



Quasar™

Installation and User Guide

CB-6404/CB-6408 Bullet Cameras



© 2021 FLIR Systems, Inc. All rights reserved. No parts of this material may be copied, translated, or transmitted (in any medium) without the prior written permission of FLIR Systems, Inc.

Names and marks appearing on the products herein are either registered trademarks or trademarks of FLIR Systems, Inc. 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:

FLIR Systems, Inc.

6769 Hollister Ave.

Goleta, CA 93117

Phone: 888.747.FLIR (888.747.3547)

International: +1.805.964.9797

For technical assistance, please call us at +1.888.388.3577 or visit the Service & Support page at www.flir.com/security.

Important Instructions and Notices to the User:

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

Note 1: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna;

Increase the separation between the equipment and receiver;

Connect the equipment into an outlet on a circuit different from that of the receiver; and/or

Consult the dealer or an experienced radio/television technician for help.

Note 2: This equipment was tested for compliance with the FCC limits for a Class B digital device using a shielded cable for connecting the equipment to an analog video output to a monitor and using a shielded USB cable for connecting the equipment to a personal computer. When making such connections, shielded cables must be used with this equipment.

Industry Canada Notice:

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

Avis d'Industrie Canada:

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

Proper Disposal of Electrical and Electronic Equipment (EEE)



The European Union (EU) has enacted Waste Electrical and Electronic Equipment Directive 2002/96/EC (WEEE), which aims to prevent EEE waste from arising; to encourage reuse, recycling, and recovery of EEE waste; and to promote environmental responsibility.

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

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

Document History

Revision	Date	Comment
100	February 2021	Initial FLIR Release

Table of Contents

1	Document Scope and Purpose	1
2	Introduction	6
2.1	Features	7
2.2	Accessing Product Information from the FLIR Website	7
2.3	Camera Dimensions	9
3	Installation	10
3.1	Supplied Components	10
3.2	Pre-Installation Checklist	10
3.3	Outdoor Mounting Recommendations	11
3.4	Hardware Description	11
3.4.1	System Cable	12
3.4.2	Internal Interfaces	12
3.5	Powering the Camera	14
3.6	Initial Configuration	15
3.6.1	Discover the Camera and Configure for Networking	16
3.6.2	Change the Video Format (Optional)	18
3.7	Mounting the Back Box and Routing the Cables	19
3.8	Mounting and Aiming the Camera	19
3.8.1	Attaching the Camera to the Back Box	19
3.8.2	Adjusting the Sun Shield	20
3.8.3	Aiming the Camera	21
3.9	Completing Camera Setup	22
3.10	Attaching the Camera to a Supported VMS	22
4	Operation	23
4.1	Accessing the Camera's Web Page	23
4.2	View Settings Home Page	24
4.3	Video Page	25
4.3.1	Viewing Live Video using a Media Player	31
4.4	Visible Page	32
4.5	I/O Page	37
4.6	Illumination Page	38
4.7	OSD Page	39
4.8	Privacy Zone Page	40
4.9	Motion Page	42
5	Configuration	44
5.1	Network Page	44
5.2	RTSP Page	47
5.3	Date & Time Page	47
5.4	Users Page	49
5.5	FTP Page	50
5.6	SD Card Page	51

5.7	Alarm Page	52
5.8	Audio Page	57
5.9	I/O Devices Page	57
5.10	Sound Page	58
5.11	Snapshot Page	59
5.12	Recording Page	59
5.13	Email Page.....	60
5.14	Cyber Page.....	61
5.14.1	Certificates.....	62
5.14.2	SNMP	64
5.14.3	802.1X	65
5.14.4	TLS/HTTPS	66
5.14.5	Ports	67
5.14.6	IP Filter	68
5.15	Firmware & Info Page.....	68
Appendices		71
A.1.	Technical Specifications	72
A.2.	Network Settings	73
A.3.	Troubleshooting	74
A.4.	Acronyms and Abbreviations.....	76
A.5.	Mounting Accessories.....	77
A.6.	Detaching the Camera from the Adapter Plate.....	78

List of Figures

Figure 1: CB-640x Bullet Camera with Sun Shield	6
Figure 2: Visible Security Cameras Page on FLIR.com	7
Figure 3: FLIR Quasar™ Premium Bullet Details Page on FLIR.com	8
Figure 4: FLIR Quasar™ Premium Bullet Support Page	8
Figure 5: Side Dimensions	9
Figure 6: Front Dimensions	9
Figure 7: Hardware	11
Figure 8: System Cable.....	12
Figure 9: Internal Interfaces	13
Figure 10: PoE Connection	14
Figure 11: DNA Discover List.....	16
Figure 12: DNA - Select Login	17
Figure 13: DNA - Login Window	17
Figure 14: DNA - IP Setup Window	17
Figure 15: DNA - IP Setup Window - Status Ok	18
Figure 16: DNA - Change Video Format Window	18
Figure 17: RJ45 Insertion Tool.....	19
Figure 18: Single Cable Rubber Seal	19
Figure 19: Alignment Triangles	20
Figure 20: Attach Camera to Back Box.....	20
Figure 21: Mounting Complete.....	20
Figure 22: Adjusting the Sun Shield.....	20
Figure 23: Supporting the Camera.....	21
Figure 24: Aiming the Camera	21
Figure 25: Aligning the Toothed Surfaces.....	22
Figure 26: Camera Web Page Login Screen	23
Figure 27: Camera Web Page First-Time Login	24
Figure 28: View Settings Home Page (Google Chrome)	24
Figure 29: Video Page	26
Figure 30: VLC Open Media Screen	31
Figure 31: Media Player Screen	32
Figure 32: Visible Page	32
Figure 33: Visible Page Advanced Settings > Auto Exposure Mode Settings (Auto Selected).....	33
Figure 34: Backlight Compensation Settings	35
Figure 35: Manual White Balance Settings.....	36
Figure 36: Additional Advanced Settings	36
Figure 37: I/O Page - Alarm Input Pin Settings.....	37
Figure 38: Alarm Output Pin - Pulse Settings	38

Figure 39: Alarm Output Pin - Normal Settings	38
Figure 40: Illumination Page	39
Figure 41: OSD Page - OSD1 Settings.....	40
Figure 42: Privacy Zone Page	41
Figure 43: Three Privacy Zones Set Up - Zone-1 Selected.....	41
Figure 44: Motion Page.....	42
Figure 45: Motion Detection Enabled and Zone Defined.....	43
Figure 46: System Settings Network Page - IP Mode Settings	44
Figure 47: QoS Settings.....	45
Figure 48: UPnP Settings.....	46
Figure 49: DDNS Settings - DynDNS Selected	46
Figure 50: Additional Networking Settings	47
Figure 51: RTSP Page	47
Figure 52: Date & Time Page - NTP Selected	48
Figure 53: Date & Time Page - Manual Selected	48
Figure 54: Users Page	49
Figure 55: Add User Dialog Box	49
Figure 56: User Management	50
Figure 57: FTP Page.....	50
Figure 58: SD Card Page – SD Card Not Inserted	51
Figure 59: SD Card Page – SD Card Inserted and Files Available	52
Figure 60: Alarm Page	52
Figure 61: Rule Configuration Trigger Screen - I/O Trigger Selected	53
Figure 62: Rule Configuration - I/O Trigger Selected	54
Figure 63: Arming Schedule Setting Screen.....	54
Figure 64: Arm Alarm and Enable Action Monday through Friday 8 AM-6 PM	55
Figure 65: Modified Alarm Armed Schedule	55
Figure 66: Rule Configuration Action Screen.....	56
Figure 67: Rule List.....	56
Figure 68: Rule List - Rule Trigger	57
Figure 69: Audio Page	57
Figure 70: I/O Devices Page.....	58
Figure 71: Sound Page	58
Figure 72: Snapshot Page	59
Figure 73: Recording Page - One Shot Record Status.....	59
Figure 74: Email Page.....	60
Figure 75: Add Contact Screen.....	61
Figure 76: Contact Management	61
Figure 77: Cyber Page - Certificate Settings	62

Figure 78: Certificate Generated.....	63
Figure 79: Upload Certificate	63
Figure 80: SNMP Settings.....	64
Figure 81: 802.1X Settings.....	66
Figure 82: TLS/HTTPS Settings	67
Figure 83: Port Settings	67
Figure 84: IP Filter Settings.....	68
Figure 85: Firmware & Info Page	69
Figure 86: Detaching the Camera from the Adapter Plate.....	78

1 Document Scope and Purpose

The purpose of this document is to provide instructions and installation procedures for physically connecting the CB-640x 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 FLIR products accept full responsibility for ensuring the suitability and considering the role of the product detection capabilities and their limitation as they apply to their unique site requirements.

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

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

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

Avis de non-responsabilité

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

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

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

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



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

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



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

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



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

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



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

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

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:



Warning

- The unit's cover is an essential part of the product. Do not open or remove it.
- Never operate the unit without the cover in place. Operating the unit without the cover poses a risk of fire and shock hazards.
- Do not disassemble the unit 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.

Avertissement

- *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.*



Warning

- 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°C to 60°C (-40°F to 140°F) cold start, with no more than 95% 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 60°C/-40° à 140°F), sans condensation d'humidité supérieur à 95%.

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.

2 Introduction

This guide is intended to help you physically install, configure settings for, and operate a CB-640x indoor/outdoor bullet IP camera. CB-640x cameras provide real-time video up to 4K UHD (CB-6408 models) or up to Quad HD (CB-6404 models); Shutter Wide Dynamic Range up to 120/130dB; line-level audio in/out; digital I/O; and infrared (IR) illumination.

The following models are available:

Specification	CB-6408-11-I	CB-6408-21-I	CB-6404-11-I	CB-6404-21-I
Image Sensor	1/1.8" CMOS		1/2.8" CMOS	
Sensor Resolution	3840 x 2160		2560 x 1440	
Scanning Mode	Progressive			
Lens Type	Varifocal 3.6-10mm 97°~46° HFOV F1.5, D/N motorized auto-focus / auto-iris P-Iris lens	Varifocal 9-22mm 62°~26° HFOV F1.6, D/N motorized auto-focus / auto-iris P-Iris lens	Varifocal 2.7-13.5mm 102°~32° HFOV F1.4, D/N motorized auto-focus / auto-iris P-Iris lens	Varifocal 9-22mm 39°~16.5° HFOV F1.6, D/N motorized auto-focus / auto-iris P-Iris lens

Additional, up-to-date specifications are available from [the FLIR Quasar™ Premium Bullet pages on FLIR.com](https://www.flir.com/products/cb-640x/).

When the camera is connected to an IP network, it functions as a server, providing services such as camera control, video streaming, and network communications. Up to three streams can operate simultaneously with H.265, H.264, or MJPEG compression, providing an ideal solution when differing levels of image quality are required. In addition, the cameras support FLIR's adaptive streaming algorithms, which provide the highest image quality with the lowest bandwidth and storage requirements.

The cameras can be powered by 802.3at Power over Ethernet (PoE+), 12VDC, or 24VAC.



Figure 1: CB-640x Bullet Camera with Sun Shield

2.1 Features

- Progressive 4K 1/1.8" or QHD 1/2.8" CMOS sensor, depending on the model
- H.265, H.264, and MJPEG compression
- Audio line in and out
- Tampering detection and notifications
- SNMP v1/v2c/v3 and SNMP traps
- Backlight compensation
- Electronic day/night (ICR)
- ONVIF support
- Two regions of interest
- 8 privacy zones
- Built-in web server
- Triple stream: 4K / Quad HD + Full HD 1080p / HD 720p + D1, depending on the model
- 64kbps-20mbps bit rate
- Alarm in and out
- Remote viewing via RTSP on media players
- 802.1X and SSL/TLS security protocols
- Gamma correction
- Shutter WDR
- Digital WDR
- Infrared LED illuminator
- Built-in heater
- Record snapshots and video on 512GB microSDXC card (not included)
- Send snapshots on alarm to FTP or 10 email addresses
- Cybersecurity features
- Motion detection event-driven alarms
- Powered by 802.3at PoE+
- UPnP support
- White balance
- 3DNR image noise reduction
- Low-lux mode without IR
- Up to 9 users

2.2 Accessing Product Information from the FLIR Website

Up-to-date resources for the camera, including the camera's specifications, the Discovery Network Assistant (DNA) software tool, and this installation and user guide, are available from [the FLIR Quasar™ Premium Bullet pages on FLIR.com](#).

To access product information from the FLIR website:

1. Open [FLIR.com](#), and then click [Products > Security > Visible Security Cameras](#).

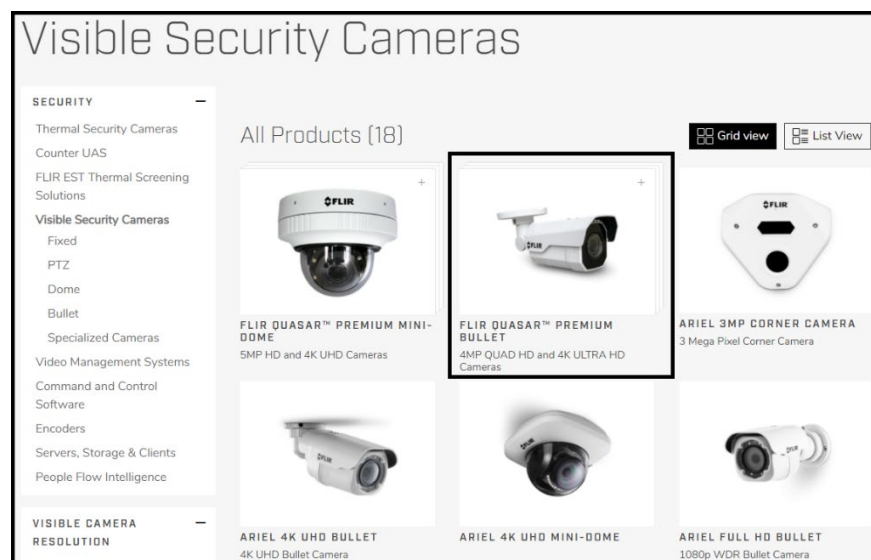


Figure 2: Visible Security Cameras Page on FLIR.com

- Click FLIR Quasar™ Premium Bullet. The camera's product details page appears.



Figure 3: FLIR Quasar™ Premium Bullet Details Page on FLIR.com

- Scroll down to see the camera's specifications and related documents.
- Click **Go to Product Support** to open the camera's support page.

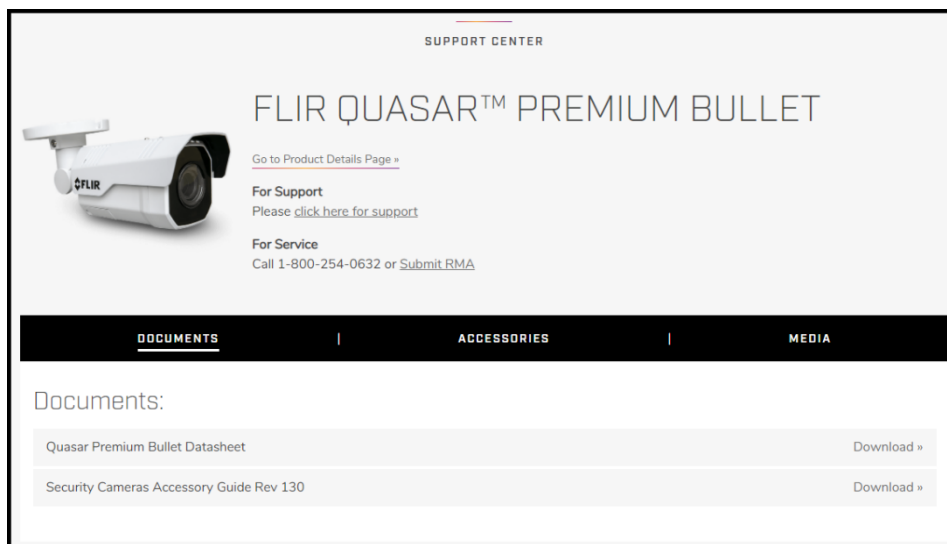


Figure 4: FLIR Quasar™ Premium Bullet Support Page

- Open the relevant tab. For example, to see the accessories available, open the Accessories tab.
- To download the resource, click the relevant **Download** link.

2.3 Camera Dimensions

Following are the CB-640x camera dimensions.

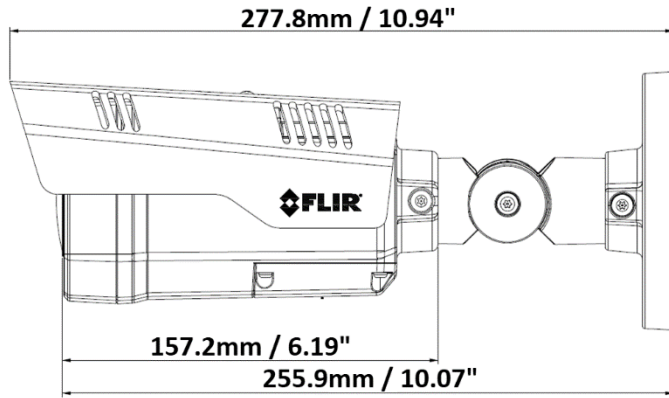


Figure 5: Side Dimensions

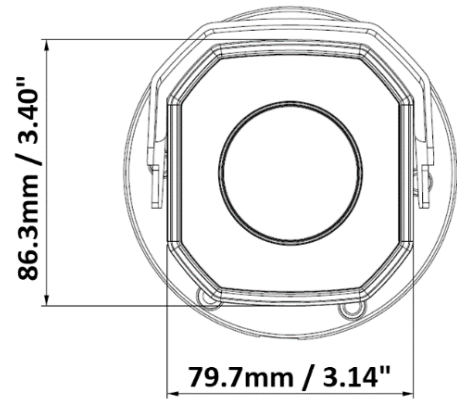


Figure 6: Front Dimensions

3 Installation

This chapter describes how to mount, connect, and initially configure the unit:

- [Supplied Components](#)
- [Pre-Installation Checklist](#)
- [Outdoor Mounting Recommendations](#)
- [Hardware Description](#)
- [Powering the Camera](#)
- [Initial Configuration](#)
- [Mounting the Back Box and Routing the Cables](#)
- [Mounting and Aiming the Camera](#)
- [Completing Camera Setup](#)
- [Attaching the Camera to a Supported VMS](#)

3.1 Supplied Components

The unit package contains the following items:

QTY	Description
1	CB-640x IR bullet camera body attached to sun shield, bracket, and adapter plate
1	T10 security Torx wrench
1	Back box
1	Two-pin terminal block
1	Mounting template
1	Part bag containing:
1	RJ45 insertion tool
1	Rubber seal for single cable
1	Rubber seal for multiple cables
1	Part bag containing:
1	Hex wrench
6	Plastic screw anchors
6	TP4x31mm tapping screw
6	M4x14 screw
1	<i>CB-640x Quick Install Guide</i>

3.2 Pre-Installation Checklist

Before installing the unit, make sure that:

- Instructions in the [General Cautions and Warnings](#) and [Site Preparation](#) sections 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°C to 60°C (-40°F to 140°F), with no more than 95% 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 60°C/-40° à 140°F), sans condensation d'humidité supérieur à 95%.

3.3 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.

3.4 Hardware Description

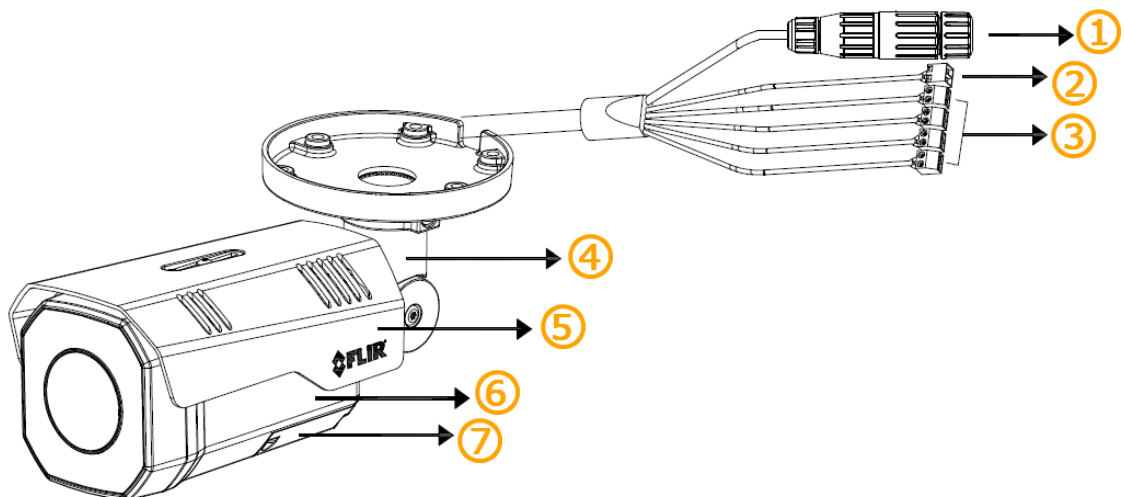


Figure 7: Hardware

Component		Description
1	RJ-45 connector	See System Cable .
2	Power connector	
3	Digital I/O connectors	

Component		Description
4	Direct mounting bracket	To install the camera directly on a wall or ceiling, without using the attached adapter plate and supplied back box. For more information, see Detaching the Camera from the Adapter Plate .
5	Sun shield	Minimizes the effects of rain and sunlight on image quality.
6	Camera body	With sun shield attached
7	Access cover	Provides access to the camera's Internal Interfaces .

3.4.1 System Cable

The camera's built-in system cable includes an RJ-45 Ethernet jack, and five (2) two-wire leads that provide audio input and output, alarm input and output, and external power supply connections. The cable includes an LED that flashes green to indicate power on and network activity.

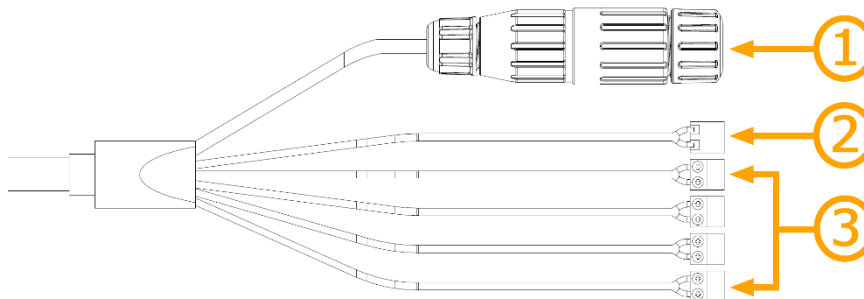


Figure 8: System Cable

Connector				
1	Black	RJ-45		
2	Black	12 VDC/24 VAC -	Red	12 VDC/24 VAC+
3	Yellow	AUDIO IN+	Orange	AUDIO IN-
	Purple	AUDIO OUT+	Green	AUDIO OUT-
	Red	ALARM IN Signal	Black	ALARM IN GND
	Brown	ALARM OUT Signal	Blue	ALARM OUT COM

3.4.2 Internal Interfaces

To access the camera's default and reset buttons, along with the camera's microSD card slot, remove the access cover by loosening two screws.

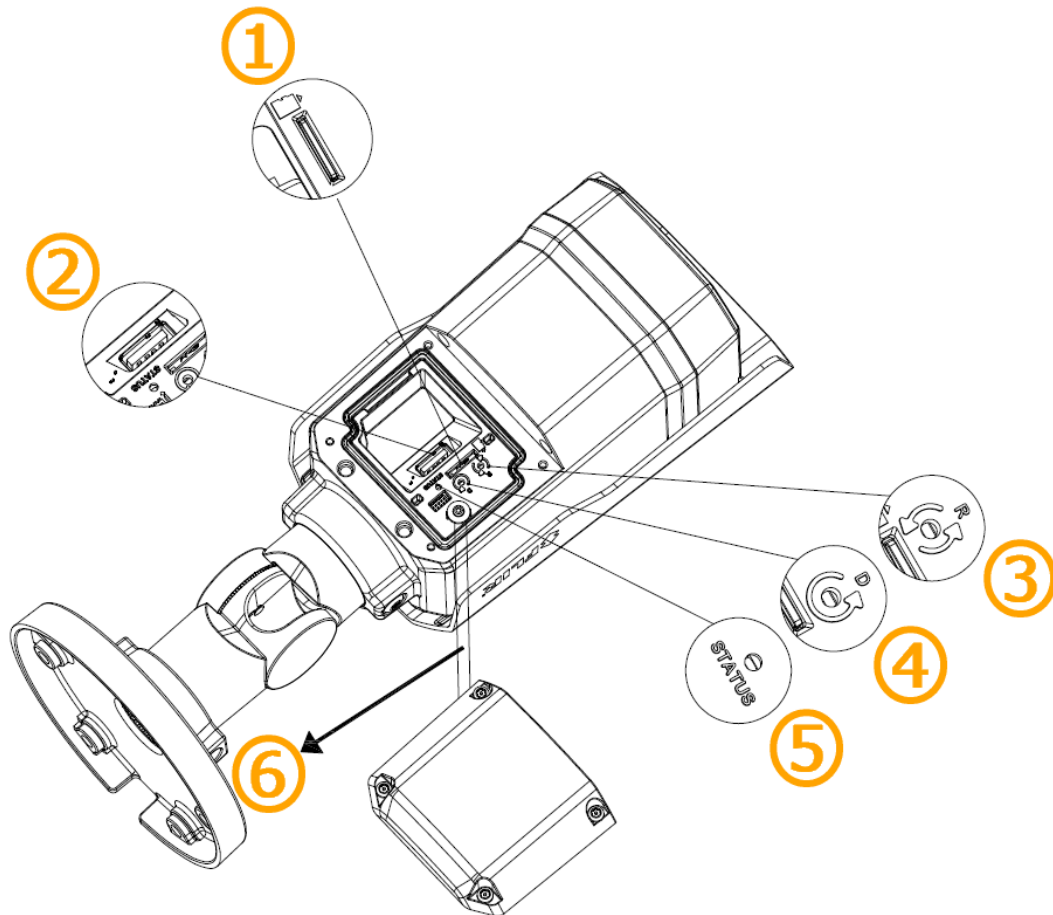


Figure 9: Internal Interfaces

Interface		Description
1	Micro SD card slot	<p>For recording and file storage, insert a microSDXC card (up to 512 GB, Class 10) in the card slot. For recording HD video, FLIR recommends an SDHC or SDXC card capable of a minimum write speed of 10 MB/sec.</p> <p>Caution</p> <p>Before you can record clips on the microSD card, it must first be formatted in the System Settings section of the camera's web page. See SD Card Page.</p>
2	USB	To be supported in a future release.
3	RESET (R)	To reboot the camera, press the button for at least one second.
4	DEFAULT (D)	To reset the camera to its factory defaults, press the button for at least six seconds.

Interface		Description			
5	STATUS	LED (green / red / amber) that indicates camera is booting up or firmware being upgraded.			
		Camera state	LED state	Description	
		Booting up	Solid red for 2-3 seconds, then:	Green	Normal After a successful boot, the LED turns off after three minutes.
				Red	An error has occurred.
Firmware upgrade	Flashing amber	During upgrade			
6	Safety wire	Makes sure the access cover does not drop. To ensure that the camera remains waterproof, store the safety wire inside the camera before locking the access cover.			

3.5 Powering the Camera

The camera can be powered by PoE or by an external DC or AC power supply (not included in the camera kit). The following diagram shows how the camera can be powered using PoE.

CB-640x Camera

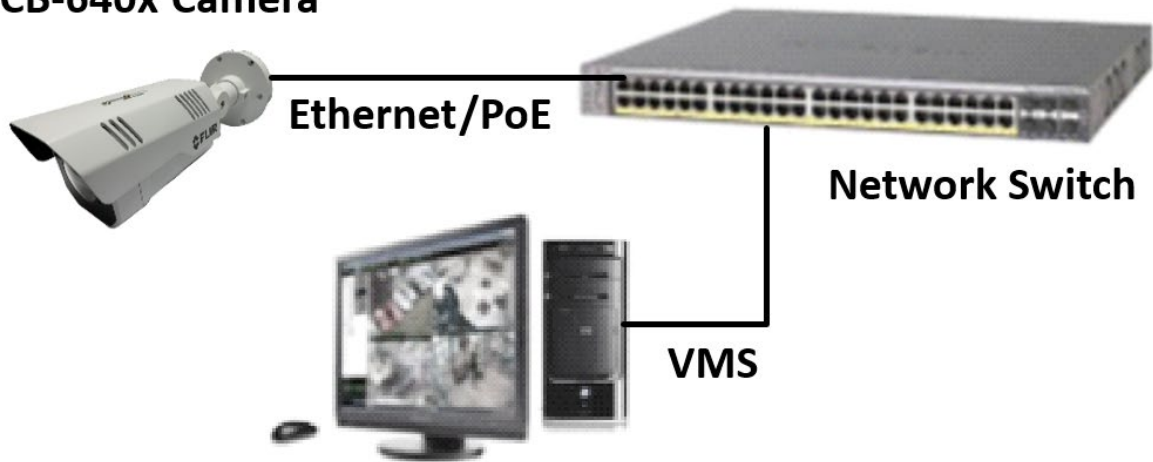


Figure 10: PoE Connection



Caution

- When powered by PoE, 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**

- *Lorsqu'il est alimenté par PoE, 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.*

3.6 Initial Configuration

FLIR recommends configuring the camera before mounting and aiming it. It is also possible to configure the camera after mounting it, which could be more appropriate for certain installations.

If you are configuring the camera before mounting and aiming it, connect the camera according to the information in [Hardware Description](#), and then proceed with initial configuration.

If you are mounting the camera prior to initial configuration, proceed as such:

1. [Mounting and Connecting the Camera](#)
2. [Adjusting the Sun Shield](#)
3. [Initial Configuration](#)
4. [Aiming the Camera](#)—FLIR recommends someone watch the camera's live video while aiming it. Therefore, perform initial configuration before aiming it.

You can perform initial configuration using version 2.3.0.20 or higher of the DNA tool, the camera's web page, or a supported VMS.

Initial configuration 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	•	•
Change video format	•	•
Configure more than one camera at the same time	•	

**Notes**

- The DNA tool does not require a license to use and is a free download from [the FLIR Quasar™ Premium Bullet pages on FLIR.com](#). For more information about using the DNA tool, including how to configure more than one camera at the same time, see the *DNA User Guide*. While the software is open, click the Help icon
- For more information about using a VMS to configure one or more cameras at the same time, see the VMS documentation.

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

- [Discover the Camera and Configure for Networking](#)
- [Change the Video Format \(Optional\)](#)
- [Attach the Camera to a VMS](#)

3.6.1 Discover the Camera and Configure for Networking


By default, DHCP (Dynamic Host Configuration Protocol) is enabled on the camera. 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's Horizon or Meridian VMS and the VMS is configured as a DHCP server, the VMS automatically assigns the camera an IP address. That IP address appears in the DNA Discover List.
- If the camera is managed by FLIR's Latitude VMS or is on a network with static IP addressing, manually specify the camera's IP address using the DNA tool.

To view and 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.

FLIR recommends using the DNA tool to discover the camera on the network.

To install the DNA tool and discover the camera on the network:

1. Download version 2.3.0.20 or higher of the DNA tool from [the FLIR Quasar™ Premium Bullet pages on FLIR.com](#) (see 2.2 Accessing Product Information from the FLIR Website). Save the ZIP file on a computer running Windows on the same VLAN to which you will connect the camera.
2. Unzip the file and then run the `dna.exe` file by clicking the  icon.
DNA opens and the camera appears in the Discover List.

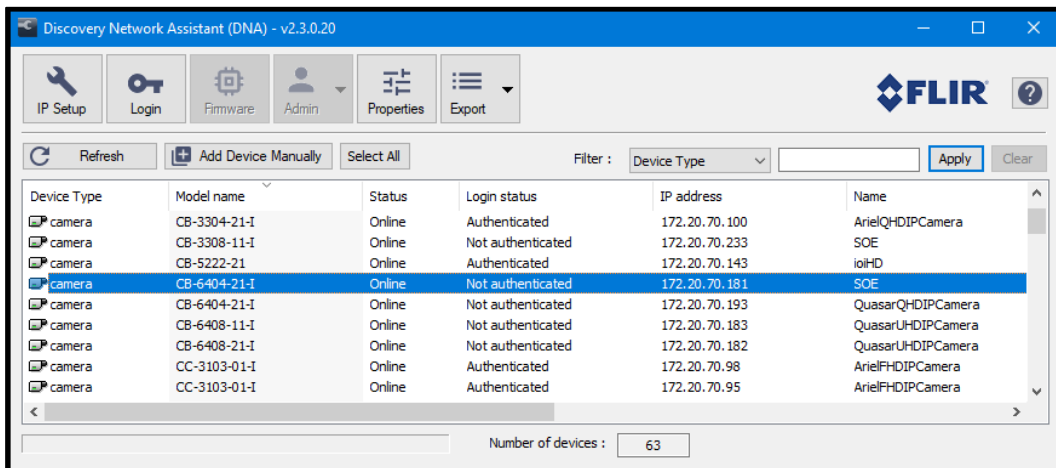


Figure 11: DNA Discover List

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

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*).

1. 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**.

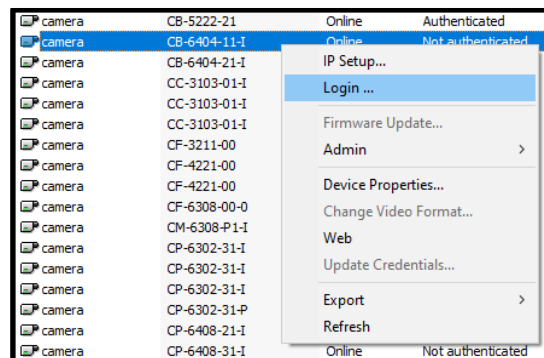


Figure 12: DNA - Select Login

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.

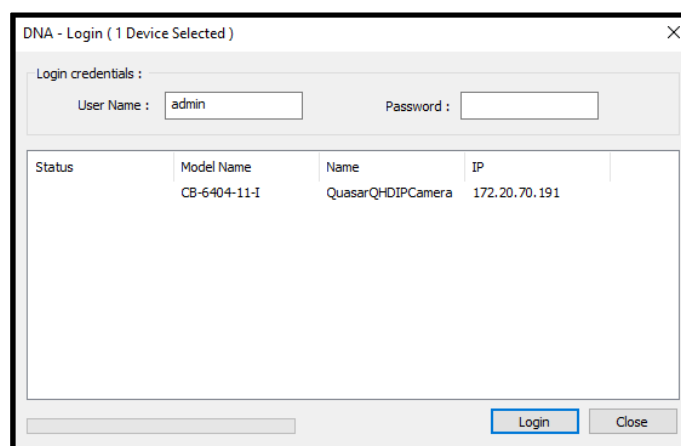



Figure 13: DNA - Login Window

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*.

- In the DNA Discover List, right-click on the unit and select **IP Setup**. The DNA - IP Setup window appears.

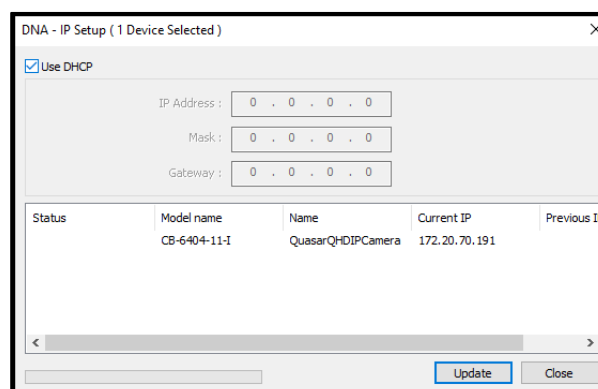


Figure 14: DNA - IP Setup Window

- Uncheck *Use DHCP*.
- Specify the camera's *IP address*, subnet *Mask*, and *Gateway* IP address.
It is possible to specify an IP address without changing the subnet.
- Click **Update**.

The camera reboots with the new settings. Wait for  Ok status to appear.

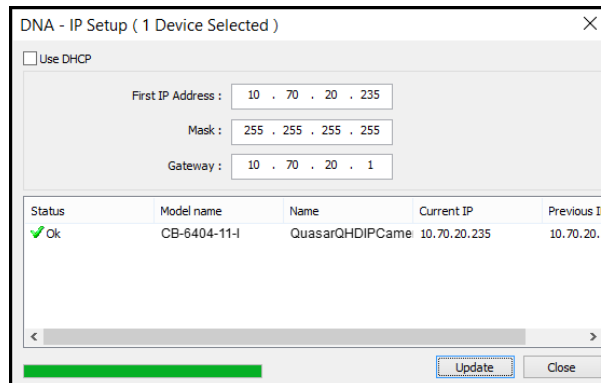


Figure 15: DNA - IP Setup Window - Status Ok

You can now [access the camera's web page](#) using the IP address you specified.

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

1. [Access the camera's web page.](#)
2. On the [View Settings Home Page](#), click **System Settings**, and make sure the [Network page](#) appears.
3. Click the **Static** button and then manually specify the camera's networking settings; for example, IP address, subnet mask, and default gateway.
4. Click **Save**. Applying any changes on the Network page requires rebooting the camera.

3.6.2 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**.

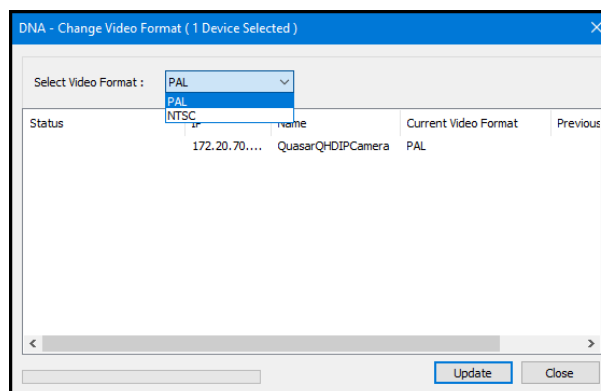


Figure 16: DNA - Change Video Format Window

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.

3.7 Mounting the Back Box and Routing the Cables

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

To maintain structural integrity, before drilling into the mounting surface, make sure it is at least 50mm (2") thick.

To mount the back box:

1. Using the mounting template, drill six holes on the wall or mounting surface: Diameter \varnothing 3/8" (9.5mm), depth 1/1/2" (40mm). To ensure proper installation, make sure the drilled holes are of correct size.
2. Hammer the six screw anchors into the drilled holes.
3. Cables can enter the back box from the rear or from the side. If the cables are going to enter from the rear, use the mounting template to drill a bottom conduit hole for the cables.
4. Route the power and network cabling into the back box.
 - If you are connecting the camera using a single Ethernet cable with an RJ45 plug attached, attach the RJ45 insertion tool included with the camera to the RJ45 plug. Then, route the tool, plug, and cable through the single cable rubber seal included with the camera.



Figure 17: RJ45 Insertion Tool



Figure 18: Single Cable Rubber Seal

- If you are connecting the camera in any other way, route the cables through the multiple cable rubber seal included with the camera.

Securely fasten the rubber seal to either the bottom or the side conduit hole. In addition, FLIR recommends applying 3M waterproofing tape on the cables that pass through either conduit hole.

5. Mount the back box onto the wall or surface. Using the Philips head screwdriver, fasten the six TP4 tapping screws into the six screw anchors.

Connect the Camera

Inside the back box, connect the camera's system cable to the other cables according to the information in [Hardware Description](#).

3.8 Mounting and Aiming the Camera

3.8.1 Attaching the Camera to the Back Box

With the camera attached to the adapter plate, align the triangle on the adapter plate with the triangle on the back box.

Alignment triangles

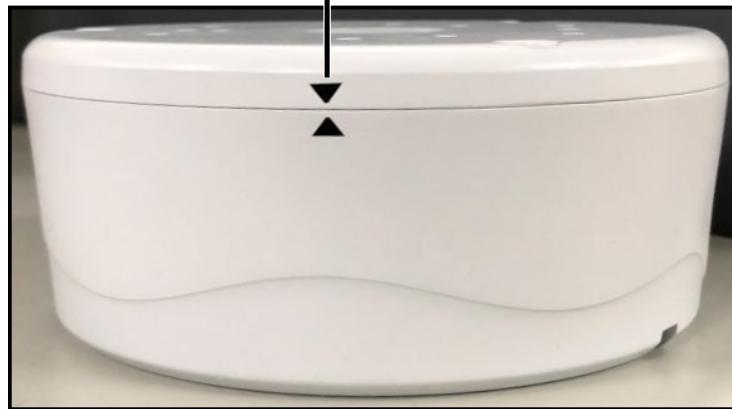


Figure 19: Alignment Triangles

Then, while carefully holding and fully supporting the camera, to make sure the screws are not bearing the camera's weight when tightening them, use the Torx wrench to tighten the three T20 screws attached to the adapter plate.

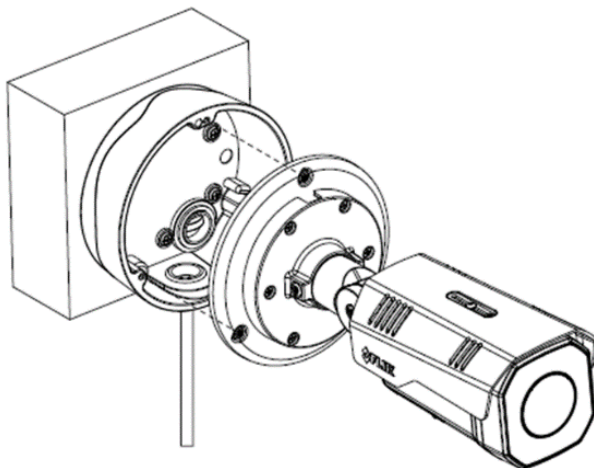


Figure 20: Attach Camera to Back Box

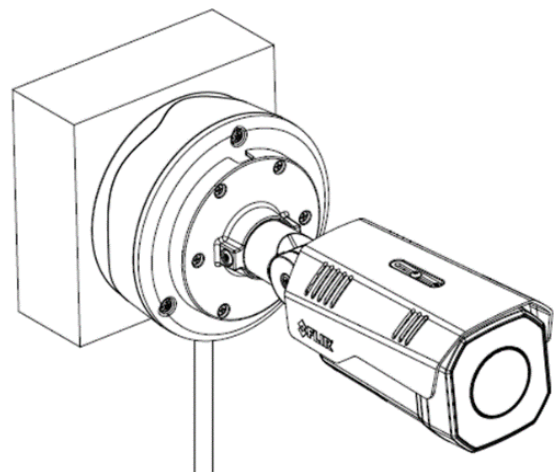


Figure 21: Mounting Complete

3.8.2 Adjusting the Sun Shield

The CB-640x cameras are designed to operate in rugged environments. The sun shield is coated to prevent damage from sunlight or rain.

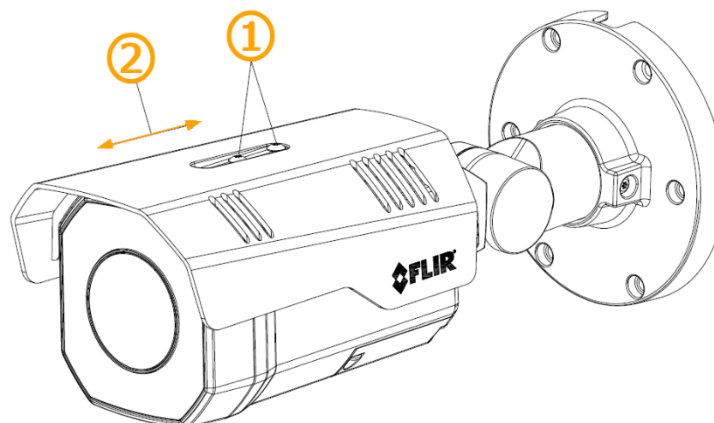


Figure 22: Adjusting the Sun Shield

To adjust the sun shield:

1. Loosen the two screws on the shield hood.
2. Move the sun shield forward or backward.
3. Tighten the two screws.



Tip

Adjust the sun shield to avoid issues with shadows. Take into account the lens coverage.



Caution

To avoid damaging the camera housing, do not adjust the sun shield beyond its limits.

3.8.3 Aiming the Camera

While supporting the camera with your hand, loosen the three locking screws and adjust the camera's pan, tilt, and rotation:

- Retaining ring for pan adjustment (1): Using the T10 torx wrench, loosen the locking screw and rotate the camera. You can also rotate the lens base until satisfied with the field of view. Do not exceed the $\pm 360^\circ$ pan range limit.
- Bracket for tilt adjustment (2): Using the T10 torx wrench, loosen the locking screw and adjust the bracket. Do not exceed the $0^\circ \sim 90^\circ$ tilt range limit.
- Retaining ring for 360° rotation (3): Using the T10 torx wrench, loosen the locking screw and rotate the camera body. Do not exceed the $\pm 360^\circ$ rotation range limit.



Figure 23: Supporting the Camera

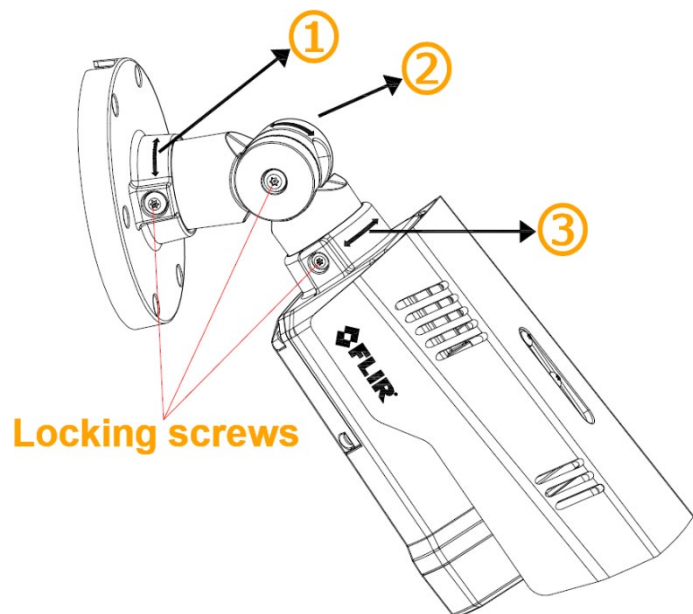


Figure 24: Aiming the Camera

Make sure that the toothed surfaces are properly aligned and meet evenly. Then, use the T10 torx wrench bit to securely tighten each locking screw.

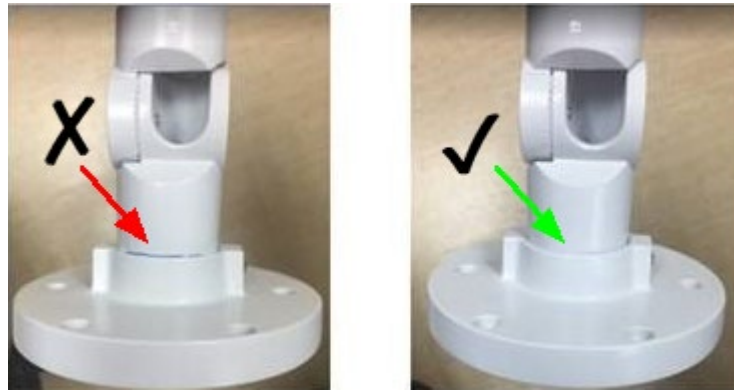


Figure 25: Aligning the Toothed Surfaces

3.9 Completing Camera Setup

Specify the camera's zoom and focus, and format the microSDXC card, by [Accessing the Camera's Web Page](#). For more information about the camera web page's zoom and focus controls, see [View Settings Home Page](#). For more information about formatting the microSDXC card, see [SD Card Page](#).

3.10 Attaching 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 includes information about how to [access the camera](#) and how to operate it using the [View Settings page](#).

4.1 Accessing the Camera's Web Page

The camera includes a web interface that enables it to be configured and operated from a web browser. FLIR recommends using Google Chrome to access the camera's web page, which also supports other browsers such as Firefox, Microsoft Edge, and Internet Explorer 11 (32-bit).

You can open the camera's web page from the DNA tool or directly in a web browser.

To access the camera's web page

- Do one of the following:
 - From the DNA Discover List, double-click the camera.
 - Open Google Chrome or another web browser, enter the camera's IP address in the browser's address bar and press ENTER.

Note

When HTTPS (secure HTTP) is enabled, by default the system uses HTTPS when you enter the IP address. For example, `https://192.168.0.250`. See [TLS/HTTPS](#).

If you want to use HTTP to log into the device, enter `http://(camera IP address)`. For example, `http://192.168.0.250`.

The camera's login screen appears.

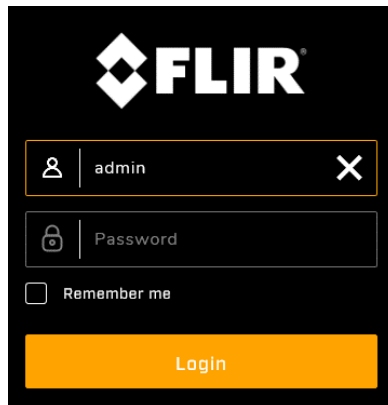


Figure 26: Camera Web Page Login Screen

- On the login screen, type a user name and the password. Both 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, type admin for the user name and for the password.

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

- Click **Login**. The camera's web page opens.

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

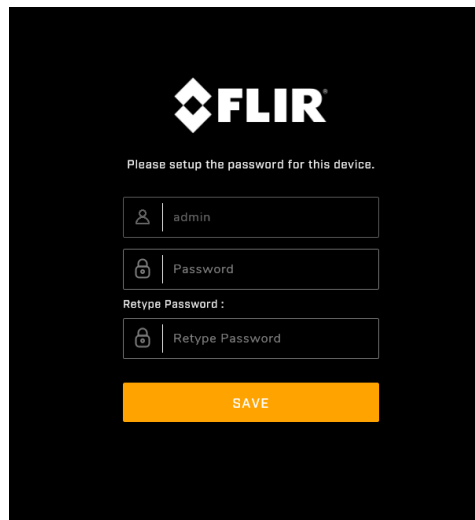


Figure 27: Camera Web Page First-Time Login

4. Log back in with the new password. The camera's [View Settings home page](#) opens.

4.2 View Settings Home Page

By default, the camera web page opens on the View Settings page.

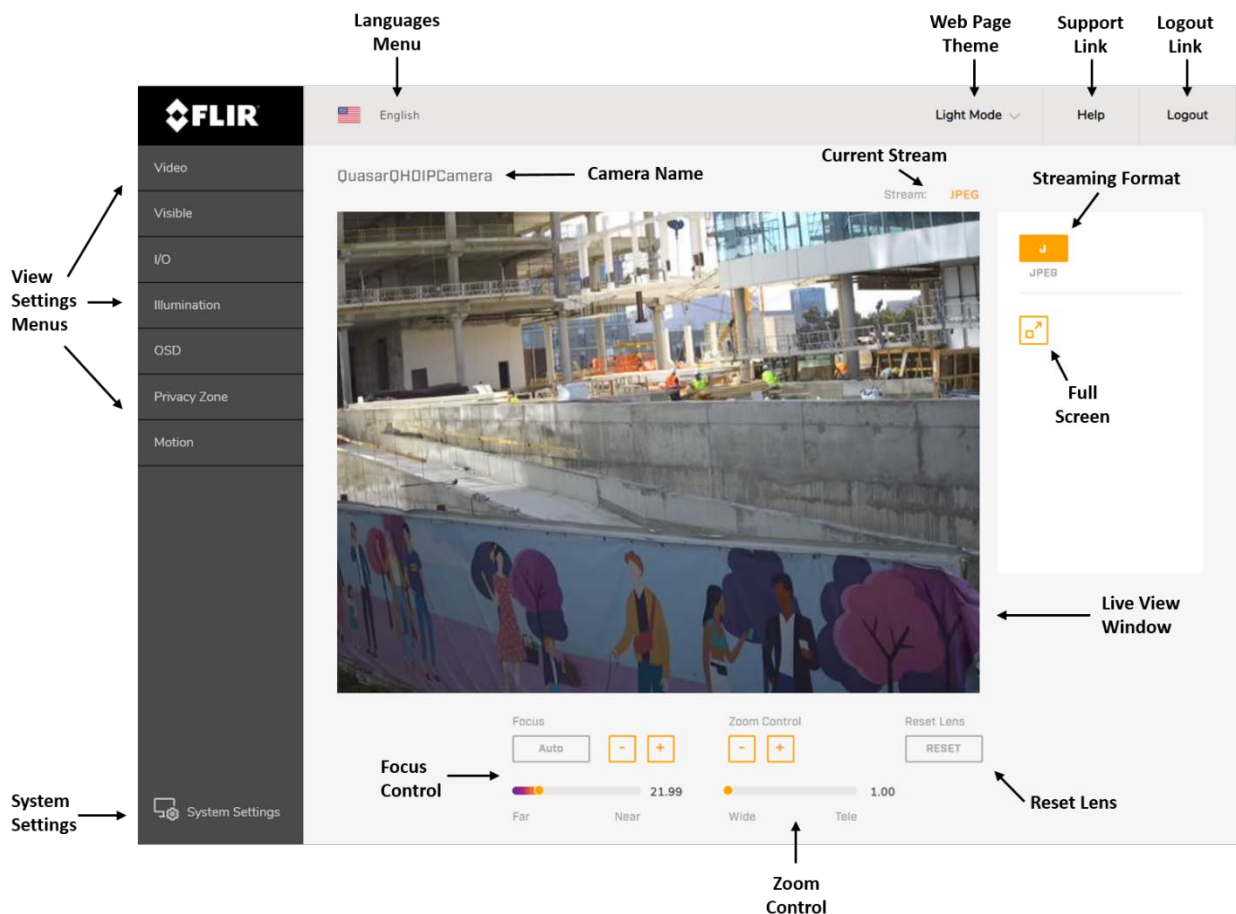


Figure 28: View Settings Home Page (Google Chrome)

To the left of the Live View window, the following View Settings Menus are displayed:

- Video – Click to open the Video page and configuration options.
- Visible – Click to open the Visible page and configuration options.
- I/O – Click to open the I/O page and configuration options.
- Illumination – Click to open the Illumination page and control options.
- OSD – Click to open the OSD page and configuration options.
- Privacy Zone – Click to open the Privacy Zone page and configuration options.
- Motion – Click to open the Motion page and configuration options.

The following information is displayed above the Live View window:

- Camera Name – Displays the specified camera name.
- Languages Menu – Select the language for the web interface: English, Arabic, Czech, Simplified Chinese, Traditional Chinese, French, German, Hungarian, Italian, Japanese, Polish, Portuguese, Russian, or Spanish.
- Stream – Displays the current live video stream (in Google Chrome, JPEG; in Internet Explorer, stream1, 2, or 3).





The following information is displayed in the upper right corner of the GUI:

- *Light Mode/Dark Mode* (Chrome and Internet Explorer only) – Select the camera web page theme. *Light Mode* is the default setting.
- Logout Link – Click **Logout** to exit the camera's web page.
- Support Link – Click **Help** to open <https://www.flir.com/support>.

The following information is displayed to the right of the Live View window:

- Streaming Format – MJPEG (JPEG, or **J**).
- Full Screen button – Click to maximize the current Live View window video stream.

The following information is displayed under the Live View window:

- Focus – To set Auto Focus, click **Auto**. To manually set the focus:
 - Click the  or  buttons.
 - Move the slider between Far (1) and Near (100).
- Zoom Control – To adjust the zoom:
 - Click the  or  buttons.
 - Move the slider between Wide (1.00) and Tele (3.00).
- Reset Lens – If Auto Focus does not produce a clear picture, click **Reset**. Then, under Focus, click **Auto**. The image refocuses.

Click **System Settings** to open the [System Settings pages and configuration options](#).

4.3 Video Page

The camera provides the capability to configure three video stream profiles. Each profile supports three concurrent streams. Each stream can be configured separately for optimized quality and bandwidth. Each stream has its own settings, which can include Resolution; Compression and associated settings; DSCP; Frame Rate; Rate Control; and Maximum Bit Rate.

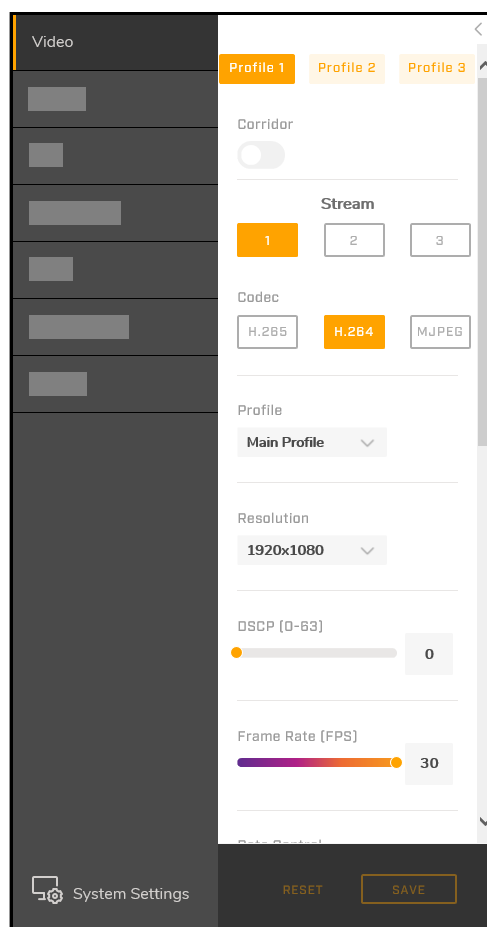


Figure 29: Video Page

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

If you want the image rotated 90° counterclockwise (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. This mode is referred to in Latitude as “90 and 270 degrees” mode.



Note

When *Corridor* is enabled, only the H.264 codec is supported.

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

Codec: Select *H.265*, *H.264* (default), or *MJPEG* based on required image quality and storage space. For information about resolutions and codecs CB-640x cameras support, see [Resolution](#).

If you select *H.265* or *H.264*, you can configure the following:

Profile: Each profile targets specific classes of applications.

- **High Profile** (default for H.264 codec; not available for H.265 codec): 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.

- **Main Profile** (only profile available for H.265 codec): 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.
- **Baseline Profile** (not available for H.265 codec): 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.

Resolution: The specific camera model and the video format selected on [the Visible Page](#) determine the resolutions, frame rates, and codecs the streams support.

CB-6408 models - NTSC		
Stream 1	Stream 2	Stream 3
3840x2160 30fps H.264/H.265	OFF	OFF
	1920x1080 30fps H264/H265 15fps MJPEG	OFF
	1280x720 30fps H264/H265/MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
1920x1080 30fps H264/H265 15fps MJPEG	OFF	OFF
	1280x720 30fps H264/H265/MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
	720x480 30fps H264/H265/MJPEG	OFF
720x480 30fps H264/H265/MJPEG		

CB-6408 models - NTSC		
Stream 1	Stream 2	Stream 3
1280x720 30fps H264/H265/MJPEG	OFF	OFF
	1920x1080 30fps H264/H265 15fps MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
	1280x720 30fps H264/H265/MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
	720x480 30fps H264/H265/MJPEG	OFF
720x480 30fps H264/H265/MJPEG		
720x480 30fps H264/H265/MJPEG	OFF	OFF
	1920x1080 30fps H264/H265 15fps MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
	1280x720 30fps H264/H265/MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
	720x480 30fps H264/H265/MJPEG	OFF
720x480 30fps H264/H265/MJPEG		

CB-6404 models - NTSC		
Stream 1	Stream 2	Stream 3
2560x1440 30fps H.264/H.265	OFF	OFF
	1920x1080 30fps H264/H265 15fps MJPEG	OFF
		1280x720 30fps H264/H265/MJPEG
		720x480 30fps H264/H265/MJPEG
	1280x720 30fps H264/H265/MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
720x480 30fps H264/H265/MJPEG	OFF	
	720x480 30fps H264/H265/MJPEG	

CB-6404 models - NTSC		
Stream 1	Stream 2	Stream 3
1920x1080 30fps H264/H265 15fps MJPEG	OFF	OFF
	1280x720 30fps H264/H265/MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
	720x480 30fps H264/H265/MJPEG	720x480 30fps H264/H265/MJPEG
1280x720 30fps H264/H265/MJPEG	OFF	OFF
	1920x1080 30fps H264/H265 15fps MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
	1280x720 30fps H264/H265/MJPEG	720x480 30fps H264/H265/MJPEG
720x480 30fps H264/H265/MJPEG	720x480 30fps H264/H265/MJPEG	OFF
	1920x1080 30fps H264/H265 15fps MJPEG	OFF
		720x480 30fps H264/H265/MJPEG
	1280x720 30fps H264/H265/MJPEG	720x480 30fps H264/H265/MJPEG
720x480 30fps H264/H265/MJPEG	720x480 30fps H264/H265/MJPEG	OFF
	720x480 30fps H264/H265/MJPEG	720x480 30fps H264/H265/MJPEG

When PAL is selected, the streams support 720x576 and 25fps instead of 720x480 and 30fps.

DSCP (Differentiated Services Code Point): Specify a value between 0-63. The default DSCP value is 0 (DSCP 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.

Frame Rate: Specify a value between 1-30 for NTSC or 1-25 for PAL. The higher the FPS, the smoother the motion in the video. The maximum frame rate for the video format is the default.

Rate Control:

- **CBR (Constant Bit Rate):** Specify a constant, maximum bit rate. 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 / Max Bit Rate: Specify 64 ~ 20000 for H.264 codec or 64 ~ 8000 for H.265 codec. 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.

Encoding Priority (available only for H.264 with CVBR): This function enables the user to adjust 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: Specify a value between 1-60 (NTSC) or 1-50 (PAL). The default is 30 for NTSC and 25 for PAL (one I-Frame transmitted every second).

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.264 and H.265 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.

If you select the **MJPEG** codec, you can configure the stream resolution, DSCP, frame rate, and the **Quality Level**: Select *High*, *Mid* (default), or *Low*. *Low* produces the highest image quality but increases the file size. *High* produces the lowest image quality but decreases the file size.

Multicast

Configure how the multicast address the camera uses for video and audio streaming is determined.

Address Type:

- **Auto** (default): A connected application such as a VMS automatically determines the camera's multicast IP address.
- **Manual:** When selected, you can configure the camera's multicast:
 - **Address:** A valid multicast address in the range 224.0.1.1 – 239.255.255.254.
 - **Port:** The port the camera uses for multicast streaming.



Note

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

Metadata

Enables embedding information regarding events, such as motion and tampering, into the video stream; required for full VMS support. Select **ON** (default) or **OFF**.

If you made any changes on the Video page, click **Save** to apply the changes. Click **Reset** to discard changes and revert to the last saved settings.

4.3.1 Viewing Live Video using a Media Player

The main live video stream and sub-stream can be viewed with a media player such as VLC (download from <http://www.videolan.org/vlc/index.html>). Streams can be viewed for the three channels and three video encoding formats (H.264, H265, and MJPEG).

To view a media stream with VLC

1. Open VLC.
2. From the **Media** tab, select *Open Network Stream*. The **Open Media** screen is displayed.

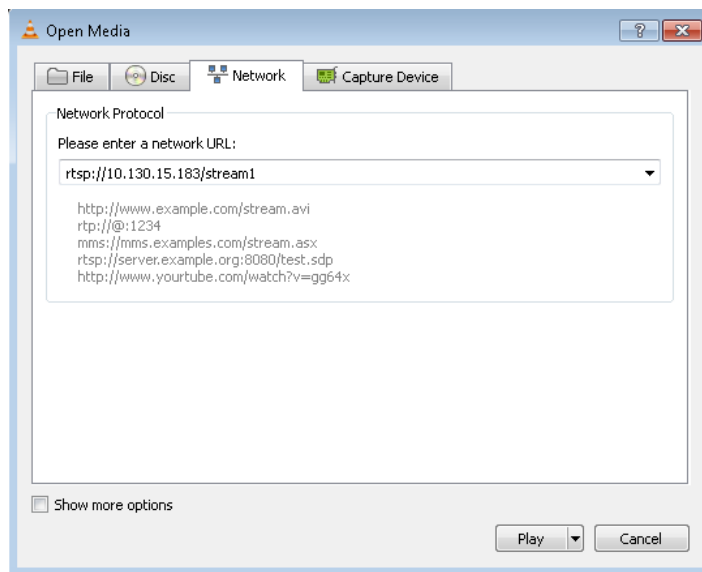


Figure 30: VLC Open Media Screen

3. On the **Network** tab, enter the network URL for the stream. The URL syntax is: `rtsp://(camera IP address)/(stream name)`.

Stream	Stream name	Example URL
Unicast stream 1	stream1	rtsp://192.168.0.250/stream1
Multicast stream 1	stream1m	rtsp://192.168.0.250/stream1m
Unicast stream 2	stream2	rtsp://192.168.0.250/stream2
Multicast stream 2	stream2m	rtsp://192.168.0.250/stream2m
Unicast stream 3	stream3	rtsp://192.168.0.250/stream3
Multicast stream 3	stream3m	rtsp://192.168.0.250/stream3m

If the URL does not specify a port, the media player attempts to open the stream using the default RTSP port, 554. Although not recommended if the camera is attached to a VMS, it is possible to configure a different RTSP port on the [RTSP Page](#). If the camera's configured RTSP port is different than 554, then the syntax for entering the URL in the media player is:

`rtsp://(camera IP address):(port)/(stream)`

For example, `rtsp://192.168.0.250:1025/stream1`.

- Click **Play**. The video stream is displayed in the media player. If available, audio will also be streamed.

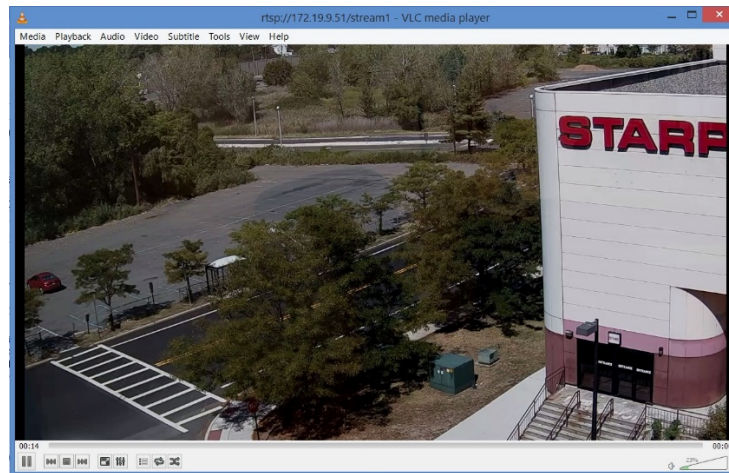


Figure 31: Media Player Screen

4.4 Visible Page

The Visible page enables you to configure picture quality, focus, zoom, and other image settings.

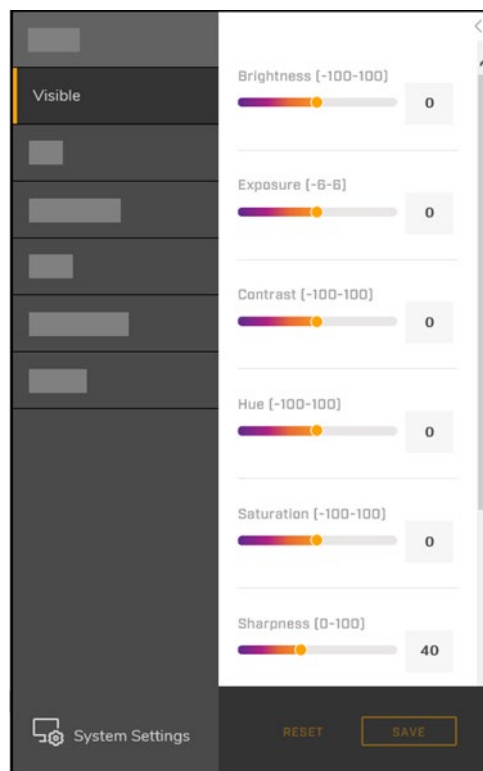


Figure 32: Visible Page

Brightness: Specify a value between *-100* and *100*, which provides the highest brightness. The default is *0*.

Exposure: Represents a combination of a camera's shutter speed and f-number, which brightens or darkens the scene accordingly. Specify a value between *-6* (darkest) and *6* (brightest). The higher the number, the brighter the image. The default setting is *0*.

Contrast: Specify a value between *-100* and *100*, which provides the highest contrast. The default is *0*.

Hue: Specify a value between *-100* and *100*, which provides the deepest hue. The default is *0*.

Saturation: Specify a value between *-100* and *100*. The lower the number, the closer the image is to a grayscale (i.e., monochrome or black-and-white) image. The higher the number, the deeper the image color (i.e., reds will be redder and blues will be bluer). The default is *0*.

Sharpness: Specify a value between *0-100*, which provides the highest sharpness around the edges and for small features. The default setting is *40*.

3D Noise Reduction: Specify a value between *0-100*. The default setting is *20*.

2D Noise Reduction: Specify a value between *0-100*. The default setting is *20*.

Advanced settings

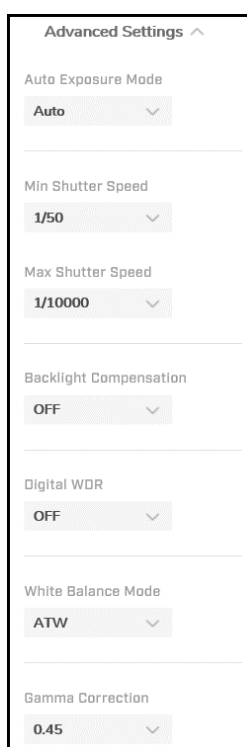


Figure 33: Visible Page Advanced Settings > Auto Exposure Mode Settings (Auto Selected)

Auto Exposure Mode

Used for configuring basic exposure settings and day/night settings. The configurable settings depend on the selected Auto Exposure Mode:

- **Auto** (default): Sets the camera's shutter speed to automatically achieve a consistent video output level. This mode 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.
- **Auto Iris:** Specify minimum and maximum shutter speeds, and the camera automatically adjusts the iris size and other exposure settings.
- **Shutter Priority:** Specify a specific shutter speed for adjustment of aperture, ensuring a correct and proper exposure.
- **Manual:** Opens the iris completely with a fixed gain. This mode should only be used in indoor scenes with consistent lighting. Manual mode requires the user to set fixed values for shutter and gain levels. Increasing the value of the fixed shutter increases the amount of light entering the sensor, which allows a brighter and more detailed image. In a similar manner, utilizing gain and increasing

its level increases the sensitivity of the image sensor, which brightens the image and add details. This increases the level of 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.

Min Shutter Speed (available when Auto Exposure Mode is set to *Auto* or *Auto Iris*): Select a suitable shutter speed according to the environmental luminance.

Min 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

Max Shutter Speed (available when Auto Exposure Mode is set to *Auto* or *Auto Iris*): Select a suitable shutter speed according to the environmental luminance.

Max 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 (only available when Auto Exposure Mode is set to *Shutter Priority* or *Manual*):

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
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 when Auto Exposure Mode is set to *Manual*): In images where a bright light source is behind the subject of interest, without backlight compensation, the subject would appear in silhouette. The camera can adjust the exposure of the entire image to properly expose the subject in the foreground. Select one of the following options: *OFF* (default), *Upper*, *Lower*, *Central 1/3rd*, *Central 1/6th*, *Left*, or *Right*:

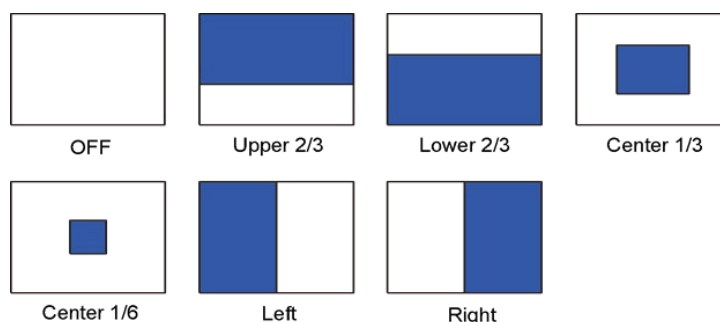


Figure 34: Backlight Compensation Settings

Gain (only available when Auto Exposure Mode is set to *Manual*): Increasing the gain lightens dark pictures resulting from low-level lighting. Move the slider or manually specify a value between 0-48, in dB. The default is 0.

Digital WDR: Improves the image quality and amount of details in high contrast scenes. Such scenes combine areas with different lighting conditions; some areas are very bright, and others are dark. Without Digital WDR, the image either would be overexposed or too bright in bright areas and completely dark in dark areas. Digital WDR helps improve image quality by producing a more detail in both the dark and bright areas of the image.

Select *High*, *Medium* (default), *Low*, or *OFF*. When High is selected, the image has the highest wide dynamic range, so that the IP camera can capture the greatest scale of brightness. Selecting OFF disables this function.

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

- *ATW* (Auto Tracing White Balance; default): Color is continuously adjusted according to the color temperature of the scene illumination.
- *Auto*: Color in a scene is automatically adjusted according to the ambient lighting between 2500°K to 10000°K.

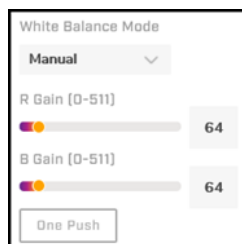


Figure 35: Manual White Balance Settings

- **Manual:** White balance is adjusted on-screen according to the type of lighting. When selected, you can configure the following gain values:
 - **R Gain:** Adjusts the red color in the image from 0 to 511. The higher the number, the redder the image. The default setting is 64.
 - **B Gain:** Adjusts the blue color in the image from 0 to 511. The higher the number, the bluer the image. The default setting is 64.

To quickly balance the color, click **One Push**.

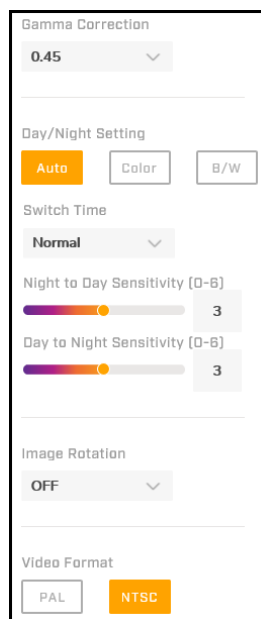


Figure 36: Additional Advanced Settings

Gamma Correction: Ensures faithful reproduction of an image. Select 0.45 (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, the image displayed on your screen has less contrast than the original image.

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:** Set the amount of time the switch takes (*Fast*, *Normal*, or *Slow*).
 - **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.
- **Color:** Locks camera in daytime mode.

- *B/W*: Locks camera in nighttime mode.

Image Rotation:

- *Flip*: Flips the image upside-down.
- *Mirror*: Displays the image from a different angle.
- *Both*: Displays the image upside-down from a different angle.
- *OFF* (default).

Video Format: Select the desired video format, *PAL* or *NTSC* (default). Then, click **Save**. The camera reboots.

Where relevant, changing the settings on the Visible page immediately affects the live visible video images and streams. To save changes, click **Save**. To discard changes and revert to the last saved settings, click **Reset**.

4.5 I/O Page

The I/O page enables you to configure the camera's alarm input and output pin states.

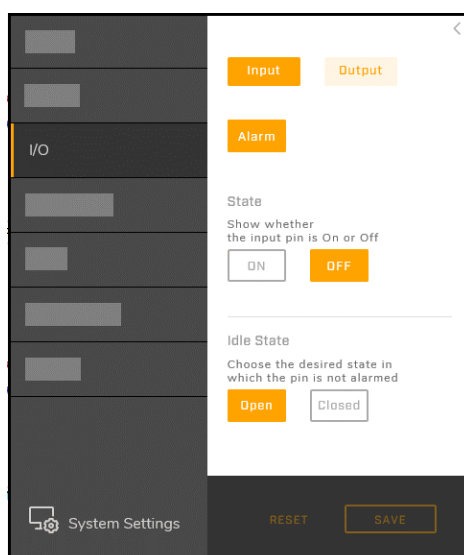


Figure 37: I/O Page - Alarm Input Pin Settings

To configure the alarm input pin state:

1. Click **Input**.
2. Click **Alarm**.
3. Select whether the display state of the alarm input pin is **On** or **Off**.
4. Select the state in which the alarm input pin is not alarmed: **Open** (default) or **Closed**.

To configure the alarm output pin state:

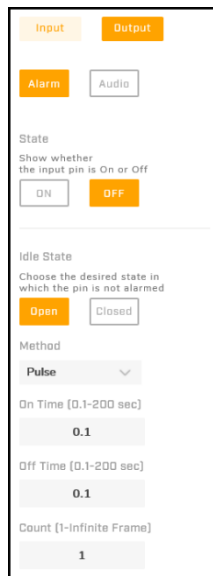


Figure 38: Alarm Output Pin - Pulse Settings

1. Click **Output**.
2. Click **Alarm**.
3. Select whether the display state of the alarm output pin is **On** or **Off**.
4. Select the state in which the alarm output pin is not alarmed: **Open** (default) or **Closed**.
5. Select the method of alarm output pin activation:
 - *Pulse*: Activates the alarm output pin for a configurable duration (*On Time*, between 0.1-200 seconds), interval (*Off Time*, between 0.1-200 seconds), and *Count* (between 1-Infinite Frame).
 - *Normal*: Activates the alarm output pin for a single configurable *Duration* (5, 10, 15, 30 seconds) or an *Infinite* duration.

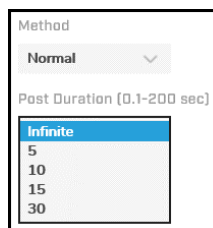


Figure 39: Alarm Output Pin - Normal Settings

If you made any changes on the I/O page, click **Save** to apply the changes. Click **Reset** to discard changes and revert to the last saved settings.

4.6 Illumination Page

The Illumination page enables you to activate and configure the camera's infrared (IR) LED illumination.

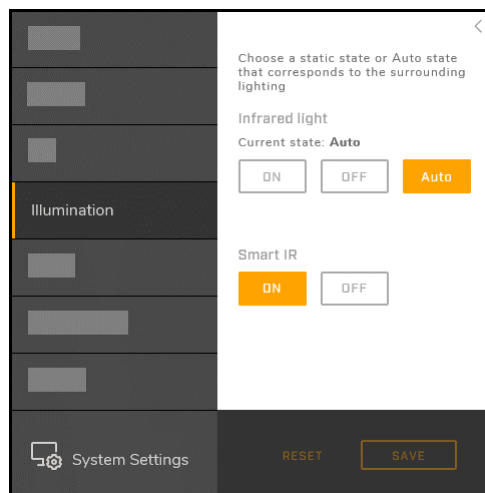


Figure 40: Illumination Page

Infrared light:

- *Auto* (default): The IR LEDs turn on or off according to surrounding lighting conditions. For example, in low-light conditions, the IR LEDs turn on.
- *On*: The IR LEDs are on.
- *Off*: The IR LEDs are off.

Smart IR:

- *On* (default): When the IR LEDs are on, the camera automatically adjusts the exposure level in zones of the image to compensate for overexposure or underexposure. For example, without Smart IR, an object in front of the camera might otherwise cause an overexposed image.
- *Off*: Disables Smart IR.

To save changes, click **Save**. To discard changes and revert to the last saved settings, click **Reset**.

4.7 OSD Page

On the OSD (On-Screen Display) page, you can:

- Enable the date, device name, or custom text to appear in two configurable locations on the Live View window and in the video streams.
- Configure the OSD background and text colors.
- Define different background and text colors for when the camera detects an event.

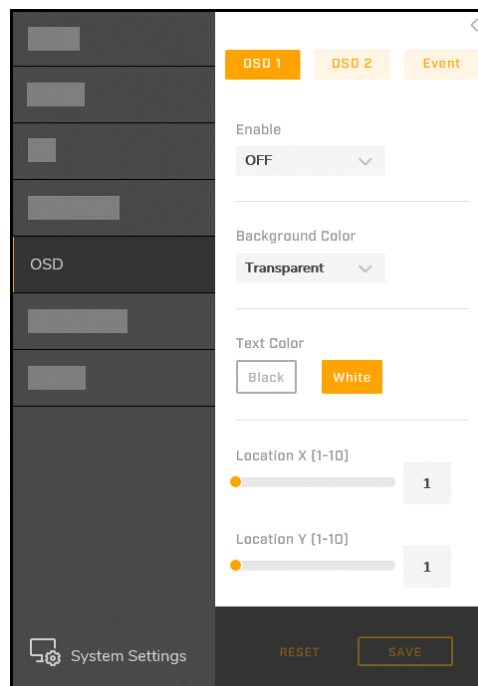


Figure 41: OSD Page - OSD1 Settings

Click **OSD1**, **OSD2**, or **Event**.

Enable (not available when configuring Event OSD settings):

- *Device Name*: The device name appears on-screen. Users assigned the role of admin or expert can configure the device name on the [Firmware & Info Page](#).
- *Date*: The date appears on-screen.
- *Text*: The time appears on-screen.
- *OFF* (default): Disables OSD.

Background Color: *Black* or *Transparent* (default).

Text Color: *Black* or *White* (default).

Location X: Determines the horizontal location of the OSD. Specify a value between 1 (far left; default) and 10 (far right).

Location Y: Determines the vertical location of the OSD. Specify a value between 1 (top; default) and 10 (bottom).

4.8 Privacy Zone Page

Privacy zones cover a configurable portion of the screen for privacy reasons. You can define up to eight privacy zones. After setting up a privacy zone, it appears in the Live View window and in the video streams as a solid area with a configurable color, size, and position.

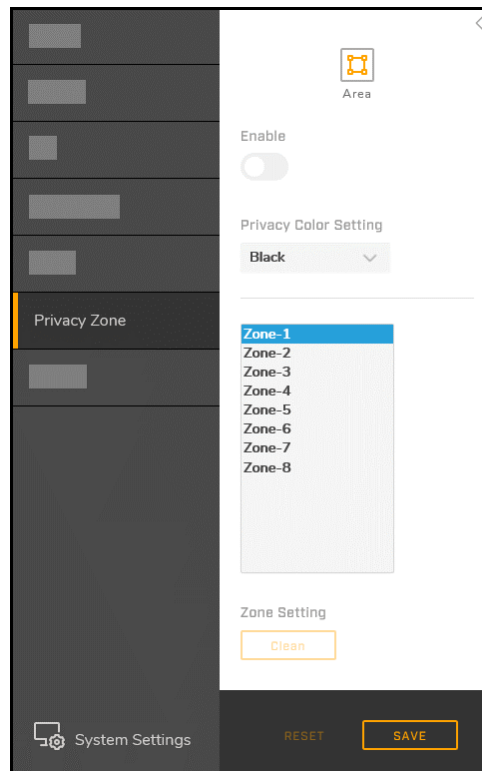


Figure 42: Privacy Zone Page

To set up a privacy zone:

1. Move the *Enable* slider to the right. By default, privacy zones are disabled.
2. Select one of the eight privacy zones: *Zone-1* through *Zone-8*.
3. From the *Privacy Color Setting* drop-down list, select *Black* (default), *Grey*, or *White*. The privacy color setting applies to all zones.
4. Using your mouse, click and drag in the Live View window to draw the privacy zone.
5. Click **Save**. The privacy zone appears in the Live View window.
6. For each privacy zone you want to set up, repeat the steps above.

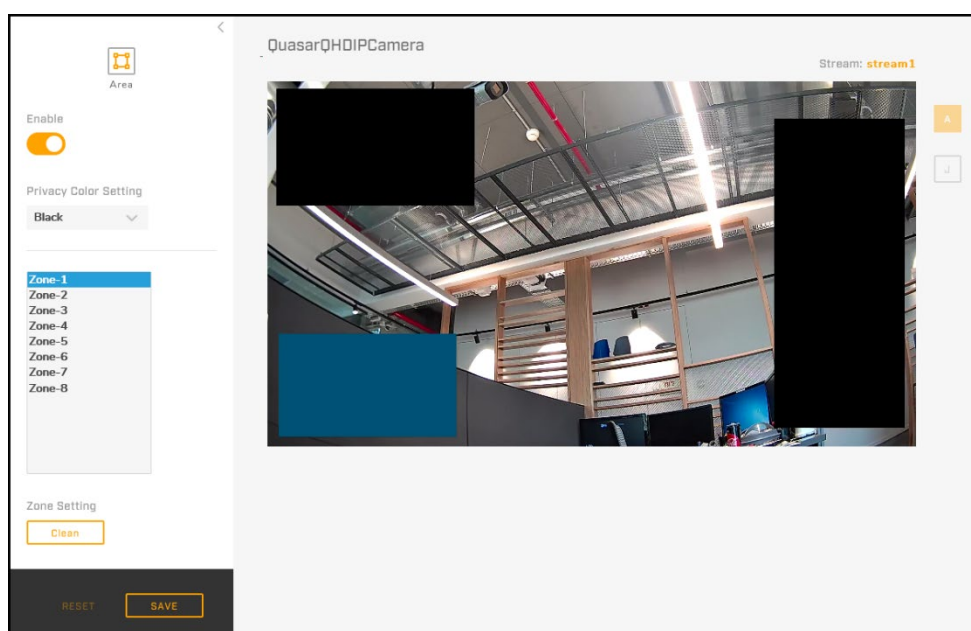


Figure 43: Three Privacy Zones Set Up - Zone-1 Selected

To delete a privacy zone:

1. Select the privacy zone.
2. Under *Zone Setting*, click **Clear**. The privacy zone is immediately deleted. You do *not* need to click **Save**.
3. For each privacy zone you want to delete, repeat the above steps.

4.9 Motion Page

On the Motion page, you can:

- Enable or disable motion detection.
- Define the motion detection zone (also known as the region of interest).
- Configure the motion detection sensitivity.

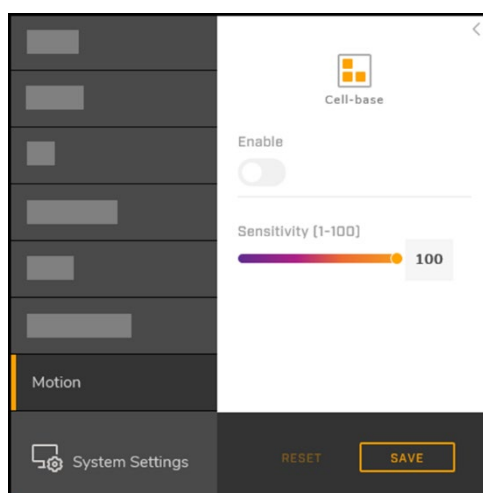


Figure 44: Motion Page

**Note**

If the camera is connected to a VMS that supports cell-based motion detection, FLIR recommends using the VMS to configure the motion detection zone.

To enable motion detection and define the detection zone:

1. Move the *Enable* slider to the right. By default, motion detection is disabled.
2. Specify the *Sensitivity* between 1-100, with 100 being the highest level of sensitivity and 1 being the lowest.
3. Using your mouse, define the detection zone. You can:
 - Click and drag on the Live View window 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 blue cells in the Live View window.

Click **Save**.

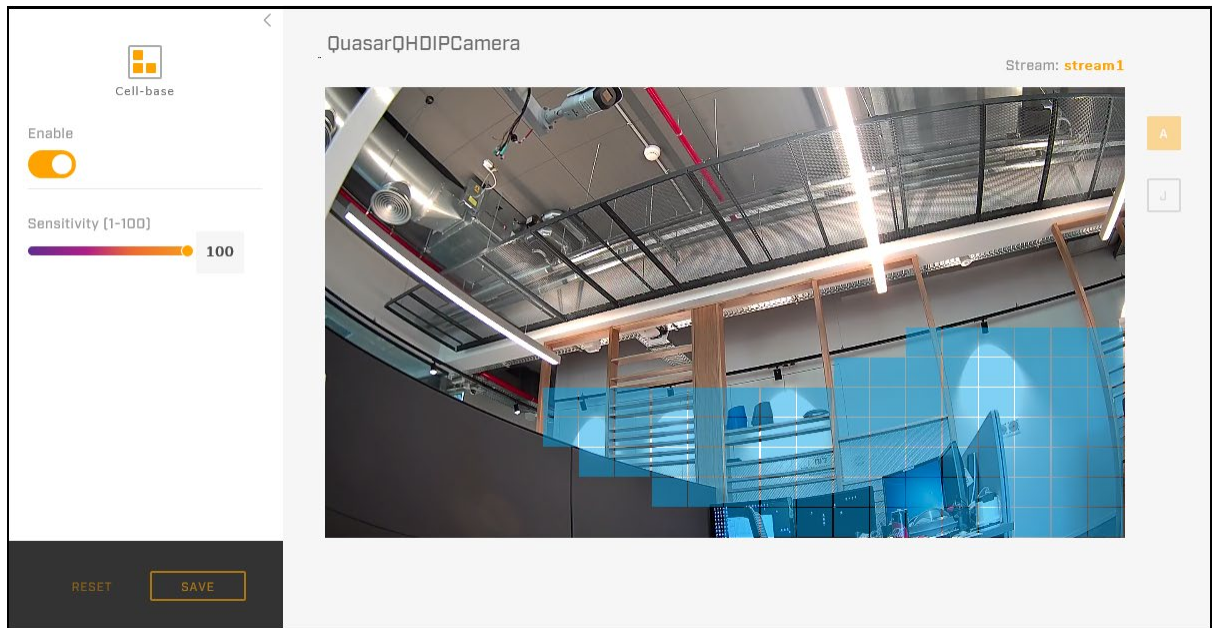


Figure 45: Motion Detection Enabled and Zone Defined

5 Configuration

Users assigned the admin or expert role can click **System Settings** on the [View Settings Home Page](#) to configure:

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

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

5.1 Network Page

On the Network page, you can configure the camera's networking settings.

Figure 46: System Settings Network Page - IP Mode Settings

Select the networking mode:

- **DHCP:** The camera is connected to a network with a DHCP server that assigns the camera its *IPv4 Address*, *IPv4 Subnet Mask*, and *IPv4 Default Gateway*.
- **Static:** Manually specify the camera's:
 - *IPv4 Address:* Identifies the camera on the network.

- *IPv4 Subnet Mask*: Determines whether destinations are on the same subnet. FLIR recommends using the default address: 255.255.255.0. If the subnet mask is not properly configured, the camera might not be able to communicate with other devices on the network.
- *IPv4 Default Gateway*: Used to forward frames to destinations in other subnets. An invalid gateway setting causes transmission to destinations in other subnets to fail.
- *Primary DNS*: Specify the primary domain name server (DNS) address.
- *Secondary DNS*: Specify the secondary DNS address.
- **PPPOE**: The camera connects to the network via a DSL modem using Point-to-Point Protocol over Ethernet (PPPOE). Manually specify the *User Name* and *Password* for the PPPOE account.

IPv6 Enable: If you are using IPv6, move the slider to the right to enable IPv6, and then configure:

- *Accept IPv6 Router Advertisement* – Move the slider to the right to accept IPv6 router advertisement. By default, *Accept IPv6 Router Advertisement* is disabled.
- *Enable DHCPv6*: If the camera is connected to a network with a DHCP server that supports IPv6 addressing, move the slider to the right. By default, DHCPv6 is disabled.

If IPv6 is enabled, but DHCPv6 is disabled, manually specify the camera's:

- *IPv6 Address*: Identifies the camera on the network. *Subnet Prefix Length*: Specify the subnet prefix length (1-128 digits).
- *IPv6 Default Router Address*: Specify the IPv6 default router address. *Subnet Prefix Length*: Specify the subnet prefix length (1-128 digits).
- *IPv6 DNS*: Specify the IPv6 DNS address.

Figure 47: QoS Settings

Enable QoS (Quality of Service): Determines resource control and traffic prioritization according to priority assigned to applications or users, assuring a certain level of data flow performance. If you are using QoS, move the slider to the right to enable it. You can then separately configure the following for *QoS Priority 1* and *2*:

- *IPv4 Address*: Specify an IPv4 address for each QoS priority level.
- *Netmask Bit*: Specify a value between 0-32 for each QoS priority level.

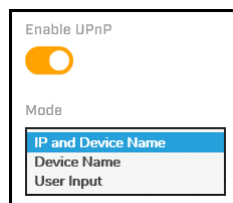


Figure 48: UPnP Settings

Enable UPnP (Universal Plug and Play): When enabled, any unit on the LAN can detect the camera and you can configure the *Mode*:

- *IP and Device Name* (default): When the camera connects to the LAN, other units on the LAN detect the camera by its IP address, model, and serial number (configurable on the [Firmware & Info Page](#)).
- *Device Name*: When the camera connects to the LAN, other units on the LAN detect the camera by its model and serial number.
- *User Input*: When selected, you can configure a *Friendly Name* for the camera. When the camera connects to the LAN, other units on the LAN detect the camera by its specified *Friendly Name*.

By default, UPnP is enabled. To disable it, move the slider to the left.

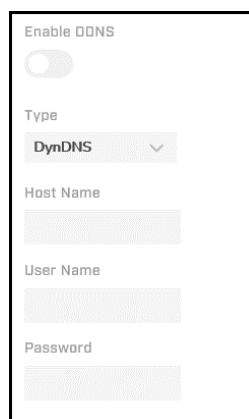


Figure 49: DDNS Settings - DynDNS Selected

Enable DDNS (Dynamic DNS): When enabled, DNS records are automatically updated. Before enabling, you must first register with a DDNS service provider. When enabled, you can configure the *Type* (provider):

- *DynDNS* (default): custom@dyndns.org
- *No-IP*: default@no-ip.com
- *Two-DNS*: default@two-dns.de
- *FreeDNS*: default@freedns.afraid.org

Specify the *Host Name*, *User Name*, and *Password* for the DDNS account.

If you are using FreeDNS, you need to specify a *Hash* value, which is an encrypted string representing your user name and password. To determine the *Hash* value, go to <http://freedns.afraid.org>.

By default, DDNS is disabled. To enable it, move the slider to the right.

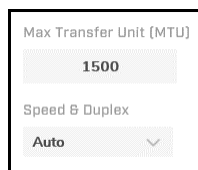


Figure 50: Additional Networking Settings

MTU (Maximum Transmission Unit): The greatest amount of data that can be transferred in one physical frame on the network. For Ethernet, the MTU is 1500 bytes (default). For PPPoE, the MTU is 1492. The range is from 1100 to 1500 bytes.

Speed & Duplex: You can select *Auto* (default), *1.0 Gbps Full Duplex*, *100 Mbps Full Duplex*, *100 Mbps Half Duplex*, *10 Mbps Full Duplex*, or *10 Mbps Half Duplex*.

5.2 RTSP Page

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 by unicast to one device or broadcasted by multicast to multiple devices. Unicast requires more network bandwidth and more server resources, but is more stable than multicast, which requires additional settings.

On the RTSP page, you can enable or disable RTSP authentication and specify the RTSP port. You can configure the additional video stream settings on the [Video Page](#).

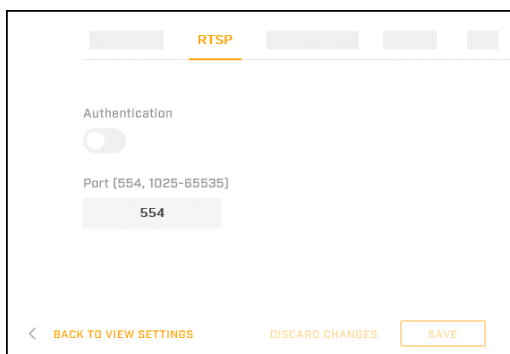


Figure 51: RTSP Page

Authentication: To encrypt the transmission, move the slider to the right. By default, RTSP authentication is disabled.

Port: Specify the RTSP network port. Valid values are 554 (default) and between 1025-65535.

5.3 Date & Time Page

On the Date & Time page, you can configure the camera's date and time settings.

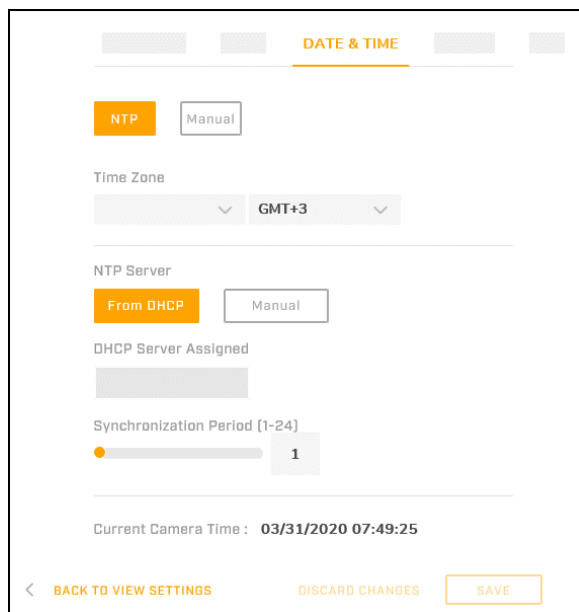


Figure 52: Date & Time Page - NTP Selected

Select the date and time mode:

- **NTP** (Network Time Protocol; default): The camera's date and time are synchronized with an NTP server.
- **Manual**: Manually specify the camera's date time.

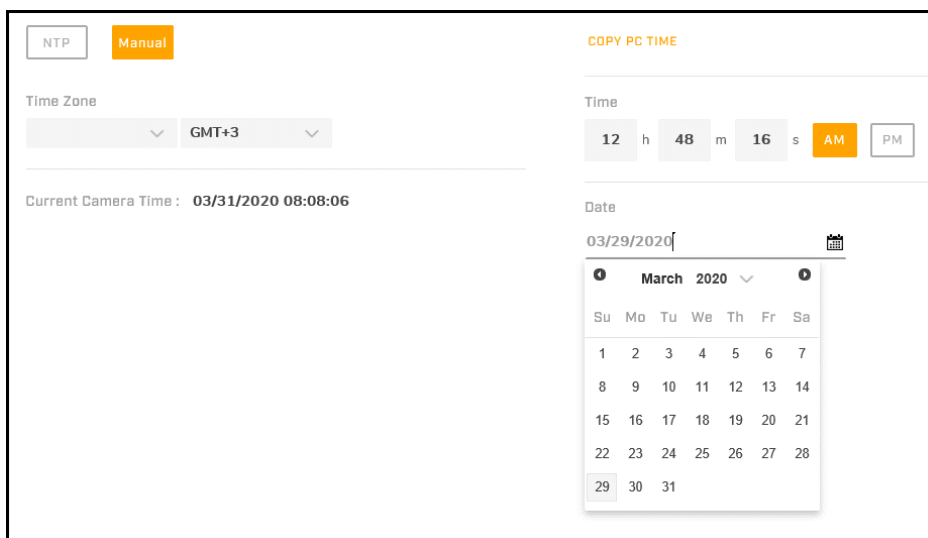


Figure 53: Date & Time Page - Manual Selected

You can copy the PC's current time or manually specify the camera's time and date.

Time Zone: Regardless of whether NTP or Manual is selected, specify the time zone in which the camera is located. If you leave the drop-down list on the left blank, you can define the time zone according to GMT offset. Otherwise, you can select a continent and city/time zone.

When NTP is selected, you can specify:

- **NTP Server:**
 - **From DHCP:** The DHCP server provides the NTP server's IP address, which appears in the *DHCP Server Assigned* field.

- **Manual** (default): The *Server Address* field appears. Specify the IP address of the NTP server (default: *time.nist.gov*).
- **Synchronization Period**: Specify the frequency the camera synchronizes with the NTP server, in number of hours between 1-24. For example, to synchronize the camera with the NTP server twice per day, specify 12.

To apply changes, click **Save**. The new time appears as the *Current Camera Time*.

5.4 Users Page

On the Users page, users assigned the role of Admin can manage camera users and passwords. You can create up to 10 users, in addition to the default administrator (*admin* user), which cannot be deleted.

Users assigned the role of Admin can also specify the authentication method on this page.

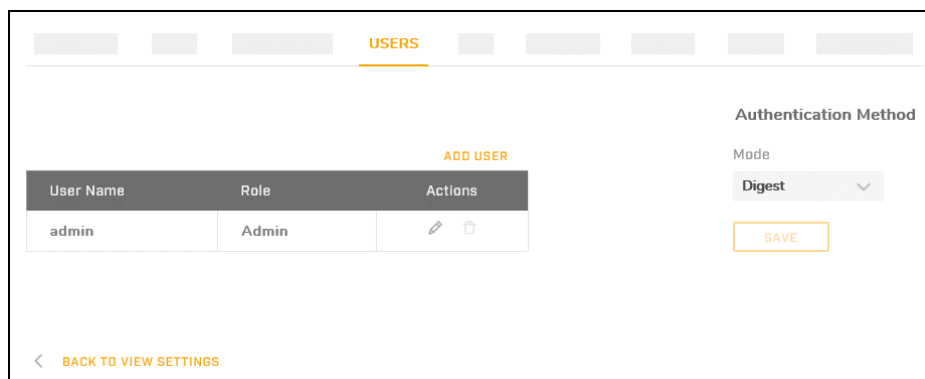


Figure 54: Users Page

You can assign one of the following roles to each user:

- **User**: Has access to the View Settings page but can only see the Live View window. Up to nine users can be assigned the User role.
- **Expert**: Does not have access to the Users page. Has access to all other View Settings and System Settings pages, menus, controls, and settings. More than one user can be assigned the Expert role.
- **Admin**: Has access to all pages. The default camera admin user is assigned the Admin role; the admin user name and role cannot be modified; and the admin user cannot be deleted. More than one user can be assigned the Admin role.

To add a new user:

1. Click **Add User**.

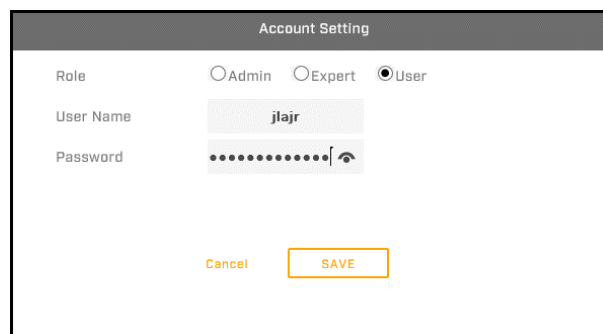


Figure 55: Add User Dialog Box

2. Select a *Role* for the user.
3. Specify a unique *User Name* and a *Password* for the user. The user name cannot be *admin*.



Notes:

- The password must consist of at least eight characters and include at least one uppercase letter, one lowercase letter, one number, and one special character.
- The user name and password are case-sensitive.

4. Click **Save**. The new user appears in the list of users.

Users assigned the role of Admin can also:

- Modify the credentials of an existing user
- Delete an existing user

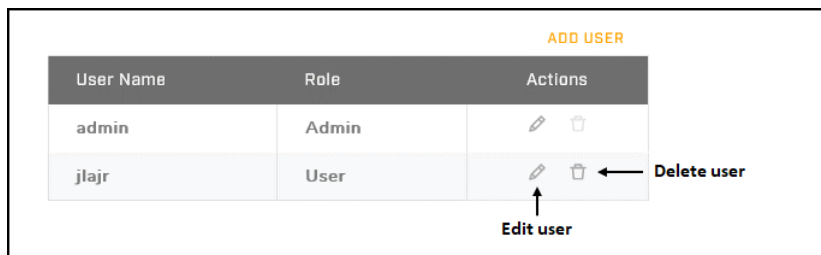


Figure 56: User Management

The default *admin* user cannot be deleted, and the *admin* user name cannot be modified.

Authentication Method

Mode: Select *Digest* (default) or *Basic*. To apply a change, click **Save**.

5.5 FTP Page

On the FTP screen, you can configure the settings of an FTP (File Transfer Protocol) server located remotely on the network. Based on the settings on the [Alarm Page](#), the camera saves snapshots to this FTP server.

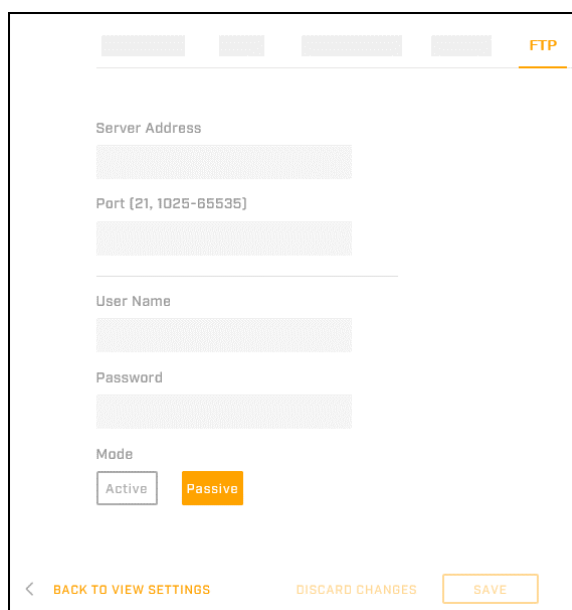


Figure 57: FTP Page

Server Address: Specify the FTP server’s IP address.

Port: Specify the FTP server’s port number as 21 (default) or between 1025-65535.

User Name: Specify the user name of the account the camera uses to access the FTP server.

Password: Specify the password of the account the camera uses to access the FTP server.

Mode:

- **Active:** The camera maintains a connection with the FTP server. This mode uses more network bandwidth but provides instant FTP responses.
- **Passive (default):** The camera only establishes a connection with the FTP server when necessary, which uses less network bandwidth. In addition, in passive mode, the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. In order to support passive mode on the server-side firewall, the following communication channels must be opened:
 - 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 a random port specified by server)
 - FTP server's ports > 1023 to remote ports > 1023 (server sends ACKs and data to client's data port)

To apply any changes to the settings, click **Save**.

5.6 SD Card Page

The camera can locally store video clips and snapshots on a microSDXC card, which is not supplied with the camera (minimum 4GB; maximum 512GB; formatted as a single partition). Before using a microSDXC card, it must be formatted. On the SD Card page, you can format and configure the microSDXC card.

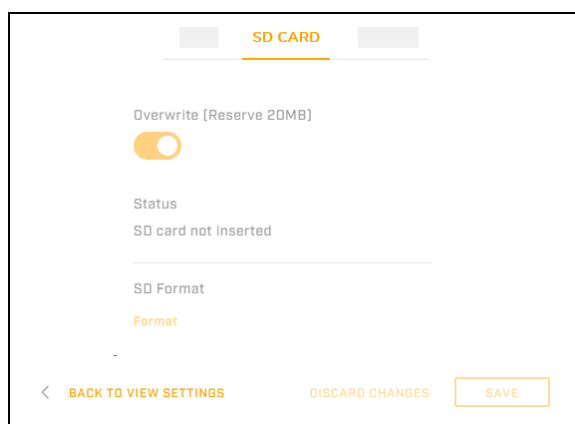


Figure 58: SD Card Page – SD Card Not Inserted

Overwrite (Reserve 20MB): When enabled and less than 20MB is available on the microSDXC card, the camera overwrites recorded files. The recording program erases the earliest file and stores the new one. By default, **Overwrite** is enabled. To disable it, move the slider to the left.

Status: Indicates whether a microSDXC card has been properly installed and mounted.

SD Format: To format a microSDXC card before using it, click **Format**.



Caution

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

Note
The card must be formatted as a single partition.

When an SD card is inserted and has stored snapshot or video clip files, you can:

- see the card's overall capacity, in MB
- how much free space is on it, in MB
- search for stored files by selecting a date
- download files

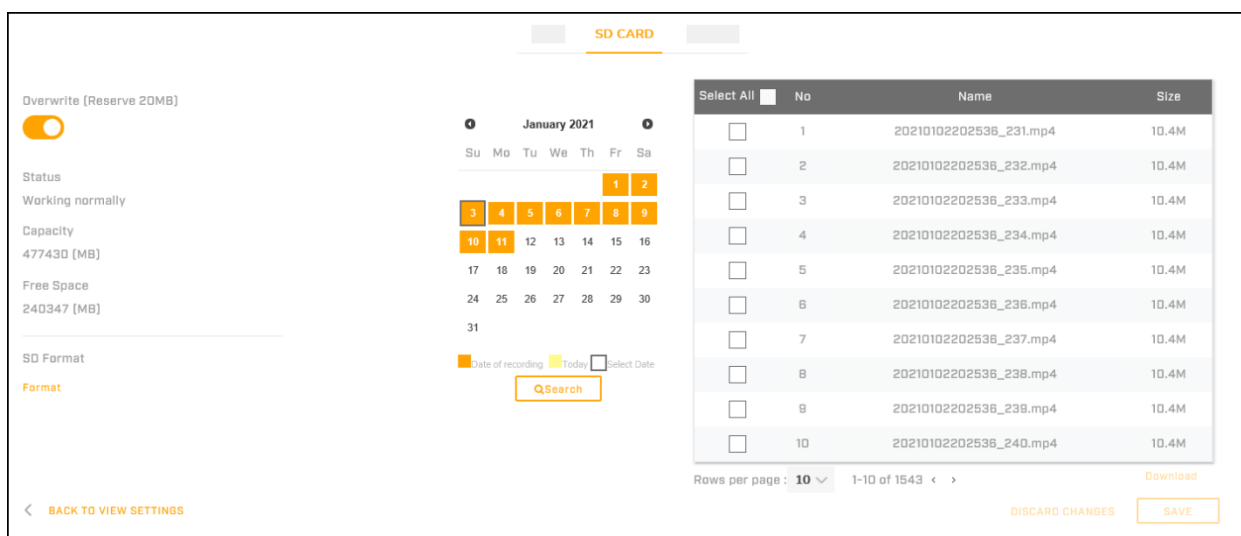


Figure 59: SD Card Page – SD Card Inserted and Files Available

5.7 Alarm Page

On the Alarm page, you can create and configure alarm rules, including triggers, arming schedules, and actions.

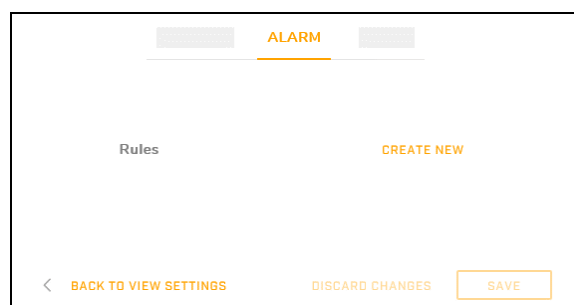


Figure 60: Alarm Page

By default, no alarm rules are defined and enabled.

To create an alarm rule:

1. Click **Create New**. The rule configuration Trigger screen appears.

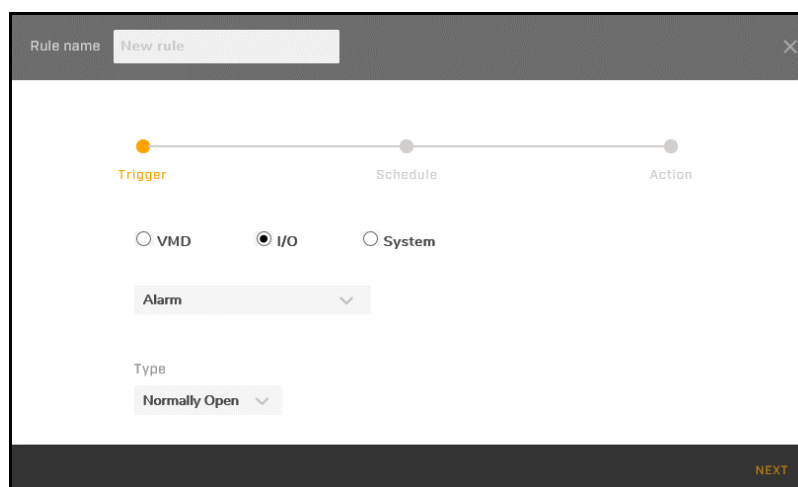


Figure 61: Rule Configuration Trigger Screen - I/O Trigger Selected

2. **Rule name:** Specify a unique and useful name for the rule.

3. Select the type of trigger event:

- **VMD:** Select whether *Motion* detection or *Tampering* triggers an alarm.

When *Motion* is selected, specify the motion *Sensitivity* (1-100). When *Tampering* is selected, specify the tampering *Sensitivity* (*High*, *Mid*, *Low*).



Note

If you are defining a *Motion* alarm rule, make sure a motion detection zone has been defined and enabled on the [Motion Page](#).

- **I/O:**
 - Select the type of input that triggers an alarm:
 - **Alarm:** Select the *Type*; that is, whether the input is Normally Open or Normally Closed.
 - **Audio:** Specify the *Sound Intensity Threshold* (0-100); lowering the value increases the camera's sensitivity to audio input, and vice versa.
- **System:** Select the type of system event that triggers an alarm:
 - *Network Loss*
 - *Network Conflict*
 - **Schedule:** The camera triggers an alarm or alarms according to a specified schedule. When selected, specify the alarm schedule *Mode*:
 - **Regular:** The camera triggers an alarm at regular intervals. When selected, specify the *Trigger Interval (Sec)*, the frequency at which the camera triggers an alarm, in seconds between 5-3600 (3600 = once per hour).
 - **Persist:** The camera triggers a persistent alarm.

4. Click **Next**. The rule configuration Schedule screen appears.

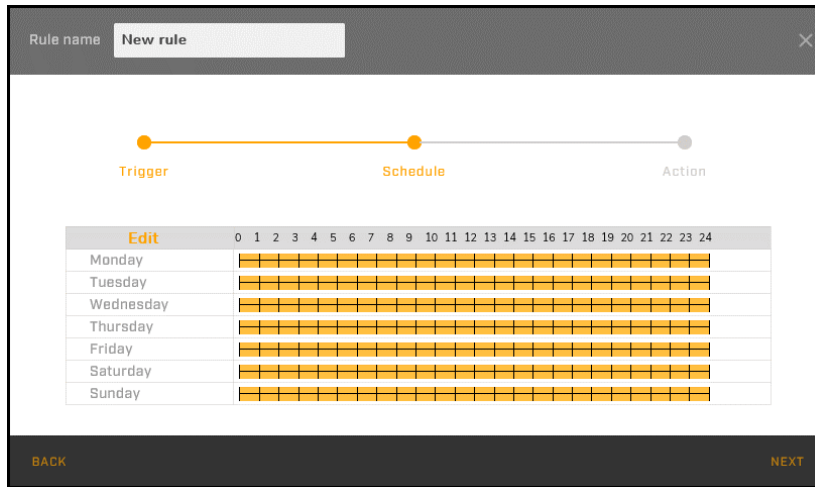


Figure 62: Rule Configuration - I/O Trigger Selected

- By default, the alarm is armed all day, every day of the week. In the schedule, orange indicates when the alarm is armed. To modify when the alarm is armed and whether the alarm triggers the action defined for the rule, click **Edit**. The arming schedule setting screen appears.

	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

Figure 63: Arming Schedule Setting Screen

For each day of the week, you can define up to three periods during which the alarm is armed.
Start Time: Specify the time the alarm arms.
End Time: Specify the time the alarm disarms.

Action: By default, the action defined for the alarm is enabled. To disable the action for a particular arming period, move the slider to the left.

The following example shows how to arm an alarm and enable the alarm action from 8 AM-6 PM Monday through Friday:

	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

Figure 64: Arm Alarm and Enable Action Monday through Friday 8 AM-6 PM

To apply changes, click **Apply**. The arming schedule setting screen closes, and the rule configuration Schedule screen appears with the modified arming schedule.

Rule name:

Trigger
Schedule
Action

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																										

BACK
NEXT

Figure 65: Modified Alarm Armed Schedule

6. Click **Next**. The rule configuration Action screen appears.

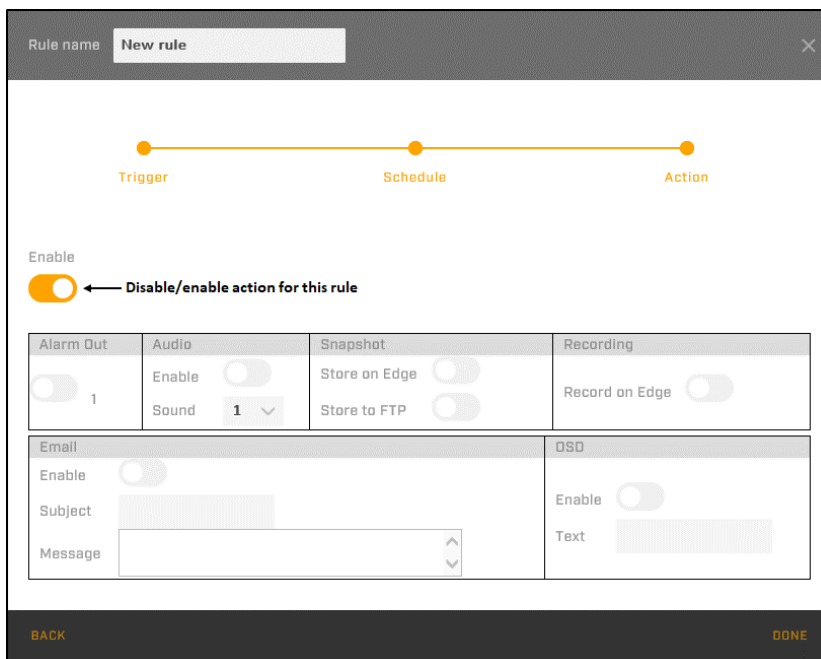


Figure 66: Rule Configuration Action Screen

7. By default, for a new rule, action for the rule is enabled. To disable action for the rule, move the slider to the left. This setting overrides any specific action setting.
8. By default, no specific actions are enabled. You can enable one or more of the following actions when the trigger event occurs by moving the relevant slider to the right:
 - *Alarm Out*: Changes the state of the camera’s alarm output. You can configure the camera’s alarm output on the [I/O Page](#).
 - *Audio*: The *Sound* (audio file) selected, between 1-10, is played through the camera’s audio output. You can upload audio files for the sounds on the [Sound Page](#).
 - *Snapshot*: Stores one or more photo snapshots. You can enable:
 - *Store on Edge*: Stores the snapshot(s) on the camera’s microSDXC card. If enabled, make sure a microSD card is properly installed and formatted. See [SD Card Page](#).
 - *Store to FTP*: Stores the snapshot(s) on the remote FTP server specified on the [FTP Page](#).
 - *Recording*: Records a video clip on the camera’s microSDXC card. You can configure the camera’s recording settings on the [Recording Page](#).
 - *Email*: Sends an email using the settings on the [Email Page](#). Specify a *Subject* and *Message* for the email.
 - *OSD*: Displays the *Text* specified in the camera’s video stream and in the Live View window.
9. Click **Done**. The new rule appears in the list of Rules.

You can also modify or delete existing rules.

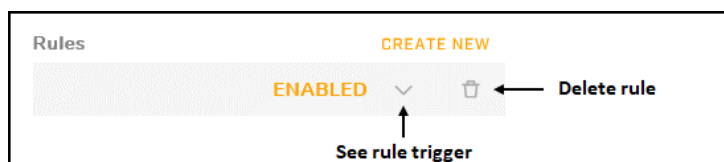



Figure 67: Rule List

To modify an existing rule:

1. In the list of rules, click the  icon next to the rule. The rule trigger appears.

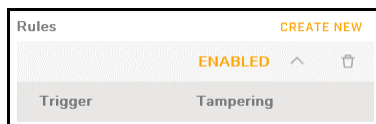


Figure 68: Rule List - Rule Trigger

2. Click the trigger. The rule configuration Trigger screen appears.
3. Modify the rule according to the procedure for [creating an alarm rule](#).
4. Click **Done**.

5.8 Audio Page

On the Audio page, you can configure the camera's audio input and output settings.

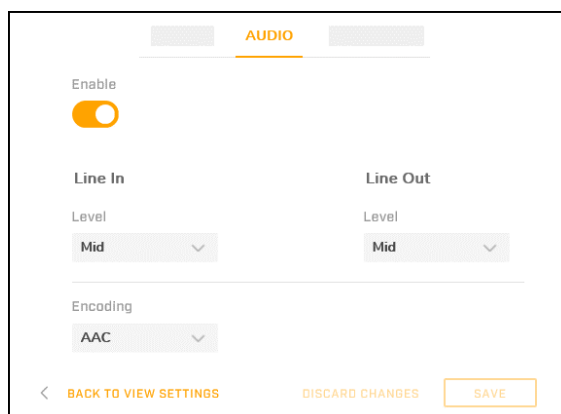


Figure 69: Audio Page

Audio is enabled by default. To disable it, move the slider to the left. The setting applies to audio input and output.

Line In

Level: Select *High*, *Mid* (default), or *Low*.

Encoding: Select *AAC* (default), *G.711 a-law*, or *G.711 μ -law*.

Line Out

Level: Select *High*, *Mid* (default), or *Low*.

To apply any changes to the settings, click **Save**.

5.9 I/O Devices Page

On the I/O Devices page, you can configure the number of input and output pins, and enable or disable individual pins.

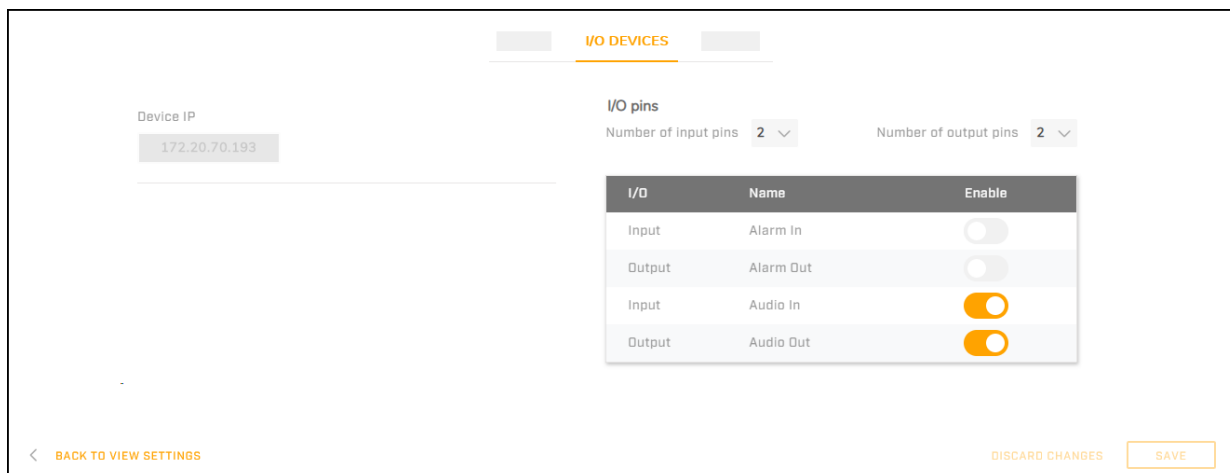


Figure 70: I/O Devices Page

Number of input/output pins: Select up to two input and up to two output pins, corresponding to the four available dry contacts: *Alarm In*, *Alarm Out*, *Audio In*, *Audio Out*. When you change the number of input or output pins, the I/O pin list immediately changes.

When enabling or disabling I/O pins, changes do not immediately take effect. To apply changes to these settings, click **Save**.

5.10 Sound Page

On the Sound page, you can upload up to 10 audio files that can be played through camera's audio output as alarm rule actions. You can define alarm rule actions on the [Alarm Page](#).

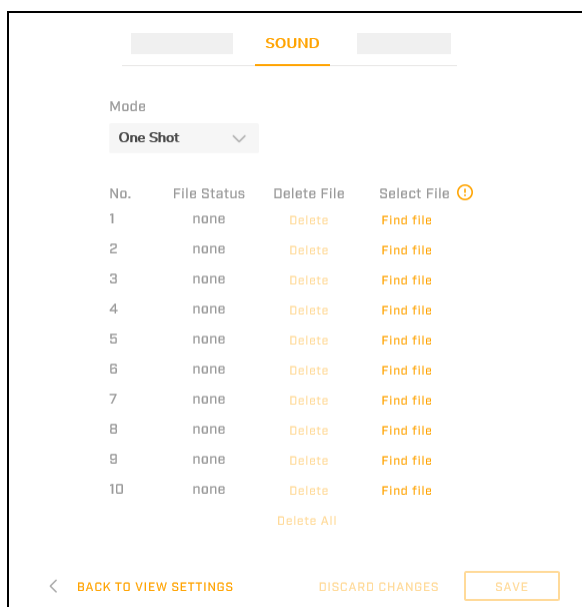


Figure 71: Sound Page

Mode:

- **One Shot:** The audio file is played once.
- **Infinite:** The audio file is played over and over.

To apply changes to this setting, click **Save**.

Find file: Browse for and upload a signed 16-bit PCM .WAV file with a sample rate of 8kHz.

Delete: Deletes an existing audio file.

Delete All: Deletes all uploaded audio files.

5.11 Snapshot Page

On the Snapshot page, you can configure the settings for photo snapshot alarm actions.

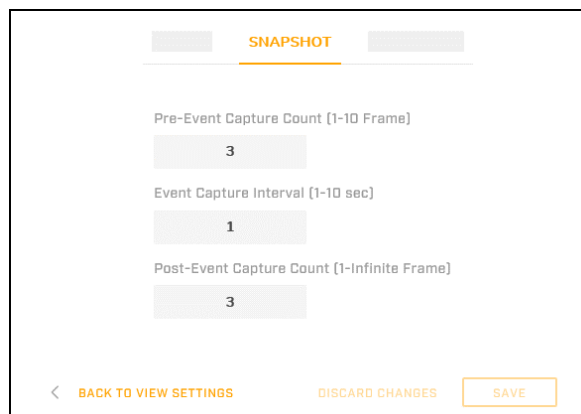


Figure 72: Snapshot Page

Pre-Event Capture Count: Specify the number of frames to capture prior to the event snapshot, between 1-10. The default is 3 frames.

Event Capture Interval: Specify the amount of time between snapshots, between 1-10 seconds. The default is 1 second.

Post-Event Capture Count: Specify the number of frames to capture after the event snapshot, at least 1. The default is 3 frames.

To apply changes to these settings, click **Save**.

5.12 Recording Page

On the Recording page, you can configure the settings for recording alarm actions.

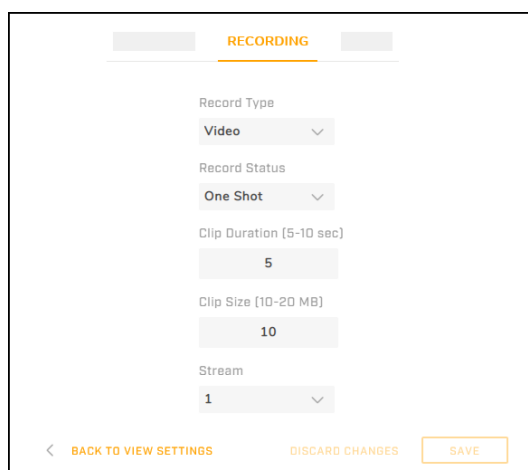


Figure 73: Recording Page - One Shot Record Status

Record Type: Select *Video* or *Audio and Video*.

Record Status:

- *One Shot* (default): The camera records a single video for the specified *Clip Duration*, between 5-10 seconds.
- *Continuous:* The camera continues to record, up to the specified *Clip Size*.

Clip Size: Specify the maximum file size for video clips, between 200-300 MB.

Stream: Select the video stream to record (1, 2, or 3).

To apply changes to these settings, click **Save**.

5.13 Email Page

On the Email page, you can configure the settings for email alarm actions.

The screenshot shows the 'EMAIL' configuration page. On the left side, there are several input fields: 'Authentication' (a dropdown menu set to 'No Auth'), 'Server Address', 'Port', 'User Name', 'Password', 'Sender Email Address', and an 'Attach Image' toggle switch. On the right side, there is an 'Email List' table with the following columns: 'Name', 'Email Address', 'Enable', and 'Actions'. The table is currently empty. At the bottom of the page, there are three buttons: 'BACK TO VIEW SETTINGS', 'DISCARD CHANGES', and 'SAVE'.

Figure 74: Email Page



Note

Before configuring email settings, check that:

- There is an SMTP mail 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: Select the authentication method the mail server requires for sending email:

- *No Auth* (default): The mail server does not require authentication.
- *SMTP Plain*: The mail server requires plain SMTP authentication.
- *Login*: The mail server requires login authentication.
- *TLS TTLS* (Transport Layer Security or Tunneled Transport Layer Security): The mail server requires TLS or TTLS authentication.

If you are not sure of the authentication the mail server requires for sending email or of any of the following mail server settings, check with the email system administrator.

- **Server Address:** Specify the mail server's IP address.

- *Port*: Specify the email server's port number.
- *User Name*: Specify the user name for the mail server account.
- *Password*: Specify the password from the mail server account.
- *Sender Email Address*: Specify the email address of the account sending the alarm notifications.
- *Attach Image*: To attach the event snapshot to alarm notifications, move the slider to the right. By default, images are not attached to alarm notifications.

Email List

You can specify up to 10 email addresses to receive alarm notifications.

To add a contact and enable alarm notifications:

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

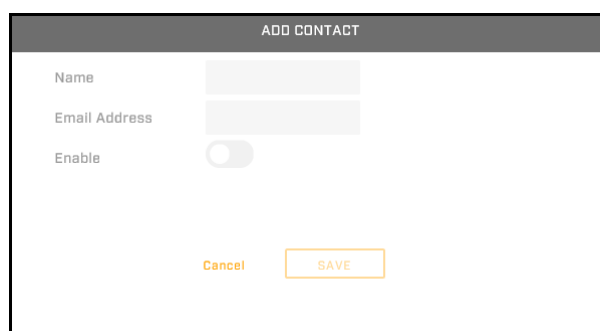


Figure 75: Add Contact Screen

2. Specify the contact's *Name* and *Email Address*.
3. Move the *Enable* slider to the right.
4. Click **Save**. The contact is added to the Email List.

You can also:

- Modify the name and address of an existing contact
- Delete an existing contact

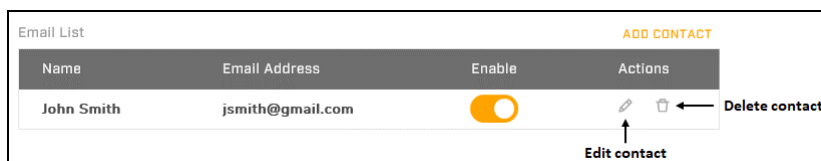


Figure 76: Contact Management

Changes to the Email List and to contacts in the list take effect immediately. To apply changes to other settings on the Email page, click **Save**.

5.14 Cyber Page

The Cyber page provides security configuration settings for:

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

- [IP Filtering](#)

5.14.1 Certificates

Before you can enable SSL/TLS/HTTPS, you need to have a valid certificate installed in the camera. You can generate a self-signed certificate, or you can upload a certificate issued by a Certificate Authority (CA).

Figure 77: Cyber Page - Certificate Settings

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*: Specify the two-letter combination 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*: Specify the state or province name.
 - *City Name*: Specify the city name.
 - *Common Name*: Specify the hostname or IP address of the camera (used to identify the camera).
 - *Organization Name*: Specify the name of the organization to which the Common Name belongs (for example, a company name).
 - *Organization Unit Name*: Specify the name of the unit within the organization (for example, department or division).
 - *Email Address*: Specify the email address of the person responsible for maintaining the certificate.



3. Click **Generate Certificate**. Wait for the camera to generate the certificate, at which point the Certificate Information appears on the screen.

Figure 78: Certificate Generated

4. If you are requesting and downloading a certificate, click **Download Certificate**.
5. Click **Save** to apply the changes.

To upload a certificate:

Figure 79: Upload Certificate

1. 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. Click **Save** to apply the changes.

5.14.2 SNMP

SNMP (Simple Network Management Protocol) enables the network management system (NMS) to remotely monitor and manage the camera. You can enable the following SNMP versions and configure their settings: SNMP v1, SNMP v2c, and SNMP v3.

If you are not sure how to configure the SNMP settings, contact your network or system administrator.

To apply changes to SNMP settings, click **Save**.

The screenshot displays the SNMP configuration page. On the left is a dark 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. Below these are fields for 'Read Community String', 'Write Community String', and 'Trap Community String'. To the right, the 'Trap' section includes a 'Mode' dropdown set to 'OFF', a 'Target IP' field, a 'Heartbeat' toggle, and a 'Heartbeat Interval [5-600]' field set to '30'. There is also an 'Event' toggle and a 'Download MIB' button labeled 'DOWNLOAD'. At the bottom, there are three buttons: 'BACK TO VIEW SETTINGS', 'DISCARD CHANGES', and 'SAVE'.

Figure 80: SNMP Settings

SNMP v1

To enable SNMP v1, move the slider to the right. By default, SNMP v1 is disabled.

SNMP v2c

To enable SNMP v2c, move the slider to the right. By default, SNMP v1 is disabled.

Read Community String: Specify the community name that has read-only access to all supported SNMP objects. The default value is *public*.

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

Trap Community String: Specify the community to use when sending a trap message to the management system. The default value is *public*. Traps are used by the camera to send messages to the management system for important events or status changes.

SNMP v3

To enable SNMP v3, move the slider to the right. By default, SNMP v1 is disabled.

User Name: Specify the user name. The default is *initial*.

Authentication Mode: Select *MD5*, *SHA*, or *NONE* (default).

Authentication Password (available when Authentication Mode is set to *MD5* or *SHA*): Specify the password for authentication.

Privacy Mode (available when Authentication Mode is set to *MD5* or *SHA*): Select *AES*, *DES*, or *NONE* (default).

Privacy Password (available when Privacy Mode is set to *AES* or *DES*): Specify the privacy password.

Trap

Mode: Select *V1*, *V2C*, *V3*, or *OFF* (default), according to the SNMP version that you enabled.

Target IP: Specify the IP address of the Trap Host.

Heartbeat: Sends SNMP notifications at regular intervals to detect network delays. To enable it, move the slider to the right. By default, *Heartbeat* is disabled.

Heartbeat Interval (5-600): Specify the interval in seconds for the camera to send heartbeat notifications. The default is 30 seconds.

Event: Automatically records the log file of events, for later review. To enable it, move the slider to the right. By default, *Event* is disabled.

Download MIB

You can download the camera's MIB (Management Information Base), 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.

Click **Download**. The database is downloaded.

5.14.3 802.1X

802.1X settings enable the camera to access a network protected by the 802.1X/EAPOL (Extensible Authentication Protocol over LAN) authentication protocol.

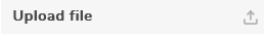
Figure 81: 802.1X Settings

802.1X is disabled by default. Before enabling 802.1X on the camera, you must register a user name and password for the 802.1X server and configure the authentication server. Contact the network administrator to obtain certificates, user IDs, and passwords.

To enable it, move the *Enable* slider to the left.

Protocol

Click **TTLS** (default) or **PEAP**.

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

Inner Authentication (available when the Protocol selected is *TTLS*): Select *CHAP* (default), *EAP-MSCHAPV2*, *MD5*, *MSCHAP*, *MSCHAPV2*, or *PAP*.

User Name and Password: Specify the user name and password.

Anonymous ID (available when the Protocol selected is *TTLS*): Specify the Anonymous ID.

5.14.4 TLS/HTTPS

You can enable the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol, which protects camera settings and user name/password information. The HTTPS protocol uses SSL/TLS for secure IP connections between the camera and a web browser over HTTP.

To use HTTPS on the camera, an HTTPS certificate must be installed. The HTTPS certificate can be obtained either by creating and sending a certificate request to a CA or by creating a self-signed HTTPS certificate. For more information, see [Certificates](#).

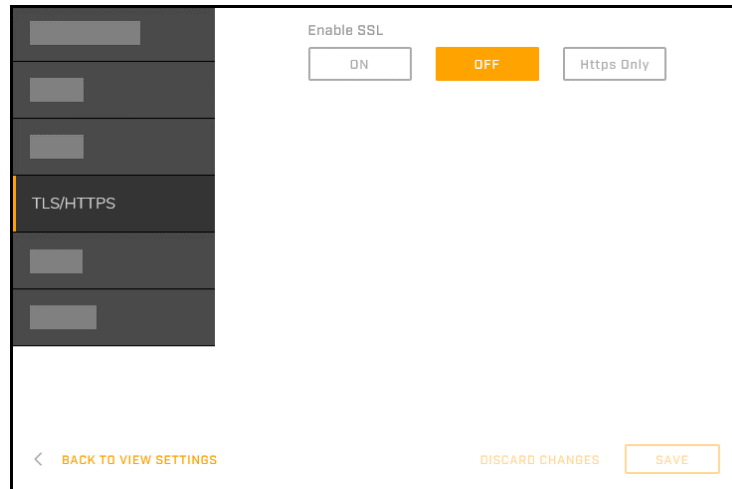


Figure 82: TLS/HTTPS Settings

Enable SSL

The following settings are available:

Setting	TLS Enabled	Access to the Camera	
		HTTPS	HTTP
<i>On</i>	Yes	Yes	Yes (can be disabled)
<i>Off</i> (default)	No	No	Yes
<i>HTTPS Only</i>	Yes	Yes	No

When this setting is *On* or *HTTPS Only*, you can define the HTTPS port as 443 (default) or between 1025-65535.

This setting affects whether the TLS and Web ports can be disabled or enabled (see [Ports](#)).

5.14.5 Ports

For enhanced security, you can enable (*On*) and disable (*Off*) default ports, and email and FTP services.

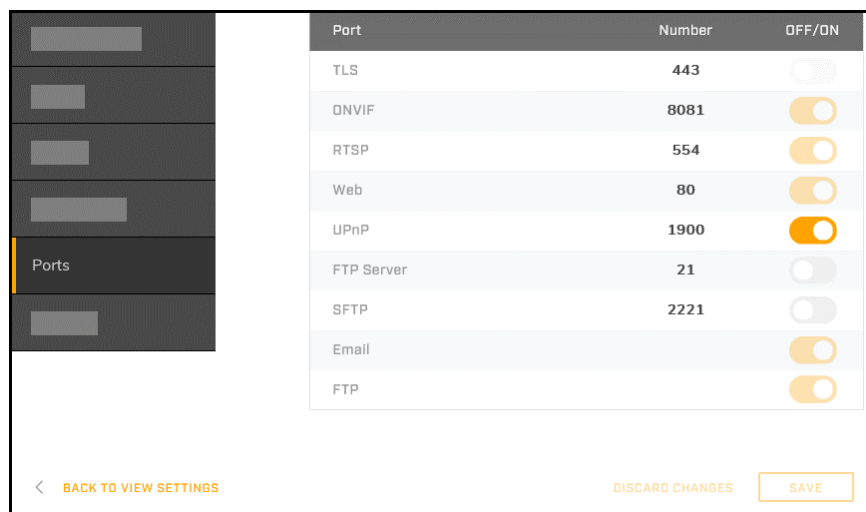


Figure 83: Port Settings

The Enable SSL setting on the [TLS/HTTPS](#) screen affects whether the TLS port (443) and the Web port (80) are enabled or disabled:

Enable SSL Setting	TLS	HTTP
On	On	On or Off
Off (default)	Off	On
HTTPS Only	On	Off

Also, to ensure communication with the camera, the ONVIF and RTSP ports cannot be disabled.

5.14.6 IP Filter

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

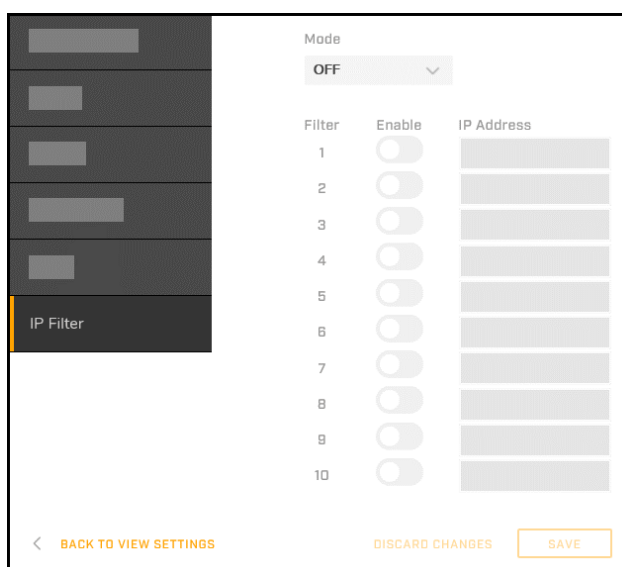


Figure 84: IP Filter Settings

To allow access for one or more specific IP addresses:

1. For *Mode*, select *Allow*.
2. Move the *Enable* slider to the right for each IP address for which you are allowing access.
3. Specify the *IP Address*.
4. Click **Save**.

To deny access for one or more specific IP addresses:

1. For *Mode*, select *Deny*.
2. Move the *Enable* slider to the right for each IP address for which you are denying access.
3. Specify the *IP Address*.
4. Click **Save**.

The default IP filter *Mode* is OFF.

5.15 Firmware & Info Page

On the Firmware & Info page, you can:

- Specify a unique name for the camera.

- See the camera's current firmware version, serial number, MAC address, model, and up time.
- Upgrade the camera's firmware.
- Reset the camera to its factory defaults.
- Reboot the camera.
- Import camera settings.
- Export the camera's current settings.
- Download system information FLIR Support can use for troubleshooting.

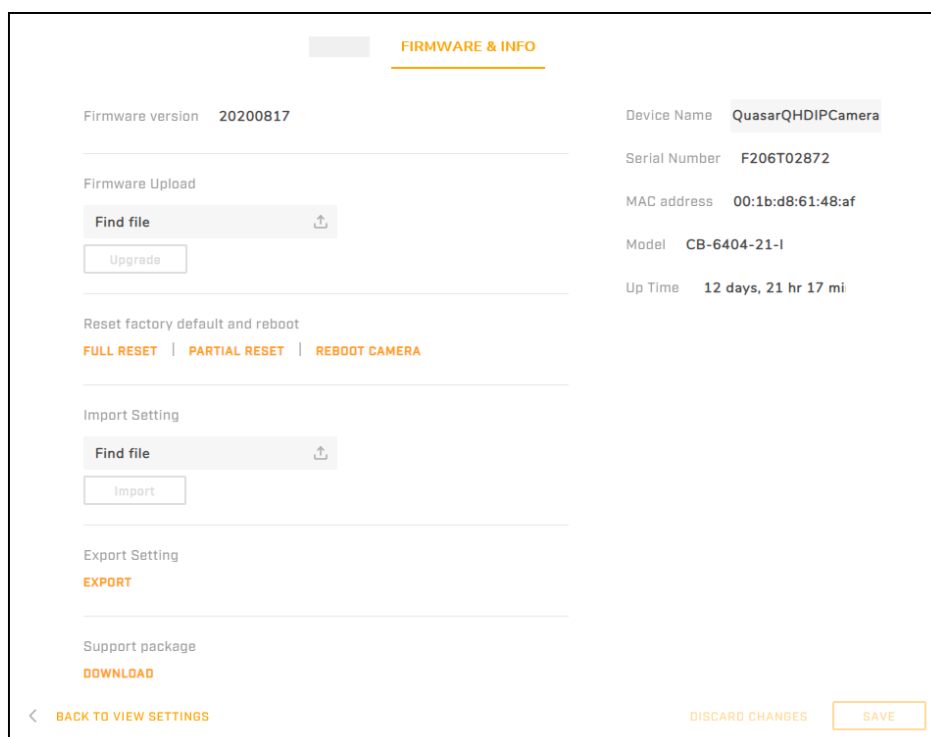



Figure 85: Firmware & Info Page

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

To upgrade the camera's firmware

1. Under *Firmware Upload*, click **Find file**.
2. On your computer or network, browse to and select the firmware file.

The file name appears (for example, **Quasar4UHDB_20210128.bin**).

 **Note**

The folder includes a checksum file, which can be used to check file validity using the checksum validation software of your choice.



Caution

Only upgrade to firmware developed for the specific Quasar CB-640x camera you are upgrading.

3. Click **Upgrade**.

The camera uploads and installs the firmware, which takes about three minutes. After installing firmware, the camera reboots.

Reset factory default and reboot

Click **Full Reset** to return the camera its original factory configuration, including the camera's original networking settings.



Caution

Clicking **Full Reset** causes the camera to lose all network settings.

Attention

En cliquant sur Réinitialisation complète, la caméra perd tous les paramètres réseau.

Click **Partial Reset** to return the camera to its factory configuration, except for the camera's network settings (IP address, subnet mask, and default gateway), video format, and image rotation settings.

Click **Reboot** to restart the camera without affecting the configured settings.

To import settings using a previously exported settings file:

1. Under **Import Setting**, click **Find file**.
2. On your computer or network, browse to and select the settings file.
3. Click **Import** to upload the file.

To export the camera's current settings:

1. Under **Export Setting**, click **Export**.
In Internet Explorer, an information bar appears.
2. In Internet Explorer, click **Save**. For other browsers, save the file.

Support package: To download camera log files for FLIR Support personnel, click **Download**.

Appendices

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

A.1. Technical Specifications

Up-to-date technical specifications for the camera, in addition to other resources such as the Discovery Network Assistant (DNA) software tool and this installation and user guide, are available from [the FLIR Quasar™ Premium Bullet pages on FLIR.com](#). For more information, see [Accessing Product Information from the FLIR Website](#).

A.2. Network Settings

The following are the network protocols and ports used by the camera:

Protocol	Port	Usage
FTP	21	Uploading files to the FTP server
HTTP ONVIF	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

A.3. Troubleshooting

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

Problem	Possible Solution
No network connection	<p>Hardware issues:</p> <p>Check that the network is working and the unit is powered on.</p> <p>Check that the network (Ethernet) cable is properly attached to the unit.</p> <p>Confirm that the network cables are not damaged and replace if necessary.</p> <p>IP Address issues:</p> <p>Change the default IP address/addresses of the unit.</p> <p>From the PC running the web browser, ping the unit IP address and confirm that it can be reached.</p> <p>Confirm that the network settings/firewalls are set according to the requirements.</p> <p>The camera might be located on a different subnet. Contact your IT administrator to get the IP address of the camera.</p>
How do I find IP address of my unit?	<p>Check the network DHCP server IP address assignments and lease.</p> <p>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.</p>
The IP address responds to a ping on the network from the workstation but does not show in the Discovery List	<p>Disconnect the unit's Ethernet port or turn off power to unit, 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.</p> <p>Check the network port and ensure that it is working OK.</p> <p>Ensure that the switch ports provide the necessary power.</p>
The unit IP address is in use by another computer (collision)	<p>Check the DHCP settings. Obtain a new IP address using DHCP. Ensure this is a unique IP address.</p> <p>Alternatively, change the unit IP address after connecting to it directly (not through the system network).</p>
Cannot log in to the camera	<p>Check the admin login user name.</p> <p>Check the admin login password.</p>
No video image displayed on the main menu or the view menu of the web interface	<p>Reset the browser security settings to the default value.</p> <p>Check that the correct port was configured. The default port is 554.</p>
Poor output video quality	<p>Check that the network cable is connected securely.</p> <p>Check that the camera settings are correct on the camera and in the unit.</p> <p>Check that the camera lens is clean and unobstructed.</p> <p>Check that the cable length is within specification.</p>

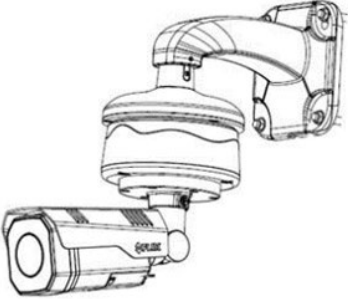

Problem	Possible Solution
Streaming video image is hanging (stopped)	<p>Confirm the unit's video streaming settings.</p> <p>Refresh your browser screen (F5).</p> <p>Check that the bandwidth and bit rate settings of the network are set properly.</p> <p>Check that other processes and applications are not causing undue latency.</p> <p>Check that the firewall analysis or blocking is not interfering with the video stream and supports the required ports and communication protocols.</p>
Bluish picture in an indoor scene (possibly mixing indoor and outdoor lighting)	<p>Change the <i>White Balance Mode</i> to <i>Auto</i>. If the lighting in the scene is fixed, manually adjust the White balance to an acceptable image.</p>
Reddish picture and incorrect colors in the image	<p>Check the PoE power supply and associated network cables. Connect directly to the PoE and compare the images. If the problem persists, contact support.</p>

A.4. Acronyms and Abbreviations

Abbreviation	Description
802.1X	Network Access Control Port-based authentication standard
AES	Advanced Encryption Standard
DES	Data Encryption Standard
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol
FTP	File Transfer Protocol
H.264	Video Compression Standard
H.265	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
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

A.5. Mounting Accessories

The following mounting accessories are available from FLIR for installing your CB-640x camera.

Image	Name	Description
	<p>CM-CAPX-W32</p>	<p>Wall mount kit</p>
	<p>CX-POLE-G32</p>	<p>Pole mount adapter for CM-CAPX-W32 wall mount kit</p>

For more information, contact your FLIR sales representative or visit www.FLIR.com/security to request details on where to get the accessory.

A.6. Detaching the Camera from the Adapter Plate

For outdoor installations, FLIR recommends mounting this camera with its wall box attached, to keep the camera and its cables waterproof. Without the wall box attached, the camera and cables are not waterproof.

However, for indoor installations and depending on mounting circumstances, you might need to detach the camera and mounting bracket from the attached adapter plate.

Using a Philips head screwdriver, loosen and remove the six M4 screws.

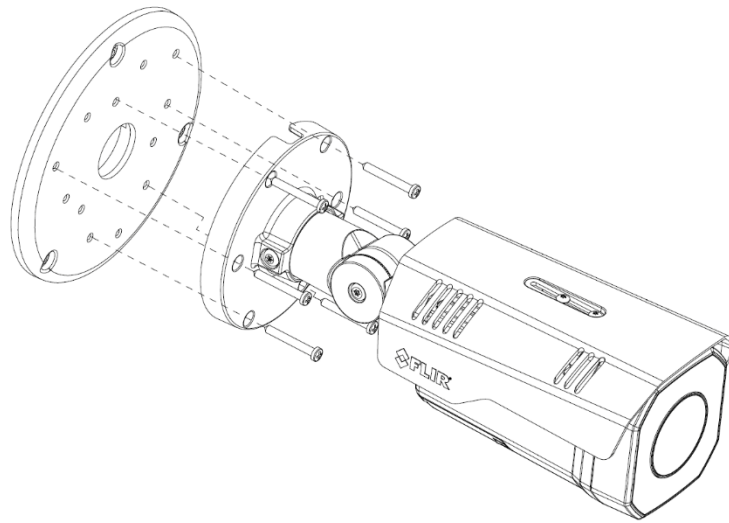


Figure 86: Detaching the Camera from the Adapter Plate



FLIR Systems, Inc.

6769 Hollister Ave.
Goleta, CA 93117
USA
PH: +1 805.964.9797
PH: +1 877.773.3547 (Sales)
PH: +1 888.747.3547 (Support)
FX: +1 805.685.2711
www.flir.com/security

Corporate Headquarters

FLIR Systems, Inc.
27700 SW Parkway Ave.
Wilsonville, OR 97070
USA
PH: +1 503.498.3547
FX: +1 503.498.3153

Document:
CB-640x Installation and User Guide
Revision: 100
Date: February 2021
Language: en-US