Quasar™ Gen IV

Installation and User Guide

4K IR PTZ Camera

CP-6408-21-I

For additional information visit www.flir.com or write to FLIR Systems, Inc.

FLIR Systems, Inc.
6769 Hollister Avenue
Goleta, CA 93117

Support: https://www.flir.com/support/.

Important Instructions and Notices to the User:

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

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

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

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

Industry Canada Notice:
This Class A digital apparatus complies with Canadian ICES-003.

Avis d'Industrie Canada:
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Proper Disposal of Electrical and Electronic Equipment (EEE)

The European Union (EU) has enacted Waste Electrical and Electronic Equipment Directive 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

Document History

Revision	Date	Comment
100	February 2020	V1.6.0.16 - Initial FLIR release

Product Registration and Limited Warranty (Extended)

By registering your Product with FLIR at https://customer.flir.com within ninety (90) days from the date the Product was delivered, you will be entitled to an Extended Limited Warranty. Obtaining an Extended Limited Warranty requires product registration. For more information, refer to the FLIR Security Limited Warranty policy.

Table of Contents

Table of Contents

1 Document Scope and Purpose

The purpose of this document is to provide installation, operation, and configuration instructions for the Quasar CP-6408-21-I camera.

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.

Remarque:

Ce document est destiné aux utilisateurs techniciens qui possèdent des connaissances de base des équipements vidéo/caméras de télésurveillance et des connexions aux réseaux LAN/WAN.

Warning:

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

Avertissement:

L'installation doit respecter les consignes de sécurité, les normes et les codes électriques, ainsi que la législation en vigueur sur le lieu d'implantation des unités.

Disclaimer

Users of 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.

FLIR Systems, Inc. and its agents make no guarantees or warranties to the suitability for the users' intended use. FLIR Systems, Inc. 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 FLIR and its agents from any resulting liability.

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

Avis de non-responsabilité

Il incombe aux utilisateurs des produits FLIR de vérifier que ces produits sont adaptés et d'étudier le rôle des capacités et limites de détection du produit appliqués aux exigences uniques de leur site.

FLIR Systems, Inc. et ses agents ne garantissent d'aucune façon que les produits sont adaptés à l'usage auquel l'utilisateur les destine. FLIR Systems, Inc. ne pourra être tenu pour responsable en cas de mauvaise utilisation ou de mise en place de mesures de sécurité insuffisantes.

Le non respect de tout ou partie des procédures recommandées ou des messages d'AVERTISSEMENT ou d'ATTENTION de la part de l'installateur, du propriétaire ou de l'utilisateur dégagera FLIR Systems, Inc. et ses agents de toute responsabilité en résultant.

Les spécifications et informations contenues dans ce guide sont sujettes à modification sans préavis.

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:

Précautions et avertissements d'ordre général

Cette section contient des informations indiquant qu'une procédure ou condition présente des risques potentiels.

CONSERVEZ TOUTES LES INSTRUCTIONS DE SÉCURITÉ ET D'UTILISATION POUR POUVOIR VOUS Y RÉFÉRER ULTÉRIEUREMENT.

Bien que l'unité soit conçue et fabriquée conformément à toutes les normes de sécurité en vigueur, l'installation de cet équipement présente certains risques.

Afin de garantir la sécurité et de réduire les risques de blessure ou de dommages, veuillez respecter les consignes suivantes:

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.

Attention:

- *Le cache de l'unité est une partie essentielle du produit. Ne les ouvrez et ne les retirez pas.*
- *N'utilisez jamais l'unité sans que le cache soit en place. L'utilisation de l'unité sans cache présente un risque d'incendie et de choc électrique.*
- *Ne démontez pas l'unité et ne retirez pas ses vis. Aucune pièce se trouvant à l'intérieur de l'unité ne nécessite un entretien par l'utilisateur.*
- *Seul un technicien formé et qualifié est autorisé à entretenir et à réparer cet équipement.*
- *Respectez les codes et réglementations locaux, et assurez-vous que l'installation et l'utilisation sont conformes aux normes contre l'incendie et de sécurité.*

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

***Avertissement** est un message préventif indiquant qu'une procédure ou condition présente un risque potentiel de blessure ou de mort.*

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.

***Attention** est un message préventif indiquant qu'une procédure ou condition présente un risque potentiel de dommages permanents pour l'équipement et/ou de perte de données.*

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

*Une **Remarque** est une information utile permettant d'éviter certains problèmes, d'effectuer une installation correcte ou de mieux comprendre les produits et l'installation.*

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

*Un **Conseil** correspond à une information et aux bonnes pratiques utiles ou apportant un avantage supplémentaire pour l'installation et l'utilisation des produits FLIR.*

2 Camera Overview

The CP-6408-21-I camera includes a 4K visible light camera with 22x optical zoom; audio; digital I/O; near-infrared (NIR) illumination; and automatic side heat sensors. 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. The server uses an open, standards-based communication protocol to communicate with FLIR and third-party video management system (VMS) clients, including systems that are compatible with ONVIF®. These clients can be used to control the camera and stream video during day-to-day operations. For a list of supported VMS clients, refer to the product's web page on FLIR.com.

If help is needed during the installation process, contact the local 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 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.

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.

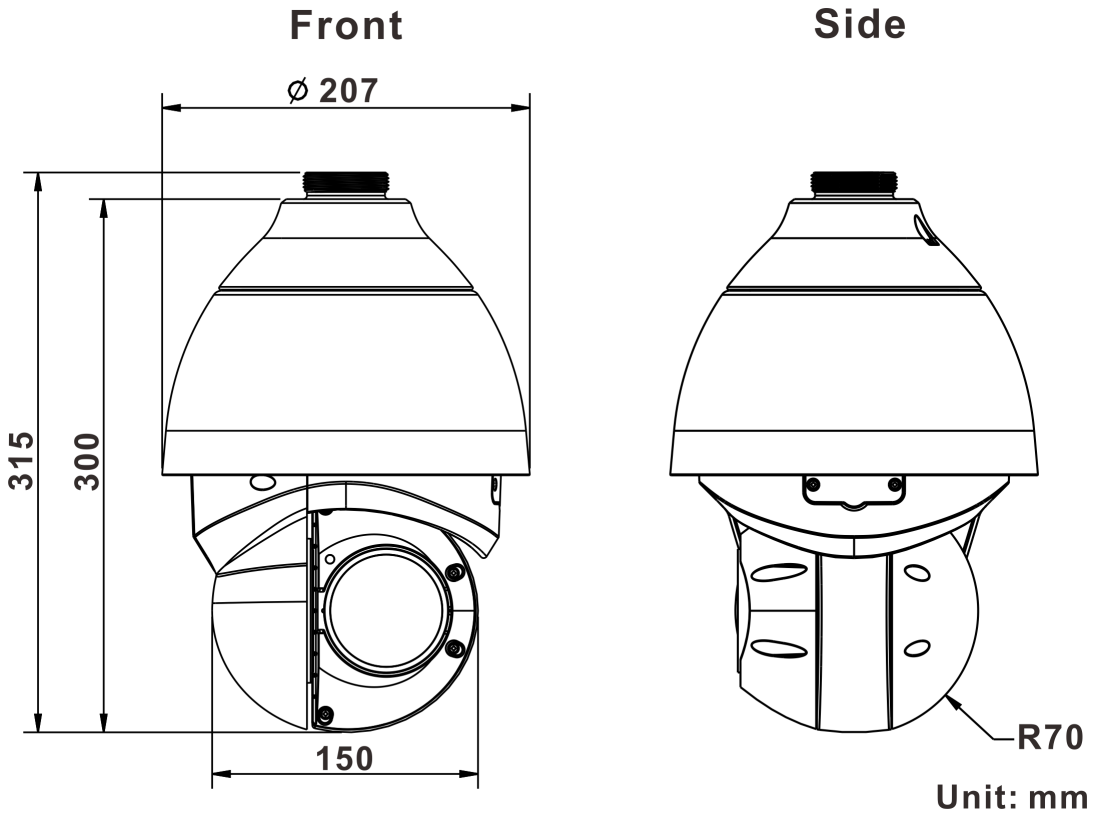
Caution

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.
Be careful not to leave fingerprints on the camera's infrared optics.
Operating the camera outside of the specified input voltage range or the specified operating temperature range can cause permanent damage.

Related Documentation

- *CP-6408-21-I Quick Install Guide*
- *FLIR CGI Interface Description 2.1*
- *Nexus CGI WebSockets Manual*
- *FLIR Sensors SDK Programmer's Guide*
- *FLIR Cloud API Documentation*

2.1 Camera Dimensions



3 Installation

This camera can be installed outdoors or indoors.

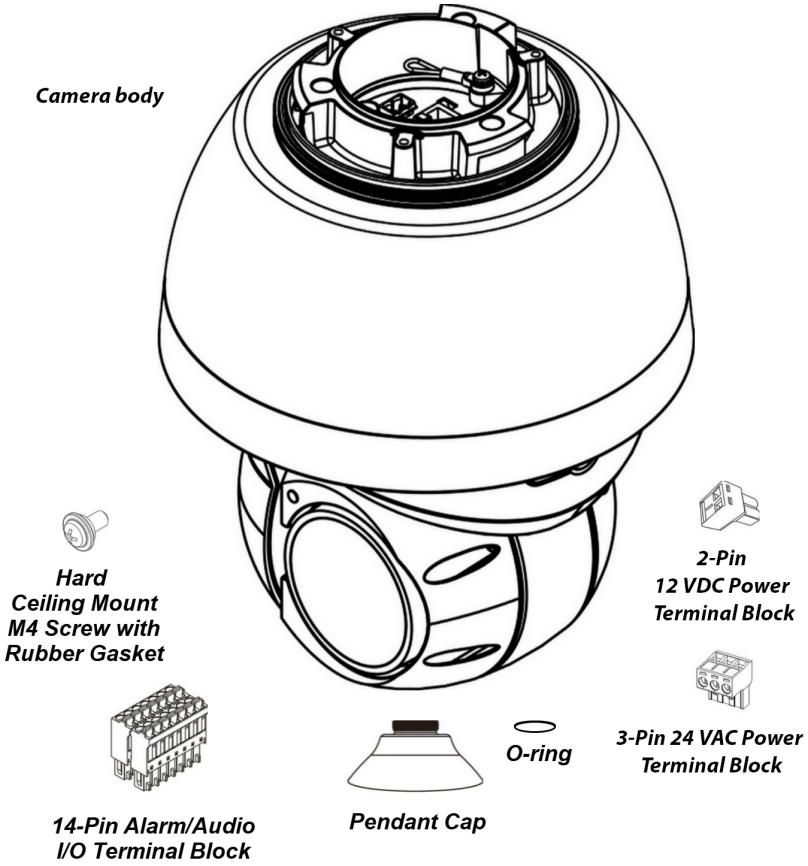
For outdoor installation, FLIR recommends:

- Always using weatherproof equipment, such as boxes, receptacles, connectors, etc.
- For electrical wiring, using the properly rated sheathed cables for conditions to which the cable will be exposed (for example, moisture, heat, UV, physical requirements, etc.).
- Planning ahead to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.
- Using best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, etc.

All electrical work must be performed in accordance with local regulatory requirements.

3.1 Supplied Components

The CP-6408-21-I camera kit includes these items:



Items Included in Kit

3.2 Site Preparation

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.

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.

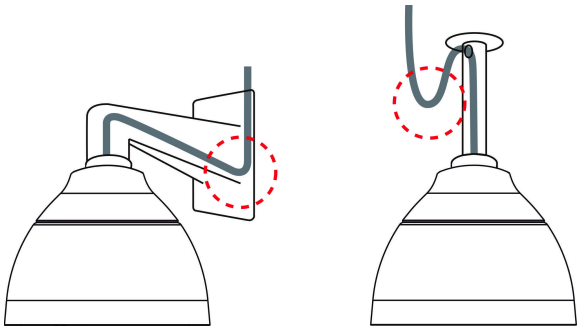
3.3 Waterproofing the Camera Cables

The camera is IP66-rated to prevent water from entering the camera. Nevertheless, water can enter the camera if it is not installed properly. Please make sure the warnings below are strictly followed when installing the camera.

1. Place all cables and the adaptor in dry and well-waterproofed environments, e.g. waterproof boxes. This prevents moisture accumulation inside the camera and moisture penetration into cables.
2. Seal the cable entry hole of the pendant cap with the rubber O-ring (supplied with the camera) and use thread seal tape to keep water from entering the camera.

Waterproofing the Pendant Cap

3. While running cables, slightly bend the cables in a U-shaped curve to create a low point. This prevents water from entering the camera along the cables from above.



U-Shaped Cable Installation

3.4 Mounting the Camera

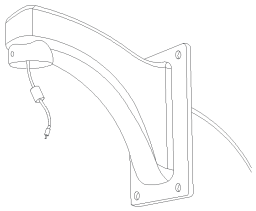
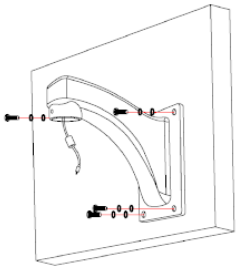
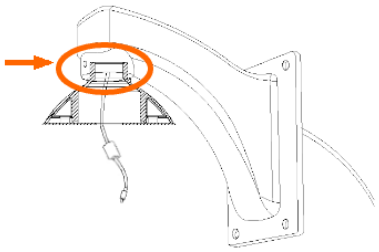
The following accessories and adapters are available for mounting the camera:

- Wall Mount Bracket CX-ARMX-G3
- Wall Mount Bracket with Power Box CX-ELBX-G3
- Gooseneck Mount with Power Box CX-GSNK-G3
- Corner Adapter CX-CRNR-G3
- Pole Adapter CX-POLE-G3

3.4.1 Wall Mount Bracket CX-ARMX-G3

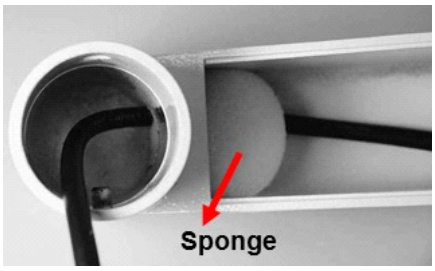
Wall mount bracket (1.5 inch threaded).

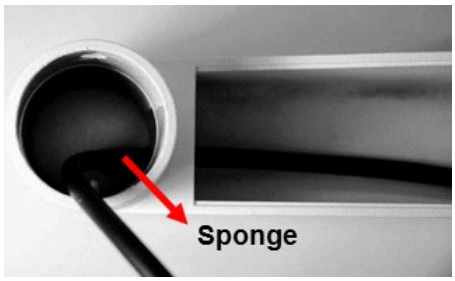
Item	Details	Qty
Wall mount bracket	CX-ARMX-G3	1
Parts package	No. 3 Allen key	1
Quick install guide	Summarized below	1

Step 1	Step 2	Step 3
		
Pull cables through bracket.	Fix bracket on wall.	Assemble pendant cap. Use Allen key and a hex head cap screw to firmly fix the pendant cap to the arm.

Detailed instructions for mounting a camera using the CX-ARMX-G3 wall mount bracket

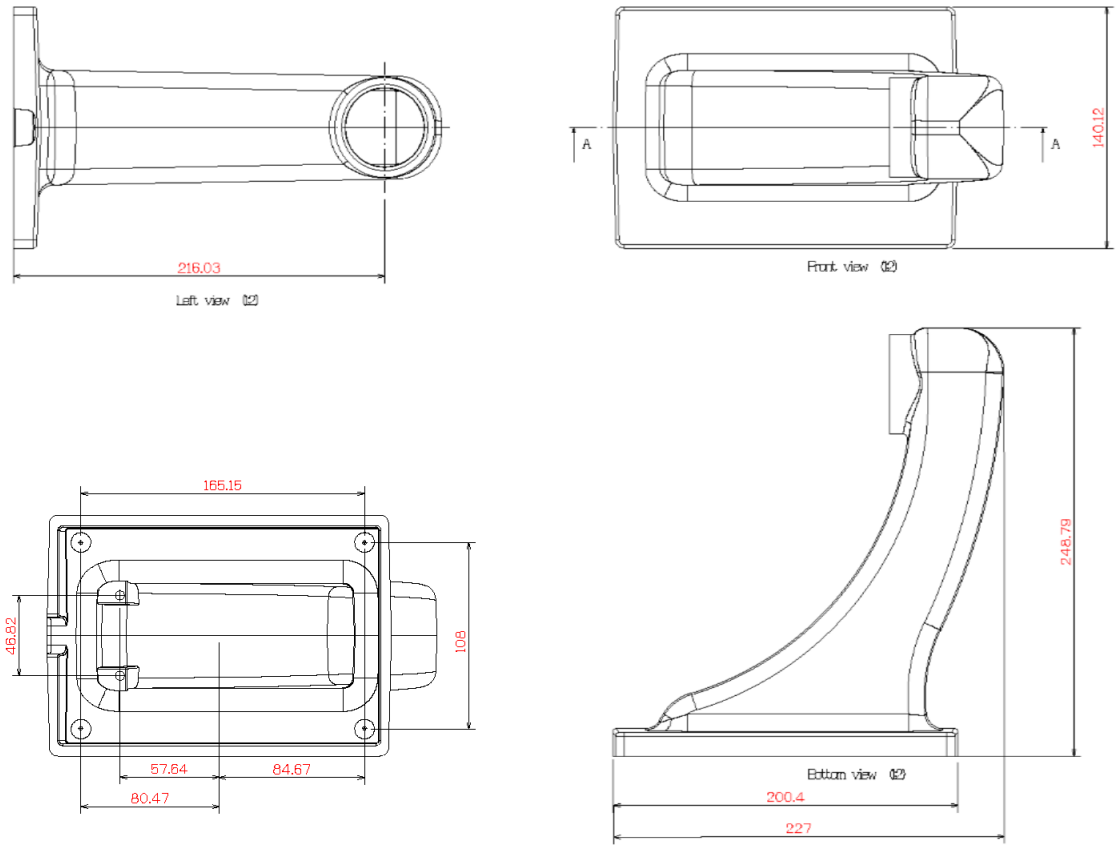
1. Cut a cable access hole in the wall.
2. Attach the wall mount to the wall using the appropriate screws and screw anchors (not provided). For outdoor models, attach the waterproof gasket to the wall mount.
3. Thread the cables through the wall mount.
4. After threading the cables, block the entry hole with the supplied sponge to prevent insects from entering. The sponge can be placed in one of two ways.





5. Thread the cables through the outdoor mount kit and attach the pendant mount kit to the wall mount using the supplied screws and washers.
6. For outdoor cameras, adjust the waterproof gasket to the joint.
7. Connect the cables to the camera (see Camera Connections).
8. Secure the camera to the outdoor mount kit.
9. Ensure the camera is fixed completely, and that the thread holes on the camera's fixing plate and the mount kit are aligned.
10. Screw in the supplied screw and washer.

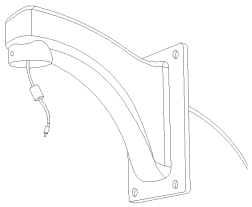
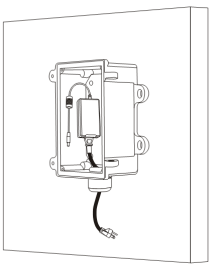
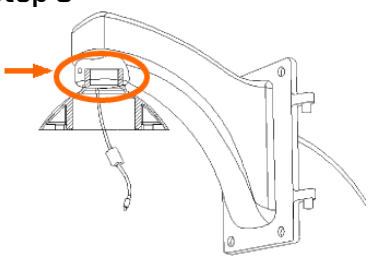
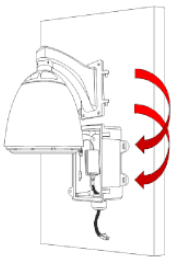
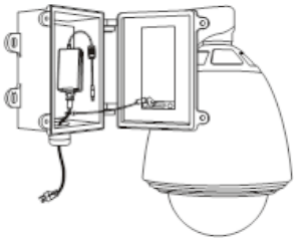
CX-ARMX-G3 dimensions



3.4.2 Wall Mount Bracket with Power Box CX-ELBX-G3

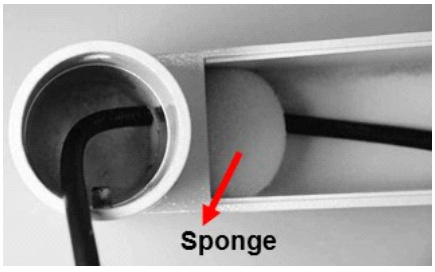
Wall mount bracket (1.5 inch threaded) with IP68 power box.

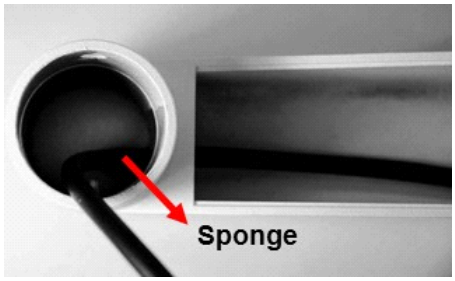
Item	Details	Qty
Wall mount bracket with power box	CX-ELBX-G3	1
Accessory bag	No. 3 Allen key	1
	No. 5 Allen key	1
	Hex head cap screw M6 x 20 (stainless steel)	2
	Cable gland	1
Quick install guide	Summarized below	1

Step 1	Step 2	Step 3
		
Pull cables through the bracket.	Fix the power box to the wall or to the column.	Assemble pendant cap. Use Allen key and a hex head cap screw to firmly fix the pendant cap to the arm.
Step 4	**Step 5**	
		
Have the bracket hooked up to the tenon of the power box.	Buckle up the safety rope, make the camera connections, tighten the two hex screws to seal the box, and then complete assembly.	

Detailed instructions for mounting a camera using the CX-ELBX-G3 wall mount bracket with power box

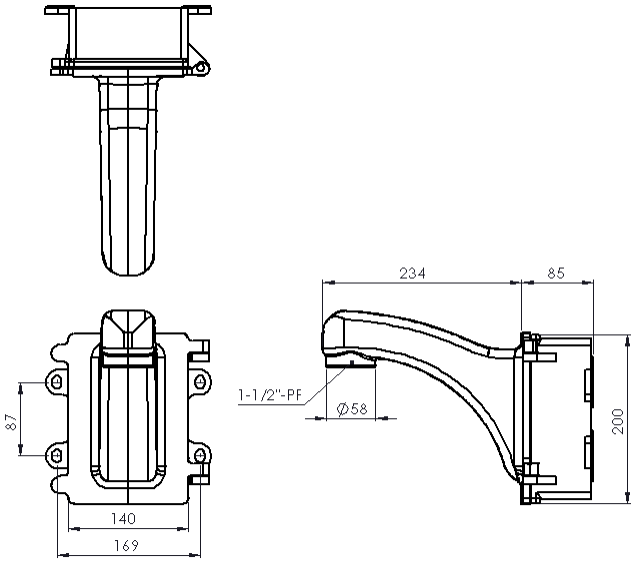
1. Cut a cable access hole in the wall.
2. Attach the CX-ELBX-G3 to the wall using the appropriate screws and screw anchors (not provided).
3. Thread the cables through the wall mount and power box.
4. Attach the wall mount to the power box mount using the supplied screws and washers.
5. Thread the cables through the wall mount with the cables coming out of the pendant mount's outlet. For outdoor cameras, attach the waterproof gasket to the pendant mount.
6. After threading the cables, block the entry hole with the supplied sponge to prevent insects from entering. The sponge can be placed in one of two ways.





7. Thread the cables through the outdoor mount kit and attach the mount kit to the wall mount using the supplied screws and washers.
8. For outdoor cameras, adjust the waterproof gasket to the joint.
9. Connect the cables to the camera. See Camera Connections.
10. Secure the camera to the outdoor mount kit.
11. Ensure the camera is fixed completely, and that the thread holes on the camera's fixing plate and the mount kit are aligned.
12. Screw in the supplied screw and washer.

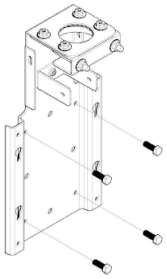
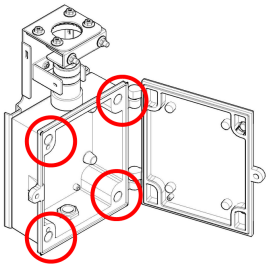
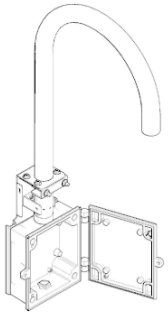
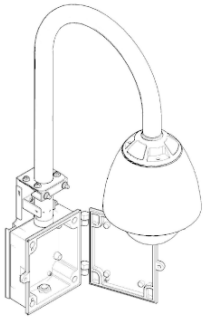
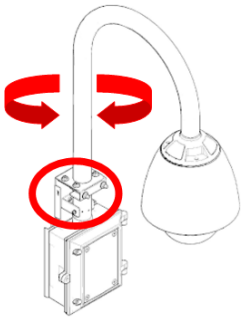
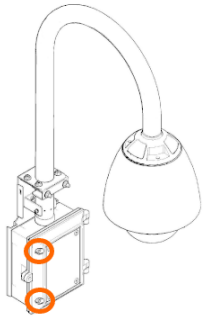
CX-ELBX-G3 dimensions



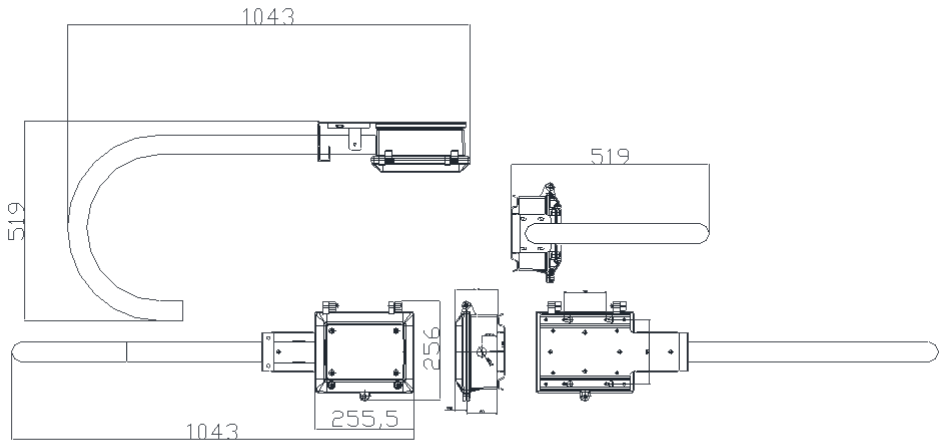
3.4.3 Gooseneck Mount with Power Box CX-GSNK-G3

Gooseneck mount (1.5 inch threaded) with IP68 power box.

Item	Details	Qty
Gooseneck bracket and power box	CX-GSNK-G3 box	1
	CX-GSNK-G3 gooseneck pipe	1
Accessory box	No. 2 Allen key	1
	No. 3 Allen key	1
	No. 5 Allen key	1
	No. 6 Allen key	1
	M4x8 hex cap double washer	2
Quick install guide	Summarized below	1

Step 1	Step 2	Step 3
		
Fix backplate on mounting surface.	Assemble power box and tighten screws with No. 6 Allen key.	Assemble gooseneck pipe on backplate and power box.
Step 4	**Step 5**	**Step 6**
		
Attach pendant cap to gooseneck pipe, complete cable connections, and connect camera to pendant cap.	Rotate gooseneck pipe to the position required. Tighten hexagon nuts to the flange and use No. 3 Allen key to tighten M4x8 hex socket screws.	Use No. 6 Allen key to fix cover screws.

CX-GSNK-G3 dimensions



3.4.4 Mount Adapters

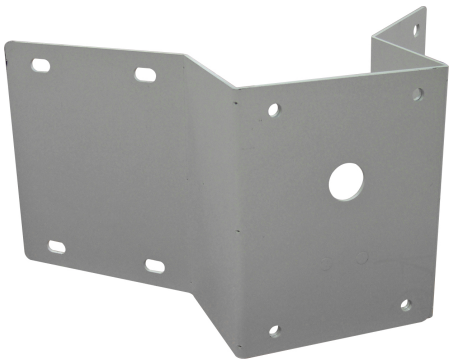
The following mount adapters are available for the camera:

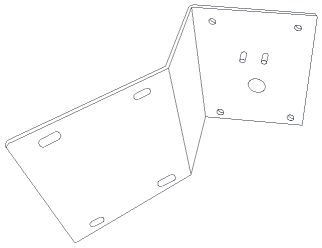
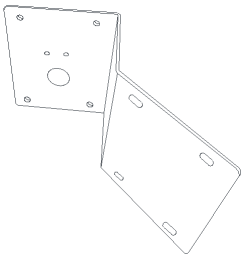
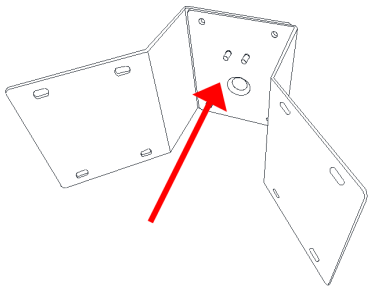
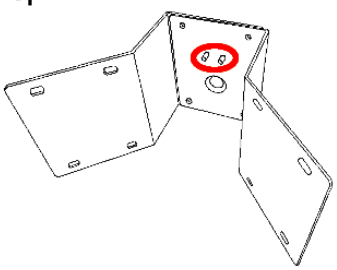
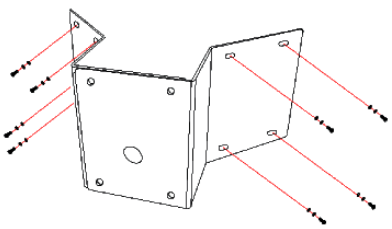
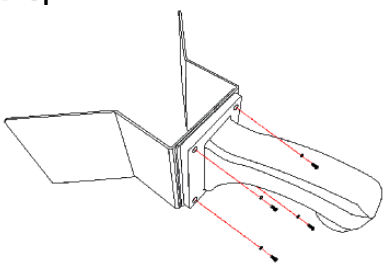
- Corner Adapter CX-CRNR-G3
- Pole Adapter CX-POLE-G3

3.4.4.1 Corner Adapter CX-CRNR-G3

90-degree exterior angle corner adapter for CX-xxxx-G3 mounts.

Item	Details	Qty
Corner mount bracket	CX-CRNR-G3	1
Accessory bag	Stainless steel truss head screw M8*25	4
	Stainless steel truss head screw M8*30	4
	M8 washer	6
	M8 screw nut	6
	M8 spring washer	6
Quick install guide	Summarized below	1

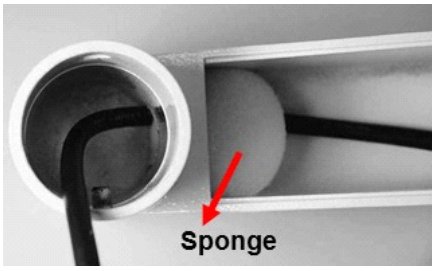


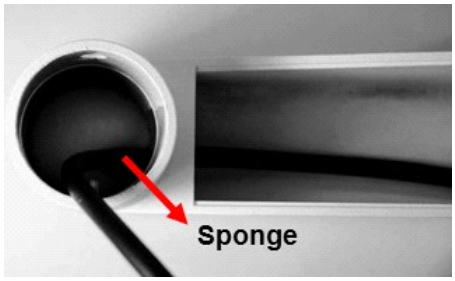
		**Step 1** 
Part 1	Part 2	Join parts 1 and 2 together.
Step 2 	**Step 3** 	**Step 4** 
Tighten hex head cap screws (clockwise).	Fix assembled corner bracket to the wall.	Fix arm (pictured) or power box to the corner bracket with washer in the front and screw nuts at the back.

Detailed instructions for mounting a camera using the CX-CRNR-G3 corner adapter with the CX-ARMX-G3 wall mount bracket

1. Cut a cable access hole in the wall.

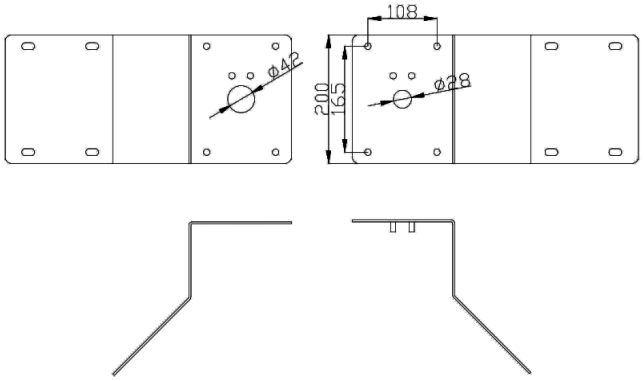
2. Attach the assembled corner bracket to the wall using the appropriate screws and screw anchors (not provided).
3. Thread the cables through the corner mounting plate.
4. Attach the wall mount to the corner mount using the supplied screws and washers.
5. Thread the cables through the wall mount with the cables coming out of the pendant mount's outlet. For outdoor cameras, attach the waterproof gasket to the pendant mount.
6. After threading the cables, block the entry hole with the supplied sponge to prevent insects from entering. The sponge can be placed in one of two ways.





7. Thread the cables through the outdoor mount kit and attach the mount kit to the wall mount using the supplied screws and washers.
8. For outdoor cameras, adjust the waterproof gasket to the joint.
9. Connect the cables to the camera. See Camera Connections.
10. Secure the camera to the outdoor mount kit.

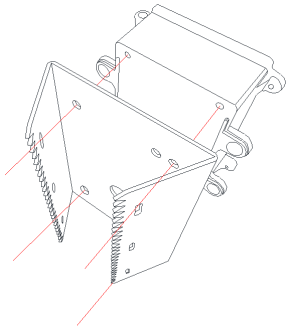
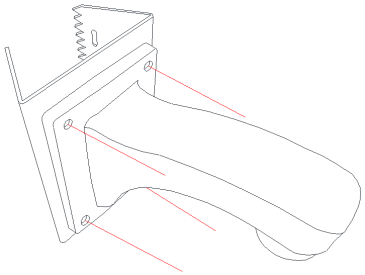
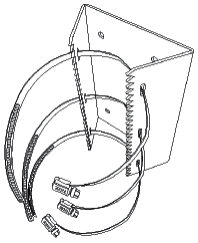
CX-CRNR-G3 dimensions

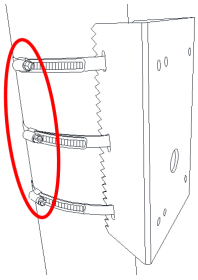


3.4.4.2 Pole Adapter CX-POLE-G3

Pole adapter for CX-xxxx-G3 mounts, including 2.5-8.5 inch straps.

Item	Details	Qty
Pole mount bracket	CX-POLE-G3	1
	8.5" ring	3
Accessory bag	Stainless streel truss head screw M8*20	4
	Stainless steel truss head screw M8*30	4
	M8 washer	4
	M8 screw nut	4
	M8 spring washer	4
Quick install guide	Summarized below	1

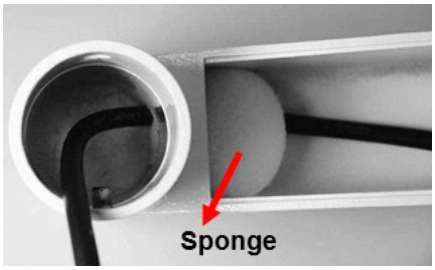
Step 1		Step 2
		
For installation with CX-ELBX-G3 wall mount bracket with power box or CX-GSNK-G3 gooseneck mount with power box, screw power box onto CX-POLE-G3.	For installation with CX-ARMX-G3 wall mount bracket, screw wall mount bracket onto CX-POLE-G3.	Thread the hoops through the CX-POLE-G3.

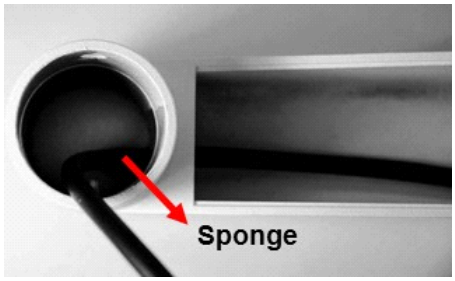
Step 3

Fasten hoops tightly with flat-head screwdriver.

Detailed instructions for mounting a camera using the CX-POLE-G3 pole adapter with the CX-ARMX-G3 wall mount bracket

1. Fasten the CX-POLE-G3 pole adapter to a pole with the supplied stainless straps, as described above.
2. Thread the cables through the pole adapter.

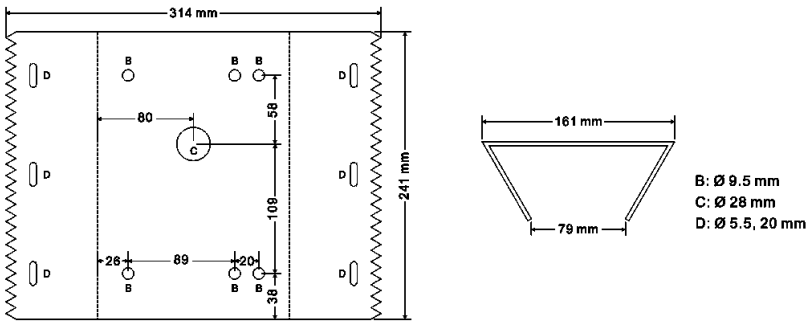
3. Attach the wall mount bracket to the pole adapter using the supplied screws and washers.
4. Thread the cables through the wall mount bracket with the cables coming out of the pendant mount's outlet. For outdoor cameras, attach the waterproof gasket to the pendant mount.
5. After threading the cables, block the entry hole with the supplied sponge to prevent insects from entering. The sponge can be placed in one of two ways.



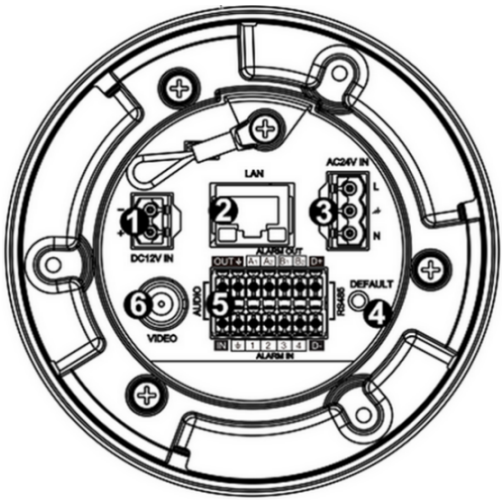


6. Thread the cables through the outdoor mount kit and attach the mount kit to the wall mount using the supplied screws and washers.
7. For outdoor cameras, adjust the waterproof gasket to the joint.
8. Connect the cables to the camera.
9. Secure the camera to the outdoor mount kit.
10. Ensure the camera is fixed completely, and that the thread holes on the camera's fixing plate and the mount kit are aligned.
11. Screw in the supplied screw and washer.

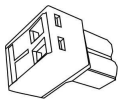
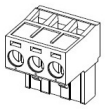
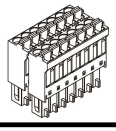
CX-POLE-G3 dimensions

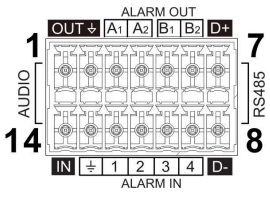


3.5 Camera Connections

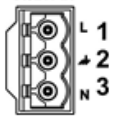


Connectors

Connector		Connection	
1	DC12V IN	If using a 12 VDC power supply, connect its wires to the two-pin terminal block. See pin assignment below. ⚠ Do not use the DC12V IN and AC24V IN connectors at the same time.	
2	LAN	Attach a Cat 5e or Cat 6 cable from the network switch to the RJ45 connector for a 10/100/1000 Mbps Ethernet and Power over Ethernet (PoE) connection. For information about using PoE, see Conecting Power to the Camera. Verify that the LAN connector LEDs are steady green and flashing yellow.	
3	AC24V IN	If using a 24 VAC power supply, connect its wires to the three-pin power terminal block. See pin assignment below. ⚠ Do not use the DC12V IN and AC24V IN connectors at the same time.	
4	DEFAULT	To reset factory defaults at any time, press the Default button for at least 20 seconds.	
5	14-pin terminal block	Attach wires from external devices to the 14-pin terminal block connector for alarm and audio in/out (see diagram and definitions below).	
6	VIDEO	BNC connector for analog video output.	

14-Pin Terminal Block	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

DC12V IN Connector	Pin	Definition
	1	-12 VDC
	2	+24 VDC

AC24V IN Connector	Pin	Definition
	1	AC 24L
	2	Ground
	3	AC 24N

Note

The camera features zero downtime (ZDT) power switching. When the DC12V IN and PoE connections are both used, the camera draws power through the DC connection. If DC power fails, the camera switches power to the PoE connection until the DC power source is restored.

Warning

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.

3.6 Connecting Power to the Camera

Power can be supplied to the camera with PoE or an external 12 VDC or 24 VAC power supply (not included in the camera kit).

- If using PoE, make sure the PoE switch or injector is a Power Sourcing Equipment (PSE) device.
- If using a PoE-capable network switch, the switch needs to support Universal PoE 4 pair forced mode. For information regarding recommended switches, contact FLIR Support. **Note:** The camera does not support CDP/LLDP.
- If using a PoE-capable injector, use an injector FLIR recommends. Contact FLIR Support.
- If using an external AC or DC power supply, connect the power supply's wires to the appropriate power terminal block.

Warnings

- Make sure the camera's power cable is properly connected. All electrical work must be performed in accordance with local regulatory requirements.
- Use a UL Listed Power Adapter that meets LPS (Limited Power Source) requirements.
- Note the camera's power consumption (12 VDC):

Mode	Current
Idle	0.7021A
Motor + camera on	0.8821A
Cold start only heater (camera off)	1.3423A
IR LED + camera on	1.8023A
IR LED + camera on + motor	2.1512A
IR + heater + camera on	2.6213A
IR + heater + motor + camera on	3.3121A

A PoE injector should be connected only to a PoE network inside a building and not routed outside the building.

- If the camera is installed outdoors with an external power supply, the power supply must be installed with proper weatherproofing.
- A qualified service person should install the camera.

3.7 Initial Configuration

To configure the camera for the first time, do the following:

- Configure for Networking
- Configure Video Format
- Attach the Camera to a VMS

3.7.1 Configure for Networking

By default, DHCP is enabled on the camera and a DHCP server on the network assigns the camera an IP address. If there is no DHCP server on the network, the IP address defaults to 192.168.0.250.

To manually specify a different IP address for the camera or to configure other networking settings, you can use either the FLIR Discovery Network Assistant (DNA) tool or the camera's web page.

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

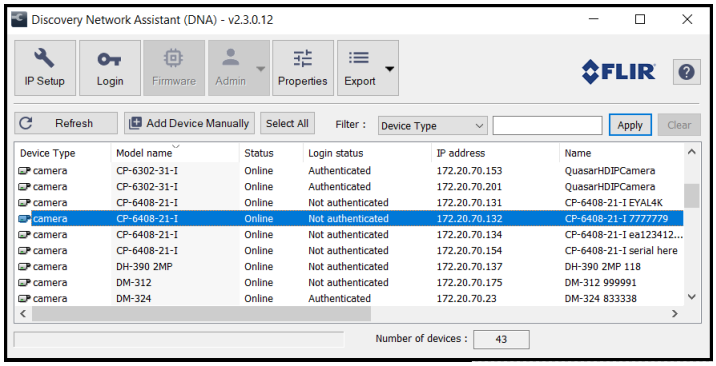
Note

The DNA tool does not require a license to use and is a free download from the product's web page on FLIR.com. For more information about using the DNA tool, including how to configure more than one camera at the same time, see the *DNA User Guide*. While the software is open, click the Help icon .

Make sure the camera and the PC are on the same network.

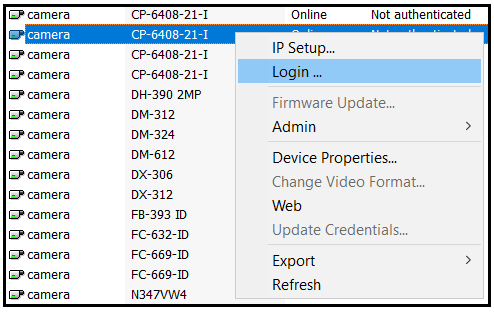
To configure the camera for networking using the DNA tool:

1. Run the DNA tool (DNA.exe) by double-clicking . The Discover List appears, showing compatible devices on the VLAN and their current IP addresses.

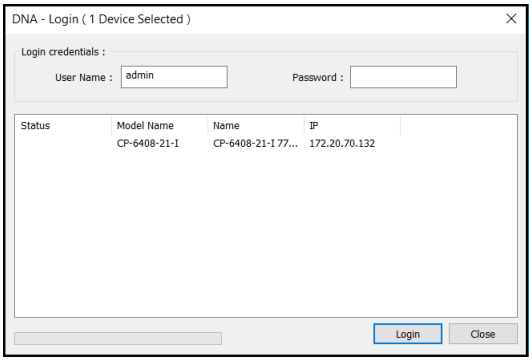


2. Authenticate the camera.

Right-click the camera and select **Login**, or click the **Login** icon in the navigation bar.



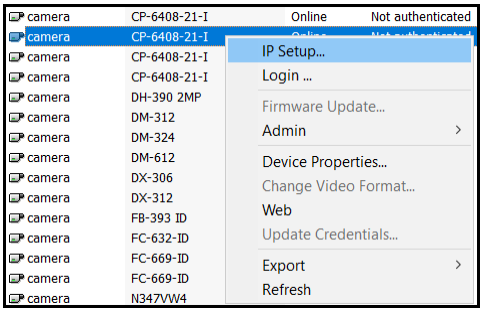
In the **DNA - Login** window, type the password for the admin user (default: *admin*). Then, click **Login**.



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

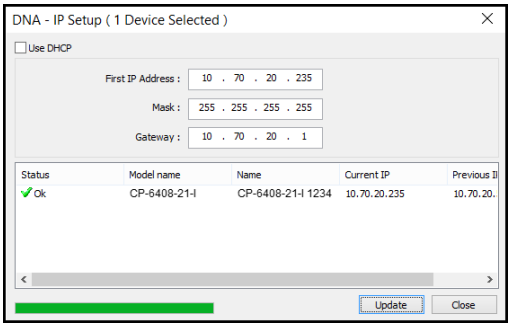
3. Configure the camera's networking settings.

Right-click the camera and select **IP Setup**, or click the **IP Setup** icon in the navigation bar.



In the **DNA - IP Setup** window, you can clear *Use DHCP* and manually specify the camera's *IP address*, *Mask*, and *Gateway*.

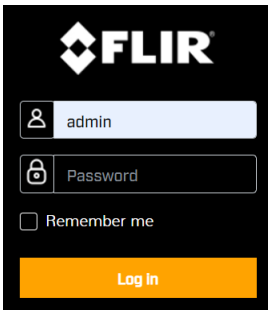
Then, click **Update** and wait for ✔ Ok status to appear.



To configure the camera for networking using the camera's web page:

1. Open the camera's web page either by double-clicking the camera in the DNA Discover List or by typing the camera's IP address in a web browser's address bar. The camera's web page supports the latest versions of popular web browsers.

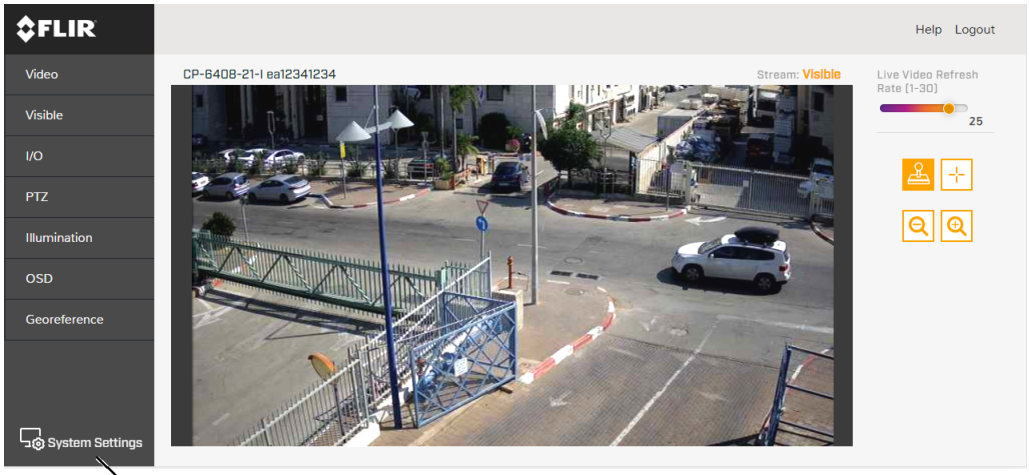
2. On the login screen, type *admin* for the user name and the password for the admin user (default: *admin*).



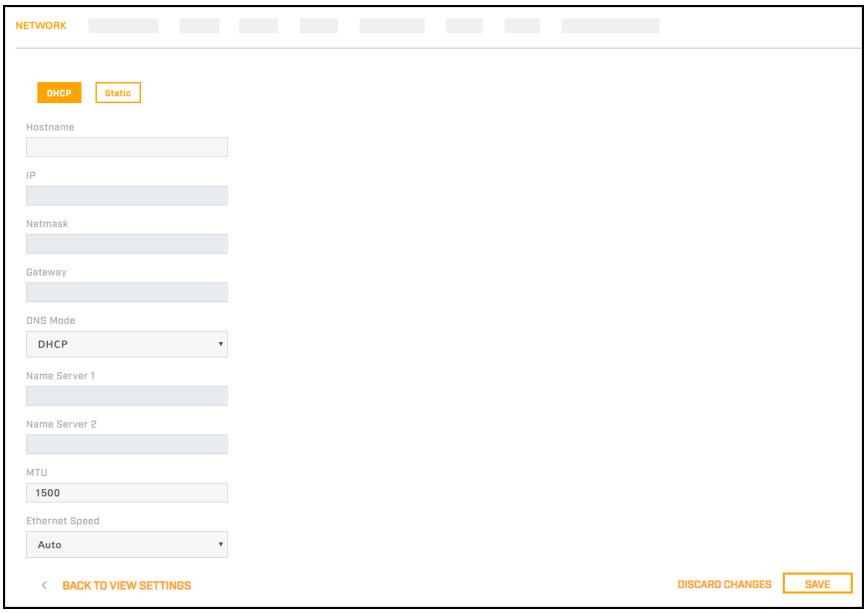
When logging in to the camera for the first time or for the first time after performing a factory default, specify a new password for the admin user. Use a strong password consisting of at least 12 characters and at least one uppercase letter, one lowercase letter, and one number. Passwords can include the following special characters: |@#~!$&<>+_-.,*?= .

Log back in with the new password.

The camera's View Settings Home Page opens.



3. Click **System Settings**, and make sure the Network page appears.



4. You can click *Static* IP addressing and manually specify the camera's *IP address*, *Netmask*, and *Gateway*. You can also specify the *DNS Mode*, *Name Servers*, *MTU* (maximum transmission unit), and *Ethernet Speed*.

   For more information about these settings, see Network Page.

5. Click **Save**. If you have made any changes on the Network page, the camera reboots.

3.7.2 Configure the Video Format

To configure the camera's video format (PAL or NTSC), do one of the following (both require being logged in to the camera):

- Using the DNA tool, select the device in the DNA Discover list, right-click, and select **Change Video Format**. Click **Update**.

- Using the camera's web page, open the Visible page; click **Advanced Settings**; and scroll down to Video Format. Click **Save**.

3.7.3 Attach the Camera to a VMS

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

4 Operation

This chapter includes information about how to access the camera and how to operate it using the View Settings page.

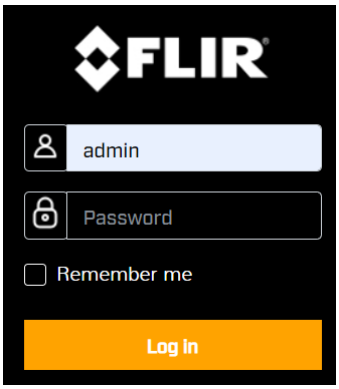
4.1 Accessing the Camera

To operate the camera, you first need to access it. You can access the camera by logging in to the camera's web page.

To log in to the camera's web page:

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

     The DNA tool does not require a license to use and is a free download from the product's web page on FLIR.com. 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, type a user name and the password.

   When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, type admin for the user name and for the password.

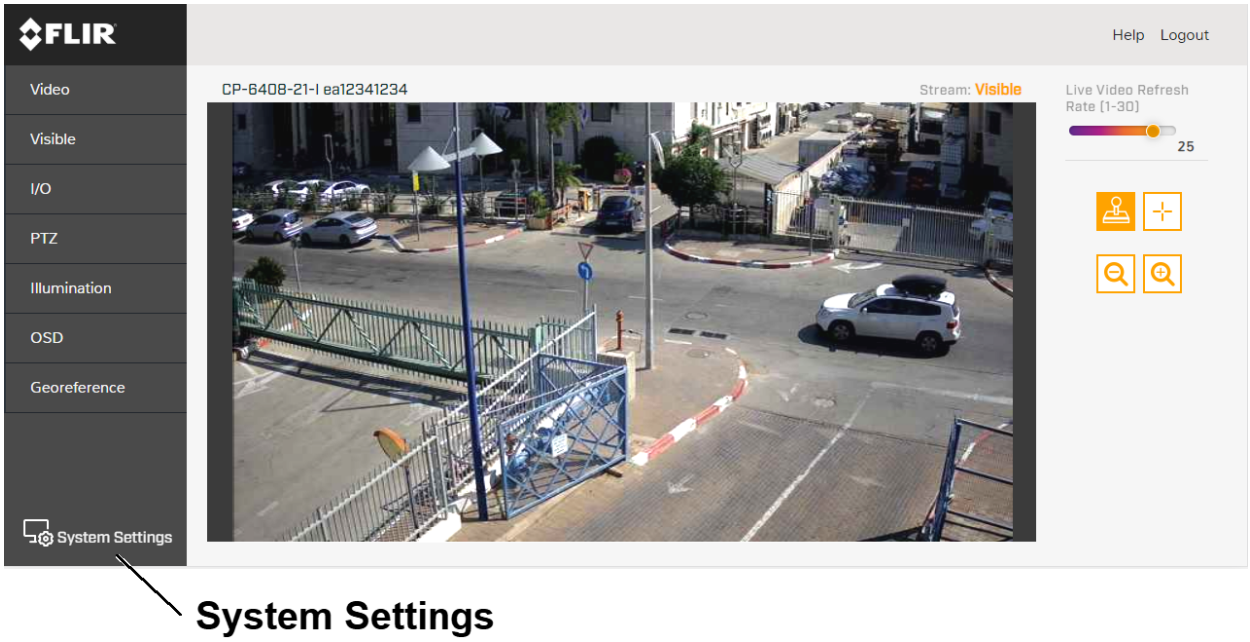
   If you do not know the user name or password, contact the person who configured the camera's users and passwords.
3. When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, specify a new password for the admin user and then log back in using the new password.

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

The camera's View Settings home page appears.

4.2 View Settings Home Page

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



View Settings page for users assigned the admin or expert role

Live Video

You can set the Live Video Refresh Rate between 1-30 image frames per second (FPS). The Live Video Refresh Rate setting only affects the live video; it does not affect the camera's video streams.

Pan, Tilt, and Zoom (PTZ)

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

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

You can zoom in and out using:

- The onscreen buttons—Click once or click and hold for continuous zoom.
- The mouse wheel, when the mouse pointer is over live video.

Tip

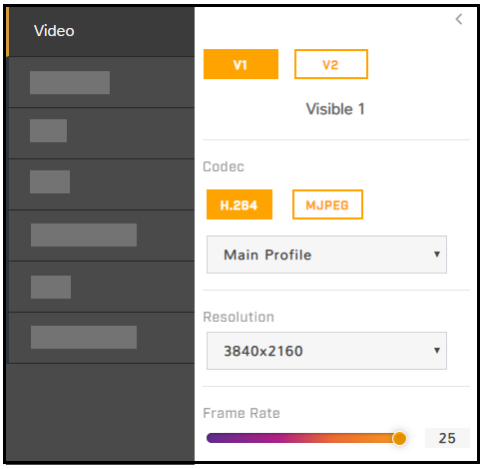
Zooming in and out affects the video streams, unlike the Live Video Refresh Rate setting.

System Settings and Other Options

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

Additional choices are for Help and Logout.

4.3 Video Page



The camera provides two video streams (V1 and V2). Video streams are available for viewing using a client program or third-party ONVIF systems.

In general, it is not necessary to modify the default parameters. In some cases, such as when an IP video stream is sent over a wireless network, it can be useful to tune the video streams to reduce the bandwidth requirements. To modify the parameters for a particular video stream, click the relevant button (V1 or V2).

Tip

On the camera web page and in the camera's cloud web application, the live video is not the actual video stream. Changes to stream settings might not affect the live video. Check any changes to stream settings using a client program or third-party ONVIF system.

Visible 1 / Visible 2

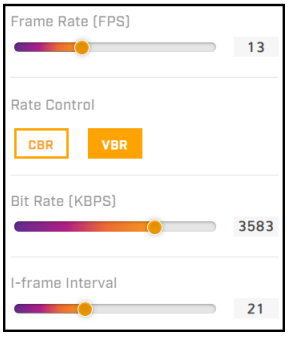
Codec options for the visible streams are H.264 or MJPEG.

Resolution options are 3840x2160 (4K), which is available only with H.264 encoding; 1920x1080 (1080p); 1280x720 (720p); and 640x480 (480p). The Frame Rate range is 5-30 FPS (frames per second).

When one stream's resolution is set to 3840x2160, the camera supports the following resolutions for the other stream:

One visible stream		Other visible stream	
Resolution	**Frame rate**	**Resolution**	**Frame rate**
3840x2160	> 15 FPS	640x480	≤ 30 FPS
	≤ 15 FPS	1280x720	
		1920x1080	

Codecs, Quality, and Bandwidth



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

With the H.264 codec, you can set the:

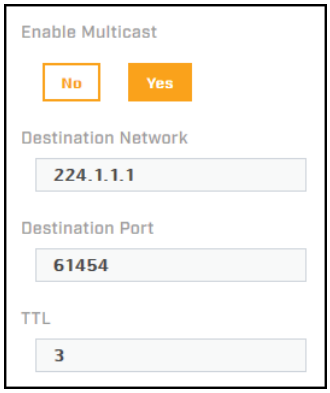
- Rate Control:
  - CBR (constant bit rate): The Bit Rate parameter defines the target bit rate; the camera attempts to keep the video at or near the target bit rate.
  - VBR (variable bit rate): The Bit Rate parameter defines the average bit rate.

- I-frame Interval: Controls the number of P-frames used between I-frames. I-frames are full frames of video and the P-frames contain the changes that occurred since the last I-frame. A smaller I-Frame Interval results in higher bandwidth (more full frames sent) and better video quality. A higher I-frame Interval means fewer I-frames are sent and therefore can result in lower bandwidth and possibly lower quality.

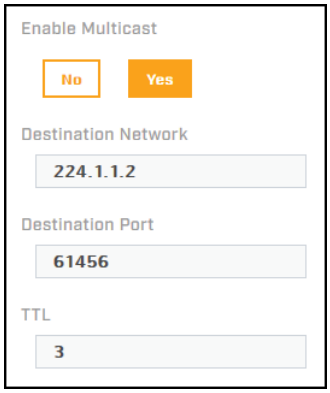
With the MJPEG codec, you can set the Quality between 10-80. Setting a higher value can increase the video stream's bandwidth requirements.

Network Options

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



Visible 1



Visible 2

If more than one camera is providing multicast streams on the network, make sure the Destination Network IP address is unique for each camera (the Destination Port can be reused). By default, the port assignment is unique per stream.

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

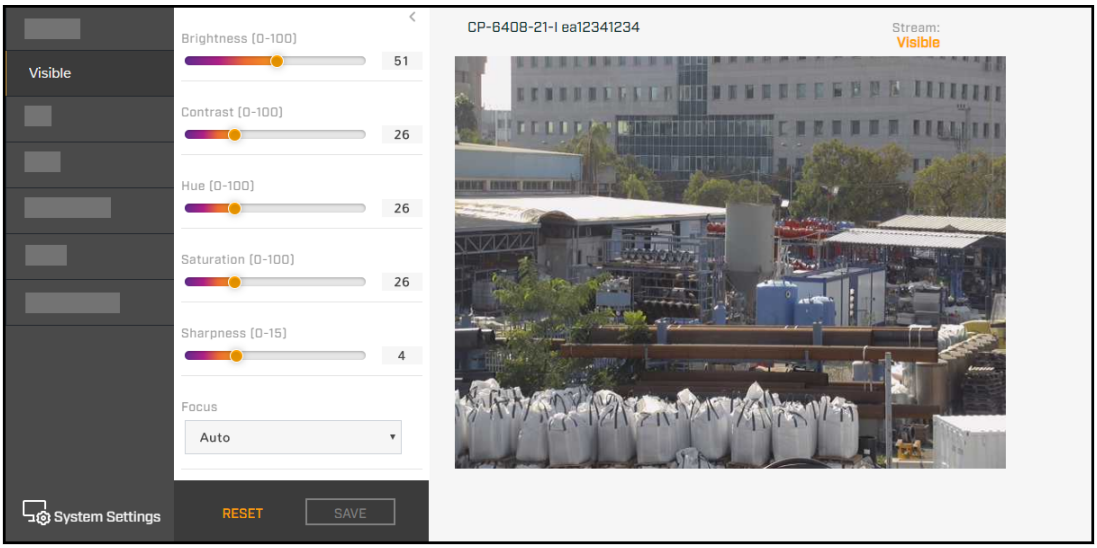
The video streaming uses a protocol generally referred to as RTP, the real-time transport protocol, although there are actually a number of protocols involved, including the Real-Time Streaming Protocol (RTSP). The video stream URLs incorporate the IP address of the camera. Using the camera's default IP address, the complete URLs are:

- **Visible 1**—rtsp://192.168.0.250:554/stream1
- **Visible 2**—rtsp://192.168.0.250:554/stream2

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

Accessing any of the camera's video streams requires authentication. You can use the name and password for any of the camera's users. See Users Page.

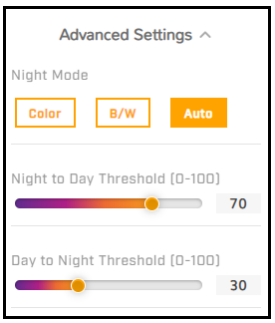
4.4 Visible Page



You can adjust the following visible video settings:

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

Advanced Settings

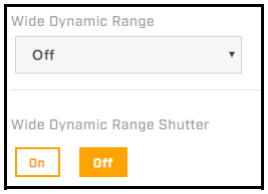


- **Night Mode**—Set the visible video to
  - **Color** (day mode)
  - **B/W** (night mode)
  - **Auto** (default)—Automatically switches the visible video mode according to light level. When Night Mode is set to Auto, you can set the thresholds at which the visible video switches from black and white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

On the Illumination Page, when infrared illumination is set to Auto and the scene becomes dark enough, the visible video automatically changes to B/W (night mode).

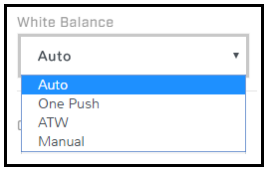
- **Wide dynamic range settings**

  WDR improves the image quality and amount of detail in high contrast scenes. High contrast scenes consist of areas with different lighting conditions; some areas are bright and others are dark. Without WDR, either the bright areas would be overexposed (too bright) or the darker areas would be completely dark. WDR can produce more detail in both the dark and the bright areas of the image.



  - **Wide Dynamic Range**—Set the level of digital Wide Dynamic Range (dWDR) to Off, Low, Mid, or High. When enabled, the camera digitally enhances the details in each frame.
  - **Wide Dynamic Range Shutter**—Enables True WDR. The camera combines two frames taken with slow- and fast-exposure shutter speeds into a single frame with a wide dynamic range, determining the optimal mix of regions within the scene.

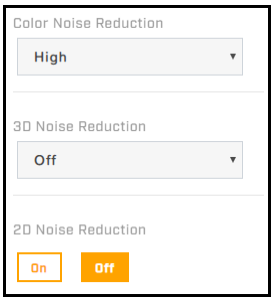
- **White Balance**—Set according to operating environment:



  - **Auto** (default)—Computes the white balance value output using color information from the entire screen. It is suitable for an environment with a light source color temperature in the range of approximately 2,700 ~ 7,500K.
  - **One Push—**Click One Push Trigger to activate the factory-optimized setting for white balance. This setting might not be ideal for every lighting environment.
  - **ATW** (Auto Tracking White Balance)—Automatically adjusts the white balance in a scene while temperature color is changing. It is suitable for an environment with a light source color temperature in the range of approximately 2500 ~ 10,000K.
  - **Manual—**Define the Rgain and Bgain between 0-100 to increase the red and blue luminance.

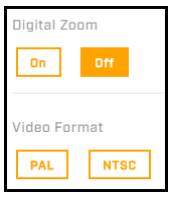
- **Noise reduction settings**

  Noise reduction settings are used 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. 3D noise reduction and 2D noise reduction settings reduce luminance noise: dots of varying brightness levels (black, white, and gray). It is not recommended to completely eliminate luminance noise, which can result in unnatural images. The 3D Noise Reduction and 2D Noise Reduction settings should be configured after configuring Color Noise Reduction.



  - **Color Noise Reduction**—Controls the noise appearing as red, green and blue dots between light and dark areas. Four settings are available: Off, Low, Mid, High. High maximizes the blending of the color noise with the image, effectively removing the dots, while Low minimizes the blending.
  - **3D Noise Reduction**—Provides superior noise reduction and is recommended for use in extra low-light conditions. It is especially useful for reducing blur with moving objects. 3D noise reduction reduces image noise/snow in low-light conditions by comparing adjacent frames. A higher level of 3D noise reduction generates relatively enhanced noise reduction, although it creates more motion blur than 2D noise reduction on moving objects. Four settings are available: Off, Low, Mid, High.
  - **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. 2D noise reduction 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 3D noise reduction. It can be set On or Off.

- **Digital Zoom**—Enables digital zoom.
- **Video Format**—When mounted indoors, the visible camera shutter speed can be synchronized to the 50 Hz or 60 Hz power used for lighting the scene. If lighting is connected to 50 Hz power, the PAL setting might provide better video and NTSC might provide better video under 60 Hz lighting.



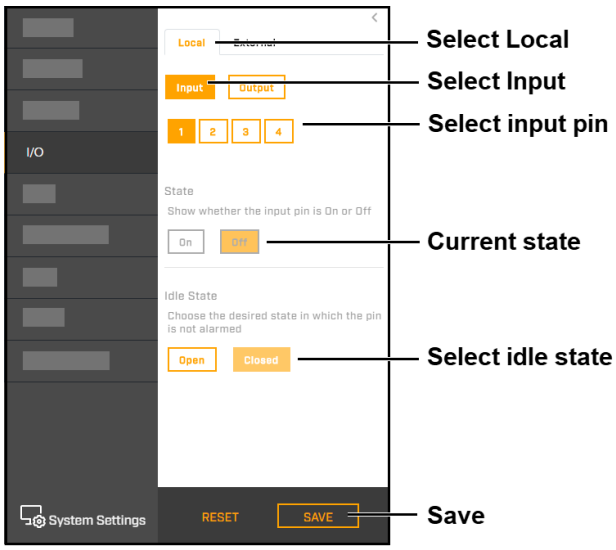
Where relevant, changing the settings on the Visible page immediately affects the live visible video images and streams. To save any changes, click **Save**. To discard changes or return to the factory defaults, click **Reset**.

4.5 Input/Output (I/O) Page

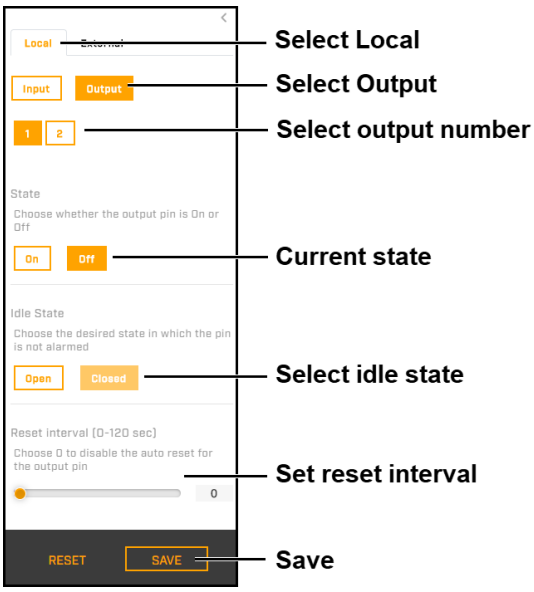
Adjust local and external I/O settings on the I/O page.

- For local I/O connections:

Input settings



Output settings



For information about the local I/O connector, see Camera Connections.

- For external I/O connections, set the current state for the input and output pins, as shown at right.

  You can configure the external I/O connections, including the number of external input and output pins, on the I/O Devices Page in System Settings.

4.6 PTZ Page

Use the PTZ page to:

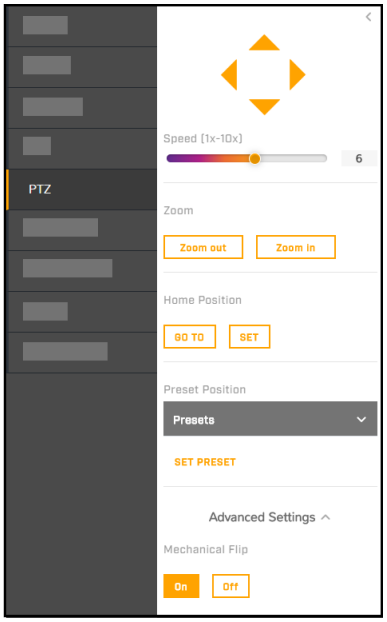
- Move the camera left, right, up, or down (pan and tilt)
- Define the pan and tilt speed, between 1x-10x
- Zoom in and out—click once or click and hold for continuous zoom
- Go to the camera's home position
- Set the camera's current position as its home position
- Define preset positions:

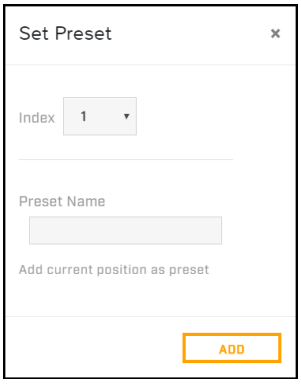
  a. Under Preset Position, click **Set Preset**.

  b. Select a preset index number from 1-128. Selecting an index number currently associated with a preset position overwrites the existing preset position.

  c. Specify a unique, descriptive name for the preset position.

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

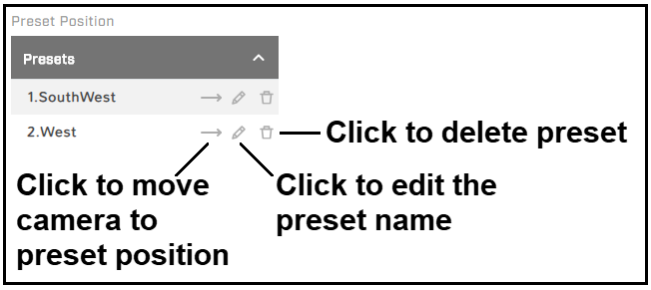




Preset positions are relative to the camera's orientation, which is defined on the Georeference page. If the camera's orientation changes and presets have been defined, redefine them with the new orientation setting.

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

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



Click **Advanced Settings** to:

- Disable or enable the camera's mechanic flip feature

  By default, Mechanical Flip is set to On and the camera can continuously track an object passing under the camera. When a tilting camera reaches its maximum angle, it pans 180° and then continues tilting to keep tracking the object.

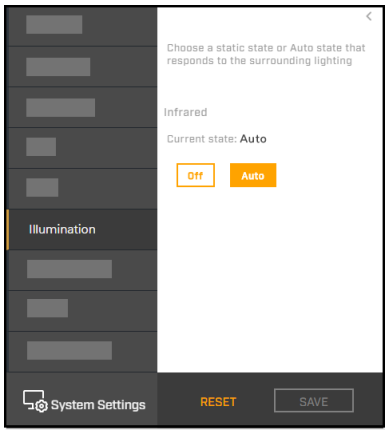
Note

If a preset position or a point for another function (for example, a tour) is set to a position that can only be reached by flipping the camera, when Mechanical Flip is set to Off, the camera cannot reach that position.

Where relevant, changing the settings immediately affects the live video and video streams. To save changes, click **Save**. To discard changes, click **Reset**.

4.7 Illumination Page

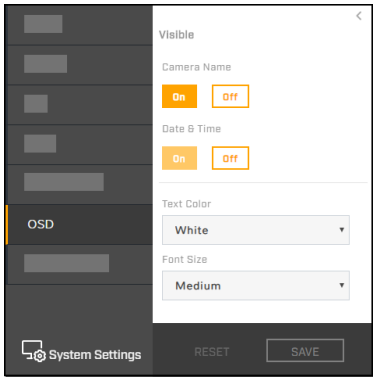
The camera features NIR illumination for the visible light camera. By default, infrared illumination is set to Auto; when the scene becomes dark enough, the infrared illumination turns on and the visible camera video changes to night mode (black and white video). You can set the night-to-day and day-to-night thresholds on the Visible Page.



You can set the infrared illumination to Off.

To save a change to the setting as the power-cycle default, click **Save**.

4.8 OSD Page



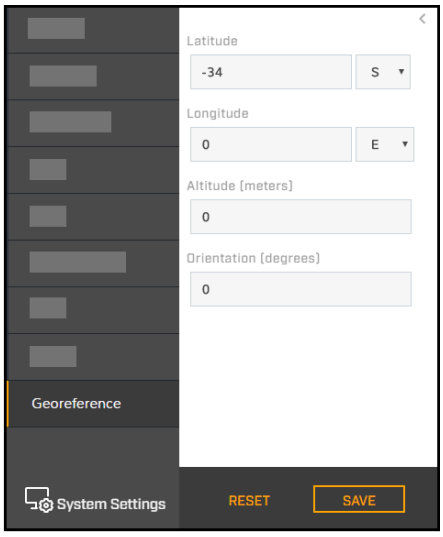
The OSD page provides separate on-screen display settings for visible video. The camera can overlay onto the video its name and the date and time:

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

Changes to OSD settings immediately take effect.

Visible video with OSD

4.9 Georeference Page



Use the Georeference page to specify the camera's geographical location and mounting position.

For geographical location, specify:

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

Tip

To obtain the camera's latitude and longitude, use a map or a mobile GPS device.

For mounting position, specify:

- **Altitude**, in meters above the surrounding ground level (must be greater than zero)
- **Orientation**: the installation angle of the “zero-pan” line of the camera, between 0-360 degrees from North

  Preset positions are relative to the camera's orientation. Changing the orientation affects existing presets. If any presets have been defined, after changing the camera's orientation, go to the PTZ page and redefine them.

After making any change on the Georeference page, click **Save** to save the changes.

The camera can report this georeference information via FLIR CGI/SDK or ONVIF, which:

- Allows the user or an application to:
  - Show the camera on a map
  - Show the direction the camera is facing (using the camera's field of view, which the camera also reports)
- Supports pan and tilt cueing. For example, the FLIR CGI protocol provides pan and tilt commands to point the camera at a specific geographic location (latitude/longitude).

5 Configuration

Users assigned the admin or expert role can click **System Settings** on the View Settings page to configure:

- Networking
- Date and time
- User accounts and passwords
- Audio parameters
- I/O devices
- Cybersecurity
- ONVIF interface

In addition, users assigned the admin or expert role can access the Firmware & Info page to upgrade the camera's firmware, reset the camera to its factory defaults, reboot the camera, and configure other parameters.

5.1 Network Page

When a user assigned the expert or admin role clicks **System Settings**, the Network page appears.

The IP address mode can be set to DHCP (default) or Static.

Define the camera's hostname, which identifies the camera.

When the IP address mode is Static, specify:

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

When the IP address mode is set to DHCP, if a DHCP server is not available on the network, the camera's default IP address is 192.168.0.250. For information about defining the camera's IP address using the DNA tool, see Initial Networking Configuration.

Caution

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

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

When the DNS Mode is set to Static, specify:

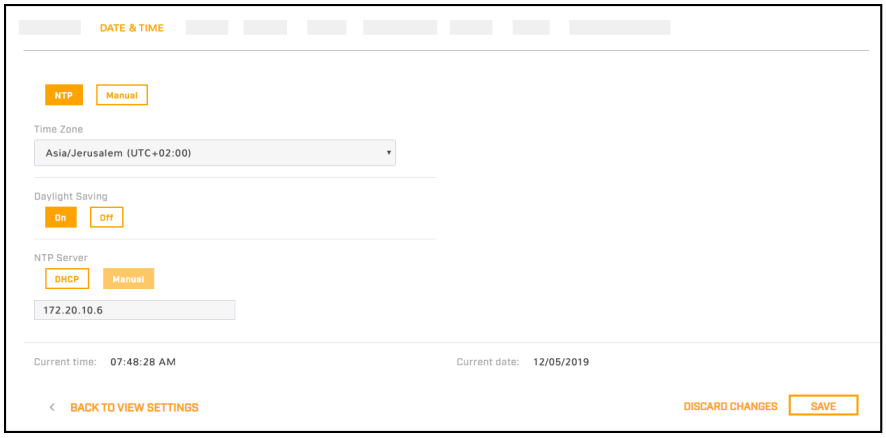
- **Name Server 1**—The primary domain name server that translates host names into IP addresses
- **Name Server 2**—A secondary domain name server that backs up the primary DNS

You can also specify the:

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

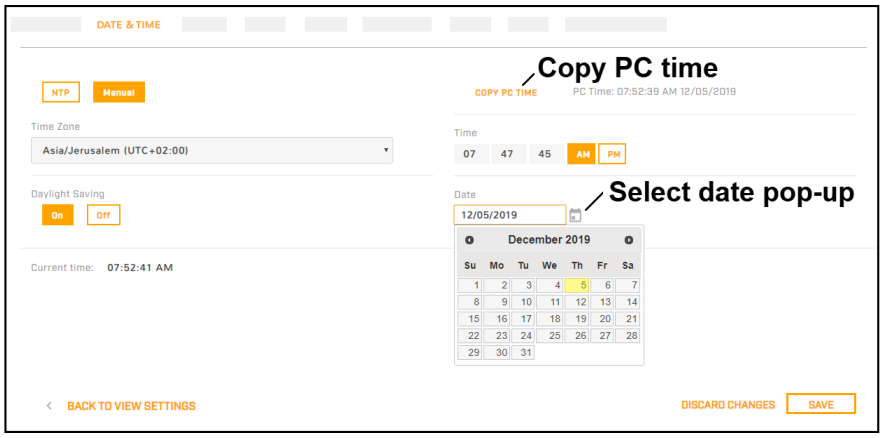
5.2 Date & Time Page

Use the Date & Time page to configure the camera's date and time settings.



The camera can obtain the date, time, and time zone from an NTP server, or you can manually specify that information.

When set to Manual, you can copy the local PC's time or specify the hour, minute, second, and date.



When set to NTP, you can specify whether the camera obtains the NTP server information from the DHCP server on the network, or manually enter the NTP server information.

After setting the date and time parameters, click **Save** at the bottom of the page. The camera requires a reboot, and a confirmation prompt appears.

5.3 Users Page

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

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

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

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

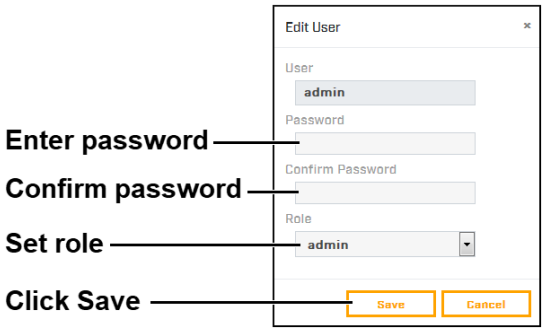
Assign one of the following roles, according to the level of access the user requires:

Role	Access
user	Can: • View live video • Pan, tilt, and zoom the camera, including toggling between the emulated joystick and crosshairs control • View the Help page • Log out
expert	Cannot manage users: • Cannot add/edit/delete users • Cannot change passwords Can access and use all other View Settings and System Settings pages, menus, controls, and settings

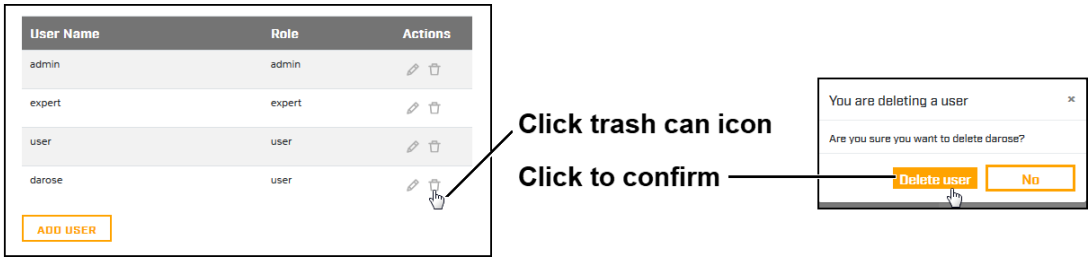
Role	Access
admin, including the default admin user	Can access and use all of the camera's web pages, including adding/editing/deleting users (but cannot delete the default admin user), and setting all passwords
All roles can access the camera's video streams, which require authentication. You can use the name and password for any of the camera's users.	

Add User

Edit User

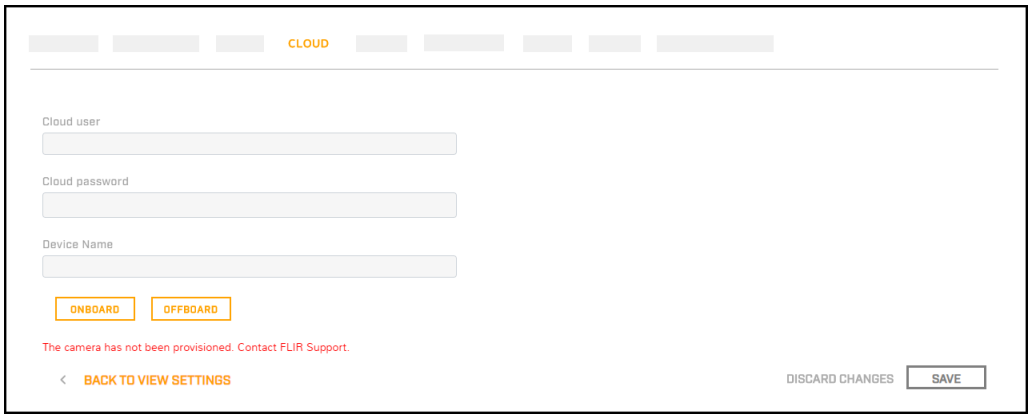


Delete User



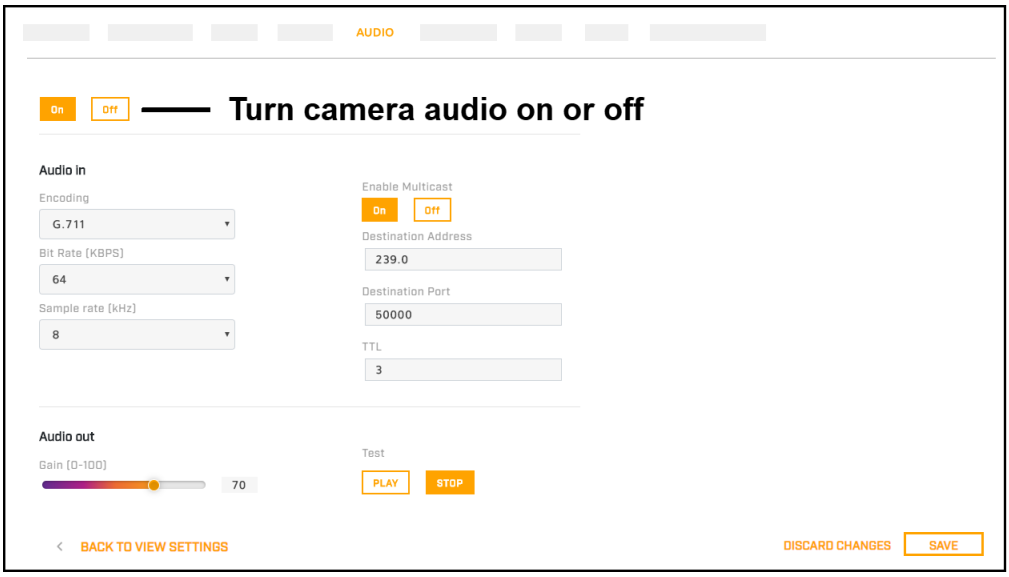
5.4 Cloud Page

The camera will support FLIR Cloud in future releases.



5.5 Audio Page

The Audio page provides configuration settings for the camera's audio input and output.



The On/Off buttons affect all audio input and output. Turning audio off immediately turns off all camera audio.

Audio In

When audio is On, the following audio input settings appear:

- **Encoding**—G.711.
- **Bit Rate**—The camera supports an audio input bit rate of 64 kilobits per second (kbps).
- **Sampling Rate**—The camera supports a sample rate of 8 kHz.
- **Enable Multicast**—Can be set to On (default) or Off. When On, specify the destination address and port, and the time-to-live (TTL).

Audio Out

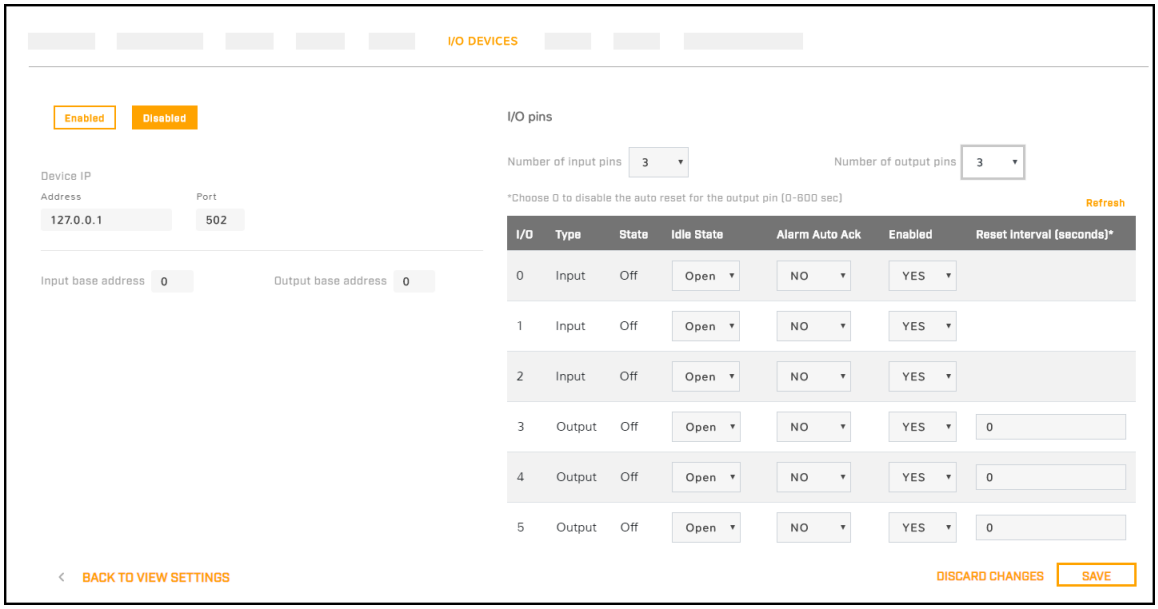
When audio is On, you can adjust the audio line output gain from 0-100 percent. The default gain is 80 percent.

Tips

- Test whether the camera's audio output is functioning properly by clicking **Play**.
- If you are monitoring the audio IP output with a video stream and change any of the audio configuration settings except gain, restart the stream. For example, if you are monitoring a video stream and turn audio on, you need to restart the stream to hear the audio with the stream.

5.6 I/O Devices Page

The I/O Devices page provides configuration settings for external I/O connections and the device managing those connections with the camera.



The following settings for the device managing the external I/O connections are available:

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

You can define the number of input and output pins the device manages.

The following information appears for each pin:

- **I/O pin number**
- **Type**—Input or Output
- **State**—the pin's current state: Open or Closed

For each pin, you can define the following:

- **Idle State**—Open or Closed
- **Alarm Auto Ack**—Yes or No
- **Enabled**—Yes or No
- **Reset Interval (for output pins only)**—between 0-600 seconds; specifying 0 seconds disables the auto reset

Related Operation and Configuration Information

For information about changing the current state of the input and output pins, see I/O Page.

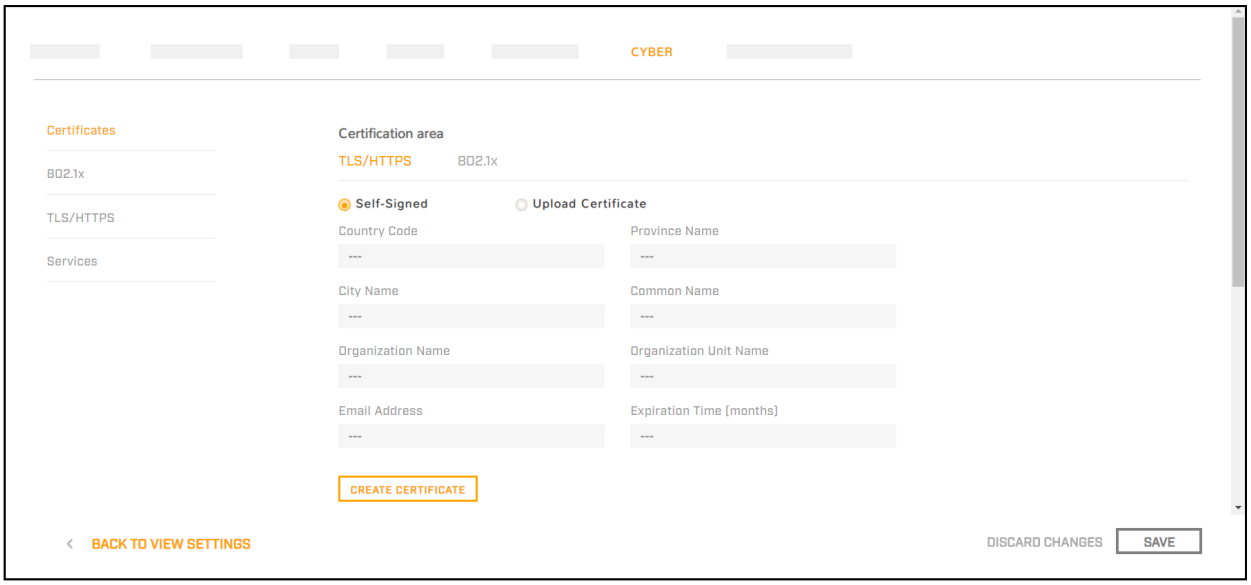
For more information about how to configure the device managing the external I/O connections, refer to the device's documentation.

5.7 Cyber Page

The Cyber page provides security configuration settings for:

- Certificates
- IEEE 802.1x-compliant communication
- Transport Layer Security (TLS) and secure HTTP (HTTPS) communication
- Other cybersecurity services

Changes to the security configuration settings on the Cyber page do not immediately take effect. To apply changes, click **Save** and then reboot the camera.



5.7.1 Certificates

Before you can enable TLS/HTTPS or 802.1x, you need to generate or upload a valid certificate. You can:

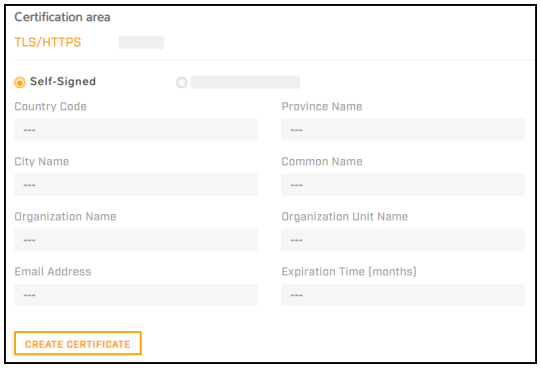
- Use the camera's web page to generate a self-signed certificate.
- Upload a self-signed certificate.
- Upload a certificate signed by a third-party.

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

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

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

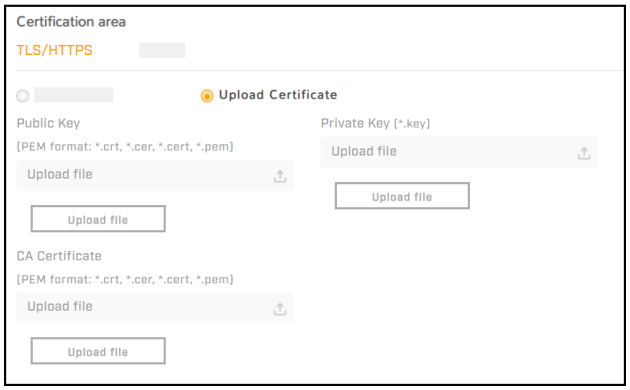
To generate and install a self-signed certificate for TLS/HTTPS:



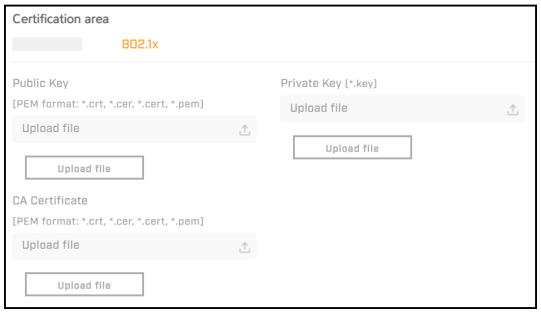
1. In the Certificates section and Certification area, select **TLS/HTTPS** and **Self-Signed**.
2. Enter information such as country code, city name, and organization name.
3. Click **Create Certificate**.
4. Allow 15 seconds for the camera to generate the certificate, at which point a confirmation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

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

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



To upload a certificate for TLS/HTTPS



To upload a certificate for 802.1x

2. If you are uploading a self-signed certificate, under **Public Key** and then under **Private Key**:
   a. Click Upload file .
   b. Select the appropriate key file.
   c. Click Upload file .

   If you are uploading a third-party CA signed certificate, select and upload the Public Key, Private Key, and CA Certificate.
3. Verify that the camera certificate files are valid and make sure *Certificates are OK* appears under the certificate information, under Download certificate.

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

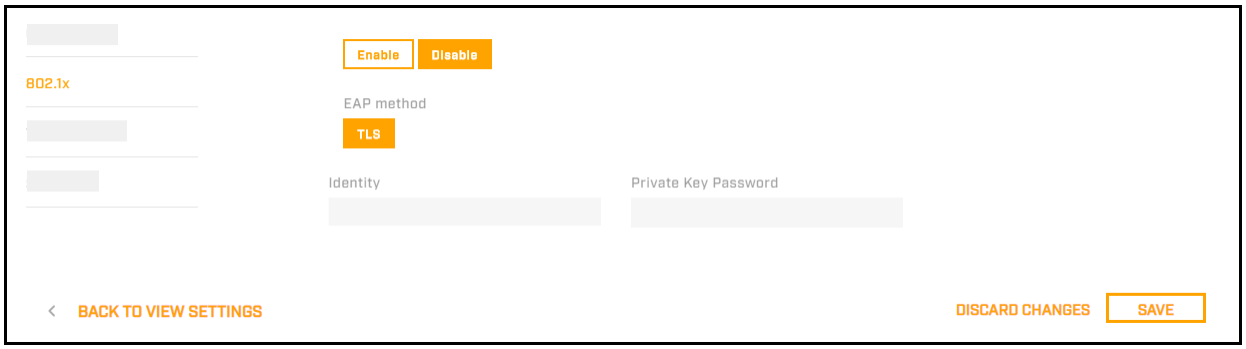
Changes in the Certificates section do not immediately take effect. To apply changes, click **Save** and then reboot the camera.

5.7.2 802.1x

Enable or disable IEEE 802.1x-compliant TLS communication.

Provide an Identity and Private Key Password.

Changing these settings does not immediately take effect. To apply a change to these settings, click **Save** and then reboot the camera.

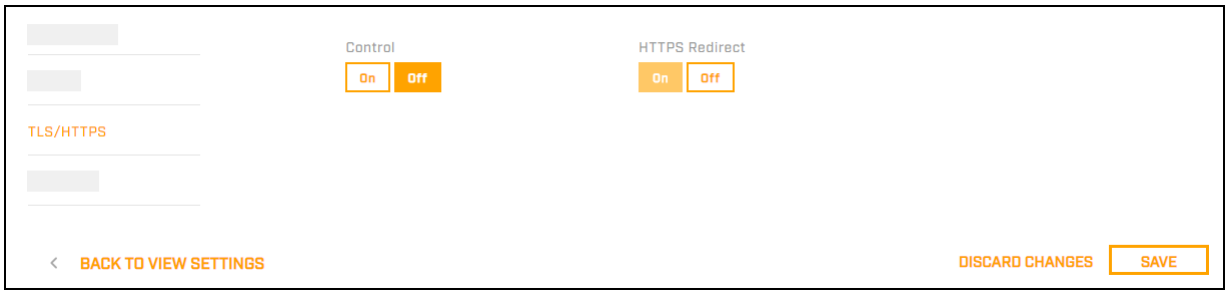


5.7.3 TLS/HTTPS

Enable or disable camera control using Transport Layer Security (TLS)/secure HTTP (HTTPS).

Enable or disable HTTPS redirect.

Changes to these settings do not immediately take effect. To apply the changes, click **Save** and then reboot the camera.



5.7.4 Services

Enable or disable digest authentication for the FLIR CGI control interface. The default setting is **On** (enabled).

Firewall Settings

For enhanced security, the camera has a firewall that you can enable by clicking **On**. By default, when you enable the firewall, the following services are set to **Allow**, which means they remain enabled and their default ports remain open:

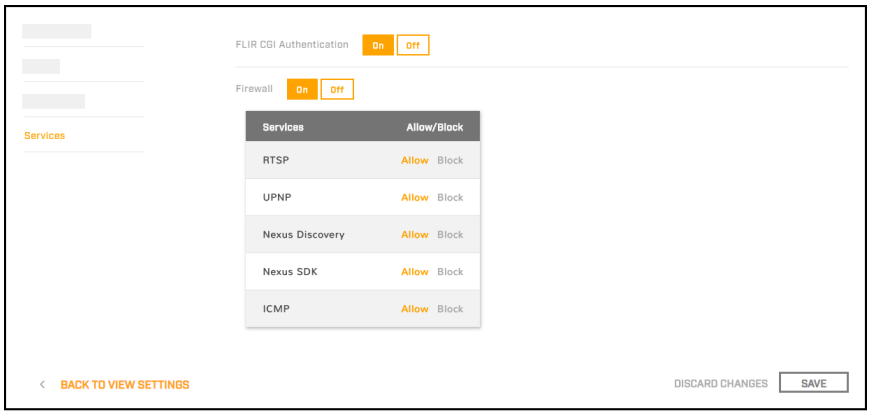
- RTSP
- UPNP
- Nexus Discovery
- Nexus SDK
- ICMP

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

Caution

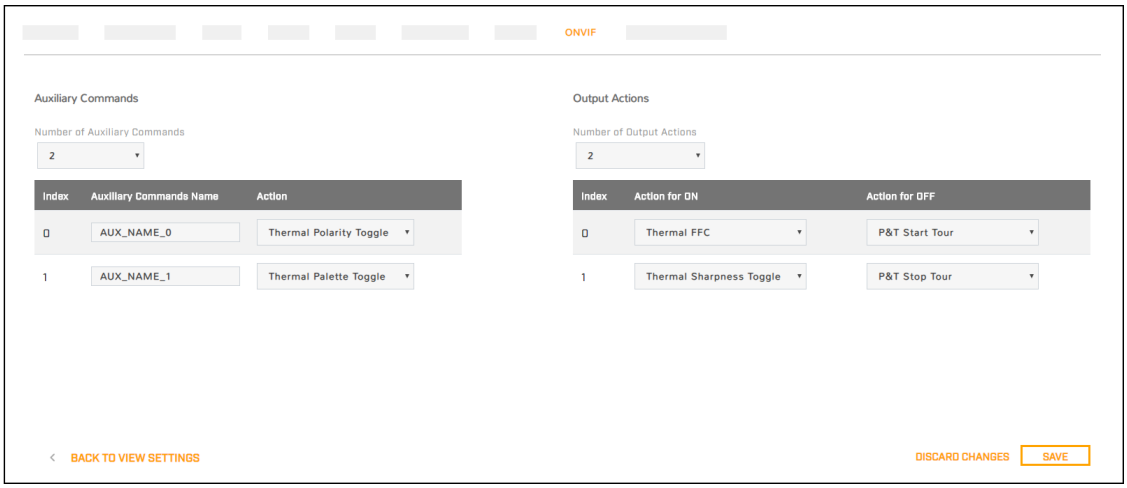
Disabling services and ports can affect product functionality.

Changes to Services settings do not immediately take effect. To apply changes to these settings, click **Save** and then reboot the camera.



5.8 ONVIF Page

The ONVIF page provides settings for auxiliary commands and for output actions.



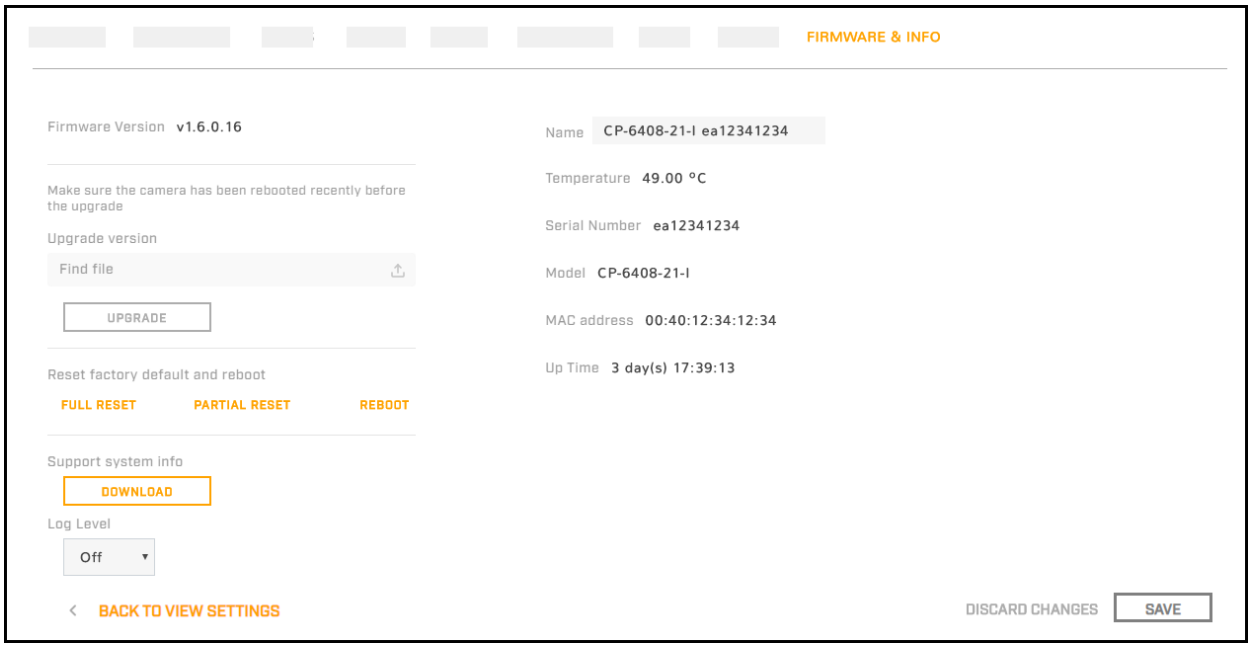
To configure the ONVIF interface:

1. Select the number of auxiliary commands (up to seven) and the number of output actions (also up to seven).
2. For each auxiliary command action, specify the ONVIF command name.
3. For each auxiliary command action, and separately for each ON and OFF output action, select one of the following:
   - **None**
   - **P&T Start Tour**—Initiates a tour of the pan and tilt preset positions (see PTZ Page).
   - **P&T Stop Tour**—Stops the tour of the pan and tilt preset positions.

5.9 Firmware & Info Page

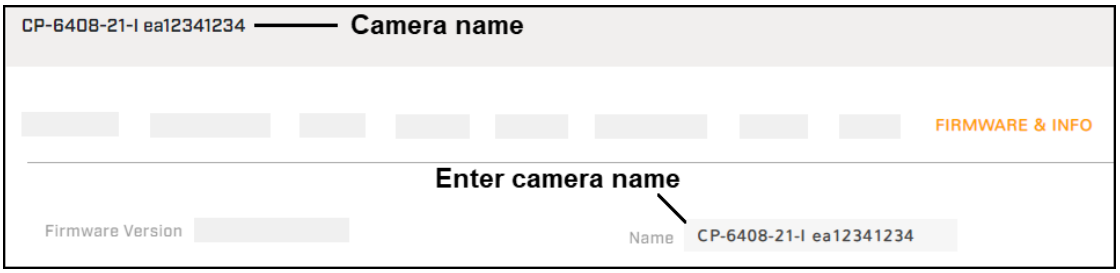
On the Firmware & Info page, you can:

- Specify a unique name for the camera
- Upgrade the camera's firmware
- Reset the camera to its factory defaults
- Reboot the camera
- Define a log level and download system information



Name

Specify a unique, friendly name for the camera, using only alphanumeric characters. The default name for the camera is the camera model followed by the camera's serial number.



To upgrade the camera's firmware:

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

Caution

Only upgrade to firmware developed for the Quasar CP-6408-21-I camera.

4. Click **Upgrade**.

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

Factory Defaults

Click **Full Reset** to return the camera its original factory configuration.

Click **Partial Reset** to keep the camera's current network and IP settings, but return all other settings to the factory configuration.

Click **Reboot** to cause the camera to power cycle and reinstall configuration files.

Tip

You can also return the camera to its original factory configuration 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 button is located on the camera's connector panel.

Support System Info

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

Click **Download** to retrieve the camera's log files.

6 Maintenance and Troubleshooting Tips

If help is needed during installation, operation, or configuration, contact the local FLIR representative, or visit the FLIR Support Center at: https://www.flir.com/support/.

6.1 Cleaning

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

Note

Do not disturb or move camera during cleaning.

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

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

Use the following procedure and solvents, as required:

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

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

6.2 Troubleshooting

No Video

If the camera will not produce an image, check the connections at the camera and at the display. If the connectors appear to be properly connected but the camera still does not produce an image, ensure that power has been properly applied to the camera and the circuit breaker is set properly. If a fuse was used, be sure the fuse is not blown.

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

Unable to Communicate over Ethernet

First check to ensure the physical connections are intact and that the camera is powered on and providing analog video to the monitor.

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

Unable to View Video Stream

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

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

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

rtsp://192.168.0.250:554/stream1 for Visible 1

rtsp://192.168.0.250:554/stream2 for Visible 2

Accessing any of the camera's video streams requires authentication. You can use the name and password for any of the camera's users. See Users Page.

Refer to Network Options for additional information on RTP settings and stream names.

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

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

Support:
https://www.flir.com/support/

Document:
CP-6408-21-I Installation and User Guide
Revision: 100
Date: February 2020