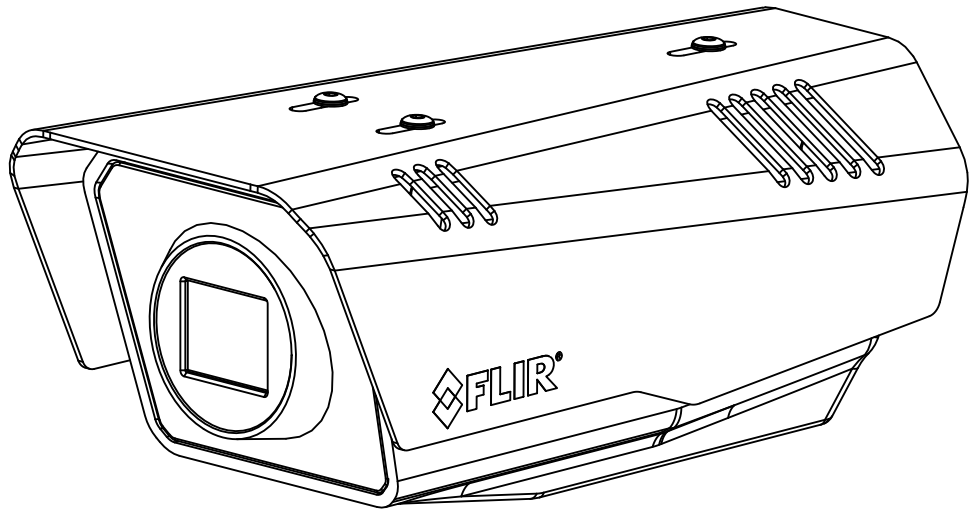




Installation Manual

FC-Series ID



© 2017 FLIR Systems, Inc. All rights reserved worldwide. No parts of this manual, in whole or in part, may be copied, photocopied, translated, or transmitted to any electronic medium or machine readable form without the prior written permission of FLIR Systems, Inc.

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

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

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: <http://www.flir.com/security/display/?id=71083>.

Important Instructions and Notices to the User:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modification of this device without the express authorization of FLIR Systems, Inc. may void the user's authority under FCC rules to operate this device.

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

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

Industry Canada Notice:

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

Avis d'Industrie Canada:

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

Proper Disposal of Electrical and Electronic Equipment (EEE)



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

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

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

Document History

Version	Date	Comment
100	July 2016	Initial Release
110	August 2016	User Interface Updates
120	January 2017	Setup Temperature/GPIO User Interface Update
130	March 2017	Added support for IEEE 802.1x authentication, Field Service log download, and IOI analytics interface

Table of Contents

Camera Installation

1.1 Warnings and Cautions	5
1.2 References	5
1.3 Installation Overview	6
1.3.1 Camera Connection Options	6
1.3.2 Camera Accessories	8
1.3.3 Supplied Components	8
1.3.4 Additional Supplies	8
1.3.5 Camera Mounting for Rear Cable Access	9
1.3.6 Camera Mounting with Concealed Cable Wall Mount	10
1.3.7 Sunshield	11
1.3.8 Removing the Cover	11
1.4 Camera Connections	12
1.4.1 Installing the microSD Card	13
1.4.2 Bench Testing	13
1.4.3 Analog Video Connections	13
1.4.4 Connecting Power	13
1.4.5 GPIO Connections	14
1.4.6 Ethernet	15
1.4.7 Camera Grounding	15
1.4.8 Rear Access Cable Gland Sealing	16
1.5 Concealed Cable Mount Accessory	17
1.6 Camera specifications	19

Basic Operation and Configuration

2.1 IP Camera, ONVIF Profile S Compliant	21
2.2 Set IP Address using the FLIR Discovery Network Assistant (DNA)	22
2.3 Camera Bench Test	23
2.3.1 Log in to the Camera Web Page	23
2.3.2 Live Video Page	24
2.4 Basic Camera Configuration	27
2.4.1 Setup Menu	27
2.4.2 Server Menu	27
2.5 Thermal Imaging Overview	35
2.6 Maintenance and Troubleshooting Tips	36

Advanced Configuration

3.1 Setup Menu	40
3.1.1 Temperature Page	41
3.1.2 Video Setup	42
3.1.3 Thermal Image Setup	45
3.1.4 Video Analytics Setup	48
3.2 Maintenance Menu	52
3.2.1 Sensor Menu	52
3.2.2 Files Menu	64
3.2.3 Product Info Menu	67



Image from a standard camera in low light



Image from a thermal camera in the same conditions

This manual describes the installation and initial configuration of the FC-Series ID thermal camera. If help is needed during the installation process, contact the local FLIR service representative or call the appropriate support number listed at: <http://www.flir.com/security/display/?id=71083>.

All installers and integrators are encouraged to take advantage of the training offered by FLIR; visit <http://www.flir.com/training> for more information.

This manual includes the following topics:

- Installation overview
- Mounting the camera and its components
- Connecting the electronics
- Bench testing the camera
- Basic configuration and operation of the camera
- Camera Specifications

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

1.1 Warnings and Cautions

Warning!



If mounting the FC-Series 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 FC-Series ID camera for any reason. Damage to the camera can occur as the result of careless handling or electrostatic discharge (ESD). Always handle the camera with care to avoid damage to electrostatic-sensitive components.

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

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

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

1.2 References

FLIR Doc # 427-00XX-YY-41 FC-Series ID Interconnect Document provides further details regarding mechanical dimensions and mounting for the FC-Series ID camera.

FLIR Doc # 427-0030-00-28 *Nexus IP Camera Configuration Guide*, provides more information on setting or changing camera parameters.

These documents are available from the FLIR website.

1.3 Installation Overview

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

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



1.3.1 Camera Connection Options

The FC-Series ID camera can be installed with an analog or digital (IP) video output (or both). Analog video will require a connection to a video monitor or an analog video matrix switch. The camera can be powered using Power over Ethernet Plus (PoE+) or with a conventional 24 Vac or 24 Vdc power supply. For a PoE+ connection, an accessory PoE+ power supply (PN 4132391, also called a PoE+ injector) is available if the camera is not connected to a PoE+ switch. The maximum Ethernet cable run is 100 meters including the PoE+ power supply. In installations using PoE+ power and IP video, only a single Ethernet cable from the camera is required.

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

Network Security

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

- Network device (Authenticator) such as an Ethernet switch configured with 802.1x
- Authentication server supporting either TLS or PEAP (MSCHAPv2)

Refer to [IEEE 802.1X Security, pg. 29](#) for information on how to configure the LAN settings.

General Purpose Input/Output (GPIO)

The camera can receive a single input signal and can provide a single output signal. By default the signals are configured for normally open alarm switch circuits. Refer to [GPIO Connections, pg. 14](#).

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.

PoE+ Power Supplies

With PoE+, camera power is delivered to the camera over the Ethernet cable via the camera's standard RJ-45 Ethernet connector. The FC-Series ID camera is a Powered Device compliant with the IEEE 802.3at-2009 standard, known as PoE+ or PoE Plus. The FC-Series ID camera is also backward compatible with the older IEEE 802.3af-2003 standard.

When connected to Power Sourcing Equipment compliant with the earlier, lower power IEEE 802.3af-2003 standard, the limited power available to the FC-Series ID will typically prevent the formation of frost and ice. However, the limited power available from 802.3af-2003 may not fully achieve the camera's stated specification of de-icing 6 mm of ice from cold start. In all other ways the camera will operate normally with Ethernet Powered Sourcing Equipment compliant to either IEEE PoE standard.

Supplemental Lens Heater

The supplemental lens heater is intended to provide lens de-fogging and de-icing in the event of:

- A power interruption which disables the camera for an extended period, and
- Freezing rain which fully covers the lens and obstructs the image.

The FC-Series ID cameras with lens windows (13 mm, 19 mm, 35 mm) are shipped from the factory with the supplemental lens heater on. The lens heater is configured to dynamically maintain the camera window at a constant temperature.

The lens heater may be turned on manually from the Live Video web page (De-Ice button). Refer to [Web Control Panel, pg. 25](#). The heater, when turned on manually, will run for approximately 2 hours unless turned off either by the user (De-Ice button) or the thermostat control.

FC-Series ID cameras with a 60 mm or a 75 mm lens are shipped from the factory with the supplemental lens heater off. These cameras require the cold weather kit accessory for installations that require using the supplemental lens heater. After installing the Cold Weather kit, contact FLIR Technical Support for configuration instructions for the specific installation.

Note

The 60 mm or 75 mm lenses are not thermally conductive. The cold weather kit provides a lens cover that will conduct heat to keep the lens free of ice or frost.

Location Considerations

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

1.3.2 Camera Accessories

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

- PoE+ power supply (PN 4132391) - For powering a single FC-Series ID camera using PoE+. In addition to PoE+ power and communications, the power supply provides surge protection. It complies with IEEE 802.3at and is backward compatible with the IEEE802.3af standard.
- Concealed Cable Wall Mount (PN 4129742) - Includes camera mount gasket and hex wrench for adjusting the ball joint controlling the camera's view angle. The FC-Series ID camera is attached to the mounting arm using the four M5 threaded bottom mounting holes. A cable gland plug is supplied with the camera for the rear of the camera housing when cables are routed using the concealed cable accessory. Refer to [Camera Mounting with Concealed Cable Wall Mount, pg. 10](#).
- Pole Mount Adapter Kit (PN 4132982) - Adapter kit that allows the Concealed Cable Wall Mount to be mounted to a pole (75 mm [3 in] min to 180 mm [7 in]; larger pole diameter requires use of customer supplied band clamps)
- FC-Series ID Cold Weather Kit (PN 421-0056-00, 60 mm lens and PN 421-0057-00, 75 mm lens) The 60 mm and 75 mm lenses are not thermally conductive. The Cold Weather kit provides a lens cover that will conduct heat to keep the lens free of ice or frost while also protecting the lens in salt or other harsh environments. Refer to [Supplemental Lens Heater, pg. 7](#).



Concealed Cable Wall Mount

1.3.3 Supplied Components

The FC-Series ID camera package includes these standard components:

- Fixed Camera Unit with sun shield and installed cable gland
- Cable gland plug and gland inserts for sealing camera housing
- Power terminal block plug (installed)
- Accessory terminal block plugs (installed)
- Tools: 3 mm hex wrench (T-Handle), small blade screwdriver

1.3.4 Additional Supplies

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

- Optional customer supplied microSD card (up to 64 GB) provides local storage of image files through power cycles.
- Power supply, 18 Vac to 32 Vac or 11 Vdc to 32 Vdc, if not using PoE power for system power.
- Power cable, 3-conductor, shielded, gauge determined by cable length and supply voltage, if used for system power
- Accessory cable 6-conductor for GPIO (optional)
- PoE+ power supply or PoE+ switch, if used for system power. Note that the camera will operate normally with PoE, but lens heaters may not operate to specification in cold environments.
- Cat5e or Cat6 Ethernet cable for digital video and/or PoE+ for system power
- Coaxial RG59U cables (BNC connector at the camera end) for analog video
- Camera grounding strap, camera mount, electrical hardware, connectors, and tools

Be sure to use cables that fit in the cable gland holes, as described below. Refer to [Rear Access Cable Gland Sealing, pg. 16](#) for more information.

1.3.5 Camera Mounting for Rear Cable Access

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

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

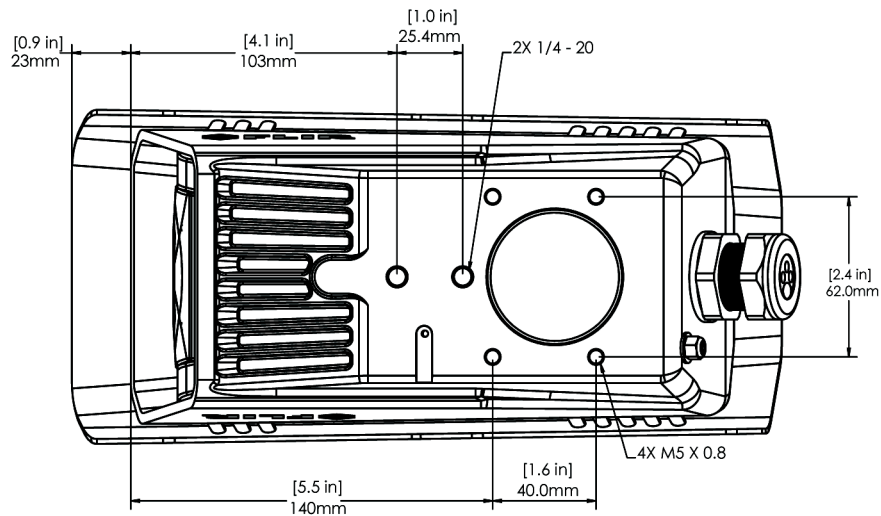


Figure 1-1: FC-Series ID Camera Bottom Mounting Holes

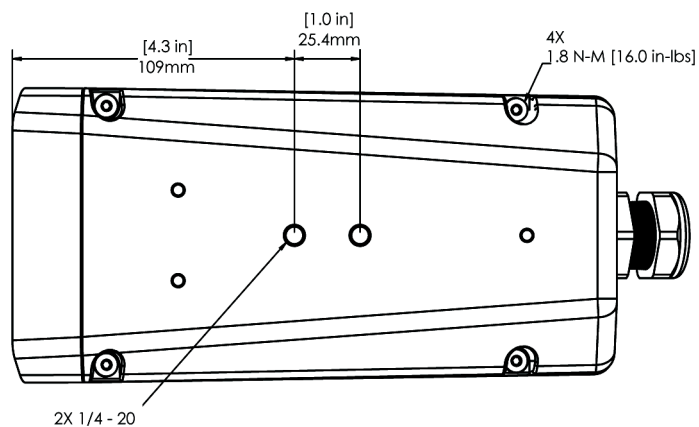


Figure 1-2: Top Mounting Holes

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

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

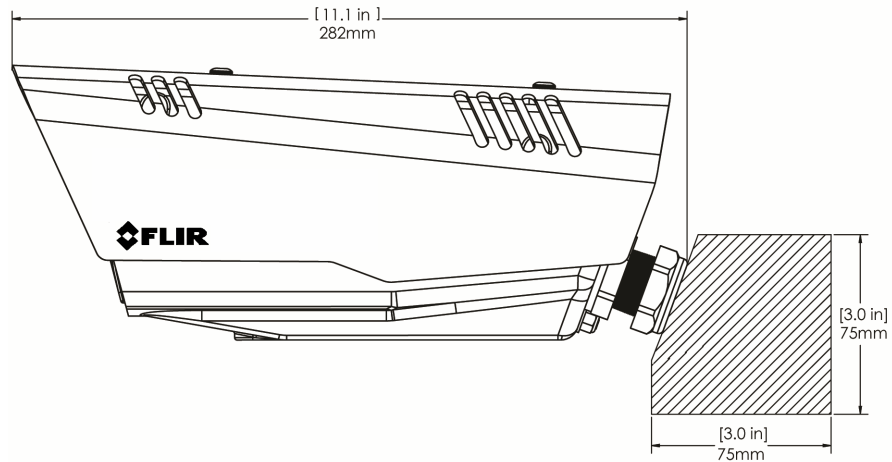


Figure 1-3: Rear Cable Bend Radius

1.3.6 Camera Mounting with Concealed Cable Wall Mount

The FC-Series ID camera can be secured to the optional Concealed Cable Wall Mount with four M5 x 0.8 threaded fasteners to the bottom of the camera. Use Loctite 222 low strength threadlocker for the mount fasteners. Refer to [Concealed Cable Mount Accessory](#), pg. 17 for additional information.

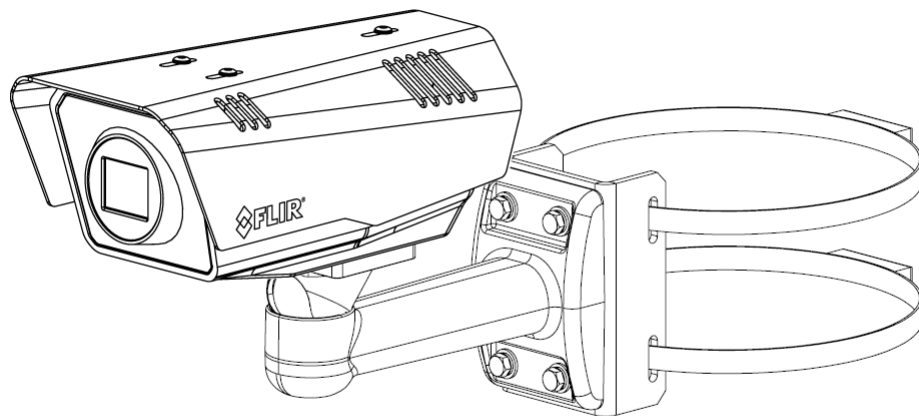


Figure 1-4: FC-Series ID Installed with Concealed Cable Wall Mount and Pole Adapter kit

1.3.7 Sunshield

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

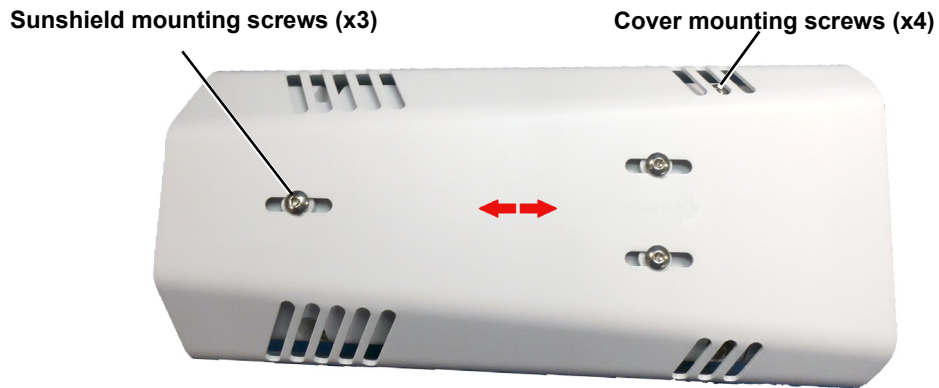


Figure 1-5: Sunshield Mounting

1.3.8 Removing the Cover

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

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

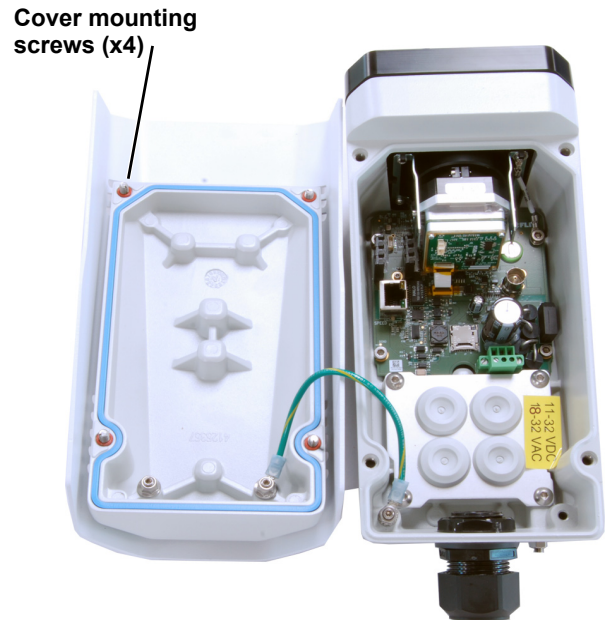


Figure 1-6: Cover Removed (Sunshield attached)

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

Caution!

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

1.4 Camera Connections

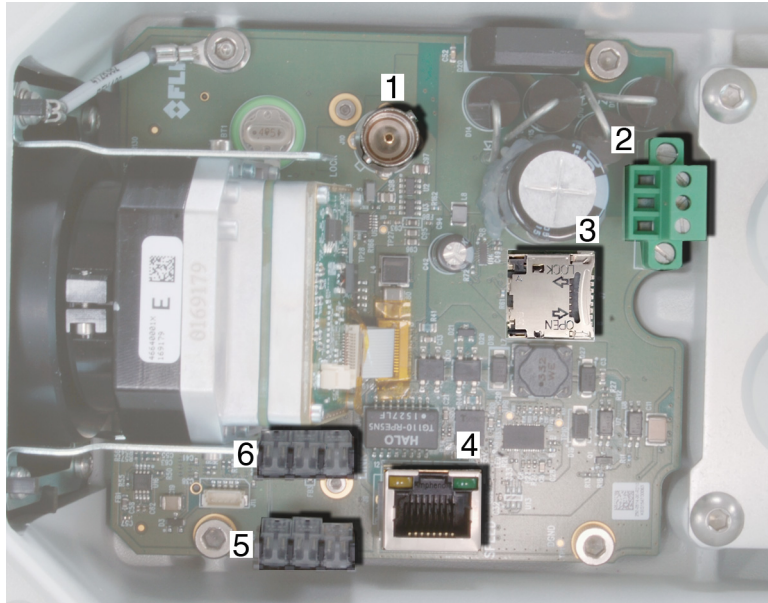


Figure 1-7: Camera Connections

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

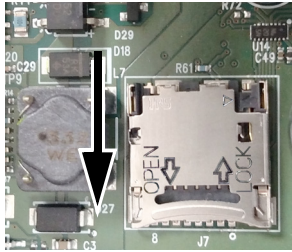
Table 1-1: FC-Series ID Camera Connections

	Connection	Purpose
1	BNC	Analog video
2	3-pin Terminal	Vac or Vdc power
3	microSD card	Local storage of image files up to 64 GB (supplied by customer)
4	Ethernet	PoE+ power, communications, IP video stream
5	6-pin terminal J5	General purpose I/O
6	Accessory inputs	Reserved for future use

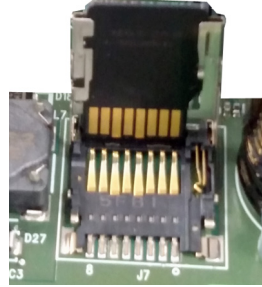
1.4.1 Installing the microSD Card

The FC-Series ID camera has local storage (on the camera) flash memory to store images captured as a result of an alarm action. However, these images are lost during a reboot or power cycle. When a customer supplied microSD card (64 GB) is installed, local storage is persistent through reboots and power cycles.

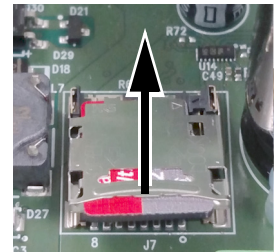
**Pull back cage to unlock
Lift edge to open**



Inset microSD card



**Close cage,
press down and
push forward to lock**



1.4.2 Bench Testing

Note

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

Connect the power, Ethernet, and video, and confirm that the video can be displayed on a monitor when the power is turned on. For configuration and basic setup information using the onboard web server, refer to [Camera Bench Test, pg. 23](#) for specific details.

1.4.3 Analog Video Connections

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

Note

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

1.4.4 Connecting Power

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

Table 1-2: Power Connections

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

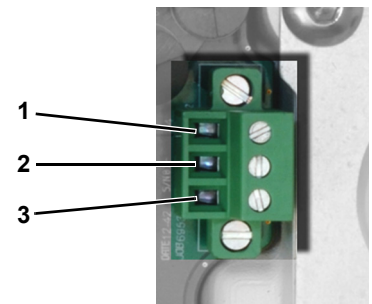
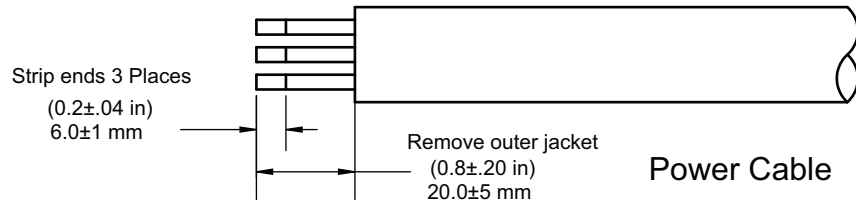


Figure 1-8: Power Connector

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



Note

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

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

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

1.4.5 GPIO Connections

Input Signal—When the camera senses an external switch closure which completes the circuit between J5 pins 4 and 5, an input signal is generated by the GPIO for the Alarm Manager. Refer to [Alarm Manager, pg. 60](#).

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

By default the GPIO alarm circuits are configured for normally open switches, to configure a GPIO alarm circuit for a normally closed switch, refer to [Devices Menu GPIO, pg. 57](#).

The terminal plug supplied for GPIO connections may be either a fast connect, spring-cage and pierce contact or a push-in spring contact.

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

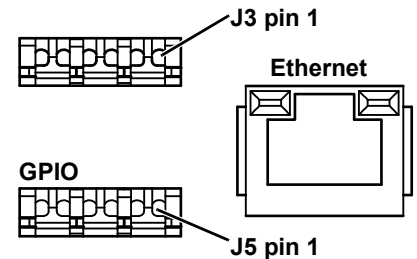
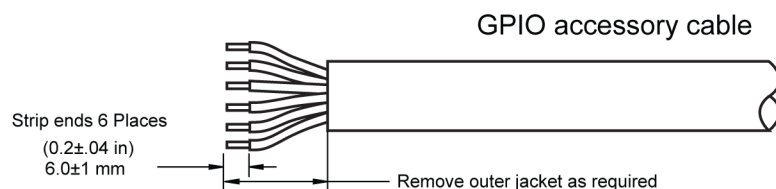


Figure 1-9: GPIO and Ethernet Connectors



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

Table 1-3: GPIO Connections - J5

Pin	Connection	Notes
1	Chassis ground	
2	GPIO Out	When the camera sends an output signal, an external voltage on one pin is applied to the other pin.
3	GPIO Out	
4	GPIO In2 (Digital ground)	When these pins are connected externally, the camera reads this as an input signal.
5	GPIO In1 (+5V)	
6	Chassis ground	

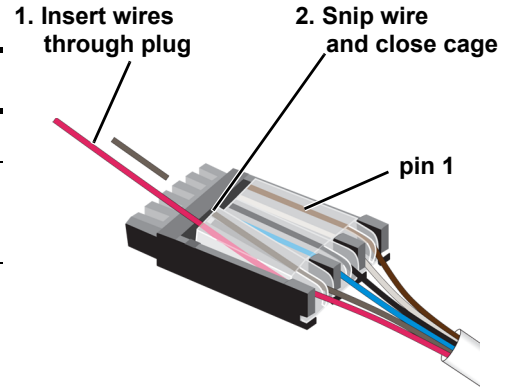


Figure 1-10: GPIO Terminal Plug

Caution!

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

1.4.6 Ethernet

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

1.4.7 Camera Grounding

Ensure the camera is properly grounded. Failure to properly ground the camera can lead to permanent damage to the camera. Typical to good grounding practices, the camera chassis ground should be connected to the lowest resistance path possible. The camera has an external ground connection on the outside back of the camera. FLIR requires a grounding strap anchored to the grounding lug and connected to the nearest earth-grounding point.

If, during installation, any ground connections inside the camera are disconnected, they should be reconnected prior to closing the camera.



Figure 1-11: Camera Ground

1.4.8 Rear Access Cable Gland Sealing

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

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

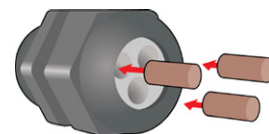
Cable	Min	Max
Power (3 conductor), Ethernet, Accessory cables	4.5 mm [0.178 in]	5.2 mm [0.205 in]
RG 59 Video cable	5.3 mm [0.209 in]	6.2 mm [0.244 in]

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

Cable Gland Seal Inserts

The FC-Series ID camera comes with a single 3/4" NPT cable gland installed in the enclosure, with a four-hole gland seal insert. The gland includes a sealing washer and is secured to the camera with a nut on the inside of the enclosure. The gland insert has one hole for the RG-59/U analog video cable (the larger hole) and three more for a power cable, Ethernet cable, and an accessory cable.

Any of the holes which are not used for cables should be filled with one of the hole plugs (supplied). Install the cables through the cable gland so that the cables line up with the connections inside the camera.



Note

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

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

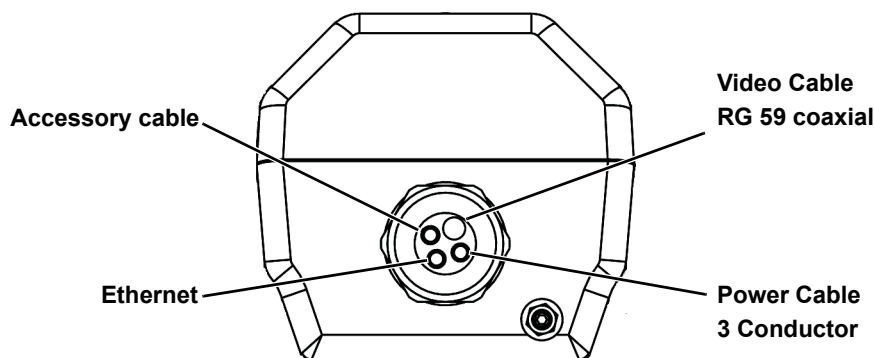


Figure 1-12: Cable Routing

1.5 Concealed Cable Mount Accessory

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

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

Cable	Min	Max
Power (3 conductor), Ethernet, Accessory cables	4.5 mm [0.178 in]	10 mm [0.394 in]
RG 59 Video cable	5.3 mm [0.209 in]	10 mm [0.394 in]

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

Prepare the Camera

- Step 1 Use a 3 mm hex key to loosen the four captive screws and remove the top cover as described above.
- Step 2 Remove the rear cable gland and replace it with the cable gland plug. Use the gasket and nut that were removed with the cable gland.
- Step 3 Use a 3 mm hex key to loosen the four captive screws and remove the seal plate, o-ring, and plug.



Figure 1-14: Removed Parts

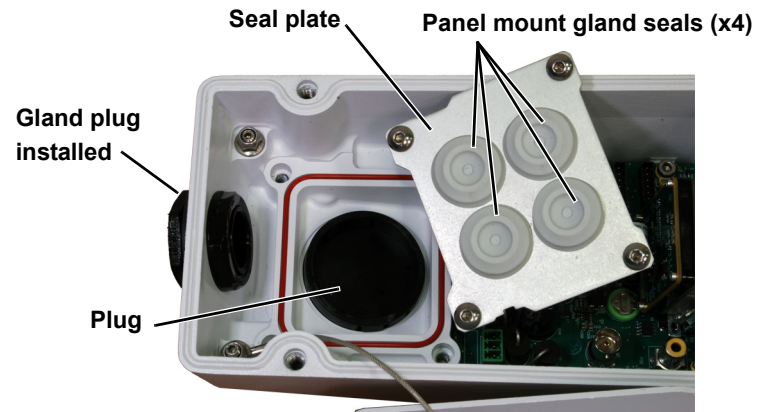


Figure 1-13: Seal Plate Removed

- Step 4 Install the wall mount (PN 4129742) to the wall and pull the cable(s) through the mount. Cut a small cross-slit in the black mount gasket and push the cable(s) through the gasket. Pull the cable(s) through the opening in the bottom of the camera. A single Ethernet cable is shown in the images.

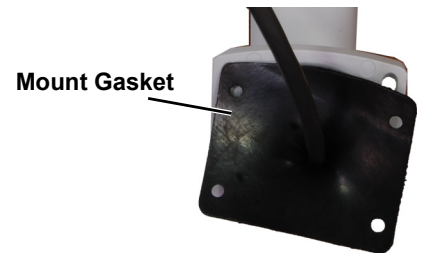


Figure 1-15: Camera Mount

- Step 5 Secure the camera to the mount using four M5 x 0.8 threaded fasteners to the bottom of the camera. Use Loctite 222 low strength thread locker for the mount fasteners.
- Step 6 As needed, clean the o-ring and the o-ring groove in the bottom of the camera using isotropy alcohol and press the o-ring into its groove.
- Step 7 For each cable, punch a hole in the center of a gland seal from the top using the 3 mm hex key. Insert the cable from the bottom through the hole.

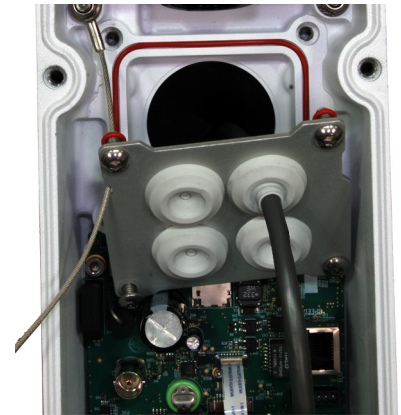
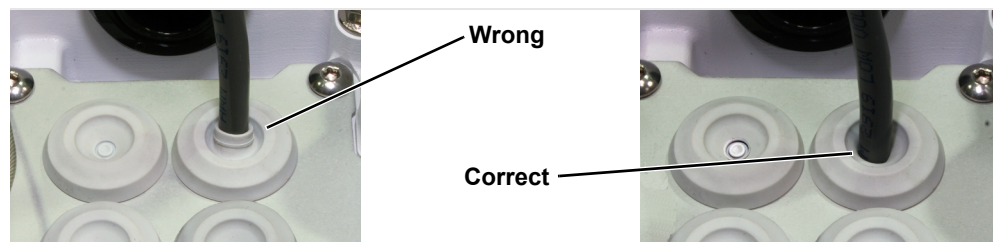


Figure 1-16: Cable through Seal Plate

- Step 8 Place the gland plate back into position and tighten the four 3 mm captive screws using a torque value of 1.8 n-m (16.0 in-lbs).
- Step 9 Check the length of each cable to ensure an appropriate bend radius and terminate the cable. Connect the cables as indicated in [Camera Connections, pg. 12](#).
- Step 10 Push the cable back through the gland seal so that the seal is extended down not up, as shown in the illustration below.



Caution!

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

- Step 11 Ensure that any ground wire that was removed during installation is reconnected. Replace the cover and tighten the four 3 mm hex screws to 1.8 n-m (16.0 in-lbs).
- Step 12 Using the hex key included with the concealed cable mount, loosen the ball joint on the bottom of the mount, position the camera as required, and then re-tighten the ball joint.

1.6 Camera specifications

Camera Model	FC-Series ID
Camera Platform Type	Fixed
Composite Video	NTSC or PAL
Thermal Camera	
Array Format	320 x 256 (34 μ m pixel pitch) 336 x 256, 640 x 512 (17 μ m pixel pitch)
Detector Type	Long-Life, Uncooled VOx Microbolometer
Effective Resolution	76,800
Field Of View (Focal Length) for available 320 x 256 and 336 x 256 camera lens configurations.	FC-344 = 44° x 36° (13 mm)—34 μ m pixel pitch FC-322 = 32° x 26° (19 mm)—34 μ m pixel pitch FC-324 = 24° x 18° (13 mm)—17 μ m pixel pitch FC-317 = 17° x 13° (19 mm)—17 μ m pixel pitch FC-309 = 9.2° x 7.0° (35 mm)—17 μ m pixel pitch FC-305 = 5.4° x 4.1° (60 mm)—17 μ m pixel pitch FC-304 = 4.3° x 3.3° (75 mm)—17 μ m pixel pitch
Field Of View (Focal Length) for available 640 x 512 camera lens configurations.	FC-690 = 90° x 69° (7.5 mm)—17 μ m pixel pitch FC-669 = 69° x 56° (9 mm)—17 μ m pixel pitch FC-644 = 44° x 36° (13 mm)—17 μ m pixel pitch FC-632 = 32° x 26° (19 mm)—17 μ m pixel pitch FC-617 = 17° x 14° (35 mm)—17 μ m pixel pitch FC-610 = 10° x 8.2° (60 mm)—17 μ m pixel pitch FC-608 = 8.6° x 6.6° (75 mm)—17 μ m pixel pitch
Spectral Range	7.5 to 13.5 μ m
Lens	Athermalized, focus-free
General	
Weight	4.65 lb (2104 g) with sun shield (13 mm, 19 mm, 35 mm) 5.25 lb (2381 g) with sun shield (60 mm) 5.41 lb (2454 g) with sun shield (75 mm)
Dimensions (L,W,H)	9.2" x 4.6" x 4.1" without sun shield, (234 mm x 117 mm x 104 mm) 11.5" x 5.1" x 4.6" with sun shield, (292 mm x 130 mm x 117 mm)
Input Voltage dc	11 Vdc to 32 Vdc
Input Voltage ac	18 Vac to 32 Vac
Input Voltage PoE+	IEEE 802.3af-2003 standard or higher power, IEEE 802.3at-2009 standard
Power Consumption	5 W nominal at 24 Vdc Peak at 24 Vdc: 23 W with lens heater 8 VA nominal at 24 Vac Peak at 24 Vac: 32 VA with lens heater

Mounting Provisions	Two 1/4-20" threaded holes on top and bottom, 1" spacing along center line front to back. Four M5 threaded holes bottom, 40 mm x 62 mm (1.6 in x 2.4 in) spacing square.
Shipping weight	6.2 lbs (2.8 kg) to 6.9 lbs (3.13 kg)
Shipping Dimensions	14.375"(L) x 7.375"(W) x 7"(H)
microSD card	Local storage of image files up to 64 GB (supplied by customer)
Environmental	
IP rating (dust and water ingress)	IP66 & IP67
Operating temperature range	-50 °C to 70 °C (-58 °F to 158 °F) continuous -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
Shock	MIL-STD-810G Method 514.6
Vibration	IEC 60068-2-27, 10g shock, 11 ms half-sine profile
Approvals	FCC Part 15, Subpart B, Class A, EN 55022 Class A, EN 55024, IEC62676-1-1 (IEC 62599-2) and CISPR 22 Class A

2 Basic Operation and Configuration

A bench test can be used to verify camera operation before the camera is configured for the local network. This chapter also provides basic configuration information.

The camera has an Ethernet connection that allows streaming video over an IP network as well as configuration and control of the camera¹. It is possible to stream video and control the camera as it is from the factory, without making any configuration changes. However in most cases the camera will have at least some configuration changes to allow it to connect with other devices or other video management systems on the existing network.

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 browser² 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 is a free download from the <http://www.flir.com/security/display/?id=73533> web page and does not require a license to use.

Getting the camera IP interface set up and working may requires familiarity with managing IP networks. Prior to configuring the IP interface and streaming video parameters, be familiar with how to manage and configure the other equipment in the network (for example, any PC or device that will connect to the camera, any router or firewall that will carry the IP traffic, and so on).

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.

There are two main components to the server software. One is a web server known as the web tool or web interface that listens on the network for web browser requests, and is used for the initial (and perhaps ongoing or occasional) configuration changes to the server. The web tool also allows the user to view video and to operate the camera.

The other process, known as the Nexus Server, listens on the network for connections from clients such as FLIR Latitude, ONVIF-compliant systems, or other VMS clients. These clients can be used to control the camera and stream video during day-to-day operations of the camera.

Server Configuration

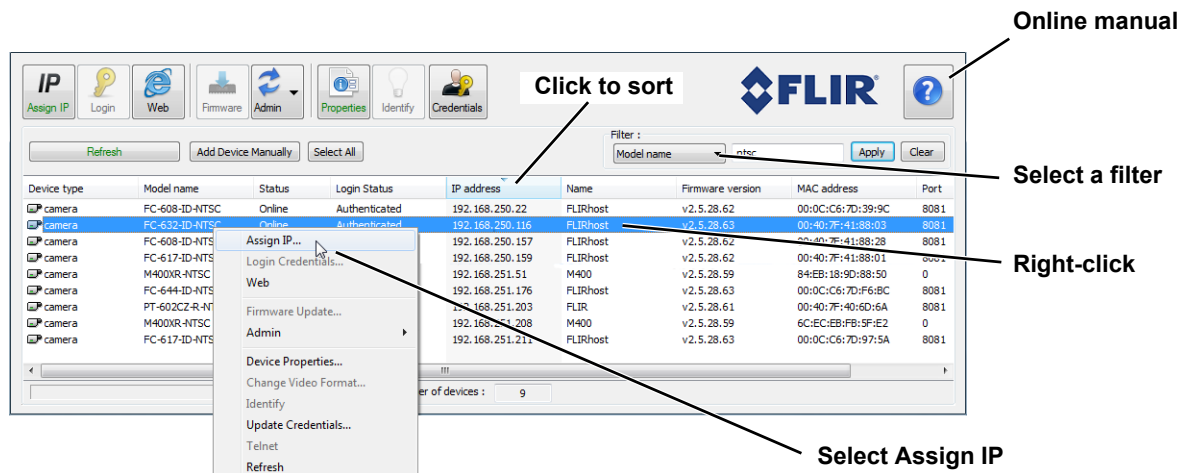
In general, it may be necessary for the installer to make a limited number of configuration changes to the camera server, such as setting the IP communication parameters. For example, each camera comes from the factory with the same default IP address, so adding more than one camera to an IP network requires each camera to be configured with a different IP address, at a minimum. On the other hand, many of the configuration parameters will remain unchanged from the factory default settings.

-
1. For this chapter, it is assumed the camera will be connected to a network via Ethernet. For installations that use only analog video output, it is not possible to make configuration changes unless an Ethernet connection is also used.
 2. The web interface is supported on the latest versions of Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox.

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

Assuming the existing network uses IP addresses that are unique and different than the default address on the camera (192.168.250.116), configuring the camera for IP communications generally involves the following steps:

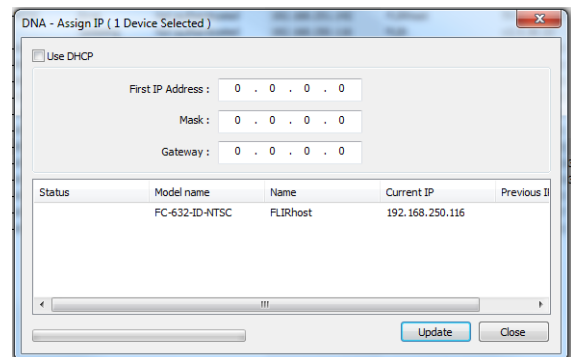
- Step 1 Connect the Ethernet port of the camera to the existing IP camera network.
- Step 2 Connect a PC or laptop to the same network.
- Step 3 From the PC connected to the camera network, use the DNA utility to discover and display the camera's current IP address.
 - a Download the DNA utility (2.1.2.7 or later) from the **FLIR Firmware & Software Downloads** page at: <http://www.flir.com/security/display/?id=73533>.
 - b Unzip the utility, then double-click to run the executable file (**DNA.exe**). All the units on the VLAN are discovered.
 - c For additional instructions on using DNA, refer to the DNA User's Manual available in the Help (?) link while the software is running.



- Step 4 Right-click on the camera, select **Assign IP** to change the IP address from the default IP (192.168.250.116) to a static IP or select DHCP.

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

- Step 6 Enter the default user name (**admin**) and password (**fliradmin**) to open the **Live Video** page. Refer to [Live Video Page](#), pg. 24.



2.3 Camera Bench Test

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

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

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

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

2.3.1 Log in to the Camera Web Page

With a web browser, log in to the camera using one of three User Names: **user**, **expert**, and **admin**. By default, the passwords are: **user**, **expert**, and **fliradmin**, respectively. The login passwords should be changed to prevent unauthorized access (refer to [Basic Camera Configuration, pg. 27](#)).

Open a web browser and enter the camera's IP address. The login screen with a picture of the camera will appear. A pull-down list in the upper right allows the user to select a language option. Enter **user** for the User Name and **user** for the Password, and click Log in.

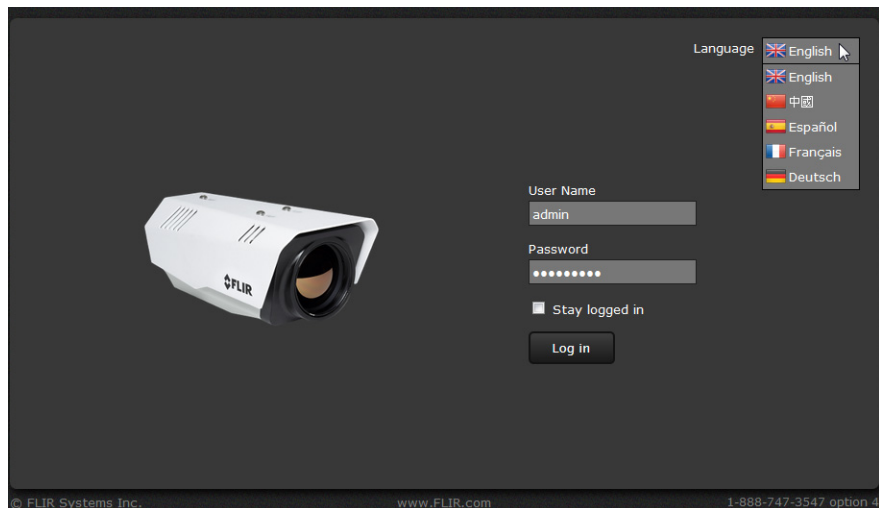


Figure 2-1: Camera Web Page Login Screen

2.3.2 Live Video Page

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

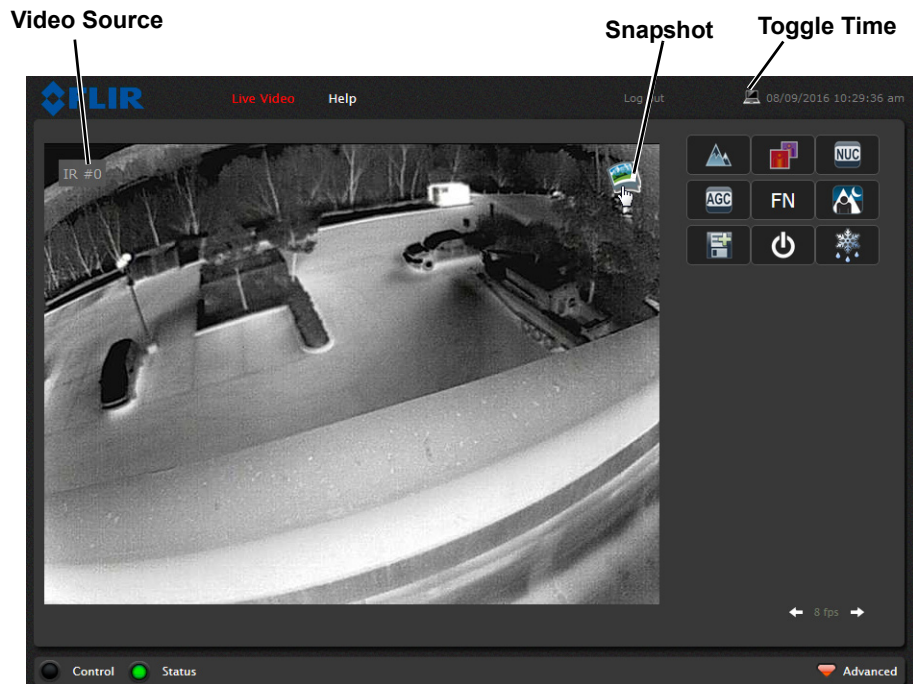


Figure 2-2: Live Video Web Page

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

Help

At the top of the page, the **Help** menu displays software version information. This page has information about the camera including hardware and software revision numbers, part numbers, and serial numbers. If it is necessary to contact FLIR Technical Support for assistance, it will be helpful to have the information from this page (such as Software Version) on hand.

Log out

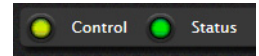
Use this button to disconnect from the camera and stop the display of the video stream. If a web session is inactive for 20 minutes, it will be stopped and it will be necessary to log in again.

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. The Status light may turn off temporarily while waiting for the response from the camera. After a short pause, the Control light should turn green.

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

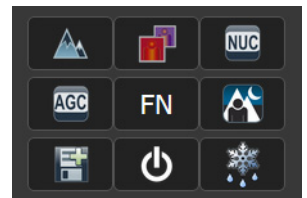
In addition, when the cursor is moved over the video, a snapshot button also appears in the upper right of the screen. After clicking the snapshot button, the video image is saved as a jpeg file and the browser will provide prompts depending on which browser is being used.



Web Control Panel

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

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



The following buttons appear for the FC-Series ID cameras:



Toggle Polarity

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



Toggle Palette

This button causes the camera to cycle through six different look up table (LUT) color palettes. Depending on the subjects viewed, one color palette may be preferable to the others. The Toggle Polarity button allows access to six more palettes (refer to [Misc. \(Lookup Table\), pg. 47](#)).



Perform IR NUC Calibration

This button causes the camera to perform a Non-Uniformity Correction operation (refer to [Image freezes momentarily, pg. 36](#)).

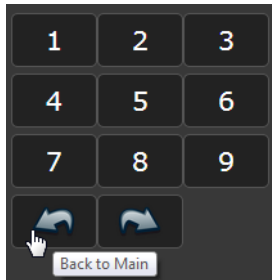


Toggle Automatic Gain Control (AGC)

This button causes the camera to cycle through different AGC options that use a combination of settings to produce different configurations that could improve the video image for a given set of conditions.

FN**Function**

The FC-Series ID cameras may have additional features or functions which can be accessed using an extra numeric keypad. When the Function button is selected, the keypad changes to a numeric keypad providing programmed functions (1 - 9). Select the back arrow to return to the main keypad. Select the forward arrow to access additional functions (10 - 18).



The available functions are specific to different camera installations. It is possible to create customized camera functions through a “macro” interface which can be programmed through XML commands. Contact FLIR Technical Support for information about the Nexus XML-Based Control Interfaces.

**Toggle Scene Preset**

This button causes the camera to cycle through different image settings. The Scene Presets cause the image brightness and contrast to adjust. Depending on the time of day, weather, and other conditions, one Scene Preset may be preferable to the others.

**Test File Transfer**

This button causes a request for the camera to transfer a file as determined by the settings on the Maintenance > Sensor > File Transfer page.

**Analytics On/Off**

The FC-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. 48](#).

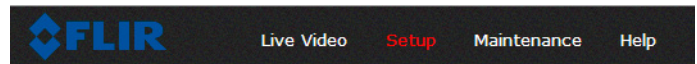
**De-Ice On/Off**

This button manually turns the lens heater on or off. The heater, when turned on manually, will run for approximately 2 hours unless turned off either by the user (De-Ice button) or the thermostat control. Refer to [Supplemental Lens Heater, pg. 7](#).

2.4 Basic Camera Configuration

The following procedures describe how to do the most common bench test camera configuration steps, such as setting the camera IP address and hostname and changing the user password. To make these changes, it is necessary to login using the **expert** user account. Additional setup and configuration options required after the camera has been installed in its final location are described after the basic steps are given, refer to [Advanced Configuration, pg. 40](#).

2.4.1 Setup Menu



The **Setup** menu is used for GEO Settings (Latitude and Longitude location), Video setup, thermal (IR) camera setup, and defining Video Analytics motion detection zones. For additional details, refer to [Setup Menu, pg. 40](#).

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 (Scene Presets, Polarity, Palettes, and AGC). Haphazard changes can lead to image problems including a complete loss of video. Additional information is provided in [Thermal Image Setup, pg. 45](#).

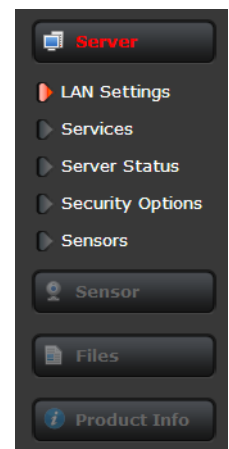
When a user logs in as **admin**, a complete **Maintenance** menu is available (refer to [Maintenance Menu, pg. 52](#)). The **Maintenance** menu also provides access to other configuration options. For more information on setting or changing other camera parameters refer to the *Nexus IP Camera Configuration Guide* (FLIR Doc #427-0030-00-28).

2.4.2 Server Menu

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

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

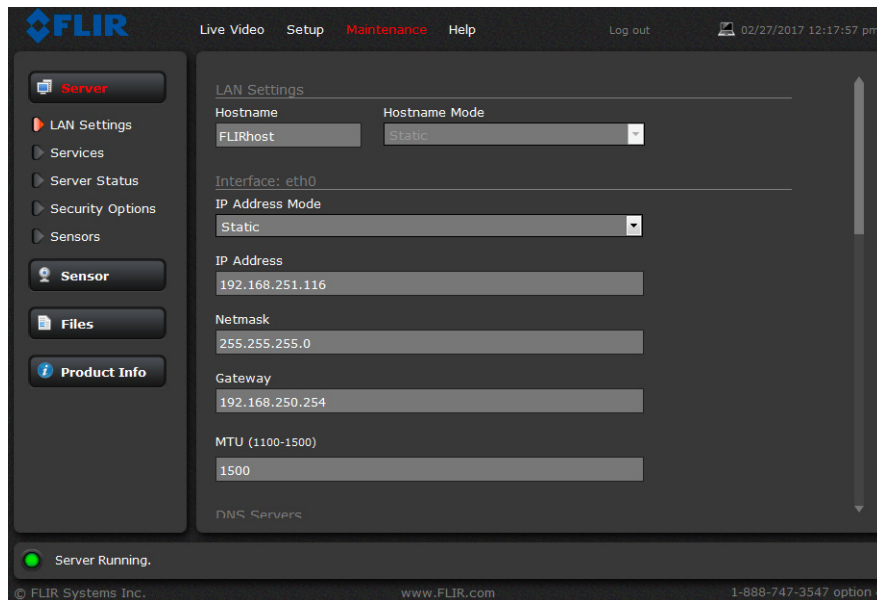
With most configuration changes through the Maintenance menu, it is necessary to save the changes, then stop and restart the server to make the changes take effect. When making configuration changes using the Setup page, most of the changes take effect immediately, and it is not necessary to start and 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.



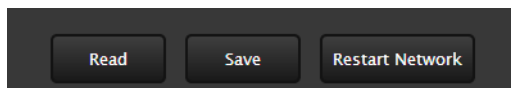
LAN Settings: The **LAN Settings** page can be used to set the hostname, default gateway, and IP address for the camera. Scroll down to see settings for Domain Name System (DNS) server and 802.1x Security.

IP Address

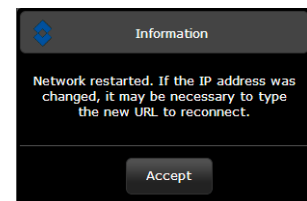
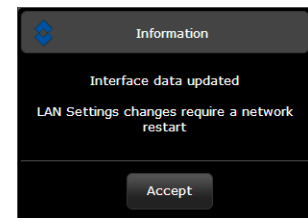
The default IP Address mode is static; the mode can also be set to DHCP. To set the IP address using DNA, refer to [Set IP Address using the FLIR Discovery Network Assistant \(DNA\)](#), pg. 22.



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



Once the IP address of the camera is changed, the PC may no longer be on the same network and therefore may not be able to access the camera until the IP address on the PC is changed also. For that reason, it makes sense to change the IP address after making other configuration changes.



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 FC-Series ID supports authentication using either Transport Layer Security (TLS) protocol or Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP MSCHAPv2).

Note

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

Configure IEEE 801.1x authentication using TLS

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

Step 2 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. Typical file extensions will be *.cer, *.crt, or *.der.

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

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

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

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

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

The screenshot shows the '802.1X Security' configuration interface. It features a dark background with white text and buttons. At the top, the title '802.1X Security' is displayed. Below it, a checkbox labeled 'Use 802.1x security' is checked. The 'Authentication' dropdown menu is set to 'TLS'. There are four main sections, each with a text input field and two buttons ('Browse' and 'Upload'): 'Identity', 'CA Certificate', 'Client Certificate', and 'Private Key'. At the bottom, there is a 'Private Key Password' field and three buttons: 'Read', 'Save', and 'Restart Network'.

To configure IEEE 801.1x authentication using PEAP MSCHAPv2

- 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 **PEAP(MSCHAPv2)**.
- Step 4 In the **Identity** text box, enter the name associated with the client certificate.
- Step 5 Use the **Browse** and **Upload** buttons to upload the associated **CA Certificate** from the server provided by the network administrator. Typical file extensions will be *.cer, *.crt, or *.der.
- Step 6 In the **Anonymous Identity** text box, enter the Anonymous Identity if required.
- Step 7 In the **Password** text box, enter the password associated with the Identity.

802.1X Security

Use 802.1x security

Authentication
PEAP(MSCHAPv2)

Identity

CA Certificate

Browse Upload

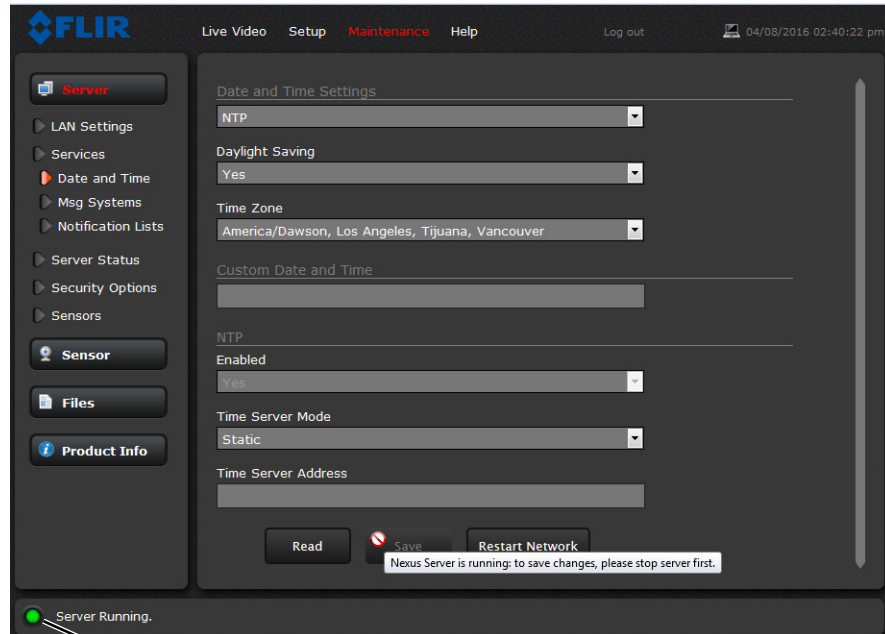
Anonymous Identity

Password

Read Save Restart Network

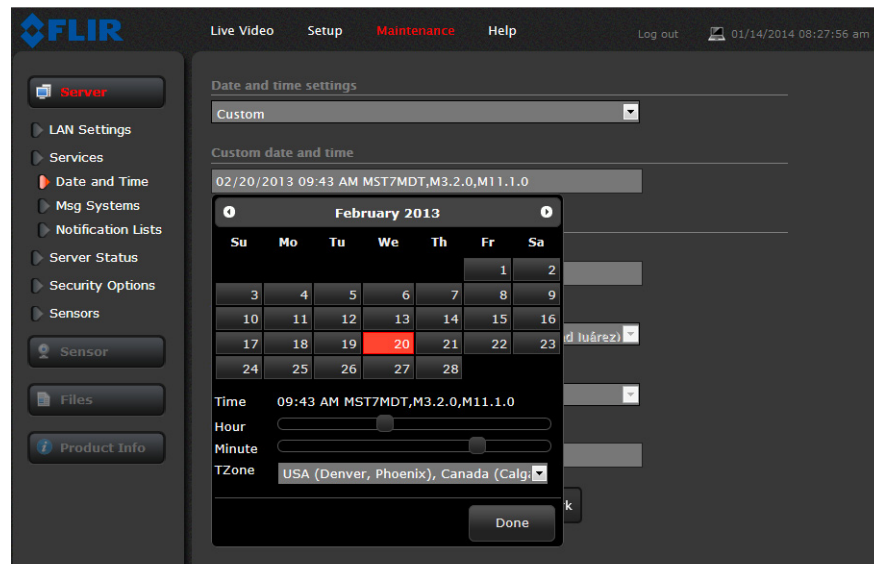
Services Menu

Date and Time: The **Date and Time** settings page is used to configure the date and time settings. The date, time, and time zone can be obtained from an NTP server, or can be entered manually. If NTP mode is selected, the NTP server information can be entered. The Nexus server must be stopped before changes can be saved. After saving changes, it is necessary to restart the server to make them effective.



Toggle Server (Stop/Start)

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



Set the date and time parameters, then select the **Save** button at the bottom of the page.

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

The screenshot shows the FLIR web interface with the 'Maintenance' tab selected. The left sidebar contains navigation options: Server, LAN Settings, Services, Date and Time, Msg Systems (highlighted), Notification Lists, Server Status, Security Options, Sensors, Sensor, Files, and Product Info. The main content area is titled 'Mail Server' and contains the following configuration fields:

- Server IP Address: [Text input field]
- Server SMTP Port: [Text input field]
- Authentication: [Dropdown menu, selected 'No']
- TLS Authentication: [Dropdown menu, selected 'No']
- User Name: [Text input field, value 'admin']
- Password: [Text input field, masked with dots]
- From Address: [Text input field]

If the email server is on a different network, ensure the IP default gateway and DNS servers are configured in the LAN Settings; refer to [LAN Settings, pg. 28](#). Configure the Msg Systems page with mail server information and then click **Save**.

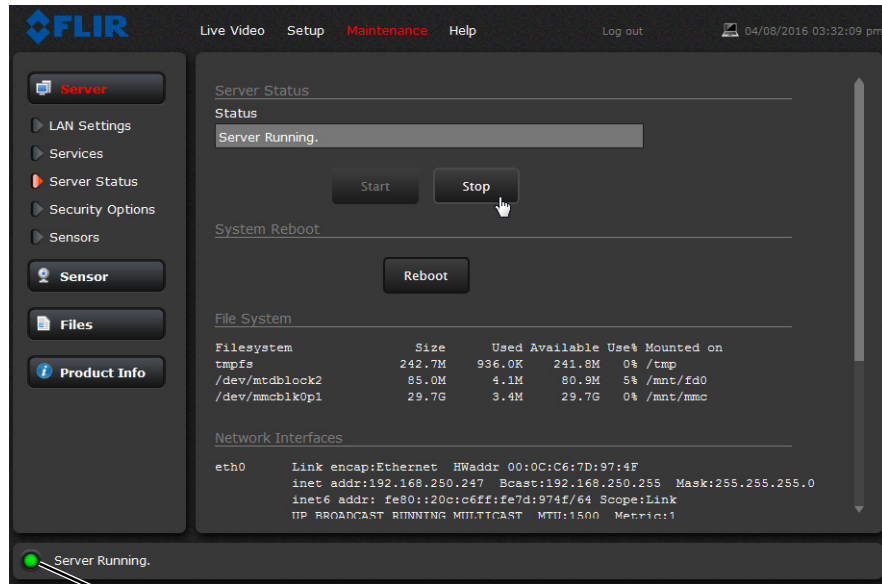
Notification Lists: Use this page to setup multiple email addresses and other notifications that can be sent as a result of alarms being processed by the Alarm Manager.

The screenshot shows the FLIR web interface with the 'Maintenance' tab selected. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Notification Lists' and contains the following configuration sections:

- Default Notification List:**
 - Email Addresses
 - Generic XML Notification
 - Milestone Generic Events Notification
- Notification List 1:**
 - Email Addresses
 - Generic XML Notification
 - Milestone Generic Events Notification

At the bottom of the page, there are two buttons: 'Read' and 'Save'.

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



Toggle Server (Stop/Start)

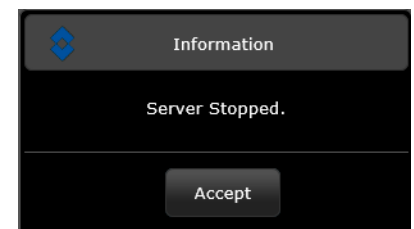
After making configuration changes, it is necessary to save the changes to the server (there is a **Save** button at the bottom of each configuration page). The configuration changes do not take effect immediately. Generally, it is also necessary to stop and restart the server for the changes to become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

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

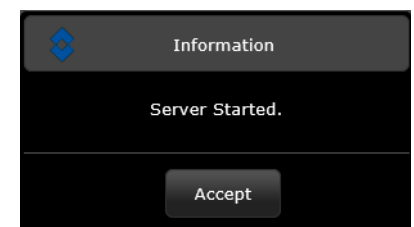
You must restart the server for the changes to be effective.

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

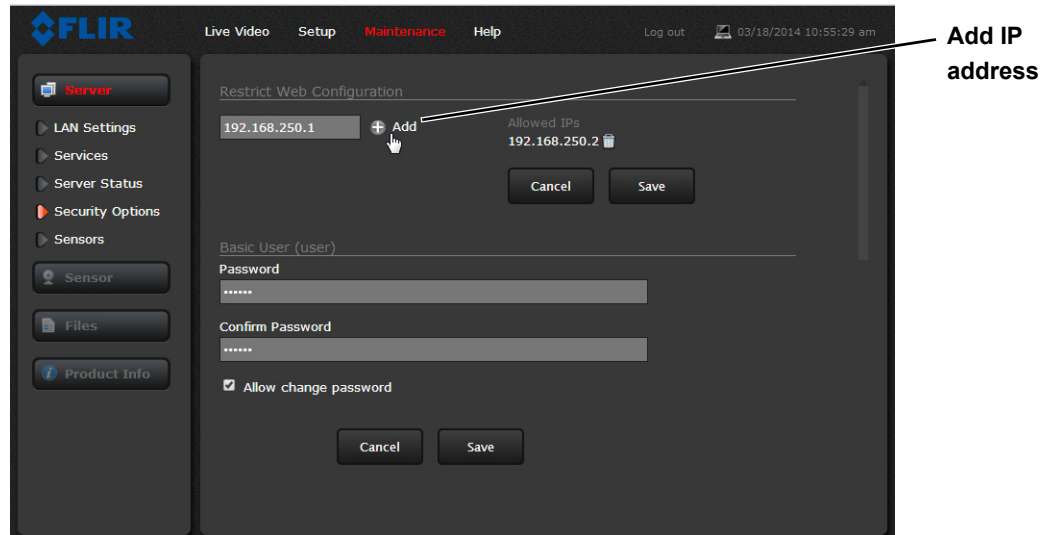
When the server is stopped and the page is refreshed, the status will show Server Stopped and the Start button will be enabled.



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



Security Options: Use the **Security Options** page to restrict access through the camera web server to specific IP addresses and to set and change passwords. As shown below, the **expert** login can only configure the **user** login password.



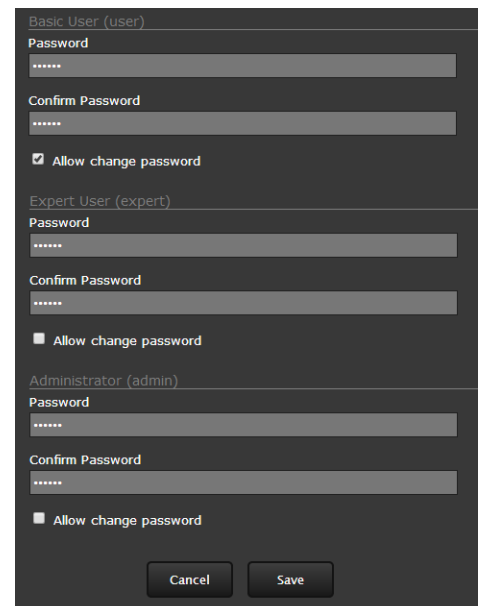
As an additional security measure, limit which computers have access to the web browser interface. Simply add a computer's IP address and click Add. After all the allowed IP addresses are entered, select the **Save** button to save the changes.

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

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

After a password is set and confirmed, select the **Save** button at the bottom (scroll down the page, if necessary).

Selecting the Allow Change Password check box will allow that login to change their own password from an icon at the top of all pages.



Note

A VMS using an ONVIF interface to the camera has specific ONVIF only passwords that are set independently from these web interface passwords. Refer to [VMS Remote, pg. 54](#).

2.5 Thermal Imaging Overview

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

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

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



This is why hot objects such as parts on an engine and exhaust pipes appear white, while the sky, puddles of water and other cold objects appear dark (or cool)³. Scenes with familiar objects will be easy to interpret with some experience. The camera automatically optimizes the image to provide the best contrast in most conditions, and in some cases the Scene Presets mentioned above and other settings can be used to further improve the image.

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

3. By default, the camera represents hot objects as white and cold objects as black. The camera can be set to use the Black Hot polarity setting, which displays hot objects as black and cold objects as white and is effectively the negative of White Hot polarity. Refer to [Toggle Polarity, pg. 25](#).

2.6 Maintenance and Troubleshooting Tips

If help is needed during the installation process, contact the local FLIR representative, or call the appropriate support number listed at: <http://www.flir.com/security/display/?id=71083>. FLIR Systems, Inc. offers a comprehensive selection of training courses to help get the best performance and value from the thermal imaging camera. Find out more at the FLIR training web page: <http://www.flir.com/training>.

Cleaning

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

Note

Ensure that the camera is not disturbed or moved during cleaning. The detection analytics are set and calibrated based on the exact position and camera angle. Inadvertent realignment may require relocation and recalibration of detection regions.

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

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

Use the following procedure and solvents, as required:

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

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

Step 2 With a new tissue each time, wipe the lens in an “S” motion (so that each area of the lens will not be wiped more than once).

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

Image freezes momentarily

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

Using the camera web server, it is possible to change the FFC interval or to disable the automatic FFC entirely by setting it to Manual mode. Refer to [Flat Field Correction \(FFC\)](#), pg. 47. For the best possible image, it is recommended that the factory settings are used.

No video

If the camera will not produce an image, check the video connection at the camera and at the display. If the connectors appear to be properly connected but the camera still does not produce an image, ensure that power has been properly applied to the camera and the circuit breaker is set properly. If a fuse was used, be sure the fuse is not blown. If the video cabling is suspected as a possible source of the problem, plug a monitor into the BNC connection inside the camera and determine if it produces an image.

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

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

Performance varies with time of day

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

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

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

Unable to View Video Stream

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

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

If necessary, test to make sure the video from the camera can be viewed by a generic video player such as VLC media player (<http://www.videolan.org/vlc/>). To view the video stream, specify RTSP port 554 and the appropriate stream name. For example:

```
rtsp://192.168.250.116:554/ch0, and  
rtsp://192.168.250.116:554/ch1
```

Port 554 is the standard RTSP port as well as the default for the camera. Typically, if the default port has not been changed, the port can be left out of the streaming command, such as:
rtsp://192.168.250.116/ch0.

Refer to [Video, pg. 42](#) for additional information on RTP settings and stream names.

Unable to control the camera

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

Noisy image

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

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

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

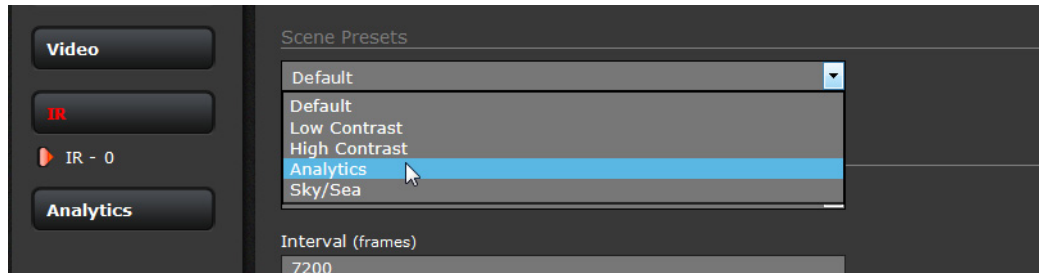
Image too dark or too light

By default the FC-Series ID camera uses an Automatic Gain Control (AGC) setting that has proven to be superior for most applications, and the camera will respond to varying conditions automatically. The installer should keep in mind that the sky is quite cold and can strongly affect the overall image. It may be possible to avoid a problem by slightly moving the camera up or down to include (or exclude) items with hot or cold temperatures that 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.

There are Scene Presets that use a combination of settings to produce different configurations that could improve the video image for a given set of conditions. The presets can be toggled with the Scene Presets button on the **Live Video** page.



The presets can also be selected from the Scene Presets in the **Setup** page. Refer to [Thermal Image Setup, pg. 45](#)



Available Scene Presets

Eastern or Western Exposure

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

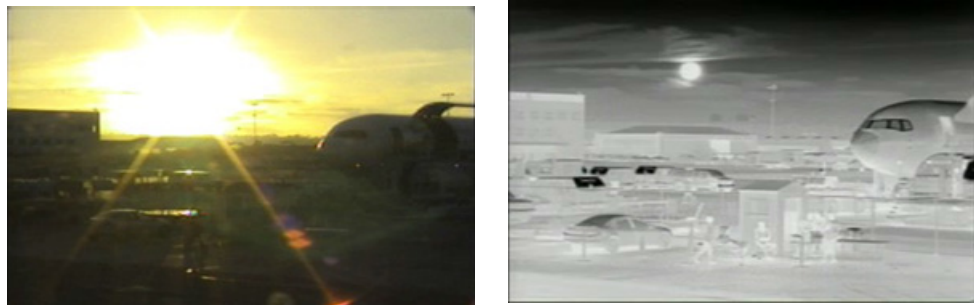


Figure 2-3: Images facing sun from standard camera (left) and thermal camera (right)

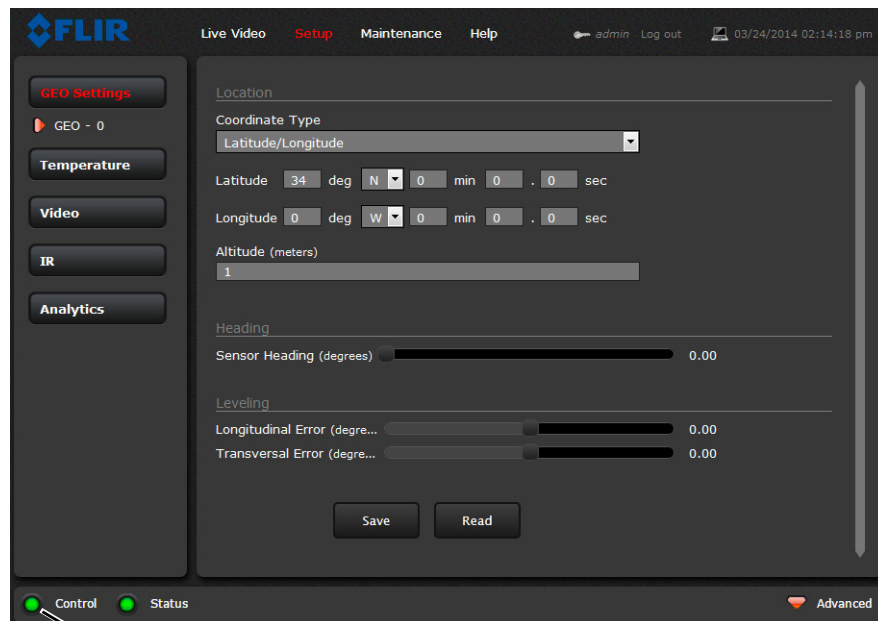
In this chapter, additional setup and configuration settings related to the following topics are described:

- Setting up the video streams to optimize quality and network performance
- 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)
- Enabling On-Screen Display (OSD) text

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. 64).

3.1 Setup Menu

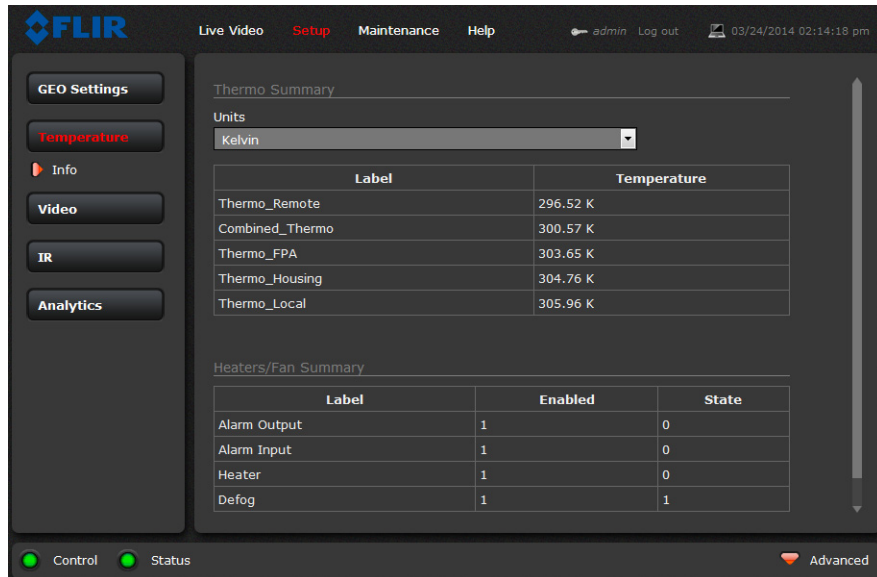
It is necessary to have control of the camera to make Setup changes. Changes made through the **Setup** menu have an immediate effect (it is not necessary to stop and restart the server). To use these settings at power up, it is necessary to save the changes ([Save Settings](#), pg. 47).



Camera Control

3.1.1 Temperature Page

The Temperature Info page displays temperature readings from the camera and GPIO signal status.



Thermo Summary

Select the temperature units to display: Kelvin, degree Celsius, or degree Fahrenheit.

Table 3-1: Temperature Labels

Thermo_Remote	Heater temperature
Combined_Thermo	Calculated window target temperature
Thermo_FPA	Tau IR core Focal Plane Array temperature
Thermo_Housing	Tau IR core housing
Thermo_Local	FC-Series camera circuit board

Heater/Fan Summary

The GPIO signal status is shown.

Table 3-2: GPIO Labels

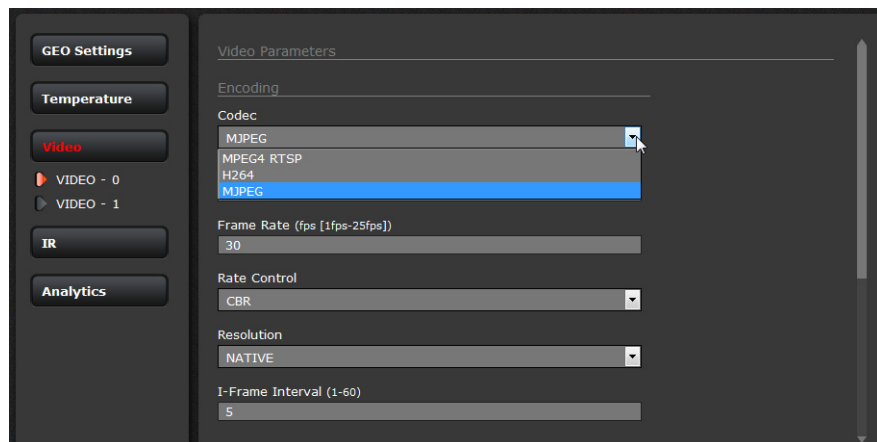
Alarm Output	User GPIO signals are enabled by default. (Refer to General Purpose Input/Output (GPIO) , pg. 6.)
Alarm Input	
Heater	Internal heater output signal
Defog	Internal heater input signal—when 0, heater power is limited ^a

- a. For example, when the camera is powered by the lower power IEEE 802.3af-2003 PoE standard. Refer to [PoE+ Power Supplies](#), pg. 7.

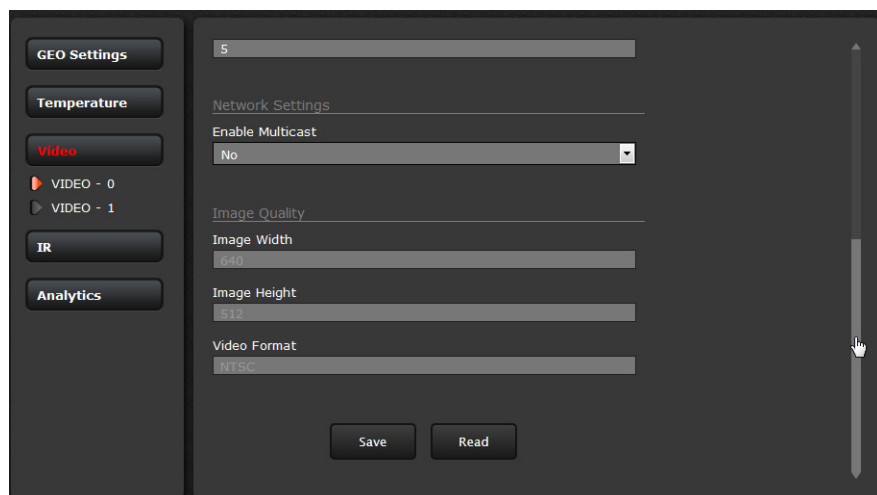
3.1.2 Video Setup

Video: By default, two video streams are enabled for the camera: Video 0 and Video 1. Both video streams are available for viewing from a client program such as FLIR Latitude, a stand-alone video player, or a third-party VMS (including ONVIF systems).

By default, Video 0 uses MJPEG encoding and Video 1 uses H.264 encoding. To modify parameters that affect a particular IP Video stream from the camera, select the appropriate link (for example, **Video - 0**).



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



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.

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

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 MPEG4 RTSP, H.264 or MJPEG. MPEG4 RTSP requires the least amount of processing, and MJPEG requires the most.

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.

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. Table 3-3 provides the corresponding resolution for each setting.

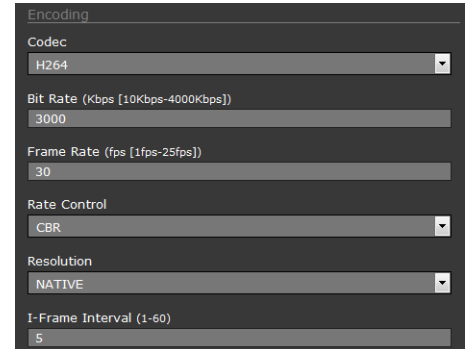


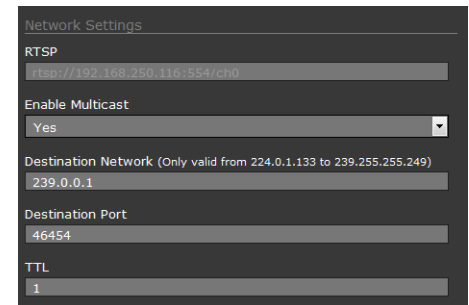
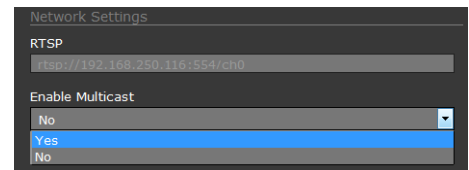
Table 3-3: Image Size Settings

Resolution	NTSC	PAL
NATIVE	640 x 512	640 x 512
D1	720 x 480	720 x 576
VGA	640 x 480	640 x 480
QVGA	320 x 240	320 x 240
CIF	352 x 240	352 x 288
4CIF	704 x 480	704 x 576
QCIF	176 x 112	176 x 144
QNATIVE	320 x 256	320 x 256

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.

By default, the video streams from the camera are sent using unicast packets rather than multicast. This means a given packet of IP Video will be sent separately to each client that has that video stream open. Therefore each additional client will cause the bandwidth to increase and cause more overhead on the system in comparison to multicast.

The Multicast option can be used to limit how much bandwidth is required for multiple clients, but it requires a higher level of network administration and an understanding of how multicast traffic is managed (multicast addresses, routers and switches, and so on). With Multicast enabled, new fields are shown, Destination Network IP address and Destination Port, as well as TTL (time-to-live). 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.



The time-to-live field controls the ability of IP packets to traverse network or router boundaries. A value of 1 restricts the stream to the same subnet. Values greater than 1 allow ever increasing access between networks.

There are some challenges with streaming video over an IP network, when compared to applications which are less time-critical, such as email and web browsing. There are requirements which must be fulfilled to ensure satisfactory video quality in professional security environments. There are many parameters and factors related to network infrastructure, protocols, codecs, and so on that can affect the quality and bit rate of a video stream when it is established between the camera and a client.

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, or 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.

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.

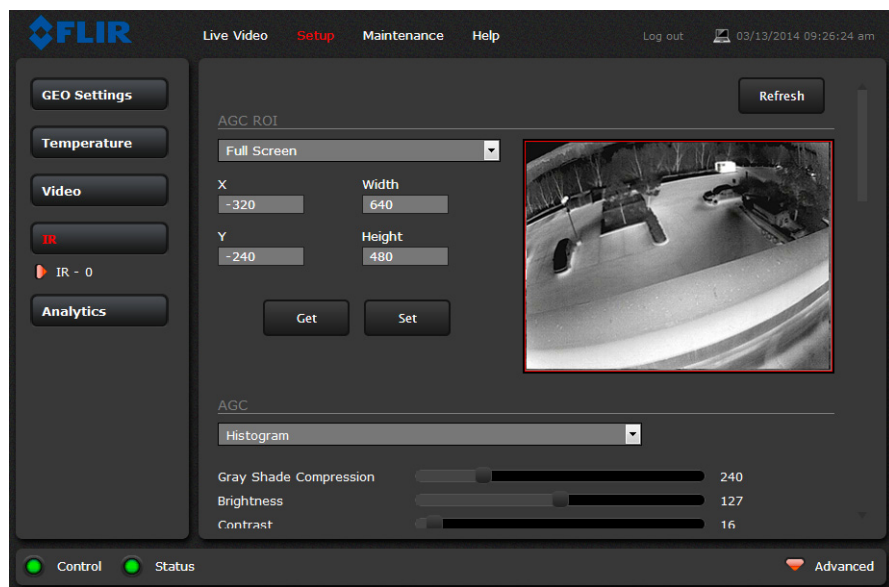
RTSP is originated and received on even port numbers and the associated RTCP communication uses the next higher odd port number; the default RTSP Port is 554.

The default value for the stream from VIDEO - 0 is ch0. For example, the complete connection string is: `rtsp://192.168.250.116/ch0`. This stream name can be used to open a video stream with a third-party video player. By default the video stream uses the IP address of the camera.

3.1.3 Thermal Image Setup

In most installations it will not be necessary to change the thermal camera from the default settings. However in some situations, depending on weather, time of day and so on, it may be useful to make changes to the video image to enhance the image by modifying one or more of the parameters. In most situations, it will be adequate to select a different Scene Preset (described below). However, be aware that when the conditions change the camera may need to be adjusted again; for that reason it is a good idea to know how to restore the factory default settings as well.

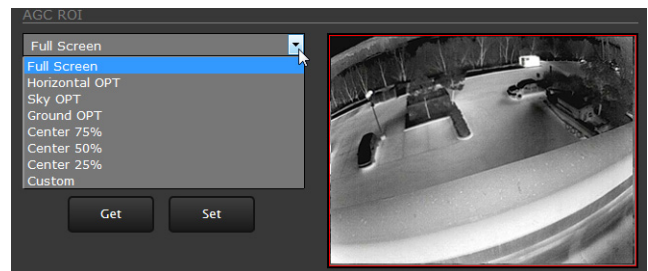
IR Page



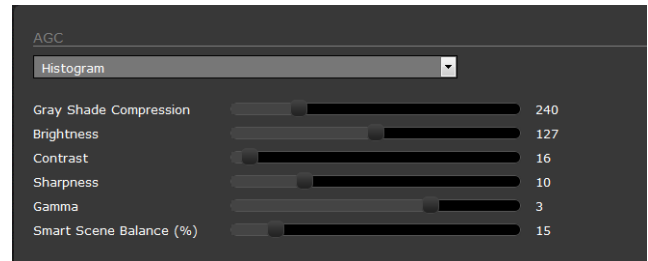
In the **IR** page, a single JPEG image (a snapshot) is displayed in the upper right-hand corner. To update this image at any time, select the **Refresh** button in the upper right. This will cause the entire page to refresh, including the image and all the parameter values (be patient, this may take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

To make adjustments to the thermal image, it is possible to modify the Automatic Gain Control (AGC) settings, which are grouped under the **AGC ROI**, **AGC**, and **Scene Presets** headings. The overall image display (also known as Polarity or Color Palette) is determined by the Look Up Table (LUT) selected in the **Misc. (Lookup Table)** section.

AGC ROI: The AGC Region Of Interest (ROI) determines what portion of the image is used in the calculation of the AGC. By default all of the pixels in the image are considered (Full Screen); in some cases it may be possible to improve the contrast if a portion of the image is excluded. For example, if the field of view includes a portion of the sky, typically quite cold, it may be desirable to restrict the ROI to the portion of the image below the horizon.



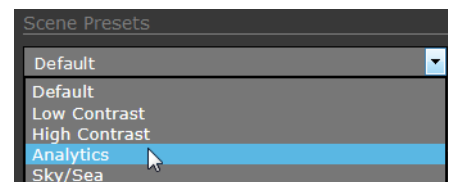
AGC: The AGC parameters control the overall brightness and contrast, and determine how the overall video image appears. The default Histogram algorithm is suitable for most installations, but in some cases one of the other selections may provide a more appealing image, depending on personal preferences. Be aware 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.



Experiment with different AGC parameters to find the settings that work best for the particular installation (it is recommended to start with one of the **Scene Presets**, see below). 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.

- **Gray Shade Compression** (Plateau value) when set high, the algorithm approaches the behavior of classic histogram equalization—gray shades are distributed proportionally to the cumulative histogram, and more gray shades will be devoted to large areas of similar temperature in a given scene. On the other hand, when the value is set low, the algorithm behaves more like a linear AGC algorithm—there is little compression in the resulting 8-bit histogram.
- **Brightness** (ITT Mean) setting determines the temperature that is at the middle of the 256 “shades of gray” available to the camera. Higher values allow more detail in hotter scenes, while lower values allow more detail in lower temperature scenes.
- **Contrast** (Max Gain) can generally be used to increase contrast, especially for scenes that have little temperature variation (although it may also increase noise due to increased gain).
- **Sharpness** (DDE) is used to enhance image details and/or suppress fixed pattern noise. Higher values increase Sharpness, while lower values soften the image and filter fixed pattern noise.
- **Gamma** (ACE) provides a contrast adjustment dependent on the relative scene temperature. Gamma values greater than 0 give more contrast to the hotter scene content and decrease contrast for the colder scene content. Gamma values less than 0 do the opposite by decreasing the contrast for hotter scene content and leaving more of the “shades of gray” to represent the colder scene content.
- **Smart Scene Balance** (SSO) value defines the percentage of the scene that will be allotted a linear mapping. With SSO enabled (greater than zero), the difference in gray shades between two objects is more representative of the difference in temperature, although the optimization in local contrast can be lost.

Scene Presets: Each Scene Preset provides a combination of AGC parameters that may be preferred for certain types of conditions. Select a preset that provides an image that is optimal for the installation. Recall the Scene preset can also be toggled by selecting the Toggle Scene Preset button from the **Live Video** page control panel.



Flat Field Correction (FFC): The FFC operation can correct for non-uniform responsiveness within the pixel array. A shutter activates inside the camera and provides a target of uniform temperature, allowing the camera to correct for ambient temperature changes and provide the best possible image. The camera performs FFC at regular intervals or when the ambient temperature changes, but FCC can also be performed manually and may cause an overall image improvement. Refer to [Image freezes momentarily, pg. 36](#).

Misc. (Lookup Table): Each Look Up Table (LUT) provides a different display of the various detected levels of thermal energy as either colors or gray-scale values. Look Up Table 1 is white hot and Look Up Table 2 is black hot; the other tables assign different colors to different temperatures. These color palettes can also be selected from the Live Video page (refer to [Toggle Palette, pg. 25](#)).

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 and then click on **Save Settings**.

FFC

Auto

Interval (frames)
7200

Temp. Change (0.1 ° C)
10

Warning Time (frames)
45

Perform FFC Get Set

Misc. (Lookup Table)

Test Pattern
No

LUT

- Look Up Table 1
- Look Up Table 2
- Look Up Table 3
- Look Up Table 4
- Look Up Table 5
- Look Up Table 6
- Look Up Table 7
- Look Up Table 8
- Look Up Table 9
- Look Up Table 10
- Look Up Table 11
- Look Up Table 12

Save Settings Factory Defaults Reboot

3.1.4 Video Analytics Setup

The Analytics function of the FC-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, or tripwire lines, or analytics masking areas. Each detection area or tripwire has independent detection properties (such as detecting a vehicle or human sized object). Use the **Maintenance** menu to define the actions resulting from each alarm condition ([Alarm Manager, pg. 60](#)).

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

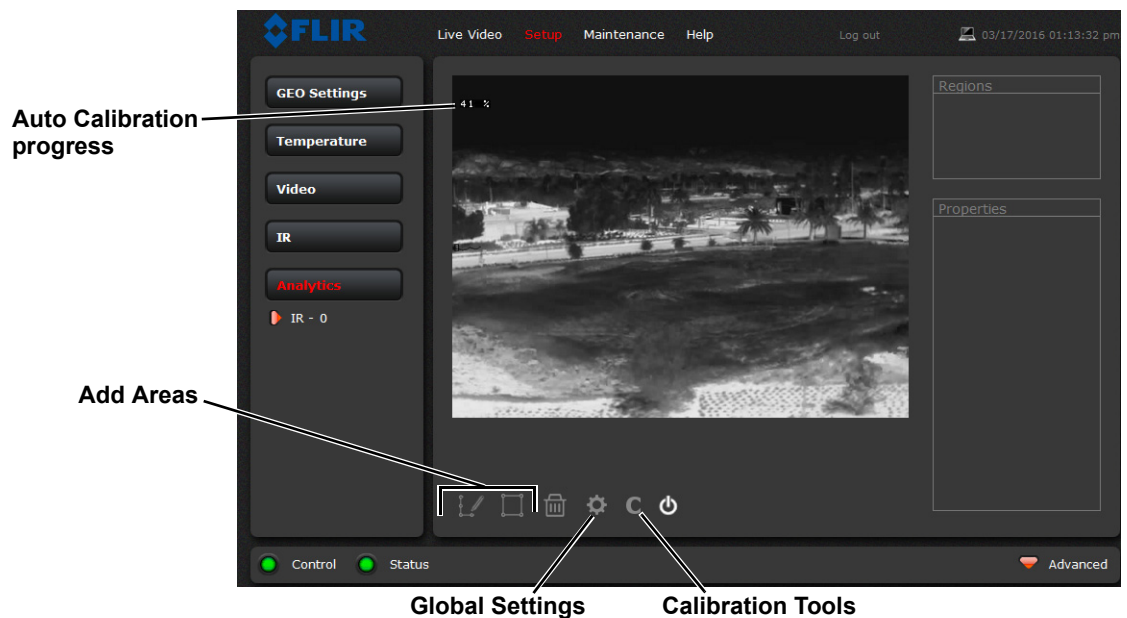


Figure 3-1: Analytics Page

Analytics Calibration

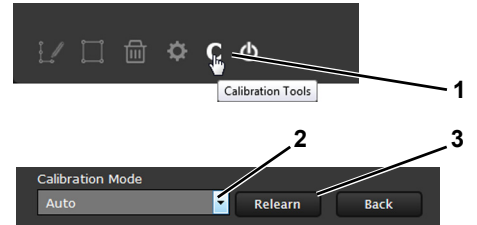
The camera must be mounted in its final location in order to calibrate the scene in the field of view using either the auto or manual calibration tool. Once the analytics are calibrated and turned on, the camera can provide recognition of moving objects based on size and aspect ratio: human or vehicle.

Use the Calibration Tools to set the classification parameters.



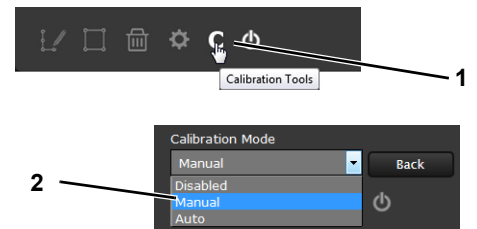
Auto Calibration

- Step 1 On the camera's **Analytics** web page, click the Calibrate icon.
- Step 2 To automatically calibrate detection settings, from the **Calibration Mode** drop-down list, select **Auto**.
- Step 3 Click **Relearn**. The camera automatically calibrates the depth of the FoV based on people walking in the scene. Be sure that people are walking along the entire vertical axis of the FoV until calibration is finished. The On-Screen Display shows the progress as a percentage in the upper left corner of the video (see Figure 3-1).



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**.



4. Far Size Calibration

3. Near Size Calibration



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**.

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

Global Settings

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

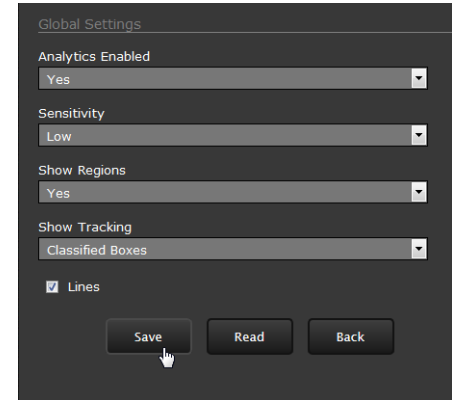
There are three settings for sensitivity which control the threshold for detection (as well as false alarms): **Low**, **Medium**, and **High**. When set to low, the analytics will detect fewer objects (also fewer false alarms) than when set to high.

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

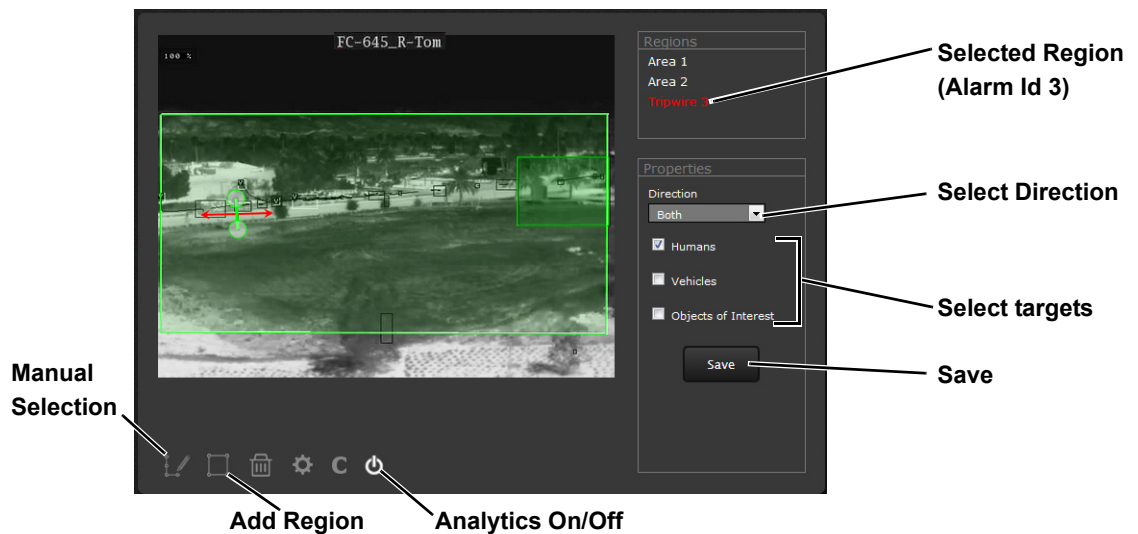
There are three tracking display options: **All Boxes**, **Classified Boxes**, and **No Boxes**. If either option to show boxes is selected, a check box enables a tracking line with each detection box.

- **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”.
- **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).


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

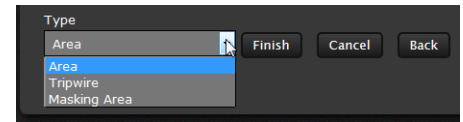


Creating Analytics Regions



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

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



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


Note

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

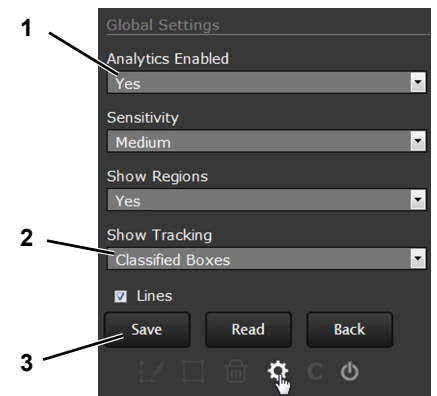
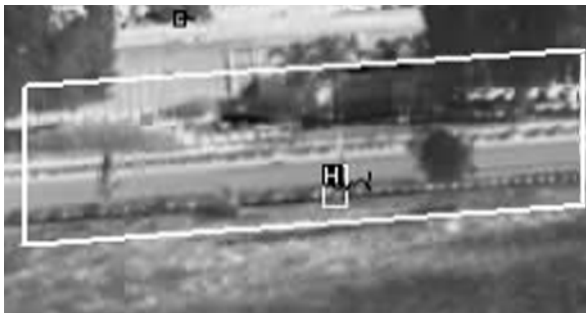
- With **Masking Area** selected, click in the video to create the first corner of the area. Continue adding corners, then select Finish to complete the area.
This is motion detection masking; not privacy masking. The video image will still be seen, but alarms will not be generated. Analytics will be disabled in the masked area. The purpose is to manually define regions that will not generate motion alarms. For example, this can be helpful to eliminate alarms from a tree or bush moving in the wind or to perform auto calibration for some scenes.

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

Check Calibration

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

The image below shows a classified human box and tracking line in a detection region. The 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 refer to the *Nexus IP Camera Configuration Guide* (FLIR Doc #427-0030-00-28) or contact the local FLIR representative or FLIR Technical Support.

The basic camera configuration settings (**LAN Settings, Services, and Security Options**) available through the **expert** login are described in [Server Menu, pg. 27](#). When logged in as **admin**, additional Maintenance menus are accessible, including **Sensor, Files** and **Product Info**.

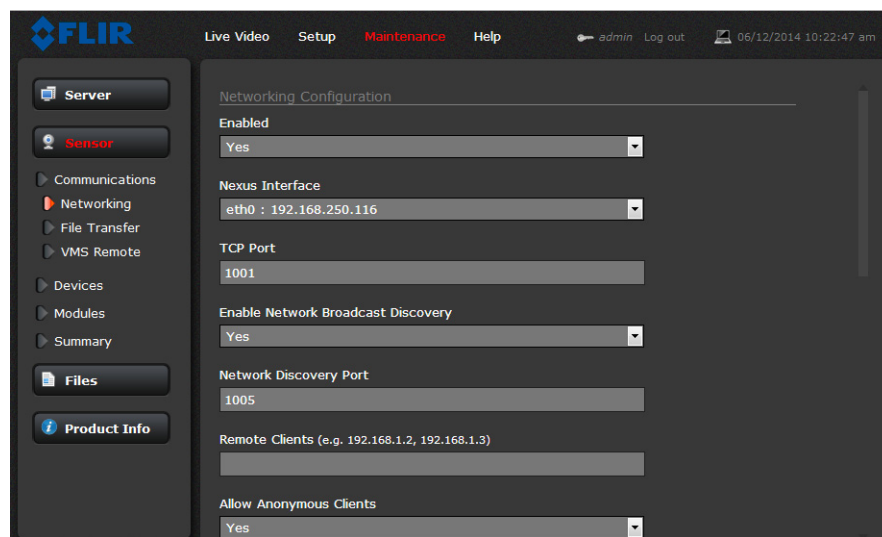
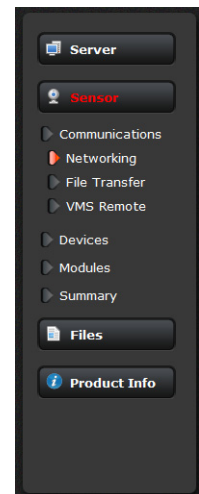
3.2.1 Sensor Menu

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

Communications Menu

The primary IP configuration parameters, such as IP address, network mask, and gateway, are configured with the LAN Settings page (refer to [LAN Settings, pg. 28](#)). The Networking page can be used to configure some of the other IP networking parameters.

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



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.

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.

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. 34](#) 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.

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 FC-Series ID supports both NAS NFS and NAS Samba. See [Alarm Actions, pg. 61](#).

VMS Remote: The VMS Remote page provides communication interfaces for devices that connect to the camera.

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. An ONVIF-compliant VMS can be used to control a FLIR camera, display video, and, for pan/tilt cameras, access up to 50 pan/tilt presets. 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).

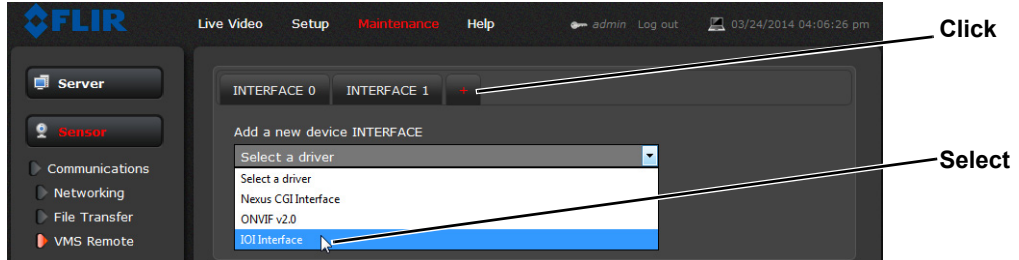
Scroll down to change ONVIF authentication passwords or other settings. After the interface is configured, scroll down and click on the **Save** button to save the configuration. The changes will not take effect until the server is stopped and started.

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

IOI Interface

Install this interface to hand-off FC-Series ID detection events to the PTZ Tracker (trk-101-P). In order to implement a hand-off from the FC-Series ID camera to a PTZ camera, the FC-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 FC-Series ID camera to monitor (refer to [Video Analytics Setup, pg. 48](#)). When a moving object is detected by the FC-Series ID, the trk-101-P can control and move the PTZ camera to autonomously track and zoom in on the motion.

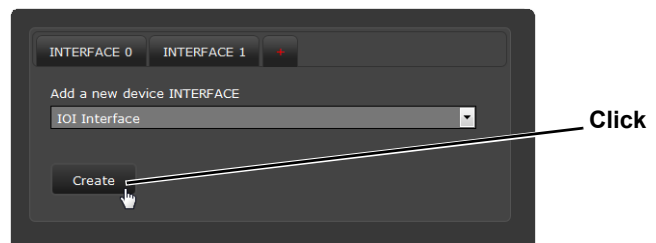
Step 1 Select **Maintenance > Sensor > VMS Remote**.



Step 2 Click **+** ().

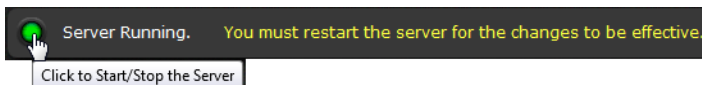
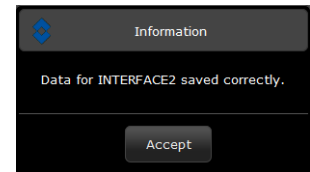
Step 3 From the drop-down list, select **IOI Interface**.

Step 4 Click **Create**.



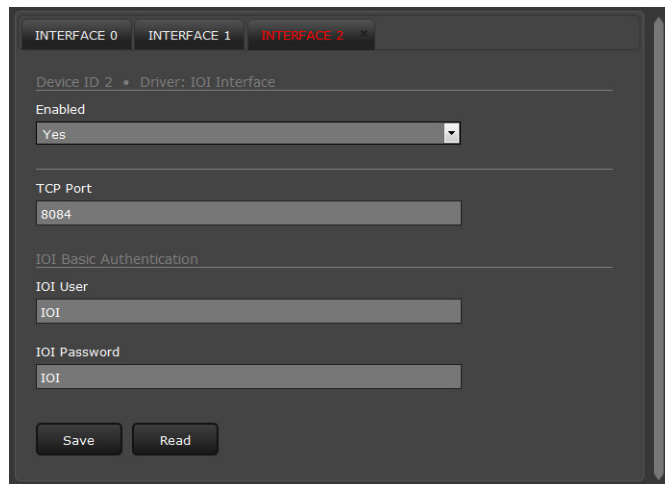
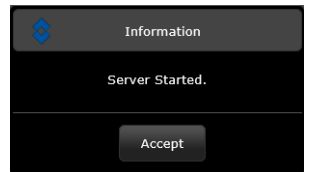
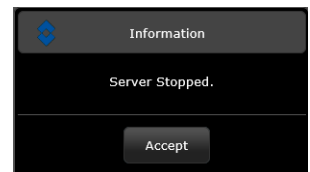
Step 5 Accept the message “Data for INTERFACE2 saved correctly”.

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



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

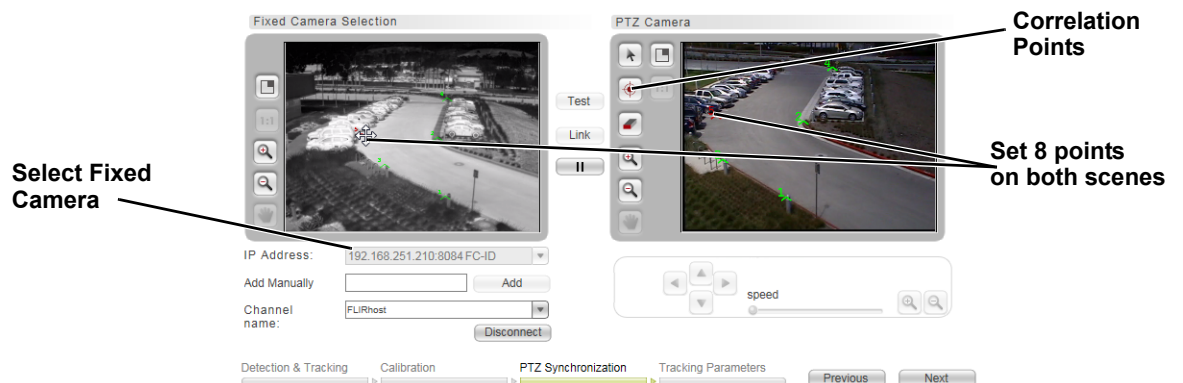
Click on the Start button again to restart the server.
Click **Accept** at the prompt.
The status will show Server Running.



Link Cameras on trk-101-P Tracker

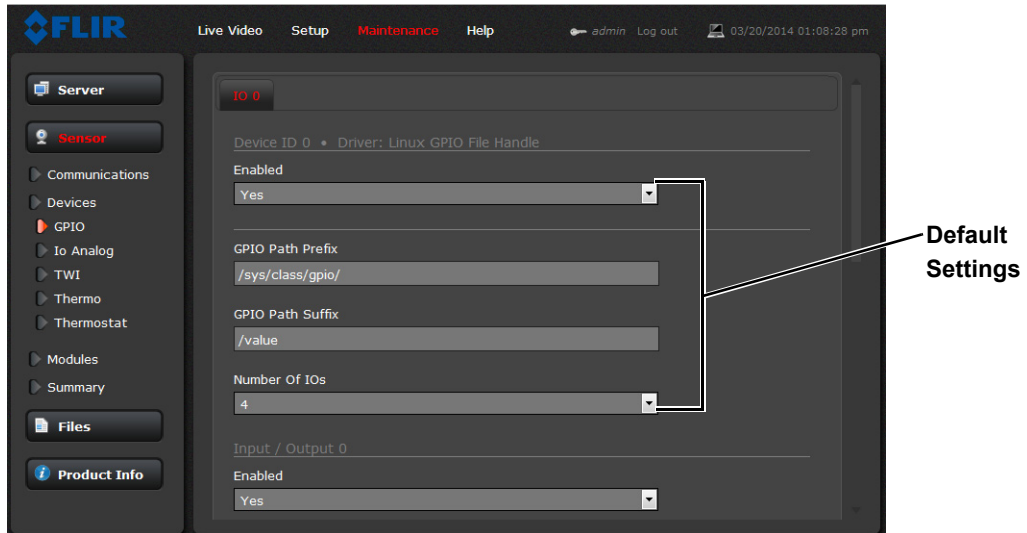
Link the PTZ camera and the FC-Series ID from the trk-101-P web interface.

- Step 1 Ensure that the FC-Series ID Analytics have been calibrated (refer to [Analytics Calibration, pg. 48](#)).
- Step 2 With the FC-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 FC-Series ID scene.
- This process is outlined here and detailed in the *FLIR ioi HTML Edition Units User Guide* which can be downloaded from the ioi Analytics section at <http://www.flir.com/security/display/?id=44516>.
- Step 3 Ensure that the FC-Series ID detection regions are setup to correspond to the presets on the trk-101-P (refer to [Creating Analytics Regions, pg. 50](#)).
- Step 4 Login to the trk-101-P web interface.
- Step 5 Select Setup
- Step 6 From the **Camera > Type & Model** screen, verify that the Camera Model is configured as PTZ.
- Step 7 Click **Start PTZ Setup**.
- Step 8 On the **Detection and Tracking** screen, select *Detection from another camera with Automatic PTZ tracking*. Click **Next**.
- Step 9 Click **Calibrate** and follow the instructions on the web interface. Click **Next**.
- Step 10 On the **PTZ Synchronization** screen, follow the procedure described in the *FLIR ioi HTML Edition Units User Guide*. Refer to “Step 3: PTZ Synchronization with Fixed Cameras” in the section “Using the PTZ Camera Definition Wizard”
- Step 11 Set 8 correlation points on the ground for each camera, select **Test**, and then **Link**. Refer to the procedure “To set correlation points in a preset” in the user guide. Click **Next** and **Finish**.



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

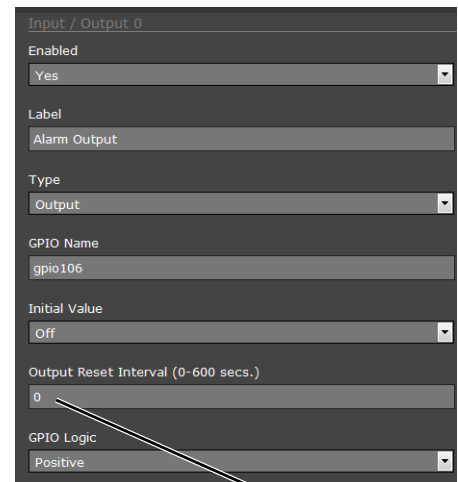
Devices Menu GPIO: On the GPIO page, scroll down to read the current I/O parameters. GPIO is enabled by default.



The GPIO must be wired during installation, refer to [GPIO Connections, pg. 14](#). The status of the GPIO signals are displayed on the Temperature page from the Setup menu, refer to [Temperature Page, pg. 41](#).

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

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



- 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. 63](#).
- 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).

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

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

Input / Output 1

Enabled: Yes

Label: Alarm Input

Type: Input

GPIO Name: gpio108

GPIO Logic: Negative

Input / Output 1

Enabled: Yes

Label: Alarm Input

Type: Input

GPIO Name: gpio108

GPIO Logic: Negative

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

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

Input/Output 2 and **Input/Output 3** are control signals for the camera heater circuits. The **Heater** output signal denotes when the De-Ice button on the Live Video page is activated. The **Defog** input signal denotes when the heater can be run at full power. These two signals perform internal functions and should not be changed.

Input / Output 2

Enabled: Yes

Label: Heater

Type: Output

Input / Output 3

Enabled: Yes

Label: Defog

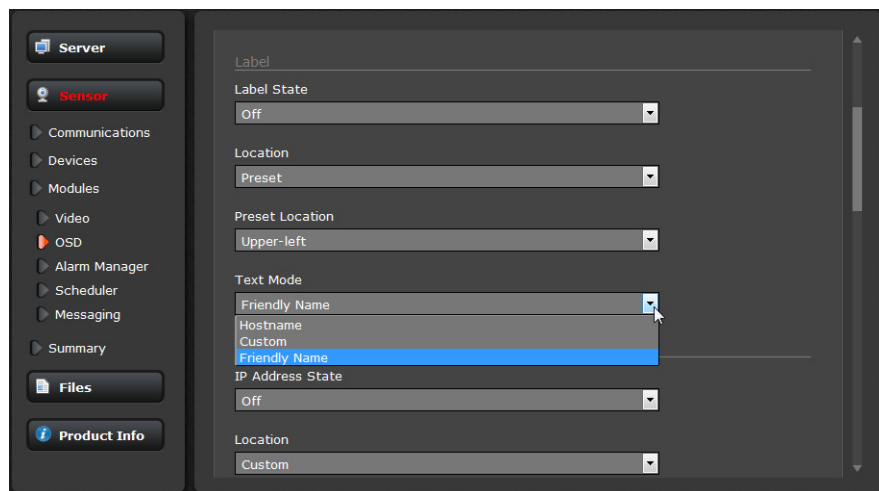
Type: Input

Refer to the following sections for a description of how to combine the GPIO inputs and outputs with other alarms. For example, the camera can send the output signal when there is a Video Analytics alarm. Similarly, the camera can save an image snapshot when there is an input. These associations are configured with the Alarm Manager module described in [Alarm Manager, pg. 60](#).

Modules Menu

This section describes the On Screen Display (OSD) page, and Alarm Manager page. Use the Video page to modify the video stream parameters that affect both image quality and transmission bandwidth. With the settings on the OSD page, it is possible to display text information (for example, camera name, date/time, etc.) as an overlay on the video. The OSD text will appear on the IP video streams as well as the analog video output. Use the Alarm Manager page to define rules for camera alarms from Video Analytics or GPIO.

On Screen Display: Use the **OSD** page to turn on and configure the On Screen Display (OSD) options. It may be desirable to display text information (such as the name of the camera or the date/time) as an overlay on the video image. The OSD configuration page allows selected camera-related information to be displayed in the analog video and in the IP video streams.



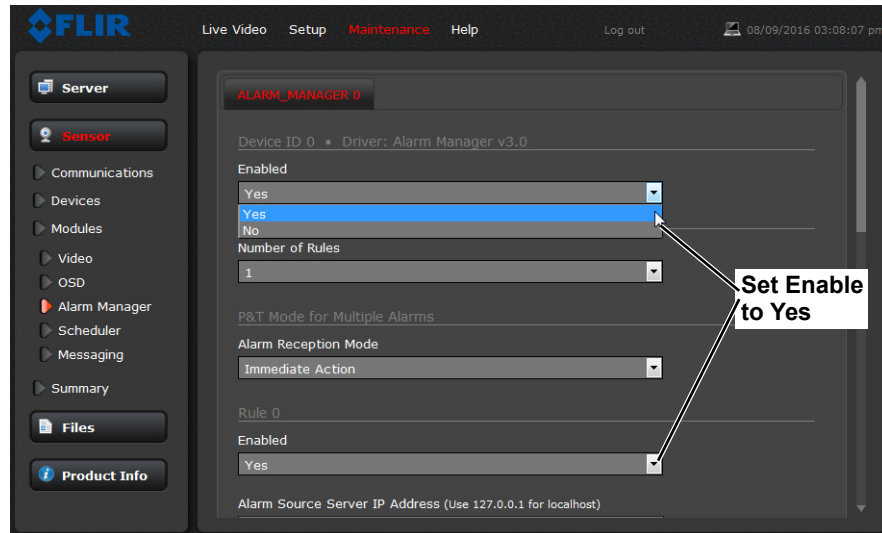
For example, the **Label** can display the Friendly Name (configured on the Product Info page), the Hostname (configured on the LAN Settings page) or a Custom text string (using the Text parameter after selecting Custom).

Each text string can be controlled with the following parameters:

- State (on or off)
- Location (preset location or a Custom X and Y Location)

The OSD text will appear on the IP video streams as well as the analog video output.

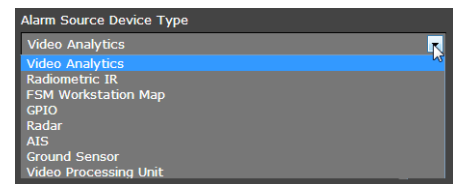
Alarm Manager: Use the **Alarm Manager** page to set the response (action) that results from an individual alarm. It is possible to have more than one action for a single alarm by adding additional rules (for example, one action could capture an image and another could generate an output). If a message 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 Menu, pg. 31](#)). See also the Media Browser ([Media Browser, pg. 65](#)).



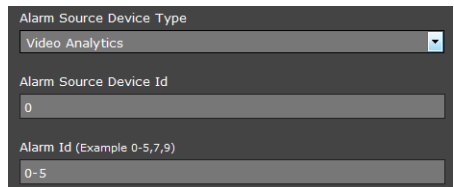
In general, each Alarm Rule describes an alarm **Source** and a single alarm **Action**. For the FC-Series ID camera, the source of the alarm typically will be internal from the camera itself, although it is also possible for the camera to receive alarms from another camera or device/server on the network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

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

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



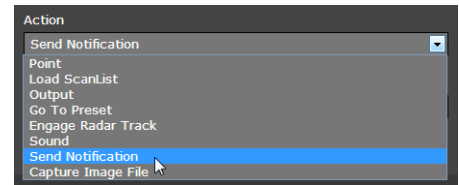
When the alarm source is Video Analytics the **Alarm ID** corresponds to the area or tripwire (1-8), as configured in the Setup menu. The **Alarm ID** is set sequentially during the setup for each alarm source. Refer to [Video Analytics Setup, pg. 48](#).



When the alarm source is from the GPIO Input the **Alarm ID** is changed to the **Input ID** and is set to 1 (recall the output is IO 0 and the input is IO 1).

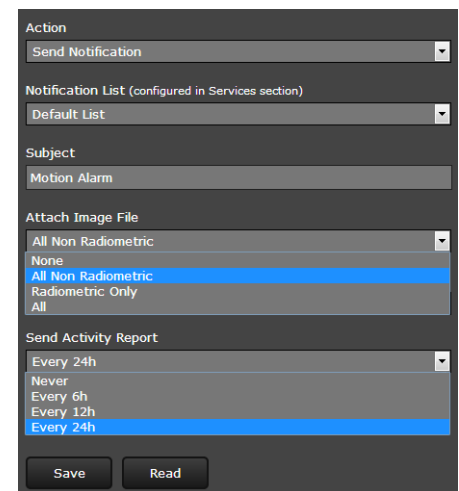


Alarm Actions: Just as there can be multiple sources of alarms, there are also a variety of actions or responses to these alarms. Some actions are only used with pan/tilt cameras. Actions such as Point, Load ScanList, Go To Preset, and Engage Radar Track would only be used with a pan/tilt camera and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



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

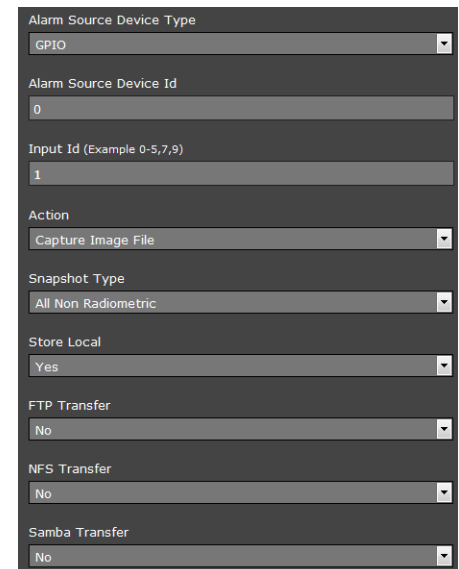
When the Alarm Action is set to **Send Notification**, a Notification List must be selected. The **Send Notification** action uses a Msg System and a Notification List that are set up in the Services menu (refer to [Msg Systems, pg. 32](#)).



To attach a snapshot, select an option from the **Attach Image File** pull down list. The option **All Non Radiometric** sends a normal JPEG image and **Radiometric** sends a radiometric JPEG (a special type of JPEG with temperature data). A radiometric camera model is required to capture radiometric images.

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

When the Alarm Action is set to **Capture Image File**, a snapshot is stored when the alarm occurs. The image file can be stored locally in temporary storage (the default), over the camera network using FTP (file transfer protocol) or to a network-attached storage device (NAS). Refer to [File Transfer, pg. 53](#) to configure settings for the FTP, NFS, or Samba transfers.



Locally stored images can be viewed in the media browser (see [Media Browser, pg. 65](#)). To store local images through a power cycle the camera must have a customer supplied microSD card installed.

The Snapshot type can be set to **All Non Radiometric** (a normal JPEG image) or **Radiometric** (a special type of JPEG with temperature data). A radiometric camera model is required to capture radiometric images.

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 FC-Series ID camera itself, and only the source type changes (Video Analytics or GPIO Input).

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

Enable each alarm rule

FC-Series ID Options: Video Analytics and GPIO

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

Refer to [Creating Analytics Regions, pg. 50](#)).

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 [Msg Systems, pg. 32](#)). The email includes alarm information, including the Area ID and if it is a human or vehicle alarm. When an email is sent, the Alarm Manager can attach a snapshot from the camera to the email. In Attach Image File, **All Non Radiometric** is selected for the type of image since the alarm type is **Analytics**.

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. 57](#)), 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. 53](#) to configure settings for the FTP, NFS, or Samba transfers.

Locally stored images can be viewed in the media browser (see [Media Browser, pg. 65](#)). To store local images through a power cycle the camera must have a customer supplied microSD card installed.

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

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

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. 57](#)).

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.

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

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): 0

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

3.2.2 Files Menu

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

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

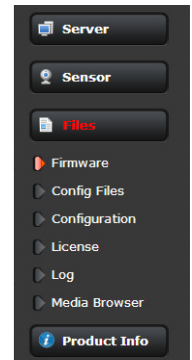
Caution!

The firmware update procedure resets the FC-Series ID camera to default settings.

Before performing the update, detach the camera from any VMS.

A firmware update resets video settings, IR settings, and rules to factory defaults. Analytics are disabled in factory default.

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



The screenshot shows the FLIR web interface with the following content:

FLIR Live Video Setup Maintenance Help admin Log out 03/26/2014 03:41:41 pm

Files (highlighted in the left sidebar)

Nexus Configuration File

```
[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 Type=1
Server Name=FC-632-R-NTSC.ini
INI version=131
```

Refresh

Backup & Recovery

Name	Date	Restore	Delete
factory.defaults	-	Restore	
FC-632-R-NTSC.ini	March 24, 2014	Restore	Delete

Backup name: Backup

Upload & Download

Browse Upload Download

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.

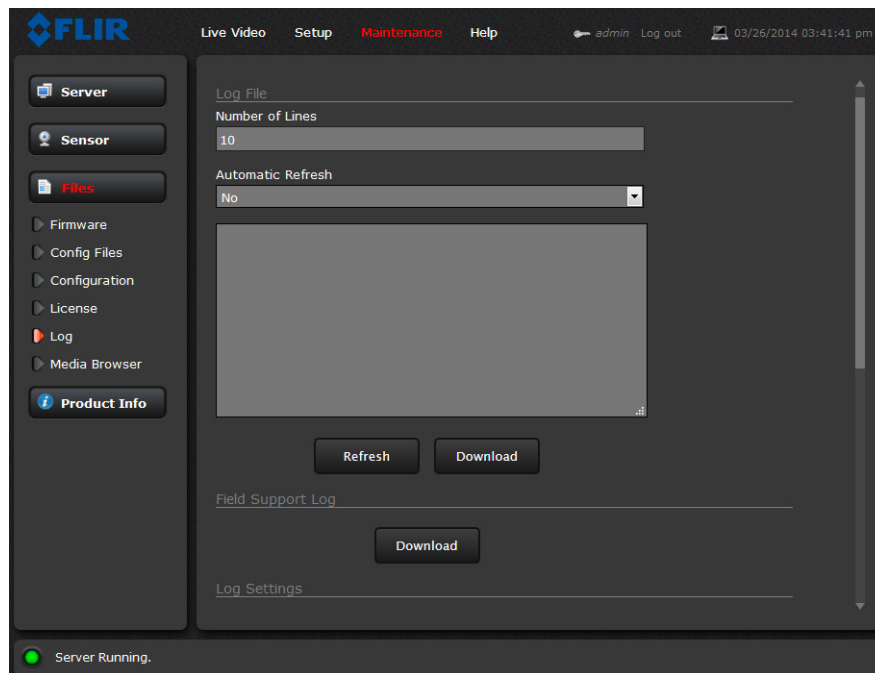
In the Backup & Recovery section, click the Restore link associated with the factory.defaults configuration to restore the camera to its factory settings. This file can not be modified or deleted, so it is always available.

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.

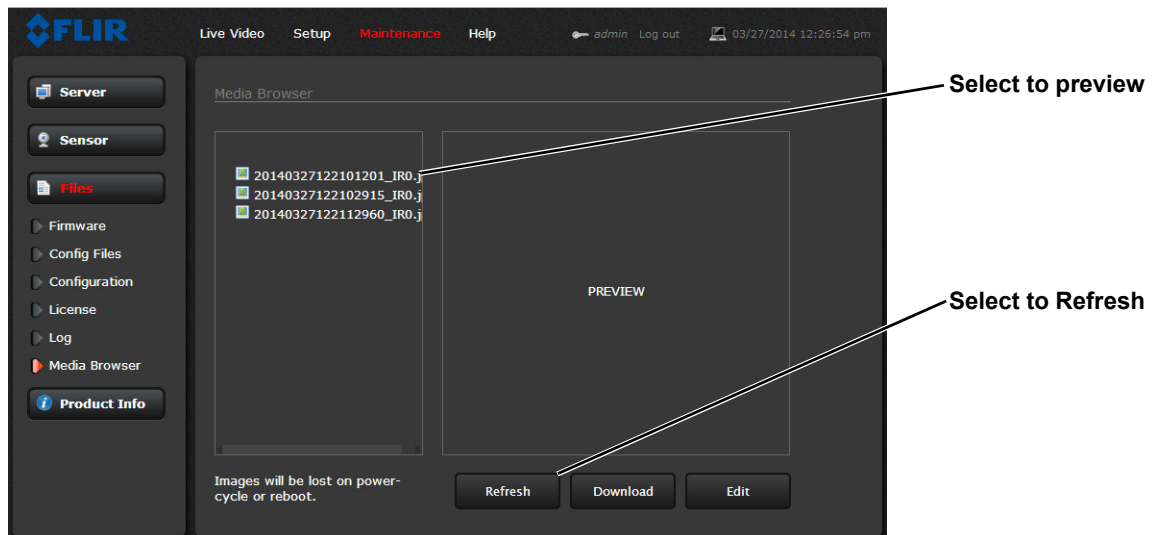
In the Upload & Download section, the **Download** button can be used to save a copy to a PC for safe keeping. A pop-up window will ask for a file name and destination folder.

The **Upload** button is used to transfer a configuration file from a PC to the camera.

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.



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

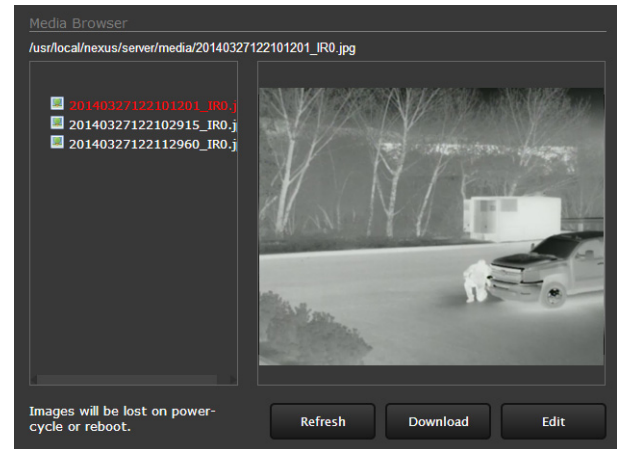


After selecting a file, the file will appear in the Preview window.

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

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

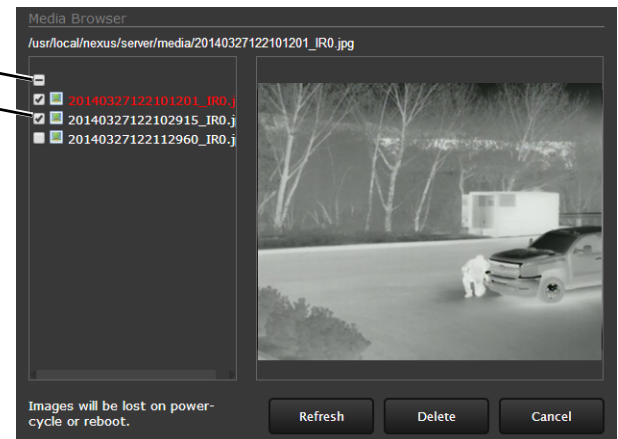
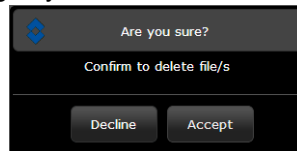
Select Edit to select and delete individual images or all images. Any time the camera is rebooted or the power removed, the media directory will be emptied.



Select All
Select Individually

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

The following prompt will appear prior to deleting any files.

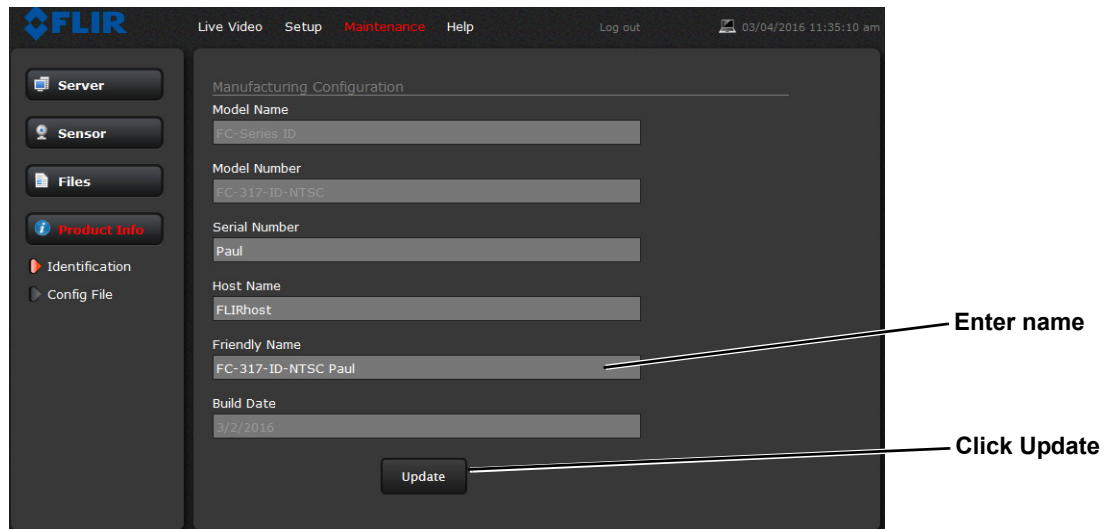
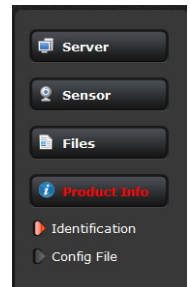


3.2.3 Product Info Menu

The **admin** functions accessed through the **Product Info** menu on the left side of the page are shown. Selected actions from the **Identification** page are described below.

Use the **Identification** page to change the Friendly Name which appears in FLIR Latitude by default. You can also include the Friendly Name on the video feeds and adjust its appearance on the OSD page (refer to [On Screen Display, pg. 59](#)).

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



Manufacturing Configuration

Model Name
FC-Series ID

Model Number
FC-317-ID-NTSC

Serial Number
Paul

Host Name
FLIRhost

Friendly Name
FC-317-ID-NTSC Paul

Build Date
3/2/2015

Update

Enter name

Click Update



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

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

Support:
<http://www.flir.com/security/display/?id=71083>

Document:
427-0089-00-12
Version: 130
Date: March 2017