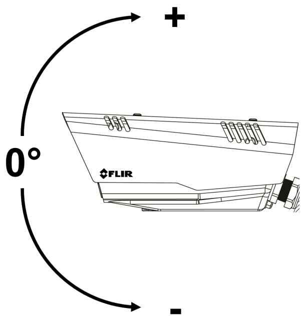
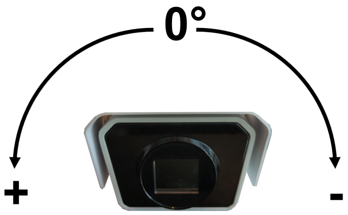
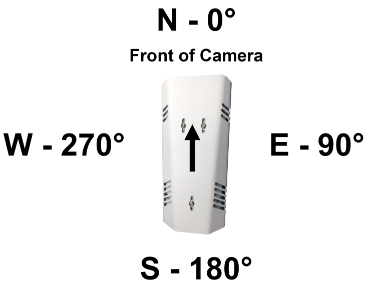
Installation Tilt (degrees) -15.16

Installation Roll (degrees) 0.59

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.
		 N - 0° Front of Camera W - 270° E - 90° S - 180°

Tips

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

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

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

4 Thermal Imaging Overview

WhiteHot Palette

A thermal camera produces an image based on differences in temperatures detected in the scene. The Palette setting on the Thermal Page determines the colors camera use to produce the image. Using the default WhiteHot palette, the object or surface in the scene with the hottest detected temperature appears white; the item with the coldest detected temperature appears black; and all other items appear in gray scale. For example, hot objects such as vehicle engines and exhaust pipes appear white or nearly white, and the sky, puddles of water, and other cold objects appear dark or black. Using the BlackHot color palette, hot objects appear black or dark and cold objects as white or nearly white.

Both thermal and visible light / daylight cameras have detectors (pixels) that detect energy. One difference between thermal and daylight cameras has to do with the source of the light that the camera detects. Visible light cameras detect reflected light. Therefore, a visible light camera requires a source of light that objects and surfaces in the scene can reflect; for example, the sun or an artificial light source. This is also true with human eyesight; the vast majority of what people see is based on reflected light.

On the other hand, a thermal camera detects the energy objects and surfaces in the scene directly radiate. Most objects in typical surroundings are not hot enough to radiate visible light. However, they do radiate infrared light in the range of the spectrum that a thermal camera can detect, long-wave infrared (LWIR). Even very cold objects, such as ice and snow, radiate this type of energy. With some experience, scenes with familiar objects will be easy to interpret.

The camera automatically optimizes the image to provide the best contrast in most conditions. In some cases, you can adjust the settings to further improve the image.

When the camera is mounted outdoors or the scene is otherwise exposed to sunlight, its performance varies throughout the day. For example, after sunset, objects warmed by the sun can remain warm and appear as such in the thermal image. Similarly, after sunrise and before the sun warms these same objects, they can appear cooler than their surroundings. Therefore, when visually monitoring the thermal image, be sure to look for subtle differences in the scene, as opposed to just hot targets. On R models, when configuring the radiometry settings, make sure to consider these changes that occur throughout the day.

5 Maintenance and Troubleshooting

If help is needed during installation, operation, or configuration, contact the local Teledyne FLIR representative, or visit the Teledyne FLIR Support Center. Teledyne FLIR LLC offers a comprehensive selection of training courses to help get the best performance and value from the thermal imaging camera.

Cleaning

Great care should be used with your camera's optics. They are delicate and can be damaged by improper cleaning. FC-Series thermal camera lenses and windows are designed for a harsh outdoor environment and have a coating for durability and anti-reflection. However, they can require occasional cleaning. When you notice deterioration in image quality, or you can see excessive contaminant build-up on the lens, Teledyne FLIR recommends cleaning the lens.

Note

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

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

Important

Do not use abrasive materials, such as paper or scrub brushes. They can damage the lens by scratching it. Wipe the lens clean only when you can visually see contamination on the surface.

Use the following procedure and solvents, as required:

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

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

Troubleshooting Tips

Unable to Communicate over Ethernet

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

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

Unable to View IP Video Stream

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

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

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

rtsp://192.168.0.250:554/stream1 for T1

rtsp://192.168.0.250:554/stream2 for T2

By default, RTSP authentication is enabled. To access any of the camera's video streams, you can use the name and password for any of the camera's users. See Users 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.

Image Freezes Momentarily

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

Performance Varies with Time of Day

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

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

See also Thermal Imaging Overview.

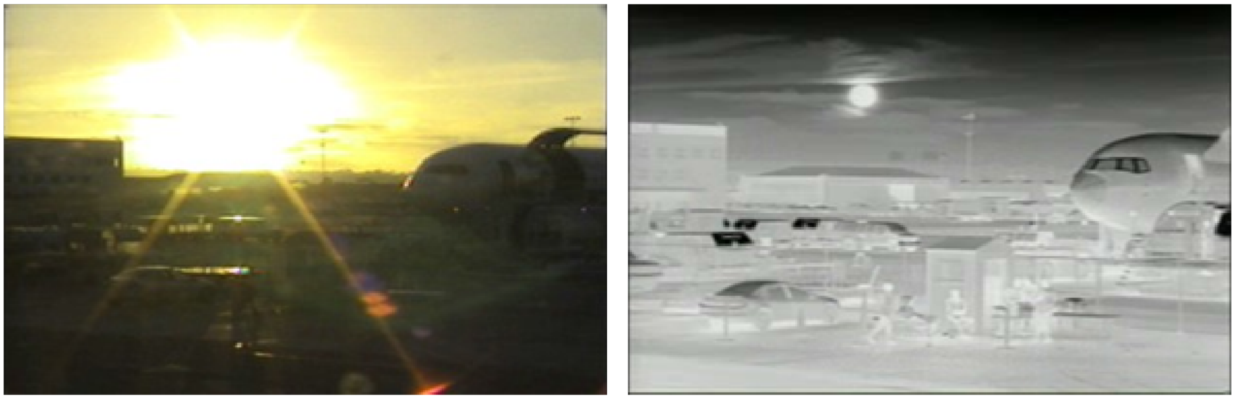
Image Too Dark or Too Light

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

Eastern or Western Exposure

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

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



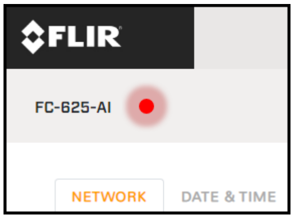
6 Configuration

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
- I/O Devices Page
- Messaging Page
- Heaters & Fans Page
- Cyber Page
- ONVIF Page
- Map Page
- Scheduler Page
- Recording Page
- SD Card Page
- Firmware & Info Page

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

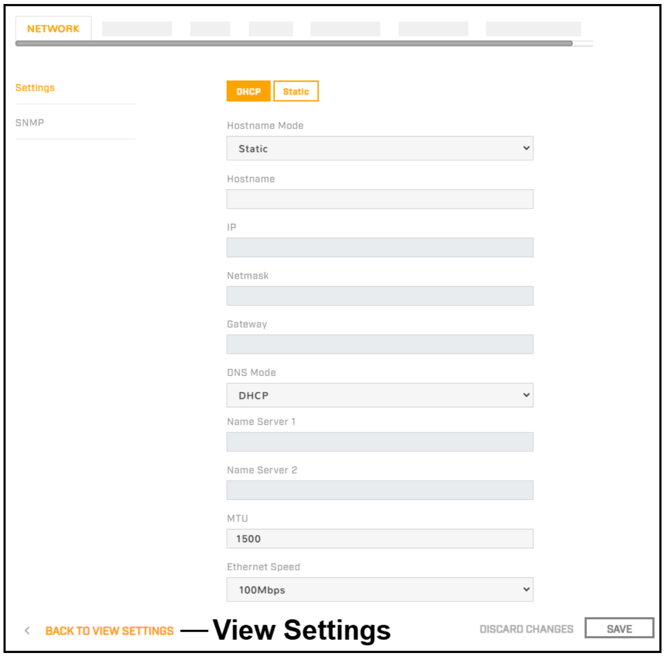
For information about making, applying, and saving changes on System Settings pages, see Making Changes to Settings.



Recording Indicator

6.1 Network Page

The Network page provides networking and SNMP settings.



Hostname Mode: Static

Hostname

IP

Netmask

Gateway

DNS Mode: DHCP

Name Server 1

Name Server 2

MTU: 1500

Ethernet Speed: 100Mbps

View Settings

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

6.1.1 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 a 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:

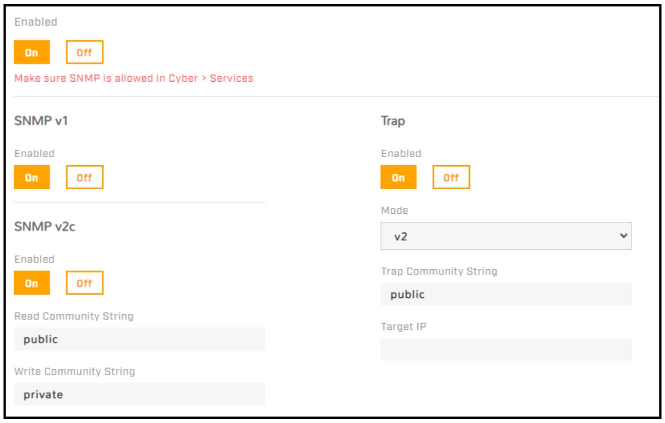
  - **Name Server 1**—The primary domain name server that translates host names into IP addresses.
  - **Name Server 2**—A secondary domain name server that backs up the primary DNS.

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 10/100 Mbps.

6.1.2 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.



Enabled: [✓ On] Off

Make sure SNMP is allowed in Cyber > Services

SNMP v1

Enabled: [✓ On] Off

SNMP v2c

Enabled: [✓ On] Off

Read Community String: public

Write Community String: private

Trap

Enabled: [✓ On] Off

Mode: v2

Trap Community String: public

Target IP:

Important

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

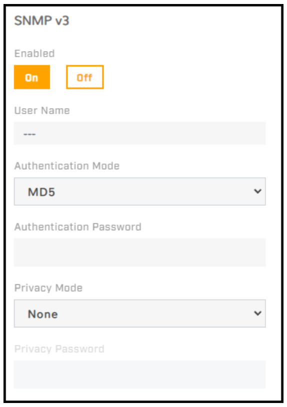
SNMP v1—Enable SNMP v1.

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

Enabled

On Off

User Name

Authentication Mode

MD5

Authentication Password

Privacy Mode

None

Privacy Password

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

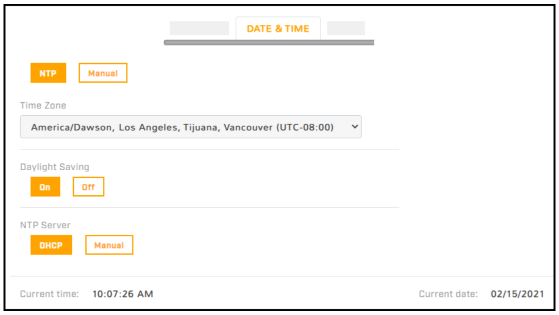
The camera uses traps to send messages to the network management system for important events or status changes.

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.

6.2 Date & Time Page

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



Time Zone: America/Dawson, Los Angeles, Tijuana, Vancouver (UTC-08:00)

Daylight Saving: On

NTP Server: DHCP

Current time: 10:07:26 AM

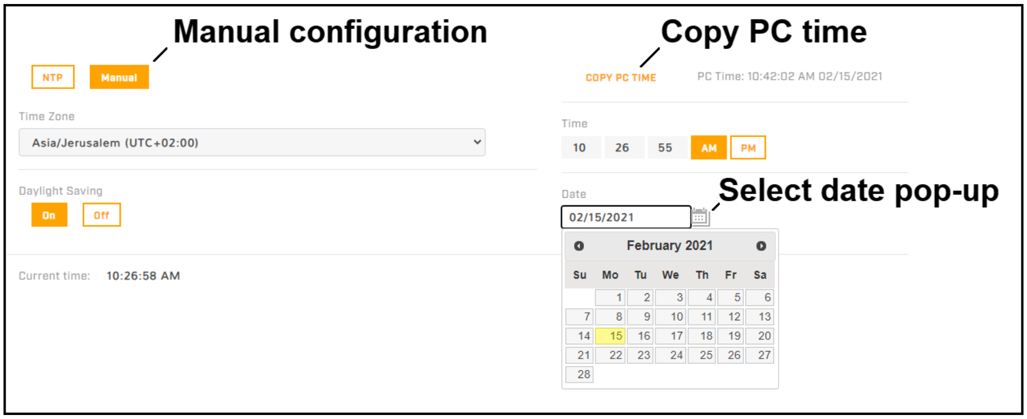
Current date: 02/15/2021

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.



Time Zone: Asia/Jerusalem (UTC+02:00)

Daylight Saving: On

Current time: 10:26:58 AM

PC Time: 10:42:02 AM 02/15/2021

Time: 10 26 55 AM

Date: 02/15/2021

February 2021

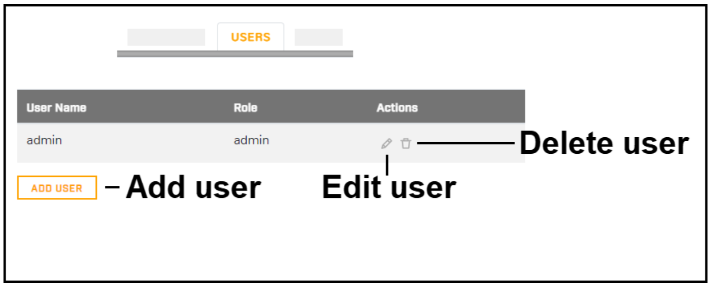
Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28						

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.

6.3 Users Page

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



User Name	Role	Actions
admin	admin	

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

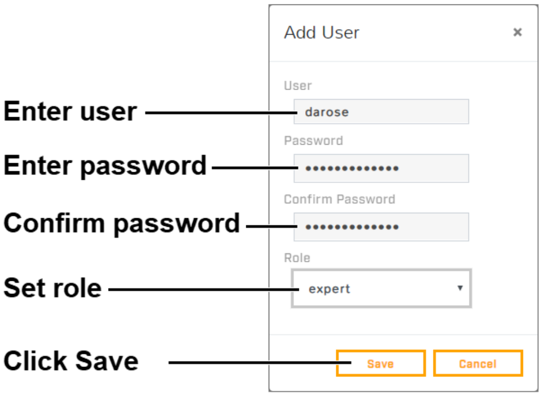
To maintain security of the system, set up user names and passwords for each required login account.

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


Add User

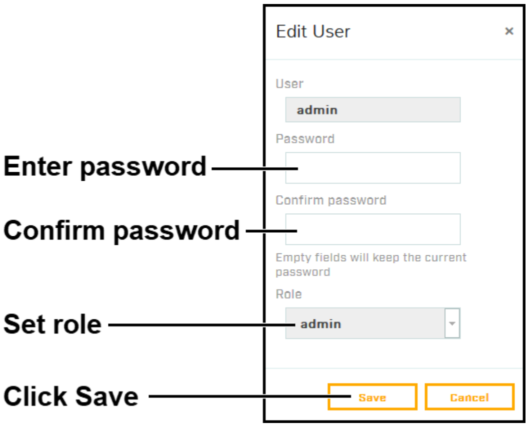
User
darose

Password
•••••••••••••

Confirm Password
•••••••••••••

Role
expert

Edit User


Edit User

User
admin

Password

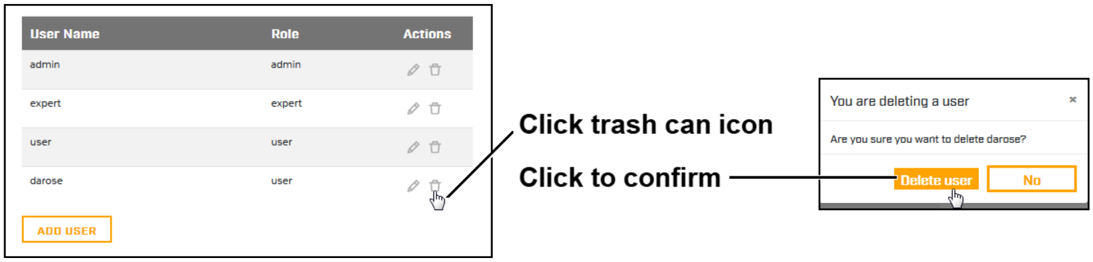
Confirm password

Empty fields will keep the current password

Role
admin

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

Delete User



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

You are deleting a user

Are you sure you want to delete darose?

6.4 Alarm Page

You can define camera alarms to be triggered by:

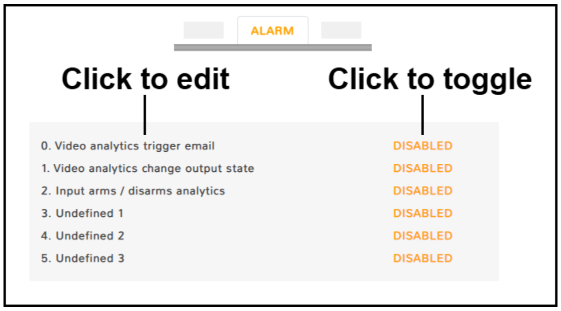
- The camera's onboard video analytics
- The camera's radiometry (R models)

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

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

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

By default, the following rules are defined and disabled:



0. Video analytics trigger email	DISABLED
1. Video analytics change output state	DISABLED
2. Input arms / disarms analytics	DISABLED
3. Undefined 1	DISABLED
4. Undefined 2	DISABLED
5. Undefined 3	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.

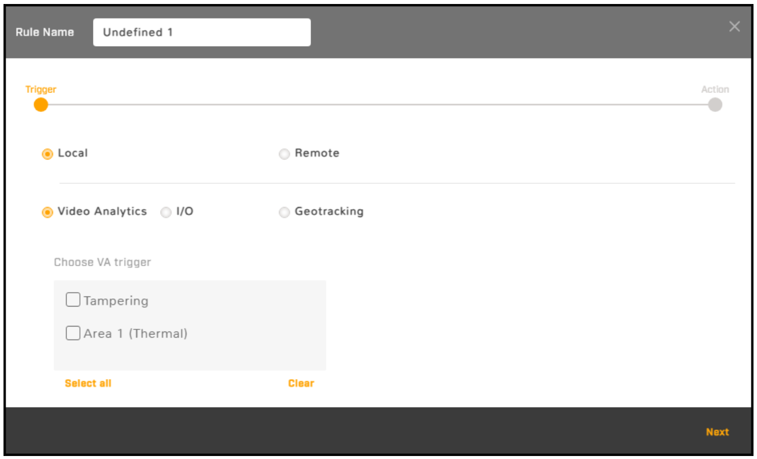
You can also define and enable three additional rules (**3. Undefined 1**, **4. Undefined 2**, and **5. Undefined 3**).

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 Name: Undefined 1

● Local ○ Remote

● Video Analytics ○ I/O ○ Geotracking

Choose VA trigger

□ Tampering

□ Area 1 (Thermal)

Rule Trigger Settings for Local Video Analytics

6.4.1 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 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.
I/O	**Local—**This camera's local I/O connections trigger this rule's action.	a. On the I/O Page, make sure local I/O connectors have been properly configured. b. Select one or more local I/O connections that trigger this rule's action.
	External—This camera's external I/O connections trigger this rule's action.	a. On the I/O Page and on the I/O Devices Page, make sure the external I/O connections and the device managing those connections with the camera have been properly configured. b. Select one or more external I/O connections that trigger this rule's action.
Geotracking	This camera's geotracking triggers this rule's action.	a. On the Geotracking Page, make sure regions have been defined. b. Select the regions 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. On the relevant page in View Settings, make sure video analytics / geotracking are enabled.

Remote Triggers

Under Discovered Devices, from the drop-down menu of supported devices on the same network as the camera, select a remote camera, radar / geotracking device, or other device; 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.

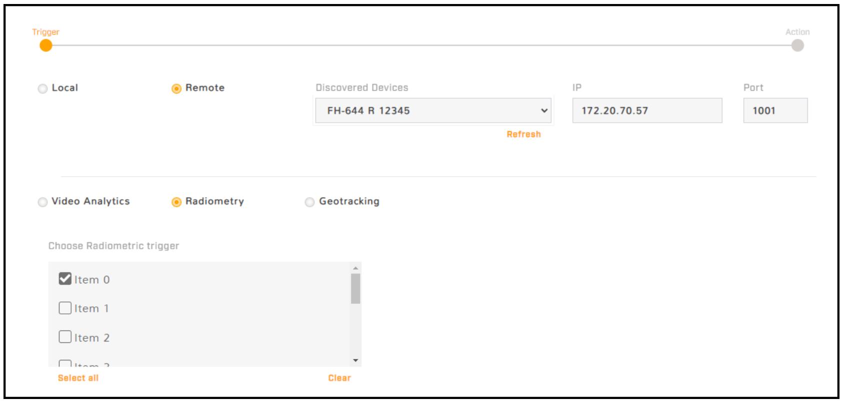
Note

The camera discovers supported devices on the same network as the camera. However, you can only use devices on the same VLAN as the camera as a trigger.

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.

Remote Triggers		
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.



○ Local ● Remote

Discovered Devices: FH-644 R 12345
IP: 172.20.70.57
Port: 1001
Refresh

○ Video Analytics ● Radiometry ○ Geotracking

Choose Radiometric trigger

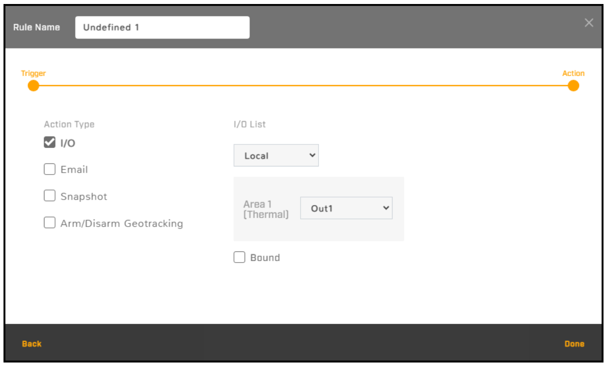
☑ Item 0
□ Item 1
□ Item 2
□ Item 3

Select all Clear

3. Click **Next**. The rule action settings appear.

4. Continue with Modifying or Defining Rule Actions.

6.4.2 Modifying or Defining Rule Actions



Rule Name: Undefined 1

Action Type

☑ I/O
□ Email
□ Snapshot
□ Arm/Disarm Geotracking

I/O List: Local

Area 1 [Thermal]: Out1

□ Bound

Rule Action Settings
Local I/O - Area 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.

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

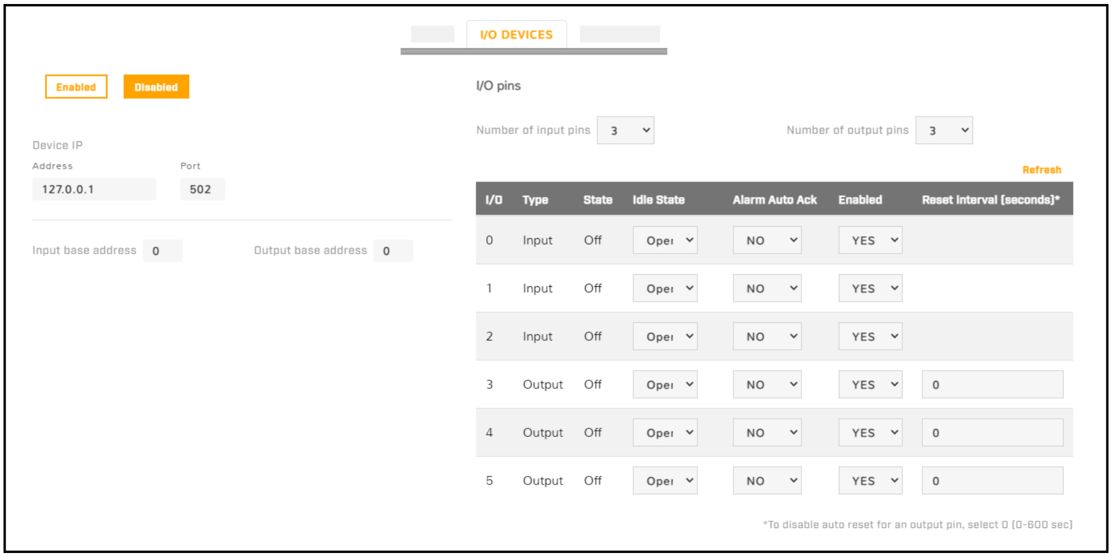
3. Click **Done**.

6.5 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**



Device IP

Address: 127.0.0.1

Port: 502

Input base address: 0

Output base address: 0

I/O pins

Number of input pins: 3

Number of output pins: 3

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

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

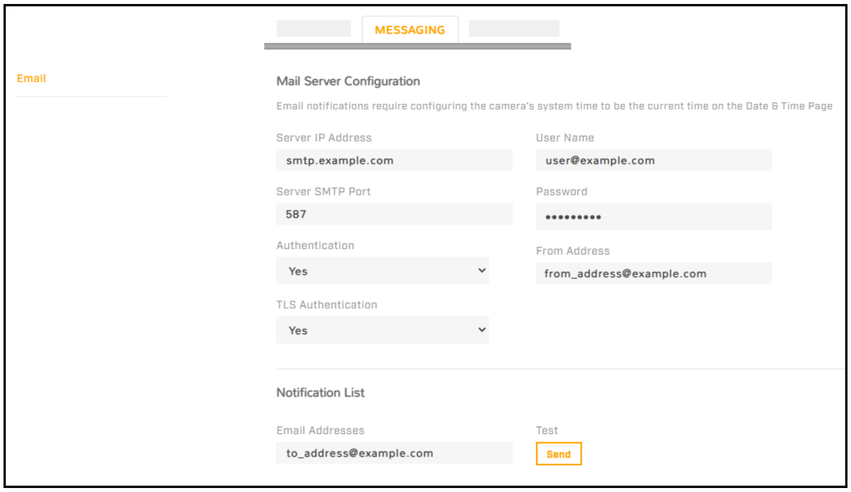
For each pin, the following information appears and you can confgure:

- **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.

6.6 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.



Mail Server Configuration

Email notifications require configuring the camera's system time to be the current time on the Date & Time Page

Server IP Address: smtp.example.com

User Name: user@example.com

Server SMTP Port: 587

Password: •••••••••

Authentication: Yes

From Address: from_address@example.com

TLS Authentication: Yes

Notification List

Email Addresses: to_address@example.com

Test: Send

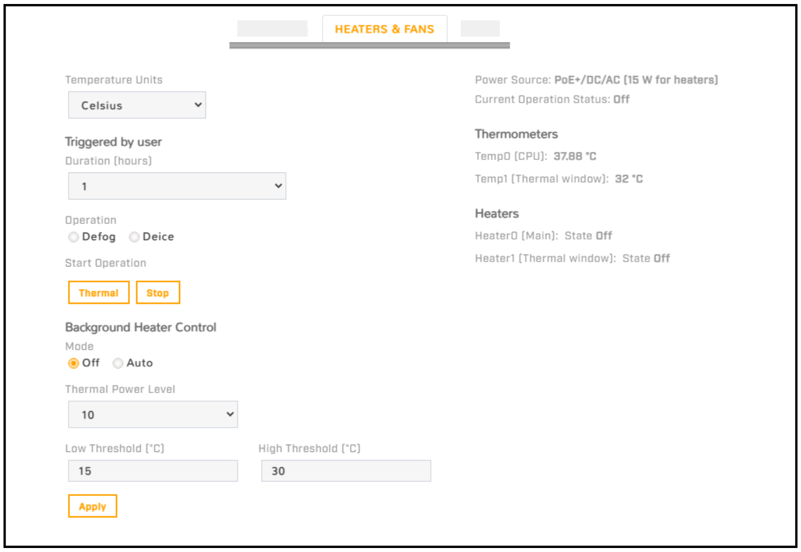
Specify the settings for the SMTP server in the appropriate fields. Settings include the SMTP server's IP address; port (the default port is 587); user name and password for the account on the mail server; whether the mail server requires authentication or TLS authentication; and the email address from 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.

6.7 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.



Temperature Units
Celsius

Triggered by user
Duration (hours)
1

Operation
○ Defog ○ Deice

Start Operation

Background Heater Control
Mode
● Off ○ Auto

Thermal Power Level
10

Low Threshold (°C)
15

High Threshold (°C)
30

Power Source: PoE+/DC/AC (15 W for heaters)
Current Operation Status: Off

Thermometers
Temp0 (CPU): 37.88 °C
Temp1 (Thermal window): 32 °C

Heaters
Heater0 (Main): State Off
Heater1 (Thermal window): State Off

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

To manually activate defogging or deicing the camera's window heater:

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

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

Background Heater Control

By default, background heater control is set to Off. If you enable it, specify:

- Thermal Power Level (0-15). Keep in mind the amount of power available to the heater (see, for example, Camera Specifications in the *FC-Series AI Installation Guide*).
- Temperatures at which the heaters activate (Low Threshold) and deactivate (High Threshold).

Status Information

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

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

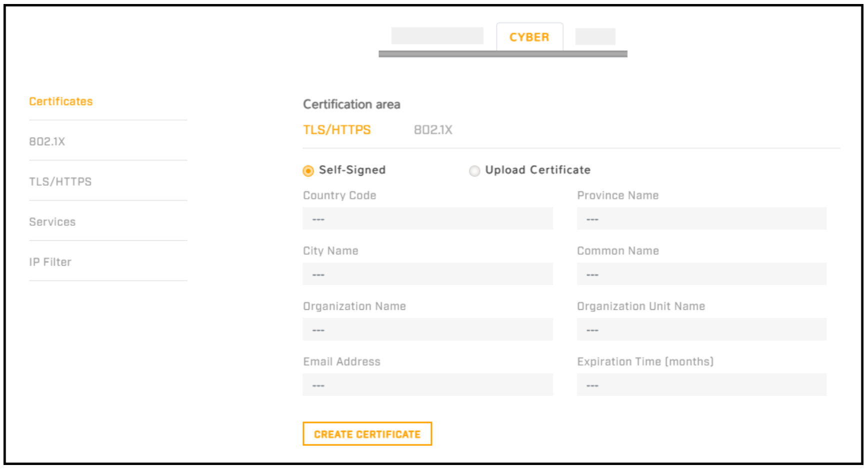
6.8 Cyber Page

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.

6.8.1 Certificates



Certification area

TLS/HTTPS 802.1X

● Self-Signed ○ Upload Certificate

Country Code: ---

Province Name: ---

City Name: ---

Common Name: ---

Organization Name: ---

Organization Unit Name: ---

Email Address: ---

Expiration Time (months): ---

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

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

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

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

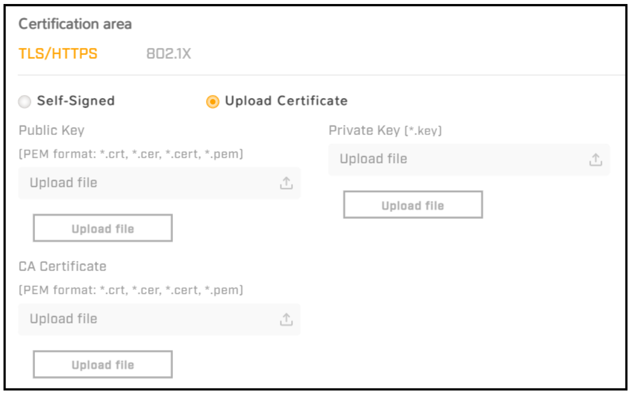
To generate and install a self-signed certificate for TLS/HTTPS:

1. In the Certificates section and Certification area, select **TLS/HTTPS** and **Self-Signed**.
2. Enter information such as country code, city name, and organization name.

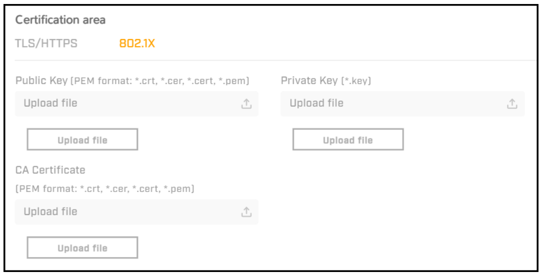
3. Click **Create Certificate**.
4. Allow 15 seconds for the camera to generate the certificate, at which point a confirmation appears.

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

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



To Upload a Certificate for TLS/HTTPS

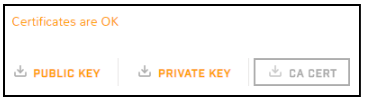


To Upload a Certificate for 802.1X

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

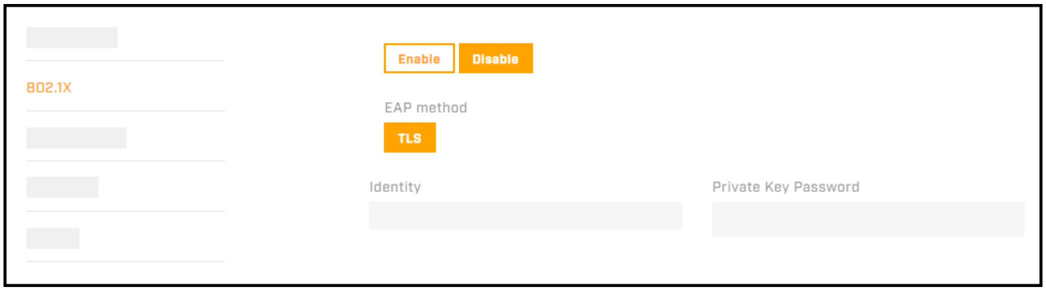


Note that you can download keys and certificates from the camera.

6.8.2 802.1X

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.



6.8.3 TLS / HTTPS

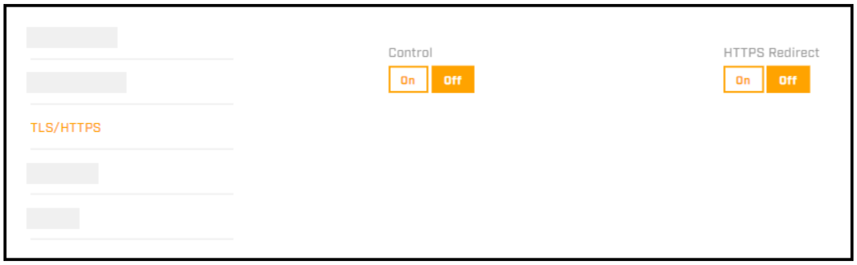
You can enable or disable:

- 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.



TLS/HTTPS

Control: On [✓ Off]

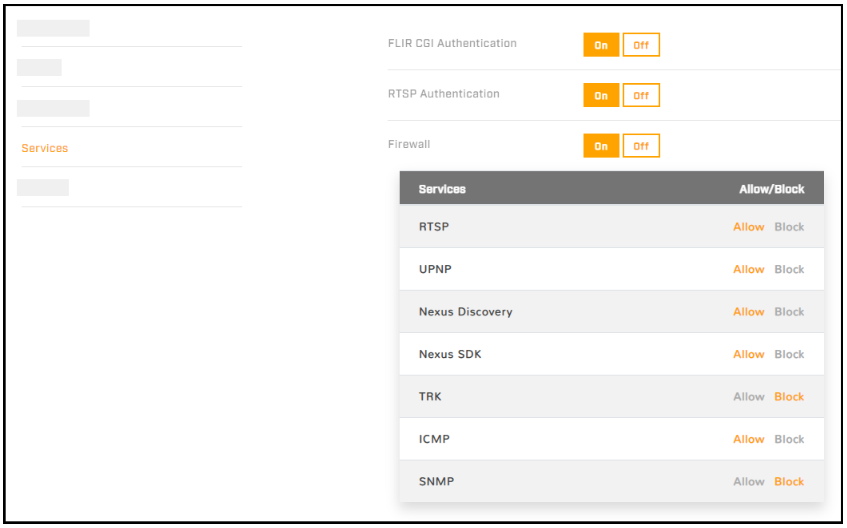
HTTPS Redirect: On [✓ Off]

6.8.4 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).



Services

FLIR CGI Authentication: [✓ On] Off

RTSP Authentication: [✓ On] Off

Firewall: [✓ On] Off

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

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**.

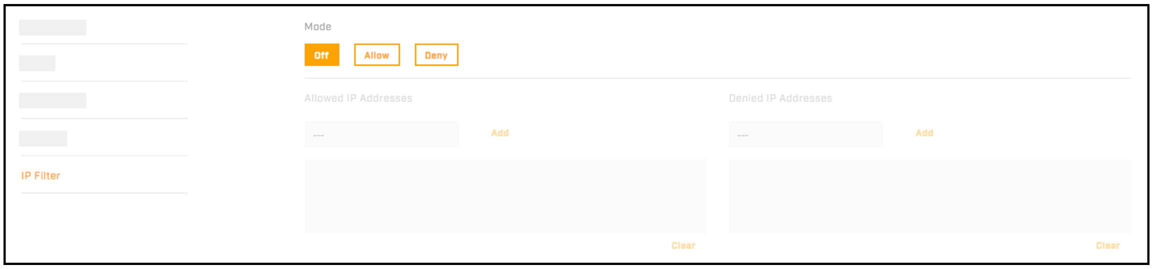
> ⚠ **Caution**
>
> Disabling services and ports can affect product functionality.

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

6.8.5 IP Filter

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

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



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

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

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

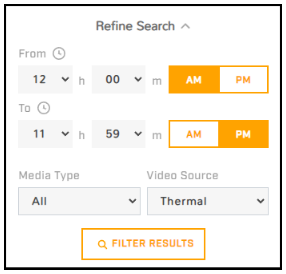
To remove an IP address from a list, click the corresponding trash icon 🗑.

6.9 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.

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)

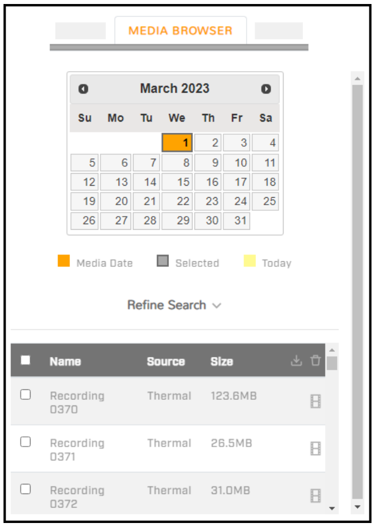


From 12 h 00 m AM

To 11 h 59 m PM

Media Type: All

Video Source: Thermal



	Name	Source	Size
□	Recording 0370	Thermal	123.6MB
□	Recording 0371	Thermal	26.5MB
□	Recording 0372	Thermal	31.0MB

Date with Recorded Files Selected

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

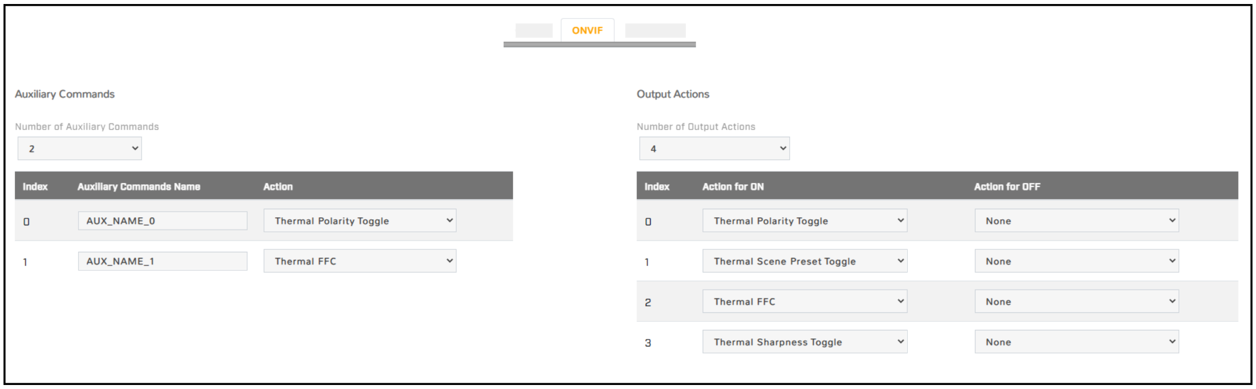
After selecting one or more files, you can download ⬇ or delete 🗑 the file(s).

6.10 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.
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.



Auxiliary Commands

Number of Auxiliary Commands: 2

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

Output Actions

Number of Output Actions: 4

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

Note

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

6.11 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.

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.

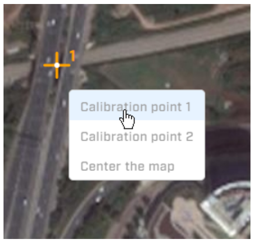
   For optimal calibration, the two calibration points should be as far apart as possible and on opposite sides of the map image. For example, at top-right and at lower-left.

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

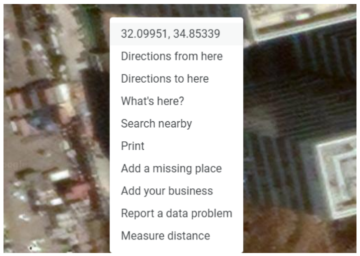
   If the map successfully uploads, a confirmation message appears.

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


32.09951, 34.85339

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.

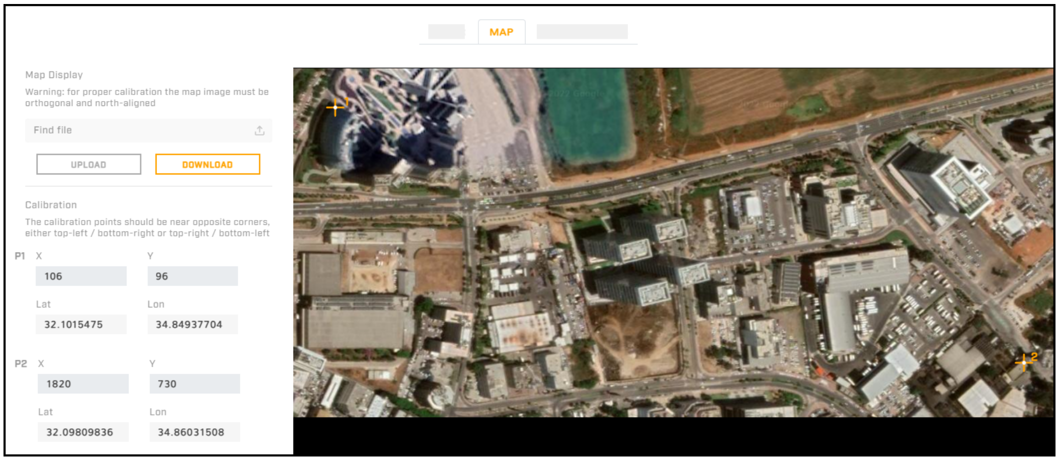
   For example, when using Google Maps, right-click on a point and select the coordinates. The point's latitude and longitude coordinates are copied to the clipboard. Paste the coordinates into the P1 **Lat** and **Lon** fields.

   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.



Map Display

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

Find file

Calibration

The calibration points should be near opposite corners, either top-left / bottom-right or top-right / bottom-left

P1 X 106 Y 96

Lat 32.1015475 Lon 34.84937704

P2 X 1820 Y 730

Lat 32.09809836 Lon 34.86031508

Map Uploaded and Calibrated

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.

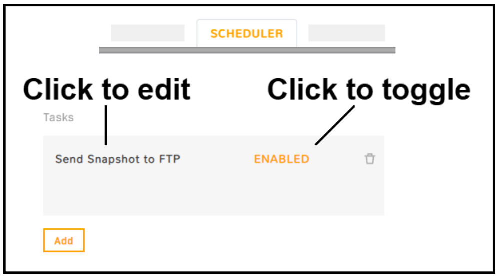
6.12 Scheduler Page

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

- Enable the camera's 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.



Tasks

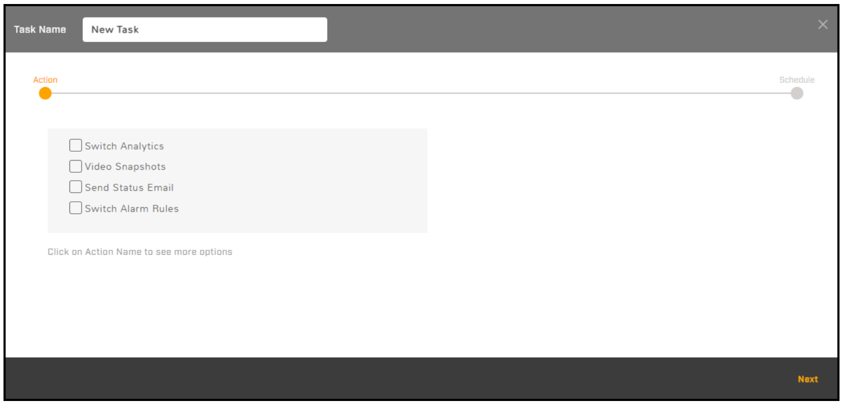
Send Snapshot to FTP ENABLED

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.



Task Name: New Task

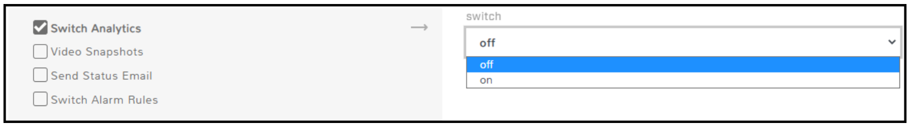
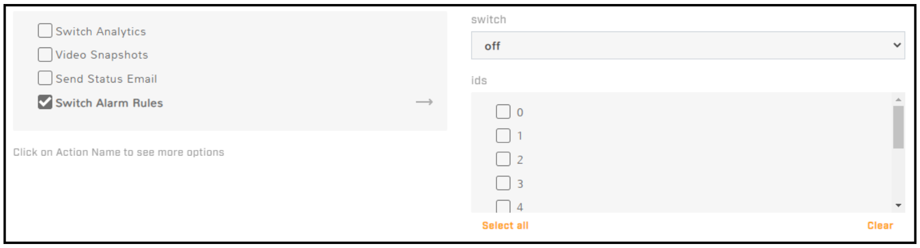
Action — Schedule

□ Switch Analytics
□ Video Snapshots
□ Send Status Email
□ Switch Alarm Rules

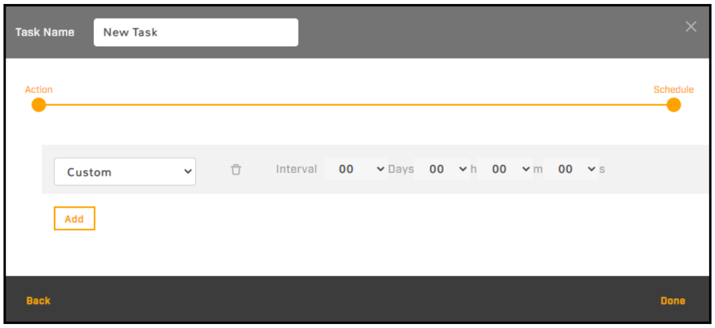
Click on Action Name to see more options

Next

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).  ☑ Switch Analytics □ Video Snapshots □ Send Status Email □ Switch Alarm Rules switch: off off 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.  □ Switch Analytics □ Video Snapshots □ Send Status Email ☑ Switch Alarm Rules Click on Action Name to see more options switch: off ids □ 0 □ 1 □ 2 □ 3 □ 4 Select all Clear b. Select the alarm rules the task affects, according to rule ID number. To determine the rule ID, check the Alarm Page.

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



Task Name: New Task

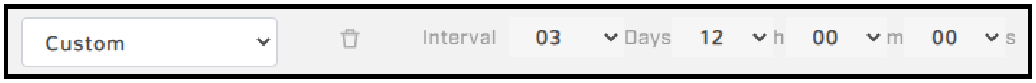
Action — Schedule

Custom | Interval 00 Days 00 h 00 m 00 s

Add

Back Done

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:  Custom Interval 03 Days 12 h 00 m 00 s
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 🗑.

6.13 Recording Page

On the Recording page, you can configure:

- Global video clip recording settings
- Recording sources

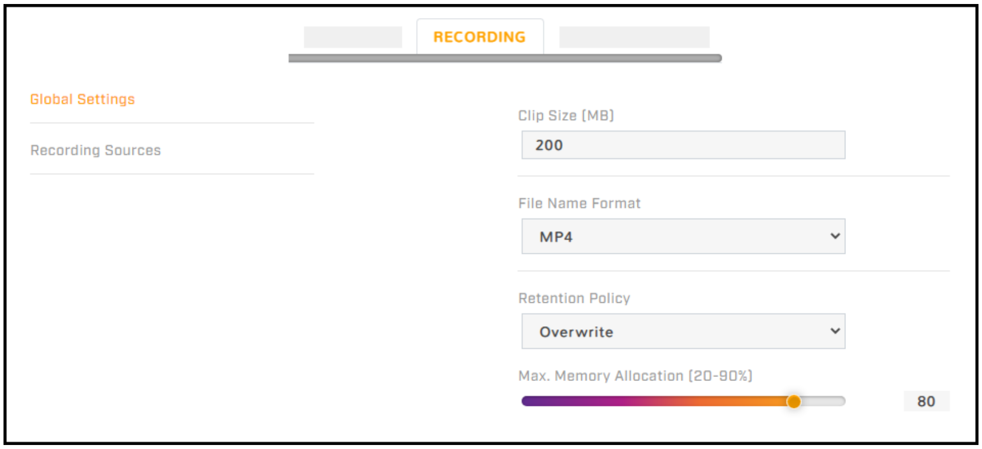
Global Settings

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

File Name Format—MP4.

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

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



Clip Size (MB): 200

File Name Format: MP4

Retention Policy: Overwrite

Max. Memory Allocation (20-90%): 80

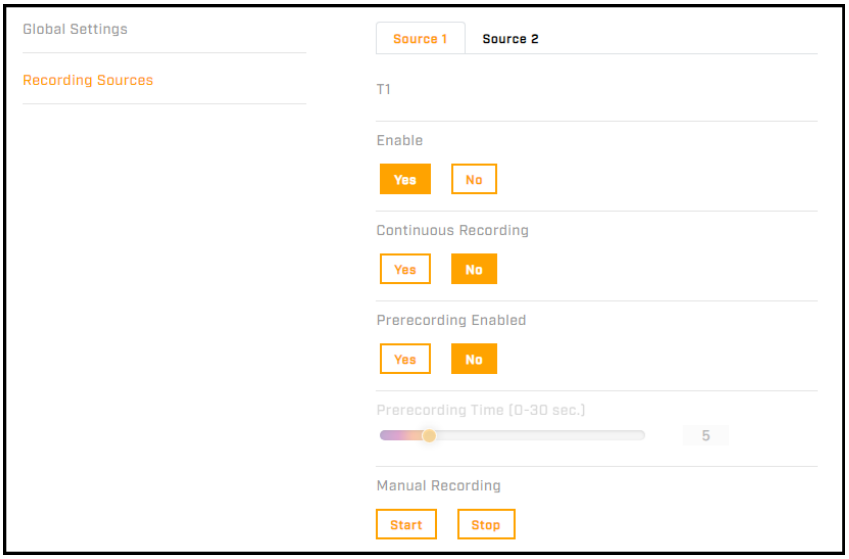
Recording Sources

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

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

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



T1

Enable: Yes [✓] No

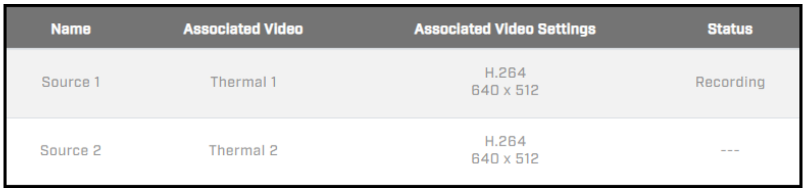
Continuous Recording: Yes No [✓]

Prerecording Enabled: Yes No [✓]

Prerecording Time (0-30 sec.): 5

Manual Recording

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

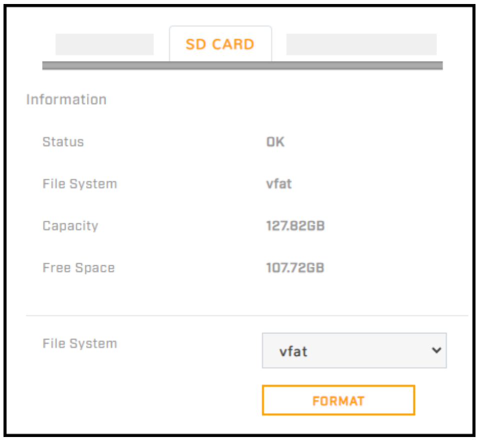


Name	Associated Video	Associated Video Settings	Status
Source 1	Thermal 1	H.264 640 x 512	Recording
Source 2	Thermal 2	H.264 640 x 512	---

Example: Source 1 - Thermal 1 is Currently Recording

6.14 SD Card Page

You can locally record up to 512 GB on a microSD card. For information about accessing the camera's microSD slot and inserting a card, see the installation guide.



Information

Status	OK
File System	vfat
Capacity	127.82GB
Free Space	107.72GB

File System: vfat

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
- **File System—**vfat or xt4.
- **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, select the file system, and then click **Format**.

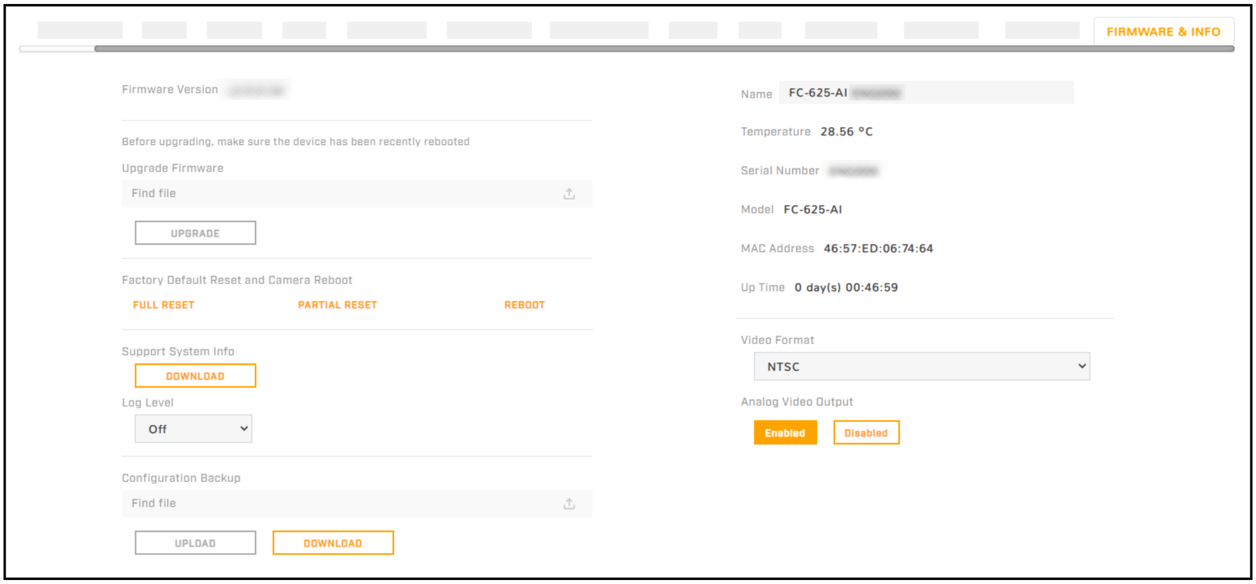
Caution

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

Notes

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

6.15 Firmware & Info Page



Firmware Version [redacted]

Before upgrading, make sure the device has been recently rebooted

Upgrade Firmware

Find file

Factory Default Reset and Camera Reboot

Support System Info

Log Level: Off

Configuration Backup

Find file

Name: FC-625-AI [redacted]

Temperature: 28.56 °C

Serial Number: [redacted]

Model: FC-625-AI

MAC Address: 46:57:ED:06:74:64

Up Time: 0 day(s) 00:46:59

Video Format: NTSC

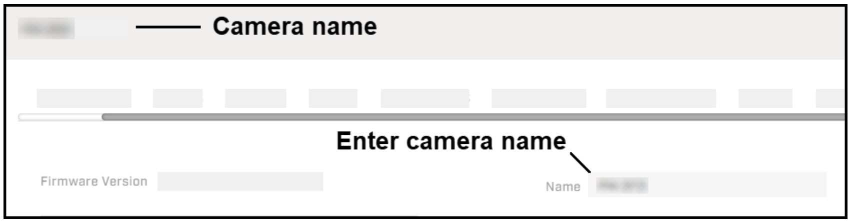
Analog Video Output: Enabled

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
- Enable / disable the camera's analog video output

Name

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



To upgrade the camera's firmware:

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

⚠ **Caution**

Only upgrade with firmware developed for FC-Series AI 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

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

To reset the camera to its factory default settings but retain previously saved 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.

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 FC-Series AI 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 Output—Specify whether the camera's analog video output is enabled or disabled.

7 Pairing an FC-Series AI Camera with a FLIR Security PTZ Camera

By default, FC-Series AI cameras support geotracking. You can pair an FC-Series AI camera with a FLIR Security PTZ camera that supports geotracking. The PTZ camera engages and tracks objects detected by the FC-Series AI 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 FC-Series AI camera. However, geotracking does require accurate location information for both paired cameras. For the FC-Series AI 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.

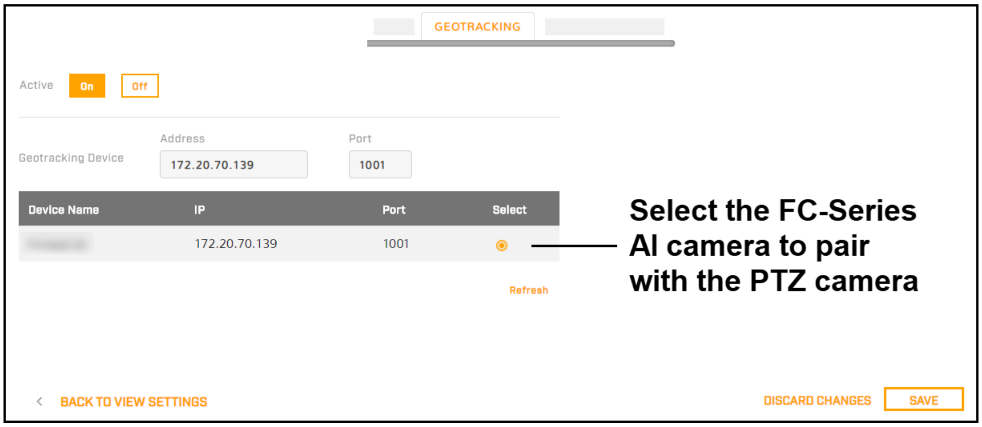
7.1 Pairing with a Quasar 4K IR PTZ, DX-Series, or DM-Series Camera

To pair one of these PTZ cameras with an FC-Series AI 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 FC-Series AI camera to pair with the PTZ camera.



Active ● On ○ Off

Geotracking Device Address: 172.20.70.139 Port: 1001

Device Name	IP	Port	Select
[redacted]	172.20.70.139	1001	●

Select the FC-Series AI camera to pair with the PTZ camera

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

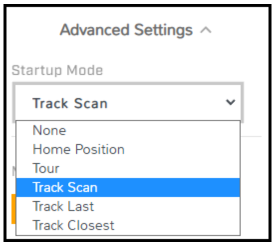
Make sure the FC-Series AI camera’s IP address and port appears next to Geotracking Device.

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**.



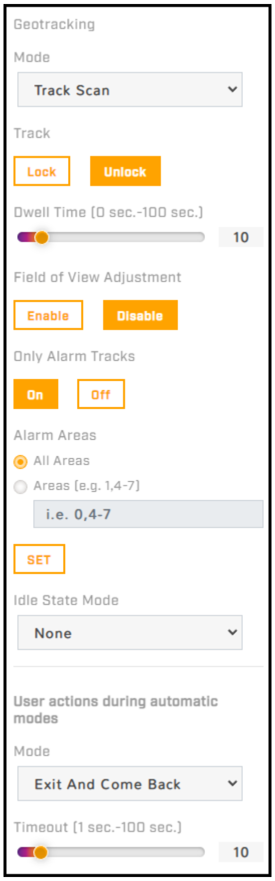
Advanced Settings

Startup Mode: Track Scan

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.



Geotracking

Mode: Track Scan

Track: Lock Unlock

Dwell Time (0 sec.-100 sec.): 10

Field of View Adjustment: Enable Disable

Only Alarm Tracks: On Off

Alarm Areas

● All Areas

○ Areas (e.g. 1,4-7)

i.e. 0,4-7

SET

Idle State Mode: None

User actions during automatic modes

Mode: Exit And Come Back

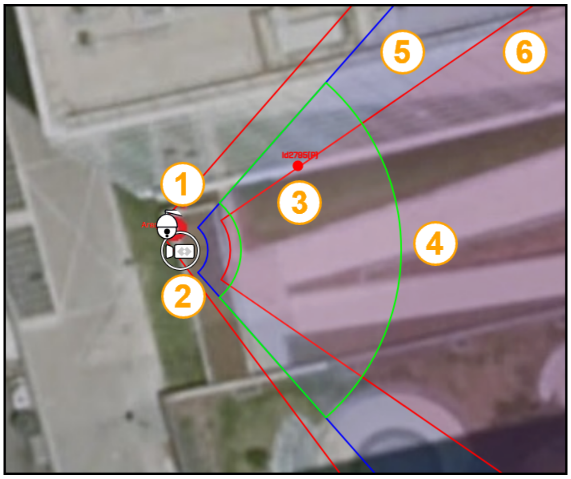
Timeout (1 sec.-100 sec.): 10

- 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 FC-Series AI camera detects the object and provides the geotracking information, the PTZ camera follows the track. When the FC-Series AI 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 FC-Series AI 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 FC-Series AI 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 FC-Series AI camera's Geotracking Page display, with the following overlaid onto a map that has been uploaded and calibrated:

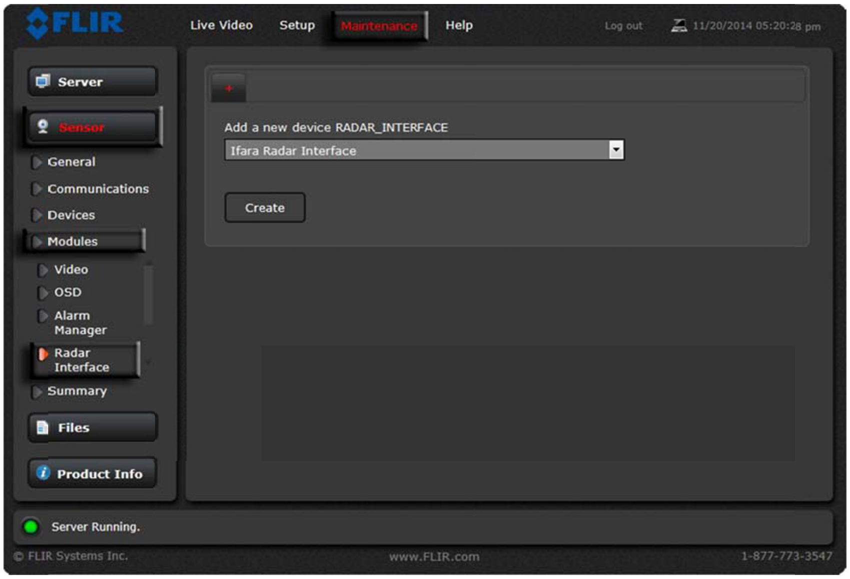
1. a supported FLIR Security PTZ camera
2. the FC-Series AI camera being accessed / configured (circled)
3. an object detected by the FC-Series AI camera inside a geotracking alarm region
4. FC-Series AI camera VA / geotracking range (green borders)
5. FC-Series AI camera thermal sensor horizontal field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

7.2 Pairing with a PT-Series HD Camera

To pair a PT-Series HD camera with an FC-Series AI 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**.

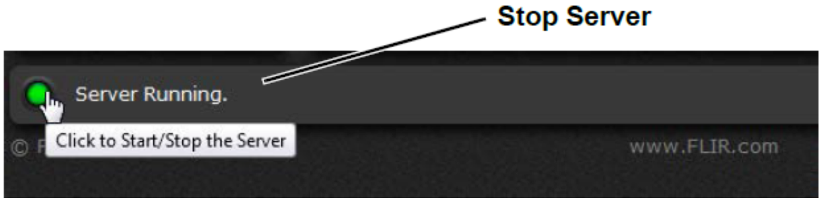


Add a new device RADAR_INTERFACE

Ifara Radar Interface

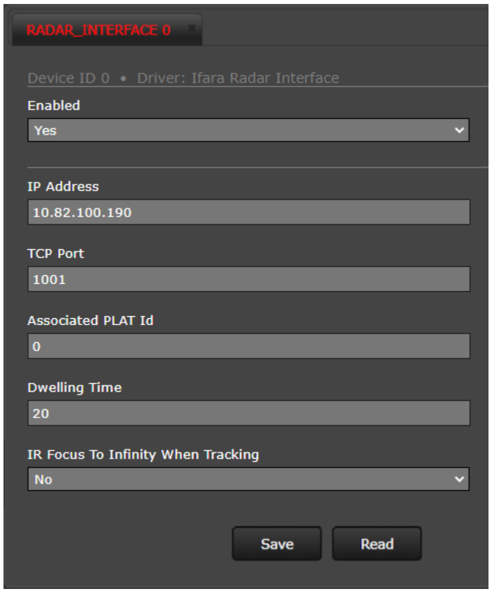
Server Running.

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.



RADAR_INTERFACE 0

Device ID 0 • Driver: Ifara Radar Interface

Enabled: Yes

IP Address: 10.82.100.190

TCP Port: 1001

Associated PLAT Id: 0

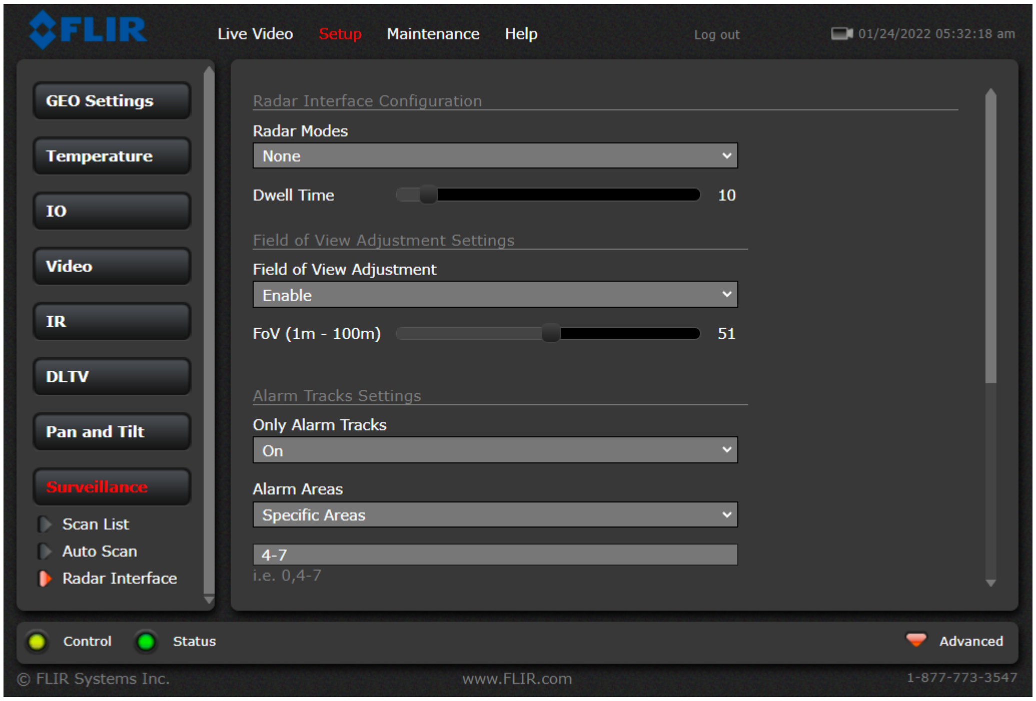
Dwelling Time: 20

IR Focus To Infinity When Tracking: No

5. Enable the interface.
6. Specify:
   - **IP Address—**The FC-Series AI camera's IP address.
   - **TCP Port—**The TCP port number the FC-Series AI camera's Nexus server uses (1001). This is not the port for the FC-Series AI 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**.



Radar Interface Configuration

Radar Modes: None

Dwell Time: 10

Field of View Adjustment Settings

Field of View Adjustment: Enable

FoV (1m - 100m): 51

Alarm Tracks Settings

Only Alarm Tracks: On

Alarm Areas: Specific Areas

4-7
i.e. 0,4-7

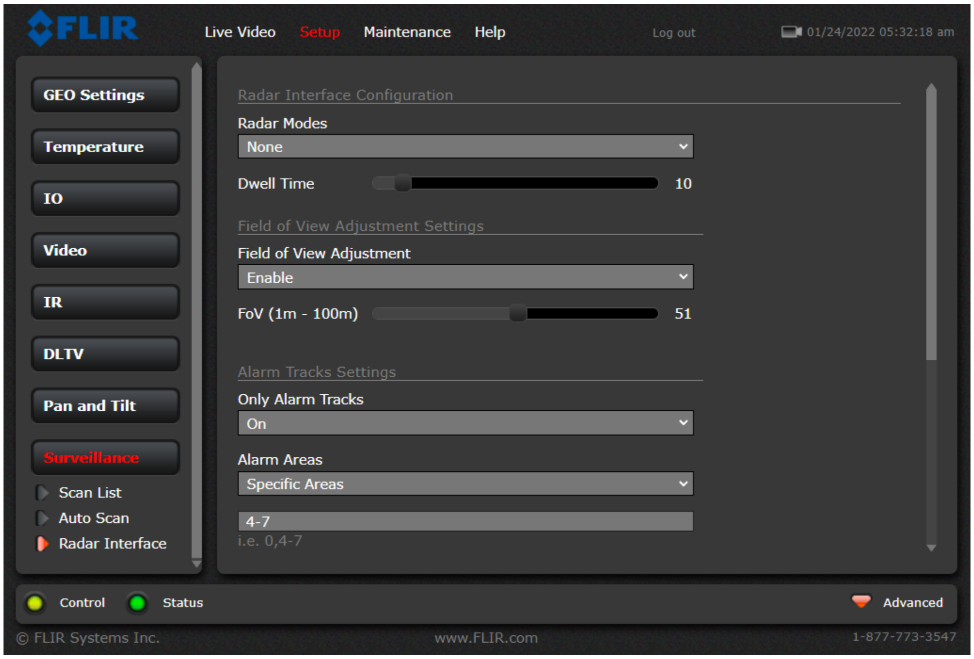
You can:

- 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 FC-Series AI 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 FC-Series AI 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**.



Radar Interface Configuration

Radar Modes: None

Dwell Time: 10

Field of View Adjustment Settings

Field of View Adjustment: Enable

FoV (1m - 100m): 51

Alarm Tracks Settings

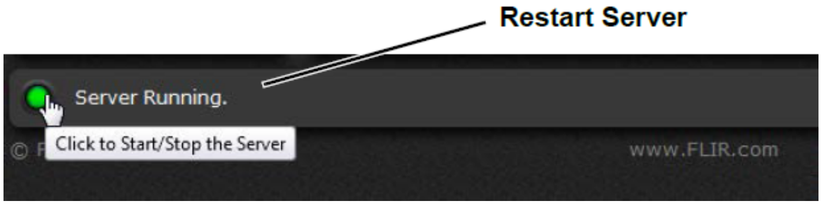
Only Alarm Tracks: On

Alarm Areas: Specific Areas

4-7

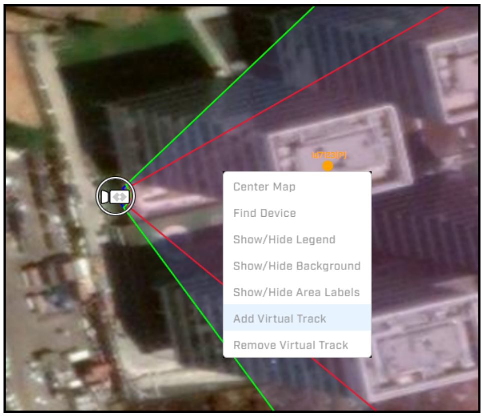
i.e. 0,4-7

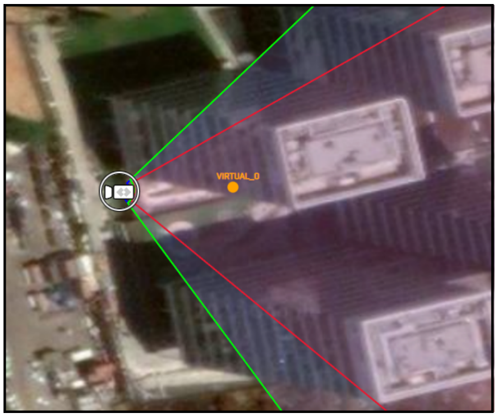
2. Under Special Functions, for Startup Mode, select one of the geotracking radar modes: Track Scan, Engage Last, or Engage Closest.
3. Scroll to the bottom of the page and click **Save**.
4. Restart the camera's server.



7.3 Confirming PTZ Camera Pairing Configuration

1. If you are not logged in to *the FC-Series AI 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 FC-Series AI 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 FC-Series AI camera ignores actual geotracks.

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

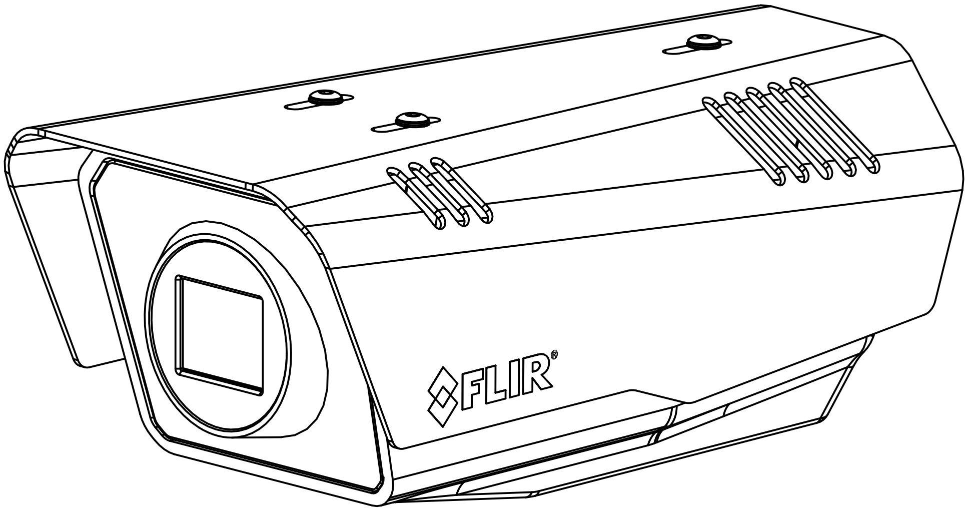
   If it is not, right-click on the FC-Series AI camera detection area display and select **Remove Virtual Track**. Then, check and adjust the PTZ camera's and the FC-Series AI camera's georeference settings.

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

TELEDYNE | Teledyne FLIR
Security Solutions

Installation Guide

FC-Series AI



FC-Series AI Installation Guide - Revision 100 - September 2023

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

The contents of this document are subject to change without notice.

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 2002/96/EC (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 2023	Initial Teledyne FLIR release

Table of Contents

Camera Installation

Image from a standard camera in low light

Image from a thermal camera in the same conditions

1 Camera Installation

This manual describes how to install an FC-Series AI thermal camera, and includes:

- Installation overview
- Mounting the camera and its components
- Connecting the camera
- Bench testing the camera
- Specifications

If help is needed during the installation process, contact the local FLIR service. All installers and integrators are encouraged to take advantage of the training offered by Teledyne FLIR;
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.

1.1 Warnings and Cautions

Warning!

If mounting the FC-Series AI camera on a pole, tower or any elevated location, use industry standard safe practices to avoid injuries.

Caution!

Except as described in this manual, do not open the FC-Series AI 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.

During a heat test in an oven, with the ambient temperature above 70°C, the maximum measured temperature on the enclosure was 72.6°C. The maximum allowed touch temperature limit for accessible parts for very short periods is 70°C.

1.2 References

For information about how to use the camera’s web page to operate and configure the FC-Series AI, see the *FC-Series AI User Guide*.

Documents are available from the Teledyne FLIR website.

1.3 Installation Overview

The FC-Series AI camera is an infrared thermal imaging camera intended for outdoor security applications, and can be installed in a fixed location or on a pan/tilt mechanism. The camera is intended to be mounted on a medium-duty fixed pedestal mount or wall mount commonly used in the security industry. The camera mount must support up to 5.4 lbs (2.5 kg).

Cables may exit from the back of the camera housing through the supplied cable gland or from the bottom of the camera housing when using the concealed cable wall mount (sold separately). A cable gland plug is supplied for the rear of the camera housing when cables are routed using the concealed cable wall mount.

1.3.1 Camera Connection Options

The camera can be installed with an analog or digital (IP) video output (or both). Analog video will require a connection to a video monitor or an analog video matrix switch.

The camera can be powered using Power over Ethernet Plus (PoE+ / IEEE 802.3at-2009) or with a conventional 24 Vac, 12 Vdc, or 24 Vdc power supply. The power supply must have PS2/LPS outputs (18-30 Vac or 12-32 Vdc or PoE 54 Vdc). If the camera is not connected to a PoE+ switch, it can be powered by a PoE+ injector; for example, Teledyne FLIR P/N 4210755. The maximum Ethernet cable run is 100 meters including the PoE+ power supply. Installations using PoE+ power and IP video require only a single Ethernet cable from the camera.

In installations using analog video and conventional power (24 Vac is commonly used in many installations), an RG59U coaxial cable and a three-conductor power cable are installed. Teledyne FLIR recommends installing an Ethernet cable for camera configuration, operation, and troubleshooting. For example, if the camera is mounted on a pole, an Ethernet cable should run at least to the bottom of the pole, for a laptop to be temporarily connected directly to the camera. The FC-Series camera does not support serial communications.

Network Security

The camera supports IEEE 802.1X authentication when connected to a network supporting the following requirements:

- Network device (Authenticator) such as an Ethernet switch configured with 802.1X
- Authentication server supporting TLS

Refer to the user guide for information on how to configure the LAN settings.

Alarm I/O Connections

The camera provides one alarm input connection and one alarm output connection. 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.

PoE+ Power Supply

With PoE+, camera power is delivered to the camera over the Ethernet cable via the camera’s standard RJ45 Ethernet connector. The FC-Series AI camera is a Powered Device compliant with the IEEE 802.3at-2009 standard, known as PoE+ or PoE Plus.

Supplemental Lens Heater

The camera's supplemental lens heater provides lens de-fogging and de-icing in the event of:

- Power interruption that disables the camera for an extended period
- Freezing rain that fully covers the lens and obstructs the image

FC-Series AI cameras are shipped from the factory with the supplemental lens heater disabled. The lens heater can be manually turned on or enabled to run automatically on the Heaters & Fans page in the System Settings section of the camera web page. For more information, see the *FC-Series AI User Guide*.

Important Note

> The windows on the 60 mm lens and the 75 mm lens (FC-610 and FC-608 AI and AI R models) are not thermally conductive. These models are not suitable for installations that would require using the supplemental lens heater.

1.3.2 Camera Accessories

The following accessories are available for purchase from Teledyne FLIR.

- PoE+ power supply (PN 4210755) - For powering a single FC-Series AI camera using PoE+. In addition to PoE+ power and communications, the power supply provides surge protection. It complies with IEEE 802.3at.
- Concealed Cable Wall Mount (PN 4129742) - Includes camera mount gasket and hex wrench for adjusting the ball joint controlling the camera's view angle. The FC-Series AI camera is attached to the mounting arm using the four M5 threaded bottom mounting holes. A cable gland plug is supplied with the camera for the rear of the camera housing when cables are routed using the concealed cable accessory. Refer to Camera Mounting with Concealed Cable Wall Mount, pg. 6.

Concealed Cable Wall Mount

- Pole Mount Adapter Kit (PN 4132982) - Adapter kit that allows the Concealed Cable Wall Mount to be mounted to a pole (75 mm [3 in] min to 180 mm [7 in]; larger pole diameter requires use of customer supplied band clamps)

1.3.3 Supplied Components

The FC-Series AI camera kit includes:

- Fixed camera unit with sunshield and cable gland attached
- Cable gland plug and gland inserts
- Power terminal connector (installed)
- Alarm I/O terminal connector (installed)
- Tools: 3 mm hex key, slotted screwdriver

1.3.4 Additional Supplies

The installer needs the following items as required (specific to the installation):

- Customer-supplied microSD card (up to 512 GB) provides local storage of image files (optional)
- Power supply, 18 Vac to 30 Vac or 12 Vdc to 32 Vdc, if not using PoE+
- Power cable, 3-conductor, shielded, gauge determined by cable length and supply voltage, if used to power the camera

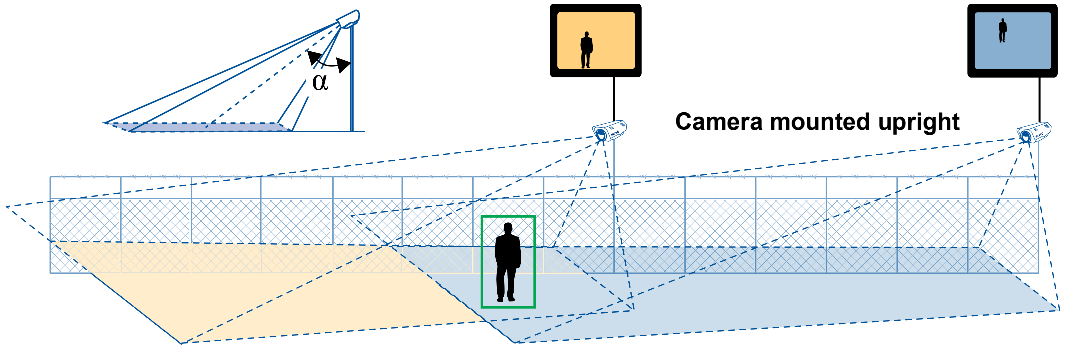
- 6-conductor alarm I/O cable (optional)
- PoE+ power supply or PoE+ switch, if not using Vac or Vdc power
- Cat5e or Cat6 Ethernet cable for PoE+, communications, and IP video
- Coaxial RG-59/U cable with BNC connector at the camera end, if using analog video
- Camera grounding strap, camera mount, electrical hardware, connectors, and tools

Be sure to use cables that fit in the cable gland holes, as described below. Refer to Rear Access Cable Gland Sealing, pg. 13 for more information.

1.3.5 Camera Placement

The FC-Series AI camera can be mounted upright, either on top of the mounting surface. or underneath an overhanging mounting surface such as eaves or an awning. The camera can also be mounted sideways to view a scene such as along a fence line or corridor. Adhere to all local and industry standards, codes, and best practices.

For installations with multiple FC-Series AI cameras with on-board video analytics, the fields of view of cameras should overlap to remove all dead zones in which a camera cannot see a target “head to toe”. The camera’s on-board analytics must be calibrated to detect targets. Refer to the user guide.



- Install the camera at a height of approximately 4 m (13 ft) or more.
- Typically direct the camera towards the ground with a tilt angle α within a range of 45° to 60° while ensuring the field of view includes as little of the skyline as possible.
- Ensure that cameras are mounted on stable mounts with minimal vibrations and maximal resistance to wind.
- The tilt angle (α) is the angle between vertical and the center of the camera field of view.
- Typically direct the camera towards the ground with a tilt angle α of 45° to 60°. Include as little skyline as possible in the field of view.

1.3.6 Camera Mounting for Rear Cable Access

The FC-Series AI camera can be secured to the mount with two in-line 1/4-20 threaded fasteners on the top or bottom of the camera. Alternatively the camera can be mounted with four M5 x 0.8 threaded fasteners to the bottom of the camera. Use Loctite 222 low strength threadlocker for the top mount fasteners (can be used with the bottom mount fasteners also).

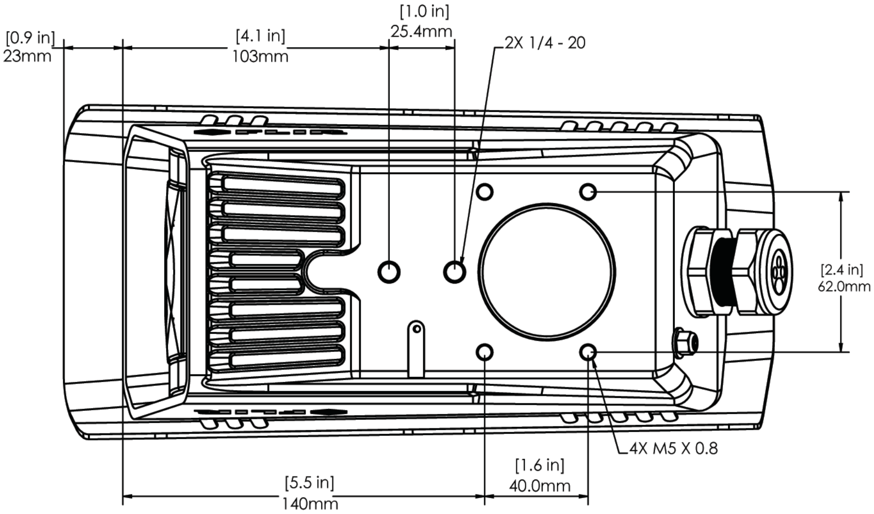


Figure 1-1: Bottom Mounting Holes

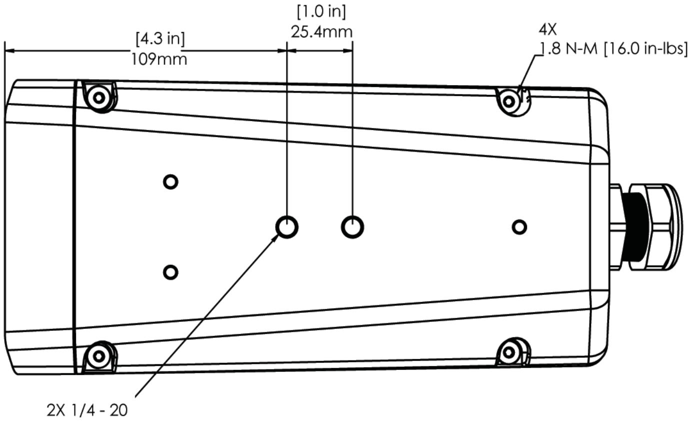


Figure 1-2: Top Mounting Holes

If using two 1/4-20 fasteners in the center of base, the maximum depth of the fastener should not exceed 12.5 mm (0.5 in). If using four M5 x 0.8 fasteners, the maximum depth of the fastener should not exceed 10.0 mm (0.4 in).

If using two 1/4-20 fasteners in the center of top, the maximum depth of the fastener should not exceed 12.5 mm (0.5 in). If the camera is mounted using the top of the camera, the sunshield must be removed.

As the diagram below indicates, be sure to allow adequate space for cable egress behind the gland. This requirement may vary, depending on the installation. Maintain the bend radius per the recommendation of the cable manufacturer. The typical cable bend radius is 50-75 mm (2-3 in).

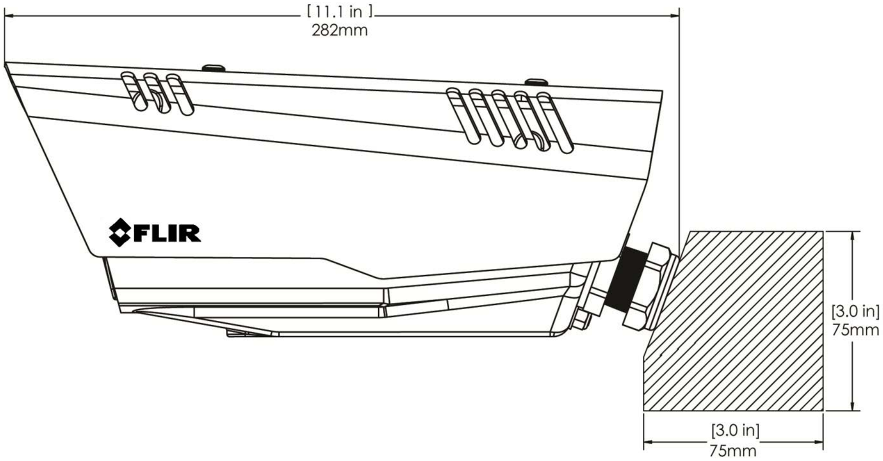


Figure 1-3: Rear Cable Bend Radius

1.3.7 Camera Mounting with Concealed Cable Wall Mount

The FC-Series AI camera can be secured to the optional Concealed Cable Wall Mount with four M5 x 0.8 threaded fasteners to the bottom of the camera. Use Loctite 222 low strength threadlocker for the mount fasteners. Refer to Concealed Cable Mount Accessory, pg. 14 for additional information.

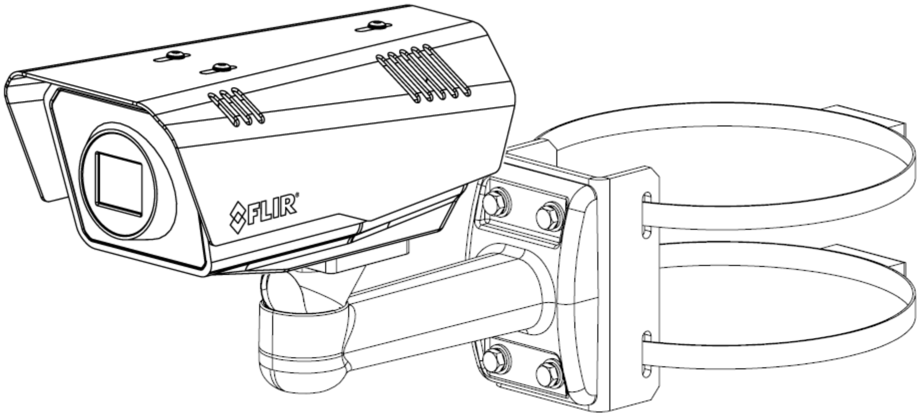


Figure 1-4: Camera with Concealed Cable Wall Mount and Pole Adapter Kit

1.3.8 Sunshield

The camera includes a sunshield that should be used for any installation where the camera is exposed to direct sunlight or precipitation. If the camera is mounted with the top mounting holes, the sunshield is not used. Depending on the needs of the installation, the sunshield can be positioned in the neutral (middle) position, or slightly forward or rearward. To change the position of the sunshield, temporarily loosen the three 3 mm hex screws on top, slide the sunshield forward or backward, and re-tighten the screws.

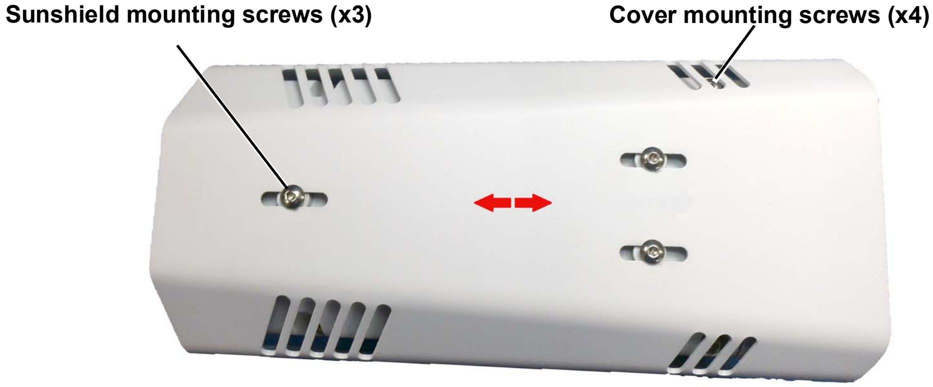


Figure 1-5: Sunshield Mounting

1.3.9 Removing the Cover

To access the electrical connections and install the cables, it is necessary to temporarily remove the top cover of the camera housing. The top cover of the camera is held in place with four 3 mm hex screws. The screws are accessible through slots in the sunshield, so the sunshield does not need to be removed from the top cover.

Use a 3 mm hex key to loosen the four captive screws, exposing the connections inside the camera enclosure. There is a grounding wire connected inside the case to the top cover, as shown. If it (or any of the grounding wires) is temporarily disconnected during the installation, it must be reconnected to ensure proper grounding of the camera.

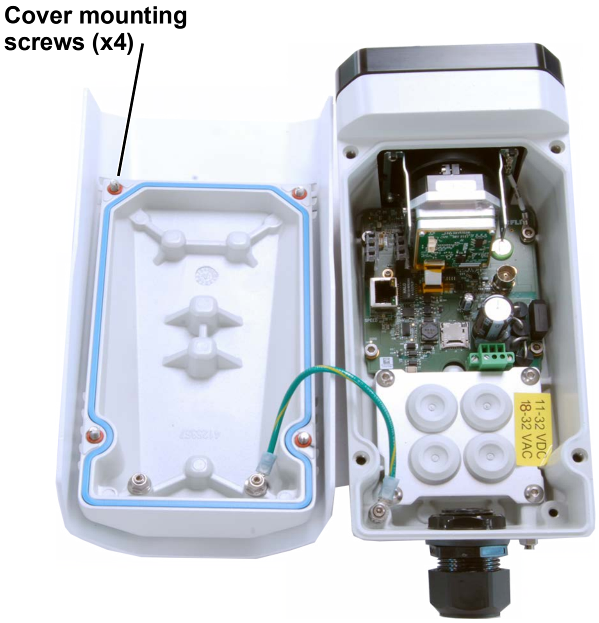


Figure 1-6: Cover Removed (Sunshield Attached)

When replacing the cover, tighten the four 3 mm hex screws to 1.8 n-m (16.0 in-lbs).

Caution!

When replacing the cover, ensure that the ground wire between the cover and the camera body is completely inside the o-ring groove. If the wire is pinched between the cover and body, the camera is not sealed against water ingress and can be damaged.

1.4 Camera Connections

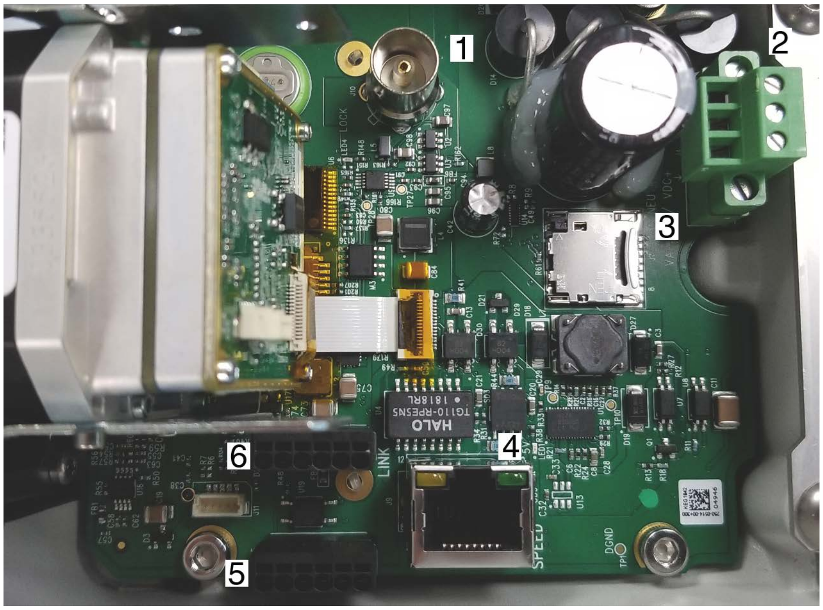


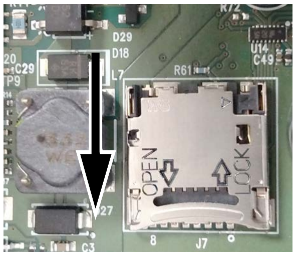
Figure 1-7: FC-Series AI Camera Connectors

Table 1-1: FC-Series AI Camera Connectors

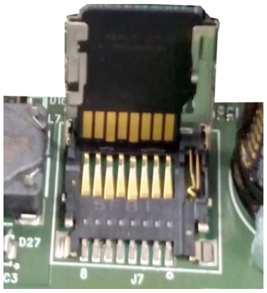
	Connector	Connection
1	BNC	Analog video
2	3-pin power terminal	Vac or Vdc
3	microSD card slot	Local storage of image files up to 512 GB (card not included)
4	Ethernet	PoE+, communications, IP video
5	6-pin terminal J5	Alarm I/O
6	6-pin terminal J3	Not in use

1.4.1 Installing the microSD Card

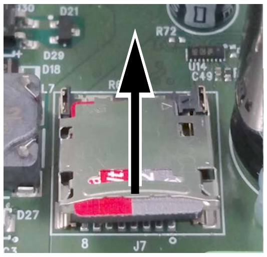
Pull back cage to unlock
Lift edge to open



Insert microSD card



Close cage,
press down and
push forward to lock



1.4.2 Bench Testing

Note

> If the camera is to be mounted on a pole or tower or other hard-to-reach location, it may be a good idea to connect and operate the camera as a bench test at ground level prior to mounting the camera in its final location.

The camera offers both analog video and IP video, and because the camera can be powered by PoE+ or by a conventional power supply, there are several ways to bench test the camera. It is recommended that the installer test the camera using the same type of connections as in the final installation.

Even if using analog video and conventional power in the final installation, it is a good idea to test the IP communications when performing the bench test. If any image adjustments are necessary, they can be done using a web browser over the IP connection, and saved as power-on default settings.

With the camera powered up, analog video can be tested at the BNC connector. Connect the camera to a video monitor and confirm the live video is displayed on the monitor.

If using a conventional power supply, connect the camera to a network switch with an Ethernet cable, and connect a PC or laptop to the switch also.

1.4.3 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.

Notes

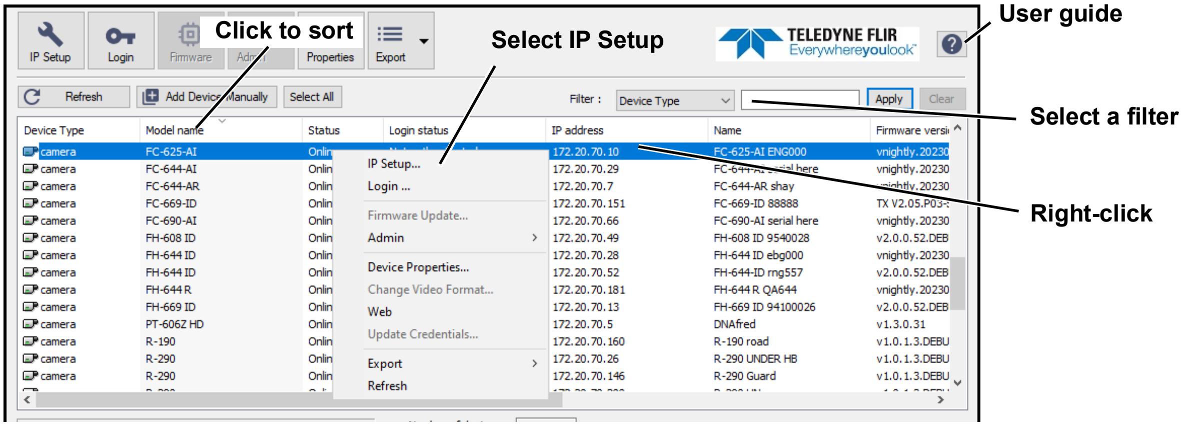
> - Teledyne FLIR recommends using the DNA tool to discover the camera on the network. Version 2.3.0.33 or higher supports FC-Series AI cameras, does not require a license to use, and is a free download from the product's web page For more information about using the DNA tool, including how to configure more than one camera at the same time, see the *DNA User Guide*. While the software is open, click the Help ❓ icon.
> - For information using the camera's web page to configure the camera for networking, see the camera's user guide.
> - For information about using a supported VMS to configure one camera or more than one camera 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.

Configure the Camera for Networking Using the DNA Tool

Step 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.



Device Type	Model name	Status	Login status	IP address	Name	Firmware versi
camera	FC-625-AI	Onlin		172.20.70.10	FC-625-AI ENG000	vnightly.20230
camera	FC-644-AI	Onlin		172.20.70.29	FC-644-AI serial here	vnightly.20230
camera	FC-644-AR	Onlin		172.20.70.7	FC-644-AR shay	vnightly.20230
camera	FC-669-ID	Onlin		172.20.70.151	FC-669-ID 88888	TX V2.05.P03-
camera	FC-690-AI	Onlin		172.20.70.66	FC-690-AI serial here	vnightly.20230
camera	FH-608 ID	Onlin		172.20.70.49	FH-608 ID 9540028	v2.0.0.52.DEB
camera	FH-644 ID	Onlin		172.20.70.28	FH-644 ID ebg000	vnightly.20230
camera	FH-644 ID	Onlin		172.20.70.52	FH-644-ID rng557	v2.0.0.52.DEB
camera	FH-644 R	Onlin		172.20.70.181	FH-644 R QA644	vnightly.20230
camera	FH-669 ID	Onlin		172.20.70.13	FH-669 ID 94100026	v2.0.0.52.DEB
camera	PT-606Z HD	Onlin		172.20.70.5	DNAfred	v1.3.0.31
camera	R-190	Onlin		172.20.70.160	R-190 road	v1.0.1.3.DEBU
camera	R-290	Onlin		172.20.70.26	R-290 UNDER HB	v1.0.1.3.DEBU
camera	R-290	Onlin		172.20.70.146	R-290 Guard	v1.0.1.3.DEBU

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.

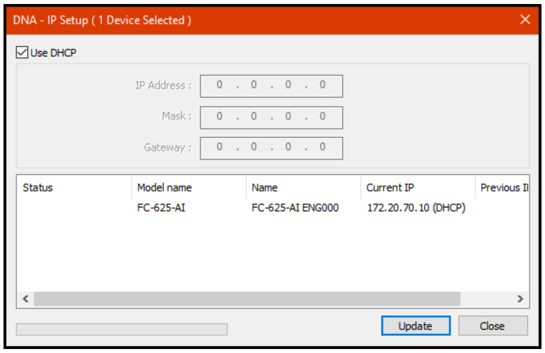
In the DNA Discover List, verify that the camera's status is *Online* and *Authenticated*.

Step 2 Change the camera’s IP address.

Right-click on 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**.


DNA - IP Setup (1 Device Selected)

☑ Use DHCP

IP Address : 0 . 0 . 0 . 0

Mask : 0 . 0 . 0 . 0

Gateway : 0 . 0 . 0 . 0

Status	Model name	Name	Current IP	Previous I
	FC-625-AI	FC-625-AI ENG000	172.20.70.10 (DHCP)	

1.4.4 Analog Video Connection

The analog video connection of the camera is a BNC connector. The video cable used should be rated as RG-59/U or better to ensure a quality video signal. Connect the shield of the external coaxial cable to the building ground.

Note

Insert the cables through the cable glands on the enclosure before terminating and connecting them. In general, terminated connectors will not fit through the cable gland. If a terminated cable is required, it is possible to make a clean and singular cut in the gland seal to install the cable.

1.4.5 Connecting Power

The camera can be powered with a conventional Vac or Vdc power supply, rather than PoE+. Prior to making any connections, ensure the power supply or circuit breaker is switched off.

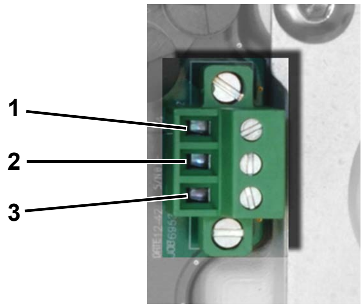
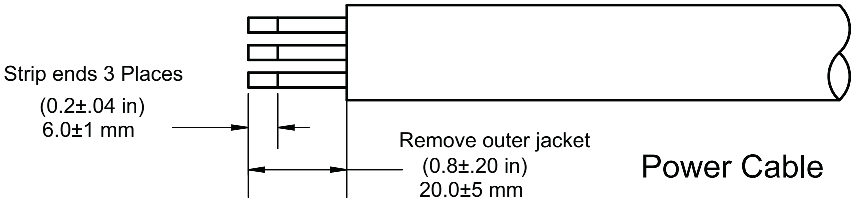


Table 1-2: Power Connections

1	Chassis
2	Vac1 or Vdc –
3	Vac2 or Vdc +

Figure 1-8: Power Connector

The power cable supplied by the installer must use wires that are sufficient size gauge for the supply voltage and length of the cable run to ensure adequate current carrying capacity (18 AWG recommended for most installations). Always follow local building/safety codes.



Note

The terminal connector for power connections will accept 16 AWG to 24 AWG wire size.

The power connector plug may be removed for cable installation. After the plug is reattached to the board, re-tighten the screw terminals.

The camera itself does not have an on/off switch. Generally, the FC-Series AI camera can 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 powered on and operating.

1.4.6 Alarm I/O Connections

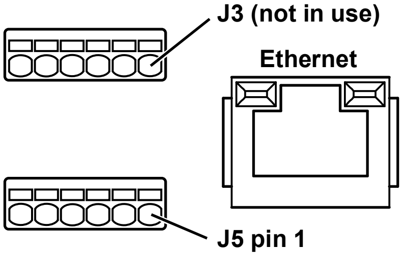


Figure 1-9: Alarm I/O and Ethernet Connectors

Input—When the camera senses an external switch closure that completes the circuit between J5 pins 4 and 5, an input signal is generated for alarm management. For information about how to configure alarms, see the user guide.

Output—Accessory connector J5 pins 2 and 3 connect to a switch in the camera to complete the circuit for the receiving device. When open, the resistance between pins 2 and 3 is greater than 100 K ohm. When closed, the resistance between pins 2 and 3 is less than 200 ohm. The maximum recommended peak voltage between the pins is 6 volts. The maximum recommended current allowed between the pins is 30 mA (0.03 A).

By default, the alarm I/O circuits are configured for normally open switches. For information about configuring an alarm for a normally closed switch, see the user guide.

The terminal plug supplied for alarm I/O connections can be either a fast-connect, spring-cage and pierce contact; or it can a push-in spring contact.

The push-in spring contact accepts 20 - 24 AWG conductors. Strip conductor ends to 6 mm.

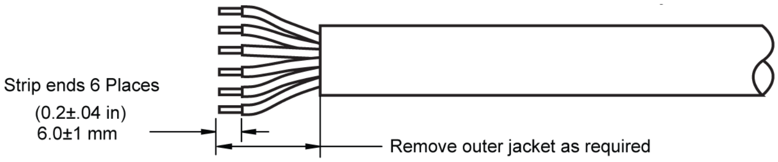


Figure 1-10: Alarm I/O Cable

The spring-cage and pierce contact accepts 22 AWG to 24 AWG, stranded conductors with a 1.6 mm maximum diameter including insulation. Do not strip insulation from conductors.

Table 1-3: Alarm I/O Connections - J5

Pin	Connection	Notes
1	Chassis ground	
2	Alarm out	When the camera sends an output signal, an external voltage on one pin is applied to the other pin.
3	Alarm out	
4	Alarm in (Digital ground)	When these pins are connected externally, the camera reads this as an input signal.
5	Alarm in (+5V)	
6	Chassis ground	

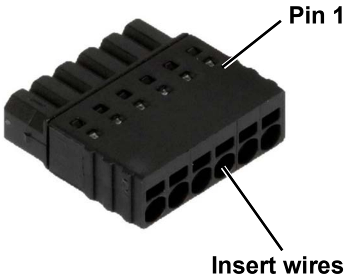


Figure 1-11: Six-Pin Terminal Plug (Push-In Spring Contact)

Caution!

J5 pins 4 and 5 must not be connected to outside voltages or power sources. Pin 5 must not be connected to chassis ground. While protection for static discharge has been placed on these pins, care should be used when making connections to avoid damage to the camera.

1.4.7 Ethernet

Connect a shielded Cat5e or Cat6 Ethernet cable to the RJ45 connector. If using PoE+ to supply power to the camera, connect the other end of the cable to a PoE+ switch or PoE+ injector. Otherwise, connect the cable to a network switch.

1.4.8 Camera Grounding

The unit is intended for outdoor installation. Ensure the camera is properly grounded. Failure to properly ground the camera can permanently damage the camera.

Permanently connect the ground stud on the back of the camera to PE (protective earth) using a 12 AWG (4mm^2) PE conductor. A skilled individual is required to install a PE conductor to the ground of the building.

If, during installation, you disconnect any ground connections inside the camera, reconnect them prior to closing the camera.

1.4.9 Rear Access Cable Gland Sealing

Proper installation of cable sealing gland and use of appropriate elastomer inserts is critical to long-term reliability. Cables enter the rear of the camera mount enclosure through a liquid-tight compression gland.

Table 1-3: Rear Exit Cable Min/Max Dimensions

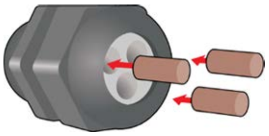
Cable	Min	Max
Power (three-conductor), Ethernet, accessory cables	4.5 mm [0.178 in]	5.2 mm [0.205 in]
RG 59 video cable	5.3 mm [0.209 in]	6.2 mm [0.244 in]

Leave the gland nut loosened until all cable installation has been completed, and ensure the manufacturer’s recommended cable bend radius is observed within the enclosure. Do not forget to tighten the cable gland seal nut to ensure a watertight seal and provide strain relief for cables.

Cable Gland Seal Inserts

The FC-Series AI camera is shipped with a single 3/4” NPT cable gland attached. The gland includes a sealing washer and is secured to the camera with nuts on the inside and on the outside of the enclosure. A gland seal insert provides four holes for Ethernet, power, alarm I/O, and RG-59/U analog video cables. Route cables through the holes so that they line up with the corresponding connectors inside the camera.

Plug any hole not used for cables with one of the supplied hole plugs.



Note

> Insert the cables through the cable glands on the enclosure before terminating and connecting them. In general, terminated connectors will not fit through the cable gland. If a terminated cable is required, make a clean and singular cut in the gland seal to install the cable into the gland seal.

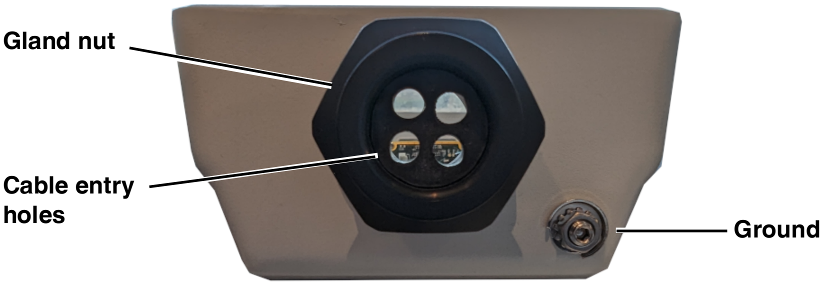


Figure 1-12: Cable Routing

To ensure a water tight seal when using the supplied rear cable gland, cable dimensions must be within the minimum and maximum as described in Table 1-3.

1.5 Concealed Cable Mount Accessory

Do not route cables through the bottom of the camera unless the concealed cable wall mount (PN 4129742) is used. The wall mount is specifically designed for the camera and allows the opening to seal properly. When using the concealed cable wall mount, cable dimensions must be within the minimum and maximum as described in Table 1-4.

Table 1-4: Cable Min/Max Dimensions using Concealed Cable Wall Mount (PN 4129742)

Cable	Min	Max
Power (three conductor), Ethernet, alarm I/O cables	4.5 mm [0.178 in]	10 mm [0.394 in]
RG 59 video cable	5.3 mm [0.209 in]	10 mm [0.394 in]

Proper installation of the seal plate and panel mount gland seals is critical to long-term reliability. Cables enter the bottom of the camera enclosure through the seal plate and panel mount glands. Be sure to insert each cable through its panel mount gland on the seal plate before terminating them (connectors will not fit through the gland). Ensure the manufacturer’s recommended cable bend radius is not exceeded within the enclosure.

Mount the Camera Using the Concealed Cable Wall Mount

Step 1 Use a 3 mm hex key to loosen the four captive screws and remove the top cover as described above.

Step 2 Remove the rear cable gland and replace it with the cable gland plug. You will use the gasket and nut that were removed with the cable gland.

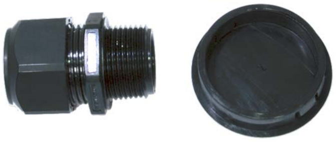


Figure 1-13: Removed Parts

Step 3 Use a 3 mm hex key to loosen the four captive screws and remove the seal plate, o-ring, and plug.

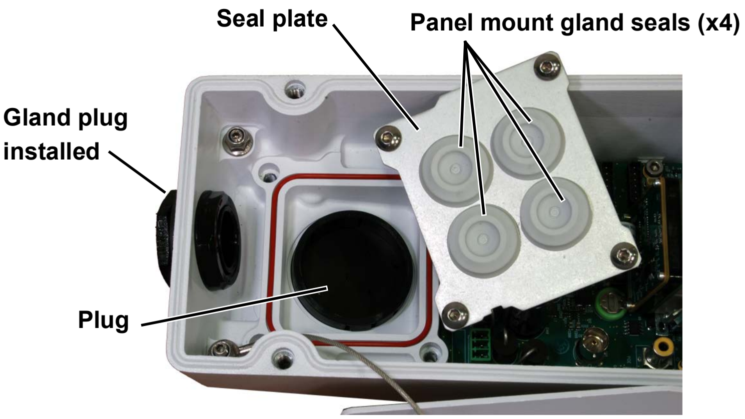


Figure 1-14: Seal Plate Removed

Step 4 Using four M5 x 16mm screws, attach the wall mount to the wall, and then pull the cable(s) through the mount. Cut a small cross-slit in the black mount gasket and push the cable(s) through the gasket. Pull the cable(s) through the opening in the bottom of the camera. A single Ethernet cable is shown in the images.

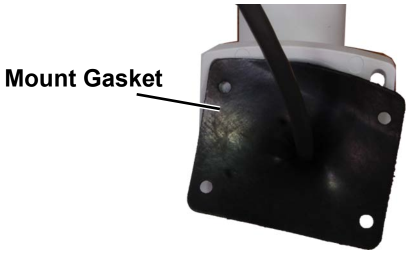


Figure 1-15: Camera Mount

Step 5 Secure the camera to the mount using the four M5 x 0.8 threaded fasteners on the bottom of the camera. Use Loctite 222 low strength thread locker for the mount fasteners.

Step 6 As needed, clean the o-ring and the o-ring groove in the bottom of the camera using isotropy alcohol and press the o-ring into its groove.

Step 7 For each cable, punch a hole in the center of a gland seal from the top using the 3 mm hex key. Insert the cable from the bottom though the hole.

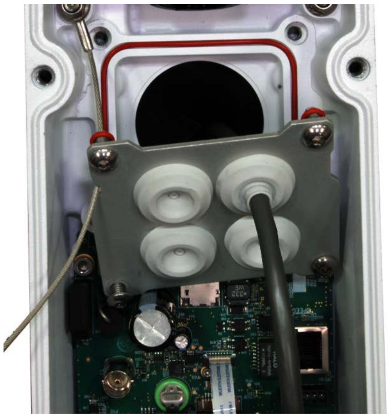
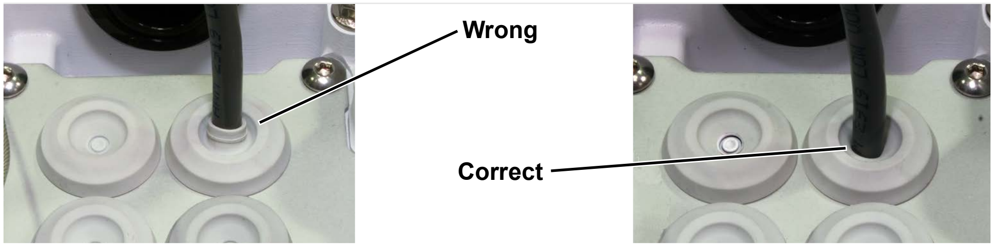


Figure 1-16: Cable through Seal Plate

Step 8 Place the gland plate back into position and tighten the four 3 mm captive screws using a torque value of 1.8 n-m (16.0 in-lbs).

Step 9 Check the length of each cable to ensure an appropriate bend radius and terminate the cable. Connect the cables as indicated in FC-Series AI Camera Connectors, pg. 8.

Step 10 Push the cable back through the gland seal so that the seal extends down not up, as shown in the illustration below.



Caution!

When replacing the cover, make sure the ground wire between the cover and the camera body is completely inside the o-ring groove. If the wire is pinched between the cover and the base, the camera will not be sealed against water ingress and could be damaged.

Step 11 Ensure that any ground wire that was removed during installation is reconnected. Replace the cover and tighten the four 3 mm hex screws to 1.8 n-m (16.0 in-lbs).

Step 12 Using the hex key included with the concealed cable mount, loosen the ball joint on the bottom of the mount, position the camera as required, and then re-tighten the ball joint.

1.6 Camera Specifications

Thermal Sensor & Optics	Array Format	640 x 512 (17 µm pixel pitch)
	Detector Type	Long-life, uncooled VOx Microbolometer
	Spectral Range	7.5 to 13.5 µm
	Focus	Athermalized, focus-free
	Sensitivity	AI models: <25 mK @ 25°C (77°F) for f/1.0
		AI - R models: <35mK @ 25°C (77°F) for f/1.0
	Model	**Field Of View (Focal Length - F/#)**
	FC-690 - AI & FC-690 - AI - R	90° × 69° (7.5 mm - F1.2)
	FC-669 - AI & FC-669 - AI - R	69° × 56° (9 mm - F1.4)
	FC-644 - AI & FC-644 - AI - R	44° × 36° (13 mm - F1.0)
	FC-632 - AI & FC-632 - AI - R	32° × 26° (19 mm - F1.0)
	FC-625 - AI & FC-625 - AI - R	25° x 20° (25 mm - F1.1)
	FC-617 - AI & FC-617 - AI - R	17° × 14° (35 mm - F1.1)
	FC-610 - AI & FC-610 - AI - R	10° × 8.2° (60 mm - F1.2)
	FC-608 - AI & FC-608 - AI - R	8.6° × 6.6° (75 mm - F1.1)
Temperature Measurement (AI - 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	Composite Video	Hybrid system with IP & analog video, dynamic NTSC or PAL settings—switchable using DNA or the camera's web page
	Analog Video Output	1Vp-p (PAL or NTSC), 1 x BNC 75 Ω
	Video Compression	Two independent channels of H.264 / H.265, or M-JPEG
	Streaming Resolution	640 × 512
	Thermal Image Settings	Auto AGC, Brightness, Contrast, Sharpness, Gamma, Smart Screen Optimization
	Thermal AGC Region of Interest (ROI)	Default, presets, and user definable to ensure optimal image quality on subjects of interest
	Analytics Management	Web-based configuration and management; masking of analytic detection areas, adjustable sensitivity, automatic responses, remote I/O control
	Analytics Features	Region entrance/intrusion detection, crossover/fence trespassing, CNN classifier
	Image Uniformity Optimization	Automatic flat-field correction (FFC) - thermal and temporal triggers
	microSD Card Snapshot Capture	Support up to 512 GB (sold separately)
System Integration	Ethernet	10/100 Mbps
	External Analytics Compatible	Yes
	Control Input/Output Network	1x dry contact in; 1x relay out (rated load 0.025 A@ 5 VDC)
	APIs	NEXUS SDK; NEXUS CGI; ONVIF Profiles S, G, T
Network	Supported protocols	IPV4, HTTP, HTTPS, UPnP, DNS, NTP, RTSP, TCP, UDP, ICMP, IGMP, DHCP, ARP, IEEE 802.1X

<table>
<tr><td rowspan="12"><b>General</b></td><td rowspan="3">Weight with Sunshield</td><td>2.2 kg (4.75 lb): all models except
FC-610 - AI & FC-610 - AI - R
FC-608 - AI & FC-608 - AI - R</td></tr>
<tr><td>FC-610 - AI & FC-610 - AI - R: 2.4 kg (5.25 lb)</td></tr>
<tr><td>FC-608 - AI & FC-608 - AI - R: 2.5 kg (5.5 lb)</td></tr>
<tr><td rowspan="3">Weight without Sunshield</td><td>1.8 kg (4 lb): all models except
FC-610 - AI & FC-610 - AI - R
FC-608 - AI & FC-608 - AI - R</td></tr>
<tr><td>FC-610 - AI & FC-610 - AI - R: 2.0 kg (4.5 lb)</td></tr>
<tr><td>FC-608 - AI & FC-608 - AI - R: 2.2 kg (4.75 lb)</td></tr>
<tr><td>Dimensions (L x W x H)</td><td>With sunshield: 282 × 129 × 115 mm / 11.1 × 5.1 × 4.5 in
Without sunshield: 259 × 114 × 106 mm / 10.2 × 4.5 × 4.2 in</td></tr>
<tr><td>Input Voltage and Power Consumption</td><td>
<table>
<tr><th>Source</th><th>Heater off</th><th>Heater on @ 100%</th></tr>
<tr><td><b>PoE+ IEEE 802.3at
54 Vdc ⎓ 0.55A</b></td><td>&lt;9 W</td><td>&lt;25 W</td></tr>
<tr><td><b>12 Vdc ⎓ 2.5A</b></td><td>&lt;10 W</td><td>&lt;28 W</td></tr>
<tr><td><b>24 Vdc ⎓ 1.25A</b></td><td>&lt;9 W</td><td>&lt;25 W</td></tr>
<tr><td><b>24 Vac 50/60 Hz 1.5A</b></td><td>&lt;15 W</td><td>&lt; 32W</td></tr>
</table>
</td></tr>
<tr><td>Immunity</td><td>ESD: EN 61000-4-2
RS: EN 61000-4-3; EN 55035 (2017 + A11: 2020); EN 50130-4
EFT: EN 61000-4-4
Surge: EN 61000-4-5
CS: EN 61000-4-6
PFMF: EN 61000-4-8</td></tr>
<tr><td>Cybersecurity</td><td>IEEE 802.1X; TLS / HTTPS; user authentication; access control via firewall; user credentials with policy enforcement; digest authentication</td></tr>
<tr><td rowspan="8"><b>Environmental</b></td><td>IP Rating
(Dust & Water Ingress)</td><td>IP66 &amp; IP67</td></tr>
<tr><td>Operating Temperature Range & Humidity</td><td>-40°C to 70°C (-40°F to 158°F), cold start; 0-90% relative humidity</td></tr>
<tr><td>Storage Temperature Range & Humidity</td><td>-50 °C to 85 °C (-58 °F to 185 °F); 0-95% relative humidity</td></tr>
<tr><td>Shock (Operational)</td><td>MIL-STD-810G, Method 516.6</td></tr>
<tr><td>Shock (Transportation)</td><td>IEC 60068-2-27:08</td></tr>
<tr><td>Vibration</td><td>IEC 60068-2-64:08</td></tr>
<tr><td>Vandalism</td><td>IK10 (except lens and windows)</td></tr>
<tr><td>De-icing / Anti-icing</td><td>MIL-STD 810F:00 + Notice 1:00 + Notice 2:02 + Notice 3:03 (excluding FC-610 and FC-608)</td></tr>
<tr><td rowspan="4"><b>Warranty & Regulatory</b></td><td>Emission</td><td>FCC 47 CFR Part 15, Subpart B, Class A (within CISPR 22:2008 Class A limits); EN55032 Class A</td></tr>
<tr><td>Safety</td><td>EN 62368-1: 2014 + A11: 2017 (pending)</td></tr>
<tr><td>Compliance</td><td>CE Marked
RoHS III Directive 2015/863/EU
WEEE Directive 2012/19/EU</td></tr>
<tr><td>Warranty</td><td>Camera: 3 years / Sensor: 10 years</td></tr>
</table>