
**Ariel™ 4K and Quad HD
Bullet Cameras**

**Installation and
User Guide**

CB-3304 / CB-3308



© 2022 Teledyne FLIR LLC All rights reserved. No parts of this material may be copied, translated, or transmitted (in any medium) without the prior written permission of Teledyne FLIR LLC.

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

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

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

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

Teledyne FLIR LLC
6769 Hollister Avenue
Goleta, CA 93117
USA

Support: <https://support.flir.com/>

Important Instructions and Notices to the User:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

Proper Disposal of Electrical and Electronic Equipment (EEE)



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

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

To identify a responsible disposal method nearby, please contact the local waste

Document History

Version	Date	Comment
Ver 0.1	September 11, 2017	Initial FLIR Release
Ver 0.3	December 2018	Firmware upgrade (Analytics), SD Card min/max
Ver 0.4	January 2019	Camera License for Basic Video Analytics
Ver 0.4a	February 2019	Access Technical Specs from FLIR Website
Ver 0.5	March, 2019	BVA License must be reloaded after full Factory Reset
Ver 0.6	November, 2019	Added mounting details and info on Waterproofing RJ-45 connector
Ver 0.6a	December, 2019	Correction - Removed references to 'Highlight Compensation'
Ver 0.6b	March 9, 2020	Correction - Replaced missing pictures
Ver 0.6c	May 31, 2020	Correction - Now includes Basic Video Analytics settings section
Ver 0.7	May 2022	New camera web page design

Product Registration and Warranty Information

Register your Product with Teledyne FLIR at <https://customer.flir.com>.

For warranty information, see <https://www.flir.com/support-center/warranty/security/flir-security-product-warranties/>.

Table of Contents

1. Document Scope and Purpose	1
2. Camera Overview	4
2.1 Features	5
2.2 Accessing Product Information from the Teledyne FLIR Website	6
2.3 Camera Dimensions	7
3. Installation	8
3.1 Preparation	8
3.1.1 Supplied Components	8
3.1.2 Site Preparation	9
3.1.3 Pre-Installation Checklist	9
3.1.4 Outdoor Mounting Recommendations	10
3.1.5 Supplying Power to the Camera	10
3.1.6 Connections and Interfaces	11
3.2 Initial Configuration	11
3.2.1 Connect the Camera	12
3.2.2 Configure for Networking	14
3.2.3 Change the Video Format (Optional)	15
3.3 Mounting	16
3.3.1 Fit Mounting Hardware	16
3.3.2 Mount and Aim the Camera	16
3.3.3 Waterproof the System Cable Connection	17
3.4 Additional Configuration	19
3.5 Attach the Camera to a Supported VMS	20
4. Operation	21
4.1 Accessing the Camera's Web Page	21
4.1.1 Camera Web Page for Administrators	22
4.1.2 Camera Web Page for Other Access Levels	23
4.2 Making Changes to Settings	24
4.3 Video Page	25
4.3.1 4MP Camera Video Resolutions	28
4.3.2 4K Camera Video Resolutions	31
4.4 Using a Media Player to View Camera Video	33
4.5 Visible Page	35
4.6 I/O Page	39
4.7 Illumination Page	40
4.8 OSD Page	40

Table of Contents

4.9	Privacy Zone Page	41
4.10	ROI Page	42
4.11	Motion Page	43
4.12	Video Analytics Page	45
4.12.1	Basic Video Analytics Licenses	48
4.12.2	General Guidelines	50
4.12.2.1	Camera Distribution	50
4.12.2.2	Camera Positioning	50
4.12.2.3	Detection Ranges	51
4.12.2.4	Mounting and Lighting	52
4.12.3	Rule Type-Specific Settings	52
4.12.3.1	Counting - Border Line	52
4.12.3.2	Loitering - Area Protection - Object Removed / Dropped	54
4.12.4	Alarm Triggers and Actions	56
5.	Configuration	58
5.1	Network Page	58
5.2	RTSP Page	60
5.3	Date & Time Page	61
5.4	Users Page	61
5.5	LDAP Page	63
5.6	FTP Page	64
5.7	SD Card Page	64
5.8	Alarm Page	65
5.8.1	Configuring the Rule Trigger	66
5.8.2	Configuring the Rule Schedule	67
5.8.3	Configuring the Rule Action	69
5.9	Audio Page	69
5.10	I/O Devices Page	70
5.11	Sound Page	70
5.12	Snapshot Page	71
5.13	Recording Page	71
5.14	Email Page	71
5.15	Cyber Page	73
5.15.1	Certificates	73
5.15.2	SNMP	75
5.15.3	802.1X	76
5.15.4	TLS/HTTPS	77

Table of Contents

5.15.5	Ports	78
5.15.6	IP Filter	78
5.16	Firmware & Info Page	79
6.	Appendices	82
6.1	Technical Specifications	82
6.1.1	Accessing Camera Information from the Web	82
6.2	Network Settings	83
6.3	Troubleshooting	84
6.4	Acronyms and Abbreviations	86
6.5	Mounting Accessories	87

1 Document Scope and Purpose

This document provides instructions and installation procedures for physically connecting the CB-330x unit. After completing the physical installation, additional setup and configurations are required before video analysis and detection can commence.



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

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

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

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

Avis de non-responsabilité

Il incombe aux utilisateurs des produits Teledyne 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.

Teledyne FLIR LLC et ses agents ne garantissent d'aucune façon que les produits sont adaptés à l'usage auquel l'utilisateur les destine. Teledyne FLIR LLC 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 Teledyne FLIR LLC et ses agents de toute responsabilité en résultant.

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



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 Teledyne 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 Teledyne FLIR.*

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.*



Caution

- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at strong light, such as the sun or an incandescent lamp, which can seriously damage the camera.
- Make sure that the surface of the sensor is not exposed to a laser beam, which could burn out the sensor.
- If the camera will be fixed to a ceiling, verify that the ceiling can support more than 50 newtons (50-N) of gravity, or over three times the camera's weight.
- The camera should be packed in its original packing if it is reshipped.



Caution

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range -40° to 50°C (-40° to 122°F), with no more than 90% non-condensing humidity.

Attention

Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage (-40° à 50°C/-40° à 122°F), sans condensation d'humidité supérieur à 90%.

2 Camera Overview

This User and Installation Guide is intended to help you physically install, configure settings for, and operate the CB-330x indoor/outdoor bullet IP camera. The CB-330x camera family includes three models:

- CB-3304-11-I
- CB-3304-21-I
- CB-3308-11-I

(all models include lens control)

The units feature the following sensor and motorized varifocal lenses:

	CB-3304-11-I	CB-3304-21-I	CB-3308-11-I
Image Sensor	1/2.9" BSI CMOS Sensor	1/2.9" BSI CMOS Sensor	1/2.5" BSI CMOS Sensor
Effective Pixels (H x V)	4MP (2560x1440)	4MP (2560x1440)	8MP (3840x2160)
Sensor resolution (pixels)	2560x1440	2560x1440	3840x2160
Field of View	2.8-8.5mm	9-22mm	3.4-9mm
Aperture	F1.2	F1.5	F1.2
Iris Control	P-Iris	P-Iris	P-Iris

The cameras support up to three streams at 4MP (CB-3304-11-I and CB-3304-21-I) or 8MP (CB-3308-11-I) with H.265, H.264 or MJPEG compression. The units feature True Day/Night (ICR) and an infrared LED illuminator. They also include Audio Line-In, Audio Line-Out, Alarm-in, and Alarm-out connections. The cameras are powered by an 802.3af Power over Ethernet (PoE) connection. They include a microSD card drive for storing recordings and snapshots.



CB-330x Bullet Camera

2.1 Features

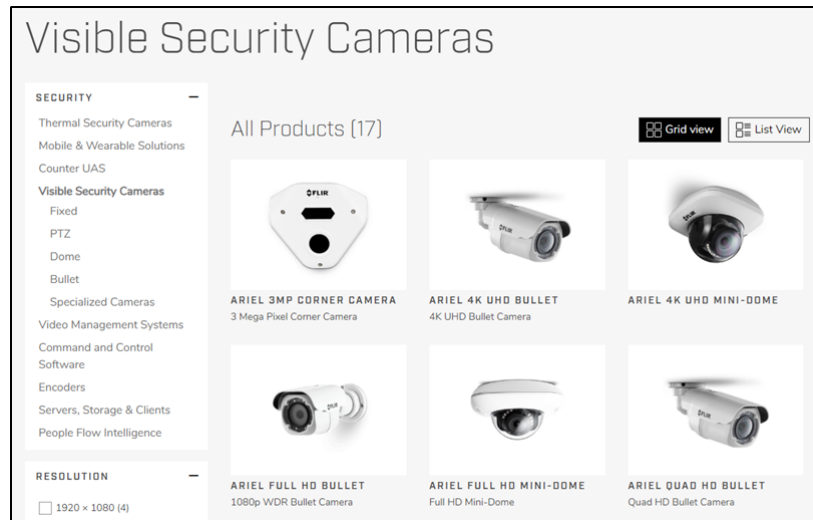
CB-3304-11-I	CB-3304-21-I	CB-3308-11-I
Sensor		
• 1/2.9" BSI CMOS	• 1/2.9" BSI CMOS	• 1/2.5" BSI CMOS
Resolutions:		
• Single-stream: 4MP/30fps	• Single-stream: 4MP/30fps	• Single-stream: 8MP/30fps
• Dual-stream: 4MP/28fps + 720p/28fps	• Dual-stream: 4MP/28fps + 720p/28fps	• Dual-stream: 8MP/15fps + 720p/15fps
• Triple-stream: 4MP/25fps + 720p/25fps + D1/25fps	• Triple-stream: 4MP/25fps + 720p/25fps + D1/25fps	• Triple-stream: 8MP/15fps + 720p/15fps + D1/15fps
Common Features		
• True day/night (ICR)	• Infrared LED illuminator	• H.265, H.264 and MJPEG compression
• True WDR	• 3DNR image noise reduction	• Backlight compensation
• Analytics	• Built-in web server	• Supports Internet Explorer, Edge, Chrome, and Firefox browsers
• Motion detection event-driven alarms	• Tampering detection and notifications	• Two regions of interest
• Gamma correction	• White balance	• 8 privacy zones
• 802.1X and SSL/TLS security protocols	• SNMP v1/v2c/v3 and SNMP traps	• Up to 9 users
• HTTP streaming MJPEG	• UPnP support	• ONVIF® Profiles S, G, & T
• Alarm In/Out	• Audio Line-In/Line-Out	• Powered by 802.3af PoE
• Supports up to 128GB microSDHC/SDXC card	• IP67 enclosure with IK7 and IK8 vandal-proof protection	• Built-in heater

2.2 Accessing Product Information from the Teledyne FLIR Website

Up-to-date resources for the camera, including the camera's specifications, the Teledyne FLIR Discovery Network Assistant (DNA) software tool, and this guide, are available from the camera's product details and support pages on [the Teledyne FLIR website](https://www.flir.com/browse/security/).

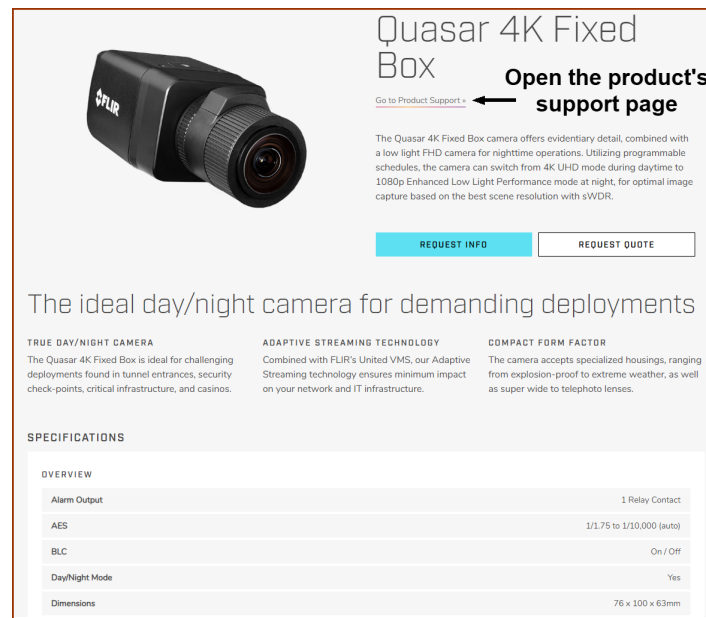
To access product information from the Teledyne FLIR website:

1. Open <https://www.flir.com/browse/security/> and navigate to [Products > Security > Visible Security Cameras](#).



Visible Security Cameras Page on the Teledyne FLIR Website

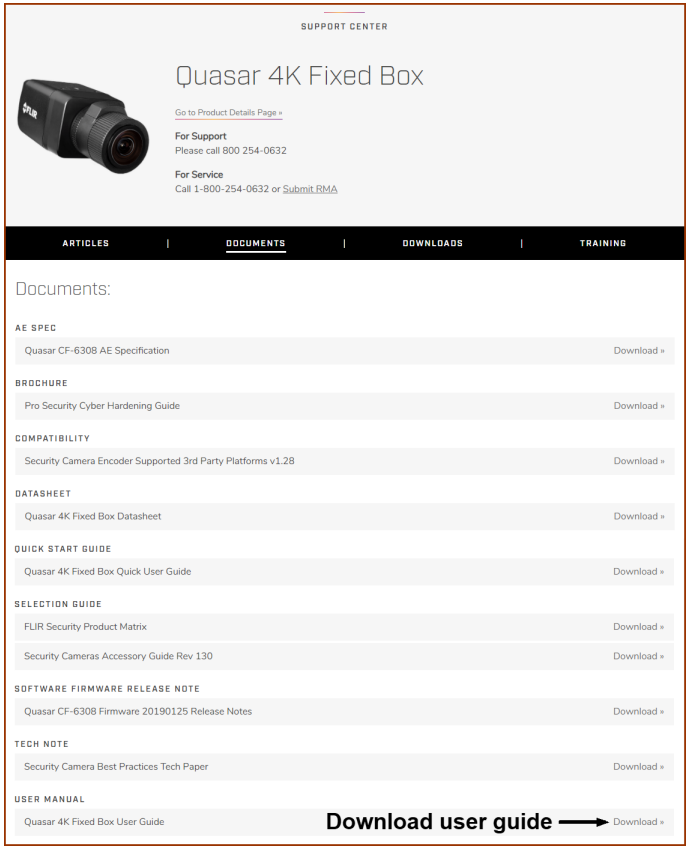
2. Find and click the camera. The camera's product details page appears.



Product Details Page (Example)

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

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



Product Support Page Documents Tab (Example)

- 5. Download the DNA tool from the Downloads tab.

2.3 Camera Dimensions

The CB-330x camera's dimensions are 215 x 86 x 80 mm (8.48 x 3.39 x 3.15 in.).

3 Installation

This section describes how to install and connect the unit. It includes the following sections:

- [Preparation](#)
- [Initial Configuration](#)
- [Mounting](#)
- [Additional Configuration](#)
- [Attach the Camera to a Supported VMS](#)

If you are enabling video analytics on one or more CB-330x cameras, see [General Guidelines](#) for information about camera distribution and positioning, detection ranges, mounting, and lighting.

3.1 Preparation

This section contains the following important preparation information:

- [Supplied Components](#)
- [Site Preparation](#)
- [Pre-Installation Checklist](#)
- [Outdoor Mounting Recommendations](#)
- [Supplying Power to the Camera](#)
- [Connections and Interfaces](#)

3.1.1 Supplied Components

The CB-330x camera kit includes these items:

Item	CB-3304	CB-3308
CB-330x bullet camera	1pc	1pc
Tapping screws (TP4 31mm)	3pcs	3pcs
Plastic anchors	3pcs	3pcs
T6 Torx wrench	1pc	1pcs
Drill template	1pc	1pcs
Quick install guide	1pc	1pcs
Waterproof cap	1pc	1pcs

Related Documentation

- *CB-330x Quick Install Guide*
- *CM-4S-31 Electrical Box Adapter Plate Installation Guide*
- *CB-WLBX-31 Junction Box Installation Guide*
- *CB-PLBX-31 Pole Mount Installation Guide*
- *DNA User Guide*

Note: For all current documentation, see [Accessing Product Information from the Teledyne FLIR Website](#).

3.1.2 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.

3.1.3 Pre-Installation Checklist

Before installing the unit, make sure that:

- Instructions in the [Document Scope and Purpose](#) section are followed.
- All related equipment is powered off during the installation.
- Use best security practices to design and maintain secured camera access, communications infrastructure, tamper-proof outdoor boxes, etc.
- All electrical work must be performed in accordance with local regulatory requirements.

**Caution**

To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range -40° to 50°C (-40° to 122°F), with no more than 90% non-condensing humidity.

Attention

Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage (-40° à 50°C/-40° à 122°F), sans condensation d'humidité supérieur à 90%.

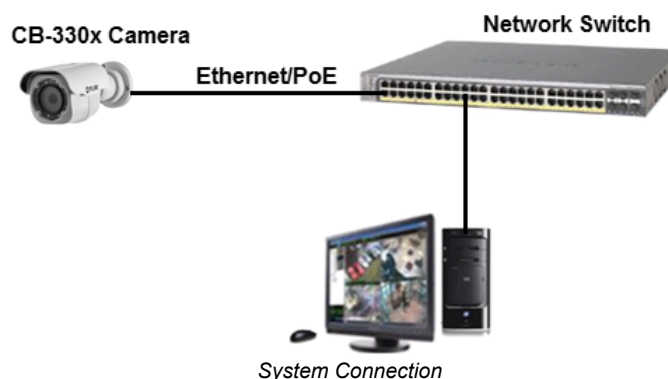
3.1.4 Outdoor Mounting Recommendations

Following are additional considerations for outdoor installation:

- For outside wiring installation, always use weatherproof equipment, such as boxes, receptacles, connectors, etc.
- For electrical wiring, use the properly rated sheathed cables for conditions to which the cable will be exposed (for example, moisture, heat, UV, physical requirements, etc.).
- Plan ahead to determine where to install infrastructure weatherproof equipment. Whenever possible, ground components to an outdoor ground.

3.1.5 Supplying Power to the Camera

The camera is powered by an 802.3af PoE (Class 3) connection over the unit's network cable.

**Caution**

- This product must be connected only to a PoE network.
- The PoE supply's rated output is 48VDC, 0.2A.
- If the camera is installed for outdoor use, the PoE supply must be installed with proper weatherproofing.
- As a Listed Power Unit, the PoE should be marked as "LPS" or "Limited Power Source".
- This product shall be installed by a qualified service person. Installation shall conform to all local codes.

**Attention**

- Ce produit doit être connecté uniquement à un réseau PoE.
- La puissance nominale de l'alimentation PoE est 48VDC, 0.2A.
- Si la caméra est installée pour une utilisation extérieure, l'alimentation PoE doit être installée avec l'étanchéisation appropriée.
- Comme une unité d'alimentation «Listed», le PoE doit être marqué comme «LPS» ou «Limited Power Source».
- Ce produit doit être installé par un technicien qualifié. L'installation doit se conformer à tous les codes locaux.

3.1.6 Connections and Interfaces

The camera's system cable provides power, network, alarm, and audio connections. A cover on the camera provides access to the camera's microSD card slot and reset button. The camera also has IR LEDs for true day/night operation.

Ethernet Connection

The camera's system cable provides an RJ-45 jack for an Ethernet connection. The camera transmits digital (IP) video output and other data through that connection. FLIR IP cameras support FLIR UVMS video management systems, along with third-party VMSs. These systems tend to evolve and change over time. Therefore, for up-to-date information, contact the local Teledyne FLIR representative or [Teledyne FLIR Support](#).

The camera can output digital video in either NTSC or PAL. You can configure the video format on the [Firmware & Info Page](#).

Alarm I/O Connection

The camera's system cable provides connections for one alarm input signal and one output signal.

Audio I/O Connection

The camera's system cable provides connections for an audio input signal and an output signal.

If you are connecting one or more external microphones, Teledyne FLIR recommends connecting them to ground (GND) using the appropriate pin on the system cable.

For more information connecting the camera, see [Connect the Camera](#).

3.2 Initial Configuration

Teledyne FLIR recommends configuring the camera on a bench or in a lab before mounting and aiming it. However, it is also possible to mount the camera before configuring it, which could be more appropriate for certain installations.

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

Task	DNA tool	Camera's web page
Discover camera IP address	•	
Configure IP address, mask, and gateway	•	•
Configure DNS settings, MTU, and Ethernet speed		•
Change user credentials	•	•

Task	DNA tool	Camera's web page
Change video format	•	•
Configure more than one camera at the same time	•	

Teledyne FLIR recommends [using the DNA tool](#) to discover the camera on the network. For more information about using a supported VMS to configure one or more cameras at the same time, see the VMS documentation.

To configure the camera for the first time:

1. [Connect the Camera](#)
2. [Configure for Networking](#)
3. [Change the Video Format \(Optional\)](#)

Using DNA to Configure the Camera

DNA is a user-friendly utility that easily discovers and configures FLIR Security edge devices on a network. It does not require a license to use and is a free download from the product's support page on [the Teledyne FLIR website](#) (see [Accessing Product Information from the Teledyne FLIR Website](#)).


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

The camera must be made accessible for setting network addresses.

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

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

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

For more information about using the DNA tool, see the *DNA User Guide*. While the software is open, click the Help icon .

3.2.1 Connect the Camera

According to the following information, connect the camera so you can configure it.

System Cable

The system cable includes:

- an RJ-45 jack with an indicator LED for a network connection
- four (2) two-wire leads for alarm and audio I/O connections

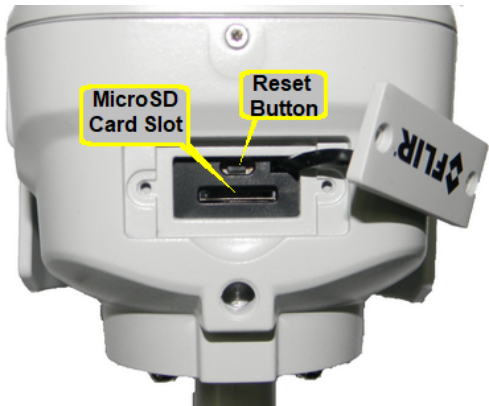


Connections		
1	RJ-45	Ethernet and PoE+
A flashing green LED indicates power on and network activity. If there is no network activity, the LED is not illuminated.		
2	Audio IN	White
	Gnd	Gray
3	Audio OUT	Purple
	Gnd	Yellow
4	Com	Blue
	Alarm OUT	Green
5	Gnd	Light Blue
	Alarm IN	Light Green

Internal Interfaces

To access the camera’s reset button and microSD card slot, remove the access cover by loosening two screws.

To locally store snapshots or recordings triggered by events, a microSD card must be inserted in the camera (min recommended 64GB, up to 128GB, Class 10; not supplied).



microSD Slot / Reset Button Access

Insert a microSDXC card in the slot. Then, replace the cover and screw shut.

To reboot the camera (Partial Reset):

Press the reset button for approximately five seconds. The unit reboots.

Configured settings are saved.

To restore factory defaults (Full Reset):

Press the reset button continuously for 30 seconds.

The unit restores factory defaults, including the original network settings.

If a Basic Video Analytics license was in use, it needs to be re-loaded.

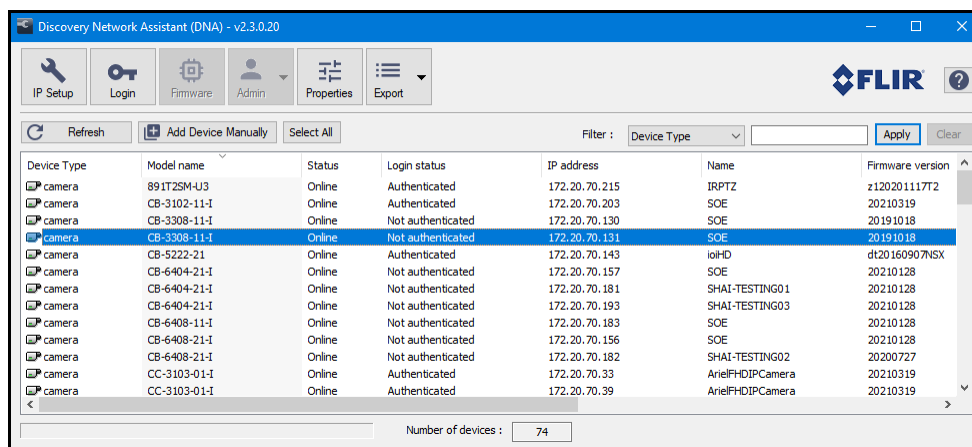
3.2.2 Configure for Networking

By default, DHCP is enabled on the camera and a DHCP server on the network assigns the camera an IP address. If the camera cannot connect to a DHCP server, the camera's default IP address is 192.168.0.250.

- If the camera is managed by FLIR Horizon or Meridian VMS and the VMS is configured as a DHCP server, the VMS automatically assigns the camera an IP address.
- If the camera is managed by FLIR Latitude VMS or is on a network with static IP addressing, you can manually specify the camera's IP address using the DNA tool or the camera's web page.

To 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.

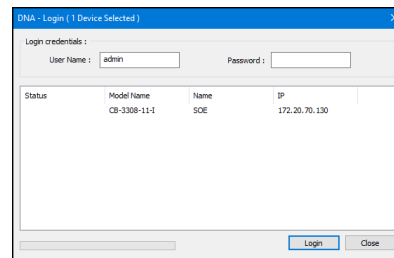
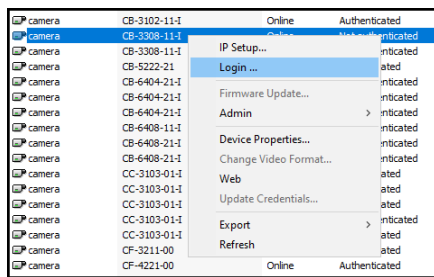


In the DNA Discover List, verify that the camera's status is *Online*.

If this is the first time you are configuring the camera or if it is the first time after resetting the camera to its factory defaults, DNA automatically authenticates the camera with the default password for the camera's admin user (*admin*).

If the admin user password has been changed, you need to authenticate the camera.

In the DNA Discover List, right-click the camera and select **Login**. In the DNA - Login window, type the password for the admin user. If you do not know the admin user password, contact the person who configured the camera's users and passwords.



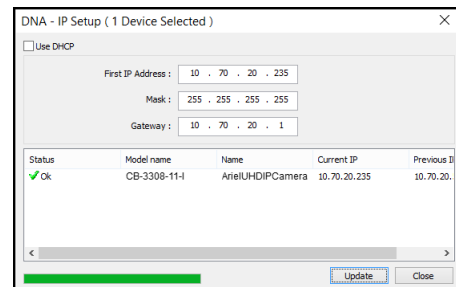
Click **Login**, wait for Ok status to appear, and then click **Close**.

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

3. Change the camera's IP address.

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

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



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

1. [Access the camera's web page](#).
2. On the [Camera Web Page for Administrators](#), click **System Settings**, and make sure the [Network Page](#) appears.
4. Click **Static** IP addressing and then manually specify the camera's Hostname, IP address, Netmask, and Gateway.

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

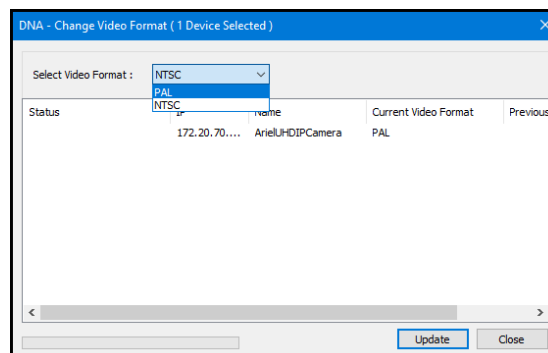
5. Click **Save**. Applying any change on the Network page requires rebooting the camera.

3.2.3 Change the Video Format (Optional)

By default, NTSC is the camera's video format.

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

1. In the DNA Discover List, right-click the camera and select **Change Video Format**.
2. In the Change Video Format window, select **PAL**.



3. Click **Update**, wait for  OK status to appear, and then click **Close**.

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

1. Open the [Visible Page](#).
2. Click **Advanced Settings**.
3. For Video Format, click **PAL**.

To apply a change to the Video Format setting, the camera needs to reboot.

3.3 Mounting

To mount and connect the camera:

1. [Fit Mounting Hardware](#)
2. [Mount and Aim the Camera](#)
3. [Waterproof the System Cable Connection](#) (optional)

3.3.1 Fit Mounting Hardware

If required, install the mounting hardware for the camera according to the instructions for the hardware.

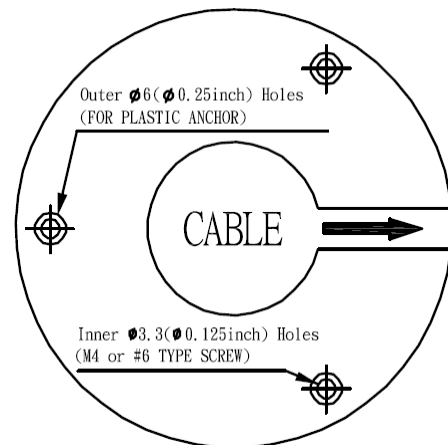
For the list of mounting accessories available from Teledyne FLIR for installing the camera, see [Mounting Accessories](#).

3.3.2 Mount and Aim the Camera

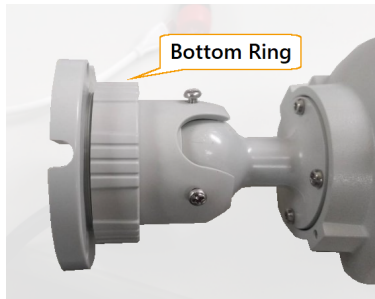
Mount the camera at the site according to your surveillance requirements.

To mount the camera:

1. Be sure to have the required accessories and tools available:
 - Electric screwdriver
 - Phillips screwdriver
 - Electric drill
 - Hammer
 - Mounting accessories (see [Mounting Accessories](#))
2. Remove the protective plastic covering the electronics in the camera body.
3. Mark the drill locations on the ceiling / wall, using the supplied drill template, ensuring correct hole spacing and orientation for cable exit.
4. Drill holes into the surfaces for the screws.
5. Hammer the screw anchors into place.



6. Screw out the bottom camera ring until the mounting plate is separate from the bottom cover.



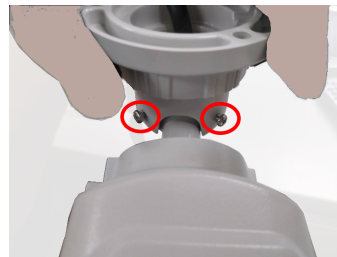
7. Select the preferred camera direction and tighten the bottom cover ring and the screws on the bottom cover.



Set Direction



Tighten Ring



Tighten Screws Carefully

8. Replace the protective plastic covering over the camera's electronics.
9. Attach the safety lanyard from the camera body to the camera cover.
10. Using the Torx wrench, screw the camera cover over the camera body.
11. Align the screw holes on the mounting plate with the positions set out by the template.
12. Using the electric screwdriver, screw the camera body onto the surface.
13. If necessary, [Waterproof the System Cable Connection](#).
14. Connect the system cable to the power, network, and other cables according to the information in [Connect the Camera](#).

3.3.3 Waterproof the System Cable Connection

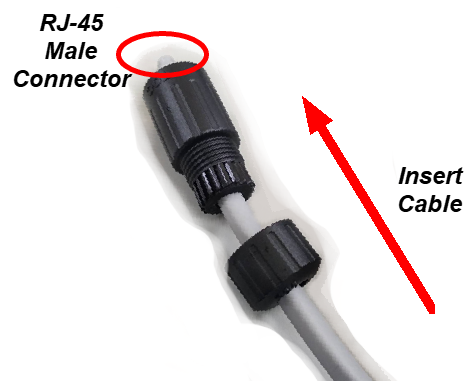
The supplied waterproof cap should be used for connecting the camera to the network cable if the camera is installed in a location prone to moisture.



Waterproof Cable Cap Assembly and Gasket

Assembly Steps

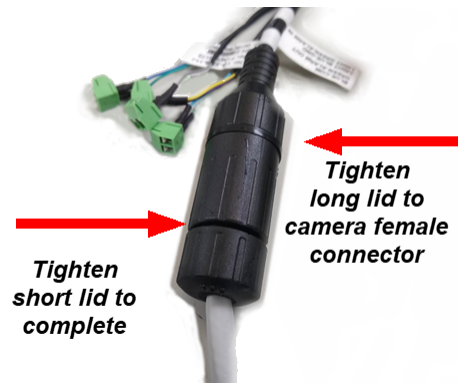
1. Pass the network cable through the short and long caps as shown.



2. Crimp and make off RJ-45 Male connector if plain cable was used.
3. Install rubber gasket on Camera RJ-45 Female cable plug



4. Connect RJ-45 Male to female, tighten long lid onto camera cable connector, and then tighten the short lid to complete the assembly.



3.4 Additional Configuration

Depending on how you are using the CB-330x camera, along with the network and VMS to which it is connected, initial configuration using the camera's web page can also consist of:

- [Configuring the camera's zoom and focus](#)
- [Formatting the microSD card](#)
- [Enabling, calibrating, and configuring the camera's video analytics](#), including acquiring a Basic Video Analytics license
- [Creating users, assign access levels, and change passwords](#)
- [Adjusting the camera's date and time settings](#)
- [Enabling and disabling the camera's alarms](#)
- [Configuring the camera's audio features](#)
- [Uploading sounds for the camera to play](#)
- [Configuring the camera's snapshot settings](#)
- [Configuring the camera's video clip recording settings](#)
- [Enabling and configuring the camera's cybersecurity settings](#)
- [Upgrading the camera's firmware, restoring factory defaults, and other system administration tasks](#)
- [Adjusting the camera's live video and video stream settings](#)
- [Adjusting the camera's image settings](#)
- [Configuring alarm input and output settings](#)
- [Configuring the camera's infrared \(IR\) illumination](#)
- [Enabling and adjusting the camera's OSD settings](#)
- [Enabling and defining privacy zones](#)
- [Defining regions of interest \(ROIs\)](#)
- [Enabling and defining the motion detection zone](#)

Administrators can perform some of these configuration tasks before or after mounting the camera, but other tasks can or should be performed only after mounting and connecting the camera.

3.5 Attach the Camera to a Supported 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 supported VMS.

4 Operation

This chapter provides information about how to [access the camera's web page](#) and how to use it to operate the camera.


4.1 Accessing the Camera's Web Page

To operate the camera, you first need to access it. You can access the camera by logging in to the camera's web page. The camera's web page supports Microsoft Internet Explorer 11, the latest version of Google Chrome®, and other popular web browsers.

To log in to the camera's web page:

1. Do one of the following:

- In the Teledyne FLIR Discovery Network Assistant (DNA) 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 [the Teledyne FLIR website](#). 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. Passwords are case-sensitive.

When logging in to the camera for the first time or for the first time after resetting the camera to its factory defaults, log in as the default Administrator; *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 default Administrator:

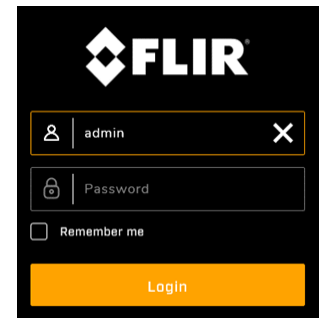
- must be 8-64 characters
- can include the following special characters: @#~!\$&<>+_-.,*?
- cannot include four-digit sequences (for example, 1234)
- cannot include four repeating characters (for example, aaaa)

Log back in using the new password.

The camera's web page opens. The access level assigned to the account logging in determines what appears on the camera's web page:

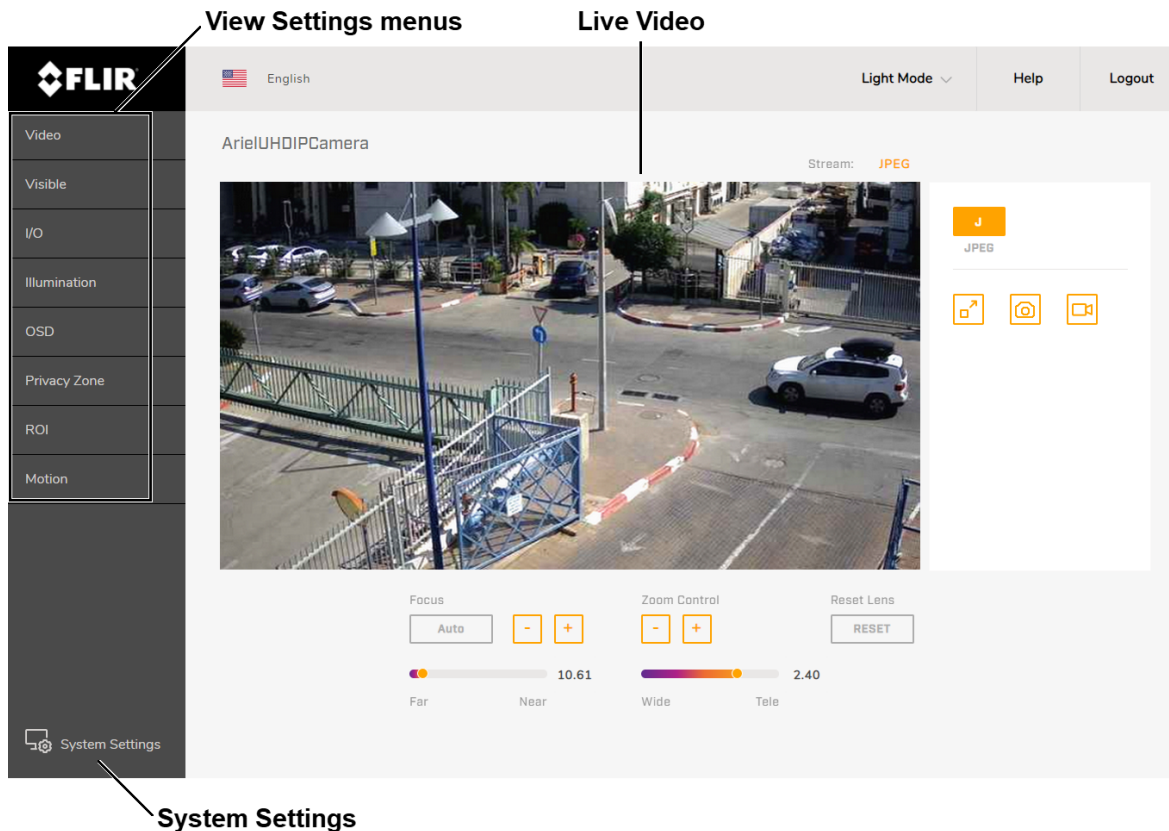
- [Camera Web Page for Administrators](#)
- [Camera Web Page for Other Users](#)

For more information about accounts and access levels, see [Users Page](#).



4.1.1 Camera Web Page for Administrators

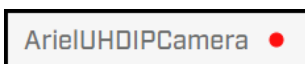
Administrators have full camera web page access.



Camera Web Page for Administrators - Google Chrome
Basic Video Analytics License Not Installed

Above the live video, the following appear:

- **Language**—The language for the camera's web page: English (default), Arabic, Czech, Simplified Chinese, Traditional Chinese, French, German, Hungarian, Italian, Japanese, Polish, Portuguese, Russian, or Spanish.
- **Theme**—Light Mode (default) or Dark Mode. Available on Chrome and Internet Explorer.
- **Logout**—Logs out of the camera's web page.
- **Help**—Opens <https://support.flir.com/>.
- **Camera Name**—As specified on the [Firmware & Info Page](#).
- **SD Card Recording Indicator**—When the camera is actively recording video clips to an installed SD card, a flashing red indicator appears next to the camera name.



- **Live Video Stream Format**—JPEG






Note

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





To the left of the live video, the following View Settings menus appear:

- [Video](#)—Opens the Video page and settings.
- [Visible](#)—Opens the Visible page and settings.
- [I/O](#)—Opens the I/O page and settings.
- [Illumination](#)—Opens open the Illumination page and settings.
- [OSD](#)—Opens the OSD (on-screen display) page and settings.
- [Privacy Zone](#)—Opens the Privacy Zone page and settings.
- [ROI](#)—Opens the ROI (region of interest) page and settings.
- [Motion](#)—Opens the Motion page and settings.
- [Video Analytics](#)—Opens the Video Analytics page and settings. Appears when a Basic Video Analytics (BVA) license has been properly installed on the camera.

To the right of the live video, the following appear (when no View Setting menu is open):

- **Stream Format**—J / JPEG.
-  **Full Screen Button**—Maximizes the live video.
-  **Snapshot Button**—Takes a snapshot of the live video.
-  **Video Recording Button**—Initiates / toggles live video recording.

Under the live video, the following appear:

- **Focus**—To enable Auto Focus, click **Auto**. To manually focus the camera:
 - Click the  or  buttons.
 - Move the slider between Far (1) and Near (100).
- **Zoom Control**—Manually adjusts the zoom:
 - Click the  or  buttons.
 - Move the slider between Wide (1.00) and Tele (3.00).
- **Reset Lens**—If Auto Focus is enabled but is not produce a clear picture, click **Reset**. Then, enable Auto Focus again. The image refocuses.

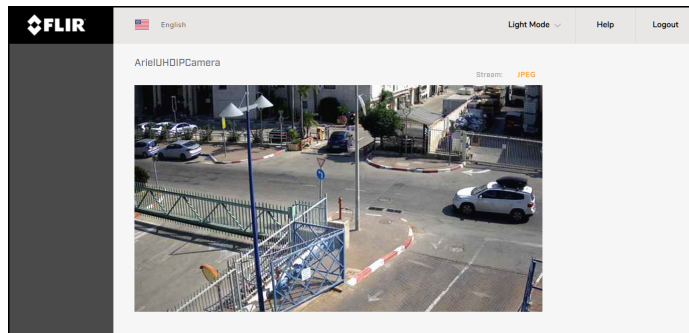
System Settings—Click to configure the camera. For more information, see [Configuration](#).

4.1.2 Camera Web Page for Other Access Levels

What appears on the camera web page for users who are not Administrators and the actions they can perform depends on the access level assigned to the user.

A User can:

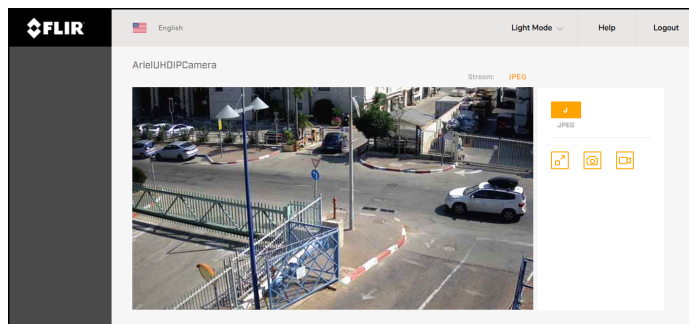
- view live video
- change the web page language
- toggle between Light Mode and Dark Mode
- click **Help**
- log out



Camera Web Page for Users

An Operator can do everything a User can, plus:

- view live video in full screen mode
- take and store a snapshot
- initiate / toggle live video recording



Camera Web Page for Operators

4.2 Making Changes to Settings

The camera stores the following sets of settings:

- **Factory default settings**—The settings when you first connect the camera to power, and when resetting the camera to its factory default settings (see [Firmware & Info Page](#)).
 - **Full Reset**—Restores all of the camera's factory default settings, including its factory default networking settings.
 - **Partial Reset**—Retains some currently saved settings and restores all of the camera's other factory default settings. Retains the following currently saved settings: networking (including, for example, IP addressing mode, IPv4 address, IPv4 subnet mask, and IPv4 default gateway; TV format; and image rotation).
- **Saved settings**—The settings you save as you operate and configure the camera. When the camera reboots, it restores these settings. Unsaved setting changes are lost.



Tip

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

View Settings

When an Administrator makes a change on many View Settings pages, the **Reset** link and **Save** button become enabled. On some View Settings pages, only a **Reset** link becomes enabled.



Depending on the page and the setting being changed, the camera does one of the following:

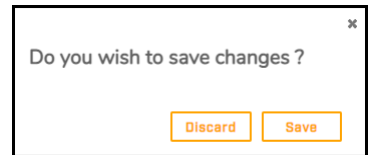
- immediately applies the change, but does not save them
- immediately applies and saves the change
- does not apply change until you save it

Regardless of whether the camera has already applied changes, to save all changes made to settings on the current page since the last time the page's settings were saved, click **Save**. This can include changes made earlier that were not saved.

To restore the previously saved settings for the current page, click **Reset**.

**Tip**

If you try to navigate to a different page before saving changes, a confirmation message appears. You can discard the changes; save them; or close the confirmation message without discarding the changes or saving them by clicking the close icon ✕.



System Settings

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

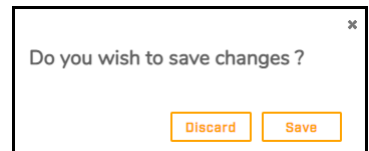


Regardless of whether the camera has already applied changes, to save changes, click **Save**. To discard changes and restore previously saved settings or the factory default settings, click **Discard Changes**.

Changes to some System Settings require the camera to reboot. After clicking **Save**, a confirmation message appears. To save the changes, and reboot the camera with the changes applied, click **Save**. To discard the changes, click **Discard** or close the confirmation message by clicking the close icon ✕.

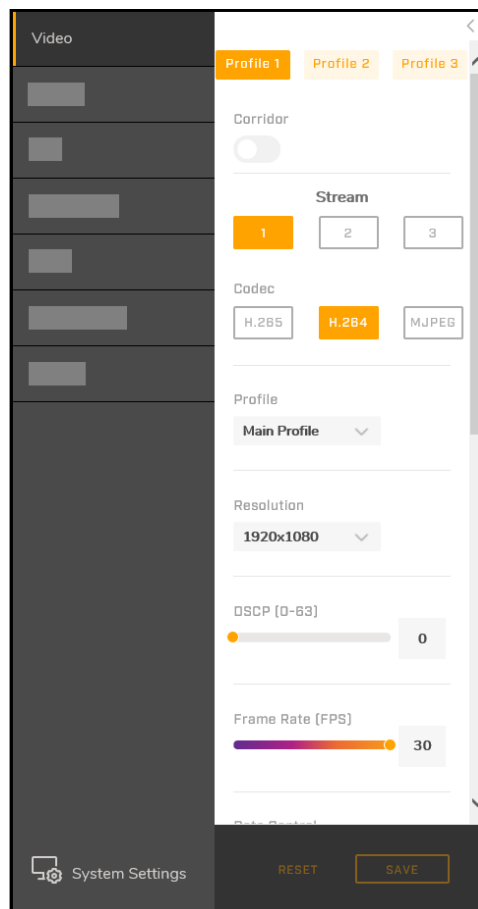
**Tip**

If you try to navigate away from the page before saving changes, a confirmation message appears. You can discard the changes; save them; or close the confirmation message without discarding the changes or saving them by clicking the close icon ✕.



4.3 Video Page

On the Video page, Administrators can configure three video profiles. For each profile, you can configure each of the camera's three concurrent streams separately for optimized quality and bandwidth.



Click **Profile 1**, **Profile 2**, or **Profile 3**.

If you want the image rotated 90° counter-clockwise (to the left) and displayed in vertically oriented 9:16 aspect ratio, enable Corridor. Corridor mode is recommended when monitoring a long, narrow area, such as an aisle, hallway, or corridor. In Latitude, it is *90 and 270 degrees* mode.



Notes

- In Corridor mode, only the H.264 codec is supported.
- Enabling Corridor mode disables analytics rules, if defined.

For each stream in each profile, you can configure the following settings:

- **Codec**—H.265, H.264 (default), or MJPEG, based on required image quality and storage space.
- **Resolution** and **Frame Rate**—For information about the resolutions and maximum frame rates available for specific CB-330x models, see:
 - [4MP Camera Video Resolutions](#)
 - [4K Camera Video Resolutions](#)
- **DSCP**—Differentiated Services Code Point (0-63). The default is 0 (disabled).

The DSCP value defines the priority level or QoS (Quality of Service) for the specified type of traffic. The higher the value that is entered, the higher the priority, which reduces network delay and congestion. The camera supports the Video DSCP class, which consists of applications such as HTTP, RTP/RTSP, and RTSP/HTTP.

**Note**

Remember to synchronize the QoS setting of the camera with the network router.

The other available video stream settings depend on the codec selected. For H.265 and H.264, the following settings are available:

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

		H.265	H.264
High Profile	Primary profile for HD broadcast applications, providing the best trade-off between storage size and video latency. It can save 10-12% of the storage cost over Main Profile. However, it may also increase video latency, depending on the stream structure.	N/A	Default
Main Profile	Provides improved picture quality at reduced bandwidths and storage costs and is becoming more common as the camera processors (DSPs) become more able to handle the processing load. Main Profile can save 10-12% over Baseline.	Default	N/A
Baseline Profile	Primarily for low-cost applications that require additional data loss robustness, such as videoconferencing and mobile applications. This is the most common profile used in IP security cameras due to the low computational cost of processing the video.	N/A	Available

- **Rate Control**

CBR (Constant Bit Rate)	Specify a constant, maximum bit rate, in kilobits per second (kbps). CBR does not optimize storage or quality, because it does not allocate enough data for complex video resulting in degraded quality and allocates too much data for simple video. Specifying a higher bit rate results in better quality but requires more storage.		
CVBR (Constrained Variable Bit Rate)	Varies the amount of data per time segment, up to the specified maximum bit rate. CVBR supports both a higher bit rate for more complex video or audio requiring more storage space, and a lower bit rate for less complex video requiring less storage space.		
CBR Bit Rate	The higher the bit rate, the better the image quality. Set the maximum bit rate high enough to allow for a high instantaneous bit rate for more complex video. A higher bit rate consumes more storage space. The default settings are 3795 kbps for stream 1, 1382 kbps for Stream2, and 750 kbps for Stream3.	H.265	H.264
CVBR Max Bit Rate		64 ~ 8000	64 ~ 20000
CVBR Encoding Priority	Adjusts the quality of the picture along a single axis. The slider ranges from 1 (low bit rate) to 10 (high picture quality). The default setting is 7.		

- **GOP**—The GOP is a group of successive pictures within a coded video stream. Each coded video stream consists of successive GOPs. GOP structure specifies the order in which intra-coded frames and inter-coded frames are arranged. The GOP uses I-Frames (Intra-coded Frames), which are static image files (frames), as a reference for efficient H.265 / H.264 video compression. Transmitted video frames are compared to the I-Frame as they are transmitted. Video quality is higher when the interval between I-Frames is shorter, but the video needs more network capacity. When the interval between I-Frames is longer, the video transmission uses less bandwidth, but the video quality is lower. The default is 30 for NTSC and 25 for PAL (one I-Frame transmitted every second). Set the GOP to a value from 1-60 (NTSC) or 1-50 (PAL).

For MJPEG encoding, you can configure the Quality Level; select High, Mid, or Low. The default is Mid. High produces the highest image quality, but increases the file size. Low produces the lowest image quality and decreases the file size.

URL—Determines the stream's URL. The default for each stream is streamx, where x is the stream number. Using the camera's default IP address (192.168.0.250), default RTSP port (554), and the default URL value for each video stream, the default URLs for each RTSP video stream are:

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



Note

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

Multicast

The camera uses the RTSP protocol to transmit encoded video streams. The protocol establishes the connection and controls the streaming data between the camera and a device over the web. Each stream can be sent to one device (unicast) or to multiple devices (multicast). Unicast requires more network bandwidth and more server resources, but is more stable than multicast, which requires additional settings.

Configure the settings for the multicast IP address the camera uses for video and audio streaming.



Note

Switches, routers and devices must be configured to support multicast.

Address Type—

- **Auto**—A connected application such as a VMS automatically determines the camera's multicast IP address. This is the default Address Type.
- **Manual**—Specify the camera's multicast:
 - **Video Address**—A valid multicast address in the range 224.0.1.1-239.255.255.254.
 - **Video Port**—The port the camera uses for multicast video streaming.
 - **Audio Address**—A valid multicast address in the range 224.0.1.1-239.255.255.254.
 - **Audio Port**—The port the camera uses for multicast audio streaming.
 - **Metadata Address**—A valid multicast address in the range 224.0.1.1-239.255.255.254.
 - **Metadata Port**—The port the camera uses for multicast metadata streaming.

Metadata—Enables or disables metadata in the stream (ON / OFF). The default is ON (enabled).

Multicast Video Auto Start—ON or OFF. The default is OFF (disabled).

Multicast Audio Auto Start—ON or OFF. The default is OFF (disabled).

4.3.1 4MP Camera Video Resolutions

CB-3304 cameras support up to three simultaneous video streams, up to: 4MP on stream 1, Full HD 1080p on stream 2, and HD 720p on stream 3.

**Notes**

- Stream 1 supports 2560 x 1440 @ 25 fps only when operating with D1.
- Corridor mode does not operate with MJPEG compression.

The following resolutions and maximum frame rates are available:

H.265/H.264-Only	
PAL	NTSC
2560 x 1440 (25 fps)	2560 x 1440 (30 fps)
1920 x 1080 (25 fps)	1920 x 1080 (30 fps)
1280 x 720 (25 fps)	1280 x 720 (30 fps)
720 x 576 (25 fps)	720 x 480 (30 fps)

H.265/H.264 + H.265/H.264/MJPEG (NTSC)	
Stream 1	Stream 2
2560 x 1440 (15 fps @ H.264/H.265)	1920 x 1080 (15 fps @ H.264/H.265/MJPEG)
	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
	720 x 480 (15 fps @ H.264/H.265/MJPEG)
2560 x 1440 (25 fps @ H.264/H.265)	720 x 480 (25 fps @ H.264/H.265/MJPEG)
1920 x 1080 (30 fps @ H.264/H.265)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)
	720 x 480 (30 fps @ H.264/H.265/MJPEG)
1280 x 720 (30 fps @ H.264/H.265/MJPEG)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)
	720 x 480 (30 fps @ H.264/H.265/MJPEG)
720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)

H.265/H.264 + H.265/H.264/MJPEG (PAL)	
Stream 1	Stream 2
2560 x 1440 (15 fps @ H.264/H.265)	1920 x 1080 (15 fps @ H.264/H.265/MJPEG)
	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
	720 x 576 (15 fps @ H.264/H.265/MJPEG)
2560 x 1440 (25 fps @ H.264/H.265)	720 x 576 (25 fps @ H.264/H.265/MJPEG)
1920 x 1080 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)
1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)
720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)

H.265/H.264 + H.265/H.264/MJPEG + H.265/H.264/MJPEG (NTSC)		
Stream 1	Stream 2	Stream 3
2560 x 1440 (15 fps @ H.264/H.265)	1920 x 1080 (15 fps @ H.264/H.265/MJPEG)	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
		720 x 480 (15 fps @ H.264/H.265/MJPEG)
	1280 x 720 (15 fps @ H.264/H.265/MJPEG)	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
		720 x 480 (15 fps @ H.264/H.265/MJPEG)
	720 x 480 (15 fps @ H.264/H.265/MJPEG)	720 x 480 (15 fps @ H.264/H.265/MJPEG)
		720 x 480 (15 fps @ H.264/H.265/MJPEG)
1920 x 1080 (30 fps @ H.264/H.265/MJPEG)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)
		720 x 480 (30 fps @ H.264/H.265/MJPEG)
	720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)
1280 x 720 (30 fps @ H.264/H.265/MJPEG)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)
		720 x 480 (30 fps @ H.264/H.265/MJPEG)
	720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)
720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)
H.265/H.264 + H.265/H.264/MJPEG + H.265/H.264/MJPEG (PAL)		
Stream 1	Stream 2	Stream 3
2560 x 1440 (15 fps @ H.264/H.265)	1920 x 1080 (15 fps @ H.264/H.265/MJPEG)	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
		720 x 576 (15 fps @ H.264/H.265/MJPEG)
	1280 x 720 (15 fps @ H.264/H.265/MJPEG)	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
		720 x 576 (15 fps @ H.264/H.265/MJPEG)
	720 x 576 (15 fps @ H.264/H.265/MJPEG)	720 x 576 (15 fps @ H.264/H.265/MJPEG)
		720 x 576 (15 fps @ H.264/H.265/MJPEG)
1920 x 1080 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
		720 x 576 (25 fps @ H.264/H.265/MJPEG)
1280 x 720 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)
		720 x 576 (25 fps @ H.264/H.265/MJPEG)
	1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
1280 x 720 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)
		720 x 576 (25 fps @ H.264/H.265/MJPEG)

H.265/H.264 + H.265/H.264/MJPEG + H.265/H.264/MJPEG (PAL)		
Stream 1	Stream 2	Stream 3
720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)

4.3.2 4K Camera Video Resolutions

The CB-3308 camera supports up to three simultaneous streams, up to: 4K UHD on stream 1, Full HD 1080p on stream 2, and HD 720p on stream 3.



Notes

- Stream 1 supports 3840 x 2160 @ 25 fps only when operating with D1.
- Stream 1 supports Full HD 1080p @ 50/60fps when configured with Auto Shutter Exposure mode.
- Stream 1 supports MJPEG on all resolutions except 3840x2160.
- The frame rate on stream 1 is limited to 15 fps when operating at 4K resolution in Corridor mode.
- Corridor mode does not operate with MJPEG compression.

The following resolutions and maximum frame rates are available:

H.265/H.264-Only	
PAL	NTSC
3840 x 2160 (25 fps)	3840 x 2160 (30 fps)
1920 x 1080 (50 fps)	1920 x 1080 (60 fps)
1920 x 1080 (25 fps)	1920 x 1080 (30 fps)
1280 x 720 (25 fps)	1280 x 720 (30 fps)
720 x 576 (25 fps)	720 x 480 (30 fps)

H.265/H.264/MJPEG + H.265/H.264/MJPEG (NTSC)	
Stream 1	Stream 2
3840 x 2160 (15 fps @ H.264/H.265)	1920 x 1080 (15 fps @ H.264/H.265/MJPEG)
	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
	720 x 480 (15 fps @ H.264/H.265/MJPEG)
3840 x 2160 (25 fps @ H.264/H.265)	720 x 480 (25 fps @ H.264/H.265/MJPEG)
	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
1920 x 1080 (60 fps @ H.264/H.265/MJPEG)	720 x 480 (25 fps @ H.264/H.265/MJPEG)
	1280 x 720 (30 fps @ H.264/H.265/MJPEG)
1920 x 1080 (30 fps @ H.264/H.265)	720 x 480 (30 fps @ H.264/H.265/MJPEG)
	1280 x 720 (30 fps @ H.264/H.265/MJPEG)
1280 x 720 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)
	720 x 480 (30 fps @ H.264/H.265/MJPEG)
720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)

H.265/H.264/MJPEG + H.265/H.264/MJPEG (PAL)	
Stream 1	Stream 2
3840 x 2160 (15 fps @ H.264/H.265)	1920 x 1080 (15 fps @ H.264/H.265/MJPEG)
	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
	720 x 576 (15 fps @ H.264/H.265/MJPEG)

H.265/H.264/MJPEG + H.265/H.264/MJPEG (PAL)	
Stream 1	Stream 2
3840 x 2160 (25 fps @ H.264/H.265)	720 x 576 (25 fps @ H.264/H.265/MJPEG)
1920 x 1080 (50 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)
1920 x 1080 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)
1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)
720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)

H.265/H.264/MJPEG + H.265/H.264/MJPEG + H.265/H.264/MJPEG (NTSC)		
Stream 1	Stream 2	Stream 3
3840 x 2160 (15 fps @ H.264/H.265)	1920 x 1080 (15 fps @ H.264/H.265/MJPEG)	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
		720 x 480 (15 fps @ H.264/H.265/MJPEG)
	1280 x 720 (15 fps @ H.264/H.265/MJPEG)	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
		720 x 480 (15 fps @ H.264/H.265/MJPEG)
	720 x 480 (15 fps @ H.264/H.265/MJPEG)	720 x 480 (15 fps @ H.264/H.265/MJPEG)
		720 x 480 (15 fps @ H.264/H.265/MJPEG)
1920 x 1080 (60 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
	720 x 480 (25 fps @ H.264/H.265/MJPEG)	720 x 480 (25 fps @ H.264/H.265/MJPEG)
1920 x 1080 (30 fps @ H.264/H.265/MJPEG)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)
	720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)
1280 x 720 (30 fps @ H.264/H.265/MJPEG)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)	1280 x 720 (30 fps @ H.264/H.265/MJPEG)
	720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)
720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)	720 x 480 (30 fps @ H.264/H.265/MJPEG)

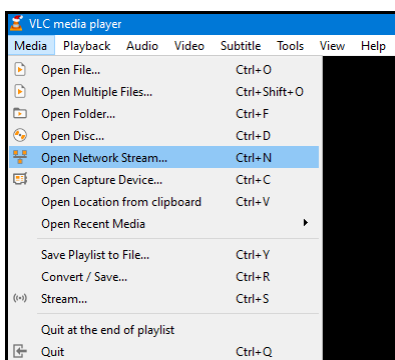
H.265/H.264/MJPEG+ H.265/H.264/MJPEG + H.265/H.264/MJPEG (PAL)		
Stream 1	Stream 2	Stream 3
3840 x 2160 (15 fps @ H.264/H.265)	1920 x 1080 (15 fps @ H.264/H.265/MJPEG)	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
		720 x 576 (15 fps @ H.264/H.265/MJPEG)
	1280 x 720 (15 fps @ H.264/H.265/MJPEG)	1280 x 720 (15 fps @ H.264/H.265/MJPEG)
		720 x 576 (15 fps @ H.264/H.265/MJPEG)
1920 x 1080 (50 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
		720 x 576 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)
1920 x 1080 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
		720 x 576 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)
1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
		720 x 576 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)
720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)

4.4 Using a Media Player to View Camera Video

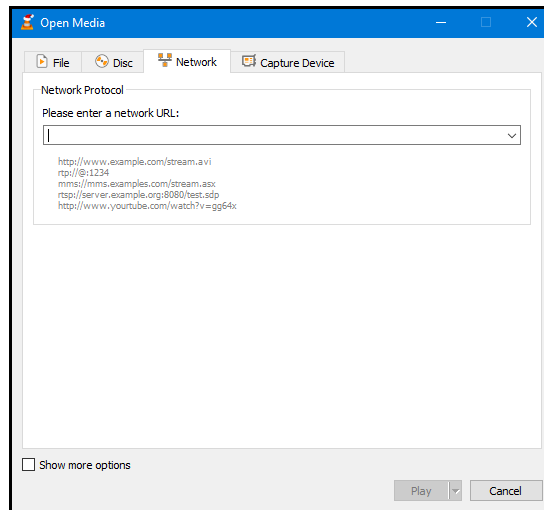
You can monitor any of the camera's video streams with a media player that supports streaming; for example, VLC (download from <http://www.videolan.org/vlc/index.html>).

To view one of the camera's video streams using VLC:

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



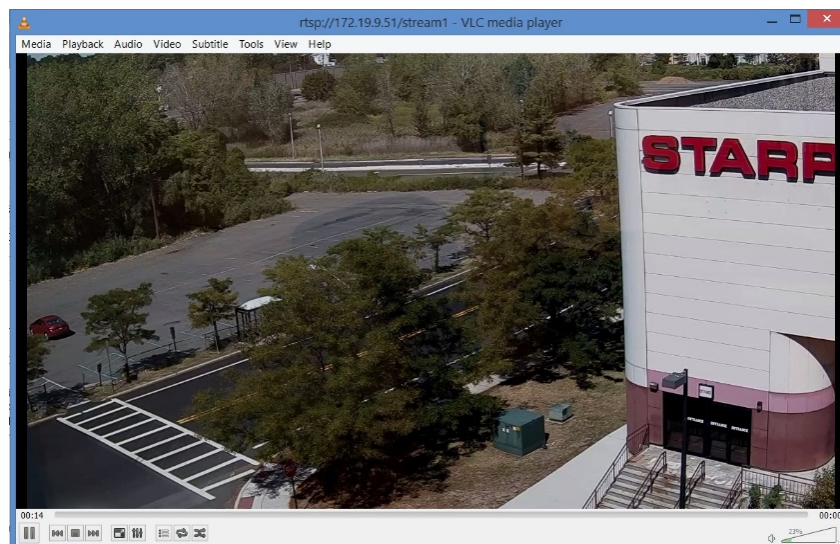
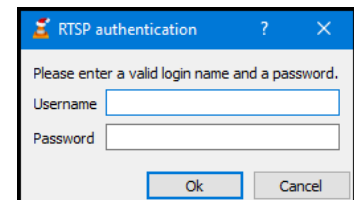
The Open Media screen appears.



3. On the Network tab, specify the network URL for the camera's video stream. The network URL syntax is: `rtsp://(camera IP address):(camera RTSP port)/(stream URL)`. Using the camera's default IP address (192.168.0.250), default RTSP port (554), and the default URL value for each video stream, the default network URLs for each RTSP video stream are:
 - **Stream 1**—`rtsp://192.168.0.250:554/stream1`
 - **Stream 2**—`rtsp://192.168.0.250:554/stream2`
 - **Stream 3**—`rtsp://192.168.0.250:554/stream3`
1. Click **Play**.

If RTSP authentication has been enabled on the [RTSP Page](#), use any of the camera's configured accounts to access the video stream.

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



4.5 Visible Page

On the Visible page, Administrators can configure picture quality, focus, zoom, and other image settings.

Brightness—Between -100 (minimum overall image brightness) and 100 (maximum). The default is 0.

Exposure Value—A combination of a camera's shutter speed and f-number that brightens or darkens the overall scene, between -6 (darkest overall exposure) and 6 (brightest overall exposure). The default is 0. Not available in Manual exposure mode.

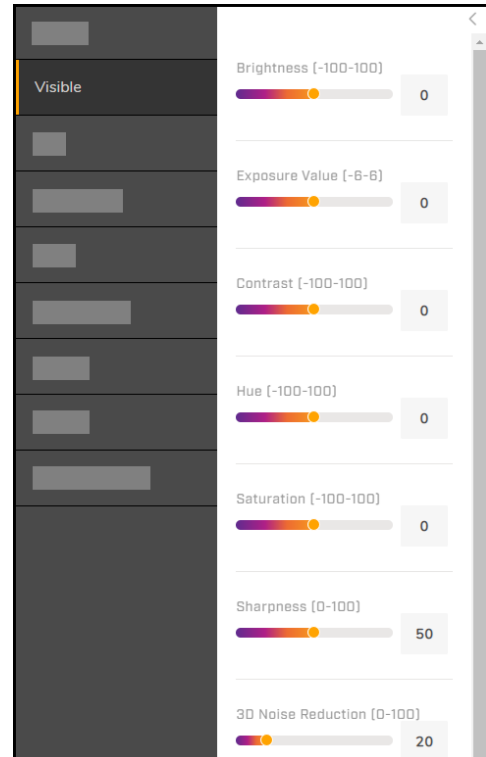
Contrast—Between -100 (minimum overall image contrast) and 100 (maximum). The default is 0.

Hue—Color, between -100 (warmest) and 100 (coolest). The default is 0.

Saturation—Amount of color, between -100 (no color; that is, grayscale / black-and-white video) and 100 (maximum color; that is, reddest reds and bluest blues). The default is 0.

Sharpness—Amount of digital edge and small feature sharpness enhancement, between 0 (no sharpness enhancement) and 100 (maximum sharpness enhancement). The default is 40.

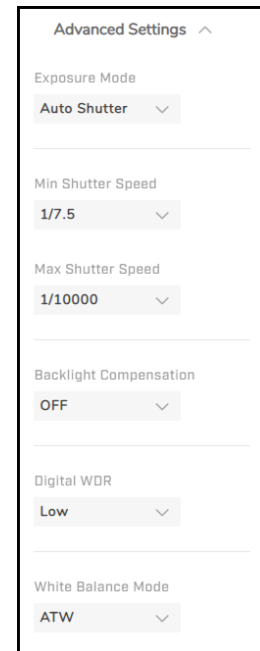
3D Noise Reduction—Amount of digital low-light noise reduction, between 0 (no noise reduction) and 100 (maximum noise reduction). The default is 20.



Advanced Settings

Exposure Mode—Basic exposure settings and day/night settings. Configurable settings depend on the selected exposure mode.

- **Auto**—The camera uses as references the selected Exposure Value, the configured minimum shutter speed, and the configured minimum shutter speed. It completely opens the iris, and adjusts gain and other parameters to achieve a consistent exposure level in the images. This is the default exposure mode and is recommended for outdoor environments and indoor environments with fluorescent lighting as the main light source.
- **Flickerless**—Eliminates flicker in indoor applications where fluorescent lighting is used. The darker the ambient lighting, the slower the shutter speed should be.
- **Shutter Priority**—Select a fixed shutter speed. The camera adjusts the iris, gain, and other exposure parameters to achieve a consistent exposure level in the images.
- **Auto Iris**—Using the selected Exposure Value, the configured minimum shutter speed, and the configured minimum shutter speed as references, the camera adjusts the iris, gain, and other exposure parameters to achieve a consistent exposure level in the images.
- **Manual**—Select a fixed P iris level (1-5), shutter speed, and gain (0-36). Increasing the P iris level or selecting a faster shutter speed decreases the amount of light entering the image sensor, which therefore produces a darker image. Likewise, decreasing the P iris level or selecting a slower shutter speed increases the amount of light entering



Visible Page Advanced Settings - Shutter WDR Exposure Mode Selected

the sensor, producing a brighter image with more detail. By default, gain is disabled (0). Utilizing gain and increasing its level increases sensor sensitivity, but can also increase noise in the image.

- **Shutter WDR**—For scenes with high contrast or changing light conditions, the camera combines two frames taken with slow- and fast-exposure shutter speeds into a single frame with a wide dynamic range. The camera uses an algorithm that determines the optimal mix of light and dark regions within the scene.

Minimum Shutter Speed—Available in Auto and Auto Iris exposure modes. Select a suitable minimum shutter speed according to the environmental luminance, in fractions of a second. The video format determines the shutter speeds available.

Minimum Shutter Speed					
PAL			NTSC		
1/2	1/100	1/1000	1/2	1/120	1/1000
1/4	1/200	1/2000	1/4	1/200	1/2000
1/6.25	1/250	1/2500	1/7.5	1/250	1/2500
1/12.5	1/400	1/4000	1/15	1/400	1/4000
1/25	1/500	1/5000	1/30	1/500	1/5000
1/50	1/800	1/8000	1/60	1/800	1/8000

Maximum Shutter Speed—Available in Auto and Auto Iris exposure modes. Select a suitable maximum shutter speed according to the environmental luminance.

Maximum Shutter Speed					
PAL			NTSC		
1/100	1/800	1/5000	1/120	1/800	1/5000
1/200	1/1000	1/8000	1/200	1/1000	1/8000
1/250	1/2000	1/10000	1/250	1/2000	1/10000
1/400	1/2500	1/32000	1/400	1/2500	1/32000
1/500	1/4000		1/500	1/4000	



Caution

Using a slow shutter speed causes moving objects to be blurred.

Attention

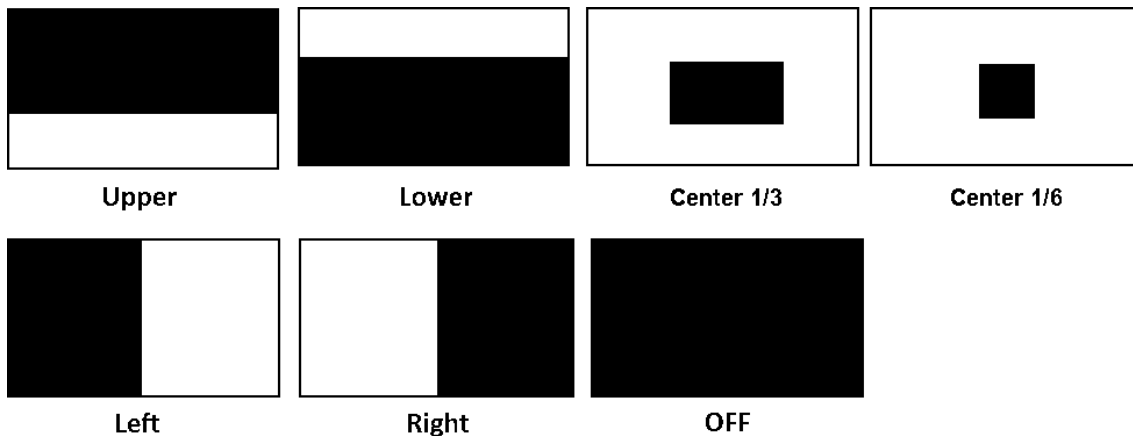
L'utilisation de vitesses d'obturation faibles peut rendre les objets en mouvement flous.

Shutter Speed—Available in Shutter Priority and Manual exposure modes. Select a suitable fixed shutter speed according to the environmental luminance.

Shutter Speed					
PAL			NTSC		
1/6.25	1/250	1/2500	1/7.5	1/250	1/2500
1/12.5	1/400	1/4000	1/15	1/400	1/4000

Shutter Speed					
PAL			NTSC		
1/25	1/500	1/5000	1/30	1/500	1/5000
1/50	1/800	1/8000	1/60	1/800	1/8000
1/100	1/1000	1/10000	1/120	1/1000	1/10000
1/200	1/2000	1/32000	1/200	1/2000	1/32000

Backlight Compensation—Not available in Manual exposure mode. By default, backlight compensation is disabled (OFF). When a bright light source is located behind the area of interest, the area of interest appears in silhouette. Enabling backlight compensation adjusts the exposure of the entire image to properly expose the area of interest in the foreground. Select the setting that most closely corresponds to the area of interest: OFF (default), Upper, Lower, Central 1/3rd, Central 1/6th, Left, or Right.



Backlight Compensation Settings

Digital WDR—Improves the image quality and amount of detail in high contrast scenes. That is, scenes containing areas with different lighting conditions; some areas are very bright, and others are dark. Without Digital WDR, the image is either overexposed (too bright in bright areas) or underexposed (completely dark in dark areas). Digital WDR helps improve image quality by producing more detail in both the dark and bright areas of the image.

- **High**—Video with the widest dynamic range.
- **Medium** (default)
- **Low**
- **OFF** (disabled)

White Balance Mode—Adjust to create the best color rendition.

- **ATW**—Auto Tracking White Balance (default). Camera continuously detects scene illumination and adjusts color to maintain consistent white balance. Recommended for scenes in which the lighting changes.
- **Auto**—Camera detects current scene illumination and adjusts color accordingly (between 2500°K to 10000°K).
- **Manual**—Based on the type of lighting in the scene, configure the following to achieve accurate white balance:
 - **R Gain**—Adjusts the red in the image (0-511). Increasing the value increases the red. The default is 64.

- **B Gain**—Adjusts the blue in the image (0-511). Increasing the value increases the blue. The default is 64.

To quickly perform white balance, click **One Push**.

Gamma Correction—Ensures faithful reproduction of an image:

- **0.45**—The on-screen image has less contrast than the original image. (default) or 1. When set to 1, the image displayed on your screen is the same as the original image. When set to 0.45,

Day/Night Setting—Controls the IR Cut (IRC) filter for electronic day/night operation.

- **Auto** (default)—Automatic operation according to the ambient light level. The camera automatically switches from Color (daytime) mode to B/W (nighttime) mode at night or in low-light conditions. When there is sufficient light, the camera automatically switches from B/W mode to Color mode. When selected, you can configure the following values:
 - **Switch Time**—Amount of time the switch takes: Fast (three seconds), Normal (seven seconds), or Slow (15 seconds).
 - **Night to Day Sensitivity** and **Day to Night Sensitivity**—Set 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 0-6, where 0 switches modes at a lower light level (darker) and 6 switches modes at a higher light level (brighter). The default setting for both thresholds is 3.

The table below translates these sensitivity settings into the Lux levels at which the camera switches from black and white to color (Night to Day Threshold) and vice versa (Day to Night Threshold).

Setting	Night to Day (Lux)	Day to Night (Lux)
0	15	0
1	14	1
2	13	2
3	12	3
4	11	4
5	10	5
6	9	6

- **Color**—Locks camera in daytime mode.
- **B/W**—Locks camera in nighttime mode.

Enable Enhanced Low Light Performance—ELLP; available on CB-3308 models. When video resolution is set to 4K, ELLP enhances the image and sensitivity. It also keeps cameras in Color mode longer, before switching to B/W mode. Disabled by default. ELLP cannot be enabled when the camera is recording images on an SoE card.

Mirror Flip Setting

Orientation

- **Flip**—Flips the image vertically (upside down).

*Advanced Settings
(Continued)*

- **Mirror**—Flips the image horizontally.
- **Both**—Flips the image upside-down and horizontally.
- **OFF** (default)

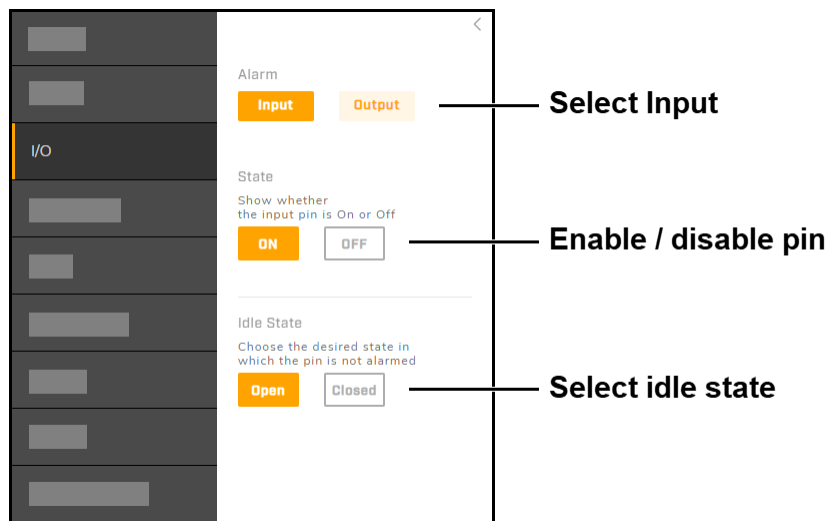
Video Format—PAL or NTSC (default). Changing the video format requires rebooting the camera.

4.6 I/O Page

On the I/O (input / output) page, Administrators can enable, disable, and configure the camera's alarm input and alarm output.

Select **Input** or **Output**, and then specify:

- **State**—Select On (enabled) or Off (disabled).
- **Idle State**—The input / output pin can be normally Open (default) or Closed.



Configuring the Alarm Input

For the output pin, specify the Method.

- **Pulse**—Alarms pulse the output pin state. Specify:
 - **On Time**—Amount of time, in seconds, that the output pin is in its alarm state (0.1~200). If the output pin is normally open, the On Time is the amount of time the pin is closed when the camera is triggering an alarm. The default is 0.1.
 - **Off Time**—Amount of time, in seconds, that the output pin is in its normal state (0.1~200). If the output pin is normally open, the Off Time is the amount of time the pin is open when the camera is triggering an alarm. The default is 0.1.
 - **Count**—Number of post-trigger buffer frames (1-9999). The default is 1.

The screenshot shows a configuration page for an alarm. It has a back arrow at the top left. The sections are:

- Alarm:** Two buttons, 'Input' (orange) and 'Output' (orange). A line points from the 'Output' button to the label 'Select Output'.
- State:** Text 'Show whether the output pin is On or Off'. Two buttons, 'ON' (white) and 'OFF' (orange). A line points from the 'OFF' button to the label 'Enable / disable pin'.
- Idle State:** Text 'Choose the desired state in which the pin is not alarmed'. Two buttons, 'Open' (orange) and 'Closed' (white). A line points from the 'Open' button to the label 'Select Idle State, Method, and Post Duration'.
- Method:** A dropdown menu showing 'Normal'.
- Post Duration:** A dropdown menu showing 'Infinite'.

Configuring the Output Pin - Normal Method Selected

- **Normal**—Alarms change the output pin state for a specified Post Duration, the amount of time that the alarm is triggered:
 - **Infinite**—The output pin remains in its alarm state until the alarm is deactivated. If the output pin is normally open, its alarm state is closed.
 - **5s, 10s, 15s, or 30s**—The output pin remains in its alarm state for five, 10, 15, or 30 seconds, and then changes back to its normal state.

For information about the camera's physical I/O connections, see [Connect the Camera](#).

4.7 Illumination Page

Administrators can configure the following IR LED settings on the Illumination page:

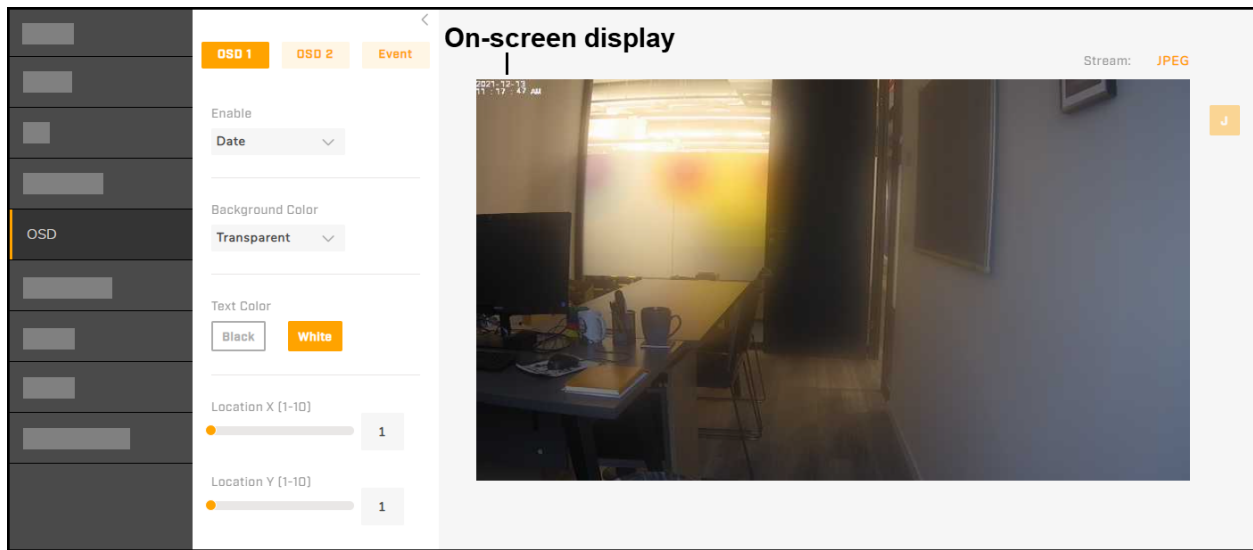
- **Infrared light**—Specify the IR LED operation state:
 - **Auto**—Camera automatically switches from Day mode (color video; IR LEDs off) to Night mode (black and white video; IR LEDs on) according to the ambient light level. You can set the night-to-day and day-to-night thresholds on the [Visible Page](#). This is the default state.
 - **On**—IR LEDs are permanently on.
 - **Off**—IR LEDs are permanently off.
- **LED Brightness (Broad / Narrow)**—High (default), Medium, or Low. When set to High, the camera switches with almost no delay between day / color and night / B/W modes.

The screenshot shows the 'Illumination' configuration page. It has a back arrow at the top right. The sections are:

- Choose a static state or Auto state that corresponds to the surrounding lighting:** Text above the 'Infrared light' section.
- Infrared light:** Text above three buttons: 'ON' (white), 'OFF' (white), and 'Auto' (orange).
- LED Brightness (Broad):** A dropdown menu showing 'High'.
- LED Brightness (Narrow):** A dropdown menu showing 'High'.

4.8 OSD Page

On the OSD (on-screen display) page, Administrators can configure settings for the background color, text color, and location for displaying the date or text in two configurable locations in the camera's video streams and in live video. You can also configure a background color and a text color upon the occurrence of an event.



Date Enabled on OSD1

Select **OSD 1**, **OSD 2**, or **Event**. For OSD 1 and OSD 2, you can enable the Date or a specify a Text Input to appear on-screen. By default, OSD 1 and 2 are disabled (OFF).

For all OSDs, you can configure:

- **Background Color**—Black or Transparent (default).
- **Text Color**—Black or White (default).
- **Location X**—Horizontal location on the screen for the selected OSD, where 1 = far left and 10 = far right. The default setting is 1 (far left).
- **Location Y**—Vertical location on the screen for the selected OSD, where 1 = top and 10 = bottom. The default setting is 1 (top).

	1	2	3	4	5	6	7	8	9	10
1	1x1	2x1	3x1	4x1	5x1	6x1	7x1	8x1	9x1	10x1
2	1x2	2x2	3x2	4x2	5x2	6x2	7x2	8x2	9x2	10x2
3	1x3	2x3	3x3	4x3	5x3	6x3	7x3	8x3	9x3	10x3
4	1x4	2x4	3x4	4x4	5x4	6x4	7x4	8x4	9x4	10x4
5	1x5	2x5	3x5	4x5	5x5	6x5	7x5	8x5	9x5	10x5
6	1x6	2x6	3x6	4x6	5x6	6x6	7x6	8x6	9x6	10x6
7	1x7	2x7	3x7	4x7	5x7	6x7	7x7	8x7	9x7	10x7
8	1x8	2x8	3x8	4x8	5x8	6x8	7x8	8x8	9x8	10x8
9	1x9	2x9	3x9	4x9	5x9	6x9	7x9	8x9	9x9	10x9
10	1x10	2x10	3x10	4x10	5x10	6x10	7x10	8x10	9x10	10x10

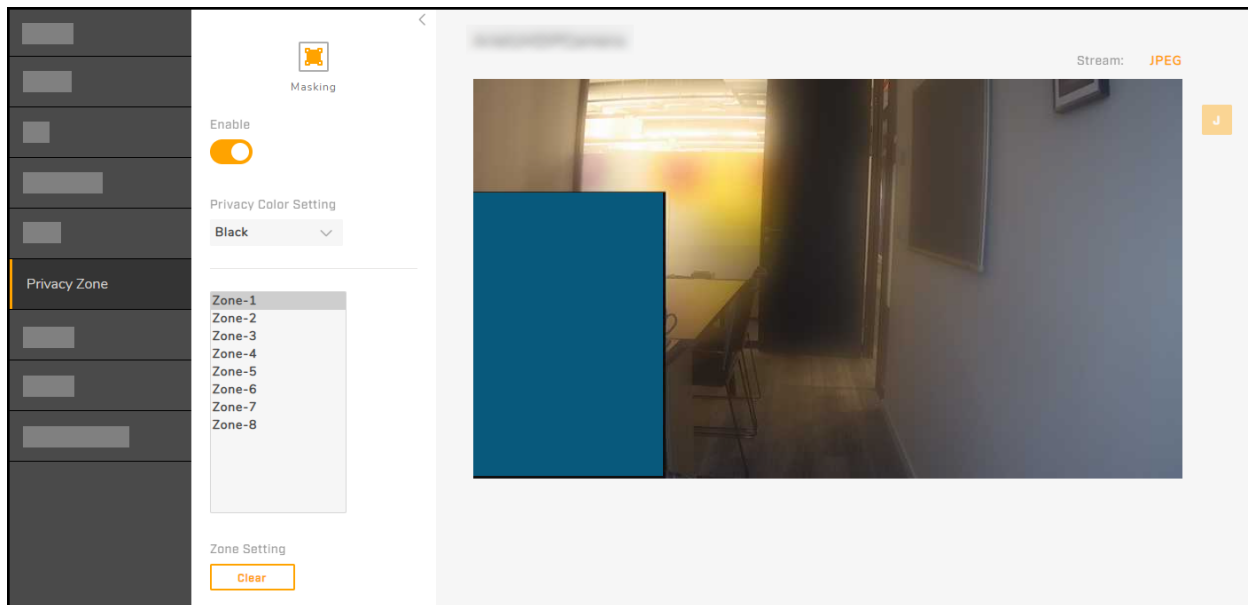
Y-Axis

X-Axis

OSD Location

4.9 Privacy Zone Page

On the Privacy Zone page, Administrators can define up eight privacy zones—areas of the scene the camera masks from appearing in the video streams and in the live video. You can configure the zone size, position, and color.



Zones Enabled - Zone 1 Being Defined

Enable—Enables all eight privacy zones. By default, privacy zones are disabled.

Privacy Color Setting—Color all defined privacy zones appear as in the video streams and in the live video. Black (default), Grey, or White.

To define a privacy zone:

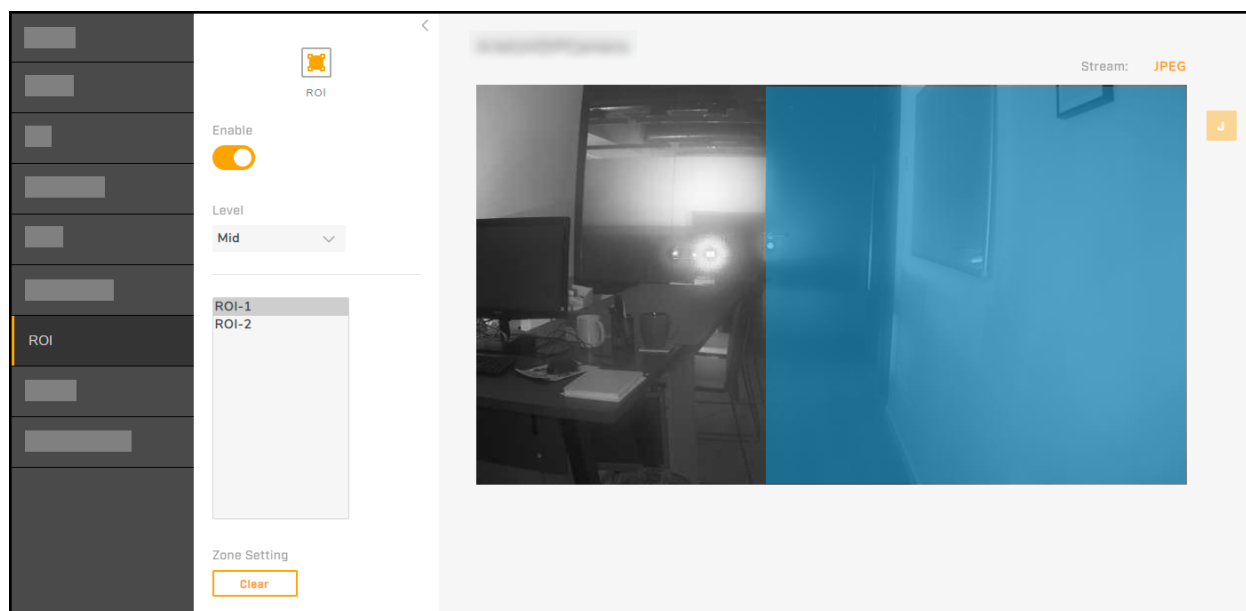
1. Select a privacy zone.
2. Define the zone. Using your mouse, click and drag on the live video.
A translucent bluish rectangle indicates the privacy zone you are defining.
3. Click **Save**. The camera saves the privacy zone, which appears in the live video and in the video streams in the specified privacy color.

Zone Setting

To delete a privacy zone, select the zone, and then click **Clear**. The camera immediately deletes the privacy zone. You do not have to click **Save** to save the change.

4.10 ROI Page

On the ROI (Region of Interest) page, Administrators can configure up to two areas of the scene that the camera streams at a higher quality than the other areas of the scene. Enabling and defining one or more ROIs does not affect the streams' overall bit rate. Improving video quality in areas of the scene that are more important consumes more bandwidth. However, the camera compensates by reducing the video quality and bandwidth consumption for the areas not in the ROI.



ROIs Enabled - One ROI Defined

Enable—Enables ROIs. By default, ROIs are disabled.

Level—Determines the relative video quality for the ROIs. High, Mid (default), or Low.

To define an ROI:

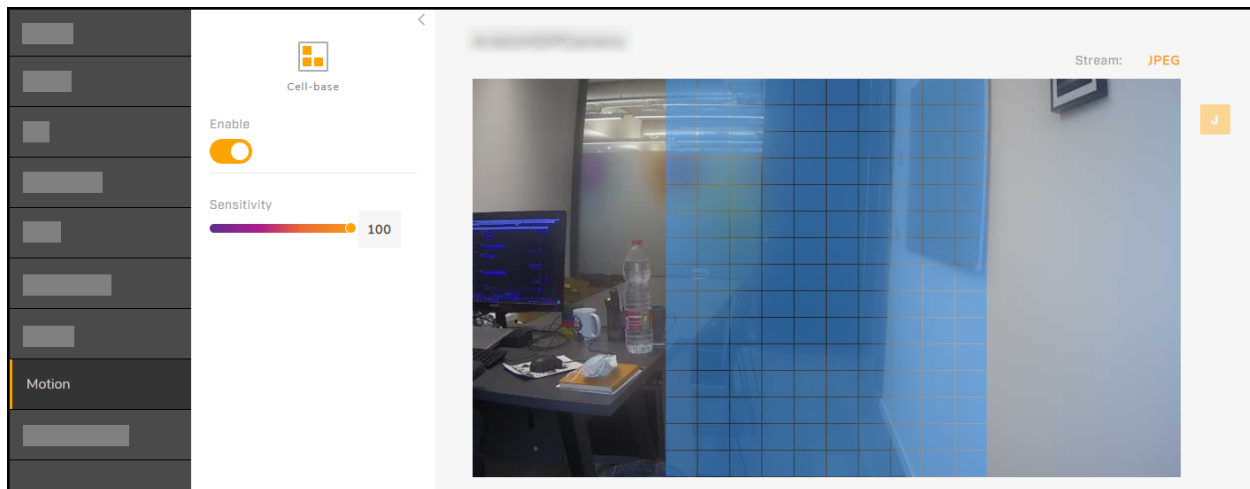
1. Select an ROI.
2. Define the ROI. Using your mouse, click and drag on the live video.
A translucent bluish rectangle indicates the ROI you are defining.
3. Click **Save**. The camera saves the ROI, which continues to appear as a translucent bluish rectangle when viewing the live video on the ROI page, but does not otherwise appear in the live video nor in the video streams.

Zone Setting

To delete an ROI, select the ROI, and then click **Clear**. The camera immediately deletes the ROI. You do not have to click **Save** to save the change.

4.11 Motion Page

On the Motion page, Administrators can enable motion detection, adjust motion detection sensitivity, and define the motion detection zone. After enabling motion detection and defining the motion detection zone, Administrators can define it as the trigger for alarms on the [Alarm Page](#).



Motion Detection Enabled - Zone Defined



Notes

- If the camera is connected to a VMS that supports cell-based motion detection, Teledyne FLIR recommends using the VMS to configure the motion detection zone.
- The camera supports motion detection or Basic Video Analytics, but not both at the same time.

Enable—Enables motion detection. By default, motion detection is disabled.

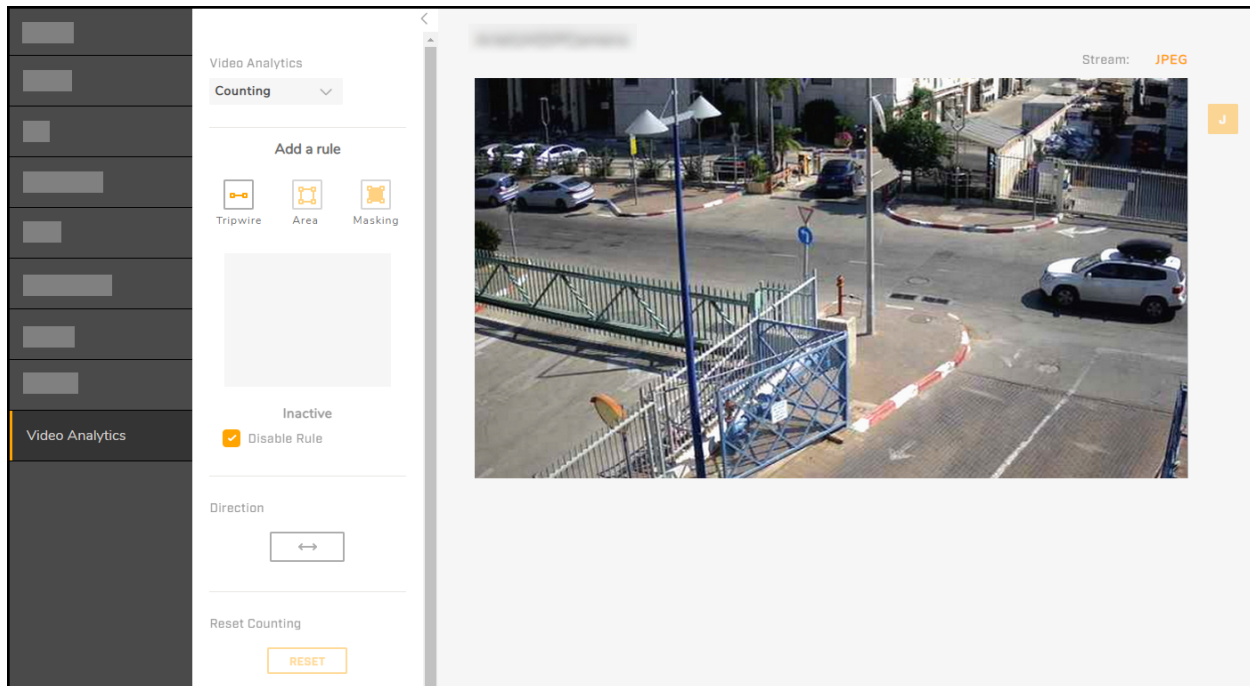
Sensitivity—Amount of sensitivity to motion that triggers an alarm (1-100), with 100 being the highest level of sensitivity (default) and 1 being the lowest.

To define the detection zone:

1. Use your mouse to:
 - Click and drag on the live video to define a detection zone.
 - Click once to add a single cell to the detection zone.
 - Right-click once on a single cell to delete it from the detection zone.
 - Right-click and drag to delete cells from the detection zone.

The detection zone appears as translucent bluish cells in the live video.
2. Click **Save**. The camera saves the motion detection zone, which continues to appear as translucent bluish cells when viewing the live video on the Motion page, but does not otherwise appear in the live video nor in the video streams.

4.12 Video Analytics Page



Video Analytics Page
Counting (Default) Selected - Default Settings

On the Video Analytics page and from the menu under Video Analytics, Administrators can:

- Select and modify [Basic Settings](#)—minimum and maximum object sizes to be detected in a scene
- Select the type of analytic rule appropriate for the physical scene according to the main objective in securing the area:

Rule Type	Purpose	Tripwire or Area	Example
Counting	Count the number of people crossing a line	Up to three separate tripwires working in concert	Monitoring customers entering a store
Border Line	Detect people or vehicles crossing a line		Intrusion detection along a fence
Loitering	Detect encroachment and trespassing based on the time spent in the scene	A single detection area	Monitoring an ATM or outside an apartment building
Area Protection	Detect people or vehicles coming into or going out of the scene		Secure a courtyard from trespassing or a no parking area
Object Removal	Detect objects being removed from the scene	Up to three detection areas	Monitoring shoplifting
Object Dropped	Detect objects being introduced to the scene	A single detection area	Securing public areas, such as transportation hubs, against suspicious objects

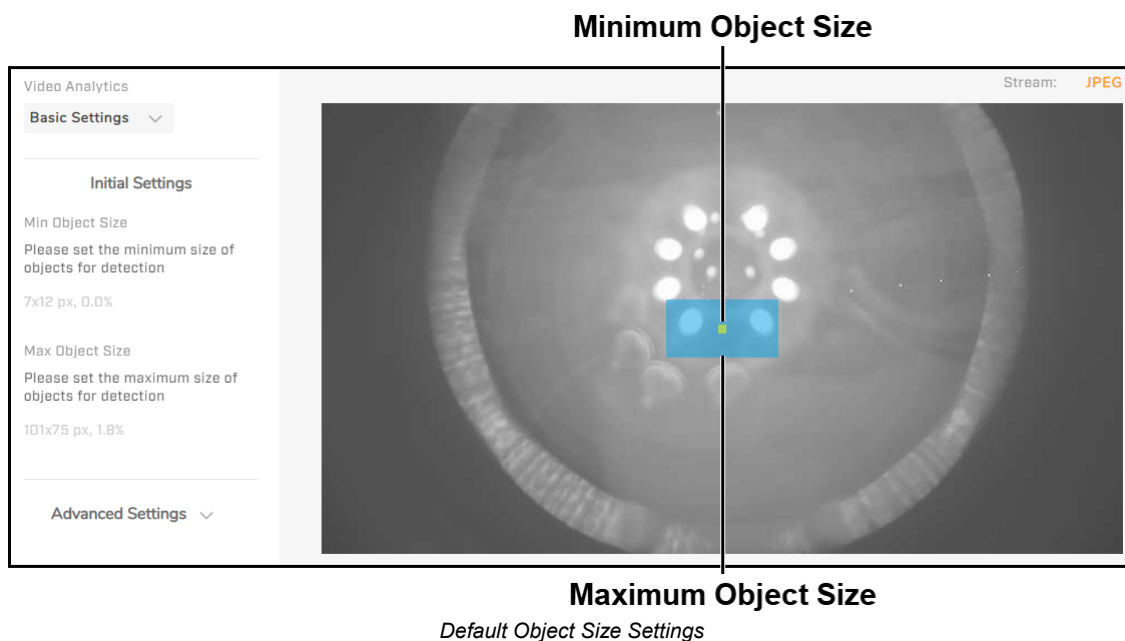
**Notes**

- The Video Analytics menu appears and the page is available when a Basic Video Analytics license has been properly installed. Also when a license has been properly installed, analytics actions appear on the Alarm page. For information about licenses, see [Basic Video Analytics Licenses](#).
- For information about camera distribution and positioning, detection ranges, mounting, and lighting, see [General Guidelines](#).

Basic Settings

Min Object Size—Minimum size of an object for the video analytics to detect

Max Object Size—Maximum size of an object for the video analytics to detect

**To modify the minimum and maximum object sizes:**

1. Click on the minimum object size box (yellow box). The box becomes editable and the maximum object size box disappears.
2. Move or adjust the size of the box. You can:
 - Click and drag the box.
 - Click and drag the corners of the box.
 - Click and draw a new box.
3. Click **Set**. The size of the box is set, but not saved.
4. Repeat the previous steps for the maximum object size box (blue box).
5. Click **Save**.

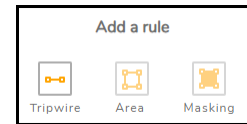
Where the boxes are located in the live video is not important. However, the following are important:

- The object sizes should reflect potential objects in the scene and their correct proportions.
- The object size shapes should be consistent for best results.

In general, the camera should be installed at a height of 2.5-4m, and inclined at an appropriate angle. For more information about positioning, See [Camera Positioning](#).

After configuring the minimum and maximum object sizes and regardless of the rule type selected, Administrators can add rules, configure rule type-specific settings, and also configure advanced / global settings.

To add a rule, click the appropriate icon to create a tripwire or an area. The selected analytics type determines whether you can add tripwires or areas (see table above).



Then, configure the rule type-specific settings according to the information in these topics:

- [Counting](#)
- [Border Line](#)
- [Loitering](#)
- [Area Protection](#)
- [Object Removed](#)
- [Object Dropped](#)

After configuring and saving one or more rules, the camera enables the rule type and the state becomes Active. You can disable any rule type by selecting **Disable Rule**. When a rule type is disabled, it becomes Inactive.



Note

Only one type of analytics rule can be enabled at any time. If you configure and try to enable one type of rule when another type of rule is already enabled, a confirmation message appears.

Advanced / Global Settings

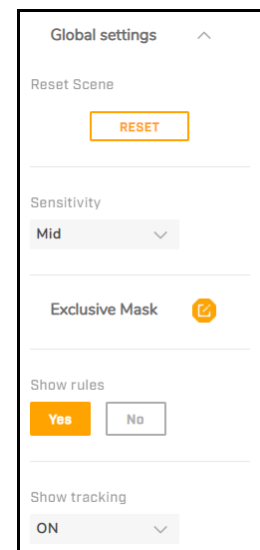
Reset Scene—If the scene has changed or the camera has been moved, click **Reset**. This re-initializes the analytics processes running in the background of the scene and adapts them to the new or changed scene. For example, after a building has been demolished. Teledyne FLIR also recommends resetting the scene after activating a new rule.

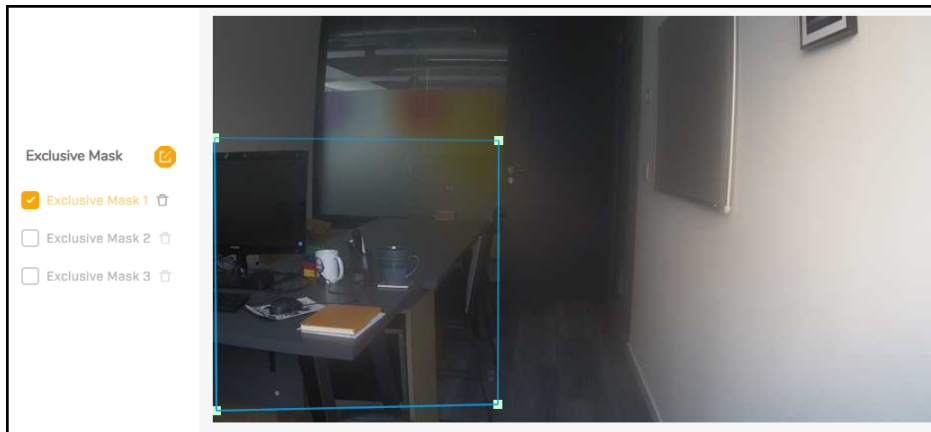
Sensitivity—Amount of sensitivity that triggers an alarm. High, Mid High, Medium (default), Mid Low, or Low. Contributes to overall detection probability. Increasing sensitivity can lead to increased false alarms. Likewise, decreasing sensitivity can lead to missed detections.

Exclusive Mask—Regions of the scene that do not generate alarms. For example, to eliminate alarms from trees or bushes moving in the wind. You can define a total of three masks.


To define a mask:

1. Click **Exclusive Mask**, and then click one of the three masks to define. By default, Exclusive Mask 1 is selected.
2. Specify each point of the mask region by clicking and releasing the mouse on the live video. Do not click and drag. For each mask, you can specify and modify 3-8 points.
3. Enable the mask by clicking the check box corresponding to the mask.
4. Click **Save**.





Exclusive Mask 1 Defined and Enabled

To clear the defined region for a mask, click the trash icon  corresponding to the mask, and then click **Save**.



Note

These masks disable analytics in the defined regions. They are not privacy masks. Within mask regions, the camera does not detect objects and trigger alarms. However, the regions appear in the live video and in the video streams.

Show rules—Determines whether defined rules appear in live video on the camera web page. Yes (default) or No.

Show tracking—Determines whether potential objects appear on screen as white boxes and detected objects appear as red, blue, or black boxes. ON (default) or OFF.

4.12.1 Basic Video Analytics Licenses


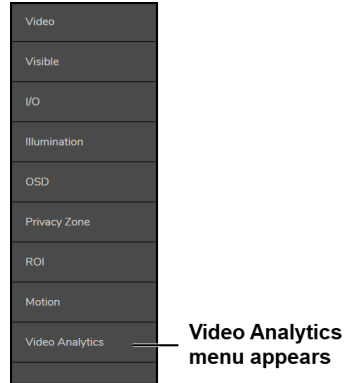
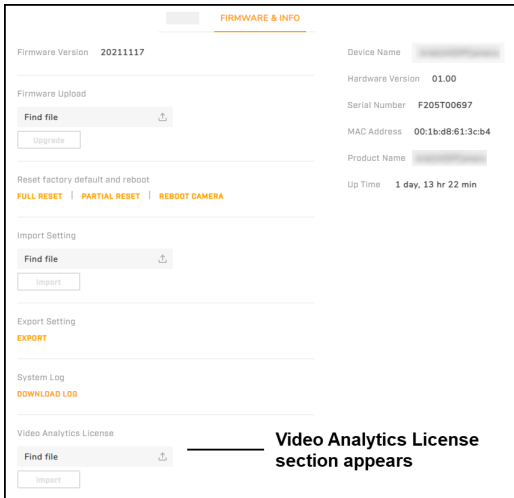
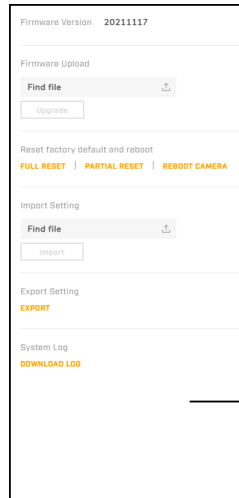
Administrators can check whether a camera has a BVA license installed and upload a license.



Note

Each camera using Basic Video Analytics (BVA) must have its own license installed.

To determine whether a camera has a BVA license installed using the camera's web page:

View Settings page	
 <p>Video Analytics menu does not appear <i>No License Installed</i></p>	 <p>Video Analytics menu appears <i>License Installed</i></p>
System Settings > Firmware & Info page	
 <p>Video Analytics License section appears <i>No License Installed</i></p>	 <p>Video Analytics License section does not appear <i>License Installed</i></p>



Note

Partial factory default resets do *not* affect an installed BVA license. On the other hand, after a full factory default reset, the license must be reinstalled. For more information about using the camera web page to reset the camera, see [Firmware & Info Page](#).

Obtaining BVA Licenses

Teledyne FLIR Operations provides BVA licenses. For help in obtaining licenses, contact your integrator or Teledyne FLIR representative.

To obtain BVA licenses:

1. Do one of the following:

- For existing cameras, send a purchase order for license activation to Teledyne FLIR Operations, along with a spreadsheet that lists the serial numbers and MAC addresses of all units.

-
- For new cameras being ordered, include the licenses in the Purchase Order for the cameras.
2. Teledyne FLIR Operations creates individual licenses and sends them in a ZIP file.
 3. Install the license. If ordering new cameras, install the licenses after the cameras are delivered.

Camera Administrators can install licenses using either DNA or the cameras' web pages. For information about using DNA to install the license, see the DNA Help or User Guide. For information about using the cameras' web pages to install the licenses, see [Firmware & Info Page](#).

4.12.2 General Guidelines

Basic Video Analytics support a range of possible applications. Utilizing the camera's analytics capabilities entails specific setup steps related to the application. However, all applications rely on a set of general principles and initial setup actions.

When setting up cameras and before configuring any specific analytics functionality, consider the following general guidelines:

- [Camera Distribution](#)
- [Camera Positioning](#)
- [Detection Ranges](#)
- [Mounting and Lighting](#)

After considering and applying these guidelines, begin configuring video analytics on the [Video Analytics Page](#), and then continue with the specific rule type-based configuration steps:

- [Counting](#)
- [Border Line](#)
- [Loitering](#)
- [Area Protection](#)
- [Object Removed](#)
- [Object Dropped](#)

4.12.2.1 Camera Distribution

When selecting where and how many cameras to deploy, no single camera should cover an area so large that targets to be detected are too small. Until reasonable on-site parameters are established, experiment with the minimum and maximum object size settings for each camera.

A camera's field of view should be able to see a target from head to toe anywhere in the area that it protects.

4.12.2.2 Camera Positioning

When determining camera placement, there are several ways to achieve optimal area coverage and fence line protection.

The specific perimeter layout, application requirements, and site topology must be considered.

In most cases, optimal performance and efficiency for border line protection is achieved by placing cameras so that their fields of view run *parallel* to the fence line perpendicular to the movement of potential intruders approaching or crossing the perimeter.

Within the camera's field of view, the highest *probability of detection* and the *lowest rate of false alarms* are achieved when targets move *horizontally* from one side of the camera image to the other.

Thus, to ensure full camera coverage across the perimeter:

- Position cameras so their fields of view run parallel to the fence line and perpendicular to intruder movement, rather than directing them to face approaching targets.
- Place cameras at an angle to show as little of the skyline as possible.

- When determining the camera positioning, consider whether you only need to detect the moment of intrusion or when a target simply approaches an area.

In general, the camera should be installed at a height of 2.5m - 4 m., and inclined at an appropriate angle. For example, a camera used for detecting intrusion would be pointed obliquely at the field to be viewed. On the other hand, if the camera used to count people crossing a line would be mounted vertically, looking down at the line (at 90°).

An urban area can present a set of difficult challenges to providing accurate detections. These include irregular lighting conditions and buildings; high density of people and animals; and movement around the clock. Also, placing the camera in an ideal location might not be possible due to legal or privacy concerns.

Take these factors into account when determining coverage and analytic rule to apply.

4.12.2.3 Detection Ranges

Detection ranges are based on the number of pixels that the object occupies in the scene, regardless of what the object may be. Therefore, configuring relevant and accurate *minimum* and *maximum object size* values is vital.

Other than the object size, which is the critical factor, detection range criteria also depend on a number of environmental and system variables, including:

- background temperature (hot desert versus cold snow)
- atmospheric conditions (clear skies versus fog)

These factors directly influence the following:

- scene contrast level
- target visibility
- analytic capability for determining the nature of the target (moving vehicle versus crawling human)
- speed and movement of the target object

The following are estimated detection ranges for an object with a width of 800mm a height of 1800mm (the typical dimensions representing a person):

Model	Object Distance	
	Wide	Tele
CF-6308-00-0 - P-Iris lens	9m	28m
CM-3308-11-I	9m	22m
CB-3308-11-I	9m	22m
CM-3304-11-I	8m	25m
CM-3304-21-I	25m	50m
CB-3304-11-I	8m	25m
CB-3304-21-I	25m	50m

**Notes**

- These ranges are rough estimates.
- Due to lens distortion, better detections occur for objects in the center of the scene, compared to the edges of the scene.
- The larger the size of the object, the earlier the detection.
- The scene and camera mounting might affect the accuracy of detections. For example, a camera with a very limited field of view might have poor detection performance.

4.12.2.4 Mounting and Lighting

To minimize vibrations and maximize resistance to wind, securely mount cameras on walls or on stable poles.

Ensure adequate lighting for the scene to be monitored.

In dark scenes, the effective detection range with the IR LEDs on is approximately 30 meters.

4.12.3 Rule Type-Specific Settings

The topics in this section describe the specific settings for each rule type and how to configure them.

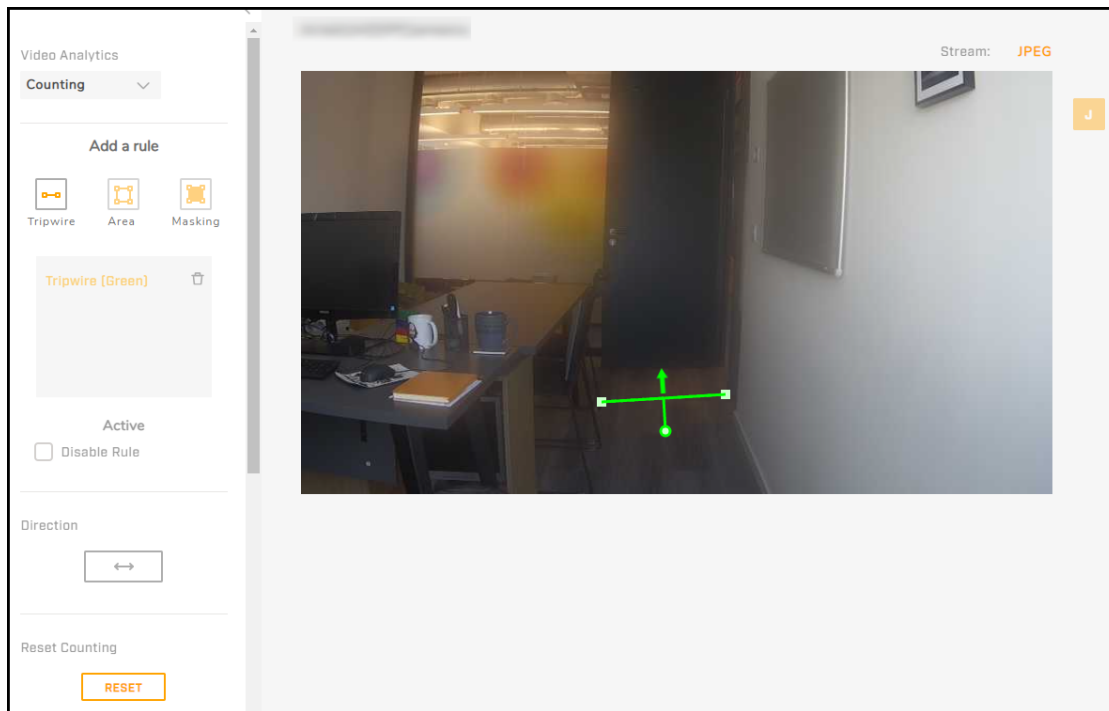
- [Counting](#)
- [Border Line](#)
- [Loitering](#)
- [Area Protection](#)
- [Object Removed](#)
- [Object Dropped](#)

4.12.3.1 Counting - Border Line

For the Counting and Border Line rule types, Administrators can define up to three tripwires. The camera counts the number of people crossing Counting tripwires. It detects people and objects crossing Border Line tripwires.

**Note**

Only one type of analytics rule type can be enabled at any time. If you define and save one type of rule when another type of rule is already enabled, a confirmation message appears.



Tripwire Defined - Counting Selected

To define a tripwire:

1. With Counting or Border Line selected as the rule type, click the Tripwire icon. A tripwire appears in the rule list.
2. On the live video, draw the tripwire by defining two end points. At each end point, click and release the mouse. Do not click and drag.

Each tripwire should cover a potential point of transit. Therefore, make sure that other objects in the scene do not obstruct or hide the tripwire region, and that the potential transit path goes through the line at close to a 90° angle.


When drawing Border Line tripwires, allow some space before the point of entry for the camera to process and analyze objects as they near the line.

You can adjust the length of the tripwire by clicking on an end point and dragging it.

While being defined, the tripwire appears as a dotted line with the default direction.

3. (Optional) Toggle the direction that crossing the tripwire the camera detects or counts. Click **Direction**.
4. Click **Save**.

To modify an existing tripwire, click the tripwire and then adjust the length of the tripwire by clicking on an end point and dragging it.

To delete a tripwire, click the tripwire and then click the trash icon  corresponding to the tripwire. Click **Save**. If no other tripwires are defined, the camera automatically disables the rule type.

Combine Rule (Available for Border Line Rules)

When more than one Border Line tripwire has been defined, you can configure the camera to trigger an alarm when two or all three tripwires have been tripped within a specified amount of time.

- Under Combine Rule, select the tripwires to combine.
- Specify the Trigger Interval, the amount of time, in seconds, during which both or all three tripwires must be tripped for the camera to trigger an alarm (1-30). The default is 5.

Reset Counting—Sets the counter back to 0 (zero). Available for the Counting rule type.

On the Alarm page, Administrators can select a Counting or Border Line tripwire, or Combine Rule, as an alarm rule trigger and can define holding the count as an alarm rule action. For more information, see [Alarm Triggers and Actions](#).

The screenshot shows the 'Combine Rule' configuration window. At the top, there is an 'Enable' checkbox. Below it, the 'Combine Rule' section contains three color-coded options: a green square with a checked checkbox, a blue square with a checked checkbox, and a yellow square with an unchecked checkbox. At the bottom, there is a 'Trigger Interval [1-30 sec]' slider with a value of 5 displayed next to it.

4.12.3.2 Loitering - Area Protection - Object Removed / Dropped

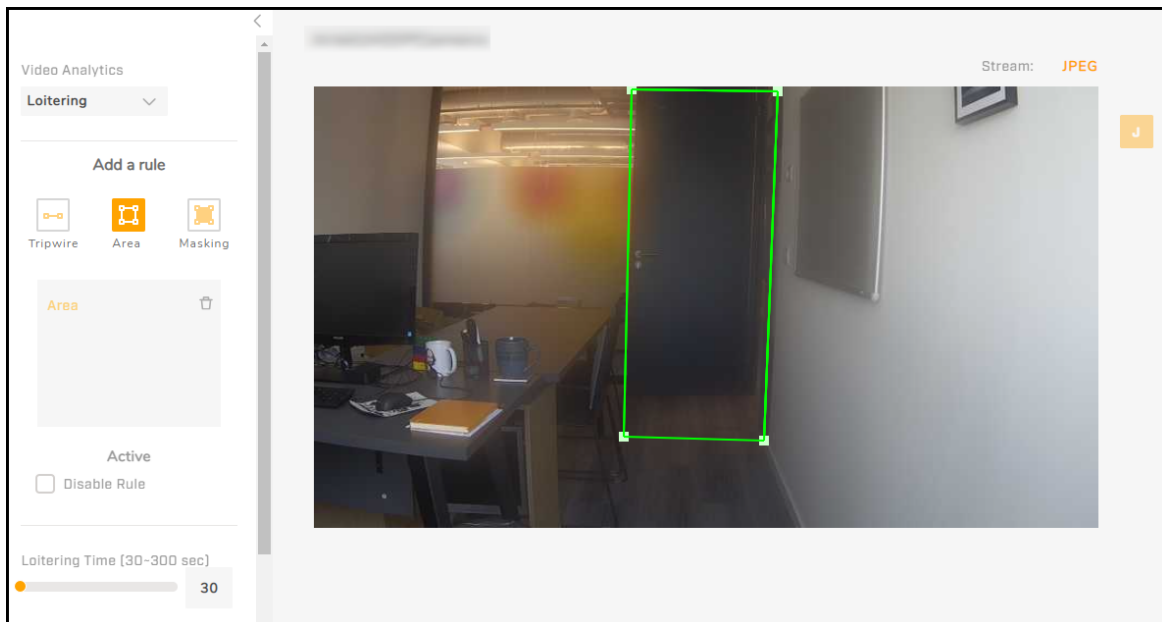
For the Loitering, Area Protection, Object Removed, and Object Dropped rule types, Administrators can define one or more detection areas.

- Use Loitering to monitor an area with relative light traffic, but in which an extended stay is prohibited. For example, the area around an ATM or in front of a door, where people are expected to move through and not linger for a long time.
- Use Area Protection to secure an area against any incoming or outgoing traffic (humans or vehicles). For example, a secluded or cordoned area, such as a police-controlled zone.
- Use Object Removed to monitor up to three areas of the scene for objects that are being taken out of it. For example, a store or a gallery with specific objects to protect.
- Use Object Dropped to secure an area against suspicious objects and litter. For example, a bus station or a public square.



Note

Only one type of analytics rule can be enabled at any time. If you define and save one type of rule when another type of rule is already enabled, a confirmation message appears.



Area Defined - Loitering Selected

To define a detection area:

1. With Loitering, Area Protection, Object Removed, or Object Dropped selected as the rule type, click the Area icon.

Area appears in the rule list or, when defining Object Removed, one of the three color-coded configurable areas appears in the list (Green, Blue, or Yellow).

2. On the live video, draw the area by defining 3-8 points. For each point, click and release the mouse. Do not click and drag. After defining the third point, the camera closes the area. You can continue defining points to define more complex detection areas. After defining five points, you can add points to the existing area border by clicking on a border line to define more specific detection areas.

When drawing an area for Area Protection, allow some space before the point of entry for the camera to process and analyze objects as they near the area.

You can adjust a point location by clicking on it and dragging it.

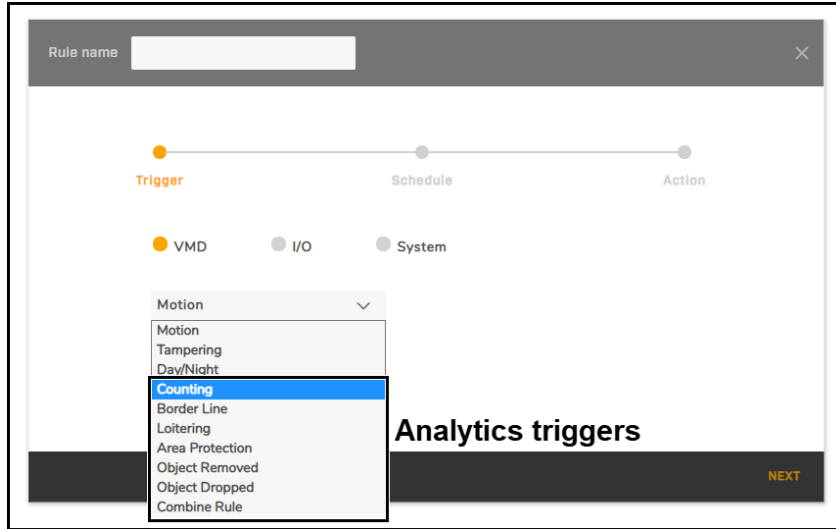
When defining Object Removed, you can define up to three detection areas.

3. (If applicable) Define the rule-type specific setting:
 - **Loitering Time**—Duration, in seconds, of a loitering event that triggers an alarm (30-300). The default is 30.
 - **Removal Duration**—Amount of time, in seconds, for an object in a detection area to be removed that triggers an alarm (1-300). The default is 5.
 - **Duration in Region**—Amount of time, in seconds, for an object to remain in the detection area that triggers an alarm (5-900). The default is 15.
4. Click **Save**. After defining and saving an Object Removed or an Object Dropped area, do not disturb the scene for about 30 seconds to a minute.

On the Alarm page, Administrators can select a Loitering, Area Protection, Object Removed, or Object Dropped area as an alarm rule trigger. For more information, see [Alarm Triggers and Actions](#).

4.12.4 Alarm Triggers and Actions

When a Basic Video Analytics license is installed in the camera, Administrators can configure analytics rules as alarm rule triggers.



Alarm Rule Triggers

When a Basic Video Analytics license is installed in the camera, you can select one of the following analytics VMD triggers:

- **Counting**—Select the Counting tripwire that triggers this rule's action.
- **Border Line**—Select the single Border Line tripwire that triggers this rule's action. To configure this trigger as the combined border line rule, select **Combine Rule**.
- **Loitering**—The Loitering detection area triggers this rule's action.
- **Area Protection**—The area defined for Area Protection triggers this rule's action.
- **Object Removed**—Select the Object Removed area that triggers this rule's action.
- **Object Dropped**—The Object Dropped area triggers this rule's action.
- **Combine Rule**—The combined Border Line rule triggers this rule's action.

After defining a Counting or Border Line tripwire as a rule trigger, Hold Count becomes available as a rule action.

Hold Count—Pauses the counter for the specified number of tripwire detections. The default is 1; that is, the camera pauses counting until the next tripwire detection.

There is no timeout on the hold count. Even if a long time passes between tripwire detections, the camera does not resume counting until the specified Hold Count has been reached.

Rule name

Trigger

Schedule

Action

Hold Count

1

Hold Count action

Alarm Out

Audio

Snapshot

Recording

1

Enable

Sound

1

Store on Edge

Store to FTP

Record on Edge

Email

OSD

Enable

Subject

Message

Enable

Text

BACK

DONE

Alarm Rule Actions

For more information about how to configure alarm rules, see Alarm Page.

5 Configuration

Administrators can click **System Settings** on the [Camera Web Page for Administrators](#) to configure:

- [Networking](#)
- [LDAP](#)
- [Audio](#)
- [Recordings](#)
- [RTSP](#)
- [FTP](#)
- [I/O connections](#)
- [Email](#)
- [Date and time](#)
- [SD card](#)
- [Sound](#)
- [Cybersecurity](#)
- [User accounts and passwords](#)
- [Alarms](#)
- [Snapshots](#)

In addition, Administrators can access the [Firmware & Info Page](#) to upgrade the camera's firmware, reset the camera to its factory defaults, reboot the camera, and export / import settings.

5.1 Network Page

When an Administrator clicks **System Settings**, the Network page appears. On the Network page, Administrators can configure the camera for networking.

If you are not sure how to configure any system setting, contact the network or system administrator.

NETWORK

DHCP Static PPPOE

[View Current Network Settings](#)

IPv4 Address:

IPv4 Subnet Mask:

IPv4 Default Gateway:

IPv6 Enable: ☐

Accept IPv6 Router Advertisement: ☐

Enable DHCPv6: ☐

IPv6 Address:

Subnet Prefix Length [1-128]:

IPv6 Default Router Address:

Subnet Prefix Length [1-128]:

IPv6 DNS:

Enable UPnP: ☒

Mode:

Enable DDNS: ☐

Type:

Host Name:

User Name:

Password:

Max Transfer Unit (MTU):

Speed & Duplex:

[BACK TO VIEW SETTINGS](#) — **View Settings** [DISCARD CHANGES](#) [Save](#)

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

In Static IP addressing mode, specify:

- **IPv4 Address**



Caution

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

- **IPv4 Subnet Mask**—The default is 255.255.255.0.
- **IPv4 Default Gateway**
- **Primary DNS**—The primary domain name server (DNS). The DNS translates host names into IP addresses.
- **Secondary DNS**—A domain name server that backs up the primary DNS.

If the camera connects to the network via a DSL modem using PPPoE (Point-to-Point Protocol over Ethernet), click **PPPOE** and type the PPPoE user name and password.

IPv6 Enable—If the camera's network uses IPv6 addressing, enable IPv6. Then, you can configure the following:

- **Accept IPv6 Router Advertisement**—If the network router supports IPv6 Router Advertisement, you can configure the camera to accept it. The default is to not accept Router Advertisement.
- **Enable DHCPv6**—If the network router supports DHCPv6, you can enable it on the camera. When DHCPv6 is disabled (default), specify the following:
 - **IPv6 Address** and **Subnet Prefix Length**
 - **IPv6 Default Router Address** and **Subnet Prefix Length**
 - **IPv6 DNS**

Click **View Current Network Settings** to see current network interface information, including the camera's MAC address (HWaddr), IP address (inet addr), multicast address (Bcast), and subnet mask (Mask). When IPv6 is enabled, the camera's IPv6 address and IPv6 DNS address also appear.

Basic Settings

Network Interface Information

eth0 Link encap:Ethernet HWaddr 00:1B:D8:61:3C:B4
inet addr:172.20.32.23 Bcast:172.20.32.255 Mask:255.255.255.0

IPv6 Address

IPv6 DNS

Enable UPnP—When enabled (default), other UPnP (Universal Plug and Play)-compliant devices on the LAN can detect the camera. Specify the Mode:

- **IP and Device Name**—Compliant devices detect the camera by its IP address and device name as defined on the [Firmware & Info Page](#). This is the default UPnP Mode.
- **Device Name**—Compliant devices detect the camera's device name.
- **User Input**—Compliant devices detect the camera by the Friendly Name that you specify.

Enable DDNS—When enabled, DNS records are automatically updated. Before enabling DDNS (Dynamic DNS), register with a DDNS service provider. When enabled:

- Specify the provider (Type):
 - **DynDNS (default)**—custom@dyndns.org
 - **No-IP**—default@no-ip.com
 - **Two-DNS**—default@two-dns.de
 - **FreeDNS**—default@freedns.afraid.org. Specify the Hash, a string encrypted with your user name and password. To retrieve the Hash, go to <https://freedns.afraid.org>.
- Specify the Host Name, User Name, and Password for the DDNS service provider account.

By default, DDNS is disabled.

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

Speed & Duplex—100 Mbps Half Duplex, 100 Mbps Full Duplex, 10 Mbps Half Duplex, 10 Mbps Full Duplex, or Auto (default).

5.2 RTSP Page

On the RTSP page, Administrators can enable or disable RTSP authentication and specify the RTSP port. The camera uses the RTSP protocol to stream video and you can configure the camera to require authentication for video stream access. By default, RTSP authentication is disabled.

Authentication—When RTSP authentication is enabled, specify the Login ID and Password.

Port—The RTSP network port (1025-65535). The default is 554.

You can configure other video stream settings on the [Video Page](#).

5.3 Date & Time Page

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

Area—Specify the camera's time zone. If you select *empty* from the continent drop-down list, you can define the time zone according to GMT offset.

When DHCP IP addressing is enabled on the [Network Page](#), you can:

- Configure the camera to obtain the NTP server information from the DHCP server.
- Manually specify one or more NTP server addresses. Use a comma to separate multiple addresses.

Synchronization Period—Daily frequency the camera synchronizes with the NTP server, in number of hours between 1-24. For example, to configure the camera to synchronize with the NTP server twice per day, specify 12.

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

1. At the top of the page, click **Manual**.
2. Specify the time zone (Area).
3. Specify the hour, minute, second, AM or PM, and date.

To synchronize the camera's date and time with the PC's date and time, click **Sync with PC**.

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

5.4 Users Page

On the Users Page, Administrators can add users or modify the settings for existing users.

User Name	Access Level	Actions
admin	Admin	
operator	Operator	

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

To add a user or modify the settings for an existing user:

1. Click **Add User** or click the edit icon for the user you are editing. The Account Settings screen appears.

Account Settings Screen - New User

2. Specify an access level for the account.

Access Level	User	Operator	Admin (Administrator)
Access	Can: <ul style="list-style-type: none"> view live video change the web page language toggle between Light Mode and Dark Mode click Help log out 	Can do everything a User can do, plus: <ul style="list-style-type: none"> view live video in full screen mode take and store a snapshot initiate / toggle live video recording 	Can access and use all of the camera's web pages
Comments	You can configure up to nine Users.	You can configure more than one Operator.	You can configure more than one Administrator. You cannot delete the default camera Administrator (user name <i>admin</i>).

3. Specify or modify the user name, up to 29 alphanumeric characters (0-9, A-Z).
4. Specify or modify the password, which:
- must be 8-64 characters
 - can include the following special characters: @#~!\$%<>+ _ . , * ?
 - cannot include four-digit sequences (for example, 1234)
 - cannot include four repeating characters (for example, aaaa)

User names and passwords are case-sensitive.

5. Click **Save**. If you were adding an account, it appears in the account list.

Administrators can delete all other accounts except for the default Administrator.

5.5 LDAP Page

On the LDAP screen, Administrators can enable LDAP (Lightweight Directory Access Protocol) and configure settings for an LDAP server on the network. LDAP is an industry-standard protocol for accessing and maintaining distributed directory information services over an IP network. By default, LDAP is disabled.

Before enabling LDAP, confirm that the LDAP settings are correct and that the LDAP server is up and running. If the settings are not valid, you will be logged out of the web application and you might not be able to log back in to the camera.

Specify or edit the following:

Server—IP address of the LDAP server.

Port—The LDAP network port (1025-65535). The default is 389.

Base DN—Default Distinguished Name (Domain Components) of the parent entry, used for searching the directory tree on the LDAP server. The default is *dc=ipcamera,dc=com*.

Bind DN Template—Attributes used for authenticating the camera on the LDAP server. The default is *uid=%u,dc=users,dc=ipcamera,dc=com*.

Search Template—Attribute used for the Common Name. The default is *cn=%u*.

Group Mappings

Admins—Attributes used for searches when an Administrator is logged in to the camera. The default is *cn=admin,ou=groups,dc=ipcamera,dc=com*.

Operators—Attributes for searches when an Operator is logged in to the camera. The default is *cn=operator,ou=groups,dc=ipcamera,dc=com*.

Users—Attributes used searches when an Operator is logged in to the camera. The default is *cn=user,ou=groups,dc=ipcamera,dc=com*.

Authentication

Specify the User Name and Password for accessing the LDAP server.

5.6 FTP Page

On the FTP screen, Administrators can configure the settings of an FTP (File Transfer Protocol) server located remotely on the network. The camera can save snapshots and audio / video to this FTP server. To configure alarm rules to trigger FTP recording, see [Alarm Page](#). To configure snapshots, see [Snapshot Page](#). To configure audio / video recording, see [Recording Page](#).

Specify or edit the following:

Server Address—IP address of the FTP server.

Port—Network port number of the FTP server (1025-65535). The default is 21.

Specify the User Name and Password for accessing the FTP server.

Mode—Specify whether the FTP mode is Active or Passive (default).

In passive mode, the client — in this case, the camera — initiates both connections to the server, which addresses the situation in which firewalls filter incoming data port connection to the client from the server. To support passive mode, on the server-side firewall, open the following communication channels:

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

5.7 SD Card Page

On the SD Card screen, Administrators can format and configure the local microSDXC card (minimum 64GB; maximum 128GB; formatted as a single partition), when installed. The camera can save snapshots and audio / video to this card. Before using the microSDXC card, it must be formatted.

For information about how to install a microSDXC card, see [Connect the Camera](#). To configure alarm rules to trigger local recording, see [Alarm Page](#). To configure snapshots, see [Snapshot Page](#). To configure audio / video recording, see [Recording Page](#).

Overwrite—When the microSDXC runs out of space, by default, the camera overwrites older files. Administrators can disable overwriting.

Status—*Working normally* indicates a properly formatted microSDXC card is installed.

SD Format—To format the microSDXC card before using it, click **Format**.

microSDXC Card Not Installed



Caution

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

When a microSDXC card is installed, Administrators can:

- specify the minimum amount of space on the card to keep free, in percentage of overall capacity

- see the overall capacity, in MB
- see how much free space is on the card, in MB

When an installed microSDXC card has stored snapshots or video clips, Administrators can:

- search for stored files by selecting a date
- download files

Select All	No	Name	Size
<input type="checkbox"/>	1	20210102202536_231.mp4	10.4M
<input type="checkbox"/>	2	20210102202536_232.mp4	10.4M
<input type="checkbox"/>	3	20210102202536_233.mp4	10.4M
<input type="checkbox"/>	4	20210102202536_234.mp4	10.4M
<input type="checkbox"/>	5	20210102202536_235.mp4	10.4M
<input type="checkbox"/>	6	20210102202536_236.mp4	10.4M
<input type="checkbox"/>	7	20210102202536_237.mp4	10.4M
<input type="checkbox"/>	8	20210102202536_238.mp4	10.4M
<input type="checkbox"/>	9	20210102202536_239.mp4	10.4M
<input type="checkbox"/>	10	20210102202536_240.mp4	10.4M

*microSDXC Card Installed
Video Clips from Selected Date Available*

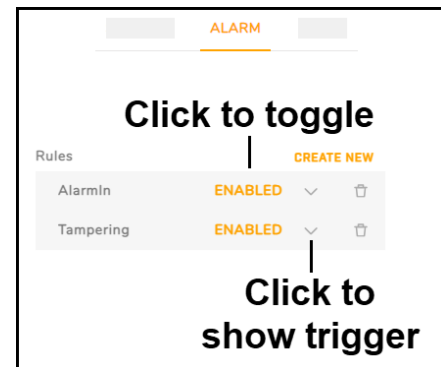
5.8 Alarm Page

On the Alarm page, Administrators can modify default alarm rules or create new alarm rules triggered by:

- The camera's motion or tampering detection or, when a Basic Video Analytics license has been installed, on-board video analytics
- Alarm or audio input
- Other camera system triggers: network loss, network conflict, or according to a configured schedule

For each rule, Administrators can specify one or more of the following actions:

- Change the state of the camera's alarm output.
- Play a sound through the camera's audio output.
- Store one or more photo snapshots on a microSDXC card installed on the camera or on an FTP server. Administrators can configure the snapshots on the [Snapshot Page](#), format and configure the microSDXC card on the [SD Card Page](#), and configure the FTP server on the [FTP Page](#).
- Record and store a video clip on the microSDXC card. Administrators can configure video recording on the [Video Page](#).
- Send a notification email. Administrators can configure email settings on the [Email Page](#).
- Display a specified text string in the camera's video streams and live video.




By default, the following rules are defined and enabled:

- **AlarmIn**—The camera's alarm input triggers an alarm.
- **Tampering**—Tampering with the camera triggers an alarm.

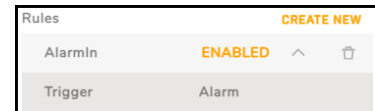
Enable or disable a rule by clicking **Enabled** or **Disabled**.

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

1. To create an alarm rule, click **Create New**.

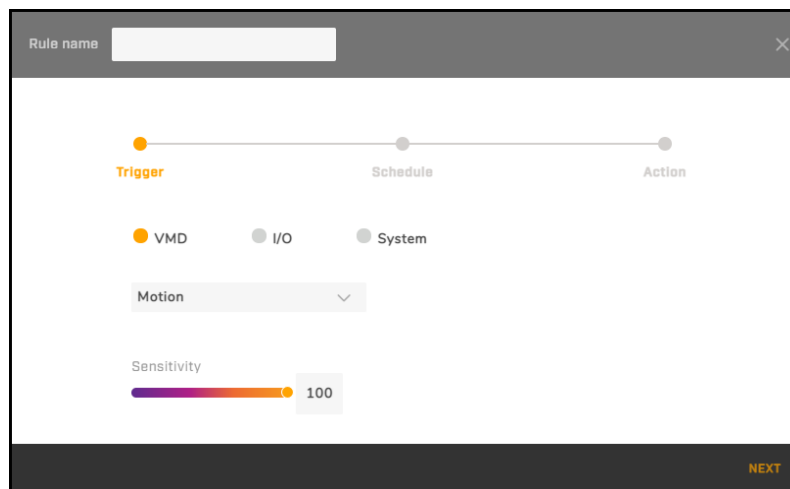
To modify an existing rule, click the relevant  icon. The rule trigger appears. Click on the rule trigger.

The rule trigger settings appear.



2. [Configuring the Rule Trigger](#)
3. [Configuring the Rule Schedule](#)
4. [Configuring the Rule Action](#)

5.8.1 Configuring the Rule Trigger



To modify or define an alarm rule trigger:

1. Modify or define the rule name.
2. Select the trigger.

Triggers		
VMD	Motion —The camera's motion detection triggers this rule's action.	<ol style="list-style-type: none"> On the Motion Page, make sure a motion detection zone has been defined and enabled. Specify the motion Sensitivity (1-100).
	Tampering —The camera's tampering detection triggers this rule's action.	Specify the tampering Sensitivity (<i>High, Mid, Low</i>).

Triggers		
I/O	Alarm —A change in the alarm input state triggers this rule's action.	a. On the I/O Page , make sure the local alarm input has been properly configured. b. Specify the Type; that is, whether the input state is <i>Normally Open</i> or <i>Normally Closed</i> .
	Audio —An audio input signal triggers this rule's action.	a. On the Audio Page , make sure the audio input has been enabled and properly configured. b. Specify the Sound Intensity Threshold (1-100). Lowering the value increases the camera's sensitivity to audio input, and vice versa.
System	Network Loss —Losing the camera's connection to the network triggers this rule's action.	
	Network Conflict —A conflict between the camera and another device on the network triggers this rule's action.	
	Schedule —This rule's action is triggered at regular intervals.	Specify the Trigger Interval (Sec), the frequency at which the camera triggers this rule's action, in seconds (5-3600; 3600 = once per hour).

For information about video analytics VMD triggers when a Basic Analytics License is installed in the camera, see [Alarm Triggers and Actions](#).



Note

For the default alarm rules, modifying the trigger is not possible.

3. Click **Next**. The rule schedule settings appear.
4. Continue with [Configuring the Rule Schedule](#).

5.8.2 Configuring the Rule Schedule

Alarm Rule Schedule Screen - Default Setting

By default, alarm rules are enabled all day, every day of the week. On the schedule, orange indicates when a rule is enabled. To modify when a rule is enabled and whether the rule triggers the action at certain times, click **Edit**. The schedule editing screen appears.

For each day of the week, you can define up to three periods during which the rule is enabled. For each period, specify a start time and an end time for the rule to be enabled.

By default, the action configured for the rule is enabled. For any defined period, you can disable the action.

The example below on the right is for a rule and action enabled from 8 AM-6 PM Monday through Friday.

	Start Time	End Time	Action
Monday			
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
Tuesday			
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
Wednesday			
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
Thursday			
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
Friday			
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
Saturday			
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
Sunday			
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
	00:00	23:59	<input checked="" type="checkbox"/>
			Apply Cancel

Schedule Editing Screen (Default)

	Start Time	End Time	Action
Monday			
	08:00	18:00	<input checked="" type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
Tuesday			
	08:00	18:00	<input checked="" type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
Wednesday			
	08:00	18:00	<input checked="" type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
Thursday			
	08:00	18:00	<input checked="" type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
Friday			
	08:00	18:00	<input checked="" type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
Saturday			
	00:00	23:59	<input type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
Sunday			
	00:00	00:00	<input type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
	00:00	23:59	<input type="checkbox"/>
			Apply Cancel

Rule and Action Enabled Monday through Friday 8 AM-6 PM

Click **Apply**. The arming schedule setting screen closes, and the modified schedule appears.

Rule name

TriggerScheduleAction

Edit

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Monday																									
Tuesday																									
Wednesday																									
Thursday																									
Friday																									
Saturday																									
Sunday																									

BACKNEXT

Modified Schedule

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

5.8.3 Configuring the Rule Action

By default, actions for alarm rules are disabled. When disabled, this setting overrides any specific action setting.

Select one or more actions.

Action Type	
Alarm Out	This rule triggers changing the state of the camera's alarm output. If enabled, make sure the camera's alarm output has been properly configured on the I/O Page .
Audio	This rule triggers playing the selected Sound (audio file) through the camera's audio output (1-10), according to the file number on the Sound Page .
Snapshot	Store on Edge —This rule triggers storing snapshots on the camera's microSDXC card. If enabled, make sure a microSDXC card is properly installed and formatted. See SD Card Page .
	Store to FTP —This rule triggers storing snapshots on a remote FTP server. If enabled, make sure the FTP server is properly configured on the FTP Page .
Recording	This rule triggers recording a video clip on the camera's microSDXC card. Administrators can configure the camera's recording settings on the Recording Page . If enabled, make sure a microSDXC card is properly installed and formatted. See SD Card Page .
Email	This rule triggers sending a notification email with the specified Subject and Message. If enabled, make sure the Email Page settings are properly configured.
OSD	This rule triggers displaying the specified Text in the camera's video streams and live video.

For information about the Hold Count action, available when a Basic Video Analytics license is installed in the camera, see [Alarm Triggers and Actions](#).

Click **Done**. If you were creating an alarm rule, it appears in the alarm rule list.

5.9 Audio Page

On the Audio page, Administrators can configure the camera's audio input and output settings. By default, audio input and output are enabled.

Administrators can configure audio input as an alarm rule trigger and audio output as an alarm rule action on the [Alarm Page](#).

Audio In Setting

Level—High, Mid (default), or Low.

Source—Line In or Mic In.

Encoding—G.711 a-law, G.711 μ -law, or AAC (default).

Audio Out Setting

Level—High, Mid (default), or Low.

For additional I/O settings, see [I/O Page](#) and [I/O Devices Page](#).

5.10 I/O Devices Page

On the I/O Devices page, Administrators can configure the camera's I/O connections.

I/O	Name	Enable
Input	Alarm In	<input checked="" type="checkbox"/>
Output	Alarm Out	<input type="checkbox"/>
Input	Audio In	<input checked="" type="checkbox"/>
Output	Audio Out	<input checked="" type="checkbox"/>

I/O pins—Specify the number of input and output pins the device manages. The default is two of each.

Administrators can enable or disable each pin individually.

For additional I/O settings, click **View Settings** and open the [I/O Page](#).

5.11 Sound Page

On the Sound page, Administrators can upload up to 10 audio files. On the [Alarm Page](#), Administrators can configure the camera to play the files through camera's audio output as an alarm rule action. For example, the camera can play an initial warning alerting a detected intruder. Then, if the intruder does not leave the scene, the camera can play a stronger warning not to proceed.

Upload PCM WAV files (signed 16 bits, sample rate 8 kHz).

Administrators can configure the camera's audio output on the [Audio Page](#), [I/O Page](#) and [I/O Devices Page](#).

No.	File Status	Delete File	Select File ⓘ
1	none	Delete	Find file
2	none	Delete	Find file
3	none	Delete	Find file
4	none	Delete	Find file
5	none	Delete	Find file
6	none	Delete	Find file
7	none	Delete	Find file
8	none	Delete	Find file
9	none	Delete	Find file
10	none	Delete	Find file
Delete All			

5.12 Snapshot Page

On the Snapshot page, Administrators can configure photo snapshot settings. On the [Alarm Page](#), Administrators can configure snapshots as an alarm rule action.

Pre-Event Capture Count—Number of frames to capture prior to the event snapshot (1-10). The default is 3.

Event Capture Interval—Amount of time between snapshots, in second (1-10). The default is 1.

Post-Event Capture Count—Number of frames to capture after the event snapshot (0-infinite). The default is 3.

5.13 Recording Page

On the Recording page, Administrators can configure video clip recording settings. On the [Alarm Page](#), Administrators can configure recording as an alarm rule action.

To record video clips, at least one video stream must be set to H.264 on the [Video Page](#).

Record Type—Video or Audio and Video (default).

Record Status:

- **One Shot (default)**—The camera records a single video for the specified Clip Duration, in seconds (5-10). The default is 5.
- **Continuous**—The camera starts recording video and does not stop recording until the file reaches the specified Clip Size.

Clip Size—Maximum file size for video clips, in MB (200-300; the default is 200).

Stream—The video stream the camera records (1-3). The default is 1.

Recording Page - One Shot Record Status

5.14 Email Page

On the Email page, Administrators can configure SMTP email server settings and define up to 10 email addresses for notifications. On the [Alarm Page](#), Administrators can configure email notification as an alarm rule action.

If you are not sure how to configure these settings, contact the email system administrator.

Before configuring email settings, make sure:

- There is an SMTP email server on the local area network (LAN).
- The camera's network is connected either to an intranet or to the internet.
- The networking settings, including the DNS server settings, are properly configured on the [Network Page](#).

Authentication—Authentication method the mail server requires for sending email. No_Auth (default), SMTP_Plain, Login, or TLS_TTLS (Transport Layer Security or Tunneled Transport Layer Security).

Server Address—IP address of the SMTP email server.

Port—SMTP network port.

User Name—User name for the email account.

Password—Password for the email account.

Sender Email Address—Email address to appear as the notification email sender.

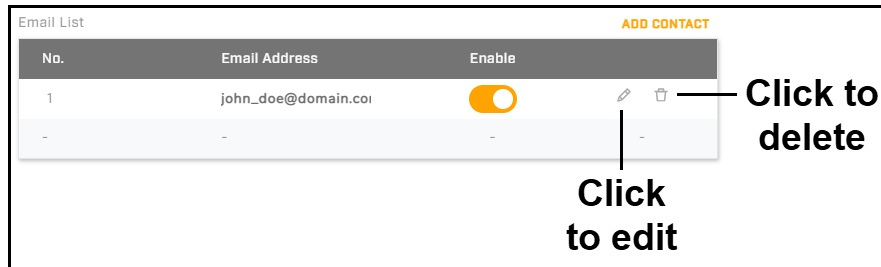
Attach Image—When enabled, the camera attaches the event snapshot to notification emails. By default, the camera does not attach images.

Test the connection to server—To make sure the email server information is correct and the camera can send notification emails, click **Test**.

Email List

To add a contact, click **Add Contact**, specify an email address, and enable the contact.

Administrators can also modify or delete existing contacts.



5.15 Cyber Page

On the Cyber page, Administrators can configure the following security features:

- [Certificates](#)
- [SNMP](#)
- [IEEE 802.1X-compliant communication](#)
- [Transport Layer Security \(TLS\) and secure HTTP \(HTTPS\) communication](#)
- [Ports](#)
- [IP Filter](#)

5.15.1 Certificates

Before Administrators can enable Secure Socket Layer (SSL), Transport Layer Security (TLS), and secure HTTP (HTTPS), the camera needs to have a valid certificate installed. Administrators can generate a self-signed certificate, or upload a certificate issued by a Certificate Authority (CA).

CERTIFICATES

Method

Self-Signed Request Upload Certificate

Certificate area

Country Code Province Name

City Name Common Name

Organization Name Organization Unit Name

Email Address

GENERATE CERTIFICATE

To generate a self-signed certificate:

1. Under Method, do one of the following:

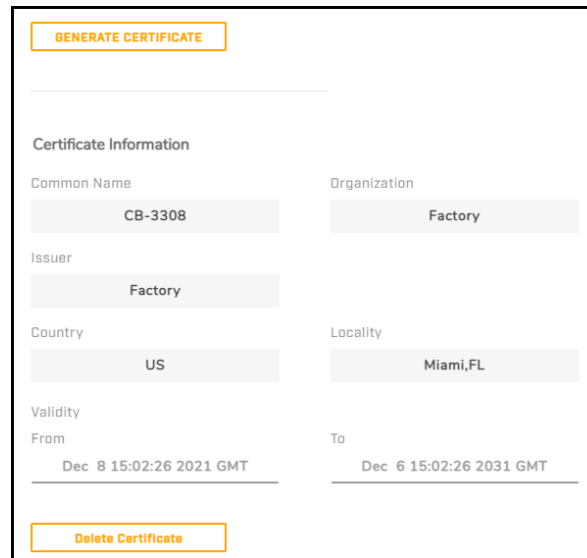
- To generate a self-signed certificate, click **Self-Signed**.
- To generate a self-signed certificate and then be able to download it for future use, click **Request**.

2. In the Certificate area, specify:

- **Country Code**—Two-letter code for the country in which the certificate will be used. For example, if you are generating a certificate to be used in the United States, enter US.
- **Province Name**—State or province name.
- **City Name**
- **Common Name**—Camera hostname or IP address (identifies the camera).
- **Organization Name**—Organization to which the Common Name belongs (for example, a company name).
- **Organization Unit Name**—Unit within the organization (for example, a department or division).
- **Email Address**—Email address of the person responsible for maintaining the certificate.

3. Click **Generate Certificate**. Wait for the camera to generate the certificate.

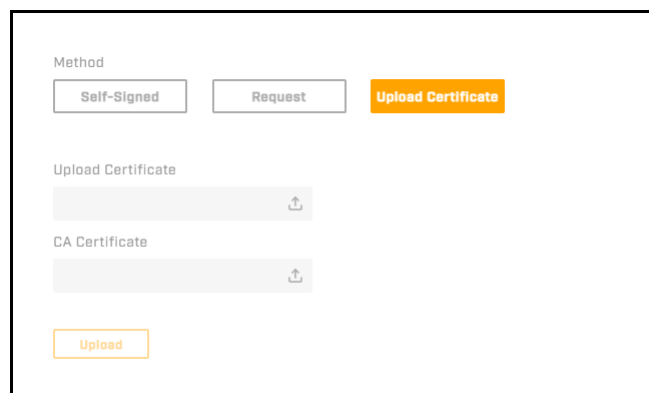
If you are generating a self-signed certificate, the Certificate Information appears.



The screenshot shows a web interface for generating a certificate. At the top is an orange button labeled "GENERATE CERTIFICATE". Below it is a section titled "Certificate Information" containing several input fields: "Common Name" (value: CB-3308), "Organization" (value: Factory), "Issuer" (value: Factory), "Country" (value: US), "Locality" (value: Miami, FL), "Validity From" (value: Dec 8 15:02:26 2021 GMT), and "Validity To" (value: Dec 6 15:02:26 2031 GMT). At the bottom of this section is an orange button labeled "Delete Certificate".

If you are requesting a self-signed certificate, you can download the certificate.



To upload a certificate:



The screenshot shows a web interface for uploading a certificate. At the top is a "Method" section with three buttons: "Self-Signed", "Request", and "Upload Certificate" (highlighted in orange). Below this is an "Upload Certificate" section with a text input field and an upload icon. Below that is a "CA Certificate" section with a text input field and an upload icon. At the bottom is an orange button labeled "Upload".

1. Under Method, click **Upload Certificate**.

2. Do one of the following:

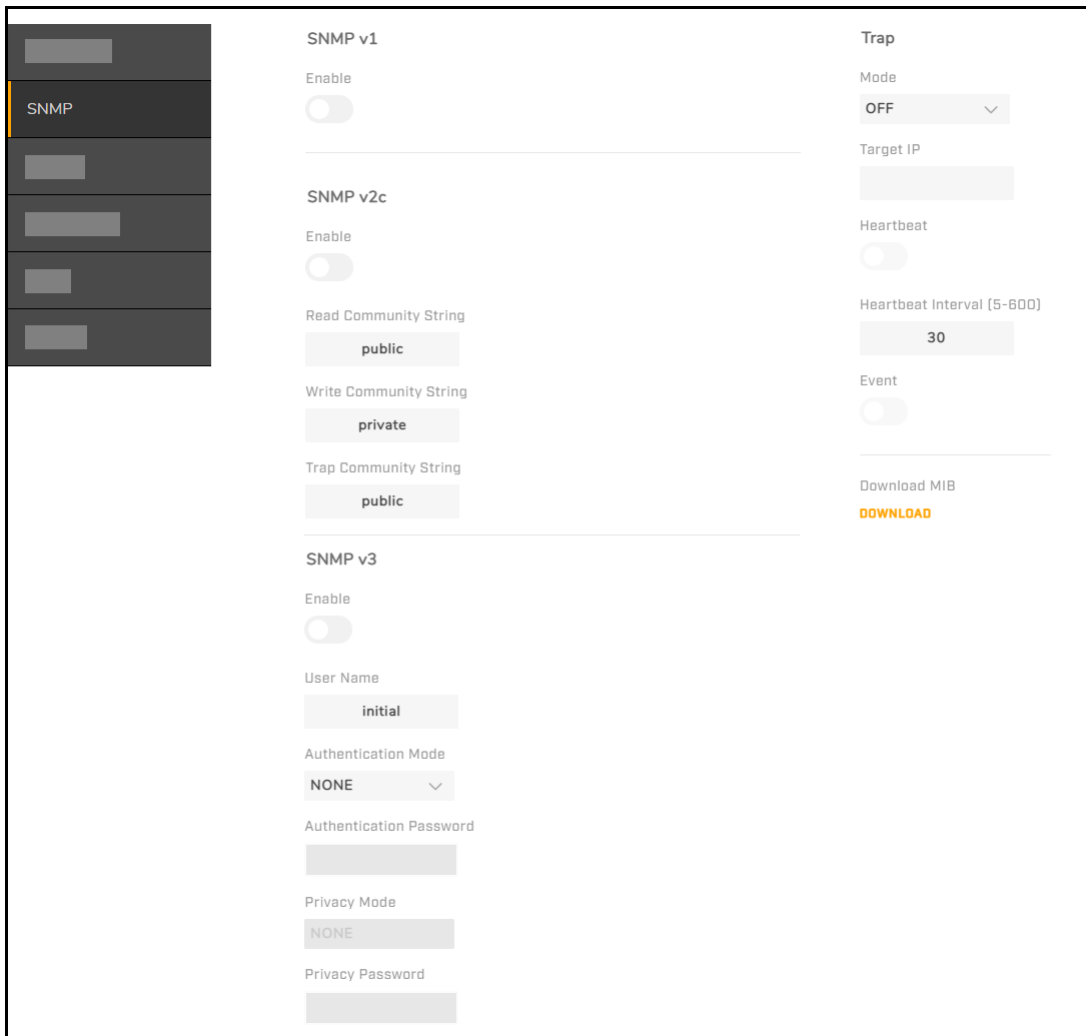
- If you are uploading a self-signed certificate, under Upload Certificate, click .
- If you are uploading a CA certificate, under CA Certificate, click .

3. Browse for and select the certificate to upload.

4. Click **Upload**. Wait for the camera to upload the certificate, at which point the Certificate Information appears on the screen.

5.15.2 SNMP

Administrators can enable and configure SNMP versions 1, 2c, and 3. SNMP (Simple Network Management Protocol) enables the network management system (NMS) to remotely monitor and manage the camera. By default, all SNMP versions are disabled.



The screenshot shows the SNMP configuration page. On the left is a sidebar with a menu where 'SNMP' is highlighted. The main content area is divided into three sections: SNMP v1, SNMP v2c, and SNMP v3. Each section has an 'Enable' toggle switch. To the right of these sections is a 'Trap' configuration area. Below the 'SNMP v1' section, there are fields for 'Read Community String' (set to 'public'), 'Write Community String' (set to 'private'), and 'Trap Community String' (set to 'public'). The 'SNMP v3' section includes fields for 'User Name' (set to 'initial'), 'Authentication Mode' (set to 'NONE'), 'Authentication Password' (empty), 'Privacy Mode' (set to 'NONE'), and 'Privacy Password' (empty). The 'Trap' area on the right includes a 'Mode' dropdown (set to 'OFF'), a 'Target IP' field (empty), a 'Heartbeat' toggle switch, a 'Heartbeat Interval [5-600]' field (set to '30'), an 'Event' toggle switch, and a 'Download MIB' button labeled 'DOWNLOAD'.

SNMP v1

Enable or disable SNMP v1.

SNMP v2c

Enable or disable SNMP v2c.

Read Community String—Community name that has read-only access to all supported SNMP objects. The default is *public*.

Write Community String—Community name that has read/write access to all supported SNMP objects (except read-only objects). The default is *private*.

Trap Community String—Community name the camera uses when sending trap messages to the management system. The default is *public*. The camera uses traps to send messages to the management system for important events or status changes.

SNMP v3

Enable or disable SNMP v3.

User Name—The default is *initial*.

Authentication Mode—MD5, SHA, or NONE (default).

Authentication Password—Available when Authentication Mode is MD5 or SHA.

Privacy Mode—AES, DES, or NONE (default). Available when Authentication Mode is MD5 or SHA.

Privacy Password—Available when Privacy Mode is AES or DES.

Trap

Mode—SNMP version for the trap messages the camera sends: V1, V2C, V3, or OFF (default).

Target IP—IP address of the Trap Host.

Heartbeat—Camera sends SNMP notifications at regular intervals to detect network delays. By default, Heartbeat is disabled.

Heartbeat Interval (5-600)—Amount of time between the camera's heartbeat notifications, in seconds. The default is 30.

Event—Camera automatically records the log file of events, for later review. By default, Event is disabled.

Download MIB

Administrators can download the camera's Management Information Base (MIB), which describes the structure of the management data of the camera's subsystem using a hierarchical namespace containing object identifiers (OIDs). Each OID identifies a variable that can be read or set via SNMP.

5.15.3 802.1X

If the camera is connected to a network protected by the 802.1X / EAPOL (Extensible Authentication Protocol over LAN) authentication protocol, Administrators can enable and configure 802.1X. 802.1X is disabled by default.

Before enabling 802.1X on the camera, a user name and password on the 802.1X server for the camera must be registered and the authentication server must be configured. To obtain certificates, user IDs, and passwords, contact the network or system administrator.

Protocol—MD5 (default), TTLS, or PEAP.

Protocol

MD5

TTLS

PEAP

CA Certificate

Upload file

Inner Authentication

CHAP

User Name

Password

Anonymous ID

Status

Not Installed

Save and Test

Protocol

MD5

TTLS

PEAP

CA Certificate

Upload file

Inner Authentication

mschapv2

User Name

Password


Status

Not Installed

Save and Test

PEAP Settings

TTLS Settings

CA Certificate—Click , and then browse for and upload the CA certificate for the 802.1X server.

Inner Authentication—CHAP (default), EAP-MSCHAPV2, MD5, MSCHAP, MSCHAPV2, or PAP. Available when the Protocol is TTLS.

User Name and Password

Anonymous ID—Available when the Protocol is TTLS.

5.15.4 TLS/HTTPS

Administrators can enable Secure Socket Layer (SSL), which provides a secure HTTP (HTTPS) connection between the camera and a web browser over IP. HTTPS uses SSL and Transport Layer Security (TLS), which protects camera settings and user name / password information. By default, SSL is disabled.

Before enabling SSL, a certificate must be installed. The certificate can be obtained either by creating and sending a certificate request to a CA or by creating a self-signed certificate. For more information, see [Certificates](#).

Enable SSL

ON

OFF

TL S/HTTPS

After enabling SSL, specify the HTTPS Port (1025-65535). The default is 443.

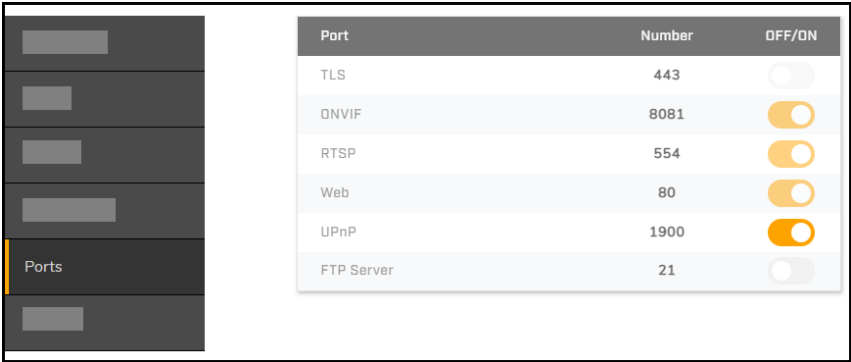
5.15.5 Ports

For enhanced security, Administrators can allow (On) or block (Off) specific ports.



Caution

Disabling ports can affect product functionality.



Port	Number	OFF/ON
TLS	443	<input type="checkbox"/>
ONVIF	8081	<input checked="" type="checkbox"/>
RTSP	554	<input checked="" type="checkbox"/>
Web	80	<input checked="" type="checkbox"/>
UPnP	1900	<input checked="" type="checkbox"/>
FTP Server	21	<input type="checkbox"/>

Default Ports

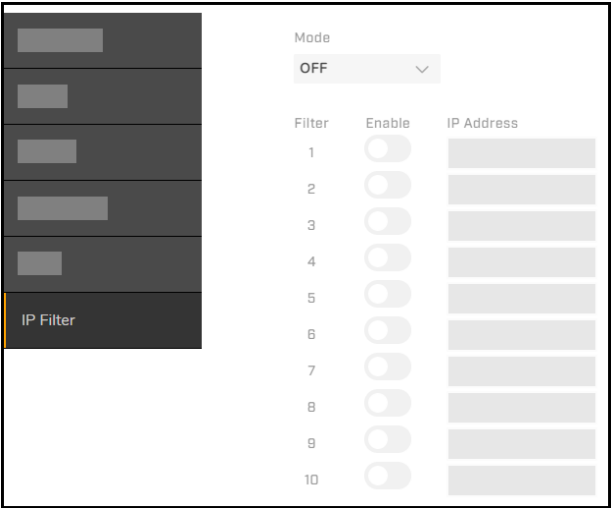
If SSL is not enabled on the [TLS/HTTPS](#) screen, TLS cannot be enabled.

To ensure communication with the camera, the ONVIF, RTSP, and Web ports cannot be disabled.

The TLS, RTSP, and FTP server port numbers reflect changes to their port assignments from their defaults.

5.15.6 IP Filter

Administrators can restrict access to the camera by either allowing or denying up to 10 specific IP addresses.



Filter	Enable	IP Address
1	<input type="checkbox"/>	
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	
8	<input type="checkbox"/>	
9	<input type="checkbox"/>	
10	<input type="checkbox"/>	

Mode—

- **OFF** (default)
- **Allow**—Only the specified IP addresses can access the camera. The camera denies access to all other IP addresses.

**Caution**

After selecting Allow, make sure to specify the IP address for the device you are currently using **before** clicking **Save**. If you do not, the camera will deny further access to your device.

- **Deny**—The camera denies access to the camera from the specified IP addresses. The camera allows access to all other IP addresses.

To specify an IP address, enable a filter and then specify the IP address.

You can disable existing filters, and you can modify or delete delete IP addresses.

5.16 Firmware & Info Page

FIRMWARE & INFO	
Firmware Version	20211117
Device Name	ArielUHDIPCamera
Hardware Version	01.00
Serial Number	F205T00697
MAC Address	00:1b:d8:61:3c:b4
Product Name	CB-3308-11-I
Up Time	1 day, 13 hr 22 min
Firmware Upload Find file Upgrade	
Reset factory default and reboot FULL RESET PARTIAL RESET REBOOT CAMERA	
Import Setting Find file Import	
Export Setting EXPORT	
System Log DOWNLOAD LOG	
Video Analytics License Find file Import	

Basic Video Analytics License Not Installed

On the Firmware & Info page, Administrators can:

- Specify a name for the camera
- See the camera's current firmware version, hardware version, serial number, MAC address, product name, and up time
- Upgrade the camera's firmware
- Reset the camera to its factory defaults
- Reboot the camera
- Import previously exported camera settings
- Export the camera's currently saved settings

- Download the system log, which Teledyne FLIR Support can use for troubleshooting
- Upload a Basic Video Analytics (BVA) license

Device Name—Unique, friendly name for the camera, using only alphanumeric characters.

Firmware Upload

To upgrade the camera's firmware:

1. Make sure the camera has been recently rebooted.
2. Under Upgrade Firmware, click **Find file**.

The firmware folder includes a checksum file, which can be used to check file validity using checksum validation software.

3. On your computer or network, browse to and select the firmware file.



Caution

Only upgrade with firmware developed for the camera model you are upgrading. For example, if you are upgrading a CB-3308 camera, make sure you upgrading with the firmware developed for the 4K UHD camera.

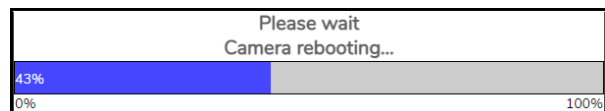
4. Click **Upgrade**.

The camera uploads and installs the firmware, which takes about three minutes. After the firmware has been successfully installed, the camera reboots.

Log in to the camera web page as an Administrator and make sure the newly installed firmware version appears as the Firmware Version.

Reset factory default and reboot

- **Full Reset**—Reboots the camera and restores all of the camera's factory default settings, including its factory default networking settings. If a BVA license is currently installed, it needs to be reinstalled after a Full Reset.



- **Partial Reset**—Reboots the camera and retains some currently saved settings and restores all of the camera's other factory default settings. Retains the following currently saved settings: BVA license (if installed), networking (including, for example, IP addressing mode, IPv4 address, IPv4 subnet mask, and IPv4 default gateway; TV format; and image rotation).
- **Reboot**—Reboots the camera with the currently saved settings. The camera does not retain any unsaved setting changes.



Caution

Full Reset causes the camera to lose all network settings.

Attention

Valeurs d'Usine par Défaut Complètes entraîne la caméra de perdre tous les paramètres réseau.



Tips

- When performing a full reset or when importing settings, the camera's IP address and IP addressing settings can change. To discover the camera after it reboots, Teledyne FLIR recommends using the DNA tool. Also, 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.
- You can also perform full and partial resets by using the camera's physical reset button. For more information, see [Connect the Camera](#).

Import Setting

To import settings using an exported settings file, click **Find file**; browse to and select the settings file; and click **Import**. The camera uploads the file, imports the settings, and reboots.

Export Setting

To export the camera's currently saved settings, click **Export** and save the file. When using Internet Explorer, an information bar appears. Click **Save**.

System Log

To download the camera's log files, for Teledyne FLIR Support personnel, click **Download Log**.

Video Analytics License

To install a BVA license that enables the camera's on-board video analytics, click **Find file**; browse to and select the license file; and click **Import**. The camera uploads the file, installs the license, and enables the Video Analytics page in View Settings. When a license has been installed and analytics are enabled, the Video Analytics License setting does not appear on the Firmware & Info page.

For more information about Basic Video Analytics, including how to obtain a license for it, see [Video Analytics Page](#).

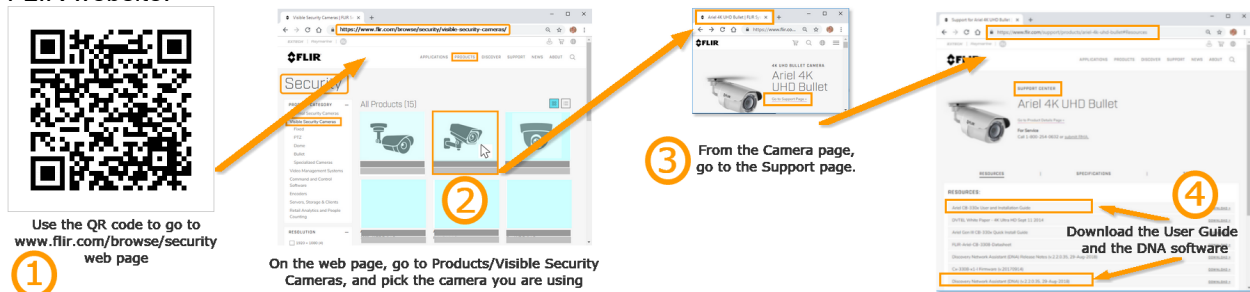
6 Appendices

- [Technical Specifications](#)
- [Network Settings](#)
- [Troubleshooting](#)
- [Acronyms and Abbreviations](#)
- [Mounting Accessories](#)

6.1 Technical Specifications

6.1.1 Accessing Camera Information from the Web

You will find the latest information, versions of documentation and releases of software on the Teledyne FLIR website.



6.2 Network Settings

The camera uses the following network protocols and default ports:

Protocol	Port	Usage
FTP	21	Uploading files to the FTP server
HTTP	80	Sending commands, requests, replies and notifications
HTTPS	443	Using the secure socket protocols SSL/TLS over HTTP. HTTPS must be enabled if your network uses SNMPv3.
Multicast Streaming	As defined in the units	Video/streaming (multicast). Uses the ONVIF address defined by the Video Management System
Multicast UDP	9766	Unit self-publishing. Uses IP address 224.9.9.9
NTP	123	Time synchronization with a network time server using SNTP
RTSP	554	RTP session setup
RTP	2000 to 65535	Multimedia streaming
SNMP	161	IP management system
SNMP Trap port	162	Sending alarm event and exception messages to the surveillance center

6.3 Troubleshooting

This section provides useful information and remedies for common situations where problems may be encountered.

Problem	Possible Solution
No network connection	Hardware issues: <ul style="list-style-type: none"> • Check that the network is working and the unit is powered on. • Check that the network (Ethernet) cable is properly attached to the unit. • Confirm that the network cables are not damaged and replace if necessary. IP Address issues: <ul style="list-style-type: none"> • Change the default IP address/addresses of the unit. • From the PC running the web browser, ping the unit IP address and confirm that it can be reached. • Confirm that the network settings/firewalls are set according to the requirements. • The camera might be located on a different subnet. Contact your IT administrator to get the IP address of the camera.
How do I find IP address of my unit?	<ul style="list-style-type: none"> • Check the network DHCP server IP address assignments and lease. • Alternatively, move the camera to an isolated network and make sure camera gets DHCP address and is accessible. Move the camera back to the network and test it. If you still have issues, reset the camera physically by pressing the reset button on the rear of the camera and test the camera again. This will ensure the camera releases the IP address.
The IP address responds to a ping on the network from the workstation but does not show in the Discovery List	<ul style="list-style-type: none"> • Disconnect the unit's Ethernet 10/100 port or turn the power to unit off, and then ping the IP address again. If the IP address responds, there is another device using the IP address. Consult with your network administrator to resolve the conflict. • Check the network port and ensure that it is working OK. • Ensure that the switch ports provide the necessary power.
The unit IP address is in use by another computer (collision)	<ul style="list-style-type: none"> • Check the DHCP settings. Obtain a new IP address using DHCP. Ensure this is a unique IP address. • Alternatively, change the unit IP address after connecting to it directly (not through the system network).
Cannot login to the camera	<ul style="list-style-type: none"> • Check the login user ID of the user or admin. • Check the login password of the user or admin.
No video image displayed on the main menu or the view menu of the web interface	<ul style="list-style-type: none"> • Reset the browser security settings to the default value. • Check that the correct port was configured. The default port is 554.
Bad output video quality	<ul style="list-style-type: none"> • Check that the network cable is connected securely. • Check that the camera settings are correct on the camera and in the unit. • Check that the camera lens is clean and unobstructed. • Check that the cable length is within specification.


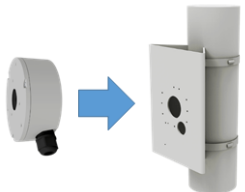
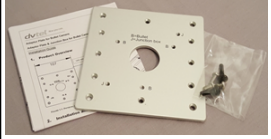
Problem	Possible Solution
Streaming video image is hanging (stopped)	<ul style="list-style-type: none"> • Confirm the unit's video streaming settings. • Refresh your browser screen (F5). • Check that the bandwidth and bit rate settings of the network are set properly. • Check that other processes and applications are not causing undue latency. • Check that the firewall analysis or blocking is not interfering with the video stream and supports the required ports and communication protocols.
Bluish picture in an indoor scene (possibly mixing indoor and outdoor lighting)	Adjust the White balance configuration to <i>Auto</i> . If the lighting in the scene is fixed, manually adjust the White balance to an acceptable image.
Reddish picture and incorrect colors in the image	Check the PoE power supply and associated network cables. Connect directly to the PoE and compare the images. If the problem persists, contact support.

6.4 Acronyms and Abbreviations

Abbreviation	Description
802.1X	Network Access Control Port-based authentication standard
AES	Advanced Encryption Standard
AGC	Automatic Gain Control
DES	Data Encryption Standard
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol
FTP	File Transfer Protocol
H.264	Video Compression Standard
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
IP	Internet Protocol
JPEG	Joint Photographic Experts Group
LDAP	Lightweight Directory Access Protocol
MD5	Message-Digest 5 encryption algorithm
MJPEG	Motion Joint Photographic Experts Group
NTP	Network Time Protocol
ONVIF®	Open Network Video Interface Forum
OSD	On-Screen Display
ROI	Region of Interest
RTP	Real-time Transport Protocol
RTSP	Real-time Streaming Protocol
SHA	Secure Hash Algorithm
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play

6.5 Mounting Accessories

The following mounting accessories are available for CB-330x bullet cameras:

Part number / item code	Description and notes	Images (not to scale)
CB-WLBX-31	<p>Wall junction box:</p> <ul style="list-style-type: none"> • IP66 wall mount with cable management box • Heavy-duty aluminum with 1/2" conduit connects <p>Dimensions 47.5 x 120 mm</p> <p>Pole diameter range ø 2.5-8.5"</p> <p>Color FLIR White</p> <p>Shipping box size 66 x 29 x 18 cm</p> <p>Shipping box weight 6.5 kg</p>	 <p>CB-WLBX-31</p> <p>Mounted with camera</p>
CB-PLBX-31	<p>Pole mount kit</p> <p>Includes pole mount and CB-WLBX-31 wall junction box</p> <p>Dimensions</p> <p>Pole bracket 240 x 180 x 60 mm</p> <p>Junction box 47.5 x 120 mm</p> <p>Pole diameter range ø 130-152 mm</p> <p>Color FLIR White</p> <p>Shipping box size 42 x 41 x 56 cm</p> <p>Shipping box weight 17 kg</p>	
CB-4S-31	<p>4S electrical box mounting adapter:</p> <ul style="list-style-type: none"> • Adapts CB-33xx bullet cameras to standard 4S electrical box mounting • For indoors or weather-protected applications <p>Dimensions 107 x 107 x 3 mm</p> <p>Color Silver</p> <p>Shipping box size 44 x 24 x 14 cm</p> <p>Shipping box weight 6.2 kg</p>	



Teledyne FLIR
Security Solutions

Teledyne FLIR LLC
6769 Hollister Ave
Goleta, CA 93117
USA

Corporate Headquarters
Teledyne FLIR LLC
27700 SW Parkway Ave.
Wilsonville, OR 97070
USA

Support:
<https://support.flir.com/>

Document:
CB-330x Installation and User Guide
Revision: 0.7
Date: May 2022