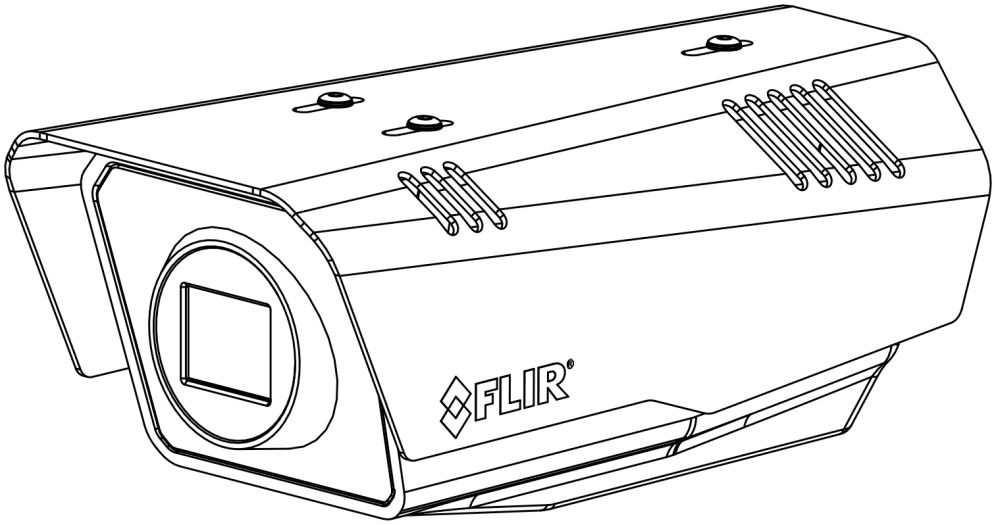
User Guide

FC-Series AI

FC-Series AI-R



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
110	August 2024	Teledyne FLIR release of firmware v3.0.0.10

Product Registration and Warranty Information

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

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

Table of Contents

Table of Contents

1 Camera Overview

This user guide is valid for firmware version 3.0.0.10 or later.

FC-Series AI cameras enable intrusion detection for perimeter security through edge AI analytics. Built-in artificial intelligence (AI)-optimized video analytics (VA) with deep neural network (DNN) technology can do the following:

- Detect threats at high and low speeds.
- Minimize false alarms.
- Minimize daily operations costs.
- Incorporates 3D optimized AI model that combines DNN and advanced motion detection to offer FLIR Fusion AI intrusion detection video analytics.
- Classifies detected objects as human or vehicle. Vehicle detection applies to cars, vans, small trucks and vehicles up to the size of 15m. Larger vehicles such as long trailers, forklifts, and heavy vehicles with special shapes, such as construction vehicles will not be detected nor filtered.
- Includes thermal video AI, which can be configured for tripwires, intrusion, and loitering detection areas.

You can pair one or more FC-Series AI cameras with a FLIR Security PTZ camera that supports geotracking.

The FC-Series AI-R camera provides radiometry that can be used along with intrusion detection.

When the camera is connected to an IP network, it functions as a server, providing services such as:

- Camera control.
- Video streaming.
- 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
- MJPEG
- 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 Guide*, which is available from the product page on the Teledyne FLIR website.

Related Documentation

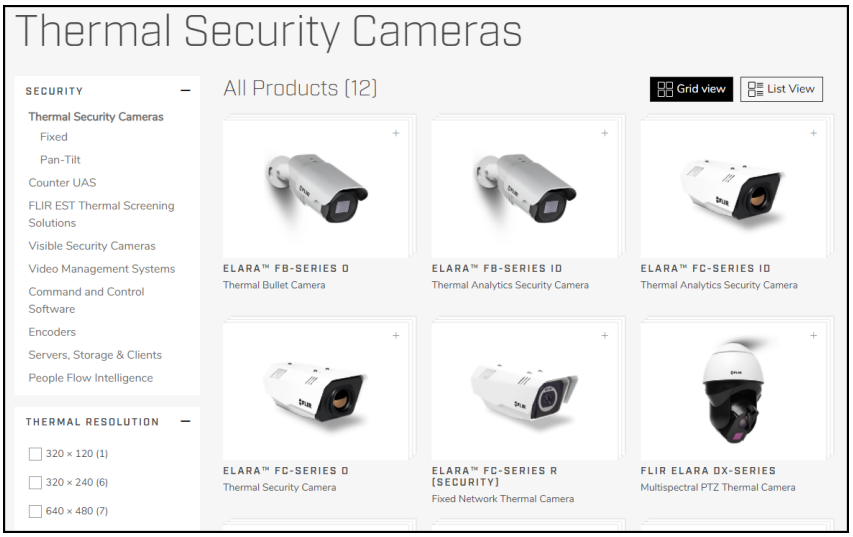
- *FC-Series AI Quick Connect Guide*
- *FLIR Security Edge Devices Accessory Guide*
- *FLIR Security PT-Series HD Pairing Configuration Guide*
- *DNA User Guide (see Accessing Product Information from the Teledyne FLIR Website)*

2 Accessing Product Information from the Teledyne FLIR Website

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

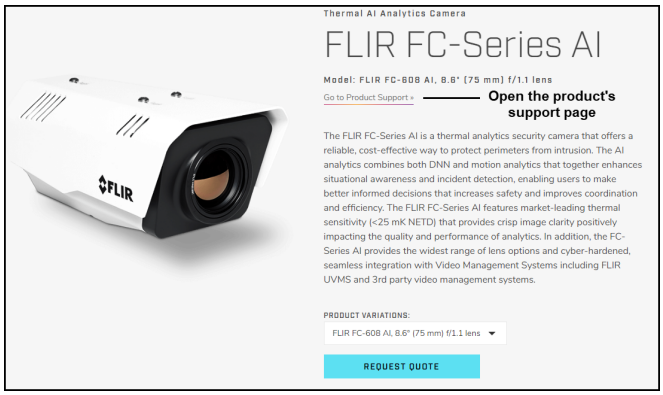
To access product information from the Teledyne FLIR website:

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



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.



FC-Series AI Product Details Page

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

FC-Series AI Product Support Page

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

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:
   a. 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.

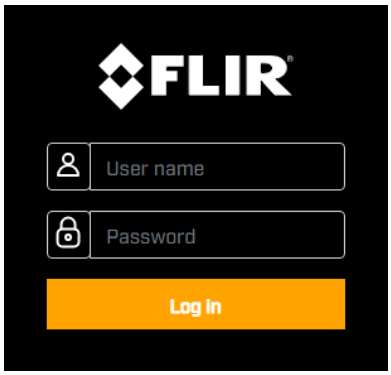
      Download the DNA tool; unzip the file; and then double-click  to run the tool (DNA.exe). The Discover List appears, showing compatible devices on the VLAN.

   b. 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



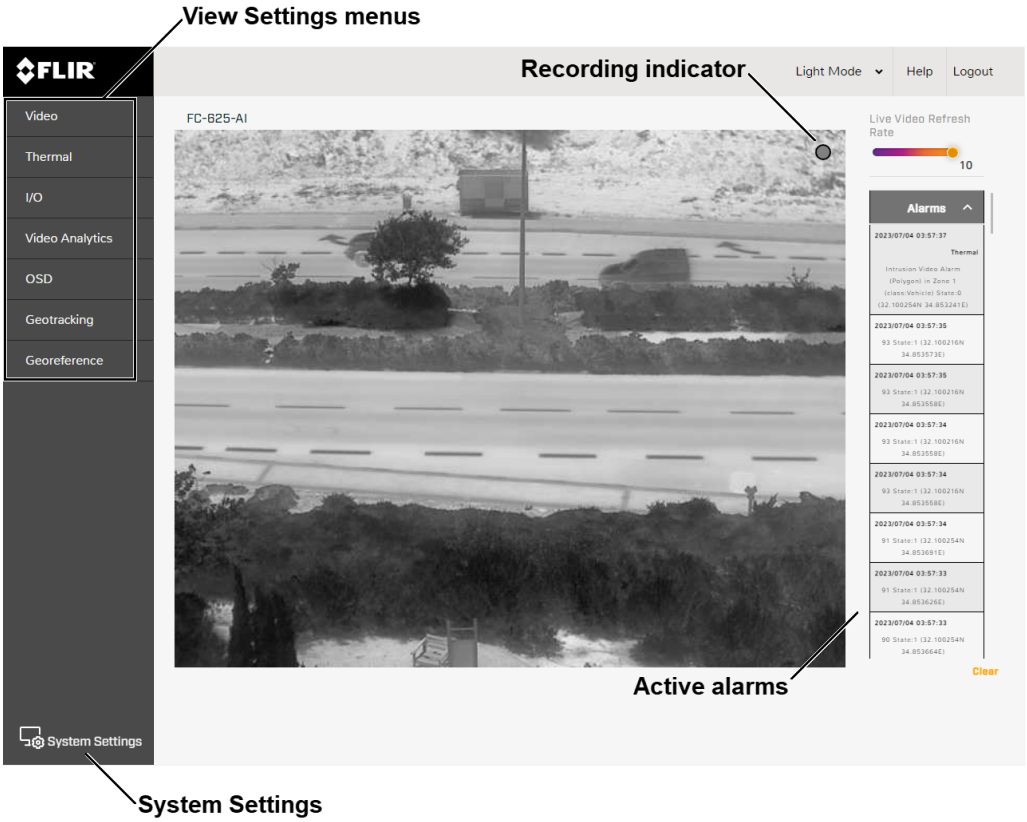
3. When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults:
   a. Specify a new password for the admin user.
   b. Log back in using the new password.
   c. Create a password consisting of:
      i. At least 12 characters.
      ii. At least one uppercase letter.
      iii. At least one lowercase letter.
      iv. At least one number.
      v. Can include the following special characters: |@#~!$&<>+_-.,*?=.

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

The camera's View Settings Home Page appears.

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.



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 settings of the following might not affect the live video:
  - video stream
  - VA tracking overlay
  - on-screen display (OSD)
- 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.

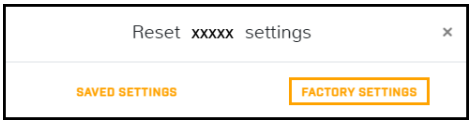
Tip

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.

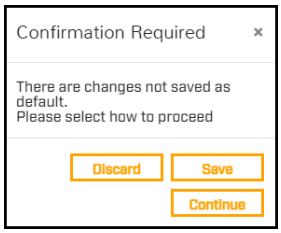
Regardless of whether the camera has already applied changes, to save all changes since the last time these settings were saved, click **Save**. This can include earlier changes that were not saved.



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

Tip

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

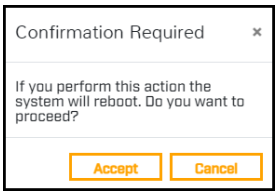


System Settings

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

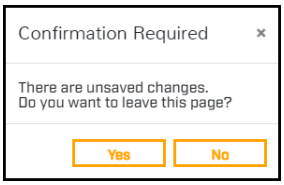
Regardless of whether the camera has already applied changes, to save changes, click **Save**. To discard changes and restore previously saved settings or the factory default settings, click **Discard Changes**.

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



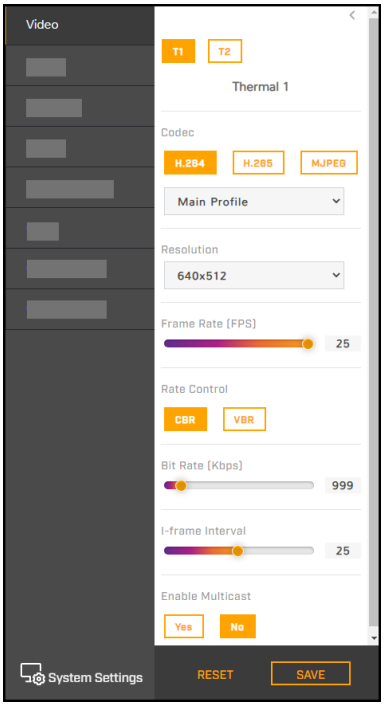
Tip

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



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.



- To change the settings for a particular video stream, click the relevant button (T1 or T2).
- Codec options:
  - H.264
  - H.265
  - MJPEG
- Resolutions available (from the dropdown):
  - 640x512 (default) (VGA)
  - 320x256 (QVGA)
- 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:

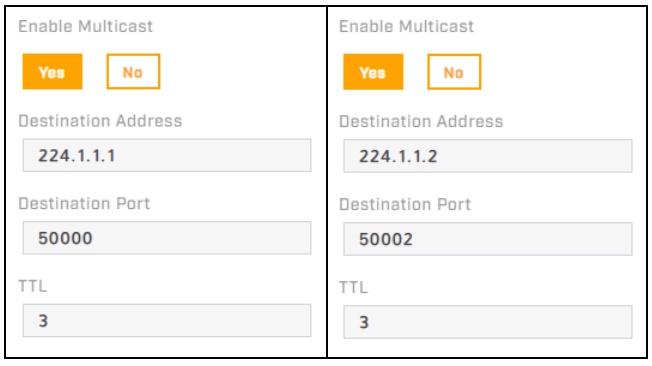
- **Quality** between 0-100.
  - Setting a higher value can increase the video stream's bandwidth requirements.
  - Teledyne FLIR recommends setting a value no higher than 80.
  - If you experience video issues when using MJPEG and high-resolution video, try adjusting the Quality and the resolution settings.

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.



T1 *T2*

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

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

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

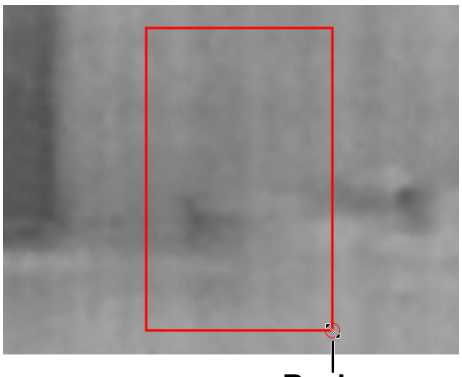
In most installations, changing the default settings of the thermal imager is not necessary. However, in some situations and depending on the scene, modifying one or more parameters can improve the image. Be aware that, when conditions change, you might need to adjust the parameters again. Teledyne FLIR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

AGC ROI

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

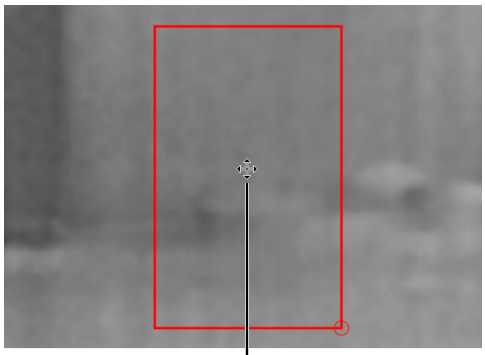
Defining a custom AGC ROI

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



Resize

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



Move

Caution

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

AGC Image Settings

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

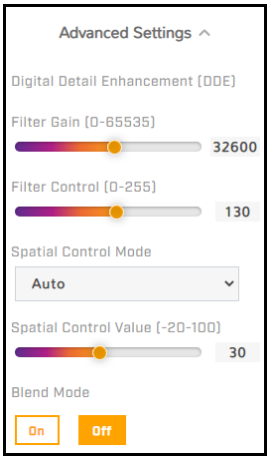
- **Sharpness** (DDE Gain)—Enhances details and/or suppresses fixed pattern noise. Range 0 to 100.
- **AGC Filter**—Determines how quickly a scene adjusts when a hot object appears (or disappears) within the AGC ROI. If set to a low value, when a hot object enters the ROI, the AGC will adjust more slowly 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 VA is enabled for thermal video on the Video Analytics Page, the camera automatically uses the WhiteHot color palette.
- **FFC (Flat-Field Correction)**—To manually trigger FFC, click **Perform FFC**. The shutter for the thermal imager closes and provides a target of uniform temperature, allowing the thermal imager to correct for ambient temperature changes and provide the best possible image. The thermal image momentarily freezes. At regular intervals or when the ambient temperature changes, the camera automatically performs FFC (also known as Non-Uniformity Correction or NUC).

- **Gain Mode** (available on FC-Series AI-R cameras)
  - **Auto—**Camera automatically switches between High Gain Mode and Low Gain Mode according to the maximum temperature detected in the radiometric items (see Radiometry Page (FC-Series AI-R)). If no radiometric items have been configured, the camera remains in High Gain / Low Temperature mode. Teledyne FLIR recommends Auto Gain Mode.
  - **Low** (default)—Camera remains in Low Gain / High Temperature (up to 380°C) Mode. Because it allocates 256 shades over a wider temperature range than in High Gain / Low Temperature Mode, the image can appear to be washed out compared to High Gain Mode. As such, the camera's onboard VA does not function in Low Gain Mode.
  - **High—**Camera remains in High Gain / Low Temperature (up to 150°C) Mode.

Advanced Settings

Caution

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



Digital Detail Enhancement (DDE)

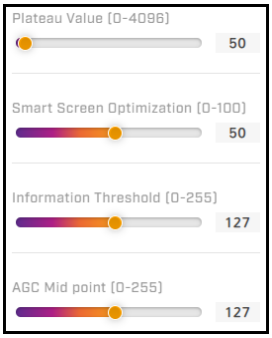
DDE is an advanced, nonlinear image processing algorithm that preserves detail in high dynamic range imagery. The camera enhances detail to match the total dynamic range of the original image, making details more visible. In a high-contrast scene, gain is higher than in a low-contrast scene, allowing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

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

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

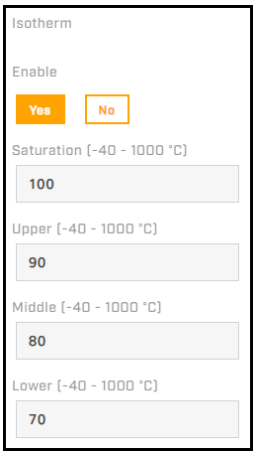
  The algorithm applies gain globally and locally to the low frequency portion of the image. Therefore, filter gain is relative.

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



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

Isotherm (FC-Series AI-R)



When you enable isotherm, the camera:

- Enables an isotherm-specific color palette. The bottom half is composed of gray shades and the upper half is composed of color shades. For example, the WhiteHot-ISO2 color palette:

- Maps pixels:
  - Above the specified Saturation threshold to the top shade of the color palette (255).
  - Between the specified Upper and Saturation thresholds to shades 224-254.
  - Between the specified Middle and Upper thresholds to shades 176-223.
  - Between the specified Lower and Middle thresholds to shades 128-175.
- For each threshold, specify a temperature between -40°C and 1000°C (-40°F and 1832°F). The default values are:

- 100 (Saturation)
- 90 (Upper)
- 80 (Middle)
- 70 (Lower)

Important

The camera’s onboard VA operates on the video signal from the thermal imager. When isotherm is enabled and the camera is using an isotherm-specific color palette for the video, VA is unable to function. Therefore, when enabling isotherm, Teledyne FLIR recommends disabling the analytics on the video.

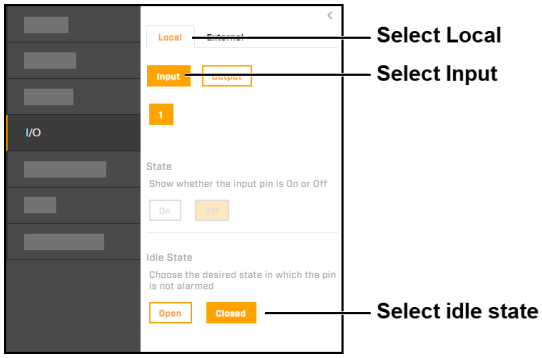
3.6 I/O Page

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

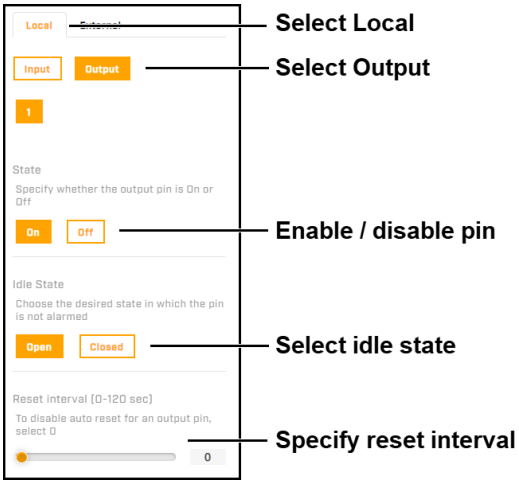
- Configure the camera's local I/O pin.
- Enable and disable the camera's external I/O pins.

Local I/O pins

Input Pin



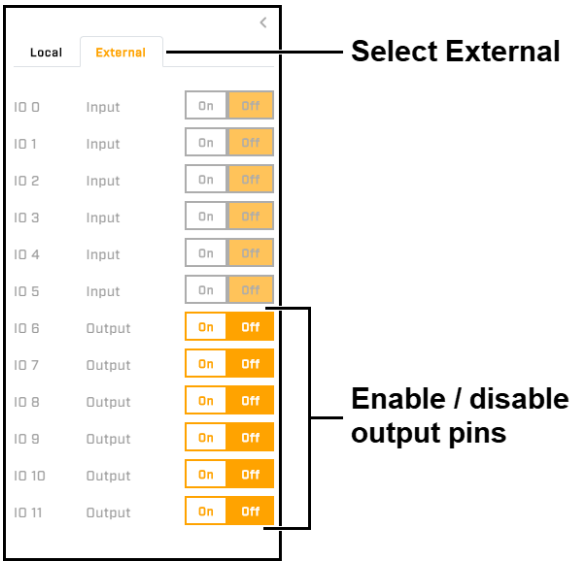
Output Pin



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.



Six Input and Six Output Pins

3.7 Video Analytics Page

The camera's advanced onboard VA:

- Incorporates 3D optimized AI model that combines DNN and advanced motion detection to offer FLIR Fusion AI intrusion detection video analytics.
- Classifies detected objects as human or vehicle. Vehicle detection applies to cars, vans, small trucks and vehicles up to the size of 15m. Larger vehicles such as long trailers, forklifts, and heavy vehicles with special shapes, such as construction vehicles will not be detected nor filtered.
- Thermal video AI can be configured for tripwires, intrusion, and loitering detection areas.

Video Analytics Page

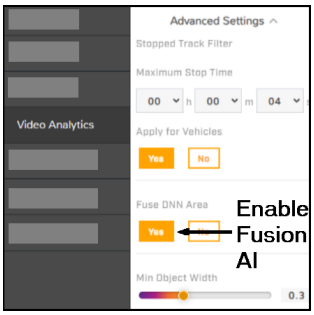
Note

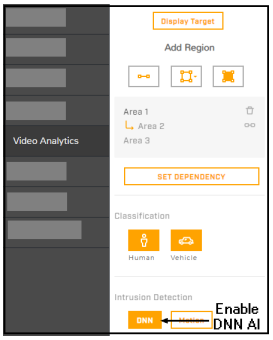
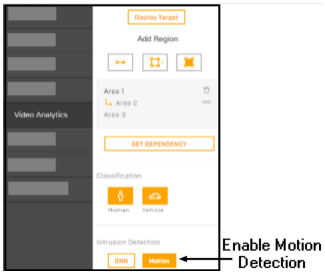
- You have the option of DNN AI, Fusion AI, or Motion detection. Fusion AI = DNN AI + Motion detection.

If you choose Fusion AI after configuring, every intrusion detection region set to DNN AI will change to Fusion AI and the regions set to Motion detection will stay set as Motion detection.

- **Fusion AI** detects upright and discreet human intrusions at short, medium to long range distances. Fusion AI is not recommended for heavy traffic scenes or scenes with dynamic vehicle activity.
- **DNN AI** detects upright human intrusions (same as in FH-ID GA 2.0).
- **Motion detection** detects movements.

Fusion AI requires site specific considerations to deliver desired results. Refer to the recommended guidelines.

Intrusion Detection Setting	Instructions	
Fusion AI	To choose Fusion AI: 1. Go to Advanced Settings. 2. Under Fuse DNN Area, choose Yes.	

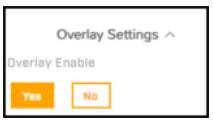
Intrusion Detection Setting	Instructions	
DNN AI	To choose DNN AI: 1. Click on an area or tripwire region. Options for Intrusion Detection display. 2. Choose DNN.	
Motion detection	To choose Motion detection: 1. Click on an area or tripwire region. Options for Intrusion Detection display. 2. Choose Motion.	

Configure the VA:

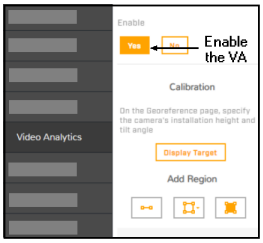
1. Make sure the camera is mounted in its final location and properly aimed. Mounting orientation (tilt) should ideally be at a horizon level close to top of the scene.

2. On the Georeference Page, specify the camera's installation height, tilt angle, and roll angle.

3. Enable the VA overlay.
   a. Click on Overly Settings. The overlay menu opens.
   b. Under Overlay Enable, choose Yes.



4. Enable VA.
   At the top of the page, under Enable, choose Yes.
   By default, VA is disabled. When VA is enabled, the camera automatically uses the WhiteHot color palette (see Thermal Page).



5. Calibrate the VA.
   Check the VA calibration.

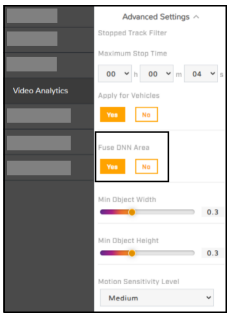
Configure the VA:

6. Choose whether to enable Fusion AI.

   a. Click on Advanced Settings. The Advanced Settings section opens.

   b. Under Fuse DNN Area, choose Yes or No.

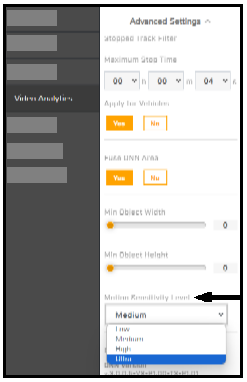
      - If you choose No:
        - You have the choice to enable DNN AI or Motion detection for Intrusion Areas and Tripwires.
        - DNN AI is enabled for Loitering Areas.



7. Specify Motion Sensitivity Level.*

   a. In Advanced Settings, go to Motion Sensitivity Level.

   b. Click on the dropdown menu to choose the appropriate level.



VA Configuration by Type of AI	Applicability
DNN AI	Detects Upright human intrusions
Fusion AI - Low Motion Sensitivity*	Enables detection of discreet human intrusions at very close range
Fusion AI - Medium Motion Sensitivity	Enables detection of discreet human intrusions at an optimal range
Fusion AI - High Motion Sensitivity**	Increases maximum detection distance for upright and discreet human intrusions
Fusion AI - Ultra Motion Sensitivity***	Increases maximum detection distance for upright and discreet human intrusions
** Can handle minor camera movements and vibration* *** Requires the camera to withstand wind gusts* **** Requires the camera to be stable, not move or vibrate* ^ *When Fusion AI is configured, vehicle classification is reliable up to 200m detection distance*	

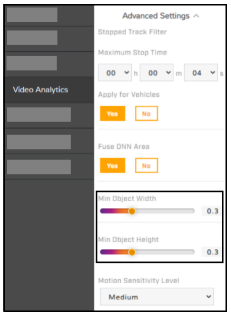
Configure the VA:

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

   a. In Advanced Settings go to Min Object Width and Min Object Height.

   b. Slide the scale to choose the correct value.

   - Use the Teledyne FLIR recommended minimum width and height of 0.3 meters to filter out small animals, such as birds, cats, or rabbits.
   - To filter out larger animals such as dogs, foxes, etc., specify a larger minimum, 0.5 meters width and 0.6 meters height, or larger if necessary.
   - The minimum object width should not exceed 0.5 meters in order to accurately detect human intruders.



Small Animals appear in video stream

- You can reduce nuisance alarms from various animals by applying the recommended object size filter settings shown in the table.

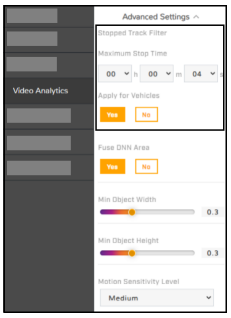
Animal filter setting (Object size)	Width (meters)	Height (meters)
Bird, Rabbit, Small Cat (Default setting)	0.3	0.3
Large Birds (Stock, Swan), Hare, Dog, Wild Cat, Fox, Wolf	0.4	0.5
Large animals	0.5	0.7

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

   a. In Advanced Settings, go to Stopped Track Filter.

   b. Here you can specify the following:

   - Maximum Stop Time—Maximum amount of time, in hours (0-12), minutes (0-60), seconds (0-60), the camera shows the track of a detected object that has stopped moving.
   - Apply for Vehicles—Filters out vehicles that are stopped so that they do not trigger an alarm.



10. Create VA Regions.

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

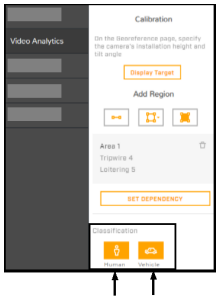
- You can reduce nuisance alarms from various animals by applying the recommended object size filter settings shown in the table.

11. For each region, detect for Vehicle and/or Human.

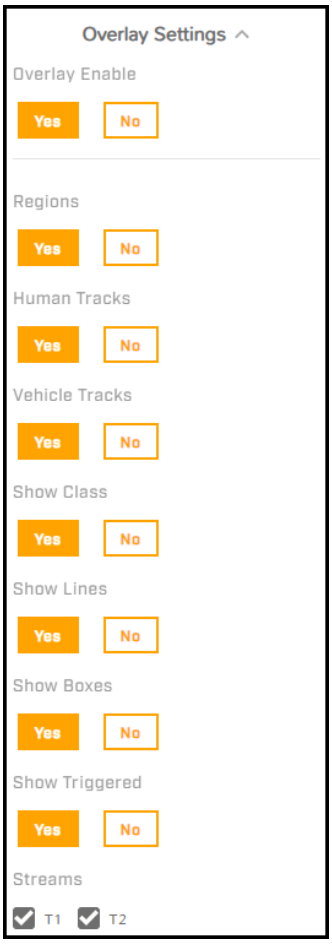
    a. Click on the name of the newly created region.

    b. Under Classification, click on the Human and/or Vehicle icon to activate.

    In the VA tracking overlay, H indicates a detected and classified human; V indicates a vehicle.



12. Enable and configure the VA tracking overlay. Click on Overlay Settings. You can enable or disable the following:



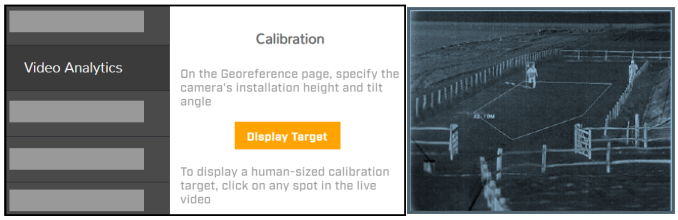
Setting	Description	Comments
Enable	Globally enable or disable the VA overlay.	
Regions	Show intrusion regions, loitering regions, and tripwires.	
Human Tracks	Show detected objects classified as humans.	Enable Show Class, Show Lines, or Show Boxes.
Vehicle Tracks	Show detected objects classified as vehicles.	
Show Class	When tracks are enabled, show the classification of the detected objects: human (H) or vehicle (V).	Enable Human Tracks or Vehicle Tracks.
Show Lines	When tracks are enabled, show the lines for the detected objects according to positions from prior frames; helps visually represent speed and direction.	
Show Boxes	When tracks are enabled, show a box around the track.	
Show Triggered	Show tracks only when they are active; that is, when they are triggering a tripwire, intrusion, or loitering alarm.	Enable Human Tracks or Vehicle Tracks. Enable Show Class, Show Lines, or Show Boxes.
Streams	Enable the VA tracking overlay for individual video streams.	• Does not override the global VA overlay Enable setting above. For the overlay to appear in a stream, the global setting and the stream must be enabled. • The live video on the camera's web page is not the actual video stream. Therefore, enabling the tracking overlay for a stream might not affect the live video.

For information about how to configure the VA for specific situations, see Recommended Guidelines for Optimal Detection Results.

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

3.7.1 Check the VA Calibration

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



Verification of the calibration is important for distinguishing between human and non-human intrusions. Detection human boxes represent the typical height of a human. Verify at different distances (closest and farthest of area or FOV). To verify the calibration, click on the Display Target button.

Checking Calibration

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. Mounting orientation (tilt) should ideally be at horizon level close to top of the scene.
- When far away, if the human box is too small, the virtual horizon needs to be higher, so increase the tilt angle.
- When far away, if the human box is too large, the virtual horizon needs to be lower, so decrease the tilt angle.

3.7.2 Recommended Guidelines for Optimal Detection Results

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

- Install the camera on a stable fixed pole, 6 meters high.
- Start the detection zone 3-5 meters from a fence line or boundary.
- Apply to flat surface terrains with no tall grass or slopes.
- Using Masking Level 2 or 3.
- Do not apply Fusion AI to road facing scenes with dynamic activity, such as frequent vehicle traffic.

Note

Refer to FC-Series AI A&E Specifications for the applicable maximum VA classification distances.

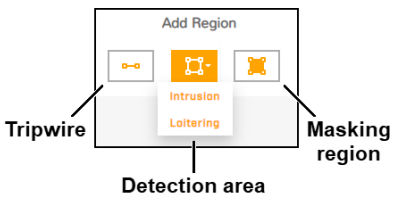
3.7.3 Create VA Regions

Detection Regions:

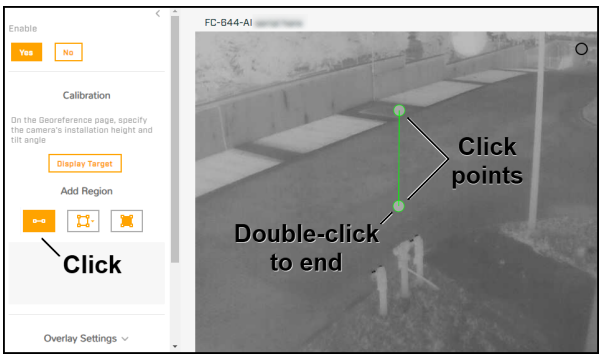
- Detection areas in the video that can classify objects as humans or vehicles including:
  - Tripwires
    - Can be configured to be bidirectional (default) or unidirectional.
  - Intrusion detection areas
    - Can be configured for DNN (default) or Motion detection.
  - Loitering detection areas
    - Specify Loitering time, the time that a person/vehicle will spend in the area until the event triggers.
- Masking regions—Regions of the video image in which VA is disabled and no alarm is triggered.
  - Use masking regions to disable VA so that trees or bushes moving in the wind do not generate events and alarms.
  - A total of eight masking regions can be created.

To create a region:

1. Under Add Region, click the appropriate icon to create:
   a. Tripwire
   b. Detection area
      i. Click on the detection area dropdown. Two options appear - Intrusion and Loitering.
   c. Masking region

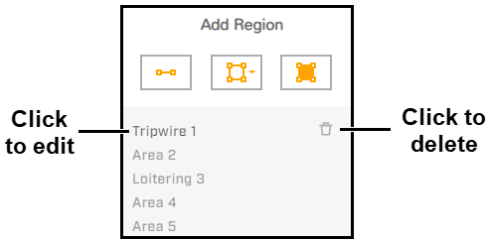


2. Specify each point of the region by clicking and releasing on the live video image.
   a. Do not click and drag.
   b. Do not draw one region line or border over another.
   c. You can create:
      i. Up to two loitering detection areas.
      ii. Up to eight tripwires or intrusion detection areas.
   a. For each region, the maximum number of points is 16.



Creating a Tripwire

3. To finish creating the region, double-click on the last point.
4. To cancel creating a region, press **Esc**.
5. 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.
   a. To move or adjust:
      i. Region points
      ii. Tripwires
      iii. Entire region
   b. Click and drag:
      i. Point
      ii. Line
      iii. Border
   c. To delete a region, click the trash icon.

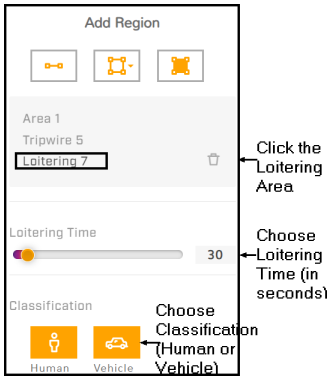


Configure the Detection Regions:

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

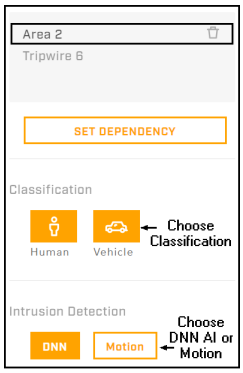
To configure Loitering detection area:

1. Click on the newly created area name. Options for Loitering Time and Classification appear.
2. Choose loitering time (0 - 600, in seconds).
3. Choose Human and/or Vehicle Classification.



To configure the Intrusion detection area:

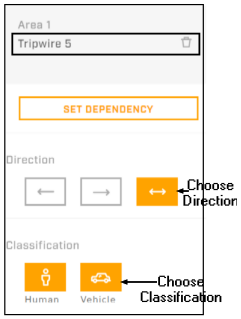
1. Click on the newly created area name. Options for Classification appear.
2. Choose Human and/or Vehicle Classification
3. Choose DNN (default) or Motion detection.



Thermal Video

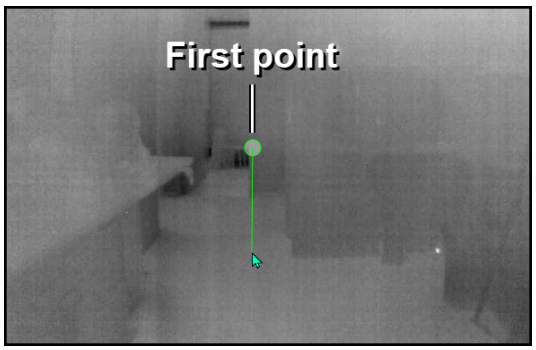
To configure Tripwires:

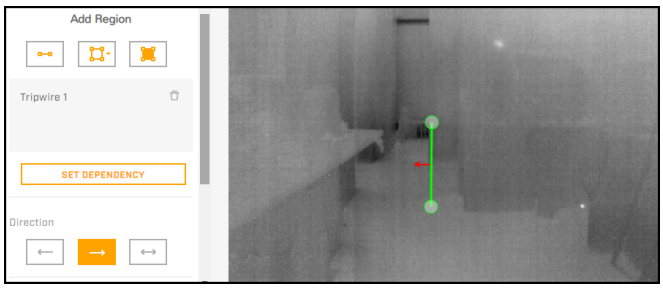
1. Click on the newly created tripwire name. Options for Direction and Classification appear.
2. Choose bidirectional (default) or unidirectional (left or right).
   a. The direction selection arrows refer to the direction of movement over the tripwire as seen from the first tripwire point created.



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

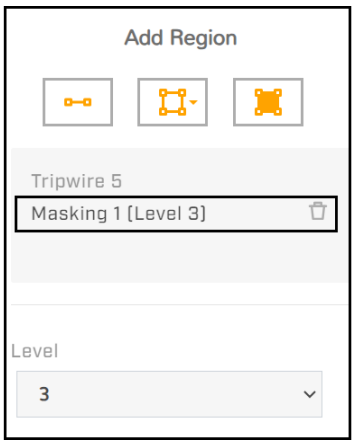
At right, the tripwire has been completed and the *left-to-right* direction button has been selected. Because detection direction relates to the first tripwire point created, the direction arrow in the video is *right to left* and the camera triggers alarms when it detects movement over the tripwire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





To configure Masking Regions:

1. Click on the newly created tripwire name. Masking Level options appear.
2. For each masking region, you can specify the Level:
   a. Level 3 (default)—Completely blocks detection of all objects in the region.
   b. Level 2—Applied for detecting normal upright and discrete human intrusions at 50% or above confidence level. Supported when DNN or Fuse DNN Area is enabled.



Display Region Labeling

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

- Region type—T = tripwire, A = intrusion detection area, or L = loitering
- Unique region ID number
- Video image type—T = thermal video
- VA type—D = DNN, M = motion detection, DM = Fuse DNN Area enabled

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

Dependency

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

The following dependencies from one region to another can be set:

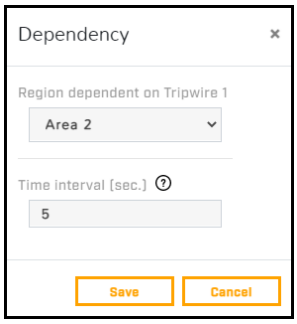
- Motion detection area to Motion detection area
- DNN area to DNN area
- DNN area to Fuse DNN area
- Fuse DNN area to Fuse DNN area

On the right, Area 1 is dependent on Area 4.

The Area 1 alarm will only trigger if the alarm on Area 4 is triggered first.

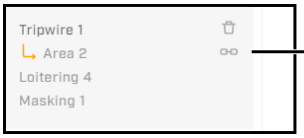
To establish dependency between two regions:

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



To remove a dependency:

Click the link icon corresponding to the dependent region.



Click to remove dependency

3.8 OSD Page

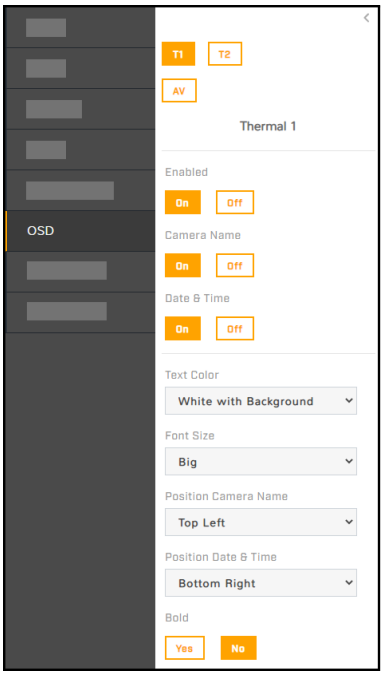
For each IP video stream (T1 and T2) and for the analog video output (AV), you can:

- 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.

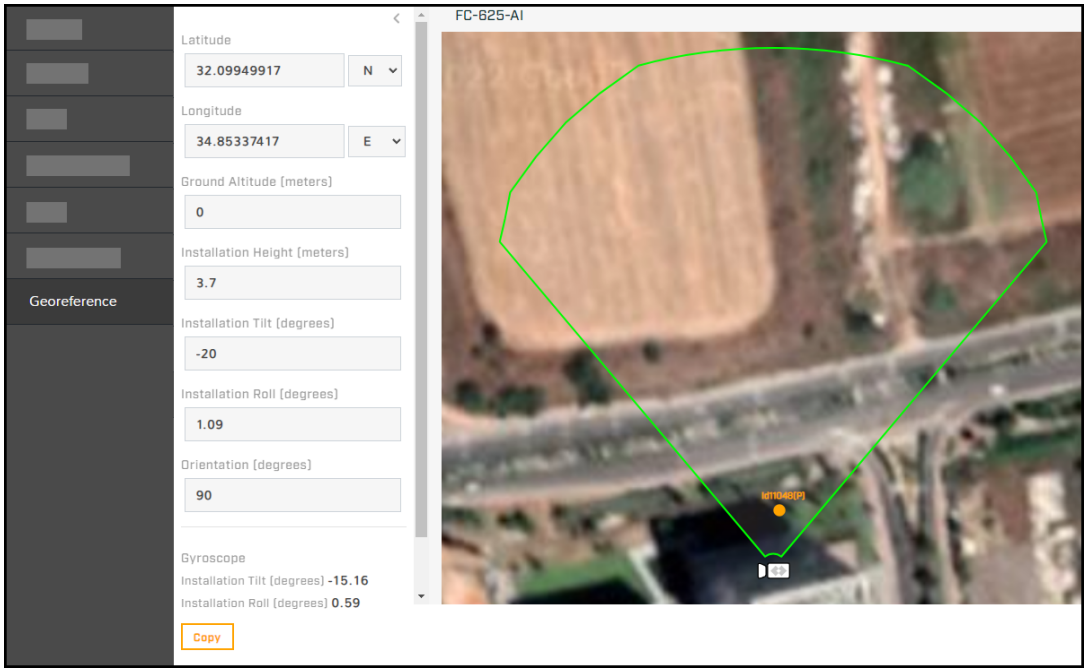


3.9 Georeference Page

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

Pairing an FC-Series AI camera with a FLIR Security PTZ camera that supports geotracking requires proper and accurate georeference configuration. For more information about how to one or more FC-Series AI cameras with a FLIR Security PTZ camera that supports geotracking, see the FLIR Security PT-Series HD Pairing Configuration Guide.

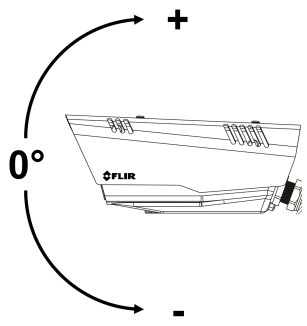
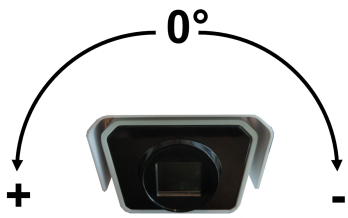
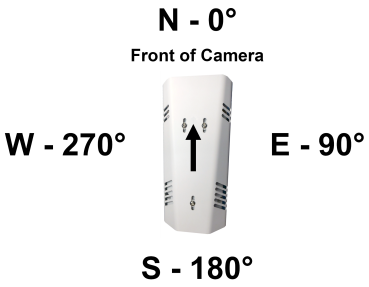
Specify the camera's Latitude in degrees North or South, and its Longitude in degrees East or West, up to eight decimal places. To obtain the camera's coordinates, you can use a map or a mobile GPS device.



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

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

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

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

Tips

- Teledyne FLIR recommends mounting the camera horizontally level; that is, with a 0º installation roll angle. For accurate VA, 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 NEXUS® SDK, 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.

3.10 Geotracking Page

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

You can pair one or more FC-Series AI cameras with a FLIR Security PTZ camera that supports geotracking. When the cameras are paired, the PTZ camera engages the geotracks from the FC-Series AI cameras. For information about how to pair cameras, including how to configure the PTZ camera when it is paired, see the FLIR Security PT-Series HD Pairing Configuration Guide.

Important

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

Detected Objects Tracked (Map Not Uploaded)

When present, the following appear in the Geotracking & Georeference page display:

Icons and Descriptions			
	Fixed camera—The circle around this icon indicates the FC-Series AI camera you are currently configuring.		Geotracking alarm region
	PTZ camera		Geotracking exclusion region
	Radar		Detected object
	Geotracking range		Detected object in geotracking alarm region
	VA detection range		Object engaged by PTZ camera

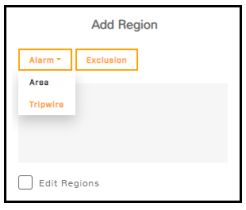
When a map has been uploaded and calibrated on the Map Page and the camera's georeference settings have been properly configured on the Georeference Page, the map appears in the display.

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

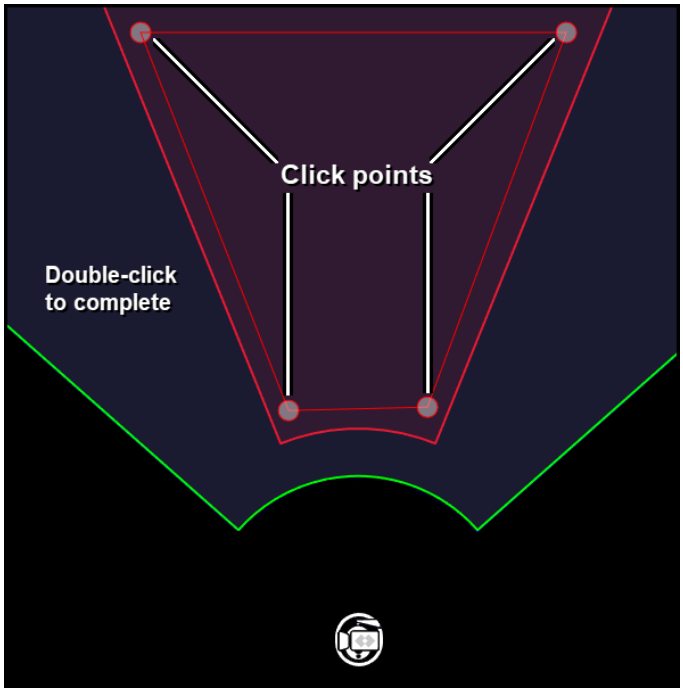
To add a geotracking region:

1. Click one of the Add Region options.

   Alarm (Area or Tripwire)—Triggers geotracking alarms. In the detection area display, alarm areas and tripwires 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 FLIR Security PTZ camera that supports geotracking, you can specify that the PTZ camera only engages geotracking alarm tracks.



Exclusion—Camera does not detect objects and does not trigger geotracking alarms. In the detection area display, exclusion regions appear in yellow. Exclusion regions can help eliminate alarms from a tree or bush moving in the wind, for example.



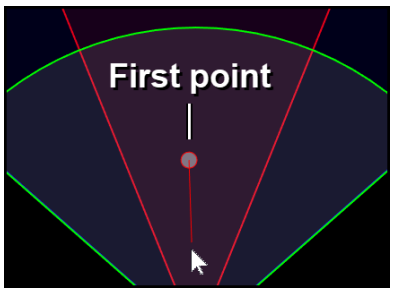
1. Create the first point of the region. Click and release on the detection area display.
2. Continue adding points (up to 25).
3. To complete the region, double-click on the detection area display.
4. To cancel creating a region, press **Esc**.
5. To define another region, repeat steps 1-4.

Managing Regions

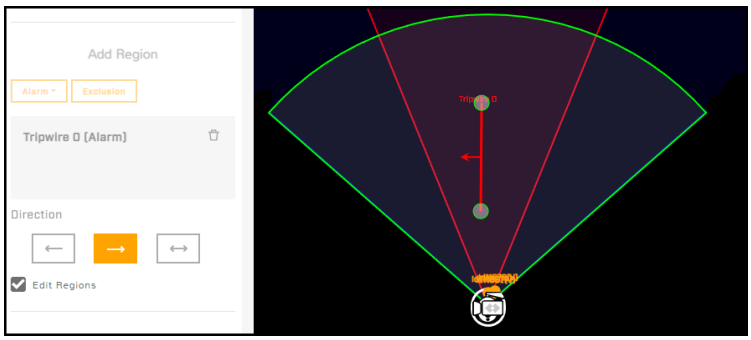
To edit an existing region, select **Edit Regions**, and click the region. You can:

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

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



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



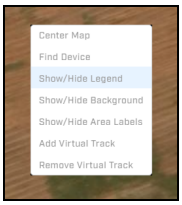
When Edit Regions is selected, it is not possible to add regions.

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

Tips

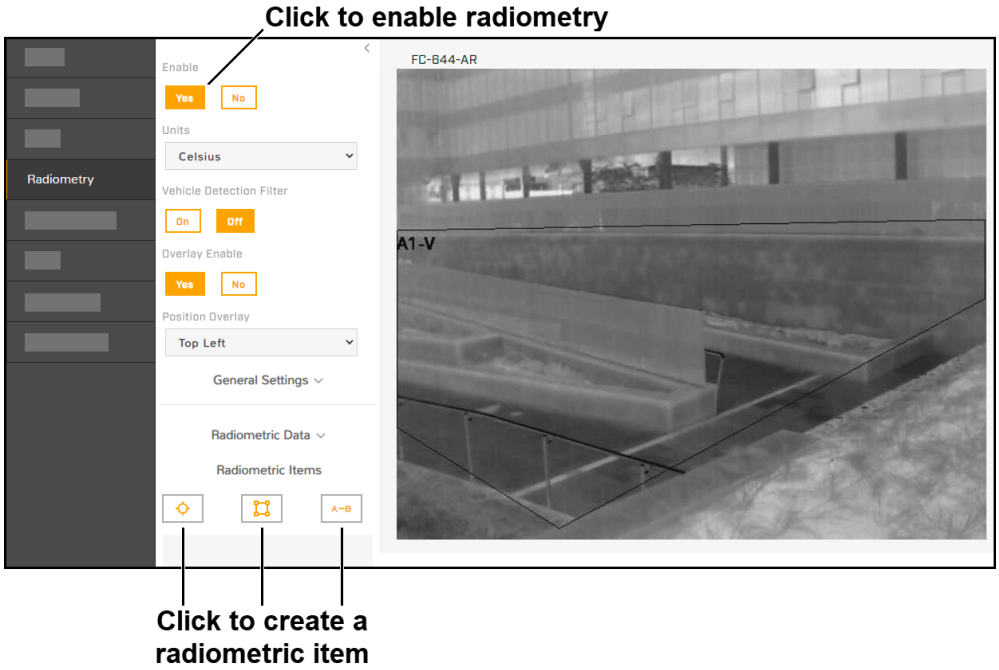
- To move the display, and to zoom in and out, you can use the mouse. To move the display, click on the display, hold, and drag. To zoom in or out, use the mouse scroll wheel.
- Right-click on the display to:
  - **Center Map—**If uploaded and calibrated, centers the map in the display.
  - **Find Device—**Centers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

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



3.11 Radiometry Page (FC-Series AI-R)

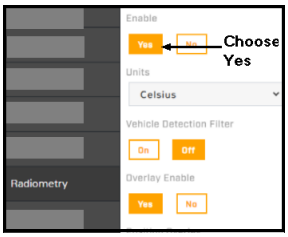
The FC-Series AI-R camera detects, measures, and monitors surface temperatures. Using a thermal camera for reasonably accurate and precise temperature measurements requires at least a minimum level of expertise in thermography; Teledyne FLIR recommends training. The Infrared Training Center (http://www.infraredtraining.com/) offers training (including online training) and certification in all aspects of thermography.



To configure the Radiometry page:

1. Enable the camera's radiometry features

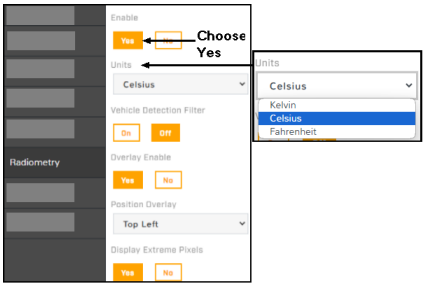
   Under Enable, click Yes.



2. Select the unit of temperature

   a. Under Units, click the dropdown menu.

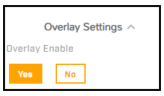
   b. Select Celsius, Kelvin, or Farenheit.



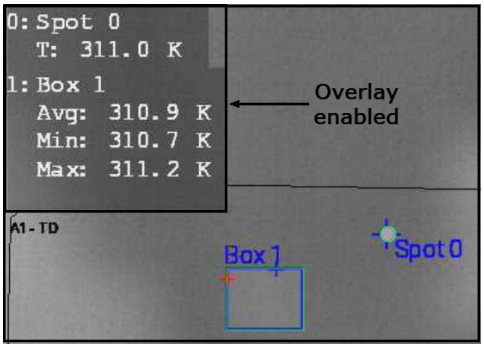
3. Decide whether to enable Overlay

   a. Under Overlay Enable, choose Yes or No.

   b. Under Position Overlay, click on the dropdown list to specify where you want the overlay to appear on the video.

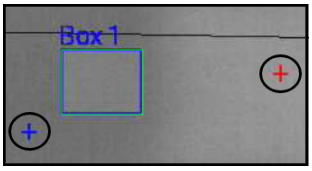


When enabled, an overlay with temperature data from defined radiometric items appears in the live thermal video on the camera web page and in the thermal video streams.



4. Decide whether to Display Extreme Pixels

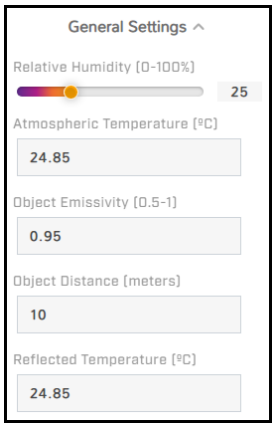
   Under Display Extreme Pixels, choose Yes or No.



- When enabled, blue and red cross hairs indicate the pixels with the coldest and warmest detected temperatures, respectively.
- These values correspond to the data on the overlay.

5. Configure General Settings

a. Click General Settings. The General Settings Menu opens.
b. Specify Relative Humidity (relative humidity where the camera is mounted) by sliding the scale to your desired value (1 - 100%).
c. Specify Atmospheric Temperature (ambient temperature where the camera is mounted).
d. Specify Object Emissivity, Object Distance, and Reflected Temperature.

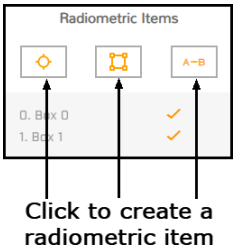


The camera can calculate detected surface temperatures of objects using general settings or values specified for a particular radiometric item (see **Local** below).

6. Create radiometric items

You can create three types of radiometric items. These include:

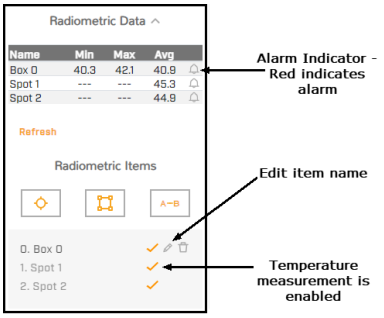
a. **Spot—**detects the surface temperature in a specific spot in the camera's field of view.
b. **Box—**detects temperatures over a defined box shaped area.
c. **Differential—**detects the difference in temperatures between two radiometric items:
   i. spot and spot
   ii. box and box
   iii. spot and box



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.

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

- For spots, the surface temperature detected at the spot appears under Avg. For boxes, the following temperatures detected in the box appear:
  - Minimum
  - Maximum
  - Average



- 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.

8. Create a spot item

a. Click the spot icon . A numbered spot appears:

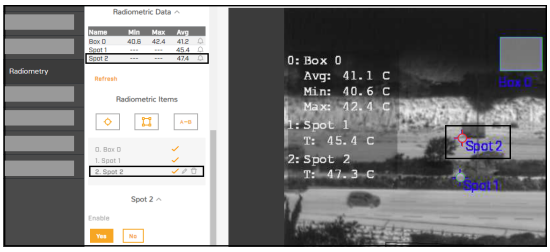
   i. In the video

   ii. Under Radiometric items

   iii. Under Radiometric Data.

b. For spots, the surface temperature detected at the spot appears as an Average.

c. Drag the spot to the desired location.

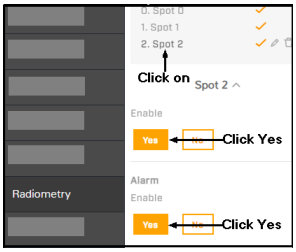


9. Configure spot item to trigger an alarm

a. Click on the spot item number under Radiometric Items to configure an alarm. A menu for the spot item appears.

b. Under Enable, choose Yes.

c. Under Alarm Enable, choose Yes.

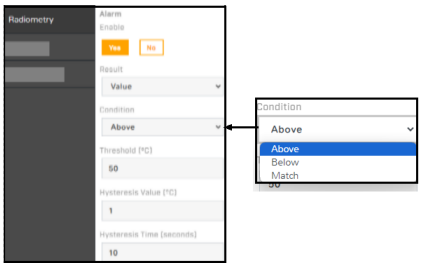


d. Under Threshold, enter the value (ºC) that you want to trigger an alarm.

e. Under Condition, choose whether the alarm should be triggered when the temperature is Above, Below or a Match to the threshold value you entered.

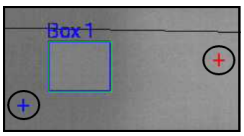
f. Specify Hysteresis Value (ºC), the number of degrees above or below the threshold, depending on which classification was chosen, that the temperature must reach before the alarm turns off.

g. Specify Hysteresis Time (seconds), after conditions are



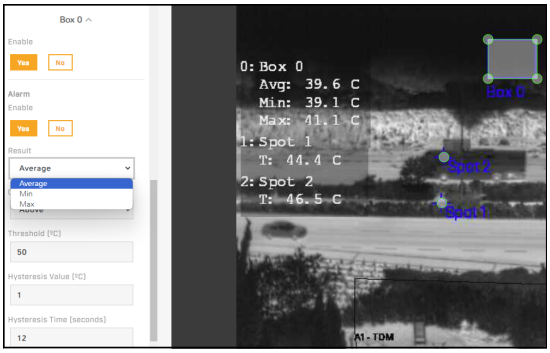
met, this is the allotted time that passes before an alarm is triggered.

10. Create a box item
    a. Click the box icon , a box item appears.
    b. Click and drag to desired location.



11. Box items display:
    a. Minimum Temperature
    b. Maximum Temperature
    c. Average Temperature

12. Configure a box item to trigger an alarm
    a. Click on the box item number under Radiometric Items to configure an alarm. A menu for the item appears.
    b. Under Enable, choose Yes.
    c. Under Alarm Enable, choose Yes.
    d. Under Result, choose whether you want to use the Minimum, Maximum, or Average temperature value.
    e. Under Threshold, enter the value (ºC) that you want to trigger an alarm.
    f. Under Condition, choose whether the alarm should be triggered when the temperature is Above, Below or a Match to the threshold value you entered.
    g. Specify Hysteresis Value (ºC), the number of degrees above or below the threshold, depending on which classification was chosen, that the temperature must reach before the alarm turns off.
    h. Specify Hysteresis Time (seconds), after conditions are met, this is the allotted time



that passes before an alarm is triggered.

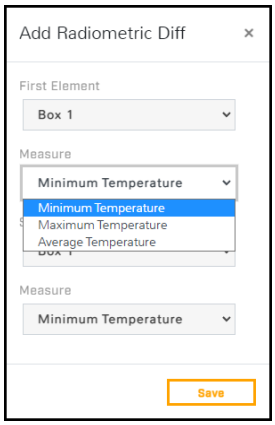
13. Create a differential item

a. Click differential item icon A–B. The Add Radiometric Diff screen appears.

b. Select the spot or box items to compare.

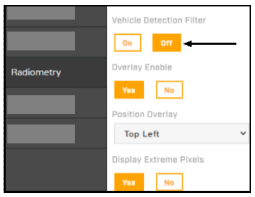
c. For boxes, select the type of temperature measurement to compare (Minimum, Maximum, or Average).

d. Click Save. The differential item appears in the Radiometric Items list.



14. Decide whether to enable the Vehicle Detection Filter

Under Vehicle Detection Filter, choose Yes or No.



After the VA detects and classifies an object as a vehicle, and that vehicle stays in the loitering region for the specified loitering time, a radiometric alarm is not triggered.

15. Before enabling Vehicle Detection make sure:

a. Vehicle classification is enabled on one or more loitering regions on the thermal video.

b. The loitering regions match the radiometric boxes.

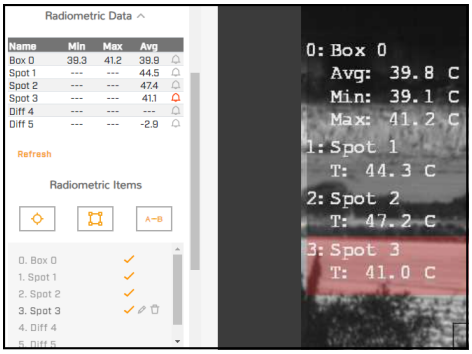
A limitation of this feature is that it only applies to the following:

- Cars
- Vans
- Small trucks
- Vehicles up to the size of 15m

Larger vehicles will not be detected and filtered, such as:

- Long trailers
- Forklifts
- Heavy vehicles with special shapes such as construction vehicles

When an alarm is triggered, the bell icon next to the radiometry item turns red. The entry on the overly also turns red.

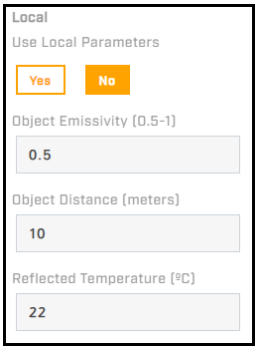


Local

Use Local Parameters—

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

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



4 Thermal Imaging Overview

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.

WhiteHot Palette

WhiteHot palette (default)—

- Objects or surfaces in the scene with the hottest detected temperatures appear white; such as:
  - hot objects
  - vehicle engines
  - exhaust pipes
- Items with the coldest detected temperatures appear black such as:
  - the sky
  - puddles of water
  - cold objects
- All other items appear in gray scale.

BlackHot palette—

- hot objects appear black or dark.
- cold objects appear 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.

FC-Series AI-R camera: When configuring the radiometry settings, make sure to consider these changes that occur throughout the day.

5 Maintenance and Troubleshooting

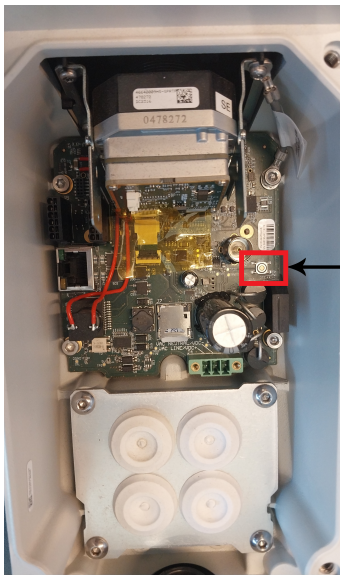
If help is needed during installation, operation, or configuration, contact the local Teledyne FLIR representative, or visit the Teledyne FLIR Support Center at: https://support.flir.com/. Teledyne FLIR LLC offers a comprehensive selection of training courses to help get the best performance and value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

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

Manual Reset

To perform a manual reset on the FC-AI camera:

1. Open the top of the camera.
2. Press the button indicated in the red box.
   a. If you hold for 3-5 sec, the camera will reboot.
   b. If you hold the button for 6-10 seconds, nothing happens.
   c. If you hold the button for more than 10 seconds, a full factory reset will be performed.



The inside of the FC-AI camera. Reset button is indicated in the red box.

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 VA is 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:

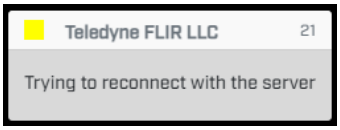
- **Acetone—**removes grease
- **Ethanol—**removes fingerprints and other contaminants
- **Alcohol—**final cleaning (before use)

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.

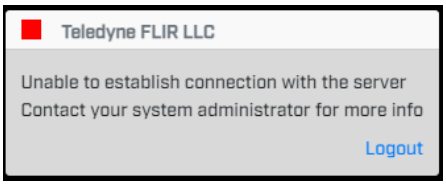
Troubleshooting Tips

Unable to Access the Camera

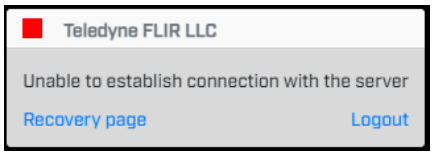
Under certain circumstances, after logging in to the camera's web page, the following messages appear:



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

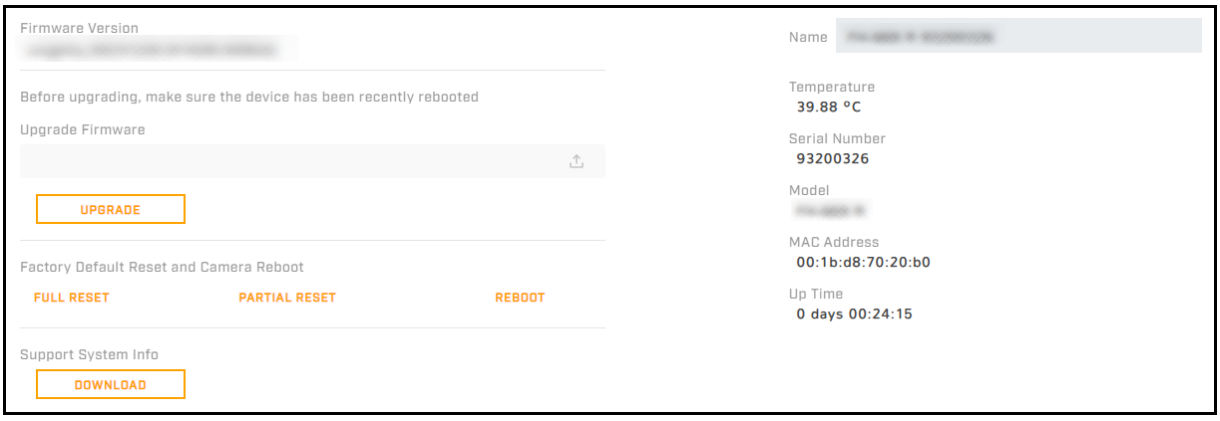


The camera's Nexus server is not available, and you logged in as a user assigned the expert or user role. For troubleshooting options, you need to log in as a user assigned the admin role. Click **Logout** and contact your system administrator.



The camera's Nexus server is not available, and you logged in as a user assigned the admin role. You can click:

- **Logout**
- **Recovery page—**Opens a page similar to the Firmware & Info Page, on which you can see some system information and perform some system-related tasks. For example, you can reboot the camera.



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.

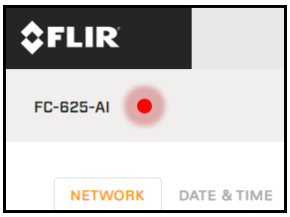
Images facing sun from visible light camera (left) and from thermal camera (right)

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.



Recording Indicator

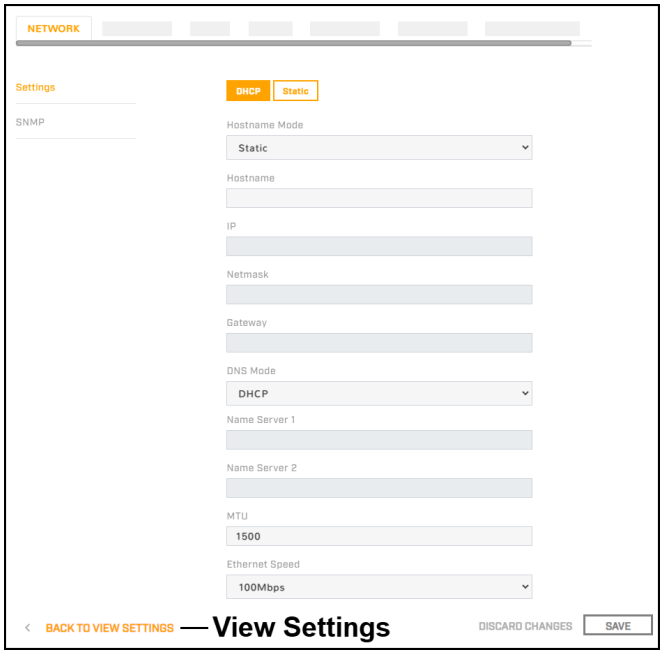
Note

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

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

6.1 Network Page

The Network page provides networking and SNMP settings.



— View Settings

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

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:

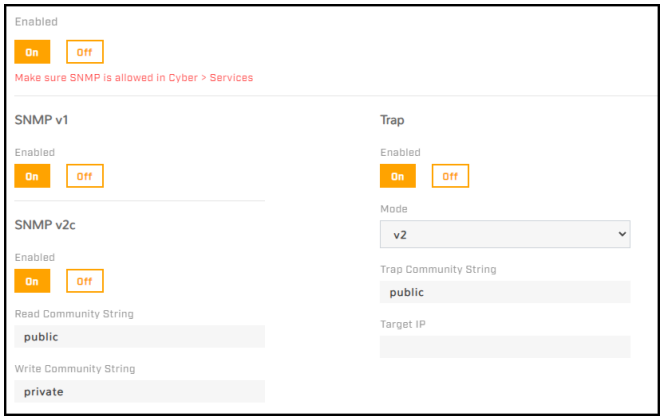
  - **Name Server 1**—The primary domain name server that translates host names into IP addresses.
  - **Name Server 2**—A secondary domain name server that backs up the primary DNS.

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.



Important

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

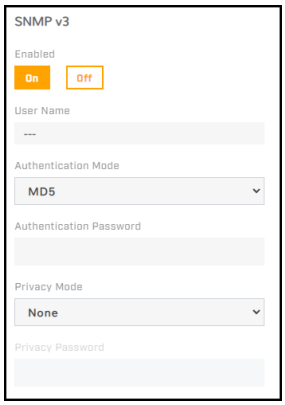
SNMP v1—Enable SNMP v1.

SNMP v2c

After enabling SNMP v2, specify:

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

SNMP v3



SNMP v3 provides security features including:

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

After enabling SNMP v3, specify:

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

Trap

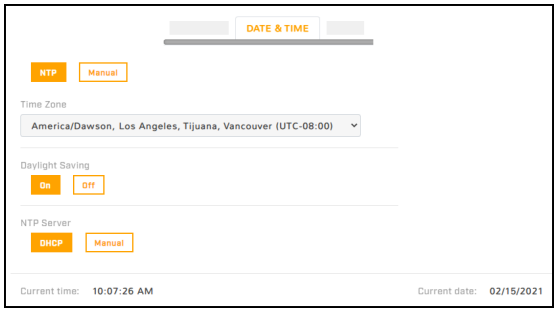
The camera uses traps to send messages to the network management system for important events or status changes.

After enabling traps, specify:

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

6.2 Date & Time Page

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

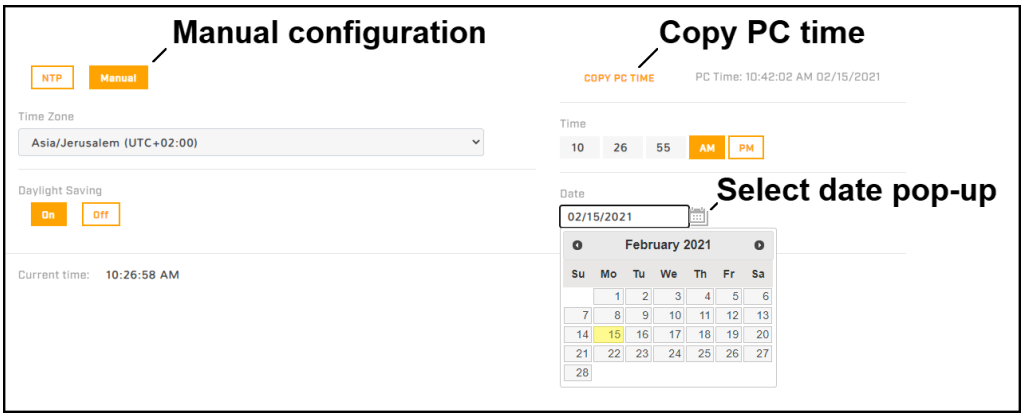


When DHCP IP addressing is enabled on the Settings, you can configure the camera to obtain the NTP server information from the DHCP server.

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

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

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

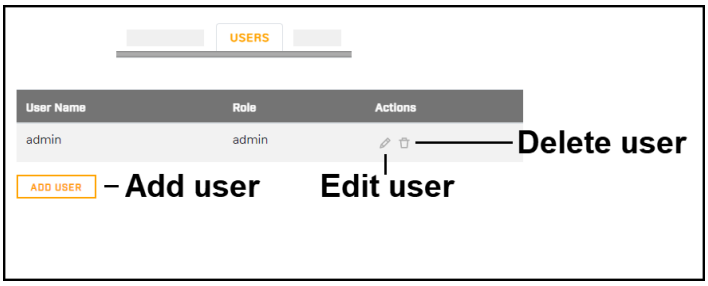


Tip

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

6.3 Users Page

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



Users assigned the expert role only see the user currently logged in, and cannot add, edit, or delete 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 have the following attributes:

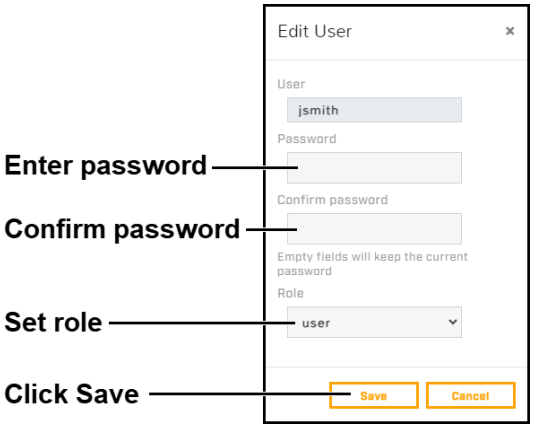
- At least 12 characters
- Contain at least one number
- Contain at least one lowercase letter
- Contain at least one uppercase letter
- Include the following special characters: |@#~!$&<>+_-.,*?=

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

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

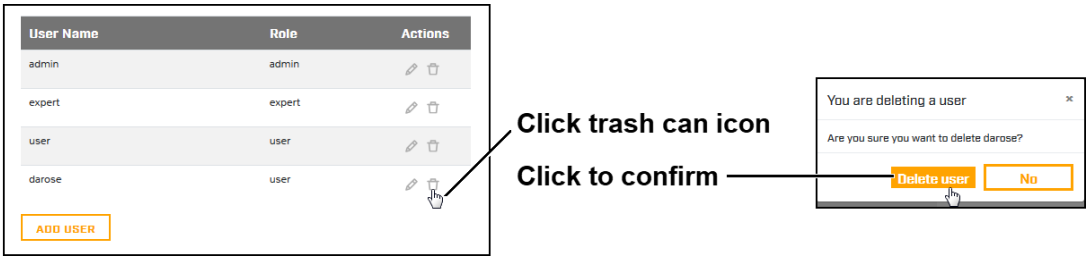
Add User

Edit User



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

Delete User



6.4 Alarm Page

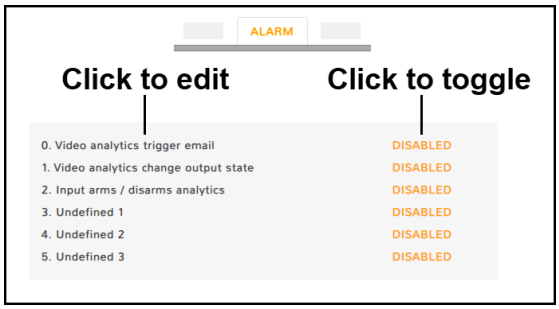
You can define camera alarms to be triggered by:

- The camera's onboard VA
- The camera's radiometry (FC-Series AI-R)
- The camera's geotracking
- VA 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 VA (available when Video Analytics is 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**—The camera's VA triggers a notification email. Set up and configure the messaging settings on the Messaging Page.
- **1. Video analytics change output state**—The camera's VA triggers a change to the state of a local alarm output connector. If the idle state of the connector is Closed, the alarm changes the state to Open. Likewise, if the idle state is Open, the alarm changes the state to Closed. For information about configuring the idle state of the camera's local I/O connector pins, see I/O Page.
- **2. Input arms / disarms analytics**—A change in the state of the local alarm input connector enables or disables the onboard VA.

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

You can also define and enable three additional rules:

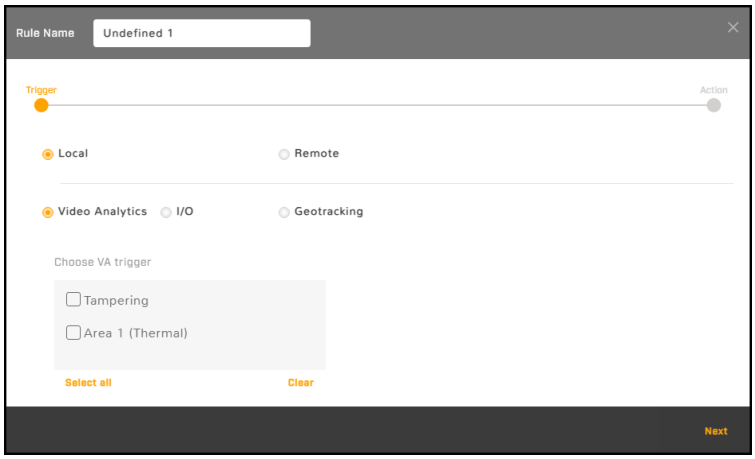
- **3. Undefined 1**
- **4. Undefined 2**
- **5. Undefined 3**

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

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

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

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



Rule Trigger Settings 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 VA triggers this rule's action.	a. On the Video Analytics Page, make sure tripwires and intrusion detection / loitering regions have been defined. b. Select the tripwires and regions that trigger this rule's action.

Local Triggers		
		You can also select tampering as a trigger. After the camera has been powered on for 24 hours, blocking the thermal sensor of the camera for one minute triggers this rule's action.
Radiometry (FC-Series AI-R)	This camera's radiometry triggers this rule's action.	a. On the Radiometry Page (FC-Series AI-R)), make sure at least one measurement item has been defined. b. Select one or more measurement items that trigger this rule's action.
I/O	**Local—**This camera's local I/O connections trigger this rule's action.	a. On the I/O Page, make sure local I/O connectors have been properly configured. b. Select one or more local I/O connections that trigger this rule's action.
	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 VA / geotracking is enabled.

Remote Triggers

1. Under Discovered Devices, from the drop-down menu of supported devices on the same network as the camera, select:
   a. A remote camera
   b. A radar / geotracking device
   c. Another device

The IP address and port appear.

2. You can also manually specify the remote device IP address and port.
3. Click **Refresh** to save. The drop-down menu of discovered devices is also refreshed.
   a. Click **Refresh** once the remote device is connected to the same network as the camera.

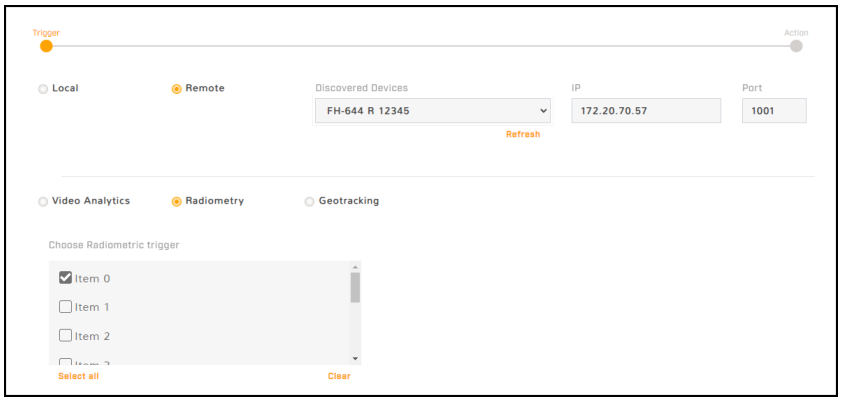
Note

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	VA from a supported remote camera or other device triggers an alarm.	a. On the remote camera or other device, make sure VA is enabled and that at least one tripwire, intrusion detection / loitering region, or another analytics item has been defined. b. Select one or more VA items that trigger this rule's action.

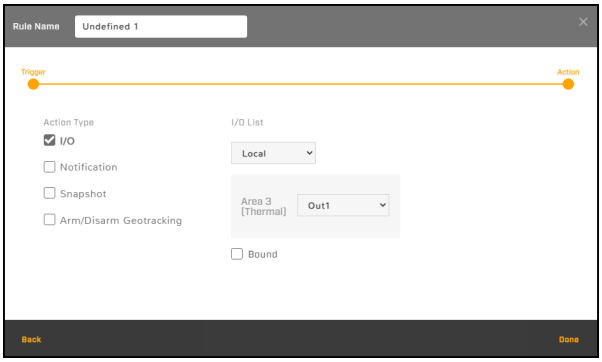
Remote Triggers		
Radiometry	Radiometry from a supported remote camera or other device triggers an alarm.	a. On the remote camera or other device, make sure radiometry is enabled and that at least one radiometric item has been defined. b. Select one or more radiometric items that trigger this rule's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

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



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

6.4.2 Modifying or Defining Rule Actions



Rule Action Settings
Local I/O - Area 3 (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 Local > Video Analytics)**—**When triggered, this rule toggles the camera's onboard VA from enabled to disabled or vice versa.	
Notification—When triggered, this rule sends notifications according to the settings on the Messaging Page. Specify a subject for the notifications. For email notifications, specify whether the camera attaches a snapshot. **Tip** When notifications are enabled for an alarm rule, the camera sends all configured notifications. It is not possible to enable or disable individual notification types. Therefore, to differentiate between notifications triggered by the camera's onboard VA, Teledyne FLIR recommends configuring alarm rules for each type of VA region (tripwire, intrusion, and loitering). Then, specify different subjects for each rule's notifications.	
Snapshot—When triggered, this rule records a snapshot image of live video.	
Arm/Disarm Geotracking (not available when this rule's trigger is the camera's onboard geotracking) **—**When triggered, this rule toggles the camera's onboard geotracking alarms from enabled to disabled or vice versa.	

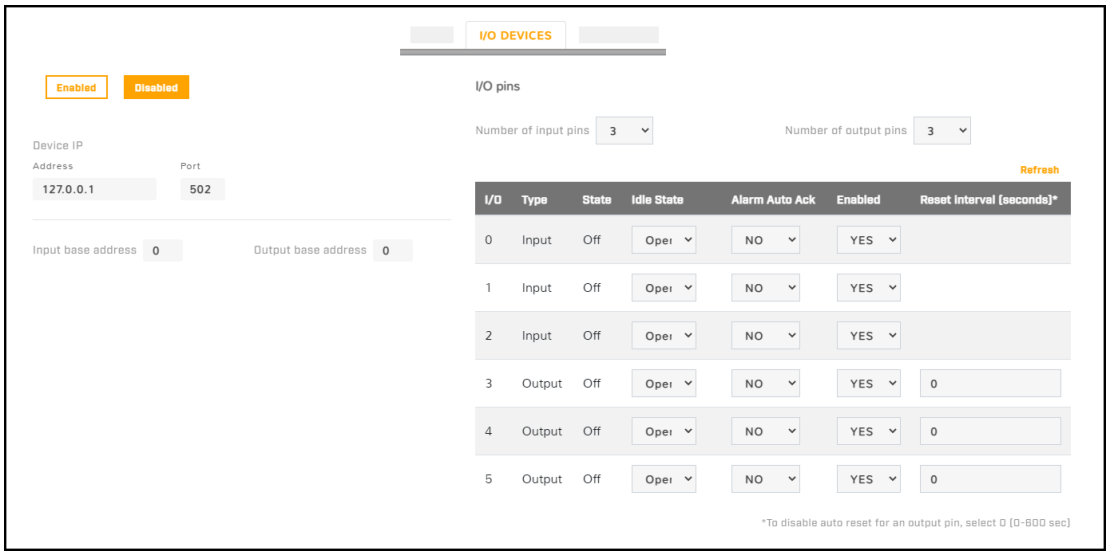
3. Click **Done**.

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**



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

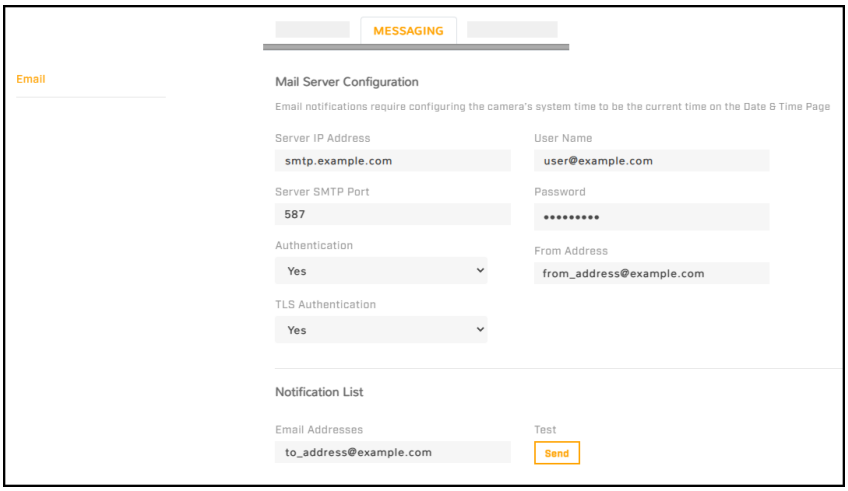
For more information about how to configure the device managing the external I/O connections, refer to the device's documentation.

6.6 Messaging Page

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

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

6.6.1 Email



Mail Server Configuration

Specify the settings for the SMTP server in the appropriate fields. Settings include:

- SMTP server's IP address.
- Port (the default port is 587).
- User name and password for the account on the mail server.
- Whether the mail server requires authentication or TLS authentication.
- Email address from which the camera sends the notification emails (also known as the reply-to address).

If you do not know the mail server's settings, contact your mail server administrator.

Notification List

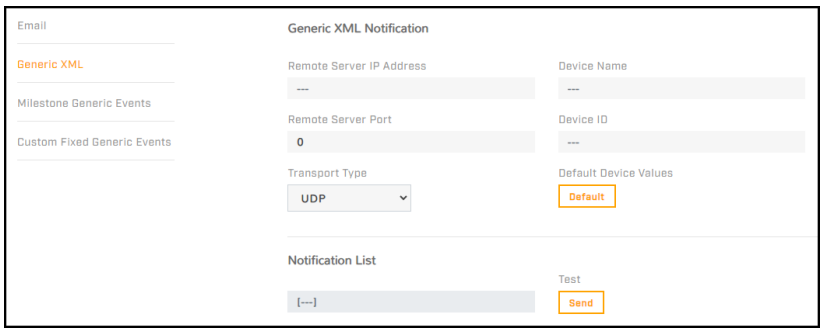
Specify one or more email addresses, separated by commas, to receive the notifications.

To test the mail server settings and the notification list, click **Send**.

Tip

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

6.6.2 Generic XML



Generic XML Notification

Specify the IP address and the port for the remote listening server or application; and the transport type (UDP or TCP). If you do not know this information, contact your system administrator.

You can specify the device name and ID that appears in the notifications, or click **Default** to use the default device values (the device name defined on the Firmware & Info Page and the device ID).

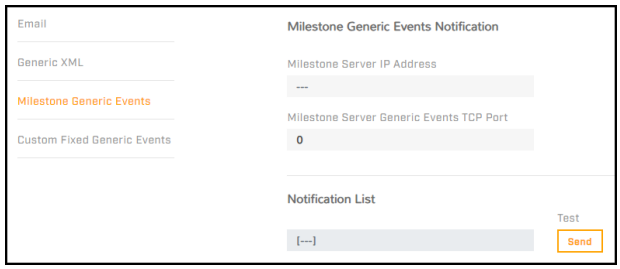
Notification List

To test the generic XML notification settings, click **Send**.

Notes

- UDP notification tests always appear to be successful, because UDP does not confirm that communication has been established. On the remote server, make sure test UDP notifications are received.
- If a TCP notification test failure message appears immediately after clicking **Send**, the specified port could be incorrect or the server is not listening. If the failure message does not appear immediately, the specified IP address is likely incorrect.

6.6.3 Milestone Generic Events



Milestone Generic Events Notification

Specify the Milestone server's IP address and generic events TCP port. If you do not know this information, contact your system administrator.

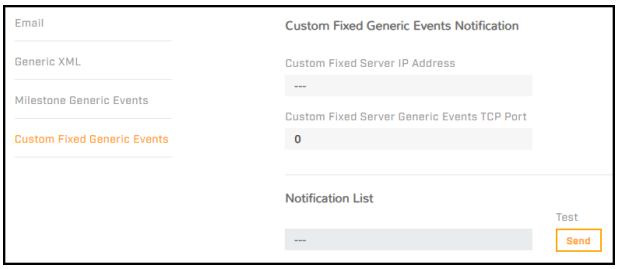
Notification List

To test the Milestone generic events notification settings, click **Send**.

Notes

If a failure message appears immediately after clicking **Send**, the specified TCP port could be incorrect or the server is not listening. If the failure message does not immediately appear, the specified IP address is likely incorrect.

6.6.4 Custom Fixed Generic Events



Custom Fixed Generic Events Notification

Specify the IP address and the TCP port for the remote listening server or application. If you do not know this information, contact your system administrator.

Notification List

To test the custom fixed generic events notification settings, click **Send**.

Notes

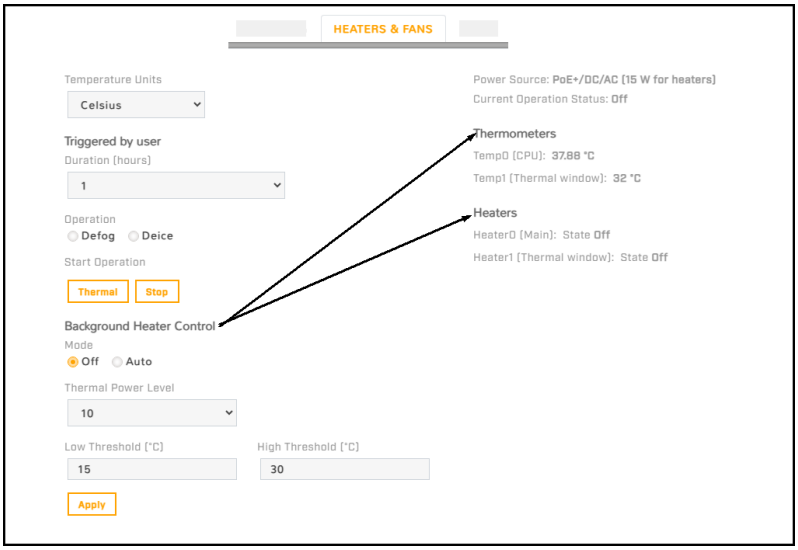
If a failure message appears immediately after clicking **Send**, the specified TCP port could be incorrect or the server is not listening. If the failure message does not immediately appear, the specified IP address is likely incorrect.

6.7 Heaters & Fans Page

The Heaters & Fans page provides configuration settings for:

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

- By default the Background Heater Control is turned off. When configuring the camera, it is recommended to turn it on Auto Mode.
- The Thermometer readings, Heaters, and Fans will function based on the user supplied settings of the Background Heater Control.



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). At least 60W of power is recommended to run the heaters (see, for example, Camera Specifications in the *FC-Series AI Installation Guide*).
- Temperatures at which the heaters activate (Low Threshold) and deactivate (High Threshold). It is recommended to set:
  - Low Threshold: 5 degrees below the ambient temperature.
  - High Threshold: 10 degrees above the ambient temperature.

Important

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

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).

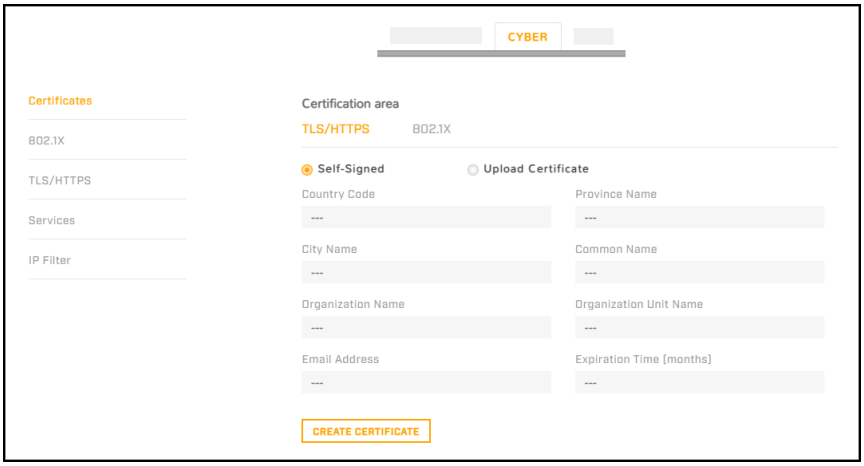
6.8 Cyber Page

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



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

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

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

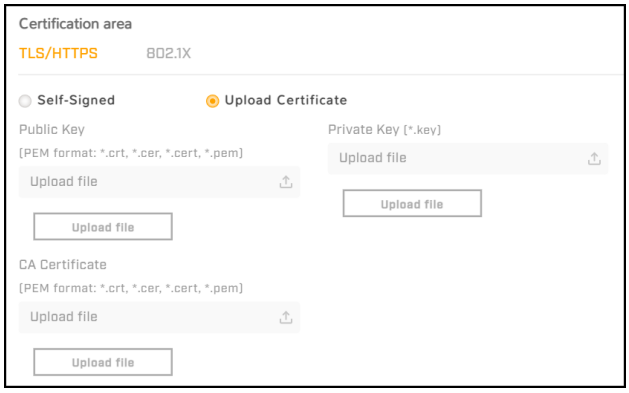
From the Certificates section of the Cyber page, you can download certificates and keys previously uploaded to or generated by the camera. If the certificate saved on the camera is self-signed, you can download the private and public key files. If the certificate was signed by a third-party CA, you can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

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

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

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

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



To Upload a Certificate for TLS/HTTPS

To Upload a Certificate for 802.1X

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

   a. Click

.

   b. Select the appropriate key file.

   c. Click 

.

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

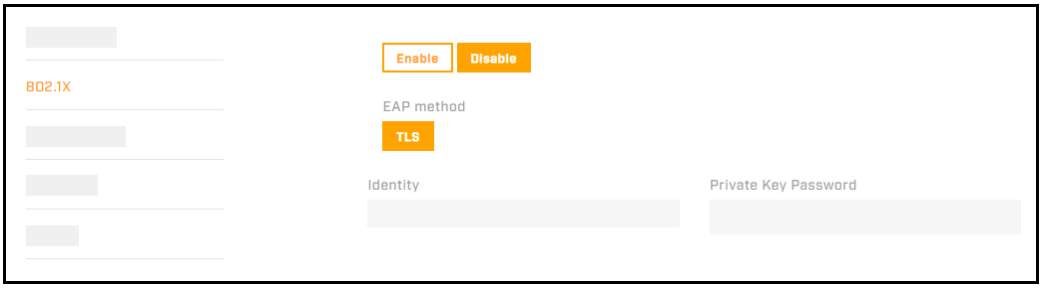
3. Verify that the camera certificate files are valid and make sure *Certificates are OK* appears under the certificate information, under Download certificate.

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

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.



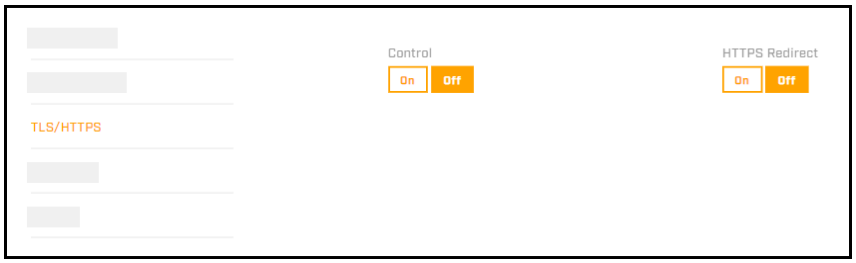
6.8.3 TLS / HTTPS

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.

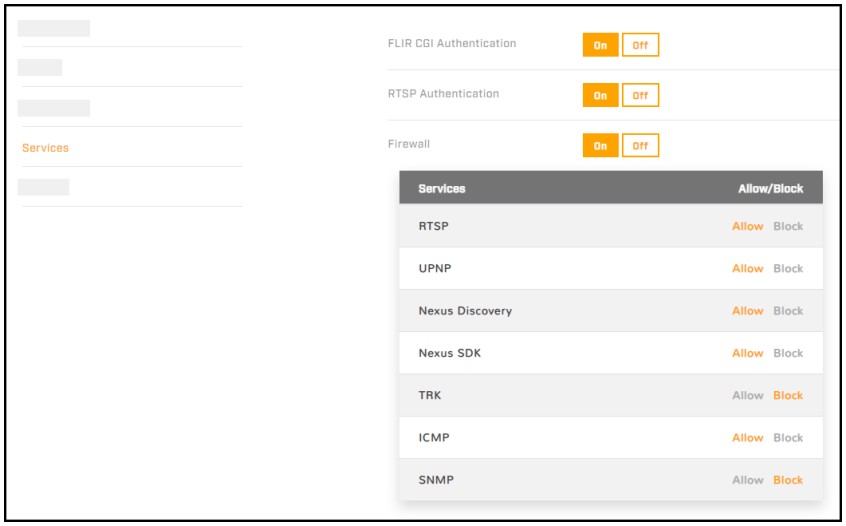


6.8.4 Services

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).



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

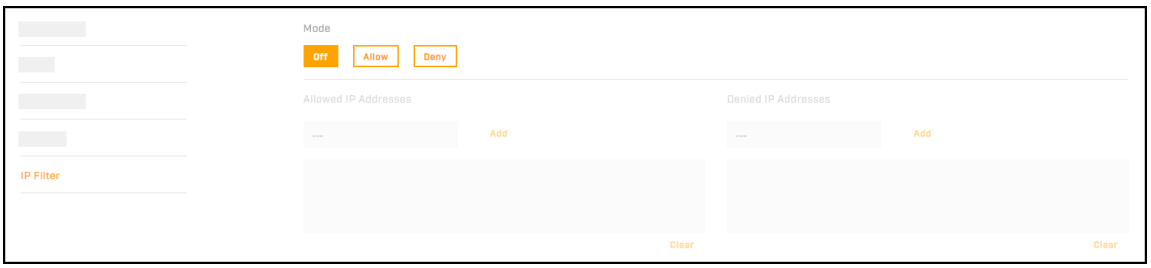
Disabling services and ports can affect product functionality.

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).



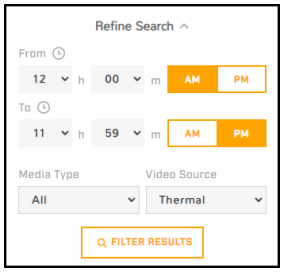
1. To define specific IP addresses that can access the camera, click **Allow**. The camera will deny access to all other IP addresses.
2. To define specific IP addresses that cannot access the camera, click **Deny**. The camera will allow access to all other IP addresses.
3. To add an IP address to a list, either under Allowed IP Addresses or under Denied IP Addresses, specify an IPv4 address and then click **Add**. You can specify up to 256 IP addresses.
4. To remove an IP address from a list, click the corresponding trash icon .

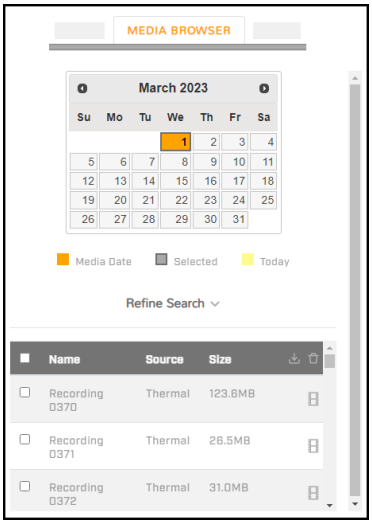
6.9 Media Browser Page

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)





Date with Recorded Files Selected

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

Tip

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

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

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

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

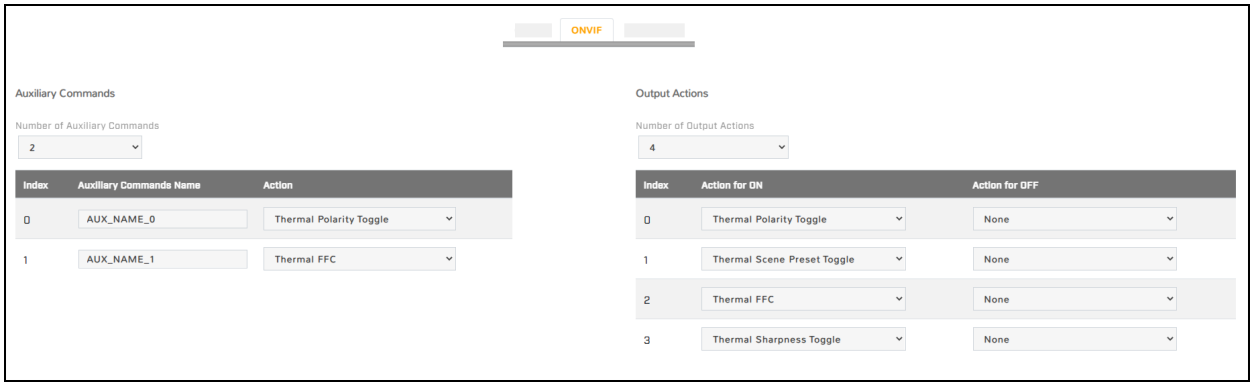
For example, SOE1-V1_VIDEO001_V1_1700982489_1700982789_3_22502.mp4.

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.



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 for geotracking. You can also:

- Download a previously uploaded map and its calibration information as a zipped file

- Upload a zipped map and calibration file
- Remove a previously uploaded map

To upload a reference map image and calibrate it:

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

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

   Tips

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

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

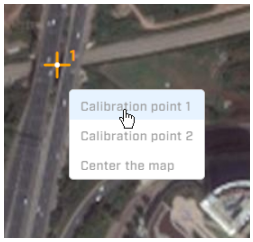
   For optimal calibration, the two calibration points should be as far apart as possible and on opposite sides of the map image. For example, at top-right and at lower-left.

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

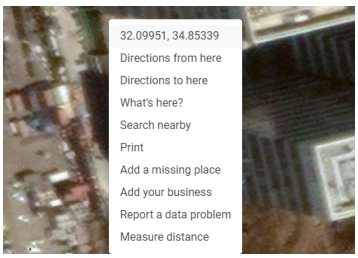
   If the map successfully uploads, a confirmation message appears.

4. Click **Accept**.

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



Right-Click on Map



Google Maps > Right-Click

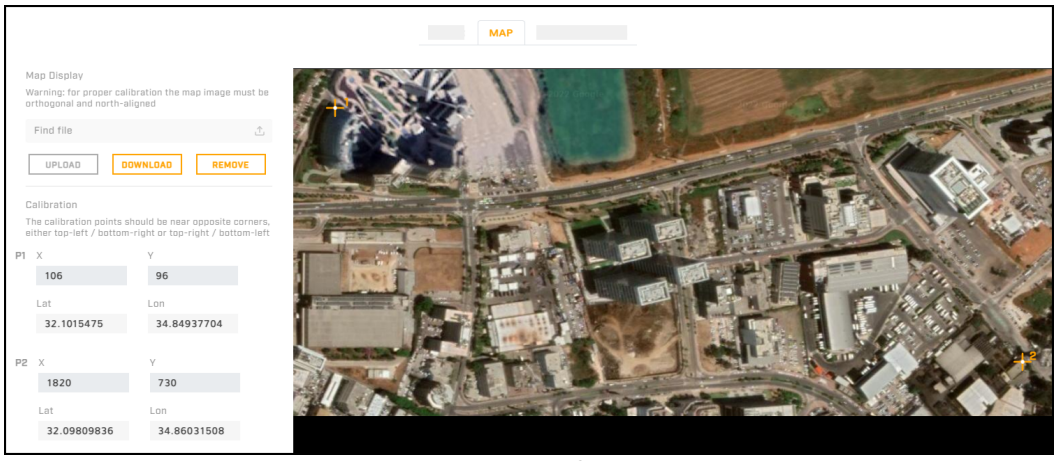
5. Right-click on the first calibration point, and then select Calibration point 1.
6. Enter the latitude (Lat) and longitude (Lon) coordinates for the first calibration point (P1). You can obtain the coordinates from the online map or from a GPS service.

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

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

7. Repeat steps 4 and 5 for the second calibration point (P2).
8. Click **Save**.

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



Map Uploaded and Calibrated

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

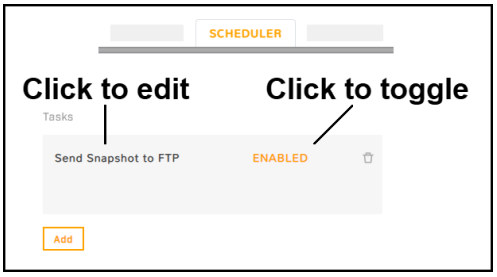
6.12 Scheduler Page

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

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

Note

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

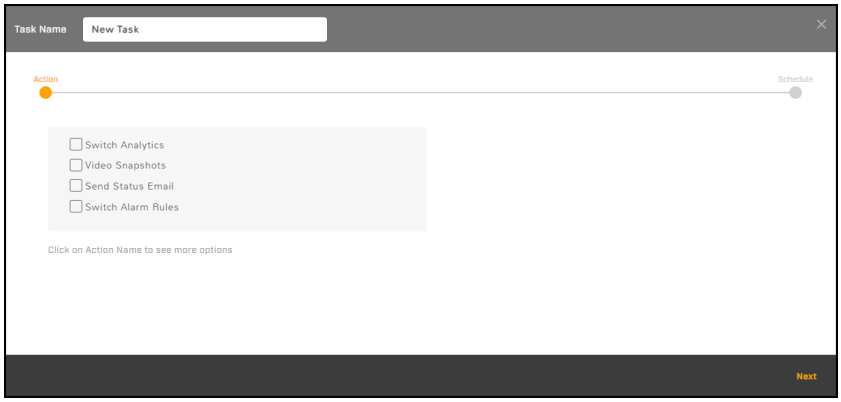


Scheduler Page with a Task Defined and Enabled

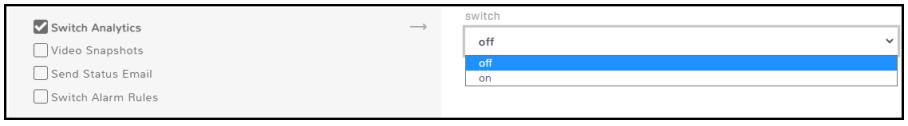
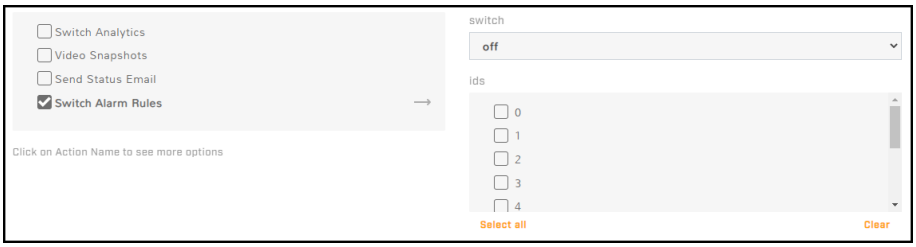
By default, no tasks are defined.

To define a task:

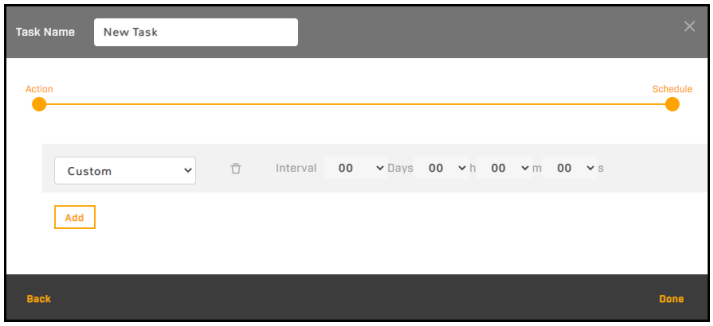
1. Click **Add**. A new task appears. By default, it is enabled.
2. Click **New Task**. The task action settings appear.



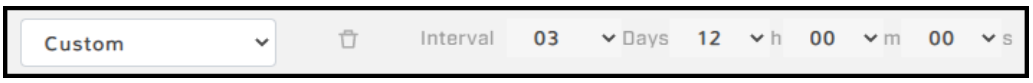
3. Define the task name.
4. Select the checkbox for one or more predefined actions.
5. To configure a predefined action, click the selected action. The selected action appears in **bold**, and the relevant settings appear.

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

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



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

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

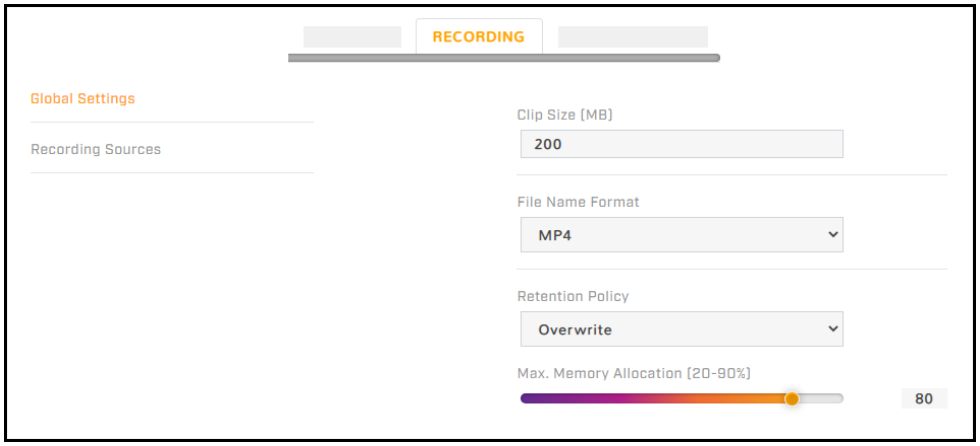
Global Settings

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.



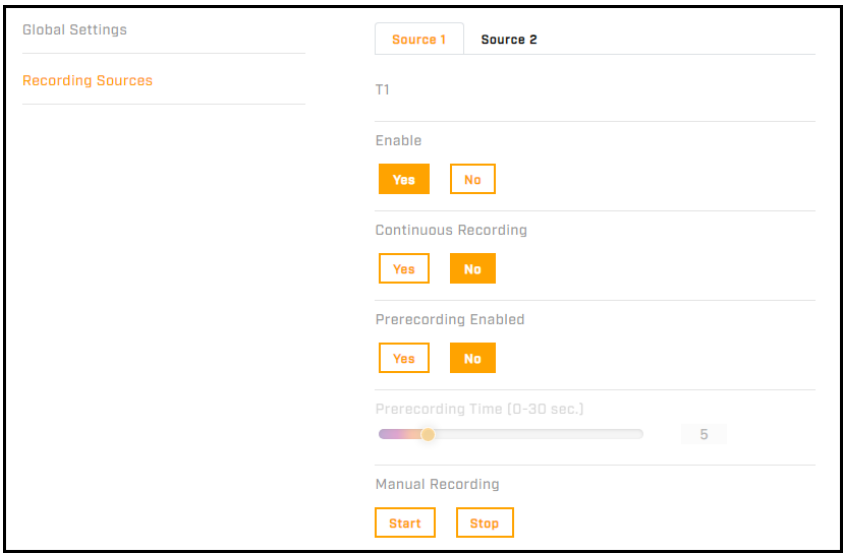
Recording Sources

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. However, manual recording of an H.265 source is not supported.



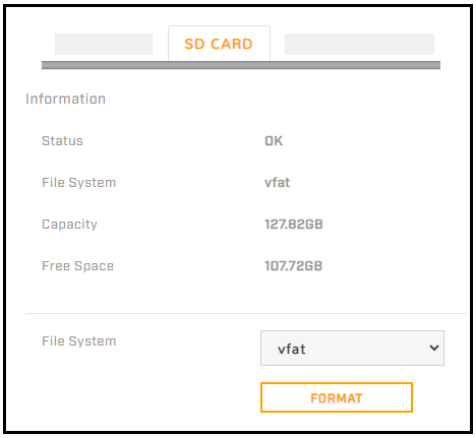
The current source and video stream settings appear to the right of the recording source settings.

Name	Associated Video	Associated Video Settings	Status
Source 1	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.



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**.

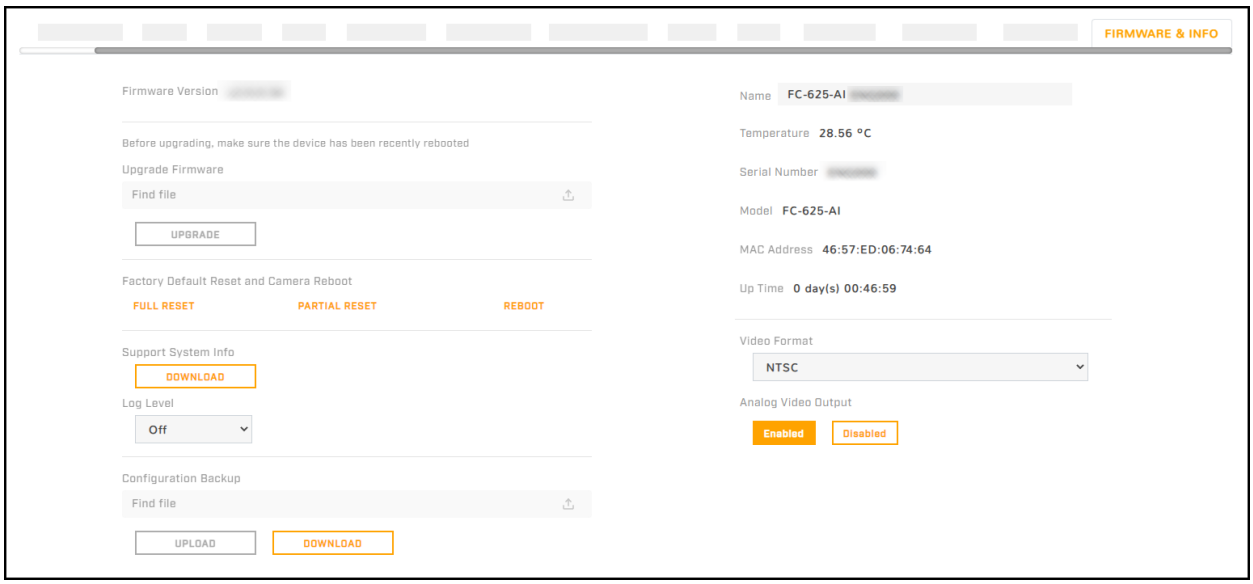
Caution

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

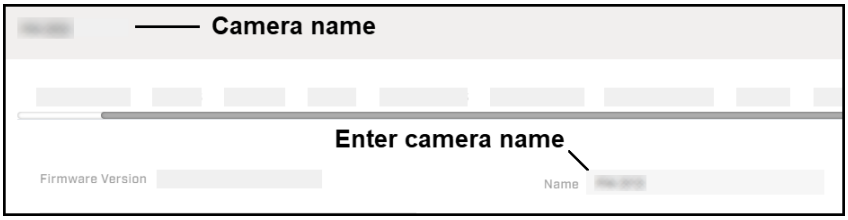


On the Firmware & Info page, you can:

- 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 Network page and 802.1X settings, click **Partial Reset**, and then confirm. The camera reboots.

Caution

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

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

Support System Info

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

Configuration Backup

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

To upload a configuration backup file:

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

   Caution

   Make sure to upload a configuration backup file that was downloaded from a FC-Series AI camera that is the exact same model and with the same firmware version installed.

3. Click **Upload**.

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

To download the camera's saved settings:

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

   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 video stream is 25 FPS (frames per second). The 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.

Snippet source EndnotesTop.xml not found!

Document:
FC-Series AI User Guide
Revision: 110
Date: August 2024