Quasar™ Premium PTZ Cameras with FLIR Edge AI Video Analytics

Installation and User Guide

CP-6402-31-RA

CP-6402-31-PA

CP-6408-21-IA
CP-6402-41-IA

CP-6408-31-IA

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	May 2025	Initial Teledyne FLIR release

Product Registration and Warranty Information

Register your Product with Teledyne FLIR at https://customer.flir.com.
For warranty information, see https://www.flir.com/support-center/warranty/security/flir-security-product-warranties/.

Table of Contents

Table of Contents

Table of Contents

1 Document Scope and Purpose

This document provides installation, operation, and configuration instructions for Quasar Premium PTZ with Edge AI Video Analytics Cameras.

Note
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.

Disclaimer

Users of Teledyne FLIR products accept full responsibility for ensuring the suitability and considering the role of the product detection capabilities and their limitation 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.

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

General Cautions and Warnings

This section contains information that indicates a procedure or condition where there are potential hazards.

SAVE ALL SAFETY AND OPERATING INSTRUCTIONS FOR FUTURE USE.

Although the unit is designed and manufactured in compliance with all applicable safety standards, certain hazards are present during the installation of this equipment.

To help ensure safety and to help reduce risk of injury or damage, observe the following:

Caution

- 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 or remove screws. 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.

A **Warning** is a precautionary message that indicates a procedure or condition where there are potential hazards of personal injury or death.

A **Caution** is a precautionary message that indicates a procedure or condition where there are potential hazards of permanent damage to the equipment and or loss of data.

A **Note** is useful information to prevent problems, help with successful installation, or to provide additional understanding of the products and installation.

A **Tip** is information and best practices that are useful or provide some benefit for installation and use of Teledyne FLIR products.

2 Camera Overview

Quasar Premium PTZ with Edge AI Video Analytics Cameras (CP-640x-xx-xA) provide 4K UHD (CP-6408) or 2MP (CP-6402) real-time video, up to 25 / 30 frames per second (fps). They feature Shutter (True) Wide Dynamic Range up to 130db; line-level audio in/out; digital I/O; motion detection; and tampering detection. CP-640x-x1-IA models provide infrared (IR) illumination.

The camera's onboard artificial intelligence (AI)-enhanced video analytics (VA) provide rules for abandoned objects, intrusion detection, camera sabotage, tripwire detection, loitering detection, object counting, object removal, stopped vehicles, and face detection.

The camera supports up to four simultaneous video streams using H.265, H.264, or MJPEG compression, providing an ideal solution when differing levels of image quality are required. The camera can increase frame rate and level of detail when events are triggered. In addition, FLIR's adaptive streaming algorithms provide the highest image quality with the lowest bandwidth and storage requirements.

When the camera is connected to an IP network, it functions as a server, providing services such as camera control, video streaming, and network communications.

If help is needed during the installation process, contact the local Teledyne FLIR service representative or call the Support number that appears on the product's page at https://www.flir.com/support/. All installers and integrators are encouraged to take advantage of the training offered by Teledyne FLIR; visit https://www.flir.com/support-center/training/ for more information.

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.

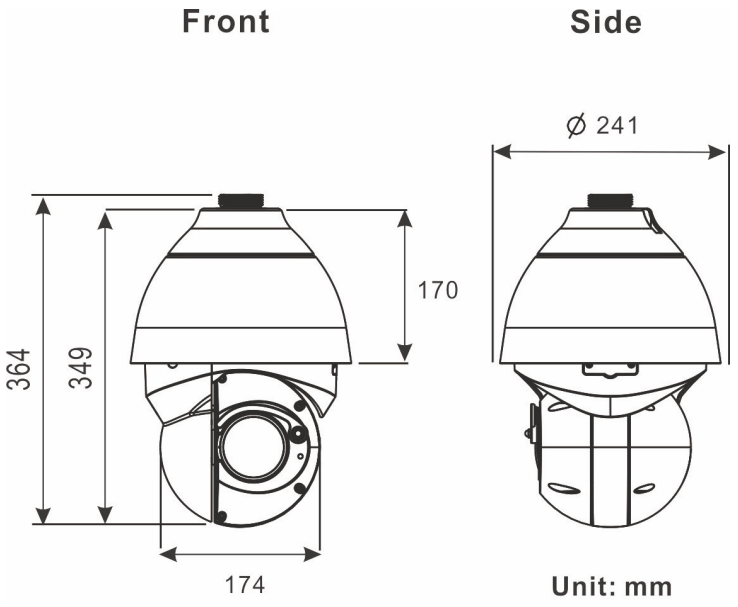
Related Documentation

- *The appropriate Quasar Premium PTZ AI Quick Install Guide:*
  - *CP-6402-30-RA - recessed model*
  - *CP-6402-31-PA - pendant model*
  - *CP-640x-x1-IA - IR PTZ models*
- *FLIR Security Edge Devices Accessory Guid*

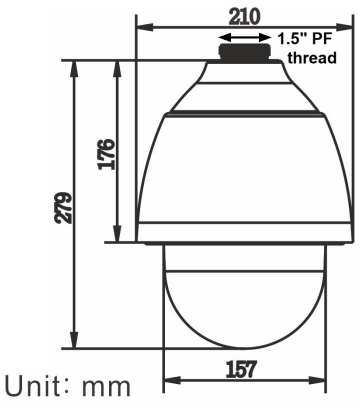
2.1 Features

- CP-6402-30-RA model features a 30x Zoom lens, P-Iris, Auto-Iris, F 1.6, 4.3 - 129 mm (1945 x 1097) resolution
- CP-6402-41-IA model features 40x Zoom lens, P-Iris, Auto-Iris, F 1.6, 4.3–170 mm and adaptive IR illumination light for up-to 200 m (656 ft.)
- CP-6408-31-IA model features advanced ball down PTZ to cover wide areas, 4K (8MP) video with advanced 31x zoom optics, and adaptive IR illumination light for up-to 200 m (656 ft.).
- CP-6402-31-PA model features Advanced ball down Pendent PTZ to cover wide areas, full HD (1080p) video with advanced 30s zoom optics, and (1945 × 1097) (2M) resolution.
- CP-6408-21-IA model features advanced ball down PTZ to cover wide areas, 4K (8MP) video with advanced 22x zoom optics and adaptive IR illumination light for up-to 200 m (656 ft.).
- Onboard AI-enhanced VA alarms for:
  - Motion Detection
  - Tampering Detection
  - Intrusion Detection
  - Loitering Detection
  - Object Counting
  - Stopped Vehicle
  - Face Detection
- Shutter (True) WDR
- IP66 enclosure with IK10 vandal-proof protection
- Powered by PoE+ or by 24V AC
- Built-in web server supports the latest version of Google Chrome® and other popular web browsers
- microSD card slot supports cards up to 1 TB
- up to 20 users
- 802.1X and SSL / TLS security protocols
- ONVIF© Profile S / G / T
- Up to five privacy zones
- Configurable white balance
- 3DNR image noise reduction
- Alarm in / out
- Backlight compensation
- H.265, H.264, and MJPEG compression
- Audio line-in / line-out
- True day / night (ICR)
- HTTP streaming MJPEG
- UPnP support
- SNMP v1 / v2 / v3 and SNMP traps
- Infrared LED illuminator (CP-640x-x1-IA models)

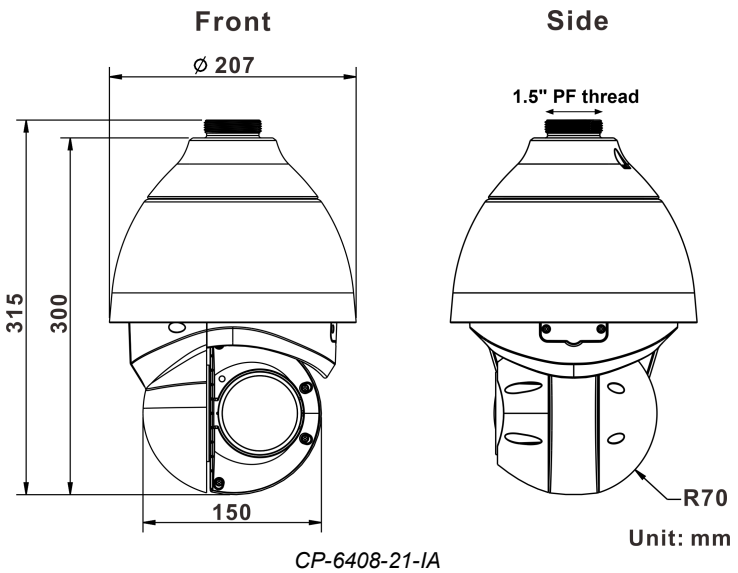
2.2 Camera Dimensions



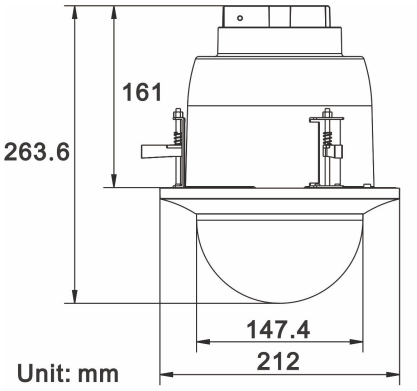
CP-6408-31-IA



CP-6402-31-PA



CP-6408-21-IA
CP-6402-41-IA



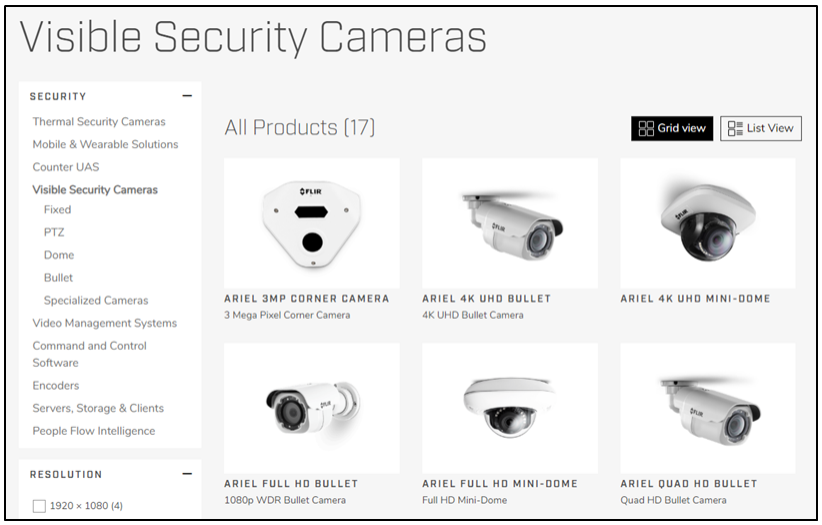
CP-6402-31-RA

3 Accessing Product Information from the Teledyne FLIR Website

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

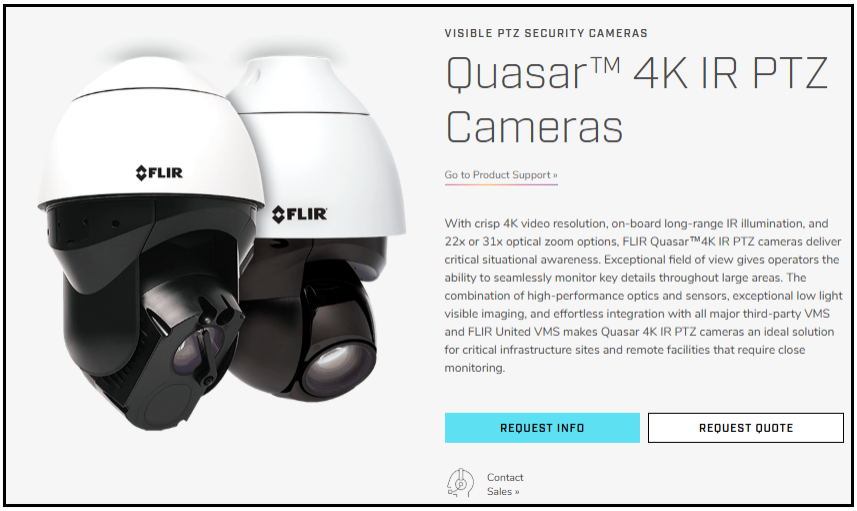
To access product information from the Teledyne FLIR website:

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



Visible Security Cameras Page on the Teledyne FLIR Website

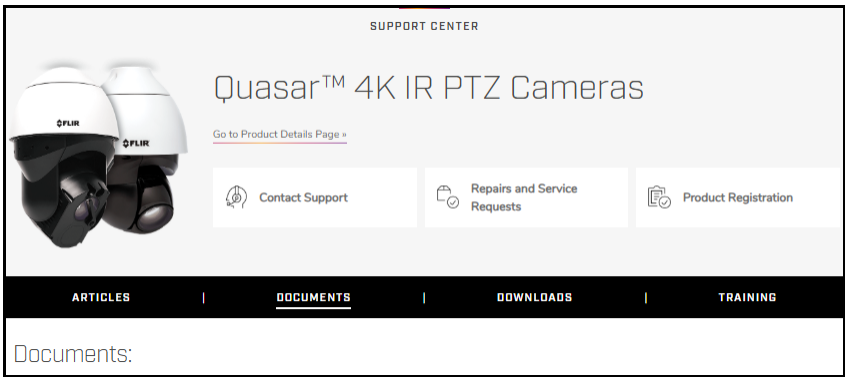
2. Find and click the camera. The camera's product details page appears.



Product Details Page (Example)

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

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



Product Support Page Documents Tab (Example)

5. Download the DNA tool from the Downloads tab.

4 Installation

Caution

- 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.

Before installing the camera, thoroughly read the instructions in this chapter.

This chapter includes information about:

- Supplied Components
- Site Preparation - General
- Indoor Mounting
- Outdoor Mounting
- Pre-Installation Checklist
- Video Analytics Scene Requirements
- Supplying Power to the Camera

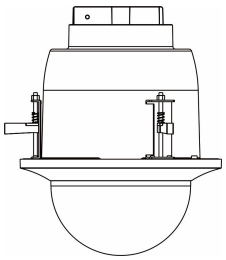
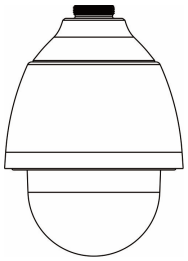
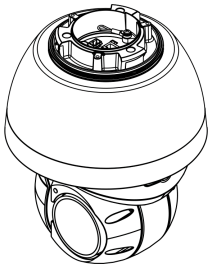
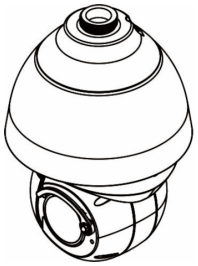
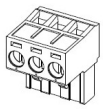
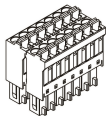
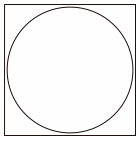
To install the camera, Teledyne FLIR recommends connecting the camera on a bench or in a lab and configuring it for networking before mounting and aiming it:

1. Connect the Camera
2. Configure for Networking
3. Change Video Format (Optional)
4. Install Mounting Hardware - Pendant and IR PTZ Models
5. Waterproof the Camera - Pendant and IR PTZ Models
6. Secure the Camera - Pendant and IR PTZ Models
7. Mount and Connect the Camera - Recessed Model
8. Additional Configuration Steps
9. Attach the Camera to a Supported VMS

However, circumstances can dictate adjusting the sequence of the steps. For example, you can mount the camera before configuring it for networking.

4.1 Supplied Components

Depending on specific model, the Quasar Premium PTZ camera kit includes these items (images not to scale):

<table>
<tr><th>CP-6402-30-RA</th><th>CP-6402-31-PA</th><th>CP-6408-21-IA
CP-6402-41-IA</th><th>CP-6408-31-IA</th></tr>
<tr><td> 
Camera Body</td><td> 
Camera Body &
Pendant Cap</td><td> 
Camera Body
 
Pendant
Cap</td><td> 
Camera Body &
Pendant Cap</td></tr>
<tr><td colspan="2"> 
Three-Pin Connector for 24V AC Terminal Block</td><td colspan="2"> 
14-pin Connector for I/O Terminal Block</td></tr>
<tr><td> 
Ceiling Hole Template</td><td> 
M5x8 Security Screw
with Rubber Gasket
 
Rubber Cable Gland</td><td> 
RJ45 Insertion Tool
 
Cable Gland Bracket
with Screws Attached</td><td> 
Safety Lanyard
(Attached to Pendant Cap)
 
PF-to-NPT Thread Adapter</td></tr>
<tr><td></td><td> 
Security Torx Wrench</td><td colspan="2"></td></tr>
</table>

4.2 Site Preparation - General

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:

- **Ambient 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.
- **Accessibility:** The location used 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 from 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:** Units should be placed in locations that are optimal for the type of video cabling used between the unit and the cameras and external devices. Using a cable longer than the manufacturer's specifications for optimal video signal may result in degradation of color and video parameters.
- **Physical Security:** The unit provides threat detection for physical security systems. In order to ensure that the unit cannot be disabled or tampered with, the system should be installed with security measures regarding physical access by trusted and un-trusted parties.
- **Network Security:** The unit transmits over IP to security personnel for video surveillance. Proper network security measures should be in place to assure networks remain operating and free from malicious interference. Install the unit on the backbone of a trusted network.
- **Electrostatic Safeguards:** The unit and other equipment connected to it (relay outputs, alarm inputs, racks, carpeting, etc.) shall 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.

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.

4.3 Indoor Mounting

When installing the camera indoors:

- There must be a fuse or circuit breaker at the starting point of the electrical wiring infrastructure.
- The camera must be protected from hostile external elements such as: a corrosive environment, metallic dust, extreme temperatures, soot, over spray, and so on.
- Do not place the camera on or near radiators and heat sources.
- All electrical work must be performed in accordance with local regulatory requirements.

4.4 Outdoor Mounting

When installing the camera outdoors, consider the following:

- For outside wiring installation, always use weatherproof equipment, such as boxes, receptacles, connectors, and so on.
- For electrical wiring, use the properly rated sheathed cables for conditions to which the cable will be exposed; for example, moisture, heat, UV, physical requirements, and so on.
- 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, and so on.
- All electrical work must be performed in accordance with local regulatory requirements.

4.5 Pre-Installation Checklist

Before installing the unit, make sure that:

- Instructions in the Document Scope and Purpose section are followed.
- All related equipment is powered off during the installation.
- Use best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, and so on.

Caution

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). In 10-90% non-condensing humidity, the camera's operating temperature range is:

	Without heater	With heater
CP-6402-30-RA CP-6402-31-PA	-25ºC~50ºC (-13ºF-122ºF)	-40ºC~50ºC (-40ºF-122ºF)
CP-640x-x1-IA	N/A	-40ºC~60ºC (-40ºF-140ºF) with heater 10% to 90%, no condensation

4.6 Video Analytics Scene Requirements

To ensure the camera's video analytics (VA) perform properly, mount the camera so that it can accurately detect objects.

In addition to rule-specific mounting and scene considerations outlined in the <%TARGETTITLE%> section, consider the following:

- Keep the camera lens clean and free from rain and water drops. Prevent condensation from forming on the camera.
- Position the camera so that the scene is mostly non-reflective.
- To make sure the camera is stable and does not shake or vibrate, mount it in a sturdy and secured location; for example, on a pole. Unstable installation can cause poor VA performance.
- Make sure the camera can clearly distinguish target objects from the scene background; for example, target objects should not camouflage themselves with similar color and texture to the background.
- Proper VA performance requires a steady and sufficient illumination source. For low-light conditions, you can use external illuminators. The camera can detect target objects under both natural and artificial lighting. When planning illumination, keep the effects of shadows in mind. Also, the camera's VA performs better with white light than with IR illumination.
- Avoid back-lit scenes and prevent unexpected light sources from projecting into the detection zone; for example, vehicles and street lights.
- Make sure that the camera has a clear line of sight to the detection zone and that there are no occlusions; for example, trees, pillars, buildings, and furniture.
- Clouds, fog, or other moving objects that appear similar appearance to target objects in the detection zone can cause poor VA performance.

- Certain weather conditions can affect and reduce detection range and accuracy; for example, heavy rain, fog, or snow.
- When the scene consists of high dynamic range, Teledyne FLIR recommends enabling the camera's WDR capabilities to ensure a sufficient amount of image detail.
- To improve VA performance by reducing flickering noise and artifacts, enable noise reduction.

4.7 Supplying Power to the Camera

Warning
All electrical work must be performed by a qualified service person in accordance with local regulatory requirements.

The camera can be powered by:

Source	Maximum Power Consumption			
	CP-6402-30-RA	CP-6402-31-PA	CP-6408-21-IA CP-6402-41-IA	CP-6408-31-IA
24V AC UL-listed L.P.S. (Limited Power Supply) unit, rated up to 60º C	17.10 W	29.04 W	59.05 W	53.10 W
PoE+ 48V DC	IEEE 802.3at 2-Pair 30 W class 4		IEEE 802.3bt 60 W type 3 class 6	
	17.71 W	25.5 W	51 W	51 W

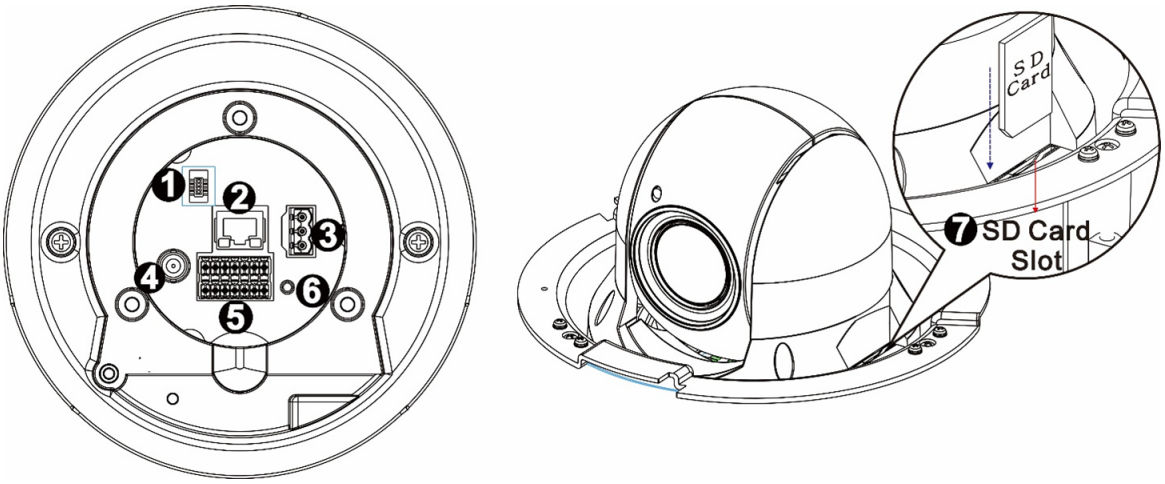
For assistance with purchasing a power supply, contact your Teledyne FLIR representative.

4.8 Connect the Camera

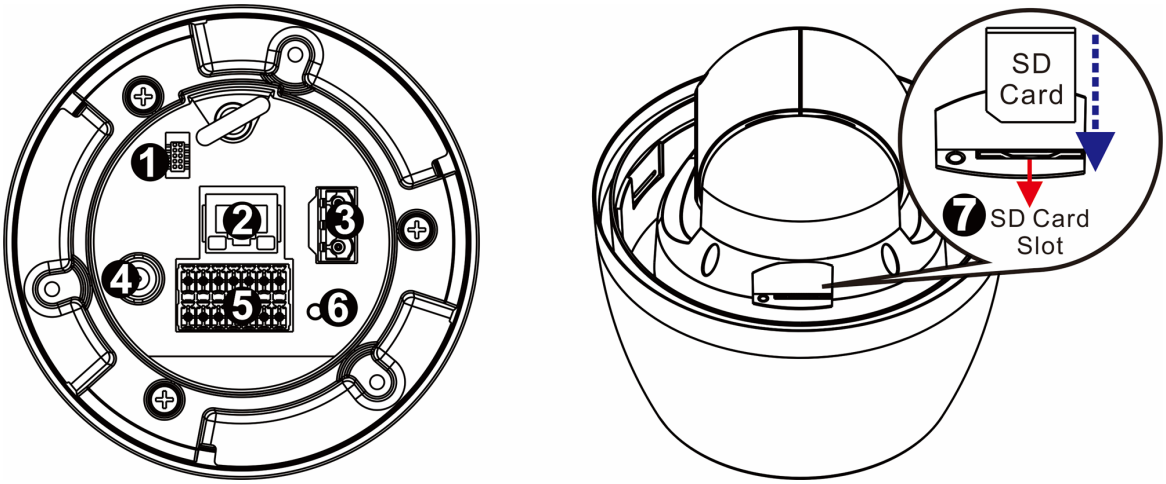
Warnings

- The camera itself does not have a power on/off switch. Do not supply power to the camera until you have completely finished connecting it.
- This product contains a battery that is soldered to the PCB. There is a risk of explosion if the battery is replaced by an incorrect type. **Do not replace the battery.** The battery should be disposed of in accordance with the battery manufacturer's instructions.

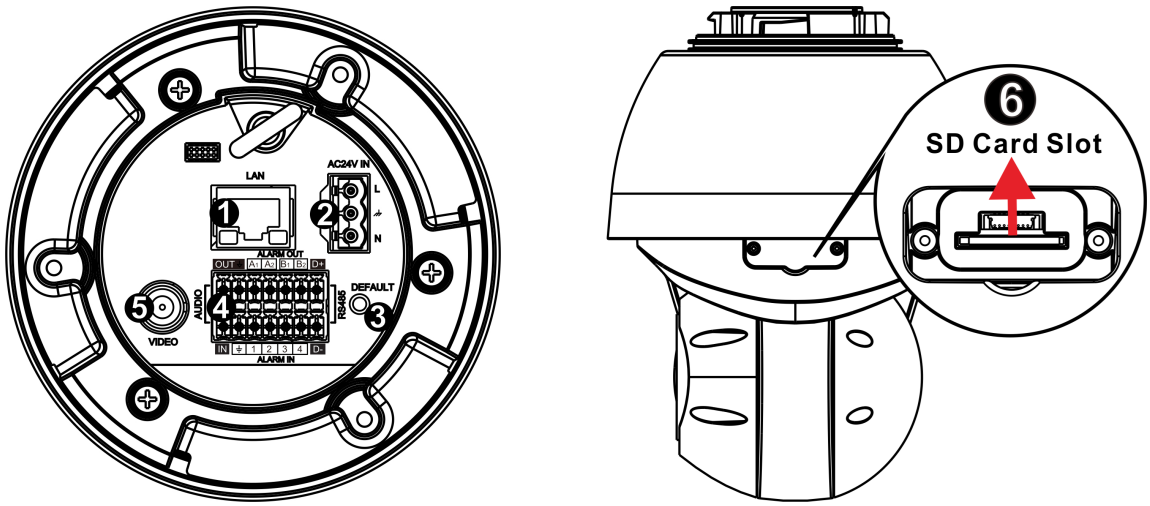
Camera Connections



CP-6402-30-RA

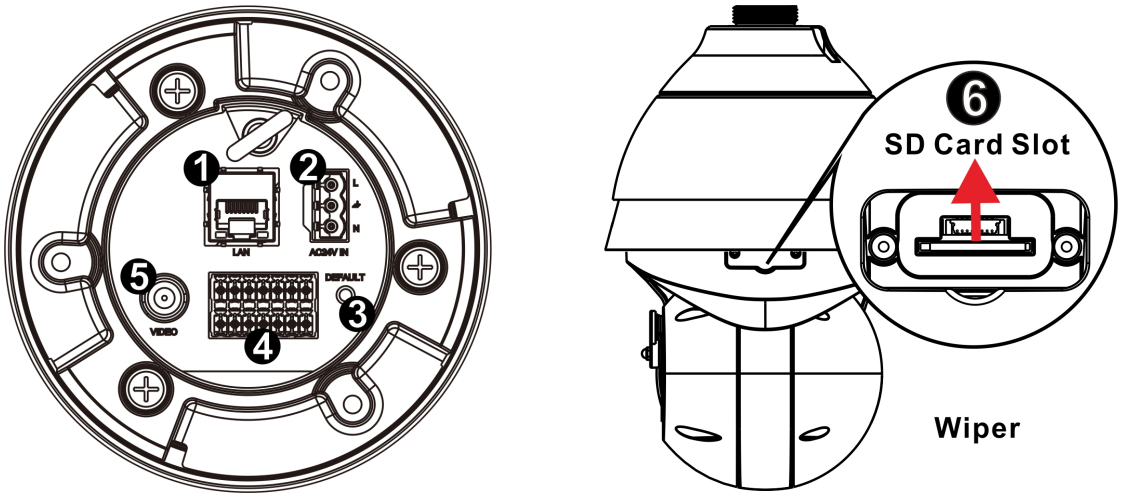


CP-6402-31-PA



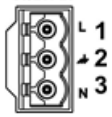
CP-6408-21-IA
CP-6402-41-IA

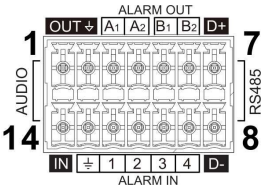
Camera Connections



CP-6408-31-IA

CP-6402-30-RA CP-6402-31-PA	CP-640x-x1-IA	Connector	Connection
2	1	LAN RJ45 w/LEDs	For a 10/100/1000 Mbps Ethernet and PoE connection, attach an Ethernet cable from the network switch to the LAN RJ45 connector. Verify that the LAN connector LEDs are steady green and flashing yellow.
3	2	AC24V IN 3-pin power terminal block	If using an external 24V AC power supply, attach wires from the power supply to the three-pin connector included in the camera kit according to the pin assignment below. Then, attach the connector to the terminal block.
6	3	DEFAULT	To reset the camera's settings to its factory defaults, press the default button for at least 20 seconds.
5	4	14-pin I/O terminal block	Attach wires from external alarm, audio, and other I/O devices to the 14-pin I/O connector included in the camera kit, according to the pin assignment below (see Connecting Leads to a Spring Clamp). Then, attach the connector to the terminal block. **Warning** Do not connect an external power supply to the 14-pin I/O terminal block.
4	5	VIDEO	BNC connector for analog video output.
7	6	microSD card slot	For video clip and snapshot recording and file storage, insert a microSD / SDHC / SDXC card (up to 1 TB) in the card slot. When the camera is powered on, do not remove the microSD card.
1	N/A	Console connector	Connector for camera repair / maintenance. For use only by Teledyne FLIR Support.

3-Pin Power Connector	Pin	24V AC
	1	L (Live; white; positive)
	2	Ground (Earth)
	3	N (Neutral; black; negative)

14-Pin I/O Connector	Pin	Definition	Pin	Definition
	1	Audio-Out	8	RS-485 D-
	2	Ground (Audio I/O)	9	Alarm-In 4
	3	Alarm-Out A1	10	Alarm-In 3
	4	Alarm-Out A2	11	Alarm-In 2
	5	Alarm-Out B1	12	Alarm-In 1
	6	Alarm-Out B2	13	Ground (Alarm I/O)
	7	RS-485 D+	14	Audio-In
On the I/O Page and on the Alarm Page: • Output 1 refers to pins 3 and 4 - Alarm-Out A1 and A2. • Output 2 refers to pins 5 and 6 - Alarm-Out B1 and B2.				

Warning

- The power cord to the 12V DC or 24V AC power supply unit must be connected to a socket outlet with an earthing connector.
- The PoE unit and all interconnected equipment must be installed indoors within the same building, including all PoE-powered network connections, as described by Environment A of the IEEE 802.3af standard.
- All electrical work must be performed by a qualified service person in accordance with local regulatory requirements.

4.9 Configure for Networking

You can configure the camera using the FLIR Discovery Network Assistant (DNA) software tool, the camera's web page, or a supported VMS.

Task	DNA tool	Camera's web page
Discover camera IP address	•	
Configure IP address, mask, and gateway	•	•
Change user credentials	•	•
Configure DNS settings, MTU, and Ethernet speed		•
Change video format	•	•
Configure more than one camera at the same time	•	

Note

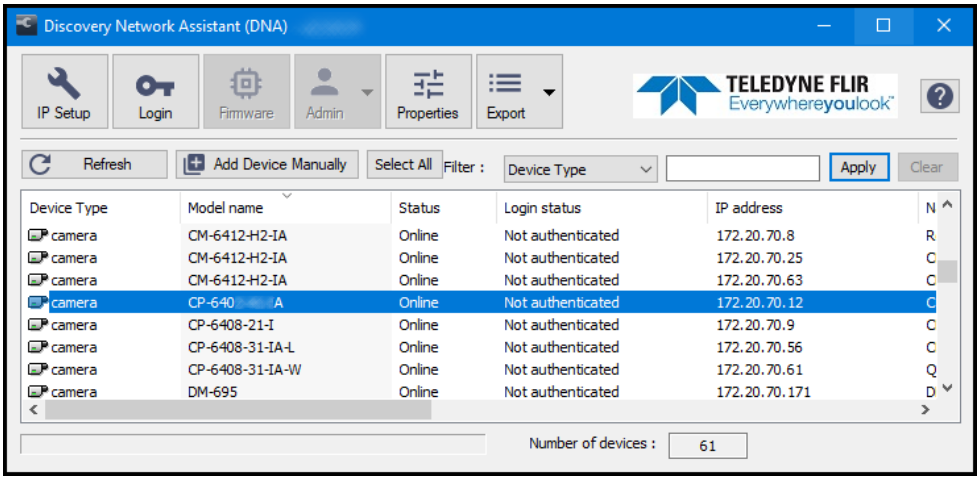
- Teledyne FLIR recommends using the DNA tool to discover the camera on the network. It does not require a license to use and is a free download from Teledyne FLIR. While the software is open, click the Help icon .
- Client side dewarping will not be supported until UVMS version 9.3.1.
- For more information 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. 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 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 is managed by FLIR Latitude VMS or is on a network with static IP addressing, you can manually specify the camera's IP address using the DNA tool or the camera's web page.

To manually specify the camera's IP address using the DNA tool:

1. Make sure the camera and the PC are on the same LAN segment.
2. Run the DNA tool (DNA.exe) by double-clicking . The Discover List appears, showing compatible devices on the VLAN and their current IP addresses.

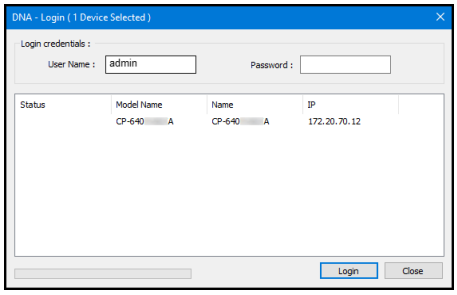


In the DNA Discover List, verify that the camera's status is *Online*.

If this is the first time you are 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 with user name *admin* and its default password (*admin*).

If the *admin* user's password is not the default password, you need to authenticate the camera.

a. In the DNA Discover List, select the camera and then click **Login**.
b. In the **DNA - Login** window, type *admin* or another name for a user assigned the Admin role and the password. If you do not know this information, contact the person who configured the camera's users and passwords.
c. Click **Login**, wait for ✔ Ok status to appear, and then click **Close**.



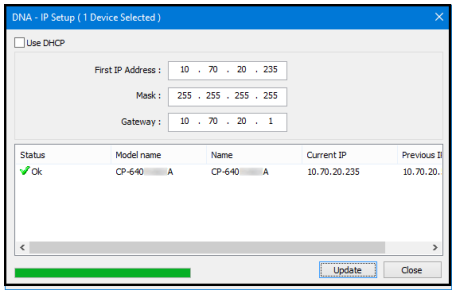
DNA - Login Window

In the DNA Discover List, verify that the camera's status is *Authenticated*.

3. Change the camera's IP address.

   Right-click the camera and select **IP Setup**.

   In the **DNA - IP Setup** window, clear *Use DHCP* and specify the camera's *IP address*. You can also specify the *Mask* (default: 255.255.255.0) and *Gateway*. Then, click **Update**, wait for ✔ Ok status to appear, and then click **Close**.



DNA - IP Setup Window

To manually specify the camera's IP address using the camera's web page:

1. Access the camera's web page with a user assigned the Admin or Expert role; for example, the default *admin* user.
2. On the View Settings Home Page, click **System Setting**, and make sure the Network Page appears.
3. Click **Static** IP addressing and then manually specify the camera's *Hostname*, *IP address*, *Netmask*, and *Gateway*.

   You can also specify the *DNS Mode*, *Name Servers*, *MTU* (maximum transmission unit), and *Ethernet Speed*.
4. Click **Save**. Applying any changes on the Network page requires rebooting the camera.

Using DNA to Configure the Camera

DNA is a user-friendly utility that easily discovers and configures FLIR Security edge devices on a network. It does not require a license to use and is a free download from Teledyne FLIR.

DNA provides a central location for listing all the supported FLIR Security camera models accessible over the network. Once listed, each camera can be right-clicked to access and change the network settings. If the network settings are changed for some reason, a new search will relist the units. The units can then be configured via the camera's web page.

The camera must be made accessible for setting network addresses.

To configure the camera via a LAN, you must attach the camera via the network switch or router to the same network segment or VLAN as the computer that manages the unit. If the PC is on a different subnet than the camera, you will not be able to access the camera via a web browser.

If there is a DHCP server on the network, Teledyne FLIR recommends using the DNA tool to discover the camera and change its IP address.

If FLIR's Latitude VMS is being used, configure the unit with a static IP address rather than with DHCP. This ensures that the IP address will not automatically change in the future and interfere with configurations and communication.

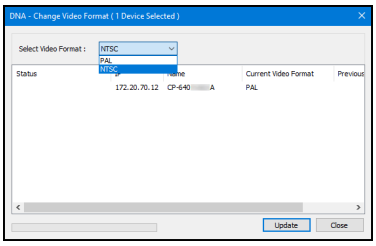
While the software is open, click the Help icon .

4.10 Change Video Format (Optional)

By default, Shutter WDR 30 FPS NTSC is the camera's video format. To change the format, you can use the DNA tool or the camera web page. Note, though, it is not possible to use DNA to change the video format between Shutter and Linear. For example, if Shutter WDR 30 FPS NTSC is the camera's current video format and you use DNA to change the video format from NTSC to PAL, the video format changes to Shutter WDR 25 FPS PAL. To change the video format between Shutter and Linear, use the camera web page.

To change the camera's video format using the DNA tool:

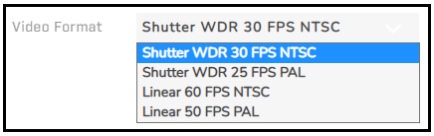
1. In the DNA Discover List, right-click the camera and select **Change Video Format**.
2. In the **Change Video Format** window, select PAL. This changes the camera's video format to Shutter WDR 25 FPS PAL.
3. Click **Update**, wait for ✔ Ok status to appear, and then click **Close**.



DNA - Change Video Format Window

To change the camera's video format using the camera's web page:

On the Firmware & Info Page, for Video Format, select another format.



To apply a video format change, the camera needs to reboot.

4.11 Install Mounting Hardware - Pendant and IR PTZ Models

Install the mounting hardware for the camera according to the instructions for the hardware, and route cables through the hardware. Make sure the cables reach the camera connections.

Important

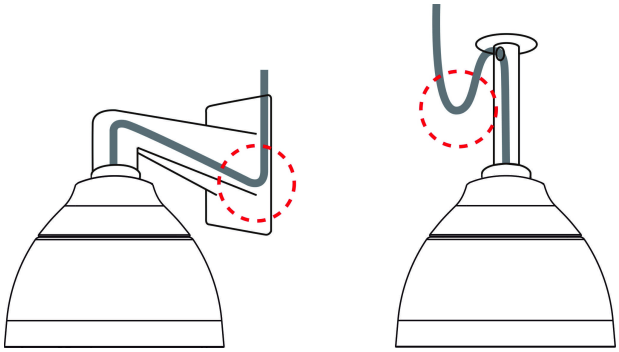
- When routing cables through the mounting hardware, make sure to follow the instructions in Waterproof the Camera - Pendant and IR PTZ Models.
- Regardless of how you mount the camera, the hardware needs to be installed to make sure the camera can be horizontally mounted, ensuring that it pans parallel to the horizon.

For the list of mounting accessories available from Teledyne FLIR for installing your camera, see Mounting Accessories.

4.12 Waterproof the Camera - Pendant and IR PTZ Models

When installed properly, the pendant and IR PTZ models are IP66-rated waterproof. However, if the camera is not installed properly, water can enter and damage it. To waterproof the camera, strictly follow these instructions:

1. Route cables in dry and waterproofed environments; for example, use waterproof cable boxes. This prevents moisture from accumulating inside the camera and from penetrating into cables.
2. When routing cables from the mounting surface to the camera, slightly bend the cables in a U-shaped curve to create a low point.
3. Wrap PTFE thread seal tape (not included in the camera kit) around the pendant cap thread about five times.



U-Shaped Cable Installation

Pendant Cap Thread

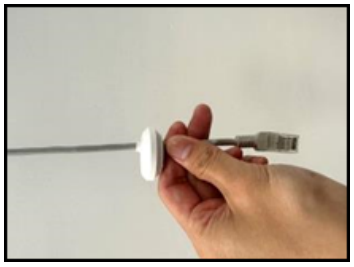
If you are using mounting hardware with an NPT thread, wrap PTFE thread seal tape around the PF-to-NPT thread adapter included in the camera kit about five times.

4. Route the cables from the mounting hardware through the pendant cap and attach the pendant cap to the mounting hardware.

   If you are using mounting hardware with an NPT thread, route the cables from the mounting hardware through the thread adapter and attach the thread adapter to the mounting hardware. Then, route the cables from the adapter through the pendant cap and attach the pendant cap to the thread adapter.

5. Route cables through the rubber cable glands.

   To route an Ethernet cable with an RJ45 plug attached, attach the supplied RJ45 insertion tool to the RJ45 plug. Then, route the tool, plug, and cable straight through one of the holes in the gland. Do not bend the cable, which can damage the gland. Remove the tool.

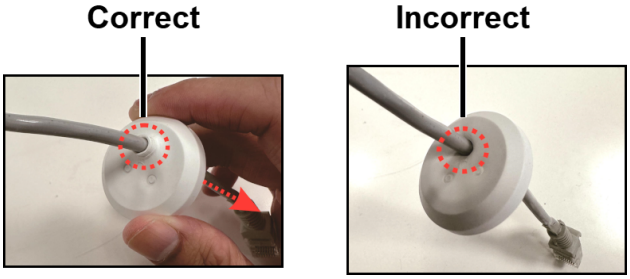


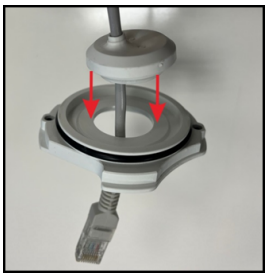
   For all other camera connections, route unterminated cables into the camera through holes in the gland.

Important	Except when using the RJ45 insertion tool, routing a terminated cable through a gland compromises the camera's waterproof integrity.

6. Pull the rubber gland toward the end of the cables so that the gland seal extends toward the mounting hardware and away from the camera, tightly wrapped around the cables, and providing an effective waterproofing seal.

7. Route the cables through the cable gland bracket and then attach the rubber gland to the bracket.

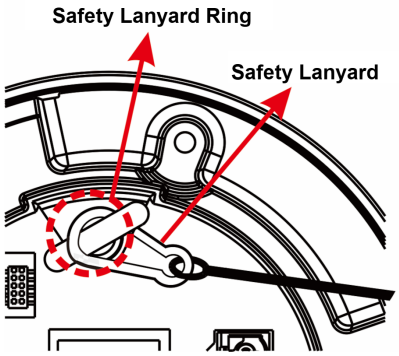




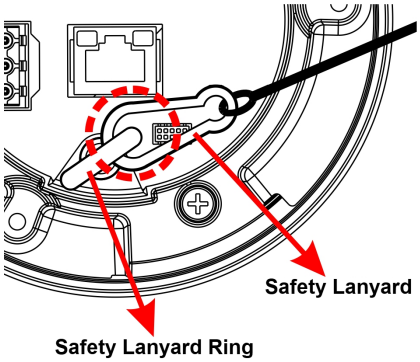
8. Using a screwdriver and the screws attached to the cable gland bracket, attach the bracket to the pendant cap.

4.13 Secure and Connect the Camera - Pendant and IR PTZ Models

To prevent a CP-6402-31-PA camera or a CP-640x-x1-IA camera from falling, you need to secure it using the safety lanyard attached to the pendant cap. Attach the lanyard to the ring on the camera.



Pendant Models



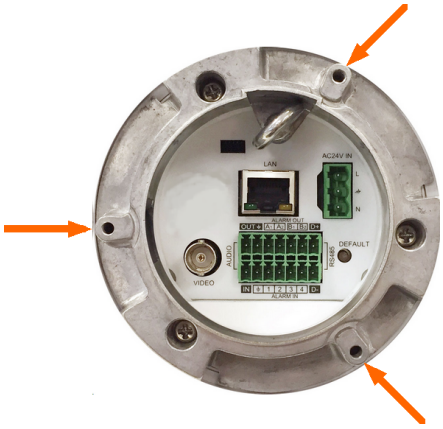
IR PTZ Models

1. According to the information in Connect the Camera, connect the cables to the camera.
2. Carefully insert the camera into the pendant cap and rotate the camera until it locks into place (1/3 turn).

> **Warning**
>
> The metal locking mechanism carries the weight of the camera. If the camera is not locked into place, it could become loose and fall.

The screw that attaches the pendant cap to the camera needs to line up with one of the corresponding screw holes on the camera.

Pendant Cap Screw



Pendant Cap Screw Holes on Camera (IR PTZ Models)

3. Securely tighten the pendant cap screw into the camera. The screw prevents the camera from rotating.
4. Try to rotate the camera and make sure it is not possible to rotate the camera.

Warning

If the camera can be rotated, it could become loose and fall.

4.14 Mount and Connect the Camera - Recessed Model

Recessed models

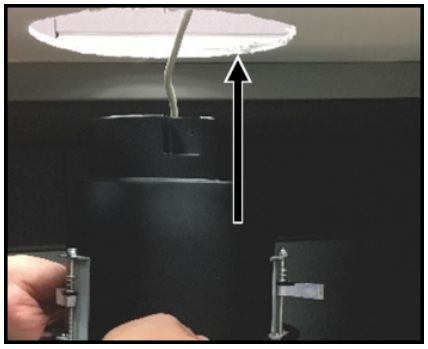
Using the hardware included in the camera kit and the following tools, you can mount recessed models in a ceiling:

- Tool for cutting or drilling a hole in the ceiling
- Philips head screwdriver for M4 thread

To mount a recessed model in a ceiling:

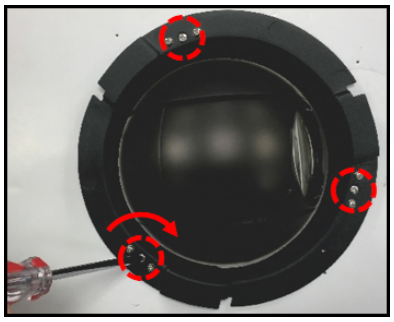
1. Determine an appropriate location in the ceiling to mount the camera. Make sure to observe all of the relevant cautions and warnings in this guide. For example, before drilling, verify that electrical or other utility service lines are not present.
2. At the determined mounting location, attach the ceiling hole template included in the camera kit to the ceiling.
3. Using the appropriate tool for cutting or drilling a hole in the ceiling, make a ⌀ 192mm hole in the ceiling.
4. Remove the camera dome cover by turning it counterclockwise.
5. Route Ethernet and other cables through the ceiling opening. Then, according to the information in Connect the Camera, connect the cables to the camera.

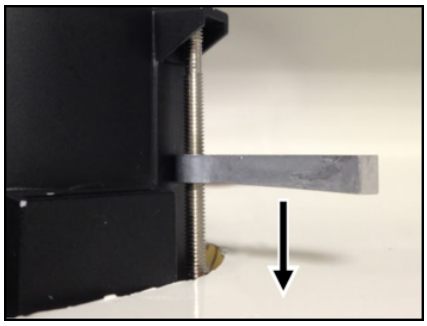
6. Align and position the camera in the ceiling opening.



7. Attach the camera to the ceiling. Use a Philips head screwdriver to turn the three ceiling clamp screws clockwise.

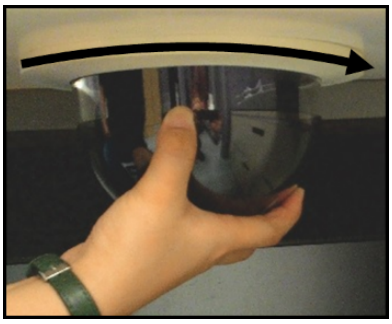
   As you tighten the screws, the clamps move toward the ceiling and then they clamp onto the ceiling.





   Make sure the clamps are tightly clamped onto the ceiling and that the camera's outer ring is flush with the ceiling.

8. Re-attach the camera dome cover.



4.15 Install and Test the Optional Wash Kit - CP-6408-31-IA model

As an optional accessory for the CP-6408-31-IA model, Teledyne FLIR recommends the Videotec line of wash kits for PTZ cameras, including the WASPT0V5L5M00 washer pump, five-liter tank, five-meter delivery kit. For general information about installing a Videotec wash kit, see the kit's instructions manual.

This section and this guide contain important information about installing the washer and using it specifically with the CP-6408-31-IA model.

Connection of the board

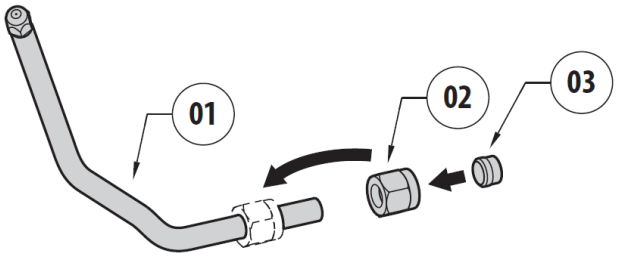
Connect the following:

J9 terminal on the washer pump control board		Camera's 14-pin terminal connector
CP pump activation (dry contact)	→	Alarm-Out A1 pin (3)
GCP GND pump activation (dry contact)	→	Alarm-Out A2 pin (4)

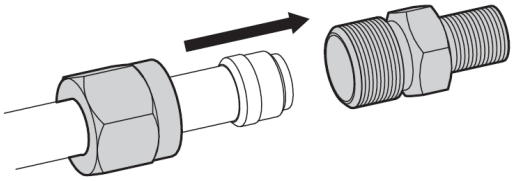
Washer installation

1. Cut the cables to size and either restore or make the connections to the positioning unit.

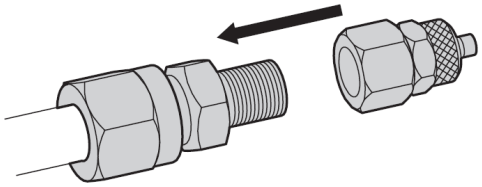
2. Shorten the semi-rigid washer pipe (01) as needed. Unscrew the nut (02) from the joint and slide it along the pipe. Insert the end of the pipe into the ogive (03).



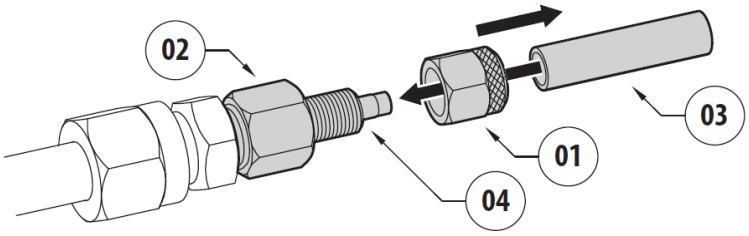
3. Lock the nut to the coupling.



4. Tighten the delivery joint.



5. Unscrew the knurled nut (01) from the delivery joint (02). Insert the knurled nut on the delivery pipe (03). Insert the end of the delivery pipe into the spinner (04). Lock the nut to the coupling.



6. Fasten the semi-rigid pipe and aim the nozzle towards the camera lens window. Depending on how and where you are installing the camera and the wash kit, you can use one of the nozzle support brackets supplied with the wash kit to secure and aim the nozzle.

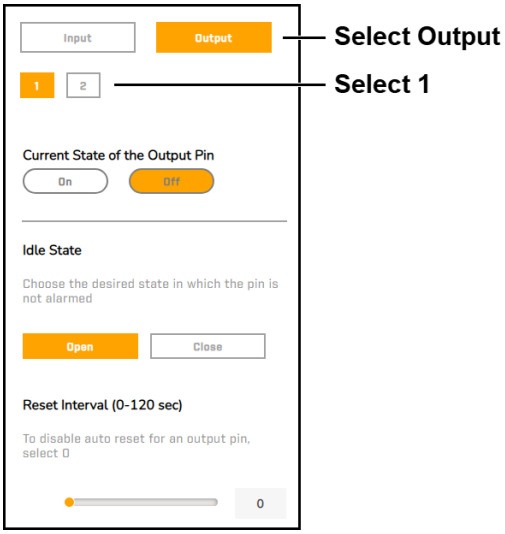
Important

When you test the wash kit, you will specify a preset for the camera's washer position using the camera's web page. Aim the washer nozzle so that it sprays liquid over the camera lens window when the camera is in what will be its washer position. Activating the camera's wiper when the lens window is dry causes irreparable damage to the window coatings and voids the camera's warranty.

Configuring the camera's local output pin 1 to control the washer pump

1. With a user assigned the Admin or Expert role, log in the camera's web page. For information about how to log in to the camera's web page, see Accessing the Camera's Web Page.
2. Open the I/O Page.
3. Select local output 1.
4. Make sure the following settings are specified:

Setting	Value
Idle State	Open
Reset Interval	0 seconds (automatic output pin reset is disabled)



Testing the washer and wiper

Before testing the washer and wiper, make sure:

- You install the wash kit according to the kit's instructions manual and according to the instructions above.
- You fill the washer liquid tank.
- The camera is not moving, and that it is not running a cruise, an auto pan, or a tour.

1. Create a preset for the washer position.

   On the PTZ Page, use the PTZ controls to move the camera into a position so that the washer sprays liquid over the camera lens window. Under Preset Position, click **Set Preset**. Specify Washer Position as the Preset Name and then click **Save**.

2. Create a manual alarm that activates the washer pump.

   On the Alarm Page, create an alarm whose trigger is Manual and whose action changes the state of output 1. Make sure Idle State is Open.

3. Trigger the manual alarm to activate the washer pump.

   On the View Settings home page, to the right of the live video, click the manual trigger button . Make sure the washer activates.

Important

If the washer does not spray liquid over the camera lens window, adjust the washer position preset and try again.

4. Activate the wiper.

   On the <%TARGETTITLE%>, under Wiper, click **Activate Wiper**. Make sure the wiper performs one full wiper cycle.

Caution

Before activating the wiper, make sure the lens window is wet. Using the wiper when the window is dry causes irreparable damage to the window coatings and voids the warranty.

Note: The wiper can be controlled in UVMS. In UVMS, the wiper is presented as an auxiliary command. In the UVMS Admin Center, click the **AUX** button. This will enable **Wiper/Push** to be the selected preset. The wiper can then be controlled using the play and stop buttons.

4.16 Additional Configuration Steps

To complete camera setup, you need to access the camera's web page with the default *admin* user or with another user assigned the Admin or Expert role. The camera web page supports the latest version of Google Chrome® and other popular web browsers.

Depending on installation and use, completing camera setup can also consist of:

- formatting the microSD card
- adjusting the camera's zoom and focus
- configuring the camera's video analytics
- configuring or modifying the default video stream settings
- configuring or modifying exposure, white balance, WDR, and other picture settings
- configuring or modifying security, advanced networking, alarms, and other system settings
- configuring handoff from a Quasar Premium Fixed BoxCamera with Edge AI Video Analytics (CF-6408-00-0A) to the camera

Many configuration steps can be performed before or after mounting the camera. However, some of them can or should only be performed after mounting the camera. For example, configure the camera's video analytics after mounting the camera.

4.17 Attach the Camera to a Supported VMS

After you have mounted the camera and discovered or defined its IP address, use VMS Discovery/Attach procedures to attach the camera to a supported VMS.

5 Operation

This chapter includes information about how to access the camera and how to operate it using the camera's web page.

5.1 Accessing the Camera's Web Page

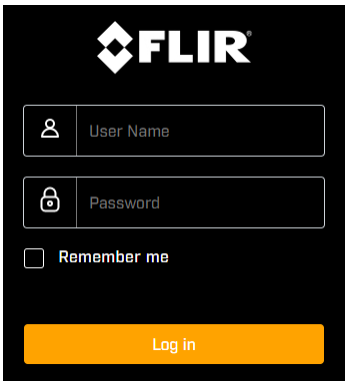
To operate the camera, you need to access it and log in its web page. The camera's web page supports the latest version of Google Chrome and other popular web browsers.

To log in to the camera's web page:

1. Do one of the following:
   - In the Teledyne FLIR Discovery Network Assistant (DNA) version 2.3.0.35 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 then double-click  to run the tool (DNA.exe). The Discover List appears, showing compatible devices on the VLAN.
   - Type the camera's IP address in a browser's address bar (when the PC and the camera are on the same network). If you do not know the camera's IP address, you can use the DNA tool to discover it.
2. On the login screen, enter a user name and the password. Passwords are case-sensitive. If you do not know a user name or password, contact the person who configured the camera's users and passwords.

   When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults:

   a. Log in with user name *admin* and the default password, *admin*.

   b. Specify a new password for *admin*:

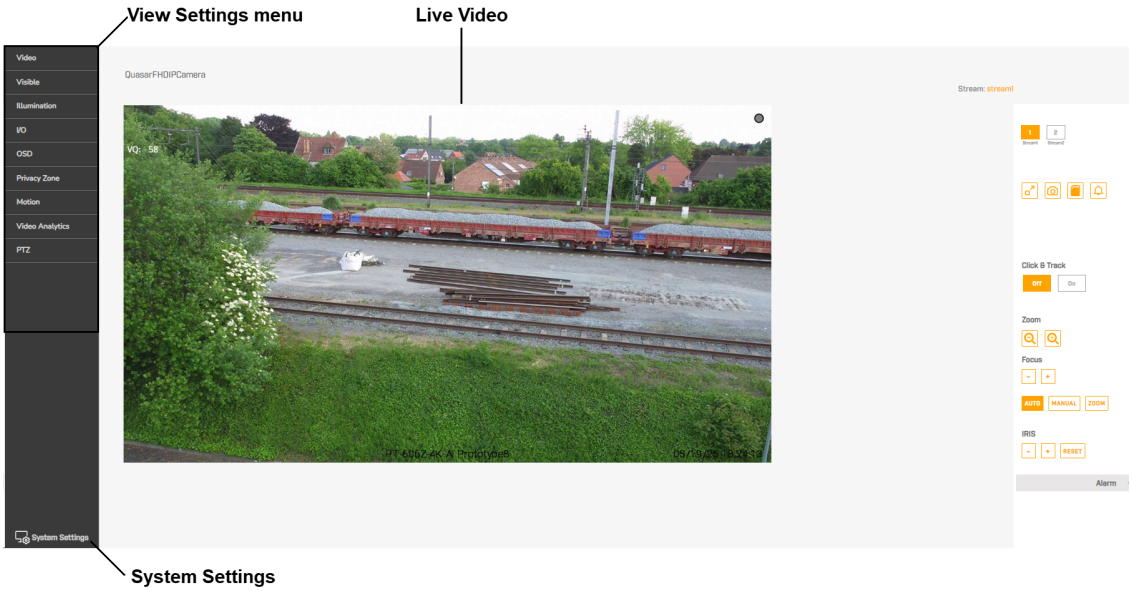
   - must be 8-64 characters
   - can include the following special characters: `@#~!$&<>+_-.,*?`
   - cannot include four-digit sequences (for example, 1234)
   - cannot include four repeating characters (for example, aaaa)

   a. Log back in using the new password.

The camera's View Settings Home Page opens.

5.2 View Settings Home Page

On the View Settings page, a navigation menu, live video images, and camera controls appear. Camera configuration and the role assigned to the user accessing the camera determines which settings and controls are available.



CP-6402-30-RA Camera Web Page - Light Mode - Two Streams Enabled

Above the live video, the following appear:

- **Languages—**The language for the camera's web page: English (default), Czech, Simplified Chinese, Traditional Chinese, French, German, Hungarian, Italian, Japanese, Polish, Portuguese, Russian, and Spanish.
- **Theme—**Dark Mode (default) or Light Mode; affects all users.
- **Help—**Opens https://www.flir.com/support/ in a new browser window.
- **Logout—**Logs out of the camera's web page.
- **Camera Name—**As specified on the Firmware & Info Page.
- **Stream—**Video stream providing current live video images.

Note

The live video on the camera's web page is not one of the camera's configurable video streams. Changes to video stream settings might not affect the live video.

To the left of the live video, the View Settings menu appears:

- **Video—**Opens the Video settings page.
- **Visible—**Opens the Visible settings page.
- **Illumination—**Opens the Illumination settings page.
- **I/O—**Opens the I/O settings page.
- **OSD—**Opens the OSD (on-screen display) settings page.
- **Privacy Zone—**Opens the Privacy Zone settings page.
- **Motion—**Opens the Motion settings page.
- **Video Analytics—**Opens the Video Analytics settings page.

- **PTZ—**Opens the PTZ settings page.

Below the View Settings menu, users assigned the Admin or Expert role can click **System Setting** to access system settings pages and configure the camera. For more information, see Configuration.

To the right of the live video, up to four enabled stream buttons appear. To see live video images from one of the enabled streams, click one of the buttons.

Camera Controls

When no settings page is open, the following can appear to the right of the live video:

	**Full Screen Button**	Maximizes live video in the computer display. To exit full-screen video, use the browser control. For example, on Google Chrome, you can press **ESC** or **F11**.
	**Snapshot Button**	Takes a snapshot of the live video. At least one video stream must be encoded in MJPEG.
	**SD Card Recording Button**	Initiates / stops SD card video recording.  indicates the camera is currently recording video to the SD card.
	**Manual Trigger Button**	Triggers a camera alarm.

Notes

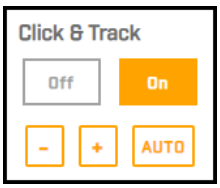
- The settings available might be different depending on the type of lens installed. If you are not sure how to configure the lens installed, contact Teledyne FLIR Support.
- In extreme cases, after adjusting the focus settings, it might be necessary to manually re-zoom the camera and focus it again.
- See also the digital zoom setting on the Visible Page.

To focus a new camera:

1. Manually adjust the lens to an approximate zoom and focus position.
2. Click **Push AF**. The camera performs a one-time auto-focus.
3. Click **Lock**. The camera locks focus.

You can also use this procedure to re-focus a camera after it has been moved or its focus has been accidentally changed by a VMS or network video recorder (NVR). **Click & Track—**Enables user-initiated PTZ tracking.

When Click & Track is **On**:



- On any View Settings page, you can:
  - Click on a detected object in the live video and the camera tracks it. When the camera is tracking an object, you can manually adjust the camera zoom you can enable automatic zoom (available on the View Settings home page, when no menu page is open).
- The camera disables any active PTZ mode such as a cruise or auto pan. To disable Click & Track and re-enable the automatic mode specified on the PTZ Page, click **Off**.

Zoom, Focus, and Iris

	Manual zoom out / in buttons.
	Manual focus out / in buttons.
	Focus mode buttons.
	Manual iris out / in and reset buttons.

Alarm

If the camera is currently triggering any alarms, they appear here.

5.3 Making Changes to Settings

The camera's configuration files store the following sets of settings:

- **Factory default settings—**The settings when you first connect the camera to power, and when resetting the camera to its factory default settings (see Firmware & Info Page). A partial factory reset restores all factory default settings except the settings on the Network Page.
- **Saved settings—**The settings you save as you operate and configure the camera. When the camera reboots, it restores these settings. Changes made to any setting since saving changes are lost.

Tip

Whenever possible, Teledyne FLIR recommends testing new settings before saving them because saving changes overwrites the previously saved settings.

View Settings

On View Settings pages, when an account assigned the Admin or Expert role makes a change to a setting, the camera does one of the following:

- immediately applies the change, but does not save it
- immediately applies and saves the change
- does not apply the change until you save it

On most View Settings pages, **Reset** and **Save** are available and when you make a change, they become enabled. To restore the previously saved settings for the current page, click **Reset**. Regardless of whether the camera has already applied changes, to save all changes made to settings on the current page since the last time the page's settings were saved, click **Save**. This can include changes made earlier that were not saved.

If the camera immediately applies and saves changes, a **Save** button does not appear and clicking **Reset** restores the previously saved settings for the current page. For example, on the Visible Page.

System Setting

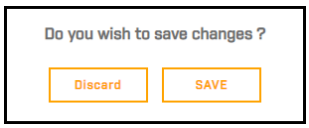
When Administrators make a change to most system settings, the **Discard Changes** link and the **Save** button become enabled. On some System Setting pages, the camera immediately applies the changes, but does not save them. On others, the camera does not apply changes until you save them.

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

Changes to some system settings require the camera to reboot and a confirmation message appears.

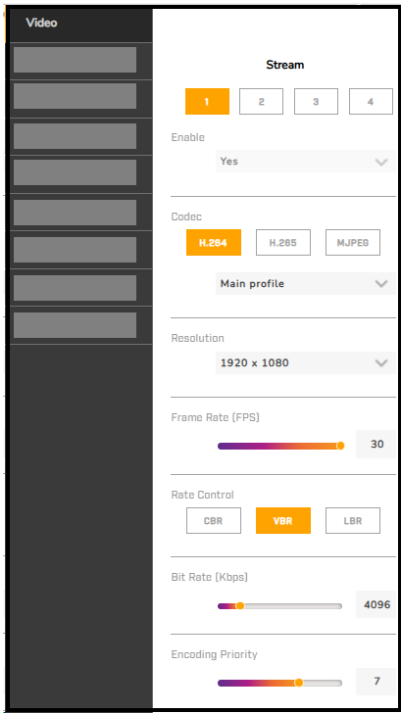
Tip

If you try to navigate away from a System Setting page before saving changes, a confirmation message appears. You can discard the changes or save them.



5.4 Video Page

On the Video page, users assigned the Admin or Expert role can configure the camera's four video streams for optimum quality and bandwidth.



Stream

Select one of the camera's four video streams, which you can enable or disable. For each enabled stream, you can specify:

- **Codec—**H.265, H.264 (default), or MJPEG, based on required image quality and storage space.

Notes

For the camera to be able to send images by FTP or email, MJPEG must be selected as the Codec for one of the streams.
When all enabled streams are set to H.265, the camera reduces the frame rate of the live video in the camera web page.

Resolution

- Resolutions for Stream 1 include:

- 1920x1080, 1280x1024, 1280x720, 800x600, 720x480

- Resolutions for Stream 2 include:
  - 1920x1080, 1280x1024, 1280x720, 1024x768, 800x600, 720x480, 640x480, 352x240, 320x240
- Resolutions for Stream 3 include:
  - 1920x1080, 1280x1024, 1280x720, 1024x768, 800x600, 720x480, 640x480, 352x240, 320x240
- Resolutions for Stream 4 include:
  - 320x240

Frame Rate

- Frame Rate is 1-30 (Frames Per second)

The other available stream settings depend on the codec selected.

H.265 and H.264 settings

- **Profile—**Each profile targets specific classes of applications.

High Profile	The primary profile for HD broadcast applications, providing the best trade-off between storage space required and video latency. High Profile can require 10-30% less storage space compared to Main Profile. However, depending on the stream structure, it can have higher video latency.
Main Profile (default)	The default setting. For SD broadcast applications, provides improved picture quality at reduced bandwidth and storage space required over Baseline Profile.

- **Rate Control**

CBR (Constant Bit Rate)	The camera constantly streams video at the specified bit rate, regardless of video content. CBR is not optimal for storage or quality; it does not stream enough data for complex video (which can result in poor video quality), and consumes too much storage space for simple video. Choosing a higher bit rate results in better quality, but requires more storage space.
VBR (Variable Bit Rate)	Varies the amount of data per time segment, up to the specified bit rate. VBR enables a higher bit rate (and therefore requires more storage space) for more complex video or audio, while a lower bit rate and less storage space is allocated to less complex media. VBR files can take longer to encode and be more problematic for streaming when the maximum bit rate is not set high enough for high instantaneous bit rates. Specify: • **Encoding Priority—**Adjusts the quality of the picture along a single axis, between 1 (low bit rate) and 10 (high picture quality). The default setting is 7.
LBR (Low Bit Rate)	Used primarily for speech at rates below 4kbps, the camera does not encode the entire audible frequency range. LBR consumes less storage space than CBR or VBR. Specify: • **Compression—**Hi (default), Mid, or Low. Low produces the highest image quality and requires the most storage space. High produces the lowest image quality and requires the least storage space. • **Dynamic GOV—**Enabled or Disabled (default). When enabled, specify: ○ **Max. GOV—**Between the I-frame Interval value and 4094. The default is 255.

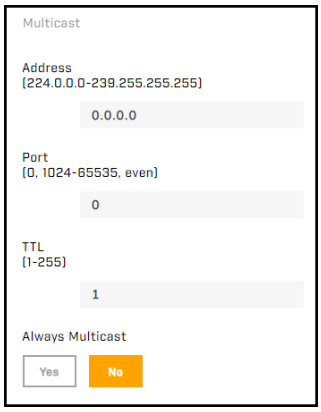
- **Bit Rate (Kbps)—**The higher the bit rate, the better the image quality. Set the maximum bit rate high enough to allow for a high instantaneous bit rate for more complex video. A higher bit rate consumes more storage space. Specify between 64 and 20480 kbps. The default is 4096.
- **I-frame Interval—**The number of P-frames the camera streams between I-frames; I-frames are full frames of video and P-frames contain the changes in the image since the last I-frame. Reducing the I-Frame Interval requires more stream bandwidth, because the camera streams more full frames, and improves video quality. Increasing the I-Frame Interval requires less bandwidth, but can degrade video quality. Specify a value between 1-4094. The default is 60; that is, by default, the camera streams one I-Frame every second.

MJPEG setting

- **Q Factor—**Higher values imply higher bit rates and higher video quality, between 1 and 70. The default is 35.

Multicast

For each video stream, specify:



- **Address (224.0.0.0-239.255.255.255)—**A valid multicast address.
- **Port (0, 1024-65535, even)—**The port the camera uses for multicast video streaming.
- **TTL (1-255)—**Time to live, the maximum number of network hops before routers discard the camera's data packets. Each time one router forwards the datagram to another router, it subtracts 1 (one) from the packet's TTL. If the TTL of a packet reaches zero (0), a router discards the packet. Teledyne FLIR recommends setting TTL at 64.
- **Always Multicast—**Yes or No.

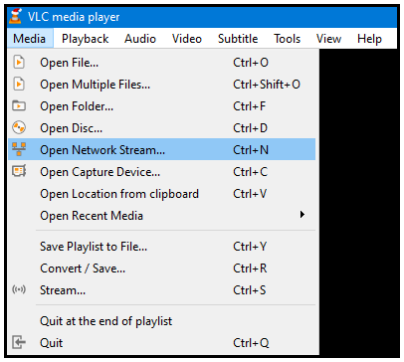
5.4.1 Viewing Live Video Using a Media Player

You can monitor any of the camera's enabled video streams with a media player that supports streaming; for example, VLC (download from http://www.videolan.org/vlc/index.html).

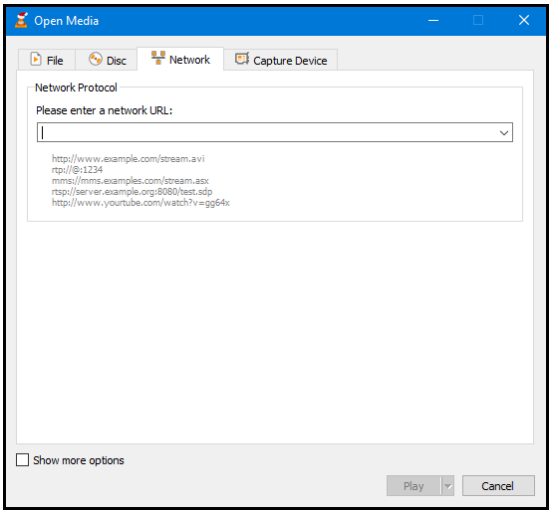
To view a video stream using VLC:

1. Open VLC.
2. In the navigation menu, click **Media** and then select **Open Network Stream**.

   The Open Media screen appears.



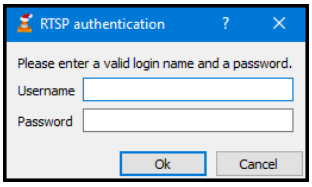
3. On the Network tab, specify the network URL for the camera's video stream. The network URL syntax is: rtsp:///(camera IP address):(camera RTSP port)/(stream). Using the camera's default IP address (192.168.0.250) and default RTSP port (554), the default network URLs are:



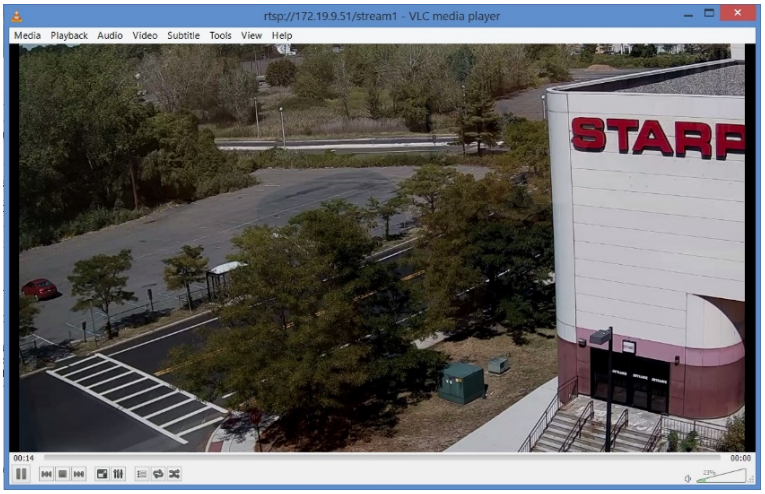
- **Stream 1—**rtsp://192.168.0.250:554/stream1
- **Stream 2—**rtsp://192.168.0.250:554/stream2
- **Stream 3**—rtsp://192.168.0.250:554/stream3
- **Stream 4**—rtsp://192.168.0.250:554/stream4

4. Click **Play**.

If RTSP authentication has been enabled in the Services section of the Cyber page, provide the user name and password for any of the camera's configured users.

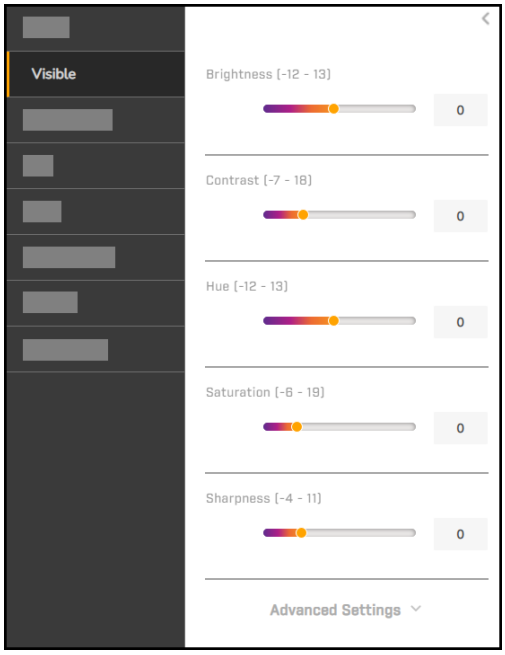


The video stream appears in the media player. If available, audio is also streamed.



5.5 Visible Page

Accounts assigned the Admin or Expert role can access and change the settings on the Visible page.



You can adjust:

Setting	Range
Brightness	Between -12 and +13
Contrast	Between -7 and +18
Hue	Between -12 and +13
Saturation	Between -6 and +19
Sharpness	Between -4 and +11

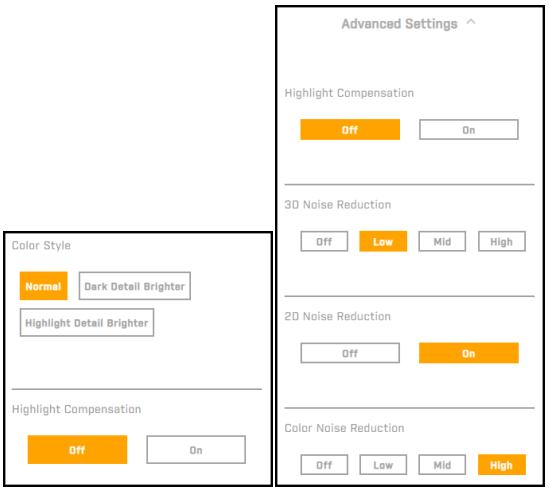
Zero (0) is the default for these settings.

Advanced Settings

Available settings depend on the current video format specified on the Firmware & Info Page and on the camera model. For example:

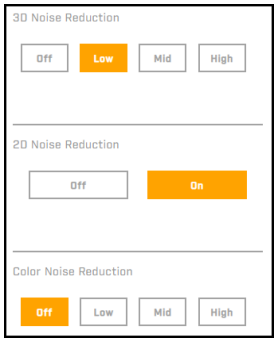
Video Format	Low Light Performance	Night Mode Priority	BLC
Linear	-	-	•
Shutter WDR	•	•	-

- **Color Style—**Normal, Dark Detail Brighter, or Highlight Detail Brighter. The default is Normal.
- **Highlight Compensation (HLC)—**Detects areas of the image overexposed by bright light sources such as headlights or spotlights and reduces image exposure only in these areas to enhance overall image quality. The default is Off.



Noise Reduction Settings

You can use the camera's noise reduction settings to reduce or eliminate artifacts that can limit the ability to positively identify an object. There are two types of noise: luminance and color (chroma) noise.

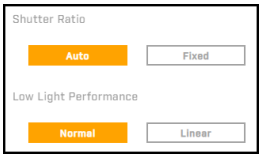


3DNR (three-dimensional noise reduction) and 2DNR (two-dimensional noise reduction) reduce luminance noise, which is composed of dots of various brightness levels (black, white and gray) luminance noise contains dots of varying brightness levels (black, white, and gray).

Teledyne FLIR recommends against completely eliminating luminance noise; doing so can result in unnatural images. We recommend adjusting ColorNR before configuring 3DNR and 2DNR.

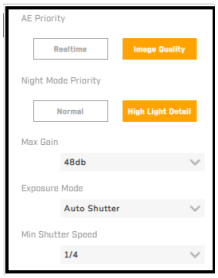
Setting	Description	Valid Values	Default
3D Noise Reduction	Provides superior noise reduction and is recommended for use in in extra low-light conditions. It is especially useful for reducing blur with moving objects. The 3DNR function reduces image noise/snow in low-light conditions by comparing adjacent frames. A higher level of 3DNR generates relatively enhanced noise reduction, although it creates more motion blur than 2DNR on moving objects.	Off Low Mid High	Low
2D Noise Reduction	Analyzes individual frames pixel by pixel and frame by frame to eliminate environmental noise and deliver optimized image quality, especially in low-light conditions. 2DNR tends to produce superior results for moving objects when applied to areas in the field of view where movement is present. However, it is less precise than 3DNR.	On Off	On
Color Noise Reduction	Controls noise that appears as red, green, and blue dots visible at edges between light and dark areas. Color High maximizes the blending of the color noise with the image, effectively removing the dots. Color Low minimizes the blending.	Off Low Mid High	Off

- **Shutter Ratio—**For scenes in which the amount of light changes dynamically, set to Auto (default). The camera automatically adjusts the ratio of the longest exposure to the shortest exposure. For scenes in which the amount of light remains constant, you can set it to Fixed. The camera does not automatically adjust the ratio. Available only for Shutter WDR video formats.

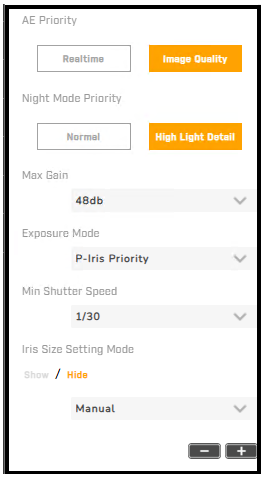


- **Low Light Performance**—For well-lit scenes, set to Normal (default). For dimly-lit scenes, set to Linear. When increasing gain to compensate for low light level, image noise increases. When set to Linear, the camera reduces that image noise. Available only for Shutter WDR video formats.

Exposure Settings



- **AE Priority—**By default (Image Quality), the camera simultaneously adjusts gain and shutter speed to achieve the highest possible image quality; therefore, the camera cannot guarantee real-time frame rates. When set to Realtime, maintaining real-time streaming is the camera's highest priority. It increases gain to its maximum level before adjusting shutter speed.
- **Night Mode Priority—**When set to High Light Detail, in Night Mode, the camera detects well-lit objects in the scene, and decreases overall exposure to increase detail visibility for those objects. At the same time, darker areas of the scene appear even darker. By default (Normal), the camera does not decrease exposure to increase detail visibility for well-lit objects.
- **Max Gain—**When not Off, determines the maximum allowed increase in image sensor sensitivity. Increasing gain brightens the image, and adds details. It also increases the level of noise in the image. Select between Off-48db, in 3db increments; the default is 48db.
- **Exposure Mode—**The amount of time the camera shutter is open (shutter speed) and other exposure settings determine the amount of light the image sensor receives; that is, its exposure. The camera can use a programmed algorithm to automatically select an exposure level or you can manually configure exposure settings. Available settings depend on the selected exposure mode. Exposure Modes include:

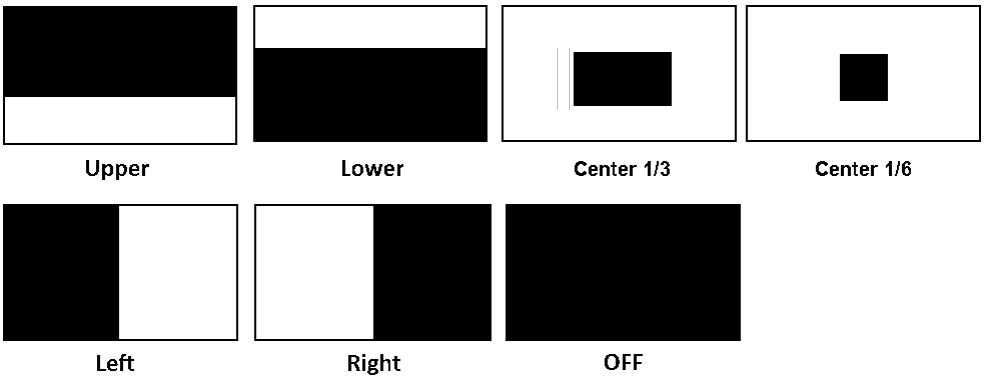


  - Auto Iris
  - P-Iris Priority
  - Iris Priority
  - Auto Shutter (default)
  - Shutter Priority
  - Manual Mode

    - Auto Shutter Mode (default)
    - <%TARGETTITLE%>
    - Auto Shutter Mode
    - <%TARGETTITLE%>

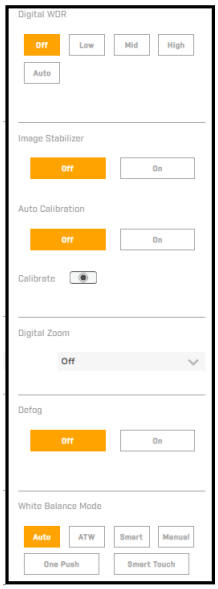
    - Manual Mode
    - <%TARGETTITLE%>
    - Manual Mode

- **Backlight Compensation** (BLC)—When a bright light source puts the region of interest (ROI) in shadow or silhouette, enabling BLC can improve the image. By default, BLC is disabled and the camera's auto exposure algorithm considers the entire image. With BLC enabled, the algorithm considers only the selected ROI.

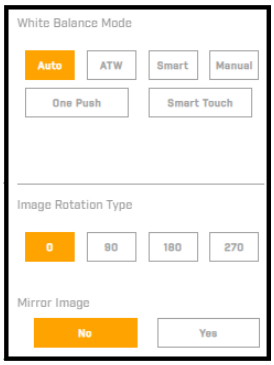


- **Digital WDR** (dWDR)—Digitially enhances the details in each frame to improve image quality and the amount of detail in high contrast scenes. That is, scenes consisting of areas with different lighting conditions; some areas are bright and others are dark. Without dWDR, either the bright areas would be too bright (overexposed) or the darker areas would be completely dark (underexposed). dWDR can produce more detail in both the dark and the bright areas of the image. You can increase the dWDR setting as the level of scene contrast increases. Select Off (default), Low, Mid, High, or Auto.

  The camera also supports Shutter WDR (see the Video Format setting on the Firmware & Info Page). Digital WDR is available with all of the camera's video formats.



- **Image Stabilizer**—Select Off (default) or On.
- **Auto Calibration**—Select Off (default) or On, for ongoing automatic image stabilizer calibration.
- **Calibrate**—To manually trigger a one-time image stabilizer calibration, click  .
- **Digital Zoom**—Select Off (default) or between 2x-10x.
- **Defog**—Select Off (default) or On.
- **White Balance Mode—**The camera needs a reference color temperature of the ambient light source to calculate all other colors. The unit for measuring this ratio is in Kelvin (°K) degrees. The table shows the color temperature of some light sources for reference.



Light Source	Color Temperature in K°
Cloudy sky	6,000 to 8,000
Noon sun and clear sky	6,500
Household lighting	2,500 to 3,000
75-watt bulb	2,820
Candle flame	1,200 to 1,500

  - **Auto—**If the light source color temperature changes, the camera automatically adjusts the white balance. Suitable for light source color temperatures ranging from approximately 2,700K to 7,800K.
  - **ATW (Auto Tracking White Balance)—**If the light source color temperature changes, the camera automatically adjusts the white balance. Suitable for light source color temperatures ranging from approximately 2,500K to 10,000K.

- **Smart—**Suitable for environments with a single background color that is strongly saturated; for example, in a forest.
- **Manual—**Specify the Rgain and Bgain to define the red and blue luminance, respectively. Might not be ideal for every lighting environment. Specify 0-249.
- **One Push—**When you click , the camera adjusts and fixes the white balance according to the scene at that moment. Works best with minimal scene changes and continuous lighting. Suitable for light sources at any color temperature.

> **Note**
>
> The camera's white balance is fixed and does not change as the scene or the light source varies. You might have to re-adjust the white balance by clicking the button again when needed.

- **Smart Touch—**Camera uses the specified portion of the scene as the white balance reference. Move and resize the reference area by clicking and dragging the area or its borders. Make sure that the background color of the selected area is white. Then, click . Suitable for environments in which the brightness level does not change.

Default reference area

Image Orientation

- **Image Rotation Type—**Select 0, 90, 180, or 270 (degrees clockwise), where 0 (zero) does not rotate the image. If the video analytics metadata overlay is enabled on the OSD Page, rotating the image 90 or 270 degrees disables the VA metadata OSD.
- **Mirror Image—**Yes flips the image along its vertical axis.

Mirror Image Disabled

Mirror Image Enabled

5.5.1 Auto Iris Mode

In Auto Iris mode, based on the amount of light in the scene, speed of moving objects, and noise, specify the minimum shutter speed, the camera's slowest shutter speed. Reducing the shutter speed - that is, keeping the shutter open longer - can cause moving objects to be blurred. To achieve a consistent exposure level, the camera adjusts the iris size and other exposure settings. The video format determines the valid values, as shown, in fractions of a second.

Min Shutter Speed - Auto Iris Mode					
PAL			NTSC		
1/25	1/6	1/1.5	1/30	1/8	1/2
1/12	1/3	-	1/15	1/4	1

5.5.2 P-Iris Priority Mode

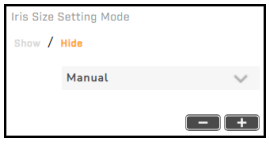
In P-iris Priority mode, adjust the iris size, which then remains fixed, and the minimum shutter speed. To achieve a consistent exposure level, the camera adjusts the other exposure settings. However, if the amount of light entering the camera lens drops below the exposure level required, the camera automatically fully opens the iris.

The settings and valid values available depend on the camera model.

- **Min Shutter Speed—**Based on the amount of light in the scene, speed of moving objects, and noise, specify the slowest shutter speed. Reducing the shutter speed - that is, keeping the shutter open longer - can cause moving objects to be blurred. The video format determines the valid values, as shown, in fractions of a second:

Min Shutter Speed - P-Iris Priority Mode			
PAL		NTAC	
	1/6		1/8
	1/3		1/4
	1/1.5		1/2
1/25	-	1/30	1
1/12	-	1/15	-

- **Iris Size Setting Mode—**Click **Show** and then select one of the following:
  - **Auto Detect—**Initiates a one-time automatic iris size setting.
  - **Manual—**



closes the iris

opens the iris

Increasing the iris size increases the amount of light reaching the camera sensor when the shutter is open; therefore, to maintain a consistent exposure level, increase the minimum shutter speed.

5.5.3 Iris Priority Mode

In Iris Priority mode, specify a fixed iris size and the minimum shutter speed. To achieve a consistent exposure level, the camera adjusts the other exposure settings.

- **Iris Size (0-10)—**Specify the fixed iris size, where 10 is fully open. Increasing the iris size increases the amount of light reaching the camera sensor when the shutter is open and therefore, the faster the minimum shutter speed should be.
- **Min Shutter Speed—**Based on the amount of light in the scene, speed of moving objects, and noise, specify the slowest shutter speed. Reducing the shutter speed - that is, keeping the shutter open longer -

can cause moving objects to be blurred. The video format determines the valid values, as shown, in fractions of a second:

Min Shutter Speed - Iris Priority Mode					
PAL			NTSC		
1/25	1/6	1/1.5	1/30	1/8	1/2
1/12	1/3	-	1/15	1/4	1

5.5.4 Auto Shutter Mode

In Auto Shutter mode, the camera fully opens the iris. Based on the amount of light in the scene, speed of moving objects, and noise, specify the slowest shutter speed. Reducing the shutter speed - that is, keeping the shutter open longer - can cause moving objects to be blurred. To achieve a consistent exposure level, the camera adjusts other exposure settings, including the automatic gain control (AGC), and prioritizes the fully open iris.

Teledyne FLIR recommends Auto Shutter mode for indoor environments involving mixed lighting sources, where the main source is fluorescent lighting combined with natural light that enters the scene through windows and other exposed areas.

The video format determines the valid values, as shown, in fractions of a second:

Min Shutter Speed - Auto Shutter Mode									
PAL					NTSC				
1/425	1/150	1/75	1/12	1/1.5	1/500	1/180	1/90	1/15	1/2
1/300	1/120	1/50	1/6	-	1/350	1/120	1/60	1/8	1
1/215	1/100	1/25	1/3	-	1/250	1/100	1/30	1/4	-

5.5.5 Shutter Priority Mode

In Shutter Priority mode, based on the amount of light in the scene, speed of moving objects, and noise, specify the fixed shutter speed. Reducing the shutter speed - that is, keeping the shutter open longer - can cause moving objects to be blurred. To achieve a consistent exposure level, the camera adjusts other exposure settings.

The video format determines the valid values, as shown, in fractions of a second.

Fixed Shutter Speed - Shutter Priority Mode					
PAL			NTSC		
1/425	1/150	1/75	1/500	1/180	1/90
1/300	1/120	1/50	1/350	1/120	1/60
1/215	1/100	1/25	1/250	1/100	1/30

5.5.6 Manual Mode

Teledyne FLIR recommends Manual mode for scenes with fixed light levels and fixed lighting contrast such as indoor scenes; when requiring a consistent, precise exposure level; and the camera is not providing the desired exposure using other modes.

- **Shutter Speed—**Based on the amount of light in the scene, speed of moving objects, and noise, specify the fixed shutter speed. Reducing the shutter speed - that is, keeping the shutter open longer - can cause

moving objects to be blurred. The video format determines the valid values, as shown, in fractions of a second.

Shutter Speed - Manual Mode							
PAL				NTSC			
1/32000	1/600	1/120	1/12	1/32000	1/725	1/120	1/15
1/10000	1/425	1/100	1/6	1/10000	1/500	1/100	1/8
1/3500	1/300	1/75	1/3	1/3000	1/350	1/90	1/4
1/2500	1/215	1/50	1/1.5	1/2000	1/250	1/60	1/2
1/1250	1/150	1/25	-	1/1000	1/180	1/30	1

- **Iris Size (0-10)**

  Increasing the iris size increases the amount of light reaching the camera sensor when the shutter is open and therefore, the faster the minimum shutter speed should be.

  Specify the fixed iris size, where 10 is fully open. The default is 6.

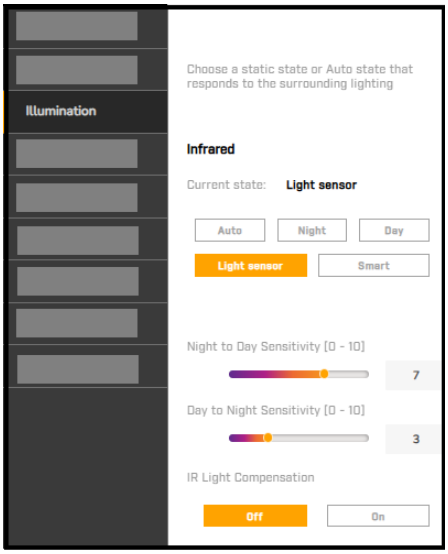
- **Gain—**When not Off (no gain), increases the image sensor sensitivity. Increasing gain brightens the image, and adds details. It also increases the level of noise in the image. Select Off or between 3-48db, in 3db increments; the default is Off.

5.6 Illumination Page

On the Illumination page, users assigned the Admin or Expert role can enable and configure settings that control the camera's IR Cut (IRC) filter, which improves the camera's color video quality by filtering out IR light.

- IR Cut (IRC) filter, which improves the camera's color video quality by filtering out IR light
- IR LED illuminator, which enhances the camera's monochrome (black and white) video in low-light conditions and at night

Select an Infrared state.



State	Video	IRC filter	IR LED	Use
Auto	The ambient light level detected by the camera's image sensor determines when the camera switches: • video between color and monochrome • the IRC filter on and off		Disabled	When the ambient light level changes throughout the day and IR illumination is not desired

State	Video	IRC filter	IR LED	Use
Night	Monochrome	Disabled	Disabled	When the ambient light level is permanently low and IR illumination is not desired
Day	Color	Enabled	Disabled	Daytime outdoors when the IRC filter is desired and IR illumination is not desired
Light Sensor (default)	The ambient light level detected by the camera's light and image sensors determines when the camera switches: • video between color and monochrome • the IRC filter on and off • the IR LED on and off			Most situations; when available, Teledyne FLIR recommends using this IR mode
Smart	Improves monochrome video stability and prevents the camera from switching back and forth between monochrome and color video. When the image sensor detects that the main light source is IR illumination - that is, when the camera is providing monochrome video in night mode - it keeps the IRC filter enabled.			

Night to Day / Day to Night Sensitivity—Thresholds at which the video switches from monochrome to color (Night to Day Sensitivity) and vice versa (Day to Night Sensitivity). Select 0-10, where 0 switches the video at a lower light level (darker) and 10 switches the video at a higher light level (brighter). The default Night to Day Sensitivity setting is 7 and the default Day to Night Sensitivity setting is 3.

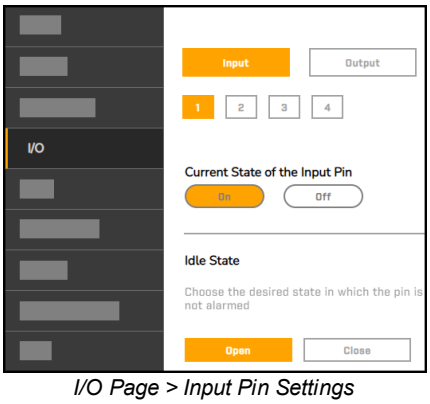
Note

During day-night transitions, video can appear off-color. Within a few seconds, as the level of light decreases or increases, and depending on the time of day, accurate color reproduction should return.

IR Light Compensation—When an external IR LED illuminator is on, prevents objects close to the camera in the center of the field of view from being too bright. Off by default.

5.7 I/O Page

On the I/O (input / output) page, users assigned the Admin or Expert role can see the current state of the input and output pins (On = open; Off = closed), and can specify whether they are normally open or normally closed.



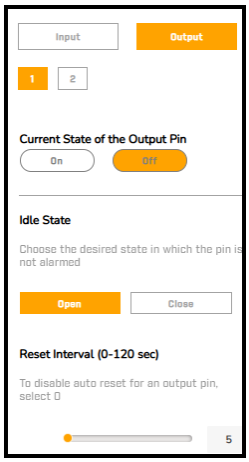
I/O Page > Input Pin Settings

To Configure the I/O Page:

1. Select **Input** or **Output**.
2. Select the pin.
   a. If you selected Input, select pin (1-4).
   b. If you selected Output, select pin (1-2).
3. Under **Idle State,** the normal state of the pin when there is no alarm, choose:
   a. Open

b. Close

4. If you chose **Output**, specify the **Reset Interval**.
   a. 0-120 seconds (default is 5).
   b. After the specified amount of time, the output pin automatically resets its idle state
   c. To disable this automatic reset, specify 0 (zero).



I/O Page Output Settings

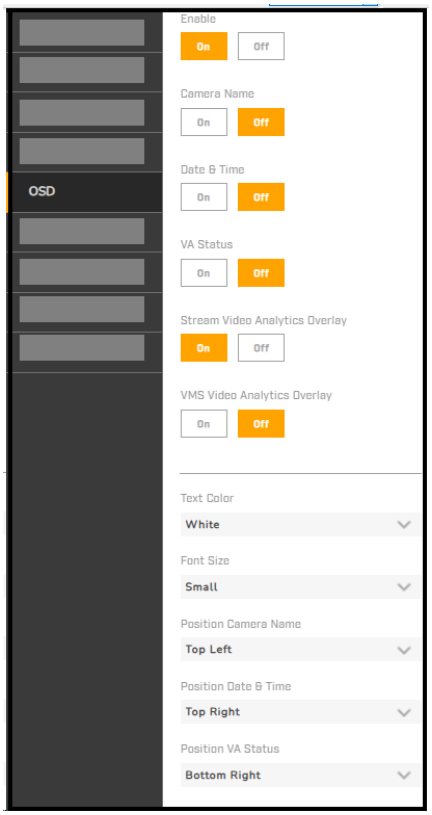
For information about how to configure a change in the state of the an input pin as an alarm trigger or how to configure changing the output state of the an output pin as an alarm action, see Alarm Page.

Important - CP-6408-31-IA

If an optional washer pump is connected to pins 3 and 4 (Alarm-Out A1 and A2) on the camera's 14-pin alarm and I/O terminal block connector, local output pin 1 is reserved for washer pump operation. For information about how to configure local output pin 1 so that it controls the washer pump, see Install and Test the Optional Wash Kit - CP-6408-31-IA model. Then, to activate the washer pump, on the Alarm Page, you can configure an alarm that specifies local output pin 1 as the alarm action.

5.8 OSD Page

Users assigned the Admin or Expert role can configure the OSD page.



To Configure:

1. Enable or disable the on-screen display (OSD) for all video streams.
2. Enable or disable the camera name appearing in the OSD.
3. Enable or disable the date & time appearing in the OSD.
4. Enable or disable video analytics (VA) overlay in all video streams.
   a. Green boxes indicate detected objects, which are labeled Person or Vehicle.
   b. Red boxes indicate objects triggering alarms.
   c. If the image is rotated 90 or 270 degrees, it is not possible to enable the stream VA overlay.
   d. You can change the image rotation on the Visible Page.
5. Enable or disable VMS VA overlay.
   a. When enabled, the camera provides VA metadata that the VMS uses to draw detection zones and detected object boxes; supported in FLIR UVMS version 9.2.3 and higher.
6. Enable or disable VMS Video Analytics Overlay.

a. Teledyne FLIR recommends enabling either VMS Video Analytics Overlay or Stream Video Analytics Overlay, but not both at the same time.

7. Specify **Text Color**—black, white (default), yellow, red, green, blue, cyan, or magenta; does not apply to stream VA overlay box labels
8. Specify **Font Size**—small (default), medium, or large
9. Choose the **Position Camera Name**—top left (default), top right, bottom left, bottom right.
10. Choose the **Position Date & Time**—top right (default), top left, bottom left, bottom right.
11. Choose the **Position VA Status**—top right, top left, bottom left, bottom right (default).

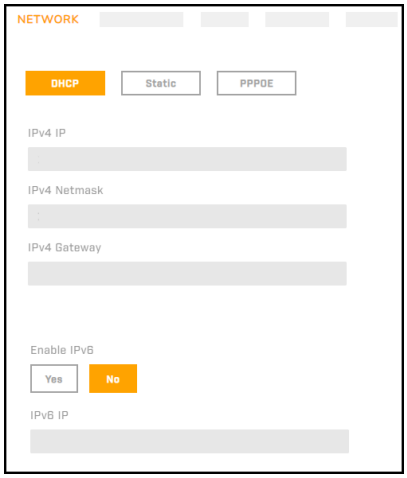
5.8.1 Configuration

Users assigned the Admin or Expert role can click **System Setting** on the View Settings page to access the following configuration pages:

- Network Page
- Date & Time Page
- Users Page
- SD Card Page
- Alarm Page
- Schedule Page
- Audio Page
- Recording Page
- Email Page
- FTP Page
- HTTP Page
- Cyber Page
- Firmware & Info Page

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

5.8.1.1 Network Page



When you click **System Setting**, by default, the Network page appears.

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

Specify the camera's IP addressing mode:

- **DHCP (default)—**Dynamic Host Configuration Protocol server on the network assigns the camera its IP addresses, and determines the IPv4 Netmask and Gateway. The information appears in these fields, which you cannot modify. If the IP addressing mode is set to DHCP but a DHCP server is not available on the network, the camera's default IP address is 192.168.0.250.
- **Static—**Specify:
  - **IPv4 IP**—Camera's IPv4 address.

Caution

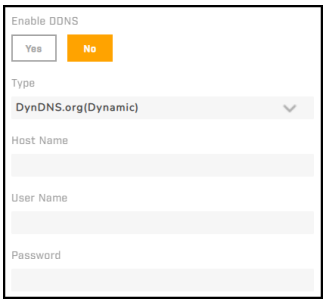
After changing the camera's IPv4 address, the PC you are using to access the camera's web page might no longer be on the same network as the camera and can no longer access the camera's web page. To access the camera web page again, change the PC's IPv4 address to be on the same network as the camera.

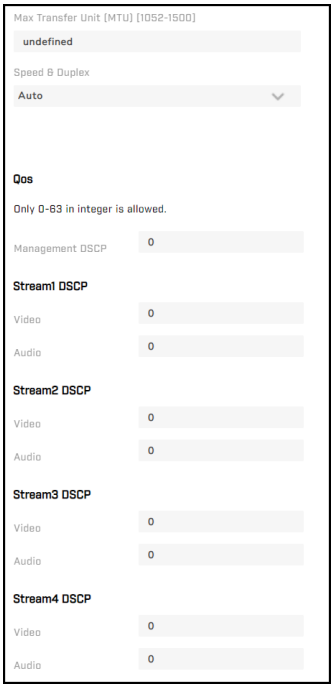
  - **IPv4 Netmask**—Determines whether devices are on the same subnet. The default value is 255.255.255.0.
  - **IPv4 Gateway—**IP address of the server that passes data between devices on different subnets. An invalid gateway setting causes communication between the camera and devices on other subnets to fail.
  - **Primary DNS—**IP address of the domain name server that translates host names into IP addresses.
  - **Secondary DNS—**IP address of the domain name server that backs up the primary DNS.
- **PPPoE—**Camera connects to the network using Point-to-Point Protocol over Ethernet and is assigned an IP address. Specify the User Name and Password for the PPPoE account. Then, click **Save**. If the PPPoE connection is successful, the camera's assigned IPv4 address appears.

Tips

- You can also use the DNA tool to specify the IP addressing mode as DHCP or Static for one or more of the same camera model. For more information, see Configure for Networking.
- For future reference, record the camera's MAC address, which is found on the camera label.

- **Enable IPv6—**When IPv6 is enabled and the IP addressing mode is Static, specify the camera's IPv6 address. By default, IPv6 is disabled.
- **Enable DDNS—**The Dynamic Domain Name System (DDNS), which allows a static device host name to be constantly synchronized with its dynamic IP address. This allows access to the device using the static host name. By default, DDNS is disabled. When enabled, specify:
  - **Type—**DDNS host provider. DynDNS.org (Dynamic) is the default.
  - **Host Name—**Name that identifies the camera for DDNS.
  - **User Name—**User name required by the DDNS provider for authentication.
  - **Password—**Password required by the DDNS provider for authentication.





- **Maximum Transmission Unit (MTU) (1052-1500)—**Largest amount of data the camera can transmit in one physical frame on the network. For Ethernet, the MTU is 1500 bytes (default). For PPPoE, the MTU is 1492.
- **Speed & Duplex—**Select:
  - **100 Mbps Full Duplex—**Camera supports 100 Mbps Ethernet and can simultaneously transmit and receive data.
  - **100 Mbps Half Duplex—**Camera supports 100 Mbps Ethernet, but cannot transmit and receive data at the same time.
  - **Auto—**Camera supports and automatically detects 10 / 100 / 1000 Mbps Ethernet.

QoS

QoS (quality of service) provides differentiated service levels for different types of traffic packets and guarantees delivery of priority services during periods of network congestion. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Code Point) values, and as a result receive the corresponding forwarding treatment from DiffServ-capable routers.

Specify values (0 to 63) for:

- **Management DSCP—**Class of service for camera management via HTTP.

And for each of the camera's four streams:

- **Video DSCP—**Class of service for the stream's video.
- **Audio DSCP—**Class of service for the stream's audio.

By default, DSCP disabled; that is, the value for each service class is 0 (zero).

Note

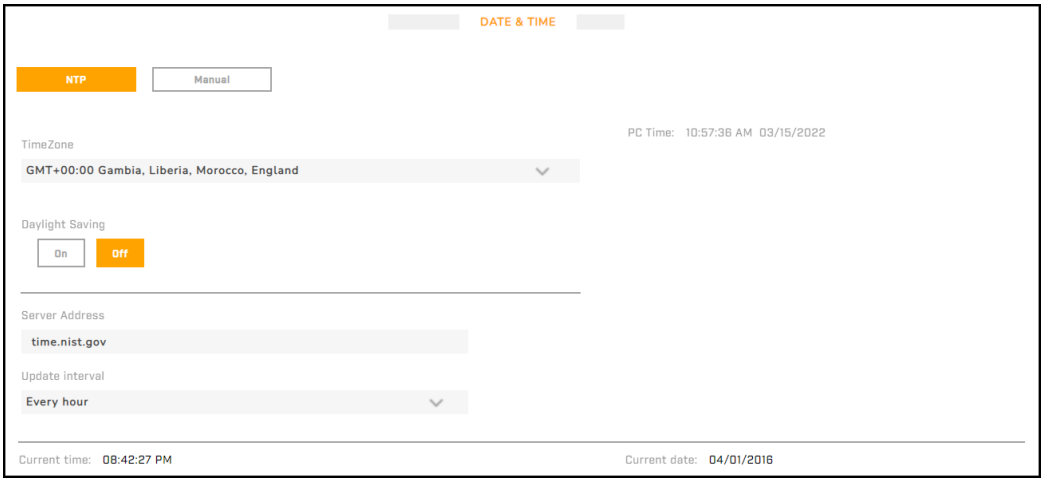
Before assigning DSCP values, make sure the switches / routers on the network support QoS.

5.8.1.2 Date & Time Page

On the Date & Time page, users assigned the Admin or Expert role can select **NTP** (default) or **Manual**.

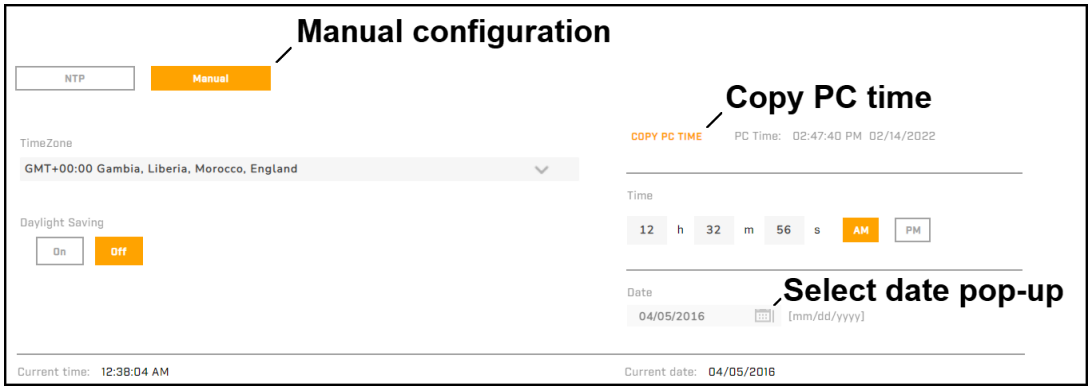
NTP—Camera synchronizes its date and time with an NTP server. Specify:

- **Server Address—**IP address of the NTP server or URL of an NTP service (default: time.nist.gov)
- **Update Interval—**every hour (default), every day, or every week



NTP Date & Time Configuration

Manual—Manually configure the camera's date and time. Click **Copy PC Time** or manually specify the hour, minute, second, AM or PM, and date.



Manual Date & Time Configuration

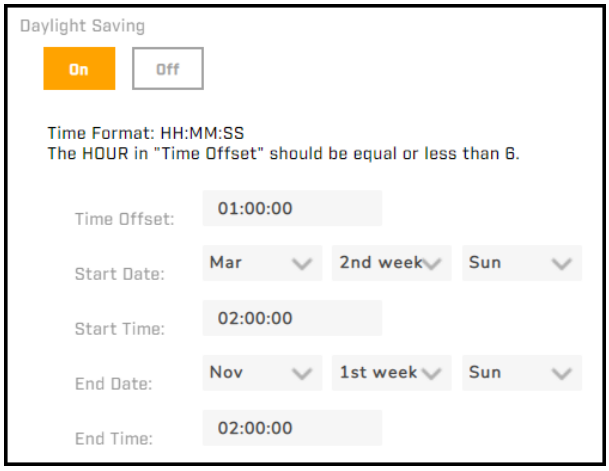
In either NTP or manual configuration, specify:

- **Time Zone**
- **Daylight Saving—**By default, the camera time does not change according to daylight saving time (Off).

  If you enable Daylight Saving (On), specify:

  - **Time Offset—**Number of hours, minutes, and seconds between daylight saving time and standard time. The time offset format is hh:mm:ss. 1:00:00, or one hour, is the default.

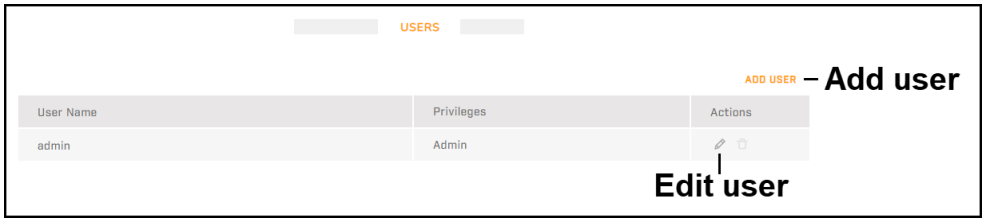
- **Start Date, Start Time, End Date, and End Time—**Select the date and time specified by law. For example, in most places in the US, specify 2 AM on the second Sunday in March and 2 AM on the first Sunday in November, respectively:



US Daylight Saving Time Settings

5.8.1.3 Users Page

On the Users page, users assigned the Admin role can add and remove users, and can change or set passwords.

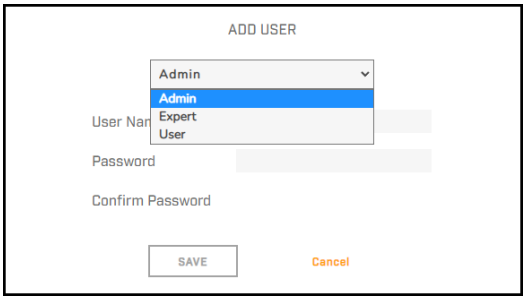


To prevent unauthorized access to the camera:

- Make sure the default password for the admin user has been changed.
- Add users for each required login account, up to a maximum of 20 users.

To add a new user:

1. Click **Add User**. The Add User screen appears.



2. Assign one of the following roles (Privileges), according to the access the user requires:

Role	Access
User	Can: • Select a different web page language • View live video images from any enabled video stream • View live video in a full-screen browser window • Take a snapshot • View alarms • Toggle the web page between Light Mode and Dark Mode • View the Help page • Log out
Expert	Cannot manage users: • Cannot add/edit/delete users • Cannot change passwords Can access and use all other View Settings and System Settings pages, menus, controls, and settings
Admin, including the default *admin* user	Can access and use all of the camera's web pages, including adding/editing/deleting users (but cannot delete the default admin user), and setting all passwords
All roles can access the camera's video streams, which require authentication. You can use the name and password for any of the camera's users.	

3. Specify a user name and password, and then confirm the password, according to the following requirements:

   - User names and passwords are case-sensitive.
   - User names are limited to 29 characters and can only include alphanumeric characters A-Z, a-z, 0-9.
   - Use strong passwords consisting of 8-64 characters. Passwords can include special characters @#~!$&<>+_-.,*?. Passwords cannot contain four-digit sequences (for example, 1234). They also cannot contain four repeating characters (for example, aaaa).

Managing Existing Users

To change the password for a user, click the edit icon for the user, change the password, and then confirm the change. To delete a user, click the trash icon for the user, and then confirm deleting the user. The admin user cannot be deleted.

5.8.1.4 SD Card Page

With a microSD card properly installed, the camera can locally record video clips and snapshots, up to 1 TB. For information about how to install a microSD card (not included in the camera kit), see <% TARGETTITLE%>.

On the SD Card page, users assigned the Admin or Expert role can format the microSD card, configure its settings, and view its properties.

Overwrite—When a microSD card is properly installed, the camera automatically enables Overwrite. Specify the amount of time the camera retains recorded files, in days or weeks, and when the camera begins removing the oldest recorded files, in percentage the disk is full (1-99%).

Recording file size (15-600 MB)—Specify the maximum file size. The default is 200 MB.

SD Card Information

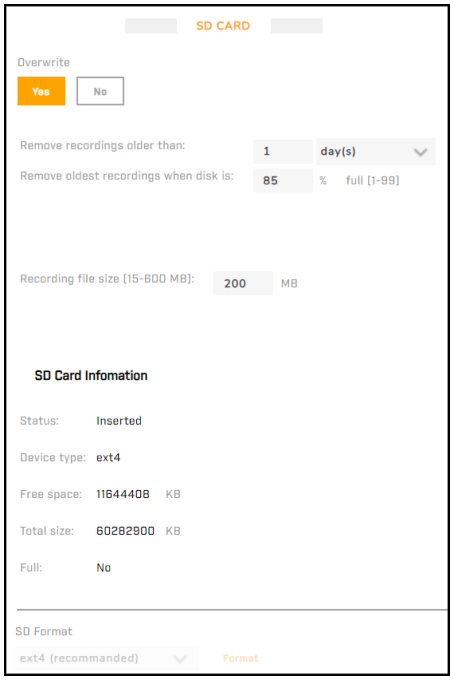
When a microSD card is properly installed:

- Inserted appears as the Status.
- Capacity information appears, in KB.

SD Format

Before using a properly installed microSD card for the first time or when the card has been previously used on a different camera, format it.

When a microSD card is properly installed, you can select the format: vfat (default) or ext4 (recommended). Then, click **Format**. The camera formats the card.



microSD Card Properly Installed

5.8.1.5 Alarm Page

On the Alarm page, users assigned the Admin or Expert role can configure alarms for the following triggers:

- a change in the state of an alarm input pin
- each motion detection profile
- network failure
- a predefined periodic interval
- audio input
- manual alarm trigger
- each VA profile

For most triggers, you can specify whether the alarm is enabled all the time or according to one of the schedules defined on the Schedule Page.

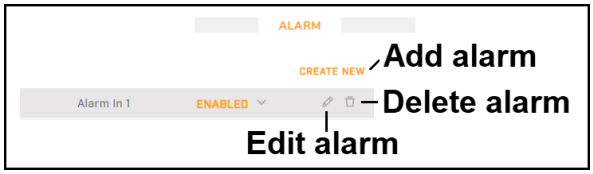
Depending on the alarm trigger, you can specify one or more of the following actions:

- change the state of one or more alarm output pins
- toggle the IR Cut (IRC) filter
- send message by FTP
- send notification email
- upload snapshot image(s) by FTP
- upload snapshot image(s) by email
- record image(s) to microSD card

- send HTTP notification
- record video clip to microSD card or to a NAS (network attached storage) server

By default, the following alarm is defined:

- **Alarm In 1—**A change in the state of alarm input pin 1 triggers a change in the state of the alarm output pin 1. You cannot modify the trigger for this alarm. You can configure the idle state of alarm input pin 1 on the I/O Page.



When you define or enable a motion detection profile or when you enable a VA profile, the camera automatically creates an alarm. For example:

- **Video Analytics 1—**The rule specified for Video Analytics Profile 1 on the <%TARGETTITLE%> triggers this alarm. However, by default, no action is enabled. Video Analytics 1 / 2 refer to the default preset profile. When you enable a preset profile, the camera creates and enables an alarm specific to the preset profile. For example, Preset Profile 1: Video Analytics 1.

When you define or enable a motion detection profile, the camera automatically creates an alarm. For example:

- **Motion 1—**The motion detection region for profile 1 configured on the <%TARGETTITLE%> triggers this alarm. However, by default, no action is enabled.

To add an alarm, click **Create New**. The alarm Trigger screen appears. Continue with Defining an Alarm Trigger.

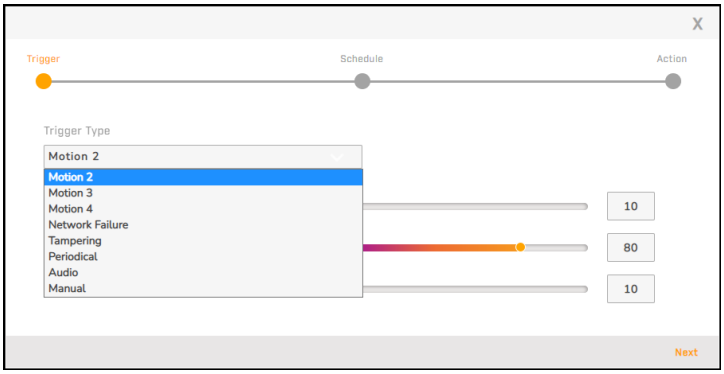
To modify an existing alarm, click the edit icon for the alarm. The alarm Trigger screen appears. Continue with Defining an Alarm Trigger.

To delete an alarm, click the trash icon for the alarm, and then confirm deleting the alarm.

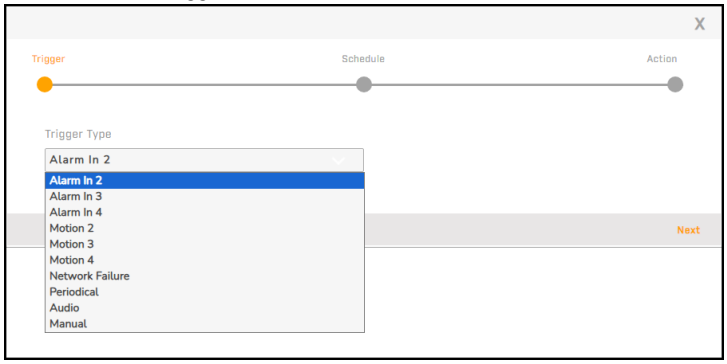
5.8.1.5.1 Modifying or Defining an Alarm Trigger

When creating a new alarm, on the Trigger screen, users assigned the Admin or Expert role can select a trigger and configure its alarm settings.

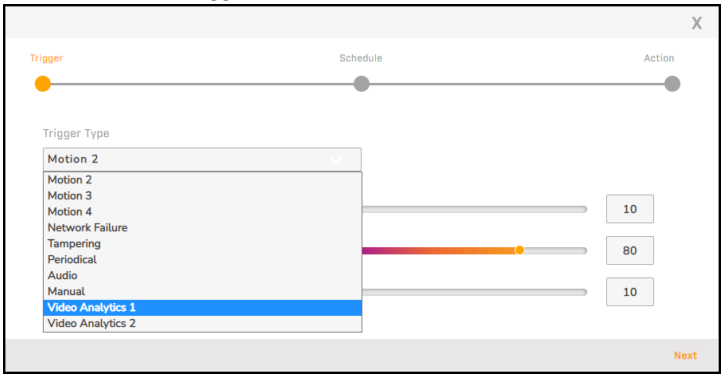
If you are modifying an existing alarm, click **Next**. If the alarm Schedule screen appears, continue with Specifying an Alarm Schedule. If the alarm Action screen appears, continue with Modifying or Defining Alarm Actions. It is not possible to modify the trigger for an existing alarm.



Trigger Screen - Motion 2 Profile Selected



Trigger Screen - Alarm In 2 Selected



Trigger Screen - Video Analytics 1 Profile Selected

To Create a new alarm:

1. Click **Create New.**
2. Select a **Trigger Type** including:
   a. **Alarm In (1 / 2 / 3 / 4)—**Alarm Input Pin.
      i. A change in the alarm input pin state triggers the alarm. You can configure the idle state of alarm input pins on the I/O Page.
   b. **Motion (1 / 2 / 3 / 4)—Motion Detection Profile** alarm**.** Specify:
      i. **Detection level (1-100)—**Sensitivity for each sampled pixel. Lowering the value increases detection sensitivity and vice versa. The default is 10.
      ii. **Sensitivity level (1-100)—**Camera's overall motion detection sensitivity. The default is 80; if 20% or more of the sample pixels are detected as being different, the camera detects motion. Increasing the value increases detection sensitivity.

iii. **Time interval (sec) (0-7200)—**Minimum amount of time, in seconds, between motion detection alarms. The default is 10.

a. **Network Failure—**Camera periodically pings another IP device on the network to confirm network connectivity. For example, the camera can ping the NAS server specified on the Recording Page.

i. Specify Ping IP address.

ii. Specify Time interval, seconds between pings, (1-6000 seconds). Default is 60.

iii. If the camera detects that it cannot connect to the server, configure the alarm to trigger local recording on a properly installed microSD card as a backup until network connectivity is restored.

a. **Periodical—**Camera triggers an alarm at the specified Minimum interval.

i. Specify Minimum interval in seconds (60-3600). The default is 60; that is, the camera triggers an alarm every minute.

a. **Audio—**Camera triggers an alarm when audio input reaches or exceeds the specified level.

i. Specify Detection Level (1-99). The appropriate setting depends on a number of factors, including:

1. The equipment connected to the audio input.

2. How that equipment is configured.

3. Overall noise level of the scene whose audio being monitored. For example, if the camera's audio input is connected to an external microphone that is monitoring a relatively quiet scene, it might be appropriate to lower the Detection Level. On the other hand, if the microphone is monitoring a noisy scene, it might be appropriate to increase the Detection Level.

ii. Specify the Time interval in seconds (0-7200), the minimum amount of time between each audio detected event, in seconds. The default is 10.

a. **Manual—**Camera triggers an alarm when a user clicks the manual trigger button on the View Settings page.

a. **Video Analytics (1 / 2)—**Camera triggers an alarm according to the settings for the rule selected for the profile on the <%TARGETTITLE%>.

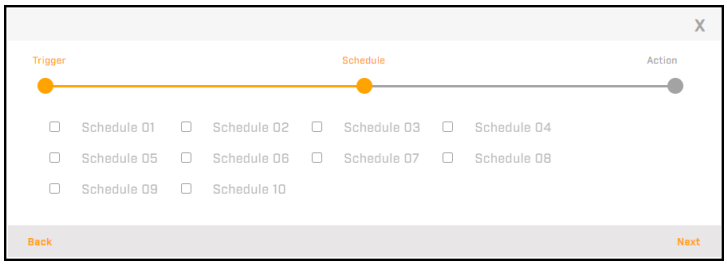
i. Video Analytics 1 / 2 refers to the default preset profile.

ii. If preset profiles have been defined, you can select any of them as the trigger. For example, Preset Profile 1: Video Analytics 1.

3. Click **Next**. If the alarm Schedule screen appears, continue with Specifying an Alarm Schedule. If the alarm Action screen appears, continue with Modifying or Defining Alarm Actions.

5.8.1.5.2 Specifying an Alarm Schedule

On the Schedule screen, users assigned the Admin or Expert role can specify one or more schedules for an alarm. You can configure up to 10 schedules on the Schedule Page.



Click **Next**. The alarm Action screen appears. Continue with Modifying or Defining Alarm Actions.

5.8.1.5.3 Modifying or Defining Alarm Actions

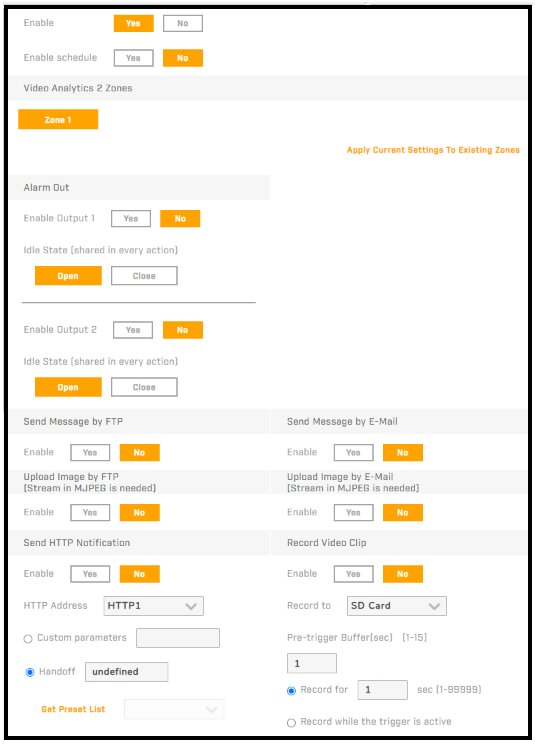
On the Action screen, users assigned the Admin or Expert role can:

- Enable and configure the actions for an alarm.
- Enable the schedule(s) selected on the alarm Schedule screen.

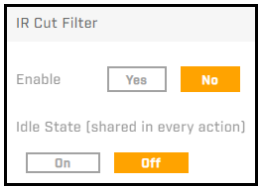
For VA alarm triggers, you can enable and configure actions for each defined detection zone.

Video Analytics 2 Alarm Trigger - 2 Detection Zones Defined

You can individually enable and configure the following alarm actions. Not all actions are available for all alarm triggers.



- **Alarm Out—**Changes the state of an alarm output pin until the camera resets it according to the specified Reset Interval setting on the I/O Page. Specify:
  - **Idle State—**To specify normally open (default), click Open. To specify normally closed, click Close. Changing this setting affects all alarms for which the Alarm Out action is enabled.
- **IR Cut Filter—** Changes the state of the IR cut filter. Not available when the IR state specified on the Illumination Page is Light Sensor (default), Auto, or Smart. Specify:

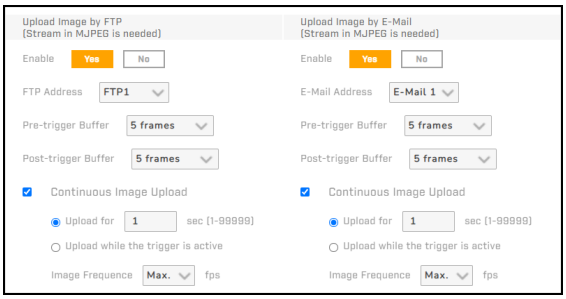


  - **Idle State—**Specify whether the IR cut filter idle state is on or off. Changing this setting affects all alarms for which the IR Cut Filter action is enabled.
- **Send Message by FTP / E-mail—**Sends a message by FTP / email, according to the settings on the FTP Page / Email Page.

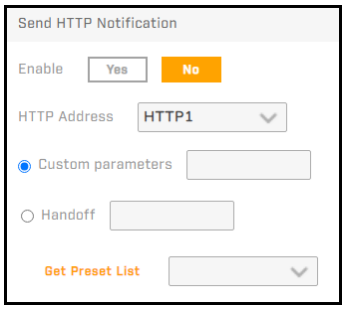
- **Upload Image by FTP / E-mail—**Uploads images to an FTP server or by email, according to the settings on the FTP / Email page. At least one video stream must be encoded in MJPEG. You can configure the video stream settings on the Visible Page.

  Specify:
  - **FTP / E-mail Address—**Select one of the FTP / email addresses defined on the FTP / Email page.
  - **Pre- / Post-trigger Buffer—**Select the number of frames before / after the trigger (1-20 frames). The default is five frames.

- **Continuous Image Upload—**When enabled, select whether the camera uploads images for a specified period of time (1-99,999 seconds), or while the trigger is active. Specify the Image Frequency, or frame rate (1-15, Max fps).



- **Send HTTP Notification—**Sends a notification to an HTTP notification server or hands off the event to a supported PTZ camera.



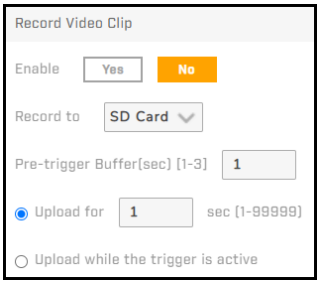
  Specify:

  - **HTTP Address—**Select HTTP server 1 or 2. You can configure the HTTP notification servers on the HTTP Page.
  - **Custom parameters—**Specify parameters the camera adds to the HTTP notification server address. For example, if you have configured an HTTP notification server address as *http://192.168.0.100/admin.php* and you specify the custom parameters as *action=1&group=2*, when the alarm is triggered, the camera sends: *http://192.168.0.100/ admin.php/action=1&group=2*.

    Select:

    - **Custom parameters—**Specify parameters the camera adds to the HTTP notification server address. For example, if you have configured an HTTP notification server address as *http://192.168.0.100/admin.php* and you specify the custom parameters as *action=1&group=2*, when the alarm is triggered, the camera sends: *http://192.168.0.100/ admin.php/action=1&group=2*.
    - **Handoff—**Hands off the event to a supported PTZ camera. To retrieve the list of presets from the PTZ camera, click **Get Preset List**. Then, select the preset to which the PTZ camera moves when this camera hands off the event.

- **Record Video Clip—**Records a video clip to a local microSD or to a NAS, according to the settings on the SD Card or Recording page. Make sure that a microSD card is properly installed, formatted, and active; or that the NAS is properly configured. Specify:



  - **Pre- / Post-trigger Buffer—**Number of seconds before / after the trigger (1-3 seconds). The default is one second.
  - Whether the camera records images for a specified period of time (1-99,999 seconds), or while the trigger is active.

File Name Settings

File Name—Specify the generic name for image files the camera stores or uploads. *image.jpg* is the default.

Select one of the following suffixes the camera adds to the file names to identify individual images:

- **Add date / time suffix (default)**

  File name format: imageYYMMDD_HHNNSS_XX.jpg

  Y: year, M: month, D: day

  H: hour, N: minutes, S: seconds

  XX: sequence number

- **Add sequence number suffix (no maximum value)**

  File name format: imageXX.jpg

  XX: sequence number

- **Add sequence number suffix up to <specify maximum sequence number> and then start over**

  The file names end at the specified maximum number. For example, if image.jpg is the specified File Name and 10 is the specified maximum sequence number, file names start at *image00.jpg*, end at *image10.jpg*, and then start over again.

  File name format: imageXX.jpg

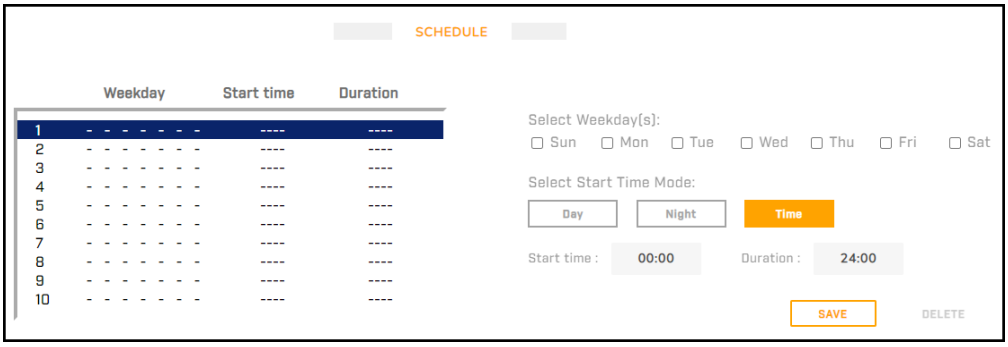
  XX: sequence number

- **Overwrite—**New images replace old images. The file name is static; the camera does not add any suffixes.

Click **Done**. The alarm appears in the list of alarms.

5.8.1.6 Schedule Page

On the Schedule page, users assigned the Admin or Expert role can define up to 10 schedules that can be assigned to alarms. For example, you can define a schedule that starts when a facility closes for the night or for the weekend and ends when it opens, and then apply that schedule to a motion detection alarm.



Note

The schedules and settings on the Schedule page do not apply to live video recording. Accounts assigned the Admin or Expert role can configure live video recording settings on the Recording Page.

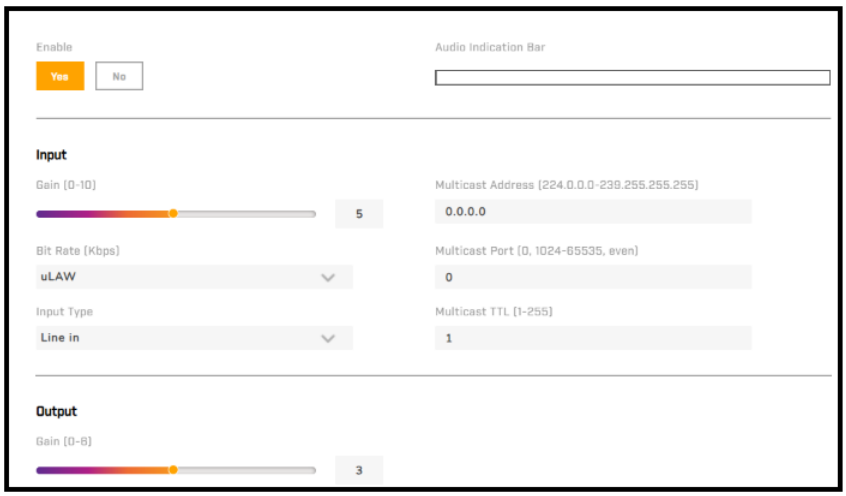
To define or modify a schedule:

1. From the list of schedules on the left, select a schedule.
2. Select one or more days of the week the schedule applies.
3. Select which of the following determines the schedule start time:
   - **Day—**Schedule starts when night turns to day and ends when day turns to night.
   - **Night—**Schedule starts when day turns to night and ends when night turns to day.
   - **Time—**Define the specific Start time for the schedule, in 24-hour format (for example, 09:00), and the Duration (for example, 4:00 hours).
4. Click **Save**. The schedule settings appear in the list of schedules and the **Delete** button becomes available for the schedule.
5. To delete a schedule, select the schedule and click **Delete**. The schedule's settings are cleared.

5.8.1.7 Audio Page

On the Audio page, users assigned the Admin or Expert role can enable and configure the camera's audio features.

When audio is enabled on this page and the Audio alarm trigger has been enabled on the Alarm Page, the audio input level appears on the Audio Indication Bar.



Alarm with Audio Trigger Enabled

1. Enable the Audio Page.
2. Under **Input**, configure the following:
   a. **Gain (0-10)—**The default is 5.
   b. **Bit Rate (Kbps)—**Select on of the following:

i. 40 kbps (G.726)	i. uLAW* (G.711)	i. PCM (256 Kbps)
ii. 32 kbps (G.726)	ii. ALAW* (G.711)	ii. PCM (384 Kbps)
iii. 24 kbps (G.726)	iii. AAC	iii. PCM (768 Kbps)
iv. 16 kbps (G.726)	iv. PCM (128 Kbps)	

*The bit rate for uLAW and ALAW is 64 kbps, but using different compression formats. A higher bit rate can provide higher audio quality, but requires more bandwidth. uLAW is the default.

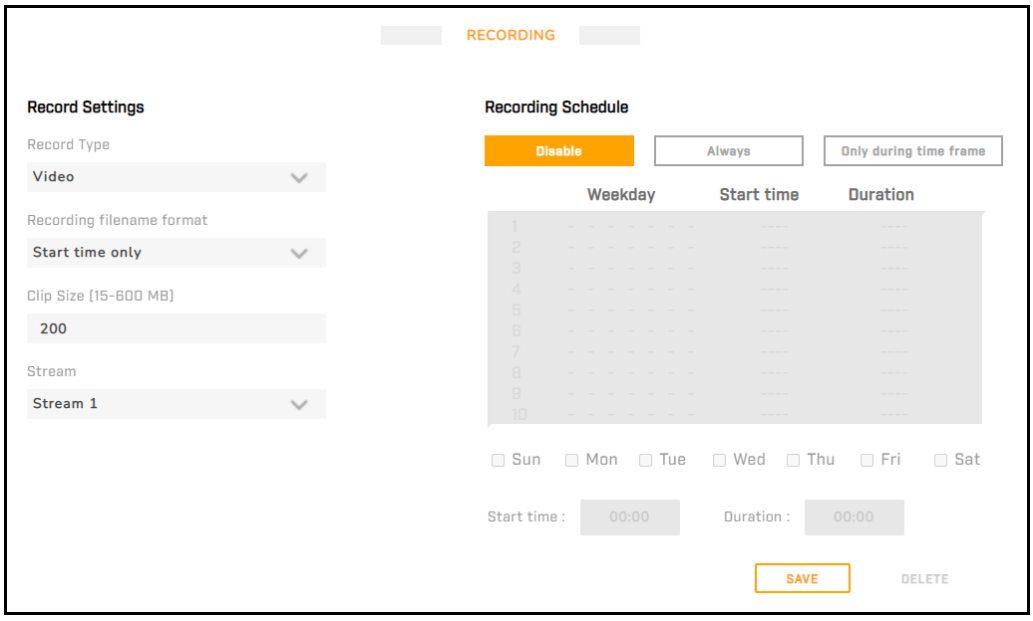
Note

Latitude / UVMS does not support G.726.

3. **Input Type—**Line in.
4. Enter **Multicast Address (224.0.0.0-239.255.255.255)—**A valid multicast address in the specified range.
5. Enter **Multicast Port (0, 1024-65535, even)—**The port the camera uses for multicast audio streaming.
6. Enter **Multicast TTL (1-255)—**Time to live, the maximum number of network hops before routers discard the camera's data packets.
   a. Each time one router forwards a datagram to another router, it subtracts 1 (one) from the packet's TTL.
   b. If the TTL reaches zero (0), a router discards the packet.
   c. Teledyne FLIR recommends setting TTL at 64.
7. Under **Output,** enter **Gain (0-6)—**The default is 3.

5.8.1.8 Recording Page

On the Recording page, users assigned the Admin or Expert role can configure the camera's audio and video recording settings.



Record Settings

- **Record Type—**Select Audio and Video or Video (default).
- **Recording Filename Format—**Select Start time only (default) or Start time + end time.
- **Clip Size (15-600 MB)—**Maximum clip file size. The default is 200 MB.
- **Stream—**Specify the video stream the camera records. Stream 1 is the default.

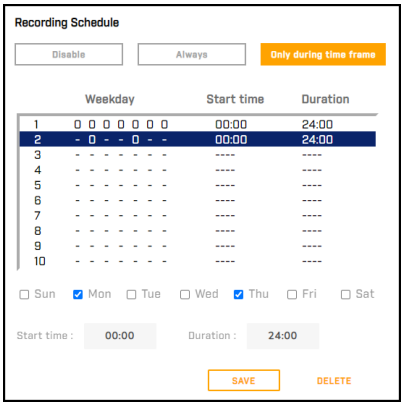
Recording Schedule

By default, recording is disabled. To permanently enable recording, click **Always**. You can configure up to 10 schedules; that is, times during the week recording is enabled.

To define or modify a recording schedule:

1. Click **Only during time frame**.
2. From the list of schedule numbers on the left, select a number.
3. Select one or more days of the week the schedule applies.
4. Define the Start time, in 24-hour format (for example, 00:00 = midnight).
5. Define the Duration (for example, 24:00 hours).
6. Click **Save**. The schedule settings appear and the **Delete** button becomes available for the schedule.

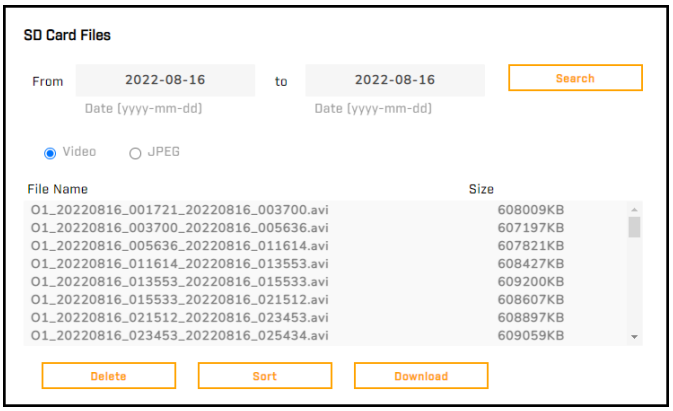
The example at right shows a recording schedule for all day Monday and Thursday.



Schedule for recording all day Monday and Thursday

SD Card Files

A list of the files recorded on the card, if any exist.



By default, files recorded today appear in the list (if any exist). To see other files, specify start and end dates using the format yyyy-mm-dd, and then click **Search**.

Uppercase letters at the beginning of the file names indicate the recording trigger:

- R—regular (always or schedule)
- N—network failure
- M—motion (M0 indicates the first motion trigger)
- A—alarm (A0 indicates the first alarm input trigger)
- T—tampering
- O—manual SD card video recording (see View Settings Home Page)

You can:

- Filter the list to show video clips (default) or snapshots (JPEG).
- Delete one or more files.
- Sort the list by file name, trigger type, or date.
- Download up to 50 files / up to 300 MB, as a ZIP file.

To select more than one file, use the CTRL and SHIFT keys.

5.8.1.9 Email Page

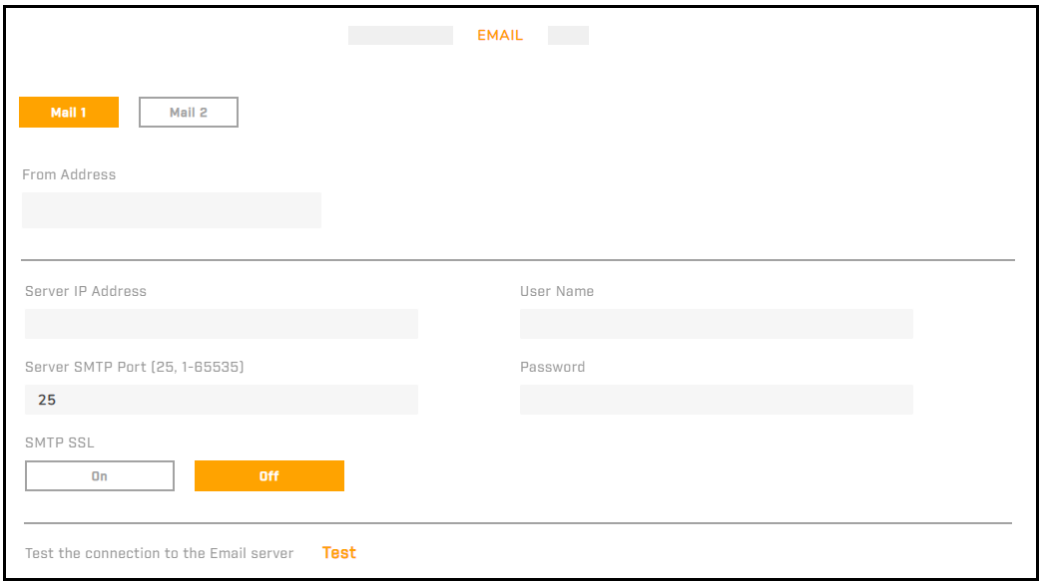
On the Email page, users assigned the Admin or Expert role can configure the settings of two servers the camera can use for sending alarm notification messages or uploading images by email.

Email servers use Simple Mail Transfer Protocol (SMTP) to send and receive email. If you do not know how to configure these settings, contact your email service provider.

Select Mail 1 (primary server) or Mail 2 and then configure:

- **From Address—**Email address that appears as the sender on notification emails the camera sends.
- **Server IP Address—**IP address of the server.
- **Server SMTP Port (25, 1-65535)—**Port the server uses for SMTP communication. The default is 25.
- **User Name—**User name of the account on the server.

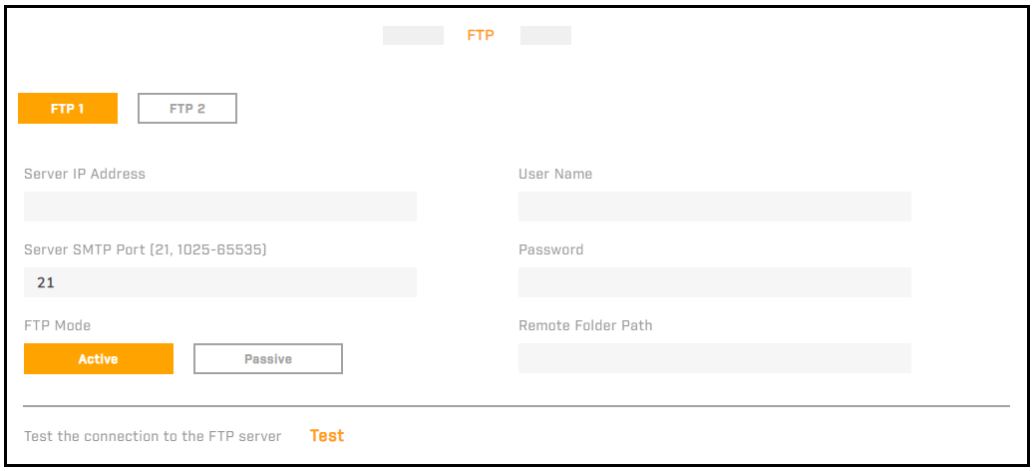
- **Password—**Password for the account on the server.
- **SMTP SSL—**To enable SSL (Secure Socket Layers) for communication with the selected SMTP server, click **On**.



To test the connection with the selected SMTP server using the specified values, click **Test**.

5.8.1.10 FTP Page

On the FTP page, users assigned the Admin or Expert role can configure the settings of two File Transfer Protocol servers to which the camera can upload images or send alarm notifications.



Select FTP 1 or FTP 2 and then configure:

- **Server IP Address—**IP address of the FTP server.
- **Server FTP Port (21, 1025-65535)—**Port the server uses for FTP communication. The default is 21.
- **User Name—**User name of the account on the FTP server.
- **Password—**Password for the account on the FTP server.
- **FTP Mode—**Click **Active** (default) or **Passive**.

In passive mode, the client - in this case, the camera - initiates the connections both to and from the FTP server, which addresses the issue of the client-side firewall blocking incoming data from the server.

To support passive mode on the server side, the following communication channels must be open:

- FTP server port 21 from anywhere (client initiates connection)
- FTP server port 21 to ports > 1023 (server responds to client's control port)
- FTP server ports > 1023 from anywhere (client initiates data connection to random port specified by server)
- FTP server ports > 1023 to remote ports > 1023 (server sends ACKs and data to client's data port)

- **Remote Folder Path—**Path of the file folder on the FTP server to which the camera uploads images.

To test the connection with the selected FTP server using the specified values, click **Test**.

5.8.1.11 Cyber Page

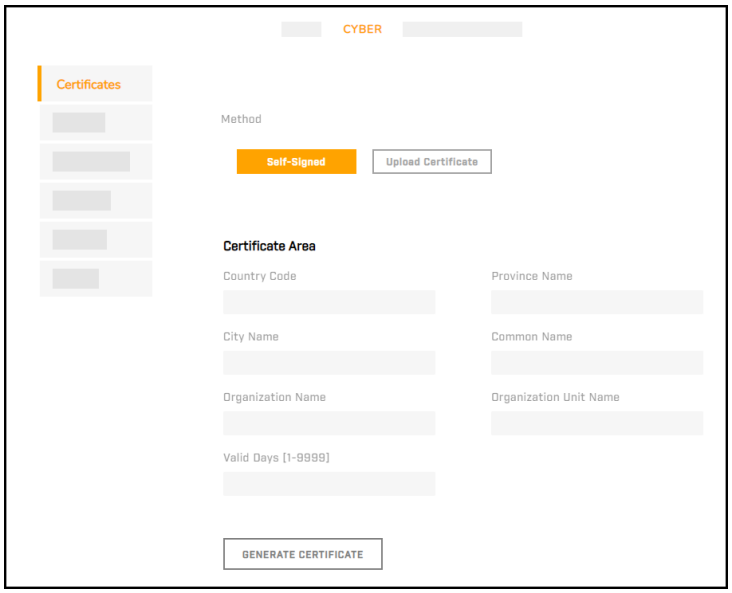
On the Cyber page, users assigned the Admin or Expert role can enable and configure the following cybersecurity settings:

- Certificates
- 802.1X
- TLS / HTTPS
- Services
- IP Filter
- SNMP

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

5.8.1.11.1 Certificates

Before you can enable TLS/HTTPS or 802.1X, you need to install a certificate on the camera.



In the Certificates section, you can:

- generate a self-signed certificate
- upload a self-signed certificate
- upload a certificate issued by a certificate authority (CA)

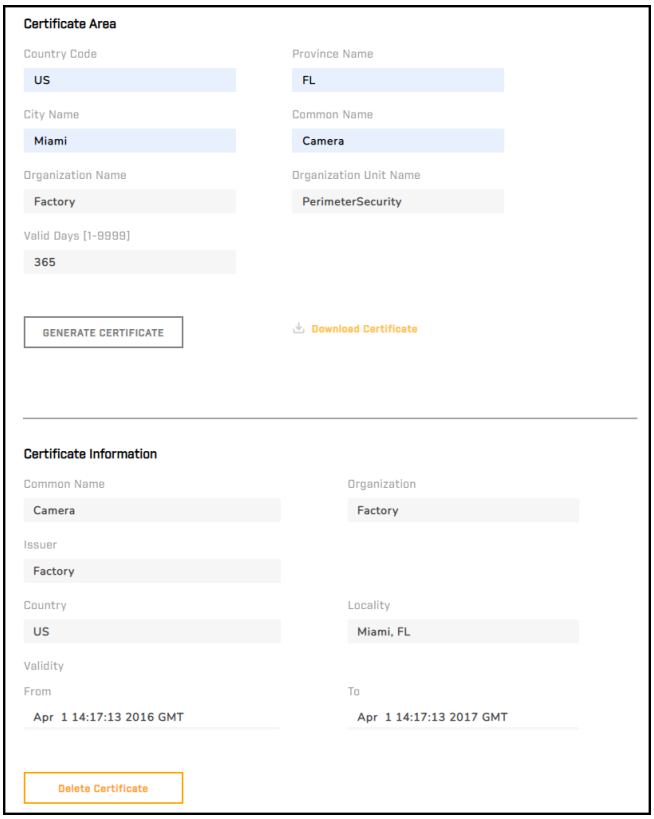
Note

CA-issued certificates are publicly recognized and provide a higher level of security than self-signed certificates. For example, browsers do not trust self-signed certificates.

To generate a self-signed certificate:

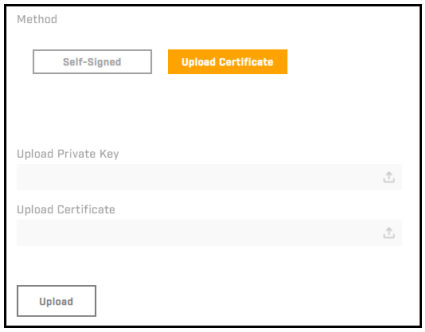
1. On the Date & Time Page, make sure the camera's date and time is the current date and time. Synchronize the camera's time with an NTP server or copy the PC's time.
2. Under Method, select **Self-Signed**.
3. Enter information such as country code, city name, common name, and organization name. For the common name, you can specify the name of the person or other entity the certificate identifies; for example, it can identify the website.
4. Click **Create Certificate**.

After the camera generates the certificate, the certificate information appears.



You can now enable TLS/HTTPS and 802.1X; download the certificate as a PEM file; or delete the certificate.

To upload a certificate:



1. Under Method, select **Upload Certificate**.
2. Under **Upload Private Key**, and then under **Upload Certificate**:
   a. Click .
   b. Browse for and select the appropriate file.
   c. Click **Upload**. The camera uploads and installs the key and the certificate.

5.8.1.11.2 802.1X

In the 802.1X section, users assigned the Admin or Expert role can enable and configure the camera to access a network protected by 802.1X / EAPOL (Extensible Authentication Protocol over LAN). To obtain certificates, user IDs, passwords, and other information, contact the network administrator.

Enable 802.1X; select the Protocol (EAP-MD5, EAP-TLS, EAP-TTLS, or EAP-PEAP); and then specify the information the protocol requires. You can use the following special characters: _ . / \ ~ ! @ # $ % ^ & + - * .

802.1X Enabled - EAP-MD5 Selected

EAP-MD5

- **User Name**
- **Password**

EAP-TLS

- **User Name—**User name associated with the certificate, up to 16 characters.
- **Private Key Password—**Password for the private key, up to 16 characters.
- **CA Certificate / Client Certificate—**Click **Upload file**, and then browse for and select the certificate file.
- **Private Key—**Click **Upload file**, and then browse for and select the key file.

EAP-TTLS

- **Inner Auth—**Select the inner tunnel authentication method (CHAP, EAP-MSCHAPV2, EAP-MD5, MSCHAP, MSCHAPV2, or PAP).
- **User Name—**User name associated with the certificate, up to 16 characters.
- **Password—**Password for the user, up to 16 characters.
- **Anonymous ID—**Anonymous ID for the user, up to 16 characters.
- **CA Certificate—**Click **Upload file**, and then browse for and select the CA-issued certificate file.

EAP-PEAP

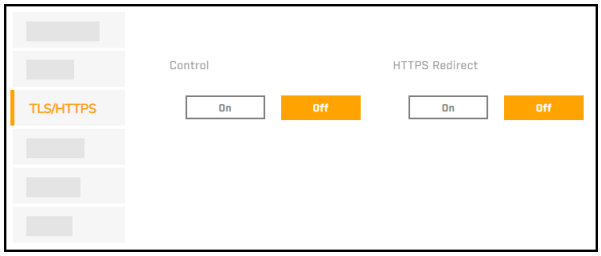
- **User Name—**User name associated with the certificate, up to 16 characters.
- **Password—**Password for the user, up to 16 characters.
- **CA Certificate—**Click **Upload file**, and then browse for and select the CA-issued certificate file.

Fields with red borders are required.

To save any changes to the IEEE 802.1X settings and to upload files, click **Save**.

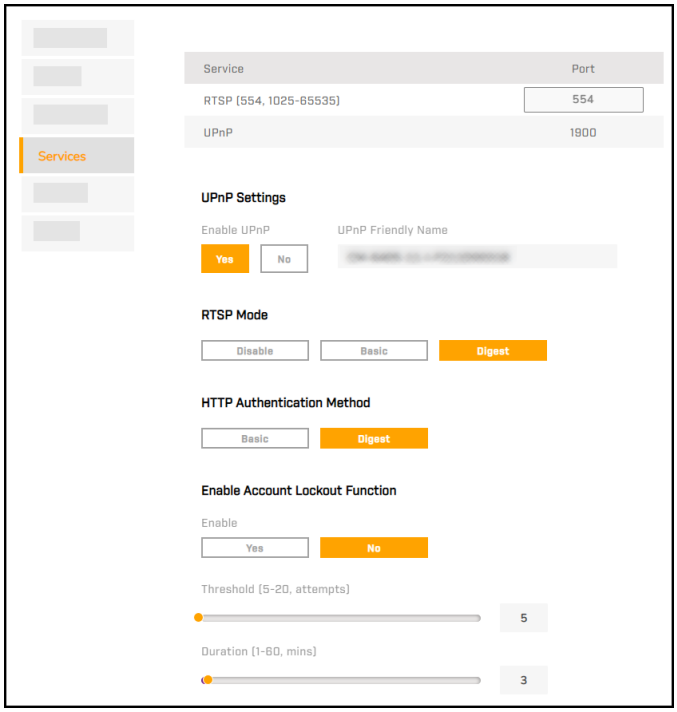
5.8.1.11.3 TLS / HTTPS

In the TLS / HTTPS section, users assigned the Admin or Expert role can enable camera control using Transport Layer Security (TLS) / secure HTTP (HTTPS), which secures communication between the camera and web browser.



Enabling control requires generating a self-signed certificate or uploading a CA-signed certificate in the Certificates section. When control is enabled, you can enable HTTPS redirect.

5.8.1.11.4 Services

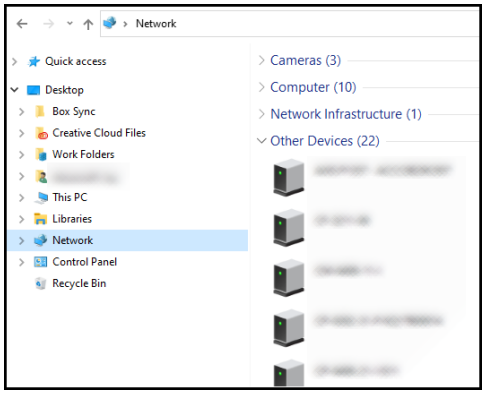


In the Services section, users assigned the Admin or Expert role can:

- Specify the RTSP port (554, 1025-65535). The default is 554.
- **Enable UPnP—**By default, UPnP is enabled. Windows computers and other compliant devices can discover the camera on the LAN. In Windows, the connected camera appears as a Network device.

> **Note**
>
> To use UPnP on a computer, make sure UPnP is installed on the computer. For information about how to install UPnP components on a Windows computer, see Installing UPnP Components.

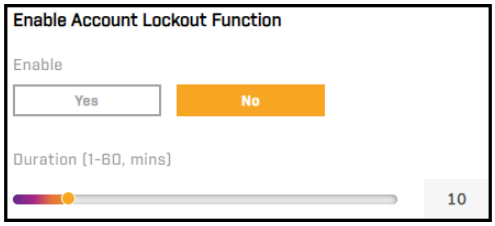
- **UPnP Friendly Name—**Name that identifies the camera on UPnP devices.



Cameras with UPnP Enabled - Windows File Explorer

- Enable RTSP basic or digest authentication for accessing the camera's video streams:
  - **Disable—**Accessing the camera's video streams does not require authentication. By default, RTSP authentication is disabled.
  - **Basic—**Uses unencrypted base64 encoding. Teledyne FLIR recommends enabling basic authentication only when TLS / HTTPS is enabled.
  - **Digest—**Encrypts the credentials when transmitted.

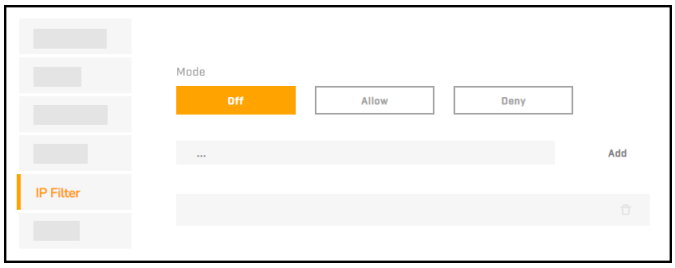
  When RTSP authentication is enabled, accessing the camera's video streams requires providing the name and password for a camera user. All camera users have access to the camera's video streams.
- Configure the HTTP Authentication Method for accessing the camera's web page. Select Disable, Basic (default), or Digest.
- Enable and configure account lockout. When enabled, if a user unsuccessfully attempts to log in exceeding the specified duration, the account is locked. By default, account lockout is disabled.



  - **Duration (1-60, mins)—**The default is 20 minutes.

5.8.1.11.5 IP Filter

In the IP Filter section, users assigned the Admin or Expert role can enable and configure the camera's IP filter.



Select the IP filter mode:

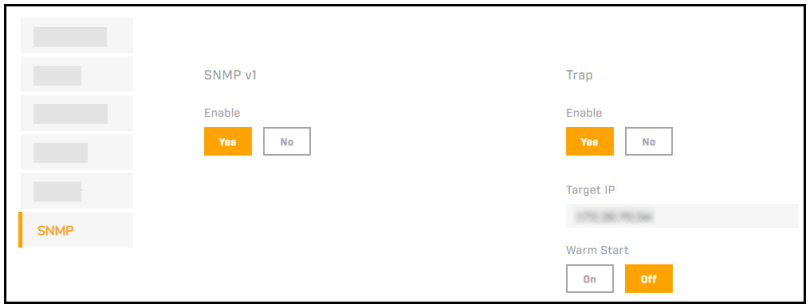
- **Allow—**Allows access to the camera only from the specified IP addresses.
- **Deny—**Denies access to the camera from the specified IP addresses.

To add an IP address to the list, in the text field under the Mode selection buttons, specify an IPv4 address and then click **Add**. You can specify up to 256 IP addresses.

To remove an IP address from the list, click the corresponding trash icon .

5.8.1.11.6 SNMP

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



SNMP v1—Enable SNMP v1.

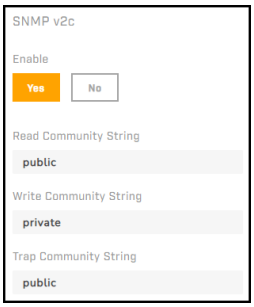
Trap

The camera uses traps to send messages to the network management system for important events or status changes.

After enabling traps, specify:

- **Target IP—**IP address of the network management system server.
- **Warm Start—**Enables traps that indicate when the camera is rebooting, but configuration data or MIB variable values have not changed.

SNMP v2



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*.
- **Trap Community String—**Name of community camera uses when sending traps to the network management system. The default value is *public*.

Important

For cybersecurity reasons, change the default community strings.

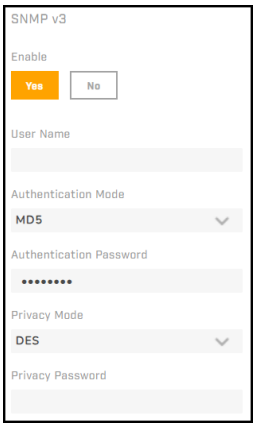
SNMP v3

SNMP v3 provides security features including:

- **Confidentiality—**Packet encryption prevents snooping by unauthorized sources.

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

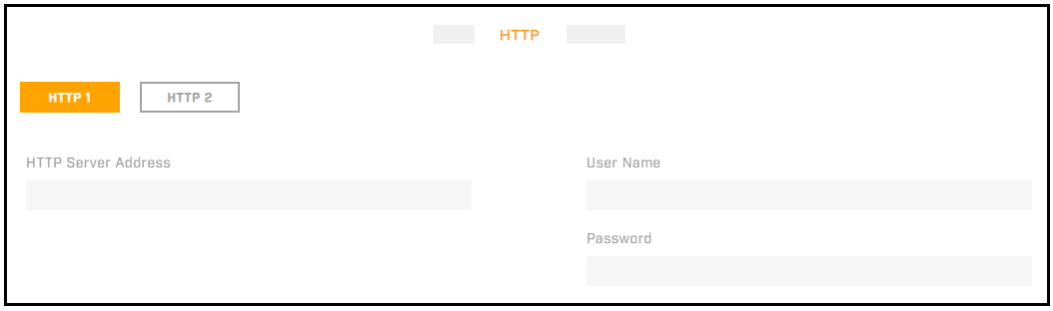
After enabling SNMP v3, specify:



- **User Name—**Name of user on network management system using SNMP v3.
- **Authentication Mode—**Select MD5 (default) or SHA.
- **Authentication Password—**Password for authentication on network management system.
- **Privacy Mode—**Select DES (default) or AES.
- **Privacy Password—**Password for privacy on network management system.

5.8.1.12 HTTP Page

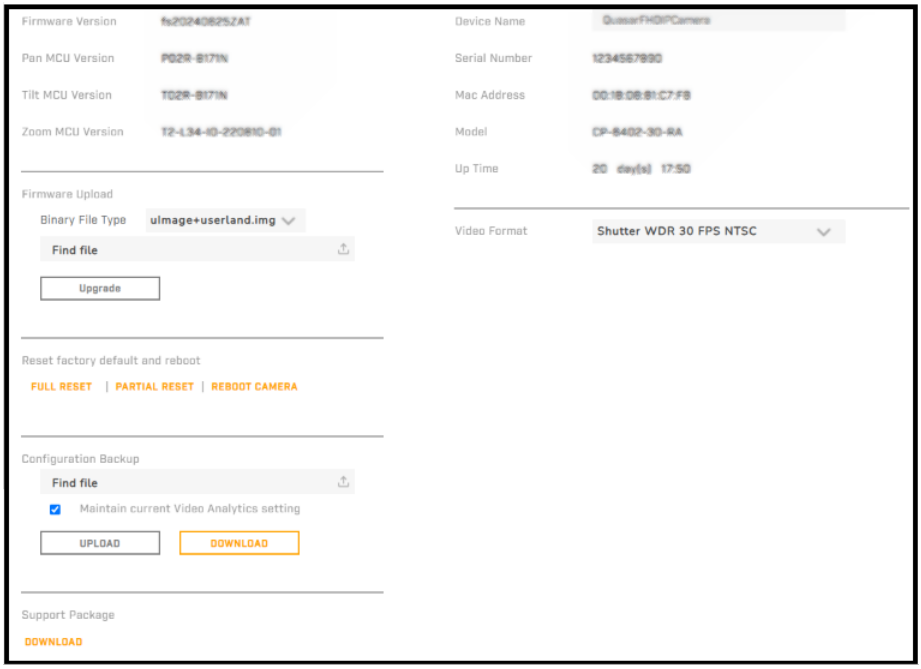
On the HTTP page, users assigned the Admin or Expert role can configure the settings of two HTTP servers to which the camera can send alarm notifications.



Select HTTP 1 or HTTP 2 and then configure:

- **HTTP Server Address—**IP address of the HTTP server.
- **User Name—**User name of the account on the HTTP server.
- **Password—**Password for the account on the HTTP server.

5.8.1.13 Firmware & Info Page

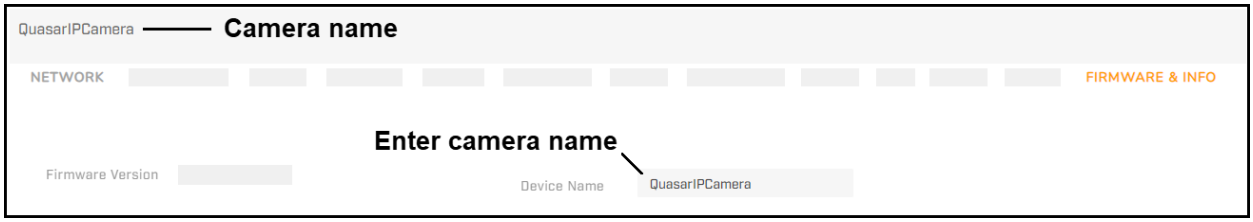


On the Firmware & Info page, users assigned the Admin or Expert role can:

- 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
- Download or upload a configuration backup file
- Download system information
- Configure the camera's video format, including enabling a Shutter WDR format

Device Name

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



Firmware Upload

To upgrade the camera's firmware:

1. Under Firmware Upload, click **Find file**.

2. Select the Binary File Type. For example, **uImage+userland.img**.
3. On your computer or network, browse to and select the firmware file.

Notes

- Do not change the firmware file name. If you change the file name, the system fails to find the file.
- Firmware can also be upgraded via DNA version 2.3.0.31 or higher.

Caution:
Do not unplug power or change the screen while upgrading software.

4. Click **Upgrade**. The system verifies that the upgrade file exists and begins to upload the file. An upgrade status bar appears. When the camera completes the upgrade, the View Settings page appears.

Reset factory default and reboot

Full Reset—Reboots the camera and restores factory default settings, including its networking settings; for example, the camera's IP addressing mode and its IP address. To discover the camera again and reconfigure its network configuration, use the DNA tool. For more information, see Configure for Networking.

Partial Reset—Reboots the camera and restores factory default settings, except its current networking and video format settings.

Reboot Camera—Reboots the camera without changing its current settings.

Tip

You can also reboot and reset the camera to its factory default settings by pressing the camera's physical Default button for at least 20 seconds; for example, if you are unable to access the camera via its web page or other communication method. The Default / Reset button is located on .

Configuration Backup

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

To upload a configuration backup file:

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

Caution

Make sure to upload a configuration backup file that was downloaded from another camera that is the exact same model.

3. To retain the camera's current VA settings, make sure **Maintain current Video Analytics setting** is selected.

   To overwrite the camera's current VA settings with the VA settings in the configuration backup file, make sure **Maintain current Video Analytics setting** is not selected.

4. Click **Upload**.

   The camera uploads the backup file and reboots.

To download the camera's saved settings:

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

config_file.bin is the backup file name. Do not change the file name.

Support Package

To download the camera's log file, click **Download**. Teledyne FLIR Support can use this file to help resolve issues.

Video Format

Select Shutter WDR 60 FPS NTSC (default), Shutter WDR 50 FPS PAL, Linear 60 FPS NTSC, or Linear 50 FPS PAL. When a Shutter WDR format is selected:

- The camera analyzes the exposure and level of detail in two frames taken at different exposure settings and shutter speeds, uses an algorithm to determine the optimal combination of regions within the scene, and generates a single, composite frame with wide dynamic range.
- The maximum frame rate of the camera's video output is 30 / 25 (NTSC / PAL).

When a Shutter WDR is not selected, the camera operates in linear mode; that is, the camera streams every frame it takes. In scenes with high contrast or changing light issues, bright areas can be overexposed and dark areas can be underexposed.

Shutter WDR Format Selected

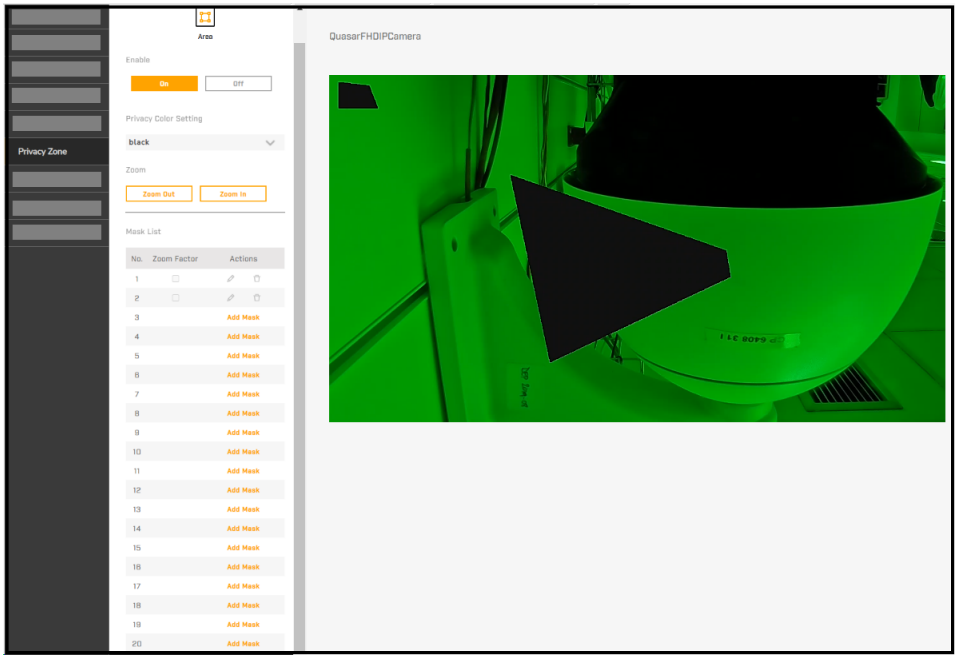
Shutter WDR Format Not Selected

Tips

- For most lighting conditions, to achieve video with a consistent exposure level regardless of changing contrast or lighting conditions, Teledyne FLIR recommends selecting a Shutter WDR format.
- When the frequency of a light source around the camera (including reflected light) is closely synced with the Shutter WDR operation, a pixelization effect can appear. Under these conditions, Teledyne FLIR recommends selecting a linear format; that is, 60 FPS NTSC or 50 FPS PAL.
- For more information about video resolutions and frame rates supported in linear and shutter modes, see Video Page.

After changing the Video Format, the camera reboots. If the camera is attached to a VMS, after it reboots, you need to re-attach the camera to the VMS.

5.9 Privacy Zone Page

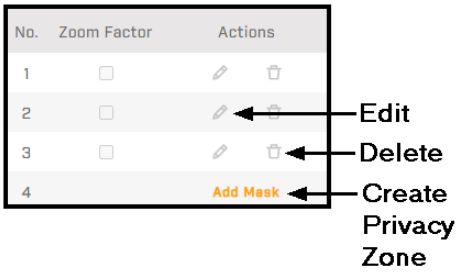


Privacy Zone Page - Zone 1 and 2 Enabled

On the Privacy Zone page, users assigned the Admin or Expert role can enable and configure up to twenty privacy zones. Privacy zones conceal sensitive portions of the scene to avoid intrusive monitoring.

To Configure Privacy Zones:

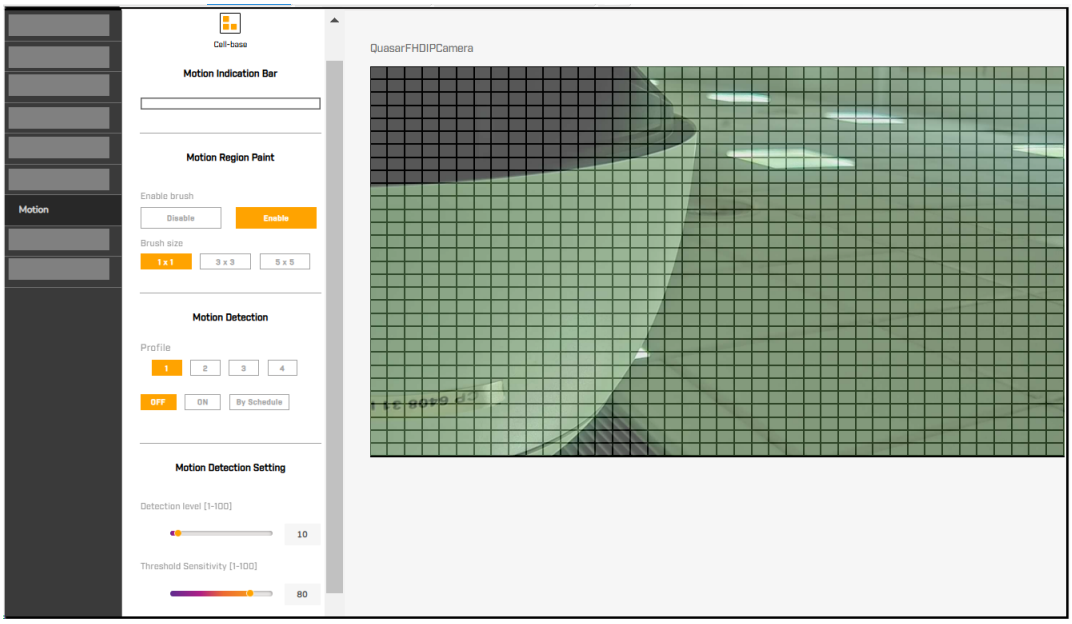
1. **Enable**—Click On to create the Privacy zones.
2. Specify **Privacy Color Setting—**the color that fills all of the zones. Choices include:
   - black (default)
   - white
   - yellow
   - red
   - green
   - blue
   - cyan
   - magenta
3. Zoom in or out incrementally to your chosen view.
4. Click Add Mask to create a new Privacy Zone.
5. The borders appear in red in the top left of the live video.
6. Change the size of the zone by clicking a side or corner and dragging.
7. Move the zone by clicking inside the zone and dragging.
8. Edit the zone by clicking the edit icon.



9. Delete the zone by clicking the delete icon.
10. Click the Zoom Factor box if you want to zoom in or out without the size of the privacy zone changing.
11. Click Set to save changes.

5.10 Motion Page

On the Motion page, users assigned the Admin or Expert role can enable and configure up to four motion detection profiles. On the Alarm page, Administrators can select one of the four profiles as a trigger. For more information, see Defining an Alarm Trigger.



Motion Page - Brush and Profile 1 Enabled

By default, motion detection is disabled. When enabled, motion in the detected region that reaches or exceeds the specified detection and threshold sensitivity levels triggers alarms. If the camera is connected to FLIR UVMS, Teledyne FLIR recommends using AdminCenter to configure motion detection.

Detected motion appears in the 10-step Motion Indication Bar. Green indicates detected motion below the specified detection and threshold sensitivity levels; alarm not triggered. Red indicates motion exceeding those levels; triggers alarm.

Motion Region Paint

To draw the motion detection region for the profile selected:

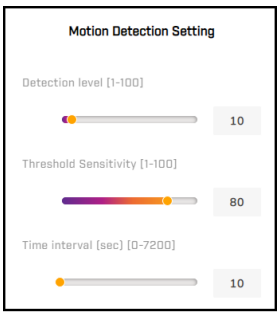
1. Enable the brush.
2. Select the brush size to draw the region, in cells (1 x 1, 3 x 3, or 5 x 5).
3. To draw or erase cells, click and drag or click and release on the cell grid overlay.
   a. Each mouse click on the cell grid toggles between drawing and erasing.

To Configure Motion Detection:

1. Select the profile and then specify:
   a. **Off—**The motion alarm for the selected profile is permanently disabled (default).
   b. **On—**The motion alarm for the selected profile is permanently enabled.
   c. **By Schedule—**The motion alarm for the selection profile is enabled and disabled according to the selected schedule(s). Select up to 10 schedules. You can configure schedules on the Schedule Page.

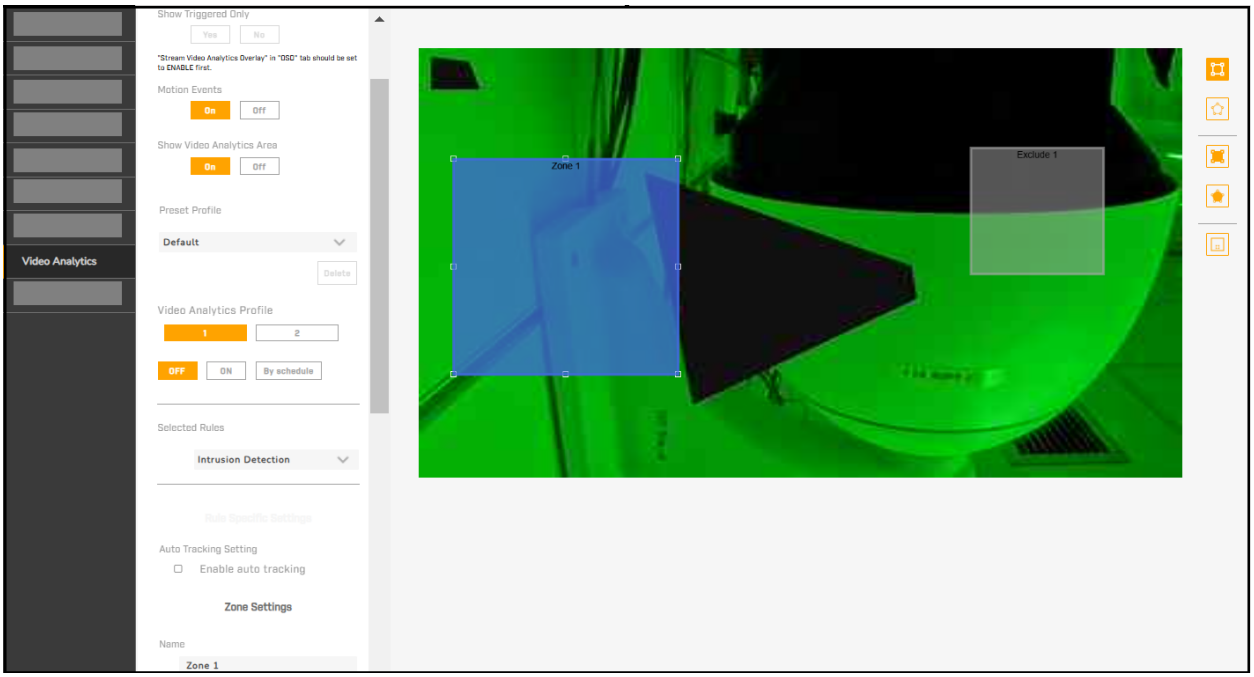
   You can also enable and disable motion alarms, or specify motion alarm schedules, on the Alarm Page.

2. Specify **Detection level (1-100)—**the difference between two sampling pixels the camera accepts.
   a. Lowering the detection level means the camera detects smaller motion, but can increase false alarms.
   b. Increasing it means the camera detects larger motion, but can increase missed detections.
   c. The default is 10.



3. Specify **Threshold Sensitivity (1-100)—**the percentage of sampling pixels the camera detects differently to determine whether motion has been detected.
   a. Increasing the value increases the sensitivity, but can also increase false alarms.
   b. Decreasing the value decreases the sensitivity, but can also increase missed detections.
   c. The default is 80; that is, when 20% or more sampling pixels are detected differently, the camera detects motion.
4. Specify **Time interval (in seconds) (0-7200)—**Specify the minimum amount of time, in seconds, between motion detection alarms. The default is 10.

5.11 Video Analytics Page



Video Analytics Page

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

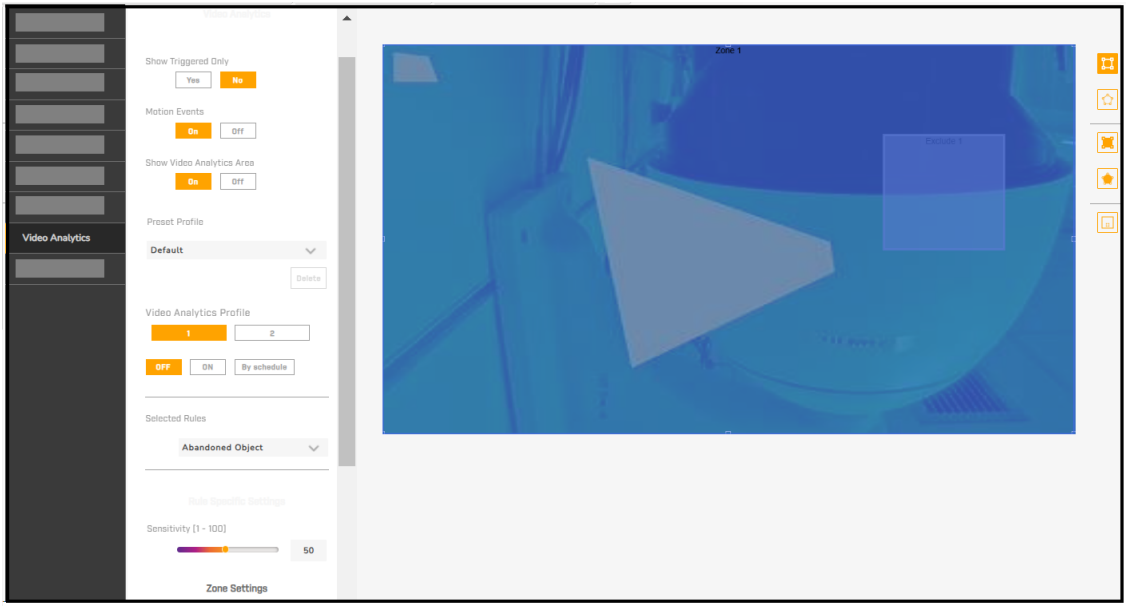
- Enable, schedule, and configure two video analytics (VA) profiles for specific presets or as the default profile; that is, two VA rules can be simultaneously active. When Defining an Alarm Trigger, you can select a VA profile. To enable one or more of the schedules configured on the Schedule Page,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

  During a preset tour, when the camera is stationary on a preset and a VA profile has been defined for that preset, that preset profile is active. If a VA profile has not been defined for that preset, the default profile is active.

  Regardless of whether VA is enabled on this page, VA is temporarily disabled when the camera is moving; that is, when an operator is manually panning, tilting, or zooming the camera, or when the camera is running a cruise, an auto pan path, or moving from one preset to another during a tour.

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

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

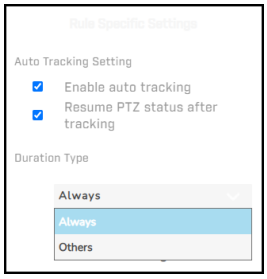


Video Analytics Page - Default Preset Profile - VA Profile 1 - Abandoned Object

Rule	Purpose	Examples
Abandoned Object	Detect objects placed in the scene that remain stationary for longer than a specified amount of time	Securing public areas, such as transportation hubs, against suspicious objects
Intrusion Detection	Detect people or vehicles coming into the scene	Secure a courtyard from trespassing or a no parking area
Camera Sabotage	Detect significant changes in the camera's field of view, unauthorized repositioning, or lens obstruction	Bank robbers use spray paint on the camera lens to obscure their robbery
Tripwire Detection	Detect people or vehicles entering the scene from a particular direction	Airport intrusion detection
Loitering Detection	Detect encroachment and trespassing based on the time spent in the scene	Monitoring an ATM or school grounds
Object Counting	Count the number of objects entering the scene	Counting customers entering a store
Object Removal	Detect objects being removed from the scene	Monitoring shoplifting
Stopped Vehicle	Detect vehicles that remain stationary in the scene for longer than a specified amount of time	Parking enforcement
Face Detection	Target marketing by detecting and identifying people in the scene by gender and approximate age range	Merchandising and campaign evaluation

Show Ruled Area—Enables a VA overlay that includes detection zones and an object counter, if relevant.

Rule Specific Settings > Auto Tracking Setting



Enable auto tracking—The camera automatically tracks objects detected by the selected rule and that are triggering alarms. When enabled (default), you can select:

- **Resume PTZ status after tracking—**After tracking an object, the camera reverts to the automatic mode specified on the PTZ Page. When enabled (default), specify the Duration Type:
  - **Always (default)—**Camera tracks objects until they are no longer triggering alarms. Then, the camera returns to the automatic mode specified on the PTZ Page.
  - **Others—**Camera tracks objects triggering alarms for up to the specified Duration (0-1800 seconds; 20 seconds is the default). Then, it returns to the automatic mode specified on the PTZ Page.

5.11.1 Rule Configuration

Except for Camera Sabotage, configuring a video analytics rule consists of:

- Configuring Detection Zones
- Modifying the Minimum and Maximum Object Sizes

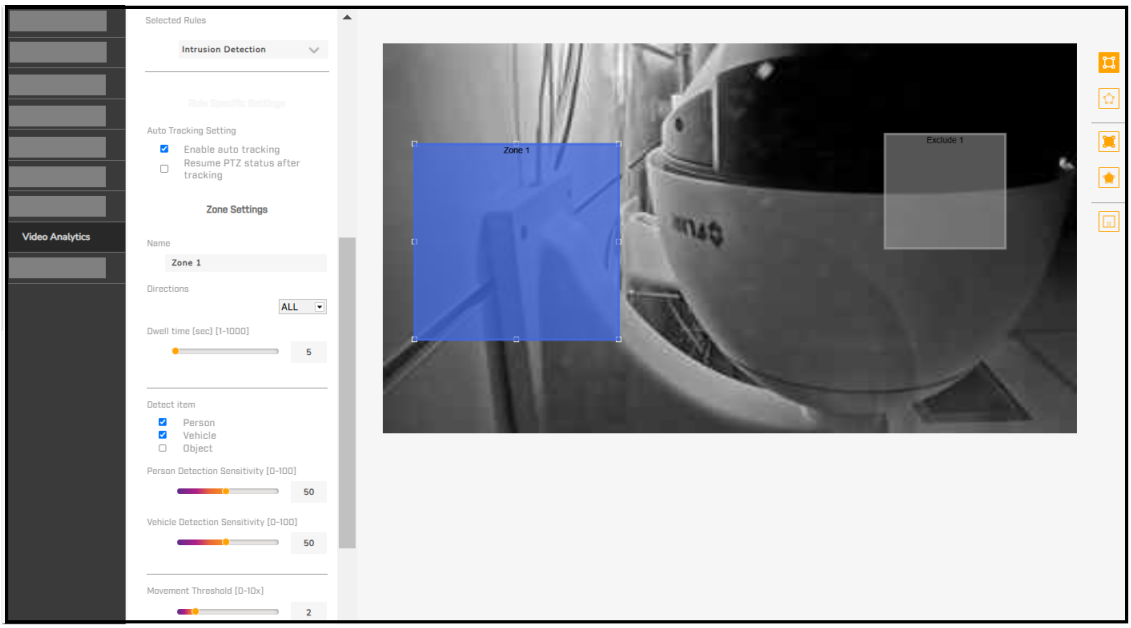
For certain rules, you can configure VA masking zones.

5.11.1.1 Configuring Detection Zones

Accounts assigned the Admin or Expert role can configure up to eight detection zones (square, polygon, or line).

To configure a detection zone:

1. To the right of the video window, click one of the detection zone icons: square  , polygon  , or line  . The rule you are configuring determines the detection zone icons that are available.
2. On the live video, draw one or more detection zones. When the mouse cursor appears as a crosshair, you can begin drawing a detection zone.
   a. When you begin creating a detection zone, the settings available for the zone appear
3. **To define a square zone:**
   a. Click, drag, and release the mouse.



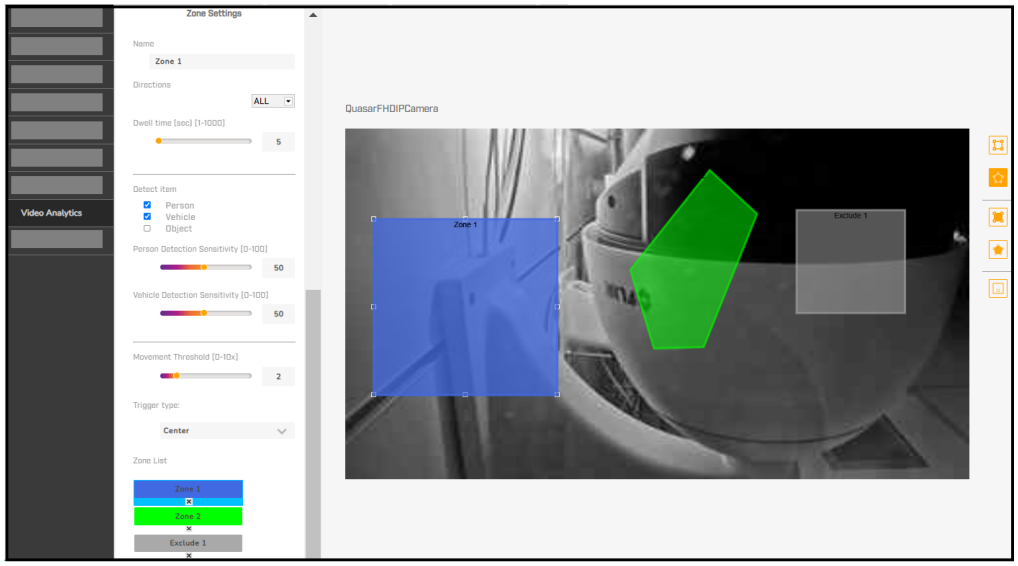
4. **To define a polygon zone:**

   a. Define the first border by clicking, dragging, and releasing the mouse.

   b. Define at least one more point by clicking and releasing the mouse. Do not click and drag.

   c. To close the zone, click the first point.

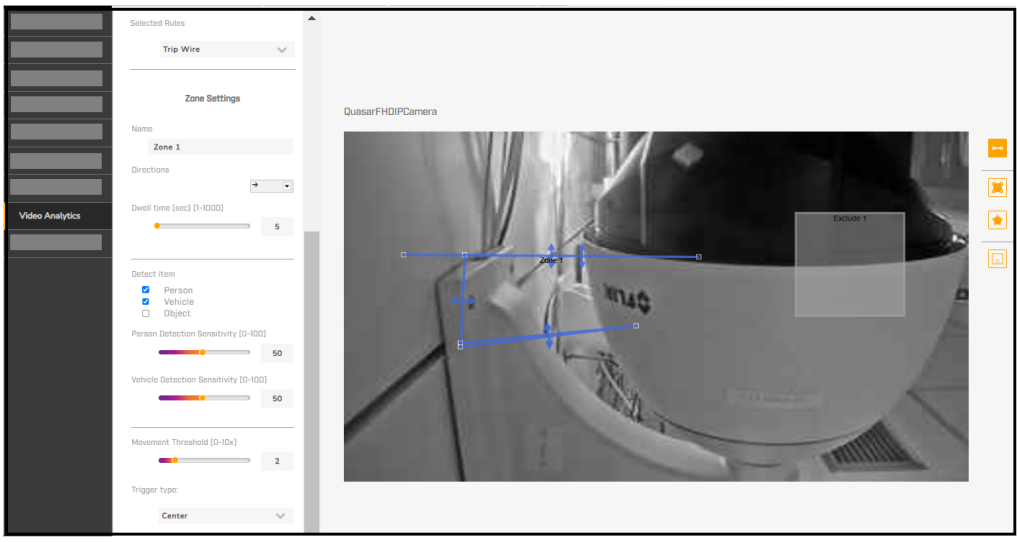
   d. For each polygon zone, you can draw up to five points.



5. **To define a single line:**

   a. Click, drag, and release the mouse.

   b. To add additional points and lines to the zone, continue clicking points. For information about line direction detection, see below.



Multi-Point Line Zone Defined

After you have drawn a detection zone, you can move it or adjust the point locations.

6. Configure the zone settings. The rule you are configuring determines the settings available.

Rule	Settings available
Abandoned Object	Name, Dwell time, Delay before alarm, Sensitivity
Intrusion Detection	Name, Directions, Dwell time, Detect item, Person, Vehicle and Object Sensitivity, Movement Threshold, Trigger type, Auto Tracking Setting
Camera Sabotage	Name, Sensitivity, Dwell time, Delay before alarm
Tripwire Detection	Name, Directions, Dwell time, Detect item, Person, Vehicle and Object Sensitivity, Movement Threshold, Trigger type
Loitering Detection	Name, Dwell time, Delay before alarm, Detect item, Person, Vehicle and Object Sensitivity, Trigger type
Object Counting	Name, Directions, Alarm at, Dwell time, Reset counter on alarm, Detect item, Person, Vehicle and Object Sensitivity, Movement Threshold, Trigger type
Object Removal	Sensitivity, Name, Dwell time, Delay before alarm
Stopped Vehicle	Name, Dwell time, Delay before alarm, Vehicle Detection Sensitivity, Trigger type
Face Detection	Face Detection Item, Name, Dwell time, Face Detection Sensitivity

Tip

For optimum video analytics performance in most conditions, Teledyne FLIR recommends using the default settings for:

- **Person / Vehicle / Object / Face Detection Sensitivity—**Overall probability of detection (0-100). For persons, vehicles, and face detection, the default is 50; for objects, it is 20. Increasing sensitivity can increase false alarms.
- **Movement Threshold—**Specify the amount of movement that triggers an alarm, in the multiple of the minimum object pixel size (0-10x, with 0 being the most sensitive setting.). The default is 2; the camera triggers an alarm when the camera detects an object moving more than 2x the width of the minimum object pixel size. Decreasing the threshold can increase false alarms.
- Minimum and Maximum Object Sizes

Note

The Detect item, Detection Sensitivity, and Movement Threshold settings are not available under the following conditions:

- Camera dewarping + ceiling mount + hemispheric dewarping
- VMS dewarping + ceiling mount

7. **Choose a Name—**Meaningful name for the zone.
8. If you chose Face Detection, decide whether to select **Face Detection Item.**
   a. Select whether the camera's VA subjects are wearing a mask / facial covering.
9. Choose a **Direction,** a motion that triggers an alarm.
   a. By default, except for Tripwire Detection, all directions trigger an alarm (ALL).
10. If you chose Object Counting, choose a number of objects for **Alarm at (objects).**
    a. This is the number of counted objects that triggers an alarm (1-1000). The default is 1.
11. Specify **Dwell time (sec)—**Maximum amount of time, in seconds, the camera triggers an alarm (1-1000),
    a. This can affect auto tracking if enabled.
    b. The default is 5.
    c. Intrusion Detection example: When a detected object meets the Intrusion Detection alarm trigger settings – for example, the Person Detection Sensitivity setting – the camera triggers an alarm for up to one second.
12. Under **Detect item,** choose **People, Vehicles, and/or Objects.**
    a. This triggers an alarm when VA detects the chosen items.
13. Configure **Delay before alarm (sec)—**Amount of time, in seconds, object must remain in a detection zone to trigger an alarm.
    a. For Abandoned Object and Object Removal, the range is 5-1000 seconds and the default is 5.
    b. For Camera Sabotage, the range is 1 - 60 seconds and the default is 5.
    c. For Loitering Detection, the range is 1 - 1800 seconds and the default is 10.

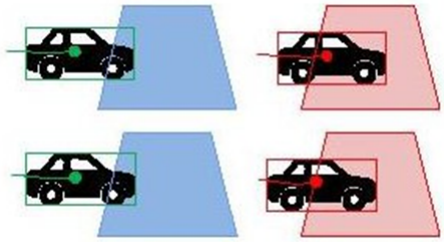
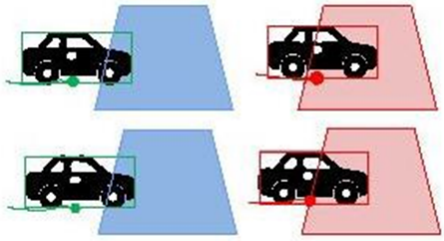
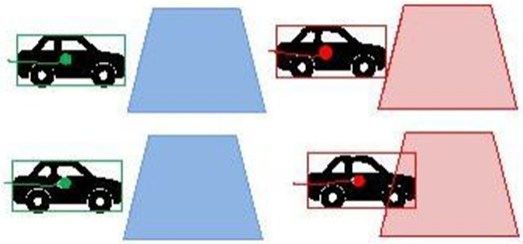
d. For Stopped Vehicle, the range is 20 - 1800 seconds and the default is 30.

e. For Face Detection, the range is 1 - 1000 and the default is 5.

14. Decide whether to choose **Reset counter on alarm.**

a. Alarms reset the object counter to zero (0).

15. Choose **Trigger type,** see below**:**

Setting	Description	Vehicle example
Center	Trigger an alarm when the center point of the detected object box touches or is within the detection zone.	
Bottom center (default)	Trigger an alarm when the bottom-center point of the detected object box touches or is within the detection zone.	
Edge	Trigger an alarm when an edge of the detected object box touches or is within the detection zone.	
Fully inside	Trigger an alarm when the detected object box is fully within the detection zone.	
Fully cover	Trigger an alarm when the detected object box fully covers the detection zone.	

16. Click **Save**.

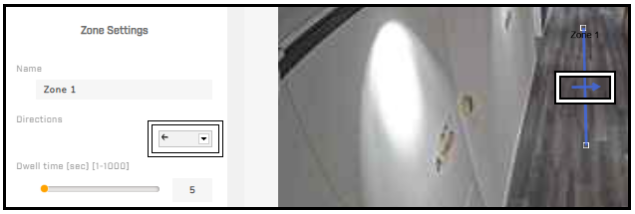
Tripwire Line Direction Detection

To configure Tripwire Direction:

- By default, line detection is bidirectional. However, you can configure it to be unidirectional.

- When configured as unidirectional, the direction selection arrows refer to the direction of movement over the line *as seen from the first line point created*.

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



5.11.1.2 Configuring VA Masking Zones

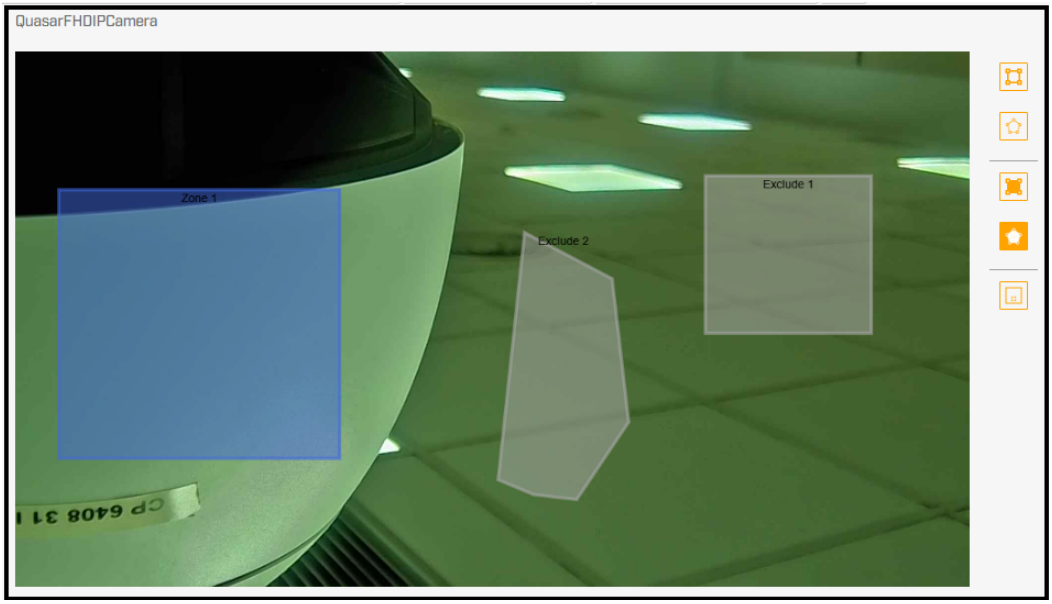
- For certain rules, accounts assigned the Admin or Expert role can configure VA masking zones; that is, portions of the video image in which analytics are disabled and the camera does not generate alarms. However, these are not privacy zones and the zones themselves appear in the video image.
- VA masking zones are used to eliminate alarms from trees or bushes moving in the wind.
- You can also configure privacy zones — that is, zones that do *not* appear in the video image, or are entirely blackened out on the video stream — on the <%TARGETTITLE%>.

To configure a VA masking zone:

1. To the right of the video window, click one of the VA masking icons: square or polygon .
   a. The rule you are configuring determines the detection zone icons that are available.
2. On the live video, draw the exclusion zone. When the mouse cursor appears as a crosshair, you can begin drawing an exclusion zone.
   a. **To define a square zone:** Click, drag, and release the mouse.
   b. **To define a polygon zone:** Define the first border by clicking, dragging, and releasing the mouse.
      i. Define at least one more point by clicking and releasing the mouse.
      ii. Do not click and drag.
      iii. To close the zone, click the first point.
      iv. For each polygon zone, you can draw up to five points.

c. After you have drawn an exclusion zone, you can move it or adjust the point locations.

3. Click **Save**.
4. You can draw up to eight masking areas/exclusion zones.



Square and Polygon Masking Zones (Exclustion 1 and 2)

5.11.1.3 Modifying the Minimum and Maximum Object Sizes

Tip

For optimum video analytics performance in most conditions, Teledyne FLIR recommends using the default minimum and maximum object size settings. Under certain conditions, modifying these settings can improve VA performance.

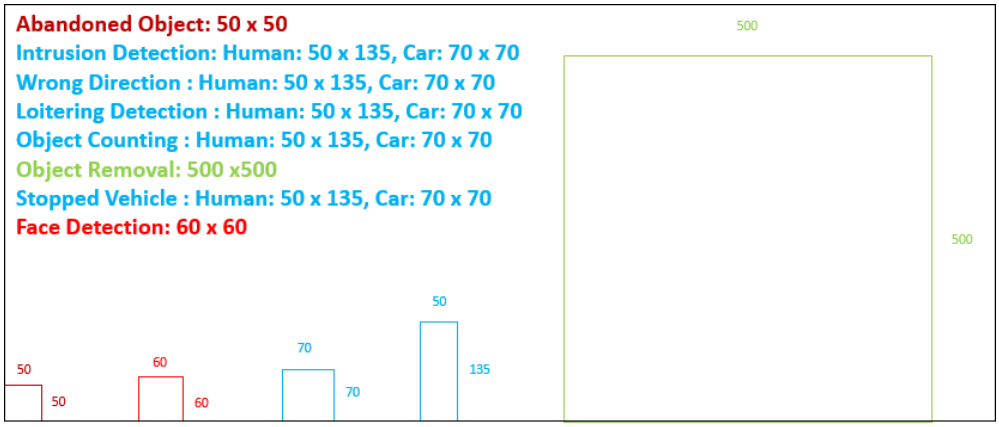
To modify the minimum and maximum size of the objects the VA detects:

1. Click the object size icon. Minimum and maximum object size boxes appear in the live video.

2. Move or adjust the size of the boxes. You can:
   - Click and drag the boxes.
   - Click and drag the corners of the boxes.

The location of the boxes in the live video is not important. However, the following are important:

- The object sizes should reflect potential objects in the scene and their correct proportions.
- The object size shapes should be consistent for best results.
- The short side of the maximum object size must be longer than any side of the minimum object size.
- The minimum target size for the selected rule.

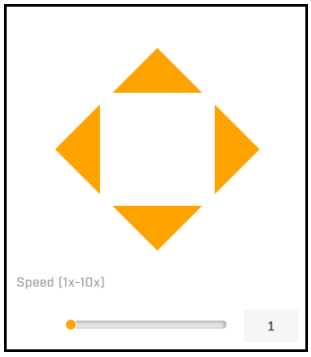


For example, 50 x 135 pixels is the minimum human target size VA detects for the intrusion detection, loitering detection, object counting, and stopped vehicle rules; at 1080p resolution; and with other mounting and scene considerations being met. Therefore, specify a minimum object size larger than 50 x 135 pixels.

5.12 PTZ Page

Use the PTZ page to:

- Move the camera left, right, up, or down (pan and tilt)
- Define the pan, tilt, and zoom speed, between 1x-10x
- Zoom out or zoom in—clicking a Zoom button zooms one step; for continuous zoom, click and hold a Zoom button.



1. Go to the camera's home position

2. Set the camera's current pan, tilt, and zoom position as its home position (also known as preset index 256)

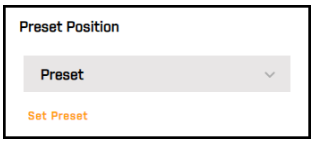
3. Specify the camera's current pan, tilt, and zoom position as a preset position

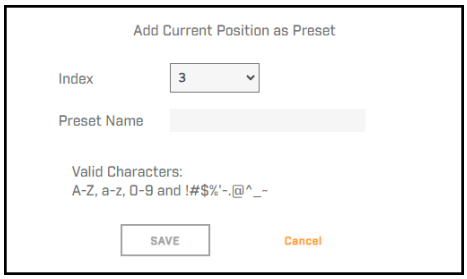
   a. Under Preset Position, click **Set Preset**.

   b. Select an available preset index number from 1-255.

   c. Specify a unique, descriptive name for the preset position. You can use alphanumeric characters, along with `!#$%'-.@^_~`.

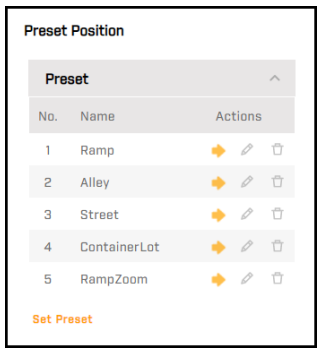
   d. Click **Save**. The camera adds the current position as a preset.





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

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

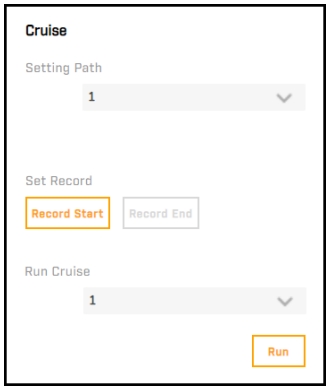


6. Record and run camera cruises

   To record a cruise: Select a cruise setting path, from 1-8; click **Record Start**; move the camera; and then click **Record End**. If you select a setting path for a previously defined cruise, you will record over the existing path.

   To run a cruise, select the cruise and then click **Run**.

   When the camera is running a cruise, video analytics are disabled.



7. Define and run auto pan paths

To define an auto pan path:

a. Select an auto pan setting path, from 1-8. If you select a previously defined auto pan path, you will record over the existing path.

b. Select an auto pan speed, from 1-4.

c. Select a direction. Left is the default.

d. Move the camera to the start point.

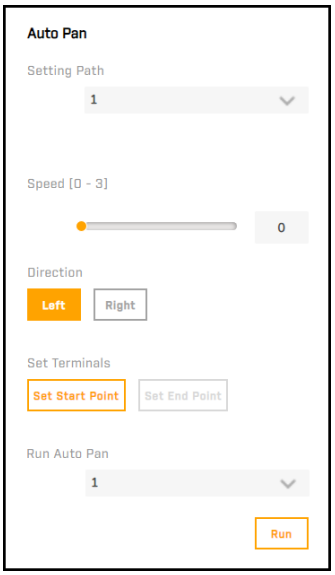
e. Click **Set Start Point**.

f. Move the camera to the end point.

g. Click **Set End Point**.

To run an auto pan path, select the auto pan path and then click **Run**.

When the camera is running an auto pan path, video analytics are disabled.



8. Create and manage up to eight preset tours

To create a tour:

a. Make sure presets have been defined.

b. Select a tour line, from 1-8.

c. Click **Edit Tour**.

d. For each tour stop:

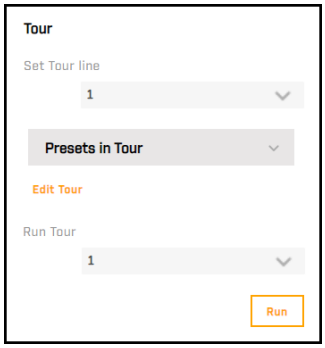
   i. Click **Add Preset Into Sequence**. A stop is added to the tour.

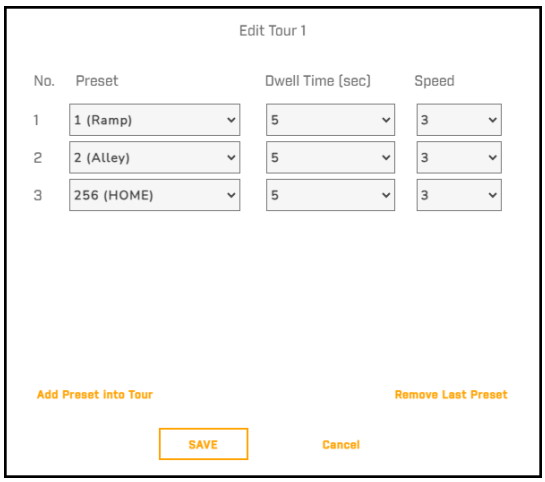
   ii. Select the preset, dwell time (1-127 seconds), and speed (0-14) for the stop.

e. Click **Save**.

f. To run a tour, select the tour line and then click **Run**.

When the camera is moving from one preset to another, video analytics are temporarily disabled. On the <%TARGETTITLE%>, you can configure specific video analytics profiles for when the camera is stationary on a preset position.

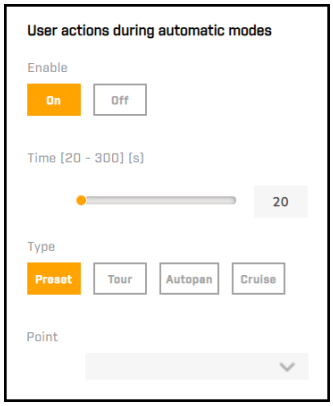




To specify the camera's behavior after a specified period of inactivity:

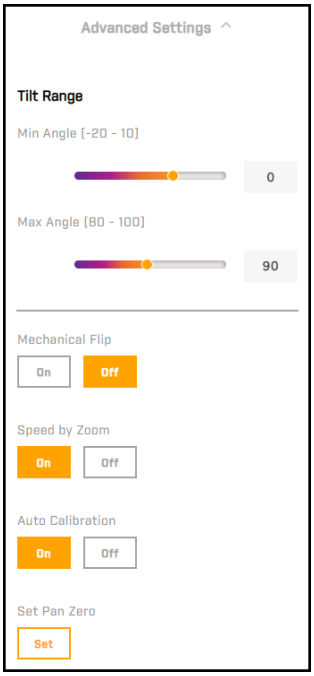
1. Click **Enable**.
2. Specify **Time—**Period of inactivity after which the camera resumes the specified type of behavior.
   a. 20-300 seconds (default is 20).
3. Specify **Type—**Select:
   a. Preset
      i. Select Preset Point
   b. Tour
      i. Select Tour Line (1-8)
   c. Auto Pan
      i. Select Auto Pan Line (1-4)
   d. Cruise
      i. Select Cruise Line (1-8)

When disabled, the camera does not automatically resume any type of behavior.



Configure Advanced Settings

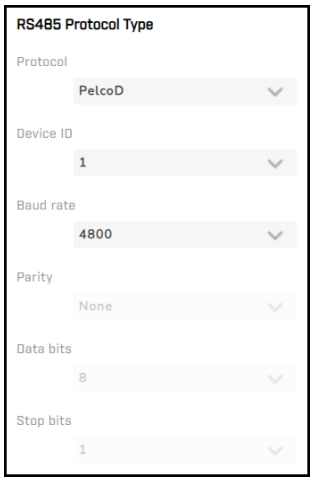
1. Choose Min and Max angle for **Tilt Range**
   a. **Min Angle—**The minimum tilt angle (from -20° to 10°, relative to the horizon).
   b. **Max Angle—**The maximum tilt angle (from 80° to 100° if Mechanical Flip is Off; from 170° to 190° if Mechanical Flip is On).
2. Disable or Enable **Mechanical Flip**
   a. By default, Mechanical Flip is set to On and the camera can continuously track an object passing under the camera.
   b. When a tilting camera reaches its maximum angle, it pans 180° and then continues tilting to keep tracking the object.
3. Disable or enable **Speed by Zoom**
   a. The camera's pan and tilt speed is proportional to zoom position.
   b. Also known as proportional pan and tilt.
4. Disable or enable **Auto Calibration**
   a. The camera automatically calibrates itself when it detects a deviation of dome pivot.
   b. The camera aligns itself against vertical and horizontal checkpoints to maintain accurate operation. On by default.



5. **Set Pan Zero**

   a. To specify the camera's current pan position as its zero (due north) position, click **Set**.

RS485 Protocol Type



6. Specify **Protocol**

   a. PelcoD (default) or PelcoP.

7. **Device ID—**ID number (1-254) provided by the camera according to the camera model and protocol. The default is 1.

8. Specify **Baud Rate**

   a. Baud Rate for the RS-485 connection (2400, 4800, 9600, or 19200).

   b. For PelcoD and PelcoP the default is 2400.

When enabled, you can specify:

- **Parity—**Checks whether corruption has occurred. Specify None (default), Odd, or Even.
- **Data Bits—**Number of bits in each data series, with the least significant bit (LSB) sent first. Specify 5, 6, 7, or 8 (default).
- **Stop Bits—**Number of bits that indicate the last character has been sent. Specify 1 (default) or 2.

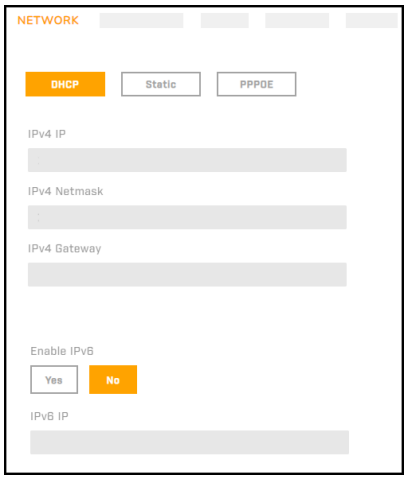
6 Configuration

Users assigned the Admin or Expert role can click **System Setting** on the View Settings page to access the following configuration pages:

- Network Page
- Date & Time Page
- Users Page
- SD Card Page
- Alarm Page
- Schedule Page
- Audio Page
- Recording Page
- Email Page
- FTP Page
- HTTP Page
- Cyber Page
- Firmware & Info Page

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

6.1 Network Page



When you click **System Setting**, by default, the Network page appears.

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

Specify the camera's IP addressing mode:

- **DHCP (default)—**Dynamic Host Configuration Protocol server on the network assigns the camera its IP addresses, and determines the IPv4 Netmask and Gateway. The information appears in these fields, which you cannot modify. If the IP addressing mode is set to DHCP but a DHCP server is not available on the network, the camera's default IP address is 192.168.0.250.
- **Static—**Specify:
  - **IPv4 IP**—Camera's IPv4 address.

    Caution

    After changing the camera's IPv4 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 can no longer access the camera's web page. To access the camera web page again, change the PC's IPv4 address to be on the same network as the camera.

  - **IPv4 Netmask**—Determines whether devices are on the same subnet. The default value is 255.255.255.0.
  - **IPv4 Gateway—**IP address of the server that passes data between devices on different subnets. An invalid gateway setting causes communication between the camera and devices on other subnets to fail.

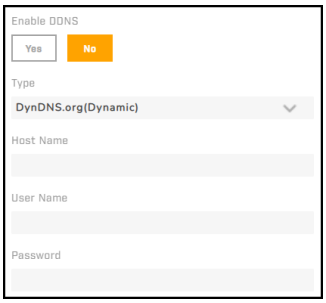
- **Primary DNS—**IP address of the domain name server that translates host names into IP addresses.
- **Secondary DNS—**IP address of the domain name server that backs up the primary DNS.

- **PPPoE—**Camera connects to the network using Point-to-Point Protocol over Ethernet and is assigned an IP address. Specify the User Name and Password for the PPPoE account. Then, click **Save**. If the PPPoE connection is successful, the camera's assigned IPv4 address appears.

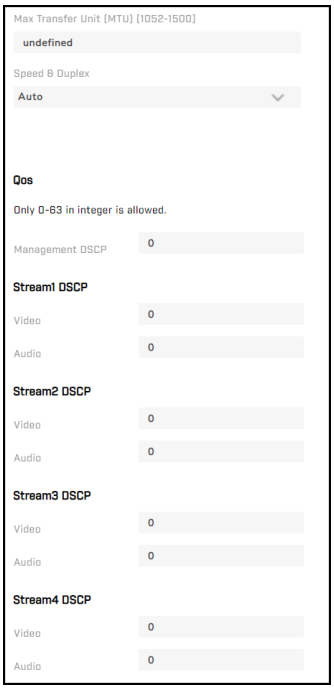
Tips

- You can also use the DNA tool to specify the IP addressing mode as DHCP or Static for one or more of the same camera model. For more information, see Configure for Networking.
- For future reference, record the camera's MAC address, which is found on the camera label.

- **Enable IPv6—**When IPv6 is enabled and the IP addressing mode is Static, specify the camera's IPv6 address. By default, IPv6 is disabled.
- **Enable DDNS—**The Dynamic Domain Name System (DDNS), which allows a static device host name to be constantly synchronized with its dynamic IP address. This allows access to the device using the static host name. By default, DDNS is disabled. When enabled, specify:
  - **Type—**DDNS host provider. DynDNS.org (Dynamic) is the default.
  - **Host Name—**Name that identifies the camera for DDNS.
  - **User Name—**User name required by the DDNS provider for authentication.
  - **Password—**Password required by the DDNS provider for authentication.



- **Maximum Transmission Unit (MTU) (1052-1500)—**Largest amount of data the camera can transmit in one physical frame on the network. For Ethernet, the MTU is 1500 bytes (default). For PPPoE, the MTU is 1492.
- **Speed & Duplex—**Select:
  - **100 Mbps Full Duplex—**Camera supports 100 Mbps Ethernet and can simultaneously transmit and receive data.
  - **100 Mbps Half Duplex—**Camera supports 100 Mbps Ethernet, but cannot transmit and receive data at the same time.
  - **Auto—**Camera supports and automatically detects 10 / 100 / 1000 Mbps Ethernet.



QoS

QoS (quality of service) provides differentiated service levels for different types of traffic packets and guarantees delivery of priority services during periods of network congestion. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Code Point) values, and as a result receive the corresponding forwarding treatment from DiffServ-capable routers.

Specify values (0 to 63) for:

- **Management DSCP—**Class of service for camera management via HTTP.

And for each of the camera's four streams:

- **Video DSCP—**Class of service for the stream's video.
- **Audio DSCP—**Class of service for the stream's audio.

By default, DSCP disabled; that is, the value for each service class is 0 (zero).

Note

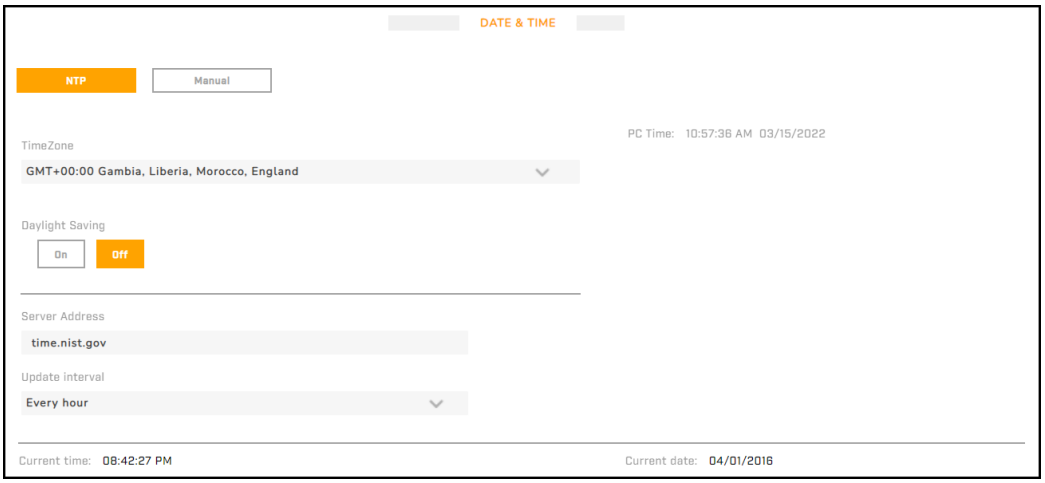
Before assigning DSCP values, make sure the switches / routers on the network support QoS.

6.2 Date & Time Page

On the Date & Time page, users assigned the Admin or Expert role can select **NTP** (default) or **Manual**.

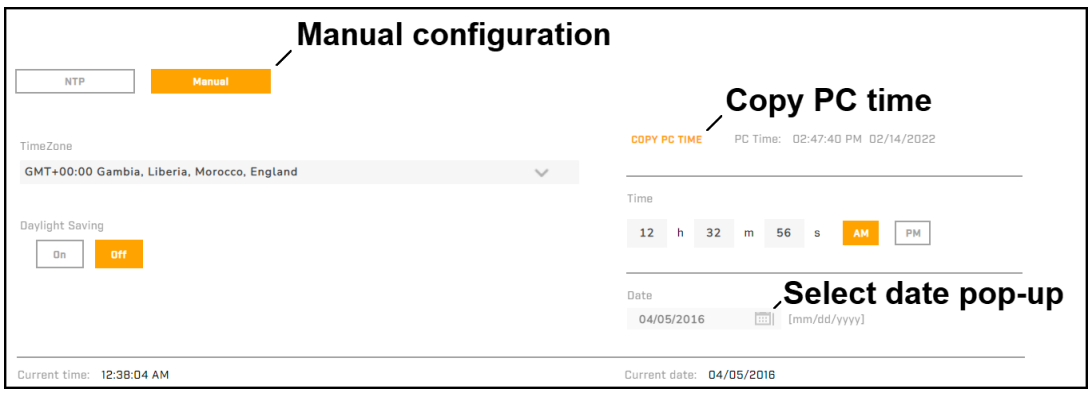
NTP—Camera synchronizes its date and time with an NTP server. Specify:

- **Server Address—**IP address of the NTP server or URL of an NTP service (default: time.nist.gov)
- **Update Interval—**every hour (default), every day, or every week



NTP Date & Time Configuration

Manual—Manually configure the camera's date and time. Click **Copy PC Time** or manually specify the hour, minute, second, AM or PM, and date.



Manual Date & Time Configuration

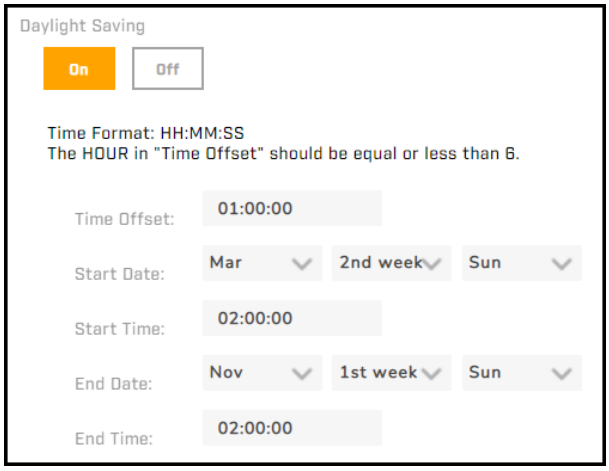
In either NTP or manual configuration, specify:

- **Time Zone**

- **Daylight Saving—**By default, the camera time does not change according to daylight saving time (Off).

  If you enable Daylight Saving (On), specify:

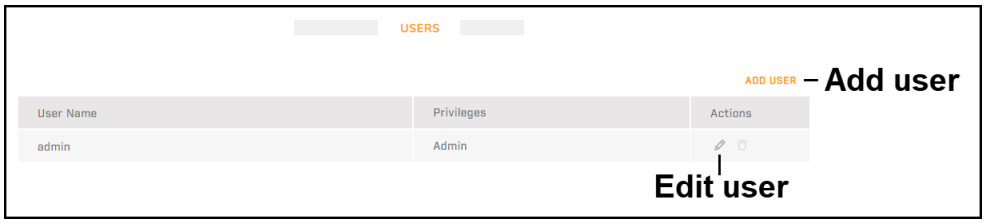
  - **Time Offset—**Number of hours, minutes, and seconds between daylight saving time and standard time. The time offset format is hh:mm:ss. 1:00:00, or one hour, is the default.
  - **Start Date, Start Time, End Date, and End Time—**Select the date and time specified by law. For example, in most places in the US, specify 2 AM on the second Sunday in March and 2 AM on the first Sunday in November, respectively:



US Daylight Saving Time Settings

6.3 Users Page

On the Users page, users assigned the Admin role can add and remove users, and can change or set passwords.

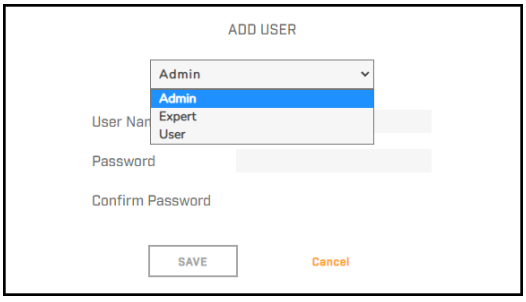


To prevent unauthorized access to the camera:

- Make sure the default password for the admin user has been changed.
- Add users for each required login account, up to a maximum of 20 users.

To add a new user:

1. Click **Add User**. The Add User screen appears.



2. Assign one of the following roles (Privileges), according to the access the user requires:

Role	Access
User	Can: • Select a different web page language • View live video images from any enabled video stream • View live video in a full-screen browser window • Take a snapshot • View alarms • Toggle the web page between Light Mode and Dark Mode • View the Help page • Log out
Expert	Cannot manage users: • Cannot add/edit/delete users • Cannot change passwords Can access and use all other View Settings and System Settings pages, menus, controls, and settings
Admin, including the default *admin* user	Can access and use all of the camera's web pages, including adding/editing/deleting users (but cannot delete the default admin user), and setting all passwords
All roles can access the camera's video streams, which require authentication. You can use the name and password for any of the camera's users.	

3. Specify a user name and password, and then confirm the password, according to the following requirements:

   - User names and passwords are case-sensitive.
   - User names are limited to 29 characters and can only include alphanumeric characters A-Z, a-z, 0-9.
   - Use strong passwords consisting of 8-64 characters. Passwords can include special characters @#~!$&<>+_-.,*?. Passwords cannot contain four-digit sequences (for example, 1234). They also cannot contain four repeating characters (for example, aaaa).

Managing Existing Users

To change the password for a user, click the edit icon for the user, change the password, and then confirm the change. To delete a user, click the trash icon for the user, and then confirm deleting the user. The admin user cannot be deleted.

6.4 SD Card Page

With a microSD card properly installed, the camera can locally record video clips and snapshots, up to 1 TB. For information about how to install a microSD card (not included in the camera kit), see <% TARGETTITLE%>.

On the SD Card page, users assigned the Admin or Expert role can format the microSD card, configure its settings, and view its properties.

Overwrite—When a microSD card is properly installed, the camera automatically enables Overwrite. Specify the amount of time the camera retains recorded files, in days or weeks, and when the camera begins removing the oldest recorded files, in percentage the disk is full (1-99%).

Recording file size (15-600 MB)—Specify the maximum file size. The default is 200 MB.

SD Card Information

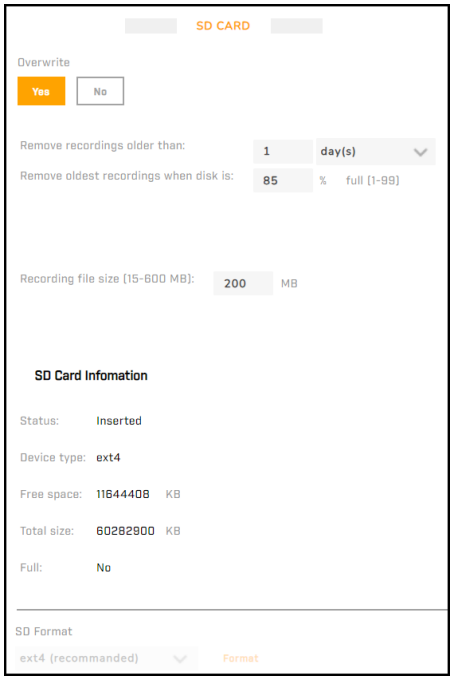
When a microSD card is properly installed:

- Inserted appears as the Status.
- Capacity information appears, in KB.

SD Format

Before using a properly installed microSD card for the first time or when the card has been previously used on a different camera, format it.

When a microSD card is properly installed, you can select the format: vfat (default) or ext4 (recommended). Then, click **Format**. The camera formats the card.



microSD Card Properly Installed

6.5 Alarm Page

On the Alarm page, users assigned the Admin or Expert role can configure alarms for the following triggers:

- a change in the state of an alarm input pin
- each motion detection profile
- network failure
- tampering detection
- a predefined periodic interval
- audio input
- manual alarm trigger
- each VA profile

For most triggers, you can specify whether the alarm is enabled all the time or according to one of the schedules defined on the Schedule Page.

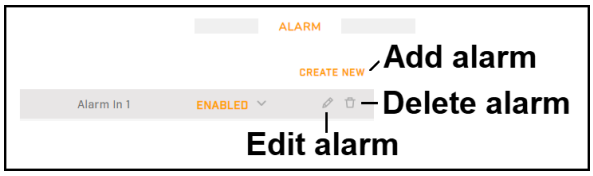
Depending on the alarm trigger, you can specify one or more of the following actions:

- change the state of one or more alarm output pins
- toggle the IR Cut (IRC) filter
- send message by FTP
- send notification email
- upload snapshot image(s) by FTP
- upload snapshot image(s) by email

- record image(s) to microSD card
- send HTTP notification or hand off event to supported PTZ camera
- record video clip to microSD card or to a NAS (network attached storage) server

By default, the following alarm is defined:

- **Alarm In 1—**A change in the state of alarm input pin 1 triggers a change in the state of alarm output pin 1. You cannot modify the trigger for this alarm. You can configure the idle state of alarm input pin 1 on the I/O Page.



When you define or enable a motion detection profile or when you enable a VA profile, the camera automatically creates an alarm. For example:

- **Video Analytics 1—**The rule specified for Video Analytics Profile 1 on the <%TARGETTITLE%> triggers this alarm. However, by default, no action is enabled. Video Analytics 1 / 2 refer to the default preset profile. When you enable a preset profile, the camera creates and enables an alarm specific to the preset profile. For example, Preset Profile 1: Video Analytics 1.

When you define or enable a motion detection profile, the camera automatically creates an alarm. For example:

- **Motion 1—**The motion detection region for profile 1 configured on the <%TARGETTITLE%> triggers this alarm. However, by default, no action is enabled.

To add an alarm, click **Create New**. The alarm Trigger screen appears. Continue with Defining an Alarm Trigger.

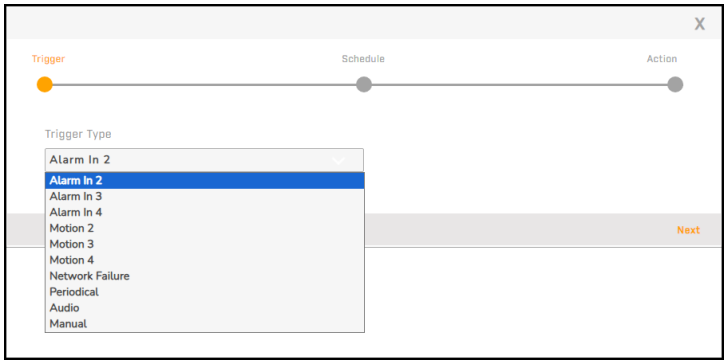
To modify an existing alarm, click the edit icon for the alarm. The alarm Trigger screen appears. Continue with Defining an Alarm Trigger.

To delete an alarm, click the trash icon for the alarm, and then confirm deleting the alarm.

6.5.1 Defining an Alarm Trigger

When creating a new alarm, on the Trigger screen, users assigned the Admin or Expert role can select a trigger and configure its alarm settings.

If you are modifying an existing alarm, click **Next**. If the alarm Schedule screen appears, continue with Specifying an Alarm Schedule. If the alarm Action screen appears, continue with Modifying or Defining Alarm Actions. It is not possible to modify the trigger for an existing alarm.



Trigger Screen - Alarm In 2 Selected

Trigger Type—Select:

- **An Alarm Input Pin (Alarm In 1 / 2 / 3 / 4)—**A change in the alarm input pin state triggers the alarm. You can configure the idle state of alarm input pins on the I/O Page.
- **A Motion Detection Profile (Motion 1 / 2 / 3 / 4)—**Specify:
  - **Detection level (1-100)—**Sensitivity for each sampled pixel. Lowering the value increases detection sensitivity and vice versa. The default is 10.
  - **Sensitivity level (1-100)—**Camera's overall motion detection sensitivity. The default is 80; if 20% or more of the sample pixels are detected as being different, the camera detects motion. Increasing the value increases detection sensitivity.
  - **Time interval (sec) (0-7200)—**Minimum amount of time, in seconds, between motion detection alarms. The default is 10.
- **Network Failure—**Camera periodically pings another IP device on the network to confirm network connectivity. For example, the camera can ping the NAS server specified on the Recording Page. If the camera detects that it cannot connect to the server, you can configure the alarm to trigger local recording on a properly installed microSD card, as a backup until network connectivity is restored. Specify the Ping IP address and the Time interval (seconds) (1-6000) between pings.
- **Tampering—**Specify**:**
  - **Minimum duration (sec) (1-3600)—**Amount of time, in seconds, tampering must occur before the camera triggers an alarm. The default is 20.
  - **Sensitivity level (1-100)—**Amount of tampering - that is, moving the camera - that triggers an alarm. Increasing the value increases detection sensitivity. The default is 80.
- **Periodical—**Camera triggers an alarm at the specified Minimum interval (sec) (60-3600). The default is 60; that is, the camera triggers an alarm every minute.
- **Audio—**Camera triggers an alarm when audio input reaches or exceeds the specified Detection Level (1-100). The appropriate setting depends on a number of factors, including the equipment connected to the audio input, how that equipment is configured, and the overall noise level of the scene whose audio being monitored. For example, if the camera's audio input is connected to an external microphone that is monitoring a relatively quiet scene, it might be appropriate to lower the Detection Level. On the other hand, if the microphone is monitoring a noisy scene, it might be appropriate to increase the Detection Level.

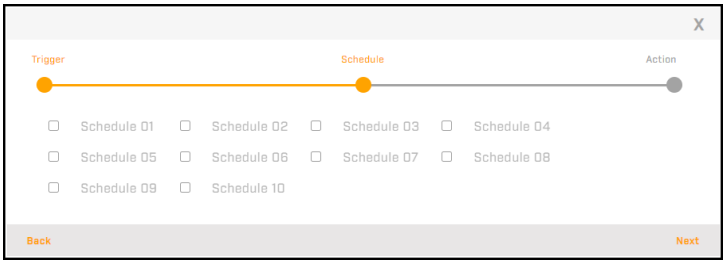
  You can also specify the Time interval (sec) (0-7200), the minimum amount of time between each audio detected event, in seconds. The default is 10.

- **Manual—**Camera triggers an alarm when a user clicks the manual trigger button on the View Settings page.
- **An Enabled Video Analytics Profile —**Camera triggers an alarm according to the settings for the rule selected for the profile on the <%TARGETTITLE%>. Video Analytics 1 / 2 refer to the default preset profile. If preset profiles have been defined, you can select any of them as the trigger. For example, Preset Profile 1: Video Analytics 1.

Click **Next**. If the alarm Schedule screen appears, continue with Specifying an Alarm Schedule. If the alarm Action screen appears, continue with Modifying or Defining Alarm Actions.

6.5.2 Specifying an Alarm Schedule

On the Schedule screen, users assigned the Admin or Expert role can specify one or more schedules for an alarm. You can configure up to 10 schedules on the Schedule Page.



Click **Next**. The alarm Action screen appears. Continue with Modifying or Defining Alarm Actions.

6.5.3 Modifying or Defining Alarm Actions

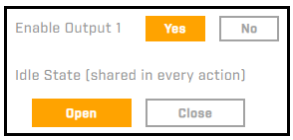
On the Action screen, users assigned the Admin or Expert role can:

- Enable and configure the actions for an alarm.
- Enable the schedule(s) selected on the alarm Schedule screen.

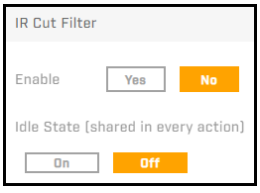
For VA alarm triggers, you can enable and configure actions for each defined detection zone.

Video Analytics 2 Alarm Trigger - 2 Detection Zones Defined

You can individually enable and configure the following alarm actions. Not all actions are available for all alarm triggers.



- **Alarm Out—**Changes the state of an alarm output pin until the camera resets it according to the specified Reset Interval setting on the I/O Page. Specify:
  - **Idle State—**To specify normally open (default), click Open. To specify normally closed, click Close. Changing this setting affects all alarms for which the Alarm Out action is enabled.



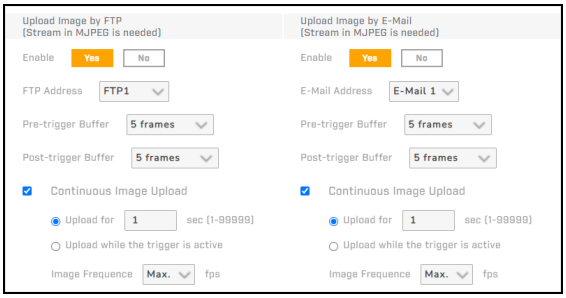
- **IR Cut Filter—**Changes the state of the IR cut filter. Not available when the IR state specified on the Illumination Page is Light Sensor (default), Auto, or Smart. Specify:
  - **Idle State—**Specify whether the IR cut filter idle state is on or off. Changing this setting affects all alarms for which the IR Cut Filter action is enabled.

- **Send Message by FTP / E-mail—**Sends a message by FTP / email, according to the settings on the FTP Page / Email Page.

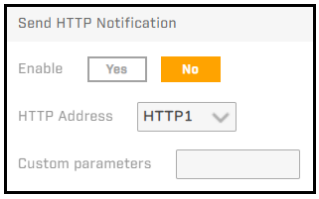
- **Upload Image by FTP / E-mail—**Uploads images to an FTP server or by email, according to the settings on the FTP / Email page. At least one video stream must be encoded in MJPEG. You can configure the video stream settings on the Visible Page.

  Specify:

  - **FTP / E-mail Address—**Select one of the FTP / email addresses defined on the FTP / Email page.
  - **Pre- / Post-trigger Buffer—**Select the number of frames before / after the trigger (1-20 frames). The default is five frames.
  - **Continuous Image Upload—**When enabled, select whether the camera uploads images for a specified period of time (1-99,999 seconds), or while the trigger is active. Specify the Image Frequency, or frame rate (1-15, Max fps).



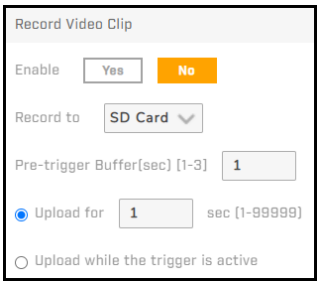
- **Send HTTP Notification—**Sends a notification to an HTTP notification server or hands off the event to a supported PTZ camera.



  Specify:

  - **HTTP Address—**Select HTTP server 1 or 2. You can configure the HTTP notification servers on the HTTP Page.
  - **Custom parameters—**Specify parameters the camera adds to the HTTP notification server address. For example, if you have configured an HTTP notification server address as *http://192.168.0.100/admin.php* and you specify the custom parameters as *action=1&group=2*, when the alarm is triggered, the camera sends: *http://192.168.0.100/ admin.php/action=1&group=2*.

- **Record Video Clip—**Records a video clip to a local microSD or to a NAS, according to the settings on the SD Card or Recording page. Make sure that a microSD card is properly installed, formatted, and active; or that the NAS is properly configured. Specify:



  - **Pre- / Post-trigger Buffer—**Number of seconds before / after the trigger (1-3 seconds). The default is one second.
  - Whether the camera records images for a specified period of time (1-99,999 seconds), or while the trigger is active.

File Name Settings

File Name—Specify the generic name for image files the camera stores or uploads. *image.jpg* is the default.

Select one of the following suffixes the camera adds to the file names to identify individual images:

- **Add date / time suffix (default)**

  File name format: imageYYMMDD_HHNNSS_XX.jpg

  Y: year, M: month, D: day

  H: hour, N: minutes, S: seconds

  XX: sequence number

- **Add sequence number suffix (no maximum value)**

  File name format: imageXX.jpg

  XX: sequence number

- **Add sequence number suffix up to <specify maximum sequence number> and then start over**

  The file names end at the specified maximum number. For example, if image.jpg is the specified File Name and 10 is the specified maximum sequence number, file names start at *image00.jpg*, end at *image10.jpg*, and then start over again.

  File name format: imageXX.jpg

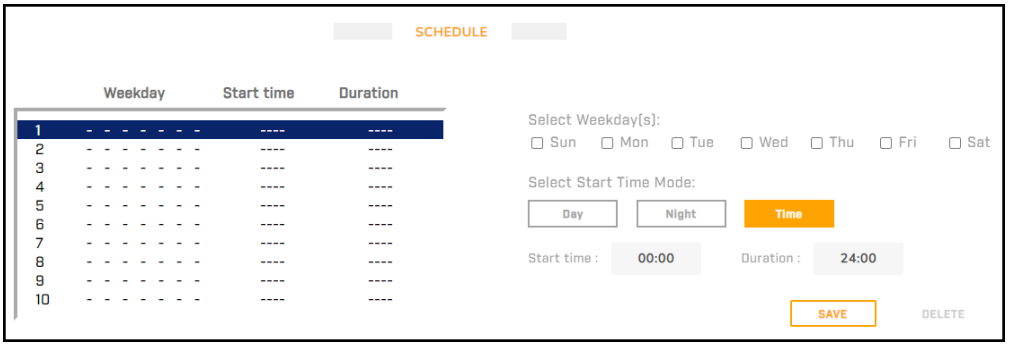
  XX: sequence number

- **Overwrite—**New images replace old images. The file name is static; the camera does not add any suffixes.

Click **Done**. The alarm appears in the list of alarms.

6.6 Schedule Page

On the Schedule page, users assigned the Admin or Expert role can define up to 10 schedules that can be assigned to alarms. For example, you can define a schedule that starts when a facility closes for the night or for the weekend and ends when it opens, and then apply that schedule to a motion detection alarm.



Note

The schedules and settings on the Schedule page do not apply to live video recording. Accounts assigned the Admin or Expert role can configure live video recording settings on the Recording Page.

To define or modify a schedule:

1. From the list of schedules on the left, select a schedule.
2. Select one or more days of the week the schedule applies.
3. Select which of the following determines the schedule start time:
   - **Day—**Schedule starts when night turns to day and ends when day turns to night.
   - **Night—**Schedule starts when day turns to night and ends when night turns to day.
   - **Time—**Define the specific Start time for the schedule, in 24-hour format (for example, 09:00), and the Duration (for example, 4:00 hours).
4. Click **Save**. The schedule settings appear in the list of schedules and the **Delete** button becomes available for the schedule.

To delete a schedule, select the schedule and click **Delete**. The schedule's settings are cleared.

6.7 Audio Page

On the Audio page, users assigned the Admin or Expert role can enable and configure the camera's audio features.

When audio is enabled on this page and the Audio alarm trigger has been enabled on the Alarm Page, the audio input level appears on the Audio Indication Bar.

Alarm with Audio Trigger Enabled

Line In

- **Gain (0-10)—**The default is 5.
- **Bit Rate (Kbps)—**Select 40 kbps (G.726), 32 kbps (G.726), 24 kbps (G.726), 16 kbps (G.726), uLAW (G.711), ALAW (G.711), AAC, PCM (128 Kbps), PCM (256 Kbps), PCM (384 Kbps), or PCM (768 Kbps). The bit rate for uLAW and ALAW is 64 kbps, but using different compression formats. A higher bit rate can provide higher audio quality, but requires more bandwidth. uLAW is the default.

Note

Latitude / UVMS does not support G.726.

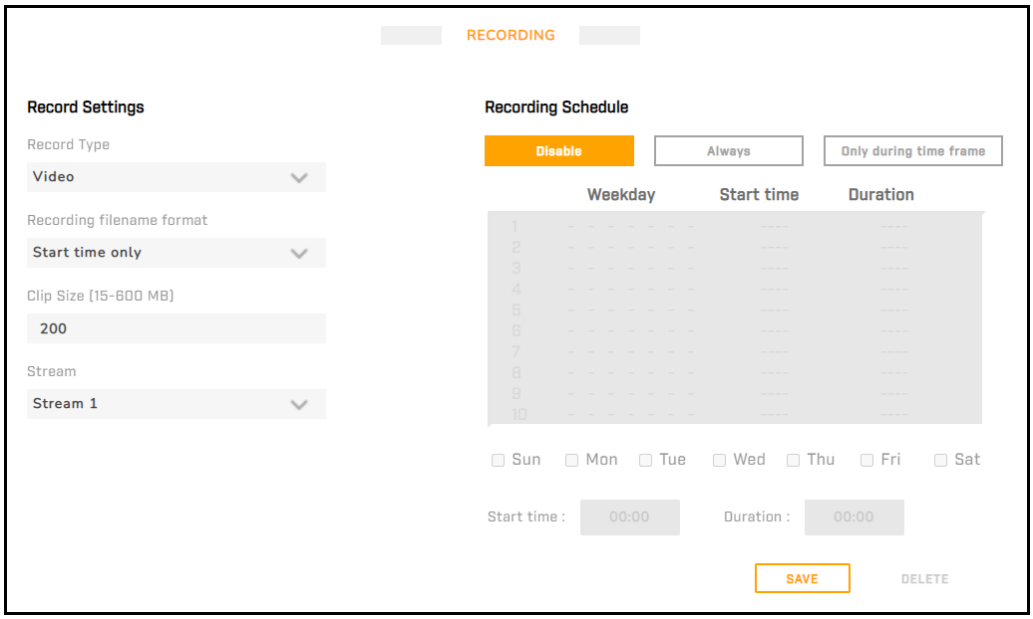
- **Input Type—**Line in.
- **Multicast Address (224.0.0.0-239.255.255.255)—**A valid multicast address in the specified range.
- **Multicast Port (0, 1024-65535, even)—**The port the camera uses for multicast audio streaming.
- **Multicast TTL (1-255)—**Time to live, the maximum number of network hops before routers discard the camera's data packets. Each time one router forwards a datagram to another router, it subtracts 1 (one) from the packet's TTL. If the TTL reaches zero (0), a router discards the packet. Teledyne FLIR recommends setting TTL at 64.

Line Out

- **Gain (0-6)—**The default is 3.

6.8 Recording Page

On the Recording page, users assigned the Admin or Expert role can configure the camera's audio and video recording settings.



Record Settings

- **Record Type—**Select Audio and Video or Video (default).
- **Recording Filename Format—**Select Start time only (default) or Start time + end time.
- **Clip Size (15-600 MB)—**Maximum clip file size. The default is 200 MB.
- **Stream—**Specify the video stream the camera records. Stream 1 is the default.

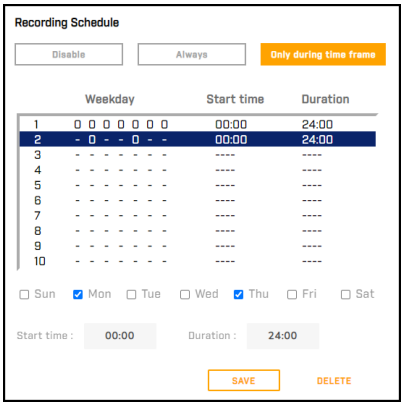
Recording Schedule

By default, recording is disabled. To permanently enable recording, click **Always**. You can configure up to 10 schedules; that is, times during the week recording is enabled.

To define or modify a recording schedule:

1. Click **Only during time frame**.
2. From the list of schedule numbers on the left, select a number.
3. Select one or more days of the week the schedule applies.
4. Define the Start time, in 24-hour format (for example, 00:00 = midnight).
5. Define the Duration (for example, 24:00 hours).
6. Click **Save**. The schedule settings appear and the **Delete** button becomes available for the schedule.

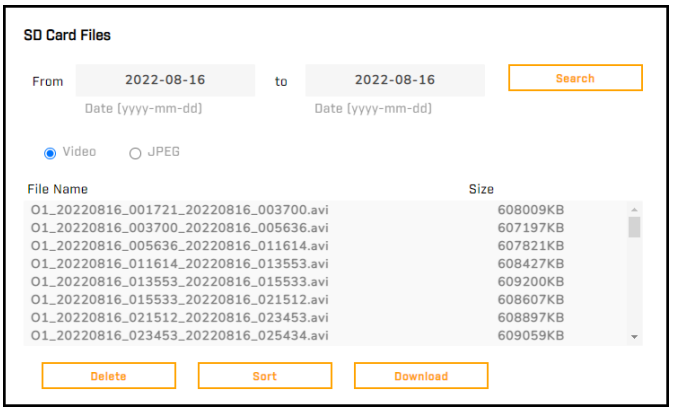
The example at right shows a recording schedule for all day Monday and Thursday.



Schedule for recording all day Monday and Thursday

SD Card Files

A list of the files recorded on the card, if any exist.



By default, files recorded today appear in the list (if any exist). To see other files, specify start and end dates using the format yyyy-mm-dd, and then click **Search**.

Uppercase letters at the beginning of the file names indicate the recording trigger:

- R—regular (always or schedule)
- N—network failure
- M—motion (M0 indicates the first motion trigger)
- A—alarm (A0 indicates the first alarm input trigger)
- T—tampering
- O—manual SD card video recording (see View Settings Home Page)

You can:

- Filter the list to show video clips (default) or snapshots (JPEG).
- Delete one or more files.
- Sort the list by file name, trigger type, or date.
- Download up to 50 files / up to 300 MB, as a ZIP file.

To select more than one file, use the CTRL and SHIFT keys.

6.9 Email Page

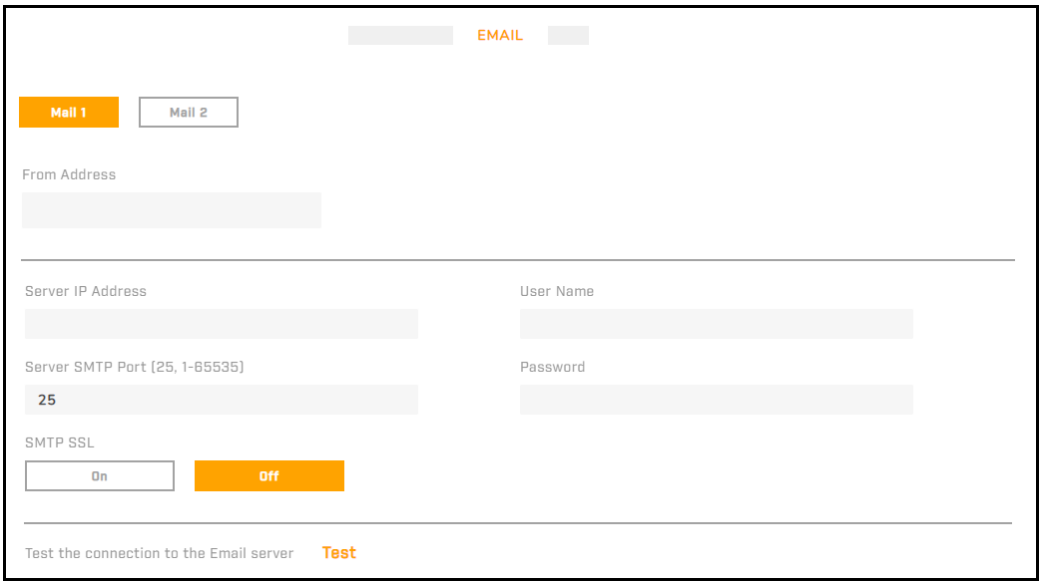
On the Email page, users assigned the Admin or Expert role can configure the settings of two servers the camera can use for sending alarm notification messages or uploading images by email.

Email servers use Simple Mail Transfer Protocol (SMTP) to send and receive email. If you do not know how to configure these settings, contact your email service provider.

Select Mail 1 (primary server) or Mail 2 and then configure:

- **From Address—**Email address that appears as the sender on notification emails the camera sends.
- **Server IP Address—**IP address of the server.
- **Server SMTP Port (25, 1-65535)—**Port the server uses for SMTP communication. The default is 25.
- **User Name—**User name of the account on the server.

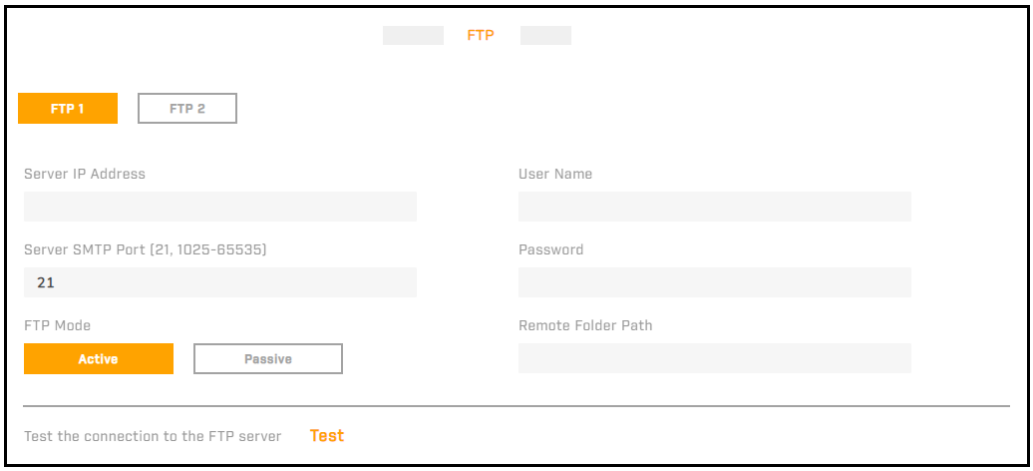
- **Password—**Password for the account on the server.
- **SMTP SSL—**To enable SSL (Secure Socket Layers) for communication with the selected SMTP server, click **On**.



To test the connection with the selected SMTP server using the specified values, click **Test**.

6.10 FTP Page

On the FTP page, users assigned the Admin or Expert role can configure the settings of two File Transfer Protocol servers to which the camera can upload images or send alarm notifications.



Select FTP 1 or FTP 2 and then configure:

- **Server IP Address—**IP address of the FTP server.
- **Server FTP Port (21, 1025-65535)—**Port the server uses for FTP communication. The default is 21.
- **User Name—**User name of the account on the FTP server.
- **Password—**Password for the account on the FTP server.
- **FTP Mode—**Click **Active** (default) or **Passive**.

In passive mode, the client - in this case, the camera - initiates the connections both to and from the FTP server, which addresses the issue of the client-side firewall blocking incoming data from the server.

To support passive mode on the server side, the following communication channels must be open:

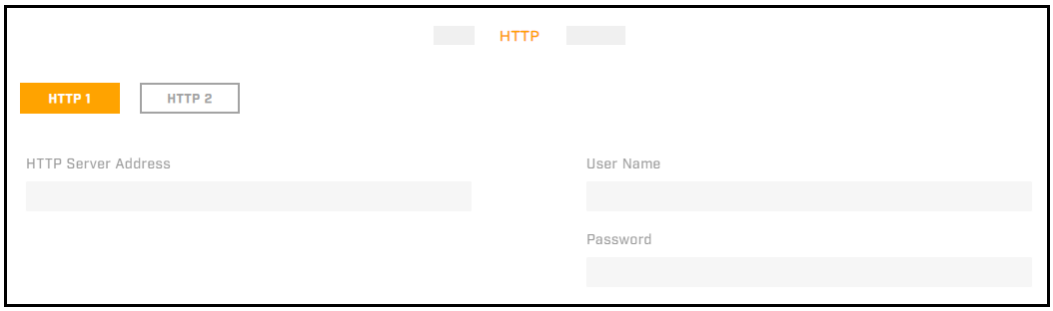
- FTP server port 21 from anywhere (client initiates connection)
- FTP server port 21 to ports > 1023 (server responds to client's control port)
- FTP server ports > 1023 from anywhere (client initiates data connection to random port specified by server)
- FTP server ports > 1023 to remote ports > 1023 (server sends ACKs and data to client's data port)

- **Remote Folder Path—**Path of the file folder on the FTP server to which the camera uploads images.

To test the connection with the selected FTP server using the specified values, click **Test**.

6.11 HTTP Page

On the HTTP page, users assigned the Admin or Expert role can configure the settings of two HTTP servers to which the camera can send alarm notifications.



Select HTTP 1 or HTTP 2 and then configure:

- **HTTP Server Address—**IP address of the HTTP server.
- **User Name—**User name of the account on the HTTP server.
- **Password—**Password for the account on the HTTP server.

6.12 Cyber Page

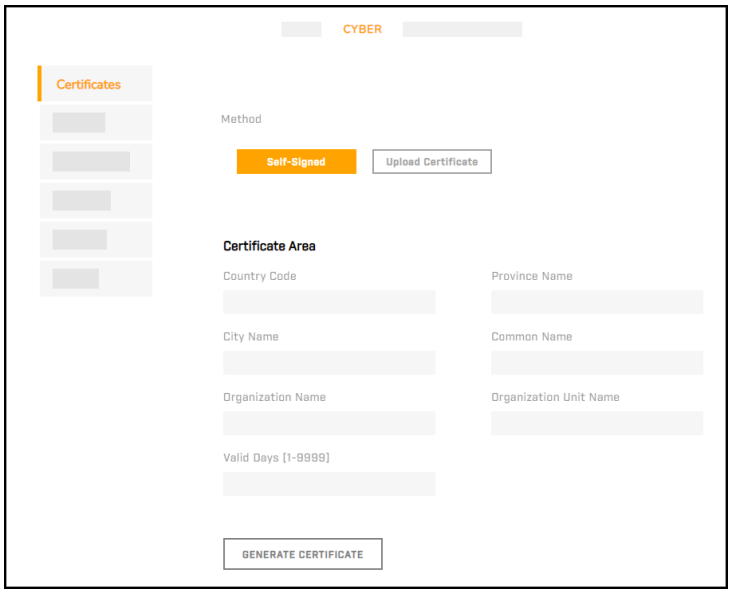
On the Cyber page, users assigned the Admin or Expert role can enable and configure the following cybersecurity settings:

- Certificates
- 802.1X
- TLS / HTTPS
- Services
- IP Filter
- SNMP

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

6.12.1 Certificates

Before you can enable TLS/HTTPS or 802.1X, you need to install a certificate on the camera.



In the Certificates section, you can:

- generate a self-signed certificate
- upload a self-signed certificate
- upload a certificate issued by a certificate authority (CA)

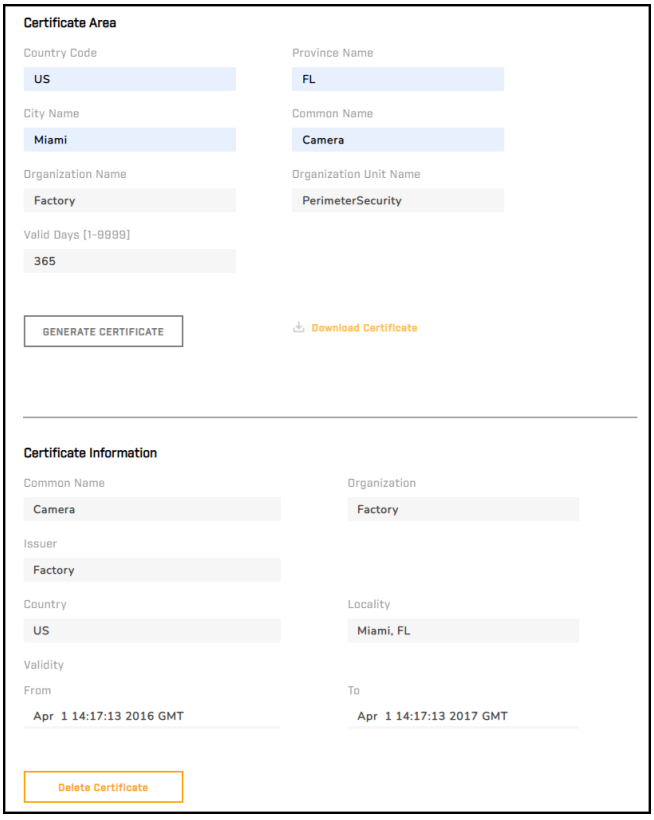
Note

CA-issued certificates are publicly recognized and provide a higher level of security than self-signed certificates. For example, browsers do not trust self-signed certificates.

To generate a self-signed certificate:

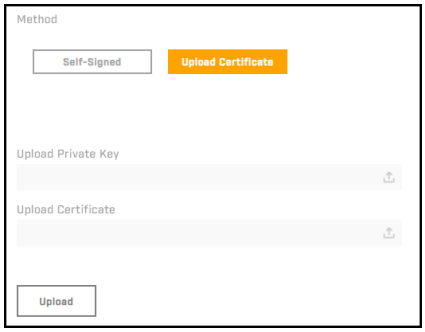
1. On the Date & Time Page, make sure the camera's date and time is the current date and time. Synchronize the camera's time with an NTP server or copy the PC's time.
2. Under Method, select **Self-Signed**.
3. Enter information such as country code, city name, common name, and organization name. For the common name, you can specify the name of the person or other entity the certificate identifies; for example, it can identify the website.
4. Click **Create Certificate**.

After the camera generates the certificate, the certificate information appears.



You can now enable TLS/HTTPS and 802.1X; download the certificate as a PEM file; or delete the certificate.

To upload a certificate:



1. Under Method, select **Upload Certificate**.
2. Under **Upload Private Key**, and then under **Upload Certificate**:
   a. Click .
   b. Browse for and select the appropriate file.
   c. Click **Upload**. The camera uploads and installs the key and the certificate.

6.12.2 802.1X

In the 802.1X section, users assigned the Admin or Expert role can enable and configure the camera to access a network protected by 802.1X / EAPOL (Extensible Authentication Protocol over LAN). To obtain certificates, user IDs, passwords, and other information, contact the network administrator.

Enable 802.1X; select the Protocol (EAP-MD5, EAP-TLS, EAP-TTLS, or EAP-PEAP); and then specify the information the protocol requires. You can use the following special characters: _ . / \ ~ ! @ # $ % ^ & + - * .

EAP-MD5

- **User Name**
- **Password**

802.1X Enabled - EAP-MD5 Selected

EAP-TLS

- **User Name—**User name associated with the certificate, up to 16 characters.
- **Private Key Password—**Password for the private key, up to 16 characters.
- **CA Certificate / Client Certificate—**Click **Upload file**, and then browse for and select the certificate file.
- **Private Key—**Click **Upload file**, and then browse for and select the key file.

EAP-TTLS

- **Inner Auth—**Select the inner tunnel authentication method (CHAP, EAP-MSCHAPV2, EAP-MD5, MSCHAP, MSCHAPV2, or PAP).
- **User Name—**User name associated with the certificate, up to 16 characters.
- **Password—**Password for the user, up to 16 characters.
- **Anonymous ID—**Anonymous ID for the user, up to 16 characters.
- **CA Certificate—**Click **Upload file**, and then browse for and select the CA-issued certificate file.

EAP-PEAP

- **User Name—**User name associated with the certificate, up to 16 characters.
- **Password—**Password for the user, up to 16 characters.
- **CA Certificate—**Click **Upload file**, and then browse for and select the CA-issued certificate file.

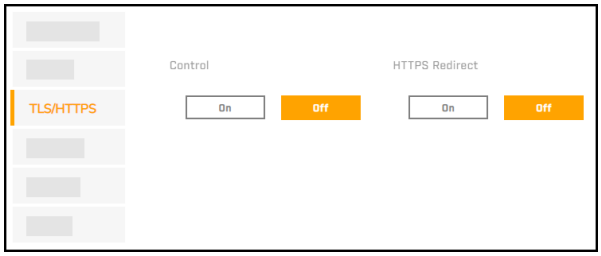
Fields with red borders are required.

To save any changes to the IEEE 802.1X settings and to upload files, click **Save**.

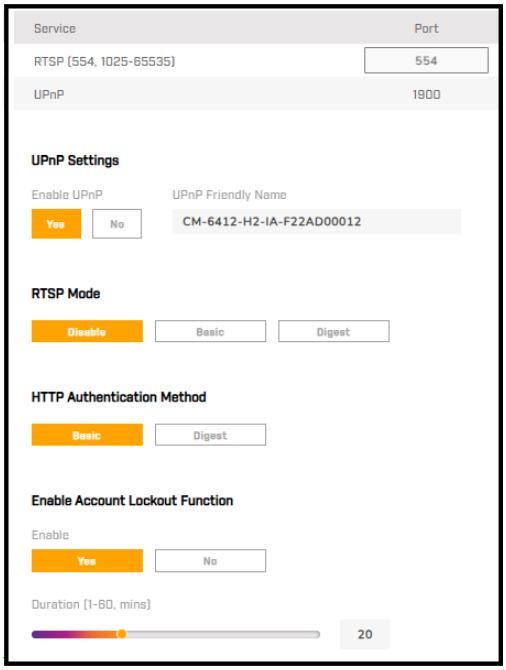
6.12.3 TLS / HTTPS

In the TLS / HTTPS section, users assigned the Admin or Expert role can enable camera control using Transport Layer Security (TLS) / secure HTTP (HTTPS), which secures communication between the camera and web browser.

Enabling control requires generating a self-signed certificate or uploading a CA-signed certificate in the Certificates section. When control is enabled, you can enable HTTPS redirect.



6.12.4 Services

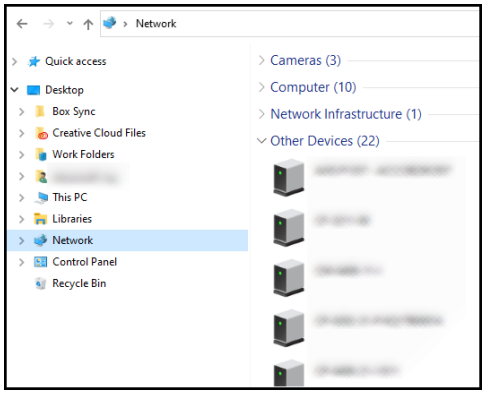


In the Services section, users assigned the Admin or Expert role can:

- Specify the RTSP port (554, 1025-65535). The default is 554.
- **Enable UPnP—**By default, UPnP is enabled. Windows computers and other compliant devices can discover the camera on the LAN. In Windows, the connected camera appears as a Network device.

> **Note**
>
> To use UPnP on a computer, make sure UPnP is installed on the computer. For information about how to install UPnP components on a Windows computer, see Installing UPnP Components.

- **UPnP Friendly Name—**Name that identifies the camera on UPnP devices.



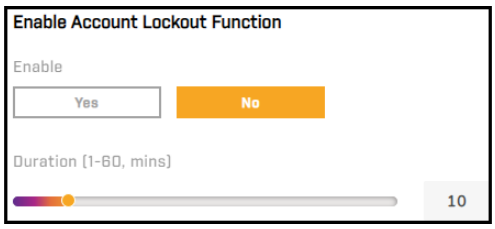
Cameras with UPnP Enabled - Windows File Explorer

- Enable RTSP basic or digest authentication for accessing the camera's video streams:
  - **Disable—**Accessing the camera's video streams does not require authentication. By default, RTSP authentication is disabled.

- **Basic—**Uses unencrypted base64 encoding. Teledyne FLIR recommends enabling basic authentication only when TLS / HTTPS is enabled.
- **Digest—**Encrypts the credentials when transmitted.

When RTSP authentication is enabled, accessing the camera's video streams requires providing the name and password for a camera user. All camera users have access to the camera's video streams.

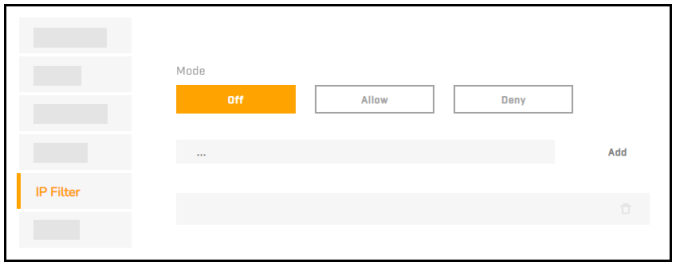
- Configure the HTTP Authentication Method for accessing the camera's web page. Select Basic (default) or Digest.
- Enable and configure account lockout. When enabled, if a user unsuccessfully attempts to log in exceeding the specified duration, the account is locked. By default, account lockout is disabled.



- **Duration (1-60, mins)—**The default is 20 minutes.

6.12.5 IP Filter

In the IP Filter section, users assigned the Admin or Expert role can enable and configure the camera's IP filter.



Select the IP filter mode:

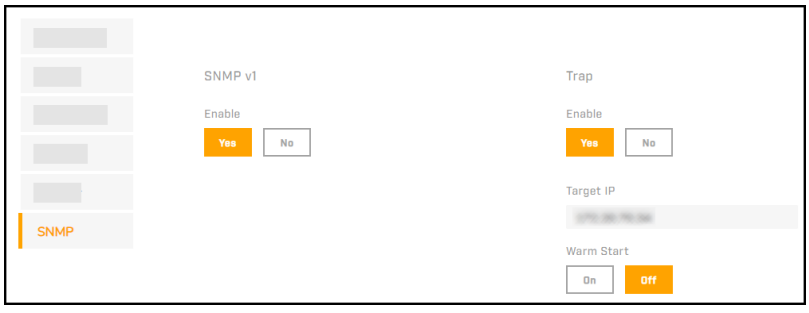
- **Allow—**Allows access to the camera only from the specified IP addresses.
- **Deny—**Denies access to the camera from the specified IP addresses.

To add an IP address to the list, in the text field under the Mode selection buttons, specify an IPv4 address and then click **Add**. You can specify up to 256 IP addresses.

To remove an IP address from the list, click the corresponding trash icon .

6.12.6 SNMP

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



SNMP v1—Enable SNMP v1.

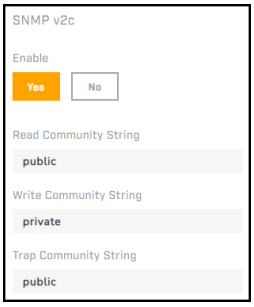
Trap

The camera uses traps to send messages to the network management system for important events or status changes.

After enabling traps, specify:

- **Target IP—**IP address of the network management system server.
- **Warm Start—**Enables traps that indicate when the camera is rebooting, but configuration data or MIB variable values have not changed.

SNMP v2



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*.
- **Trap Community String—**Name of community camera uses when sending traps to the network management system. The default value is *public*.

Important

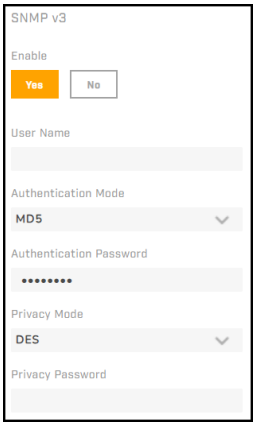
For cybersecurity reasons, change the default community strings.

SNMP v3

SNMP v3 provides security features including:

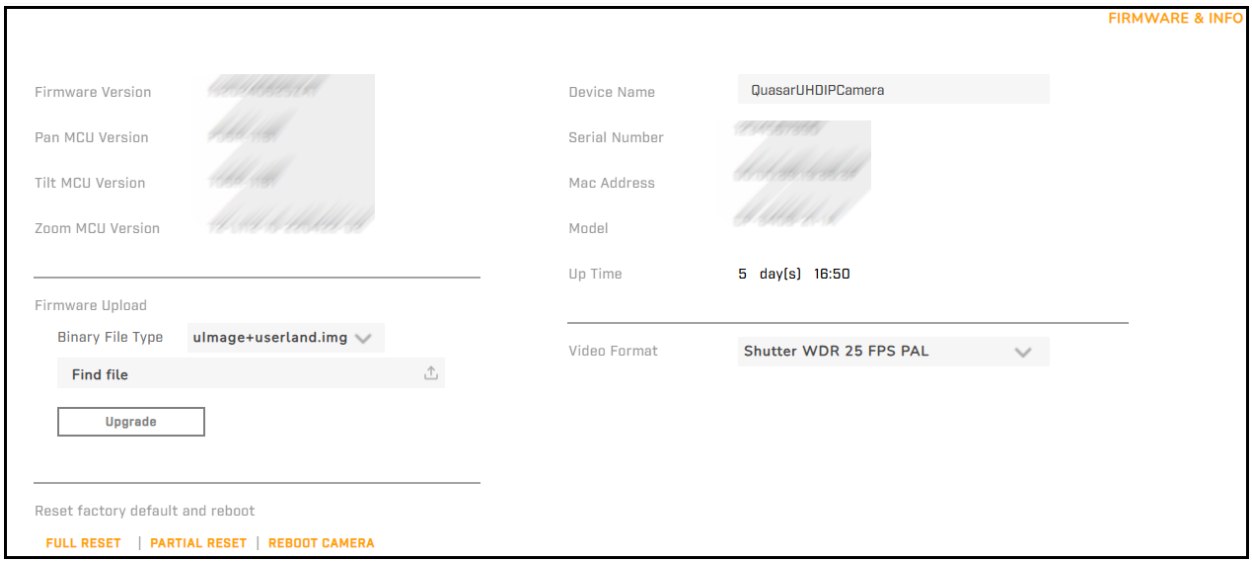
- **Confidentiality—**Packet encryption prevents snooping by unauthorized sources.
- **Message Integrity—**Ensures that packets have not been tampered with in transit, including an optional packet replay protection mechanism.
- **Authentication—**Verifies the message is from a valid source.

After enabling SNMP v3, specify:



- **User Name—**Name of user on network management system using SNMP v3.
- **Authentication Mode—**Select MD5 (default) or SHA.
- **Authentication Password—**Password for authentication on network management system.
- **Privacy Mode—**Select DES (default) or AES.
- **Privacy Password—**Password for privacy on network management system.

6.13 Firmware & Info Page

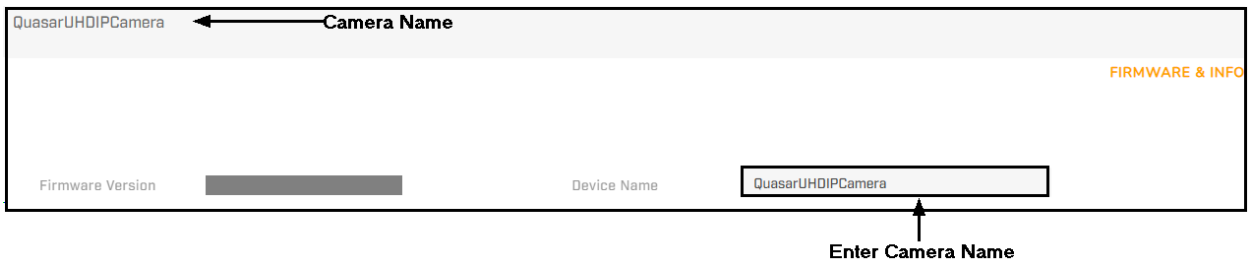


On the Firmware & Info page, users assigned the Admin or Expert role can:

- 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
- Download or upload a configuration backup file
- Download system information
- Configure the camera's video format, including enabling a Shutter WDR format

Device Name

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



Firmware Upload

To upgrade the camera's firmware:

1. Under Firmware Upload, click **Find file**.
2. Select the Binary File Type. For example, **uImage+userland.img**.
3. On your computer or network, browse to and select the firmware file.

Notes

- Do not change the firmware file name. If you change the file name, the system fails to find the file.
- Firmware can also be upgraded via DNA version 2.3.0.35 or higher.

Caution:
Do not unplug power or change the screen while upgrading software.

4. Click **Upgrade**. The system verifies that the upgrade file exists and begins to upload the file. An upgrade status bar appears. When the camera completes the upgrade, the View Settings page appears.

Reset factory default and reboot

Full Reset—Reboots the camera and restores factory default settings, including its networking settings; for example, the camera's IP addressing mode and its IP address. To discover the camera again and reconfigure its network configuration, use the DNA tool. For more information, see Configure for Networking.

Partial Reset—Reboots the camera and restores factory default settings, except its current networking and video format settings.

Reboot Camera—Reboots the camera without changing its current settings.

Tip

You can also reboot and reset the camera to its factory default settings by pressing the camera's physical Default button for at least 20 seconds; for example, if you are unable to access the camera via its web page or other communication method. The Default / Reset button is located here.

Configuration Backup

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

To upload a configuration backup file:

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

Caution

Make sure to upload a configuration backup file that was downloaded from another camera that is the exact same model.

3. To retain the camera's current VA settings, make sure **Maintain current Video Analytics setting** is selected.

   To overwrite the camera's current VA settings with the VA settings in the configuration backup file, make sure **Maintain current Video Analytics setting** is not selected.
4. Click **Upload**.

   The camera uploads the backup file and reboots.

To download the camera's saved settings:

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

config_file.bin is the backup file name. Do not change the file name.

Support Package

To download the camera's log file, click **Download**. Teledyne FLIR Support can use this file to help resolve issues.

Video Format

Select Shutter WDR 60 FPS NTSC (default), Shutter WDR 50 FPS PAL, Linear 60 FPS NTSC, or Linear 50 FPS PAL. When a Shutter WDR format is selected:

- The camera analyzes the exposure and level of detail in two frames taken at different exposure settings and shutter speeds, uses an algorithm to determine the optimal combination of regions within the scene, and generates a single, composite frame with wide dynamic range.
- The maximum frame rate of the camera's video output is 30 / 25 (NTSC / PAL).

When a Shutter WDR is not selected, the camera operates in linear mode; that is, the camera streams every frame it takes. In scenes with high contrast or changing light issues, bright areas can be overexposed and dark areas can be underexposed.

Shutter WDR Format Selected

Shutter WDR Format Not Selected

Tips

- For most lighting conditions, to achieve video with a consistent exposure level regardless of changing contrast or lighting conditions, Teledyne FLIR recommends selecting a Shutter WDR format.
- When the frequency of a light source around the camera (including reflected light) is closely synced with the Shutter WDR operation, a pixelization effect can appear. Under these conditions, Teledyne FLIR recommends selecting a linear format; that is, 60 FPS NTSC or 50 FPS PAL.
- For more information about video resolutions and frame rates supported in linear and shutter modes, see Video Page.

After changing the Video Format, the camera reboots. If the camera is attached to a VMS, after it reboots, you need to re-attach the camera to the VMS.

7 Appendices

7.1 Technical Specifications

Up-to-date resources for the camera, including the camera's specifications, are available from the camera's product information and support pages on the Teledyne FLIR website. See <%TARGETTITLE%>.

7.2 PTZ Handoff Configuration

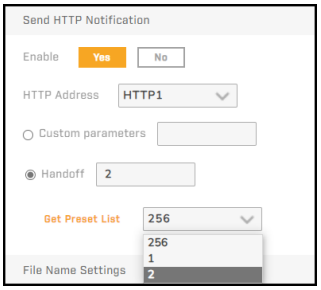
A Quasar Premium Fixed Box Camera with Edge AI Video Analytics (CF-6408-00-0A) can hand off alarms to a Quasar Premium PTZ with Edge AI Video Analytics Camera (CP-640x-x1-xA), which moves to a specified preset and tracks the detected objects. The handoff requires configuring a video analytics alarm on the fixed box camera with an HTTP action that moves the PTZ camera to the preset.

To configure PTZ handoff:

1. With a user assigned the Admin or Expert role, access the PTZ camera and log in to its web page.
2. On the <%TARGETTITLE%>, define a preset larger than the fixed box camera's field of view.
3. With a user assigned the Admin or Expert role, access the Quasar Premium Fixed Box Camera with Edge AI Video Analytics and log in to its web page.V
4. On the HTTP System Settings page, configure an HTTP server (HTTP1 or HTTP2) with:
   - the IP address of the PTZ camera
   - the user name and password for a PTZ camera user assigned the Admin or Expert role

   Click **Save**.
5. On the Alarm page, configure a video analytics alarm to trigger the HTTP action.
   a. For a video analytics alarm, click the edit icon . Then, click **Next** twice to see the Action screen.
   b. Enable Send HTTP Notification.
   c. Select the HTTP server you configured with the IP address of the PTZ camera (HTTP1 or HTTP2).
   d. Select **Handoff**.
   e. Click **Get Preset List**.
   f. Select the preset you defined on the <%TARGETTITLE%>.

The following image shows the HTTP action enabled, the HTTP1 server selected, and preset 2 selected.



g. Click **Done**.

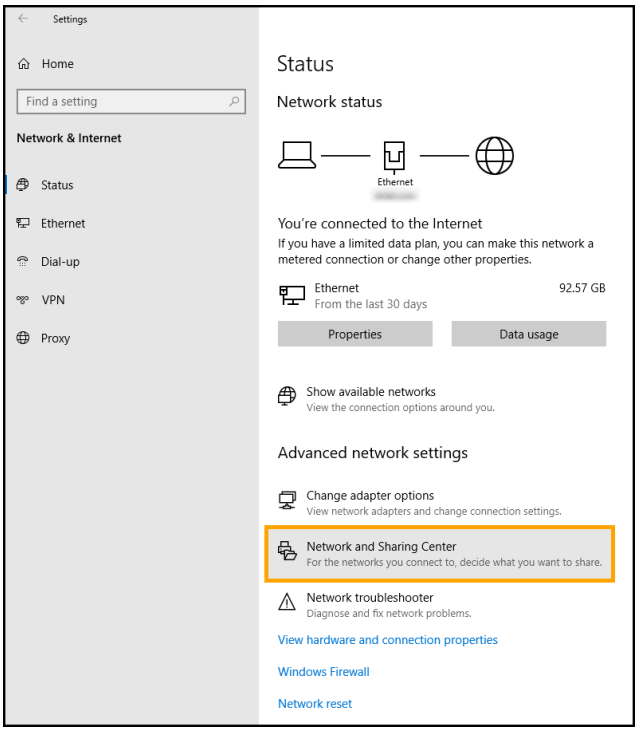
7.3 Install UPnP Components

Windows PCs can discover the camera on the network when network discovery is enabled, and the UPnP (Universal Plug and Play) Device Host service is running.

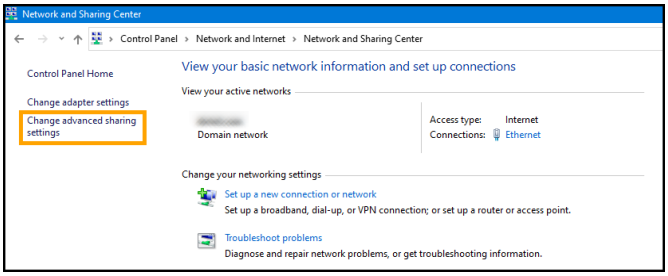
To enable network discovery:

1. Using an Administrator account, log in to Windows.
2. Open the Windows Network and Sharing Center.

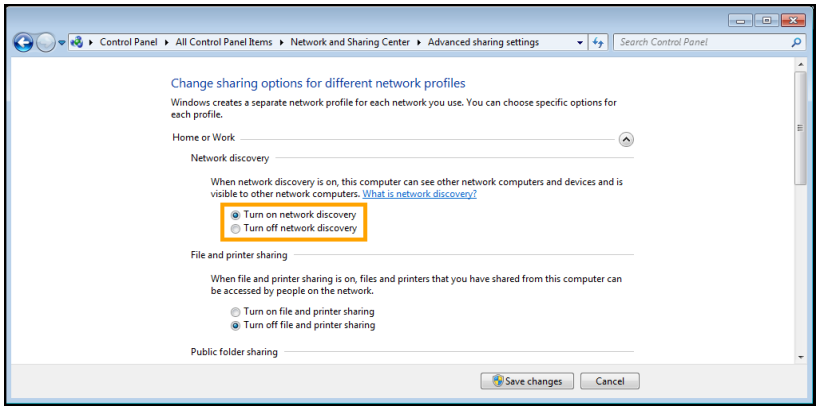
   In Windows 10, you can click **Start** **> Settings.** Then, click **Network & Internet**. In the Advanced network settings section, click **Network and Sharing Center**.



3. Click **Change advanced sharing settings**.



4. Expand the Home or Work section. Then, under **Network discovery**, select **Turn on network discovery**.



5. Click **Save Changes**.

Note

Network discovery requires that the DNS Client, Function Discovery Resource Publication, SSDP Discovery, and UPnP Device Host services are started, that network discovery is allowed to communicate through Windows Firewall, and that other firewalls are not interfering with network discovery.

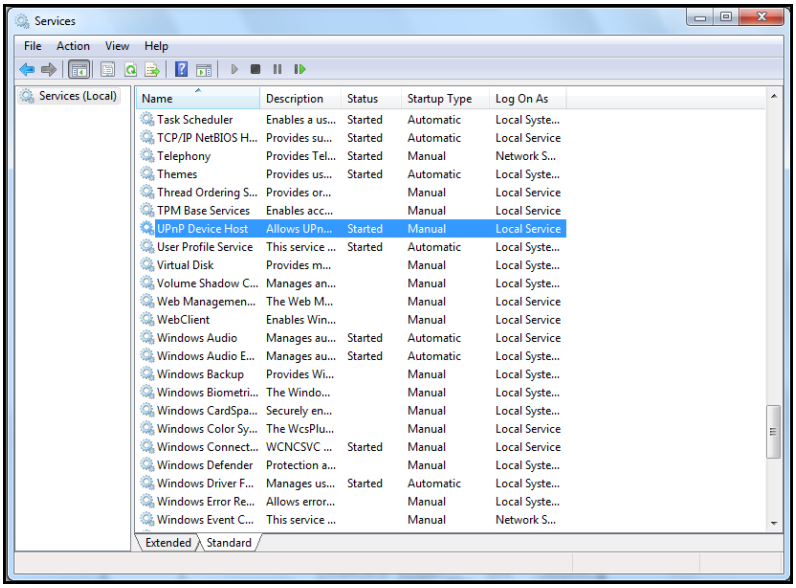
To check that the UPnP Device Host services are running:

1. Run the Windows *Services* app.

   In Windows 10, you can click **Start** ; search for *services*; and then click *Services* app 

.

2. Scroll down the list to *UPnP Device Host* and verify that the status is *Started*.



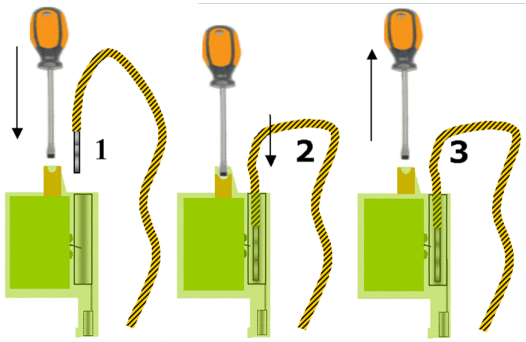
If the status is not *Started*, right-click and select *Start*.

7.4 Connecting Leads to a Spring Clamp Terminal Block

The camera kit includes a 14-pin connector with spring clamps for I/O connections. Use the instructions below and the pin assignment information in Connect the Camera to attach the wires from alarm, audio, and other I/O devices to the connector. Then, attach the connector to the 14-pin I/O terminal block on the camera.

To connect a wire to the spring clamp:

1. Strip the insulation from the end of each wire that is to be connected to the spring clamp. Approximately 1 cm (2.54”) of wire should be exposed.
2. With a small screwdriver, press in and hold the orange spring clamp button next to the female outlet where the wire will be inserted.
3. Insert the stripped end of the wire into the female outlet.
4. Release the orange spring clamp button.



Connecting a Wire to a Spring Clamp

7.5 Troubleshooting

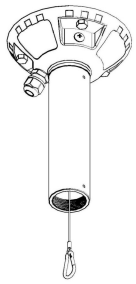
This section provides useful information and remedies for common situations.

Problem	Possible Solution
No network connection	**Hardware issues:** • Check that the network is working and the unit is powered on. • Check that the network (Ethernet) cable is properly attached to the unit. • Confirm that the network cables are not damaged and replace if necessary. **IP address issues:** • Change the default IP address/addresses of the unit. • From the PC running the web browser, ping the unit IP address and confirm that it can be reached. • Confirm that the network settings/firewalls are set according to the requirements. • The camera might be located on a different subnet. Contact your IT administrator to get the IP address of the camera.
How do I find the IP address of my unit?	• Check the network DHCP server IP address assignments and lease. • Alternatively, move the camera to an isolated network and make sure camera gets DHCP address and is accessible. Move the camera back to the network and test it. If you still have issues, reset the camera physically by pressing the reset button on the rear of the camera and test the camera again. This will ensure the camera releases the IP address.
The IP address responds to a ping on the network from the workstation but does not show in the Discovery List	• Disconnect the Ethernet cable from the camera's RJ-45 connector or turn the unit off. Then, ping the IP address again. If the IP address responds, there is another device using the IP address. Consult with your network administrator to resolve the conflict. • Check the network port and ensure that it is working OK. • Ensure that the switch ports provide the necessary power.
The unit IP address is in use by another computer (collision)	• Check the DHCP settings. Obtain a new IP address using DHCP. Ensure this is a unique IP address. • Alternatively, change the unit IP address after connecting to it directly (not through the system network).
Cannot log in to the camera	• Check the login user ID of the user or admin. • Check the login password of the user or admin.

Problem	Possible Solution
No video image displayed on the camera's web page	• Reset the browser security settings to the default value. • Check that the correct port was configured. The default port is 554.
Poor video quality	• Check that the network cable is connected securely. • Check that the camera settings are correct on the camera and in the unit. • Check that the camera lens is clean and unobstructed. • Check that the cable length is within specification.
Streaming video image is hanging (stopped)	• Confirm the unit's video streaming settings. • Refresh your browser screen (F5). • Check that the bandwidth and bit rate settings of the network are set properly. • Check that other processes and applications are not causing undue latency. • Check that the firewall analysis or blocking is not interfering with the video stream and supports the required ports and communication protocols.
Bluish picture in an indoor scene (possibly mixing indoor and outdoor lighting)	Change the white balance setting to *Auto*. If the lighting in the scene is fixed, manually adjust the white balance to an acceptable image.
Reddish picture and incorrect colors in the image	Check the PoE power supply and associated network cables. Connect directly to the PoE and compare the images. If the problem persists, contact Support.
IR LEDs do not function	The camera has a circuit protection mechanism that activates if the cover is removed while the IR LEDs are on. • Power cycle the camera.

7.6 Mounting Accessories

Teledyne FLIR offers the following mounting accessories for the CP-6402-31-PA pendant and CP-640x-x1-IA IR PTZ cameras:

Part number / item code	Description	Images (not to scale)
CX-XTND-G3	Extendable gooseneck mount kit with cable box and wall mount plate (1.5" PF inner thread)	
CX-GSNK-G32	Gooseneck mount kit, including base plate and pipe (1.5" PF inner thread) • Can use with CX-GSNK-G32-B mounting bracket	
CX-DRP-G32-B	Ceiling mount kit, including base and 20cm drop-down pipe (1.5" PF inner thread) • Can use with CX-PIPE-G325 50 cm extension pipe	
CX-ARMX-G3	Wall mount bracket (1.5" PF inner thread) • Can use with CX-CRNR-G3 corner mount and CX-POLE-G3 pole mount kits	
CX-ELBX-G3	Wall mount bracket (1.5" PF inner thread) with IP66 electrical box enclosure • Can use with CX-CRNR-G3 corner mount and CX-POLE-G3 pole mount kits	
CX-GSNK-G3	Gooseneck mount (1.5" PF inner thread) with IP66 electrical box enclosure • Attaches directly to a wall • Can use with CX-CRNR-G3 corner mount and CX-POLE-G3 pole mount kits	

For more information about accessories, including specifications such as dimensions and weights, see the *FLIR Security Edge Devices Accessory Guide*, contact your Teledyne FLIR sales representative, or visit https://support.flir.com/ to request details on where to get the accessory.