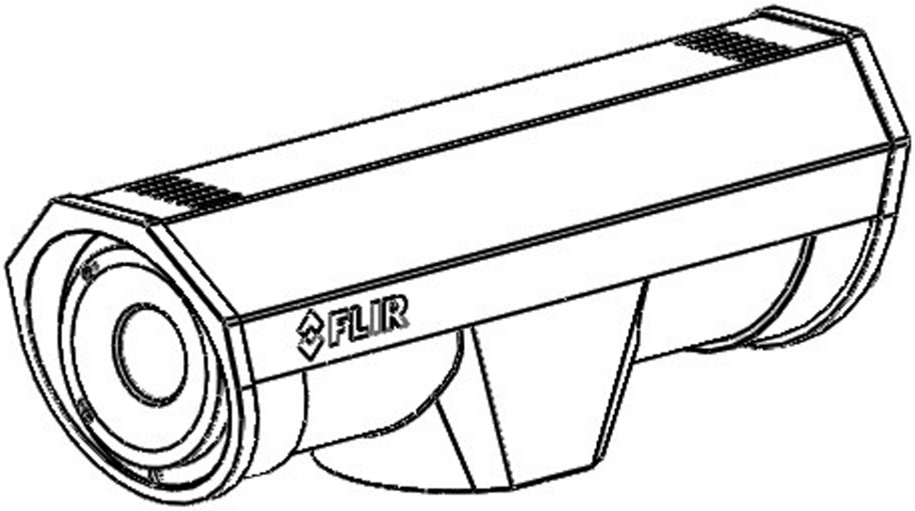
Installation Manual

F-Series ID



427-0033-00-12 Version 110 **February 2019**

This document does not contain any export-controlled information.

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-center/support-hq/

Important Instructions and Notices to the User:

Modification of this device without the express authorization of FLIR Systems, Inc., may void the user's authority under the 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 his own expense. Shielded cables must be used to connect this device to other devices.

Note 2: If ferrites are supplied with this equipment, the equipment was tested for compliance with the FCC limits for a Class A digital device using power cables with the ferrites installed. When connecting one or two power cables to the equipment, the supplied ferrites must be used with this equipment.

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 a 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

Version	Date	Comment
100	December 2018	V1.3.0
110	February 2019	Updated video encoding defaults and firmware update information; added 802.1x support, TLS configuration, and Nexus CGI interface

Table of Contents

F-Series ID Camera Installation

Basic Operation and Configuration

This document does not contain any export-controlled information.

Advanced Configuration

This document does not contain any export-controlled information.

1 F-Series ID Camera Installation

This manual describes the installation and initial configuration of the F-Series ID thermal camera. The F-Series ID camera has software providing for on-board video analytics: setting of detection regions, trip lines, and classification of detected objects. Refer to Video Analytics Setup, pg. 38.

1.1 Camera Overview

The F-Series ID 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^{TM}.

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 contact support at: https://www.flir.com/support-center/support-hq/. 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.

1.2 Warnings and Cautions

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

Warning!

⚠

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

Caution!

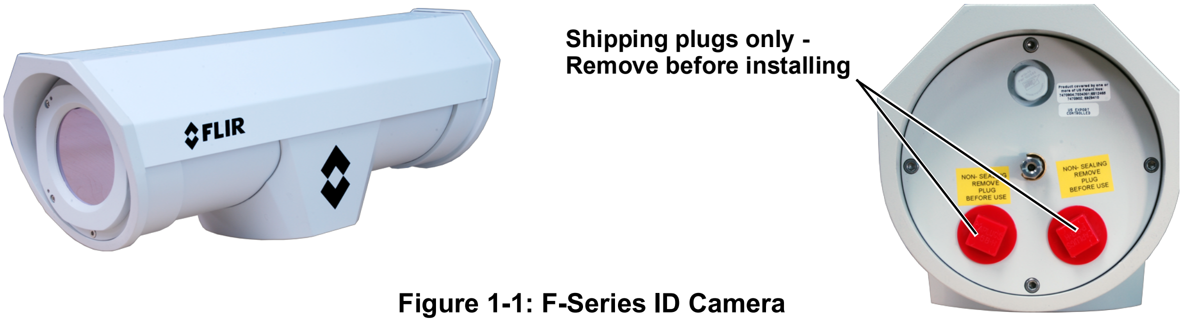
Except as described in this manual, do not open the F-Series ID camera for any reason. Disassembly of the camera can cause permanent damage and will void the warranty.

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

The F-Series ID camera requires a power supply of 24 V. Operating the camera outside the specified input voltage range or the specified operating temperature range can cause permanent damage.

1.3 Installation Overview

The F-Series ID Camera is an infrared thermal imaging camera intended for outdoor applications, and can be installed in a fixed location or on a pan/tilt mechanism.


FLIR
NON-SEALING REMOVE PLUG BEFORE USE
NON-SEALING REMOVE PLUG BEFORE USE

Shipping plugs only - Remove before installing

Figure 1-1: F-Series ID Camera

The F-Series ID camera is intended to be mounted on a medium-duty fixed pedestal mount or wall mount commonly used in the CCTV industry. Cables exit from the back of the camera housing. The mount must support up to 30 lbs. (15 KG).

1.3.1 Camera Connection Options

Camera connections are made through water-tight cable gland seals on the rear of the camera. Refer to Cable Gland Sealing, pg. 9 to ensure the glands are used correctly and the connections are properly sealed.

The camera is powered with a conventional power supply using 21 - 30 Vac or 21 - 30 Vdc.

The F-Series ID camera produces both analog video and digital (IP) video output. Analog video will require a connection to a video monitor or an analog video matrix switch.

An Ethernet connection is required for IP video streaming and for command and control communications.

Several third-party video management systems 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 for information.

General Purpose Input/Output (GPIO)

The camera can receive a single input signal and can provide a single output signal. Refer to GPIO Alarm Connections, pg. 12.

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 Camera Mounting Accessories

The following accessories are available for purchase from FLIR Systems, Inc.

- Wall Mount Kit (500-0462-00) – The wall mount is designed to safely support loads up to 40 pounds (18 kg). The mount features a fully adjustable swivel head allowing 360 degree horizontal and 75 degree vertical adjustment. The mount is constructed of aluminum with a gray polyester powder coat finish.
- Pole Mount Adapter (4119507) – The pole mount adapter is designed for use with the wall mount kit (500-0462-00) when installation is required on a pole. The adapter attaches on poles having 1.5-inch (3.81 cm) to 8-inch (20.32 cm) diameters. The mount is constructed of aluminum with a gray polyester powder coat finish and stainless steel straps.
- Pedestal Mount Kit (500-0463-00) – The pedestal mount is designed to support loads up to 40 pounds (18 kg). The mount features a fully adjustable swivel head allowing 360 degree horizontal and 75 degree vertical adjustment. The mount is constructed of aluminum and has a gray polyester powder coat finish.

1.3.3 Supplied Components

The F-Series ID camera includes these standard components:

- Fixed Camera Unit
- Cable Glands and Spare Parts kit

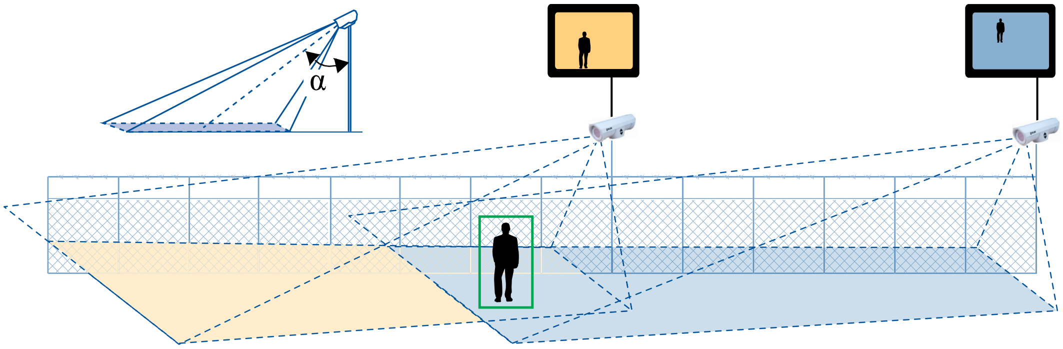
1.3.4 Additional Supplies

The installer will need to supply the following items, which are specific to the installation.
Refer to Camera Connections, pg. 11.

- 24 V Power supply
- Electrical wire: system power, 3-conductor, shielded, gauge determined by cable length; GPIO alarm cable (optional), 5-conductor, 20 AWG maximum
- Camera grounding strap
- Coaxial RG59U video cables (BNC connector at the camera end) for analog video (optional)
- Shielded Category 6 Ethernet cable for control, streaming video, and for software updates.
- Hardware/software for viewing the video (streaming IP video or analog video)
- Miscellaneous electrical hardware, camera mount, connectors, and tools

1.3.5 Camera Placement

The F-Series ID camera should be mounted upright on top of the mounting surface. Adhere to all local and industry standards, codes, and best practices.



For installations with multiple 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, pg. 38.

- Install the camera at a height of approximately 4 m (13 ft) or more.
- Typically direct the camera towards the ground with the maximum possible tilt angle (α) to ensure that 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.

1.3.6 Bench Testing

Connect the power, analog video, and Ethernet connections and confirm that the video is shown on a monitor when the power is turned on. The IP address of the camera web server is shown on the analog video for approximately 90 seconds after power is applied. For configuration and basic setup information using the onboard web server, refer to Camera Bench Test, pg. 15.

1.3.7 Prior to Cutting/Drilling Holes

When selecting a mounting location for the F-Series ID camera, consider cable lengths and cable routing. Ensure the cables are long enough, given the proposed mounting locations and cable routing requirements, and route the cables before you install the components.

Use cables that have sufficient dimensions to ensure safety (for power cables) and adequate signal strength (for video and communications).

1.3.8 Camera Mounting

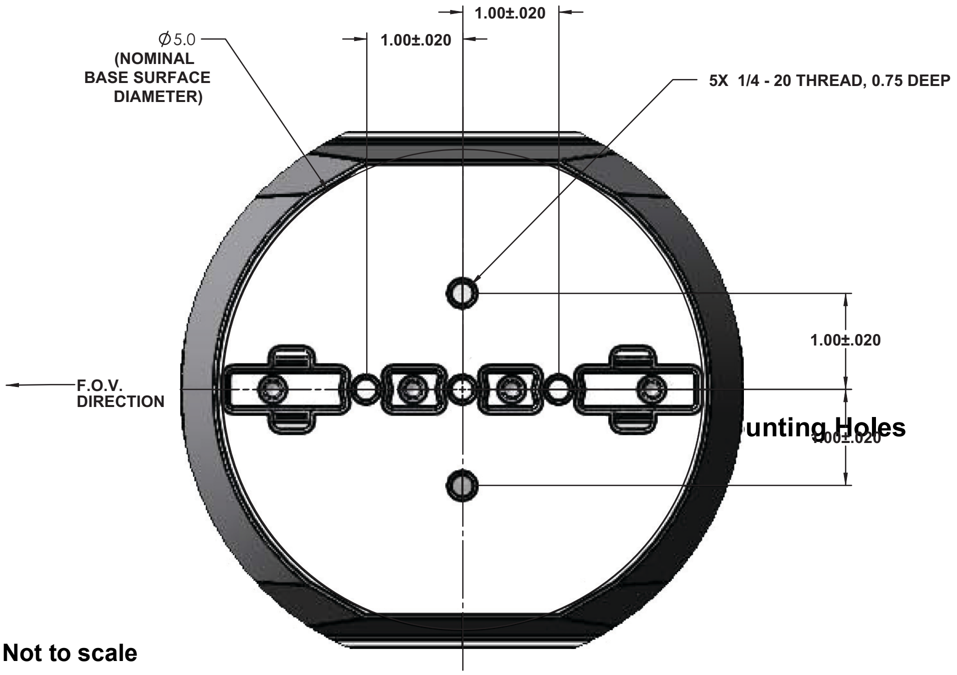
F-Series ID cameras must be mounted upright on top of the mounting surface, with the base below the camera. The unit should not be hung upside down.

Verify both sides of the mounting surface are accessible.

Use a thread locking compound such as Loctite 242 or equivalent with all metal to metal threaded connections.

Once the holes are drilled in the mounting surface, install three (3) to five (5) 1/4-20 threaded fasteners into the base of the camera with thread-locking compound.

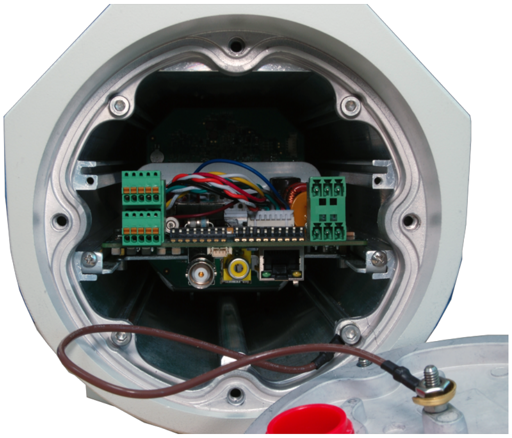
Secure the camera to the mount with three (3) to five (5) 1/4-20 threaded fasteners as shown below.



Not to scale
All dimension are in inches

1.3.9 Removing the Back Cover

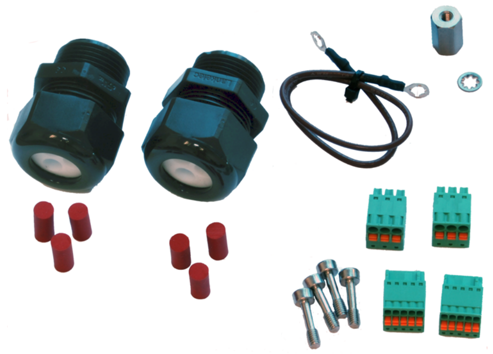
Use a 3 mm hex key to loosen the four captive screws, exposing the connections at the back of the camera enclosure. There is a grounding wire connected between the case and the back cover as shown. If the grounding wire is temporarily disconnected during the installation, it must be reconnected to ensure proper grounding of the camera.



1.3.10 Cable Gland Sealing

Proper installation of cable sealing glands and use of appropriate elastomer inserts is critical to long term reliability. Cables enter the camera mount enclosure through liquid-tight compression glands. Leave the gland nuts loosened until all cable installation has been completed. Inspect and install gland fittings in the back cover with leak sealant and tighten to ensure water tight fittings. Teflon tape or pipe sealant (i.e. DuPont RectorSeal T™) are suitable sealants.

1.3.11 Cable Glands and Spare Parts Kit



The kit contains the two 3/4” cable glands and gland seal plugs required for non-conduit installations.

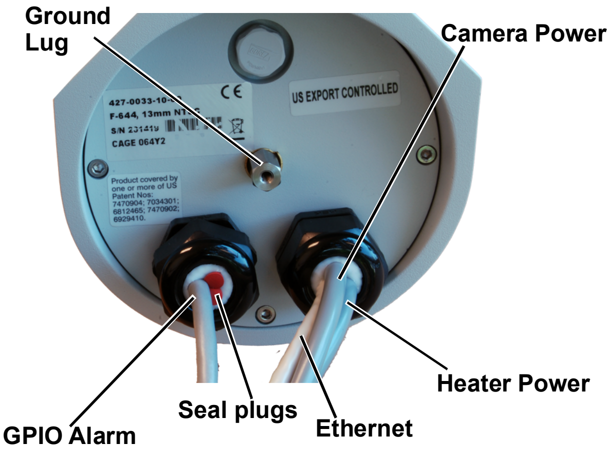
The remaining parts included in the kit are:

- a spare ground wire
- a spare ground nut and lock washer
- two spare power terminal block plugs
- two spare terminal block plugs
- four spare F-Series back cover screws

1.3.12 Cable Gland Seal Inserts

The camera comes with two 3/4” NPT cable glands, each with a three hole gland seal insert. Cables may be between 0.23" to 0.29" OD. Up to five cables may be needed. Plugs are required for any insert hole(s) not used.

If non-standard cable diameters are used, you may need to locate or fabricate the appropriate insert to fit the desired cable. FLIR Systems, Inc. does not provide cable gland inserts other than the inserts supplied with the system.



Note

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

1.4 Camera Connections

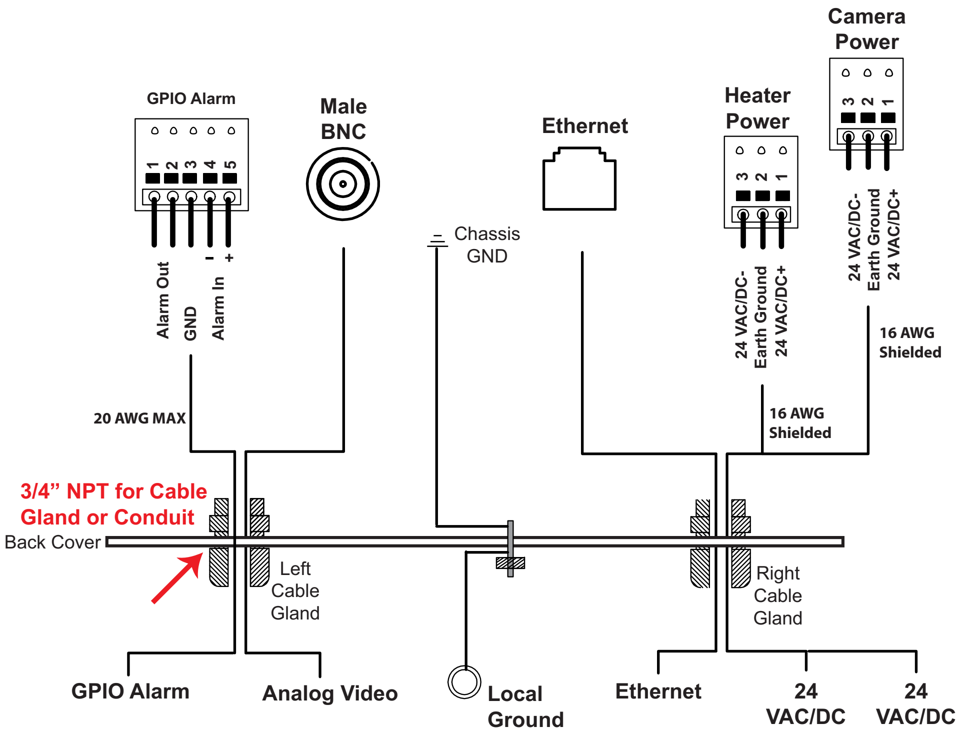


Figure 1-3: Camera Connections

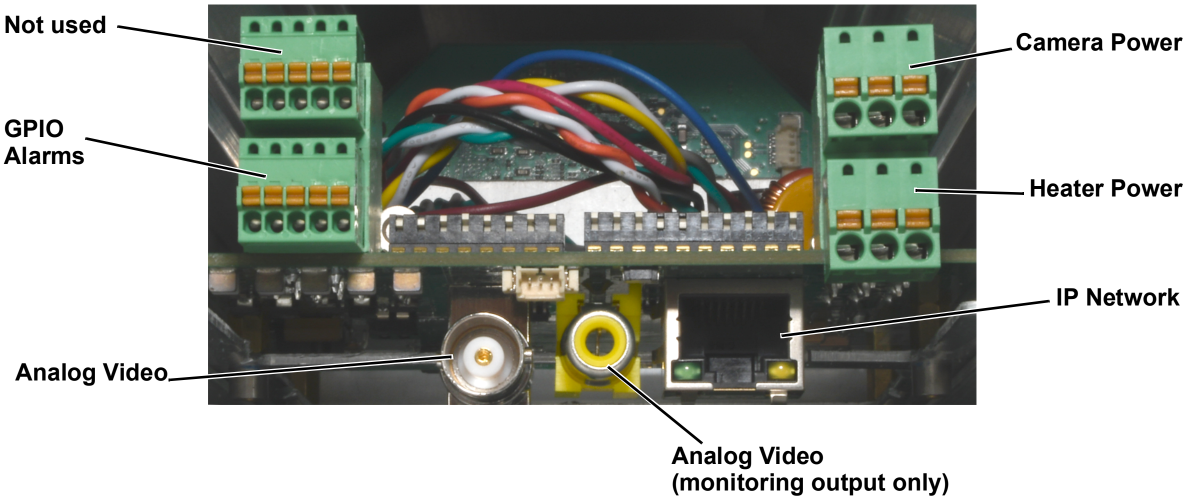


Figure 1-4: Connector locations

1.4.1 Connecting power

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

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

Ensure the camera is properly grounded. Typical to good grounding practices, the camera chassis ground should be connected to the lowest resistance path possible. FLIR requires a grounding strap anchored to the grounding lug on the back plate of the camera housing and connected to the nearest earth-grounding point.

Note

The terminal blocks for power connections will accept a maximum 16 AWG wire size.

1.4.2 Video Connection

The analog video connection on the back of the camera is a BNC connector. The camera also provides an RCA video connector that can be used to temporarily monitor the video output, without disconnecting the BNC connection.

The video cable used should be rated as RG59U or better to ensure a quality video signal.

1.4.3 GPIO Alarm Connections

The camera can receive a single input signal and can provide a single output signal.

Table 1-1: GPIO Connections - J102A

Pin	Connection	Notes
1	Alarm Out1	Relay contact rated load 0.09 A @ 5 Vdc
2	Alarm Out2	
3	GND	
4	Alarm In1 –	Dry alarm contact
5	Alarm In2 +	

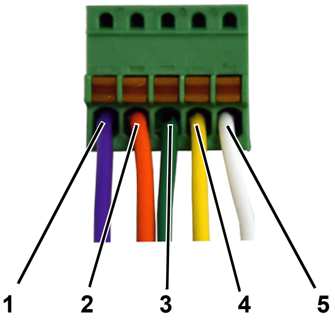


Figure 1-5: GPIO Terminal Plug

1.4.4 Ethernet Connection

The cable gland seal is designed for use with Shielded Category 6 Ethernet cable.

1.5 F-Series ID Camera Specifications

Uncooled Thermal Camera	Array Format	640 × 480	
	Detector Type	Long-Life, Uncooled VOx Microbolometer	
	Effective Resolution	307,200	
	Pixel Pitch	17 µm	
	Thermal Frame Rate	NTSC: 30 Hz PAL: 25 Hz /8.33 Hz	
Optical Characteristics	**Model**	**FOV**	**Focal Length**
	F-608 ID	8.6° × 6.6°	75 mm, f/1.1
	F-612 ID	12° × 10°	50 mm, f/1.2
	F-617 ID	17° × 14°	35 mm, f/1.1
	F-625 ID	25° × 18°	25 mm, f/1.1
	F-644 ID	44° × 36°	13 mm, f/1.0
	Sensitivity <35 mK @ 25 °C F# 1.0		
	Spectral Range 7.5 µm to 13.5 µm		
	Focus Range Athermalized, Focus-Free		

Video	Composite Video	NTSC or PAL Standard; 1 Vp-p, BNC 75 ohm switchable from web page. Refer to Video Setup, pg. 34.
	Video Compression	Two independent channels of streaming H.264 or M-JPEG
	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
	Video Analytics AGC Mode	Engaged when analytics is enabled
	Thermal AGC Region of Interest (ROI)	Default Presets and User definable ROI to insure optimal image quality for subjects of interest
	Analytics Management	Web-based configuration and management
	Analytics Features	Region Entrance/Intrusion Detection, Crossover/Fence Trespassing, Auto/Manual Depth Setup, Human and Vehicle Rules, Hand-off target to PTZ tracking, Tampering
	Image Uniformity Optimization	Automatic Flat Field Correction (FFC) with thermal and temporal triggers

System Integration	Ethernet	10/100 Mbps
	General Purpose Input/Output (GPIO)	One dry contact input; One relay output, rated load 0.09 A @ 5 Vdc
	Network API	ONVIF Profile S, FLIR SDK, FLIR CGI Library
	Supported Protocols	IPV4, HTTP, UPnP, DNS, NTP, RTSP, RTCP, RTP, TCP, UDP, ICMP, IGMP, DHCP, ARP

General	Weight	~9.5 lb (4.4 kg); Configuration Dependent
	Dimensions (L, W, H)	18.1" × 5.5" × 6.3" (460 × 140 × 160 mm)
	Input Voltage	24 Vac (21-30 Vac) 24 Vdc (21-30 Vdc)
	Power Consumption	24 Vdc = 10 W (max no heater); 46 W (max w/ heaters) 24 Vac = 15 VA (max no heater); 51 VA (max w/ heaters)
Environmental	IP rating (dust and water ingress)	IP66
	Operating temperature range	-40 °C to 70 °C (-40 °F to 158 °F) cold start
	Storage Temperature range	-55 °C to 85 °C (-67 °F to 185 °F)
	Humidity	0-95% relative
	Vibration	IEC 60068-2-27
	Mechanical Shock	MIL-STD-810F Transportation
	De-Icing	MIL-STD-810F, Method 521.1; De-Icing of 3/6mm, model dependent
Compliance and Certifications	EN 61000-6-4:2007+A1:2011	
	AS/NZS CISPR 32 Class A:2015	
	AS/NZS 61000.6.4:2012	
	ICES-003 Issue 6 Class A:2016	
	EN 50130-4:2011+A1:2014	
	EN 55032 Class A:2015	
	EN 55024:2010+A1:2015	
	EN 61000-6-4:2007+A1:2011	
	FCC Part 15, Subpart B, Class A/CFR 47 FCC Class A:2015	
	IP 66—IEC 60529:2013/EN 60529:1991 + A1:2000	
	Information Technology Equipment Safety—IEC 60950-1:2005 + Am1:2009 + AM2:2013 EN 60950-1:2006 + Am11:2009 + Am1:2010 + Am12:2011 + Am2:2013	
Warranty and Regulatory	Compliance and Certifications	FCC Part 15 (Subpart B, class A) CE Marked RoHS IP66 ONVIF Profile S WEEE
	Warranty	Camera: 3 years Sensor: 10 years

2 Basic Operation and Configuration

This chapter provides basic information on how to operate the F-Series ID 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

2.1.1 Server Configuration

It may be necessary for the installer to make a limited number of configuration changes to the camera server, such as setting the IP communication parameters, setting new login passwords, as well as some scene specific parameters. For example, each camera comes from the factory with the same default IP addressing (DHCP), so adding more than one camera to an IP network may require each camera to be configured with a different static IP address. On the other hand, many of the configuration parameters will remain unchanged from the factory default settings.

2.2 Camera Bench Test

The camera provides both analog video and IP video. Test the analog video at the test connector (RCA) with the back plate removed. When installing the camera into an analog network, connect the video cable to the BNC connector. Do not use both video connections simultaneously. 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.

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 FLIR Discovery Network Assistant (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/.

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

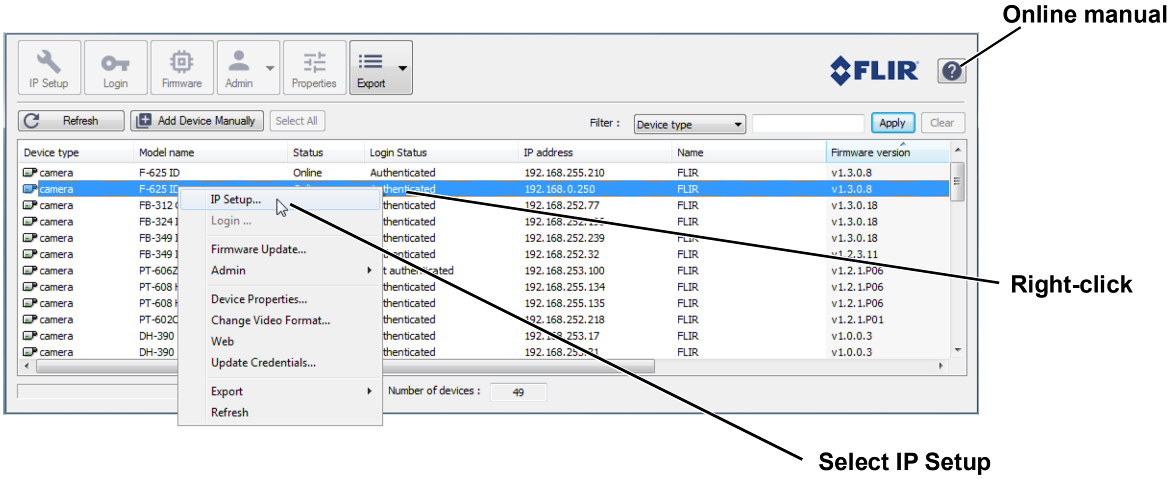
2.2.1 Set IP Address using the FLIR Discovery Network Assistant (DNA)

The F-Series ID 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.



Device type	Model name	Status	Login Status	IP address	Name	Firmware version
camera	F-625 ID	Online	Authenticated	192.168.255.210	FLIR	v1.3.0.8
camera	F-625 ID		thenticated	192.168.0.250	FLIR	v1.3.0.8
camera	FB-312 (		thenticated	192.168.252.77	FLIR	v1.3.0.18
camera	FB-324 I		thenticated	192.168.252.[illegible]	FLIR	v1.3.0.18
camera	FB-349 I		thenticated	192.168.252.239	FLIR	v1.3.0.18
camera	FB-349 I		enticated	192.168.252.32	FLIR	v1.2.3.11
camera	PT-606Z		t authenticated	192.168.253.100	FLIR	v1.2.1.P06
camera	PT-608 I		thenticated	192.168.255.134	FLIR	v1.2.1.P06
camera	PT-608 I		thenticated	192.168.255.135	FLIR	v1.2.1.P06
camera	PT-602C		thenticated	192.168.252.218	FLIR	v1.2.1.P01
camera	DH-390		thenticated	192.1[illegible]8.253.17	FLIR	v1.0.0.3
camera	DH-390		thenticated	192.168.25[illegible]	FLIR	v1.0.0.3

Number of devices : 49

Online manual

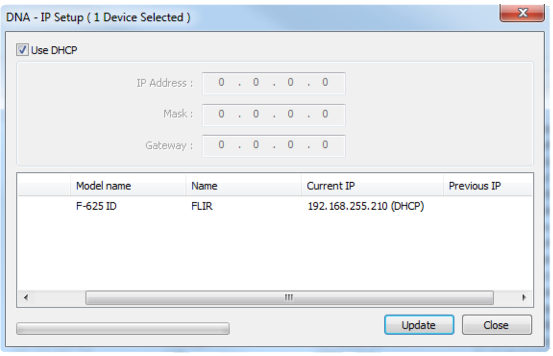
Right-click

Select IP Setup

Step 4 Right-click on the camera, select **IP Setup** to change the IP address or select between static IP or DHCP addressing.

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

Step 6 Using the web browser, configure the camera settings, such as camera date/ time, and other parameters, so the camera is compatible with the existing network.


DNA - IP Setup (1 Device Selected)

☑ Use DHCP

IP Address : 0 . 0 . 0 . 0

Mask : 0 . 0 . 0 . 0

Gateway : 0 . 0 . 0 . 0

Model name	Name	Current IP	Previous IP
F-625 ID	FLIR	192.168.255.210 (DHCP)	

2.2.2 Log in to the Camera Web Page

Use a web browser to connect to the camera's web server using one of three User Names: **user**, **expert**, or **admin** (the default passwords are **user**, **expert**, and **admin** respectively).

Important Note

To prevent unauthorized access, change all of the login passwords (**admin** login required). For information on how to change the passwords, refer to Security Options, pg. 28.

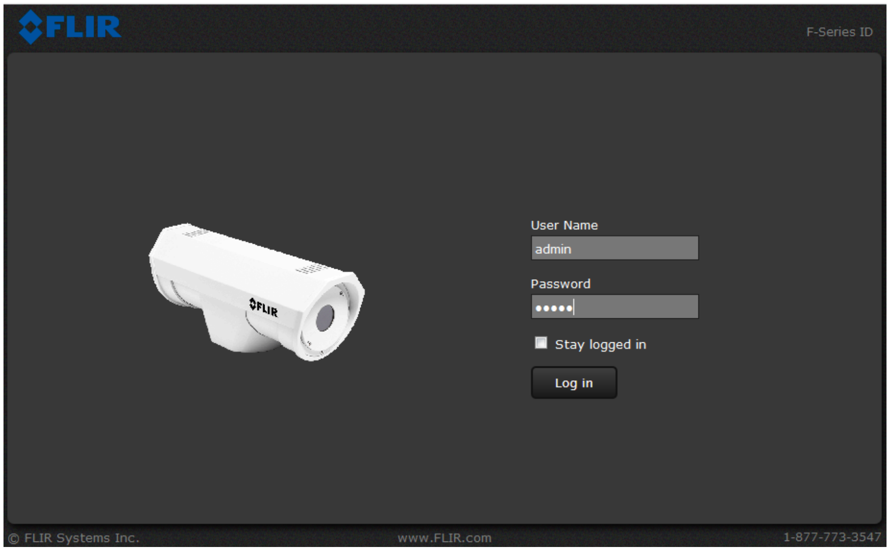
The **user** login can be used to do the initial bench test of the camera. The **expert** login may be used to make configuration changes such as setting the IP address and other server settings. The **admin** login has access to all configuration, setup, and maintenance settings.

Two web sessions can be active at once. An inactive session will be logged out after 20 minutes.

Note

> A VMS Remote to the camera, ONVIF or Nexus CGI, uses the same password as the web interface. Refer to VMS Remote, pg. 46.

Open a web browser — Google Chrome, Mozilla Firefox, Microsoft Internet Explorer 11, or Microsoft Edge — and enter the camera IP address. The login screen with a picture of the camera will appear. Enter **admin** for the User Name and **admin** for the Password, and click Log in.



User Name: admin

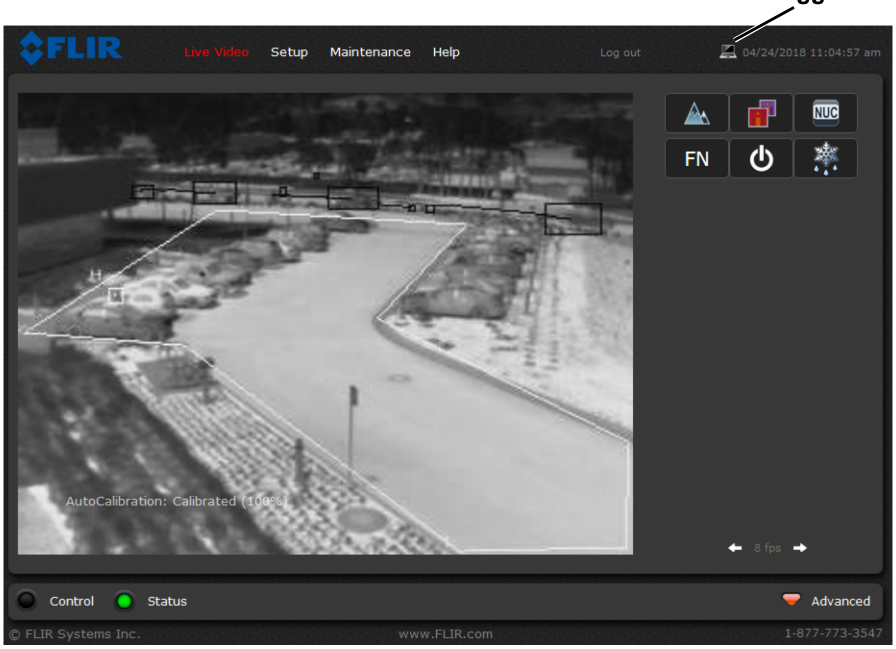
Password: •••••

□ Stay logged in

2.2.3 Live Video Page

The **Live Video** page displays a live image from the camera on the left part of the screen. Along the top of the screen are some menu choices, including **Live Video** (the red text indicates it is selected), **Setup**, **Maintenance**, **Help,** and **Log out**.

On the right side are some control buttons.



Toggle Time

AutoCalibration: Calibrated (100%)

Figure 2-1: Live Video Web Page – admin login

The frame rate selector, in the lower right corner of the web page, allows the user to change the frame rate in the browser from the default 8 fps up to 16 fps. This controls the frame rate of the user's own web browser only, and does not affect the video streams to other users or to an NVR. If the live video is not displayed, refer to Troubleshooting Tips, pg. 30.

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 factory configuration of the camera refer to the Maintenance > Product Info > Identification web page (requires Admin login).

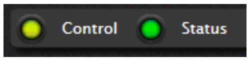
Log out

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.

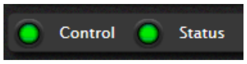
Toggle PC/Camera time

Use this button to display either the PC time or the camera time.

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.



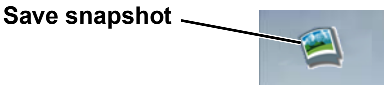
A user is able to request control of the camera by clicking on the yellow or black light, or simply by sending a command to the camera. After a short pause, the Control light should turn green. Be patient, there may be a slight delay between each command while the browser waits for a response from the camera.

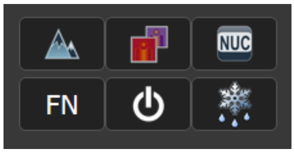
If a command is sent to the camera when the user does not have control, the command will not be executed, and it is necessary to send the command again once the light is green.

Web Control Panel

The control buttons on the right side of the page can control the camera. When the mouse cursor is positioned over a button, a tool tip is displayed which explains the function of the button.

When the mouse is positioned over the video window, a snapshot button is shown in the upper right corner of the video image. The snapshot button will save an image as a .jpg file to the selected destination folder or as determined by the web browser.





The functions of the buttons appearing for the F-Series ID cameras are described below:

Toggle Polarity

This button changes the way various objects are displayed in the image, for example, with hot objects displayed as white and cold objects as black, or vice versa.

Toggle Palette

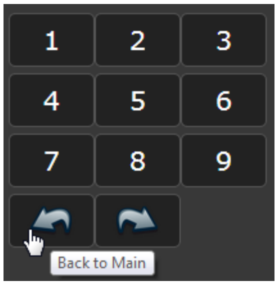
This button causes the IR camera to cycle through different color palettes. Each of the palettes presents the IR image using a different color scheme. Use the Toggle Polarity button to invert the palette, for example, between white hot and black hot.

Perform IR NUC Calibration

This button causes the camera to do a manual Non-Uniformity Correction (NUC) operation. The F-Series ID camera, by default, does an automatic NUC calibration as required based on changes in temperature.

Function

When the Function button is selected, the keypad changes to a numeric keypad. A tool tip can be shown when a function has been assigned to a number. Use the back (↶) arrow to return to the Control Panel.



Analytics On/Off

The F-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, pg. 38.

De-Ice On/Off

This button will turn the De-Ice heater on or off. The heater will run, controlled by the thermostat, for approximately one hour unless turned off by the user again selecting the De-Ice button.

2.3 Basic Camera Configuration

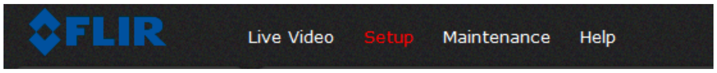
The following procedures describe how to do the most common basic camera configuration steps, such as setting the camera IP address and hostname and changing the user passwords.

2.3.1 Expert and Admin Accounts

When a user logs in as **expert** or **admin**, **Setup** and **Maintenance** menus are available. The **Setup** menu is used to make adjustments to the camera features.

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 (Maintenance Menu > Server Page, pg. 21). The **expert** login has access to the **Server** pages. The **admin** login provides access to all configuration options. The login passwords should be changed (**admin** login required) to prevent unauthorized access.

2.3.2 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 F-Series ID camera. For additional details, refer to Setup Menu, pg. 33.

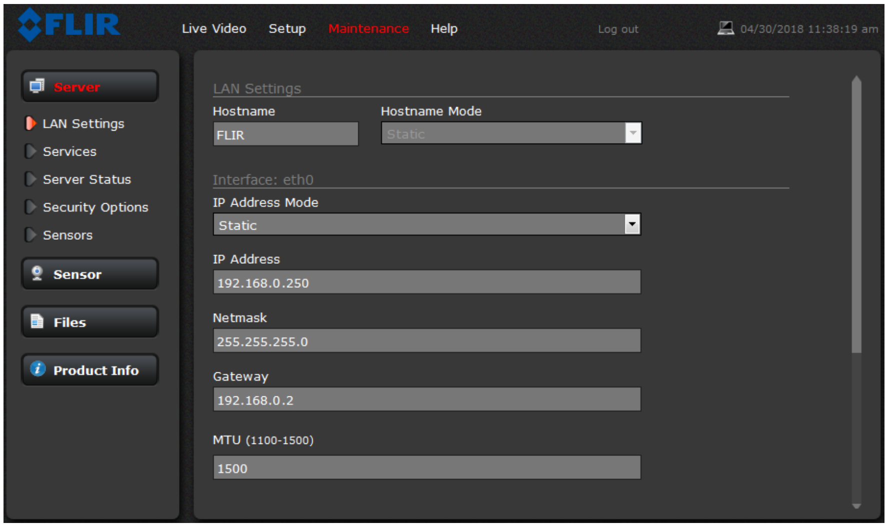
Adjustments to the IR settings should only be made by someone who has expertise with thermal cameras and a thorough understanding of how the various settings affect the image. In most installations, the only camera settings needed are available from the Web Control panel on the Live Video page (Palettes 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. 36.

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. 43). The **Maintenance** menu also provides access to other configuration options.

2.3.3 Maintenance Menu > Server Page

The basic camera configuration steps are accessed through the **Maintenance** menu, using the **Server** page. When a user logs in as **expert** or **admin** the **Server** page is available. The **LAN Settings**, **Date and Time**, **Server Status**, and **Security Options** selections are described below.



LAN Settings

Hostname: FLIR

Hostname Mode: Static

Interface: eth0

IP Address Mode: Static

IP Address: 192.168.0.250

Netmask: 255.255.255.0

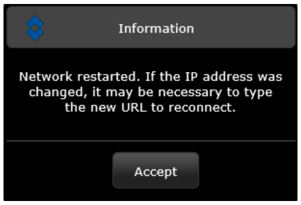
Gateway: 192.168.0.2

MTU (1100-1500): 1500

LAN Settings

If the IP address of the camera is changed, the PC may no longer be on the same network and may not be able to access the camera. Also refer to Set IP Address using the FLIR Discovery Network Assistant (DNA), pg. 15.

When the LAN settings are changed and the Save button is clicked, a pop-up message will appear to indicate the network interface should be restarted. Once all the changes have been made and saved, click on the **Restart Network** button at the bottom of the page.



Information

Network restarted. If the IP address was changed, it may be necessary to type the new URL to reconnect.

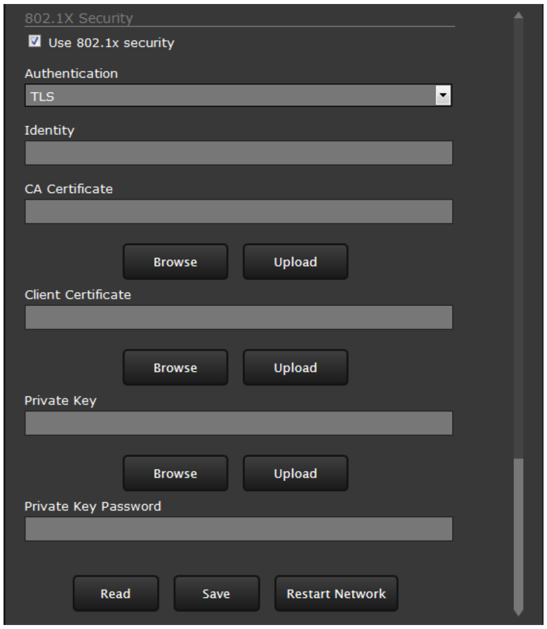
LAN Settings > IEEE 802.1X Security

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 central authority. The F-Series ID supports authentication using Transport Layer Security (TLS) protocol.

Notes

> The camera must be connected to a switch or other device on the network that supports IEEE 802.1x.
>
> The camera also supports TLS for communication with clients outside the LAN, such as web browsers. For information about enabling and configuring TLS for communication outside the LAN, see Services > TLS Config, pg. 25.

Configure IEEE 802.1x authentication using TLS



802.1X Security

☑ Use 802.1x security

Authentication: TLS

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

Step 2 Select the **Use 802.1x security** checkbox.

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.

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 **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.

If uploading a PKCS #12 file, the private key must be a valid PKCS #12 file.

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

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

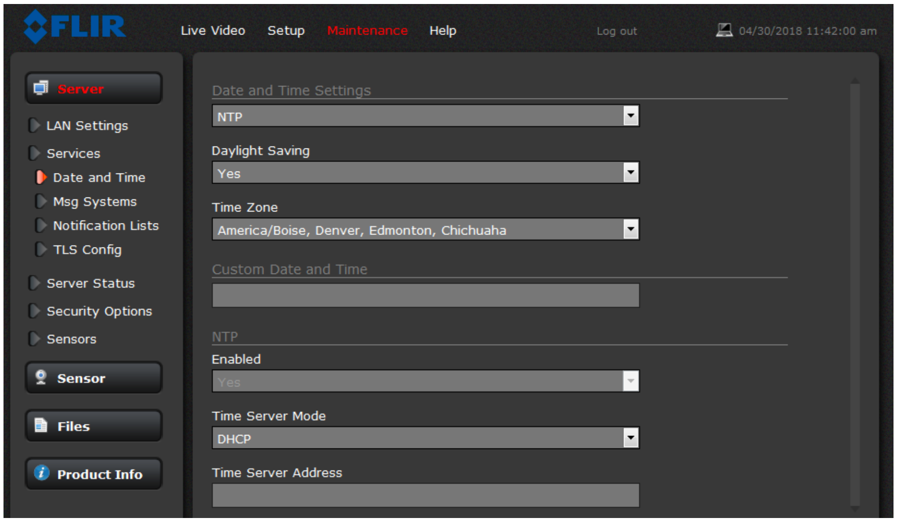
Services > Date and Time

The camera can be directed to an available NTP server that synchronizes all the system clocks on the network or the date and time can be set manually for only the current camera.

Note

> The server must be stopped before date and time settings can be saved.

NTP Mode: If your network uses an NTP server, select NTP and enter the NTP server information (static IP or DHCP). Ensure that the NTP server can be found if it is public or located on a different network.



Date and Time Settings: NTP

Daylight Saving: Yes

Time Zone: America/Boise, Denver, Edmonton, Chichuaha

Custom Date and Time:

NTP

Enabled: Yes

Time Server Mode: DHCP

Time Server Address:

Stop the server. The server must be stopped before date and time settings can be saved.

Click the Save button at the bottom of the page.

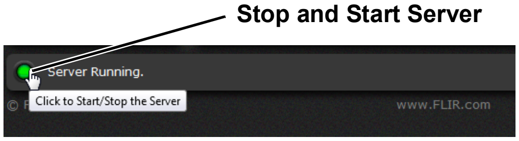
After the settings are saved, reboot the system. Refer to Server Status, pg. 27.

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

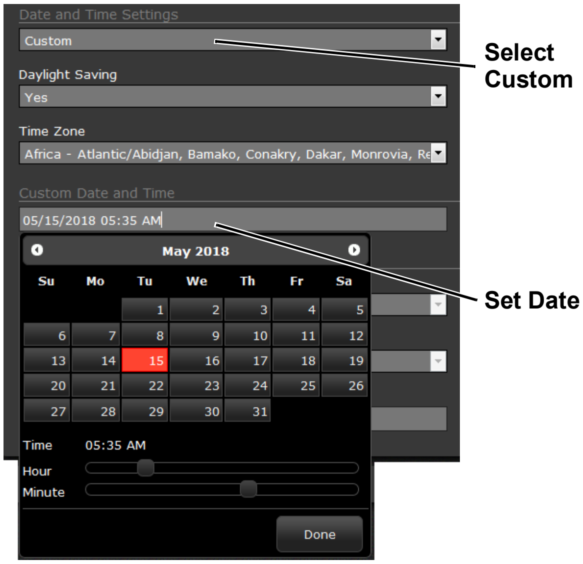
Stop the server. The server must be stopped before date and time settings can be saved.

Set the date and time parameters and click the Save button at the bottom of the page.

After the settings are saved, restart the server.



Server Running.



Date and Time Settings: Custom

Daylight Saving: Yes

Time Zone: Africa - Atlantic/Abidjan, Bamako, Conakry, Dakar, Monrovia, Re

Custom Date and Time: 05/15/2018 05:35 AM

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

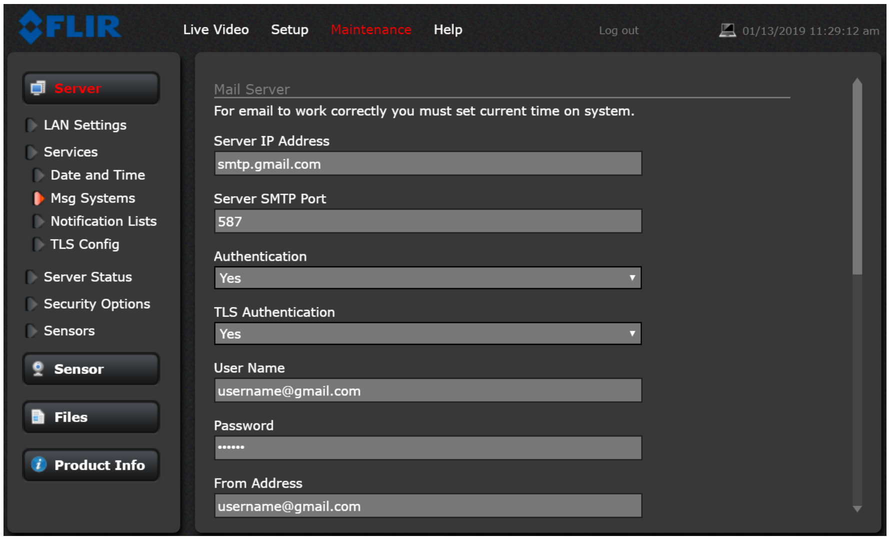
Time 05:35 AM

Hour

Minute

Services > Msg Systems

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



Mail Server

For email to work correctly you must set current time on system.

Server IP Address: smtp.gmail.com

Server SMTP Port: 587

Authentication: Yes

TLS Authentication: Yes

User Name: username@gmail.com

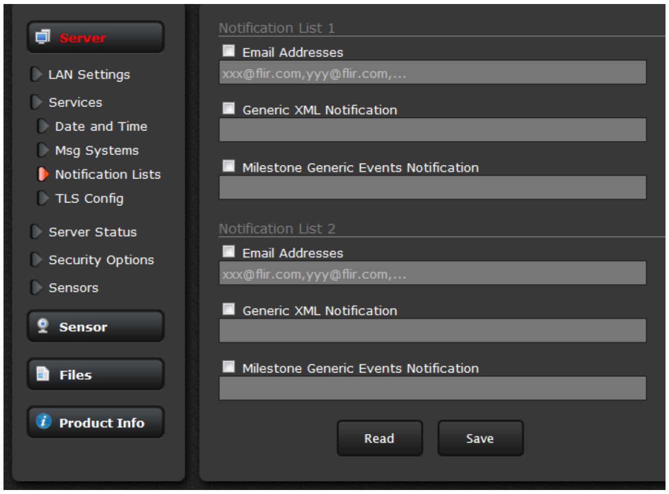
Password: ••••••

From Address: username@gmail.com

Consult with your network/IT administrator to determine the IP Address/name of the mail server, the appropriate port for SMTP and authentication settings. If the email server is on a different network, ensure the IP default gateway and DNS servers are configured in LAN Settings, pg. 21. Configure the Msg Systems page with mail server information and then click **Save**. Using the admin login, check that Messaging is enabled. Refer to Maintenance > Sensor > Summary Page, pg. 56.

Services > 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. When a message it sent, it can be sent to one of three different email lists: Default Notification List, Notification List 1, or Notification List 2. Separate the email addresses by commas or semicolons. This allows the system to be configured to send certain alarm notifications to one group and other alarm notifications to a different group. The appropriate notification list is specified when setting up the Alarm Manager rule.



Notification List 1

□ Email Addresses: xxx@flir.com,yyy@flir.com,...

□ Generic XML Notification

□ Milestone Generic Events Notification

Notification List 2

□ Email Addresses: xxx@flir.com,yyy@flir.com,...

□ Generic XML Notification

□ Milestone Generic Events Notification

Services > TLS Config

The settings on this page enable secure, encrypted communication between clients and the camera; for example, when your web browser accesses the camera's web interface.

Note

> The camera also supports TLS authentication over the camera's LAN. For information about configuring TLS authentication for LAN communication, see LAN Settings > IEEE 802.1X Security, pg. 22.

By default, TLS is disabled. Before enabling it, you need to generate or upload a valid certificate. You can:

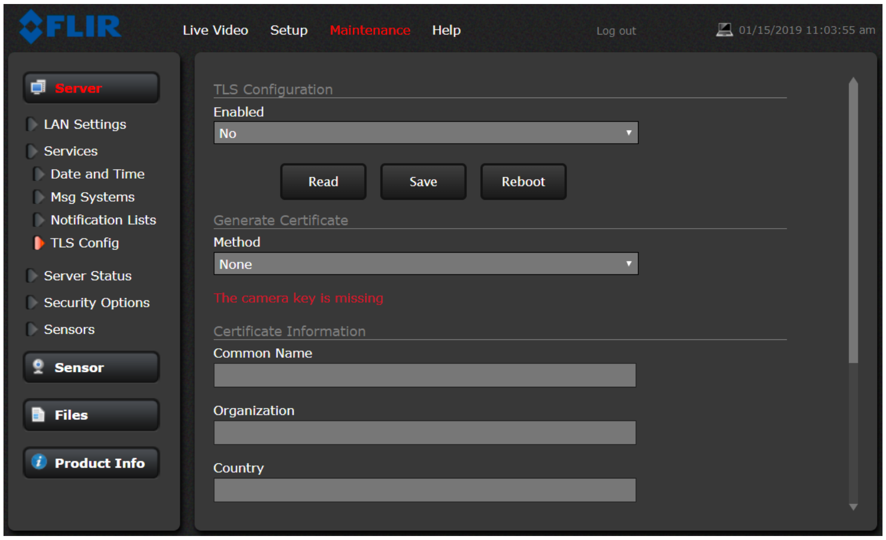
- Use the camera web interface to generate a self-signed certificate.
- Upload a self-signed certificate.
- Upload a certificate signed by a third-party.

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

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

For private key files: *.key

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



TLS Configuration

Enabled: No

Generate Certificate

Method: None

The camera key is missing

Certificate Information

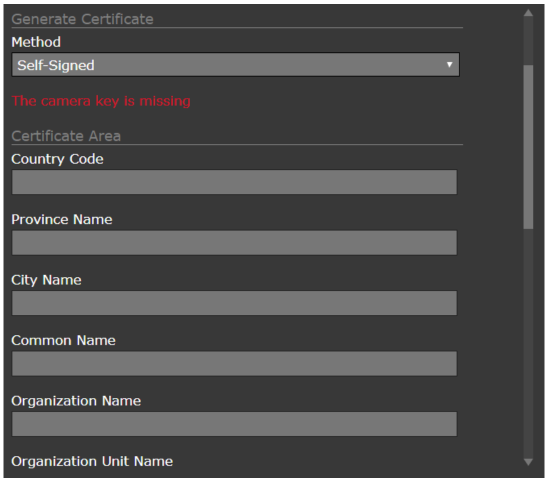
Common Name:

Organization:

Country:

To generate and install a self-signed certificate:

Step 1 Under Generate Certificate, for **Method**, select **Self-Signed**.



Generate Certificate

Method: Self-Signed

The camera key is missing

Step 1 Enter information such as country code, city name, and organization name.

Step 2 Scroll to the bottom of the page and click **Generate Certificate**.

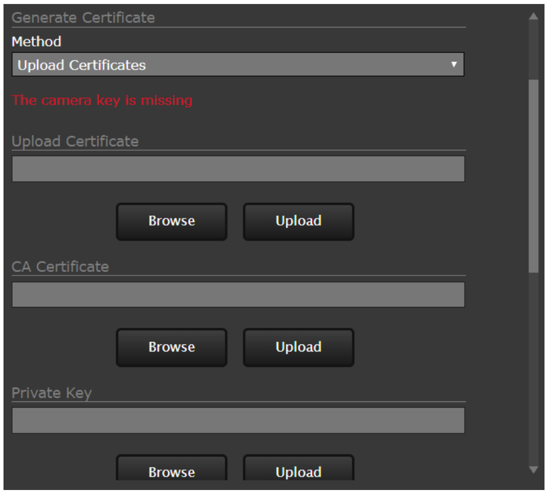
Step 3 Allow 15 seconds for the camera to generate the certificate, at which point a confirmation appears.

To upload a self-signed or third-party CA signed certificate:

Step 1 For **Method**, select **Upload Certificates**.

Step 2 If you are uploading a self-signed certificate, under **Upload Certificate**, browse for and upload the public key file. Then, under **Private Key**, browse for and upload the private key file.

If you are uploading a third-party CA signed certificate, under **Upload Certificate**, browse for and upload the public key file. Under **CA Certificate**, browse for and upload the CA certificate file. Under **Private Key**, browse for and upload the private key file.



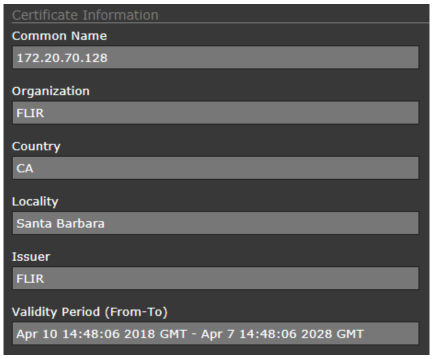
Generate Certificate

Method: Upload Certificates

The camera key is missing

Step 3 Verify that the camera certificate files are valid. Make sure *Certificates are OK* appears under **Method**.

Certificate information appears at the bottom of the **TLS Config** page, under **Certificate Information**:



Certificate Information

Common Name: 172.20.70.128

Organization: FLIR

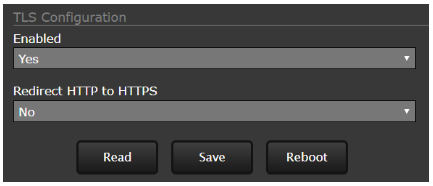
Country: CA

Locality: Santa Barbara

Issuer: FLIR

Validity Period (From-To): Apr 10 14:48:06 2018 GMT - Apr 7 14:48:06 2028 GMT

To enable and configure TLS:



TLS Configuration

Enabled: Yes

Redirect HTTP to HTTPS: No

Step 1 Under TLS Configuration, for **Enabled**, select **Yes**.

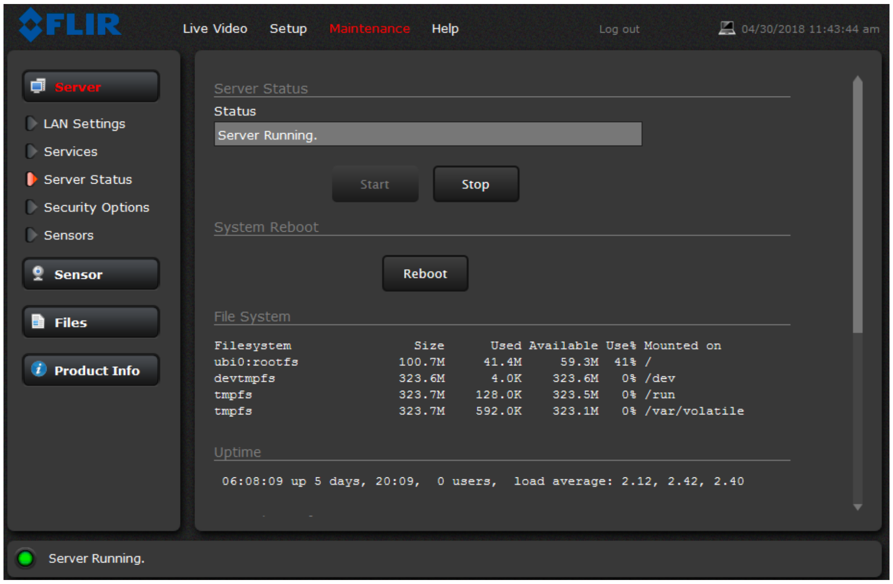
Step 2 Select whether to redirect HTTP requests to HTTPS.

Step 3 Click **Save**.

Step 4 Click **Reboot**. The camera reboots. After the camera reboots, TLS is enabled.

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 and for rebooting the system. The **Uptime** section of the **Server Status** page shows how long the camera has been running, number of users, and the load on the camera processor. All values are updated only when the Server Status page is first accessed.



Server Status

Status: Server Running.

System Reboot

File System

```
Filesystem              Size      Used Available Use% Mounted on
ubi0:rootfs           100.7M     41.4M     59.3M  41% /
devtmpfs              323.6M      4.0K    323.6M   0% /dev
tmpfs                 323.7M    128.0K    323.5M   0% /run
tmpfs                 323.7M    592.0K    323.1M   0% /var/volatile
```

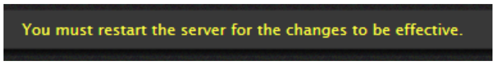
Uptime

```
 06:08:09 up 5 days, 20:09,  0 users,  load average: 2.12, 2.42, 2.40
```

Server Running.

After making configuration changes, save the changes (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 active. The server has a configuration that is active and running, and another configuration that is saved (and possibly different than the running configuration).

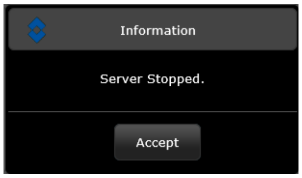
The message at the bottom of the page indicates that it is necessary to restart the server.



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.

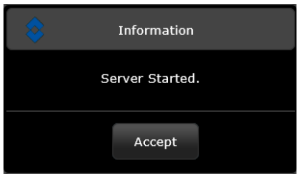
When the server is stopped and the page is refreshed, the status will show Server Stopped and the Start button will be enabled.



Information

Server Stopped.

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.

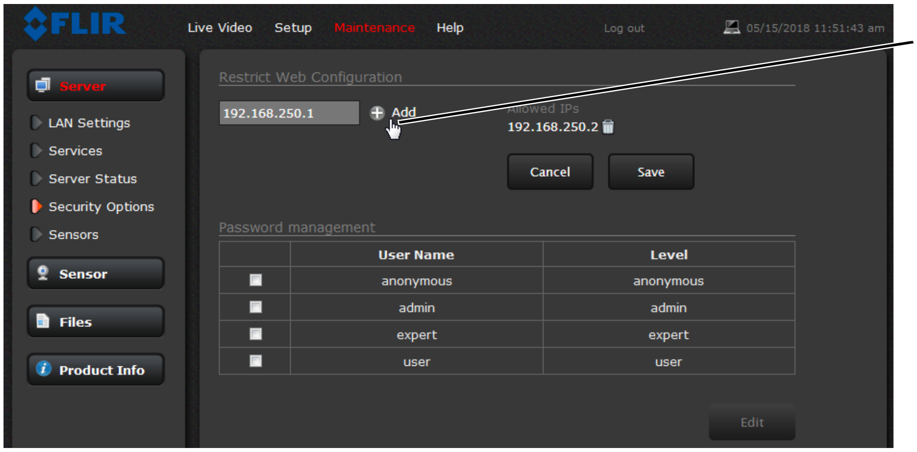


Information

Server Started.

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 can change or set any password. The **expert** login can only configure the **expert** login password.



Restrict Web Configuration

192.168.250.1

Allowed IPs

192.168.250.2

Password management

	User Name	Level
□	anonymous	anonymous
□	admin	admin
□	expert	expert
□	user	user

Add IP address

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.

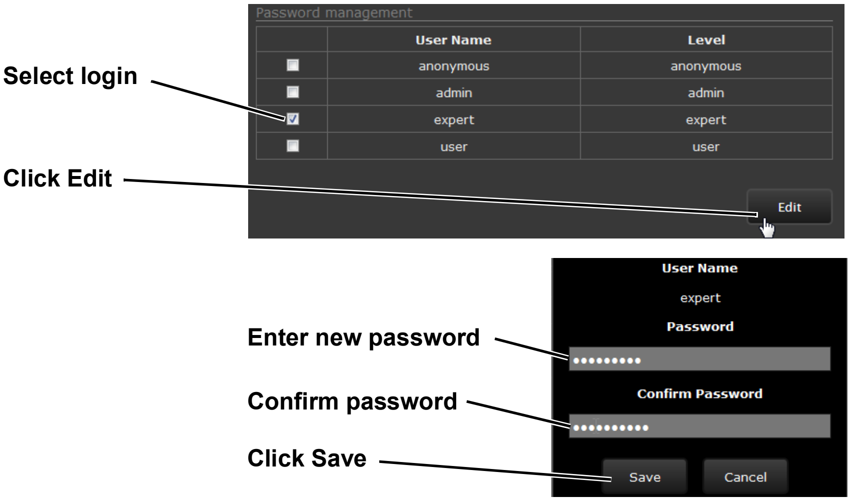
Note

> A VMS Remote to the camera, ONVIF or Nexus CGI, uses the same password as the web interface. Refer to VMS Remote, pg. 46.

This document does not contain any export-controlled information.

To maintain security of the system, set new passwords for all of the login accounts.

- **anonymous**—Used for ONVIF communication.
- **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 passwords.



Password management

	User Name	Level
☐	anonymous	anonymous
☐	admin	admin
☑	expert	expert
☐	user	user

User Name

expert

Password

•••••••••

Confirm Password

••••••••••

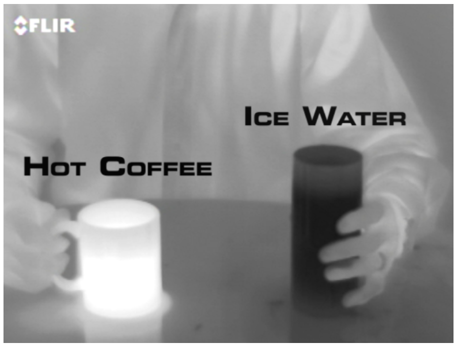
2.4 Thermal Imaging Overview

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.

It takes some time getting used to the thermal imagery from the camera, especially for someone who only has experience with normal daylight cameras. An understanding of the differences between thermal and daylight cameras can help with getting the best performance from the thermal camera.

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 an daylight camera, there has to be a source of visible light (such as the sun or lights) that reflects off the objects in the scene to the camera. The same is true with human eyesight; the vast majority of what people see is based on **reflected** light energy.

On the other hand, the thermal camera 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 the type of infrared energy that the thermal camera can detect. Even very cold objects, like ice and snow, radiate this type of energy.



The camera is capable of sensing very small temperature differences, and produces a video image that typically has dramatic contrast in comparison to daylight cameras. This high contrast level from the thermal video enables intelligent video analytic software to perform more reliably.

The performance of the camera varies throughout the day. Right 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.

While the imagery on the monitor may at first look similar to ordinary black and white daylight video, experience with the camera in varying conditions and seasons will lead to an appreciation of the characteristics that make thermal imaging distinct. A few tips on how to interpret some of the imagery may help to make the most of the system.

The camera senses small differences in apparent radiation from the objects in view, and displays them as either white (or lighter shades of gray) for warmer objects, and black (or darker shades of gray) for colder objects. This is why hot objects such as parts on an engines and exhaust pipes appear white, while the sky, puddles of water and other cold objects appear dark (or cool). 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.

2.5 Troubleshooting Tips

If help is needed during the installation process, contact a local FLIR representative. FLIR Systems, Inc. offers a 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/

No video: 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 RCA connection inside the camera and determine if it produces an image.

If the camera still does not produce an image, contact the FLIR dealer or reseller who provided the camera, or contact FLIR directly (contact information is provided on the rear cover of this manual).

Performance varies with time of day: It may be possible to observe 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, compared to other times of the day. 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 generally will allow the camera to produce higher-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 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. Confirm that the IP address for the PC is on the same network as the camera.

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.

Determine if Windows Personal Firewall is blocking the packets. Turn off the firewall or add an exception for the client program. Typically when a program runs for the first time, a pop-up notification may ask for permission to communicate on the network. Select the check boxes (domain/private/public) that are appropriate for the network.

Image too dark or too light: By default the F-Series ID 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.

Unable to View Video Stream: If the video stream from the camera is not displayed in a client program, 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. Given the camera IP address of 192.168.0.250, the complete connection string for each of the video stream is as follows:
VIDEO 0 - rtsp://192.168.0.250:554/stream1/sensor1
VIDEO 1 - rtsp://192.168.0.250:554/stream2/sensor1

To maintain compatibility with legacy systems the stream names are aliased as:
ch0 = stream1/sensor1 and ch1 = stream2/sensor1.

Refer to Video Setup, pg. 34.

Noisy image: A noisy image is usually attributed to a cable problem (too long or inferior quality) or the cable is picking up electromagnetic interference (EMI) from another device. Although coax cable has built-in losses, the longer the cable, or the smaller the wire gauge, 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.

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.

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. The thermal imaging camera often provides a considerable advantage over a visible camera in a back-lit situation. However, the sun may introduce image artifacts that eventually will be corrected but it may take some time to recover. The amount of time needed will depend on how long the camera was exposed to the sun. The longer the exposure, the longer the recovery time needed.

visible camera **thermal camera**

Figure 2-2: Images facing sun

3 Advanced Configuration

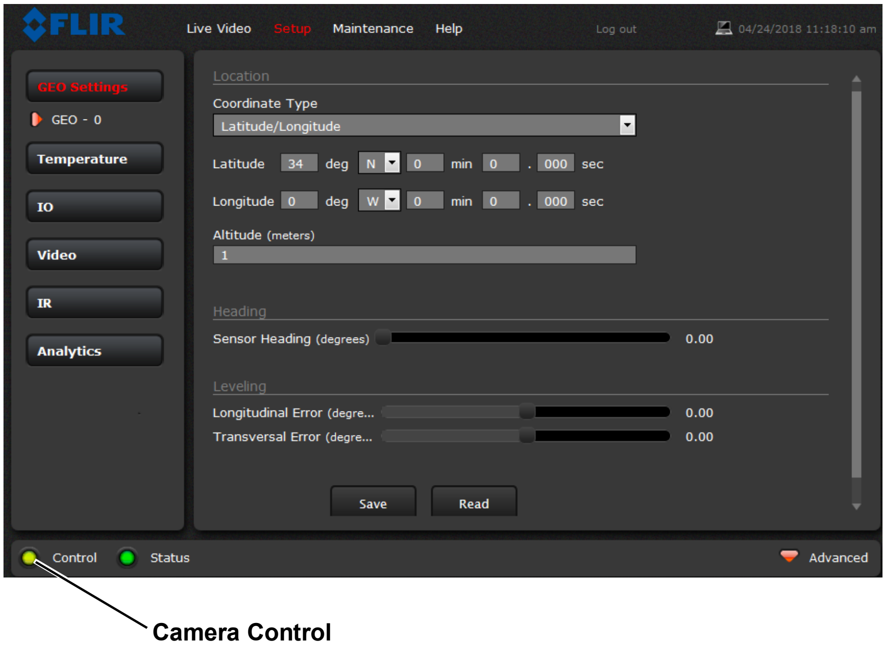
In this chapter, additional setup and configuration settings related to the following topics are described:

- Setting up the video streams to optimize quality and network performance
- 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. 57).

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. 38).



Location

Coordinate Type: Latitude/Longitude

Latitude 34 deg N 0 min 0 . 000 sec

Longitude 0 deg W 0 min 0 . 000 sec

Altitude (meters) 1

Heading

Sensor Heading (degrees) 0.00

Leveling

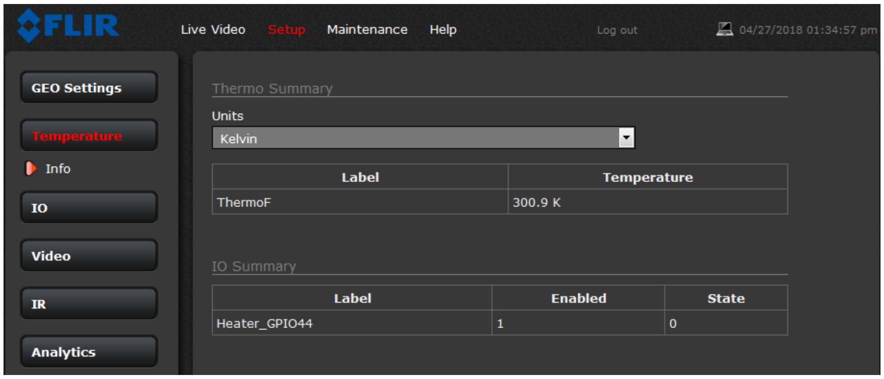
Longitudinal Error (degre... 0.00

Transversal Error (degre... 0.00

Camera Control

3.1.1 Temperature Page

The Temperature Info page displays temperature readings from the camera and Heater status. Select the temperature units to display Kelvins, degrees Celsius, or degrees Fahrenheit. The Heater_GPIO44 signal state when equal to one indicates that the heater is on. The heater can be turned on under thermostat control for approximately one hour with the De-Ice button on the Live Video page.



Thermo Summary

Units: Kelvin

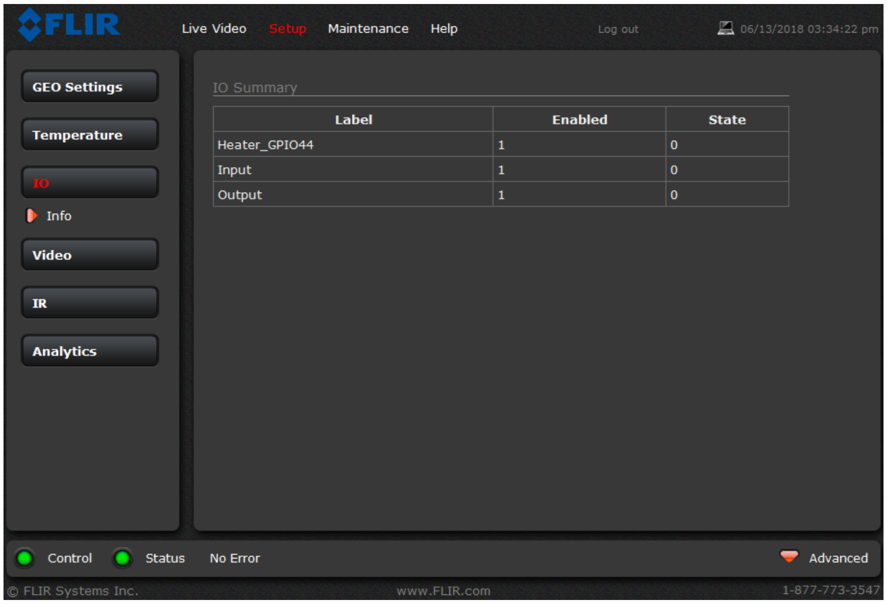
Label	Temperature
ThermoF	300.9 K

IO Summary

Label	Enabled	State
Heater_GPIO44	1	0

3.1.2 Input/Output (IO) Page

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



IO Summary

Label	Enabled	State
Heater_GPIO44	1	0
Input	1	0
Output	1	0

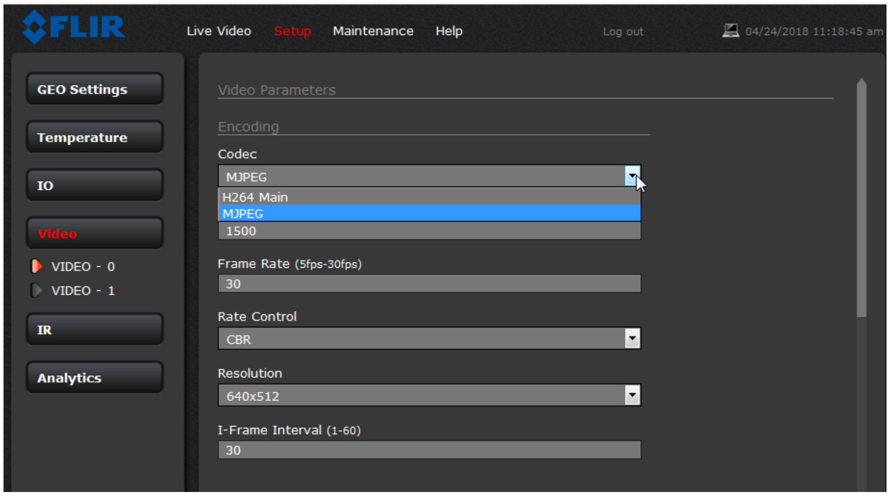
Table 3-1: GPIO Labels

Heater_GPIO44	Internal heater control output signal
Alarm Input	User GPIO signals are enabled by default. Refer to General Purpose Input/Output (GPIO), pg. 6, GPIO Alarm Connections, pg. 12, and Devices Menu GPIO, pg. 48.
Alarm Output	

3.1.3 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).

By default, both streams use H.264 encoding. To modify parameters that affect a particular IP Video stream from the camera, select the appropriate link (for example, **Video - 0**).



Video Parameters

Encoding

Codec: MJPEG (H264 Main, MJPEG, 1500)

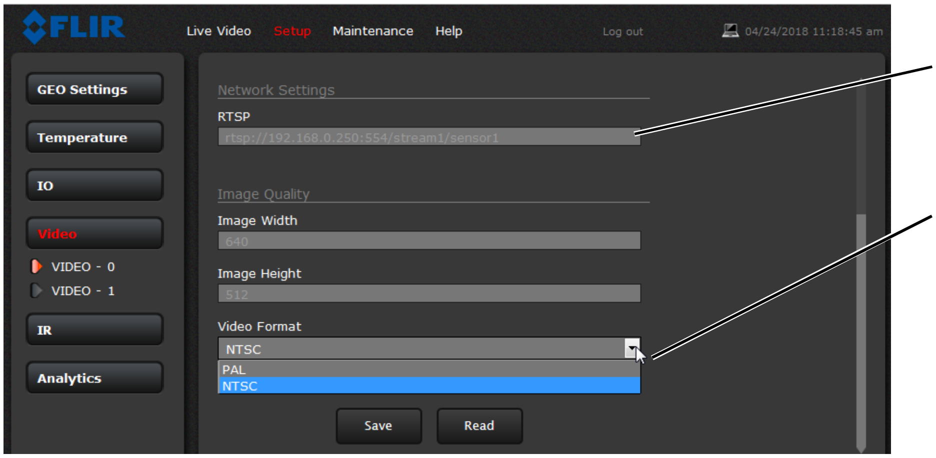
Frame Rate (5fps-30fps): 30

Rate Control: CBR

Resolution: 640x512

I-Frame Interval (1-60): 30

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. In particular, the Encoding parameters described below.



Network Settings

RTSP: rtsp://192.168.0.250:554/stream1/sensor1

Image Quality

Image Width: 640

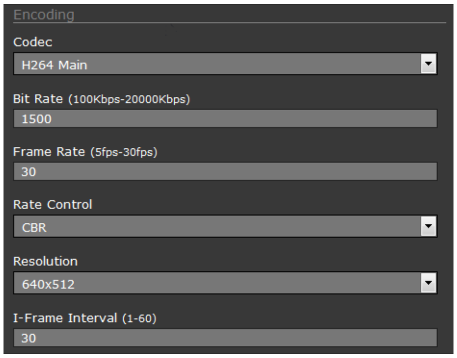
Image Height: 512

Video Format: NTSC (PAL, NTSC)

Streaming address for VIDEO-0

Select analog video format

Scroll down to save the changes through power cycles.



Encoding

Codec
H264 Main

Bit Rate (100Kbps-20000Kbps)
1500

Frame Rate (5fps-30fps)
30

Rate Control
CBR

Resolution
640x512

I-Frame Interval (1-60)
30

The parameters in the Encoding section will have a significant impact on the quality and bandwidth requirements of the video stream. In general it is recommended that the default values are used initially, and then individual parameters can be modified and tested incrementally to determine if the bandwidth and quality requirements are met.

For the video streams, the Codec options are H.264 or MJPEG. MJPEG requires the most amount of processing.

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.

When the Rate Control parameter is set to VBR (Variable Bit Rate), the Bit Rate parameter is used as an upper limit bit rate and the system keeps the stream at or under the target bit rate.

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 Resolution parameter controls the video resolution and therefore can have a large impact on bandwidth usage. The higher the resolution, the larger the size of the frame and the higher the network bandwidth required.

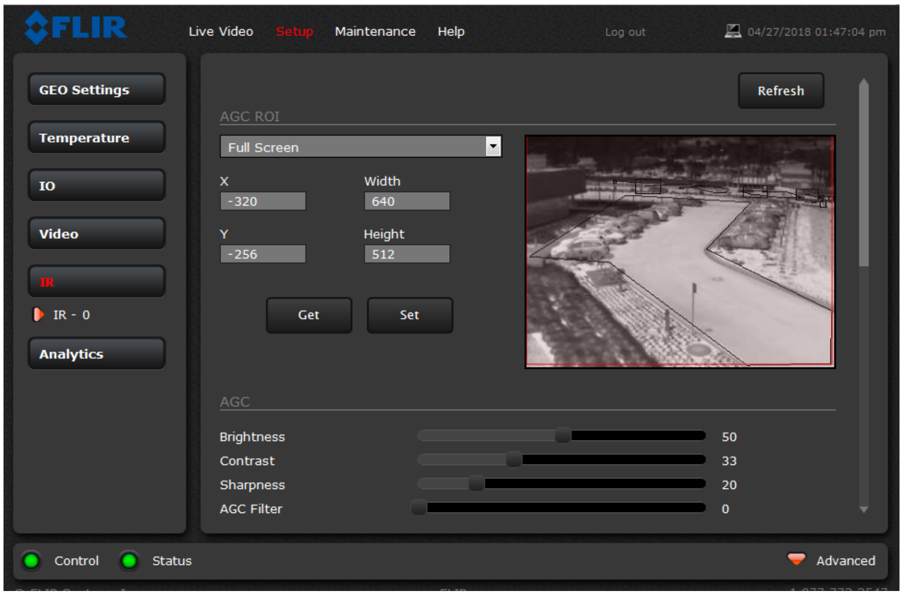
As a rule of thumb, if the video will be viewed on its own and on a reasonably large screen, a large image size setting may look better. On the other hand, if the video is shown as a tile in a video wall, a smaller image size may look as good and consume less bandwidth.

3.1.4 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).



AGC ROI

Full Screen

X: -320 Width: 640

Y: -256 Height: 512

AGC

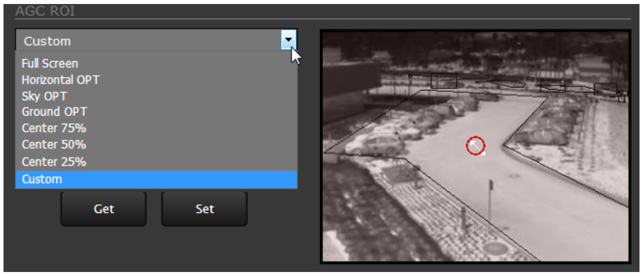
Brightness 50

Contrast 33

Sharpness 20

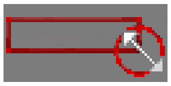
AGC Filter 0

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.

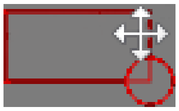


When Custom is selected, a handle is shown in the center of the screen.

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.



AGC

The AGC parameters affect how the overall IR video image appears. A combination of manual adjustments may provide a more appealing image, depending on personal preferences. Be aware that the settings that are optimal at one time may be less optimal a short time later, since conditions such as weather and time of day affect the image and are constantly changing.

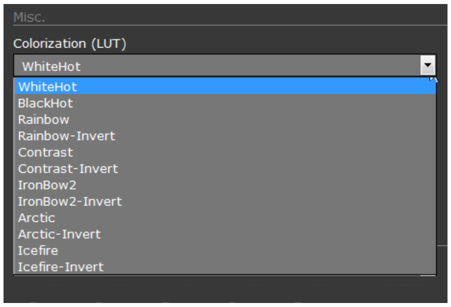
Note

> The Video Analytics default AGC Mode parameters are invoked when analytics is enabled. If parameters have been changed while analytics is disabled, they will be changed to the VA defaults when analytics is enabled again, but will be saved and invoked when analytics is disabled.

Experiment with different AGC parameters to find the settings that work best for a particular installation. Select **Save Settings** button at the bottom of the page to keep the settings after a power cycle or select the **Factory Defaults** button to return the settings to default values.

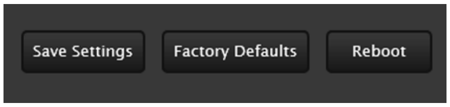
- **Brightness** (Gamma) setting determines the allocation of the 256 “shades of gray” produced by the AGC. Values above 50 allocate more shades of gray to hotter objects, while values below 50 allocate more shades of gray to lower temperature objects. Range 0 to 100.
- **Contrast** (Max Gain) can be 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** (AGC 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: Each Colorization Look Up Table (LUT) provides a different display of the various detected levels of thermal energy as either colors or gray-scale values. These color palettes can also be selected from the Live Video page (refer to Toggle Palette, pg. 19).



Save Settings

Click the **Save Settings** button at the bottom of the page to store the current settings as power up defaults. To restore the original settings, select the **Factory Defaults** button. Select **Reboot** to restart the sensor.



3.1.5 Video Analytics Setup

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

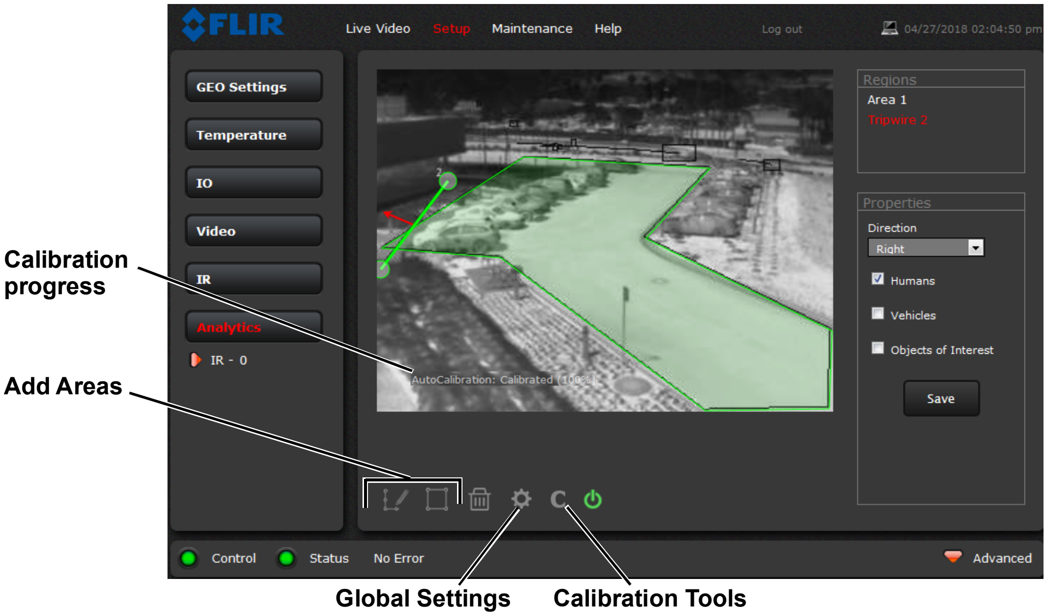
Note

> 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. 52).

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.



AutoCalibration: Calibrated (100%)

Direction: Right

☑ Humans

☐ Vehicles

☐ Objects of Interest

No Error

Figure 3-1: Analytics Page

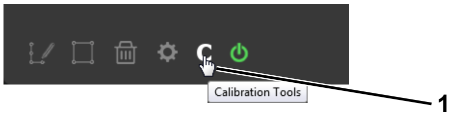
Analytics Calibration

- 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. Set detection Properties for each region.
- After calibration is finished, verify that the analytics detect and classify objects as expected.

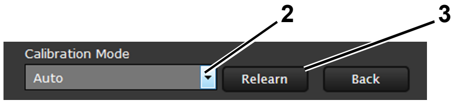
Auto Calibration

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 bottom left 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**.

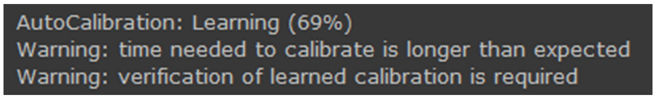


Calibration Mode: Auto

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 bottom left of the video (see Figure 3-1).

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

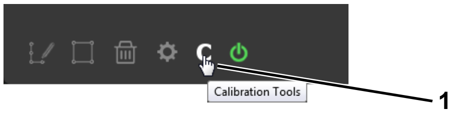


```
AutoCalibration: Learning (69%)
Warning: time needed to calibrate is longer than expected
Warning: verification of learned calibration is required
```

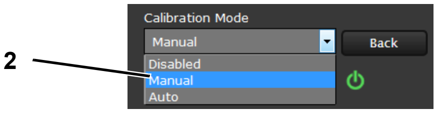
Step 4 After calibration is complete set up detection areas and check calibration. Refer to Global Settings, pg. 41, Creating Analytics Regions, pg. 42, and Check Calibration, pg. 43.

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**.

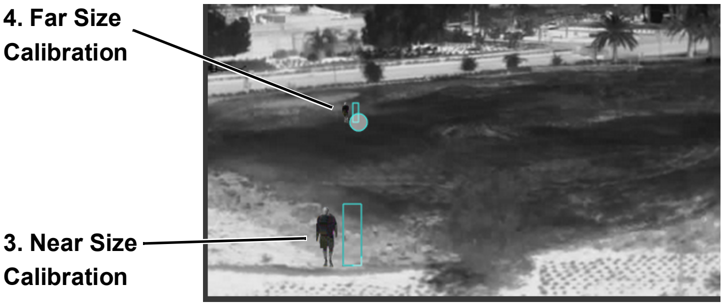


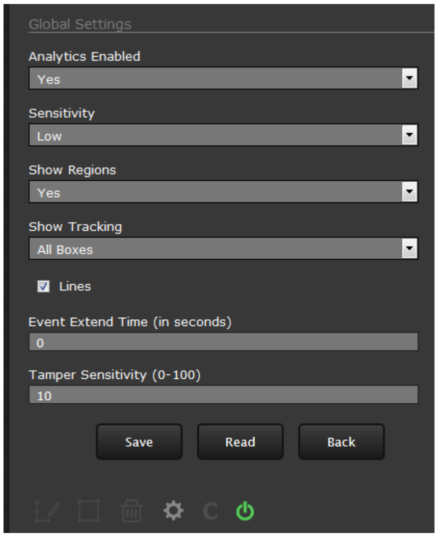
Figure 3-2: Manual Calibration

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. 41, Creating Analytics Regions, pg. 42, and Check Calibration, pg. 43.

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



Global Settings

Analytics Enabled: Yes

Sensitivity: Low

Show Regions: Yes

Show Tracking: All Boxes

☑ Lines

Event Extend Time (in seconds): 0

Tamper Sensitivity (0-100): 10

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.

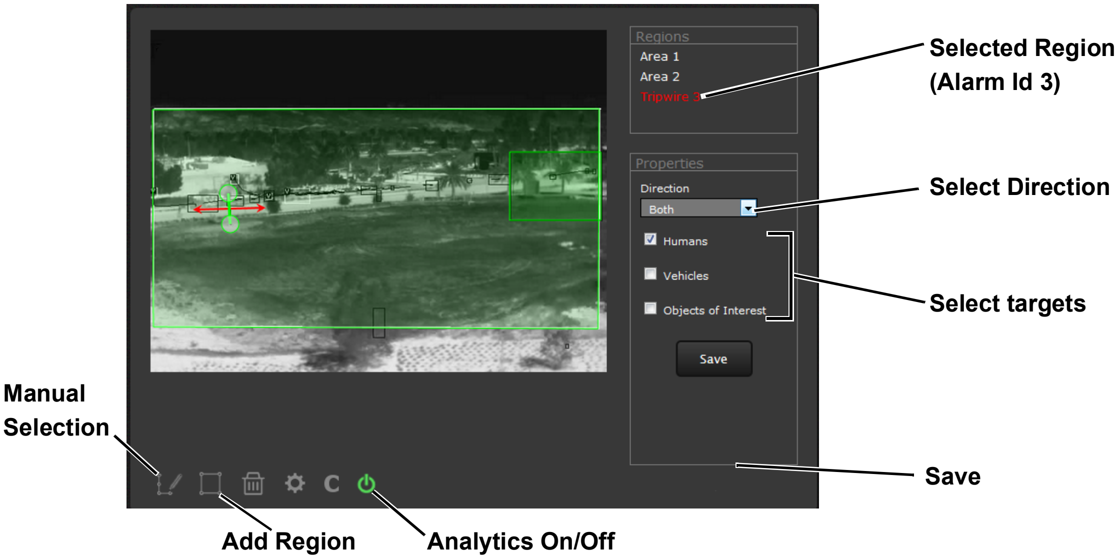
The tracking display options are: **All Boxes**, **Classified Boxes**, **Show Triggered**, and **No Boxes**. If either option to show boxes is selected, a check box enables a tracking line with each detection box.

- **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).
- **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 to return to the Analytics Setup page.

This document does not contain any export-controlled information.

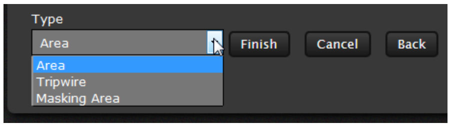
Creating Analytics Regions



Regions
Area 1
Area 2
Tripwire 3

Properties
Direction: Both
☑ Humans
□ Vehicles
□ Objects of Interest

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.



Type: 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.

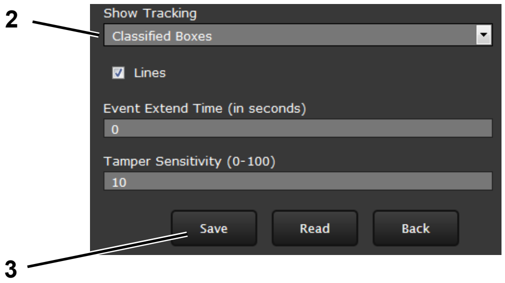
- With **Masking Area** selected, click in the video to create the first corner of the area. Continue adding corners, then select Finish to complete the area.

  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.

Check Calibration

1. Click the ⚙ icon and set **Analytics Enabled** to **Yes**.
2. Set **Show Tracking** to **Classified Boxes** or **Show Triggered** and 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.

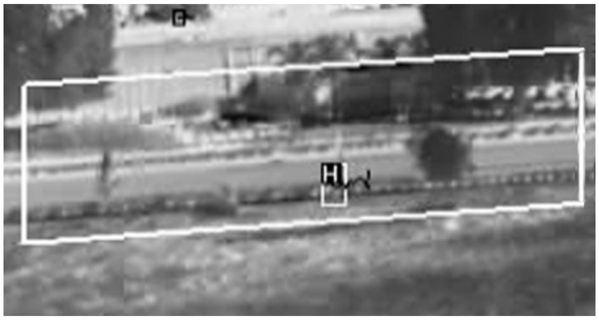

Show Tracking: Classified Boxes

☑ Lines

Event Extend Time (in seconds): 0

Tamper Sensitivity (0-100): 10

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

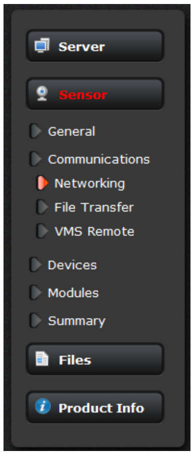


3.2 Maintenance Menu

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. Additional configuration options are available that are not described in this manual. For more information on setting or changing these camera parameters contact the local FLIR representative or FLIR Technical Support.

The basic camera configuration settings (**LAN Settings**, **Services**, and **Security Options)** available through the Maintenance Server menus are described in Maintenance Menu > Server Page, pg. 21. When logged in as **admin**, additional Maintenance menus are accessible, including **Sensor**, **Files** and **Product Info**.

3.2.1 Sensor Menu

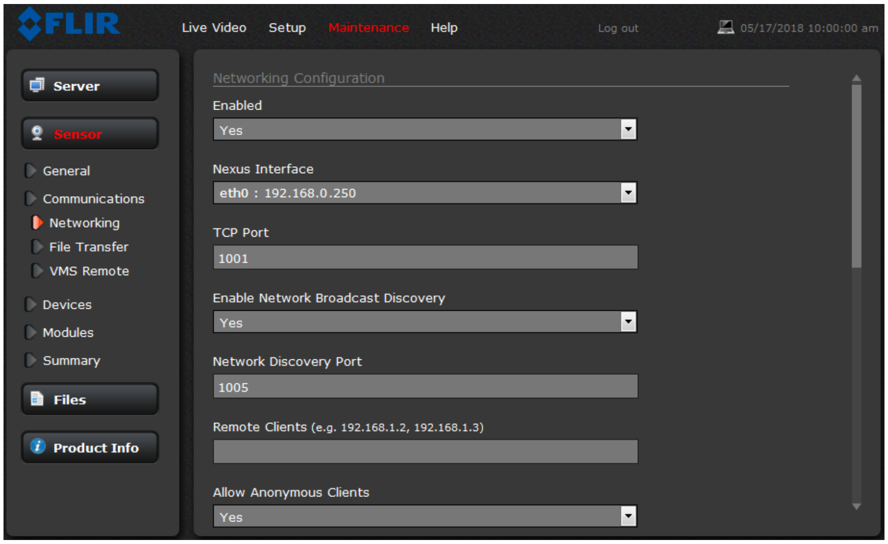


The configuration changes commonly used are done through the Sensor menu. Described below are configuration steps from the **Communications**, **Modules**, and **Summary** selections.

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. 21). 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 by remote clients by setting the "Allow Anonymous Clients" to No, and then enter IP addresses for the clients that are allowed access in the Remote Clients parameter.



Networking Configuration

Enabled: Yes

Nexus Interface: eth0 : 192.168.0.250

TCP Port: 1001

Enable Network Broadcast Discovery: Yes

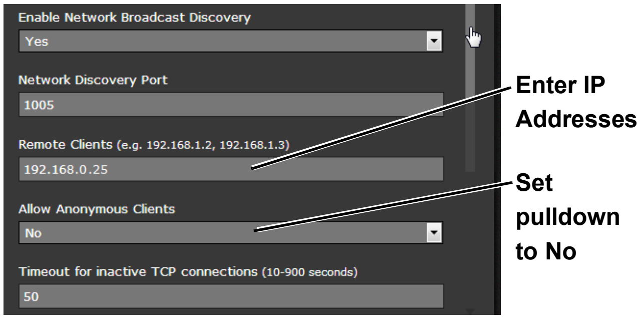
Network Discovery Port: 1005

Remote Clients (e.g. 192.168.1.2, 192.168.1.3):

Allow Anonymous Clients: Yes

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.

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): 192.168.0.25

Allow Anonymous Clients: No

Timeout for inactive TCP connections (10-900 seconds): 50

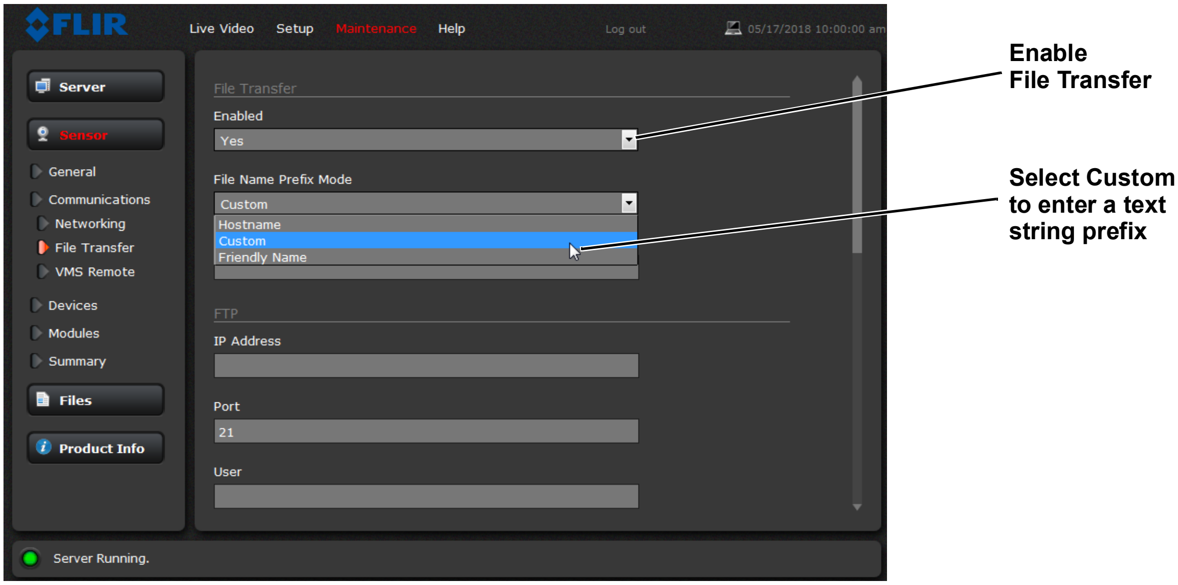
Enter IP Addresses

Set pulldown to No

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.

It is also possible to restrict access to the camera from a web browser. Refer to Security Options, pg. 28 to add an 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
21

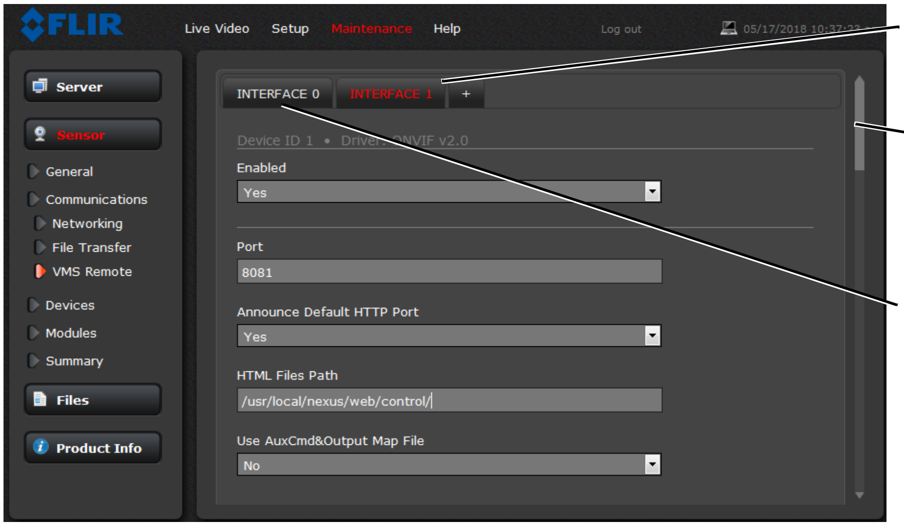
User

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 F-Series ID supports both NAS NFS and NAS Samba. To define rules for saving files to FTP server or NAS refer to Alarm Actions, pg. 53.

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. 28.



Device ID 1 • Driver: ONVIF v2.0

Enabled: Yes

Port: 8081

Announce Default HTTP Port: Yes

HTML Files Path: /usr/local/nexus/web/control/

Use AuxCmd&Output Map File: No

For ONVIF, use the settings in Interface 1

Scroll down

For Nexus CGI, use the settings in Interface 0

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

The ONVIF (Open Network Video Interface Forum) is an open industry forum for the development of a global standard for the interface of network video products. Refer to the VMS documentation to determine what parameter values are needed. By default, the camera is configured with a VMS Remote interface with ONVIF 2.0 parameters (Profile S).

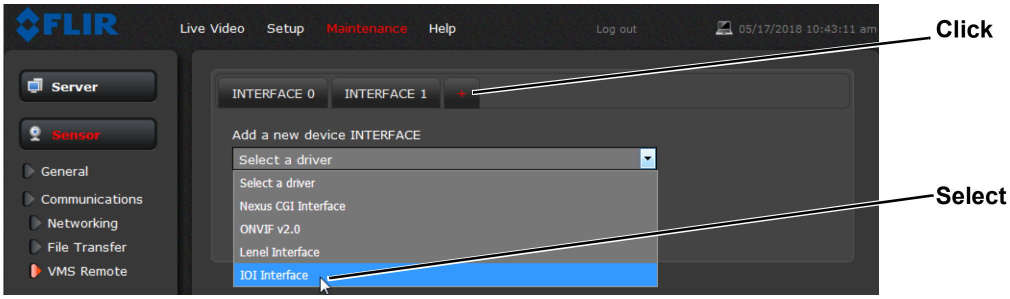
Several types of third-party Video Management Systems (VMS) are supported by FLIR IP cameras. Because these systems tend to evolve and change over time, contact the local FLIR representative or FLIR Technical Support to resolve any difficulties or questions about using this feature.

IOI Interface

Install this interface to hand-off F-Series ID detection events to the PTZ Tracker (trk-101-P). In order to implement a hand-off from the F-Series ID camera to a PTZ camera, the F-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 F-Series ID camera to monitor (refer to Video Analytics Setup, pg. 38). When a moving object is detected by the F-Series ID, the trk-101-P can control and move a PTZ camera to track and zoom in on the motion.

This document does not contain any export-controlled information.

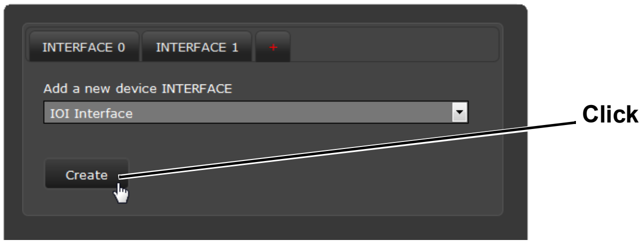
Step 1 Select **Maintenance > Sensor > VMS Remote**.



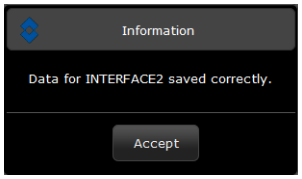
Step 2 Click **+** (+).

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

Step 4 Click **Create**.

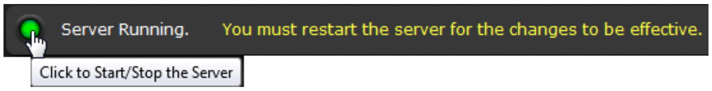


Step 5 Accept the message “Data for INTERFACE2 saved correctly”.



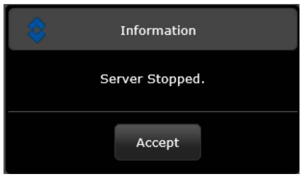
Data for INTERFACE2 saved correctly.

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

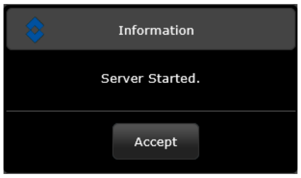


Server Running. You must restart the server for the changes to be effective.

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



Server Stopped.



Server Started.

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

Link Cameras on trk-101-P Tracker

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

Step 1 Ensure that the F-Series ID Analytics have been calibrated (refer to Analytics Calibration, pg. 39).

Step 2 With the F-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 F-Series ID scene.

This process is only outlined here. Refer to the *FLIR ioi HTML Edition Units User Guide* which can be downloaded from the ioi documents section of the product web page at: https://www.flir.com/products/ioi-ptz-tracker/.

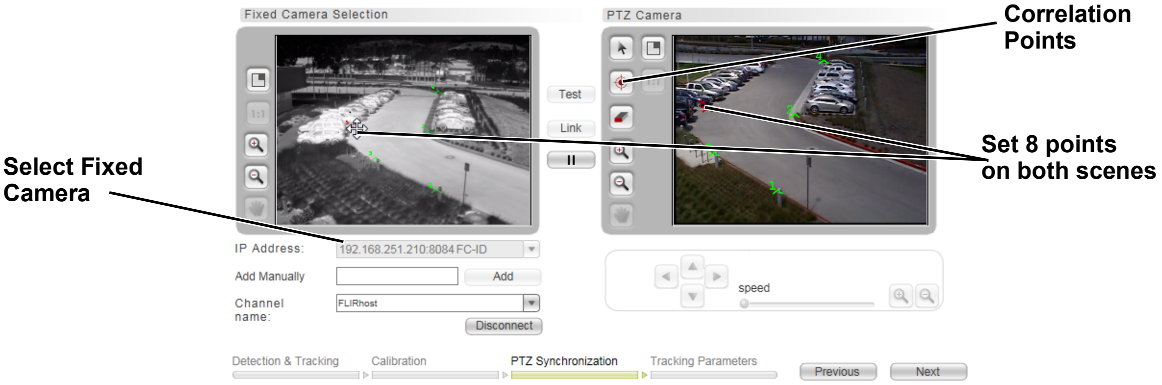
Step 3 Ensure that the F-Series ID detection regions are setup to correspond to the presets on the trk-101-P (refer to Creating Analytics Regions, pg. 42).

Step 4 Login to the trk-101-P web interface.

Step 5 Verify that the trk-101-P is bound to a PTZ camera.

Step 6 Setup the trk-101-P for *Detection from another camera with Automatic PTZ tracking*.

Step 7 Follow the procedure described in the *FLIR ioi HTML Edition Units User Guide* to synchronize the F-Series ID to the PTZ camera.



IP Address: 192.168.251.210:8084 FC-ID

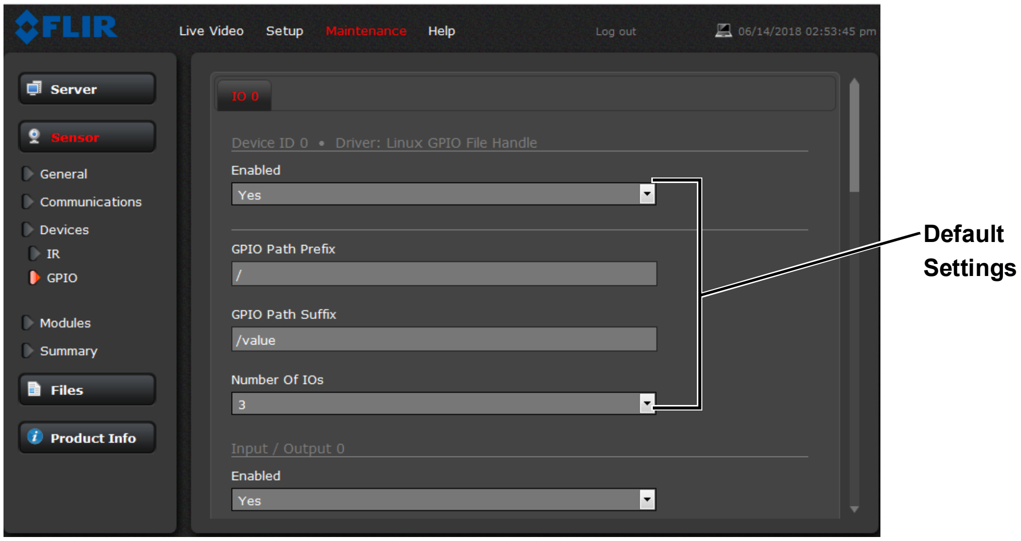
Add Manually

Channel name: FLIRhost

Step 8 When finished, return to the F-Series ID and enable Video Analytics.

Devices Menu GPIO

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



Device ID 0 • Driver: Linux GPIO File Handle

Enabled: Yes

GPIO Path Prefix: /

GPIO Path Suffix: /value

Number Of IOs: 3

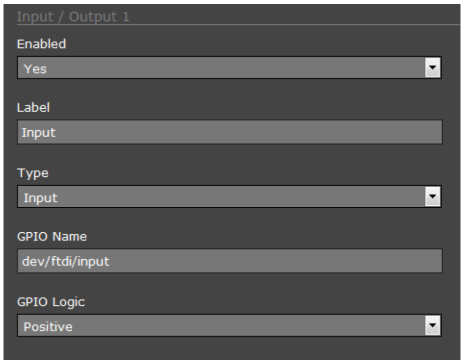
Input / Output 0

Enabled: Yes

The GPIO must be wired during installation, refer to GPIO Alarm Connections, pg. 12. The status of the GPIO signals are displayed on the IO page from the Setup menu, refer to Input/Output (IO) Page, pg. 34.

Input/Output 0 is a control signal for the camera heater circuits. The **Heater_GPIO44** output signal performs internal functions and should not be changed.

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


Input / Output 1

Enabled: Yes

Label: Input

Type: Input

GPIO Name: dev/ftdi/input

GPIO Logic: Positive

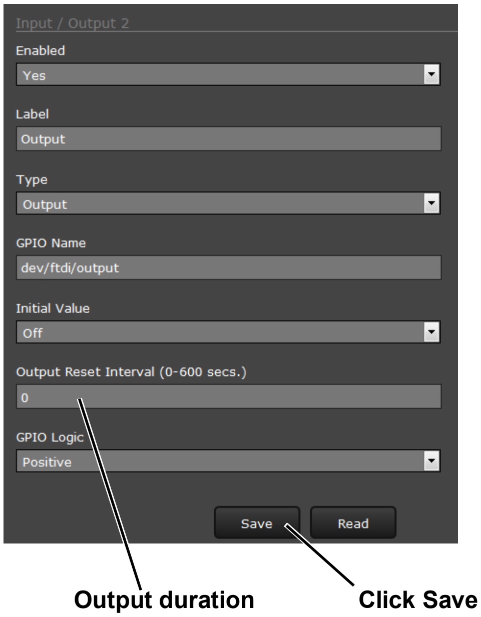
- The Label setting can be changed to reflect more specific alarm information which can then appear in VMS systems such as FLIR Latitude.
- The **GPIO Name** determines the circuit point for the GPIO driver and must not be changed.

Type: Input

GPIO Name: dev/ftdi/input

- Set **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).

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


Input / Output 2

Enabled: Yes

Label: Output

Type: Output

GPIO Name: dev/ftdi/output

Initial Value: Off

Output Reset Interval (0-600 secs.): 0

GPIO Logic: Positive

- 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.

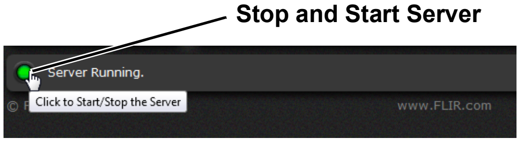
Type: Output

GPIO Name: dev/ftdi/output

Initial Value: Off

- 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. 56.
- 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).

Scroll to the bottom of the page and click on the **Save** button to save changed settings. Changes will not take effect until the server is stopped and started.


Server Running.

Refer to the Alarm Manager, pg. 52 for a description of how to combine the GPIO inputs and outputs with other alarms. For example, the camera can send the output alarm when there is a Video Analytics alarm. Similarly, the camera can save an image snapshot when there is an input.

Modules Menu

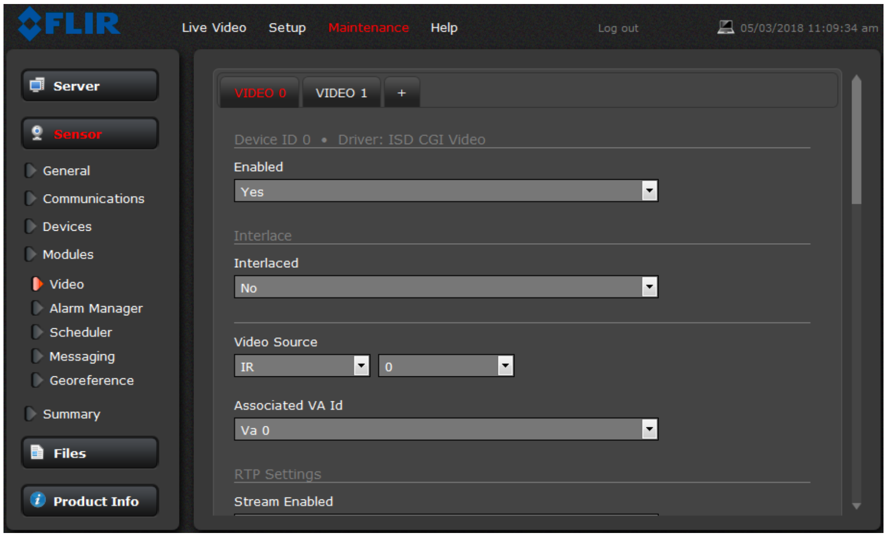
This section describes the Video page and Alarm Manager page. Use the Alarm Manager page to define rules for camera alarms from Video Analytics.

Video: By default, two video streams are enabled for the camera: Video 0 and Video 1. The 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.

Caution!

> Adjustments to these settings should only be made by someone trained with thermal cameras and a thorough understanding of how the various settings affect the image.
> Haphazard changes can lead to image problems including a complete loss of video.

To modify parameters that affect a particular IP Video stream from the camera, select the appropriate link at the top of the page (for example, **Video 0**).



Device ID 0 • Driver: ISD CGI Video

Enabled: Yes

Interlace

Interlaced: No

Video Source: IR 0

Associated VA Id: Va 0

RTP Settings

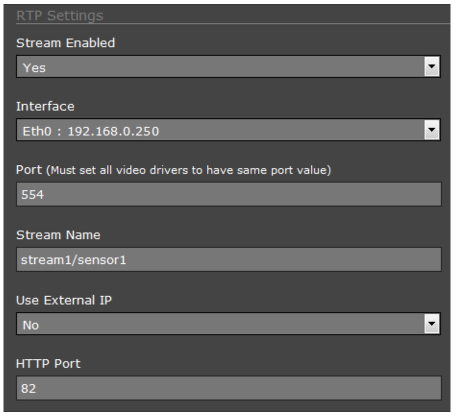
Stream Enabled

RTP Settings for connecting to an IP video stream from the F-Series ID are shown in the illustration below. The RTP Port and the Stream Name are used when establishing a session from a client.

Given the camera IP address of 192.168.0.250, the complete connection string for each of the video streams is as follows:
VIDEO 0 - rtsp://192.168.0.250:554/stream1/sensor1
VIDEO 1 - rtsp://192.168.0.250:554/stream2/sensor1

To maintain compatibility with legacy systems the stream names are aliased as: ch0 = stream1/sensor1 and ch1 = stream2/sensor1.

In some networks, the RTP/RTSP traffic is carried (tunneled) over Hypertext Transfer Protocol (HTTP) as that may allow the traffic to cross network boundaries and firewalls. While this method involves more overhead due to encapsulation, it may be necessary for clients to access the video streams when HTTP proxies are used.



RTP Settings

Stream Enabled: Yes

Interface: Eth0 : 192.168.0.250

Port (Must set all video drivers to have same port value): 554

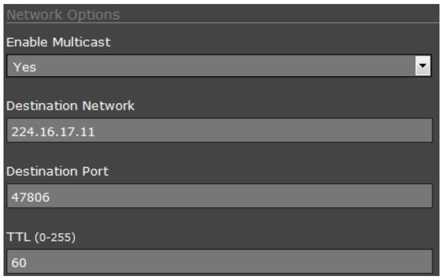
Stream Name: stream1/sensor1

Use External IP: No

HTTP Port: 82

By default, the video streams from the camera are sent using multicast packets. With Multicast enabled, video packets are shared by streaming clients, so additional clients do not cause bandwidth to increase as dramatically.

If more than one camera is providing multicast streams on the network, be sure to configure each stream with a unique multicast Destination Network IP address and Destination Port combination.



Network Options

Enable Multicast: Yes

Destination Network: 224.16.17.11

Destination Port: 47806

TTL (0-255): 60

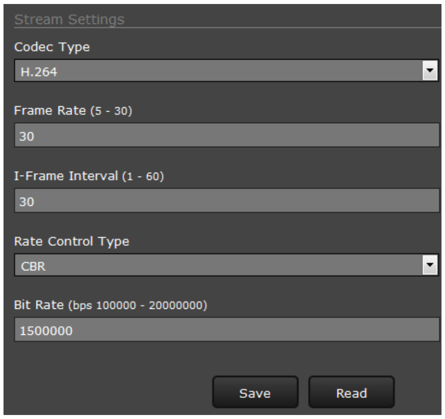
The time-to-live field controls the ability of IP packets to traverse network boundaries. A value of 1 restricts the stream to the same subnet. Greater values allow increasing access between networks.

The video streaming 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). In the background, a “negotiation” takes place to establish a session between the client (such as FLIR Latitude, a third party VMS, or video player) and the camera. The ports which form a session are negotiated using a protocol such as RTSP. A client typically requests a video stream using its preferred settings, and the camera can respond with its preferred settings. As a result, many of the details are established dynamically, which may run contrary to network security requirements.

The parameters in the Stream Settings section will have a significant impact on the quality and bandwidth requirements of the video stream. In general it is recommended that the default values be used initially, and then individual parameters can be modified and tested incrementally to determine if the bandwidth and quality requirements are met.

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

The Bit Rate parameter is used with the CBR (Constant Bit Rate) setting to attempt to keep the resulting bit rate of the video at or near the target bit rate.



Stream Settings

Codec Type: H.264

Frame Rate (5 - 30): 30

I-Frame Interval (1 - 60): 30

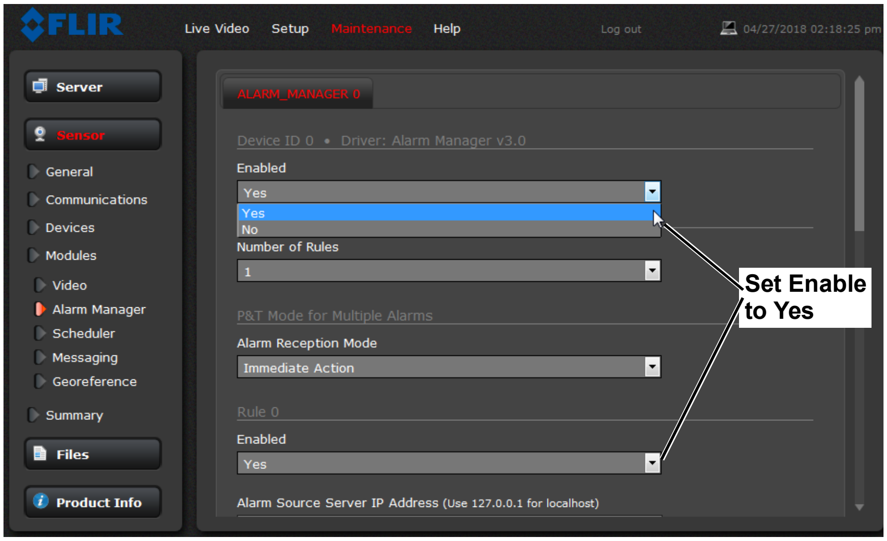
Rate Control Type: CBR

Bit Rate (bps 100000 - 20000000): 1500000

When the Rate Control parameter is set to VBR (Variable Bit Rate), the Bit Rate parameter is used as an upper limit bit rate and the system keeps the stream at or under the target bit rate.

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 lower bandwidth and possibly lower quality.

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 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 > Notification Lists, pg. 24).



Device ID 0 • Driver: Alarm Manager v3.0

Enabled: Yes

Number of Rules: 1

P&T Mode for Multiple Alarms

Alarm Reception Mode: Immediate Action

Rule 0

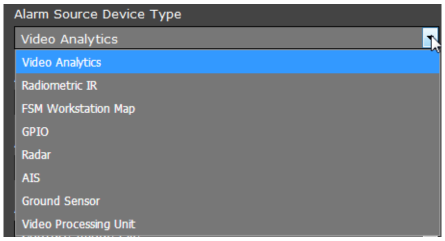
Enabled: Yes

Alarm Source Server IP Address (Use 127.0.0.1 for localhost)

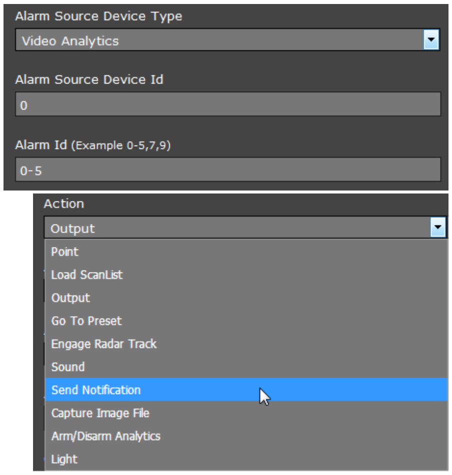
In general, each Alarm Rule describes a single alarm **Source** and a single alarm **Action**. For the F-Series ID camera, the source of the alarm typically will be internal from the video analytics, although it is also possible for the camera to receive alarms from another camera or device/server on 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, 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 F-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.



Alarm Source Device Type: Video Analytics



Alarm Source Device Type
Video Analytics

Alarm Source Device Id
0

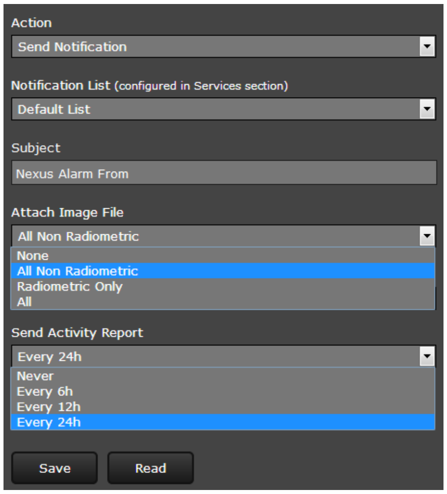
Alarm Id (Example 0-5,7,9)
0-5

Action
Output

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, pg. 38.

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 F-Series ID fixed camera.

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



Action
Send Notification

Notification List (configured in Services section)
Default List

Subject
Nexus Alarm From

Attach Image File
All Non Radiometric

Send Activity Report
Every 24h

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 > Msg Systems, pg. 24).

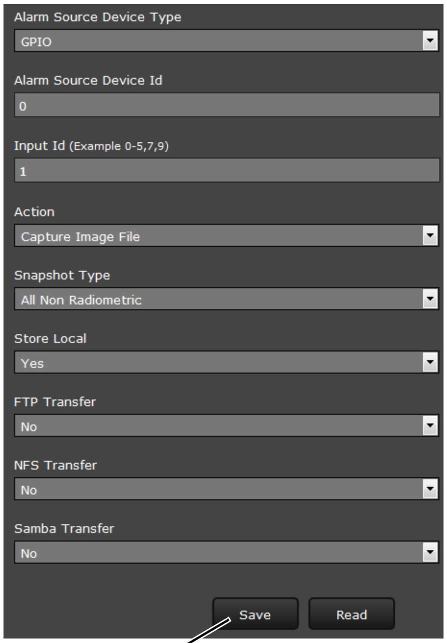
To attach a snapshot, select the option **All Non Radiometric** to send a normal JPEG image from the **Attach Image File** pull down list. **Radiometric** (a special type of JPEG with temperature data) is not available on the F-Series ID camera.

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 (Store Local), over the camera network using FTP (file transfer protocol) or to a network-attached storage device (NAS). Refer to File Transfer, pg. 45 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 F-Series ID camera.

Scroll to the bottom of the page and click on the **Save** button to save settings. Changes will not take effect until the server is stopped and started.



Alarm Source Device Type: GPIO

Alarm Source Device Id: 0

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

Action: Capture Image File

Snapshot Type: All Non Radiometric

Store Local: Yes

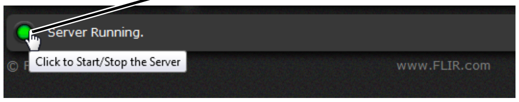
FTP Transfer: No

NFS Transfer: No

Samba Transfer: No

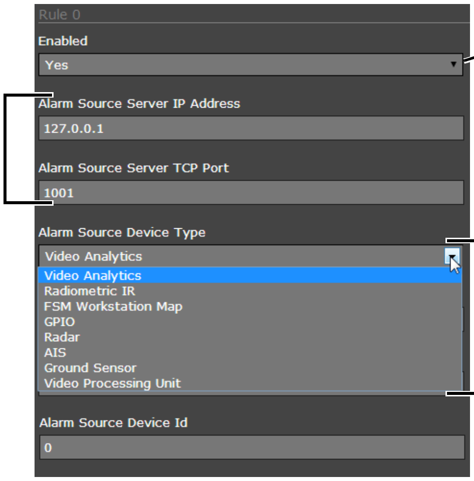
Click Save

Stop and Start Server



Server Running.

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 is always the same for the alarms coming from the F-Series ID camera itself.



Rule 0

Enabled: Yes

Alarm Source Server IP Address: 127.0.0.1

Alarm Source Server TCP Port: 1001

Alarm Source Device Type: Video Analytics

Alarm Source Device Id: 0

Enable each alarm rule

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

F-Series ID Options: Video Analytic

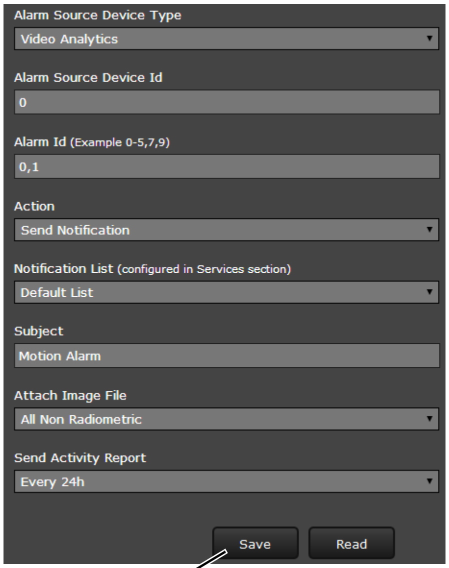
This document does not contain any export-controlled information.

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. 42).

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 > Msg Systems, pg. 24). 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.

After making any changes you must scroll to the bottom of the page and click on the **Save** button to save settings. Changes will not take effect until the server is stopped and started.



Alarm Source Device Type
Video Analytics

Alarm Source Device Id
0

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

Action
Send Notification

Notification List (configured in Services section)
Default List

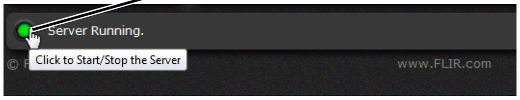
Subject
Motion Alarm

Attach Image File
All Non Radiometric

Send Activity Report
Every 24h

Click Save

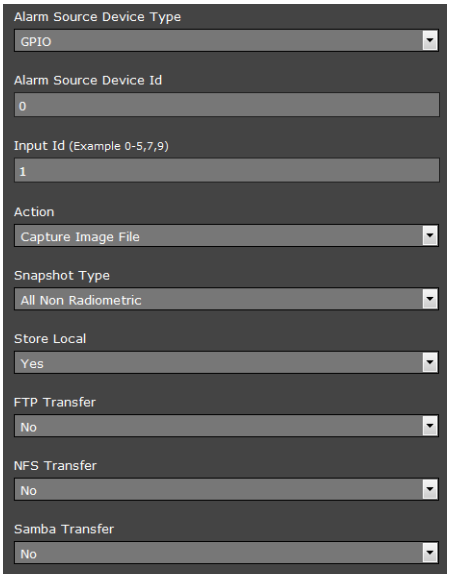
Stop and Start Server



Server Running.

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. 48), 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. 45 to configure settings for the FTP, NFS, or Samba transfers.



Alarm Source Device Type
GPIO

Alarm Source Device Id
0

Input Id (Example 0-5,7,9)
1

Action
Capture Image File

Snapshot Type
All Non Radiometric

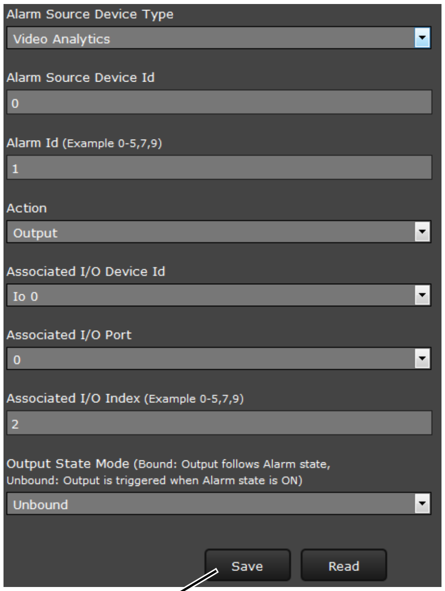
Store Local
Yes

FTP Transfer
No

NFS Transfer
No

Samba Transfer
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.



Alarm Source Device Type: Video Analytics

Alarm Source Device Id: 0

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

Action: Output

Associated I/O Device Id: Io 0

Associated I/O Port: 0

Associated I/O Index (Example 0-5,7,9): 2

Output State Mode (Bound: Output follows Alarm state, Unbound: Output is triggered when Alarm state is ON): Unbound

Click Save

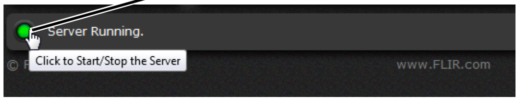
Note: the Associated I/O Port is set to 0, and the Associated I/O Index is set to 2 (corresponding to Input/Output 2).

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. 48).

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

After making any changes you must scroll to the bottom of the page and click on the **Save** button to save settings. Changes will not take effect until the server is stopped and started.

Stop and Start Server

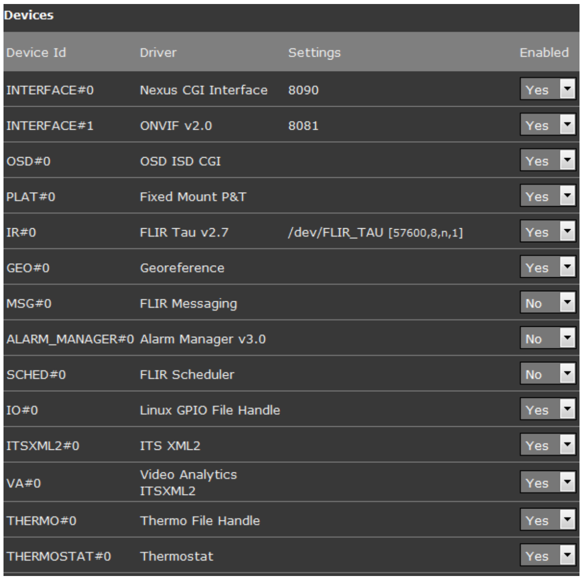


Server Running.

Maintenance > Sensor > Summary Page

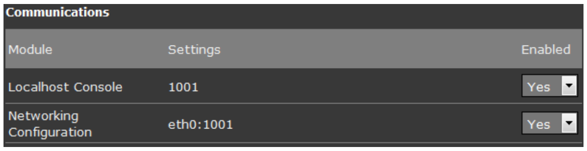
The **Summary** page provides a list of the Devices, Communications modules, and Video drivers installed on the system. The status (enabled or not) of each, the specific driver, and settings for items are listed as appropriate.

Items can be enabled or disabled from this page, but generally additional setup is required. For more information on setting or changing these camera parameters contact the local FLIR representative or FLIR Technical Support.



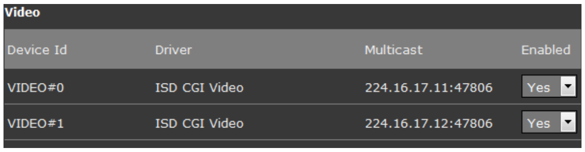
Devices

Device Id	Driver	Settings	Enabled
INTERFACE#0	Nexus CGI Interface	8090	Yes
INTERFACE#1	ONVIF v2.0	8081	Yes
OSD#0	OSD ISD CGI		Yes
PLAT#0	Fixed Mount P&T		Yes
IR#0	FLIR Tau v2.7	/dev/FLIR_TAU [57600,8,n,1]	Yes
GEO#0	Georeference		Yes
MSG#0	FLIR Messaging		No
ALARM_MANAGER#0	Alarm Manager v3.0		No
SCHED#0	FLIR Scheduler		No
IO#0	Linux GPIO File Handle		Yes
ITSXML2#0	ITS XML2		Yes
VA#0	Video Analytics ITSXML2		Yes
THERMO#0	Thermo File Handle		Yes
THERMOSTAT#0	Thermostat		Yes



Communications

Module	Settings	Enabled
Localhost Console	1001	Yes
Networking Configuration	eth0:1001	Yes

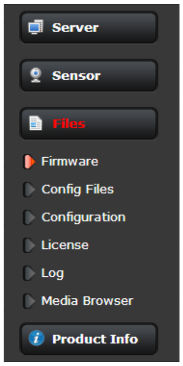


Video

Device Id	Driver	Multicast	Enabled
VIDEO#0	ISD CGI Video	224.16.17.11:47806	Yes
VIDEO#1	ISD CGI Video	224.16.17.12:47806	Yes

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.



Firmware Page

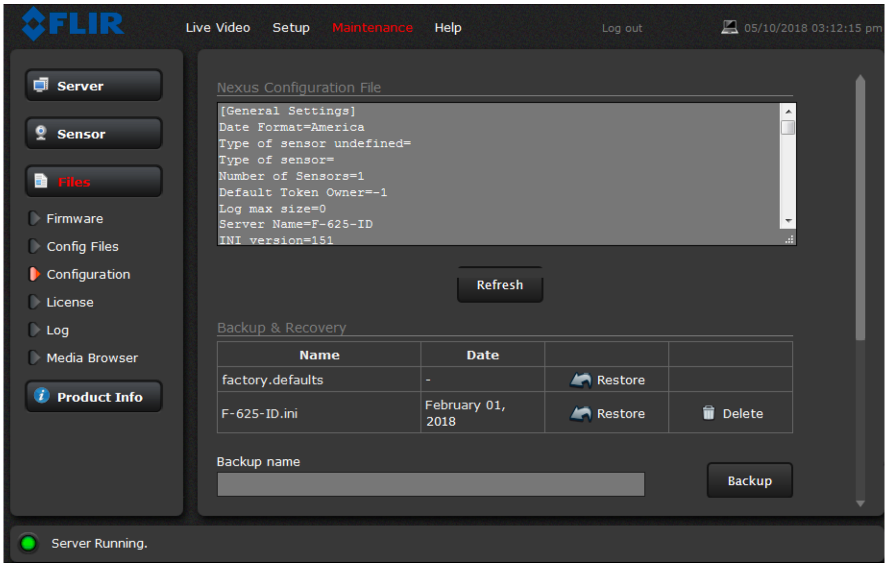
For camera firmware updates, manually install a firmware update file by first stopping the camera server, browsing to select the update file on your computer, and then selecting Upload. The firmware files will be uploaded and installed.

Caution!

Before updating camera firmware, detach the camera from any VMS.

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 a computer for backup, or to install a new configuration file to the camera.



```
[General Settings]
Date Format=America
Type of sensor undefined=
Type of sensor=
Number of Sensors=1
Default Token Owner=-1
Log max size=0
Server Name=F-625-ID
INI version=151
```

Name	Date		
factory.defaults	-	Restore	
F-625-ID.ini	February 01, 2018	Restore	Delete

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

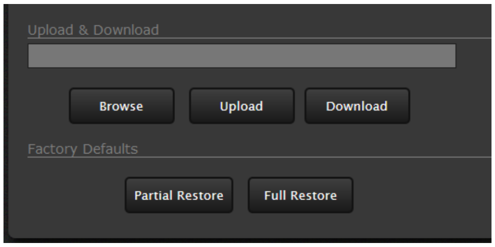
In the Backup & Recovery section, click the Restore link associated with the factory.defaults configuration to restore the camera to its factory settings. This file can not be modified or deleted, so it is always available.

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.

Upload & Download

The **Download** button is used to save a copy of the current server.ini file 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.



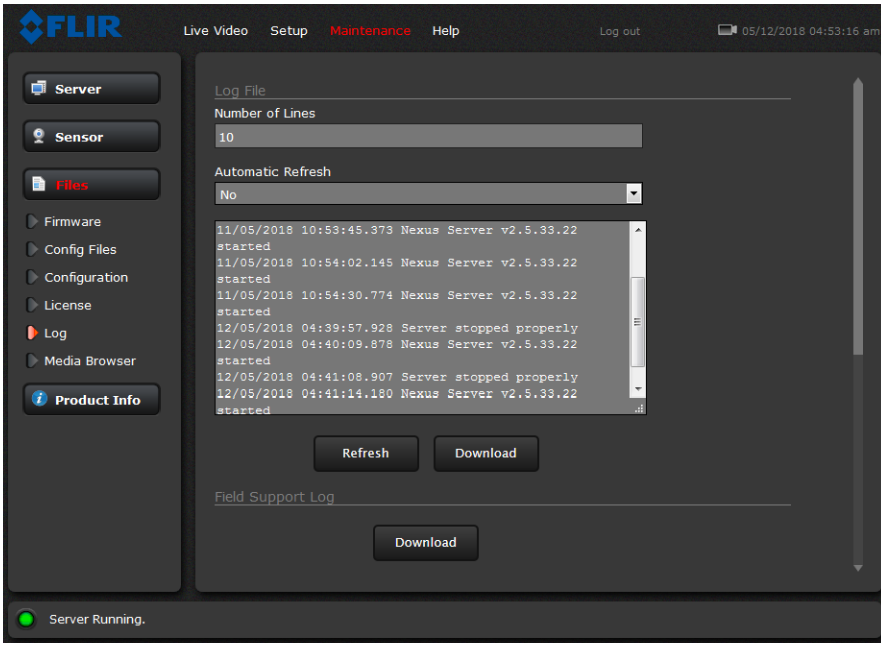
Factory Defaults

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.

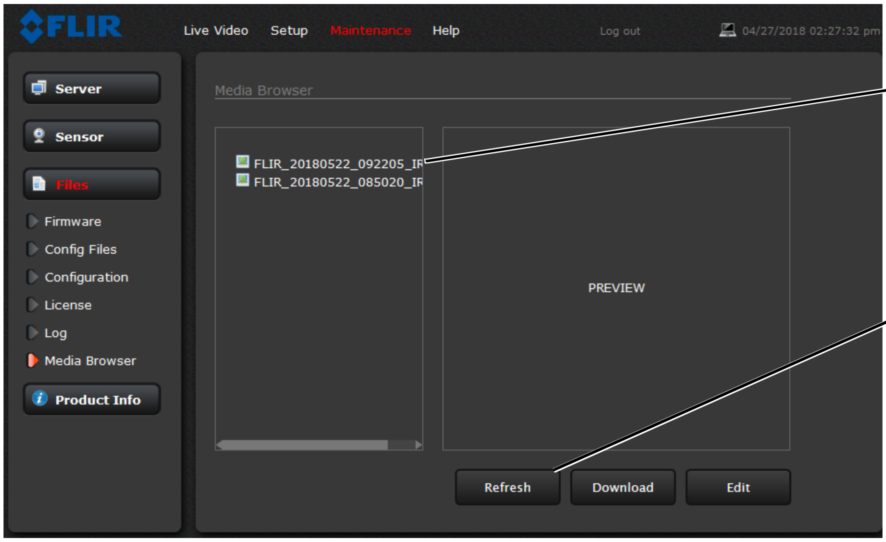


Number of Lines: 10

Automatic Refresh: No

```
11/05/2018 10:53:45.373 Nexus Server v2.5.33.22
started
11/05/2018 10:54:02.145 Nexus Server v2.5.33.22
started
11/05/2018 10:54:30.774 Nexus Server v2.5.33.22
started
12/05/2018 04:39:57.928 Server stopped properly
12/05/2018 04:40:09.878 Nexus Server v2.5.33.22
started
12/05/2018 04:41:08.907 Server stopped properly
12/05/2018 04:41:14.180 Nexus Server v2.5.33.22
started
```

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.



FLIR_20180522_092205_IR
FLIR_20180522_085020_IR

Select to preview

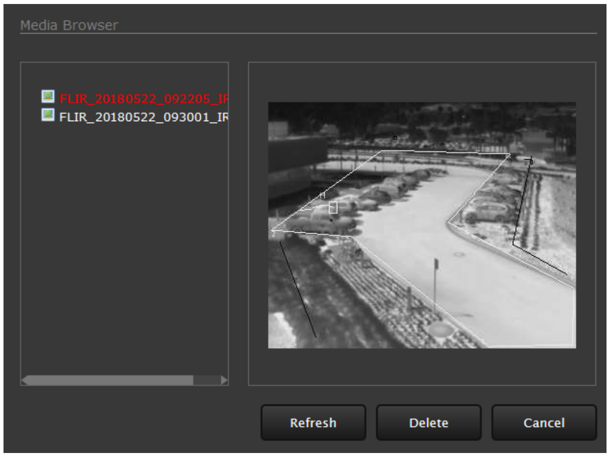
Select to Refresh

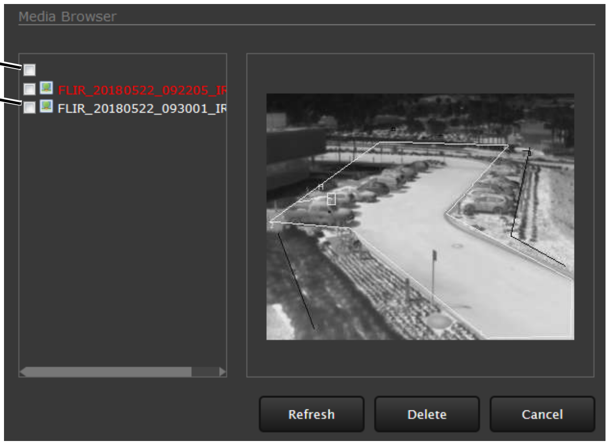
After selecting a file, the file will appear in the Preview window.

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

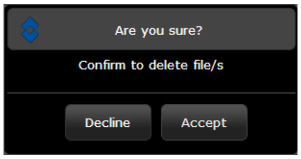
Select Edit to select and delete individual images or all images. Any time the camera is rebooted or the power removed, the media directory will be emptied.





Select all media files by clicking the Select All check box.

The following prompt will appear prior to deleting any files.

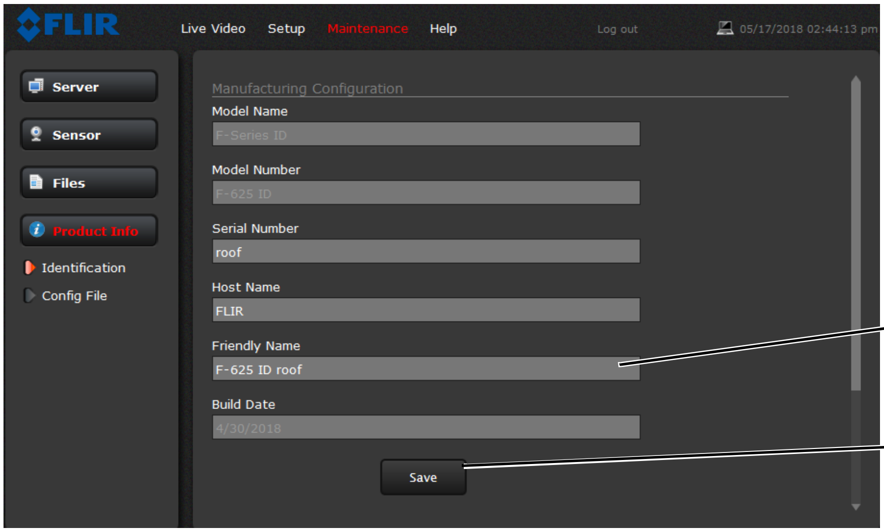

Are you sure?

Confirm to delete file/s

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



Manufacturing Configuration

Model Name: F-Series ID

Model Number: F-625 ID

Serial Number: roof

Host Name: FLIR

Friendly Name: F-625 ID roof

Build Date: 4/30/2018

Enter Name

Click Save

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-center/support-hq/

Document:
427-0033-00-12
Version: 110
Date: February 2019

This document does not contain any export-controlled information.