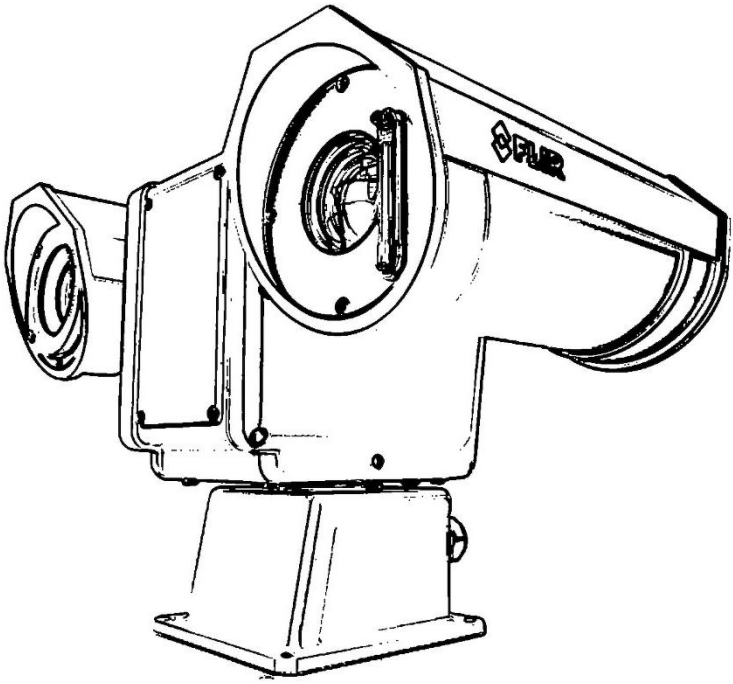
# INSTALLATION & USE GUIDE



# PT-Series AI SR

**PT-644 AI PT-625 AI PT-617 AI PT-612 AI PT-608 AI**
**PT-606 AI PT-606Z AI**

V 120. January 2026.

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

Protected by one or more patents and patent applications. Learn more here: www.flir.com/patentnotice.

Photographs and images appearing in this manual may have been modified for illustrative purposes using commercial image editing software and may not always reflect an actual product configuration. The contents of this document are subject to change without notice.

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

Proper Disposal of Electrical and Electronic Equipment (EEE)

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

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

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

# Document History

| Revision | Date | Comment |
|---|---|---|
| **110** | December 2025 | Revised format and content. |
| **113** | January 2026 | Small fixes. |
| **120** | January 2026 | Fixed US-only/World model references |

# Contents

# 1- Product Registration and Warranty Information

## 1.1- Register Your Product with Teledyne FLIR

Ensure you get the most out of your Teledyne FLIR product by registering it at https://customer.flir.com. By registering, you'll receive exclusive benefits, updates, and support tailored to your product.

## 1.2- Warranty Information

For comprehensive warranty details, visit https://www.teledyneflir.com/support-center/warranty/security/flir-security- product-warranties/. Here, you'll find all the information you need to understand the coverage and support available for your FLIR security products.

# 2- Document Scope and Purpose

This document provides installation, operation, and configuration instructions for PT-Series AI SR cameras with FLIR Edge AI Video Analytics.

This document is intended for use by technical users who have a basic understanding of CCTV camera/video equipment and LAN/WAN network connections.

**WARNING**

Installation **must follow safety, standards, and electrical codes as well as the laws** that apply where the units are being installed.

## 2.1- Disclaimer

Users of Teledyne FLIR products accept full responsibility for ensuring their suitability and considering the role of the product detection capabilities and their limitations as they apply to their unique site requirements.

Teledyne FLIR LLC and its agents make no guarantees or warranties to the suitability for the users' intended use. Teledyne FLIR LLC accepts no responsibility for improper use or incomplete security and safety measures.

Failure in part or in whole of the installer, owner, or user in any way to follow the prescribed procedures or to heed WARNINGS and CAUTIONS shall absolve Teledyne FLIR and its agents from any resulting liability.

**WARNING**

- The unit's cover is an essential part of the product. **Do not open or remove it**.
- **Never operate the unit without the cover in place.** Operating the unit without the cover poses a risk of fire and shock hazards.
- **Do not disassemble the unit.** There are no user serviceable parts inside the unit.
- Only **qualified trained personnel** should service and repair this equipment.
- **Observe local codes and laws** and ensure that installation and operation are in accordance with fire, security, and safety standards.

Specifications and information in this guide are subject to change without notice.

For installation support, visit https://www.flir.com/support/ or contact your local Teledyne FLIR representative. Installers and integrators can also access Teledyne FLIR training at https://www.flir.com/support-center/training/.

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

# 3- Camera Overview

The FLIR PT-Series AI SR is our most advanced multi-sensor security camera, featuring a high-performance <25 mK NETD uncooled thermal sensor with 640 × 512 resolution, a 4K visible-light imaging sensor and outstanding low-light performance. Enhanced with FLIR Fusion AI video analytics, the PT-Series AI SR offers reliable edge-based detection and classification of human and vehicle targets at extended ranges. Combined with FLIR Nexus®, the PT-Series AI SR allows users to seamlessly track objects or people and provides uninterrupted target tracking—even beyond a radar's field of view. The PT-Series AI SR integrates easily with other major third party video management systems, making it an extremely versatile solution for critical infrastructure protection in total darkness, bright sun, and adverse conditions.

## 3.1- Related Documentation

- PT-Series AI SR Quick Install Guide
- FLIR Security Edge Devices Accessory Guide
- DNA User Guide

# 4- 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 | |
| | **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° | 100 mm, 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 | |
| | **Sensor Type** | 4K (2160p), 1/1.8-type STAVIS II CMOS | |

| | | |
|---|---|---|
| **Visible Spectrum Camera Specs** | **Effective resolution** | 327,680 |
| | **Lens Field of View** | 59.0° (wide end) to 2.3° (tele end) |
| | **Zoom** | 25x optical zoom |
| | **Focal Length F/#** | 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):**<br>H.264: 3840x2160, 1920x1080, 1280x720, 640x480<br>H.265: 3840x2160, 1920x1080, 1280x720, 640x480<br>MJPEG: 1920x1080, 1280x720, 640x480 |

| | | |
|---|---|---|
| | | **Steam V2 (visual):**<br>H.264: 1920x1080, 1280x720, 640x480<br>H.265: 1920x1080, 1280x720, 640x480<br>MJPEG: 1920x1080, 1280x720, 640x480 |
| | | **Stream T1 (Thermal):**<br>H.264: 640x512<br>H.265: 640x512<br>MJPG: 640x512 |
| | | **Stream T2 (Thermal):**<br>H.264: 640x512<br>H.265: 640x512<br>MJPG: 640x512 |
| | **Thermal AGC Settings** | Auto AGC, Dynamic Detail Enhancement (DDE), Sensitivity. |
| | **Thermal AGC Region of Interest (ROI)** | Default Presets and User are definable to ensure 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** | US-only models: 24 VAC/24 VDC.<br>World models: 24 VDC. |
| | **Power Consumption**[1] | Uncooled thermal camera: 195 W max. |
| **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: 2000 m. |
| | **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.

# 4.1- Safety Restrictions

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

# 5- Models & Product Numbers

The PT-Series AI SR comprises the following camera models:

| US-only Models Part Number | World Models Part Number | Thermal Camera Focal Length | Thermal Sensor Resolution | Visible Spectrum Camera |
|---|---|---|---|---|
| PT-644 AI<br>427-2075-27-00 | PT-644 AI<br>427-2075-07-00 | 13 mm, f/1.0<br>(44° × 36°) | 640 x 512<br>30 Hz | 4K (2160p), 1/1.8-type STAVIS II CMOS.<br>25x optical zoom.<br>6.5 mm (wide) to 162.5 mm (tele)<br>F1.6 to F4.8. |
| PT-625 AI<br>427-2075-26-00 | PT-625 AI<br>427-2075-06-00 | 25 mm f/1.1<br>(25° × 18°) | | |
| PT-617 AI<br>427-2075-25-00 | PT-617 AI<br>427-2075-05-00 | 35 mm, f/1.1<br>(17° × 14°) | | |
| PT-612 AI<br>427-2075-24-00 | PT-612 AI<br>427-2075-04-00 | 50 mm, f/1.2<br>(12° × 10°) | | |
| PT-608 AI<br>427-2075-23-00 | PT-608 AI<br>427-2075-03-00 | 75 mm, f/1.1<br>(8.6° × 6.6°) | | |
| PT-606 AI<br>427-2075-22-00 | PT-606 AI<br>427-2075-02-00 | 100 mm, f/1.6<br>(6.2° × 5°) | | |
| PT-606Z AI<br>427-2075-21-00 | PT-606Z AI<br>427-2075-01-00 | 26-105 mm, f/1.6<br>(Continuous zoom 24° to 6°) | | |

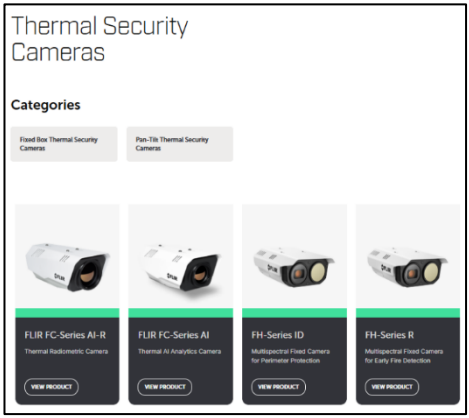
Please note that all cameras are available in an “S” variant, which utilizes an 8.3 Hz thermal sensor in place of the standard 30 Hz sensor.

# 6- Product Information on the Teledyne FLIR Website

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

## 6.1- Accessing Product Information from the Teledyne FLIR Website:

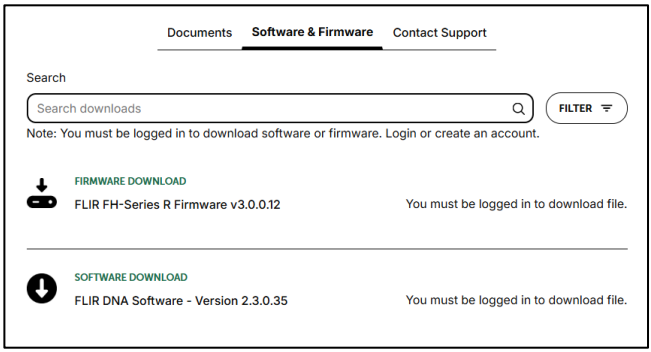
1. **Open** FLIR Security Thermal Cameras




2. **Find and click on the camera**. The camera's product details page is displayed.


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

4. To access the camera's support page, including documentation, select the **Resources & Support** tab.




1. 5. **Download** the latest firmware and FLIR DNA application, if necessary.

# 7- Installing the Camera

The order of the installation steps described in this manual follow a standard procedure, but the order can be changed to accommodate the site or installation needs. For instance, before installing the camera, Teledyne FLIR recommends **connecting the camera on a bench or in a lab** and configuring it for networking before mounting and aiming it.

### WARNING

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

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

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

## 7.1- Supplied Components

The PT-Series AI SR camera kit includes:

- **Multi-sensor pan/tilt camera unit**.
- **Galvanic isolation kit**.
- **Cable glands and spare parts kit**.
- **One printed Quick Installation Card.** If any of these items are missing or damaged, contact your dealer or Teledyne FLIR Support.

## 7.2- Site Preparation

The physical installation of the unit is the first phase of making the unit operational in a security plan. The goal is to physically place the unit, connect it to other devices in the system, and to establish network connectivity. When finished with the physical installation, complete the second phase of installation, which is the setup and configuration of the unit.

There are several requirements that should be properly addressed prior to installation at the site. The following specifications are requirements for proper installation and operation of the unit:

- A**mbient Environment Conditions**: Avoid positioning the unit near heaters or heating system outputs. Avoid exposure to direct sunlight. Use proper maintenance to ensure that

the unit is free from dust, dirt, smoke, particles, chemicals, smoke, water or water condensation, and exposure to EMI. The camera must be protected from hostile external elements such as a corrosive environment, metallic dust, extreme temperatures, soot, over spray, etc.

- **Accessibility**: Camera placement should allow easy access to unit connections and cables.
- **Safety**: Cables and electrical cords should be routed in a manner that prevents safety hazards such as tripping, wire fraying, overheating, etc. Ensure that nothing rests on the unit's cables or power cords.
- **Ample Air Circulation**: Leave enough space around the unit to allow free air circulation.
- **Cabling Considerations**: All electrical work must be performed in accordance with local regulatory requirements. There must be a fuse or circuit breaker at the starting point of the electrical wiring infrastructure. Units should be placed in locations that are optimal for the type of video cabling used between the cameras and external devices.
- **Physical Security**: To prevent the unit from being disabled or tampered with, the system should incorporate security measures that address physical access by both trusted and untrusted individuals.
- **Network Security**: Proper network security measures should be in place to ensure networks remain operative and free from malicious interferences. Install the unit on the backbone of a trusted network.
- **Electrostatic Safeguards:** The unit and other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc.) should be properly grounded to prevent electrostatic discharge.

### ⚠ WARNING

- **Before drilling into surfaces for camera mounting**, verify that electrical or other utility service lines are not present. Serious injury or death may result from failure to heed this warning.
- Ensure the **power supply or circuit breaker is off**.

## 7.3- Additional Considerations for Outdoor Mounting

For cameras that will be installed outdoors, also consider the following:

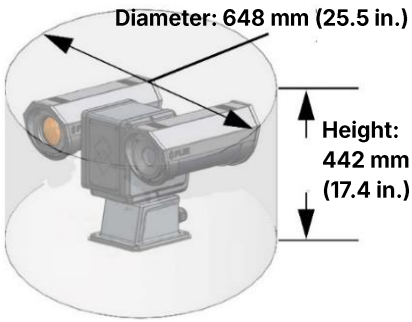
- **For outside wiring installation, always use weatherproof equipment**, such as boxes, receptacles, connectors, etc.

- **For electrical wiring, use properly rated sheathed cables** for the conditions to which the cable will be exposed, for example, moisture, heat, UV, physical requirements, etc.
- **Plan ahead** to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.
- **Use best security practices** to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, etc.
- To avoid damage from overheating or unit failure, assure that there is **sufficient temperature regulation** to support the unit's requirements (cooling/heating). The camera's operating temperature range is -40 °C to 70 °C (-40 °F to 158 °F); cold start -40 °C (-40 °F); and no more than 95% non-condensing humidity.
- **All electrical work must be performed in accordance with local regulatory requirements**.

# 7.4- Location Requirements

Install the camera in **a location that will allow access for regular periodic cleaning** (freshwater 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.

Since this device features fully rotating pan and tilt capabilities, please **ensure that adequate space is maintained around the camera** to permit unobstructed movement. **Avoid placing objects or cables nearby** that might hinder its operation, as such obstructions could result in damage or place undue strain on the pan and tilt mechanisms.




# 7.5- Power Requirements

The PT-Series AI SR cameras are provided in two variants depending on the market where they are sold: the **US-only models** and the **World models**. The Power requirements vary depending on the model:

## US-only Models

The US-only models must be powered using a 24 VAC or 24 VDC power supply.

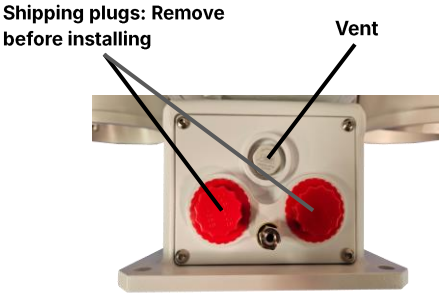
## World Models

The World models must be powered using a 24 VDC power supply.

| Maximum Power Consumption | 24 VDC/24 VAC |
|---|---|
| Heater OFF | 55 W |
| Heater ON | 195 W |

## 7.6- Installation Overview

Typical installation




Back cover

The PT-Series AI SR 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.

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.

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

## 7.7- Before Mounting the Camera

Before installing the PT-Series AI SR camera, **it is essential to be aware of several important considerations to ensure a safe and effective setup**. This section highlights the key factors to evaluate, including suitable mounting options, electrical requirements, proper handling of cable connections, and adherence to safety standards. Careful attention to these details will help facilitate a smooth installation process and support the reliable operation of the camera system.

- Installation and service should be performed by **qualified installation and service personnel** only.

- Installation should be performed **according to all local and national electrical and mechanical codes**, using only approved materials.

2. PT-Series AI SR 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.

3. The camera needs to be **installed properly leveled in all three axes** for better operational accuracy. This helps to avoid wearing out of the mechanical components.

- The camera should be installed in **a location which is not reachable by users**. 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**.

> ⚠ **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.

- **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.**

4. When lifting the camera use the camera body and base, not the tubes.

5. **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: **Earth ground connection** and **galvanic isolation**.

## Earth Ground Connection

Establishing **a proper earth ground connection is essential to safeguard the camera against surge-induced failures and corrosion** resulting from stray current or ground loops. **Connect a ground wire (16 AWG or larger) to the ground lug located on the back cover.** Secure the ground wire to the lug on the access panel using the large hex nut. The ground stud is threaded for #8-32 hardware.

## Galvanic Isolation

When installing the PT-Series AI SR camera, **always use the Galvanic Isolation Kit** (FLIR PN 4204960). 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 SR 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.

The Galvanic Isolation Kit contains:

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

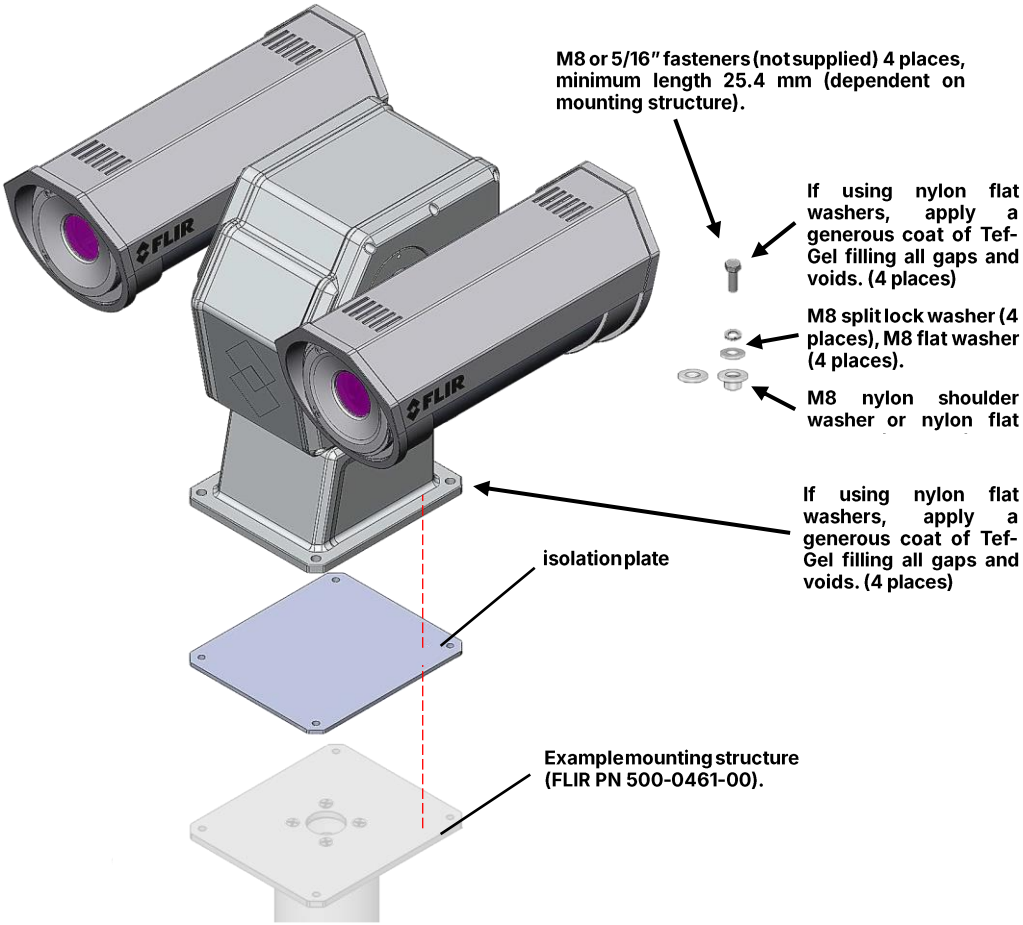
Notes: 1- Use the alternate nylon flat washers and Tef-Gel lubricant on fasteners for PT-Series AI SR camera bases with mounting holes that are too small to accept the shoulder washers. A syringe of Tef-Gel will be supplied in the mounting kit when the nylon flat washer is required. 2- Two extra pieces of each attaching part are supplied in the kit.

Please, follow the steps below to install the kit.

### ⚠ CAUTION

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

1. **Determine the correct positioning of the isolation plate** (see figure below).
2. **Place the isolation plate and the camera on the mounting structure** aligning the bolt holes or studs.
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.
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.
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.



# Installing a microSD Card

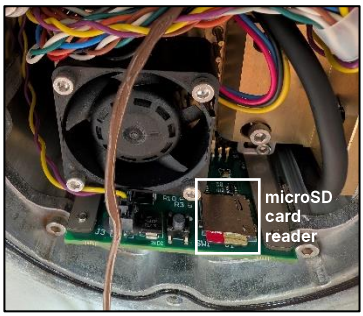
The microSD card slot on the PT-Series AI SR camera serves as a **convenient local storage solution for video recordings, snapshots, and event logs** generated by the camera. By inserting a compatible microSD card, users can enable the camera to automatically save footage and important data directly onto the card, which is especially useful for backup purposes or when network connectivity is limited.

This onboard storage feature allows for easy retrieval and transfer of recorded content. Users can remove the microSD card and access its data using a standard card reader on a computer, simplifying the process of archiving, or reviewing footage. It is recommended to use high-quality, high-capacity microSD cards that meet the camera's specifications to ensure reliable performance and data integrity.

To install the microSD card:

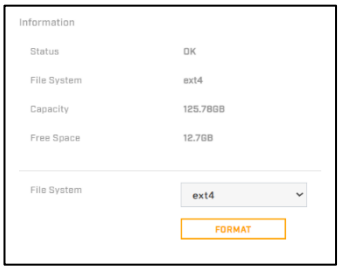
1. **Remove the back cover** of the visual payload (the one on the left when looking from behind).


2. Locate the microSD card reader and **insert the card**.




3. **Close the back cover** again, making sure that the screws are tightly fastened and that the cover fits neatly in its place.

4. On the camera's web interface, **go to System Settings and select the SD card tab**.



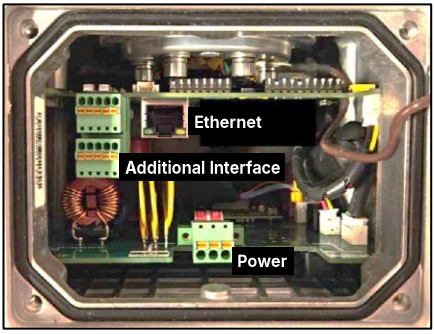

5. Click on **Format** and confirm.
6. **Wait until the card is formatted** and exit.

# 8- Connecting the Camera

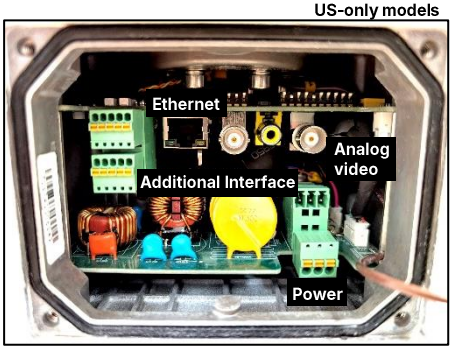
## 8.1- Remove the Back Cover

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. The location of the connectors is shown in the pictures below for both **US-only** and **World** models.

World models




US-only models

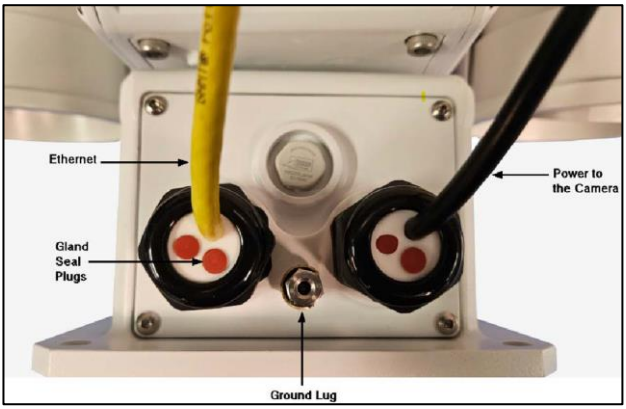



## 8.2- Cable Gland Sealing

Proper installation of cable sealing glands and the use of appropriate elastomer inserts are essential for ensuring long-term reliability. **Cables must be routed into the camera mount enclosure through the liquid-tight compression glands**. It is important to **insert cables through the cable glands before terminating and connecting them**, as connectors will not fit through the gland openings. Gland nuts may remain loose until all cable installations are complete. Inspect and install gland fittings on the back cover with suitable leak sealant, then tighten them to maintain watertight integrity. Acceptable sealants for this application include Teflon tape or pipe sealant, such as DuPont RectorSeal T™.

The supplied **Cable Glands and Spare Parts kit** includes the two 3/4″ cable glands and gland seal plugs required for non-conduit installations. Also included are: A spare ground wire, a spare ground nut and lock washer, a spare power terminal block plugs, and four spare back cover screws.

The **cable glands support cables between 5.84 and 7.37 mm**. Up to **six cables** may be installed. **Plugs are required for the hole(s) not being used**. The photograph below 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.

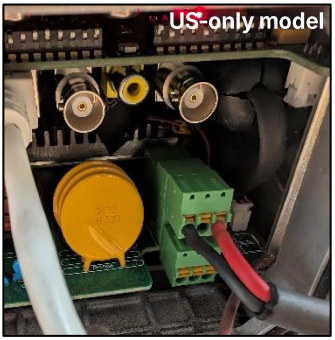
# 8.3- Connecting Power

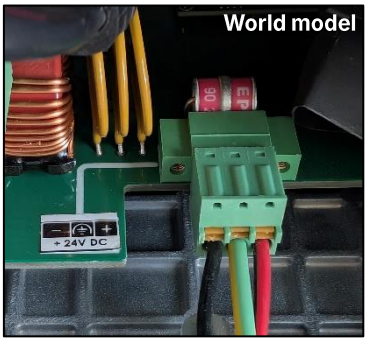
**The camera does not feature an on/off switch**. Power is typically controlled via a circuit breaker that applies or removes electrical supply to the unit. Once powered, the camera will either be in the Booting Up or Powered On state.

The **US-only models must be powered using a 24 VDC or 24 VAC** power supply, while the **World models require a 24 VDC** power supply.

| Maximum Power Consumption | 24 VDC/24 VAC |
|---|---|
| Heater OFF | 55 W |
| Heater ON | 195 W |

Connect the power cables to the power connector block using the diagram on the left as guidance, as seen in the picture below.




Installers must ensure that the **power cable utilizes wires of an adequate gauge** (16 AWG is recommended) suitable for the application's voltage and cable length. **All installations must comply with relevant local building codes**.

**Proper grounding of the camera is essential**. Consistent with established grounding practices, the chassis ground should be routed through the lowest resistance path available. FLIR requires the use of a grounding strap attached to the grounding lug located on the camera housing's back cover, which should then be connected to the nearest earth-grounding point.

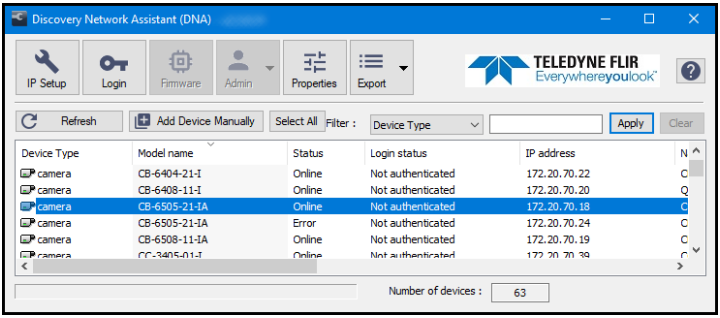
# 8.4- Connecting to the Network

Use a **shielded Ethernet cable to connect the camera to the network**. Once connected, the camera can be discovered and configured for networking using the **FLIR Discovery Network Assistant (DNA)** software tool; the **camera's web interface**; or a **supported VMS**. Using the DNA tool or the camera's web interface requires using the default admin user or any user assigned the admin or expert role. The table below indicates which tasks can be performed using each of these methods.

| Task | DNA Tool | Camera's Web Interface |
|---|---|---|
| Discover camera IP address | * | |
| Configure IP address, mask, and gateway | * | * |
| Configure IP address, mask, and gateway for more than one camera at the same time | * | |

| | | |
|---|---|---|
| Change user credentials | * | * |
| Configure DNS settings, MTU, and Ethernet speed | | * |

**Teledyne FLIR recommends using the DNA tool to discover the camera on the network**. It does not require a license to use and is a free download from Teledyne FLIR. For more




information about using the DNA tool, including how to configure more than one camera at the same time, see the *DNA User Guide* clicking on the Help icon while the software is open.

For more information about using a supported VMS to configure one or more cameras at the same time, see the VMS documentation.

**By default, DHCP is enabled on the camera** and a DHCP server on the network assigns the camera an IP address. For example, if the camera is managed by FLIR Horizon or Meridian VMS and the VMS is configured as a DHCP server, the VMS automatically assigns the camera an IP address. If the camera cannot connect to a DHCP server, the camera's **default IP address is 192.168.0.250.**

If the camera is managed by FLIR Latitude VMS or is on a network with static IP addressing, users can **manually specify the camera's IP address** using the DNA tool or the camera's web interface.

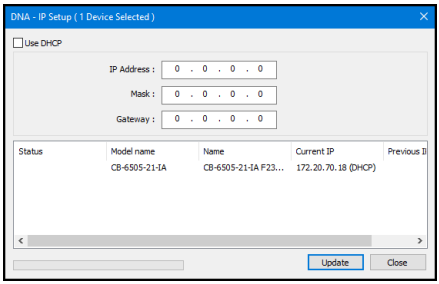
# 8.5- Changing the IP Address Using FLIR DNA Tool

When the camera is connected to a network where several other cameras are connected, it is highly advisable to make sure that **all cameras have unique IP addresses**. To do so, the **DNA tool** can be used to manually set up each individual camera's address.

1. Make sure the camera and the PC are on the **same LAN segment**.
2. **Open the DNA tool** (DNA.exe). The Discover List is displayed, showing compatible devices on the LAN segment and their current IP addresses.
3. In the DNA Discover List, verify that the camera's **status is Online**. If this is the first time configuring the camera or if it is the first time after resetting the camera to its factory

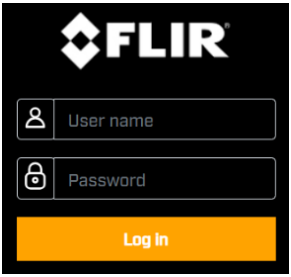
defaults, DNA automatically logs in to the camera using the **default username and password (admin)**.

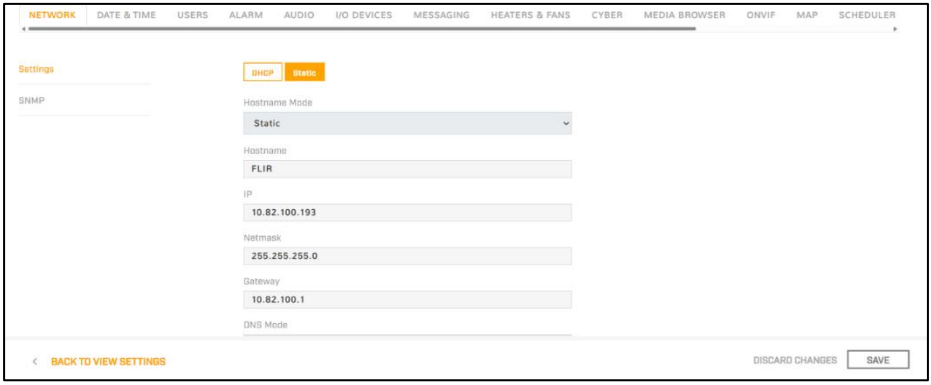
4. Verify that the camera's Login **status is Authenticated**. If not, authenticate the camera using the custom username and password.
5. Select the camera from the Discover List, and then select **IP Setup**.
6. In IP Setup window, **uncheck the Use DHCP box and specify the new IP address**. It is also possible to specify the **Mask and Gateway**.
7. Finally, **select Update** and wait until OK is displayed in the status column, and select **Close**.




## 8.6- Changing the IP Address Using the Camera's Web Interface

1. **Access the camera's web interface** entering the camera's IP address on a modern browser such as Google Chrome, Microsoft Edge, or Modzilla Firefox, etc.
2. **Enter the username and password**. By default, these are both **"admin."**
3. On the View Settings Home screen, click **System Settings** in the lower-left part of the screen.
4. By default, the **Network** tab is selected.
5. Click **Static IP addressing** and then manually specify the camera's *Hostname*, *IP address*, *Netmask*, and *Gateway*.

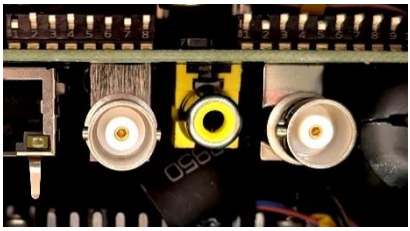


6. Users can also **specify the DNS Mode, Name Servers, MTU (maximum transmission unit), and Ethernet Speed**.

7. Click **Save**. Applying any changes on the Network screen **requires rebooting the camera**.

# 8.7- Connecting Analog Video (US-only models)

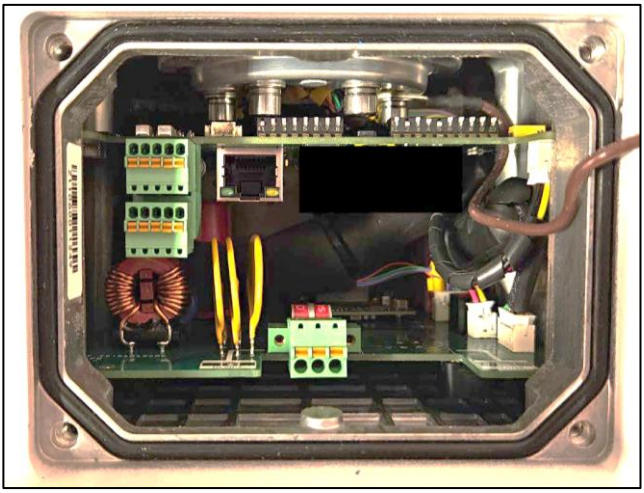


The **US-only models** feature analog video output. To connect analog video from the camera, **locate the RCA and BNC video output** connectors on the camera body. Use a standard RCA cable or BNC video cable to **link the camera's video output to the corresponding input** on your monitor, DVR, or video capture device. Ensure that the cable is **firmly seated** in both connectors to maintain a stable signal and avoid video interruptions.

After securing all connections, power on the camera and the receiving device; you should see live analog video displayed. Adjust the cable routing to prevent strain on the connectors and avoid placing the cables near sources of electrical interference to maintain optimal video quality.

# 8.8- 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.

# 9- Additional Configuration

When configuring the PT-Series AI SR camera and integrating it with a network and VMS, the setup process may involve enabling, disabling, or adjusting various settings through the camera's web interface. **The available settings for configuration are determined by user roles**, each associated with specific permissions. The following table outlines which settings are accessible for each user group.

| Settings | User Role |
|---|---|
| • Other networking settings<br>• Date and time<br>• Alarms<br>• Audio<br>• Live video and video<br>• Enabling and configuring streams external I/O devices<br>• Visible imager<br>• Notification emails<br>• Current and idle I/O states<br>• Onboard heaters and fans<br>• On-screen display (OSD)<br>• Cybersecurity<br>• Geotracking<br>• Map<br>• Georeference<br>• Scheduled tasks<br>• Recording<br>• Format a microSD card<br>• Firmware, factory defaults, and other system settings | Default admin user / any user assigned the admin or expert role |
| • Users, roles, and passwords | Default admin user / any user assigned the admin role |
| • Pairing one or more PT-Series AI SR with FLIR Edge AI Video Analytics with a FLIR Security PTZ camera that supports geotracking—see the corresponding pairing guide of the PTZ camera. | PT-Series AI SR with FLIR Edge AI Video Analytics: Default admin user / any user assigned the admin or expert role |

# 10- Attach the Camera to a Supported Video Management System

Once the camera has been mounted and its IP address identified or assigned, users may utilize the VMS Discovery and Attach procedures to connect the camera to a compatible Video Management System (VMS).

For more information, please refer to the VMS software documentation.

# 11- Thermal Imaging Overview

A thermal camera creates images by **detecting temperature differences** in its surroundings. Unlike visible light (daylight) cameras, which rely on photodetectors to capture reflected light from external sources such as sunlight or artificial illumination, **thermal cameras sense energy directly emitted by objects and surfaces**. This fundamental difference means that while visible light cameras—and even the human eye—depend on reflected light to reveal what's present within a scene, **thermal cameras can visualize environments regardless of lighting conditions**.

Objects in everyday settings rarely emit visible light due to their relatively low temperatures, but **all objects continuously radiate infrared energy within the long-wave infrared spectrum (LWIR)**. Thermal cameras are specifically designed to detect this energy, enabling them to capture imagery even from extremely cold items like ice and snow. With time, users tend to find it more intuitive to interpret scenes containing familiar objects in thermal imagery.


**The appearance of these thermal images is determined by palettes**—color schemes that map different temperatures to specific shades. For example, using the standard WhiteHot palette displays warmer areas in white and cooler ones in black, as seen in the image above. The **Palette** option on the **Thermal** settings allows users to customize how temperatures are visually represented in the image.

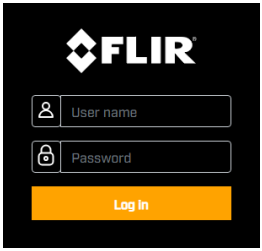
Thermal cameras automatically adjust **image contrast** for most conditions, but **users can manually refine these settings for improved clarity**. Outdoor installation or exposure to sunlight may affect performance at different times of day. For instance, after sunset, surfaces warmed by the sun can retain heat and appear warm in thermal images, whereas those same objects might seem cooler than their surroundings before sunrise. Thus, **effective interpretation of thermal imagery involves noting subtle changes across the scene**, not just concentrating on the most prominent hot spots.

# 12- Accessing the Camera's Web Interface

The camera can be **configured and used as a stand-alone unit** using the **web interface**. The camera's web interface supports Google Chrome® and other popular web browsers. This guide uses Chrome as reference.

## 12.1- Logging in to the Camera's Web Interface

1. Do one of the following:




- In the FLIR Discovery Network Assistant (DNA) tool, **double-click the camera in the Discover List**.
    - The DNA tool does not require a license to use and is a free download from Teledyne FLIR. Download the DNA tool, unzip the file, and execute the application (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, **enter your username and password**.

- When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, users need to log in with the camera's default credentials:
    - **Username**: admin
    - **Password**: admin

3. When logging in to the camera for the first time or for the first time after resetting the camera to its factory default:

- Specify **a new password** for the admin user.
- Create a password consisting of:
    - At least 12 characters.
    - At least one uppercase letter.
    - At least one lowercase letter.
    - At least one number.
    - Can include the following special characters: |@#~!$&<>+_-.,*?=
- **Log back in using the new password**.

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. When changing passwords via a web browser, it is essential to use HTTPS to safeguard the security of sensitive data.

# 13- Making Changes to Settings

The camera's configuration files store two sets of settings:

- **Factory Default Settings**: The original settings provided on the camera when it leaves the manufacturer. A partial factory reset restores all factory default settings except those on the System Settings.
- **Saved Settings**: These are the settings users save as they operate and configure the camera. When the camera reboots, it restores these settings, so changes made since the last save are lost.

**TIP**

Whenever possible, **test new settings before saving them**, since saving changes overwrites the previously saved settings.

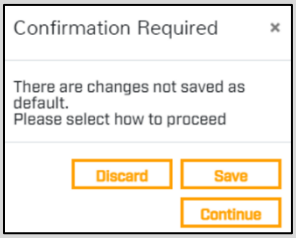
## 13.1- Camera Settings


Changing most Camera Settings activates the **Reset** and **Save** buttons. Some settings apply changes instantly without saving (like on the Thermal Page), while others require users to save before changes take effect. Select **Save** to keep all unsaved modifications since the last save.

**TIP**

If you move to a different page before saving your changes, a confirmation message will appear. You can:

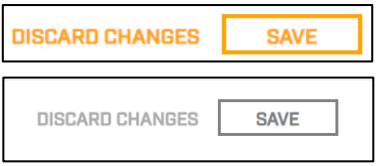
- Click **Continue** to navigate and test the changes, then return to save them.
- **Discard** the changes.
- **Save** the changes.
- Close the confirmation message without discarding or saving by clicking the **Close** icon.




To restore previously saved settings or factory defaults, click **Reset**. The camera can be restored to the last saved settings or to the factory settings. To close the message without restoring settings, click the close icon on the top-right corner.

# 13.2- System Settings

When users adjust most System Settings, the **Discard Changes** and **Save** buttons become active. Some settings are applied immediately but not saved (such as on the Alarm Page), while others require users to save before changes take effect.

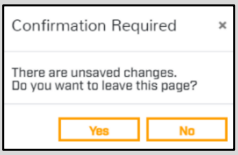



Click **Save** to keep changes, or **Discard Changes** to revert to the previous settings or factory defaults.

Some System Setting changes require the camera to reboot, such as those on the Settings and Date & Time page. After selecting **Save**, a confirmation message appears. To apply the changes and restart the camera, select **Accept**. To close the message without saving or discarding changes, select **Cancel** or the close icon.

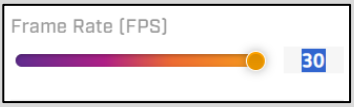
**TIP**

If you navigate away from a page before saving your changes, a confirmation message will appear. To leave the page and discard your changes, click **Yes**. To close the message without discarding or saving, click **No** or the close icon.



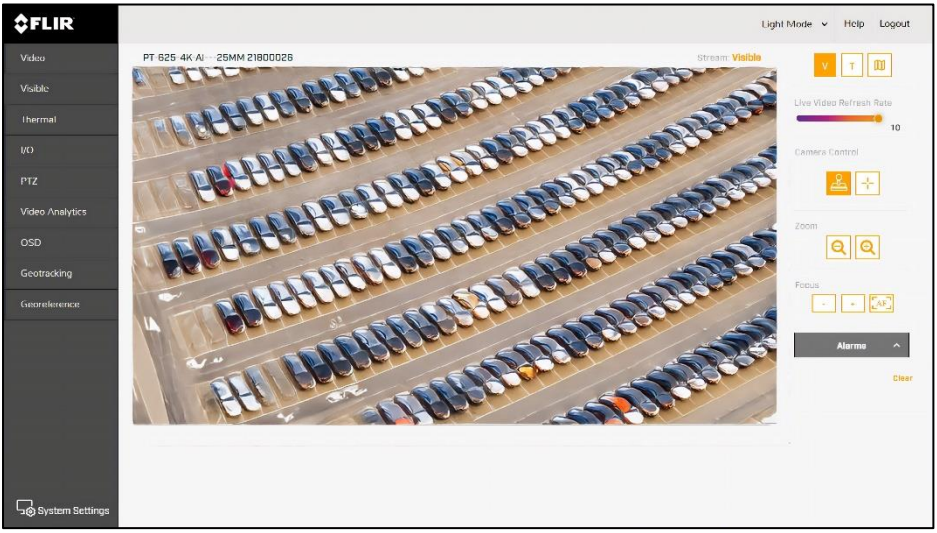

**TIP**

When adjusting sliders, you can either **slide the handle** left or right to change the value or **double click on the number and enter the desired value**, then pressing **Enter** to apply.



# 14- Web Interface Home Screen

The camera's web interface is organized to facilitate navigation and monitoring. The home screen is divided into sections that offer access to primary functionalities. The number of options displayed will depend on the user's role, for more information please see Users section.

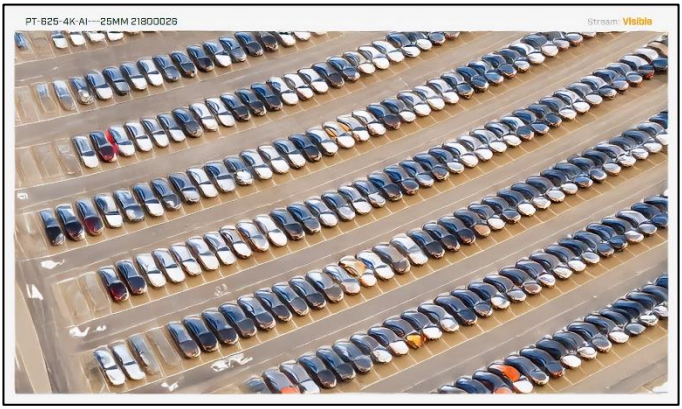



## 14.1- Top Navigation Bar


Located in the upper-right corner, this bar features:

6. **Light Mode**: Switches between light and dark display themes.
7. **Help**: Provides access to assistance through official guides or comprehensive documentation.
8. **Logout**: Exit the interface securely.

## 14.2- Main Video Feed Area




At the center of the window, users will see a live video feed from the camera, providing real-time surveillance visuals.

## 14.3- Video Feed Selector

Located on the top-right corner, it enables users to choose which video feed is displayed on the Main window:


- Visible spectrum.
- Thermal vision.
- Georeference map.

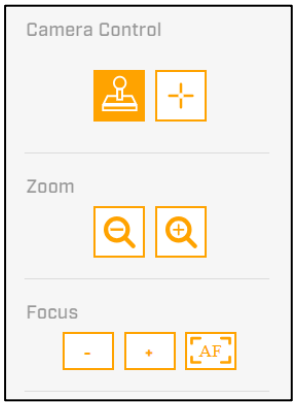
## 14.4- Live Video Refresh Rate Slider

The **Live Video Refresh Rate** slider, located above the Alarms section, adjusts the refresh rate for the Live video preview. It is important to note that this setting does not impact the video stream delivered by the camera via ethernet.


## 14.5- Recording Indicator

On the top-right corner, a circular icon indicates if the camera is recording its feed to the internal microSD card.

# 14.6- PTZ Control Panel

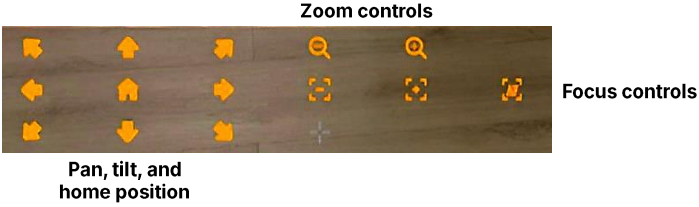



Located to the right of the Main Video Feed window, it provides users with different control methods to control the Pant, Tilt and Zoom of the camera.

- **Camera control**:
  - **Virtual joystick**: Users can click on the sides of the screen to move the camera in that direction. The further they click from the center of the screen, the faster the camera will move.
  - **Target**: When users click anywhere on the screen the camera automatically moves to center that point on the screen.
- **Zoom**:
  - Users can click on the **Zoom In** and **Zoom Out** buttons to adjust the area presented in the live feed.
- **Focus:**
  - Using the **(-)** and **(+)** buttons, users can adjust the focal point distance to ensure the object of interest is in perfect focus.
  - If users select **AF (Autofocus)**, the camera will automatically select the focus distance based on its algorithms.

# 14.7- Quick PTZ Controls

At the bottom-right corner of the live feedback video, users can find the **Quick PTZ Controls switch**. Selecting this switch displays, in the lower part of the video feed, **the full set of PTZ controls**, including pan, tilt, zoom, and focus. This enables users to **adjust the camera PTZ settings at any time**, even when the main PTZ control panel is not visible, such as during the editing of camera settings.



# 14.8- Left Sidebar - Camera Settings Menu


Available to Expert and Admin users only, this vertical menu provides quick access to the core camera settings:

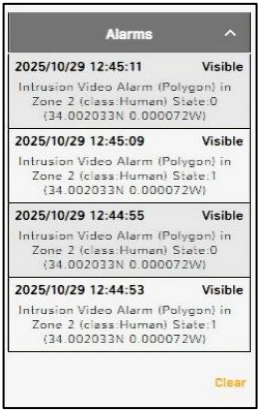
- **Video**: Configure the video stream, including codec, resolution, bitrate, etc.
- **Visible**: Configure specific settings for the visual spectrum video stream.
- **Thermal**: Configure specific settings for the thermal video stream.
- **I/O**: Configure internal and external input/output settings.
- **PTZ**: Configure different settings related to the pan, tilt and zoom functionality.
- **Video Analytics**: Configure Video Analytics, including managing regions and calibration.
- **OSD (On-Screen Display)**: Configure on-screen display elements, such as date and time and camera name.
- **Geotracking**: Configure the Geotracking functionality, including arming or disarming alarms and managing regions.
- **Georeference**: Enter the geographical camera information, including coordinates, height, tilt angle, etc.

Click the **System Settings** gear icon at the bottom of the sidebar to open the system configuration panel.

# 14.9- Right Sidebar – Alarms Section

This section lists recent alarms with detailed metadata:

- **Timestamp**: Date and time of the event.
- **Alarm Type**: e.g., Intrusion Video Alarm.
- **Zone Number**: Identifies the monitored area.
- **Coordinates**: Latitude and longitude of the detected event.

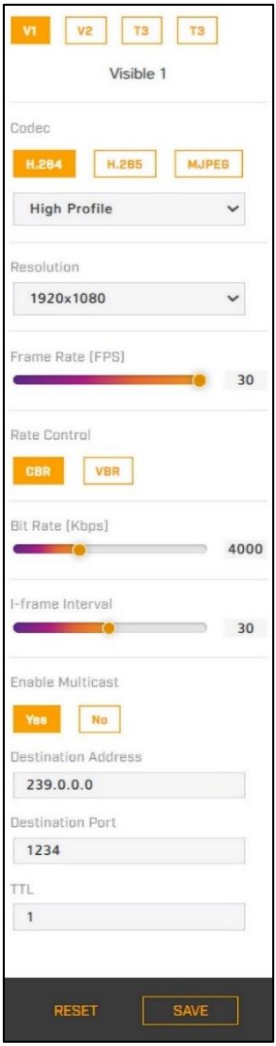


# 15- Camera Settings

## 15.1- Video

The camera delivers **four IP video streams** (two visible spectrum (V1 and V2) and two thermal (T1 and T2)). Typically, it is not required to alter the default video configurations. However, in certain instances—such as transmitting a stream over a wireless network—adjusting the video stream parameters may be beneficial for reducing bandwidth consumption.

To change the settings for a particular video stream, click the relevant button (T1 or T2).




### Codec Options

Choosing the right codec is crucial for ensuring compatibility with your intended workflow. The codec you select can impact the quality, storage requirements, and accessibility of your video footage. The available options are:

- **H.264**: This codec is widely used in security cameras for its high compression efficiency, which means it can deliver good video quality at lower bitrates. This helps in saving storage space and bandwidth, making it suitable for continuous recording and remote streaming.
- **H.265**: Also known as HEVC (High Efficiency Video Coding), this codec offers even better compression efficiency than H.264, providing higher quality video at lower bitrates. It's ideal for high-definition and 4K security cameras, as it allows for longer storage durations and smoother streaming without compromising on video quality.
- **MJPEG**: Motion JPEG compresses each video frame as a separate JPEG image. While it doesn't offer the same compression efficiency as H.264 or H.265, it is simpler and can be useful for applications where individual frames need to be accessed quickly, such as in forensic analysis or video editing.

## Resolution

This dropdown menu offers the different resolution options available for the video streams.

## Frame Rate

The frame rate can be adjusted within a range of 5 to 30 frames per second.

## Codecs, Quality, and Bandwidth

The video codec determines which settings are available. The values of those settings can have a significant impact on the quality and bandwidth requirements of the video stream.

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

- **Profile**:
  - **High Profile** (only available for H.264): Designed for HD TV applications, provides the best trade-off between storage size and video latency. Compared to Main Profile, it requires 10-12% less storage, but can experience increased latency, depending on the stream structure.
  - **Main Profile**: Designed for SD TV applications, provides good picture quality over lower bandwidth.
- **Rate Control**:
  - **CBR** (constant bit rate): The Bit Rate parameter defines the target bit rate; the camera attempts to keep the video at or near the target bit rate.
  - **VBR** (variable bit rate): The Bit Rate parameter defines the average bit rate.
- **Bit Rate (Kbps)**: The Bit Rate slider allows users to adjust the amount of data transmitted per second in the video stream. Increasing the bit rate typically results in higher video quality but also requires more bandwidth, while decreasing the bit rate can reduce bandwidth usage at the expense of video clarity.
- **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, users can set the:

- **Quality** (0-100).
  - Setting a higher value can increase the video stream's bandwidth requirements.
  - Teledyne FLIR recommends setting a value no higher than 80.

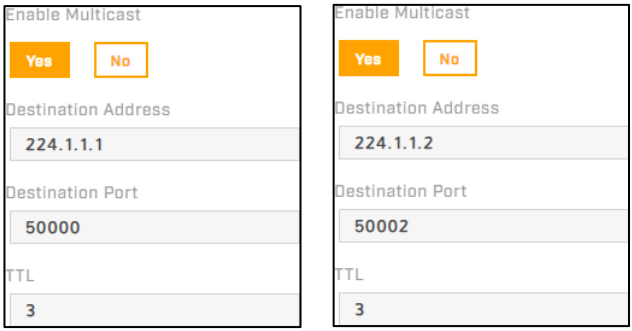
If you experience video issues when using MJPEG and high-resolution video, try adjusting the **Quality** and the **Resolution** settings.

## TIPS

1. **Initially use the default values.** Then, incrementally modify and test individual parameters to determine when bandwidth and quality requirements are met.
2. On the camera's web interface, **the live video is not an actual video stream.** Changes to stream settings might not affect the live video. Before saving changes, Teledyne FLIR recommends checking them using a FLIR UVMS, client program, or third-party ONVIF system.
3. Users can **view a snapshot of live video** using the following URL: http://<camera_IP_address>/images/snapshots/IRimage.jpeg.

## Enable Multicast

By default, **multicast is enabled**. Multicast video packets are distributed among streaming clients. The addition of more clients does not significantly increase bandwidth usage compared to unicast. Requests for video streams from ch0/stream1 are handled using unicast, meaning each client receives an individual stream. The way multicast requests are processed may vary depending on the client's capabilities or settings, which can influence whether the client receives a dedicated multicast stream or connects differently.




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.

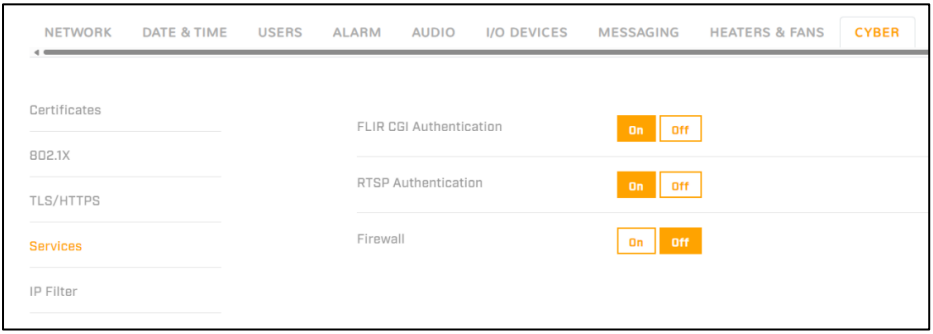
Video streaming uses a protocol generally referred to as RTP, the real-time transport protocol, although there are several protocols involved, including the Real-Time Streaming

Protocol (RTSP). The video stream URLs incorporate the IP address of the camera. The complete URLs are:

- **T1**: rtsp://<camera_IP_address>:554/stream1
- T2: rtsp://<camera_IP_address>:554:554/stream2

To maintain compatibility with legacy systems, the stream names are aliased as ch0 = stream1; and ch1 = stream2.

By default, **RTSP authentication is enabled**. To access any of the camera's video streams, users can use the name and password for any of the camera's users. Users assigned to the role of admin or expert can disable RTSP authentication on the Services section of the Cyber tab in the System Settings.



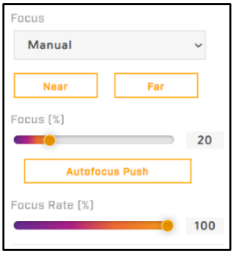

# 15.2- Visible

This section outlines the configurable video parameters available for the camera system's video streams. These settings enable precise adjustment of image quality and clarity, allowing users to tailor the video output to a variety of environments and operational needs. By making use of these controls, optimal performance and visual fidelity can be maintained across diverse applications.

## Image Settings

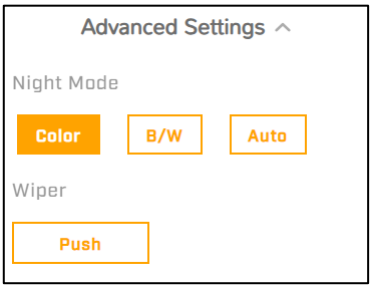
- **Brightness**: Adjusts the overall lightness or darkness of the video image. Increasing brightness makes the picture lighter; while decreasing it makes the image darker.
- **Contrast**: Controls the difference between the darkest and lightest parts of the image. Higher contrast makes shadows deeper and highlights brighter, while lower contrast results in a more muted appearance.
- **Hue**: Alters the overall tint of the video by shifting colors around the color wheel. This can be used to correct or change the general color balance of the image.
- **Saturation**: Modifies the intensity of colors in the video. Increasing saturation makes colors more vivid; while decreasing it makes them appear more muted or closer to grayscale.

- **Sharpness**: Enhances the definition and clarity of edges within the image. Higher sharpness makes details more pronounced, while lower settings produce a softer appearance.
- **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**. When Manual is selected, an additional set of controls is displayed:




  - **Near/Far**: Incrementally adjust the focus point.
  - **Focus (%)**: Select the focus distance, 0% being the closest focus point to the camera and 100% infinity.
  - **Autofocus Push**: Automatically overrides manual controls and performs a one-time autofocus operation.
  - **Focus Rate (%)**: Adjusts the value (speed) of the Near/Far increments.

## Advanced Settings




- **Night Mode**: Set the visible video to:
  - **Color** (day mode)
  - **B/W** (night mode)
- **Auto** (default): Automatically switches the visible video mode according to light level. When Night Mode is set to Auto, users can set the **Night to Day Threshold** at which the visible video switches between black and white and color. Move the slider 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.

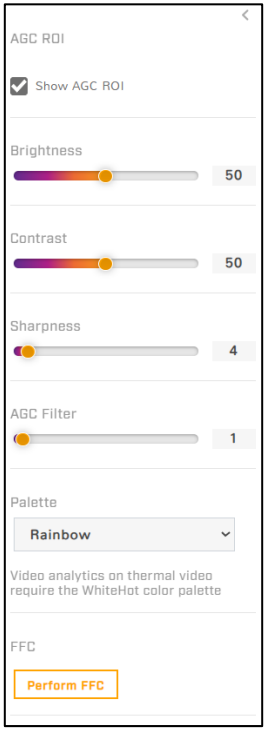
## Device Information

This pane, found at the bottom of the Visible panel, displays the firmware version of the visible sensor. This information is essential for troubleshooting and servicing the device.

# 15.3- Thermal

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

## AGC ROI




The AGC ROI, or **Automatic Gain Control Region of Interest**, **determines which part of the camera's image is analyzed to set the optimal brightness and contrast in thermal vide**o. By defining a specific area of the scene as the ROI, the AGC algorithm focuses on that region to adjust the overall gain, **ensuring that important details within the selected area are properly enhanced**, while less relevant parts of the image have less influence on the final output.

By default, the Show **AGC ROI option is enabled**. This setting **displays the AGC ROI overlay on the live video feed viewed through the camera's web interface**; however, **it does not appear in the recorded or transmitted video streams**. The ROI is initially defined as the entire frame, which allows the AGC algorithm to analyze and evaluate the full image for optimal gain adjustment.

**In some situations, it may be beneficial to specify a custom ROI that excludes certain areas of the scene**. For example, if the scene contains colder regions such as the sky, setting the AGC ROI to omit these areas can help reduce their influence on the overall image quality. By focusing the AGC algorithm on more relevant parts of the image, users can often achieve improved thermal contrast and detail in areas of interest.

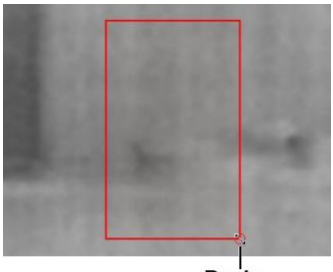
### WARNING

The camera's thermal Video Analytics rely on **accurate and adequate** AGC ROI settings. Changes to the ROI can affect VA.

## Defining a Custom AGC ROI

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

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




## Adjusting AGC ROI Image Settings

In some cases, adjusting the AGC image settings can improve the quality of the thermal image. The effectiveness of these changes often depends on factors such as personal preferences and the type of display device being used. By fine-tuning the available AGC parameters, **users have the flexibility to enhance image clarity, contrast, and overall visibility** to better suit their specific viewing conditions and requirements.

- **Brightness**: Determines the allocation of the 256 shades produced by the AGC. Values above 50 allocate more shades to hotter objects, while values below 50 allocate more shades to lower temperature objects. Range: 0 to 100.
- **Contrast**: 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.

### TIPS

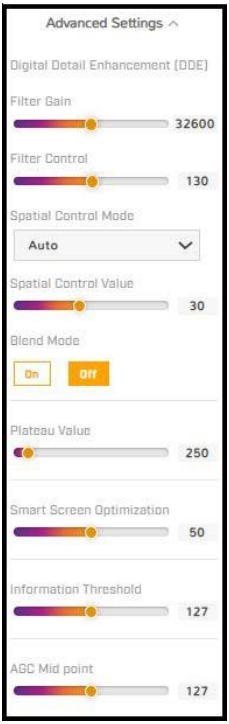
Changes to the default contrast setting **affect scenes with little temperature variation more than they affect scenes with greater temperature variation**.

- **Sharpness**: Enhances details and/or suppresses fixed pattern noise. Range: 0 to 100.
- **AGC Filter**: Determines how quickly a scene adjusts when a hot object enters (or exits) 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**: Selects the color palette the camera uses to indicate detected levels of thermal energy. WhiteHot and BlackHot are gray-scale palettes; other palettes assign different colors to different temperatures. When VA is enabled on the Video Analytics settings, the camera automatically uses the WhiteHot color palette.
- **FFC** (Flat-Field Correction): Is **a process used to maintain the accuracy and quality of thermal imaging**. To manually perform FFC, click the "Perform FFC" button. When FFC is initiated, the thermal imager's shutter temporarily closes, creating a uniform temperature reference. **This action allows the device to adjust for any changes in ambient temperature**, helping to ensure that the resulting thermal images remain accurate and reliable. During this adjustment period, the live thermal image will pause briefly while the

correction takes place. In addition to manual activation, **the camera automatically performs FFC at regular intervals or whenever it senses significant changes in ambient temperature**. This automatic adjustment further supports consistent image quality and device performance. The FFC process is also known as Non-Uniformity Correction (NUC), reflecting its function in correcting inconsistencies across the thermal image.

# Advanced Settings

## Digital Detail Enhancement (DDE)




- **Filter Gain:** is a key parameter in Manual Spatial Control Mode, determining the amount of gain the Digital Detail Enhancement (DDE) algorithm applies to image details. Users can specify a Filter Gain value within the range of 0 to 65,535. Setting the value to 0 disables DDE. For any value other than zero, the algorithm either attenuates or enhances details by a factor calculated as Filter Gain Value divided by 2,048. For example, setting the Filter Gain to 1 results in detail attenuation by 1/2,048, whereas a value of 8,192 yields a 4x enhancement of detail.

  The gain is applied both globally and locally to the low frequency portion of the image, making the effect of filter gain relative to the overall image content. In Automatic Spatial Control Mode, the camera automatically determines and adjusts the Filter Gain value as needed, optimizing detail enhancement according to the scene.

- **Filter Control:** Also referred to as the DDE Threshold, this setting determines the extent of detail enhancement applied by the algorithm when operating in Manual Spatial Control Mode. Users should specify a value within the range of 0 to 255; details above this threshold will not be enhanced by the DDE algorithm. In Automatic Spatial Control Mode, the camera autonomously sets and adjusts the Filter Control value based on scene content.

9. **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**.

10. **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.

11. **Blend Mode:** Allows the camera to address and minimize the appearance of halos that can be introduced by the Digital Detail Enhancement (DDE) process. When Blend Mode is enabled, the camera actively works to suppress these halos, resulting in a cleaner and more visually accurate thermal image. By default, Blend Mode is set to Off (disabled), meaning that halo suppression is not applied unless the user specifically enables this option.

12. **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.

13. **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.

14. **Information Threshold:** Specifies the differential between adjacent pixels utilized by the AGC algorithm to assess whether a local area contains *information*. Lowering the threshold increases the amount of information identified as present within the scene. Conversely, raising the threshold reduces this amount, producing an image where the depiction depends more on prominent details. Flat areas, such as sky or sea, are rendered with reduced contrast, while pixels surpassing the information threshold receive enhanced contrast. Range: 0 to 255.

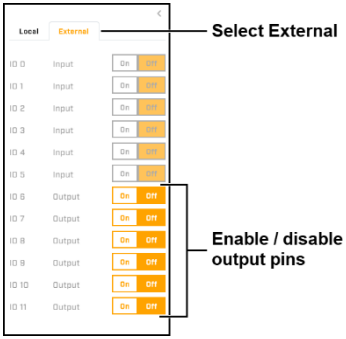
15. **AGC Mid Point:** Specifies the temperature corresponding to the midpoint among the 256 shades generated by the AGC. Raising this value enhances detail in higher temperature scenes while lowering it emphasizes detail in lower temperature scenes. Range: 0 to 255.

## Device Information

This pane, found at the bottom of the Thermal panel, displays information regarding the firmware and software version, serial and part number, and the FPA temperature. This information is essential for troubleshooting and servicing the device.

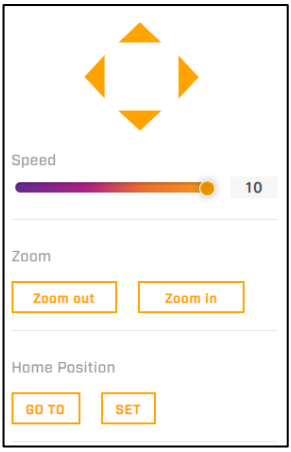
# 15.4- I/O (Input/Output) Configuration

On the I/O (input/output) panel, users can **configure the camera's external I/O settings** to suit their specific requirements. The external I/O section provides access to six input and six output pins. Within the I/O Devices settings, located in the System Settings menu, users with Admin or Expert privileges have the ability to configure the camera's external I/O connections. This includes specifying the devices that will manage these connections in conjunction with the camera.



# 15.5- PTZ

## PTZ Controls



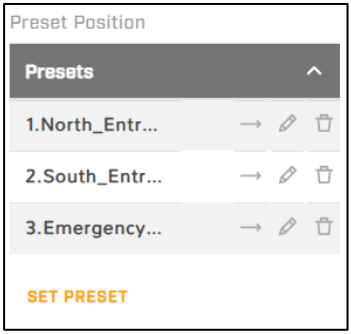

This set of controls enables users to adjust camera positioning and zoom levels to achieve optimal framing. The provided controls include:

- **Directional Pad**: By pressing the respective arrows, the camera moves up, down, left, or right, allowing precise adjustment of the viewing angle.
- **Speed Control**: This feature adjusts the speed of camera movement, with options ranging from 1x to 10x, enabling users to select the most suitable pace for their needs.
- **Zoom In/Out**: Operators can increase or decrease image magnification using dedicated buttons, providing flexibility to focus on specific areas within the scene.
- **Home Position**: Users can define the current camera position as Home Position by using the Set button. At any time, the camera can be returned to this recorded position by pressing the Go To button, ensuring quick access to a preferred viewpoint.

## Presets Positions

The Preset Positions menu allows users to **quickly save and recall specific camera viewpoints** for efficient and consistent monitoring. By configuring preset positions, users can ensure that the camera can return to key areas of interest in one click, streamlining surveillance operations and making routine monitoring tasks more effective.

To **create** a new Preset Position**:**




- **Navigate to the Preset Positions menu**: Access the PTZ controls section and select the Preset Positions option.
- **Position the camera**: Use the directional pad and zoom controls to move the camera to the desired viewpoint and adjust the zoom level as needed.
- **Save a preset**: Once the camera is correctly positioned, select Set Preset. A pop-up menu will be displayed where users need to provide a preset number and name.

To **recall** a Preset Position:

- To quickly return the camera to a saved viewpoint, **click on the Go To (→) button of the desired Preset Position**. The camera will automatically move to the saved position and zoom level.

To **rename** a Preset Position:

- To change the name of a Preset Position, **click on the Rename button (pencil) and enter a new name**.

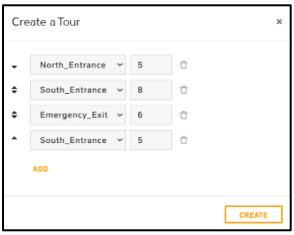
To **delete** a Preset Position:

- To permanently delete a Preset Position, **click on the Delete button (trashcan)**, a confirmation pop-up will be displayed prior to deleting the preset.

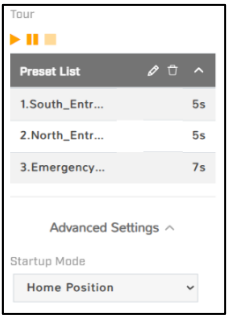
# Tour

The PTZ (Pan-Tilt-Zoom) tour feature allows users to **automate camera movement by cycling through a series of preset positions**. This functionality is useful for monitoring multiple viewpoints in sequence without manual intervention, ensuring comprehensive coverage of key areas.

To set up and use the PTZ tour:




- Navigate to the PTZ controls section and **select the Create Tour** option.
- **Add the desired preset positions** to the tour by **clicking on the Add button** and selecting them from the list and specifying the time the camera will stay in that position. Users can **rearrange** the order of presets in the tour, if needed, by **dragging the positions up or down on the list**.

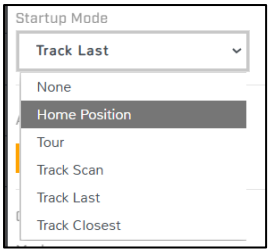



- **Start the tour by clicking the Play button**. The camera will automatically move through all the presets in the defined order and timing.
- Operators can **Pause** the tour by **clicking on the Pause button.**
- To **stop** the tour at any time**, click the Stop button**. The camera will remain in its current position.

# Advanced Settings

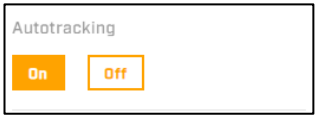
## Startup Mode

Startup Mode in Advanced Settings allows users to **select how the camera operates when it is powered on or restarted**. The available options are as follows:




- **None**: The camera returns to its factory default position upon startup.
- **Home Position**: The camera moves to the user-defined home position.
- **Tour**: The camera automatically initiates the tour of preset positions. This feature cycles through selected preset positions in a programmed sequence.
- **Track Scan**: The camera performs a tour that scans all active geotracks. Each geotrack is followed for a specified dwell time before moving to the next.
- **Track Last**: On startup, the camera tracks the most recently detected geotrack, allowing immediate attention to the last identified area of interest.
- **Track Closest**: The camera follows the geotrack that is closest to the PTZ camera at the time of startup, prioritizing nearby activity.

## Autotracking

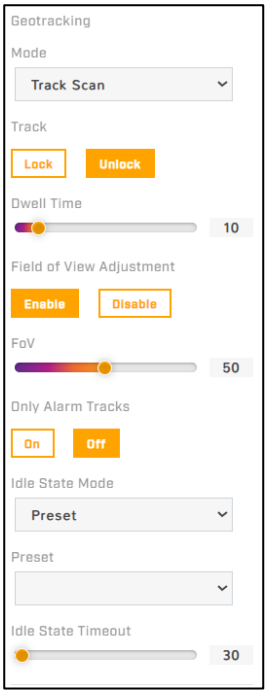



Using this switch, operators can enable or disable the Autotracking functionality. Autotracking is an advanced camera function that **enables the device to automatically follow moving subjects or objects** within its field of view. This feature uses intelligent algorithms to detect motion and keep the tracked target centered, allowing for hands-free monitoring in dynamic environments.

When Autotracking is enabled, the camera **prioritizes its own video analytics detections over the one coming from external compatible devices** such as radars, sensors or other geotracking enabled cameras.

## Geotracking

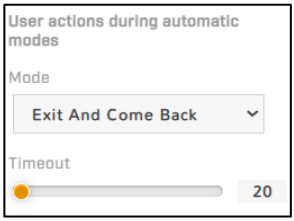
Within the geotracking pane, users can specify the behavior of the PTZ functionality for events associated with geotracking.




- **Mode**:
  - **None**: The camera doesn´t engage with any event received by geotracking.
  - **Track scan**: The camera cycles through active events.
  - **Engage last**: The camera engages with the last detected event.
  - **Engage closest**: The camera engages with the event that's closest to the camera.
- **Track**:
  - **Unlock**: When this setting is selected, the camera disengages from its current geotracking target, allowing it to resume normal automated patrols or respond to new incoming events.
  - **Lock**: Enabling this option secures the camera's attention on the current event, preventing it from switching focus to other geotracking triggers until the operator or system determines otherwise
- **Dwell time**: This parameter defines the duration for which the camera remains focused on a particular event before moving on to the next geotracking target or resuming its previous automatic mode. Setting an appropriate dwell time ensures that each event receives sufficient observation for effective monitoring, while maintaining efficient transitions between multiple active events.
- **Field of view adjustment**: When this option is enabled, the camera automatically adjusts its field of view to the object being tracked, making it easier for operators to assess the level of threat or follow its actions.
- **Field of view**: Using this slider, operators can specify the strength of the Field of View functionality, from 0 to 100.
- **Only alarm tracks**: When this option is enabled, the camera will only engage with tracks corresponding to an alarm, ignoring the ones that aren´t associated with one.
- **Idle state mode**: Defines what the camera does when there are no tracks to follow.
  - **None**: The camera remains static in the last position.
  - **Home position**: The camera goes back to the specified Home Position.
  - **Preset**: The camera moves to the chosen preset position. When this option is selected, a dropdown menu will appear, allowing operators to pick from the available preset positions.

- **Idle state timeout**: The amount of time, in seconds, the camera needs to be idle before executing the action defined in the previous menu.

## User Actions During Automatic Modes




The User Actions During Automatic Modes dropdown menu enables operators to specify **how the camera should respond when a user interrupts an ongoing automatic PTZ operation**, such as a tour or tracking mode, by providing manual input. The available options are described below:

- **None**: Selecting this option ensures that users cannot interrupt automatic operations. If a user attempts to execute a command, the system ignores it, and the automatic operation continues without any change.
- **Exit**: With this setting, when a user performs a manual command, the current automatic operation is immediately halted. The user is then able to control the camera freely. Once the user has finished their manual actions, the automatic operation does not resume automatically and must be restarted manually by the operator.
- **Exit and Come Back**: Choosing this option temporarily suspends the automatic operation when a user issues a manual command. After the manual intervention, if the user does not continue to control the camera for a duration specified in the Timeout slider, the automatic operation will resume automatically.

# 15.6- Video Analytics

PT-Series AI SR cameras are equipped with advanced **onboard AI Video Analytics** that utilize a 3D-optimized AI model. This system integrates **Deep Neural Network** (DNN) technology with sophisticated motion detection, delivering **FLIR Fusion AI** intrusion detection video analytics for enhanced scene understanding and security monitoring.

The analytics engine is capable of **classifying detected objects as either humans or vehicles**. Vehicle detection specifically covers cars, vans, small trucks, and vehicles up to 15 meters in length. However, the system is not designed to detect or filter larger vehicles such as long trailers, forklifts, or heavy vehicles with unique shapes, including construction vehicles.

Flir Fusion AI can be configured to monitor for specific activities within a scene. It supports the setup of **tripwires, intrusion zones, and loitering detection areas**, enabling targeted alerts and responses based on user-defined perimeters and behaviors.

## Detection Engines

PT-Series AI SR cameras use three distinctive detection engines to maximize the performance and effectiveness of the Video Analytics functionality:

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


**TIP**

Please note that **Fusion AI is used as a global preset**, if you select the Fuse DNN Area option in the advanced settings, every intrusion detection region set to DNN AI will change to Fusion AI and the regions set to Motion detection will stay set as Motion detection.

Please, see the Recommended Guidelines section to achieve >95% detection accuracy.

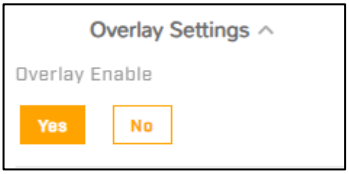
## Configuring Video Analytics

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

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

3. **Enable VA overlay**:

- Click on Overlay Settings. The overlay menu opens.
- Under **Overlay Enable, select Yes**.




4. **Enable VA**:

- At the top of the page, under Enable, select Yes.
- By default, VA is disabled.


5. **Calibrate VA**:

- See VA Calibration section.


6. Choose whether to enable **Fusion AI**:

- Click on **Advanced Settings**; the Advanced Settings section opens.
- Under **Fuse DNN Area**, select Yes or No.
  - Fusion AI is not applicable to Loitering Areas.

7. Specify **Motion Sensitivity Level**:

- In Advanced Settings, go to **Motion Sensitivity Level**.
- Click on the dropdown menu to choose the appropriate level.


| VA Configuration by Type of AI | Applicability |
|---|---|
| DNN AI | Detects Upright human intrusions. |
| Fusion AI - Low Motion Sensitivity* | Enables detection of discreet human intrusions at very close range. |
| Fusion AI - Medium Motion Sensitivity | Enables detection of discreet human intrusions at an optimal range. |
| Fusion AI - High Motion Sensitivity** | Increases maximum detection distance for upright and discreet human intrusions. |
| Fusion AI - Ultra Motion Sensitivity*** | Increases maximum detection distance for upright and discreet human intrusions. |

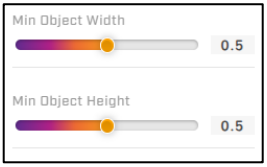
* Can handle minor camera movements and vibration

** Requires the camera to withstand wind gusts

*** Requires the camera to be stable, not move or vibrate

^ When Fusion AI is configured, vehicle classification is reliable up to 200 m detection distance

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



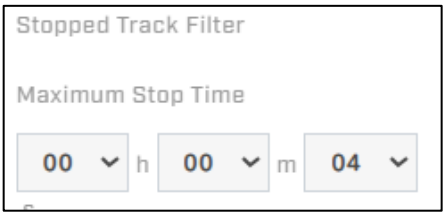

- In Advanced Settings go to Min Object Width and Min Object Height.
- Enter t**he correct value**:
  - Use the Teledyne FLIR recommended minimum width and height of 0.3 meters to filter out small animals, such as birds, cats, or rabbits.
  - To filter out larger animals such as dogs, foxes, etc., specify a larger minimum, 0.5 meters width and 0.6 meters height, or larger if necessary.
  - The minimum object width should not exceed 0,5 meters to accurately detect human intruders and not small animals such as the rabbits seen in the picture. You can reduce nuisance alarms from various animals by applying the recommended object size filter settings shown in the table:

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

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

- In Advanced Settings, go to Stopped Track Filter.

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

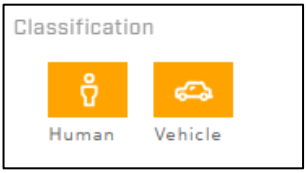



10. **Create VA Regions**:

- The camera's onboard VA detects intrusion or loitering and classifies detected objects separately for each region.
- To create regions and tripwires, see Creating VA Regions. For more information regarding these regions, see Types of Video Analytics Regions.

11. **Activate human and/or vehicle detection** in each region:

- Click on the name of the region.
- Under Classification, click on the Human and/or Vehicle icon to activate.
- In the VA tracking overlay, H indicates a detected and classified human; V indicates a vehicle.




12. **Configure the VA tracking overlay**.

- Expand the dropdown menu where users can enable or disable the following:

| Setting | | Comments |
|---|---|---|
| Enable | Globally enable or disable the VA overlay. | |
| Regions | Show intrusion regions, loitering regions, and trip wires. | |
| Human Tracks | Show detected objects classified as humans. | Enable Show Class, Show Lines, or Show Boxes. |
| Vehicle Tracks | Show detected objects classified as vehicles. | |

| | | |
|---|---|---|
| Show Class | When tracks are enabled, show the classification of the detected objects: human (H) or vehicle (V). | Enable Human Tracks or Vehicle Tracks. |
| Show Lines | When tracks are enabled, show the lines for the detected objects according to positions from prior frames; helps visually represent speed and direction. | |
| Show Boxes | When tracks are enabled, show a box around the track. | |
| Show Triggered | Show tracks only when they are active; that is, when they are triggering a trip wire, intrusion, or loitering alarm. | Enable Human Tracks or Vehicle Tracks.<br>Enable Show Class, Show Lines, or Show Boxes. |
| Streams | Enable the VA tracking overlay for individual video streams. | Does not override the global VA overlay Enable setting above. For the overlay to appear in a stream, the global setting and the stream must be enabled.<br>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. |

## TIPS

For information regarding how to configure the VA for specific situations and optimal detection results, see Recommended Guidelines.

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

## Video Analytics Calibration Check

Before users can check the camera's VA calibration, they need to **specify the camera's installation height, tilt angle, and roll angle** on the Georeference settings.


Verification of calibration is essential for accurately distinguishing between human and non-human intrusions. To perform this verification, select the **Display Target** button on the Visible or Thermal tab, and **request a person in the field to move to different locations** within the camera's coverage area, including both the closest and farthest points from the camera. When the person stops, **click on the corresponding position** on the screen to generate the **target box**. The detection human boxes indicate the standard height of a person. If the target box closely aligns with the actual size of the subject, the calibration is correct. Should the target box appear disproportionately large or small, please **recalibrate the camera in the** Georeferencing settings, changing the height, tilt, and roll values.


## TIPS

1. Make sure that a person about **1.8m (5" 11') tall** is in the camera's field of view.
2. On the Video Analytics page, make sure **analytics are enabled**.
3. Expand Overlay Settings and make sure **Overlay Enable is On**.

If the height of the box does not correspond to the size of the person:

1. On the Georeference settings, **verify the camera's installation height, tilt angle, and roll angle**. Mounting orientation (tilt) should ideally be at horizon level close to top of the scene.
2. When far away, if the **human box is too small**, the virtual horizon needs to be higher, so increase the tilt angle.
3. When far away, if the **human box is too large**, the virtual horizon needs to be lower, so decrease the tilt angle.

## Recommended Guidelines for Optimal Detection Results

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

- **Install the camera on a** stable fixed pole, 6 meters high, if possible.
- **Start the detection zone** 3-5 meters away from a fence line or boundary.
- **Apply to** flat surface terrains with no tall grass or slopes.

- **Use** Masking Level 2 or 3.
- Do not ap**ply Fusion AI to road facing scenes** with dynamic activity, such as frequent vehicle traffic.

## Types of Video Analytics Regions

There are two main types of regions in video surveillance systems: **Detection** and **Masking regions**.

**Detection regions** are user-defined areas within the video feed **where the system actively monitors and classifies objects,** such as humans or vehicles. These regions include **tripwires, intrusion detection areas, and loitering detection areas**, each serving a unique purpose in identifying and responding to potential security threats.

On the other hand, **Masking regions** are areas **where video analytics are intentionally disabled** to prevent false alarms caused by non-threatening movements, such as swaying trees or moving shadows. By strategically configuring both detection and masking regions, users can ensure that their surveillance system is both efficient and accurate, focusing on relevant activities while minimizing unnecessary alerts.

## Detection Regions:

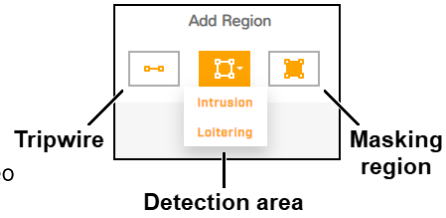
Detection regions can classify objects as humans or vehicles. These regions include:

- **Tripwires**:
  - Tripwires may be configured as either bidirectional (the default setting) or unidirectional. This configuration allows the system to monitor movement in both directions or in a single direction, depending on operational requirements.
- **Intrusion detection areas**:
  - Intrusion detection zones may be configured to utilize either Deep Neural Network (DNN) detection, which is the default setting, or Motion detection. DNN detection employs sophisticated algorithms to accurately identify and categorize objects, whereas Motion detection relies on monitoring variations within the video stream.
- **Loitering detection areas**:
  - Loitering detection areas enable users to define a specific loitering time, representing the period during which an individual or vehicle must stay within the designated area before an event is activated. This functionality is valuable for monitoring and identifying potentially suspicious activities or unauthorized presence in particular zones.

## Masking Regions:

Masking regions are areas of the video image where Video Analytics (VA) are disabled, and no alarms are triggered. These regions are useful for preventing false alarms caused by non-threatening movements, such as trees or bushes swaying in the wind. Users can create up to eight masking regions.

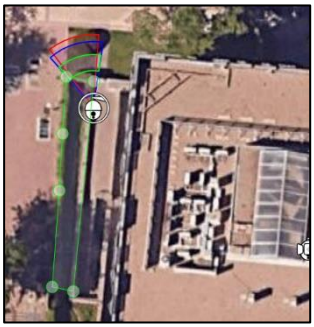
## Creating VA Regions




## Adding Regions

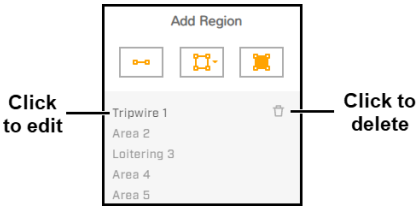
To add a region, select the **Map** tab in the Video Analytics pane and follow these steps:

1. **Tripwire**: Click the Tripwire icon to create a tripwire.
2. **Detection Area**: Click the Detection Area icon to create a detection area.
   - **Intrusion**: Select this option to create an intrusion detection area.
   - **Loitering**: Select this option to create a loitering detection area.
   - **Masking Region**: Click the Masking Region icon to create a masking region.
3. **Draw the region** by clicking on the map to add points to the polygon.
4. **Do not click and drag**.
5. Make sure the **regions do not overlap**.
6. To finish creating the region, **double-click on the last point** and a line will be drawn automatically closing the polygon.
7. To cancel creating a region, press **Esc**.



## Editing VA Regions

To modify the settings for or to delete an existing region, **select the region either from the region list or in the map**.




- To move **or adjust**:
  - **Region points:** click and drag the points.
  - **Tripwires:** click and drag the lines.
  - **Entire regions:** click and drag the border.
- To delete **a region**, click on the trash icon nest to its name.

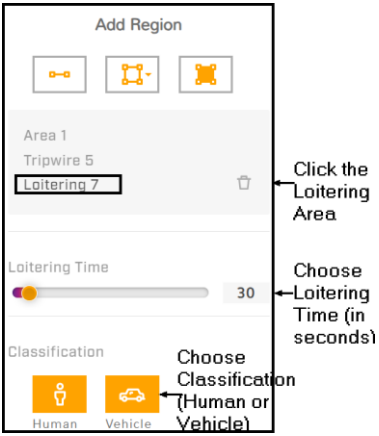
The specific configuration parameters vary depending on the region type, as seen in the table below:

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

## Configuring Loitering Detection Areas

To configure a Loitering Detection area:

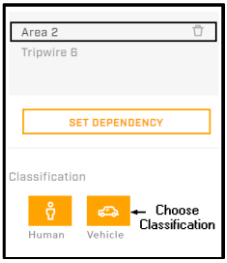
1. **Select the area from the list**: Options for Loitering Time and Classification are displayed.
2. **Choose loitering time** (0 - 600, in seconds).
3. **Choose Human and/or Vehicle Classification**.




## Configuring Intrusion Detection Areas

To configure an Intrusion Detection area:

1. **Select the area from the list**: Options for classification are displayed.
2. Choose **Human and/or Vehicle** classification.

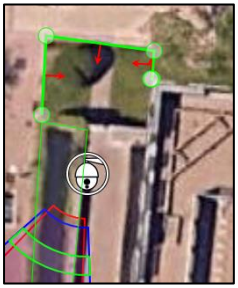


## Configuring Tripwires


To configure a Tripwire:

1. **Select the tripwire from the list**: Options for Direction and Classification are displayed.
2. **Choose bidirectional** (default) **or unidirectional** (left or right).
3. The direction selection arrows refer to the **direction of movement** over the tripwire.

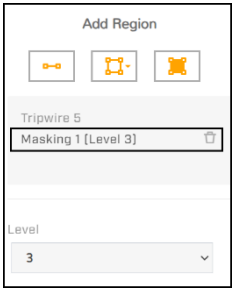
In this image, the tripwire has been completed, and the **left-to-right** button has been selected. Because detection direction relates to the first tripwire point created (bottom left) the **direction arrow in the video is always pointing towards the center since the direction changes with every turn of the tripwire**.



## Configuring Masking Regions

To configure a Masking region:

1. **Select the tripwire from the list**. Masking Level options are displayed.
2. For each masking region, users can **specify the level**:
3. **Level 3** (default): Completely blocks detection of all objects in the region.
4. **Level 2**: Apply for detecting normal upright and discrete human intrusions at 50% or above confidence level. Supported when DNN or Fuse DNN Area is enabled.




## Display Region Labelling

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

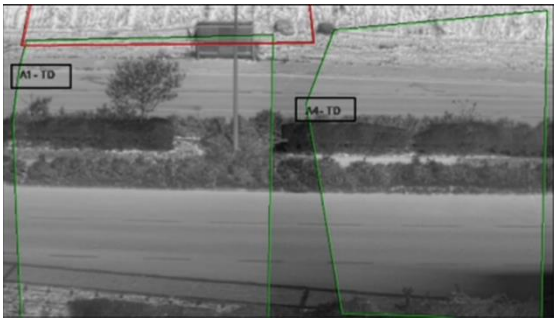
1. **Region type**: T = tripwire, A = intrusion detection area, or L = loitering.
2. **Unique region ID number**.
3. **VA type**: D=DNN, M=motion detection, DM=Fuse DNN Area enabled.

For example, **A2-DM= intrusion detection area 2 with Fuse DNN Area enabled**.

## Region Dependencies

In order to make the most of the Video Analytics, it is possible to establish the following dependencies between two regions:

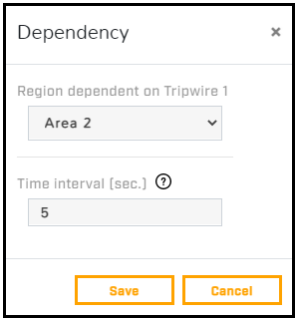
1. **Motion detection area to Motion detection area**.
2. **DNN area to DNN area.**
3. **DNN area to Fuse DNN area.**
4. **Fuse DNN area to Fuse DNN area.**




In the image above, Area 1 is dependent on Area 4. This means **that Area 1 will only trigger an alarm if Area 4 is triggered first**.

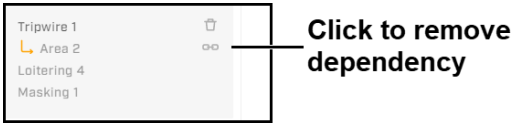
To **establish a dependency** between two regions:

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




To **remove a dependency:**

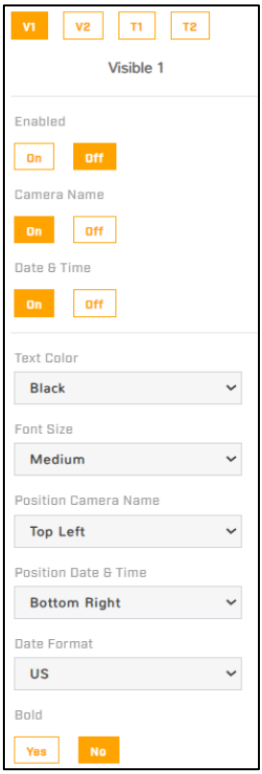
1. Click the link icon corresponding to the dependent region**.**



# 15.7- OSD (On-Screen Display)

Operators can independently configure each IP video stream (V1, V2, T1, and T2) with a range of **configurable On-Screen Display (OSD) options** to enhance usability and information clarity during monitoring.

To do so, operators need to s**elect which video stream they want to configure** using the stream selector at the top of the panel.




## OSD Feature Controls

- Operators can **enable or disable the OSD** for any camera stream as needed.
- It is possible to **turn on or off only the display of the camera name** independently.
- Similarly, the **date and time display can be enabled or disabled** separately from other OSD elements.

## Customizable Display Options

- **Text Color**: Choose between black or white text, with the option to add or remove a background for contrast and readability.
- **Font Size**: Select from small, medium, big, or giant font sizes to suit different display preferences and visibility requirements.
- **Camera Name Position**: Position the camera name at the top or bottom of the screen, and align it to the left, center, or right as needed.
- **Date & Time Position**: Place the date and time at either the top or bottom of the display, with left, center, or right alignment options.
- **Bold Text**: Enable bold formatting to further emphasize OSD information.

## Stream-Specific OSD Behavior

When OSD is turned on for the **V1 stream**, the OSD elements are visible in real time on the camera's web interface as part of the Visible video feed. Similarly, enabling OSD for the **T1 stream** displays the OSD elements live on the Thermal video feed accessible via the camera's web interface.

Turning on OSD for the V2 or T2 stream does not affect the live video shown on the camera's web interface.

# 15.8- Geotracking

The geotracking functionality **enables advanced spatial awareness and automated tracking capabilities** by integrating fixed cameras—such as the PT-Series AI SR—with FLIR Security PTZ cameras that support geotracking. Once paired, **the PTZ camera dynamically engages geotracks generated by the fixed camera's video analytics**, allowing for real-time object tracking across defined alarm regions and exclusion zones. This system leverages georeferenced mapping, calibrated coordinates, and classification filters to ensure precise detection and engagement of targets classified as people or vehicles. Configuration is managed independently from video analytics, offering flexible control over detection thresholds, virtual tracks, and camera behavior within mapped environments.


Intrusions have been detected and are being tracked.

## IMPORTANT

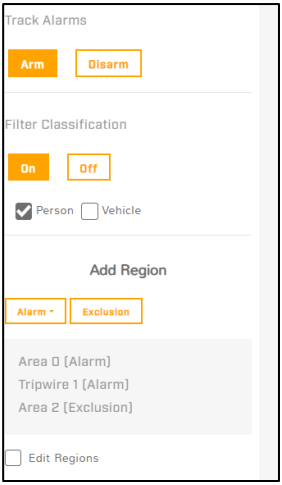
Before enabling geotracking, make sure that the **camera's VA is enabled** on the Video Analytics settings. However, even though geotracking requires the camera's VA to be enabled, geotracking configuration is separate from VA configuration.

## NOTE

Users can **pair more than one geotracking-enabled devices** with a FLIR Security PTZ camera that supports geotracking. When the cameras are paired, **the PTZ camera engages with the geotracks from the geotracking-enabled devices**.

| The following objects are recognized and displayed on the Geotracking and Georeference screens: | | | |
|---|---|---|---|
|  | Fixed camera—The circle around this icon indicates the FC-Series AI camera you are currently configuring. |  | Geotracking alarm region |
|  | PTZ camera |  | Geotracking exclusion region |
|  | Radar |  | Detected object |
|  | Geotracking range |  | Detected object in geotracking alarm region |
|  | VA detection range |  | Object engaged by PTZ camera |

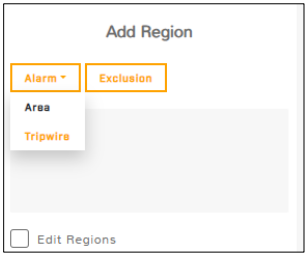
The Geotracking menu includes the following options:



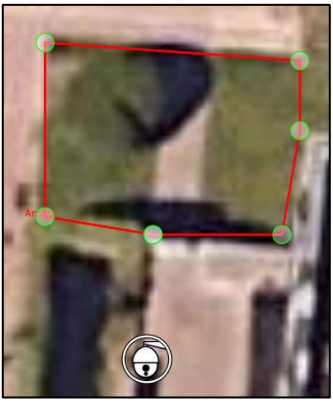

- **Track Alarms**: Allows users to activate or deactivate tracking using the "Arm" and "Disarm" buttons.
- **Filter Classification**: Enables filtering by object type including a toggle button ("On"/"Off") and checkboxes for "Person" (enabled) and "Vehicle" (disabled).
- **Add Region**: Lets users define new areas with options to add either "Alarm" (Areas or Tripwires) or "Exclusion" regions.
- **Regions List**: Displays existing regions and their types, such as "Area 0 (Alarm)", "Tripwire 1 (Alarm)", and "Area 2 (Exclusion)".
- **Edit Regions**: A button at the bottom which enables modifying the listed regions.

# Adding a Geotracking Region

1. **Select one of the Add Region options**:




- **Alarm (Area or Tripwire):** Triggers geotracking alarms. In the detection area display, alarm areas and tripwires are displayed in red. Users can specify a geotracking alarm region as the trigger for a camera alarm. When a camera is paired with a FLIR Security PTZ camera that supports geotracking, users can specify that the PTZ camera only engages with geotracking alarm tracks.
- **Exclusion**: The camera does not detect objects and does not trigger geotracking alarms. In the detection area display, exclusion regions appear in yellow. Exclusion regions can help eliminate alarms from a tree or bush moving in the wind, for example.



2. **Create the first point of the region** by clicking on the map.
3. **Continue adding points** by clicking on the map (up to 25).
4. To complete the region, **double-click on the last point users want to add**, and a line will be automatically drawn, closing the polygon.
5. To cancel creating a region, press **Esc.**

# Managing Geotracking Regions

## Editing Regions

To edit an existing region, select **Edit Regions**, and select the region by clicking its name on the list or the region on the map. Once selected, users can:

- **Move region points** by holding and dragging the points or **move the entire region** by dragging the region's border.
- **Define a tripwire's detection direction**.

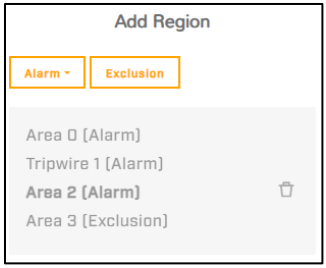
By default, tripwires are bidirectional. However, users can configure them to be unidirectional. When configured as unidirectional, the direction selection arrows refer to the **direction of movement over the tripwire as seen from the first tripwire point created**.

In this image, the tripwire was created by placing the top point first. Because of this, selecting the left arrow direction button produces a right facing arrow on the map.

Please note, when Edit Regions is selected, it is not possible to add regions.

### Deleting Regions

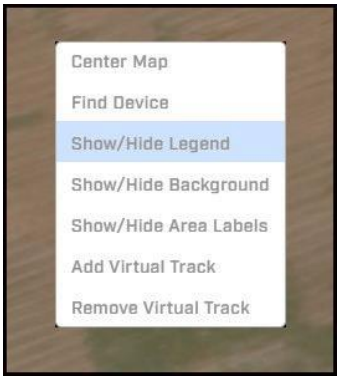
To **delete a region**, select the region and click the trash can icon next to it.




## Navigating the Map

To move the map, click and drag with your mouse. Use your mouse scroll wheel to zoom in or out.

Right-click on the map 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 users save the camera's coordinates or calibrate a map, the camera's position can be outside the display window.
- **Show/Hide Legend**: Toggles legend display.
- **Show/Hide Background**: Toggles the map or background image.
- **Show/Hide Area Labels**: Toggles area labels in the display.
- **Add/Remove Virtual Track**: Toggles a virtual geotrack that users can use to test features such as PTZ pairing and geotracking.

Please note that these right-click options are also available in the Georeference screen display.

# 15.9- Georeference

On the Georeference page, users can **specify the camera's geographical location and mounting information** needed for calibrating the geotracking and video analytics functionalities.

**NOTE**

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

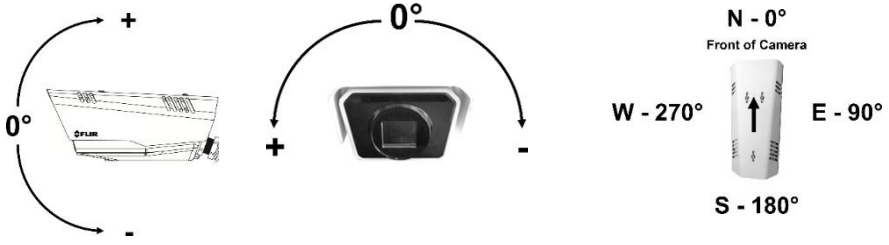
1. Identify the camera's **geographical information**, which includes latitude (specified as degrees North or South) and longitude (specified as degrees East or West), accurate to eight decimal places. Coordinates may be obtained using a map, a GPS-enabled mobile device, or the **Flir Raven site-planning tool** (see Using Flir Raven Site Planning Tool to Download the Map and Calibration Data**)**.


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 users do not save changes within a few seconds, the camera restores the previous latitude and longitude settings and moves the camera icon back.

2. Enter the **mounting information,** including:

- Ground Altitude: in meters above or below sea level, up to two decimals.

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




**Tilt** **Roll** **Orientation**

## TIPS

- Teledyne FLIR recommends **mounting the camera horizontally level**; that is, with a 0º installation roll angle. For accurate VA, mount the camera with an **installation roll angle within ±5º**.
- The camera's configuration files do not store factory default Georeference settings. **To restore Georeference settings to the camera's factory condition, manually change them to zero (0)**.

The camera can report georeference information via **FLIR NEXUS® SDK, CGI, or ONVIF**, which:

- Enables the user or an application to show the camera on a map including the direction the camera is facing, along with the camera’s detection range.
- Supports **cueing or showing tracks and I/O alarms**.

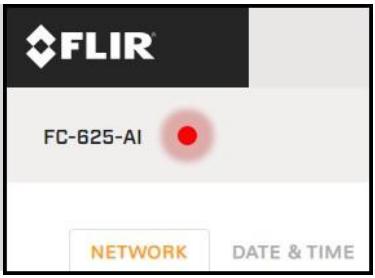
# 16- System Settings

Users assigned to the admin or expert roles are authorized to access System Settings. By choosing System Settings from the menu, they can navigate to the relevant configuration tabs. This access enables them to efficiently manage and modify system parameters and configurations, as necessary.

- Network
- Date & Time
- Users
- Alarm
- I/O Devices
- Messaging
- Heaters & Fan
- Cyber
- Media Browser
- ONVIF
- Map
- Geotracking
- Additional Interfaces
- Scheduler
- Recording
- SD Card
- Firmware & Info

**TIP**

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.

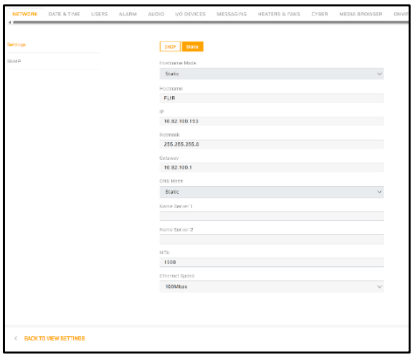



**IMPORTANT**

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

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

# 16.1- Network



The Network tab allows users to access and modify networking and SNMP (Simple Network Management Protocol) settings for system configuration. These settings are essential for ensuring proper device connectivity and communication within a networked environment.

If unsure about how to configure the networking or SNMP settings, it is recommended that you consult your network administrator for assistance. Proper configuration is important to maintain stable connectivity and optimal system performance.

The Network tab includes two different configuration panels: **Settings** 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.


### CAUTION

After changing the camera's IP address, the PC you are using to access the camera's web page **might no longer be on the same network** as the camera and access the camera's web interface. To access the web interface again, change the PC's IP address to be on the same network as the camera.

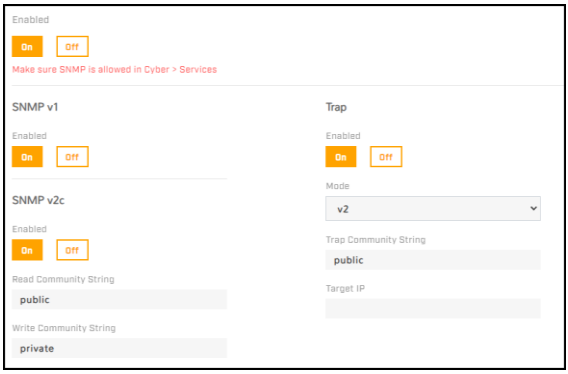
- **Netmask**: The default value is 255.255.255.0.
- **Gateway:** Specify the gateway address, which acts as an access point or IP router that the camera uses to communicate with devices outside its local network segment.
- **DNS Mode**: When the IP address mode is DHCP, users can set the DNS Mode to 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.

- **MTU**: Maximum Transmission Unit, the largest amount of data that can be transferred in one physical frame on the network. For Ethernet, the MTU is 1500 bytes (the default setting). For PPPoE, the MTU is 1492. Valid values are 1000-1500.
- **Ethernet Speed**: When set to 100Mbps (default), the camera supports 100Mbps. When set to Auto, the camera supports 10/100 Mbps.

## SNMP

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

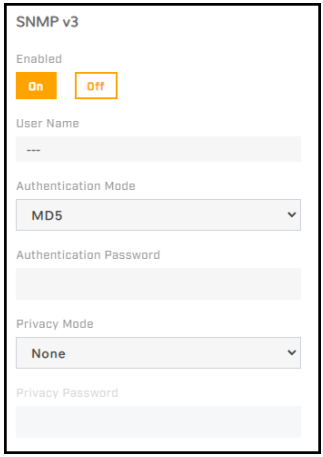



### IMPORTANT

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

- **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*.

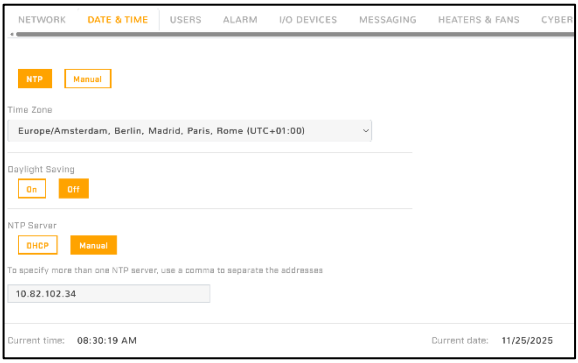
- **SNMP v3** introduces robust security features designed to protect network communications. It ensures **confidentiality** by encrypting packets, thereby preventing unauthorized sources from snooping. It also provides **message integrity**, guaranteeing that packets remain unaltered during transit and optionally includes protection against packet replay attacks. Additionally, SNMP v3 supports **authentication**, verifying that each message originates from a legitimate 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 it, 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.

# 16.2- Date & Time

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

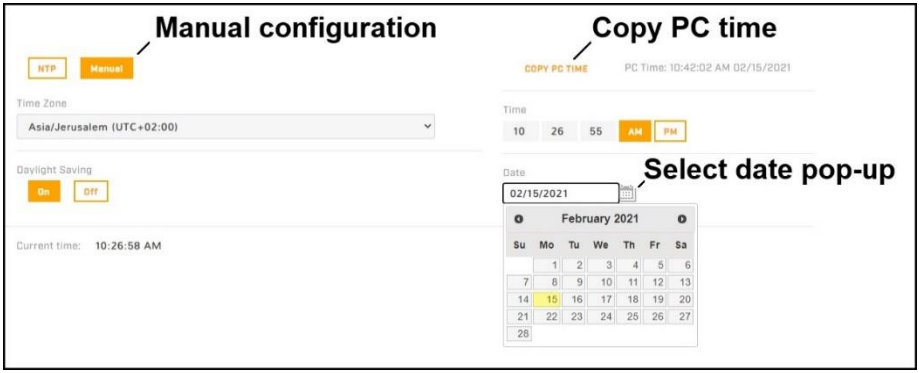



When DHCP IP addressing is enabled on the settings, users can configure the camera to **obtain the NTP server information from the DHCP server**.

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.

## Manually configuring the camera's time zone, time, and date

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



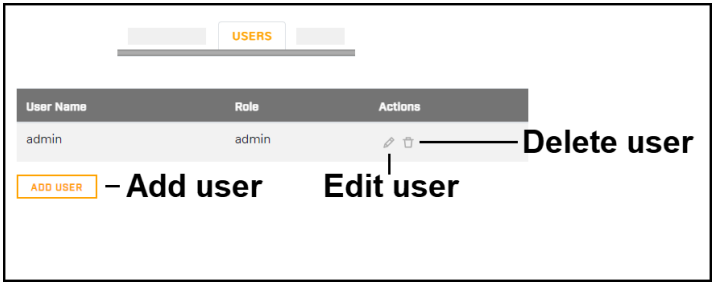
**TIP**

To **ensure that email notifications and other camera features work correctly, make sure the camera's system time is accurately set**. Users can configure email notifications on the Messaging settings.

# 16.3- Users

Only users who have been assigned the **Admin** role have the authority to add, edit, and delete users, as well as to change or set all passwords within the system. This ensures that sensitive user management functions are restricted to those with the necessary level of access.

Users assigned the **Expert** role are limited in their capabilities regarding user management. They can only view the account of the user currently logged in and do not have the ability to add, edit, or delete any user accounts. This restriction supports system security by limiting access to key administrative functions.




To maintain the security of the system, it is important to establish unique usernames and passwords for every required login account. The camera enforces a maximum username length of 29 characters.

## Password Requirements

- Passwords must be at least 12 characters long.
- Each password must contain at least one number.
- Each password must include at least one lowercase letter.
- Each password must include at least one uppercase letter.
- Passwords are required to contain at least one of the following special characters: | @ # ~ ! $ + _ - . , * ? =

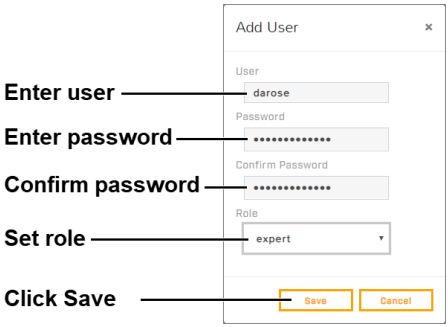
Assign one of the following roles, according to the level of access the user requires:

| Role | User | Expert | Admin |
|---|---|---|---|
| Access | Can:<br>• View live video<br>• View the Help page<br>• Log out | Can access and use all View Settings and System Settings pages, menus, controls, and | Can access and use all of the camera's web pages, including the Users page (but cannot |

| | | | |
|---|---|---|---|
| | | settings, except the Users page. | delete the default admin user). |
| | When the camera's video streams require RTSP authentication, accessing the camera's video streams requires the name and password for any camera user. All roles provide access to the camera's video streams. | | |

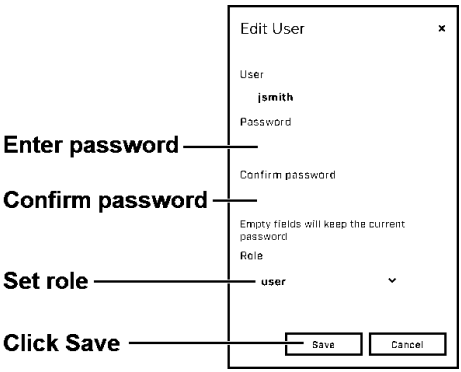
## Adding a User

- Open the Add User dialog box.
- Fill in the following fields:
  - **User** (e.g., "darose").
  - **Password** and **Confirm Password.**
  - **Role** selection (e.g., "expert").
- To retain the current password, leave the password fields empty.
- Click **Save** to create the user or **Cancel** to discard changes.

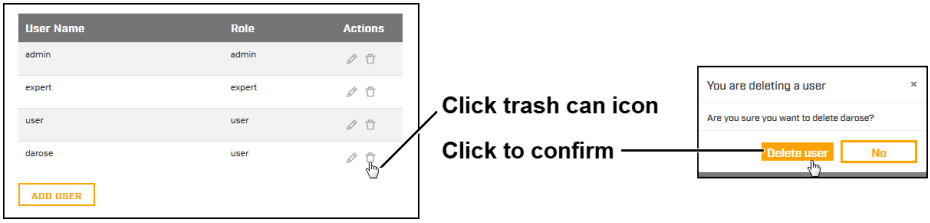



## Editing a User

- Access the **Edit User** dialog box. The **User** field is pre-filled and **cannot be changed**. To rename a user, delete it and create it again.
- **Update** the following, as needed:
  - **Password** and **Confirm Password**
  - **Role** selection (e.g., "user")
- Click **Save** to apply changes or **Cancel** to exit without saving.



# Deleting a User




- **Locate the user in the list** (e.g., "darose").
  - Click the **trash can icon** in the Actions column.
- A confirmation dialog will appear:
  - Click **Delete user** to confirm.
  - Click **No** to cancel the deletion.

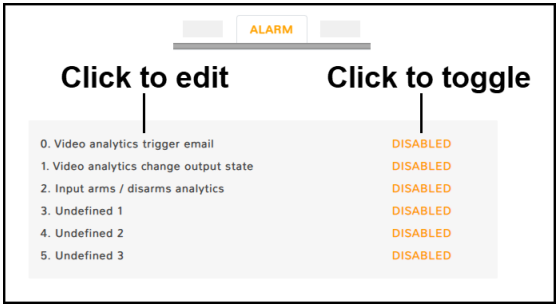
# 16.4- Alarm

Users can define camera alarms to be triggered by:

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

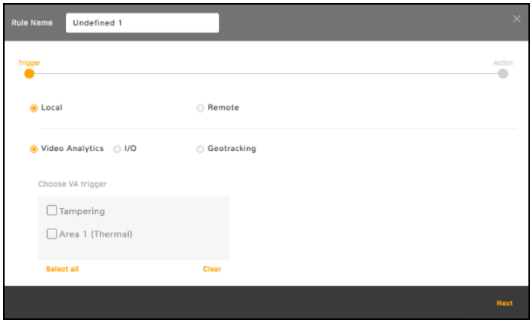
For each alarm, users can specify one or more of the following actions, such as:

- **Change the state** of local or external I/O connections, i.e., to turn on a light or play a prerecorded P.A. message.
- **Arm/disarm the camera's Video Analytics** (available when Video Analytics is not the rule's trigger).
- **Send a notification email.**
- **Save a snapshot image of the live video.**



## Modifying or Defining an Alarm Rule:

1. **Click the** alarm name. The rule trigger settings appear.
2. Modify or Define the **Rule Triggers**, see section below.
3. Modify or Define the **Rule Actions**, see section below.
4. Enable or disable a rule by clicking **Enabled** or **Disabled.**




## Modifying or Defining Rule Triggers

1. Modify or define the **rule name**.
2. Select whether the triggers are **local** (onboard the camera) or **remote** (external), see tables below.
3. Click **Next**. The rule action settings are displayed.
4. Continue with **Modifying or Defining Rule Actions**.

| **Local Triggers** | | |
|---|---|---|
| **Video Analytics** | **The camera's onboard VA** trigger this rule's action. | • On the Video Analytics settings, **make sure tripwires, intrusion detection and/or loitering regions have been defined**.<br>• **Select the tripwires and/or regions** that trigger this rule's action.<br>• **Users can also select tampering as a trigger**. After the camera has been powered on for 24 hours, blocking the thermal sensor of the camera for one minute triggers this rule's action. |
| **I/O** | **Local:** The camera's local I/O connections trigger this rule's action. | • On the I/O settings, **make sure local I/O connectors have been properly configured**.<br>• **Select one or more local I/O connections** that trigger this rule's action. |

| | | |
|---|---|---|
| | **External:** The camera's external I/O connections trigger this rule's action. | • On the I/O settings and on the I/O Devices settings, **make sure the external I/O connections and the device managing those connections with the camera have been properly configured**.<br>• Select **one or more external I/O connections** that trigger this rule's action. |

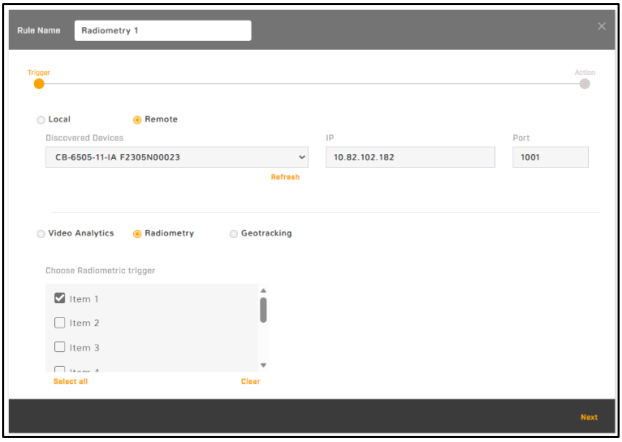
**TIP**

Specifying a trigger for an alarm rule and enabling the rule **does not enable alarms for the trigger**, make sure VA/geotracking is enabled.

| **Remote Triggers** | | |
|---|---|---|
| 1. **Select the triggering device** from the Discovered Devices drop-down menu:<br>The IP address and port are displayed.<br>2. Users can also **manually specify** the remote device IP address and port.<br>3. Click **Refresh** to save. The drop-down menu of discovered devices is also refreshed.<br>○ Click Refresh once the remote device is connected to the same network as the camera.<br>○ The camera discovers supported devices on the same network as the camera. However, users **can only use devices on the same VLAN as the camera as a trigger**. | | |
| **Video Analytics** | **VA from a supported remote camera or device** trigger an alarm. | • On the remote camera or other device, **make sure VA is enabled and that at least one tripwire, intrusion detection/loitering region, or another analytics item has been defined**.<br>• **Select one or more VA items** that trigger this rule's action. |

| | | |
|---|---|---|
| **Radiometry** | **Radiometry from a supported device** triggers an alarm. | • On the remote device, **make sure radiometry detection is enabled and that at least one temperature threshold or region of interest has been defined**.<br>• **Select one or more radiometry conditions** that trigger this rule's action. |
| **Geotracking** | **A remote geotracking device** triggers an alarm. | • On the remote geotracking device, **make sure detection is enabled and that at least one alarm area, tripwire, or other area has been defined**.<br>• **Select one or more geotracking device areas** that trigger this rule's action. |

The image below shows a discovered camera selected as the remote device and its radiometry item 0 selected as the trigger.



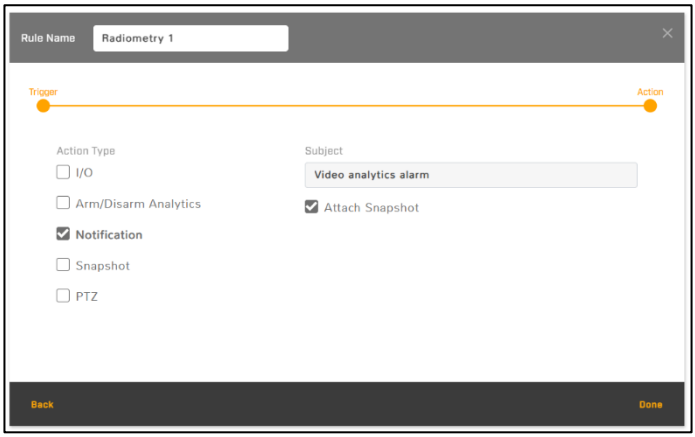

## Modifying or Defining Rule Actions

1. For the alarm rule you are modifying or defining, **select the checkbox for one or more action types**, see table below.
2. To configure an action type, **click the selected action type**. The selected action type is shown in bold, and the relevant settings are displayed.
3. Click **Done**.

<table>
<tr><th colspan="2">Action Type</th></tr>
<tr><td rowspan="2">I/O</td><td>Under I/O List, select Local or External:<ul><li>Local: This rule changes the state of one or more local output pins.<ul><li>On the I/O settings, make sure local I/O connectors have been properly configured.</li><li>For each trigger defined for the alarm rule, select the local output pin that changes.</li></ul></li><li>External: This rule changes the state of one or more local output pins.<ul><li>On the I/O settings and on the I/O Devices settings, make sure the external I/O connections and the device managing those connections with the camera have been properly configured.</li><li>For every trigger defined for the alarm rule, select the external output pin that changes.</li><li>Users can map individual local or remote triggers to specific local or external output.</li></ul></li></ul></td></tr>
<tr><td>Bound:<ul><li>When selected, the camera changes the state of the output when the alarm is triggered and when it is cleared.</li><li>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. Users can configure the Reset Interval for the local outputs on the I/O settings and for the external outputs on the I/O Devices settings.</li></ul></td></tr>
<tr><td colspan="2">Arm/Disarm Analytics (not available when this rule's trigger is Local > Video Analytics): When triggered, this rule toggles the camera's onboard VA from enabled to disabled or vice versa.</td></tr>
<tr><td colspan="2">Notification: When triggered, this rule sends notifications according to the settings on the Messaging Page. Specify a subject for the notifications. For email notifications, specify whether the camera attaches a snapshot.<br><br>When notifications are enabled for an alarm rule, the camera sends all configured notifications. It is not possible to enable or disable individual notification types. Therefore,</td></tr>
</table>

| |
|---|
| to differentiate between notifications triggered by the camera's onboard VA, Teledyne FLIR recommends configuring alarm rules for each type of VA region (tripwire, intrusion, and loitering). Then, specify different subjects for each rule's notifications. |
| **Snapshot:** When triggered, this rule **records a snapshot image of live video**. |
| **Arm/Disarm Geotracking** (not available when this rule's trigger is the camera's onboard geotracking)**:** When triggered, this rule **toggles the camera's onboard geotracking alarms** from enabled to disabled or vice versa. |

The image below shows that the previously configured rule triggers a notification, including a snapshot of the video. Sais notification is configured in the Messaging tab.

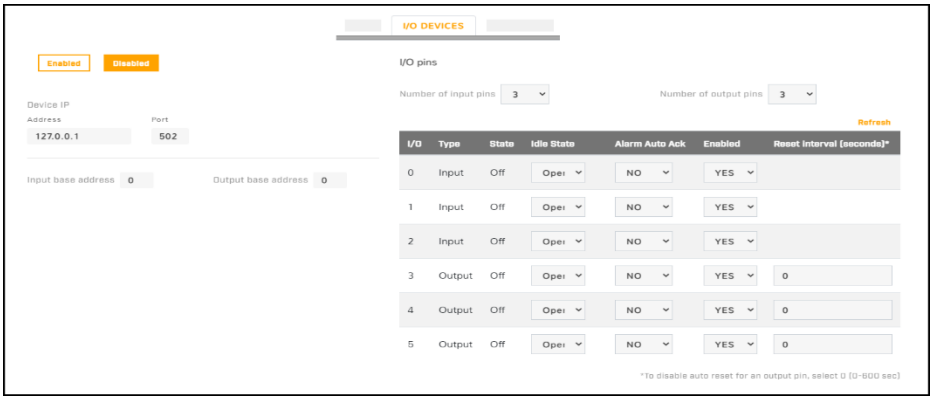


# 16.5- I/O Devices

In the I/O Devices settings, users can **configure the camera's external I/O connections** and the **device managing those connections** with the camera.

The following options can be configured for the device managing the external I/O connections:

- **Enabled** or **Disabled**.
- **Device IP address** and **port**.
- **Input** and **output** base addresses.
- The **number of input and output pins** the device manages.




For each pin, the following information is displayed and can be configured:

- **I/O pin number.**
- **Type**: Input or Output.
- **State**: The pin's current state (Open or Closed).
- **Idle State**: Normally Open or Normally Closed.
- **Alarm Auto Ack**: Yes or No.
- **Enabled**: Yes or No.
- **Reset Interval** (for output pins only): Between 0-600 seconds; to disable auto reset for an output pin, select 0.

Additional details on configuring the device that manages external I/O connections can be found in the device's documentation.

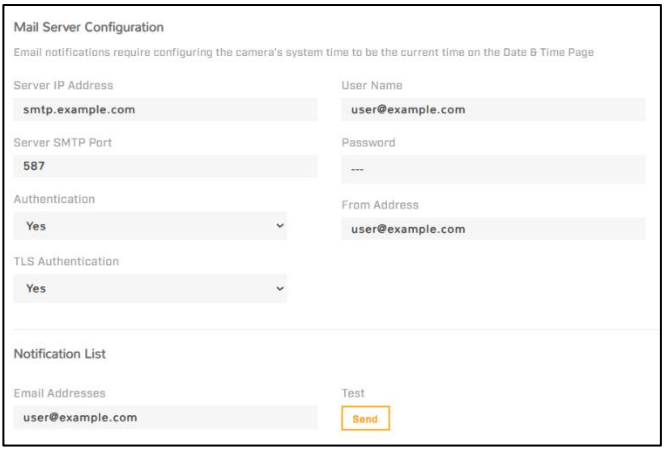
# 16.6- Messaging

As an action for an alarm rule, the camera can **send notifications** in the following formats:

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

## Configuring Email Notifications

To enable email notifications from the camera, follow these steps:




- **Server IP Address:** Enter the SMTP server address provided by your email service (e.g., smtp.example.com).
- **Server SMTP Port:** Enter the SMTP port number. The default for TLS is usually 587.
- **User Name:** Enter the email account username (e.g., user@example.com).
- **Password:** Enter the password for the email account. *Note: The password field may be hidden for security.*
- **From Address:** Enter the email address that will appear as the sender (e.g., user@example.com).
- **Authentication:** Select Yes if your SMTP server requires authentication.
- **TLS Authentication:** Select Yes to enable TLS encryption for secure email transmission.
- **Email Addresses:** Enter the recipient email address(es) that should receive notifications (e.g., user@example.com). Separate multiple addresses with commas.

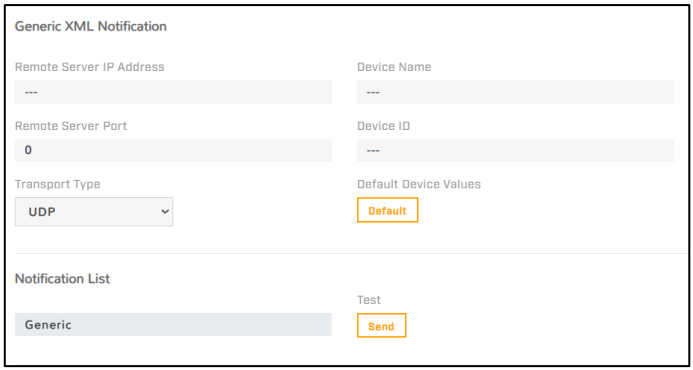
- **Test:** After entering all settings, click the **Send** button to send a test email and confirm that notifications are working correctly.

**NOTE**

- **Email notifications require the camera's system time to be accurately set**. Go to the Date & Time page to verify or adjust the system time.

## Configuring Generic XML Notifications

To enable generic XML notifications from the camera, follow these steps:

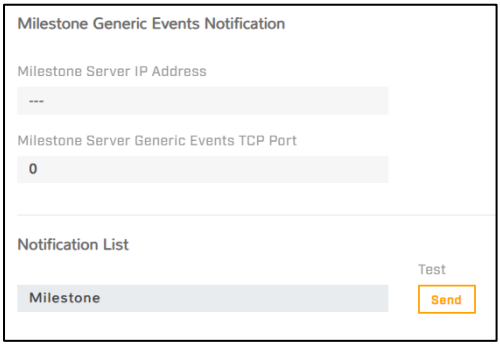



- **Remote Server IP Address:** Enter the IP address of the remote server that will receive the XML notifications.
- **Remote Server Port:** Enter the port number used by the remote server to receive notifications (e.g., 0 by default; update as required by your system).
- **Transport Type:** Select the transport protocol for sending notifications. Choose between UDP and other available options as required by your server.
- **Device Name:** Enter a name to identify the device sending notifications. This helps distinguish between multiple devices on the same server.
- **Device ID:** Enter a unique identifier for the device, if required by your notification system.
- **Default Device Values:** Click the **Default** button to reset device-related fields to their default values.
- **Notification List:** The field displays the current notification profile (e.g., Generic). This is typically pre-set and may not require changes.

- **Test:** After configuring all settings, click the **Send** button to send a test notification and verify that the server receives it correctly.

## Configuring Milestone Generic Events Notification

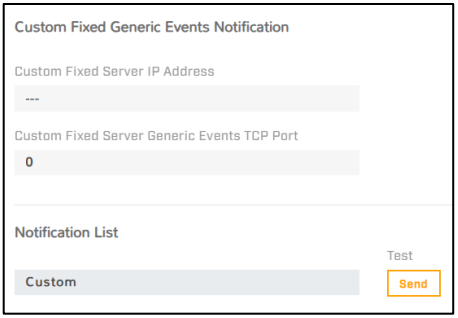
Follow these steps to set up Milestone Generic Events notifications for your camera:




- **Milestone Server IP Address:** Enter the IP address of the Milestone server that will receive generic event notifications.
- **Milestone Server Generic Events TCP Port:** Enter the TCP port number used by the Milestone server for receiving generic events (e.g., 0 by default; update as required by your system).
- **Notification List:** This field displays the current notification profile (e.g., Milestone). It is typically pre-set and does not require changes.
- **Test:** After configuring all settings, click the **Send** button to send a test notification and verify that the Milestone server receives it correctly.

## Configuring Custom Fixed Generic Events Notification

Follow these steps to set up Custom Fixed Generic Events notifications for your camera:




- **Custom Fixed Server IP Address**: Enter the IP address of the custom server that will receive generic event notifications.

- **Custom Fixed Server Generic Events TCP Port**: Enter the TCP port number used by the custom server for receiving generic events (e.g., 0 by default; update as required by your system).
- **Notification List**: This field displays the current notification profile (e.g., Custom). It is typically pre-set and does not require changes.
- **Test:** After configuring all settings, click the **Send** button to send a test notification and verify that the custom server receives it correctly.

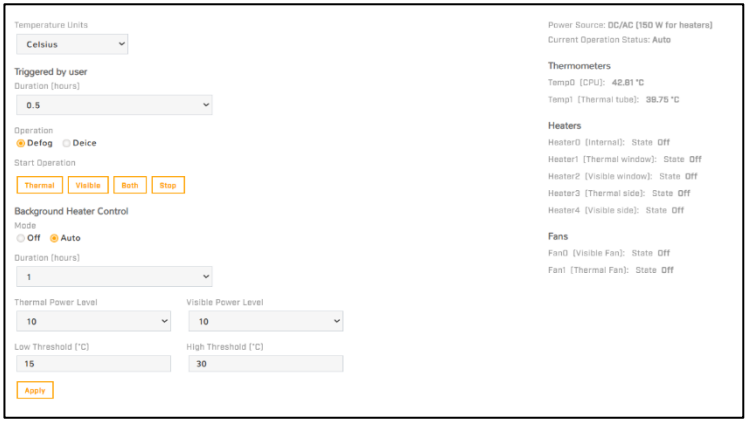
# 16.7- Heaters & Fans

The Heaters & Fans settings provide configuration for:

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

By default, the **Background Heater Control is turned off**. When configuring the camera, it is recommended to **turn on Auto Mode**.

The thermometer readings, heaters, and fans will function **based on the user supplied settings** of the Background Heater Control.




## Background Heater Control

By default, background heater control is set to Off. If you enable it, specify:

- **Thermal Power Level** (0-15): adjusts the **intensity or output of the heater** when it is active, being 0 the lowest setting and 15 the maximum.
- **Temperatures at which the heaters activate** (Low Threshold) **and deactivate** (High Threshold). It is recommended to set:
  - **Low Threshold**: 5 degrees below the ambient temperature.
  - **High Threshold**: 10 degrees above the ambient temperature.

It is also possible to select the unit of temperature: Celsius, Fahrenheit, or Kelvin.

## IMPORTANT

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

## To manually activate defogging:

1. Under Triggered by user, **select the duration** (0.5, 1, or 2 hours).
2. **Select Defog**.
3. Click **Thermal, Visible or Both**. The status of the thermal window heater changes from Off to On. To deactivate the operation, click **Stop**.

## Status Information

On the right side of the window, the following status information is displayed:

- **Power Source**: Indicates which power supplies are connected to the camera (PoE+ / DC / AC).
- **Thermometers:** Temperatures for camera components.
- **Heaters:** Status of the camera's heaters (On or Off).
- **Fans:** Status of the camera’s fan.

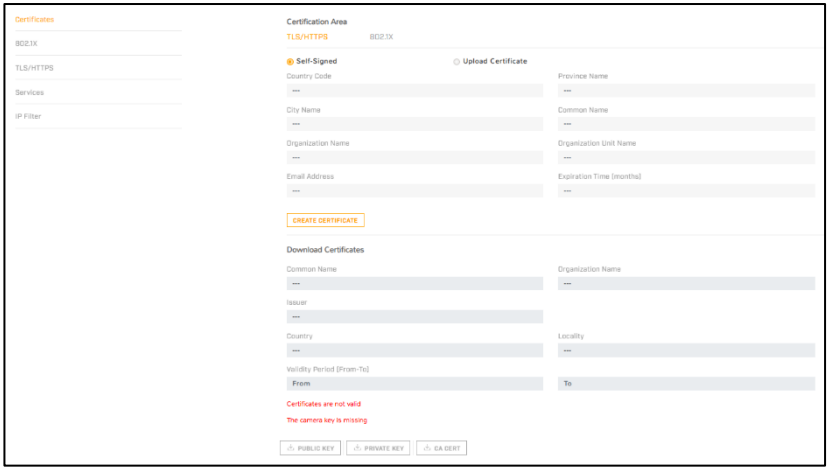
# 16.8- Cyber

The Cyber settings provide security configuration settings for:

- **Certificates.**
- **802.1Z.**
- **TLS/HTTPS.**
- **Services.**
- **IP Filter.**

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

## Certificates




Prior to enabling TLS/HTTPS or 802.1X, it is necessary to **generate or upload a valid certificate**. This can be accomplished using the camera's web interface to either create a self-signed certificate, upload an existing self-signed certificate, or upload a certificate issued by a trusted third party. If assistance with these configurations is required, please consult 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, users can download certificates and keys previously uploaded to or generated by the camera. If the certificate saved on the camera is self-signed, users can download the private and public key files. If the certificate was signed

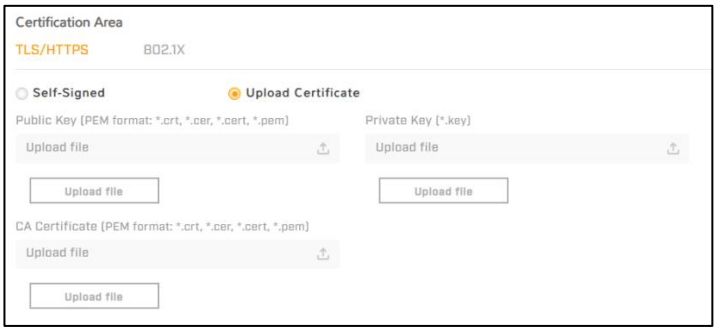
by a third-party CA, users can download the CA Certificate and the private and public key files.

### Generating and installing a self-signed certificate for TLS/HTTPS

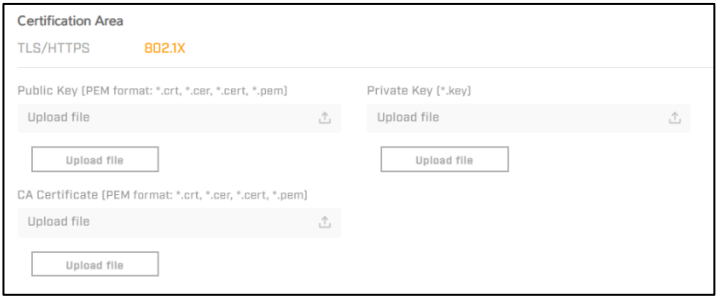
1. In the Certificates section and Certification area, select **TLS/HTTPS** and **Self-Signed**.
2. Enter information such as country code, city name, and organization name.
3. Click **Create Certificate**.
4. Allow 15 seconds for the camera to generate the certificate, at which point a confirmation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

### Uploading a self-signed or third-party CA signed certificate for TLS/HTTPS or for 802.1X

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




*To Upload a Certificate for TLS/HTTPS*

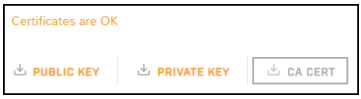



*To Upload a Certificate for 802.1X*

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

- **Select the Public Key file.**
- **Click on Upload File.**
- **Select the Private Key.**
- **Click on Upload File.**

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



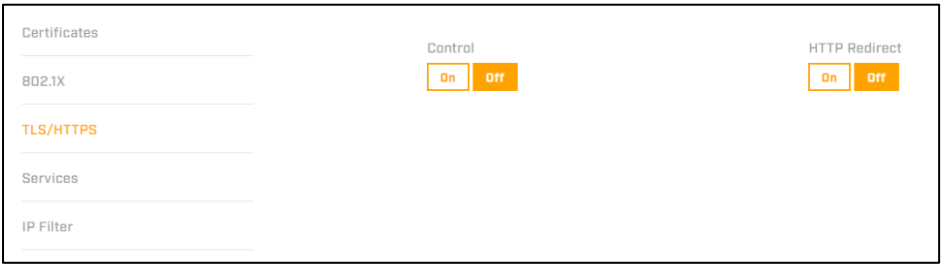

3. **Verify that the camera certificate files are valid** and make sure *"Certificates are OK"* is displayed above the certificate information, under Download certificate.

## 802.1X


Users can enable or disable **IEEE 802.1X-compliant TLS communication**. To configure it, provide the **Identity** and the **Private Key Password**. The default value is disabled.

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

## TLS/HTTPS



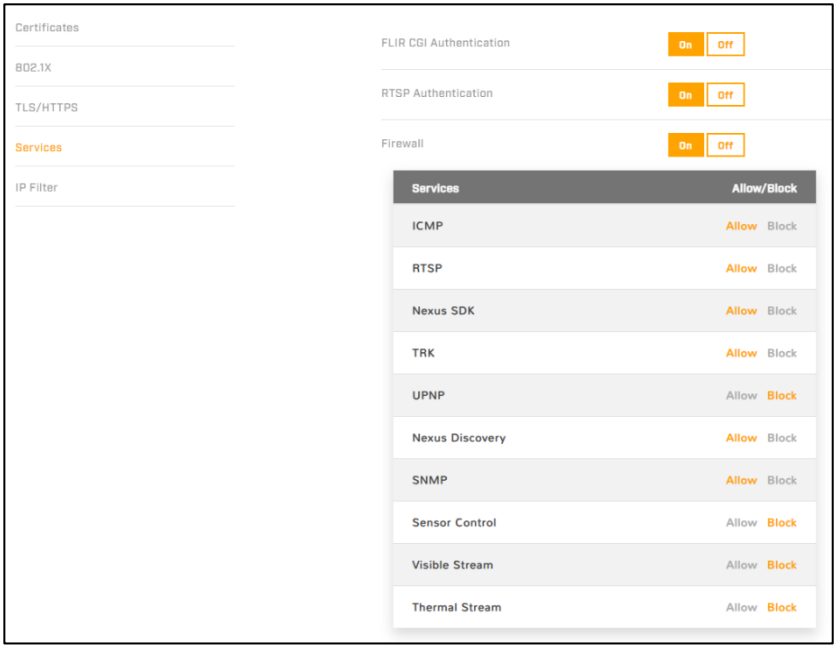

Users can enable or disable the following security options for camera communication:

- **Control:** Enabling **Transport Layer Security (TLS)** and **Secure HTTP (HTTPS)** ensures that all communication between the client and the camera is encrypted. This prevents sensitive data, such as login credentials or control commands, from being intercepted by unauthorized parties. TLS provides encryption and integrity checks, while HTTPS uses TLS to secure HTTP traffic.

- **HTTPS redirect:** When this option is enabled, any attempt to access the camera using an unsecured HTTP connection will automatically be redirected to HTTPS. This guarantees that all sessions use a secure channel, reducing the risk of man-in-the-middle attacks or data exposure.

Both options are disabled by default. This means that, unless configured, the camera will accept unencrypted HTTP connections, which **could expose sensitive information on unsecured networks**.

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




## Services

Users can enable or disable the following security and access control options for the camera:

- **FLIR CGI authentication:** Enables Digest authentication, which adds a layer of security when accessing the camera's CGI (Common Gateway Interface) control interface. Instead of sending credentials in plain text, it uses a challenge-response mechanism with hashing, which helps protect against credential theft during transmission. This is **especially important when managing cameras over unsecured networks**.
- **RTSP authentication**: The Real-Time Streaming Protocol (RTSP) is used to deliver live video streams from the camera. When RTSP authentication is enabled, users must provide valid credentials before accessing the video stream. Disabling this option removes the authentication requirement, which can make the stream vulnerable to

unauthorized access. For security reasons, it is **strongly recommended to keep RTSP authentication enabled**, particularly in production or public-facing environments.

The default setting for both settings is **On** (enabled).

- **Firewall**: The built-in firewall allows users to manage which services can communicate with the camera. Users can **allow** or **block** specific protocols such as:
  - **RTSP**: Controls video streaming access.
  - **UpnP**: Universal Plug and Play for device discovery.
  - **Nexus Discovery / Nexus SDK:** Used for integration with FLIR Nexus services.
  - **TRK:** Tracking-related services.
  - **ICMP:** Internet Control Message Protocol, often used for ping and diagnostics.
  - **SNMP:** Simple Network Management Protocol for monitoring and management.
  - **Sensor control**: Allows or blocks commands that control the camera's sensors.
  - **Visible stream**: Controls access to the visible (optical) video stream
  - **Thermal stream**: Controls access to the thermal video stream.

By selectively allowing or blocking these services, users can reduce the attack surface and prevent unauthorized access to unused or unnecessary protocols.

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

### CAUTION

**Disabling services and ports** can affect product functionality.

## IP Filter

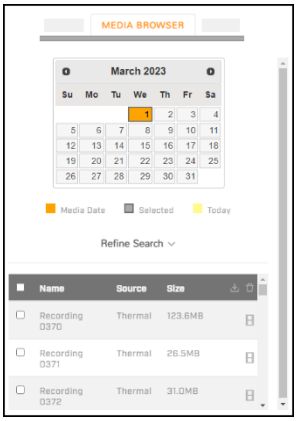

The camera's IP filter can **deny or allow access according to specific IPv4 addresses** that users define. By default, the **IP filter is disabled** (Off).

1. To define specific IP addresses that can access the camera, click **Allow**. The camera will deny access to all other IP addresses.
2. To define specific IP addresses that cannot access the camera, click **Deny**. The camera will allow access to all other IP addresses.

3. To add an IP address to a list, either under Allowed IP Addresses or under Denied IP Addresses, specify an IPv4 address and then click **Add**. Users can specify up to 256 IP addresses.
4. To remove an IP address from a list, click the corresponding **trash icon** .

# 16.9- Media Browser

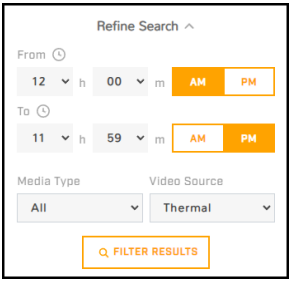

When recorded files exist on a properly installed and formatted microSD card, users can **preview and access** those files on the Media Browser tab.




Users can:

- **View files by clicking on the date**: orange indicates recorded files exist for that date.
- **Refine the search** filtering using:
  - Specific times.
  - Media type (Snapshot, Video, or All).
  - Video source: Visible or Thermal, if available.

When users select a single file, a preview of the file is displayed, except for video files encoded using H.265.




**TIP**

Video file previews do not play back at the full recorded frame rate. To view the video in its original quality and to watch video files encoded with H.265, please download the files and use multimedia playing software, such as VLC.

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

When users download a file, the default file name format is:

SOE1-<source>_VIDEO001_<source>_<start_time>_<end_time>_<x>_<yyyyy>.mp4, where:

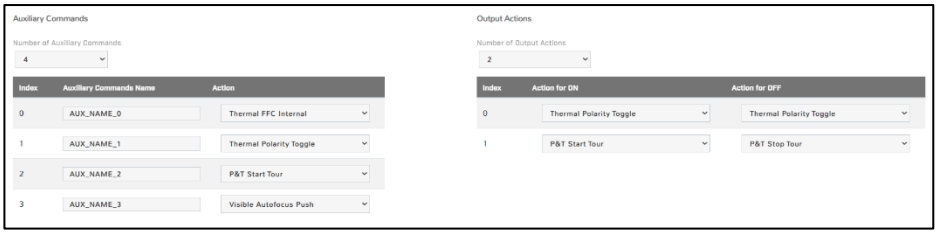
- <source> is the stream recorded: T1 / T2.
- <start_time> and <end_time> are Unix timestamps.

For example, SOE1-V1_VIDEO001_V1_1700982489_1700982789_3_22502.mp4.

**TIP**

Index numbering starts with 0 (zero). In the ONVIF Device Manager, index numbering starts with 1 (one).

# 16.10- ONVIF




ONVIF settings include options for **auxiliary commands** and **output actions**.

## Configuring the ONVIF interface:

1. Select the **number of auxiliary commands** (up to seven) and the **number of output actions** (also up to seven).
2. For each auxiliary command action, **specify the ONVIF command name**.
3. For each auxiliary command action, and separately for each ON and OFF output action, **select one of the following**:
   - **None**.
   - **Thermal Polarity Toggle**: Toggles the thermal video polarity (see Thermal Settings). For example, toggles the colorization from WhiteHot to BlackHot or vice versa; RedHot to RedHotInverse or vice versa; etc.
   - **Thermal FFC**: Initiates flat-field correction on the thermal sensor.
   - **Thermal Palette Toggle**: Toggles through the thermal video colorization options.
   - **P&T Start Tour:** Starts the Pan & Tilt tour.
   - **P&T End Tour:** Ends the Pan & Tilt tour.
   - **Visible Autofocus Push:** Forces a push autofocus on the visible camera.
   -

# 16.11- Map

In order for the Geotracking functionality to work, users need to upload and calibrate a map of the area covered by the camera. This can be done in the Map tab using different methods:

- Users can **upload their own map** or blueprint and calibration coordinates**.**
- Users can **log in to the Flir Raven site planning tool and download the map and calibration info** for each of the installed cameras**.**

## Manually Uploading a Reference Map and Calibrating It

1. **Select the image** that will be used as map. This can be an already existing image, or it can be obtained using an online map or GPS service such as Google Maps.

   For example, users can find the site's location on Google Maps or another online map and take a screenshot of a satellite view of the camera's detection range. In Windows 11, users 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.

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

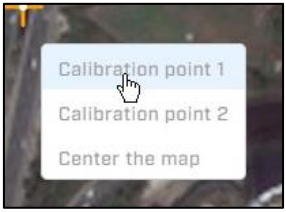
   For optimal calibration, the two calibration points should be as far apart as possible and on opposite sides of the map image. For example, at top-right and at lower-left.

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

   If the map successfully uploads, a confirmation message is displayed.

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.

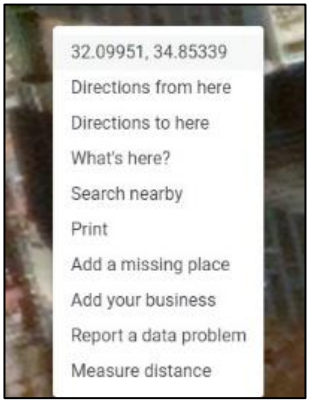



5. **Right-click on the first calibration point**, and then select Calibration point 1.

6. **Enter the latitude (Lat) and longitude (Lon) coordinates** for the first calibration point (P1). It is possible to obtain the coordinates from an 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**.

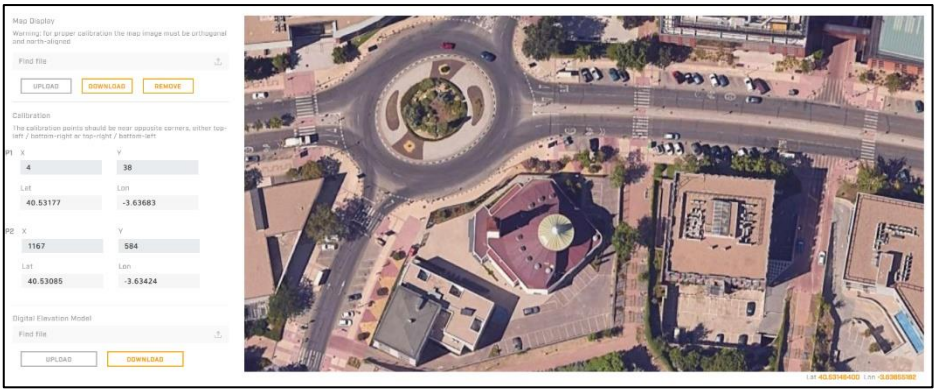
   The calibration point appears on the map as a crosshair icon.




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 on the screen.




*Uploaded and calibrated map.*

If users have not yet set up the camera's georeference calibration, they need to do so on the Georeference settings page. **The web interface will continue to display a black map until the correct latitude and longitude for the camera are entered**, since the default coordinates do not match those of the actual map, resulting in an area without available map data.

### TIPS

- When taking a 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** set to its native resolution without zoom. For best results, take the screenshot in full-screen mode (press F11 in Google Chrome). If you're using Google Maps, consider turning off labels to improve clarity.
- 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 navigate the map, click and drag with your mouse. To zoom in or out, use the scroll wheel.
- It might take a few attempts at different settings to achieve the best result.

## Using Flir Raven Site Planning Tool to Download the Map and Calibration Data

The FLIR Raven site planning tool is designed to assist users in the **layout and optimization of thermal and visible camera deployments** for enhanced security across perimeters and designated areas. Through the use of detailed product information and simulation capabilities, the tool enables users to **visualize coverage and field of view**, ensuring effective placement of cameras and related devices.

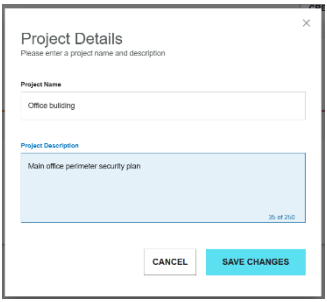
Operators can input a specific address into the FLIR Raven site planning tool, which **automatically generates a map** of the selected area. Within this map interface, users have the option to **add a variety of FLIR Edge devices**, such as cameras and radars, tailoring the deployment to their security requirements.

The tool allows precise **configuration of each device's position, height, and rotation**, supporting the design of a security system that meets all operational needs. This step-by-step simulation helps operators maximize coverage and optimize device placement for effective surveillance. Once a camera has been correctly positioned and configured on the map, **users can export the specific camera map, including calibration data, and the Digital Elevation Model, and import these files into the camera to streamline the set up process**.

Please note that in order to access and utilize the FLIR Raven site planning tool, users must create **a free Teledyne FLIR account**. Registration grants access to the full suite of planning features, enabling comprehensive site design and device management.

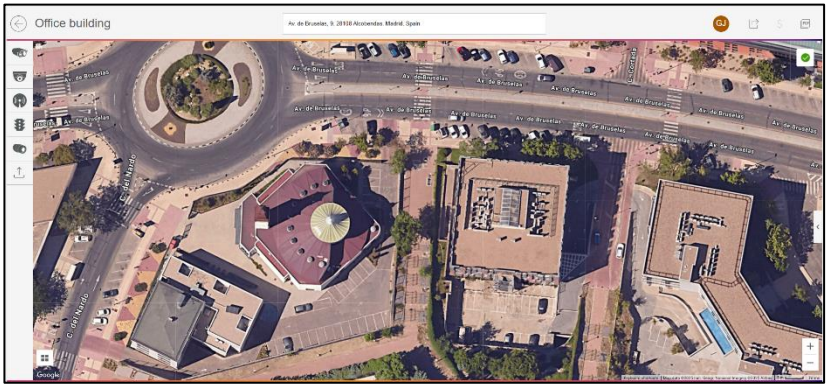
Follow these steps to create the map and calibration data for a camera using Raven:

1. **Visit** https://flirraven.com/.
2. **Log in** or **create a new account**.
3. **Create a new project.**
4. Enter a **project name** (required) and a **project description** (optional) and **save changes**.



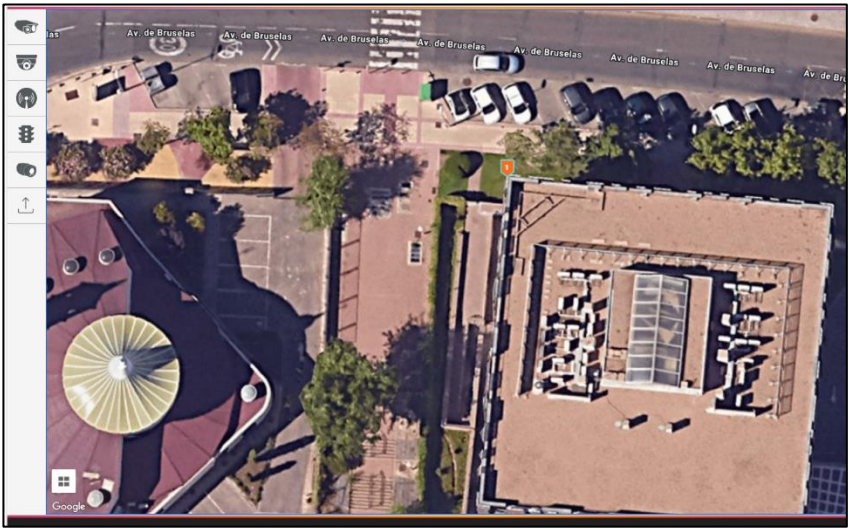

5. A new project is created, and the world map is displayed.
6. **Enter the site's address** in the address box at the top-center of the screen.


7. The map is updated to display the selected address.
8. Using the mouse, **pan and zoom the map** to maximize the area the cameras and devices are meant to cover.

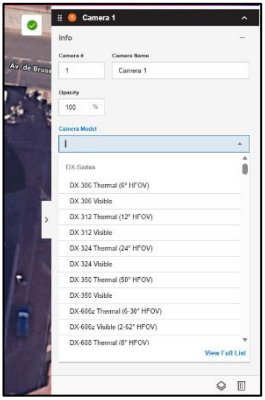


9. Using the toolbar on the left, **select the type of camera** to be added to the map.

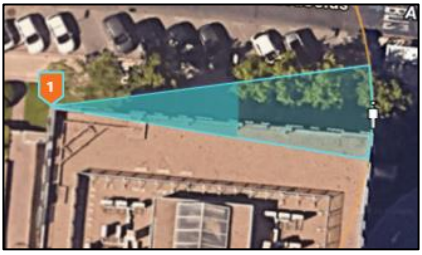

10. **Click on the map** to place the camera. Remember that you can use the mouse to pan and zoom the map as needed in order to place the camera with maximum precision.

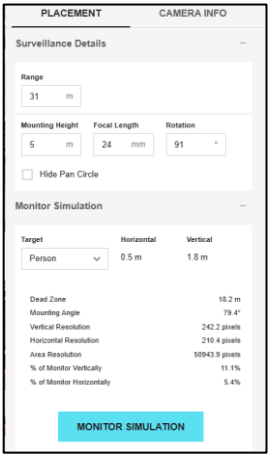



11. A device panel is displayed on the right side of the screen where users need to **enter the camera's name** and **select the camera model**.

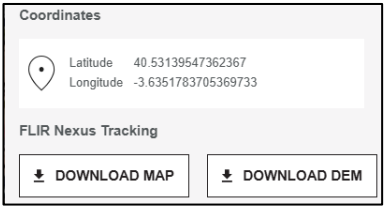


12. Using the **Placement tab** details and dragging the **person icon of the Field of View preview** on the map, configure the camera to cover the desired area.

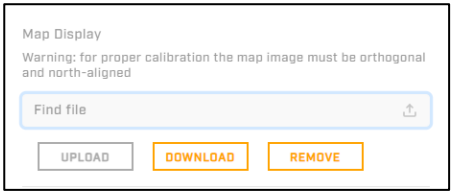



13. Once the camera set up is complete, scroll down the device panel. Select **Download map** and choose the destination folder. If the camera supports Digital Elevation Maps, select **Download DEM** file and the destination folder. Leave this panel open to later copy the latitude and longitude of the camera.



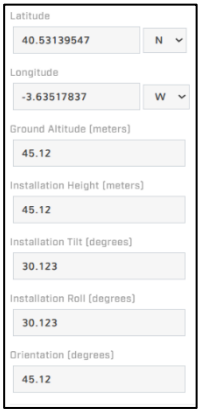

14. Access the camera's web interface and **navigate to the Map tab in the System settings**.




15. On the **Map Display** pane, click on the **Find File box** and select the downloaded map file, then click **Upload**.
16. The map will be displayed on the main window, and the calibration data will be populated automatically.

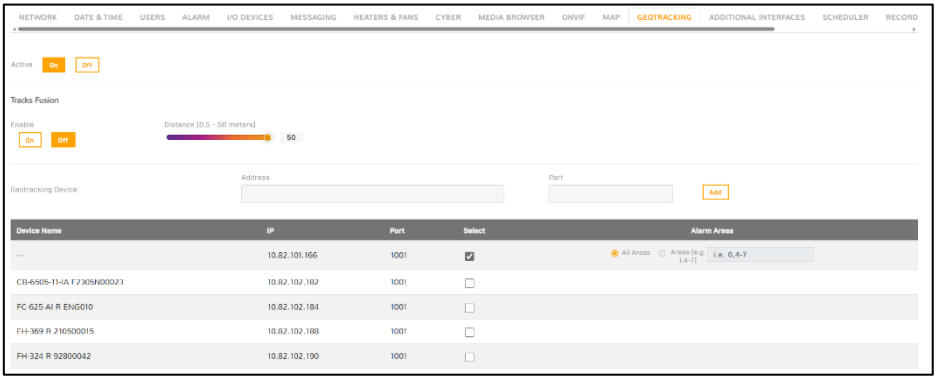
17. To upload the Digital Elevation Model, if supported, click on the **Find File box** on the Digital Elevation Model pane, select the downloaded DEM file, and click **Upload.**


18. **Save the changes** and **exit the System Settings** and **open the Georeference panel**.
19. **Copy the latitude in Raven and paste it into the corresponding field. Do the same for Longitude**. You can fill out the rest of the fields and **save the changes.**




19. If you added several devices to the Raven project, once all the devices have been calibrated, **close the Raven project** by clicking on the arrow icon on the top-left corner of the screen. Changes are automatically saved.

# 16.12- Geotracking




The Geotracking System Settings page allows users to configure how the PT-Series AI SR camera interacts with paired devices for georeferenced tracking.

## Activate Geotracking

Use the **Active** toggle (**On/Off**) to enable or disable the geotracking system.

## Tracks Fusion

Tracks Fusion combines object tracks from multiple sources for improved accuracy.

**Enable:** Switch **On** or **Off**.

**Distance:** Adjust the fusion threshold between **0.5 m and 50 m** using the slider. This defines the maximum distance between tracks to consider them the same object.

## Manually Add Geotracking Devices

To pair additional devices, i.e., devices in a different subnet:

1. Enter the device **Address** (IP) and **Port**.
2. Click **Add** to include the device in the list.

## Device List

The table displays all paired devices. This list is automatically populated with all compatible devices available in the network, and also the devices that were manually paired. The list includes the following columns:

- **Device Name:** Identifier of the paired camera or sensor.
- **IP:** Device IP address.

- **Port:** Communication port (default: 1001).
- **Select:** Check to enable geotracking for this device.
- **Alarm Areas:** Choose the areas that will interact with this camera:
  - **All Areas:** is the default value.
  - **Specific Areas:** by entering area tags (e.g., 0,4-7).

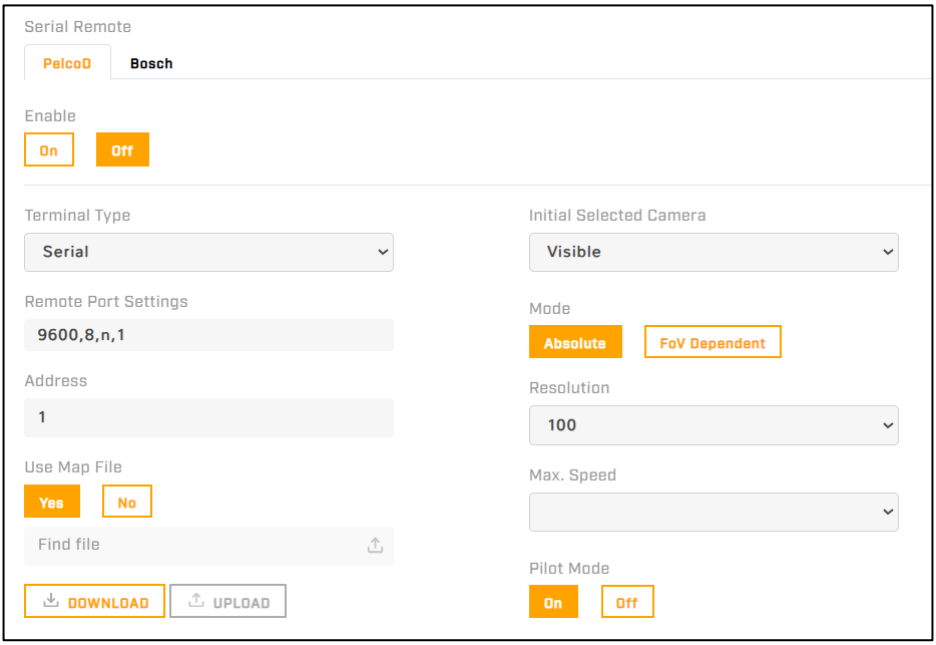

## TIPS

- Ensure all paired devices have **correct IP and port settings**.
- Use **specific area tags** to limit geotracking to critical zones.
- **Multiple devices can be selected simultaneously** for broader coverage.

Please note that **the last element on the device list is the camera itself** (with IP address 127.0.0.1), please make sure that the **Select box is checked for this element** in order for the camera to listen to its own geotracking events.

# 16.13- Additional Interfaces

In this tab, operators can configure different PTZ control devices, using Pelco-D or Bosch protocols.



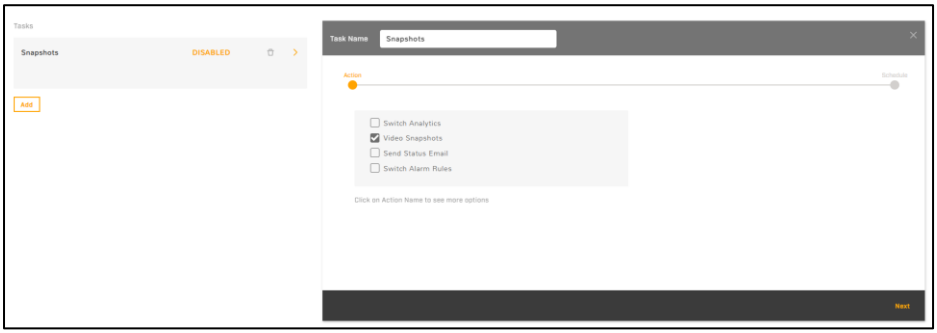

In order to set up the controller, consult the product manual and fill out the following fields:

- **Enable:** Set to **On** to allow remote Pelco-D control.
- **Terminal Type:** Choose **Serial**, **UDP or TCP Server**, and fill out the specific information fields that will be displayed for each type.
- **Remote Port Settings**: Enter **9600,8,n,1.** This is the standard Pelco-D framing (9600 baud, 8 data bits, no parity, 1 stop bit).
- **Address**: Set **1** (camera ID). The camera address must match the controller's target ID; addresses typically range **1–255**. If your installation uses multiple PTZs on a shared bus, assign each a unique address.
- **Use Map File**: Select **Yes** only if you have a **Pelco map file** that remaps commands or presets for a specific controller workflow.
  To upload the map, click on **Find file**, then select the mapping file and **Upload**. Use **Download** to export the currently loaded map.
- **Initial Selected Camera**: Choose **Visible, Thermal or None.**This determines which video channel (e.g., Visible vs Thermal) the PTZ control binds to on connect.
- **Mode**: Choose **Absolute** or **FoV Dependent**:

- **Absolute**: Pan/Tilt/Zoom commands go to exact positions (useful for deterministic presets).
- **FoV Dependent**: Positioning/zoom scales with the current field of view (better for adaptive framing across lenses).
- Pick **Absolute** when you require reproducible presets across sessions; select **FoV Dependent** when the operator prioritizes consistent framing of targets at varying zoom.

- **Resolution**: Select 5, 10, 25, 50 or **100**. This is the **command granularity** for position/zoom steps; higher values generally mean finer PTZ resolution. Keep in mind the controller must support the same step model.
- **Max. Speed**: Select 5, 10, 25, 50 or 100 from the dropdown to cap **pan/tilt/zoom speed** for Pelco-D commands. Set this to match site safety/accuracy requirements (e.g., lower speeds for close-range tracking to reduce overshoot).
- **Pilot Mode**: **On** enables pilot aids (for example, smoothing or guidance behaviors the firmware provides while driving PTZ). **Off** disables such aids for raw, direct Pelco-D response.
- **Save/Discard changes:** Click **Save** to store the configuration. If your unit has hardware DIP-switches and a **Software Override** feature, ensure **software control** is active; otherwise, DIP settings will override your web configuration.

# 16.14- Scheduler




Using the Scheduler tab, operators can define automatically executed **one-time or recurring tasks**, including their start and stop times. For example, users can:

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

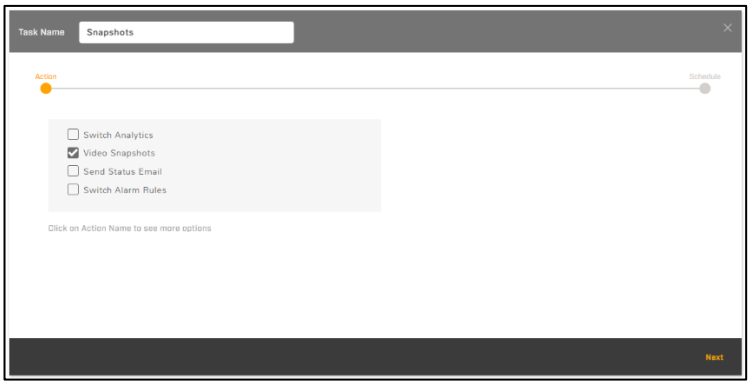
**NOTE**

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

To avoid unnecessary or unwanted data, no tasks are defined by default.

## To Define a Task:

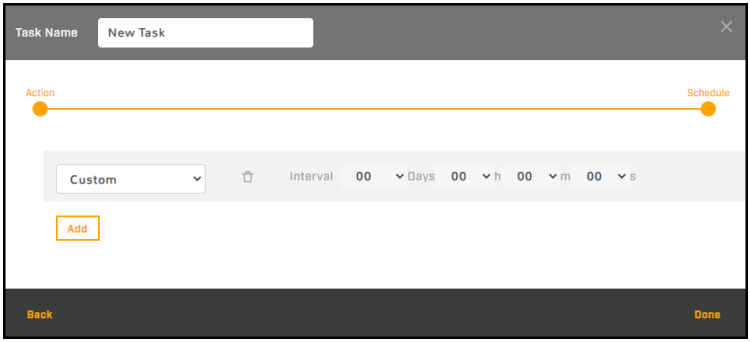
1. Select **Add**. A new task is added. By default, it is enabled.
2. Click on **New Task** to edit the task. The task's name and action settings are displayed.



3. **Define the task name** by overwriting the task's name.
4. **Select the checkbox** for one or more predefined actions.
5. To configure a predefined action, **click the selected action**. The selected action is shown in **bold**, and the relevant settings are displayed.

| **Predefined Actions** | |
|---|---|
| **Switch Analytics** | Select whether the task disables the camera's onboard VA (off) or enables it (on). |
| **Video Snapshots** | Records live video snapshots according to settings configured in the Recording settings, 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 settings. |
| **Switch Alarm Rules** | Select whether the task disables (off) or enables (on) alarm rules.<br>Select the rules affected by the task, according to rule ID number. To determine the rule ID, check the Alarm settings. |

6. Click **Next**. The task schedule settings are displayed.




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** | **Define the time of the day** for the task to run.<br>Either **select the day of the week** for the task to run **or select All days**. |
| **Monthly** | **Define the day of the month and the time of day** for the task to run. |
| **Yearly** | **Define the month, day of the month, and time of day** for the task to run. |


## TIPS

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

- **Define** the 08:00 Monday's weekly schedule.
- Click **Add**.
- **Define** the first-of-every-month monthly schedule.

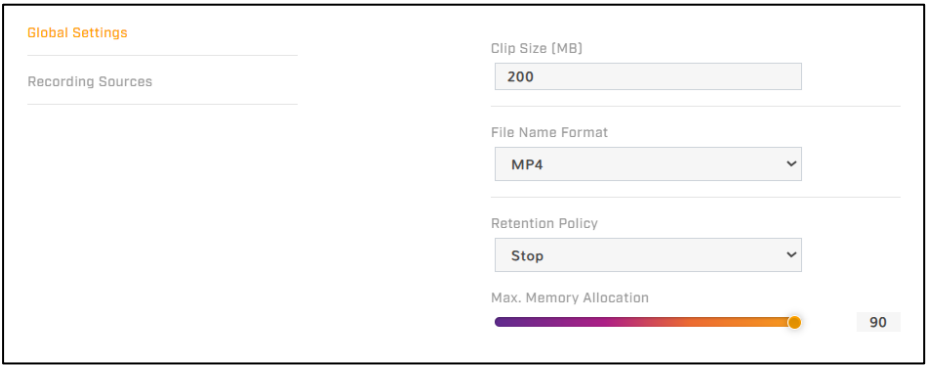
8. Click **Done.**

Users can enable or disable a task by selecting **Enabled** or **Disabled**. To **delete a task**, click on the corresponding trash icon .

# 16.15- Recording

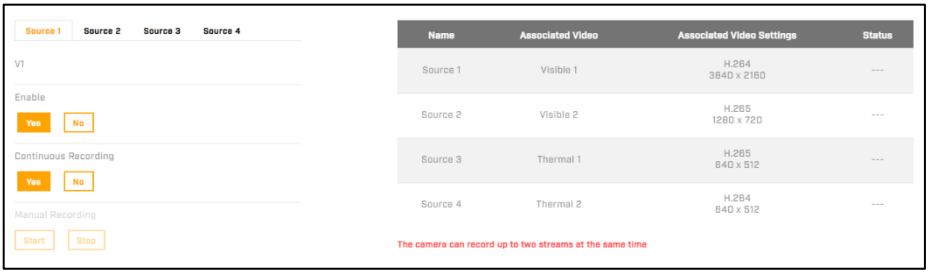
On the Recording tab, users can configure the global video recording settings and manage which video sources are recorded.

## Global Settings




- **Clip Size**: Specify, in MB, the maximum allowed recording file size.
- **File Name Format**: MP4.
- **Retention Policy**: Upon reaching or exceeding the designated Maximum Memory Allocation percentage, designate whether the camera should cease recording (Stop) or overwrite existing files to accommodate new recordings (Overwrite; default).
- **Maximum Memory Allocation**: This is the percentage of microSD card space used that will activate the chosen retention policy. Range: 20-90.

## Recording Sources




The camera **streams two visible and two thermal video streams** (V1, V2, T1 and T2) which can be recorded to the microSD card.

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

- **Recording is enabled** for the stream.
- The camera **continuously records the stream**.

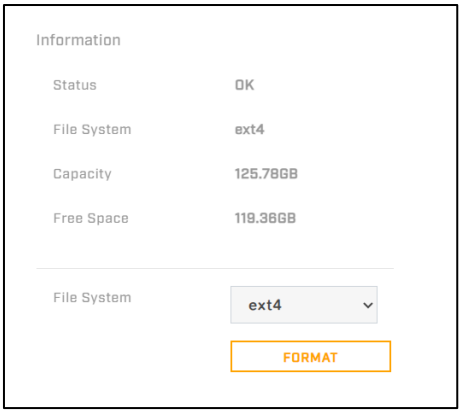
Users can also **manually start and stop recording** a selected stream. However, manual recording of an H.265 source is not supported.

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

| Name | Associated Video | Associated Video Settings | Status |
|---|---|---|---|
| Source 1 | Visible 1 | H.264<br>3840 x 2160 | --- |
| Source 2 | Visible 2 | H.265<br>1280 x 720 | --- |
| Source 3 | Thermal 1 | H.265<br>640 x 512 | --- |
| Source 4 | Thermal 2 | H.264<br>640 x 512 | --- |

# 16.16- SD Card

Users can **locally record up to 512 GB on a microSD card**. For information on accessing the camera's microSD slot and inserting a card, see Installing a microSD card.




The following information is displayed on the SD Card tab:

- **Status**:
  - **OK**: a microSD card has been properly installed and formatted.
  - **Error.**
  - **Formatting.**
  - **Done.**
  - **No SD Card.**
- **File System**: ext4.
- **Capacity**: The card's overall capacity, in GB.
- **Free Space**: How much free space is available, in GB.

To format a microSD card before using it, **insert the microSD card** and then click **Format**.

## NOTES

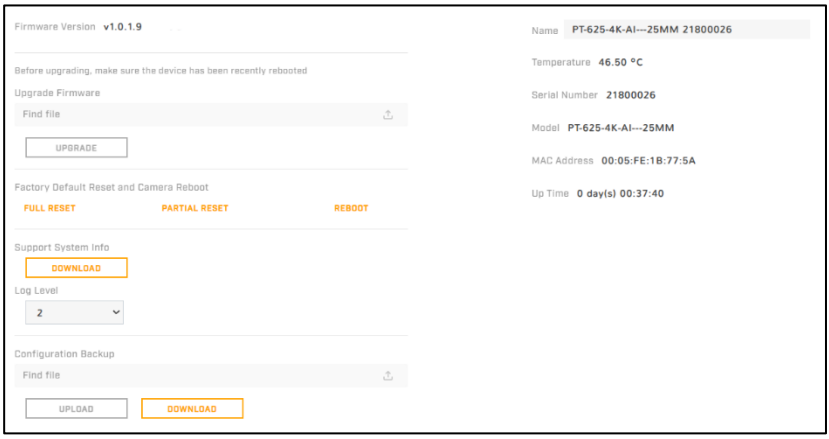
- **Format the microSD card when using it for the first time** or when **the card has been used with another camera** or device and was transferred to this camera.
- The card must be **formatted as a single partition**.
- Please note that the **ext4 format is not natively supported by Windows**, so third-party software (Ext2Fsd, Explore2fs, etc.) is needed to access the files in the card.

## CAUTION

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

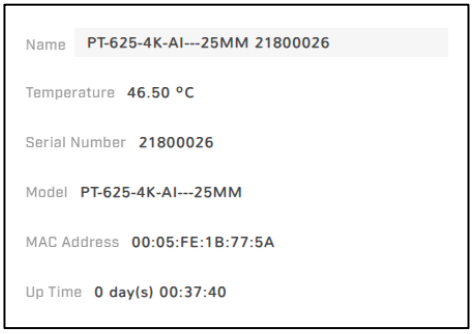
# 16.17- Firmware & Info

On the Firmware & Info tab, users 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.**

## Name




The camera name is displayed on the top-left corner of the System Settings window and is the one that will be visible on the video streams when that OSD option is enabled. Users can

**change the default camera name** by entering a new name in the Name box at the top of the System Information column on the right. It is recommended to 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.

## Upgrading 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**.

### CAUTION

Please ensure that **only firmware specifically developed for the PT-Series AI** cameras is used for upgrades.

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

## Factory Defaults

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

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

### CAUTION

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

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

## Support System Info

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

## Configuration Backup

Users can back up the camera's saved settings or upload a configuration backup file; for example, when a camera needs to be replaced.

### Uploading a Configuration Backup File

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


**CAUTION**

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

3. Click **Upload**.

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

### 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**.

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

# 17- Maintenance & Troubleshooting

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

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

## 17.1- Cleaning

It is essential to **exercise great caution when handling the camera's optical components**. These elements are sensitive and may be compromised by improper cleaning methods. The PT-Series AI SR camera lenses and windows are engineered for challenging outdoor conditions and feature coatings that enhance durability and minimize reflection. Nonetheless, **periodic cleaning may be necessary**. If there is a noticeable decline in image quality or visible accumulation of contaminants on the lens, Teledyne FLIR advises performing a lens cleaning.


**TIP**

While cleaning the camera, **do not disturb or move it**. The PT-Series AI SR cameras are set and calibrated according to the exact position and camera angle. Inadvertent realignment can require relocation and recalibration of detection regions.

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

If further cleaning is needed, please use the following procedure and solvents, as required:

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

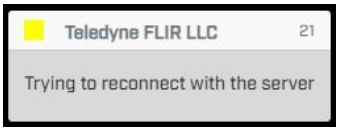
To clean the lens using the aforementioned products:

1. **Immerse lens tissue** (optical grade) in alcohol, acetone, or ethanol (reagent grade).
2. With a new tissue each time, **wipe the lens in an "S" motion** (so that each area of the lens will not be wiped more than once).
3. **Repeat** until the lens is clean. Use a new tissue each time.

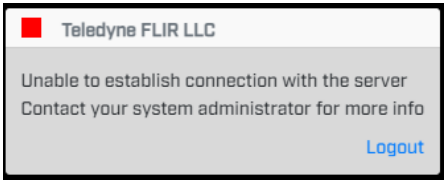
# 17.2- Troubleshooting Tips

## Unable to Access the Camera

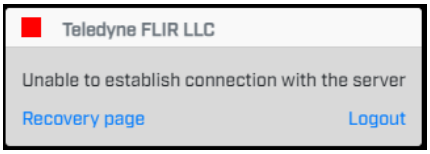
Under certain circumstances, after logging in to the camera's web interface, the following messages might be displayed.




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

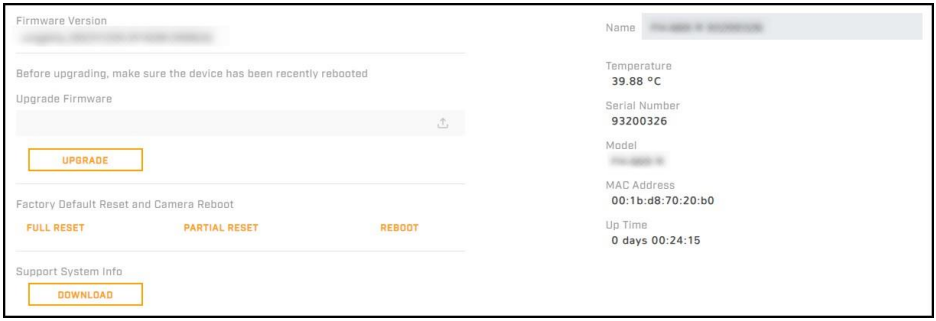



The camera's **Nexus server is not available**, and you logged in as a user assigned the expert or user role. For troubleshooting options, you need to log in as a user assigned the admin role. Click **Logout** and contact your system administrator.




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

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




## Unable to Communicate over Ethernet

First check to ensure the **physical connections are intact** and that the **camera is powered on**.

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

## Unable to View IP Video Stream

If the IP video stream from the camera is not displayed, the firewall might be blocking packets, or there could be a conflict with video codecs installed for other video programs.

When displaying video on a VMS for the first time, the Windows Personal Firewall might ask for permission to allow the video player to communicate on the network. Select the appropriate type of network(s) (domain, private, or public).

If necessary, **make sure the video from the camera can be viewed by a generic video player** such as VLC media player (http://www.videolan.org/vlc/). To view the video stream, specify RTSP port 554 and the appropriate stream name. For example, using the camera's default IP address when there is no DHCP server on the network (192.168.0.250):

- rtsp://192.168.0.250:554/stream1 for T1
- rtsp://192.168.0.250:554/stream2 for T2

By default, RTSP authentication is enabled. To access any of the camera's video streams, users can use the name and password for any of the camera's users. See Users settings. Users assigned the role of admin or expert can disable RTSP authentication in the Services section of the Cyber settings.

For more information on RTSP settings and stream names, see Video settings.

## No IP Video

If the camera is not producing an image, **check the connections at the camera and at the display**. If all connections are confirmed to be correct and the camera continues to fail to

produce an image, verify that **power is correctly supplied** to the camera and that the circuit breaker is appropriately set. If a fuse was used, be sure the fuse is not blown.

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

## Thermal Image Freezes Momentarily

By design, the camera's thermal stream **momentarily freezes during Flat-Field Correction** (FFC and also known as Non-Uniformity Correction or NUC). At regular intervals or when the ambient temperature changes, the camera automatically performs FFC. Users can also manually trigger FFC on the Thermal Page. The shutter for the thermal imager closes and provides a target of uniform temperature, allowing the thermal imager to correct for ambient temperature changes and provide the best possible image.

## Thermal Performance Varies with Time of Day

The diurnal **cycle of the sun can cause difference thermal imager performance** at different times of the day. The thermal imager produces an image based on temperature differences. At certain times of the day, such as just before dawn, all of the objects in the scene could be the same temperature. Compare that type of scene to right after sunset, when objects in the scene might be radiating heat energy absorbed during the day. As temperature differences in the scene increase, the thermal imager can produce higher-contrast images.

When **objects in the scene are wet** rather than dry, performance also can be affected. For example, on a foggy day or early in the morning, when surfaces might be coated with dew. Under such conditions, the thermal imager might not be able to accurately detect the temperature of the object itself; instead, it detects the temperature of the surface water.

See also Thermal Imaging Overview.

## Thermal Image Too Dark or Too Light

By default, the camera's thermal imager uses an Automatic Gain Control (AGC) setting that has proven to be superior for most applications, and the camera automatically responds to varying conditions. Keep in mind that the sky is quite cold and can strongly affect the overall image. To avoid issues, it might be possible to slightly **move the camera up or down to include (or exclude) hot or cold areas** that influence the overall image. For example, a very cold background (such as the sky) can cause the camera to detect and display a wider temperature range than appropriate.

# 17.3- Eastern or Western Exposure

Once installed, the camera might point directly east or west, which can cause the sun to be in the field of view during certain portions of the day. Teledyne FLIR does **not recommend intentionally pointing the camera at the sun**. The sun can introduce image artifacts that the imager eventually corrects. However, recovery can take some time. The amount of time depends on how long the thermal imager was exposed to the sun. The longer the exposure, the longer the recovery time needed. Nonetheless, it does not permanently damage the imager. At the same time, in back-lit scenes, the thermal imager often provides a considerable advantage over a visible imager.

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