



Installation and User Guide

FB-Series



FB-Series O
FB-Series ID

© 2020 FLIR Systems, Inc. All rights reserved worldwide. No parts of this manual, in whole or in part, may be copied, photocopied, translated, or transmitted to any electronic medium or machine readable form without the prior written permission of FLIR Systems, Inc.

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

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

Photographs and images appearing in this manual may have been modified for illustrative purposes using commercial image editing software and may not always reflect an actual product configuration.

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

For additional information visit www.flir.com or write to FLIR Systems, Inc.

FLIR Systems, Inc.
6769 Hollister Avenue
Goleta, CA 93117

Support: <https://www.flir.com/support/>.

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 FLIR Systems, Inc. may void the user's authority under FCC rules to operate this device.

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

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

Industry Canada Notice:

This Class A digital apparatus complies with Canadian ICES-003.

Avis d'Industrie Canada:

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Proper Disposal of Electrical and Electronic Equipment (EEE)



The European Union (EU) has enacted Waste Electrical and Electronic Equipment Directive 2002/96/EC (WEEE), which aims to prevent EEE waste from arising; to encourage reuse, recycling, and recovery of EEE waste; and to promote environmental responsibility.

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

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

Document History

Revision	Date	Comment
100	December 2017	Initial release of FB-Series ID camera with video analytics intrusion detection
110	May 2018	Updated intrusion detection, web page links, added FB-Series FB-309 and FB-312 camera models
120	December 2018	Updated to support IEEE 802.1X, added FB-6XX models
130	November 2019	Updated Support URL and added Event Extend Time
140	January 2020	Added M4 screw length

Table of Contents

Camera Installation

1.1 Camera Overview	5
1.2 Warnings and Cautions	5
1.3 Installation Overview	6
1.3.1 Camera Connection Options	6
1.3.2 Supplied Components	6
1.3.3 Additional Supplies	6
1.3.4 Camera Placement	7
1.3.5 Mounting Accessories	7
1.3.6 Site Preparation	8
1.3.7 Camera Mounting	8
1.4 Camera Connections	9
1.4.1 Bench Testing	9
1.4.2 Analog Video Connections	10
1.4.3 Connecting Power	10
1.4.4 Alarm Connections	10
1.4.5 Ethernet	10
1.4.6 Camera Grounding	10
1.5 Mounting the Camera	11
1.6 Camera Specifications	12

Basic Operation and Configuration

2.1 IP Camera, ONVIF Profile S Compliant	14
2.2 Camera Bench Test	14
2.3 Set IP Address using the FLIR Discovery Network Assistant (DNA)	14
2.3.1 Log in to the Camera Web Page	15
2.3.2 Live Video Page	16
2.4 Basic Camera Configuration	18
2.4.1 Setup Menu	18
2.4.2 Server Menu	19
2.5 Thermal Imaging Overview.....	27
2.6 Maintenance and Troubleshooting Tips	28

Advanced Configuration

3.1 Setup Menu	32
3.1.1 Input/Output (IO) Page	33
3.1.2 Video Setup	33
3.1.3 Thermal Image Setup - IR Page	35
3.1.4 Video Analytics Setup—FB-Series ID Only	37
3.2 Maintenance Menu	42
3.2.1 Sensor Menu	42
3.2.2 Files Menu	52
3.2.3 Product Info Menu	56



Image from a standard camera in low light



Image from a thermal camera in the same conditions

This manual describes the installation and initial configuration of the FB-Series thermal camera. The FB-Series O and the FB-Series ID are based on identical hardware. The FB-Series ID camera has software installed providing for on-board video analytics—setting of detection regions, tripwire, and classification of detected objects which is not available with the FB-Series O camera.

1.1 Camera Overview

The FB-Series cameras are components within the FLIR Thermal Fence. The video from the camera can be viewed over a traditional analog video network or it can be viewed by streaming it over an IP network using M-JPEG and H.264 encoding. The Ethernet connection also provides for camera configuration and control using either a web browser or a video management system (VMS) such as FLIR Latitude™.

The FLIR Thermal Fence combines FLIR thermal security cameras and the FLIR Latitude control and management software in a fully integrated perimeter security solution. The FLIR Thermal Fence provides automated perimeter surveillance, intrusion detection, and alert capabilities for perimeter security applications including critical infrastructure, petrochemical facilities, nuclear facilities, commercial campuses, and residential neighborhoods. The FLIR Thermal Fence gives you instant, automated threat detection and visual threat assessment capability around the clock in one easy-to-use package.

If help is needed during the installation process, contact the local FLIR service representative or call the appropriate support number listed at: <https://www.flir.com/support/>. All installers and integrators are encouraged to take advantage of the training offered by FLIR; visit <https://www.flir.com/support-center/training/> for more information.

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

1.2 Warnings and Cautions

Warning!



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

Caution!

Except as described in this manual, do not open the FB-Series camera for any reason. Damage to the camera can occur as the result of careless handling or electrostatic discharge (ESD). Always handle the camera with care to avoid damage to electrostatic-sensitive components.

Prior to making any connections, ensure the power supply or circuit breaker is switched off.

Be careful not to leave fingerprints on the FB-Series camera's infrared optics.

Operating the camera outside of the specified input voltage range or the specified operating temperature range can cause permanent damage.

1.3 Installation Overview

The FB-Series camera is an infrared thermal imaging camera for indoor or outdoor security applications. The camera mounting must support up to 5.4 lbs (2.5 kg). Refer to [Mounting Accessories, pg. 7](#) for wall and pole mounts that can be purchased from FLIR Systems, Inc.

1.3.1 Camera Connection Options

The FB-Series camera can be installed with an analog or digital (IP) video output (or both). Analog video requires a connection to a video monitor or an analog video matrix switch. The camera can be powered using Power over Ethernet (PoE) or with a conventional 24 Vac or 12 Vdc power supply. For a PoE connection, an accessory PoE power supply (also called a PoE injector) is required if the camera is not connected to a PoE switch. The maximum Ethernet cable run is 100 meters including the PoE power supply. In installations using PoE power and IP video, only a single Ethernet cable to the camera is required. The FB-Series camera is a Powered Device compliant with the IEEE 802.3af-2003 standard.

In installations using analog video and conventional power, an RG59U coaxial cable and a power cable are installed. It is recommended an Ethernet cable should also be installed for camera configuration and troubleshooting. The FB-Series camera does not support serial communications.

General Purpose Input/Output (GPIO)

The camera can receive two input signals and can provide a single output signal. By default the signals are configured for normally open alarm switch circuits. Refer to [Alarm Connections, pg. 10](#).

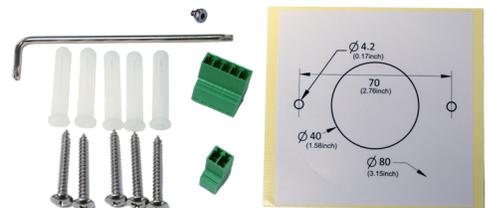
Input Signal—When an external alarm device closes a switch to complete the circuit for the camera, an input alarm is generated by the GPIO for the Alarm Manager.

Output Signal—When an output alarm is generated by the Alarm Manager for the GPIO, the camera closes its internal switch to complete the circuit for the receiving device.

1.3.2 Supplied Components

The FB-Series camera package includes these standard components:

- Fixed Camera Unit with sun shield and cable pigtail
- Power terminal block, if not using PoE
- Accessory terminal block—GPIO
- Five plastic screw anchors
- Five M4 x 31 mm screws
- Tools: Torx wrench to remove cover and spare Torx cover screw
- Installation Template



1.3.3 Additional Supplies

The installer may need to supply the following items as required (specific to the installation).

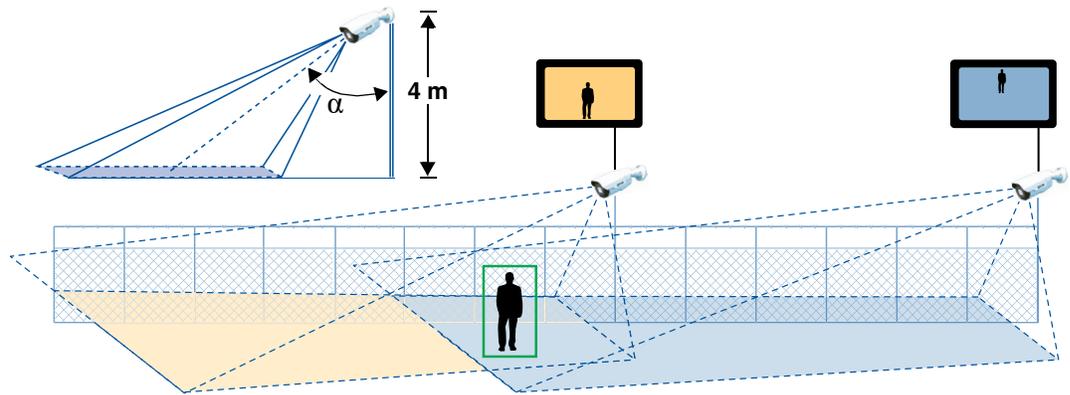
- Power supply, 24 Vac or 12 Vdc if not using PoE power for system power.
- Power cable, 2-conductor, gauge determined by cable length and supply voltage, if used for system power

Camera Installation

- Accessory cable 5-conductor for Alarm In/Out (optional)
- PoE power supply or PoE switch, if used for system power.
- Cat5e or Cat6 Ethernet cable for digital video and/or PoE for system power
- Coaxial RG59U cables (BNC connector at the camera end) for analog video
- Camera grounding strap, camera mount, electrical hardware, connectors, and tools

1.3.4 Camera Placement

For installations with multiple FB-Series ID cameras with on-board video analytics, the fields of view of cameras should overlap in order to remove all dead zones in which a camera cannot see a target “head to toe”. The camera’s on-board analytics must be calibrated to detect targets. Refer to [Video Analytics Setup—FB-Series ID Only, pg. 37](#).



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

1.3.5 Mounting Accessories

The following mounting accessories are available from FLIR Systems, Inc. for installing the FB-Series camera. For more information on available options, contact your FLIR sales representative to request details on where to get the accessories you need.



Wall Mount Junction Box CB-WLBX-62



Pole Mount Junction Box CB-PLBX-62

1.3.6 Site Preparation

There are several requirements to address prior to installation at the site. The following recommendations provide for proper installation and operation of the unit. Adhere to all local and industry standards, codes, and best practices.

- **Ambient Environment Conditions:** Avoid positioning the unit near heaters or heating system outputs. Avoid exposure to direct sunlight.
- **Safety:** Cables and electrical cords should be routed in a manner that prevents safety hazards. Ensure that nothing rests on the unit's cables or power cords.
- **Ample Air Circulation:** Leave enough space around the unit to allow free air circulation.
- **Cabling Considerations:** Using a cable longer than the manufacturer's specifications for optimal video signal may result in degradation of color and video parameters.
- **Physical Security:** The unit provides threat detection for physical security systems. In order to ensure that the unit cannot be disabled or tampered with, the system should be installed with security measures regarding physical access by trusted and untrusted parties.
- **Network Security:** The unit transmits over IP to security personnel for video surveillance. Proper network security measures should be in place to assure networks remain operating and free from malicious interference. Install the unit on the backbone of a trusted network.
- **Electrostatic Discharge Safeguards:** The unit and other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc.) shall be properly grounded to prevent electrostatic discharge.

1.3.7 Camera Mounting

The FB-Series camera can be mounted with two fasteners in the bracket slots. Alternatively, the camera can be mounted with a 1/4-20 threaded fastener on the bottom of the camera.

If using the 1/4-20 fastener on the bottom of the camera, the maximum depth of the fastener should not exceed 10.0 mm (0.4 in).

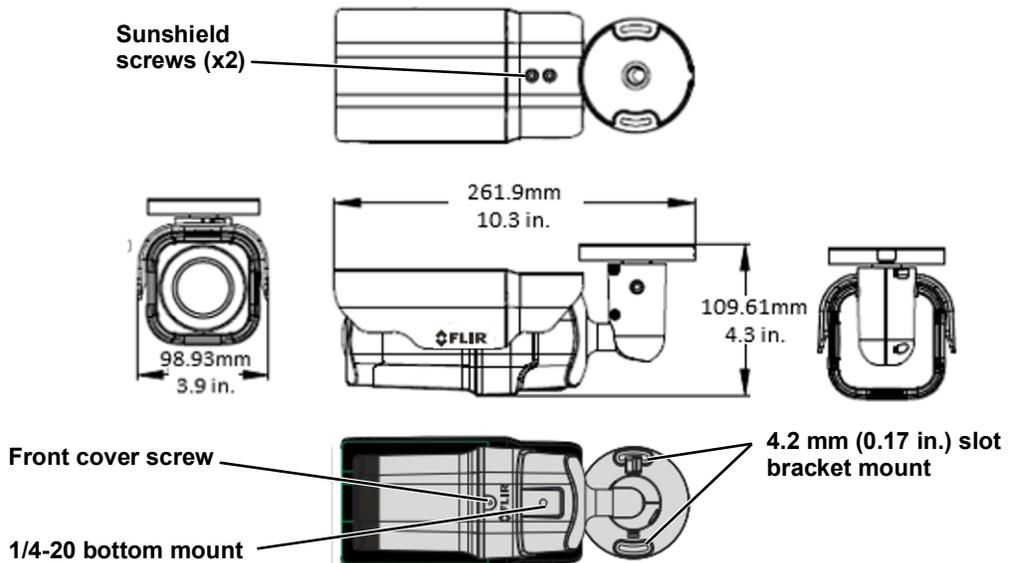
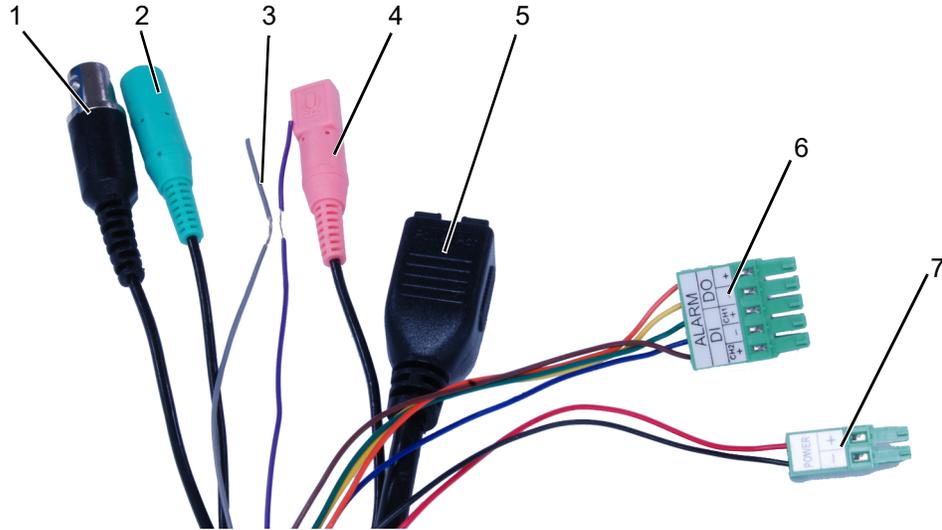


Figure 1-1: FB-Series Camera Mounting

1.4 Camera Connections



Refer to Table 1-1 for a description of these camera connections.

Table 1-1: FB-Series Camera Connections

	Connection	Purpose
1	BNC	Analog video
2	Green barrel	not supported
3	Purple D-	not supported
	Grey D+	
4	Pink barrel	not supported
5	Ethernet	PoE power, communications, IP video stream
6	5-pin plug	General purpose I/O
7	2-pin plug	Vac or Vdc power

1.4.1 Bench Testing

Note

If the camera is to be mounted on a pole or tower or other hard-to-reach location, connect and operate the camera as a bench test prior to mounting the camera in its final location.

Connect the power, Ethernet, and video, and confirm that the video can be displayed on a monitor when the power is turned on. For configuration and basic setup information using the on-board web server, refer to [Camera Bench Test, pg. 14](#) for specific details.

1.4.2 Analog Video Connections

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

1.4.3 Connecting Power

The camera can be powered with a conventional 24 Vac or 12 Vdc power supply, rather than PoE. Prior to making any connections, ensure the power supply or circuit breaker is switched off.

Table 1-2: Power Connections

1	Vac or Vdc (-)
2	Vac or Vdc (+)

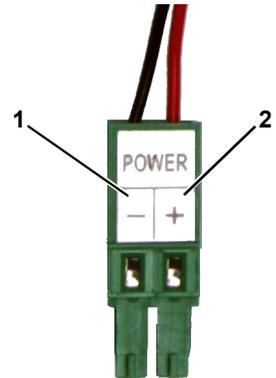


Figure 1-2: Power Connector

The camera itself does not have an on/off switch. Generally the FB-Series camera may be connected to a circuit breaker and the circuit breaker will be used to apply or remove power to the camera. If power is supplied to it, the camera will be powered on and operating.

1.4.4 Alarm Connections

Table 1-3: GPIO Connections - J5

Pin	Connection	Notes
1	Input Channel 2+	Dry alarm contact
2	Input -	
3	Input Channel 1+	
4	Output-	Relay contact 130 mA max at 300 Vac /Vdc
5	Output+	

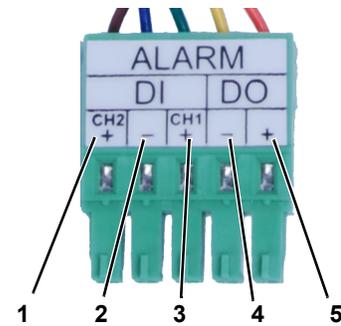


Figure 1-3: GPIO Terminal Plug

1.4.5 Ethernet

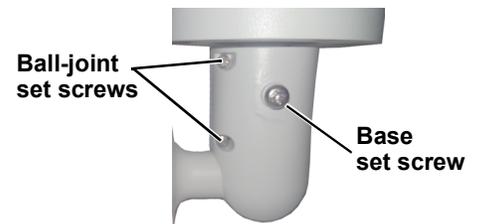
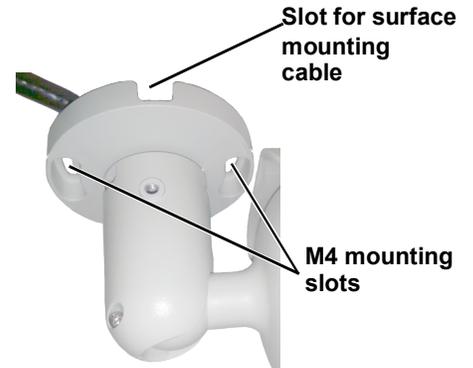
Connect a shielded Cat5e or Cat6 Ethernet cable to the RJ-45 jack. If using PoE to supply power to the camera, connect the other end of the cable to a PoE switch or PoE injector. Otherwise connect the cable to a network switch.

1.4.6 Camera Grounding

Ensure the camera is properly grounded. Failure to properly ground the camera can lead to permanent damage to the camera. Typical to good grounding practices, the camera chassis ground should be connected to the lowest resistance path possible.

1.5 Mounting the Camera

1. Place the supplied template where you will install the camera. Mark the position of the two screw holes for the base of the mounting bracket.
2. At the center of the template, a cable entry hole 40 mm (1.57") in diameter will provide for hidden cables.
3. Drill the cable entry hole for cables or use the slot for surface mounting the cables.
4. Drill holes slightly smaller than the supplied plastic screw anchor on each marked screw hole.
5. Insert the plastic screw anchors into the drilled holes.
6. Connect the camera cables and thread them through the cable entry hole. Refer to [Camera Connections, pg. 9](#) for cable connections.
7. Match the mounting slots of the camera with the plastic screw anchors at the installation location.
8. Fasten the camera with the supplied M4 screws.
9. Loosen the set screws in order to manipulate the camera positioning at the ball joint. The camera can be rotated, twisted, and pointed up or down at the ball joint.
10. Point the camera in the desired direction and fasten the screws.



1.6 Camera Specifications

Thermal Camera Specifications	Array Format	320 x 240 640 x 480
	Detector Type	Long-Life, Uncooled VOx Microbolometer
	Effective Resolution	320 x 240: 76,800 640 x 480: 307,200
	Spectral Range	8 μm to 14 μm
	Lens	Athermalized, focus-free
Camera Models	Field of View (Focal Length) for available 320 x 240 camera lens configurations.	
	FB-309	9° HFoV (24 mm)—12 μm pixel pitch
	FB-312	12° HFoV (18 mm)—12 μm pixel pitch
	FB-324	24° × 19° (12.8 mm)—17 μm pixel pitch
	FB-349	49° × 37° (6.8 mm)—17 μm pixel pitch
	FB-393	93° × 70° (3.7 mm)—17 μm pixel pitch
	Field of View (Focal Length) for available 640 x 480 camera lens configurations.	
	FB-618	18° HFoV (24 mm)—12 μm pixel pitch
	FB-632	32° HFoV (14 mm)—12 μm pixel pitch
	FB-650	50° HFoV (8.7 mm)—12 μm pixel pitch
	FB-695	95° HFoV (4.9 mm)—12 μm pixel pitch
	Camera Platform Type	Bullet
Video	Composite Video	NTSC or PAL—switchable from the Video Setup web page.
	Video Compression	Two independent channels of streaming H.264 or M-JPEG
	Streaming Resolution	Native: 320 x 256/640 x 512
	Thermal AGC Modes	Optimized Video Analytics AGC Mode and manual controls for Brightness (ITT Mean/gamma), Contrast (Max Gain), Sharpness (DDE Gain), and AGC Filter (damping factor)
	Video Analytics AGC Mode	Engaged when analytics is enabled
	Thermal AGC Region of Interest (ROI)	Default, Presets and User definable to insure optimal image quality for subjects of interest
	Image Uniformity Optimization	Automatic Flat Field Correction (FFC) - Thermal and Temporal Triggers
System Integration	Ethernet	10/100 Mbps
	Serial Control Interfaces	Nexus SDK for comprehensive system control and integration; Nexus CGI for http command interfaces; ONVIF Profile S
	External Analytics Compatible	Yes
Measurement and Analysis	Analytics Features	Region Entrance/Intrusion Detection, Crossover/Fence Trespassing; Auto/Manual Depth Setup, Human and Vehicle Rules, Hand-off target to autonomous PTZ tracking, Tampering Detection
	Analytics Management	Web-based configuration and management, Masking of analytic detection areas, adjustable sensitivity, automatic responses, remote I/O control

Camera Installation

General	Weight	2.3 lb (1 kg) with sun shield
	Dimensions (L,W,H)	11.1" x 3.8" x 3.7" (285 mm x 96 mm x 94 mm) with sun shield and fully extended mounting arm
	General Purpose Input/ Output (GPIO)	Two input dry alarm contacts; One output relay contact 130 mA max at 300 Vac /Vdc
	Input Voltage dc	12 Vdc ($\pm 10\%$)
	Input Voltage ac	24 Vac ($\pm 10\%$)
	Input Voltage PoE	IEEE 802.3af-2003 standard
	Power Consumption	17 W at 12 Vdc maximum with heaters 13 VA at 24 Vac maximum with heaters
	Mounting Provisions	One 1/4-20" threaded holes on bottom. Two M4 hole slots on mounting arm.
	Shipping weight	3.85 lbs (1.75 kg)
	Shipping Dimensions	14.375"(L) x 7.375"(W) x 7"(H)
Environmental	IP rating (dust and water ingress)	IP66
	Operating temperature range	-40 °C to 50 °C (-40 °F to 122 °F) cold start
	Storage Temperature range	-20 °C to 70 °C (-4 °F to 158 °F)
	Humidity	10% to 90% relative
	Approvals	FCC Part 15 (Subpart B, Class A), CE mark, EN55032, EN55024, RoHS, WEEE

This chapter provides basic information on how to operate the FB-Series camera. A bench test can be used to verify camera operation before the camera is configured for the local network. This chapter also provides general configuration information.

2.1 IP Camera, ONVIF Profile S Compliant

When the camera is connected to the network it functions as a server; it provides services such as camera control, video streaming, network communications, and geo-referencing capabilities. The communications protocol used is an open, standards-based protocol that allows the server to communicate with a video management client, such as FLIR Latitude™ or with a third-party VMS client, including systems that are compatible with ONVIF Profile S. These clients can be used to control the camera and stream video during day-to-day operations. Refer to the individual product web page at <https://www.flir.com/browse/security/thermal-security-cameras/> for a listing of supported VMS clients.

2.2 Camera Bench Test

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

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

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

If using a conventional power supply, connect the camera to a network switch with an Ethernet cable, and connect a PC or laptop to the switch also. Use a web browser to access and test the camera as described below, and if necessary make configuration changes prior to installation.

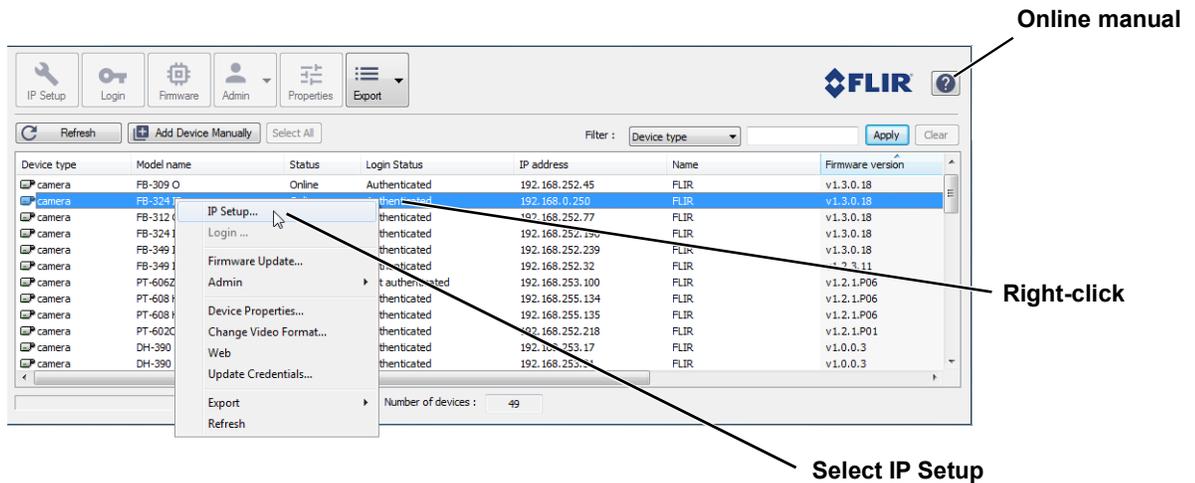
Once the camera is connected to a network and powered on, set camera network parameters using the FLIR Discovery Network Assistant (DNA) software, perform a bench test by using a web browser to view the video and control the camera, or view video in the local Network Video Management System (for example, FLIR Latitude™). The DNA software does not require a license to use and is a free download from the individual product web page at: <https://www.flir.com/browse/security/thermal-security-cameras/>.

2.3 Set IP Address using the FLIR Discovery Network Assistant (DNA)

The FB-Series camera is shipped with Dynamic Host Configuration Protocol (DHCP) IP addressing. If the existing network has a DHCP server, the camera will be assigned an appropriate IP address. If the network does not have a DHCP server, the camera will default to an IP address of 192.168.0.250. Configuring the camera for IP communications generally involves the following steps:

- Step 1 Connect the Ethernet port of the camera to the existing IP camera network.
- Step 2 Connect a PC or laptop to the same network.
- Step 3 From the PC connected to the camera network, use the DNA utility to discover and display the camera's current IP address.
 - a Download the DNA utility.

- b Unzip the utility, then double-click to run the executable file (**DNA.exe**). All the units on the VLAN are discovered.
- c For additional instructions on using DNA, refer to the DNA User's Manual available in the Help (?) link while the software is running.



Step 4 Right-click on the camera, select **IP Setup** to change the IP address. When set to DHCP, if a DHCP server is not available on the network, the IP address will default to 192.168.0.250.

Step 5 Double-click the camera in DNA's **Discovery List** to open the camera's web server **Login** page in Internet Explorer or point your web browser to the camera's IP address.



Step 6 Enter the default user name (**admin**) and password (**admin**) to open the **Live Video** page. Refer to [Live Video Page, pg. 16](#).

2.3.1 Log in to the Camera Web Page

With a web browser, log in to the camera using one of three User Names: **user**, **expert**, and **admin**. By default, the passwords are: **user**, **expert**, and **admin**, respectively. Login passwords should be changed (**admin** login required) to prevent unauthorized access (refer to [Security Options, pg. 26](#)).

Open a web browser and enter the camera's IP address. The login screen with a picture of the camera will appear. Enter **user** for the User Name and **user** for the Password, and click Log in.

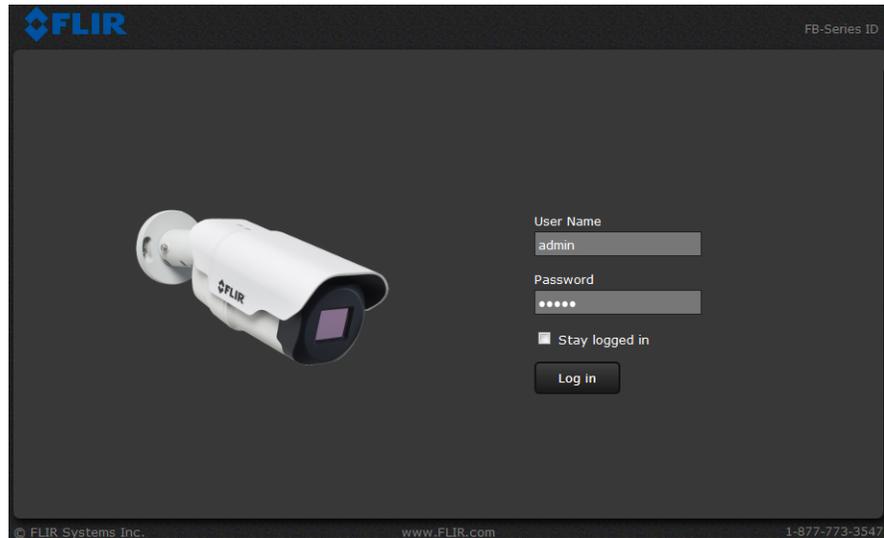


Figure 2-1: Camera Web Page Login Screen

2.3.2 Live Video Page

The **Live Video** page displays a live image from the camera on the left part of the screen and at the top of the screen menu choices: including **Live Video** (the red text indicates it is selected), **Help**, and **Log out**. The **expert** and **admin** logins provide additional menu choices.

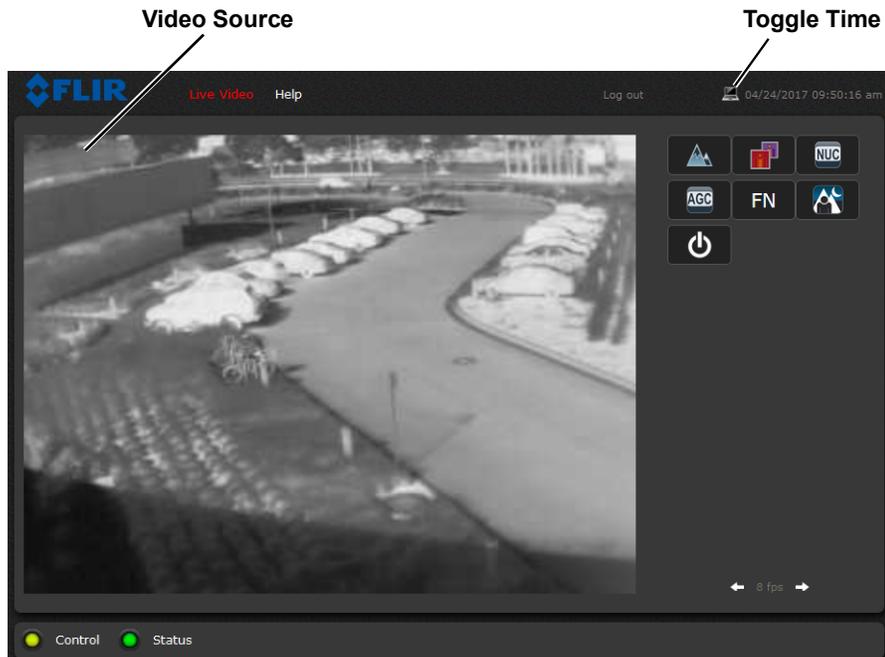


Figure 2-2: Live Video Web Page

In the lower right of the web page there is a frame rate selector. This selector allows the user to change the rate at which the frames are displayed in the browser from the default 8 fps up to 16 fps. This rate controls the user's own web browser only, and does not affect the video streams to other users or to an NVR. For slow communication links, if there is a problem displaying the video image, it may help to slow down the frame rate.

Help

The **Help** menu displays software version information. If it is necessary to contact FLIR Technical Support for assistance, it will be helpful to have the information from this page on hand. For information about the camera refer to [Product Info Menu, pg. 56](#) (requires Admin login).

Log out

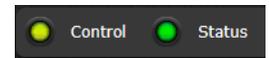
Use this button to disconnect from the camera and stop the display of the video stream. If a web session is inactive for 20 minutes, it will be stopped and it will be necessary to log in again.

Toggle PC/Camera time

Use this button to display either the PC time or the camera time. To set the camera time refer to [Date and Time, pg. 22](#).

Camera Control and Status

In the lower left of the screen are two indicator “lights”: Control and Status. Initially the Control light is off, as in the image above, indicating the user is not able to control the camera immediately. When multiple users are connected to a camera, only one user at a time can issue commands to the camera. If another user has control of the camera, the Control light is yellow.



A user is able to request control of the camera by clicking on the yellow or black “light”, or simply by sending a command to the camera. The Status light may turn off temporarily while waiting for the response from the camera. After a short pause, the Control light should turn green.

If a command is sent to the camera when the user does not have control, the command will not be executed, and it is necessary to send the command again once the light is green.

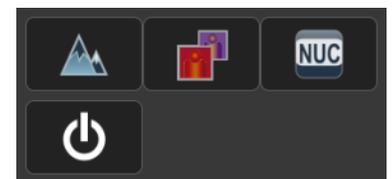
In addition, when the cursor is moved over the video, a snapshot button also appears in the upper right of the screen. After clicking the snapshot button, the video image is saved as a jpeg file and the browser will provide prompts depending on which browser is being used.



Web Control Panel

The control buttons on the right side of the page provide a way to control the camera in a limited number of ways. When the mouse cursor is positioned over a button, a tool tip is displayed.

This same web interface is used with various FLIR cameras—some are fixed, such as the FB-Series cameras, and some are pan/tilt cameras. The control panel may appear different for different FLIR cameras.



The following buttons appear for FB-Series cameras:



Toggle Polarity

This button changes the polarity of the assigned colors to the different temperatures in a scene. In the black and white palette for example, hot objects are displayed as white and cold objects as black, or vice versa.



Toggle Palette

This button causes the camera to cycle through six different look up table (LUT) color palettes. Depending on the subjects viewed, one color palette may be preferable to the others. The Toggle Polarity button allows access to six more palettes (refer to [Misc. \(Lookup Table\)](#), pg. 36).



Perform IR NUC Calibration

This button causes the camera to perform a Non-Uniformity Correction operation (refer to [Image freezes momentarily](#), pg. 28).



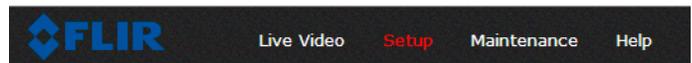
Analytics On/Off—FB-Series ID Only

The FB-Series ID camera Intrusion Detection analytics can be enabled or disabled from the Live Video page. Detection area and tripwire alarms must be setup prior to use. Refer to [Video Analytics Setup—FB-Series ID Only](#), pg. 37.

2.4 Basic Camera Configuration

The following procedures describe how to do the most common bench test camera configuration steps, such as setting the camera IP address and hostname and changing the user password. To make these changes, it is necessary to login using the **expert** user account. Additional setup and configuration options required after the camera has been installed in its final location are described after the basic steps are given, refer to [Advanced Configuration](#), pg. 32.

2.4.1 Setup Menu



The **Setup** menu is used for GEO Settings (Latitude and Longitude location), Video setup, thermal (IR) camera setup, and defining Video Analytics motion detection zones for the FB-Series ID camera. For additional details, refer to [Setup Menu](#), pg. 32.

Adjustments to the IR settings should only be made by someone who has expertise with thermal cameras and a thorough understanding of how the various settings affect the image. In most installations, the only camera settings needed are available from the Web Control panel on the Live Video page (Palettes and Polarity). Haphazard changes can lead to image problems including a complete loss of video. Additional information is provided in [Thermal Image Setup - IR Page](#), pg. 35.

When making configuration changes using the **Setup** page, most of the changes take effect immediately, and it is not necessary to start and stop the server. However it is necessary to save the changes (with the Save Settings button at the bottom of the page) if it is desirable to use the new settings as a default when the camera is powered on.

When a user logs in as **admin**, a complete **Maintenance** menu is available (refer to [Maintenance Menu](#), pg. 42). The **Maintenance** menu also provides access to other configuration options.

2.4.2 Server Menu

When a user logs in as **expert** or **admin**, the **Maintenance Server** menus are available. When the **Server** menu is selected, the **LAN Settings** page appears.

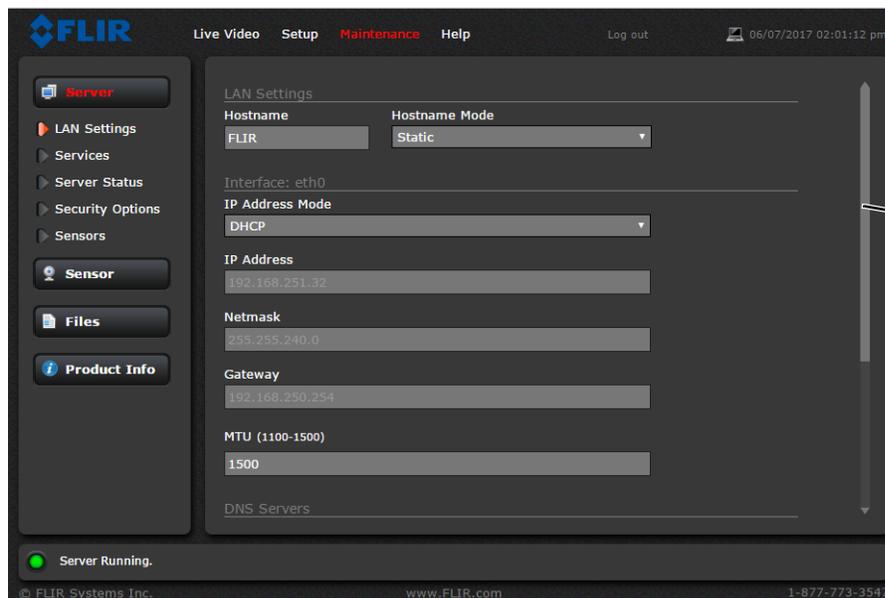
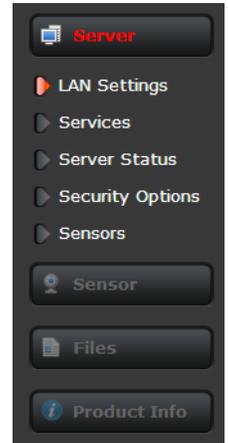
The basic camera configuration steps are accessed through the **Maintenance Server** menu, using the menus on the left side of the page. The **LAN Settings**, **Services**, and **Security Options** selections are described below. The **expert** login has access to these **Server** pages, but will only see the security settings for the expert login.

With most configuration changes through the **Maintenance** menu, it is necessary to save the changes, then stop and restart the server to make the changes take effect.

LAN Settings: The **LAN Settings** page can be used to set the hostname, default gateway, and IP address for the camera. Scroll down to see settings for Domain Name System (DNS) server.

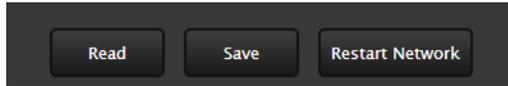
IP Address

The IP Address mode can be set to DHCP or Static. When set to DHCP, if a DHCP server is not available on the network, the IP address will default to 192.168.0.250. To set the IP address using DNA, refer to [Set IP Address using the FLIR Discovery Network Assistant \(DNA\)](#), pg. 14.

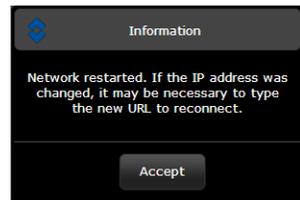
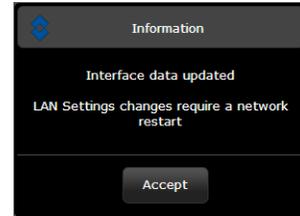


Scroll down to Save

When the IP address is changed and the **Save** button is clicked, a pop-up message will appear to indicate the network interface must be restarted.



Once the IP address of the camera is changed, the PC may no longer be on the same network and therefore may not be able to access the camera until the IP address on the PC is changed also.



IEEE 802.1X Security: The 802.1x standard is designed to enhance the security of local area networks. The standard provides an authentication framework, allowing a user to be authenticated by a certification authority (CA). The FB-Series supports authentication using either Transport Layer Security (TLS) protocol or Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP MSCHAPv2).

Note

The camera must be connected to a switch or other device on the network that supports IEEE 802.1x.

Configure IEEE 801.1x authentication using TLS

Step 1 On the **LAN Settings** page, scroll down to **802.1x security**.

Step 2 Check **Use 802.1x security**.

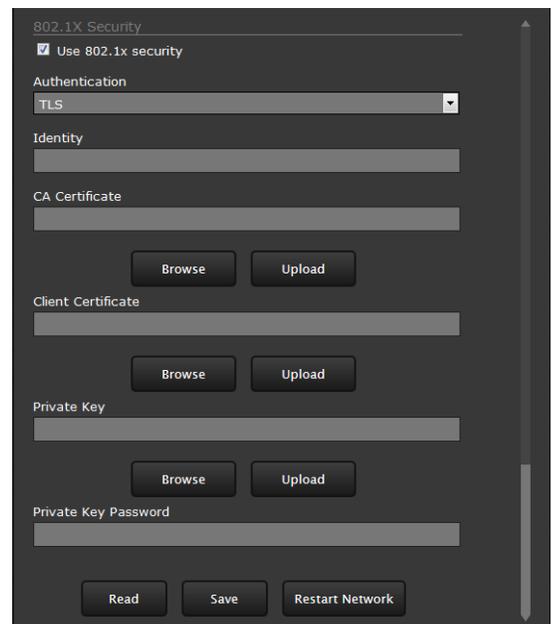
Step 3 From the **Authentication** drop-down menu, select **TLS**.

Step 4 In the **Identity** text box, enter the name associated with the client certificate.

Step 5 If uploading a PKCS #8 certificate file, use the **Browse** and **Upload** buttons to upload the associated **CA Certificate** from the server provided by the network administrator. Typical file extensions will be *.cer, *.crt, or *.der.

If uploading a PKCS #12 certificate file, you do not need to upload a CA Certificate.

Step 6 Use the **Browse** and **Upload** buttons to upload the **Client Certificate** from the server provided by the network administrator.



Step 7 Using the **Browse** and **Upload** buttons, upload the **Private Key** and enter the **Private Key Password** associated with the identity. The **Private Key Password** field can be left blank if a password is not required.

If uploading a PKCS #8 file, the private key must be a valid PKCS #8 file. A typical key has a “.per” file extension.

If uploading a PKCS #12 file, the private key must be a valid PKCS #12 file. A typical key has a “.p12” or “.pfx” file extension.

Step 8 Click **Save** and then **Restart Network** to save and implement the configuration.

To configure IEEE 801.1x authentication using PEAP MSCHAPv2

Step 1 On the **LAN Settings** page, scroll down to **802.1X Security**.

Step 2 Check **Use 802.1x security**.

Step 3 From the **Authentication** drop-down menu, select **PEAP(MSCHAPv2)**.

Step 4 In the **Identity** text box, enter the name associated with the client certificate.

Step 5 Use the **Browse** and **Upload** buttons to upload the associated **CA Certificate** from the server provided by the network administrator. Typical file extensions will be *.cer, *.crt, or *.der.

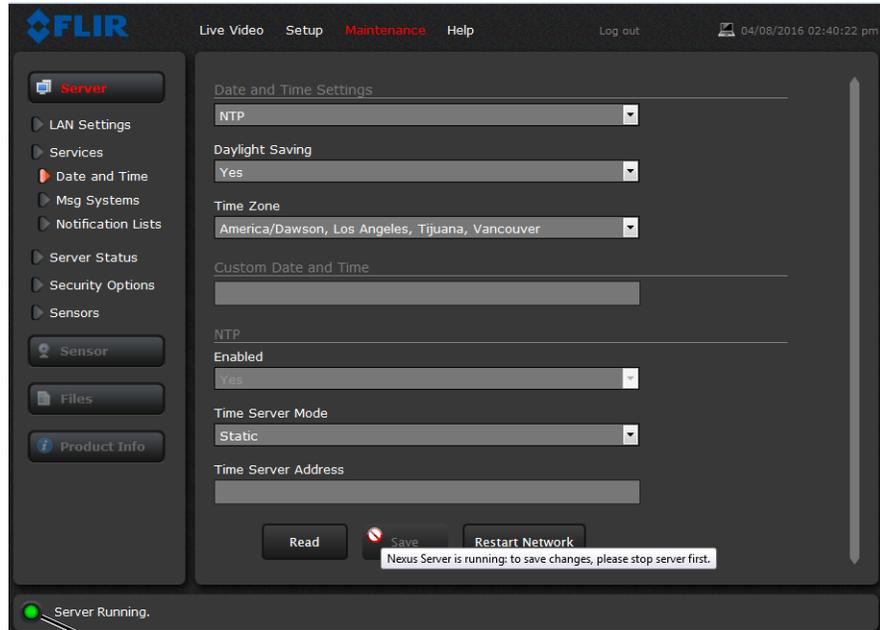
Step 6 In the **Anonymous Identity** text box, enter the Anonymous Identity if required.

Step 7 In the **Password** text box, enter the password associated with the Identity.

Step 8 Click **Save** and then **Restart Network** to save and implement the configuration.

Services Menu

Date and Time: The **Date and Time** settings page is used to configure the date and time settings. The date, time, and time zone can be obtained from an NTP server, or can be entered manually. If NTP mode is selected, the NTP server information can be entered.



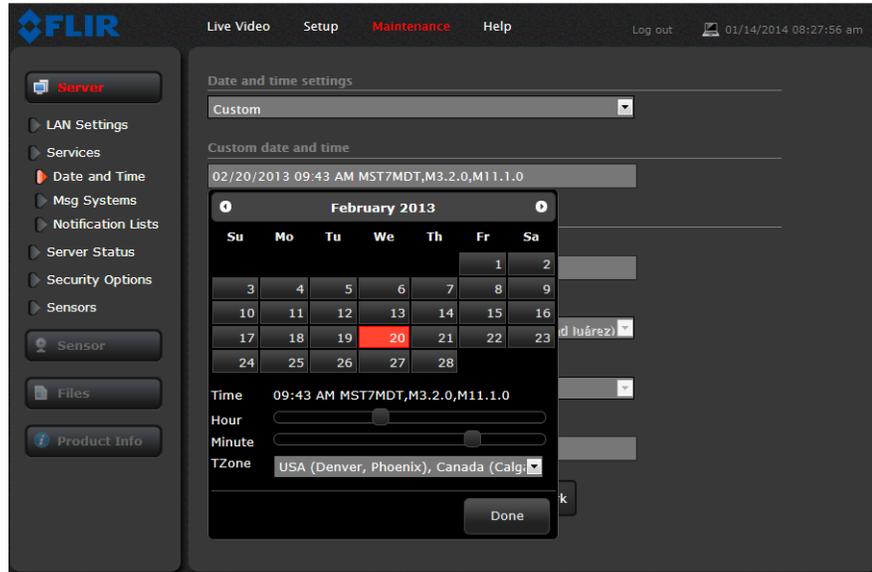
Toggle Server (Stop/Start)

Note

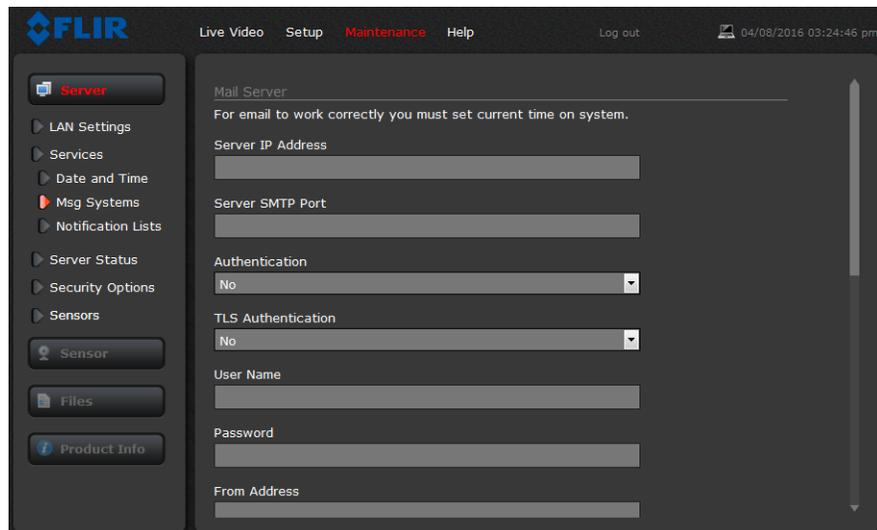
The Nexus server must be stopped before changes can be saved.

Set the date and time parameters, then select the Save button at the bottom of the page. After saving the settings, reboot the system. Refer to [Server Status, pg. 24](#).

If the Custom mode is selected, a pop-up window allows the information to be entered manually.

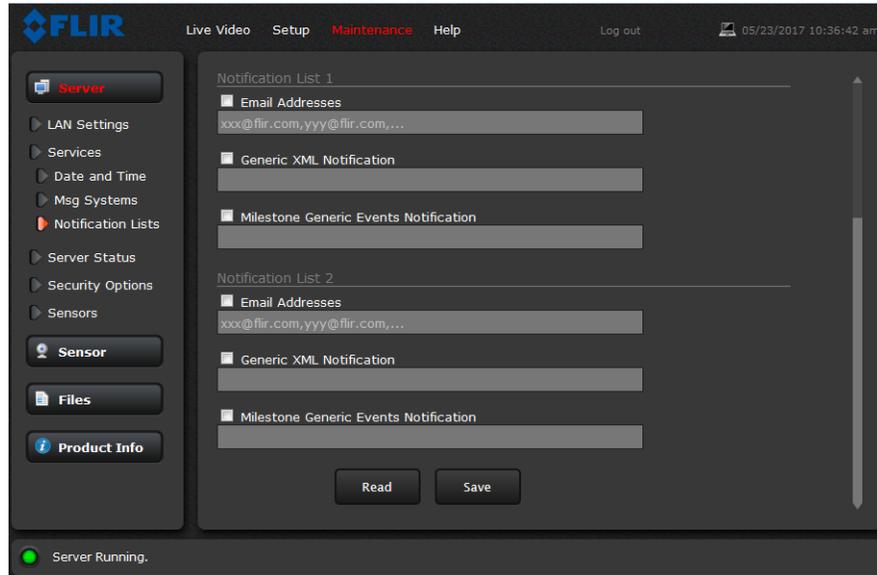


Msg Systems: Use the **Msg Systems** page to setup a connection to a mail server to send outgoing email notifications.

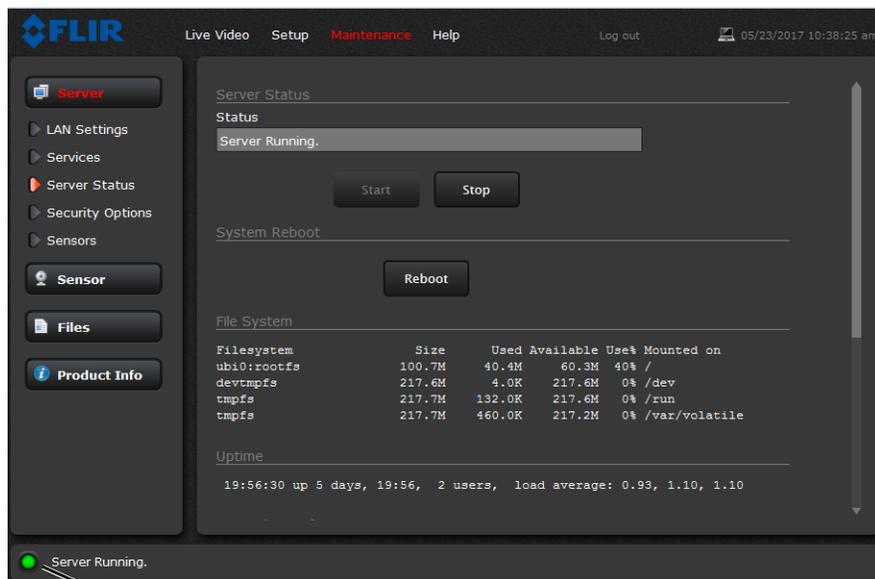


If the email server is on a different network, ensure the IP default gateway and DNS servers are configured in the LAN Settings; refer to [LAN Settings, pg. 19](#). Configure the Msg Systems page with mail server information and then click **Save**.

Notification Lists: Use this page to setup multiple email addresses and other notifications that can be sent as a result of alarms being processed by the Alarm Manager.



Server Status: The **Server Status** page provides an indication of the current server status (either running or stopped) and buttons for starting or stopping the server or for rebooting the system.



Toggle Server (Stop/Start)

After making configuration changes, it is necessary to save the changes to the server (there is a **Save** button at the bottom of each configuration page). The configuration changes do not take effect immediately. Generally, it is also necessary to stop and restart the server for the changes to become effective. The server has a configuration that is active and running, and another configuration that is saved (and possibly different than the running configuration).

Basic Operation and Configuration

The message at the bottom of the page indicates the saved configuration is different than the active (running) configuration, and it is necessary to restart the server.

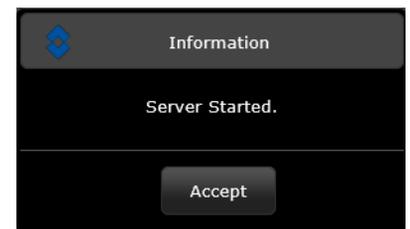
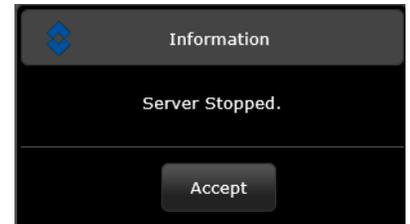
You must restart the server for the changes to be effective.

It may take up to 20 seconds or more to stop the server, especially when there are multiple video streams open. Be patient when stopping the server.

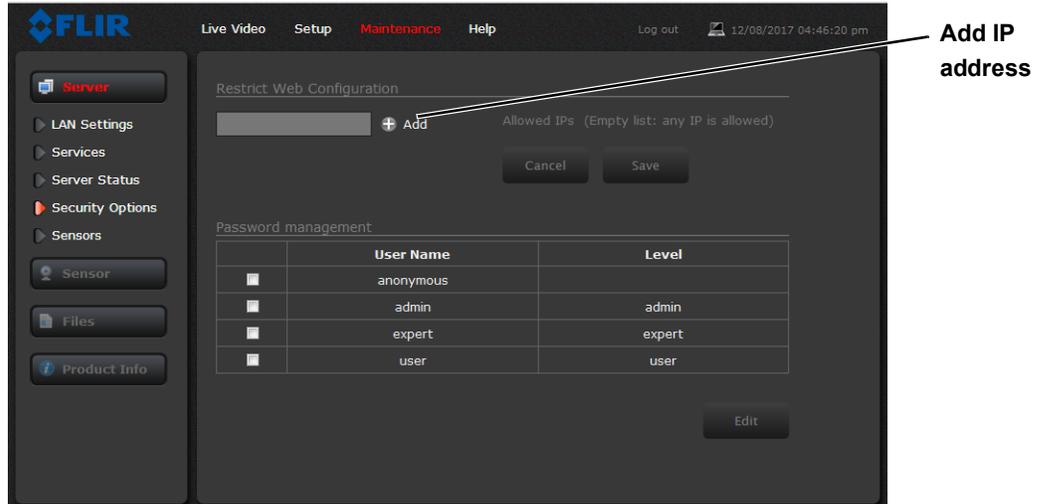
When the server is stopped and the page is refreshed, the status will show Server Stopped and the Start button will be enabled.

Click on the Start button to restart the server, and when the page refreshes, the status will again show Server Running. The Start button will be replaced by a Stop button when the startup procedure has completed.

After stopping the server, if the server is not manually started within one hour, the server automatically starts.



Security Options: Use the **Security Options** page to restrict access through the camera web server to specific IP addresses and to set or change passwords. The **admin** login may change or set all passwords. The expert login can only change the expert password.



As an additional security measure, limit which computers have access to the web browser interface. Simply add a computer's IP address and click Add. After all the allowed IP addresses are entered, select the **Save** button to save the changes.

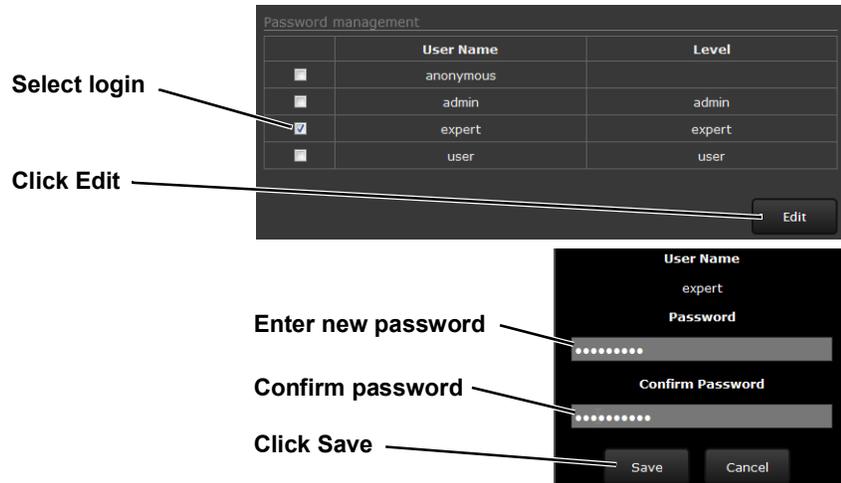
Note

A VMS Remote to the camera, ONVIF or Nexus CGI, uses the same password as the web interface. Refer to [VMS Remote, pg. 44](#).

To maintain security of the system set new passwords for each of the three login accounts (requires the **admin** login).

- **user**—The user account can only use the **Live Video** page and controls.
- **expert**—The expert account can use the **Live Video** page, the camera **Setup** page, the Server pages on the **Maintenance** menu, and set the password for the expert login.

- **admin**—The admin account can use all pages and set all passwords.



2.5 Thermal Imaging Overview

The thermal camera makes an image based on temperature differences. In the thermal image, by default the hottest item in the scene appears as white and the coldest item is black, and all other items are represented as a gray scale value between white and black.

Both thermal and daylight cameras have detectors (pixels) that detect energy. One difference between thermal and daylight cameras has to do with where the energy comes from to create an image. When viewing an image with a daylight camera, there has to be a source of visible light (something hot, such as the sun or lights) that reflects light off the objects in the scene. The same is true with human eyesight; the vast majority of what people see is based on **reflected** light.

The thermal camera, on the other hand, detects energy that is **directly radiated** from objects in the scene. Most objects in typical surroundings are not hot enough to radiate visible light, but they easily radiate energy in the portion of the infrared spectrum that the camera can detect, the long wave infrared (LWIR). Even very cold objects, like ice and snow, radiate this type of energy.

This is why hot objects such as parts on an engine and exhaust pipes appear white, while the sky, puddles of water and other cold objects appear dark (or cool)¹. Scenes with familiar objects will be easy to interpret with some experience. The camera automatically optimizes the image to provide the best contrast in most conditions, and in some cases other settings can be used to further improve the image.



The performance of the camera will likely vary throughout the day. After sunset, objects warmed by the sun will appear warmest. Early in the morning, many of these objects will appear cooler than their surroundings, so be sure to look for subtle differences in the scene, as opposed to just hot targets.

1. By default, hot objects are represented as white and cold objects as black. The Black Hot polarity setting, displays hot objects as black and cold objects as white. Refer to [Toggle Polarity, pg. 18](#).

2.6 Maintenance and Troubleshooting Tips

If help is needed during the installation process, contact the local FLIR representative, or visit the FLIR Support Center at: <https://www.flir.com/support/>. FLIR Systems, Inc. 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 FLIR training web page: <https://www.flir.com/support-center/training/>.

Cleaning

Great care should be used with your camera's optics. They are delicate and can be damaged by improper cleaning. The FB-Series thermal camera lenses and windows are designed for a harsh outdoor environment and have a coating for durability and anti-reflection, but may require cleaning occasionally. FLIR Systems, Inc. suggests that you clean the lens when image quality degradation is noticed or excessive contaminant build-up is seen on the lens.

Note

Do not disturb or move camera during cleaning. The detection analytics on the FB-Series ID camera are set and calibrated based on the exact position and camera angle. Inadvertent realignment may 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 the front window of the camera gets water spots, wipe it with a clean soft cotton cloth dampened with fresh water.

Do not use abrasive materials, such as paper or scrub brushes as this will possibly damage the lens by scratching it. Only wipe the lens clean when you can visually see contamination on the surface.

Use the following procedure and solvents, as required:

- Acetone – removal of grease
- Ethanol – removal of fingerprints and other contaminants
- Alcohol – final cleaning (before use)

Step 1 Immerse lens tissue (optical grade) in Alcohol, Acetone, or Ethanol (reagent grade).

Step 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).

Step 3 Repeat until the lens is clean. Use a new tissue each time.

Image freezes momentarily

By design, the camera image freezes momentarily on a periodic basis during the Flat Field Correction (FFC) cycle (also known as Non-Uniformity Correction or NUC). Every so often, the image will momentarily freeze for a fraction of a second while the camera performs a flat field correction. A shutter activates inside the camera and provides a target of uniform temperature, allowing the camera to correct for ambient temperature changes and provide the best possible image.

No video

If the camera will not produce an image, check the video connection at the camera and at the display. If the connectors appear to be properly connected 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 video cabling is suspected as a possible source of the problem, plug a monitor into the BNC connection inside the camera and determine if it produces an image.

When the camera is powered on, it will do a NUC operation shortly after startup. If it is uncertain if the camera is receiving power, it may be useful to listen to the camera to hear if the click-click of the shutter mechanism can be heard. It may only be possible to perform this test when the camera is on a work bench rather than in its installed position.

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

Performance varies with time of day

There may be differences in the way the camera performs at different times of the day, due to the diurnal cycle of the sun. Recall that the camera produces an image based on temperature differences.

At certain times of the day, such as just before dawn, the objects in the image scene may all be roughly the same temperature. Compare this to imagery right after sunset, when objects in the image may be radiating heat energy that has been absorbed during the day due to solar loading. Greater temperature differences in the scene will allow the camera to produce high-contrast imagery.

Performance may also be affected when objects in the scene are wet rather than dry, such as on a foggy day or in the early morning when everything may be coated with dew. Under these conditions, it may be difficult for the camera to show the temperature of the object itself, rather than of the water coating.

Unable To Communicate Over Ethernet

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

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

Unable to View Video Stream

If the video stream from the camera is not displayed, it could be that the packets are blocked by the firewall, or there could be a conflict with video codecs that are installed for other video programs.

When displaying video with FLIR Latitude or a VMS for the first time, the Windows Personal Firewall may ask for permission to allow the video player to communicate on the network. Select the check boxes (domain/private/public) that are appropriate for the network.

If necessary, test to 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:

```
rtsp://192.168.0.250:554/stream1/sensor1, and  
rtsp://192.168.0.250:554/stream2/sensor1
```

Port 554 is the standard RTSP port as well as the default for the camera. Typically, if the default port has not been changed, the port can be left out of the streaming command, such as:

```
rtsp://192.168.0.250/stream1/sensor1.
```

In addition, to maintain compatibility with legacy systems the stream names are aliased as:

```
ch0 = stream1/sensor1 and ch1 = stream2/sensor1.
```

The video streams can be accessed with the shortened strings, such as `rtsp://192.168.0.250/ch0`.

Refer to [Video, pg. 33](#) for additional information on RTP settings and stream names.

Unable to control the camera

If the camera does not respond to commands, the user may not have control of the camera. The web server allows two sessions to be connected to the camera at a time. By default, control of the camera will automatically be requested.

Noisy image

With the analog video signal, 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 losses, the longer the cable is (or the smaller the wire gauge/thickness), the more severe the losses become; and the higher the signal frequency, the more pronounced the losses. Unfortunately this is one of the most common and unnecessary problems that plagues video systems in general.

Cable characteristics are determined by a number of factors (core material, dielectric material, and shield construction, among others) and must be carefully matched to the specific application. Moreover, the transmission characteristics of the cable will be influenced by the physical environment through which the cable is run and the method of installation. Use only high quality cable and ensure the cable is suitable to the environment.

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

Image too dark or too light

By default the FB-Series thermal camera uses Automatic Gain Control (AGC) settings that have proven to be superior for most applications while also responding automatically to varying conditions. The installer should keep in mind that the sky is quite cold and can strongly affect the overall image. Slightly moving the camera to include (or exclude) items with hot or cold temperatures will influence the overall image. For example, a very cold background (such as the sky) could cause the camera to use a wider temperature range than appropriate.

Eastern or Western Exposure

Once installed, the camera may point directly east or west, and this may cause the sun to be in the field of view during certain portions of the day. We do not recommend intentionally viewing the sun, but looking at the sun will not permanently damage the sensor. In fact the thermal imaging camera often provides a considerable advantage over a conventional camera in this type of back-lit situation. However, the sun may introduce image artifacts that will eventually correct out and it may take some time for the camera to recover. The amount of time needed for recovery will depend on how long the camera was exposed to the sun. The longer the exposure, the longer the recovery time needed.



Figure 2-3: Images facing sun from standard camera (left) and thermal camera (right)

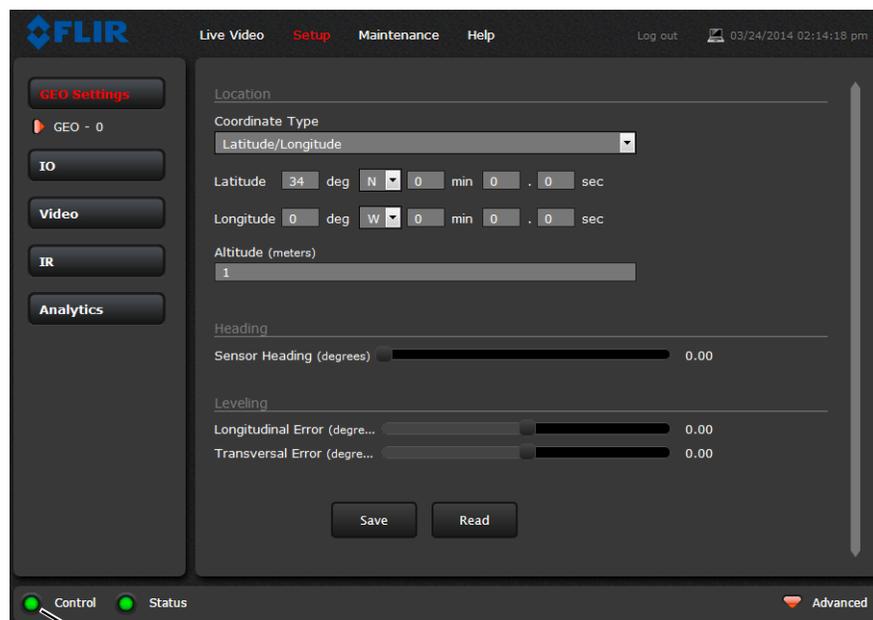
In this chapter, additional setup and configuration settings related to the following topics are described:

- Setting up the video streams to optimize quality and network performance
- Selecting NTSC or PAL analog video format
- Optimizing the thermal image
- Setting up detection areas for Analytics
- Configuring alarm responses and email notifications
- Configuring the camera to work with a third-party VMS (ONVIF)

When configuration changes are made with the web browser, the settings are saved to a configuration file. It is a good idea to make a backup of the existing configuration file prior to making changes, and another backup once the changes are finalized. If necessary the camera can be restored to its original factory configuration or one of the saved configurations (refer to [Files Menu](#), pg. 52).

3.1 Setup Menu

It is necessary to have control of the camera to make Setup changes. Changes made through the **Setup** menu have an immediate effect (it is not necessary to stop and restart the server). To use these settings at power up, it is necessary to save the changes ([Save Settings](#), pg. 36).



Camera Control

3.1.1 Input/Output (IO) Page

The IO Info page shows a summary of the status of the GPIO signals.

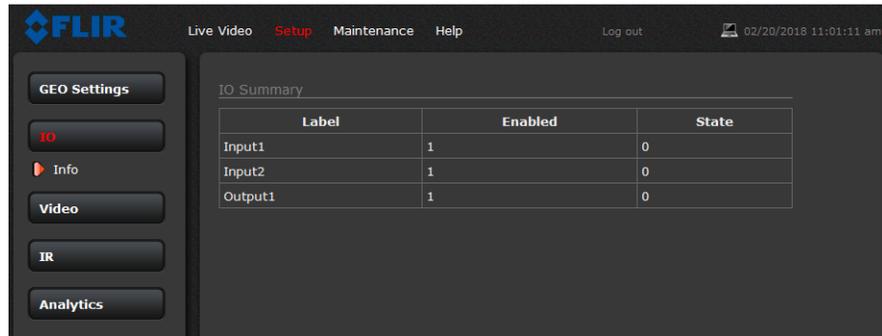
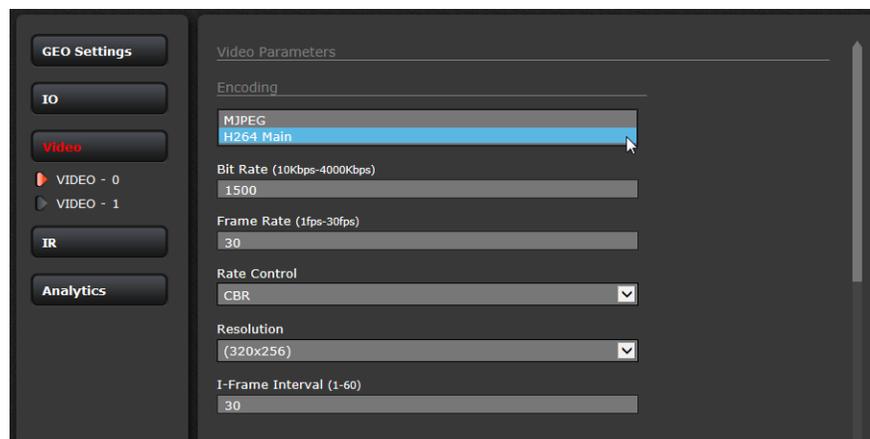


Table 3-1: GPIO Labels

Alarm Input1	User GPIO signals are enabled by default. (Refer to General Purpose Input/Output (GPIO) , pg. 6.)
Alarm Input2	
Alarm Output	

3.1.2 Video Setup

Video: By default, two video streams are enabled for the camera: Video 0 and Video 1. Both video streams are available for viewing from a client program such as FLIR Latitude, a stand-alone video player, or a third-party VMS (including ONVIF systems). To modify parameters that affect a particular IP Video stream from the camera, select the appropriate link (for example, **Video - 0**).



With the factory configuration, the default parameters provide high-quality full frame-rate video streams with reasonable bandwidth usage. In general, for most installations it will not be necessary to modify the default parameters. However in some cases, such as when a video stream is sent over a wireless network, it may be useful to “tune” the video stream to try to reduce the bandwidth requirements. The Encoding parameters are described below.

After making adjustments, scroll down to save the changes through power cycles.

Advanced Configuration

The parameters in the Encoding section will have a significant impact on the quality and bandwidth requirements of the video stream. Use the default values initially, and then individual parameters can be modified and tested incrementally to determine when bandwidth and quality requirements are met.

For the video streams, the Codec options are H.264 or MJPEG.

The Bit Rate parameter is only used when the Rate Control parameter is set to CBR (Constant Bit Rate). With the CBR setting, the system attempts to keep the video at or near the target bit rate.

With Rate Control set to VBR (Variable Bit Rate) the Bit Rate parameter is replaced with a Quality parameter.

The I-Frame Interval parameter 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 number means fewer I-frames are sent and therefore results in possibly lower bandwidth and possibly lower quality.

The video streaming is done using a protocol generally referred to as Real-time Transport Protocol (RTP), but there are actually many protocols involved, including Real-Time Transport Control Protocol (RTCP) and Real Time Streaming Protocol (RTSP). The default value for the stream from VIDEO - 0 is stream1/sensor1.

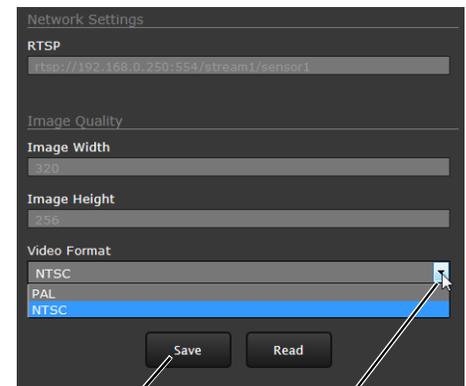
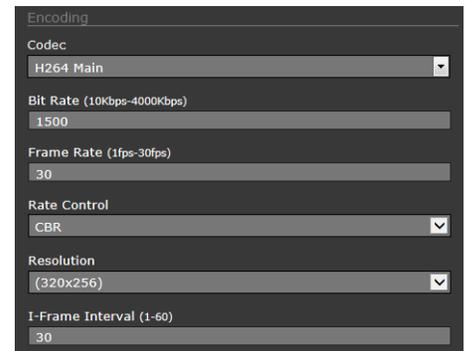
The complete connection strings are:

rtsp://192.168.0.250:554/stream1/sensor1 for VIDEO - 0 and

rtsp://192.168.0.250:554/stream2/sensor1 for VIDEO - 1. By default the video stream uses the IP address of the camera.

Select Video format

The video format only applies to the video output on the analog video BNC connector. Select either **NTSC** or **PAL** depending on the video viewing and recording devices connected to the camera. Select **Save**.



Save

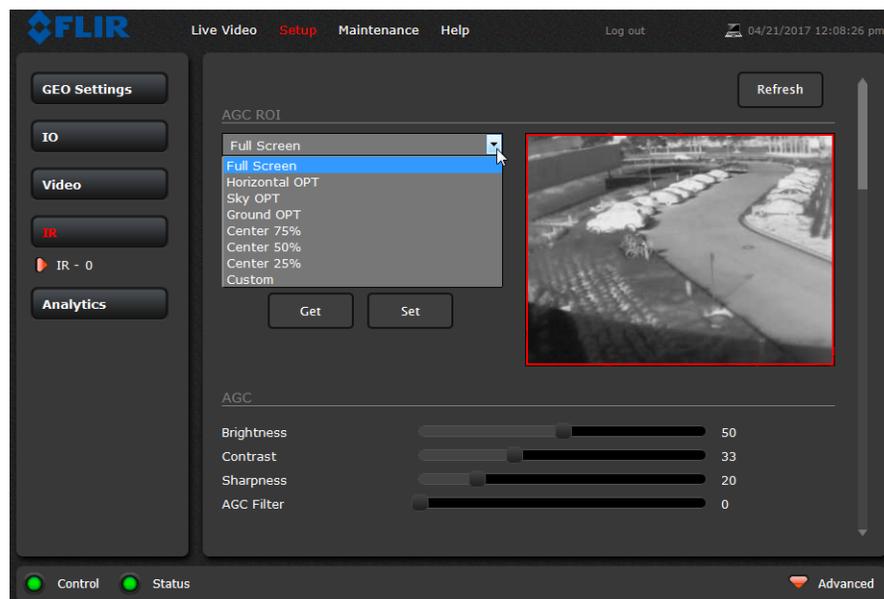
Select video format

3.1.3 Thermal Image Setup - IR Page

In most installations it is not necessary to change the default settings of the thermal camera. However in some situations, depending on weather, time of day, or scene, it may be useful to make changes to the video image to enhance the image by modifying one or more parameters. Be aware that when the conditions change the camera may need to be adjusted again; it is also a good idea to know how to restore the factory default settings.

AGC ROI

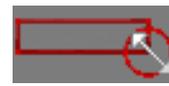
In the **IR** page, a single JPEG image (a snapshot) is displayed in the upper right-hand corner. To update this image at any time, select the **Refresh** button in the upper right. This will cause the entire page to refresh, including the image and all the parameter values (be patient, it may take some time).



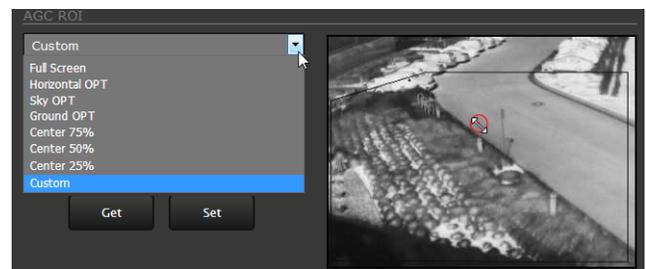
The IR camera adjustments to the region of interest (ROI) determine what portion of the image is used by the Automatic Gain Control (AGC) algorithm. By default all of the pixels in the image are considered; in some cases it may provide an improved image if a portion of the image is excluded. For example, the sky is generally very cold, so if the ROI excludes the sky it may add more contrast to the rest of the image. A pull-down list offers some convenient options.

When Custom is selected, a handle is shown in the center of the screen.

Drag the handle to set the size of the ROI box.



Drag the ROI box over the portion of the scene that will control the AGC.



Advanced Configuration

AGC: The AGC parameters control the overall brightness and contrast, and determine how the overall video image appears. The defaults are suitable for most installations, but in some cases different settings may provide a more appealing image, depending on personal preferences.



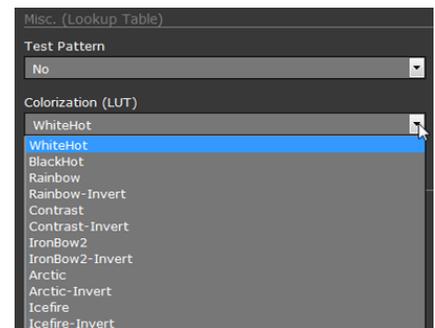
Note

The Video Analytics default AGC Mode parameters are invoked whenever analytics is enabled. If AGC parameters are changed while analytics is disabled, they will be invoked whenever analytics is disabled.

- **Brightness** (gamma) setting determines the allocation of the 256 “shades of gray” produced by the AGC. Values above 50 allocate more shades of gray to hotter objects, while values below 50 allocate more shades of gray to lower temperature objects. Range 0 to 100.
- **Contrast** (Max Gain) can be used to increase contrast, especially for scenes with little temperature variation (it may also increase noise due to increased gain). Range 0 to 100.
- **Sharpness** (DDE Gain) is used to enhance image details and/or suppress fixed pattern noise. Positive values increase Sharpness, while negative values soften the image and filter fixed pattern noise. A setting of 20 is neutral and will not have any effect. Range 0 to 100.
- **AGC Filter** (Damping filter) determines how quickly a scene will adjust when a hot object appears (or disappears) within the AGC ROI. A low value causes the AGC to adjust more slowly when a hot object enters the ROI, resulting in a more gradual transition. Range 0 to 100.

Misc. (Lookup Table): Each Look Up Table (LUT) provides a different representation of the detected levels of thermal energy as colors or gray-scale values. White hot and black hot are gray scale palettes; other tables assign different colors to different temperatures. These color palettes can be selected from the Live Video page (refer to [Toggle Palette](#), pg. 18).

Save Settings: Click **Save Settings** to store the current settings as power up defaults. To restore the original settings, select **Factory Defaults**.



3.1.4 Video Analytics Setup—FB-Series ID Only

The Analytics function of the FB-Series ID camera provides the capability to detect motion, send an alarm, and classify detected objects as Human, Vehicle, or Object of Interest based on size and aspect ratio (height and width).

Note

Objects of interest are detected objects that do not quite match the human or vehicle aspect ratio, but move through the scene uniformly. For example, a deer, bus, or oversized truck.

Using the **Setup** menu Analytics page, create motion detection areas, tripwire lines, or masking areas—up to four of each. Each detection area or tripwire has independent detection properties (such as detecting a vehicle or human sized object). Use the alarm manager in the **Maintenance** menu to define the actions resulting from each alarm condition ([Alarm Manager, pg. 48](#)).

Analytics Page

Use this page to set up areas (or regions) or tripwires for analysis. In some situations it may also be useful to use multiple regions to include (or exclude) different areas in the scene and to set area-specific detection parameters. The Analytics page allows the user to add four areas and four tripwires. Each area/tripwire is assigned an Alarm ID number (1 to 8) based on the order in which they are created and the available IDs. If an area is deleted, its Alarm Id will be available for reuse.



Figure 3-1: Analytics Page

Analytics Calibration

- The camera must be mounted in its final location in order to calibrate the scene in the field of view using either the auto or manual calibration tool.
- Analytics must be enabled to calibrate the scene.
- Set detection areas and tripwires.
- After calibration is finished, verify that the analytics detect and classify objects as expected.

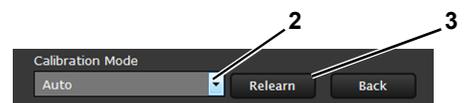
Auto Calibration

If the scene is well ordered and without random motion from things such as trees, shrubs, or small animals, and access is limited to people (the calibration target), then Auto calibration is a good choice. Auto calibration relearning adjusts the detection size parameters as people (the calibration target) are detected walking in all areas of the scene. The progress of the auto calibration is shown as a percent in the top left corner of the image.

Step 1 On the camera's **Analytics** web page, click the Calibrate icon.



Step 2 To automatically calibrate detection settings, from the **Calibration Mode** drop-down list, select **Auto**.



Step 3 Click **Relearn**. The camera automatically calibrates the depth of the FoV based on people walking in the scene. Be sure that people are walking along the entire vertical axis of the FoV until calibration is finished. The On-Screen Display shows the progress as a percentage in the lower left corner of the video (see [Analytics Page, pg. 37](#)).

If the calibration takes too long, the scene may require manual calibration.

AutoCalibration: Learning (69%)
Warning: time needed to calibrate is longer than expected
Warning: verification of learned calibration is required

Step 4 After calibration is complete set up detection areas and check calibration. Refer to [Global Settings, pg. 39](#), [Creating Analytics Regions, pg. 40](#), and [Check Calibration, pg. 41](#).

Manual Calibration

Step 1 On the camera's **Analytics** web page, click the Calibrate icon.



Step 2 Select **Manual** for the Calibration mode.

Step 3 Set the near size aspect ratio for a person. Have a person walk around at the bottom of the area. Select the blue box at the bottom of the screen and drag to fit the subject. Click **Save**.



Figure 3-2: Manual Calibration

Advanced Configuration

- Step 4 Set the far size aspect ratio for a person.
Have a person walk around at the top of the area. Select the blue box at the top of the screen and drag to fit the subject. Click **Save**.
- Step 5 After calibration is complete set up detection areas and check calibration. Refer to [Global Settings, pg. 39](#), [Creating Analytics Regions, pg. 40](#), and [Check Calibration, pg. 41](#).

Based on these settings, the analytics calculate a human size that is proportional to the near and far size calibration over the detection area. The vehicle size is extrapolated from the human size. If a detected object matches these parameters, a box will be labeled either H for human, V for vehicle, or O for object of interest.

Global Settings

Click the settings icon  below the image to access Global Settings.

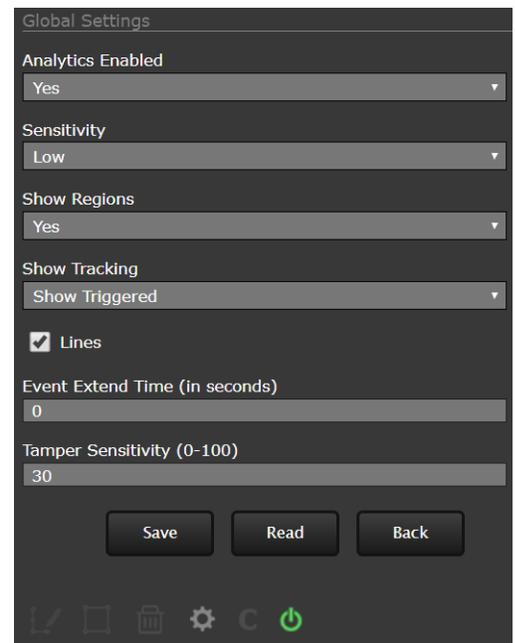
There are three settings for sensitivity which control the threshold for detection (as well as false alarms): **Low**, **Medium**, and **High**. When set to low, the analytics will detect fewer objects (also fewer false alarms) than when set to high.

Set **Show Regions** to **Yes** to show any detection areas as black boxes and tripwires as black lines in the video.

There are four tracking display options: **All Boxes**, **Classified Boxes**, **Show Triggered**, and **No Boxes**. If any of options to show boxes is selected, a check box enables a tracking line with each detection box.

- **All Boxes**—Every detected motion is shown with a box around it.
- **Classified Boxes**—Detected motion classified as vehicle, human, or object of interest is shown with a box around it labeled “H”, “V”, or “O”.
- **Show Triggered**—Detected motion that triggers an alarm is shown with a box around it.
- **No Boxes**—Detected motion is not shown with a box.
- **Lines**—Show the track of an object based on its position from prior frames. This helps to visually represent speed and direction of motion (only available if All or Classified Boxes is selected).
- **Event Extend Time**—The amount of time an analytics zone stays active after an object leaves the zone.
- **Tamper Sensitivity**—Enables the camera to alarm with tampering such as blocking, paint-spraying, or obscuring the lens. The higher the value; the greater the sensitivity. The camera interprets such events as ONVIF “Bad Video” and can react by sending ONVIF notifications.

When done, click **Save**, and then click the gear icon or **Back** to return to the Analytics Setup page.

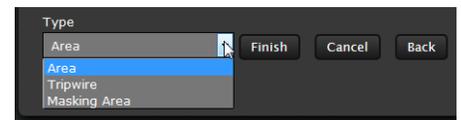


Creating Analytics Regions



To create a detection area, click the add region icon and a new four corner area will appear on the image. Drag any of the highlighted circles to expand and define the detection area.

To create a more complex area with more than four corners or a Tripwire, or to mask an area of the video from motion detection, select the manual selection icon .



- With **Area** selected, click in the video to create the first corner of the area. Continue adding corners (up to 16), then select **Finish** to complete the area.
- With **Tripwire** selected, click in the video to create the first point of the line. Continue to the second point (and more if desired), then select **Finish** to complete the line.

Note

The direction (left or right) for an alarm over a tripwire line is controlled by both the properties of each tripwire and the direction in which the line was originally drawn. A direction to the right is to the right of a person moving from the first point to the second point of the line, etc.

- With **Masking Area** selected, click in the video to create the first corner of the area. Continue adding corners, then select **Finish** to complete the area.

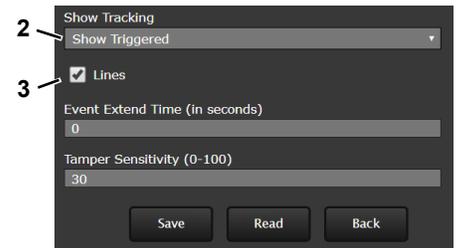
This is motion detection masking; not privacy masking. The video image will still be seen, but alarms will not be generated. Analytics will be disabled in the masked area. The purpose is to manually define regions that will not generate motion alarms. For example, this can be helpful to eliminate alarms from a tree or bush moving in the wind or to perform auto calibration for some scenes.

Configure the parameters in the Properties box to set the area-specific parameters. Once the parameters are set up properly, scroll down and click the **Save** button.

Advanced Configuration

Check Calibration

1. Click the  icon and set **Analytics Enabled** to **Yes**.
2. Set **Show Tracking** to **Show Triggered** then check the **Lines** box.
3. Click **Save**.
4. Have subjects (person, car, truck, etc) enter the area or cross the tripwire at various distances from the camera. The boxes should be classified correctly and the direction across tripwires should be as expected.



The image below shows a classified human box and tracking line in a detection region. The box is white indicating an alarm condition has occurred.



3.2 Maintenance Menu

The following sections describe more advanced camera configuration options that require the **admin** login. For the configuration changes in the remainder of this chapter, it is necessary to save the changes, then stop and restart the server to make the changes effective.

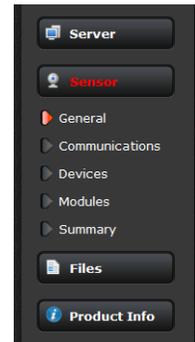
The basic camera configuration settings (**LAN Settings**, **Services**, and **Security Options**) available through the **expert** login are described in [Server Menu, pg. 19](#). When logged in as **admin**, additional Maintenance menus are accessible, including **Sensor**, **Files** and **Product Info**.

3.2.1 Sensor Menu

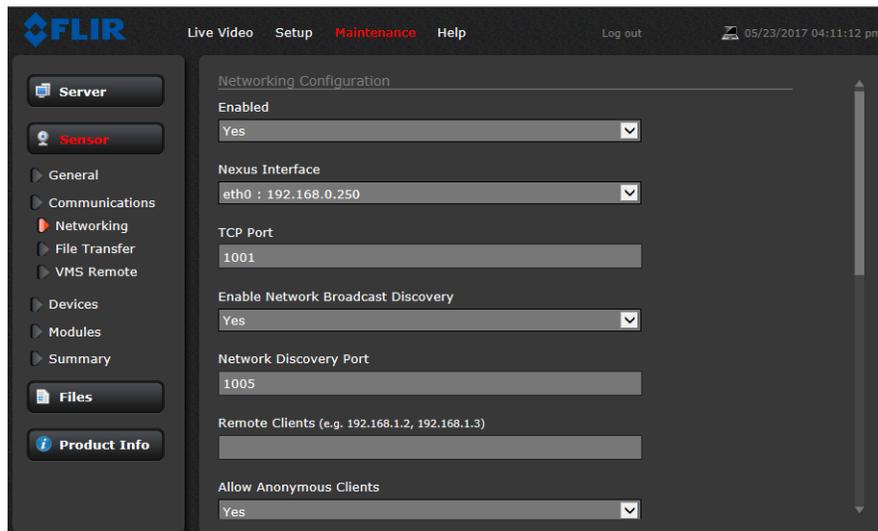
The configuration changes commonly used are done through the Sensor menu. Described below are configuration steps from the **Communications** and **Modules** selections.

Communications Menu

The primary IP configuration parameters, such as IP address, network mask, and gateway, are configured with the LAN Settings page (refer to [LAN Settings, pg. 19](#)). The Networking page can be used to configure some of the other IP networking parameters.



Networking Page: Generally it is assumed the camera network will be secured through recognized network security measures and best practices, such as limited physical access, firewalls, and so on. As an additional security consideration, it is possible to restrict access to the camera to a limited number of IP Addresses.



The default TCP port for most FLIR IP cameras is 1001. This is the port number that a client program such as FLIR Latitude can use to communicate with the camera. If using an ONVIF-compliant VMS as a client, refer to VMS Remote, below.

Advanced Configuration

If the Enable Network Broadcast Discovery parameter is set to Yes, the camera sends out a “discovery” packet on the network every half second as an Ethernet broadcast. To restrict client programs to allowed IP addresses, enter allowed IP addresses in the Remote Clients list, then set the Allow anonymous clients parameter to No, and click **Save**. The changes will not take effect until the server is stopped and started.

Enable Network Broadcast Discovery	Yes
Network Discovery Port	1005
Remote Clients (e.g. 192.168.1.2, 192.168.1.3)	192.168.250.2
Allow Anonymous Clients	No
Timeout for inactive TCP connections (10-900 seconds)	50

Enter IP Addresses
Set pull-down to No

It is also possible to restrict access to the camera web server. Refer to [Security Options, pg. 26](#) to add allowed IP address to the list in the Restrict Web Configuration section.

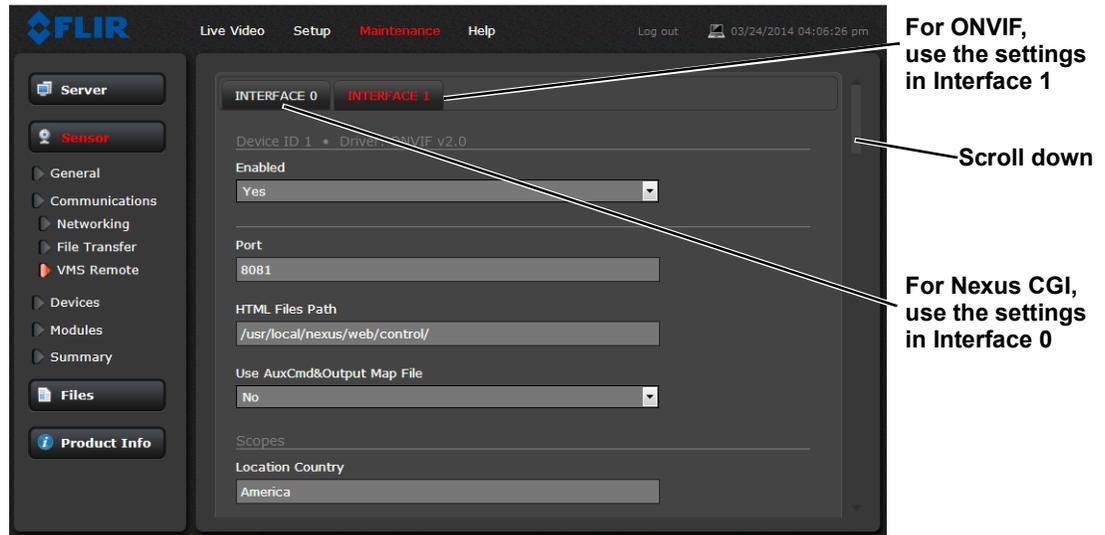
File Transfer: The camera can send a captured image when an alarm occurs (as well as storing the image locally on the camera) if the camera network is configured with an associated FTP or a Network-attached storage (NAS) server.

File Transfer	Enabled	Yes
File Name Prefix Mode	Custom	
FTP	IP Address	
	Port	
	User	

Enable File Transfer
Select Custom to enter a text string prefix

Enter the IP address, path, port, user name and password as required by the network. The FB-Series supports both NAS NFS and NAS Samba. See [Alarm Actions, pg. 50](#).

VMS Remote: The VMS Remote page provides communication interfaces for devices that connect to the camera. Authentication when enabled uses the same passwords set from the **Server Security Options** page. Refer to [Security Options, pg. 26](#).



Nexus CGI Interface

After the interface is configured, scroll down and click on the **Save** button to save the configuration. The changes will not take effect until the server is stopped and started.

ONVIF Interface

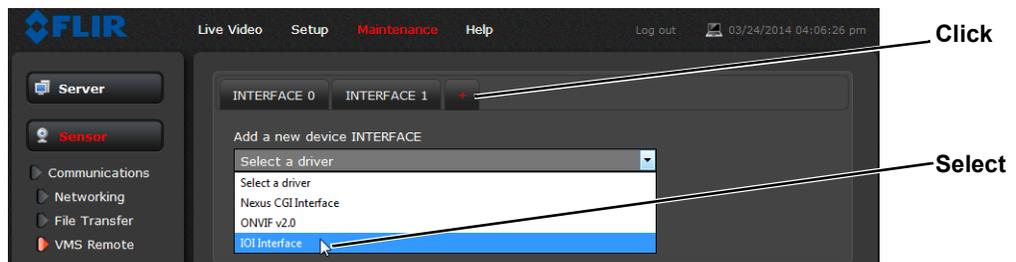
An ONVIF-compliant VMS can be used to control a FLIR camera. Refer to the VMS documentation to determine what parameters are needed. By default, the camera is configured with a VMS Remote interface with ONVIF 2.0 parameters (Profile S). After the interface is configured, scroll down and click on the **Save** button to save the configuration. The changes will not take effect until the server is stopped and started.

Several types of third-party Video Management Systems (VMS) are supported by FLIR IP cameras. Because these systems tend to evolve and change over time, contact the local FLIR representative or FLIR Technical Support to resolve any difficulties or questions about using this feature.

IOI Interface

Install this interface to hand-off FB-Series ID detection events to the PTZ Tracker (trk-101-P). In order to implement a hand-off from the FB-Series ID camera to a PTZ camera, the FB-Series ID camera and trk-101-P are bound together from the web interface of the trk-101-P or from the FLIR Latitude Network Video Management System. Users can define perimeters and areas for the FB-Series ID camera to monitor (refer to [Video Analytics Setup—FB-Series ID Only, pg. 37](#)). When a moving object is detected by the FB-Series ID, the trk-101-P can control and move the PTZ camera to autonomously track and zoom in on the motion.

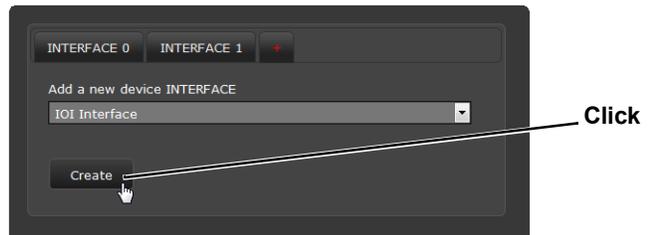
Step 1 Select **Maintenance > Sensor > VMS Remote**.



Step 2 Click + (+).

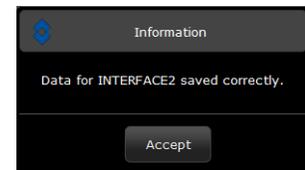
Step 3 From the drop-down list, select **IOI Interface**.

Step 4 Click **Create**.



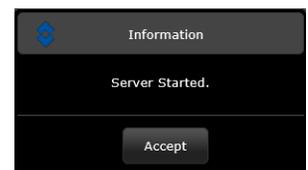
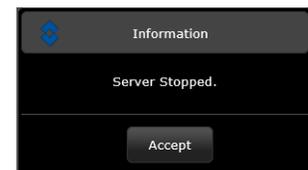
Step 5 Accept the message “Data for INTERFACE2 saved correctly”.

Step 6 Using the Start button at the bottom of the page, Stop and Start the server.



Click **Accept** at the prompt.
The status will show Server Stopped.

Click on the Start button again to restart the server.
Click **Accept** at the prompt.
The status will show Server Running.



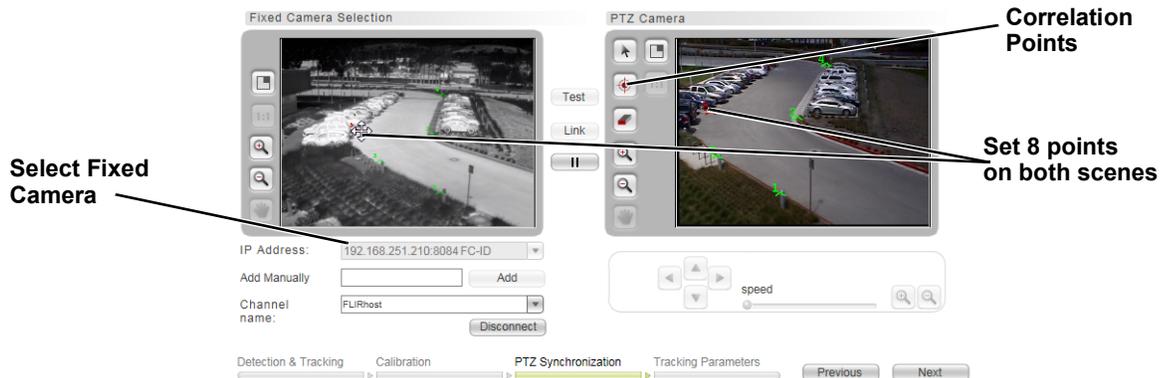
Advanced Configuration

Link Cameras on trk-101-P Tracker

Link the PTZ camera and the FB-Series ID from the trk-101-P web interface.

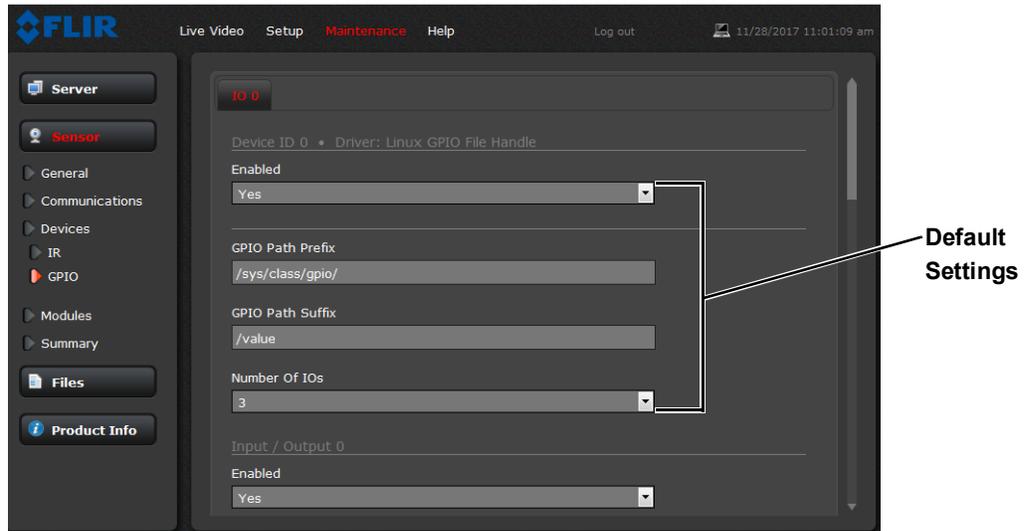
- Step 1 Ensure that the FB-Series ID Analytics have been calibrated (refer to [Analytics Calibration, pg. 37](#)).
- Step 2 With the FB-Series ID Analytics turned off, login to the trk-101-P and set presets for the bound PTZ camera and link the preset scenes to the FB-Series ID scene.

This process is outlined here and detailed in the *FLIR ioi HTML Edition Units User Guide* which can be downloaded from the ioi Analytics section of the individual product web page at <https://www.flir.com/products/ioi-ptz-tracker/>.
- Step 3 Ensure that the FB-Series ID detection regions are setup to correspond to the presets on the trk-101-P (refer to [Creating Analytics Regions, pg. 40](#)).
- Step 4 Login to the trk-101-P web interface.
- Step 5 Select Setup
- Step 6 From the **Camera > Type & Model** screen, verify that the Camera Model is configured as PTZ.
- Step 7 Click **Start PTZ Setup**.
- Step 8 On the **Detection and Tracking** screen, select *Detection from another camera with Automatic PTZ tracking*. Click **Next**.
- Step 9 Click **Calibrate** and follow the instructions on the web interface. Click **Next**.
- Step 10 On the **PTZ Synchronization** screen, follow the procedure described in the *FLIR ioi HTML Edition Units User Guide*. Refer to “Step 3: PTZ Synchronization with Fixed Cameras” in the section “Using the PTZ Camera Definition Wizard”
- Step 11 Set 8 correlation points on the ground for each camera, select **Test**, and then **Link**. Refer to the procedure “To set correlation points in a preset” in the user guide. Click **Next** and **Finish**.



- Step 12 When finished, return to **Live View** and click **Arm**.

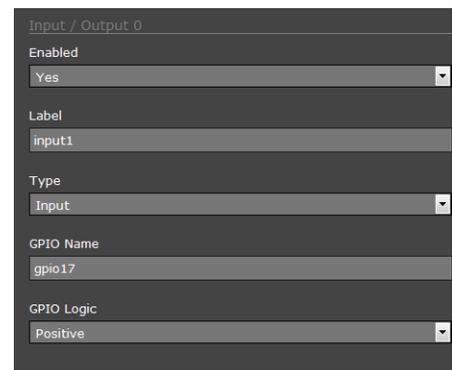
Devices Menu GPIO: On the GPIO page, scroll down to read the current I/O parameters. GPIO is enabled by default.



The GPIO must be wired during installation, refer to [General Purpose Input/Output \(GPIO\), pg. 6](#).

The illustration at the right shows the default settings for the input signal channel, **Input/Output 0**.

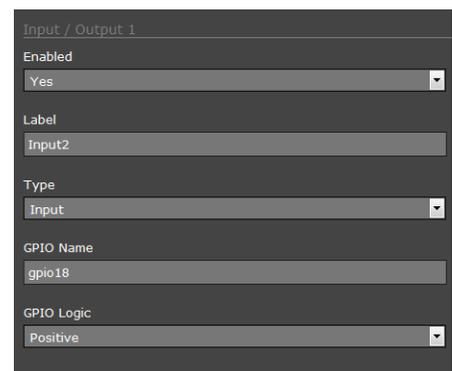
- The Label setting can be changed to reflect more specific alarm information which can then appear in VMS systems such as FLIR Latitude.
- The **GPIO Name** determines the circuit point for the GPIO driver and must not be changed.



- Set **GPIO Logic** to Negative for a normally open switch signal (circuit closes for alarm), Set **GPIO Logic** to Positive for a normally closed switch signal (circuit opens for alarm).

The illustration at the right shows the default settings for the input signal channel, **Input/Output 1**.

- The Label setting can be changed to reflect more specific alarm information which can then appear in VMS systems such as FLIR Latitude.
- The **GPIO Name** determines the circuit point for the GPIO driver and must not be changed.



- Set **GPIO Logic** to Negative for a normally open switch signal (circuit closes for alarm), Set **GPIO Logic** to Positive for a normally closed switch signal (circuit opens for alarm).

Advanced Configuration

The illustration at the right shows the default settings for the output signal channel, **Input/Output 2**.

- The **Label** setting can be changed to reflect more specific alarm information which can then appear in VMS systems such as FLIR Latitude.
- The **GPIO Name** determines the circuit point for the GPIO driver and must not be changed. Set an **Initial Value** (On or Off) for this output signal.



A screenshot of a configuration panel for a GPIO output. It shows three fields: 'Type' set to 'Output', 'GPIO Name' set to 'gpio99', and 'Initial Value' set to 'Off'. Each field is a dropdown menu.

- The **Output Reset Interval** is used to automatically reset the output signal after a set time. Setting the value to 0 prevents the output from resetting automatically after a timeout. See also the Alarm Manager GPIO Output State Mode parameter, [GPIO Output from Motion Alarm, pg. 52](#).
- Set Alarm Output **GPIO Logic** to Positive for a normally open switch signal (circuit closes for alarm), Set **GPIO Logic** to Negative for a normally closed switch signal (circuit opens for alarm).



A screenshot of the 'Input / Output 2' configuration panel. It shows several settings: 'Enabled' is 'Yes', 'Label' is 'Output1', 'Type' is 'Output', 'GPIO Name' is 'gpio99', 'Initial Value' is 'Off', 'Output Reset Interval (0-600 secs.)' is '0', and 'GPIO Logic' is 'Positive'. At the bottom, there are 'Save' and 'Read' buttons.

Click on the **Save** button to save any changed settings. The changes will not take effect until the server is stopped and started.

Refer to the following sections for a description of how to combine the GPIO inputs and outputs with other alarms. For example, the camera can send the output signal when there is a Video Analytics alarm. Similarly, the camera can save an image snapshot when there is an input. These associations are configured with the Alarm Manager module described in [Alarm Manager, pg. 48](#).

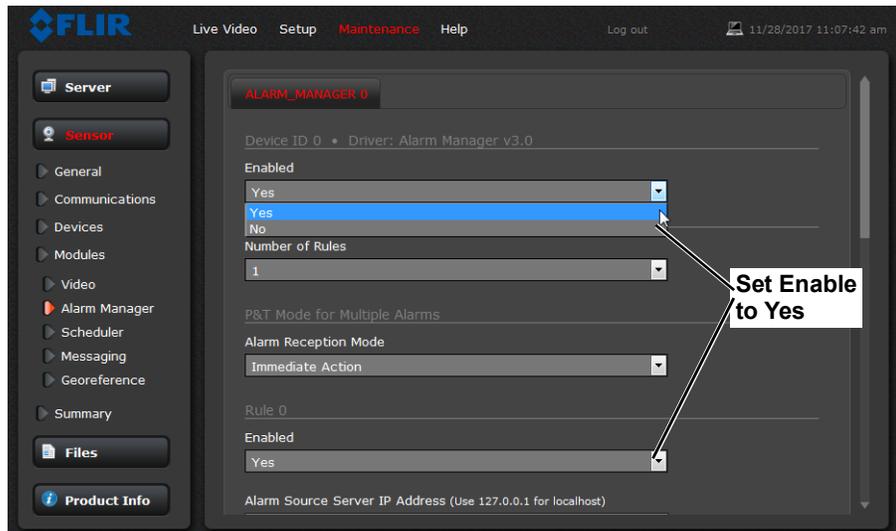
Modules Menu

This section describes the Alarm Manager page. Use the Alarm Manager page to define rules for camera alarms from Video Analytics or GPIO.

Alarm Manager: Use the **Alarm Manager** page to set the response (action) that results from an individual alarm. It is possible to have more than one action for a single alarm by adding additional rules (for example, one action could capture an image and another could generate an output). If a

Advanced Configuration

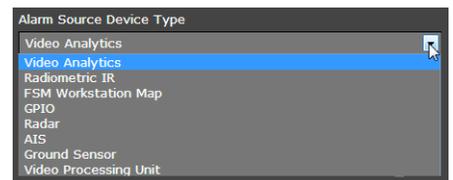
message is to be sent from the camera as a result of an alarm, it is necessary to define Message Systems and set up Notification Lists (refer to [Services Menu, pg. 22](#)).



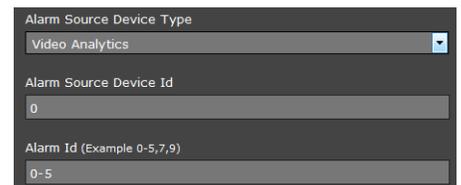
In general, each Alarm Rule describes an alarm **Source** and a single alarm **Action**. For the FB-Series ID camera, the source of the alarm typically will be internal from the video analytics, although it is also possible for the camera to receive alarms from another camera or device/server on the network (such as a radar server, input/output server, ground sensor, fence system, or other security sensor).

Alarm Source: When the source of alarms are internal, for example, from Video Analytics or GPIO Input, the Alarm Source Server IP Address is set to the localhost value of 127.0.0.1 and the TCP port is the default 1001. For internal alarms, the FB-Series ID camera Alarm Source Device ID is set to 0.

The **Alarm Source Device Type** is chosen from a pull down menu; not all options are available for a specific camera or installation.



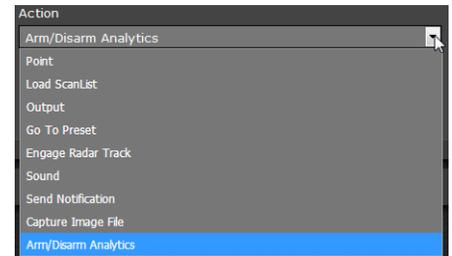
When the alarm source is Video Analytics the **Alarm ID** corresponds to the area or tripwire (1-8), as configured in the Setup menu. The **Alarm ID** is set sequentially during the setup for each alarm source. Refer to [Video Analytics Setup—FB-Series ID Only, pg. 37](#).



When the alarm source is from the GPIO Input the **Alarm ID** is changed to the **Input ID** and can be set to 0 or 1 (recall that inputs are I/O 0 and I/O 1).

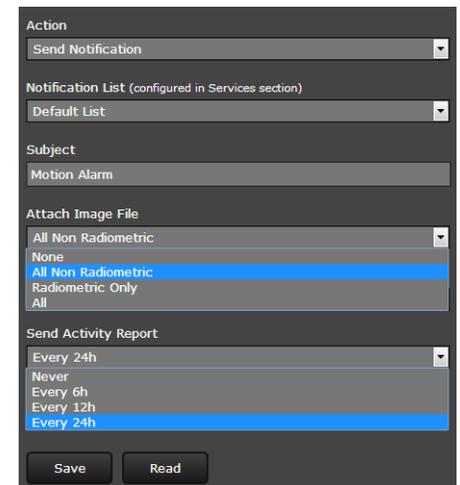


Alarm Actions: Just as there can be multiple sources of alarms, there are also a variety of actions or responses to these alarms. Some actions are only used with pan/tilt cameras. Actions such as Point, Load ScanList, Go To Preset, and Engage Radar Track would only be used with a pan/tilt camera and are not used with the FB-Series ID fixed camera.



For the FB-Series ID, typically a rule will be configured to **Send a Notification**, **Capture an Image**, **Arm/Disarm Analytics**, or generate an **Output** on the GPIO device. If more than one of these actions is needed, it is necessary to configure multiple rules. Examples of these actions are provided below.

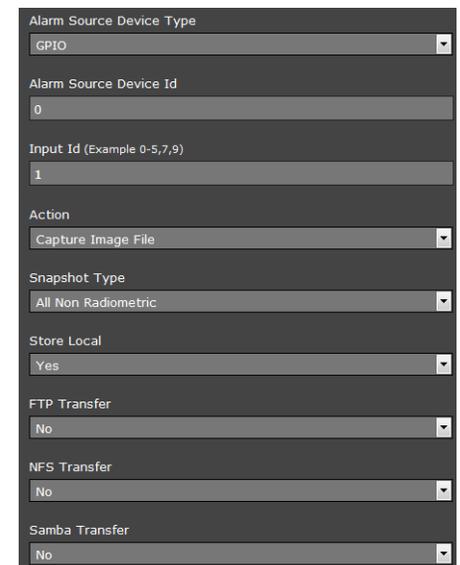
When the Alarm Action is set to **Send Notification**, a Notification List must be selected. The **Send Notification** action uses a Msg System and a Notification List that are set up in the Services menu (refer to [Services Menu, pg. 22](#)).



To attach a snapshot, select **All Non Radiometric** (a normal JPEG image) from the **Attach Image File** pull down list. **Radiometric** (a special type of JPEG with temperature data) is not available on the FB-Series ID camera.

Each rule that sends a notification also has the option to send an activity report to the same notification list every 6, 12, or 24 hours. The activity report indicates whether or not an alarm was triggered during the specified time period. Note that this can be selected on a rule by rule basis.

When the Alarm Action is set to **Capture Image File**, a snapshot is stored when the alarm occurs. The image file can be stored locally in temporary storage (the default), over the camera network using FTP (file transfer protocol) or to a network-attached storage device (NAS). Refer to [File Transfer, pg. 43](#) to configure settings for the FTP, NFS, or Samba transfers.



The Snapshot type should be set to **All Non Radiometric** (a normal JPEG image). **Radiometric** (a special type of JPEG with temperature data) is not available on the FB-Series ID camera.

Alarm Rule Examples: The following examples show rules that control actions from alarms that are internal to the camera (rather than coming from another source on the network). The first three lines and the fifth line of these rules

Advanced Configuration

is always the same for the alarms coming from the FB-Series ID camera itself, and only the source type changes (Video Analytics or GPIO Input).

Indicates the alarm comes from the camera itself, rather than another device on the network.

Enable each alarm rule

FB-Series ID Options: Video Analytics and GPIO

Video Analytics Alarm to Email: Shown at the right is an example of an alarm rule that causes an email notification (with a snapshot image) to be sent when a motion alarm occurs in Analytics Region 0 or Region 1 (Area or Tripwire).

Refer to [Creating Analytics Regions, pg. 40](#)).

The Alarm Source Device Type is set to **Video Analytics** with Alarm Id set to “1” corresponding to Analytics Area 1.

The **Send Notification** action uses a Msg System and a Notification List that are set up in the Services menu (refer to [Services Menu, pg. 22](#)). The email includes alarm information, including the Area ID and if it is a human or vehicle alarm. When an email is sent, the Alarm Manager can attach a snapshot from the camera to the email. In Attach Image File, **All Non Radiometric** is selected for the type of image since the alarm type is **Analytics**.

Alarm Source Device Type: Video Analytics

Alarm Source Device Id: 0

Alarm Id (Example 0-5,7,9): 1

Action: Send Notification

Notification List (configured in Services section): Default List

Subject: Motion Alarm

Attach Image File: All Non Radiometric

Send Activity Report: Every 24h

GPIO Input to Snapshot: In the example rule shown at the right the source type of the alarm is GPIO, with the Input ID set to 1, which corresponds with the input IO 1 (refer to [Devices Menu GPIO, pg. 47](#)), then takes a snapshot and stores it locally onboard the camera and/or over the camera network using FTP or an NAS server.

The Action is set to **Capture Image File**; a snapshot is stored when the alarm occurs. The image file can be stored locally in temporary storage (the default), over the camera network using FTP (file transfer protocol) or to a network-attached storage device (NAS). Refer to [File Transfer, pg. 43](#) to configure settings for the FTP, NFS, or Samba transfers.

The screenshot shows a configuration panel for an alarm rule. The 'Alarm Source Device Type' is set to 'GPIO'. The 'Alarm Source Device Id' is '0'. The 'Input Id (Example 0-5,7,9)' is '1'. The 'Action' is 'Capture Image File'. The 'Snapshot Type' is 'All Non Radiometric'. The 'Store Local' option is set to 'Yes'. The 'FTP Transfer', 'NFS Transfer', and 'Samba Transfer' options are all set to 'No'.

GPIO Output from Motion Alarm: The final example shows an alarm rule that causes a GPIO output when a motion alarm is detected. The source Alarm Id set to 1 corresponds to Region number 1 on the Analytics Setup page.

Note: the Associated I/O Port is set to 0, and the Associated I/O Index is set to 2 (corresponding to Input/Output 2).

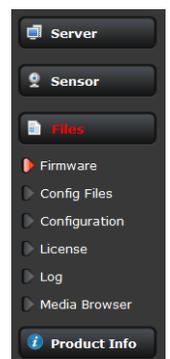
The GPIO Output State Mode can be set as **Bound** or **Unbound**. If **Bound**, the output turns on when an alarm occurs and turns off when the alarm is cleared or the Output Reset Interval is reached (see [Devices Menu GPIO, pg. 47](#)).

If **Unbound**, the output turns on when an alarm occurs and remains on until it is reset by the Output Reset Interval timeout or by a command from the network.

The screenshot shows a configuration panel for an alarm rule. The 'Alarm Source Device Type' is 'Video Analytics'. The 'Alarm Source Device Id' is '0'. The 'Alarm Id (Example 0-5,7,9)' is '1'. The 'Action' is 'Output'. The 'Associated I/O Device Id' is 'Io 0'. The 'Associated I/O Port' is '0'. The 'Associated I/O Index (Example 0-5,7,9)' is '2'. The 'Output State Mode (Bound: Output follows Alarm state, Unbound: Output is state is ON)' is set to 'Unbound'.

3.2.2 Files Menu

The administrative actions for accessing, updating, and transferring files are accessed through the **Files** menu on the left side of the page. Selected actions from the **Firmware**, **Configuration**, and **Log** pages are described below.



Advanced Configuration

Firmware Page

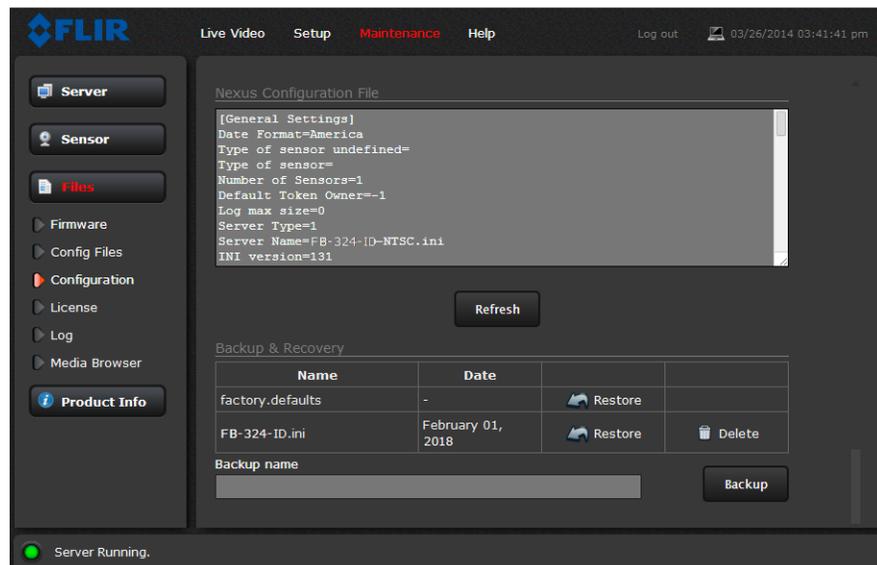
For camera firmware updates, manually install a firmware update file by first stopping the camera server, browsing to select the update file on your computer, and then selecting Upload. The firmware files will be uploaded and installed.



Caution!

The firmware update procedure resets the FB-Series camera to default settings. Before performing the update, detach the camera from any VMS. A firmware update resets video settings, IR settings, and rules to factory defaults.

Configuration Page



Use the **Configuration** page to view the Nexus Configuration File, perform Backup & Recovery of local files (on the camera), and perform Upload & Download of configuration files to another computer for backup, or to install a new configuration file to the camera.

Shown at the top of the screen is the configuration script file in a scrollable window. This can be useful if help is ever need help from a support engineer.

Backup & Recovery

In the Backup & Recovery section, click the Restore link associated with the factory.defaults configuration to restore the camera to its factory settings. This file can not be modified or deleted, so it is always available.

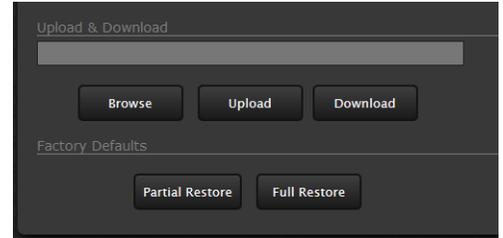
Use the **Backup** button to make a backup of the final settings. This will make a backup copy of the configuration file and store it locally on the camera.

Advanced Configuration

Upload & Download

The **Download** button is used to save a copy to a PC for safe keeping. A pop-up window will ask for a file name and destination folder.

To transfer a configuration file (server.ini) from a PC to the camera, use the **Browse** button to select the file on the PC, then use the **Upload** button to upload the file. After a file upload you must stop and restart the server.



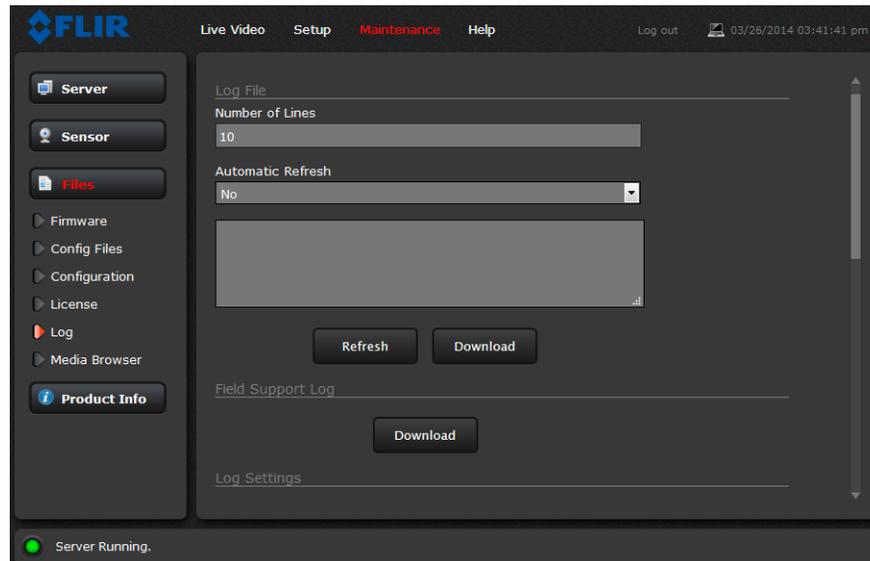
Factory Defaults

Select **Full Restore** to return the camera its original factory configuration.

Select **Partial Restore** to maintain network and IP settings while returning all other settings to the factory configuration.

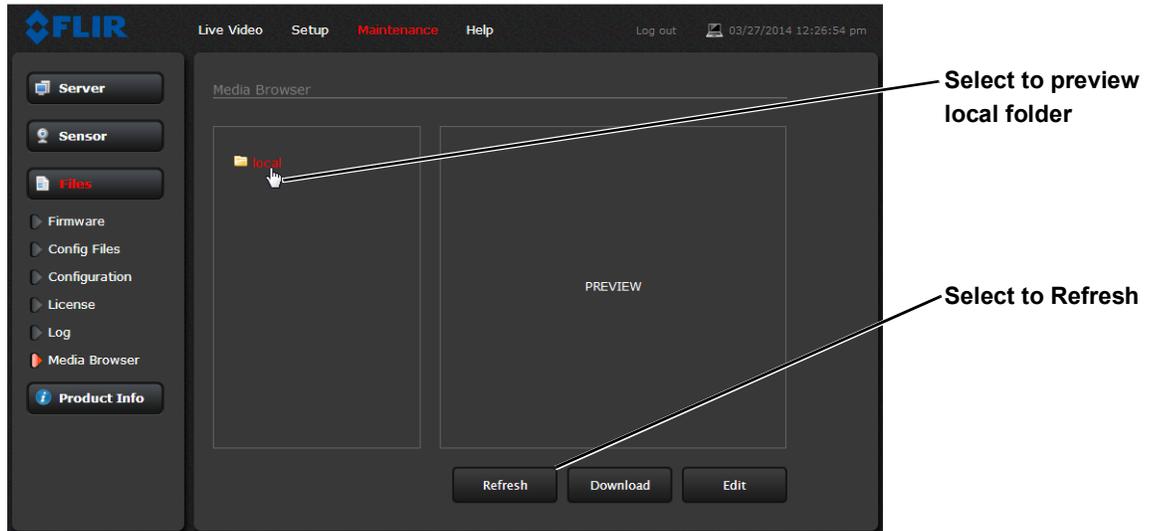
Log Page

Use the **Log** page to set logging parameters. Scroll down and select the **Download** button under Field Support Log to download a zip file to the computer for field service evaluation.



Advanced Configuration

Media Browser: The Media Browser page shows all of the images captured by the camera as a result of an alarm action. The image files can be downloaded to another computer for backup.

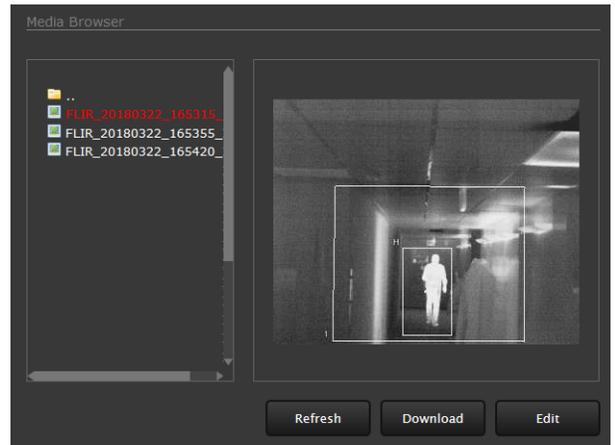


After selecting a file, the file will appear in the Preview window.

The file name contains the year, month, day, 24 hour clock time, and the sensor that captured the image. In this case IR0 is the only sensor.

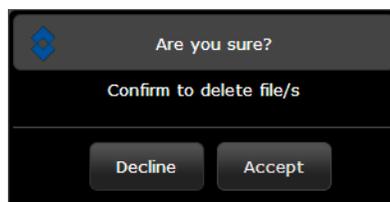
Select Download to download the selected file to the PC. Select Refresh to check for any additional images since landing on the Media Browser page.

Select Edit to select and delete individual images or all images. Any time the camera is rebooted or the power removed, the media directory will be emptied.

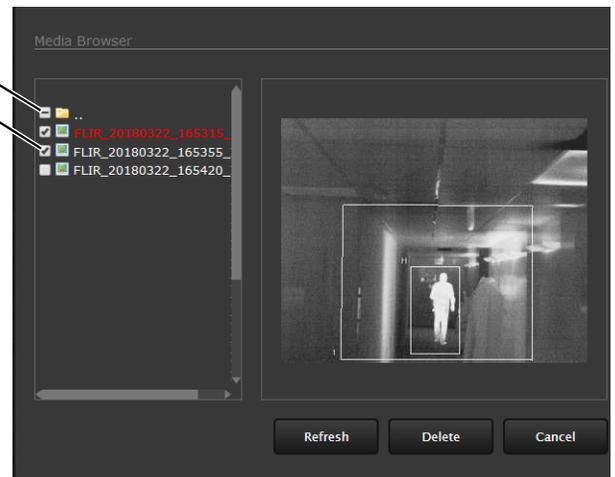


Select all media files by clicking on the Select All check box. If all files are not selected, the Select All box will have a minus sign.

The following prompt will appear prior to deleting any files.



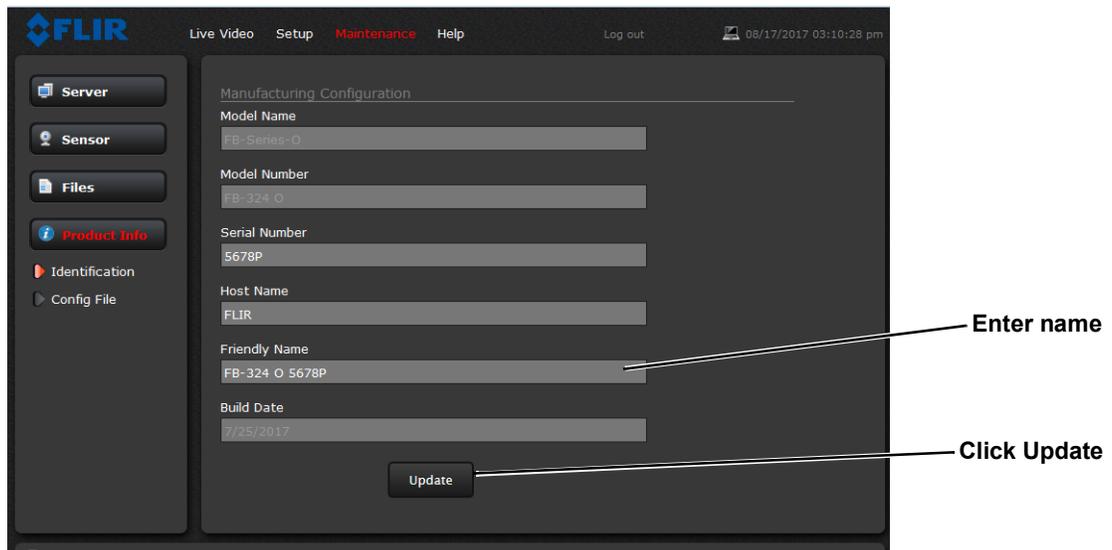
Select All
Select Individually



3.2.3 Product Info Menu

The **Identification** page shows information for the camera and allows changing the Friendly Name of the camera for easier identification when multiple cameras are used on the network. The friendly name is included in network traffic, in the Name field in FLIR Latitude, and shown on the Property tab in DNA.

Click on the **Update** button to save any changes. The changes will not take effect until the server is stopped and started.





FLIR Systems, Inc.
6769 Hollister Ave
Goleta, CA 93117
USA

Corporate Headquarters
FLIR Systems, Inc.
27700 SW Parkway Ave.
Wilsonville, OR 97070
USA

Support:
<https://www.flir.com/support/>

Document:
427-1065-00-12
Revision: 140
Date: January 2020