Installation and User Guide

PT-Series AI SR

427-0075-01-12 Revision 110 September 2025

For additional information visit www.flir.com or write to:

Teledyne FLIR LLC
Antennvägen 6
PO Box 7376, SE-187
15 Täby
Stockholm County, 187 66
Sweden
Support: https://support.flir.com/

Important Instructions and Notices to the User:

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

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

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

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

Industry Canada Notice:

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

Avis d'Industrie Canada:

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

Proper Disposal of Electrical and Electronic Equipment (EEE)

The European Union (EU) has enacted Waste Electrical and Electronic Equipment Directive 2012/19/EU (WEEE), which aims to prevent EEE waste from arising; to encourage reuse, recycling, and recovery of

EEE waste; and to promote environmental responsibility.
In accordance with these regulations, all EEE products labeled with the “crossed out wheeled bin” either on the product itself or in the product literature must not be disposed of in regular rubbish bins, mixed with regular household or other commercial waste, or by other regular municipal waste collection means. Instead, and in order to prevent possible harm to the environment or human health, all EEE products (including any cables that came with the product) should be responsibly discarded or recycled.
To identify a responsible disposal method nearby, please contact the local waste collection or recycling service, the original place of purchase or product supplier, or the responsible government authority in the area. Business users should contact their supplier or refer to their purchase contract.

Document History

Version	Date	Comment
100	April 2025	Initial FLIR Release
110	September 2025	Various Fixes

PT-Series AI Camera Installation

Basic Operation and Configuration

1

PT-Series AI Camera Installation

The PT-Series AI pan/tilt thermal security camera for medium- to long-range applications can be used with IP video networks. It incorporates a high-sensitivity thermal camera with a choice of lenses and a long-range daylight camera all within a precision pan/tilt platform.

This manual describes the installation of the PT-Series AI cameras. If help is needed during the installation process, please refer to https://www.flir.com/support/ for support. All installers and integrators are encouraged to take advantage of the training offered by FLIR; visit https://www.flir.com/support-center/training/ for more information.

This manual includes the following topics:

- Installation overview
- Mounting the camera and its components
- Connecting the electronics
- Bench testing the camera
- Configuration and operation of the camera
- Camera specifications

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

Warning!

If mounting the 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 camera for any reason. Disassembly of the camera (including removal of the cover) can cause permanent damage and will void the warranty.

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

The camera requires a power source of 24 VDC, which is supplied with the camera. Other voltages can cause permanent damage to the camera.

FLIR Security PTZ Pairing Guide for DX-Series, DM-Series, and Quasar 4K PTZ Cameras

1.1 Camera Overview

The PT-Series AI camera is an IP camera. The video from the camera can be viewed by streaming it over an IP network using MJPEG, H.264, or H.265 encoding. The IP video will require a connection to an Ethernet network switch and the appropriate software for viewing the video stream.

1.2 Installation Overview

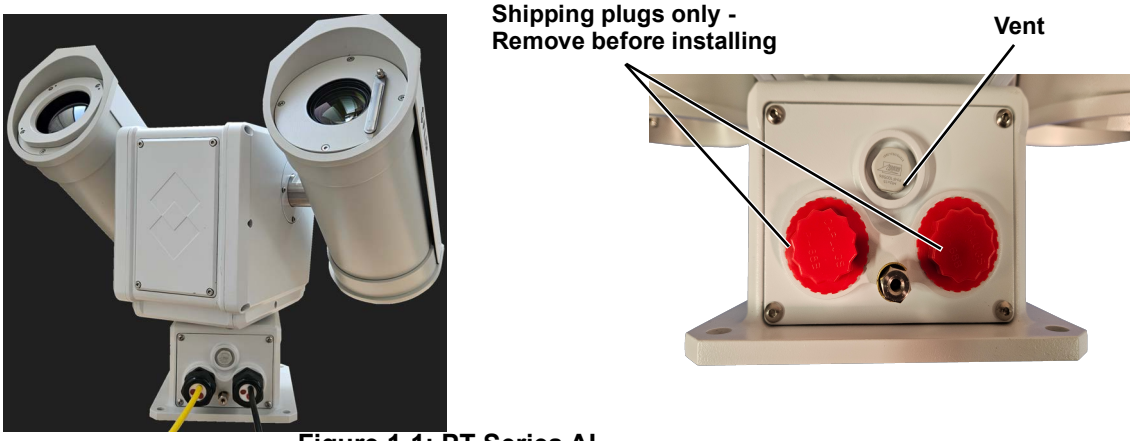


Figure 1-1: PT-Series AI

The PT-Series AI camera is intended to be mounted outdoors on a medium-duty fixed pedestal mount or wall mount commonly used in the CCTV industry. Cables will exit from the back of the camera housing. The mount must support up to 45 lbs (20 KG). The camera can be controlled through IP communications. The camera operates on 24 VDC.

In order to access the electrical connections and install the cables, it is necessary to temporarily remove the back cover of the camera housing. Ensure the back cover is replaced in the same orientation, with the two cable glands below the central pressure equalization vent.

1.2.1 Camera Connection Options

Camera connections are made through water-tight cable gland seals on the rear of the camera. Refer to Cable Gland Sealing, pg. 10 to ensure the glands are used correctly and the connections are sealed.

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

It is recommended to install an Ethernet cable to allow easy remote access for camera configuration, operation, and troubleshooting.

1.2.2 Supplied Components

The PT-Series AI camera ships with these standard components:

- Multi-sensor pan/tilt camera unit
- Galvanic isolation kit (PN 4204960)
- Noise suppression ferrite
- Cable glands and spare parts kit

1.2.3 Required Components

The installer will need to supply the following items; the cable lengths are specific to the installation.

Note

A single ferrite is supplied with this equipment, the equipment was tested for compliance with the FCC limits for a Class A digital device using the ferrite installed on the system power cable. When connecting the power cable to the equipment, the supplied ferrite must be installed with this equipment.

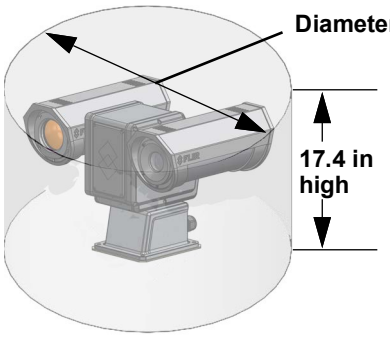
- Camera grounding strap
- Shielded CAT6 Ethernet cable for streaming video, control, and for software updates. Shielded CAT5e Ethernet cable may be adequate in many installations except when closely installed with power cables in demanding video streaming networks.
- Miscellaneous electrical hardware, camera mount (with stainless steel washers and bolts), connectors, and tools

1.3 Location Considerations

Install the camera in a location that will allow access for regular periodic cleaning (fresh water rinse), inspection of mounting integrity and mechanical soundness, and preventative maintenance. Ensure the camera and the camera mount are routinely inspected on a periodic basis.

The camera will require a connection for power, and communications (IP Ethernet).

- Ensure the 360° pan and 180° tilt exclusion zone is free of all obstructions.
- Install all cameras with an easily accessible Ethernet connection to support future software updates.
- Ensure that cable distances do not exceed the specifications and that cables adhere to all local and industry standards, codes, and best practices.



Maximum keep-out cylinder

1.4 Bench Testing

Connect the power and Ethernet connections and confirm that the video is displayed on a monitor when the power is turned on. Confirm the camera can be controlled by moving it (pan/tilt). For configuration and basic setup information using the onboard web server.

1.5 Camera Mounting

Caution!

- Ensure that the camera base is electrically isolated and properly grounded when it is secured to its mount. Contact between the stainless steel fasteners and any bare aluminum may cause galvanic corrosion which will shorten the life of the installation and may void the camera warranty.
- The camera needs to be installed properly leveled in all three axes for better operational accuracy. This helps to avoid wear out of the mechanical components.
- The camera should be installed on a location which is not reachable by users.
- When lifting the camera use the camera body and base, not the tubes.

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

Galvanic isolation is critical in preventing corrosion. Proper installation of galvanic isolation pad and washers is important for long product life.

There are two critical steps related to proper galvanic isolation camera mounting:

- Installation of galvanic isolation kit
- Proper grounding (bonding) to earth ground

1.5.1 Galvanic Isolation

The Galvanic Isolation Kit (FLIR PN 4204960) is for use with all PT-Series AI cameras. The isolation plate and nylon shoulder or flat washers provide electrical isolation between the stainless steel fasteners and the aluminum camera base, and electrically isolates the complete PT-Series AI camera from the customer mount. Galvanic isolation is critical in preventing corrosion. Proper installation of galvanic isolation pad and washers is important for long product life. Refer to the Installation of Camera and Galvanic Isolation Kit, pg. 5 for specific instructions.

1.5.2 Earth Ground Connection

Earth ground connection is very important to protect PT-series from surge induced failures and corrosion caused by stray current/ground loops. Attach ground wire (16 AWG or larger) to ground lug on access panel. Use the large hex nut to secure ground wire to stud on access panel. Ground stud is #8-32 thread.

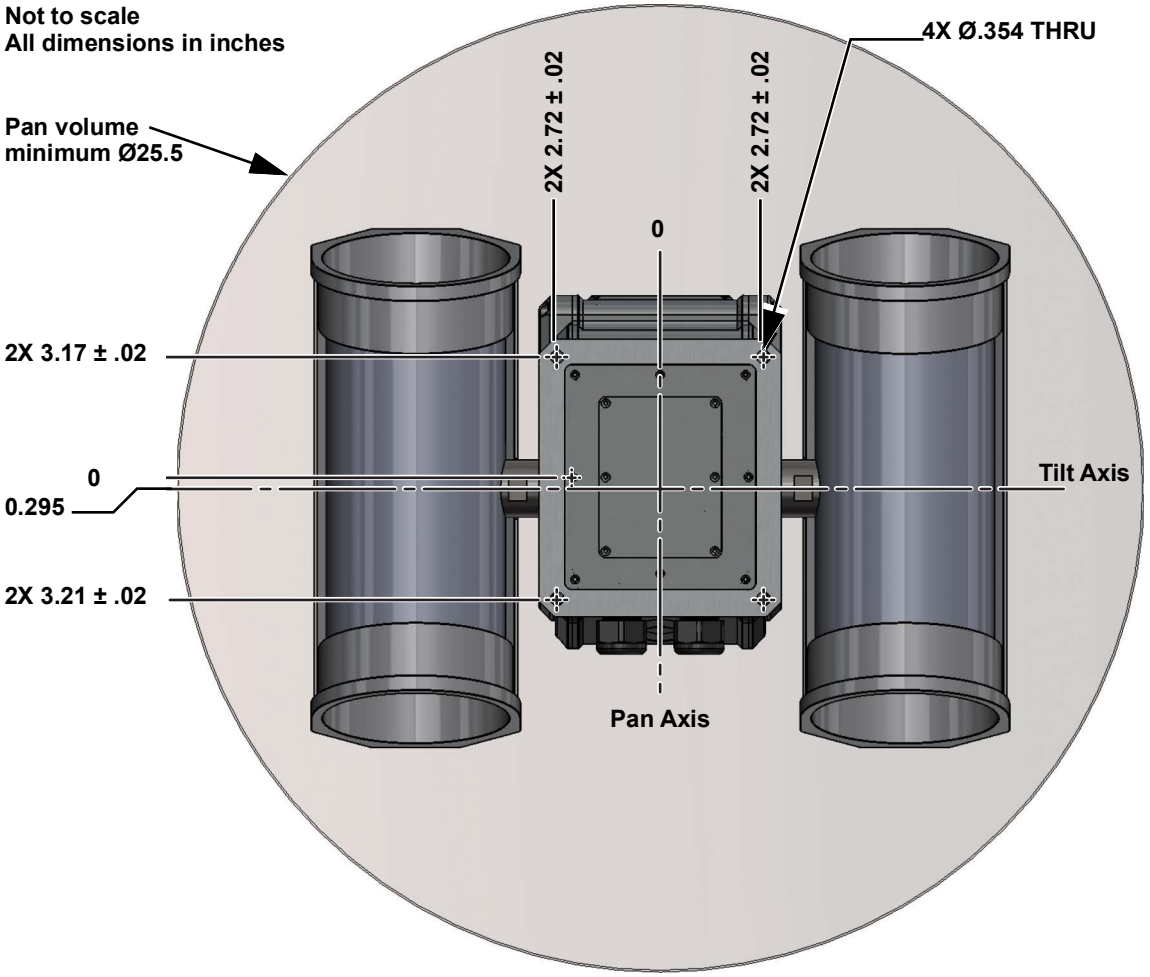


Figure 1-2: PT-Series AI Camera Mounting

1.5.3 Installation of Camera and Galvanic Isolation Kit

Important Safeguards and Warnings

- Installation and servicing should be done by qualified installation and service personnel only.
- Installation should be done according to all local and national electrical and mechanical codes, using only approved materials.

Warning!

Before drilling into walls or ceilings for mounting the camera, verify that areas behind these positions do not contain electrical or other utility service lines. Serious injury or death may result from failure to heed this warning.

- Once the mounting location has been selected, verify both sides of the mounting surface are accessible and free of utility service lines or other obstructions.
- Use stainless steel hardware to fasten mounts to outdoor surfaces.
- Use a thread locking compound such as Loctite 242 or equivalent with all metal to metal threaded connections.
- To prevent damage from water leakage when installing outdoors, apply sealant around the bolt holes between the mount and the mounting surface.

Caution!

Following this procedure is critical to maintaining the warranty on your PT-Series AI product. Failure to follow these instructions can potentially void the camera warranty.

Table 1-1: Kit Contents

Description	Qty
Isolation plate	1
M8 nylon flat washer[1] M8 nylon shoulder washer	6 6
M8 split washer, S.S.	6
M8 washer, S.S.	6
Tef-Gel TG 0.25, 3 cc syringe[1]	optional

Two extra pieces of each attaching part are supplied in the kit.

1. Use the alternate nylon flat washers and Tef-Gel lubricant on fasteners for PT-Series AI camera bases with mounting holes that are too small to accept the shoulder washers. A syringe of Tef-Gel will be supplied in the mounting kit when the nylon flat washer is required.

Step 1 Determine the correct positioning of the isolation plate (See Figure 1-3 on page 7).

Step 2 Place the isolation plate and the camera on the mounting structure aligning the bolt holes or studs.

Step 3 Install nylon shoulder washers (4x) or nylon flat washers (4x) onto camera base. If using nylon flat washers, apply a generous coat of Tef-Gel filling all gaps and voids.

Step 4 Secure the camera using 5/16” or M8 fasteners (4x) with stainless steel flat washers and split washers on top of the nylon washers.

Step 5 Ensure the camera is properly grounded. FLIR requires using a 14 AWG to 16 AWG grounding strap anchored to the ground lug on the back plate of the camera housing and then terminated to the nearest earth-grounding point.

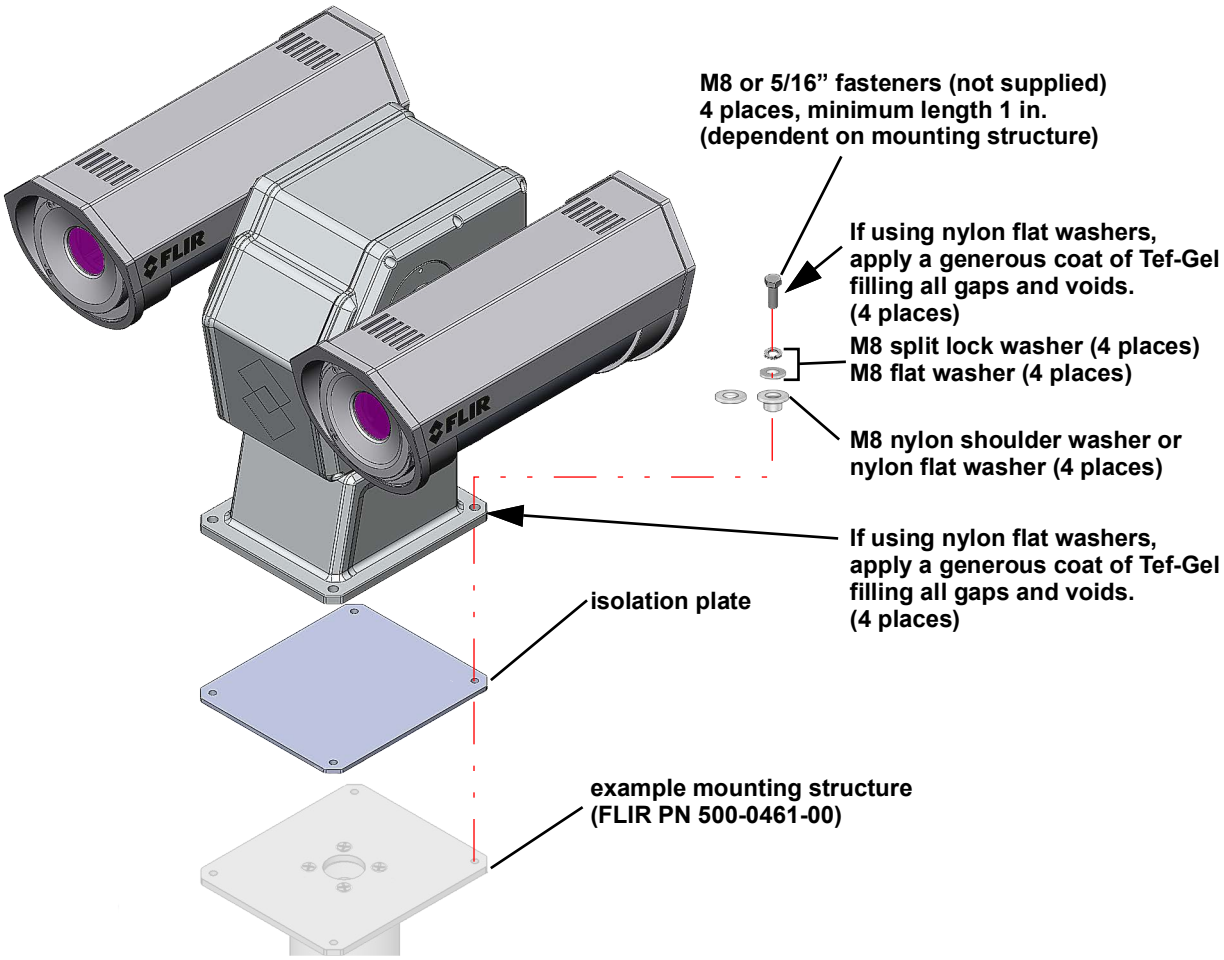


Figure 1-3: PT-Series AI Galvanic Isolation Kit (PN 4204960)

1.6 Camera Connections

1.6.1 Remove the Back Cover

Use a 2.5 mm hex key to loosen the captive screws and remove the cover, exposing the connections at the back of the camera. There is a grounding wire connected between the case and the back cover.

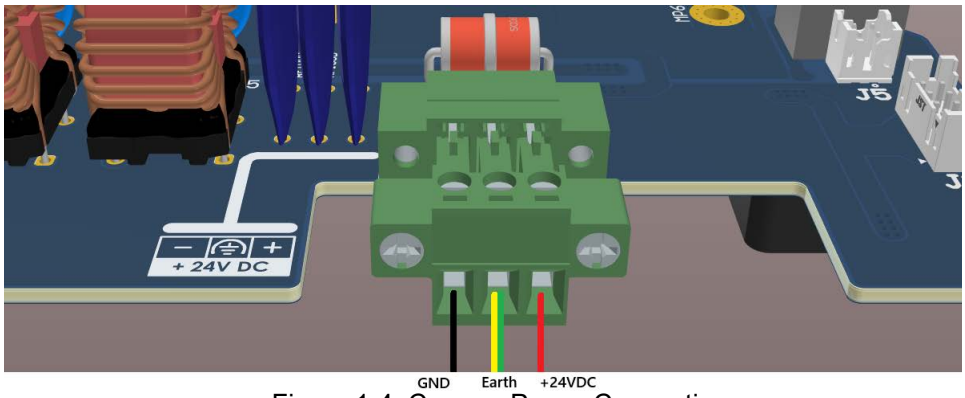


Figure 1-4: Camera Power Connections

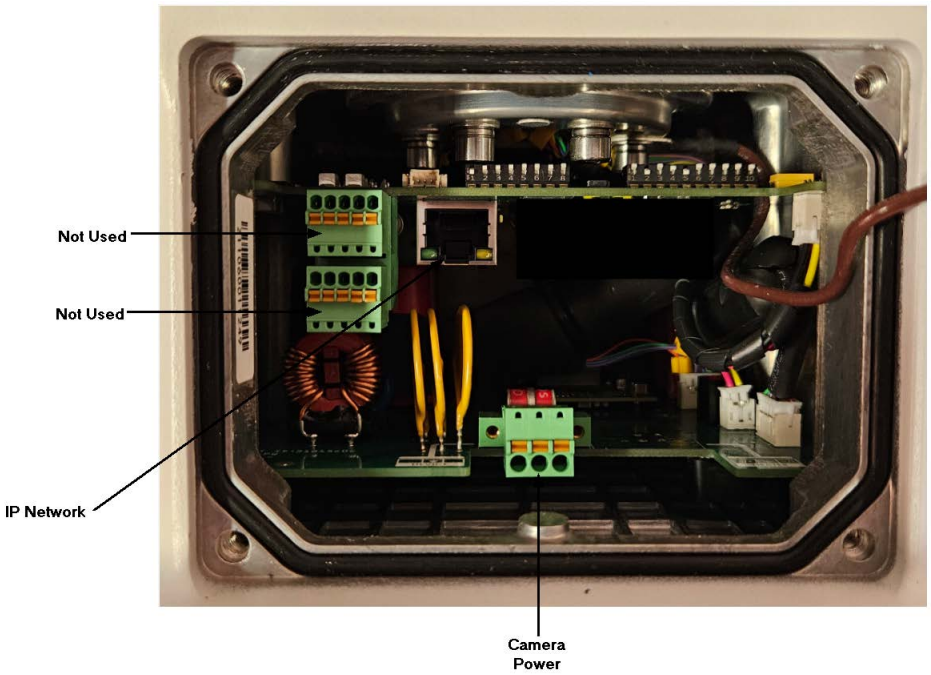
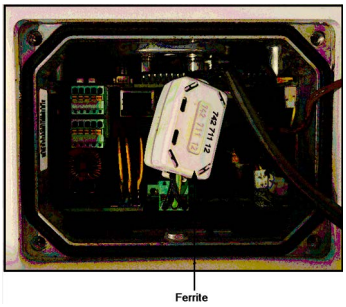


Figure 1-5: PT-Series AI Camera Connections

1.6.2 Connecting power

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

The power cable supplied by the installer must use wires that are sufficient size gauge (16 AWG recommended) for the supply voltage and length of the cable run. Use wire ferrules and crimp tooling to attach the wire to the power plug connector. Always follow local building codes!



The supplied noise suppression ferrite must be installed on the camera system power cable.

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

Note

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

Lens Heaters

The lens heaters are intended to provide lens de-fogging and de-icing in the event of:

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

The PT-Series AI cameras are shipped from the factory with the lens heaters enabled. The lens heaters are configured to dynamically maintain the camera window at a constant temperature.

The lens heaters may be turned on manually from the Live Video web page (De-Ice, De-Fog button). Refer Web Control Panel. The heaters, when turned on manually, will run for approximately one hour unless turned off either by the user (De-Ice, De-Fog button) or the thermostat control.

1.6.3 Ethernet Connection

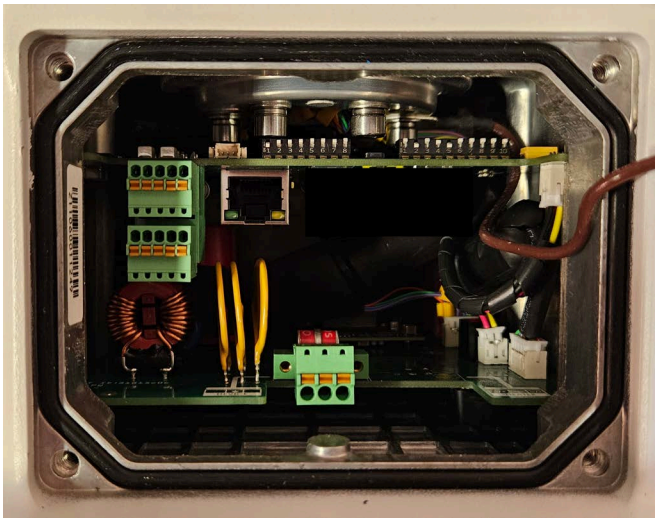
The cable gland seal is designed for use with shielded Ethernet cable.

Note

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

1.6.4 Back Cover Gasket

When preparing to re-attach the back cover, make sure that the gasket rests securely in the groove so that attaching the cover does not cut or otherwise damage the gasket. The picture below shows the black gasket properly in place.



If possible, lay the camera down to install the gasket and cover. If doing so is not possible, before installing the cover, apply a small amount of O-ring lubricant to the gasket to help hold it in place.

1.6.5 Cable Gland Sealing

Proper installation of cable sealing glands and use of appropriate elastomer inserts is critical to long term reliability. Cables enter the camera mount enclosure through liquid-tight compression glands. Be sure to insert the cables through the cable glands on the enclosure before terminating and connecting them (the connectors will not fit through the cable gland). Leave the gland nuts loosened until all cable installation has been completed. Inspect and install gland fittings in the back cover with suitable leak sealant and tighten to ensure water tight fittings. Teflon tape or pipe sealant (for example DuPont RectorSeal T™) are suitable for this purpose.

Cable Glands and Spare Parts Kit

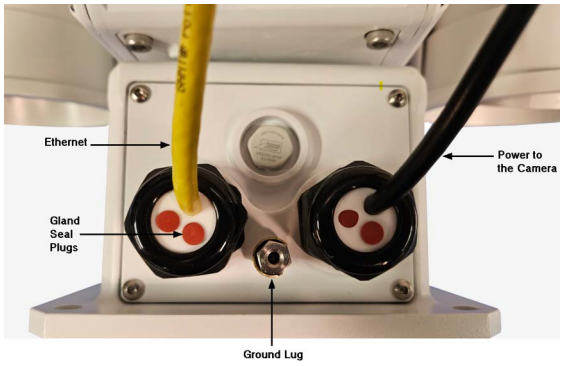
The kit contains the two 3/4” cable glands and gland seal plugs required for non-conduit installations.

The remaining parts included in the kit are:

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

Cable Gland Seal Inserts

Cables may be between 0.23" to 0.29" OD.



Up to six cables may be installed. Plugs are required for the hole(s) not being used. The photograph above shows a power cable, an Ethernet cable, and two gland seal plugs.

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

1.7 PT-Series AI Camera Specifications

Thermal Camera Specs	Array Format	640 × 512	
	Detector Type	Long-Life, Uncooled VOx Microbolometer	
	Pixel Pitch	17 µm	
	Thermal Frame Rate	30 Hz or 9 Hz depending on the model	
Optical Characteristics	**Model**	**FOV**	**Focal Length**
	PT-644 AI	44° × 36°	13 mm, f/1.0
	PT-625 AI	25° × 18°	25 mm f/1.1
	PT-617 AI	17° × 14°	35 mm, f/1.1
	PT-612 AI	12° × 10°	50 mm, f/1.2
	PT-608 AI	8.6° × 6.6°	75 mm, f/1.1
	PT-606 AI	6.2° × 5°	100mm, f/1.6
	PT-606Z AI	Uncooled continuous zoom, 24° to 6°	26-105 mm, f/1.6
	Spectral Range 7.5 µm to 13.5 µm		
	Focus Range Athermalized, Focus-Free		
Visible Camera	Sensor Type	4K (2160p), 1/1.8-type STAVIS II CMOS	
	Effective resolution	327,680	
	Lens Field Of View	59.0° (wide end) to 2.3° (tele end)	
	Zoom Focal Length F/#	25x optical zoom 6.5 mm (wide) to 162.5 mm (tele) F1.6 to F4.8	
	Wiper	Included as default	
Compliance and Certifications	ONVIF Profile S, G, T		
	IP66		
	RoHS		
	CE Marked		
	FCC		
	WEEE		

Video	Video Compression	Two independent channels of H.265, H.264 & M-JPEG for each sensor

	Streaming Resolution	• Steam V1 (visual):
		  • H.264: 3840x2160, 1920x1080, 1280x720, 640x480
		  • H.265: 3840x2160, 1920x1080, 1280x720, 640x480
		  • MJPEG: 1920x1080, 1280x720, 640x480
		• Steam V2 (visual): 1920x1080, 1280x720, 640x480
		  • H.264: 1920x1080, 1280x720, 640x480
		  • H.265: 1920x1080, 1280x720, 640x480
		  • MJPEG: 1920x1080, 1280x720, 640x480
		• Stream T1 (Thermal):
		  • H.264: 640x512
		  • H.265: 640x512
		  • MJPG: 640x512
		• Stream T2 (Thermal):
		  • H.264: 640x512
		  • H.265: 640x512
		  • MJPG: 640x512

	Thermal AGC Settings	Auto AGC, Dynamic Detail Enhancement (DDE), Sensitivity
	Thermal AGC Region of Interest (ROI)	Default Presets and User definable to insure optimal image quality for subjects of interest
	Image Uniformity Optimization	Automatic Flat Field Correction (FFC) with thermal and temporal triggers—Uncooled thermal camera only

System Integration	Ethernet	100Base-TX IEEE 802.3u
	Network APIs	NEXUS® SDK, NEXUS® CGI, ONVIF Profile S, G, T
	External Analytics Compatible	Yes
Pan/Tilt	Pan Angle/Speed	Continuous 360°; 0.1° to 60°/sec
	Tilt Angle/Speed	+90° to -90°; 0.1° to 30°/sec
	Programmable presets	256
General	Weight	37 lb (16.8 kg); configuration dependent
	Dimensions (L,W,H)	13.7” × 18.4” × 12.8” (348 mm × 467 mm × 326 mm)
	Input Voltage	24 VDC (Range 21-30VDC)
	Power Consumption[1]	Uncooled thermal camera: 24 VDC: 240W
Environmental	IP rating (dust and water ingress)	IP66
	Operating temperature range	Uncooled thermal: -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
	Altitude	Max: 2000m
	Vibration	IEC 60068-2-27, 10 g shock, 11 ms half-sine profile
	Mechanical Shock	MIL-STD-810H Transportation
	De-Icing	MIL-STD-810H, Method 521.1

1. Power consumption is independent of the input voltage when the heater is off. The power drawn by the heaters increases with the input voltage to a maximum at 30 Volts.

1.8 Safety Restrictions

Table 1-2: Safety Restrictions

Installation Environment	EUT Overall: Class A
SELV Supply	• Ethernet Port: Class A • Power Ports: Class A • No direct mains allowed
Installation	Inaccessible location
ESD Hazard symbol on sensitive surfaces	• EUT overall: Coupling planes - 2x2x10 (+/-) Contact discharge 6kV 1s • No damage or function loss (stable outputs) - indicator disturbance permissible.
Supply cables	• Maximum length 3m • Ethernet port: Line-Earth (2+40Ω): 500V & 1kV - Discharges: 2.5 (+/-) • No damage or function loss (stable outputs) - Indicator disturbance permissible • Ethernet port: 150kHz - 100MHz 1%/3s - Modulated 80%/1kHz & Pulse 100%/1Hz • 1V: No impact • 3V: Minor deterioration of the picture • 10V: Major deterioration of the picture & indicator disturbance permissible • Never damage or function loss (stable outputs)
Power supply	Must contain a UPS covering power drops >5s

1.9 Accessing the Camera

To operate the camera, you first need to access it by logging in to the camera's web page. The camera's web page supports Google Chrome® and other popular web browsers. This guide supports and reflects Chrome.

To log in to the camera's web page:

1. Do one of the following:
    - o In the FLIR Discovery Network Assistant (DNA) tool, double-click the camera in the Discover List.

      The DNA tool does not require a license to use and is a free download from FLIR. Download the DNA tool (v2.3.0.35); unzip the file; and then double-click the DNA icon to run the tool (DNA.exe). The Discover List appears, showing compatible devices on the VLAN.

- Type the camera’s IP address in a browser’s address bar (when the PC and the camera are on the same network). If you do not know the camera's IP address, you can use the DNA tool to discover it.

2. On the login screen, type a user name and the password.

   When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, you need to log in with the camera's default credentials:

   User name—admin

   Password—Flir12345678

   If you do not know the user name or password, contact the person who configured the camera's users and passwords.

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

   Use a strong password consisting of at least 12 characters and at least one uppercase letter, one lowercase letter, and one number. Passwords can include the following special characters: |@#~!$&<>+_-.,*?=.

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

4. After performing a factory reset, use the following credentials:

   User name—admin

   Password—admin

2 Basic Operation and Configuration

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

2.1 IP Camera, ONVIF Profile S Compliant

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

2.1.1 Server Configuration

It may be necessary for the installer to make a limited number of configuration changes to the camera server, such as setting the IP communication parameters, setting new login passwords, as well as some scene specific parameters. Many of the configuration parameters will remain unchanged from the factory default settings.

2.2 Camera Bench Test

Since the camera offers IP video, the installer should test the camera using the same type of connections as the final installation. 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.

Test serial communications by connecting a serial device such as a keyboard and confirm the camera is responding to serial commands. It may be necessary to configure the serial device interface to operate with the camera.

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

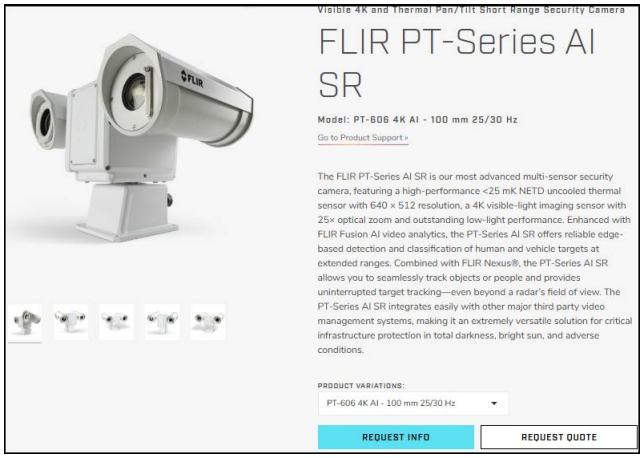
2.2.1 Accessing Product Information from the Teledyne FLIR Website

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

To access product information from the <%COMPANY_NAME%> website:

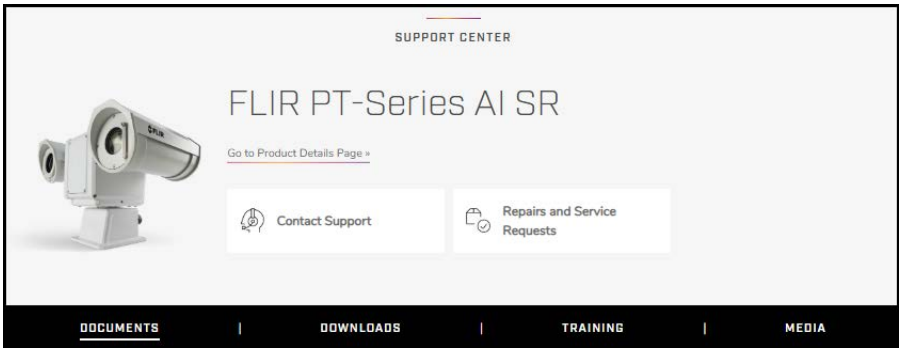
1. Open https://www.flir.com/browse/security/thermal-security-cameras/.

2. Find and click the camera. The camera's product details page appears.



To see the camera's specifications and related content, scroll down.

3. Click **Go to Product Support**. The camera's support page appears.
4. Download product documentation from the Documents tab.



Download the DNA tool from the Downloads tab.

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

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

Step 1 Connect the Ethernet port of the camera to the existing IP camera network.

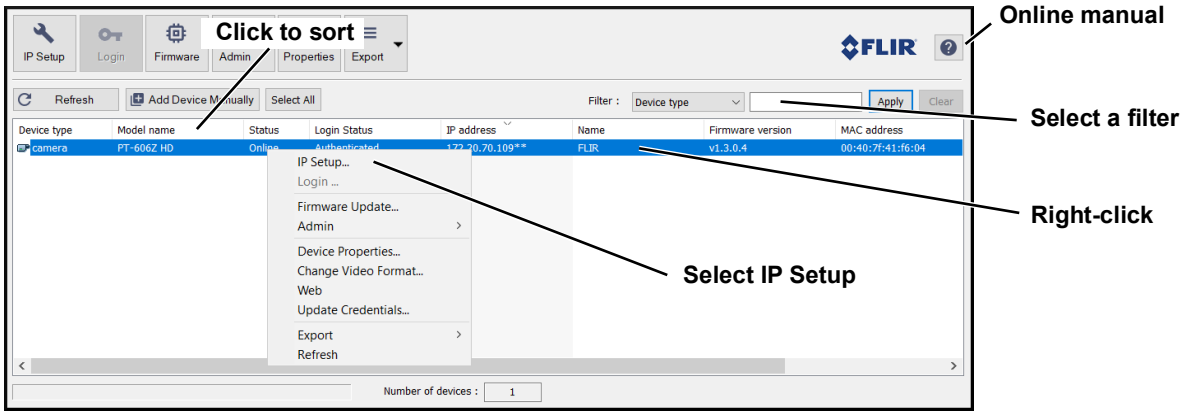
Step 2 Connect a PC or laptop to the same network.

Step 3 From the PC connected to the camera network, use the DNA utility to discover and display the camera's current IP address.

a Download the DNA utility.

b Unzip the utility, then double-click to run the executable file (**DNA.exe**). All the units on the VLAN are discovered.

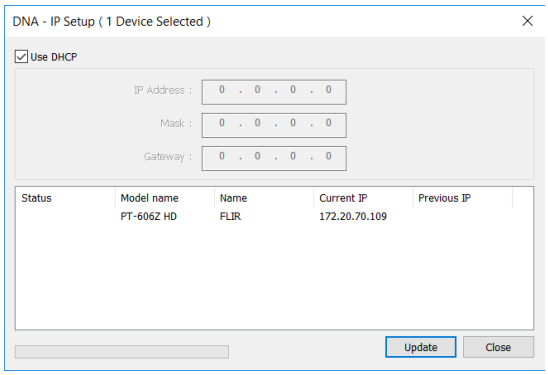
c For additional instructions on using DNA, refer to the DNA User's Manual available in the Help ( ) link while the software is running.



Step 4 Select **IP Setup** to change the IP address from the default DHCP to a static IP.

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

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



2.3 Log into the Camera Web Page

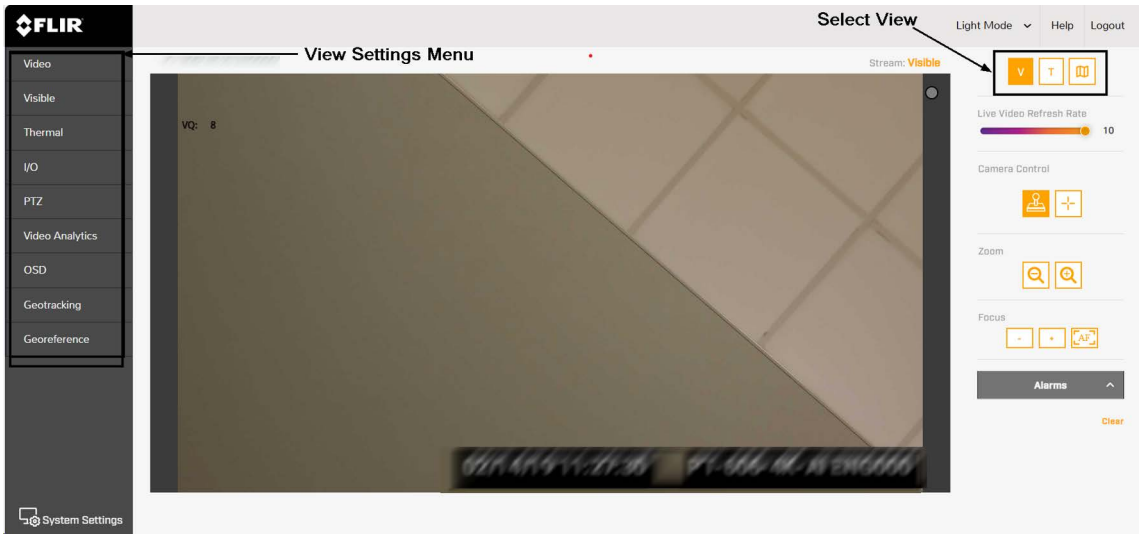
Use a web browser to connect to the camera's web server using one of three User Names: **user**, **expert**, or **admin** (the default passwords are **user**, **expert**, and **admin** respectively).

Important Note

To prevent unauthorized access, change all of the login passwords (**admin** login required).

2.3.1 View Settings Home Page

The View Settings page displays live video images of the selected view. When a user assigned the expert or admin role logs in to the camera's web page, the page also displays View Settings menus along the left side banner and other options.



Pan, Tilt, and Zoom (PTZ)

You can toggle controlling the camera's pan and tilt between:

	Emulated Joystick	When the mouse pointer is over live video, it becomes a directional arrow. To move the camera, you can: • Click and release—Moves the camera once. • Click and hold—Moves the camera until it reaches its physical limit or you release. • Click and drag—Moves the camera as you drag the mouse.
	Crosshairs	When the mouse pointer is over live video, it becomes a crosshairs. Clicking and releasing centers the camera on the crosshairs location.

You can zoom in and out using:

• The onscreen buttons—Click once or click and hold for continuous zoom.

• The mouse wheel, when the mouse pointer is over live video.

System Settings and Other Options

Users assigned the admin or expert role can click **System Settings** to configure the camera. For more
information, see the Configuration chapter.

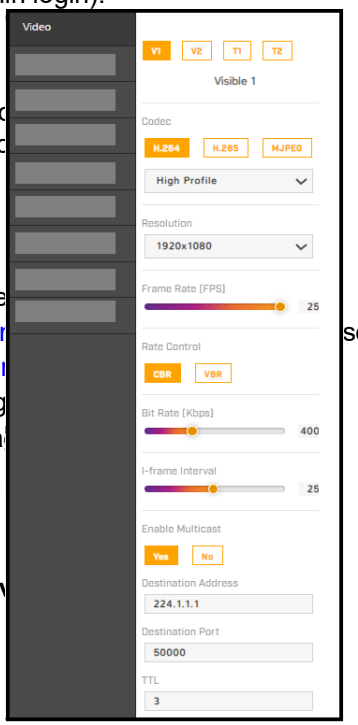
Additional choices are for Help and Logout.

Help

The **Help** menu displays software version information. If it is necessary to contact FLIR Technical Support for assistance, it will be helpful to have the information from this page on hand. For information about the camera including hardware part numbers and serial numbers refer to the Maintenance > Product Info > Identification web page (requires Admin login).

Log out

Use this button to disconnect from the camera and stop the display c
session is inactive for 20 minutes, it will be stopped and it will be nec



2.3.2 Making Changes to Settings

The camera's configuration files store the following sets of settings:
• **Factory default settings—**The settings when you first connect the
resetting the camera to its factory default settings (see Firmware & I
restores all factory default settings except the settings on the Networ
• **Saved settings—**The settings you save as you operate and config
camera reboots, it restores these settings. Changes made to any pa
lost.

set

2.3.3 View Settings

When you make a change to most View Settings, the **Reset** and **Sav**

For some View Settings, the camera immediately applies the changes, but does not save them; for example, on the Visible Page and on the Thermal Page. For others, the camera does not apply changes until you save them.

Regardless of whether the camera has already applied changes, to save all changes since the last time these settings were saved, click **Save**. This can include earlier changes that were not saved. To restore previously saved settings or the factory default settings, click **Reset**. To close the message and return to the page without restoring settings, click the close icon .

2.3.4 System Settings

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

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

Changes.

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

2.4 Video Page

The camera provides four video streams: two visible streams (V1 and V2) and two thermal stream (T1 and T2). Video streams are available for viewing using a client program or third-party ONVIF systems.
In general, it is not necessary to modify the default parameters. In some cases, such as when an IP video stream is sent over a wireless network, it can be useful to tune the video streams to reduce the bandwidth requirements. To modify the parameters for a particular video stream, click the relevant button (V1, V2, T1, or T2).

Visible 1 / Visible 2
Codec options for the visible streams are H.264, H.265 or MJPEG.

Resolution options are 3840x2160 (4K), which is available only on V1; 1920x1080 (1080p); 1280x720 (720p); and 640x480 (480p). The Frame Rate range is 5-25 FPS (frames per second).

Thermal 1 / Thermal 2
Codec options are H.264, H.265 or MJPEG.

The resolution is 640x512 and the Frame Rate range is 5-30 FPS.

Codecs, Quality, and Bandwidth
The codec used determines which parameters you can set that have a significant impact on the quality and bandwidth requirements of the video stream. Use the default values initially, and then individual parameters can be modified and tested incrementally to determine when bandwidth and quality requirements are met.

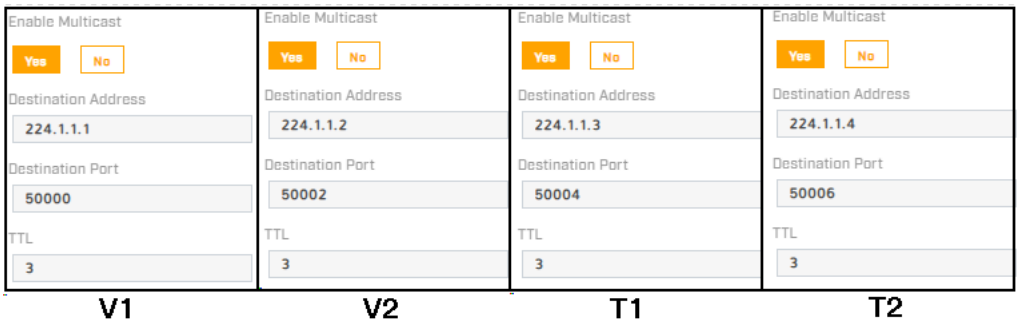
With the H.264 and H.265 codecs, you can set the:

- Profile:
  - o Main Profile
  - o High Profile
- Rate Control:
  - o CBR (constant bit rate): The Bit Rate parameter defines the target bit rate; the camera attempts to keep the video at or near the target bit rate.
  - o VBR (variable bit rate): The Bit Rate parameter defines the average bit rate.
- I-frame Interval: Controls the number of P-frames used between I-frames. I-frames are full frames of video and the P-frames contain the changes that occurred since the last I-frame. A smaller I-Frame Interval results in higher bandwidth (more full frames sent) and better video quality. A higher I-frame Interval means fewer I-frames are sent and therefore can result in lower bandwidth and possibly lower quality.

With the MJPEG codec, you can set the Quality between 0-100. Setting a higher value can increase the video stream's bandwidth requirements.

Network Options

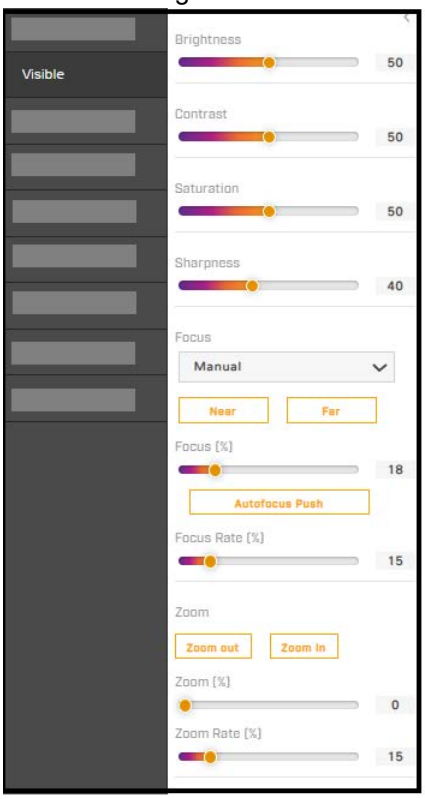
By default, multicast is enabled. Multicast video packets are shared by streaming clients. Additional clients do not cause bandwidth to increase as dramatically as with unicast. Video stream requests for ch0/stream1 are unicast. Client-specific multicast requests vary according to the client.



If more than one camera is providing multicast streams on the network, make sure the Destination Network IP address is unique for each camera (the Destination Port can be reused). By default, the port assignment is unique per stream. The time-to-live field controls the ability of IP packets to traverse network boundaries. A value of 1 restricts the stream to the same subnet. Greater values allow increasing access between networks.

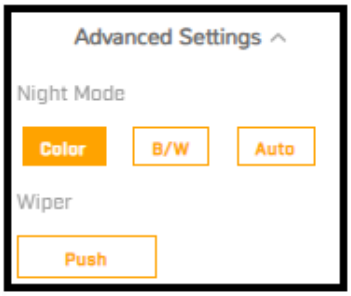
2.5 Visible Page

You can adjust the following visible video settings:



- **Brightness** (Gamma)
- **Contrast** (Max Gain)
- **Hue**
- **Saturation**
- **Sharpness**
- **Focus**—Select Auto for continuous auto-focus: The camera automatically and continuously maintains focus regardless of view changes. To manually focus the camera, select **Manual** and then click **Near** or **Far**.

Advanced Settings

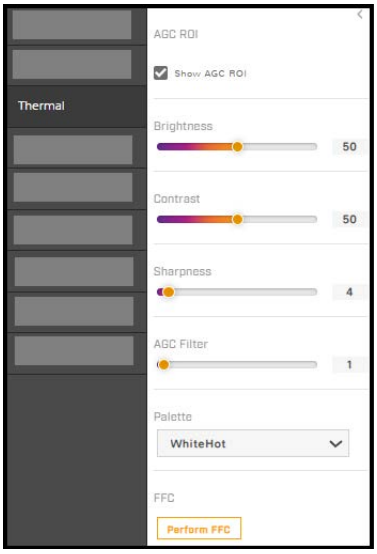


- **Night Mode**—Set the visible video to:

o **Color** (day mode)
o **B/W** (night mode)
o **Auto** (default)—Automatically switches the visible video mode according to light level. When Night Mode is set to Auto, you can set the thresholds at which the visible video switches from black and white to color (Night to Day Threshold) and vice versa (Day to Night Threshold). Move the sliders between 0-100, where 0 switches modes at a lower light level (darker) and 100 switches modes at a higher light level (brighter).

- **Wiper**—Click **Push** to start the wiper.

2.6 Thermal Page



In most installations, it is not necessary to change the default settings of the thermal sensor. However, in some situations, depending on weather, time of day, or scene, modifying one or more parameters can improve the video stream image. Be aware that, when the conditions change, the parameters might need to be adjusted again. It is also a good idea to know how to restore the factory default settings.

AGC ROI
The camera's Automatic Gain Control (AGC) algorithm adjusts the thermal video according to the region of interest (ROI). By default, **Show AGC ROI** is selected and the AGC ROI appears as an overlay in the live video on the camera web page. The AGC ROI overlay does not appear in the video stream itself.

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

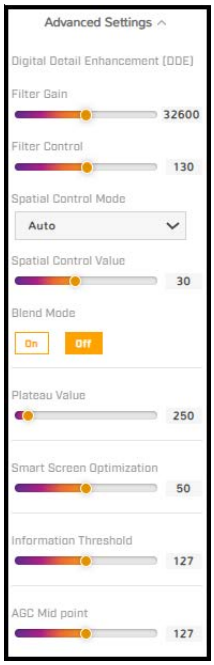
- **Brightness** (Gamma)—Determines the allocation of the 256 “shades of gray” produced by the AGC. Values above 50 allocate more shades of gray to hotter objects, while values below 50

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

Tip: Changes to the default contrast setting affect scenes with little temperature variation more than they affect scenes with greater temperature variation.

- **Sharpness** (DDE Gain)—Enhances image details and/or suppresses fixed pattern noise. Range 0 to 100.
- **AGC Filter**—Determines how quickly a scene adjusts when a hot object appears (or disappears) within the AGC ROI. If set to a low value, when a hot object enters the ROI, the AGC will adjust more slowly to the hot object, resulting in a more gradual transition. Range 0 to 100.
- **Palette**—Provides a selection of palettes for representing the detected levels of thermal energy as colors or gray-scale values. WhiteHot and BlackHot are grayscale palettes; other palettes assign different colors to different temperatures.

Advanced Settings
Digital Detail Enhancement (DDE)



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

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

In Automatic Spatial Control Mode, the camera automatically sets the Filter Gain value.
Filter Control—Also known as DDE Threshold, determines how much detail the algorithm enhances in Manual Spatial Control Mode. Specify a value between 0-255. The DDE algorithm does not enhance details above the specified value. Specify a value between 0-255. In Automatic Spatial Control Mode, the camera automatically sets and adjusts the Filter Control value according to scene content.
Spatial Control Mode—Automatic (default) or Manual. For all users and applications, FLIR recommends Automatic, also known as Dynamic DDE. FLIR strongly recommends not using Manual.
Spatial Control Value—Controls the Automatic Spatial Control Mode. Range -20 to 100. 0 (zero) is

neutral and the DDE filter has no effect. Decreasing the value below 0 softens the image, reducing sharp edges. Typical factory settings are between 10 and 30.

Blend Mode—The camera attempts to suppress halos caused by DDE. The default is Off (disabled).

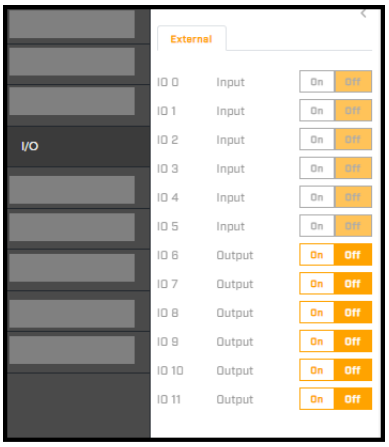
Plateau Value—The number of shades the AGC algorithm devotes to large areas of similar detected temperature in a given scene. Decreasing plateau value increases contrast and detail in the other areas of the scene; that is, decreasing the number of shades AGC allocates to those large areas increases the number of shades the algorithm allocates to other areas of the scene. Because AGC ROI has minimum size limitations that rely on plateau value, if you decrease the plateau value and have a very small AGC ROI, you might need to increase the AGC ROI to preserve proper AGC corrected video. Range 0 to 4095.

Smart Screen Optimization—Percentage of the AGC histogram allotted a linear mapping; helps provide the highest level of perceived contrast in every scene. Increasing SSO increases how well the radiometric aspects of an image are preserved; that is, the difference in shades between two objects is more representative of the difference in detected temperature. Range 0 to 100.

Information Threshold—Defines the difference between neighboring pixels the AGC algorithm uses to determine whether the local area contains *information*. Decreasing the threshold increases the amount of information the algorithm determines to be present in the scene. Increasing the threshold decreases that amount and results in a more information-dependent image. Flat portions of the scene - for example, sky or sea - are given less contrast, and pixels exceeding the information threshold are given more contrast. Range 0 to 255.

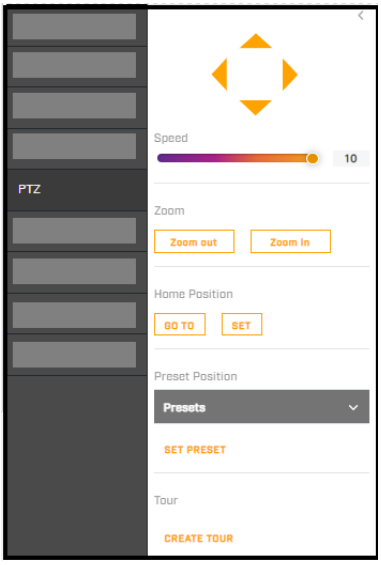
AGC Mid Point—Determines the temperature represented by the middle of the 256 shades the AGC produces. Increasing the value increases detail in hotter scenes; decreasing the value increases detail in lower temperature scenes. Range 0 to 255.

2.7 I/O Page



For external I/O connections, set the current state for the input and output pins.

2.8 PTZ

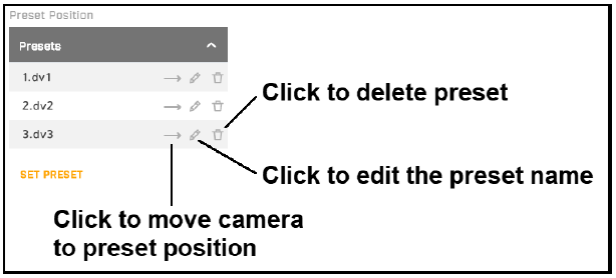


Use the PTZ page to:

- Move the camera left, right, up, or down (pan and tilt)
- Define the pan and tilt speed, between 1x-10x
- Zoom in and out—click once or click and hold for continuous zoom
- Go to the camera's home position
- Set the camera's current position as its home position
- Define preset positions:
  a. Under Preset Position, click **Set Preset**.
  b. Select a preset index number from 1-128.
  Selecting an index number currently associated with a preset position overwrites the existing presetposition.
  c. Specify a unique, descriptive name for the preset position.
  You can use alphanumeric characters, underscores (_), or dashes (-).
  d. Click **Set**. The camera adds the current position as a preset.

1. Move the camera to a preset position, edit a preset name, or delete a preset:

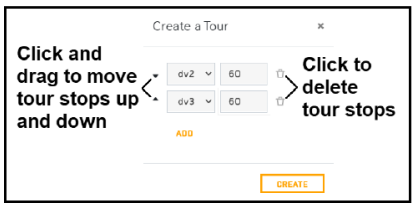
Under Preset Position, click **Presets**.
The list of presets appears, in ascending index number order.

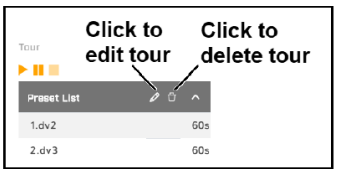


2. Create and manage a tour of preset positions (only available if presets have been defined):

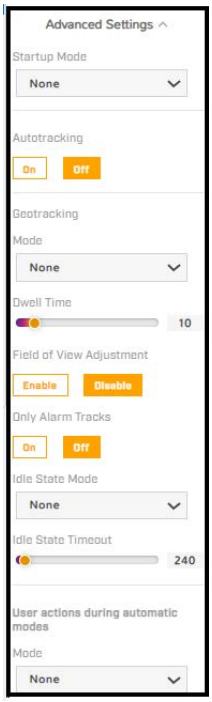
To create a tour, click **Create Tour**. For each tour stop, click **Add**, select a preset, and define the amount of time in seconds the tour stops at the preset. You can also move tour stops up or down in the list and delete tour stops.

After you create a tour, you can start ▶, pause ⏸, stop ■, edit, or delete it.





Advanced Settings
Startup Mode—
o **None—**Factory default home position.
o **Home Position—**User-defined home position.
o **Tour—**Automatically starts tour of preset positions.
o **Track Scan—**The camera performs a tour scanning all active geotracks. It follows each geotrack for a specified dwell time.
o **Track Last—**The camera follows the most recently detected geotrack.
o **Track Closest—**The camera follows the geotrack closest to the PTZ camera.

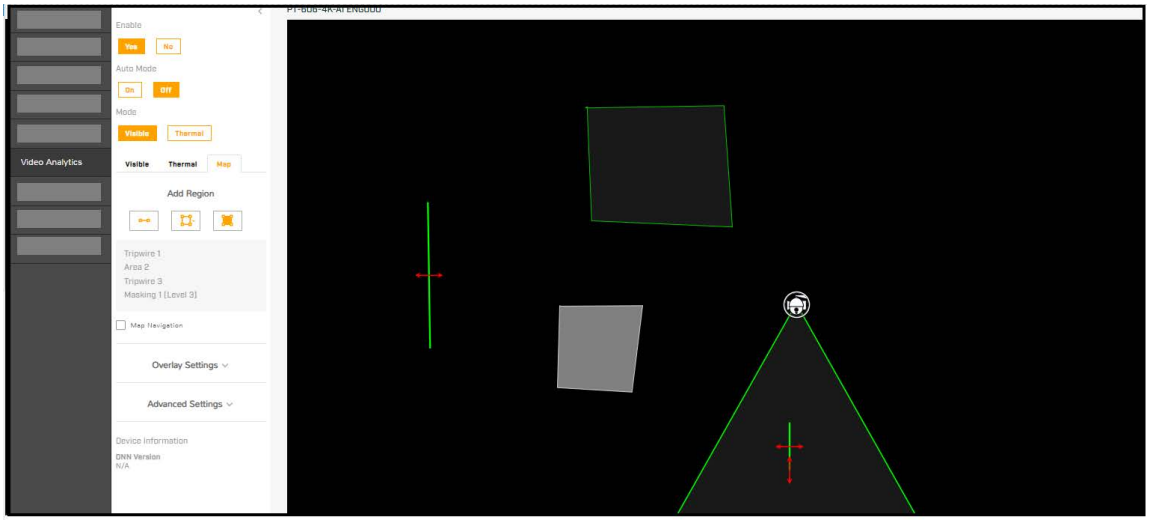


When the camera is paired with a FLIR Security Edge device that supports geotracking, you can specify a geotracking mode.

Geotracking Mode
o None—Factory default home position.
o Engage Last—The last track ID detected from fixed cameras with VA or radar.
o Engage Closest—The track ID closest to the camera provided from fixed cameras with VA or radar.

Dwell Time—Maximum amount of time, in seconds, the camera triggers an alarm (1-100), which can affect auto tracking if enabled. The default is 10.

2.9 Video Analytics



On the Video Analytics page, users assigned the Admin or Expert role can:

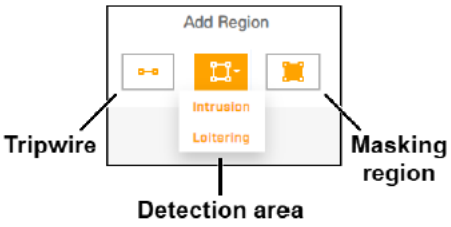
• Enable, schedule, and configure two video analytics (VA) profiles; that is, two VA rules can be simultaneously active. When Defining an Alarm Trigger, you can select a VA profile. To enable one or more of the schedules configured on the Schedule Page, select **By schedule**.

You can also enable and disable VA alarms, or specify VA alarm schedules, on the Alarm Page.

- Enable, for each profile:
  - o **Show Triggered Only—**Only detected objects that are triggering alarms appear in the display and in video streams. When set to No (default), all detected objects appear. Only available when the Stream Video Analytics Overlay setting on the OSD Page is On.
  - o **Motion Events—**Determines whether the rule selected for the profile generates motion events in addition to VA events. The default is On.
- Select and configure the analytics rule appropriate for the physical scene according to the main objective in securing the area.

To create a region:

1. Select the Map tab.
2. Under Add Region, click the appropriate icon to create:
   a. Tripwire
   b. Detection area
      i. Click on the detection area dropdown. Two options appear - Intrusion and Loitering.
   c. Masking region
3. Specify each point of the region by clicking and releasing on the live video image.
   • Do not click and drag.
   • Do not draw one region line or border over another.
   • For both the visible and thermal video, you can create:



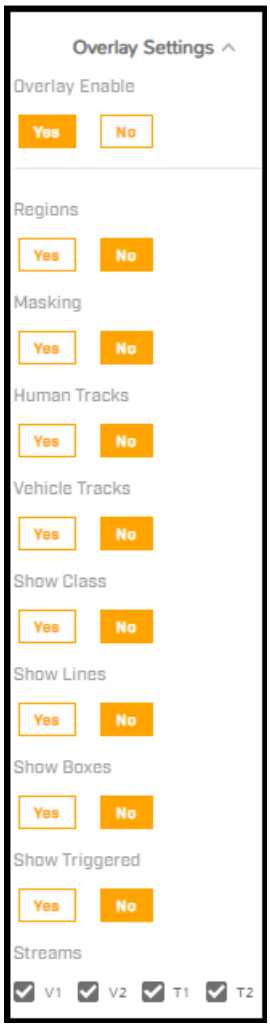
o up to two loitering detection areas
o up to eight tripwires or intrusion detection areas

• For each region, the maximum number of points is 16.

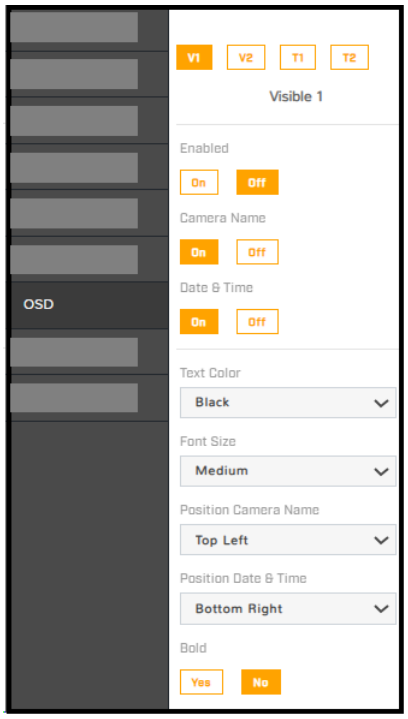
4. To finish creating the region, double-click on the last point.
5. To cancel creating a region, press **Esc**.
6. To modify the settings for or to delete an existing region, click the region either in the region list or in the live video image.
   o To move or adjust the region points, tripwires, or an entire region, click on a point, line, or border, and drag.
   o To delete a region, click the trash icon

2.9.1 Overlay Settings

Table 2-1: Overlay Settings

	Setting	Description	Comments
	Overlay Enable	Globally enable or disable the VA overlay.	Enable one or more individual streams.
	Regions	Show intrusion regions, loitering regions, and tripwires.	
	Masking	Regions of the video image in which VA is disabled and no alarm is triggered.	
	Human Tracks	Show detected objects classified as humans.	Enable Show Class, Show Lines, or Show Boxes.
	Vehicle Tracks	Show detected objects classified as vehicles.	
	Show Class	When tracks are enabled, show the classification of the detected objects: human (H) or vehicle (V).	
	Show Lines	When tracks are enabled, show the lines for the detected objects according to positions from prior frames; helps visually represent speed and direction.	
	Show Boxes	When tracks are enabled, show a box around the track.	
	Show Triggered	Show tracks only when they are active; that is, when they are triggering a tripwire, intrusion, or loitering alarm.	Enable Human Tracks or Vehicle Tracks. Enable Show Class, Show Lines, or Show Boxes.
	Enable the VA tracking overlay for individual video streams.	Does not override the global VA overlay Enable setting above. For the overlay to appear in a stream, the global setting and the stream must be enabled. · The live video on the camera's web page is not the actual video stream. Therefore, enabling the tracking overlay for a stream might not affect the live video.	

2.10 OSD Page



The OSD page provides separate on-screen display settings for visible and thermal video.

The camera can overlay onto the video its name and the date and time:

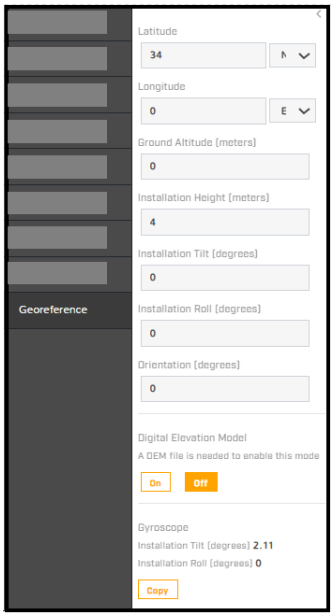
- with either black or white text
- with or without a contrasting background
- in either regular or **bold** style in small, medium, or large size

Changes to OSD settings immediately take effect.

2.11 Georeference Page

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

- **Latitude**, in degrees North or South
- **Longitude**, in degrees East or West



Retrieve the camera's latitude and longitude coordinates by:

- Right-clicking on the display and then selecting **Georeference Sensor**.

Manually specifying the coordinates, up to eight decimal places. To obtain the camera's latitude and longitude, you can use a map or a mobile GPS device.

Setup Menu

The **Setup** menu is used for GEO Settings, camera setup, and defining parameters for surveillance zones.

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.

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

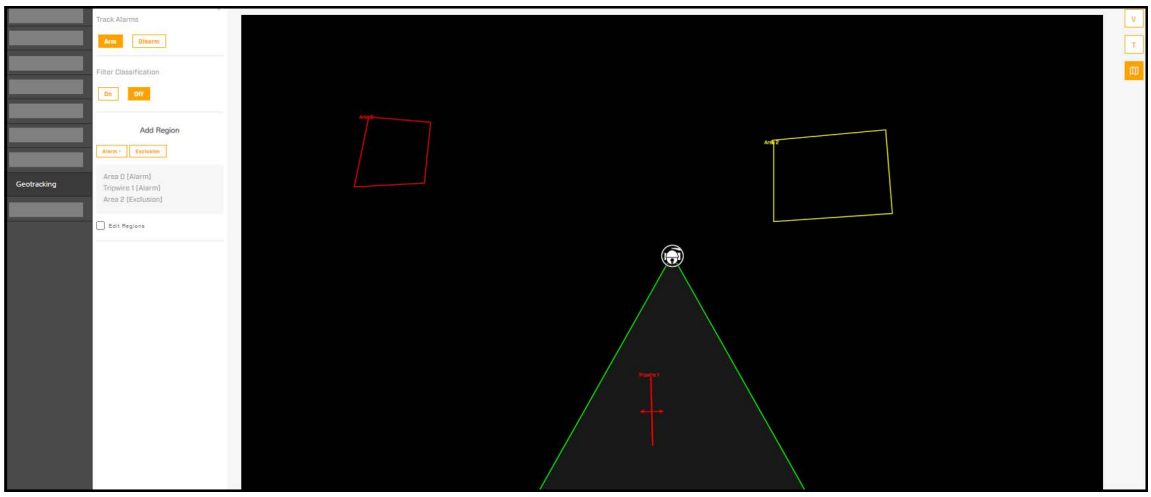
- **Ground Altitude**, in meters above or below sea level, up to two decimal places
- **Installation Height**, in meters above the ground, up to two decimal places (must be greater than zero)
- **Installation Tilt—**camera mounting angle in the longitudinal (front-to-rear) axis, in degrees, up to three decimal place.
- **Installation Roll—**camera mounting angle in the transversal (left-to-right) axis, in degrees, up to three decimal place.
- **Orientation—**value that aligns the camera's detection range as it appears on a calibrated map, with the video field of view; between 0-360 degrees from North, up to two decimal places. For geotracking, the camera's orientation must be accurate and precise.

Digital Elevation Model—After creating a DEM file and uploading it to the camera on the map page, you can turn DEM on. When DEM is off, the camera does not adjust detected object tracking according to elevation.

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.

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.

2.12 Geotracking Page



On the Geotracking page, you can enable (Arm), configure, and disable (Disarm) geotracking. You can pair the PT-Series AI camera with one or more camera that supports geotracking. When the cameras are paired, the PTZ camera engages the geotracks. For information about how to pair cameras, including how to configure the PTZ camera when it is paired, see the PTZ Pairing Guide.

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

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

Icons and Descriptions			
	Fixed camera—The circle around this icon indicates the Quasar Premium BulletCamera with FLIR Edge AI Video Analytics you are currently configuring.		Geotracking alarm region
	PTZ camera		Geotracking exclusion region
	Radar		Detected object
	Geotracking range		Detected object in alarm region
	Video analytics detection range		Object engaged by PTZ camera

1. Click one of the Add Region options.

   Alarm (Areas or Tripwires)—Regions where the camera generates geotracking alarms. In the detection area display, the borders of these regions and detected objects appear in red. When a Camera with FLIR Edge AI Video Analytics is paired with a the PT-Series AI camera, you can specify that the PTZ camera only engages geotracking alarm tracks.

   Exclusion—Regions where the camera's video analytics does not detect objects and does not generate geotracking alarms. In the detection area display, the borders of these regions appear in yellow. Exclusion regions can help eliminate alarms from a tree or bush moving in the wind, for example.
2. Create the first point of the region. Click and release on the detection area display.
3. Continue adding points (up to 25).
4. Complete the region. Double-click on the detection area display.

   To cancel creating a region, press **Esc**.

   To define another region, repeat steps 1-4.

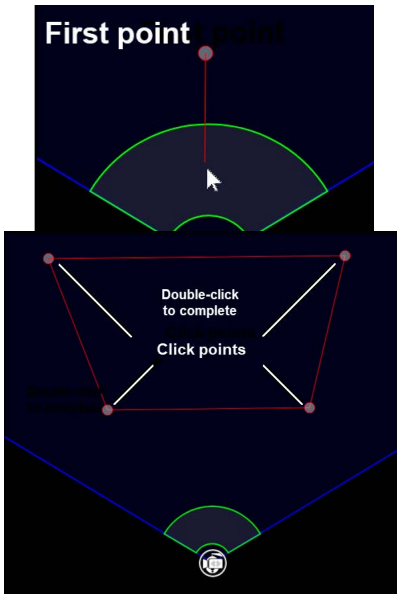
Managing Regions

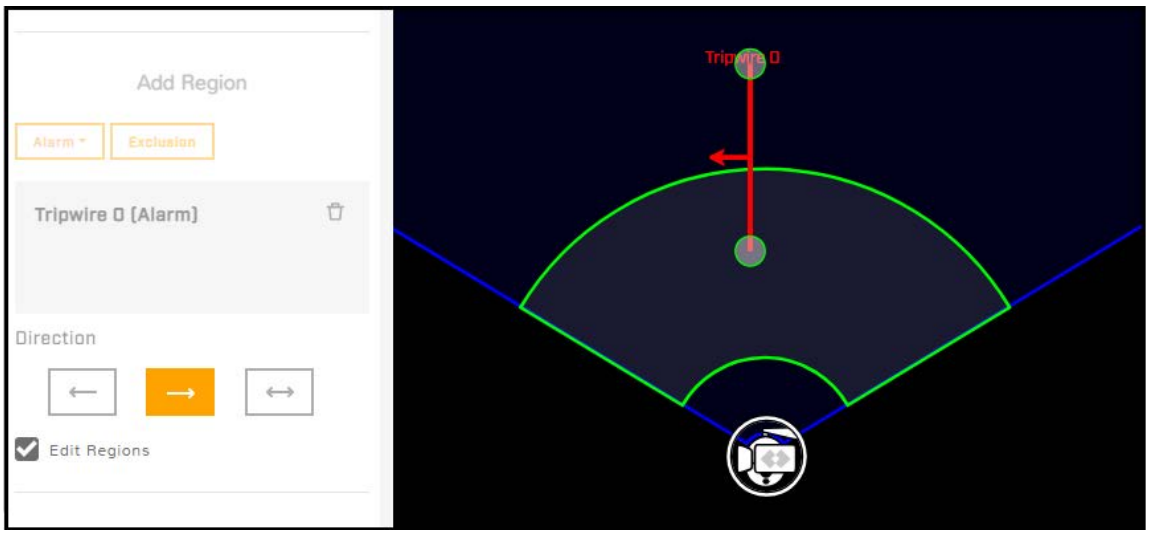
To edit an existing region, select **Edit Regions**, and click the region. You can:

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

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

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





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

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

To move the display, and to zoom in and out, you can use the mouse. To move the display, click on the display, hold, and drag. To zoom in or out, use the mouse scroll wheel.

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

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

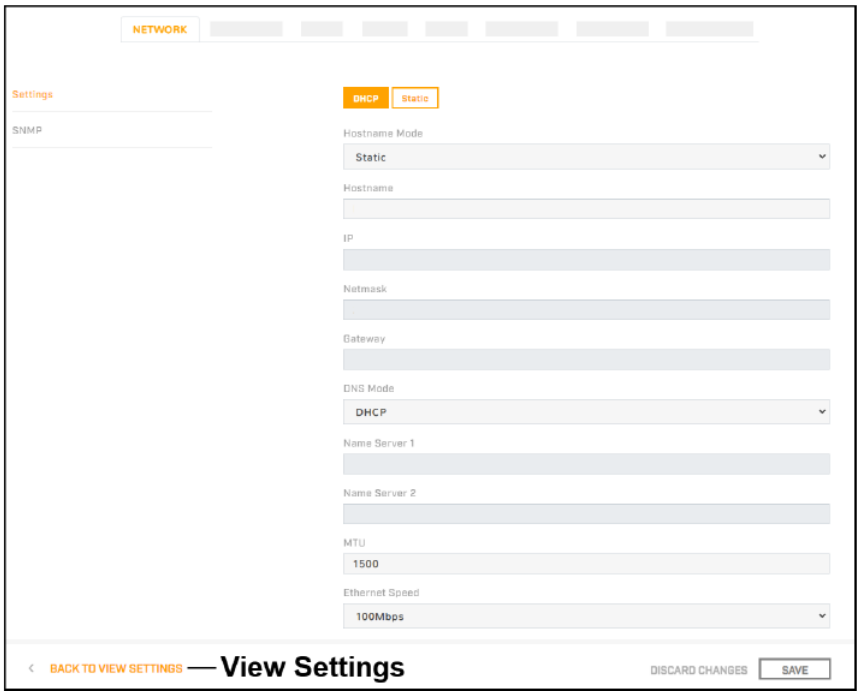
2.13 Configuration

Users assigned the admin or expert role can click System Settings on the View Settings home page to access the following configuration pages:

Network, Date & Time, Users, Alarm, I/O Devices, Messaging, Heaters & Fans, Cyber, Media Browser, ONVIF, Map, Geotracking, Scheduler, Recording, SD Card, Firmware & Info.

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

2.13.1 Network Page



The Network page provides networking and SNMP settings.

The DHCP (default) and Static buttons at the top of the page specify the IP addressing mode. If the IP addressing mode is set to DHCP but a DHCP server is not available on the network, the camera's IP address defaults to 192.168.0.250.

In Static IP addressing mode, specify:

- **IP**—The camera's IP address.
- **Netmask**—The default value is 255.255.255.0.
- **Gateway**

The Hostname Mode can be set to DHCP or Static (default); if set to Static, specify the hostname for the camera's server.

- **DNS Mode**—When the IP address mode is DHCP, you can set the DNS Mode to DHCP or Static. When the IP address mode is Static, the DNS Mode is also Static.

  When the DNS Mode is set to Static, specify:

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

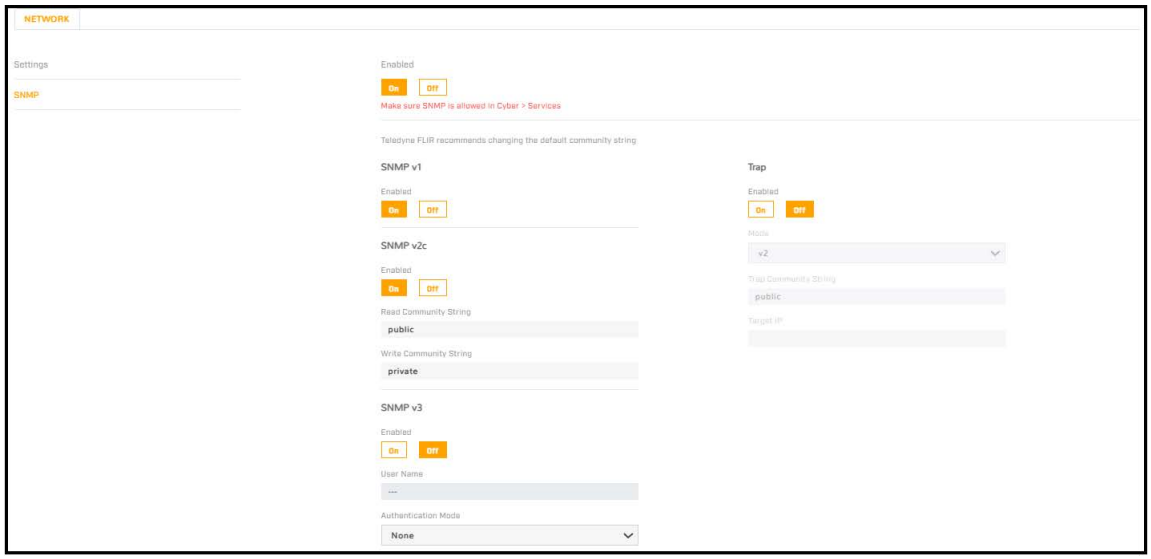
You can also specify the:

- **MTU**—Maximum transmission unit, the largest amount of data that can be transferred in one physical frame on the network. For Ethernet, the MTU is 1500 bytes (the default setting). For PPPoE, the MTU is 1492. Valid values are 1000-1500.

Ethernet Speed—When set to 100Mbps (default), the camera supports 100 Mbps. When set to Auto, the camera supports 10/100/1000 Mbps. Teledyne FLIR recommends 100 Mbps.

2.13.2 SNMP

In the SNMP section, you can enable and configure SNMP (Simple Network Management Protocol). SNMP allows network management systems to monitor and to remotely manage the camera. By default, all SNMP features are disabled.



SNMP v1—Enable SNMP v1.

SNMP v2c

After enabling SNMP v2, specify:

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

SNMP v3

SNMP v3 provides security features including:

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

After enabling SNMP v3, specify:

- **User Name—**Name of user on network management system using SNMP v3.

- **Authentication Mode—**Select None, MD5 (default), or SHA.
- **Authentication Password—**Password for authentication on network management system.
- **Privacy Mode—**Select None (default), DES, or AES.

Privacy Password—Password for privacy on network management system.

Trap

The camera uses traps to send messages to the network management system for important events or status changes. After enabling traps, specify:

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

Target IP—IP address of the network management system server.

2.13.3 Date and Time Page

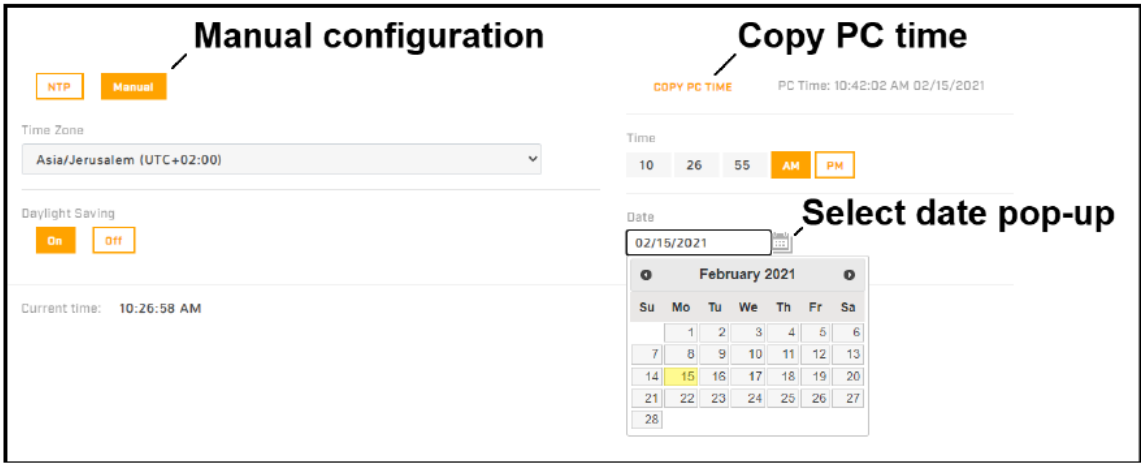
By default, the camera synchronizes its date, time, and time zone with an NTP server.

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

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

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

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



Email notifications and other camera features require configuring the camera’s system time to be the

current time.

2.13.4 Users Page

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

It is not possible to change the role of the default admin user.

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

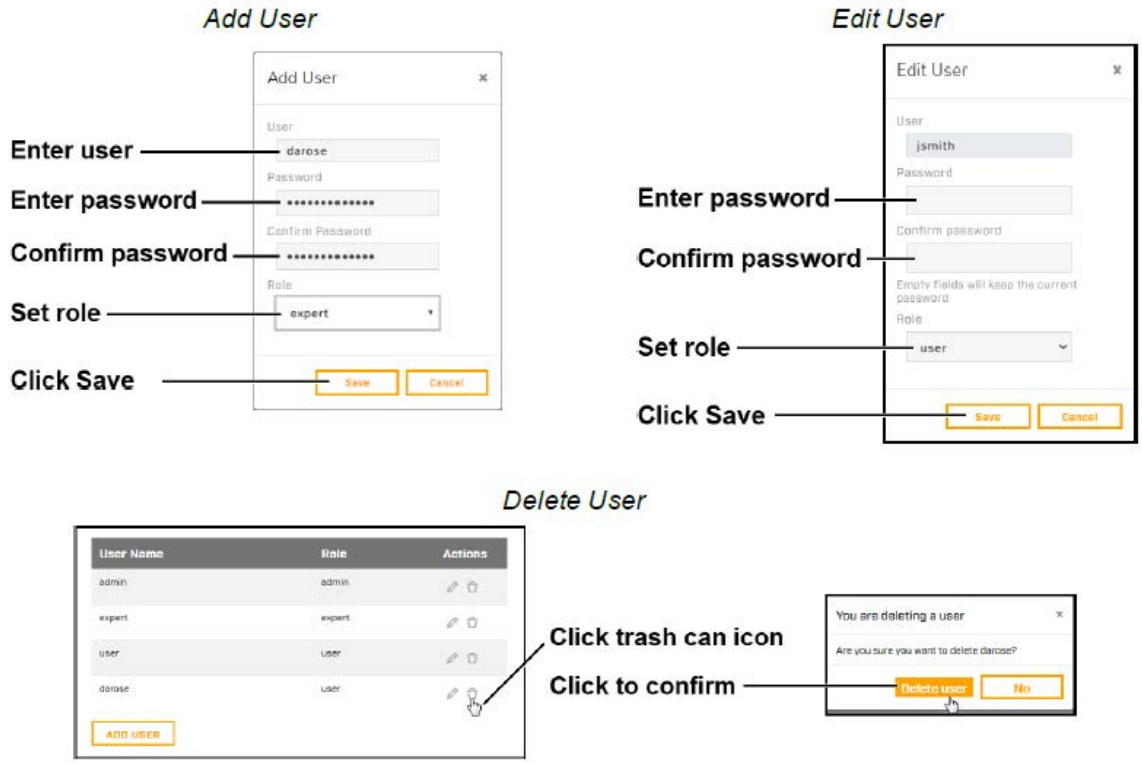
To maintain security of the system, set up user names and passwords for each required login account.

The camera limits user name length to 29 characters. Passwords must be at least 12 characters; must contain at least one number, one lowercase letter, and one uppercase letter; and can include the following special characters: |@#~!$&<>+_-.,*?= .

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

Role	Access
user	Can: • View live video • Switch between visible and thermal live video • Pan, tilt, and zoom the camera, including toggling between the emulated joystick and crosshairs control • View the Help page • Log out
expert	Cannot manage users: • Cannot add/edit/delete users • Cannot change passwords Can access and use all other View Settings and System Settings pages, menus, controls, and settings
admin, including the default admin user	Can access and use all of the camera's web pages, including adding/editing/deleting users (but cannot delete the default admin user), and setting all passwords

When the camera's video streams require RTSP authentication, accessing the camera's video streams requires the name and password for any camera user. All roles provide access to the camera's video streams.



2.13.5 Alarm Page

You can define camera alarms to be triggered by the following:

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

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

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

By default, the following rules are defined and disabled:

- **0. Video analytics trigger email**—The camera's VA triggers a notification email. Set up and configure the messaging settings on the Messaging Page.
- **1. Video analytics change output state**—The camera's VA triggers a change to the state of an

local alarm output connector. If the idle state of the connector is Closed, the alarm changes the state to Open. Likewise, if the idle state is Open, the alarm changes the state to Closed. For information about configuring the idle state of the camera's local I/O connector pins, see IO Page.

- **2. Input arms / disarms analytics**—Changes in the state of the local alarm input connector enable or disable the onboard VA.

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

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

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

2.13.5.1 Modify or Edit an Alarm Rule

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

1. Click the alarm name. The rule trigger settings appear

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

2. Modify or define the rule name.

Select whether the triggers are local (onboard the camera) or remote (external).

Local Trigger		
I/O	**Local**—This camera's local I/O connections trigger this rule's action.	a. On the Input/Output (I/O) Page, make sure local I/O connectors have been properly configured. b. Select one or more local I/O connections that trigger this rule's action.
	External—This camera's external I/O connections trigger this rule's action.	a. On the Input/Output (I/O) Page and on the I/O Devices Page, make sure the external I/O connections and the device managing those connections with the camera have been properly configured. b. Select one or more external I/O connections that trigger this rule's action.

Remote Triggers
Under Discovered Devices, select the remote camera, radar, or other device from the drop-down menu of supported devices on the same network as the camera; its IP address and port appear. You can also manually specify the remote device IP address and port, and then click **Refresh** to save it. Clicking **Refresh** also refreshes the drop-down menu of discovered devices. For example, if you just connected the remote device to the same network as the camera.
Note The camera discovers supported devices on the same network as the camera. However, to be used as a trigger, the device must be on the same VLAN as the camera.

Remote Triggers		
Video Analytics	Video analytics from a supported remote camera or other device triggers this rule's action.	a. On the remote camera or other device, make sure video analytics are enabled and that at least one tripwire, intrusion detection / loitering region, or another analytics item has been defined. b. Select one or more video analytics items that trigger this rule's action.
Radiometry	Radiometry from a supported remote camera or other device triggers this rule's action.	a. On the remote camera or other device, make sure radiometry is enabled and that at least one radiometric item has been defined. b. Select one or more radiometric items that trigger this rule's action.
Geotracking	Geotracking from a supported radar or remote camera triggers this rule's action.	a. On the radar or remote camera, make sure detection or geotracking is enabled and that at least one alarm area, tripwire, or other area has been defined. b. Select one or more radar or geotracking areas that trigger this rule's action.

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

2.13.5.2 Modify or define alarm rule actions

1. For the alarm rule you are modifying or defining, select the checkbox for one or more action type.
2. To configure an action type, click the selected action type. The selected action type appears in **bold**, and the relevant settings appear.

Action Type	
I/O	Under I/O List, select Local or External.
	Local—This rule changes the state of the local output (Out1). a. On the I/O Page, make sure local I/O connectors have been properly configured. b. For each trigger defined for the alarm rule, select Out1.
	External—This rule changes the state of one or more external output pins. a. On the I/O Page and on the I/O Devices Page pages, make sure the external I/O connections and the device managing those connections with the camera have been properly configured. b. For each trigger defined for the alarm rule, select an external output pin.
	Tip You can map individual local or remote triggers to specific local or external outputs.
	Bound—When selected, the camera changes the state of the output when the alarm is triggered and when it is cleared. When not selected, the camera changes the state of the output when the alarm is triggered. However, the output state remains changed until it is reset according to the configured Reset Interval or by a command from the network. You can configure the Reset Interval for the local output on the I/O Page and for the external output pins on the I/O Devices Page.
Arm/Disarm Analytics (not available when this rule's trigger is Video Analytics)—When triggered, this rule toggles the camera's onboard VA between enabled and disabled.	
Email—When triggered, this rule sends a notification email according to the settings on the Messaging Page. Specify a subject for the email and whether the camera attaches to the email a snapshot image of live video.	
Snapshot—When triggered, this rule records a snapshot image of live video.	
Arm/Disarm Geotracking (not available when this rule's trigger is Geotracking)—When triggered, this rule toggles the camera's geotracking between enabled and disabled.	

3. Click Done.

2.13.6 I/O Devices Page

On the I/O Devices page, you can configure the camera's external I/O connections and the device managing those connections with the camera.

You can configure the following for the device managing the external I/O connections:

- **Enabled or Disabled**
- **Device IP address and port**
- **Input and output base addresses**

- **The number of input and output pins the device manages**

  By default, six input pins and six output pins are specified.

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

- **I/O pin number**
- **Type**—Input or Output
- **State**—the pin's current state: Off or On
- **Idle State**—Open or Closed
- **Alarm Auto Ack**—Yes or No
- **Enabled**—Yes or No

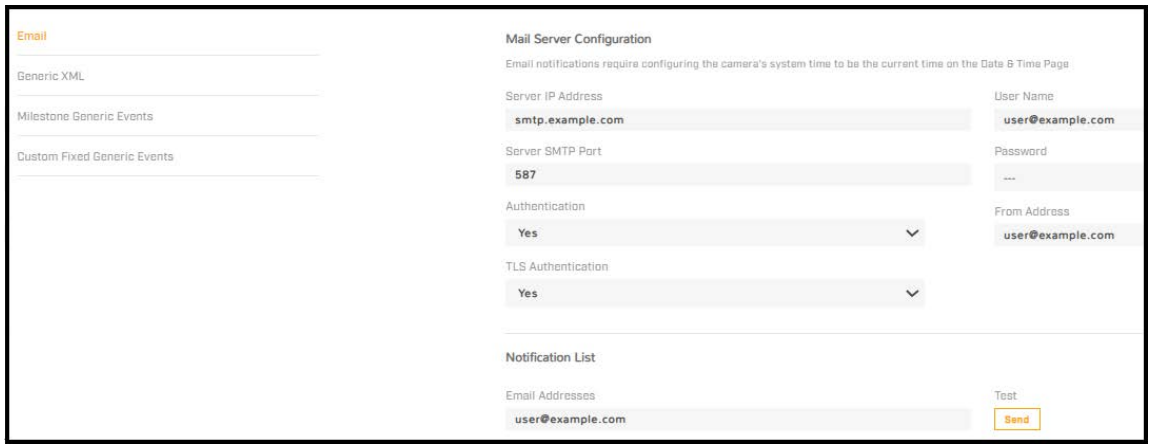
Reset Interval (for output pins only)—between 0-600 seconds; to disable auto reset for an output pin, select 0

2.13.7 Messaging Page

As an action for an alarm rule, the camera can send a notification email using the mail server settings you can configure on the Messaging page.

Specify the settings for the SMTP server in the appropriate fields. Settings include the SMTP server's IP address; port (the default port is 587); user name and password for the account on the mail server; whether the mail server requires authentication or TLS authentication; and the email address from which the camera sends the notification emails (also known as the reply-to address). If you do not know the mail server's settings, contact your mail server administrator.

Under Notification List, specify one or more email addresses, separated by commas, to receive the notifications.



2.13.8 Heaters and Fans

The Heaters & Fans page provides defogging and background heating controls, and information about the camera's CPU temperature, heater, and cooling fan.

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

To manually activate defogging:

1. Under Triggered by user, select the Duration (0.5, 1, or 2 hours).
2. Select **Defog**.
3. Click **Start**. The state of the heater changes from Off to On.

To deactivate defogging, click **Stop**.

Background Heater Control

By default, the background heater control is set to Off. Teledyne FLIR strongly recommends selecting Auto.

To manually activate defogging or deicing:

1. Under Trig Upload file the Duration (0.5, 1, or 2 hours).
2. Select **Defog** or **Deice**.
3. To start, ch Upload file , Visible, or Both. The state of the heater changes from Off to On.
4. To deactivate defogging or deicing click **Stop**.

To set the background heater control:

1. Under mode choose Auto.
2. Under duration, choose 0.5, 1, or 2 hours.
3. Choose a thermal and visual power limit (0 - 15).
4. Choose a low and high threshold (in Celcius).
5. Click **Apply**.

Status Information

Down the right side of the Heaters & Fans page, the following information appears:

- **Power Source—**24VDC
- **Current Operation Status—**Current background heater control setting (Off or Auto).
- **Thermometers—**Temperature of the camera's CPU.
- **Heaters—**State of the camera's heater (On or Off).

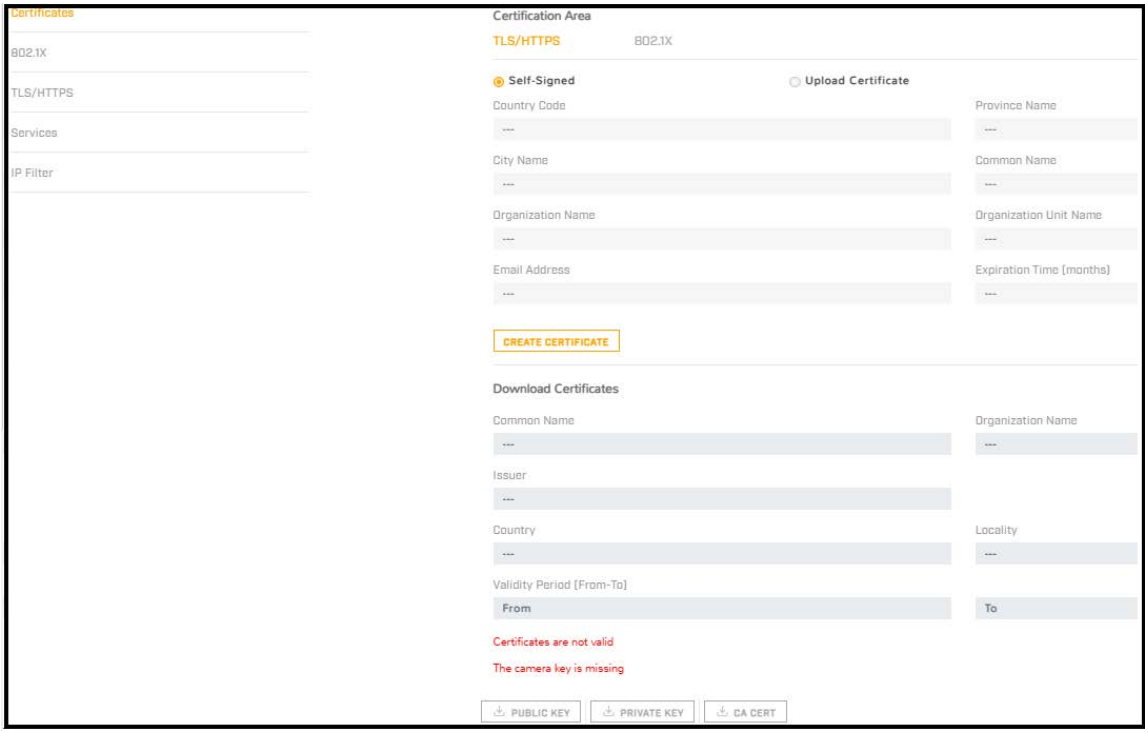
Fans—State of the camera's cooling fan (On or Off).

2.13.9 Cyber Page

Certificates

Before you can enable TLS/HTTPS or 802.1X, you need to generate or upload a valid certificate. You can use the camera's web page to generate a self-signed certificate; upload a self-signed

certificate; or upload a certificate signed by a third-party. If you do not know how to configure these settings, contact your network administrator.



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

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

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

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

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

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

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

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

   a. Click .

   b. Select the appropriate key file.

   c. Click .

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

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

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

2.13.9.1 802.1X

You can enable or disable IEEE 802.1X-compliant TLS communication provide the Identity and the Private Key Password. The default is disabled.

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

2.13.9.2 TLS/HTTPS

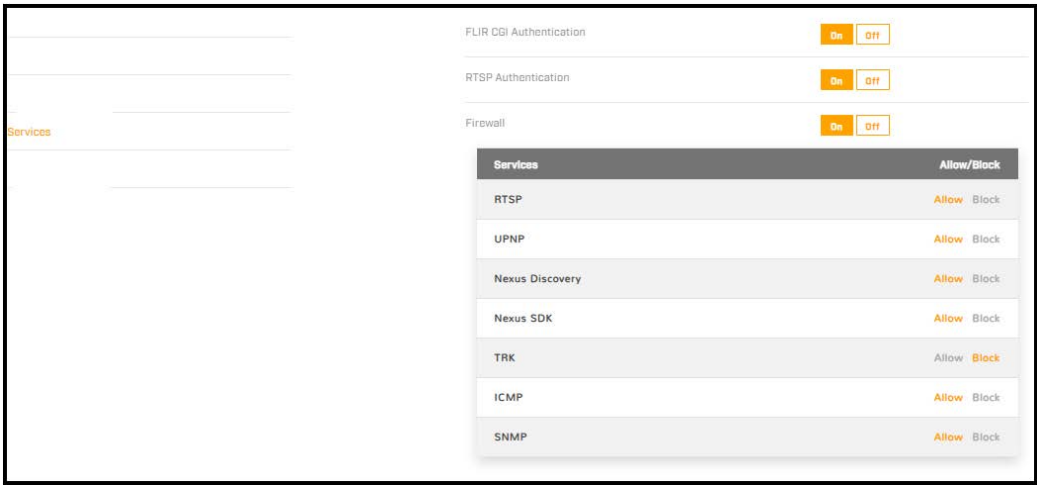
You can enable or disable IEEE 802.1X-compliant TLS communication provide the Identity and the Private Key Password. The default is disabled.

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

2.13.9.3 Services

You can enable or disable:

- Digest authentication for the FLIR CGI control interface. Default is on.
- RTSP authentication. When disabled, accessing the camera's video streams does not require authentication. Default is on.



Firewall Settings

For enhanced security, the camera has a firewall that is disabled by default. You can enable it by

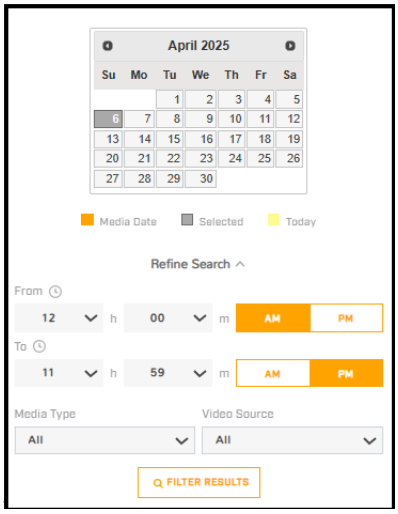
clicking **On**. By default, when you enable the firewall, the following services are set to **Allow**, which means they remain available and their default ports remain open:

- RTSP
- UPNP
- Nexus Discovery
- Nexus SDK
- TRK
- ICMP
- SNMP

To disable a service and its default port, click **Block**.

2.13.9.4 Media Browser Page

When recorded files exist on a properly installed and formatted microSD card, you can preview and access those files on the Media Browser page.



You can:

- view files by date—orange indicates recorded files exist for that date.
- filter the list by:
  - specific times
  - media type (Snapshot , Video , or All)

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

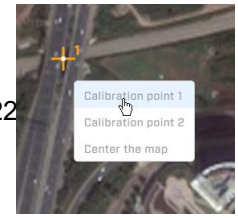
After selecting a file, you can download or delete the file. It is not possible to download more than one file at a time.

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

· <source> is the stream recorded—V1 / V2.

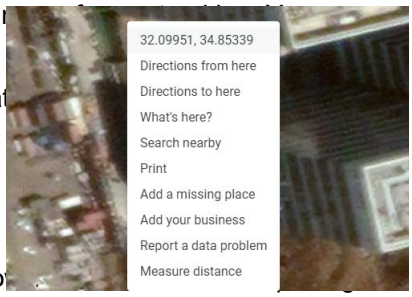
· <start_time> and <end_time> are Unix timestamps.

For example, SOE1-V1_VIDEO001_V1_1700982489_1700982789_3_22



2.13.10 Map Page

On the Map page, you can upload and calibrate a reference map i
also:



· download a previously uploaded map and its calibration informat

· upload a zipped map and calibration file

remove a previously uploaded map

To upload a reference map image and calibrate it:

1. Using an online map or GPS service such as Google Maps, do

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

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

2. It might take a few attempts at different settings to achieve the best result.

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

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

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

   If the map successfully uploads, a confirmation message appears.

4. Click **Accept**.

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

.

.

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

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

   The calibration point appears in the map as a crosshairs icon.
7. Repeat steps 4 and 5 for the second calibration point (P2).
8. Click **Save**.

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

· Even though it is not possible to delete an uploaded map image, you can upload a black image and replace the existing map.

2.13.11 Scheduler Page

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

· Enable the camera's onboard VA during certain times of the day.

· Schedule periodic uploads of snapshots of live video images to an FTP/SFTP server.
By default, no tasks are defined.

To define a task:

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

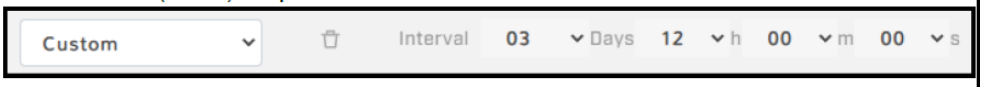
3. Define the task name.
4. Select the checkbox for one or more predefined actions.
5. To configure a predefined action, click the selected action. The selected action appears in **bold**,

and the relevant settings appear.

Table 2-2: PredefinedActions

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

6. Click **Next**. The task schedule settings appear.
7. From the drop-down list, select the first schedule for the task.

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

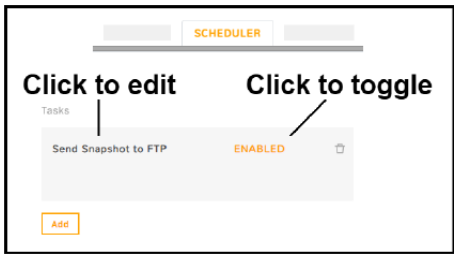
You can define more than one schedule for a task. For example, if you want to schedule an action for every Monday at 08:00 and for midnight on the first of every month:

a. Define the 08:00 Mondays weekly schedule.
b. Click **Add**.
c. Define the first-of-every-month monthly schedule.

8. Click **Done**.

When you click **Done**, new tasks and changes to tasks immediately take effect. Unless you have made other changes on the Alarm page, clicking **Save** is not necessary.

Enable or disable a task by clicking **Enabled** or **Disabled**. To delete a task, click the corresponding trash icon



2.13.12 Recording Page

On the Recording page, you can configure:

- Global video clip recording settings
- Recording sources

Global Settings

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

File Name Format—MP4.

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

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

Recording Sources

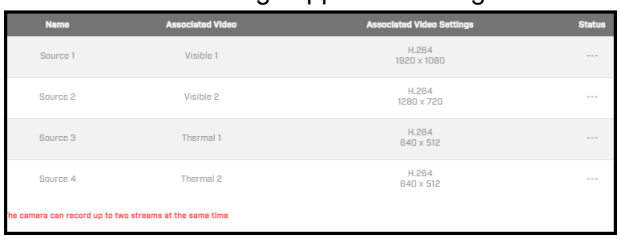
The camera has four recording sources, the four video streams (V1, V2, T1, and T2). The camera can record up to two sources / streams at the same time.

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

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

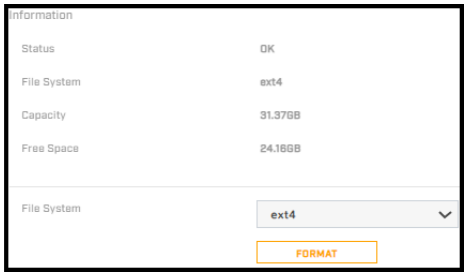
You can also manually start and stop recording the selected source / stream. However, manual recording of an H.265 source is not supported.

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



2.13.13 SD Card Page

You can locally record up to 512GB on a Class 10 microSD/microSDHC/microSDXC card (minimum 8GB).



The following information appears on the SD Card page:

- **Status**
  - OK—a microSD card has been properly installed and formatted
  - Error
  - Formatting
  - Done
  - No SD Card
- **Capacity—**The card's overall capacity, in GB.
- **Free Space—**How much free space is on it, in GB.

To format a microSD card before using it, click **Format**.

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

- Format the microSD card when using it for the first time, or when the card has been used with another camera or other device and transferred to this camera.
- The card must be preformatted as a single partition.
- For information about accessing the camera's microSD slot and inserting a card, see Connect Camera

2.13.14 Firmware and Info Page

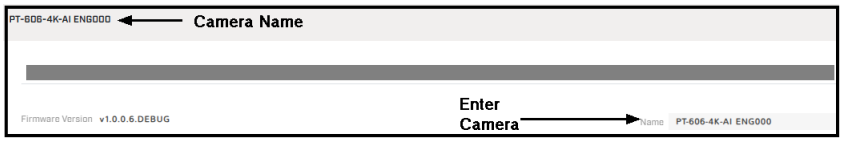
On the Firmware & Info page, you can:

- See the currently installed firmware version and other information about the camera
- Specify a unique name for the camera
- Upgrade the camera's firmware
- Reset the camera's settings to their factory defaults
- Reboot the camera
- Enable logs, define a log level, and download system information

· Download or upload a configuration backup file

· Configure the video format

Name



· Specify a unique, friendly name for the camera, using only alphanumeric characters.

The default name for the camera is the camera model followed by the camera's serial number.

To upgrade the camera's firmware:

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

   The camera uploads and installs the firmware, which takes a minute or two. After installing firmware, the camera requires a reboot. When prompted, confirm rebooting the camera.

Factory Defaults

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

To reset the camera to its factory default settings but retain previously saved Network page and 802.1X settings, click **Partial Reset**, and then confirm. The camera reboots.

After confirming a reset, do not click on the camera web page until the camera reboots and the login screen appears.

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

You can also:

· Reset the camera to its factory default settings by pressing the camera's physical default button for at least six seconds.

· Reboot the camera by pressing the camera's physical reset button for at least one second.

· The default and reset buttons are located on the camera's bottom panel.

For example, if you are unable to access the camera via its web page or other communication method.

Support System Info

To retrieve the camera's log files, click **Download**.

Set the logging detail up to four levels; higher log levels increase the size of the log file.

Configuration Backup

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

To upload a configuration backup file:

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

Make sure to upload a configuration backup file that was downloaded from the exact same model and with the same firmware version installed.

3. Click **Upload**.

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

To download the camera's saved settings:

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

   backup.tar.gz is the default backup file name. You can change the backup file name, but do not change the **.tar.gz**.

Video Format

- Select NTSC (default) or PAL. The video format determines the video stream frame rates available on the Video Page and the exposure times (shutter speeds) available on the Visible Page.