FLIR

Quasar Gen III

User and Installation Guide

CF-6308 Box IP Camera



Ver. 8

March 10, 2019

© 2019 FLIR Systems, Inc. All rights reserved worldwide. No parts of this manual, in whole or in part, may be copied, photocopied, translated, or transmitted to any electronic medium or machine readable form 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.
This product is protected by patents, design patents, patents pending, or design patents pending.
The contents of this document are subject to change.

FLIR Systems, Inc.
6769 Hollister Avenue
Goleta, California 93117
USA
Phone: 888.747.FLIR (888.747.3547)
International: +1.805.964.9797

For technical assistance, please call us at +1-800-254-0632 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.

Proper Disposal of Electrical and Electronic Equipment (EEE)



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

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

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

Document History

Version	Date	Comment
Ver. 1	July 2017	Initial FLIR Release
Ver 6	Dec 2018	Firmware Update (Analytics) Min/Max SD Card Size
Ver 7	Jan 2019	Camera License for Basic Video Analytics Add Digital Zoom
Ver 7a	Feb 2019	Access Technical Specs from FLIR Website
Ver 8	Mar 2019	Note on Resetting to Factory Defaults - Basic Video Licenses must be re-loaded Consolidate info on BVA License

Table of Contents

1. Document Scope and Purpose 1
2. Introduction 5
2.1 Features 5
2.2 Package Contents 6
2.3 Hardware Description 6
2.4 System Requirements 8
3. Installation 9
3.1 Pre-Installation Checklist 9
3.2 Attaching and Adjusting the Lens 9
3.3 Powering the Camera 10
3.4 Resetting the Camera 11
4. Preparing to Configure the Camera 12
4.1 Connecting the Camera to the Network 12
4.2 Using DNA to Access the Camera 12
4.3 Configuring the Unit's Initial IP Address 13
4.4 Configuring Communication Settings 16
5. Configuration and Operation 22
5.1 CF-6308 Web Interface 22
5.2 Live View 25
5.2.1 Recording 26
5.2.2 Capturing a Picture 26
5.2.3 Viewing Live Video from a Media Player 27
5.2.4 Basic Video Analytics 28
5.3 Settings 30
5.3.1 System Tab 30
5.3.1.1 Lens Control 31
5.3.1.2 Basic Configuration 32
5.3.1.2.1 Date & Time 32
5.3.1.2.2 Audio 33
5.3.1.2.3 Firmware 33
5.3.1.2.4 Basic Operations 34
5.3.1.2.5 OSD 36
5.3.1.3 User Accounts 38
5.3.1.4 Network 40
5.3.1.4.1 General 40

Table of Contents

5.3.1.4.2 FTP Server 42
5.3.1.4.3 RTSP 43
5.3.1.4.4 SNMP 45
5.3.1.4.5 802.1X 46
5.3.1.4.6 IP Filter 48
5.3.1.4.7 DDNS 48
5.3.1.4.8 LDAP 49
5.3.1.4.9 SSL 50
5.3.1.5 Events Source 52
5.3.1.5.1 Alarm 52
5.3.1.5.2 Audio 55
5.3.1.5.3 Motion 56
5.3.1.5.4 Network 58
5.3.1.5.5 Schedule 59
5.3.1.5.6 Tampering 60
5.3.1.5.7 Day/Night 61
5.3.1.6 Events Handler 63
5.3.1.6.1 Email 63
5.3.1.6.2 Alarm Out 64
5.3.1.6.3 FTP 65
5.3.1.6.4 Recording Settings 66
5.3.1.6.5 SD Card 67
5.3.1.6.6 Snapshot 67
5.3.1.6.7 Sound 67
5.3.1.6.8 Basic Video Analytics 68
5.3.1.6.8.1 Initial Settings 69
5.3.1.6.8.2 Basic Video Analytics Camera License 71
5.3.1.6.8.3 Providing cameras with Basic Video Analytics Licenses 71
5.3.1.6.8.4 Camera Distribution 72
5.3.1.6.8.5 Camera Positioning 72
5.3.1.6.8.6 Detection Ranges 73
5.3.1.6.8.7 Mounting and Lighting 74
5.3.1.6.8.8 Rule-based Settings 74
5.3.1.6.8.1 Counting 75
5.3.1.6.8.2 Border Line 76

Table of Contents

5.3.1.6.8.3 Loitering 79
5.3.1.6.8.4 Area Protection 81
5.3.1.6.8.5 Object Removal 82
5.3.1.6.8.6 Object Dropped 83
5.3.1.6.8.7 Advanced Options 85
5.3.1.6.8.8 Analytics Actions 87
5.3.1.6.8.9 Analytics Troubleshooting 88
5.3.2 Streaming Tab 90
5.3.2.1 Video Settings 91
5.3.2.1.1 Video Resolutions 91
5.3.2.1.2 Configuring Video Settings 94
5.3.2.2 Privacy Zone 97
5.3.2.3 ROI 98
5.3.3 Camera Tab 99
5.3.3.1 Exposure Screen 99
5.3.3.1.1 Auto Shutter Mode 100
5.3.3.1.2 Flickerless Mode 103
5.3.3.1.3 Auto Iris Mode 104
5.3.3.1.4 Manual Mode 106
5.3.3.1.5 Shutter WDR Mode 108
5.3.3.2 Picture Adjustment 110
5.3.3.3 White Balance 111
5.3.3.4 Digital Zoom 112
5.4 Logout 113
6. Appendices 114
6.1 Technical Specifications 115
6.1.1 Accessing Camera Information from the Web 115
6.2 Internet Security Settings on Internet Explorer 115
6.3 Installing UPnP Settings on Internet Explorer 117
6.4 Deleting Temporary Internet Files on Internet Explorer 121
6.5 Installing and Deleting the Web Player 122
6.6 Network Settings 127
6.7 Troubleshooting 128
6.8 Acronyms and Abbreviations 130
6.9 Mounting and Lens Accessories 131

1 Document Scope and Purpose

The purpose of this document is to provide instructions and installation procedures for physically connecting the CF-6308 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 dégagera FLIR Systems, Inc. et ses agents de toute responsabilité en résultant.

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



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:



Caution:

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

Attention:

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



Caution:

- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the 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 20 newtons (20-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 --20° to 50°C (-4° to 122°F), with no more than 90% non-condensing humidity.
Attention:
Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage (-20° à 50°C/-4° à 122°F), sans condensation d'humidité supérieur à 90%.

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 User and Installation Guide is intended to help you physically install, configure settings for, and operate, the CF-6308 indoor/outdoor fixed box IP camera. The camera body includes a CS mount and is supplied without a lens. The body accepts P-Iris, DC-Iris, and i-CS mount lenses. The camera supports three streams with the following maximum resolutions: 3840x2160 (UHD/4K) + 1920x1080 (Full HD 1080p) + 720x480/576 (D1) with H.265, H.264, or MJPEG compression (3840x2160 @ H.265/H.264 only). It also includes audio-in, audio-out, alarm-in, and alarm-out connections.The camera is powered by an 802.3af Power over Ethernet (PoE), 12VDC, or 24VAC connection. It includes a microSD card drive for storing recordings and snapshots.



CF-6308 Box Camera

2.1 Features

- 4K 1/2.5” BSI CMOS sensor
- Triple stream: UHD +Full HD 1080p + D1
- H.265, H.264, and MJPEG compression
- DC-Iris, P-Iris, or i-CS mount lens
- One-push focus
- External Auto Back Focus button
- Audio In/Out
- Alarm In/Out
- Video Analytics
- Low-lux mode without IR
- True day/night (ICR)
- Supports up to 128GB microSDXC card
- True and Digital WDR
- 3DNR image noise reduction
- Backlight compensation
- Built-in web server
- Supports Internet Explorer, Edge, Chrome, and Firefox browsers
- HTTP streaming MJPEG
- Motion detection event-driven alarms
- Tampering detection and notifications
- Two regions of interest
- Gamma correction
- White balance
- 8 privacy zones
- 802.1X and SSL/TLS security protocols
- SNMP v1/v2c/v3 and SNMP traps
- Up to 9 users
- RS-485 connection
- UPnP support
- ONVIF© Profile S & G

- Powered by 802.3af PoE or optional 12VDC/24VAC supply
- IP66 enclosure with IK10 vandal-proof protection
- External Default button

2.2 Package Contents

The unit package contains the following items:

Quantity	Description
1	CF-6308 box camera
1	Two-pin female terminal connector for optional AC/DC power supply
1	*CF-6308 Quick Install Guide*

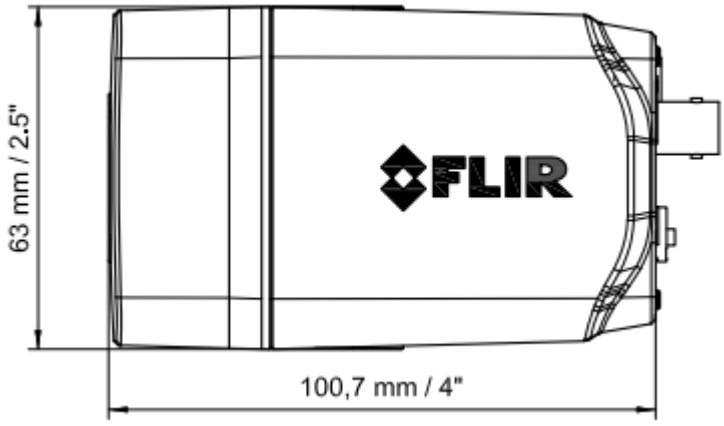
Note: For all current documentation, see Accessing Camera Information from the Web

- *This User Guide*
- *DNA 2.2 User Manual*

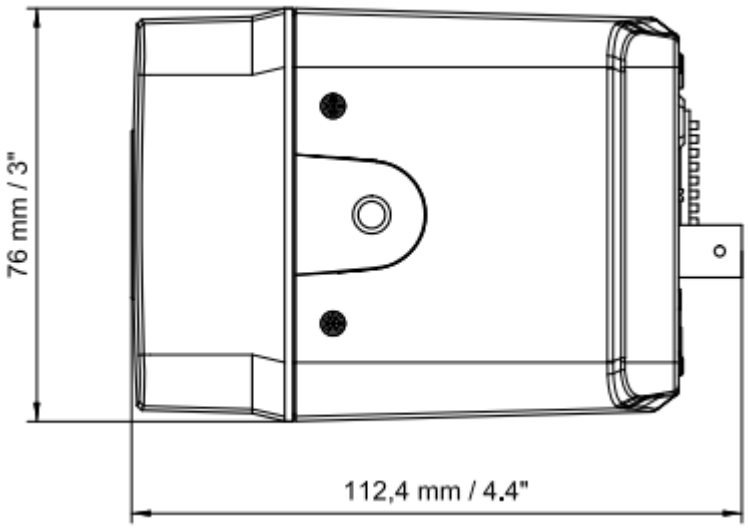
  etc.

2.3 Hardware Description

Following are the CF-6308 box camera's dimensions.

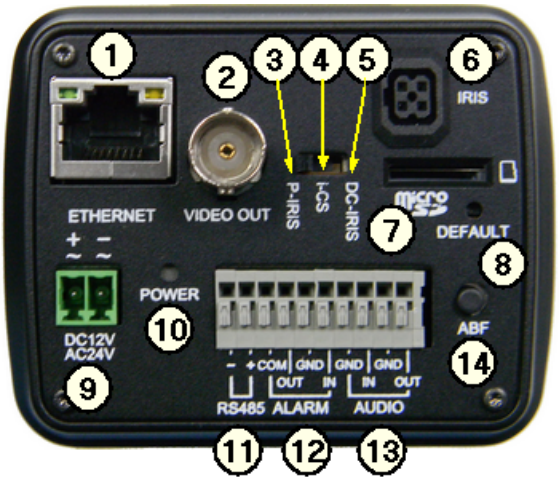


Side View



Top View

The connector panel includes the following:



CF-6308 Connector Panel

Item	Legend	Description
1	ETHERNET	RJ45 port for Network and Power over Ethernet (PoE) connection.
2	VIDEO OUT	BNC connector for analog video outout.
3	P-IRIS	Move toggle switch to left side to enable use of P-Iris lens.
4	i-CS	Move toggle switch to middle to enable use of i-CS mount lens.
5	DC-IRIS	Move toggle switch to right side to enable use of DC-Iris lens.
6	IRIS	Connector for attaching cable from lens.
7	microSD	microSD card drive supporting microSDXC card (Min recommended 4GB, up to 128GB, Class 10). The card is not included.

8	DEFAULT	Button to reboot the unit to full factory defaults. **Notes:** 1. Network settings are not saved. 2. If the Camera has a Basic Video Analytics License installed, resetting to Factory Defaults will clear it and it will have to be reloaded.
9	DC12V/AC24V	Male two-pin terminal block connector for attaching optional 12VDC or 24VAC power supply.
10	POWER	LED indicating Power On. The LED flashes green to indicate power on and network activity. The link is not illuminated if there is no network activity.
11	RS485	Spring input terminals on terminal block for Positive (+) and Negative (-) wires from device attached via RS-485 serial connection.
12	ALARM	Spring input terminals on terminal block for COM, Ground, Alarm In, and Alarm Out wires.
13	AUDIO	Spring input terminals on terminal block for two Ground, Alarm In, and Alarm Out wires.
	ABF	Press the button to activate Auto Back Focus. This button activates the One-Push AF feature on the **System >Lens Control** screen.

Note:

When the camera is set to P-Iris, be sure to select the correct lens type on the **Camera > Exposure** screen in order for the camera to operate correctly.

2.4 System Requirements

Item	Minimum System Requirement
Personal Computer	Intel® Pentium® IV, 2.4GHz or higher with >1GB RAM Monitor display with minimum 1024 x 768 resolution (NVIDIA GeForce 6 Series or ATI Mobility Radeon 9500)
Operating System	Windows 7, 8, 8.1, and 10 (all 64-bit versions) Windows Server 2003, Windows Server 2008 (32-bit version)
Web Browser	Microsoft Internet Explorer 10 and above (32-bit version); Microsoft Edge 38 and above; Chrome v.55 and above; Firefox v.50 and above
Network Card	10Base-T (10 Mbps) or 100Base-TX (100 Mbps) operation
Viewer	ActiveX control plug-in for Internet Explorer; MJPEG viewer for Edge, Chrome, and Firefox

3 Installation

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

- Pre-Installation Checklist
- Powering the Camera
- Connecting the Camera to the Network
- Resetting the Camera

3.1 Pre-Installation Checklist

Before installing the unit, make sure that:

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



Caution:
To avoid damage from overheating or unit failure, assure that there is sufficient temperature regulation to support the unit's requirements (cooling/heating). Operating temperature should be kept in the range -20° to 50°C (-4° to 122°F), with no more than 90% non-condensing humidity.
Attention:
Afin d'éviter tout dommage dû à une surchauffe ou toute panne de l'unité, assurez-vous que la régulation de température est suffisante pour répondre aux exigences de l'unité (refroidissement/chauffage). La température de fonctionnement doit être maintenue dans la plage (-20° à 50°C/-4° à 122°F), sans condensation d'humidité supérieur à 90%.

3.2 Attaching and Adjusting the Lens

The camera is shipped without a lens. You must attach and adjust the lens before viewing video.

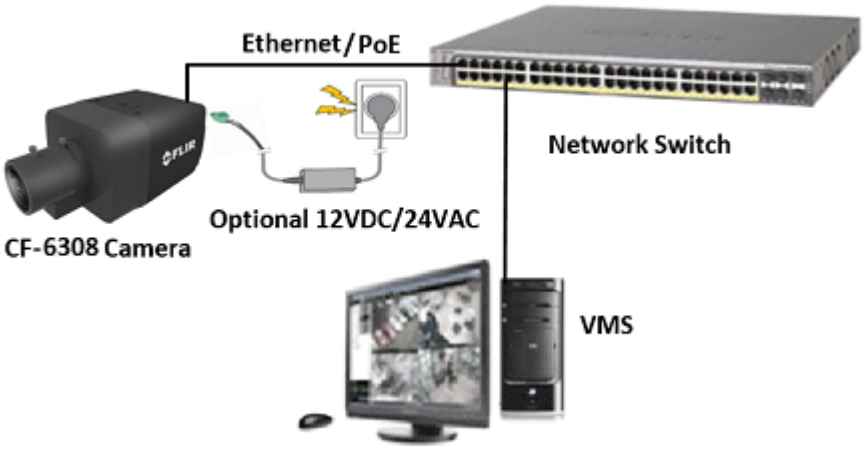
To attach and adjust the lens

1. Remove the plastic insert covering the threaded camera lens mount. Do not touch the sensor or allow dust to accumulate in the lens mount.
2. If you are using a C-mount lens, screw a 5mm adapter ring into the C-Mount to convert it to a CS-Mount.
3. Align the lens threads into the lens mount and screw in the lens.
4. If you are using a P-Iris lens, plug the auto iris cable from the lens assembly into the IRIS port of the camera. Verify that the P-Iris/i-CS/DC-Iris toggle switch is in the P-iris position.
5. If you are using an i-CS lens, plug the auto iris cable from the lens assembly into the IRIS port of the camera. Verify that the P-Iris/i-CS/DC-Iris toggle switch is in the i-CS position.
6. When using a DC auto iris lens, plug the auto iris cable from the lens assembly into the IRIS port of the camera. Verify that the P-Iris/i-CS/DC-Iris toggle switch is in the DC-Iris position.
7. When using a manual lens, verify that the P-Iris/i-CS/DC-Iris toggle switch is in the DC-Iris position.

8. For P-Iris or DC-Iris manually adjust the zoom and focus. If using i-CS please visit the Lens Control page on the camera's web UI for zoom control; focus is automatic.
9. When using a P-Iris or DC-Iris, press the ABF button on the connector panel to fine-tune the focus.

3.3 Powering the Camera

The camera can be powered by an 802.3af PoE (Class 3) connection over the unit's network cable, or by a two-pin terminal block connection to a 12VDC or 24VAC power supply (not supplied).



System Connection

Caution:

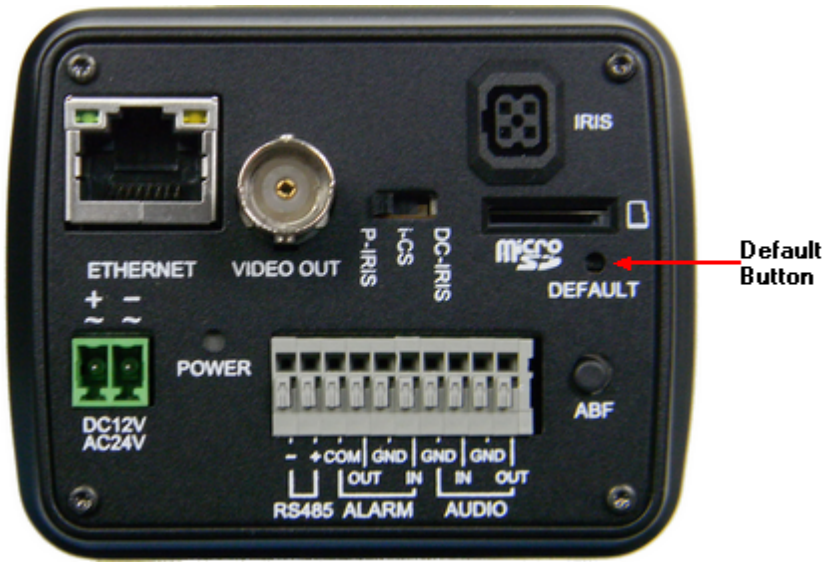
1. If the camera is connected to a PoE network, note that the PoE supply's rated output is 48VDC, 0.2A.
2. If the camera is installed for outdoor use, the PoE supply must be installed with proper weatherproofing.
3. As a Listed Power Unit, the PoE should be marked as "LPS" or "Limited Power Source".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

Attention:

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

3.4 Resetting the Camera

The connector panel includes a **Default** button for easily resetting the camera. The button enables you to save configured settings and to restore factory defaults, including network settings.



Default Button

To reboot the camera (Partial Reset)

Press the Default button for approximately five seconds. The unit reboots. Configured settings are saved.

To restore factory defaults (Full Reset)

Press the Default button continuously for 30 seconds.
The unit restores factory defaults, including the original network settings.

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

4 Preparing to Configure the Camera

- Connecting the Camera to the Network
- Using DNA to Access the Camera
- Configuring the Unit's Initial IP Address
- Configuring Communication Settings

4.1 Connecting the Camera to the Network

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. If the PC is on a different subnet than the camera, you will not be able to access the camera via a web browser.

If there is a DHCP server on the network, it is recommended to use FLIR's Discovery Network Assistant (DNA) utility to search for and change the camera's initial IP address. If there is no DHCP server on the network, the camera will initialize with the default IP (192.168.0.250). You can then use DNA to change its IP address.

4.2 Using DNA to Access the Camera

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. If the PC is on a different subnet than the camera, you will not be able to access the camera via a web browser.

If there is a DHCP server on the network, it is recommended to use FLIR's Discovery Network Assistant (DNA) utility to search for and change the camera's initial IP address.

See Accessing Camera Information from the Web

DNA is a user-friendly utility that is designed to easily discover and configure FLIR Professional Security edge devices on a network. The DNA tool has a simple user interface and does not require any installation. The software is provided as a single, standalone executable. It runs on any PC. See Accessing Camera Information from the Web

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

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

If there is no DHCP server on the network, the camera will initialize with the default IP (192.168.0.250). You can then use DNA to change its IP address.



Note:

For detailed guidelines about DNA and its usage, refer to the *DNA 2.2 User Manual. See Accessing Camera Information from the Web*

4.3 Configuring the Unit's Initial IP Address

Use the FLIR DNA utility to discover the unit on the network and to set the unit's initial IP address.

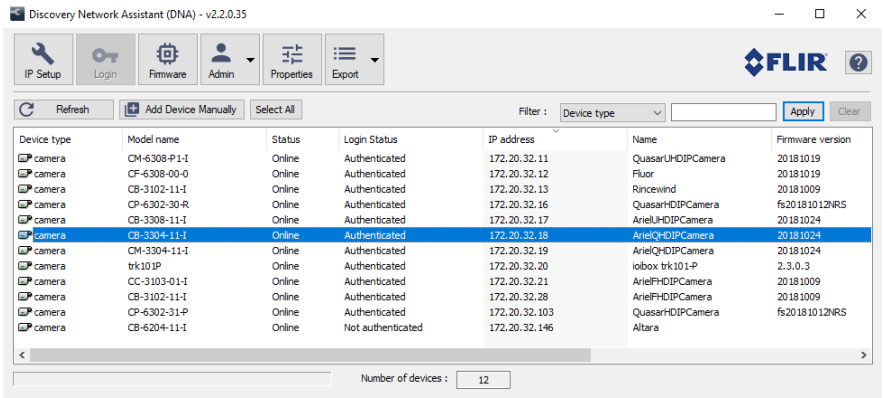
- If the camera is located on a network that uses a DHCP server, or is managed by FLIR's Horizon or Meridian VMS and is configured as a DHCP server, configure the camera with *DHCP-enabled*. Horizon or Meridian automatically assigns the camera an IP address.
- If the camera is located on a network that does not use a DHCP server, or is managed by FLIR's Latitude VMS, manually enter its IP address in the DNA utility.

Note:

1. It is possible to set the IP address without changing the subnet.
2. The unit and the PC must be physically connected on the same network segment.

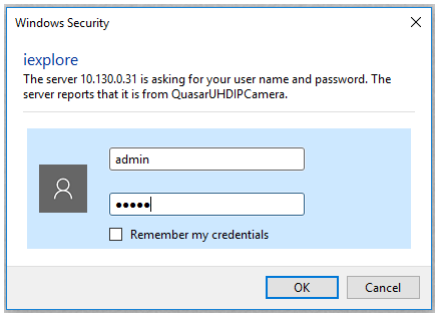
To manage the camera using Horizon, Meridian, or on a DHCP-enabled network

1. Download and run DNA. See Accessing Camera Information from the Web
2. Run the `dna.exe` file by clicking the icon. The DNA application opens and the device is displayed in the window.



DNA Discovery Window

3. Click on the unit in DNA's Discover List. The CF-6308 **Login** window opens.



Login Window

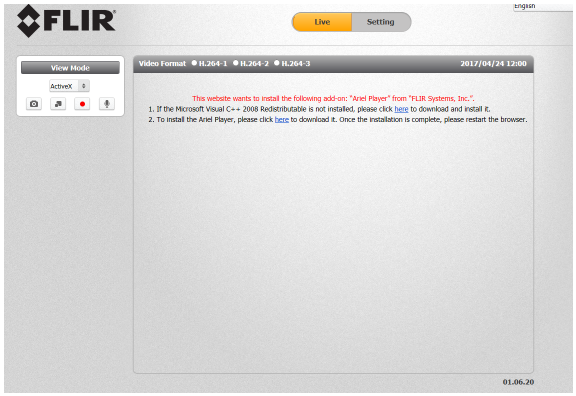
4. If the camera cannot connect to a DHCP server, enter the unit's default IP address (192.168.0.250).

5. Enter the default User Name (*admin*) and Password (*admin*).

Note:

The user name and password are case-sensitive.

6. Click **OK**. The camera's web interface opens.
   - If your browser is Edge, Chrome or Firefox, the video is displayed in the Live View window.
   - If your browser is Internet Explorer, a message is displayed, requesting you to download the Microsoft Visual C++ 2008 Redistributable package and/or to install the Ariel Player add-on.



Web Interface with Internet Explorer Browser

   a. If the Microsoft Visual C++ 2008 Redistributable package is not installed in your computer, click the link to install it. Then proceed to Step 7.
   b. If the Microsoft Visual C++ 2008 Redistributable folder is installed in your computer, proceed to Step 7.

7. Click "*here*" on the screen to download the Ariel Player add-on. The Ariel Player information bar opens.



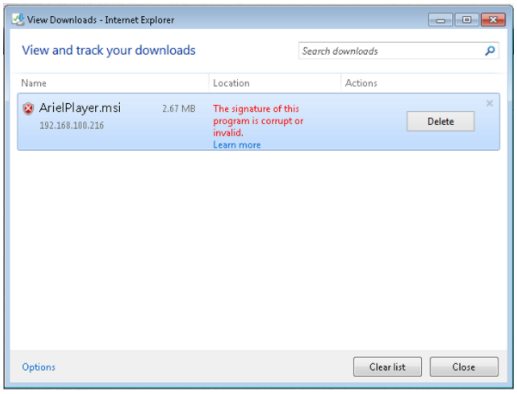
Run Ariel Player Information Bar

When using Internet Explorer in closed networks, occasionally the browser will not install the Ariel Player on the client PC because it cannot verify the Ariel Player's digital signature. This may be because the local certificate is out of date, invalid or missing. The following message is displayed:



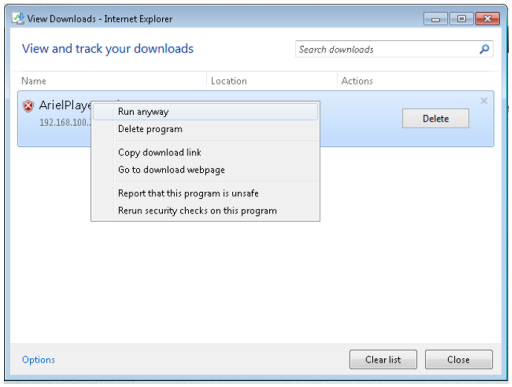
Corrupt/Invalid Signature

a. Click **View downloads**. The **View Downloads** screen opens.



View Downloads Screen

b. Right-click on the ArielPlayer.msi file.



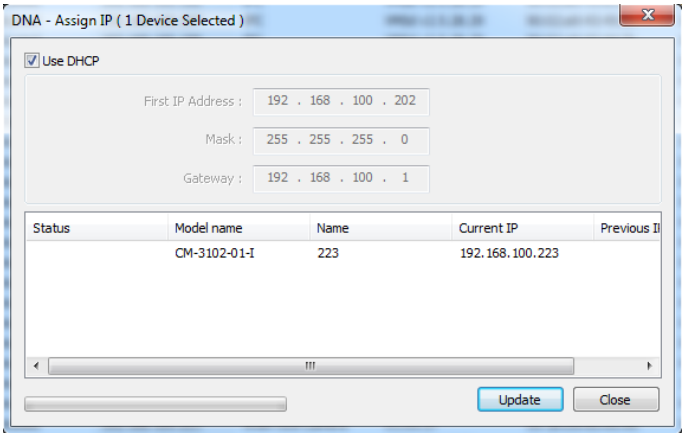
Run Anyway Option

c. Select “Run anyway”. The normal installation process starts.

8. Follow the instructions in Appendix 10.5 for installing the Player. After installing the Player, the Live View is displayed.

To manage the camera using Latitude or on a network with static IP configuration

1. Download and run DNA. See Accessing Camera Information from the Web
2. Run the `dna.exe` file by clicking the icon. The DNA application opens and the device is displayed in the **DNA Discovery** window. See Figure: DNA Discovery Window.
3. Select the unit by right-clicking it. The **DNA - Assign IP** window is displayed.



DNA Assign IP - Use DHCP Screen

4. Uncheck *Use DHCP*.
5. Enter the unit's default IP address (192.168.0.250), Subnet mask, and Gateway IP address in the respective field.
6. Click **Update**. The unit reboots with the new settings.
7. Click on the unit in DNA's Discover List. The camera's **Login** window opens. See Figure: Login Window.
8. Enter the default User Name (*admin*) and Password (*admin*).

Note:

The user name and password are case-sensitive.

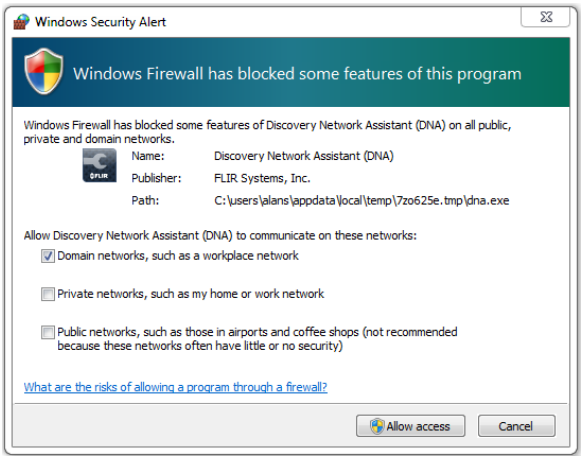
9. Click **Login**. The camera's web interface opens. See Figure: Web Interface.
10. Click the on-screen message to install the Ariel Player plug-in. The Ariel Player Plug-in message is displayed. See Figure: Ariel Player Plug-in Download Information Bar.

4.4 Configuring Communication Settings

To configure communication settings on the camera

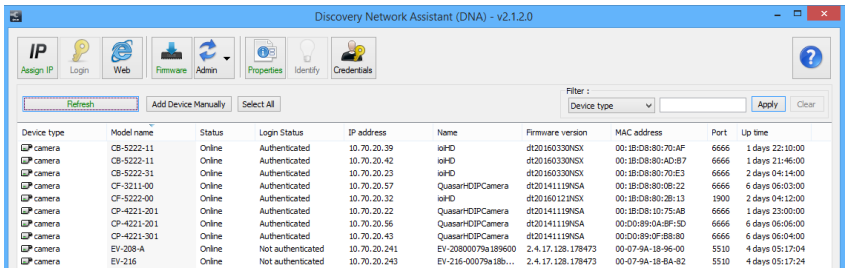
1. Connect the camera to the network on the same VLAN/LAN as the workstation.
2. If the network supports the default, open the DNA utility by running `dna.exe`. (See Accessing Camera Information from the Web)
3. Click the DNA icon .

4. In the DNA application, click the **DNA** button.
5. If the Windows Firewall is enabled, a security alert window pops up.
6. To continue, click **Allow Access**. Latitude users should consult the Latitude Installation Instructions on disabling the Windows Firewall.



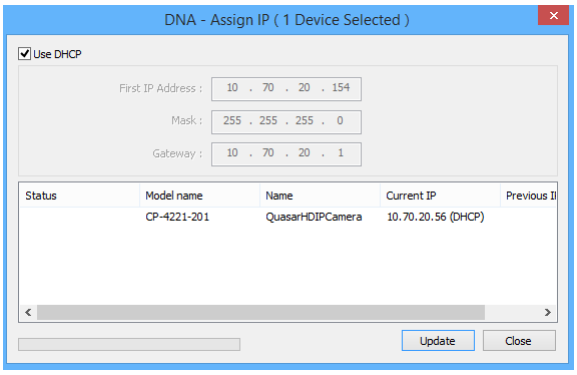
Windows Firewall Screen

7. Click **Assign IP**. All the discovered IP devices will be listed in the page, as shown in the figure below. The camera's default IP Address is automatically supplied by the DHCP server.



Discovered IP Devices

8. Right-click the camera whose network property is to be changed. From the context menu that opens, select **Assign IP**. The **Assign IP** dialog is displayed.



DNA Assign IP – Use DHCP Dialog Box

Tip:
Record the camera's MAC address for future reference.

9. To change the IP address, do one of the following:

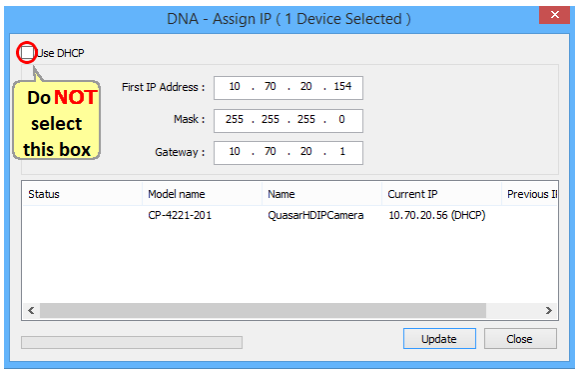
   a. For DHCP (not supported by Latitude):

      i. Select *Use DHCP*. Do not use for Latitude.

      ii. Click **Update** and wait for status.

   b. Latitude users - This is recommended for security purposes
   Static IP:

   Important: Do **not** select the ***Use DHCP*** checkbox**.**

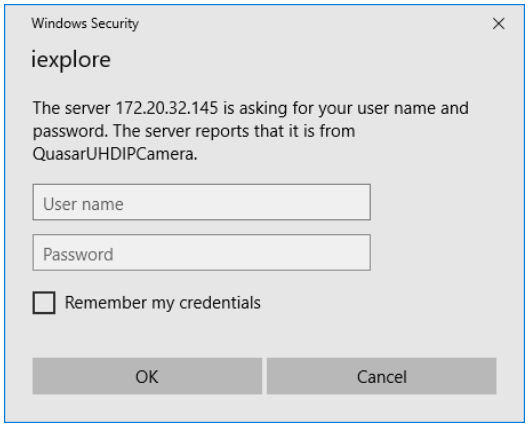


DNA Assign IP – Static IP Dialog Box

      i. In the IP Address, Gateway, and Netmask, enter the respective LAN/VLAN (optional DNS) values.

      ii. Click **Update** and wait for *OK* status to be displayed.

10. Right-click and select **Web** to directly access the camera via a web browser. The web browser opens on the unit's **Login** dialog box.



Login Dialog Box

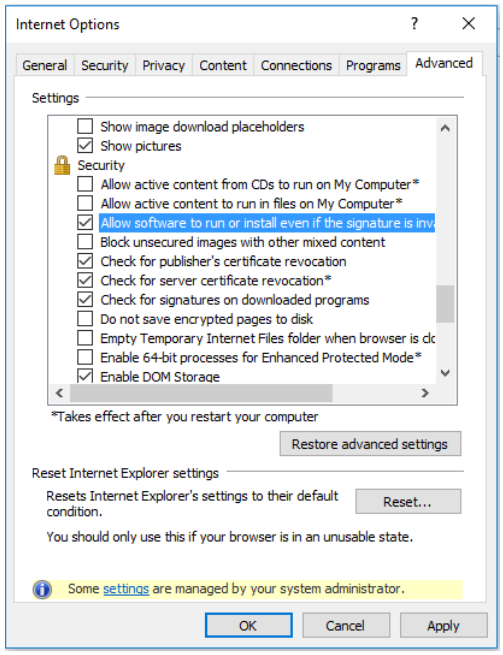
11. Log into the unit with the default user name *admin* and password admin**.**

Note:

1. Both the user name and password are case-sensitive.
2. It is strongly advised that administrator's password be altered for security reasons.

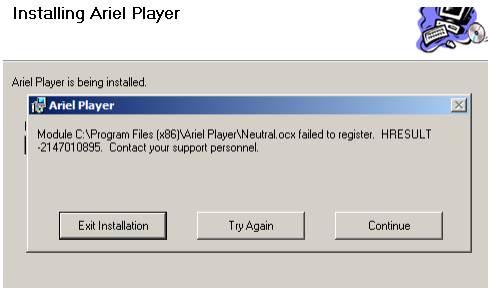
- If the **User Account Control** dialog box, opens and requests you to install the `install.cab` file, click **Yes**.

- If the ActiveX installation is not successful after performing the previous step, in the Internet Explorer **Tools > Internet Options > Advanced** *Security* section, select the *Allow software to run or install even if the signature is invalid* checkbox. Uncheck the checkbox after installing ActiveX. Then click **OK**.



IE Tools > Internet Options > Advanced Window

- If you are using ActiveX, but do not have the Microsoft Visual C++ 2008 Redistributable libraries installed on your PC, the following error message is displayed. In this case, download and install the `vcredist_x86.exe` file from the Internet, or contact your Network Administrator or FLIR Support. .



MS Visual C++ 2008 Redistributable Error Message

12. If a popup message appears for running the ActiveX add-on, click **Allow**.

Note:
If the password is changed and the Latitude AdminCenter Discovery feature is in use, deselect all other proprietary types. Select *FLIR* as the Unit Type so that the new password can be configured in the *Discovery > Add Unit Manually* setting.

Additionally, you can change the camera's network properties (either DHCP or Static IP) directly from the camera's web interface on the System > Network > General screen.

13. Install the web player.



Note:
If you have previously installed a web player application on the PC, you should delete the existing web player from the PC before accessing the camera.

5 Configuration and Operation

The Quasar Gen III camera is provided with a browser-based configuration interface for video playback and recording. In this chapter, information about main page introduction, system related settings and camera settings are described in detail.

Additionally, if FLIR's Latitude VMS is used, many of the configurations and features of FLIR's VMS provide configuration and automation of the camera.

This section includes the following information:

- Accessing the CF-6308 via a Web Browser
- Live View
- System Tab
- Streaming Tab
- Camera Tab
- Logout

5.1 CF-6308 Web Interface

The camera's web interface can be configured and operated from a 32-bit version of Internet Explorer 10 and above, Microsoft Edge 38 and above, Chrome v.55 and above, or Firefox v.50 and above.

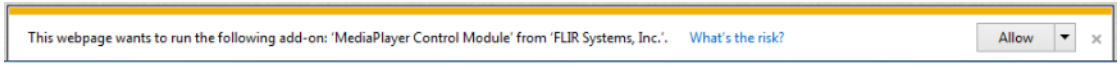
To access the unit via the web browser

1. Open your browser.
2. Enter the unit's IP address in the browser's address bar.
3. Press the ENTER key on your PC keyboard. The unit's **Login** window is displayed. See Figure: Login Window.
4. Enter the user name (default: a*dmin*) and password (default: *admin*) to log into the system. The unit's web interface opens. See Figure: Web Interface.

   Note:

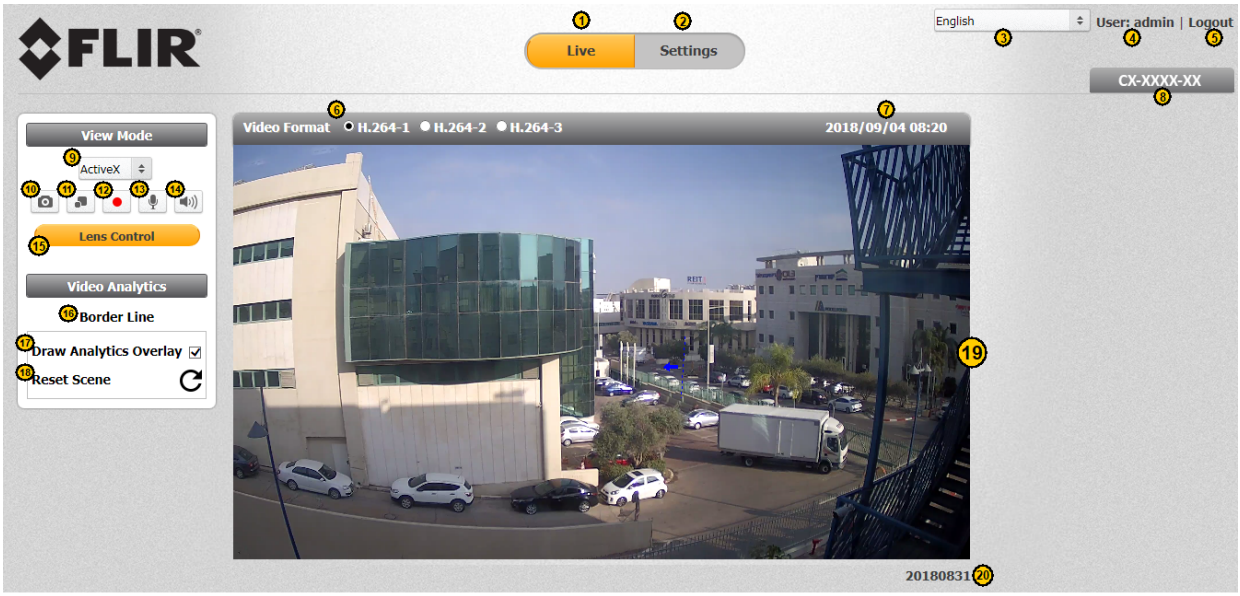
   The user name and password are case-sensitive.

5. If you are using the system for the first time or you have uploaded a new firmware version, click the message displayed on the screen to download to allow the `MediaPlayer Control Module.exe` plug-in.

6. Click **Allow**. The Windows Installer opens and the **Ariel Player Wizard** dialog box is displayed. Follow instructions in the Configuring the Unit's Initial IP Address section.

7. Configure camera settings after setting the unit's IP address.



1. Live View Tab
2. Settings Tab
3. Language Bar
4. User Name
5. Logout Button
6. Video Format
7. Date and Time
8. Model Number
9. ActiveX/MJPEG
10. Snapshot
11. Full Screen
12. Manual Recording
13. Microphone
14. Audio
15. Lens Control
16. Analytics Rule Name
17. Show Analytics Overlay
18. Reset Scene
19. Live View Window
20. Firmware Version

Live View Screen with Callouts on Internet Explorer Browser

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

- Language Bar – Select the language for the web interface: English, Arabic, Czech, Simplified Chinese, Traditional Chinese, French, German, Hungarian, Italian, Japanese, Polish, Portuguese, Russian, or Spanish.
- User Name – Displays the user name. By default, *Admin* is displayed.
- Logout Link– Click **Logout** to exit the web interface.
- Model Number – Displays the model number.

Above the **Live View** window, the selected video format, date and time are displayed. Below the **Live View** window, the firmware version is displayed.

To the left of the **Live View** window, the View Mode buttons are displayed. All buttons are displayed in Internet Explorer browsers. Only the **Snapshot** button is displayed in Microsoft Edge, Chrome, and Firefox.

Item	Description
ActiveX/MJPEG Button	Click ActiveX to use Internet Explorer or click MJPEG to using Chrome or Firefox. Displayed only with Internet Explorer browser.
Snapshot button	Click the button to take a snapshot.
Full screen button	Click the button to display the live view in full-screen mode. To switch back to Live View mode, right-click on the screen and click **Normal**

Item	Description
	Display, or press the ESC key on your keyboard. Displayed only with Internet Explorer browser.
Manual recording button	This button indicates the recording status: red when recording is On  or gray when recording is Off  . Displayed only with Internet Explorer browser.
Lens Control button	This button opens the **Lens Control** screen, on which you can set the focus (auto or manual) or reset the lens. Auto focus also can be set by pushing the **ABF** button on the connector panel.
Mic button	Click the Mic  button to listen to audio at the remote site. This function is available only to an Operator or Administrator. Click the button to switch it on/off. The button allows the user to listen to audio streaming over the web if (a) audio is enabled and (b) if an audio event is enabled and triggered by exceeding the threshold. See Audio. Displayed only with Internet Explorer browser.
Audio button	Click the audio button  to enable the playback of audio files and to hear audio-out over the web in the case of an audio event.
Analytics Rule Name	Displays the name of the currently configured Video Analytics Rule
Show Analytics Rule Overlay	Shows the configured line or area drawing configured for the currently active Video Analytics Rule
Reset Scene	Resets the scene of a configured Video Analytics Rule. Used in the case where the scene changed drastically such as a large structure being removed or the camera angle changing.

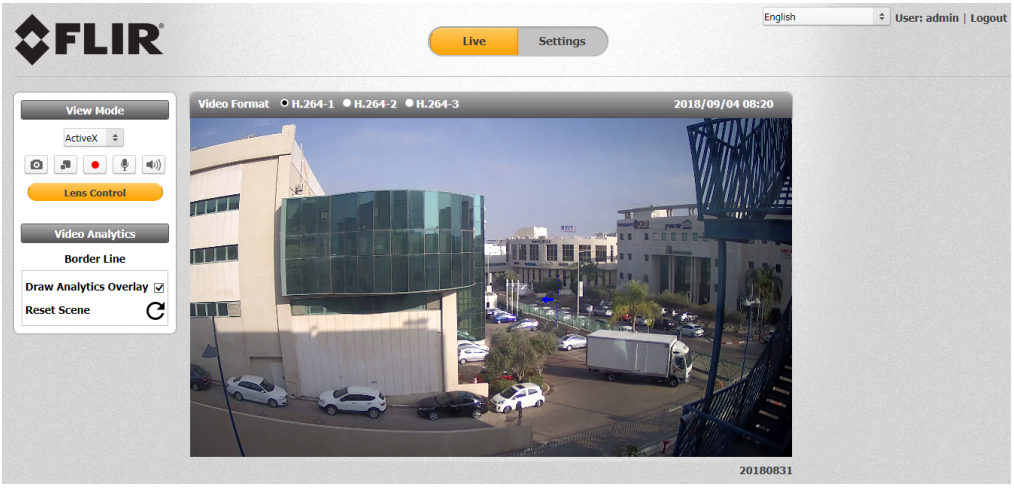
From the Navigation Bar, select one of these tabs:

- Live – Displays the **Live View** screen
- Settings – Displays the **Settings** sidebar

5.2 Live View

To start Live View

The **Live** screen opens upon login.



Live View Screen with Internet Explorer Browser

The following sections include the following topics:

- Recording
- Capturing a Picture
- Viewing Live Video from a Media Player

5.2.1 Recording

Manual recordings (which are triggered from the **Live View** screen) are stored on the PC.

To start recording a Live View scene

1. Click the red **Manual Recording** icon on the toolbar. The camera starts recording. A red dot is displayed in the upper right fixed of the **Live View** window, under the date and time display.

   Note:

   In order to save recordings on your PC, Internet Explorer should be run as Administrator.

2. Select the directory and folder to save the video, which is an `.avi` file.
3. Click the icon to stop recording. The icon turns gray .

To playback a Live View recording

1. Open the folder on the PC where the recording is stored.
2. Select the file.

Recordings that are triggered by events (such as motion detection) are stored on a microSDXC card, which can store up to 128GB of data. The card is not included.

To view a triggered event recording

1. In your browser, enter the camera's FTP address (ftp://camera_ip/).
   Note: The FTP server must be enabled. See FTP Server below.
2. Enter the Admin user name and password.
3. Open the folder for the event according to the type of event (motion detection, tampering, etc.). Files are displayed chronologically according to most recent date.
4. Select the file.

5.2.2 Capturing a Picture

It is possible to capture a picture as a snapshot in Live View mode and save it on your PC as a .jpeg or .png file image.

Note:

In order to save snapshots on your PC, Internet Explorer should be run as Administrator.

To capture a snapshot in Live View mode

1. In **Live View** mode, click the **Snapshot** button on the toolbar to capture the live pictures.

To view a Live View snapshot

1. Open the folder on the PC where the snapshot is stored.
2. Select the file.

Snapshots that are triggered by events (such as motion detection) are stored on the camera's microSD card, which can store up to 128GB of data. The card is not included.

To view a triggered event snapshot

1. In your browser, enter the camera's FTP address (ftp://camera_ip/).
2. Enter the Admin's user name and password .
3. Open the folder for the snapshots. Files are displayed chronologically according to most recent date with an indication of the type of event, for example 20170118122205_motion_1.mp4.
4. Select the file.

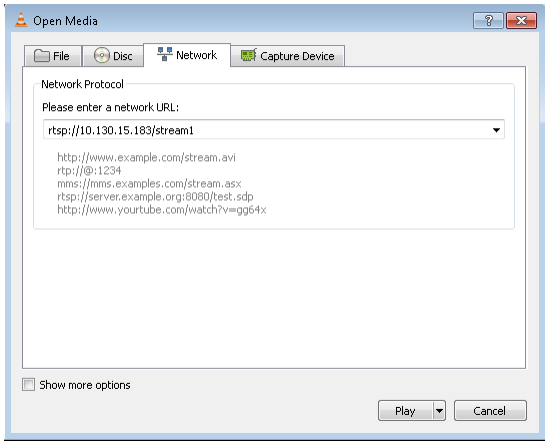
5.2.3 Viewing Live Video from a Media Player

The Live View main 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 two video encoding formats (H.264 and MJPEG).

The camera supports sending unicast and multicast streams via the RTSP protocol. Unicast streams include the suffix "stream" followed by the stream number without a space. Multicast streams include the suffix "streamXm", where "X" is the stream number (1, 2 or 3).

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.



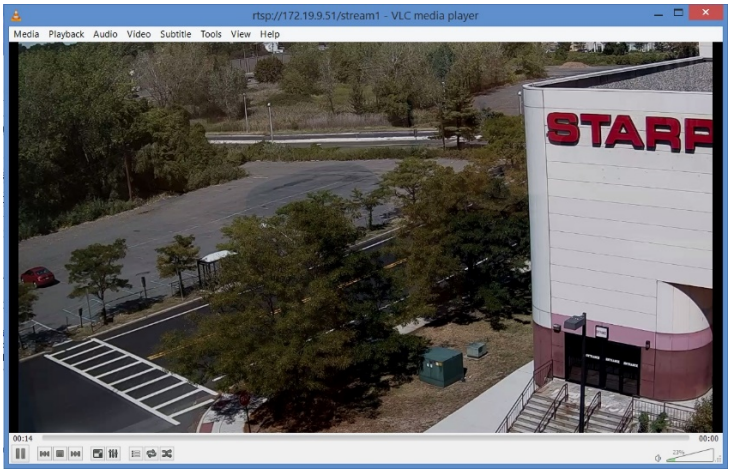
VLC Open Media Screen

3. In the **Network** tab, enter the URL for the stream in the address bar:
   - The syntax for entering the URL in the media player for the main stream is: rtsp://(camera IP address)/(Unicast stream 1) or (Multicast stream 1). For example, rtsp://192.168.0.250/stream1 for a unicast stream.
   - The syntax for entering the URL in the media player for the second stream is: rtsp://(camera IP address)/(Unicast stream 2) or (Multicast stream 2). For example, rtsp://192.168.0.250/stream2 for a unicast stream.
   - The syntax for entering the URL in the media player for the third stream is: rtsp://(camera IP address)/(Unicast stream 3) or (Multicast stream 3). For example, rtsp://192.168.0.250/stream3m for a multicast stream.

Note:

1. It is also possible to change the syntax on the RTSP page, although this is not recommended if the camera is attached to a VMS.
2. Verify that the resolution entered in URL string agree with the resolution set in the **Streaming > Video Settings** screen.

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



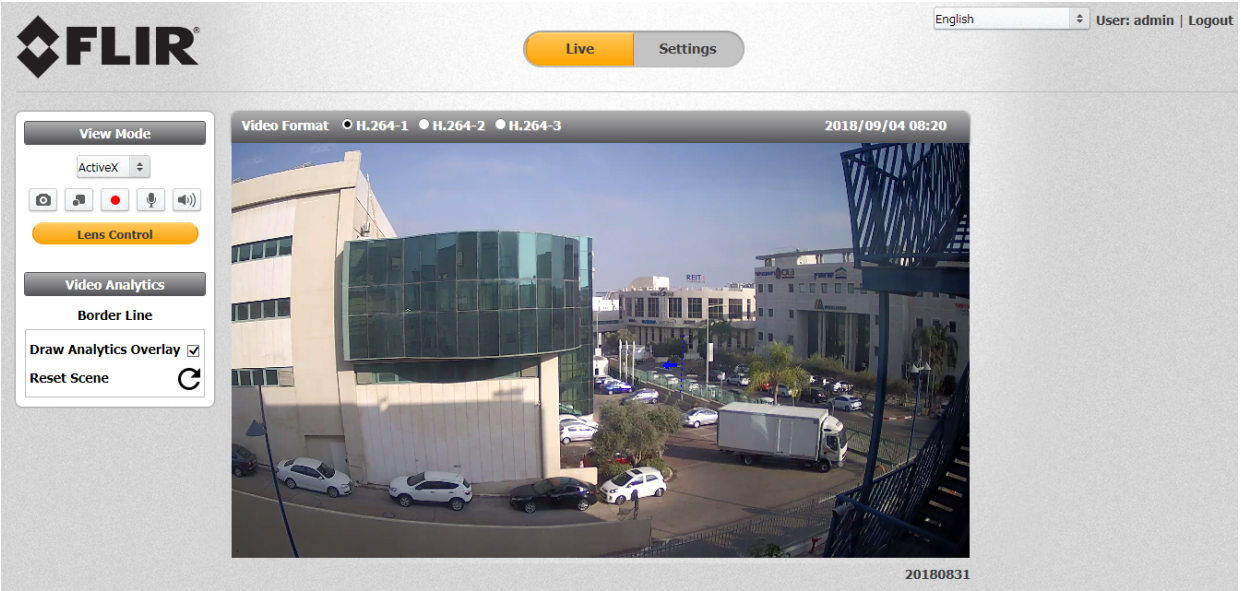
Media Player Screen

5.2.4 Basic Video Analytics

Notes:

1. When **Motion Detection** is configured, *Basic Video Analytics* is disabled.
2. **Basic Video Analytics** is only enabled when the appropriate **Camera License** has been uploaded to the camera. See Providing cameras with Basic Video Analytics Licenses

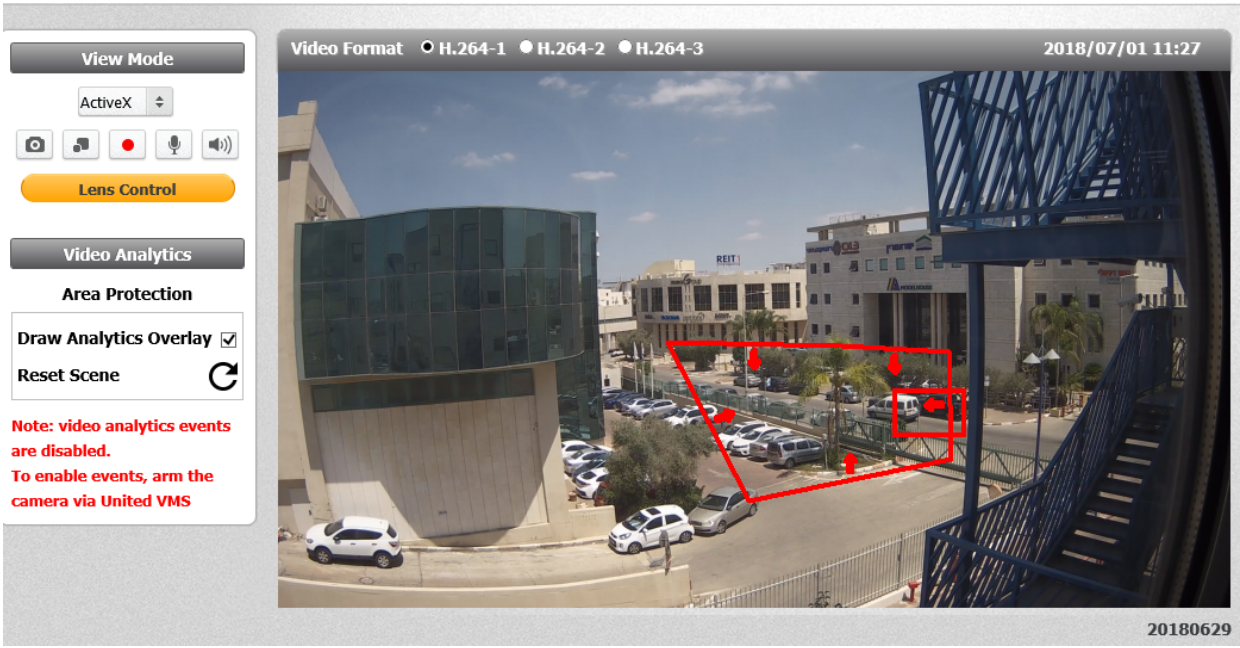
When Basic Video Analytics is enabled, the configured rule will display on the left side of the Live View page. This section will show the current active rule, and provides the ability to see the configured overlay drawing and to reset the scene.



Under the "Video Analytics" heading is the name of the current active analytic rule. The rule options are:

Counting Border Line Loitering Area Protection Object Removal Object Dropped

When "Draw Analytics Overlay" is checked, it will show the configured drawing for that rule.



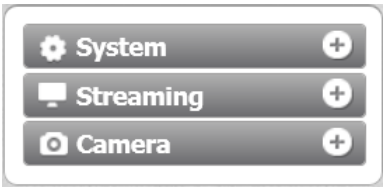
The rule cannot be edited from the Live page. In order to edit the configuration, the user must navigate to Settings > System > Video Analytics and choose the desired rule.

Reset Scene

Clicking **Reset Scene** will relearn the scene and the background in case the scene has changed or the camera has been moved.

5.3 Settings

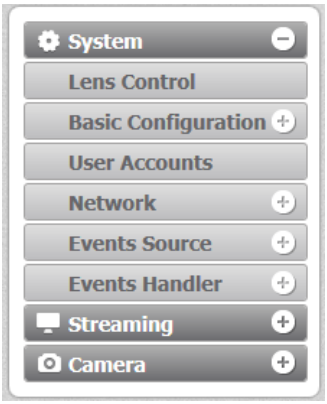
Device and client PC parameters are set from the **Settings** tab in the navigation bar. Upon clicking **Settings**, the **Settings** menu is displayed in the sidebar. Three sections are displayed: System, Streaming, and Camera.



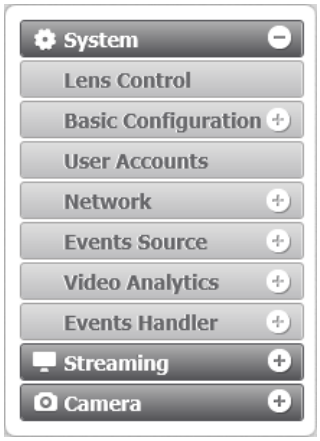
Unexpanded Sidebar

5.3.1 System Tab

The **System** tab is used for configuring essential system settings. Click the **System** tab to expand the menu.



System Menu
(Default - No Camera Analytics License installed)



System Menu - (Camera Analytics License installed)

Click the link to open the tabs for the various functions:

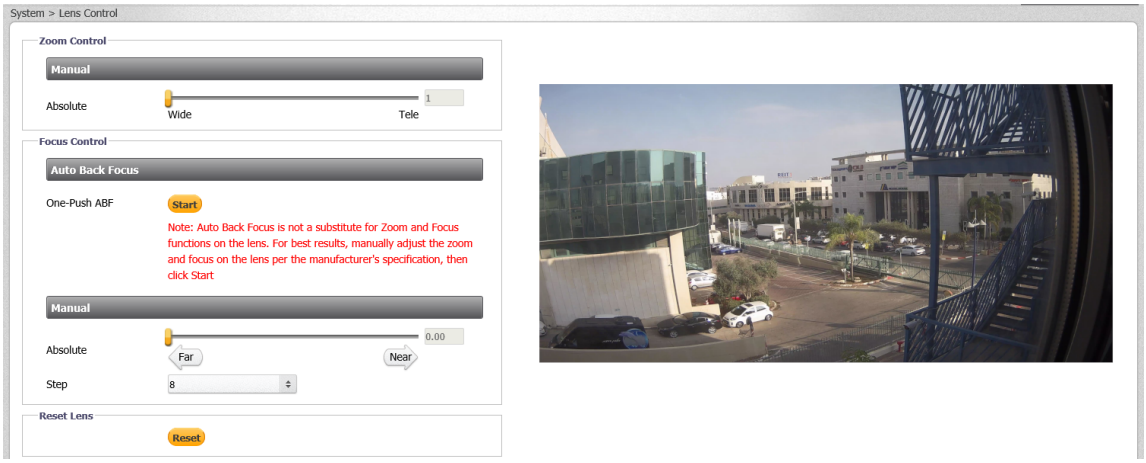
Lens Control | Basic Configuration | User Accounts | Network | Events Source | Events Handler | Video Analytics

5.3.1.1 Lens Control

The **Lens Control** screen enables control of the focus functions.

Note: See also Digital Zoom

Note: This page may be different depending on the type of lens.



Lens Control Screen

To set Auto Focus

1. In the *Focus Control* section, click **Start**. Auto Focus is adjusted.

Note:

In very extreme cases, it may be necessary to manually re-zoom the camera and focus it again.

To manually set the focus

1. In the *Focus Control* section, move the slider to the desired focus between *Far* (1) to *Near* (100).
2. From the *Step* drop-down list, select the number of steps to set the focus: 1, 2, 4, 8, 16, 32, 64, or 128.

To revert to the previous settings (To reset the lens)

1. In the *Reset Lens* section, click **Reset**. The previous settings are restored.

Note:

After clicking the **Reset** button in the *Reset Lens*, it is necessary to click the **Start** button in the *Focus Control* section to refocus the lens.

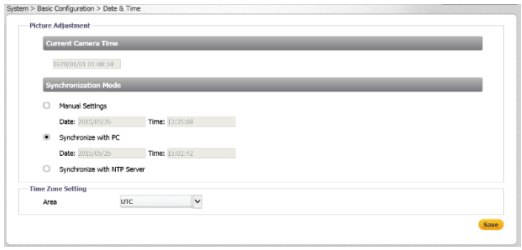
5.3.1.2 Basic Configuration

The **Basic Configuration** tab includes the following screens:

Date & Time | Audio | Firmware | Basic Operations | OSD

5.3.1.2.1 Date & Time

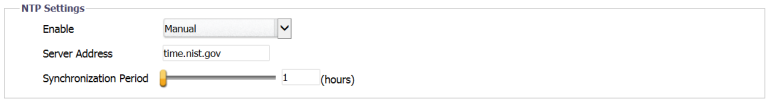
The current time is displayed in the *Current Camera Time* text box. To set the date and time, select **Basic Configuration > Date & Time**. The **Date & Time** screen is displayed.



Date & Time Screen

To change the date and time

1. Select one of the following options
   - *Manual Settings* – Enter the date and time in the respective field.
   - *Synchronize with PC* – Enter the date and time in the respective field.
   - *Synchronize with NTP Server* – Selecting this option opens the *NTP Settings* section:



NTP Setting Section

   a. Enter the following details in the *NTP Setting* section:
      - *Enable* – From the drop-down list, select *Manual* to set the NTP server manually, or *From DHCP Server* to set the time according to the network DHCP server.
      - *Server Address* – Enter the IP address for the NTP server.
      - *Synchronization Period* – Select a number between 1-24 for the frequency (in number of hours) that the camera will synchronize with the NTP time server (i.e., every one hour, every two hours, etc.).
2. In the *Time Zone Setting* section, from the *Area* drop-down list, select your local time zone.
3. Click **Save**. The new time is displayed in the *Current Camera Time* text box.

5.3.1.2.2 Audio

The **Audio** screen is used for configuring *Audio In* and *Audio Out* settings.



Basic Configuration > Audio Screen

To enable audio settings

1. From the *Audio In Settings* section:
   a. *Enable* drop-down list, select *ON*.
   b. From the *Encoding* drop-down list, select *G.711 a-law, G.711 μ-law,* or *AAC.* The default is *AAC. (Audio In Only)*
   c. From the *Level* drop-down list, select *High, Mid,* or *Low.*
2. From the *Audio Out Settings* section:
   a. *Enable* drop-down list, select *ON*.
   b. From the *Level* drop-down list, select *High, Mid,* or *Low.*

5.3.1.2.3 Firmware

The **Firmware** screen displays and is used to update the system firmware, and to display the hardware version, product name (model number), product serial number, and product MAC address. To access the **Firmware** screen, select **Basic Configuration > Firmware**.



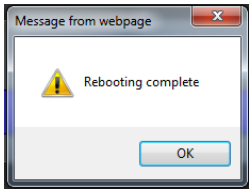
Firmware Screen

To update system firmware

1. Click **Browse** to locate the firmware file.

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

2. Select the file. The file name is displayed (for example, `ArielFHD_20161230`).
3. Click **Upgrade**. The upgrade process takes about three minutes. After the firmware has upgraded successfully, the camera reboots.



Rebooting Complete Dialog Box

4. Click **OK**. The **Live** screen opens.
5. If your browser requests you to close the window, click **Yes**. The window closes.
6. Open a new window and enter the camera's URL. The **Login** window opens. See Figure: Login Window.
7. Enter your user credentials and log into the camera. The new firmware version is displayed in the *Firmware Version* text box.

5.3.1.2.4 Basic Operations

The **Basic Operations** screen is used for the following functions:

- Setting the TV format
- Setting the video out aspect ratio – Ensures that the video image is displayed correctly on the video monitor without distortion or a black border on the edge
- Importing settings from another unit
- Exporting settings to another unit
- Rebooting the camera – Saves configured settings
- Restoring partial factory defaults – Restores factory defaults, but retain network settings (IP address, netmask address, and gateway address), TV format, and image rotation settings
- Restoring full factory defaults – Restores factory defaults, including original network settings. Basic Video IAnalytics license, if in use, must be reloaded.



Basic Operations Screen

To take the above actions, from the **Basic Configuration** tab, select the **Basic Operations** tab.

To select the TV format

1. From the drop-down list, select *NTSC* or *PAL*. The default is *NTSC*.

To set the aspect ratio of the video out signal

1. From the *TV Out* drop-down menu, select one of the following:

- Full – This sets the video stream to D1 and ensures that the video image completely fills the monitor display, regardless of its aspect ratio.
- 4:3 – Select this configuration if the video monitor is set to 4:3 aspect ratio.
- 16:9 – Select this configuration if the video monitor is set to 16:9 aspect ratio.

To import a setting

1. Click **Browse** to select the file.
2. Click **Import** to upload the file.

To export a setting

1. Click **Export**. An information bar opens.
2. Click **Save** in the information bar to save the file.

To reboot the camera

1. Click **Reboot**. The camera reboots. After the reboot finishes, a popup window opens with the message “Rebooting complete”.
2. Click **OK**. A dialog box opens, requesting you to close the tab in your browser.
3. Close the tab.
4. Open a new tab in your browser, and re-enter the camera’s IP address. The camera’s **Login** window opens.
5. Enter your login credentials. The camera’s home page opens.

To restore partial factory defaults

1. Click **Partial factory defaults**. The camera reboots. After the reboot finishes, a popup window opens with the message “Rebooting complete”.



Note:

Clicking **Partial factory defaults** restores all factory defaults except Network Settings and Video Format. If a Basic Video Analytics license was in use, it is saved..

2. Click **OK**. A dialog box opens, requesting you to close the tab in your browser.
3. Close the tab.
4. Open a new tab in your browser, and re-enter the camera’s IP address. The camera’s **Login** window opens.
5. Enter your login credentials. The camera’s home page opens.

To restore full factory defaults

1. Click **Full factory defaults**. The camera reboots. After the reboot finishes, a popup window opens with the message “Rebooting complete”.



Note:

1. Selecting Full factory defaults causes the camera to lose all network settings.
2. If a Basic Video Analytics license was in use, it will need to be re-loaded.

3. Since the unit's IP address might change when restoring full factory defaults, it is recommended to use DNA to discover the unit after rebooting.

2. Click **OK**. A dialog box opens, requesting you to close the tab in your browser.
3. Close the tab.
4. Open a new tab in your browser, and re-enter the camera's IP address. The camera's **Login** window opens.
5. Enter your login credentials. The camera's home page opens.

5.3.1.2.5 OSD

The **OSD** (On-Screen Display) screen is used for setting the background color, text color, and location for displaying the date or text in two configurable locations on the **Live View** window. It is also possible to set the background color and text color to display upon the occurrence of an event.

Set the OSD location according to the following coordinates on the X and Y axes:

	1	2	3	4	5	6	7	8	9	10
1	1x1	2x1	3x1	4x1	5x1	6x1	7x1	8x1	9x1	10x1
2	1x2	2x2	3x2	4x2	5x2	6x2	7x2	8x2	9x2	10x2
3	1x3	2x3	3x3	4x3	5x3	6x3	7x3	8x3	9x3	10x3
4	1x4	2x4	3x4	4x4	5x4	6x4	7x4	8x4	9x4	10x4
5	1x5	2x5	3x5	4x5	5x5	6x5	7x5	8x5	9x5	10x5
6	1x6	2x6	3x6	4x6	5x6	6x6	7x6	8x6	9x6	10x6
7	1x7	2x7	3x7	4x7	5x7	6x7	7x7	8x7	9x7	10x7
8	1x8	2x8	3x8	4x8	5x8	6x8	7x8	8x8	9x8	10x8
9	1x9	2x9	3x9	4x9	5x9	6x9	7x9	8x9	9x9	10x9
10	1x10	2x10	3x10	4x10	5X10	6X10	7X10	8X10	9X10	10x10

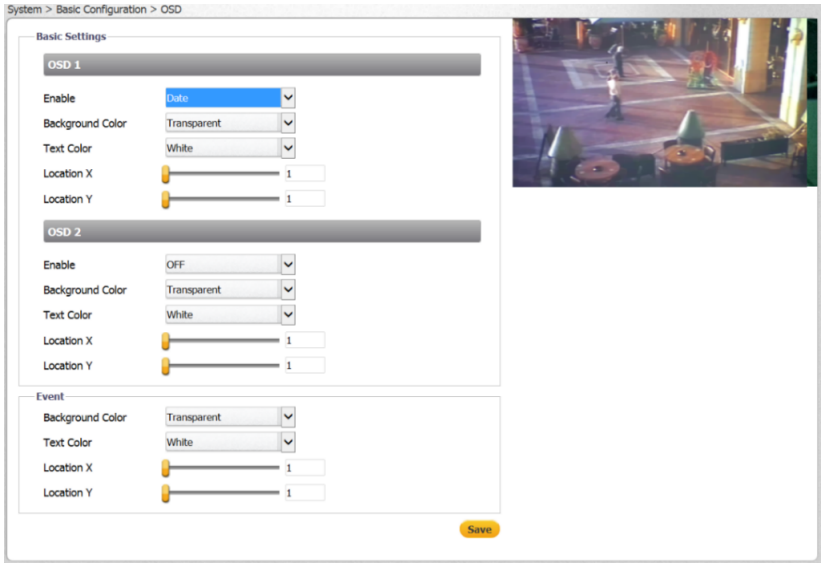
Y-Axis

X-Axis

OSD Location Coordinates

To configure OSD settings

1. Select **Basic Configuration > OSD**. The **OSD** screen is displayed.

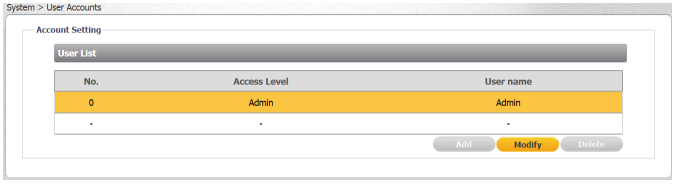


OSD Screen

2. In the *Basic Settings* section, configure the following settings for *OSD-1* and *OSD-2*:
   - *Enable* – From the drop-down list, select one of the following:
     - *Date* – Enables you to enter the date to display.
     - *Text* – Enables you to enter the time to display.
     - *OFF* – Disables the OSD function. This is the default setting.
   - *Background Color* – From the drop-down list, select *Black* or *Transparent* (default setting).
   - *Text Color* – From the drop-down list, select *Black* or *White* (default setting).
   - *Location X* – Move the slider from *1* to *10* to set the location on the screen for the OSD. The default setting is *1*.
   - *Location Y* – Move the slider from *1* to *10* to set the location on the screen for the OSD. The default setting is *1*.
3. In the *Event* section, configure the following settings in case an event occurs:
   - *Background Color* – From the drop-down list, select *Black* or *Transparent* (default setting).
   - *Text Color* – From the drop-down list, select *Black* or *White* (default setting).
   - *Location X* – Move the slider from *1* to *10* to set the location on the screen for the OSD. The default setting is *1*.
   - *Location Y* – Move the slider from *1* to *10* to set the location on the screen for the OSD. The default setting is *1*.
4. Click **Save** when finished.

5.3.1.3 User Accounts

The **User Accounts** screen is used for creating, modifying, and deleting accounts; creating or modifying credentials; and for assigning user access level (Administrator, Operator, and User). It is possible to create up to 10 users, in addition to the default Administrator, which cannot be deleted. There can be multiple users of all types.



User Accounts-Account Setting Screen

Note:

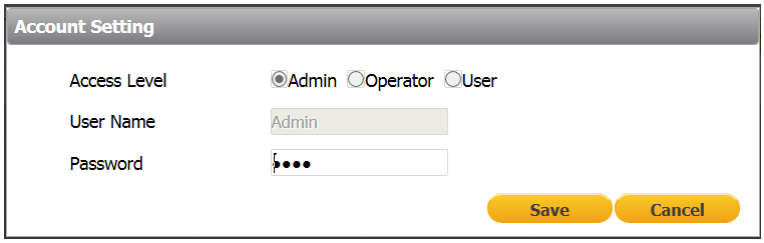
1. User Name and Password can include up to 16 characters, including '0' to '9', 'a' to 'z', 'A' to 'Z', '.', '-', '+', '_' and '@'.
2. The user name and password are case-sensitive.

The following privileges are assigned to each access level:

- An *Administrator* has access to all screens. By default, the camera includes the *Administrator* access level. There can be more than one Administrator. The default Administrator cannot be deleted.
- An *Operator* has access to the **Live View** screen. An Operator can change the playback stream, take and store a snapshot, record live video and view it in full screen mode. There can be more than one Operator.
- A *User* can only view the **Live View** screen. A maximum of 9 Users is possible.

To modify default Administrator credentials

1. Click **Modify**. The **Access Level** dialog box opens.

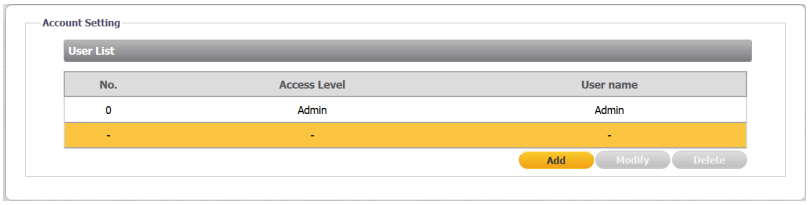


Default Administrator Access Level Dialog Box

2. For security reasons, enter a new User Name and /or Password. The default User Name is “admin” and the default Password is “admin”. See the next section for conventions regarding the User Name and Password.
3. Click **Save**.

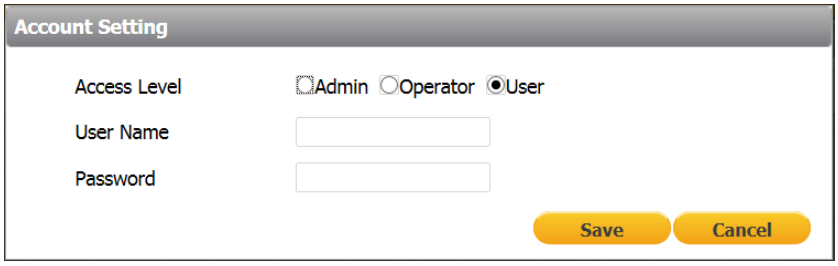
To add a new operator or user

1. Click the empty row.



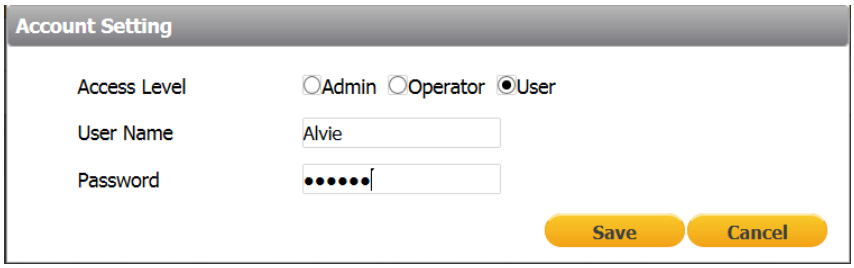
Add User Dialog Box

2. Click **Add**. The **Access Level** screen opens.



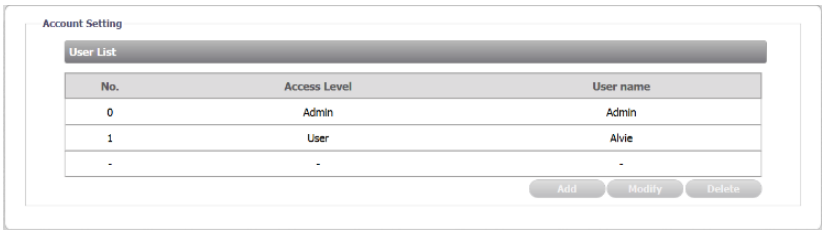
Empty Access Level Dialog Box

3. Select *Operator* or *User*, and enter the User Name and Password.



Filled Access Level Dialog Box

4. Click **Save**. The new Operator or User name is displayed in the *Account Setting* list.



Updated Account Setting List

To modify an operator or user

1. Click **Modify**.
2. Enter the new User Name or Password.

To delete an operator or user

1. Click **Delete**. The operator or user is deleted from the Account Setting list.

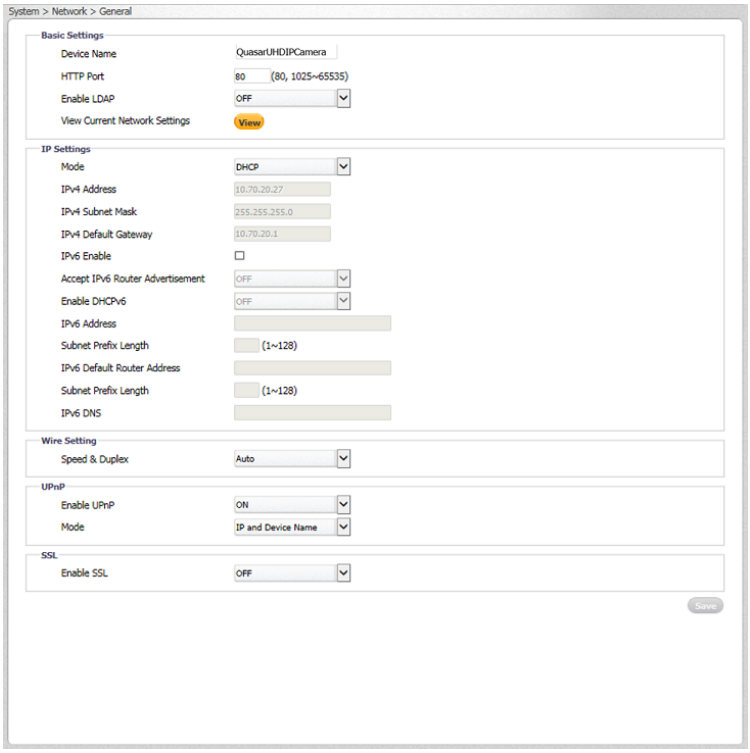
5.3.1.4 Network

The **Network** tab includes the following screens:

General	FTP Server	RTSP	SNMP	802.1X
IP Filter	DDNS	LDAP	SSL	

5.3.1.4.1 General

The **General** screen is used for configuring most network settings.

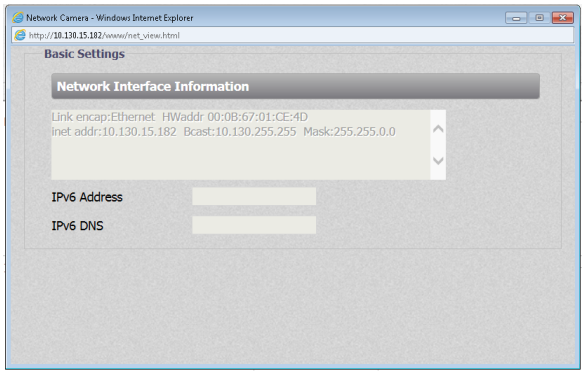


Network > General Screen

To configure basic settings

1. In the *Basic Settings* section, do the following:
   a. In the *Device Name* text box, enter a friendly name for the camera.
   b. In the *HTTP Port* text box, enter the port number. The range is from *1025* to *65535*. The default port is *80*.
   c. From the *Enable LDAP* drop-down list, select *ON* or *OFF*. If you select *ON*, verify that the information in **Network > LDAP** page is correct and that the LDAP server is online. The default is *OFF*.

2. Click **View** to view current network settings. The Internet Explorer **Basic Settings** dialog box opens, displaying network interface information, including Ethernet connection speed, Ethernet NIC MAC address, unit IP address, multicast address, and subnet mask. In the case of an IPv6 connection, the IPv6 address and IPv6 DNS address also are displayed.



Internet Explorer Basic Settings Dialog Box

To configure IP settings

1. In the *IP Settings* section, configure the following settings
   a. *Mode* – From the drop-down list, select one of the following:
      - *Manual* – Used for connecting to the network via a static IP address.
      - *PPPoE* – The camera can access the network via a DSL modem using the Point-to-Point Protocol over Ethernet (PPPoE). When connecting via a PPPoE connection, the *IP Address* field is disabled. After selecting this mode, enter the User Name and Password for the PPPoE account.
      - *DHCP* – Used for connecting to the network via a DHCP server. In DHCP mode, the *IPv4 Address, IPv4 Subnet Mask,* and *IPv4 Default Gateway* fields are disabled.
   b. *IPv4 Address* – The IP address is necessary for network identification. Enter the IPv4 address if you are using IPv4 to connect to the network in Manual mode. In PPPoE and DHCP modes, the IPv4 address is assigned automatically.
   c. *IPv4 Subnet Mask* – Used to determine if the destination is in the same subnet. The default value is 255.255.255.0. Enter the IPv4 subnet mask address if you are using IPv4 to connect to the network in Manual mode. In PPPoE and DHCP modes, the IPv4 subnet mask address is assigned automatically.
   d. *IPv4 Default Gateway* – Used to forward frames to destinations in a different subnet. An invalid gateway setting causes transmission to destinations in other subnets to fail. Enter the IPv4 default gateway address if you are using IPv4 to connect to the network in Manual mode. In PPPoE and DHCP modes, the IPv4 default gateway address is assigned automatically.
   e. *IPv6 Enable* – If you are using IPv6, select the checkbox to enable IPv6.
   f. *Accept IPv6 Router Advertisement* – If you are using IPv6, select *ON*. The default is *OFF*.
   g. *Enable DHCPv6* – If you are using IPv6, select *ON*. The default is *OFF*.
   h. *IPv6 Address* – If you are using IPv6, enter the IPv6 address.
   i. *Subnet Prefix Length* – If you are using IPv6, enter the subnet prefix length (1-128 digits).
   j. *IPv6 Default Router Address* – If you are using IPv6, enter the IPv6 default router address.
   k. *Subnet Prefix Length* – If you are using IPv6, enter the subnet prefix length (1-128 digits) for the IPv6 Default Router Address.
   l. *IPv6 DNS* – If you are using IPv6, enter the IPv6 DNS address.

To configure the Wire Setting

1. In the *Wire Setting* section, from the *Speed & Duplex* drop-down list, select one of the following:
   - *10 Mbps Half Duplex*
   - *10 Mbps Full Duplex*
   - *100 Mbps Half Duplex*
   - *100 Mbps Full Duplex*
   - *Auto* (default setting)

To enable UPnP settings

1. In the *UPnP* section, from the *Enable UPnP* drop-down list, select *ON*. The default is *ON*. This enables the camera to be detected by any unit on the LAN.
2. From the *Mode* drop-down list, select one of the following:
   - *IP and Device Name* – The camera connects to the UPnP server by using its IP address and default device name. This is the default setting.
   - *Device Name* – The camera connects to the UPnP server by using the default camera name.
   - *User Input* – The camera connects to the UPnP server by using a friendly name. Enter the name in the *Friendly Name* text box that opens when this option is selected:



UPnP User Input Screen

To enable SSL

1. In the *SSL* section, from the *Enable SSL* drop-down list, select *ON*. The default is *OFF*.

Note:

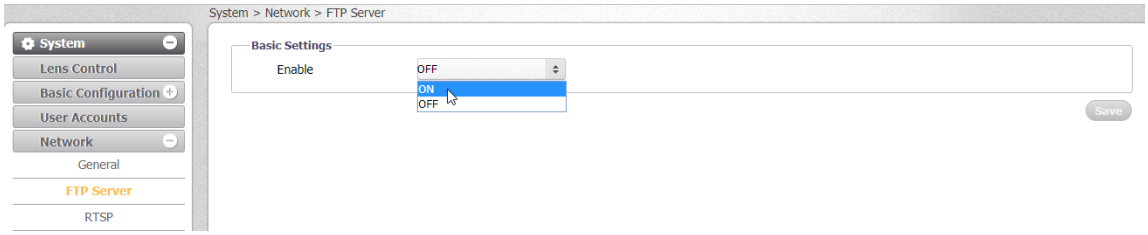
You must install or generate an SSL certificate before enabling SSL.

5.3.1.4.2 FTP Server

The camera includes a built-in FTP server which enables remote access to files of events that are captured in snapshots or recorded on clips and are stored on the camera's microSD card. The **FTP Server** screen is used to enable remote access of the camera's microSD card. No configuration of the camera's internal FTP server is required by the user. The camera's IP address is ftp://<camera IP address>.

To access the FTP server

1. From the *Enable* drop-down list, select *ON*. The default is *OFF*.



Network > FTP Screen

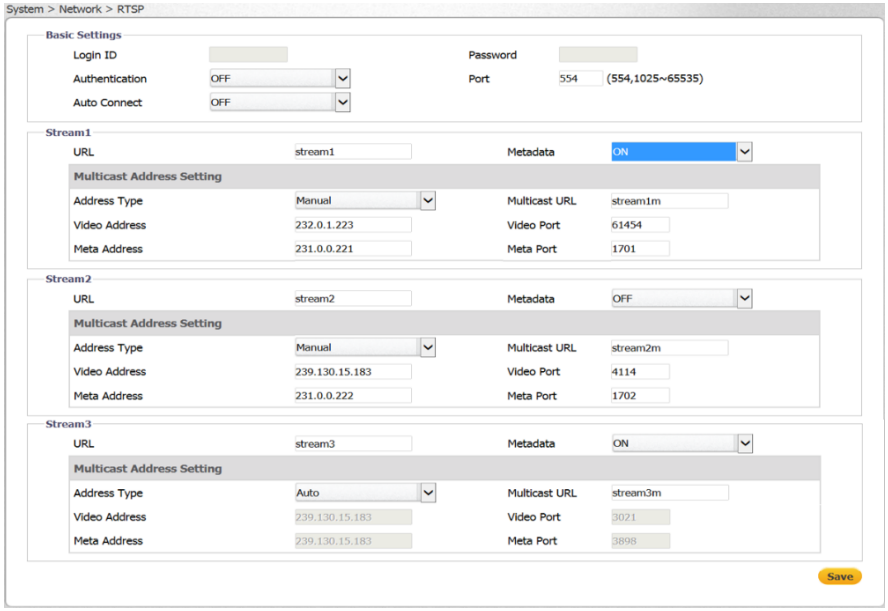
2. Click **Save**.

Note:

Even when set to *Off*, recordings and snapshots will still be stored in the camera's microSD card. However, the user will not be able to remotely access them via FTP.

5.3.1.4.3 RTSP

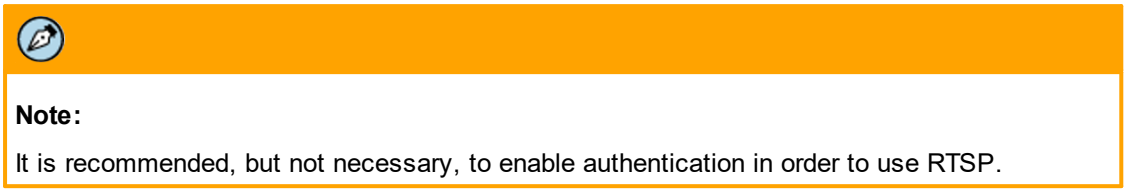
The **RTSP** screen is used for transmitting the encoded video stream. The RTSP protocol is used for establishing the connection and controlling the streaming data between the camera and a device over the web. Each stream can be sent by unicast to one device or broadcasted by multicast to multiple devices. Unicast requires larger network bandwidth and more server resources, but is more stable than multicast, which requires more settings.



Network > RTSP Screen

To configure basic settings

1. In the *Login ID* text box, enter your Login ID number.



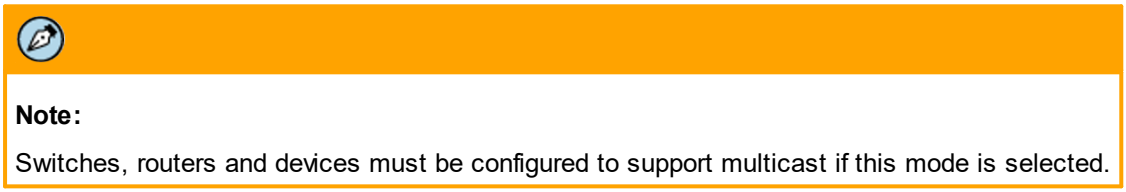
Note:

It is recommended, but not necessary, to enable authentication in order to use RTSP.

2. From the Authentication drop-down list, select *ON* to encrypt the transmission. The default is *OFF*.
3. In the *Password* text box, enter your password after selecting Authentication *ON*.
4. In the *Port* text box, enter the RTSP network port. The default is *554*. The range is *1025* to *65535*.
5. From the *Auto Connect* drop-down list, select *ON* or *OFF*. The default is *OFF*.

To configure the multicast address

1. In the *Stream1* section, in the URL text box, enter the RTSP server's URL. The default is *stream1*.
2. From the *Metadata* drop-down list, select *ON* or *OFF*. The default is *OFF*.
3. From the *Address Type* drop-down list, select *Manual or Auto*. The default is *Auto*.
4. In the *Multicast URL* text box, enter the multicast URL. The default is *stream1m*. Valid multicast addresses are in the range *224.0.1.1 – 239.255.255.254*.



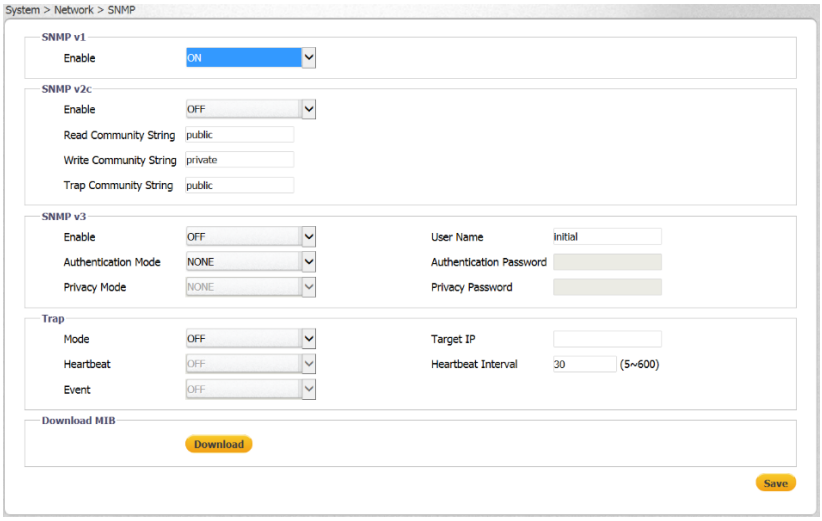
Note:

Switches, routers and devices must be configured to support multicast if this mode is selected.

5. In the *Video Address* text box, enter the IP address for the RTSP server.
6. In the *Video Port* text box, enter the network port number for communicating with the RTSP server.
7. In the *Meta Address* text box, enter the IP address to which the metadata is sent.
8. In the *Meta Port* text box, enter the network port number for transmitting the metadata.
9. If you are using the second or third stream, in the *Stream2* or *Stream3* section, repeat the above steps.
10. Click **Save**.

5.3.1.4.4 SNMP

The **SNMP** screen enables the network management system to use the Simple Network Management Protocol (SNMP) to remotely monitor and manage the camera. Select one of the following SNMP versions: SNMP v1, SNMP v2c, or SNMP v3.



Network > SNMP Screen

To use SNMP v1

1. From the *SNMP v1* section's *Enable* drop-down list, select *ON*. The default is *OFF*.
2. Click **Save**.

To use SNMP v2c

1. From the *SNMP v2c* section's *Enable* drop-down list, select *ON*. The default is *OFF*.
2. In the *Read Community String* text box, enter the community name that has read-only access to all supported SNMP objects. The default value is *public.*
3. In the *Write Community String* text box, enter the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is *private.*
4. In the *Trap Community String* text box, enter 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.
5. Click **Save**.

To use SNMP v3

1. From the *SNMP v3* section's *Enable* drop-down list, select *ON*. The default is *OFF*.
2. From the *Authentication Mode* drop-down list, select *MD5, SHA,* or *NONE* (default).
3. If you select *MD5* or *SHA*, from the *Privacy Mode* drop-down list, select *AES, DES,* or *NONE* (default).
4. Enter the User Name. The default is *initial*.
5. If you select *MD5* or *SHA*, enter the Authentication Password in the *Authentication Password* text box.
6. The *Privacy Password* text box is disabled.
7. Click **Save**.

To use traps

1. In the *Trap* section, from the *Mode* drop-down list, select *V1, V2C, V3,* or *OFF*, according to the SNMP version that you select above. The default is *OFF*.
2. From the *Heartbeat* drop-down list, select *ON* or *OFF*. The default is *OFF*. When selected, this enables you to ping the VMS.
3. From the *Event* drop-down list, select *ON* to notify the VMS in case of an event. The default is *OFF*.
4. In the *Target IP* text box, enter the IP address of the Trap Host.
5. In the *Heartbeat Interval* text box, enter the interval of time in seconds for the camera to ping the VMS, for example, every 10 seconds. The range is *5-600*. The default is *30*.
6. Click **Save**.

To download the SNMP MIB

1. In the *Download MIB* section, click **Download**. The database used for managing the entities in the communications network is downloaded.

5.3.1.4.5 802.1X

The **802.1X** screen is used for enabling the camera to access a network protected by the 802.1X/EAPOL (Extensible Authentication Protocol over LAN) authentication protocol. Before using this function, 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 802.1X

1. From the *Protocol* drop-down list, select one of the following: *EAP-MD5, EAP-TTLS, MD5-PEAP,* or *NONE*. The default is *NONE*.

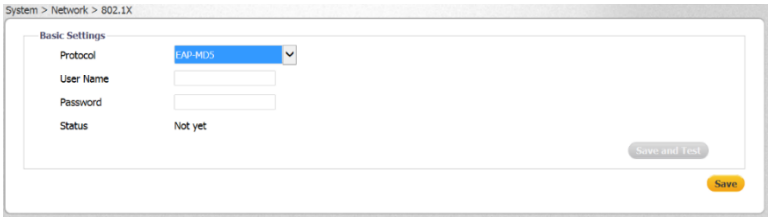


Network > 802.1X Screen

2. Click **Save**. The **Basic Settings** screen for the selected protocol opens.

To enable EAP-MD5

1. Select *EAP-MD5*. The **Basic Settings** screen opens.

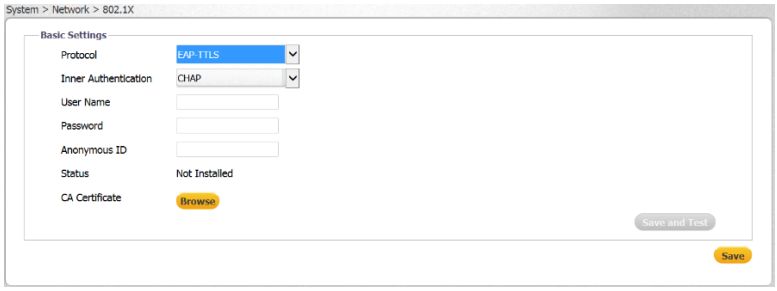


EAP-MD5 Screen

2. Enter the User Name and Password in the respective text box.
3. Do one of the following:
   - Click **Save**. The status is displayed as “Not yet” until the configuration is saved.
   - Click **Test and Save** to test and save the configuration.

To enable EAP-TTLS

1. Select *EAP-TTLS*. The **Basic Settings** screen opens.

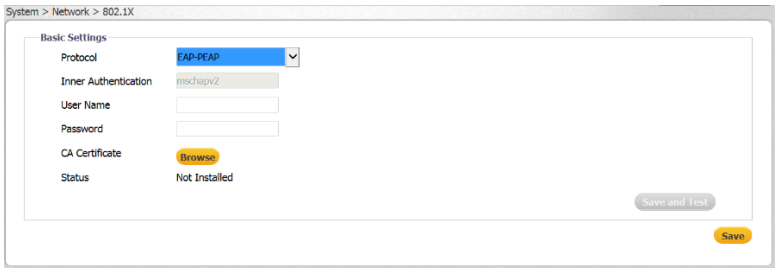


EAP-TTLS Screen

2. From the *Inner Authentication* drop-down list, select one of the following protocols: *CHAP, EAP-MSCHAPV2, MD5, MSCHAP, MSCHAPV2,* or *PAP*.
3. Enter the User Name and Password in the respective text box.
4. Enter the Anonymous ID in the *Anonymous ID* text box.
5. Click **Browse** to download the CA Certificate. The Status is displayed as “Not Installed” until the CA certificate is downloaded.
6. Do one of the following:
   - Click **Save**. The status is displayed as “Not Installed” until the configuration is saved.
   - Click **Test and Save** to test and save the configuration.

To enable EAP-PEAP

1. Select *EAP-PEAP*. The **Basic Settings** screen opens. By default the Inner Authentication protocol is MSCHAPV2.



EAP-PEAP Screen

2. Enter the User Name and Password in the respective text box.
3. Click **Browse** to download the CA Certificate.
4. Do one of the following:
   - Click **Save**. The status is displayed as “Not Installed” until the configuration is saved.
   - Click **Test and Save** to test and save the configuration.

5.3.1.4.6 IP Filter

The **IP Filter** screen is used for restricting access to the camera by allowing or denying specific IP addresses. It is possible to filter up to 10 IP addresses. The options are *Allow, Deny,* or *NONE* (default).



Network > IP Filter Screen

To allow an IP address

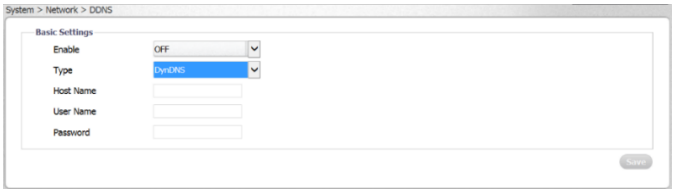
1. From the *Filter* drop-down list, select *Allow.*
2. Check the *Enable* checkbox for each IP address for which you want to allow access.
3. Enter the IP address in the *Address* text box.
4. Click **Save**.

To deny an IP address

1. From the *Filter* drop-down list, select *Deny.*
2. Check the *Enable* checkbox for each IP address for which you want to deny access.
3. Enter the IP address in the *Address* text box.
4. Click **Save**.

5.3.1.4.7 DDNS

The DDNS (Dynamic DNS) screen is used for network access if you select PPPoE as the default network connection. Before configuring the system to use DDNS, you must first register with a DDNS service provider.



Network > DDNS Screen

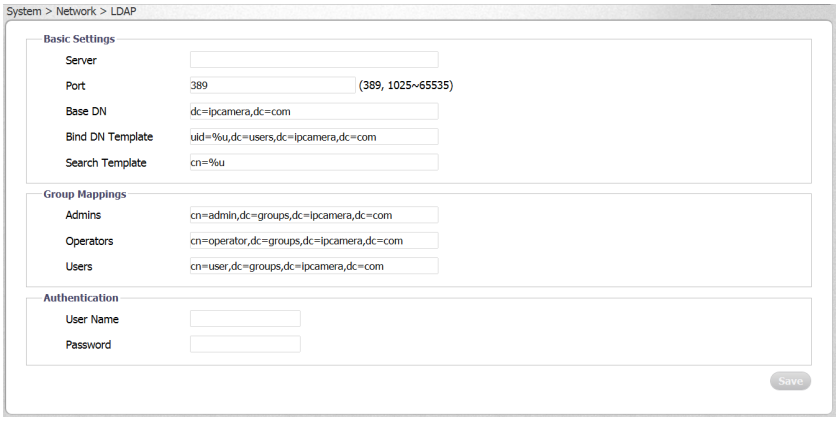
To use DDNS

1. From the *Enable* drop-down list, select ON. The default is *OFF*.
2. From the *Type* drop-down list, select the DDNS service provider:
   - DynDNS: custom@dyndns.org (default)
   - No-IP: default@no-ip.com
   - Two-DNS: default@two-dns.de
   - FreeDNS: default@freedns.afraid.org
3. Enter the Host Name, User Name, and Password in the respective text box.

4. If you are using FreeDNS, the *Hash* text box also is displayed. Enter the Hash value, which is a hash of your user name and password. It is available from http://freedns.afraid.org.
5. Click **Save**.

5.3.1.4.8 LDAP

The **LDAP** screen is used for configuring use of the Lightweight Directory Access Protocol, an industry-standard protocol for accessing and maintaining distributed directory information services over an IP network.



Network > LDAP Screen

To configure LDAP basic settings

1. In the *Server* text box, enter the LDAP server address.
2. In the *Port* text box, enter the network port number of the LDAP server. The range is *1025* to *65535*. The default is *389*.
3. In the *Base DN* text box, enter or edit the default Distinguished Name (Domain Components) of the parent entry. This is used for searching the directory tree in the LDAP server. The default setting is *dc=ipcamera,dc=com*.
4. In the *Bind DN Template* text box, enter or edit the attributes used for authenticating the camera on the LDAP server. The default setting is *uid=%u,dc=users,dc=ipcamera,dc=com*.
5. In the *Search Template* text box, enter or edit the attribute used for the Common Name. The default is *cn=%u*.

To configure group mappings

1. In the *Admins* text box, enter or edit the attributes used for searching for an Administrator.
2. In the *Operators* text box, enter or edit the attributes used for searching for an Operator.
3. In the *Users* text box, enter or edit the attributes used for searching for a User.

To configure authentication settings

1. Enter the User Name and Password in the respective text boxes to access the LDAP server.
2. Click **Save**.

5.3.1.4.9 SSL

The **SSL** screen is used for configuring the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocol, which protects camera settings and username/password information. SSL/TLS is used, in turn, by the HTTPS protocol for allowing secure IP connections between the camera and a web browser over HTTP.

Note:

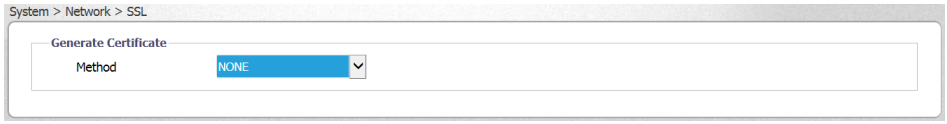
SSL is enabled from the Network > General screen.

In order 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 Certificate Authority (CA) or by creating a self-signed HTTPS certificate as described below.

Note:
The self-signed certificate does not provide the same level of security as a CA-issued certificate.

To configure SSL settings

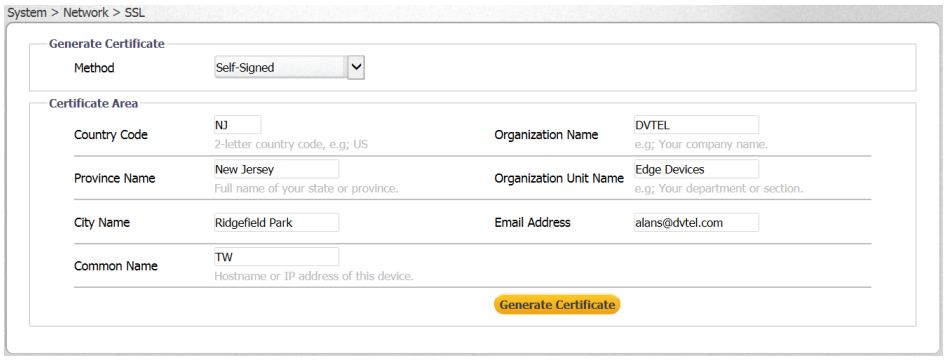
1. From the *Method* drop-down list, select one of the following: *Self-Signed, Request,* or *Upload Certificate.* The default is *NONE.*



Network > SSL Screen

To obtain a self-signed certificate

1. From the *Method* drop-down list, select *Self-Signed.* The **Self-Signed** screen is displayed.



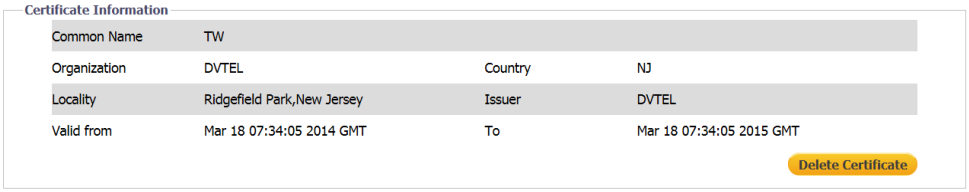
SSL Self-Signed Screen

2. Enter the following information in the appropriate field. A definition of each of the required fields follows.

   - *Country Code* – Enter a two-letter combination code to indicate the specific country in which the certificate will be used. For instance, type “US” to indicate United States.

- *Province Name* – Enter the local administrative region.
- *City Name* – Enter other geographical information.
- *Common Name* – Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).
- *Organization Name* – Enter the name of the organization to which the entity identified in *Common Name* belongs.
- *Organization Unit Name* – Enter the name of the organizational unit to which the entity identified in the *Common Name* field belongs.
- *Email Address* – Enter the email address of the person responsible for maintaining the certificate.

3. Click **Generate Certificate** to save the certificate request after completion. The details are displayed in the Certificate Information section that opens on the **SSL** screen.

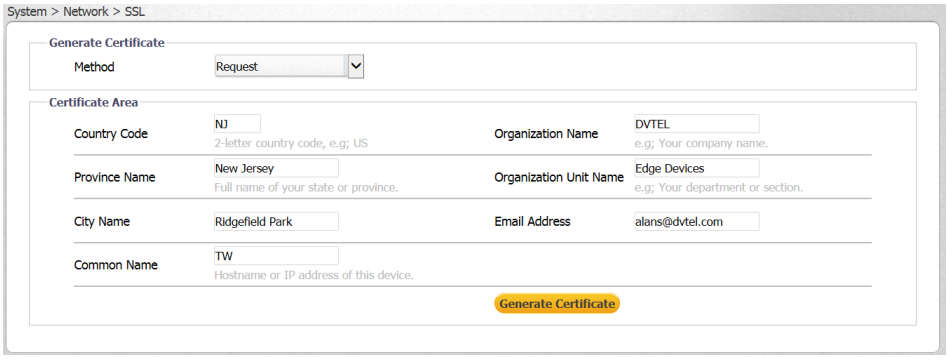


SSL Certificate Information Section

4. To delete the certificate, click **Delete Certificate**. The certificate is deleted.

To request a certificate

1. From the *Method* drop-down list, select *Request.* The **Request** screen is displayed.

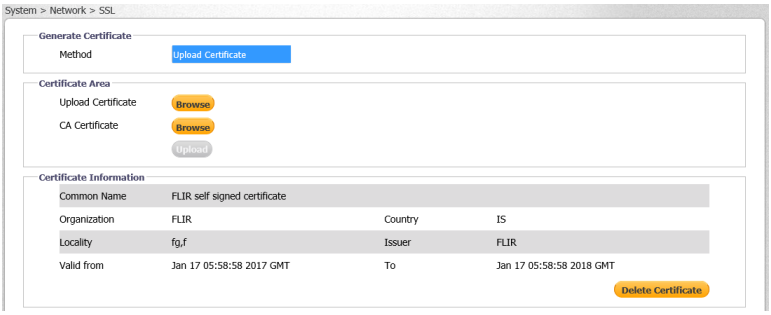


SSL Request Screen

2. Follow steps 2-4 above to obtain a self-signed certificate.

To upload a certificate

1. From the *Method* drop-down list, select *Upload Certificate*. The **Upload Certificate** screen is displayed.



Upload Certificate Screen

2. Do one of the following:
   - To locate and upload a self-signed certificate, click **Upload Certificate > Browse**.
   - To locate and upload a Certificate Authority (CA) certificate, click **CA Certificate > Browse**.
3. Click **Upload**. The certificate is uploaded.

5.3.1.5 Events Source

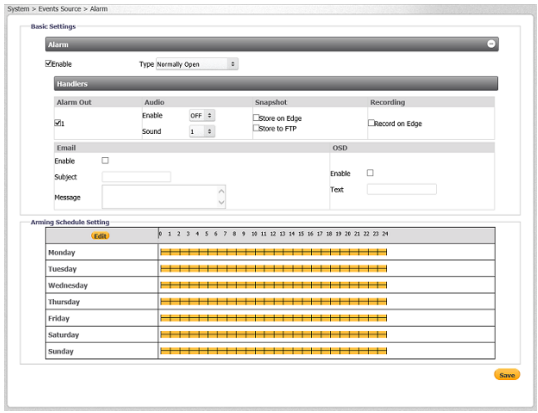
The **Events Source** tab is used for configuring general settings related to event notification. It includes the following screens:

Alarm Audio Motion Network Schedule Tampering Day/Night

5.3.1.5.1 Alarm

The **Events Source > Alarm** screen is used for enabling an alarm when an alarm-in event occurs (dry-contact) and for defining actions when an alarm occurs. Actions include:

- Sending an alarm
- Defining the method for storing a snapshot in the camera's microSD card
- Sending a snapshot of the event to an FTP server
- Recording an event in the camera's microSD card
- Sending email notifications
- Displaying text on-screen if the network connection is there is an alarm
- Setting the arming schedule



Events Source > Alarm Screen

To enable an alarm

1. Select the *Enable* checkbox.
2. Click **Save**.

To select the type of alarm

1. From the *Type* drop-down list, select *Normally Open* or *Normally Closed*.
2. Click **Save**.

To enable the Alarm Out function

1. In the *Handlers* section, select the *Alarm Out* checkbox. By default, it is not checked.
2. Click **Save**.

To enable audio

1. In the *Handlers* section, from the *Audio Enable* drop-down list, select *ON*. By default, it is not checked.
2. From the *Audio Sound* drop-down list, select the number for the audio file that you want to play. See the *Event Handler > Sound* section to load the audio files that are triggered upon occurrence of an event.
3. Click **Save**.

To define the method to store a snapshot

1. In the *Snapshot* section, select the *Store on Edge* checkbox to store a snapshot on the camera's microSD card. By default, it is not checked.
2. In the *Snapshot* section, select the *Store to FTP* checkbox to store a snapshot on a remote FTP site. By default, it is not checked.

To record an event

1. In the *Recording* section, select the *Record on Edge* checkbox to record a clip on the camera's microSD card. By default, it is not checked.
2. Click **Save**.

To send email notifications

1. In the *Email* section, select the *Enable* checkbox. By default, *Enable* is not checked.
2. In the *Subject* text box, enter the email subject text.
3. In the *Message* text box, enter the email message text.

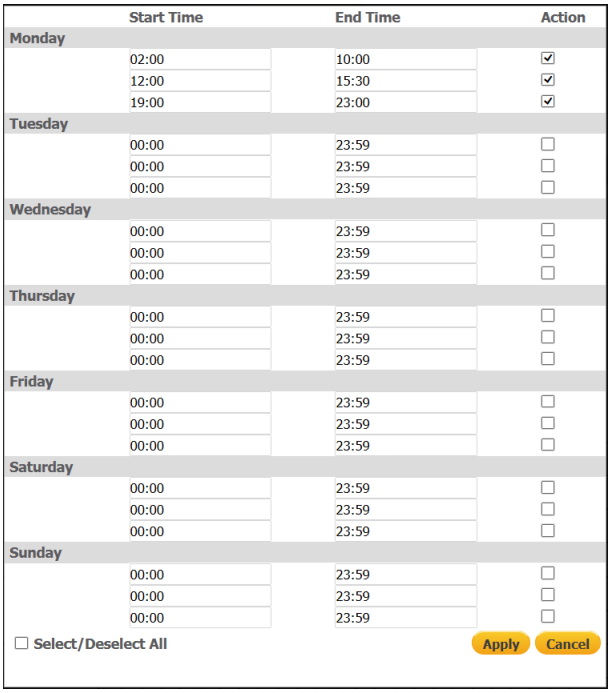
4. Click **Save**.

To activate the on-screen display

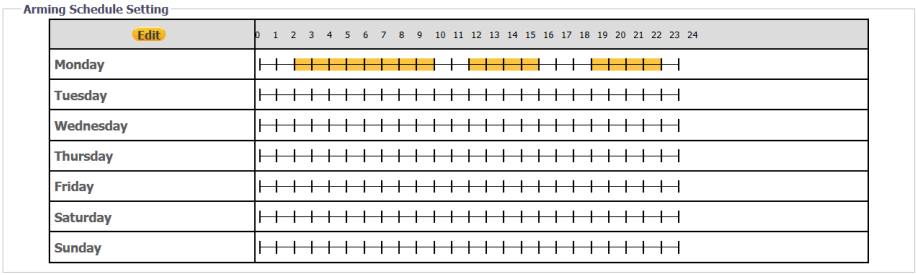
1. In the *OSD* section, select *Enable*. By default, *Enable* is not checked.
2. In the *Text* text box, enter the text to display in the on-screen display.
3. Click **Save**.

To set the arming schedule

1. In the *Arming Schedule Setting* area, click **Edit**. The **Edit** screen opens.



2. In the *Start Time* column, enter the time(s) and day(s) you want to trigger an action.
3. In the *End Time* column, enter the time(s) and day(s) you want to stop the action.
4. Select the *Action* checkbox if you want to enable the action at these times.
5. Select the *Select/Deselect All* checkbox as required.
6. Click **Apply**. The times for the schedule are displayed in orange in the *Arming Schedule Setting* section.

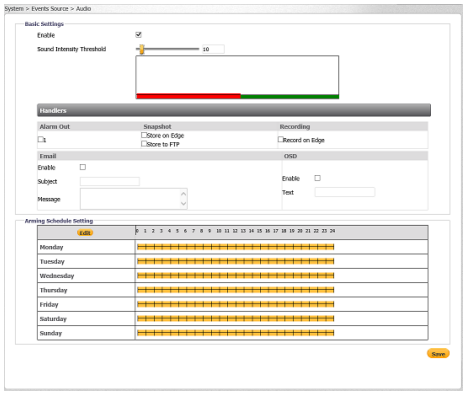


Updated Arming Schedule Setting Section

5.3.1.5.2 Audio

The **Events Source > Audio** screen is used for setting the audio threshold level of the audio input. An audio event is created when the Sound Intensity Threshold is exceeded. Actions include:

- Setting the audio threshold level, which creates an audio event when the Sound Intensity Threshold is exceeded
- Sending an alarm
- Defining the method for storing a snapshot in the camera's microSD card
- Sending a snapshot of the event to an FTP server
- Recording an event in the camera's microSD card
- Sending email notifications
- Displaying text on-screen if there is an audio event
- Setting the arming schedule

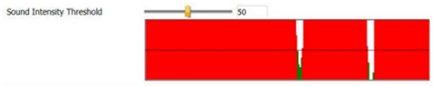


Events Source > Audio Screen

Note:

In order to use this function, audio must be enabled from the System > Basic Configuration > Audio screen.

A graph displays audio when is detected. Audio that is below the Sound Intensity Threshold is displayed in green. When audio exceeds the defined threshold, it creates an audio event and is displayed in red.



Sound Intensity Threshold

Setting a low threshold (for example, 25) means that the camera is more sensitive to noise, which results in more alerts (displayed in red). The setting depends on the situation and environment. If the scene is located in a quiet place, it is possible to use lower threshold. A noisy location requires a higher threshold.

When selecting *Record to Edge*, the recording includes the audio track. *OSD* must be enabled on the **Events Source > Audio** screen, as well as from the System > Basic Configuration > OSD screen, in order to insert on-screen displays on clips and snapshots.

Note:

Recording must be enabled from the System > Events Handler > Recording Settings screen in order to record audio.

To enable audio

1. Select the *Audio* checkbox.
2. Click **Save**.

To set the audio level

1. Move the *Sound Intensity Threshold* slider to the desired level between 1-100. The lower the setting, more sounds that are detected.
2. Click **Save**.

To define the method to store a snapshot

1. See instructions in the Alarm section.

To record an event

1. See instructions in the Alarm section.

To send email notifications

1. See instructions in the Alarm section.

To activate the on-screen display

1. See instructions in the Alarm section.

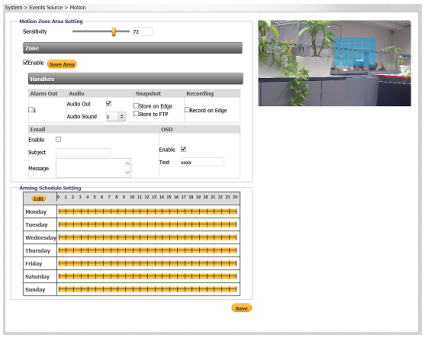
To set the arming schedule

1. See instructions in the Alarm section.

5.3.1.5.3 Motion

The **Events Source > Motion** screen is used for:

- Enabling and defining the motion zone area settings
- Sending an alarm upon a motion event
- Selecting and playing an audio file upon a motion event
- Defining the method for storing a snapshot in the camera's microSD card
- Sending a snapshot of the event to an FTP server
- Recording an event in the camera's microSD card
- Sending email notifications
- Displaying text on-screen upon a motion event
- Setting the arming schedule



Events Source > Motion Screen

Notes:
1. If the camera is attached to Latitude, motion detection configuration should be done from Latitude Admin Center, not from the web interface.
2. If Motion Detection is enabled, Basic Video Analytics is disabled.

To configure motion zone area settings

1. From the *Sensitivity* slider, select *1-100*. The camera reacts to slight changes in motion or brightness in the motion zone when set closer to *100*, while the camera reacts to big changes in brightness or motion when set closer to *1*.

To enable motion settings

1. In the *Zone* section, click *Enable*. By default, *Enable* is not checked.
2. Set the motion detection area by left-clicking the screen and dragging the cursor over the area. Right-click the detection area to delete the area.
3. Click **Save Area**.

Note: The camera can only support either motion detection or analytics at a single time, but not both at the same time.

To enable the Alarm Out function

1. See instructions in the Alarm section.

To enable the Audio Out function

1. In the *Handlers* section, select the *Audio Out* checkbox. By default, it is not checked.
2. From the *Audio Sound* drop-down list, select the number for the audio file that you want to play. See the *Event Handler > Sound* section to load the audio files that are triggered upon occurrence of an event.
3. Click **Save**.

To define the method to store a snapshot

1. See instructions in the Alarm section.

To record an event

1. See instructions in the Alarm section.

To send email notifications

1. See instructions in the Alarm section.

To activate the on-screen display

1. See instructions in the Alarm section.

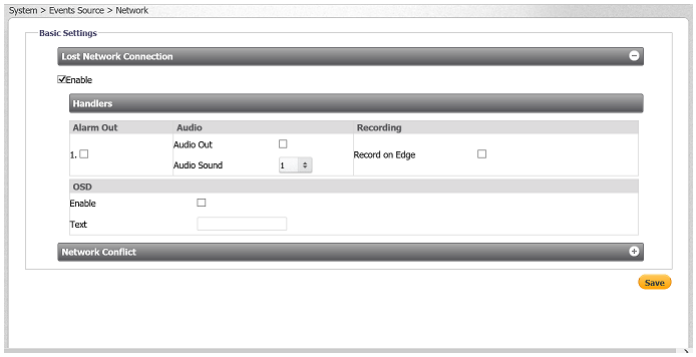
To set the arming schedule

1. See instructions in the Alarm section.

5.3.1.5.4 Network

The **Events Source > Network** screen is used for enabling notification in case the network connection is lost or if there is another device on the network that is using the same IP address as the camera. This screen enables you to:

- Send an alarm
- Select and play an audio file upon the occurrence of an event
- Record an event in the camera's microSD card
- Display text on-screen if the network connection is lost or if there is a network conflict



Events Source > Network Screen

To enable notifications

1. Select *Enable*. By default, *Enable* is not checked.
2. Click **Save**.

To enable the Alarm Out function

1. See instructions in the Alarm section.

To enable the Audio Out function

1. In the *Handlers* section, select the *Audio Out* checkbox. By default, it is not checked.
2. From the *Audio Sound* drop-down list, select the number for the audio file that you want to play. See the *Event Handler > Sound* section to load the audio files that are triggered upon occurrence of an event.
3. Click **Save**.

To record an event

1. See instructions in the Alarm section.

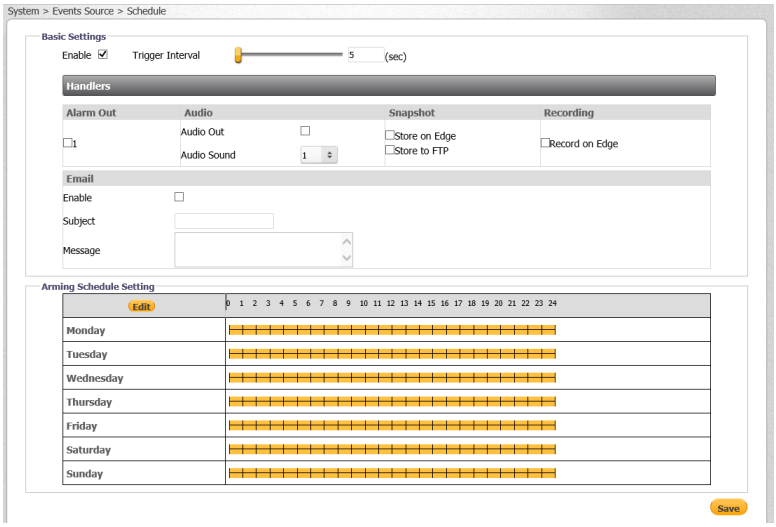
To activate the on-screen display

1. See instructions in the Alarm section.

5.3.1.5.5 Schedule

The **Events Source > Schedule** screen is used for:

- Setting a trigger interval for notifications
- Sending an alarm
- Selecting and playing an audio file upon the occurrence of an event
- Defining the method for storing a snapshot in the camera's microSD card
- Sending a snapshot of the event to an FTP server
- Recording an event in the camera's microSD card
- Sending email notifications
- Setting the alarm schedule



Events Source > Schedule Screen

To set a trigger interval

1. Select *Enable*. By default, *Enable* is not checked.
2. Move the *Trigger Interval* slider from *1* to *3600* seconds. The default setting is *10* seconds.

To enable the Alarm Out function

1. See instructions in the Alarm section.

To enable the Audio Out function

1. In the *Handlers* section, select the *Audio Out* checkbox. By default, it is not checked.
2. From the *Audio Sound* drop-down list, select the number for the audio file that you want to play. See the *Event Handler > Sound* section to load the audio files that are triggered upon occurrence of an event.
3. Click **Save**.

To define the method to store a snapshot

1. See instructions in the Alarm section.

To record an event

1. See instructions in the Alarm section.

To send email notifications

1. See instructions in the Alarm section.

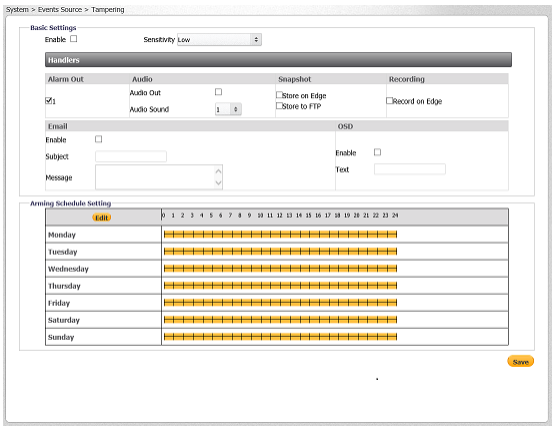
To set the arming schedule

1. See instructions in the Alarm section.

5.3.1.5.6 Tampering

The **Events Source > Tampering** screen enables you to:

- Enable and define tampering settings
- Send an alarm upon a tampering event
- Select and play an audio file upon a tampering event
- Define the method for storing a snapshot in the camera's microSD card
- Send a snapshot of the event to an FTP server
- Record an event in the camera's microSD card
- Send email notifications
- Display text on-screen if there is a tampering event
- Set the alarm schedule



Events Source > Tampering Screen

To enable tamper detection

1. Select *Enable*. (Default: Enabled).
2. From the *Sensitivity* drop-down list, select *High, Medium,* or *Low (Default: Low)*.

To enable the Alarm Out function

1. See instructions in the Alarm section.

To enable the Audio Out function

1. In the *Handlers* section, select the *Audio Out* checkbox. By default, it is not checked.
2. From the *Audio Sound* drop-down list, select the number for the audio file that you want to play. See the *Event Handler > Sound* section to load the audio files that are triggered upon occurrence of an event.
3. Click **Save**.

To define the method to store a snapshot

1. See instructions in the Alarm section.

To record an event

1. See instructions in the Alarm section.

To send email notifications

1. See instructions in the Alarm section.

To activate the on-screen display

1. See instructions in the Alarm section.

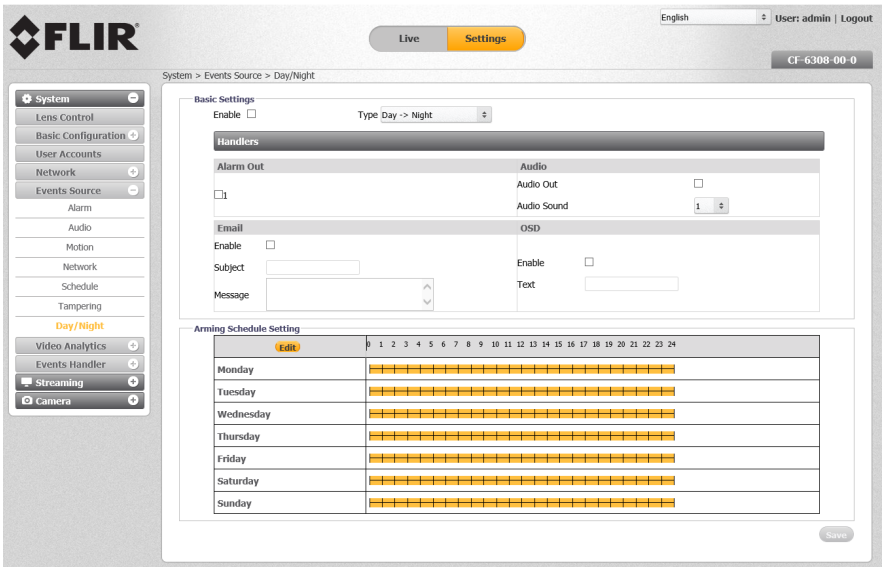
To set the arming schedule

1. See instructions in the Alarm section.

5.3.1.5.7 Day/Night

The **Events Source > Day/Night** screen enables you to:

- Enable and define Day/Night settings
- Send an alarm upon a Day/Night event
- Select and play an audio file upon a Day/Night event
- Send email notifications
- Display text on-screen if there is a Day/Night event
- Set the alarm schedule



Events Source > Day/Night Screen

To enable Day/Night detection

1. Select *Enable*. By default, *Enable* is not checked.
2. From the *Type* drop-down list, select *Day -> Night, Night -> Day or Day <-> Night*
   a. *Day -> Night* = Configured event triggers when camera detects change from daytime to nighttime.
   b. *Night -> Day* = Configured event triggers when camera detects change from nighttime to daytime.
   c. *Day <-> Night* = Configured event triggers when camera detects change from both daytime to night and nighttime to daytime

To enable the Alarm Out function

1. See instructions in the Alarm section.

To enable the Audio Out function

1. In the *Handlers* section, select the *Audio Out* checkbox. By default, it is not checked.
2. From the *Audio Sound* drop-down list, select the number for the audio file that you want to play. See the *Event Handler > Sound* section to load the audio files that are triggered upon occurrence of an event.
3. Click **Save**.

To send email notifications

1. See instructions in the Alarm section.

To activate the on-screen display

1. See instructions in the Alarm section.

To set the arming schedule

1. See instructions in the Alarm section.

5.3.1.6 Events Handler

The **Events Handler** tab is used for configuring settings for the various methods used for event notification. The tab includes the following screens:

Email | Alarm Out | FTP | Recording Settings | SD Card | Snapshot | Sound

5.3.1.6.1 Email

It is possible to send notifications to up to 10 email addresses.

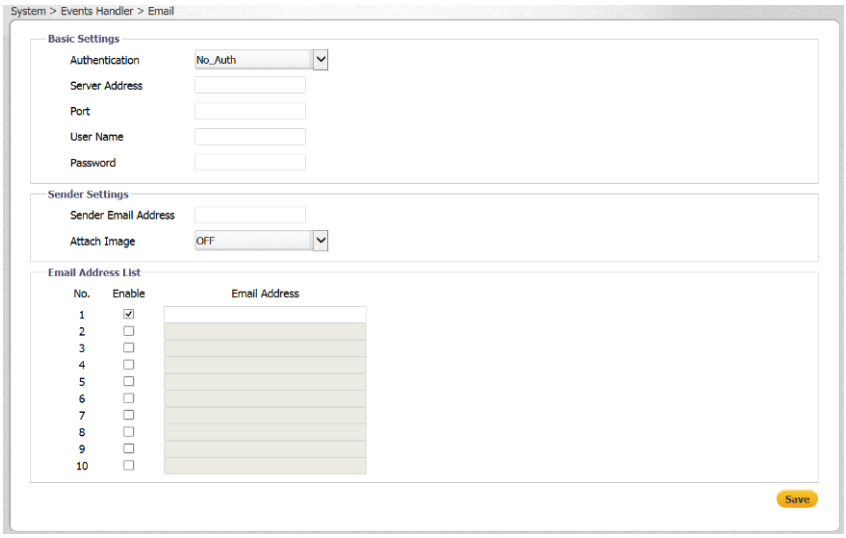
Note:

Before configuring email settings, check that:

- There is an SMTP mail server on the local area network (LAN).
- The network is connected to either an intranet or the Internet.
- TCP/IP settings, including DNS Server settings, are configured in the **Network > General** screen.

To configure email settings

1. Select the **Email** tab. The **Email** screen is displayed.



Events Handler > Email Screen

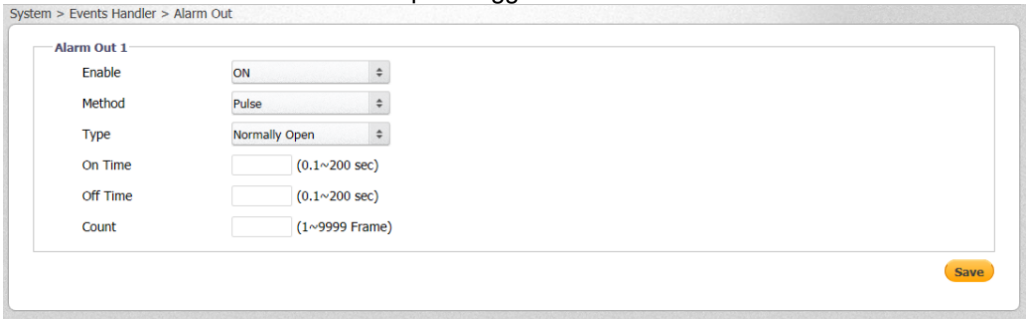
2. In the *Basic Settings* area, configure the following settings:
    a. *Authentication* – From the drop-down list, select one of the following authentication methods:
        - *No_Auth* – No email authentication method is used. This is the default setting.
        - *SMTP Plain* – PLAIN is the least secure of all the SASL (Simple Authentication and Security Layer) authentication mechanisms because the password is sent unencrypted across the network. The PLAIN authentication mechanism is described in RFC 2595.
        - *Login* – The Login mechanism is supported by Microsoft's Outlook Express and by some other clients.
        - *TLS-TTLS* – The Tunneled Transport Layer Security is used to tunnel an entire network stack to create a VPN.
    b. *Server Address* – In the text box, enter the email server IP address.
    c. *Port* – In the text box, enter the email server port number. The default port is *25*.
    d. *User Name* – In the text box, enter the email server user name.
    e. *Password* – In the text box, enter the email server password.
3. In the *Sender Settings* area, configure the following settings:
    a. *Sender Email Address* – In the text box, enter the sender's email address.
    b. *Attach Image* – From the drop-down list, select *ON* or *OFF* (default setting).
4. In the *Email Address List* section, do the following for each email address:
    a. Select the checkbox in the *Enable* column. By default, *Enable* is not checked.
    b. Enter the email address in the *Email Address* column.
    c. Click **Save**.

5.3.1.6.2 Alarm Out

The **Alarm Out** screen is used for configuring settings for the camera's single alarm output.

There are two methods for enabling Alarm Out:

- *Pulse* – When this is selected, the user can select the Type *Normally Open* or *Normally Closed.*
    - When *Normally Open* is selected, new text boxes are displayed in which the user can specify the following:
        - *On Time* – amount of time (in seconds) that the alarm is ON
        - *Off Time* – amount of time (in seconds) between ON states
        - *Count* – the number of frames for the post-trigger buffer



    - When *Normally Closed* is selected, these text boxes are not displayed, the alarm output is activated for the specified duration (*On Time*) during which the output opens. The same settings are displayed as on the *Normally Open* setting.

- *Normal* – When this is selected, a new field (*Post Duration*) is displayed. The Post Duration time determines the length of time that the alarm is triggered. It can be set to Infinite (the alarm is active until deactivated) or set to 5, 10, 15, or 30 seconds.



5.3.1.6.3 FTP

The **FTP** screen is used for configuring the settings of an FTP server located remotely on the network. The server is used for saving snapshots of events that are configured from the Events Source section and transmitted from the camera via FTP to the remote FTP server.



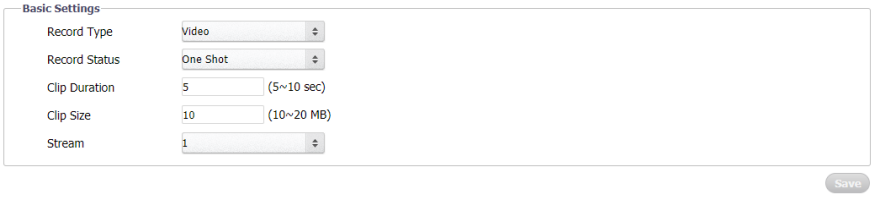
Events Handler > FTP Screen

To configure FTP server settings

1. In the *Server Address* text box, enter the FTP server IP address.
2. In the *Port* text box, enter the email server port number.
3. In the *User Name* text box, enter the FTP server user name.
4. In the *Password* text box, enter the FTP server manager's password.
5. From the *Mode* drop-down list, select *Active* or *Passive* (default setting). In passive mode, FTP 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 FTP 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 random port specified by server)
    - FTP server's ports > 1023 to remote ports > 1023 (server sends ACKs and data to client's data port)
6. Click **Save**.

5.3.1.6.4 Recording Settings

The **Recording Settings** screen is used to configure recording settings.



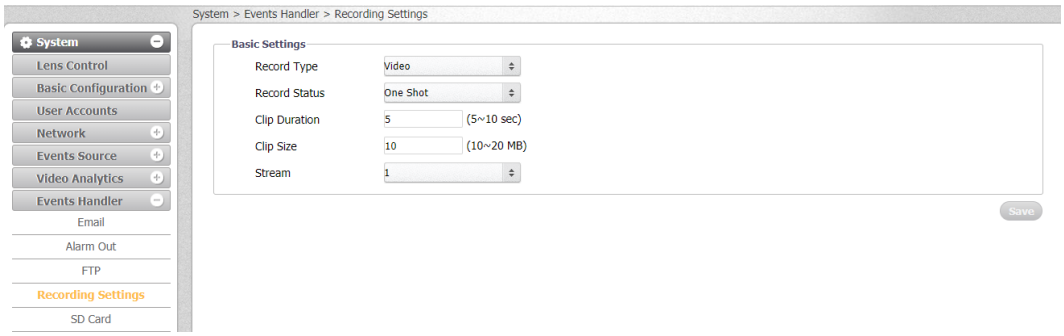
Events Handler > Recording Settings > One Shot Screen

Note:

In order to record, at least one stream must be set to *H.264*.

To configure recording settings

1. From the *Record Status* drop-down list, select *Video* or *Audio and Video*.
2. From the *Record Status* drop-down list, select *One Shot* (default) or *Continuous*.
   - If you select *One Shot*, do the following:
     a. In the *Clip Duration* text box, enter a value from *5* to *10* seconds.
     b. In the *Clip Size* text box, enter a value from *10* to *20* MB.
   - If you select Continuous, In the *Clip Size* text box, enter a value from *10* to *20* MB.
   - You can select which stream to record (out of the available streams.)



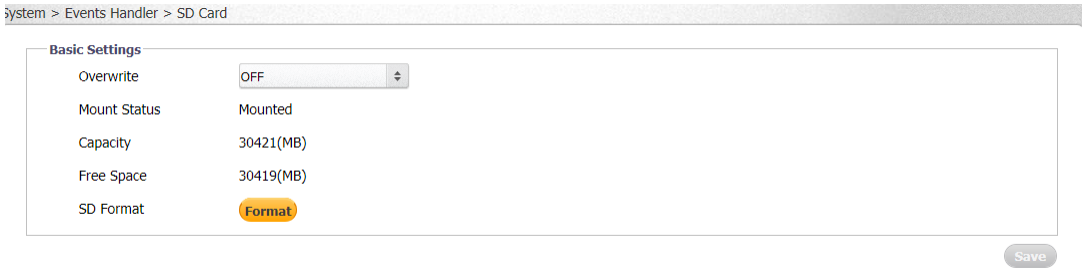
Events Handler > Recording Settings > Continuous Screen

3. Click **Save**.

5.3.1.6.5 SD Card

If the user wishes to store video clips and/or snapshots locally, an microSD card (Min 4GB, max 128GB, formatted as a single partition) must be provided. (Not supplied with the camera.)

The **SD Card** screen is used for configuring the microSD card. The card status is displayed in the *Mount Status* row. The status is displayed as *mounted* if the microSD card is installed and *not_mounted* if the card is not installed.



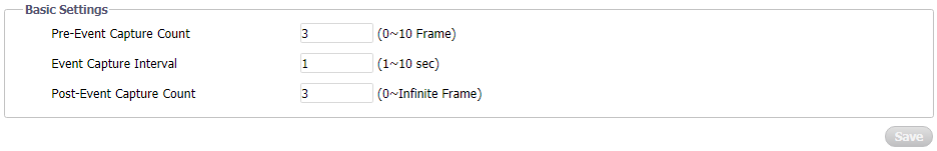
Events Handler > SD Card Screen

To configure the microSD card

1. Before use, the SD card must be formatted.
   Click the **Format** button.
   Note: It is required that the card is formatted as a single partition.
2. From the *Overwrite* drop-down list, select *ON*. The default is *ON*.
3. Click **Save**.

5.3.1.6.6 Snapshot

The **Snapshot** screen is used for configuring snapshot settings.



Events Handler > Snapshot Screen

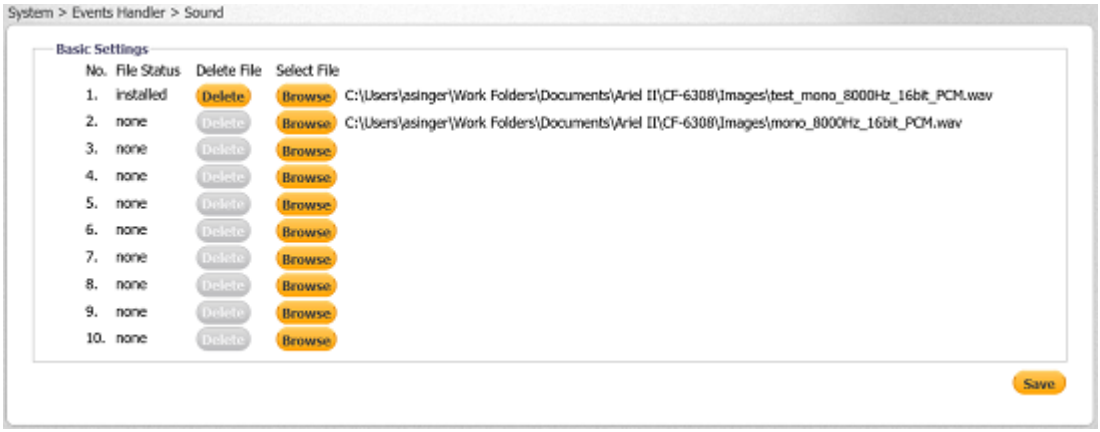
To configure snapshot settings

1. In the *Pre-Event Capture Count* text box, enter the number of frames (0 to *10*) to capture before taking a snapshot of an event. The default is *3* frames.
2. In the *Event Capture Interval* text box, enter the time interval (1 to *10* seconds) to capture between snapshots. The default is *1* frame.
3. In the *Post-Event Capture Count* text box, enter the number of frames (0~Infinite Frame) to capture after taking a snapshot. The default is *3* frames.
4. Click **Save**.

5.3.1.6.7 Sound

The sound screen enables you to upload up to 10 small PCM audio files. These sound files can be triggered upon any event that is set in the Events Source section. For example, you can trigger one warning recording that alerts an intruder that he has been detected and then a stronger warning to not to

proceed if he has not left the scene. The file will be played when the audio is enabled on the Sound screen and the triggering event occurs.



Sound Screen

5.3.1.6.8 Basic Video Analytics

The **Basic Video Analytics** tab is used for configuring settings related to this functionality.

The CF-6308 camera offers a wide variety of analytic rules that can be used in various ways. The selected rule should be appropriate for the physical scene and the main objective in securing the area.

Note: Each camera being used with this feature must have its own **Basic Video Analytics Camera License** downloaded to it.

Rule	Purpose	Usage	Example
Counting	Count the number of people crossing a line	Up to three separate lines working in concert. *Note: The camera should be mounted looking down at the line (at 90 degrees)*	Monitoring customers entering a store
Border Line	Detect people or vehicles crossing a line	Up to three separate lines working in concert	Intrusion detection along a fence
Loitering	Detect encroachment and trespassing based on the time spent in the scene	A single defined area	Monitoring an ATM or outside an apartment building
Area Protection	Detect people or vehicles coming into or going out of the scene	A single defined area	Secure a courtyard from trespassing or a no parking area
Object Removed	Detect objects being removed from the scene	Up to three defined zones	Monitoring shoplifting

Rule	Purpose	Usage	Example
Object Dropped	Detect objects being introduced to the scene	A single defined area	Securing public areas, such as transportation hubs, against suspicious objects

The following topics are covered below:

- **General Guidelines**
  - Camera Distribution
  - Camera Positioning
  - Detection Ranges
  - Mounting and Lighting
- Basic Video Analytics Camera License
- **Initial Settings**
- **Rule-based Settings**
  - Counting
  - Border Line
  - Loitering
  - Area Protection
  - Object Removal
  - Object Dropped
- **Advanced Options**
- **Analytics Actions**
  - Analytics Troubleshooting

5.3.1.6.8.1 Initial Settings

If setting up **Basic Video Analytics** for the first time, see Basic Video Analytics Camera License, Providing cameras with Basic Video Analytics Licenses

The setup for the Analytics Rules follow the same general setup sequence for all Rules. Each Rule has specific configurations that are described in detail in each relevant section.

Notes:

1. It is important that the camera is properly positioned to allow an adequate Field of View.
2. All Rules are directional. A rule's direction is indicated in the Setup screen.
3. Only **one** rule may be active at a time.

General Setup

1. The **first time** a user starts configuring the Analytics pages, the Initial Settings page must be completed. This configures the **minimum** and **maximum** object sizes to be detected in a scene.
2. The user will then draw desired lines or zones depending on the specific rule.
3. Each rule's "basic" page will vary depending on the required settings.
4. The Advanced Options section is used to change **Sensitivity**, create exclusive **Masks** and set an **Arming Schedule**.
5. The final step is to choose the Analytic Action to be trigger when a rule is activated.

Note: This section appears on every Analytic rules page and is linked between all rule. i.e. setting and changing this setting for any rule, will update those settings to all rules.

The setup process includes two simple steps:

- Setting the minimum object size to be detected in the scene
- Setting the maximum object size to be detected.

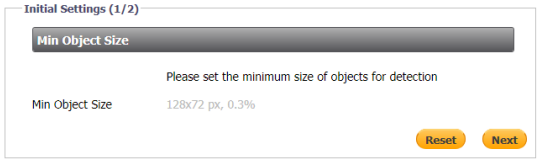
It doesn't matter where the markers are placed in the scene, but it is important that they reflect potential objects in the scene and their correct proportions.

The first time a user enters a specific Rules screen, they will be asked to define the size that an object or person on the screen might be.

The first screen is *Min. Object Size* where the user defines the minimum size of an object that they would like to be detected (yellow box).

The second screen is *Max Object Size* where the user defines the maximum size of an object that they would like to be detected (blue box).

The section can be changed at anytime by clicking the **Reset Object Size** button from the main screen for that rule.





Note: It's important to keep the shapes consistent between the min and max size for best results.

Note: In general, the camera should be installed at a height of 2.5m - 4 m., and inclined at an appropriate angle. (For example, a camera used for detecting intrusion would be pointed obliquely at the field to be viewed, whereas a camera being used for counting people would be mounted vertically.)

If the scene changes significantly, (e.g. a building being demolished), or a new rule is being activated, it's recommended to use the Reset Scene button. This will re-initialize the analytics processes running in the background of the scene and adapt it to the new or changed scene.

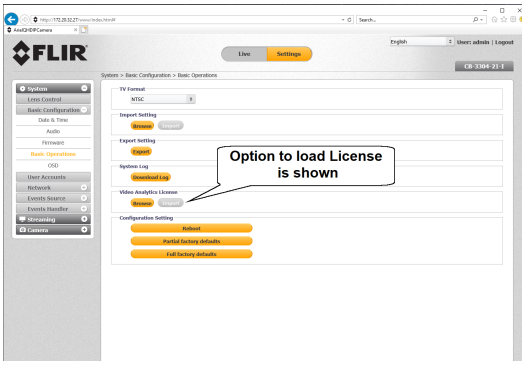
5.3.1.6.8.2 Basic Video Analytics Camera License

Each camera being used with the Basic Video Analytics (BVA) feature must have its own **Camera License** downloaded to it.

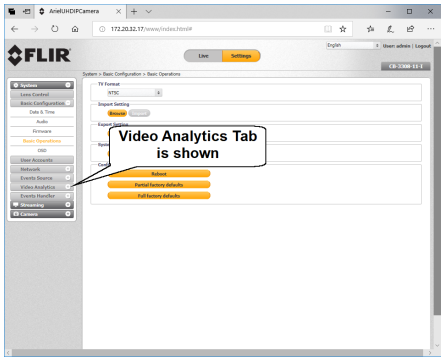
Checking the Web page to see if a camera has a BVA license:

Settings View (with **Basic Operations** selected)

No Camera License installed

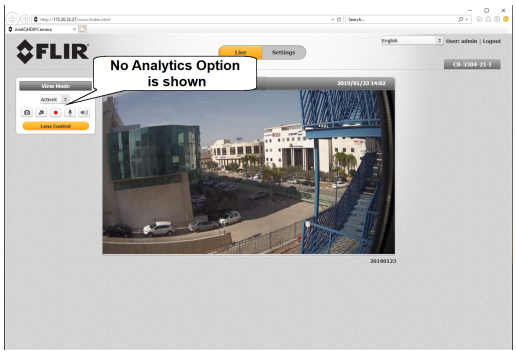


Camera License installed

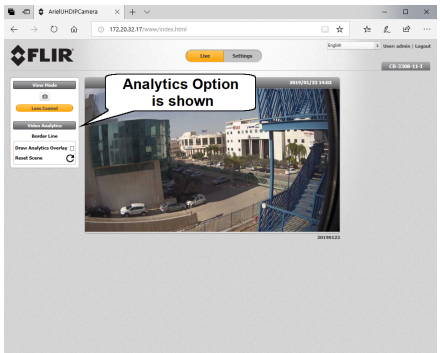


Live View

No Camera License installed



Camera License installed



If a License is required, see Providing cameras with Basic Video Analytics Licenses below.

Note:

If a Partial Reset is performed on the camera, the BVA license is unaffected.

If a Full Factory Reset is performed, the license must be reloaded.

5.3.1.6.8.3 Providing cameras with Basic Video Analytics Licenses

Camera Licenses are provided by **FLIR Operations.**

For assistance in obtaining the licenses, please contact your **Integrator** or your **FLIR representative**.

1. **For Cameras that the User already owns:**
   a. User sends a Purchase Order for license activation to FLIR Operations with a spreadsheet listing Serial Number and MAC address of all units.
   b. FLIR operations creates the individual licenses and sends them back in a .zip file.
   c. Loading the License: User unzips the file and selects specific unit licenses for activation via the camera web page.
   (In an upcoming release of DNA a tool will be provided to automate this process).

2. **For new cameras that the user is ordering:**
   a. User includes the license as an item in the Purchase Order covering the camera/s.
   b. FLIR operations creates the licenses .zip file as above.
   c. When the cameras are delivered, the User follows the Loading the License step above.

5.3.1.6.8.4 Camera Distribution

When selecting where and how many cameras are to be deployed, it is important that the area to be covered by a particular camera should not be so large that the targets to be recognized are too small. Until reasonable on-site parameters are established, the user should experiment with the Minimum and Maximum Object Size settings of each camera.

A camera's Field of View should be able to see a target 'Head-to-Toe' anywhere in the area that it protects.

5.3.1.6.8.5 Camera Positioning

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

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

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

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

Thus, to ensure full camera coverage across the perimeter.

- Position cameras so their field of view runs parallel to the fence line and perpendicular to intruder movement, rather than directing them so they will face approaching targets
- PIce caeras at an angle that shows as little of the skyline as possible.
- When determining the camera positioning, consider whether you only need to detect the moment of intrusion or when a target simply approaches an area

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

These factors need to be taken into account when determining the coverage and the analytic rule that is used.

5.3.1.6.8.6 Detection Ranges

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

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

These include:

- Background temperature (hot desert versus cold snow)
- Atmospheric conditions (clear skies versus fog).

These factors directly influence the following criteria:

- Scene’s contrast level
- Visibility of the target
- Ability to understand the nature of the target (moving vehicle vs. crawling human)
- Speed, and movement of the target object

For a 'real' Object Size of width = 800mm ; height = 1800mm. (Typically the dimensions representing a person):

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

Note:

1. These are rough estimates.

2. Due to lens distortion, better detections will occur for objects in the center of the picture, compared with the edges of the scene.
3. The larger the size of the object, the earlier the detection.
4. The scene and camera mounting may affect the accuracy of detections. For example, a camera with a very limited field of view may have poor detections.

5.3.1.6.8.7 Mounting and Lighting

Make sure that cameras are mounted securely on walls or on stable poles in order to minimize vibrations and maximize resistance to wind.

Ensure adequate lighting for the scene to be monitored.

It should be kept in mind that in dark scenes, the effective detection range with the IR LEDs 'On' is about 30 meters.

5.3.1.6.8.8 Rule-based Settings

The Basic Settings page mostly varies from rule to rule based on the required configuration.

The following items are consistent throughout all of the Basic settings screens:



Reset Object Size

Brings the user back to the Initial Settings screen to reconfigured the object sizes when a scene changes or a different rule is activated.

State

The State will show as Active or Inactive. Only a single Analytic rule can be Active at one time. This will display Active for an already configured and active rule and will display Inactive for all other rules that are not currently in use.

Disable Rule

This check box is used to disable a rule and put it into an Inactive state. If a rule shows an Inactive and the user would like to change it to active, follow the steps to configure a rule. Once the procedure is complete, that rule will become Active, disabling any other previously active rules.

The following sections will describe the specific nuances of each rule and how to configure them.

Counting Border Line Loitering Area Protection Object Removal Object Dropped

The **Video Analytics > Counting** screen is used for configuring the people counting analytic capability.

This page allows you to:

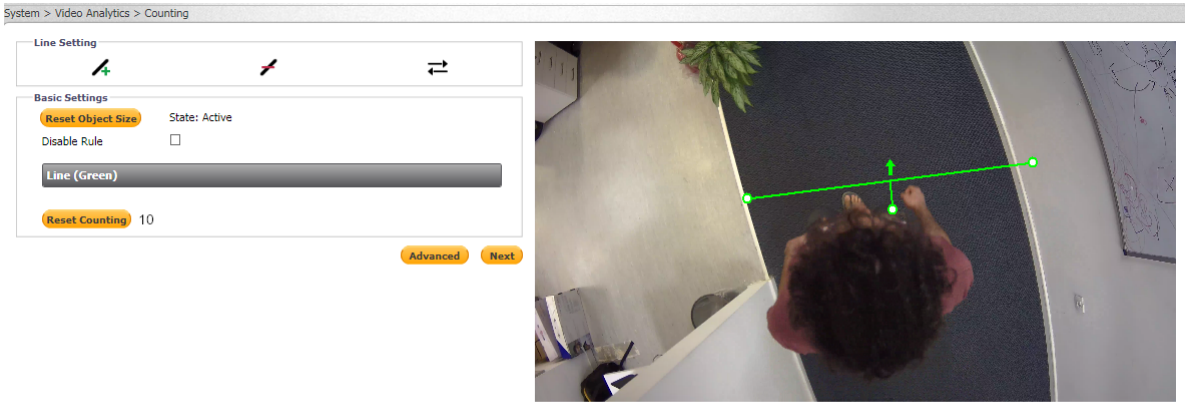
- Configure up to 3 directional lines used for people counting
- Reset Max and Min Object size
- View and reset count results
- Configure advanced settings, including sensitivity, area masking, reset scene and arming schedule
- Analytics actions

Pay special care to setting appropriate minimum and maximum size object markers, to cover a wide variety of body types, as they're viewable from above.

Draw up to three lines on the screen. Each line should cover a potential point of transit, so be sure that the area is not obstructed or hidden by other objects in the scene and that the potential transit path goes through the line at a close to 90deg angle.

See the Initial Settings section for more information on the setup process:

Line Settings:
This section allows the user to add directional lines to specify the area and direction to detect and count people walking.



Pressing the *Add Line* button the user can draw a line in the desired area of the camera view.

Pressing the *Remove Line* button the user can remove the currently selected line.

Pressing the *Direction* button the user can change the direction by which they want to count people moving.

Basic Settings:

For general "Basic Settings" see Basic Settings

The **Basic Settings** section shows which lines are currently being used and the count of people or object that have passed based on the configured rule.

Reset Counting

Clicking *Reset Counting* will set the count back to 0.

See the following sections for more information on Advanced options and Analytics actions (completion of rule configuration)

Advanced Options

Analytics Actions

The **Video Analytics > Border Line** screen is used for configuring the border line detection analytic capability.

This page allows you to:

- Configure up to 3 directional lines used for border detection
- Reset Max and Min Object size
- Configure advanced settings, including sensitivity, area masking, combine rules, reset scene and arming schedule
- Analytics actions

Draw up to three lines on the screen. Each line should cover a potential point of transit, so be sure that the area is not obstructed or hidden by other objects in the scene and that the potential transit path goes through the line at a close to a 90deg angle.

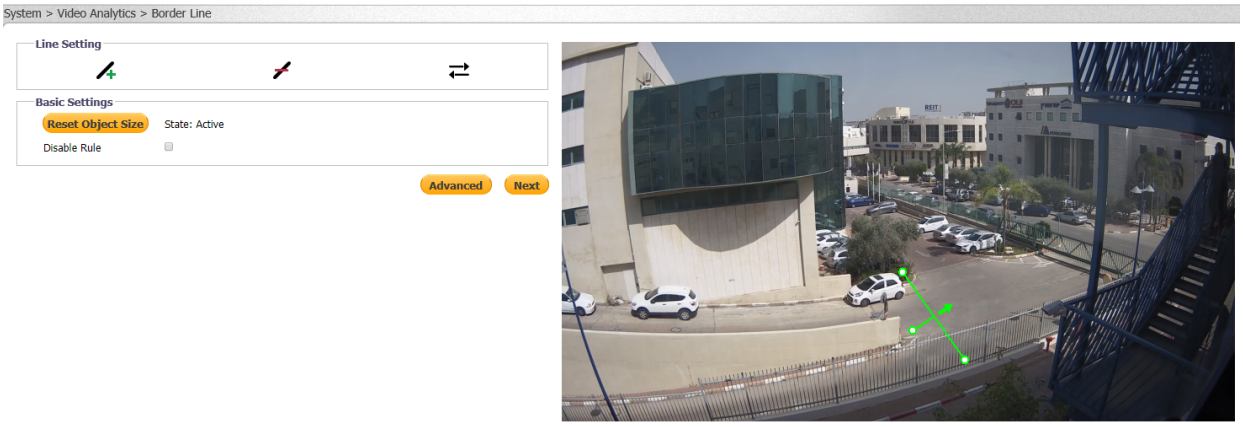
Allow some space before the point of entry for the camera to process and analyze objects as they near the line.

The line can be adjusted in angle, length, and location after it’s drawn.

See the Initial Settings section for more information on the setup process:

Line Settings:

This section allows the user to add directional lines to specify the area and direction to detect people and objects crossing a border.



Pressing the *Add Line* button the user can draw a line in the desired area of the camera view.

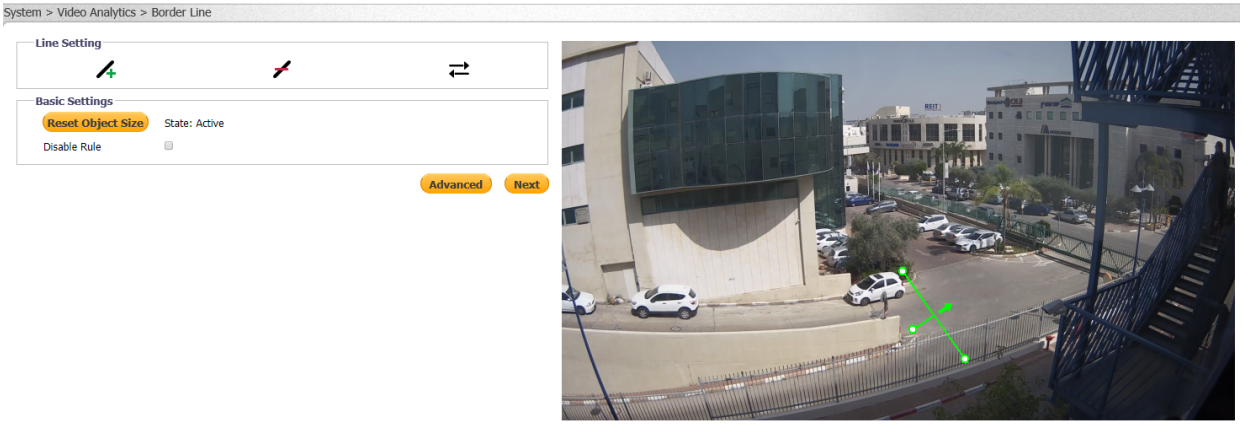
Pressing the *Remove Line* button the user can remove the currently selected line.

Pressing the *Direction* button the user can change the direction by which they want to detect people moving.

Basic Settings:

For general "Basic Settings" see Basic Settings

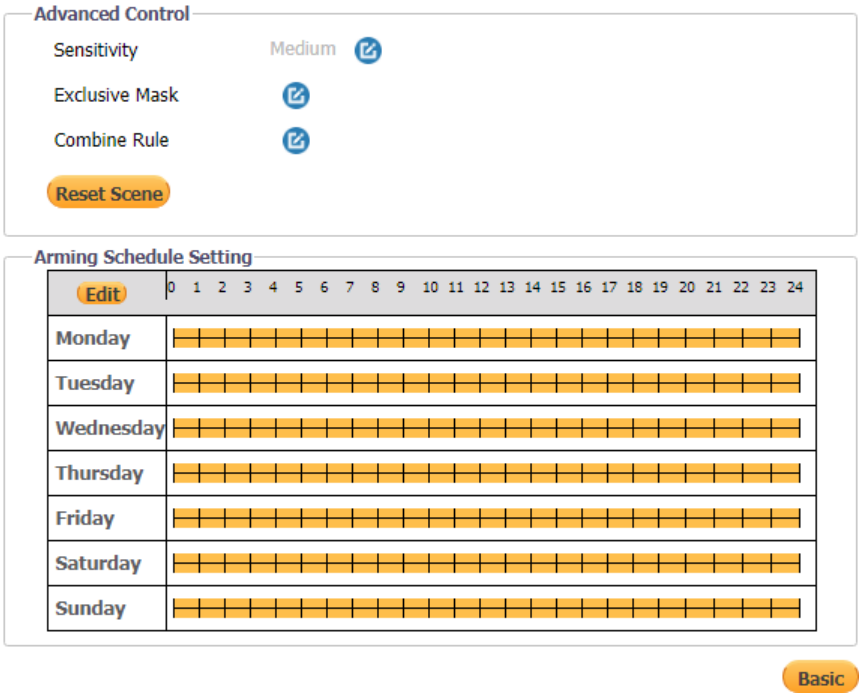
The **Basic Settings** section shows which lines are currently being used and the state of the rule



Advanced Options (Combine Rule):

The Advanced option section of Border Line, includes the feature "Combine Rule" which does not exist in other rules.

For additional information about the Advance options section, and an explanation of the other features on this page, see: Advanced Options



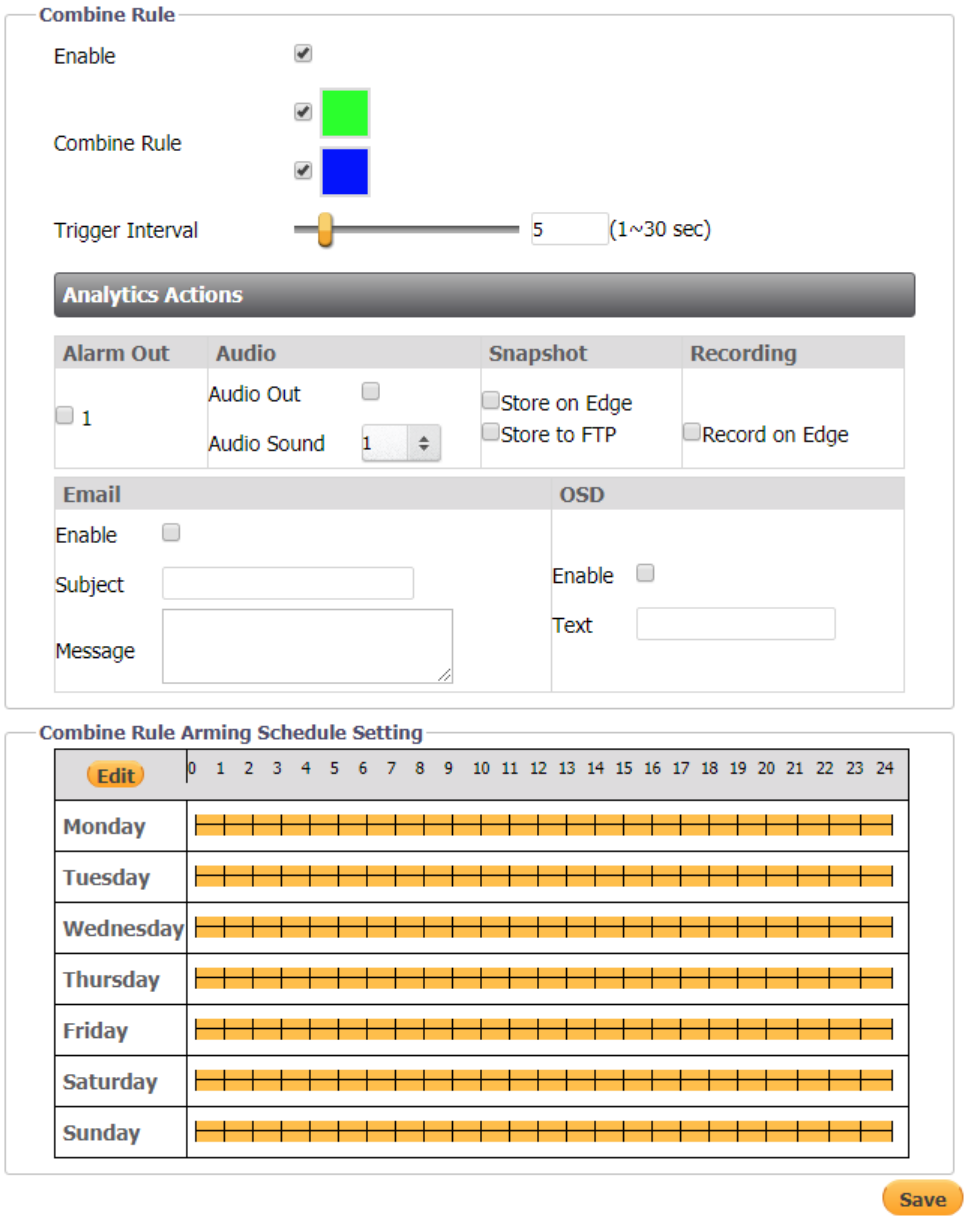
Combine Rule

When *Combine Rule* is enabled, the user has the ability to combine multiple border lines configured in the rule.

The User has the ability to choose the relevant colors associated with the specific rules they would like to combine.



By combining rules, the system will trigger the chosen actions when all of the selected rules are activated.



See the following sections for more information on Advanced options and Analytics actions (completion of rule configuration)

Advanced Options

Analytics Actions

The **Video Analytics > Loitering** screen is used for configuring the loitering analytic capability.

This page allows you to:

- Configure a loitering detection area using 3 to 8 points

- Reset Max and Min Object size
- Define Loitering Time
- Configure advanced settings, including sensitivity, area masking, reset scene and arming schedule
- Analytics actions

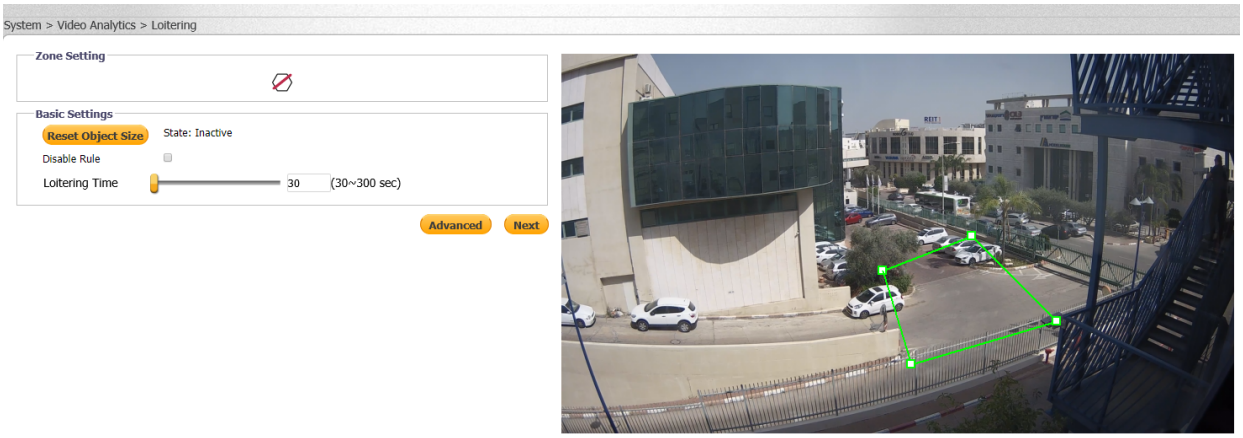
Use the Loitering rule to monitor an area with relative light traffic, but in which an extended stay is prohibited. For example, the area around an ATM or in front of a door, where people are expected to move through and not linger for a long time.

Draw a line around the protected area, forming a closed shape. The minimum loitering duration can be up to 300 seconds.

See the Initial Settings section for more information on the setup process:

Zone Settings:
This section allows the user to create an area using between 3 and 8 points in order to configure the desired space

Clicking on the video scene will produce points for area creation. Once three points are selected, a full area will appear. Clicking more, will create more points creating more complex shapes up to 8 points



Pressing the *Delete* button clears the area entirely, starting the area configuration from nothing.

Basic Settings:

For general "Basic Settings" see Basic Settings

Loitering Time

This section is used to configure the duration of a loitering event in order for a rule to be triggered. This can be changed from the default of 30 second by dragging the slider or typing a number into the text box.



See the following sections for more information on Advanced options and Analytics actions (completion of rule configuration)

Advanced Options

Analytics Actions

The **Video Analytics > Area Protection** screen is used for configuring the area detection analytic capability.

This page allows you to:

- Configure a detection area using 3 to 8 points
- Specify directional preference to detect people leaving or entering desired area
- Reset Max and Min Object size
- Configure advanced settings, including sensitivity, area masking, reset scene and arming schedule
- Analytics actions

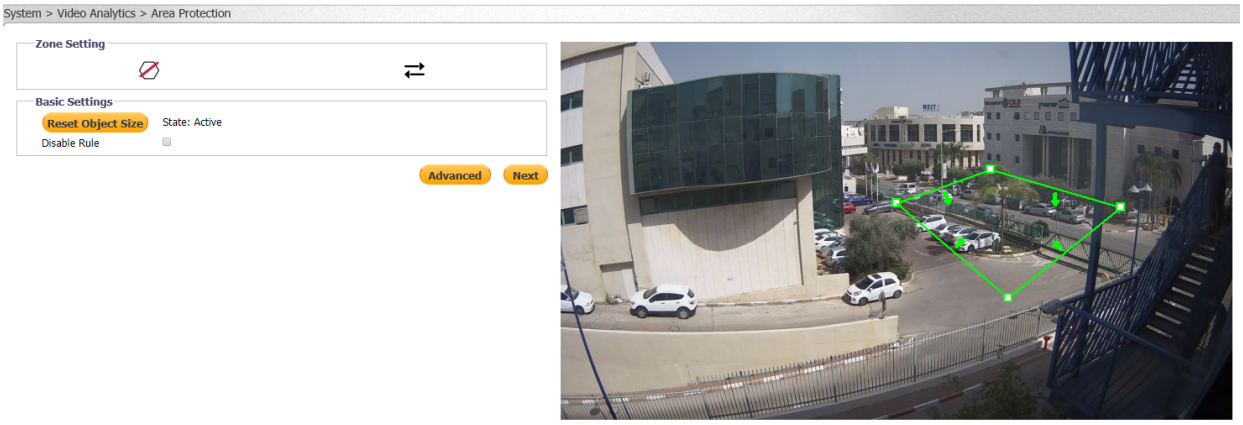
Use the Area Protection rule to secure an area against any incoming or outgoing traffic (humans or vehicles). For example, a secluded or cordoned area, such as a police controlled zone.

Draw a line around the designated zone, forming a closed shape. Allow some space before the point of entry for the camera to process and analyze objects as they near the line.

See the Initial Settings section for more information on the setup process:

Zone Settings:
This section allows the user to create an area using between 3 and 8 points in order to configure the desired space

Clicking on the video scene will produce points for area creation. Once three points are selected, a full area will appear. Clicking more, will create more points creating more complex shapes. After 5 points are created, 3 more can be added by clicking on individual lines, allowing for more specific shapes.



Pressing the *Delete* button clears the area entirely, starting the area configuration from nothing.

Pressing the *Direction* button the user can change the direction by which they want to detect people moving.

Basic Settings:

For general "Basic Settings" see Basic Settings

See the following sections for more information on Advanced options and Analytics actions (completion of rule configuration)

Advanced Options

Analytics Actions

The **Video Analytics > Object Removal** screen is used for configuring the object removal detection analytic capability.

This page allows you to:

- Configure 3 detection areas
- Reset Max and Min Object size
- Set removal duration
- Configure advanced settings, including sensitivity, area masking, reset scene and arming schedule
- Analytics actions

Use the Object Removed rule to monitor an area for objects that are being taken out of it. For example, a store or a gallery with specific objects to protect.

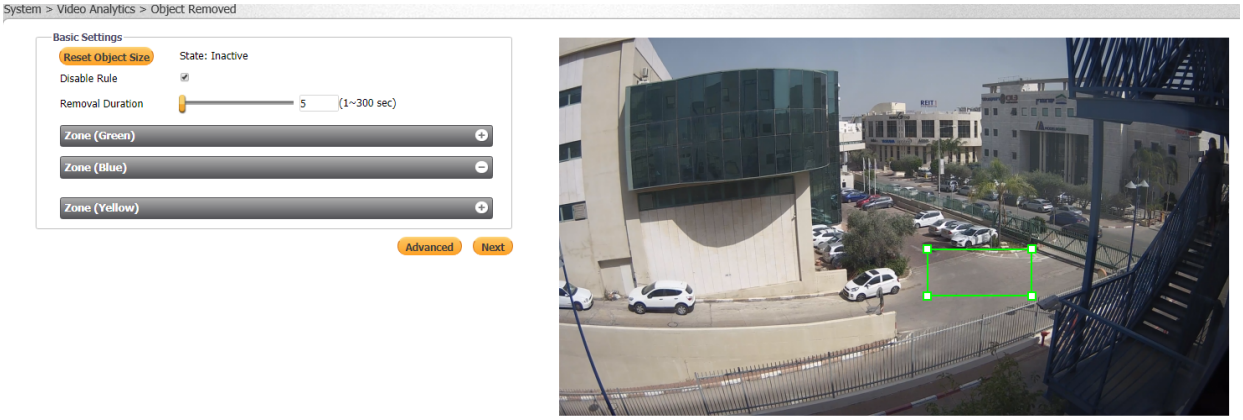
On the initial setup step, set minimum and maximum object sizes that correspond to the protected objects. Draw up to three rectangular zones around the objects.

Once the rule has been defined, do not disturb the scene for about 30 seconds to a minute.

See the Initial Settings section for more information on the setup process:

Zone Settings:
This section allows the user to create 3 zones in order to configure the desired detection areas.

Clicking and dragging on the video scene will produce a re-sizable box at can be moved and sized to mark the desired area for object removal detection



Clicking on the ⊕ button for each zone, will allow the user to draw the box according to that zone (identified by the color).

Basic Settings:

For general "Basic Settings" see Basic Settings

Removal Duration

This section is used to configure the duration that an object had removed from a defined region in order for a rule to be triggered. This can be changed from the default of 5 second by dragging the slider or typing a number into the text box.



See the following sections for more information on Advanced options and Analytics actions (completion of rule configuration)

Advanced Options

Analytics Actions

The **Video Analytics > Object Dropped** screen is used for configuring the Dropped Object detection analytic capability.

This page allows you to:

- Configure a object dropped detection area using 3 to 8 points
- Reset Max and Min Object size
- Define Object in region duration Time
- Configure advanced settings, including sensitivity, area masking, reset scene and arming schedule
- Analytics actions

Use the Object Dropped rule to secure an area against suspicious objects and litter. For example, a bus station or a public square.

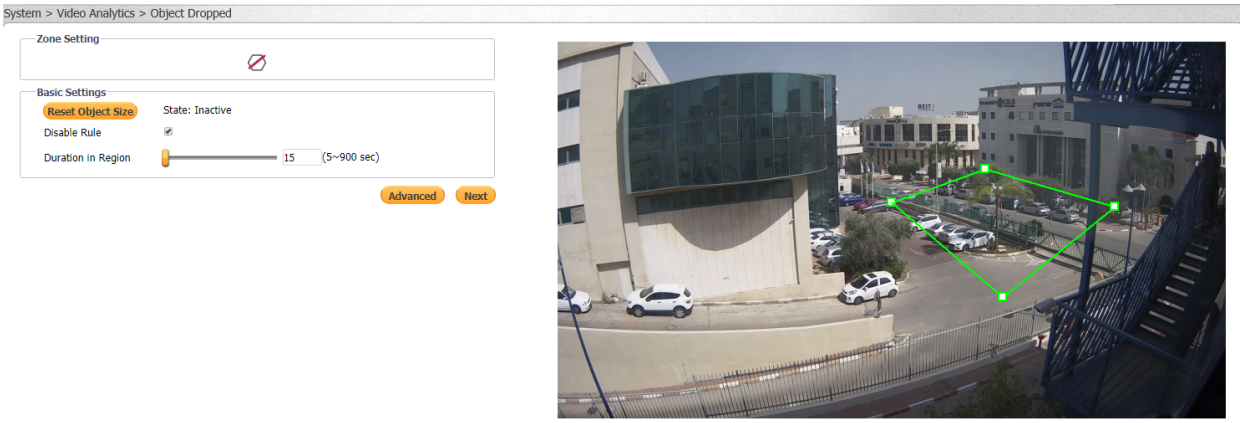
On the initial setup step, set minimum and maximum object sizes that correspond to the potential threat (smaller than people). Draw a shape using up to 8 points to cover the protected area. The minimum duration in region ranges between 5 and 900 seconds – use a reasonable value to avoid false alarms.

Once the rule has been defined, do not disturb the scene for about 30 seconds to a minute.

See the Initial Settings section for more information on the setup process:

Zone Settings:
This section allows the user to create an area using between 3 and 8 points in order to configure the desired space

Clicking on the video scene will produce points for area creation. Once three points are selected, a full area will appear. Clicking more, will create more points creating more complex shapes up to 8 points



Pressing the *Delete* button clears the area entirely, starting the area configuration from nothing.

Basic Settings:

For general "Basic Settings" see Basic Settings

Duration in Region

This section is used to configure the duration of an object left in a defined region in order for a rule to be triggered. This can be changed from the default of 15 second by dragging the slider or typing a number into the text box.

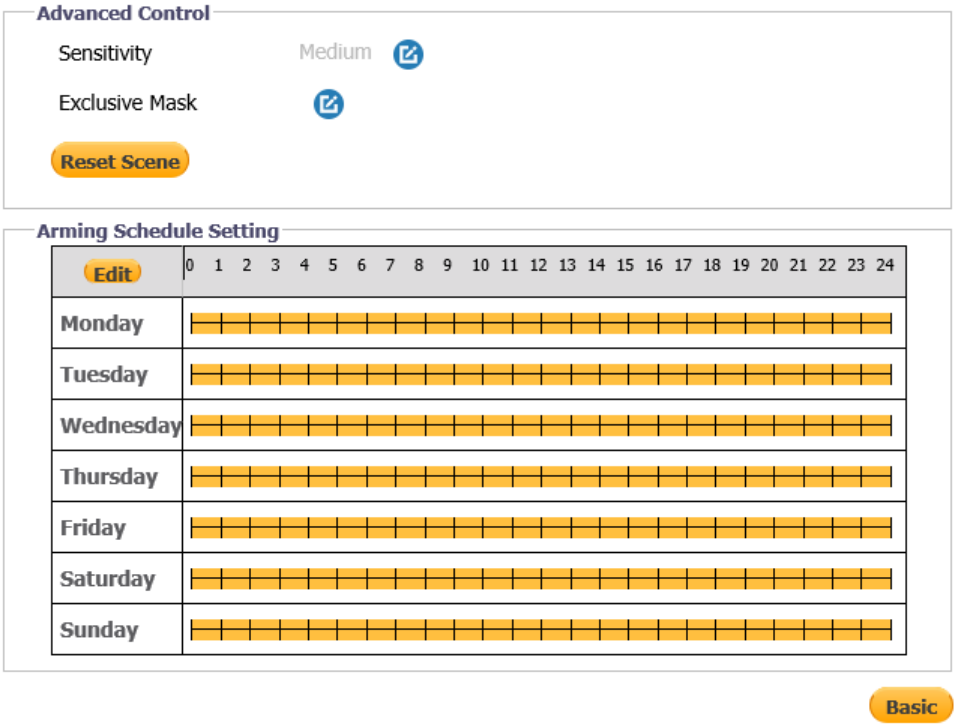


See the following sections for more information on Advanced options and Analytics actions (completion of rule configuration)

Advanced Options

Analytics Actions

Note: The Advanced options section for Border Line includes an extra feature called "Combine Rule". More more information, please navigate to: Combine Rule



Advanced Control;

Sensitivity

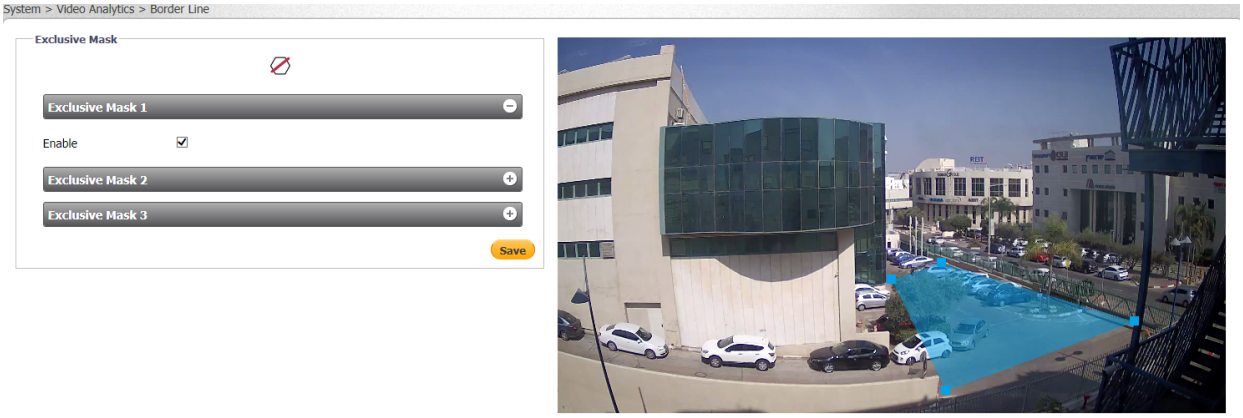
Clicking the button will allow the user to change the sensitivity settings (Default = Medium).
The available options are:

- High
- Mid High
- Medium
- Mid Low
- Low

Exclusive Mask

This section allows the user to define a section of the camera view that will be ignored by the analytics rule.

Clicking the button will bring the user into the configuration screen:



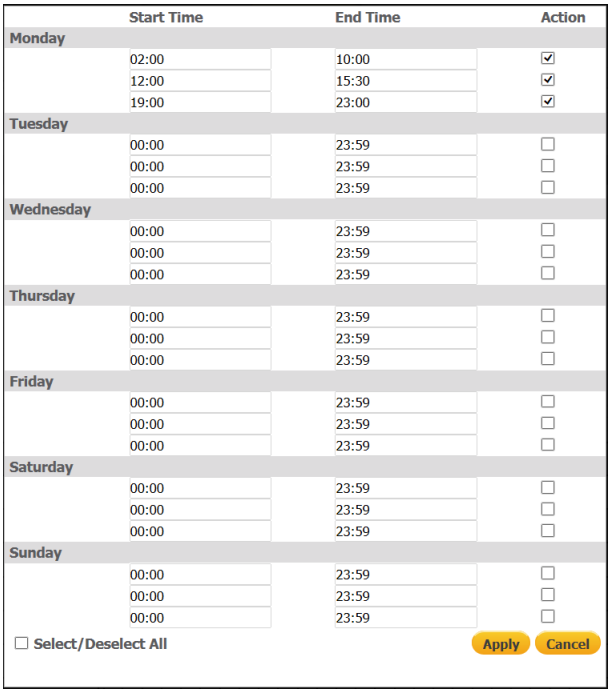
Up to 3 masks can be configured, one is enabled by default. The user sets the mask by clicking on the camera view and making 3-8 points which can be moved and reshaped to mask the desired area.

Clicking the button will clear the configured mask of the currently selected mask. Clicking **Save** will save the configurations of all "Enabled" masks.

Reset Scene
Clicking **Reset Scene** will relearn the scene and the background in case the scene has changed or the camera has been moved.

To set the arming schedule

1. In the *Arming Schedule Setting* area, click **Edit**. The **Edit** screen opens.

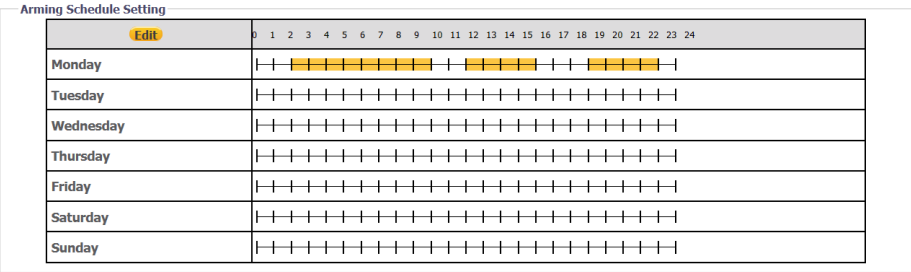


	Start Time	End Time	Action
Monday			
	02:00	10:00	☑
	12:00	15:30	☑
	19:00	23:00	☑
Tuesday			
	00:00	23:59	☐
	00:00	23:59	☐
	00:00	23:59	☐
Wednesday			
	00:00	23:59	☐
	00:00	23:59	☐
	00:00	23:59	☐
Thursday			
	00:00	23:59	☐
	00:00	23:59	☐
	00:00	23:59	☐
Friday			
	00:00	23:59	☐
	00:00	23:59	☐
	00:00	23:59	☐
Saturday			
	00:00	23:59	☐
	00:00	23:59	☐
	00:00	23:59	☐
Sunday			
	00:00	23:59	☐
	00:00	23:59	☐
	00:00	23:59	☐

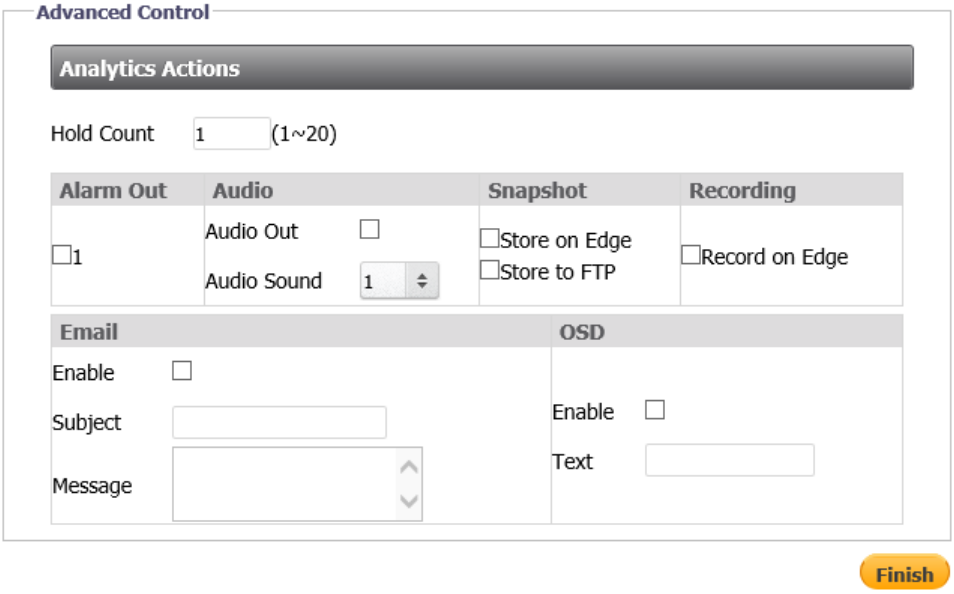
☐ Select/Deselect All Apply Cancel

2. In the *Start Time* column, enter the time(s) and day(s) you want to trigger an action.
3. In the *End Time* column, enter the time(s) and day(s) you want to stop the action.
4. Select the *Action* checkbox if you want to enable the action at these times.
5. Select the *Select/Deselect All* checkbox as required.

6. Click **Apply**. The times for the schedule are displayed in orange in the *Arming Schedule Setting* section.



To continue with the configuration of video analytics, click *Next* to arrive at the **Analytics Actions** page



The **Analytics Actions** page is used to set event handlers to take place up an analytics alarm.

Hold Count

Hold count determines the amount of people that need to pass by in order to register as a "count".

Note: There is no time limitation on the hold count. i.e. If a large amount of time occurred between people, it will wait until it has reached the "hold count" amount before registering a count.

To enable the Alarm Out function

1. In the *Handlers* section, select the *Alarm Out* checkbox. By default, it is not checked.
2. Click **Save**.

To enable audio

1. In the *Handlers* section, from the *Audio Enable* drop-down list, select *ON*. By default, it is not checked.
2. From the *Audio Sound* drop-down list, select the number for the audio file that you want to play. See the *Event Handler* > *Sound* section to load the audio files that are triggered upon occurrence of an event.
3. Click **Save**.

To define the method to store a snapshot

1. In the *Snapshot* section, select the *Store on Edge* checkbox to store a snapshot on the camera's microSD card. By default, it is not checked.
2. In the *Snapshot* section, select the *Store to FTP* checkbox to store a snapshot on a remote FTP site. By default, it is not checked.

To record an event

1. In the *Recording* section, select the *Record on Edge* checkbox to record a clip on the camera's microSD card. By default, it is not checked.
2. Click **Save**.

To send email notifications

1. In the *Email* section, select the *Enable* checkbox. By default, *Enable* is not checked.
2. In the *Subject* text box, enter the email subject text.
3. In the *Message* text box, enter the email message text.
4. Click **Save**.

To activate the on-screen display

1. In the *OSD* section, select *Enable*. By default, *Enable* is not checked.
2. In the *Text* text box, enter the text to display in the on-screen display.
3. Click **Save**.

There are two possible issues when working with video analytics:

- Missed detections
- False alarms.

In both cases, the first step is to re-check the set minimum and maximum object sizes. For example, if the minimum object size is very small, it might allow for the detection of small animals. Adjust the size, shape, and location of the zone/line to make sure that it and areas immediately adjacent to it are covered clearly by the camera's field of view.

The Sensitivity setting can be used to adjust the overall probability of detection. A high value of sensitivity may also lead to a relatively high ratio of false alarms.

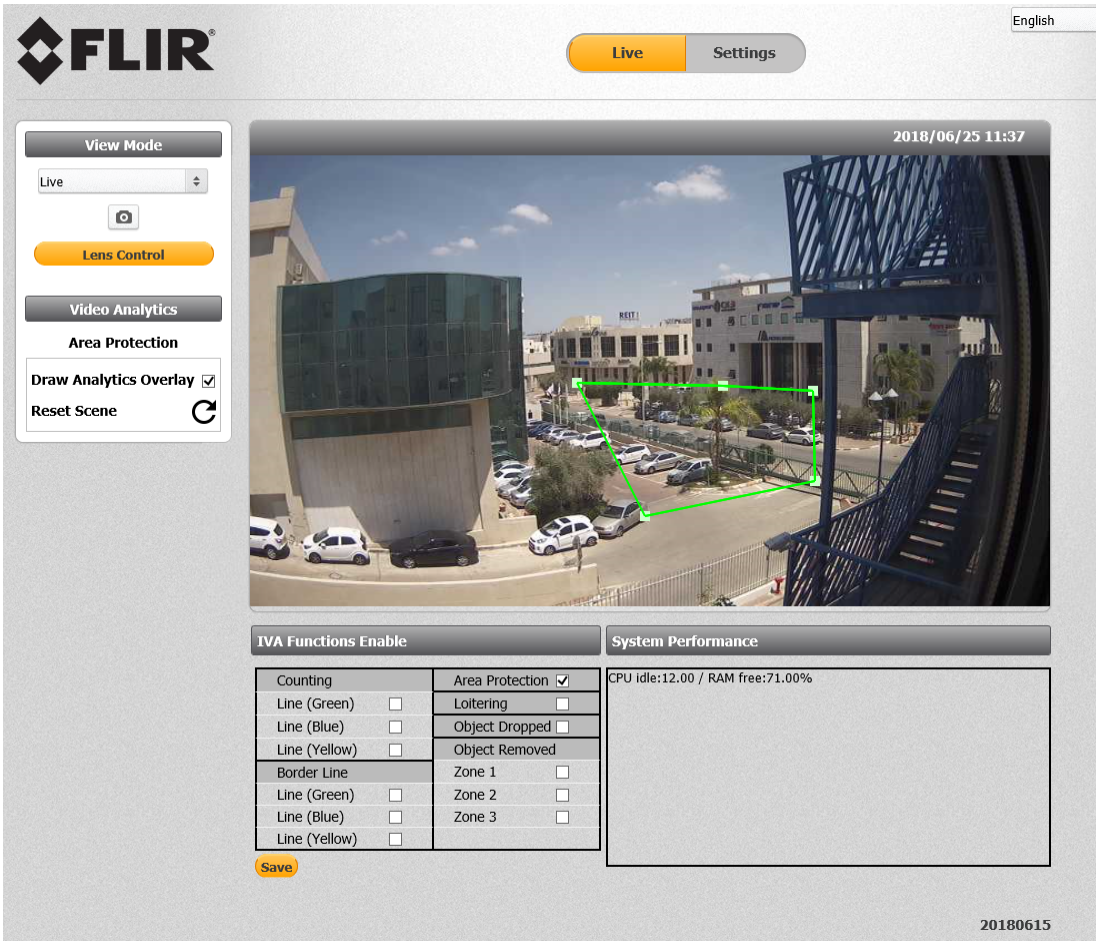
If the protected area is adjacent to or includes a zone that is likely to have a high degree of motion, like wind blowing through foliage, an Exclusive Mask may be set. The area covered by the mask will not trigger any detections

Debug Mode

Debug mode allows the user to receive additional information on the state of the camera and the analytics performance. It is accessed by entering: http://Camera_IP/www/debug.html

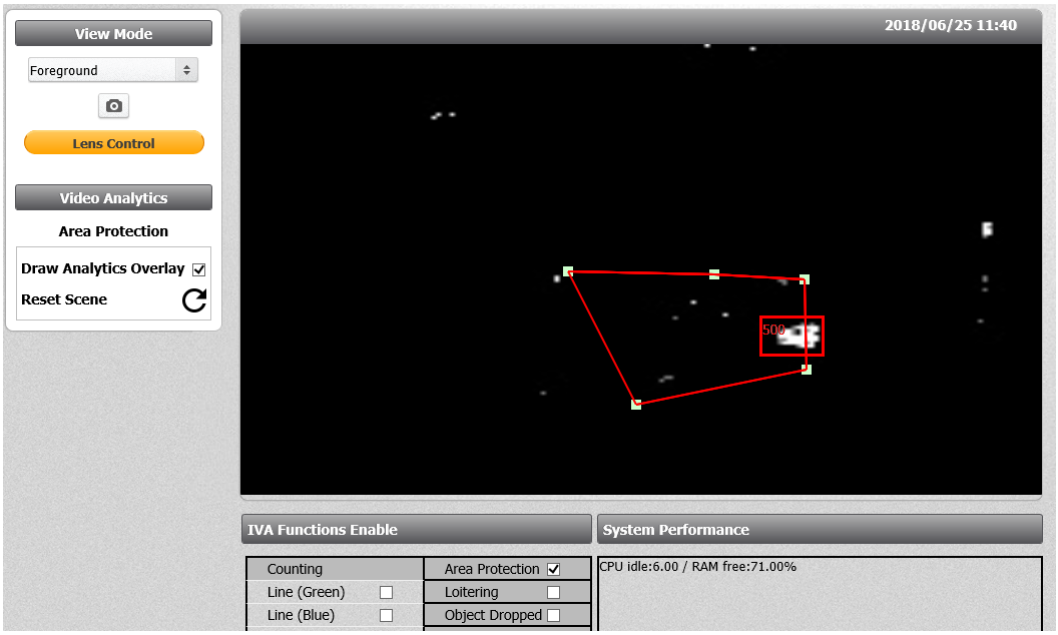
There are two view options on the Debug mode:

1. **Live** – allows the user to monitor potential objects before and as they are identified as detected objects and alerted upon. The potential objects are marked with white tracking boxes and alerted objects are marked with red, blue, or black tracking boxes.



Analytics Debug - Live View

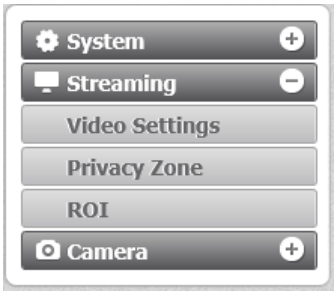
2. **Foreground** – displays the raw motion data in the scene. This data is processed by the video analytics algorithms to identify and construct objects. By viewing the raw data, the user can visually compare what is going on with the scene and the motion that the camera is registering.



Analytics Debug - Foreground View

5.3.2 Streaming Tab

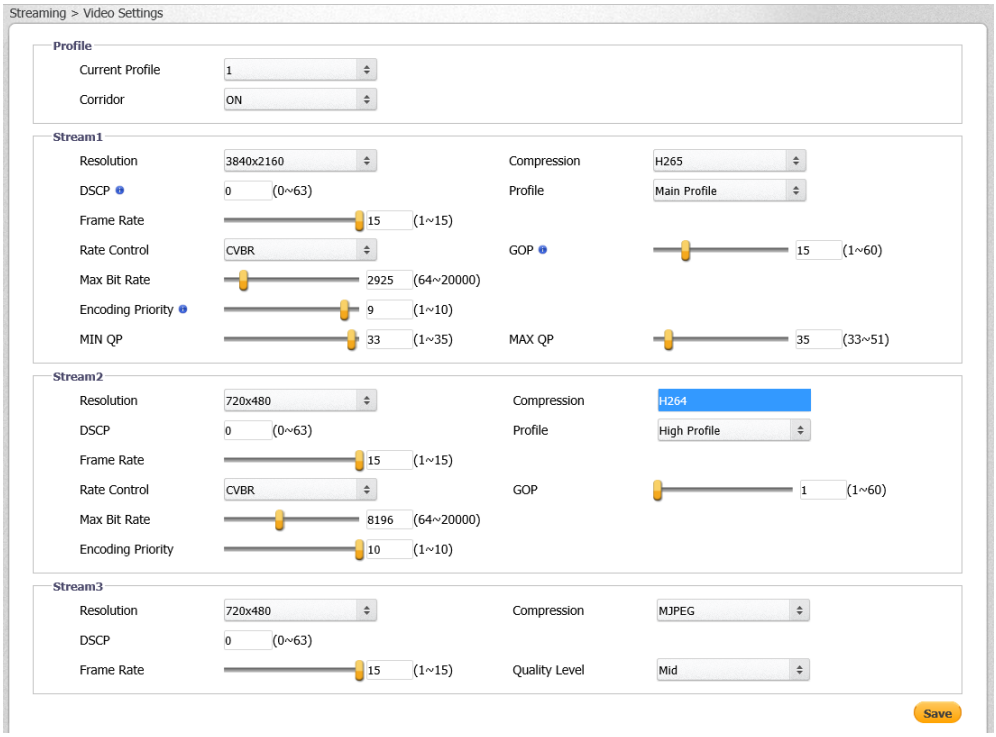
The **Streaming** tab is used for configuring video streaming settings, privacy zones, and region of interest settings.



Streaming Tab

5.3.2.1 Video Settings

The CF-6308 camera supports three simultaneous streams with H.265, H.264 or MJPEG compression. MJPEG is supported on all streams and resolutions, except UHD/4K (3840x2160) on Stream1. The **Video Settings** screen is used for configuring the streams and such video parameters as resolution; video compression type and related settings; quality of service; and frame rate. Additional settings are available when using H.265 and H.264 compression.



Video Settings Screen

5.3.2.1.1 Video Resolutions

The following resolutions are available:

H.265-Only	
PAL	**NTSC**
3840 x 2160 (25 fps)	3840 x 2160 (27 fps)
1920 x 1080 (50 fps)	1920 x 1080 (60 fps)
1280 x 720 (50 fps)	1280 x 720 (60 fps)
720 x 576 (50 fps)	720 x 480 (60 fps)
H.264-Only	
PAL	**NTSC**
3840 x 2160 (25 fps)	3840 x 2160 (30 fps)
1920 x 1080 (50 fps)	1920 x 1080 (60 fps)
1280 x 720 (50 fps)	1280 x 720 (60 fps)

720 x 576 (50 fps)	720 x 480 (60 fps)

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

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

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

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

	720 x 576 (15 fps @ H.264/H.265/MJPEG)	720 x 576 (15 fps @ H.264/H.265/MJPEG)
1920 x 1080 (50 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
		720 x 576 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)
1280 x 720 (50 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)	1280 x 720 (25 fps @ H.264/H.265/MJPEG)
		720 x 576 (25 fps @ H.264/H.265/MJPEG)
	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)
720 x 576 (50 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)	720 x 576 (25 fps @ H.264/H.265/MJPEG)

5.3.2.1.2 Configuring Video Settings

To configure video settings

1. From the *Current Profile* drop-down list, select *1, 2,* or *3*. The default is *1*.

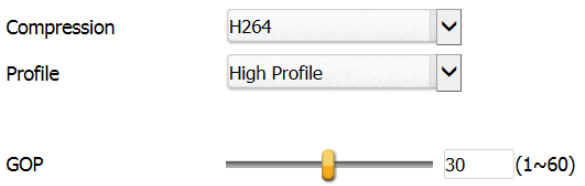
   Each of the three Current Profiles has its own settings. The available parameters depend on the selected resolution. Each profile supports up to three concurrent streams (Stream1, Stream2, and Stream3), which can be configured separately to send two streams simultaneously with optimized quality and bandwidth.

2. From the *Corridor* drop-down list, select *ON* if you want to use this viewing mode. The image rotates 90° counter-clockwise (to the left) and is displayed in 16:9 aspect ratio. This 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 when configuring the *Rotate Image* setting for the camera.
3. In the *Stream1* section, configure the following settings:
   a. From *Resolution* drop-down list, select the desired resolutions. The default is the highest resolution for each stream.
   b. From the *Compression* drop-down list, select *H.265 or H.264* according to the required resolution, image quality and storage limitations. The default is *H.264*.

   Note:

   MJPEG is supported on Stream2 and Stream3 for all the available resolutions.

   i. If you selected H.265 or H.264, the following fields are displayed:



H.264 Settings

a. From the *Profile* drop-down list, select a profile*: High Profile* (H.265 and H.264) *or Main Profile* (H.265 only). Each profile targets specific classes of applications.

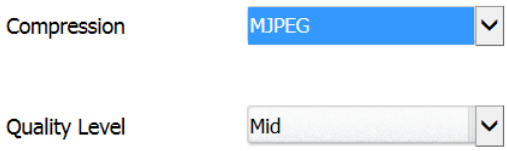
- *High Profile (HP)*
  High Profile is the primary profile for HD broadcast applications, providing the best trade-off between storage size and video latency. It can save 10-12% of the storage cost over Main Profile. However, it may also increase video latency, depending on the stream structure. This is the default profile.
- *Main Profile (MP)*
  This profile provides improved picture quality at reduced bandwidths and storage costs and is becoming more common as the camera processors (DSPs) become more able to handle the processing load.

b. Set the *GOP* to a value from 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.265 and H.264 video compression. Transmitted video frames are compared to the I-Frame as they are transmitted. Video quality is higher when the interval between I-Frames is shorter, but the video needs more network capacity. When the interval between I-Frames is longer, the video transmission uses less bandwidth, but the video quality is lower.

ii. If you select *MJPEG*, the following fields are displayed:



MJPEG Settings

a. From the *Quality Level* drop-down list, select *High, Mid,* or *Low.* The default is *Mid*. *High* produces the highest image quality, but increases the file size. *Low* produces the lowest image quality and decreases the file size.

c. In the *DSCP* text box, enter a value between *0-63*. The default DSCP value is *0* (DSCP disabled).

The DSCP (Differentiated Services Code Point) 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.

d. Move the *Frame Rate* slider to the desired value. The choice of frame rates depends on the combination of the selected resolutions for the selected streams. The maximum frame is displayed by default. The higher the FPS, the smoother the motion in the video.

e. Do one of the following:

- If you selected MJPEG, continue with step 4.
- If you selected H.265 or H.264, *Rate Control* is displayed. From the *Rate Control* drop-down list, select *CBR* or *CVBR.* The default is *CBR.*
    - Select *CBR* (Constant Bit Rate) if you are monitoring simple scenes. CBR uses more storage capacity than CVBR. It wastes storage on simple scenes, while not allocating enough storage for complex sections (resulting in degraded quality). Move the slider to a number between *64* and *20000* bits per second. The default settings are H.264 at *2925* kbps for UHD/4K, *691* kbps for HD 720p @ 15 fps, and *375* kbps for D1 @ 30 fps. The higher the bit rate, the better the image quality. Set the maximum bit rate high enough to allow for a high instantaneous bit for more complex video. A higher bit rate consumes more storage space.

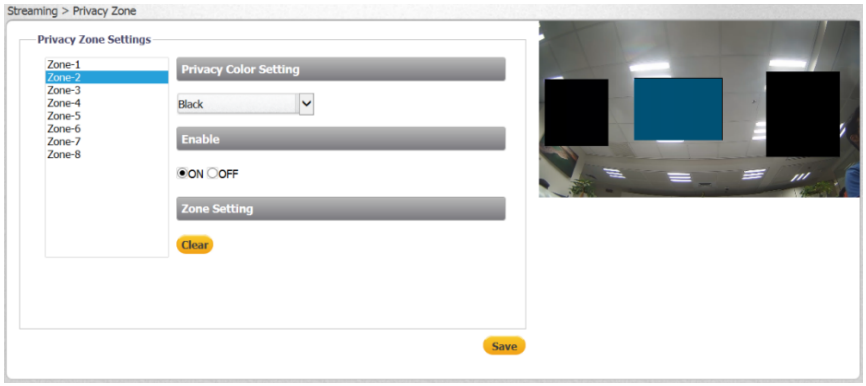
- Select *CVBR* (Constrained Variable Bit Rate) to enable greater control over image parameters. CVBR uses less storage capacity than CBR. This is helpful in complex scenes, which use more bits than simple scenes. CVBR is desirable if you want an optimum bit rate from frame-to-frame with a relatively predictable file size. Continue with the following steps.
  - Set the *Max Bit Rate* to a value between 64 to 20000. The default settings are H.264 at *2925* kbps for UHD/4K @ 15 fps, *691* kbps for HD 720p @ 15 fps, and *375* kbps for D1 @ 15 fps. The higher the bit rate, the better the image quality. Set the maximum bit rate high enough to allow for a high instantaneous bit for more complex video. A higher bit rate consumes more storage space.
  - Set the *Encoding Priority*. 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 *6*.

    The slider is configured based on Quantization Parameter (QP) values. Setting QP to a high value increases the bit rate and results in high compression, but this is at the expense of poor decoded image quality. Setting QP to a low value results in better decoded image quality, but with lower compression.

4. Repeat Step 3 for Stream2 and Stream3. If you are not using additional streams, select *Off* from the *Resolution* drop-down list.
5. Click **Save**.

5.3.2.2 Privacy Zone

A privacy zone enables users to cover a specific portion of the screen for privacy reasons. Users can define up to 8 privacy zones. After setting up a privacy zone, in the live view screen a frame is displayed whose color, size and position can be customized according to users' preference.



Privacy Zone Screen

Note:

Privacy zones are not supported when configuring 4K + Full HD 1080P + D1 streams.

To set a privacy zone

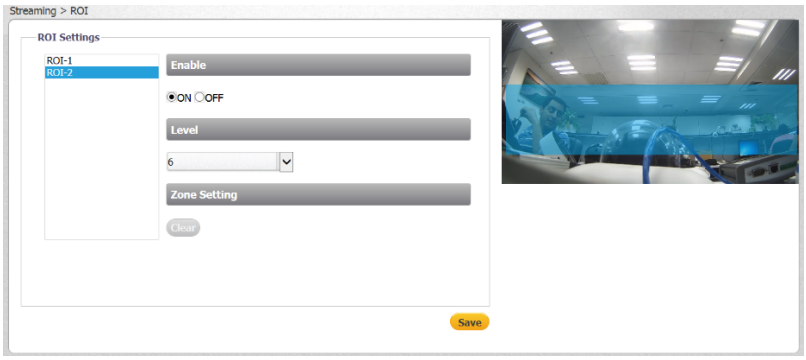
1. Select a privacy zone number from the list of *Zone-1* through *Zone-8*.
2. From the *Privacy Color Setting* drop-down list, select *Black*, *Grey,* or *White*. The default setting is *Black*.
3. In the *Enable* section, select *ON*. The default setting is *OFF*.
4. Use your mouse to draw a region of interest on the screen.
5. Click **Save**. The privacy zone is displayed on the screen. Repeat the above steps for each privacy zone.

To delete a privacy zone

1. Select the privacy zone.
2. Click **Clear**. The privacy zone is deleted.
3. Repeat the above steps for each privacy zone.

5.3.2.3 ROI

The **ROI** (Region of Interest) screen is used for configuring regions of interest on the **Live View** window.



ROI Screen

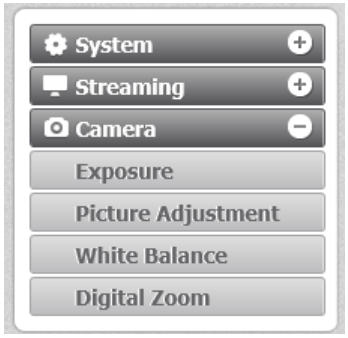
The image displayed within the ROI box can be displayed with higher quality than the image outside of the box. Overall bit rate is not affected by selecting regions of interest. Enhancing the video where the quality is very important consumes more bandwidth, but enables lowering image quality and bandwidth consumption on less important zones in the scene.

To set a region of interest

1. From the *ROI* list, select *ROI-1* or *ROI-2*.
2. In the *Enable* section, select *ON*. The default setting is *OFF*.
3. Use your mouse to draw a region of interest on the screen.
4. From the *Level* drop-down list, select a number between *1-6*, where 1 is the lowest quality and 6 is the highest quality for the image within the region of interest.
5. Click **Save**. The region of interest is displayed on the screen.
6. To delete the region of interest, select *ROI-1* or *ROI-2* and click **Clear**. The ROI is deleted.

5.3.3 Camera Tab

The **Camera** tab includes four screens: **Exposure**, **Picture Adjustment**, **White Balance** and **Digital Zoom**.

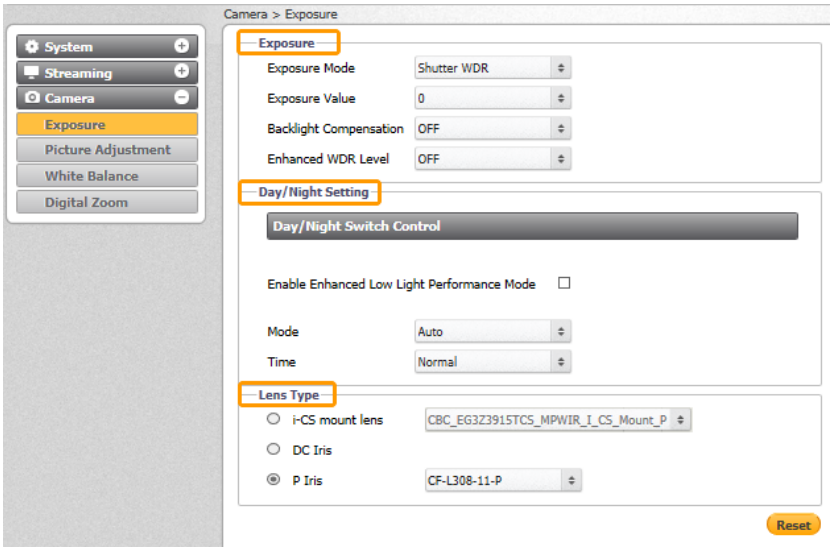


Camera Tab

Note:

Settings are saved automatically. Clicking **Reset** returns the settings to factory defaults.

5.3.3.1 Exposure Screen



The **Exposure** screen contains three sections:

- Exposure
- Day/Night Setting
- Lens Type

The *Exposure* section is used for configuring basic exposure settings. The configurable settings depend on the selected Exposure mode. You can select one of the following modes: *Auto Shutter Mode*, *Flickerless*, *Auto Iris*, *Manual*, and *True WDR*.

The *Day/Night Setting* options depend on which Exposure Mode is selected from the Exposure section.

The *Lens Type* section requires you to select the type of lens attached to the camera body. Three options are available:

- i-CS Mount Lens
- DC-Iris
- P-Iris – From the drop-down menu, select one of the following lenses:
  - CF-L308-11-P
  - CF-L304-11-P
  - CF-L304-21-P



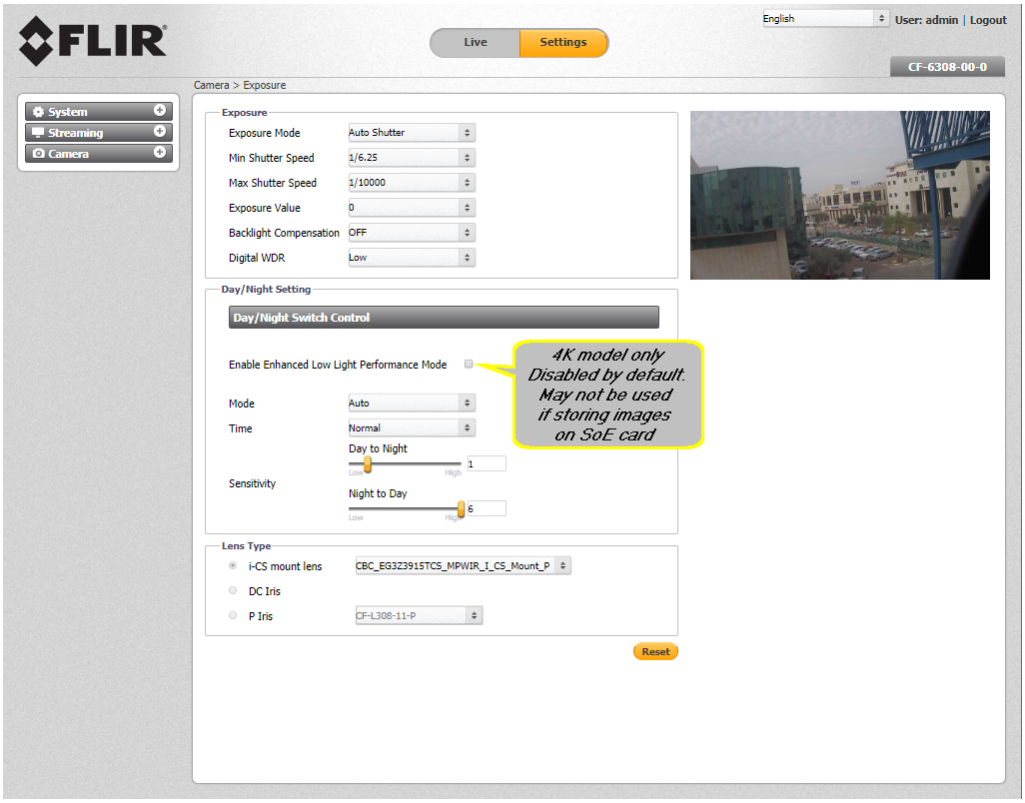
Note:

These lens selections are all done with the toggle switches on the camera itself. The web interface reports the current settings.
Be sure to select the correct toggle switch position on the camera's connector panel for the i-CS, DC-Iris or P-Iris options in order for the camera to operate correctly.

See Hardware Description.

5.3.3.1.1 Auto Shutter Mode

Auto Shutter mode opens the shutter completely. Shutter speed and the AGC circuit function automatically in cooperating with the iris to achieve a consistent exposure output. The exposure priority is given to the iris. This mode is recommended to be used in indoor environments involving mixed lighting sources where the main source is fluorescent lighting combined with natural light that enters the scene through windows and other exposed areas. This is the default setting.



Auto Shutter Exposure Mode Settings

In the *Exposure* section, configure the following settings:

- *Max Shutter Speed* – Select a suitable shutter speed according to the environmental luminance. The following table displays the options:

Auto Shutter Max Shutter Speed	
PAL	**NTSC**
1/6.25	1/7.5
1/12.5	1/15
1/25	1/30
1/50	1/60

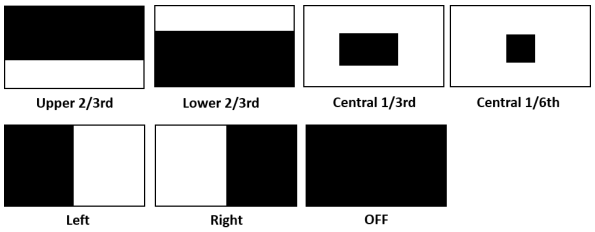
Caution:
Using a slow shutter speed causes moving objects to be blurred.

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

- *Min Shutter Speed* – Select a suitable shutter speed according to the environmental luminance. The following table displays the options:

Auto Shutter Min Shutter Speed	
PAL	**NTSC**
1/100	1/120
1/250	1/250
1/500	1/500
1/1000	1/1000
1/2500	1/2500
1/5000	1/5000
1/10000	1/10000

- *Exposure Value* – This is a number that represents a combination of a camera's shutter speed and f-number, which brightens or darkens the scene accordingly. Select from the following options: *-2, -5/3, -4/3, -1, -2/3, -1/3, 0, 1/3, 2/3, 1, 4/3, 5/3,* or *2*. The higher the number, the brighter the image. The default setting is *0*.
- *Backlight Compensation* – In images where a bright light source is behind the subject of interest, the subject would normally appear in silhouette. The backlight function of the camera allows it to adjust the exposure of the entire image to properly expose the subject in the foreground. From the drop-down list, select one of the following options for the backlight compensation: *OFF, Upper 2/3rd, Lower 2/3rd, Central 1/3rd, Central 1/6th, Left, Right,* or *OFF* (default setting). The settings are as follows:



Backlight Compensation Settings

- *Digital WDR* – This function improves the image quality and amount of details in high contrast scenes. Such scenes combine areas with different lighting conditions, where some areas are very bright and others are dark. If this function was not used, the image either would be overexposed or too bright in bright areas and completely dark in dark areas. Digital WDR helps to improve image quality by producing a larger amount of details in both the dark and bright areas of the image.

  Select *High, Medium, 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. The default setting is *Medium*.

In the *Day/Night Switch Control* section, configure the following settings:

- *Mode* – The Day/Night switch activates the IR Cut (IRC) filter for electronic day/night operation. Three modes are available: *Auto, Color,* and *B/W*.

- **4K model ONLY** - Enhanced Low Light Performance (ELLP) is checked off by default, but can be enabled. When camera is set to 4K, ELLP enhances the image and sensitivity. It also keeps cameras in color for longer before switching to black and white mode.
  Note:
  ELLP may not be used when the camera is set to record images on an SoE card.

- *Auto* – Select *Auto* for automatic operation according to the ambient light level. The camera converts from *Day* (color) mode to *Night* mode (monochrome/black and white) automatically at nighttime or in low-light conditions. When there is sufficient light, the camera converts automatically from *Night* mode to *Day* mode. This is the default setting.

- *Color* – Select *Color* for daylight operation. This deactivates IR mode by putting the camera into *Day* mode.

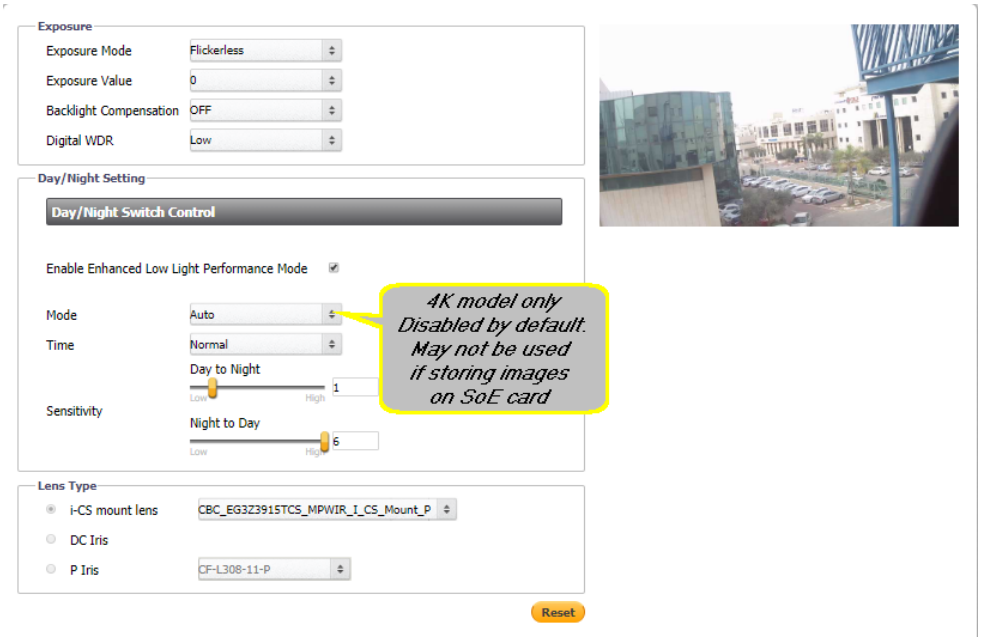
- *B/W* – Select *B/W* (black and white) for nighttime operation. This activates IR mode by putting the camera into *Night* mode.

- *Time* – Select *Fast, Normal,* or *Slow* to set the reaction time of the IRC filter. When set to *Fast*, the filter switches faster between *Day* and *Night* modes. The default setting is *Normal*.

Click **Reset** if you want to return to factory default settings.

5.3.3.1.2 Flickerless Mode

Flickerless mode eliminates flicker in indoor applications where fluorescent lighting is used. The darker the ambient lighting, the slower the shutter speed should be.



Flickerless Exposure Mode Settings

In the *Exposure* section, configure the following settings:

- *Exposure Value* – See the explanation in the *Auto Shutter* section above.
- *Backlight Compensation* – See the explanation in the *Auto Shutter* section above.
- *Digital WDR* – See the explanation in the *Auto Shutter* section above.

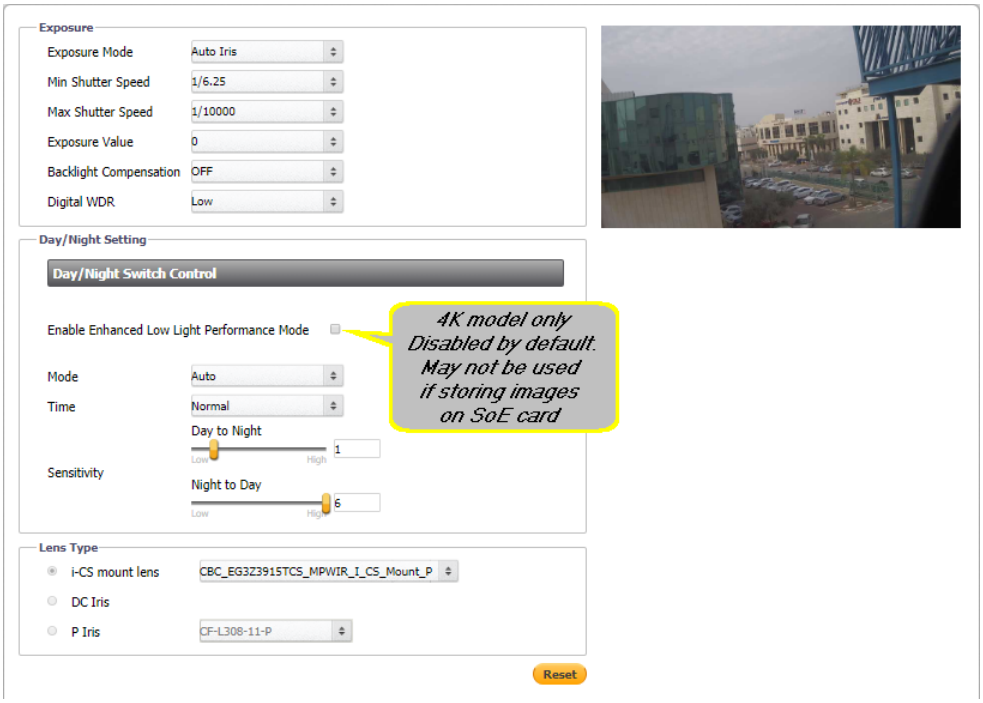
In the *Day/Night Switch Control* section, configure the following settings:

- ***4K model ONLY -*** *Enhanced Low Light Performance (ELLP) is checked off by default, but can be enabled. When camera is set to 4K, ELLP enhances the image and sensitivity. It also keeps cameras in color for longer before switching to black and white mode.*
  Note*: ELLP may not be used when the camera is set to record images on an SoE card.*
- *Mode* – See the explanation in the *Auto Shutter* section above.
- *Time* – See the explanation in the *Auto Shutter* section above.
- *Sensitivity* – See the explanation in the *Auto Shutter* section above.

Click **Reset** if you want to return to factory default settings.

5.3.3.1.3 Auto Iris Mode

Auto Iris mode sets a fixed exposure while other parameters can change.



Auto Iris Exposure Mode Settings

In the *Exposure* section, configure the following settings:

- *Max Shutter Speed* – Select a suitable shutter speed according to the environmental luminance. The following table displays the options:

Auto Iris Max Shutter Speed	
PAL	**NTSC**
1/6.25	1/7.5
1/12.5	1/15
1/25	1/30
1/50	1/60

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.

- *Min Shutter Speed* – Select a suitable shutter speed according to the environmental luminance. The following table displays the options:

Auto Iris Min Shutter Speed	
PAL	**NTSC**
1/100	1/120
1/250	1/250
1/500	1/500
1/1000	1/1000
1/2500	1/2500
1/5000	1/5000
1/10000	1/10000

- *Exposure Value* – See the explanation in the *Auto Shutter* section above.
- *Backlight Compensation* – See the explanation in the *Auto Shutter* section above.
- *Digital WDR* – See the explanation in the *Auto Shutter* section above.

In the *Day/Night Switch Control* section, configure the following settings:

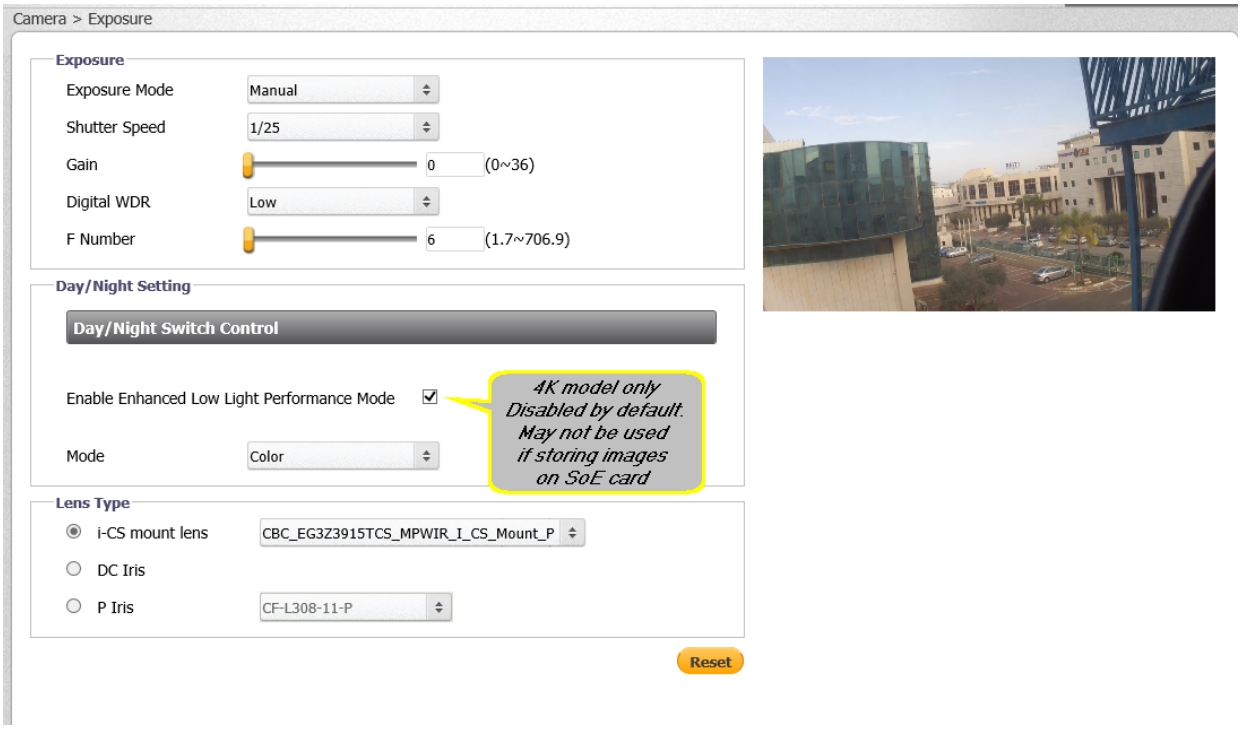
- ***4K model ONLY -*** *Enhanced Low Light Performance (ELLP) is checked off by default, but can be enabled. When camera is set to 4K, ELLP enhances the image and sensitivity. It also keeps cameras in color for longer before switching to black and white mode.*
  Note*: ELLP may not be used when the camera is set to record images on an SoE card.*
- *Mode* – See the explanation in the *Auto Shutter* section above.
- *Time* – See the explanation in the *Auto Shutter* section above.
- *Sensitivity* – Use the slider to set the sensitivity between *Low* and *High* when switching from *Day* to *Night* mode or *Night* to *Day* mode. When set to *High*, the camera automatically switches between *Day* and *Night* modes upon minor changes in light intensity. When set to *Low*, the camera automatically switches between *Day* and *Night* modes upon major changes in light intensity.

Click **Reset** if you want to return to factory default settings.

5.3.3.1.4 Manual Mode

Manual mode 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.



Manual Exposure Mode Settings

In the *Exposure* section, configure the following settings:

- *Shutter Speed* – Select the shutter speed from the following options:

Manual Shutter Speed		Manual Shutter Speed	
PAL	**NTSC**	**PAL**	**NTSC**
1/25	1/30	1/1000	1/1000
1/50	1/60	1/2500	1/2500
1/100	1/120	1/5000	1/5000
1/250	1/250	1/10000	1/10000
1/500	1/500		

- *Gain* – Set the gain between *0-48* dB. Increasing the gain lightens dark pictures resulting from low-level lighting. The default is *0.*
- *Digital WDR* – See the explanation in the *Auto Shutter* section above.

In the *Day/Night Switch Control* section, configure the following setting:

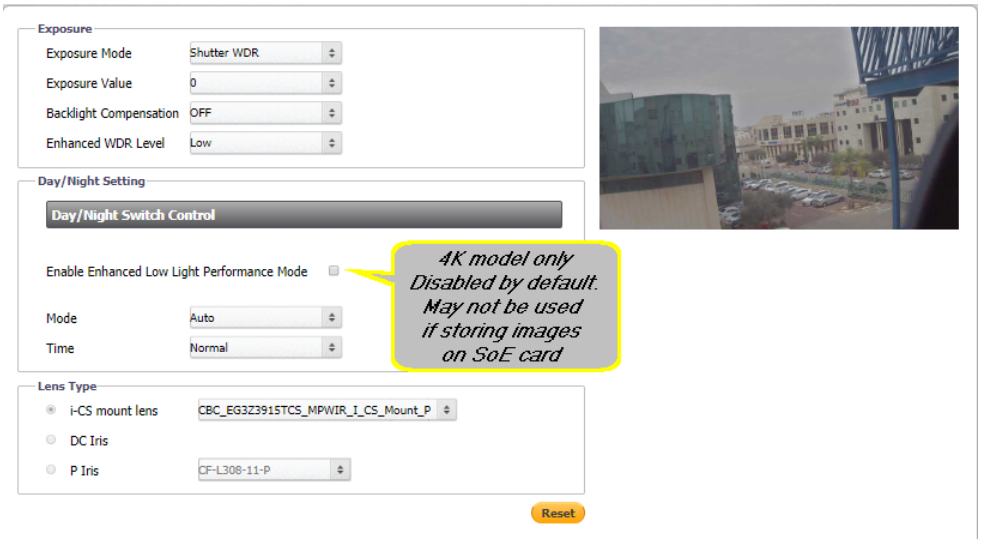
- ***4K model ONLY -*** *Enhanced Low Light Performance (ELLP) is checked off by default, but can be enabled. When camera is set to 4K, ELLP enhances the image and sensitivity. It also keeps cameras in color for longer before switching to black and white mode.*
  Note*: ELLP may not be used when the camera is set to record images on an SoE card.*

- *Mode* – See the explanation in the *Auto Shutter* section above.

Click **Reset** if you want to return to factory default settings.

5.3.3.1.5 Shutter WDR Mode

Shutter WDR mode is used to set a fixed exposure while other parameters can change. In this mode, the camera's shutter speed works automatically to achieve a consistent video output level in scenes with high contrast or changing light issues.



Shutter WDR Exposure Mode Settings

When activated, a combination of slow- and fast-exposure shutters is used to create a new image with a wide dynamic range. The camera uses an algorithm to determine the optimal mix of light and dark regions within the scene from the two shutters in order to adjust the wide dynamic range of the scene and achieve a greater scale of brightness.



Shutter WDR On



Shutter WDR Off

In the *Exposure* section, configure the following settings:

- *Exposure Value* – See the explanation in the *Auto Shutter* section above.
- *Backlight Compensation* – See the explanation in the *Auto Shutter* section above.

- *Enhanced WDR Level* – Select the setting that provides the ideal brightness according to the environmental luminance: *High, Medium, Low* or *Off* (default). Selecting *High* provides the most brightness, while *Low* reduces brightness.

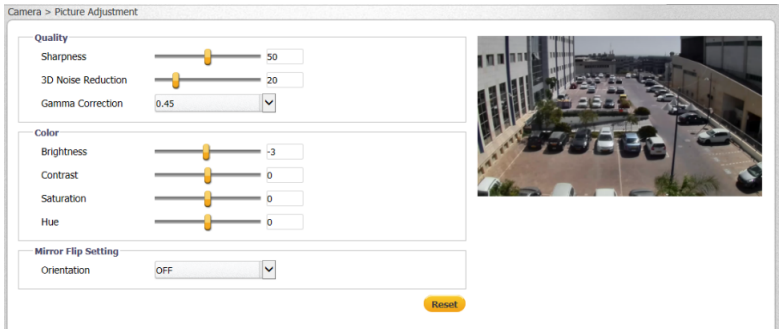
In the *Day/Night Switch Control* section, configure the following settings:

- ***4K model ONLY -*** *Enhanced Low Light Performance (ELLP) is checked off by default, but can be enabled. When camera is set to 4K, ELLP enhances the image and sensitivity. It also keeps cameras in color for longer before switching to black and white mode.*
  Note*: ELLP may not be used when the camera is set to record images on an SoE card.*
- *Mode* – See the explanation in the *Auto Shutter* section above.
- *Time* – See the explanation in the *Auto Shutter* section above.
- *Sensitivity* – See the explanation in the *Auto Shutter* section above.

Click **Reset** if you want to return to factory default settings.

5.3.3.2 Picture Adjustment

The **Picture Adjustment** screen enables you to configure picture quality, color and mirror flip settings.



Picture Adjustment Screen

Settings are saved automatically after configuration. To restore settings to factory default, click **Reset**.

To configure quality settings

1. In the *Quality* section, configure the following settings:
   - *Sharpness* – Set the slider between *0-100*, which provides the highest sharpness around the edges and for small features. The default setting is *40*.
   - *3D Noise Reduction* – Set the slider between *0-100*. The default setting is *20*.
   - Gamma Correction – From the drop-down list, select 0.45 or 1. The default setting is 0.45. Gamma correction is used to ensure faithful reproduction of an image. When gamma = 1, the original image is the same as the image displayed on your screen. If the gamma is set at 0.45, there will be less contrast.

To configure color settings

1. In the *Color* section, configure the following settings:
   - *Brightness* – Set the image brightness between *-100* to *100*, which provides the highest brightness. The default is *0*.
   - *Contrast* – Set the image contrast between *-100* to *100*, which provides the highest contrast. The default is *0*.
   - *Saturation* – Set the image saturation *-100* to *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 color image (i.e., reds will be redder and blues will be bluer). The default is *0*.

- *Hue* – Set the image hue between *-100* to *100*, which provides the deepest hue. The default is *0*.

To configure mirror flip settings

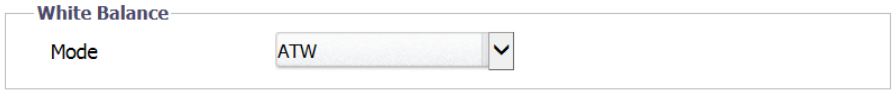
1. In the *Mirror Flip Setting* section, from the *Orientation* drop-down list, select one of the following:
   - *Flip* – This setting flips the image upside-down.
   - *Mirror* – This setting views the image from a different angle.
   - *Both* – This setting views the image upside-down from a different angle.
   - *OFF* (default)

5.3.3.3 White Balance

The **White Balance** screen is used to create the best color rendition.

To set the White Balance mode

1. From the *Mode* drop-down list, select one of the following options:
   - *ATW* – In *ATW* mode, color is continuously adjusted according to the color temperature of the scene illumination. This is the default setting.



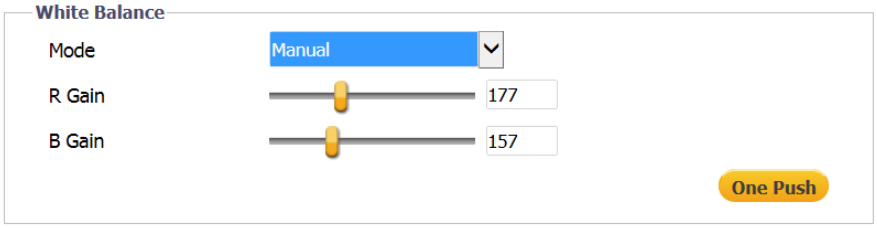
White Balance ATW Mode Screen

   - *Auto* – In *Automatic* mode, the color in a scene is automatically adjusted according to the ambient lighting between 2500°K to 10000°K.



White Balance Auto Mode Screen

   - *Manual* – In *Manual* mode, white balance is adjusted on-screen according to the type of lighting.



White Balance Manual Mode Settings

     a. To set the gain values, adjust the following settings:
        - 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*.

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

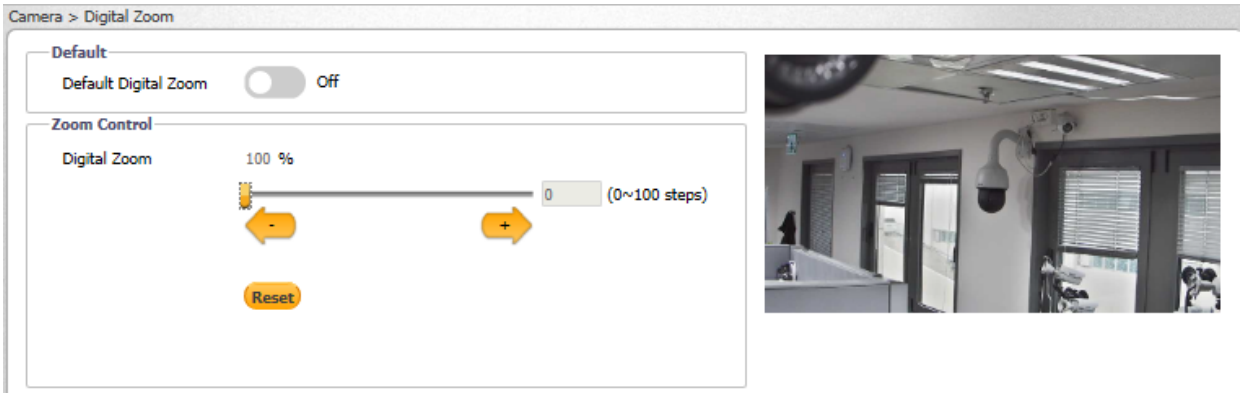
5.3.3.4 Digital Zoom

The Digital Zoom feature allows the user to adjust the zoom level beyond the optical configuration (on the Lens Control page).



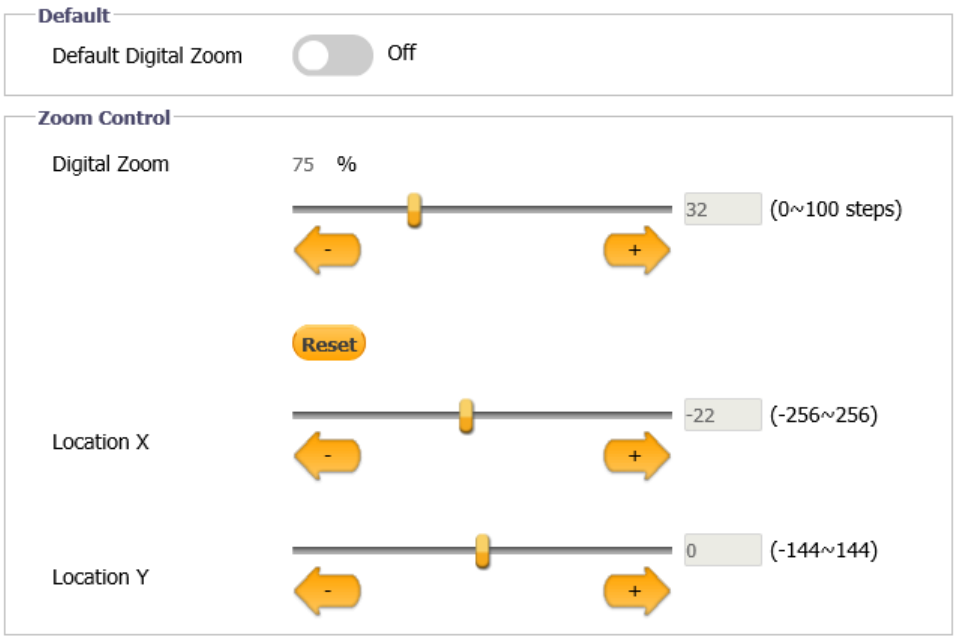
By default, the digital zoom level is 100%.

By switching the *Default* to Off, the user enables the next level of controls.



The user now can define a different Zoom level.

When the zoom level is changed, there are two additional controls on the X and Y axes, which allow the user to set the Origin (i.e. the center-point of the zoomed image).



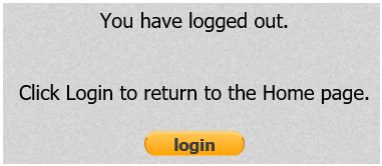
Preset Zoom of 76%

After a Zoom level has been defined, the *Default* value is changed to a preset value of **76%**, so by clicking the *Default* to **On**, the camera will be set to that zoom level.

Clicking the *Default* to **Off** will then revert the digital zoom to **100%**

5.4 Logout

Selecting the **Logout** link on the Home page to close the session. The following message appears:



Logout Message

Upon clicking **Login,** the **Login** dialog box opens. See Figure: Login Dialog Box.

6 Appendices

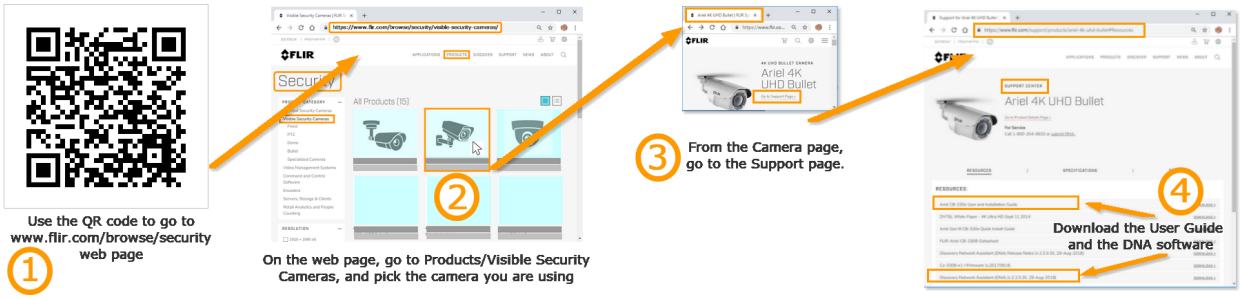
The following appendices are included in this section:

- Technical Specifications
- Internet Security Settings on Internet Explorer
- Installing UPnP Settings on Internet Explorer
- Deleting Temporary Internet Files on Internet Explorer
- Installing and Deleting the Web Player
- Network Settings
- Troubleshooting
- Acronyms and Abbreviations
- Optional Lenses

6.1 Technical Specifications

6.1.1 Accessing Camera Information from the Web

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



6.2 Internet Security Settings on Internet Explorer

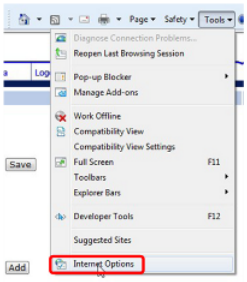
If the existing ActiveX certificate is old or invalid, the ActiveX installation may fail in systems that are not connected to the Internet, which therefore cannot update their security certificates. In this case, the relevant ActiveX **Setup.exe** file must be run. Please see Accessing Camera Information from the Web.

You can then continue with the installation.

If ActiveX control installation is blocked, either set Internet security level to default or change ActiveX controls and plug-in settings.

To set the default Internet security level

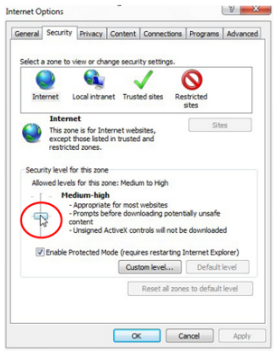
1. Start Internet Explorer (IE).
2. From the Command Bar toolbar, select **Tools** and select *Internet Options* from the menu that appears.



Command Bar Toolbar – Select Internet Options

3. In the **Internet Options** window that appears, select the **Security** tab.
4. Select 

in *Select a zone* to view or change security settings.
5. If the settings are not defined as default, select *Default Level* and move the *Allowed* levels for this zone slider to *Medium-high* and select **OK**.



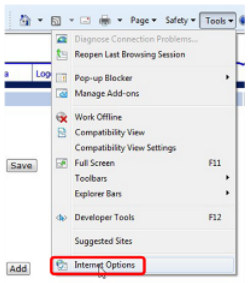
Internet Options > Security Tab

6. Close all browsers and reopen so that the settings take effect.

Configuring ActiveX Controls and Plug-in Settings

To create a custom level

1. Start Internet Explorer (IE).
2. From the Command Bar toolbar, select **Tools** and select *Internet Options* from the menu that appears.

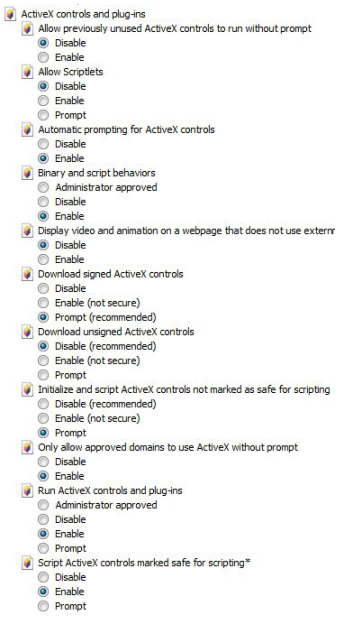


Command Bar Toolbar – Internet Options

3. In the **Internet Options** window that appears, select the **Security** tab.
4. If not already selected, select 

, then select *Custom Level*. The **Security Settings-Internet Zone** dialog box opens.
5. In the **Security Settings-Internet Zone** dialog box, under **ActiveX controls and plug-ins** set all the following options to **Enable** or **Prompt**:

- Automatic prompting for ActiveX controls
- Binary and script behaviors
- Download signed ActiveX controls
- Download using ActiveX controls
- Initialize and script ActiveX not marked as safe
- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

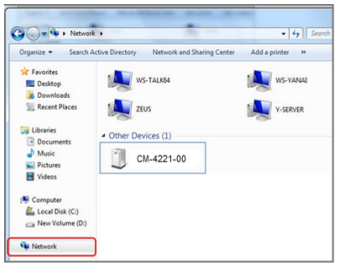


Security Settings-
Internet Zone Screen

6. Click **OK** to accept the settings and close the **Security** tab.
7. Click **OK** to close the **Internet Options** window.
8. Close the browser window and restart IE again to access the camera.

6.3 Installing UPnP Settings on Internet Explorer

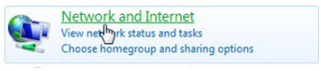
Open the **Desktop > Network** window. Follow the instructions below to enable UPnP so that the camera can be discovered and displayed in Network locations under *Other Devices*:



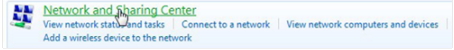
Control Panel > Network Window

To enable UPnP discovery in Windows 7, 8, and 8.1

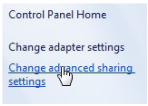
1. Click (Start) and select *Control Panel*.
2. Click *Network and Internet.*



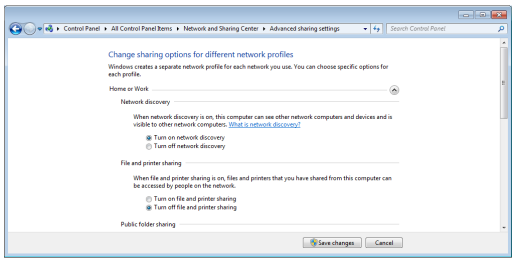
3. Click *Network and Sharing Center*.



4. Click *Change advanced sharing settings*.



5. Expand the Home or Work node, select *Turn on network discovery.*



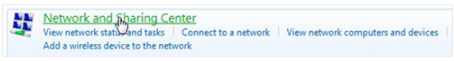
Windows 7, 8, and 8.1 Advanced Sharing Settings Dialog Box

6. Click **Save Changes**.

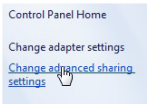
Note:
Network discovery requires that the DNS Client, Function Discovery Resource Publication, SSDP Discovery, and UPnP Device Host services are started, that network discovery is allowed to communicate through Windows Firewall, and that other firewalls are not interfering with network discovery.

To enable UPnP discovery in Windows 10

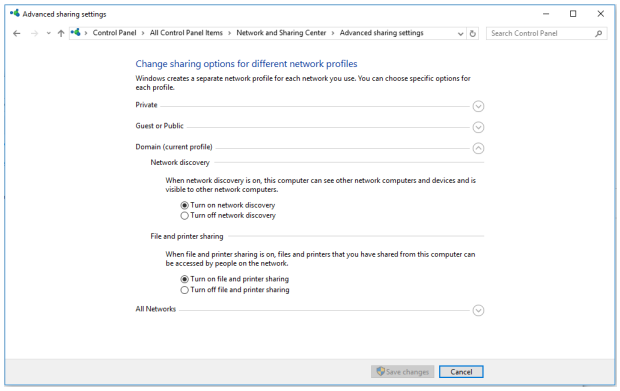
1. Open the Control Panel.
2. Click *Network and Sharing Center*.



3. Click *Change advanced sharing settings*.



4. In the *Network discovery* and *File and printer sharing* sections, select *Turn on network discovery.*

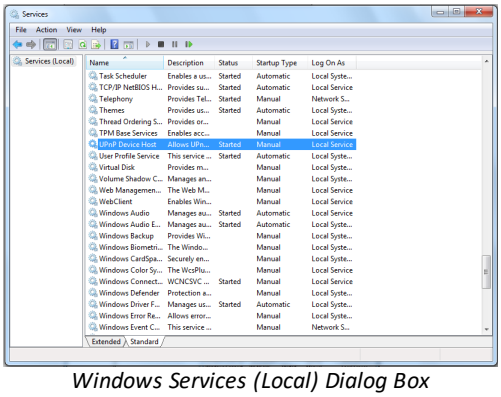


Windows 10 Advanced Sharing Settings Dialog Box

5. Click **Save Changes**.

To check that the UPnP Device Host services are running

1. Click  (Start) and type in the *Search* box **services.msc**. The **Services (Local)** dialog box appears.



Windows Services (Local) Dialog Box

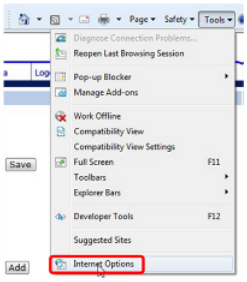
2. In the **Services (Local)** dialog box, scroll down the list to *UPnP Device Host* and verify that it shows the status *Started*. If *Started* is not displayed, right-click and select **Start** from the shortcut menu.

6.4 Deleting Temporary Internet Files on Internet Explorer

To improve browser performance, it is recommended to clean up all of the temporary Internet files.

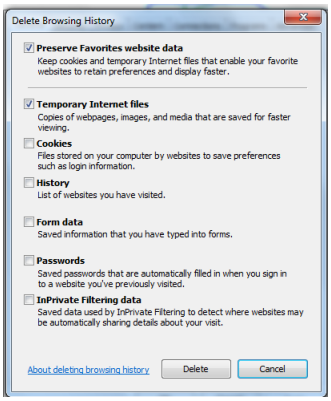
To delete temporary Internet files

1. In Internet Explorer (IE), from the Command Bar toolbar, click **Tools** and select *Internet Options* from the menu that appears.



Command Bar Toolbar – Select Internet Options

2. In the **General** tab in the *Internet Options* dialog box, click **Delete**.
3. In the **Delete Browser History** dialog box that appears, select *Temporary Internet files*. Uncheck *Cookies* and *History* to keep this data. Then click **Delete**.



Delete Browser History Dialog Box

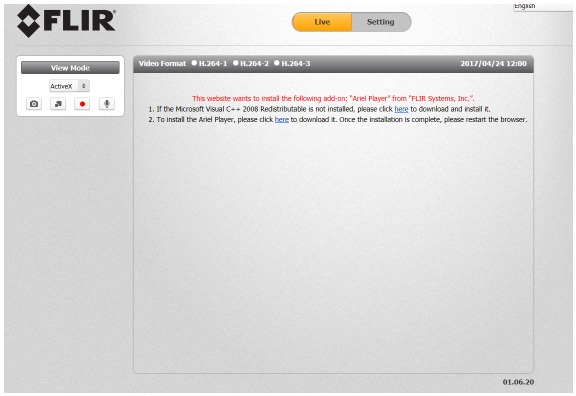
6.5 Installing and Deleting the Web Player

The Web Player enables you to view the camera's user interface.

- The Web Player installs automatically with Edge, Chrome, and Firefox browsers.
- If this is a first-time installation of the camera with Internet Explorer, the Web Player installation wizard opens after accessing the camera.

Installing the Web Player with Internet Explorer

If your browser is Internet Explorer, a message is displayed, requesting you to download the Microsoft Visual C++ 2008 Redistributable package and/or to install the Ariel Player add-on.



Web Interface with Internet Explorer Browser

- If the Microsoft Visual C++ 2008 Redistributable package is not installed in your computer, click the link to install it.
- If the Microsoft Visual C++ 2008 Redistributable folder is installed in your computer, install the Web Player.

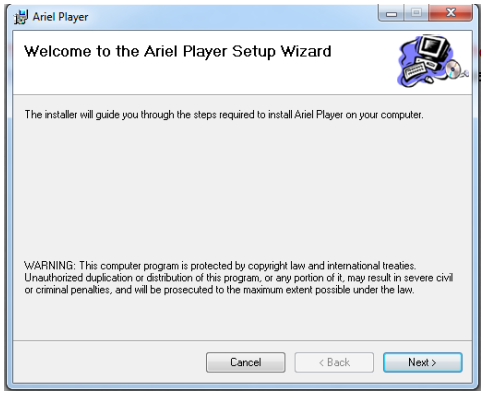
To install the Web Player

1. Click "*here*" on the screen to download the Ariel Player plug-in. The Ariel Player plug-in information bar opens.



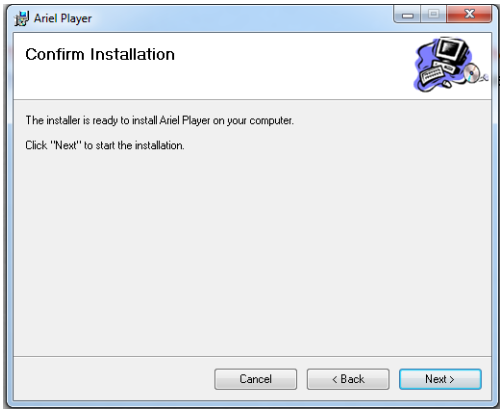
Run Ariel Player Plug-in Information Bar

2. Click **Run** on the information bar to install the Ariel Player plug-in. The Windows Installer opens and the **Ariel Player Wizard** dialog box is displayed.

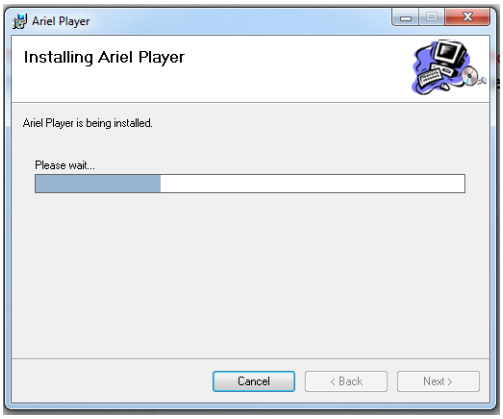


Web Player Installation Wizard

3. Click **Next** to install the Ariel Player plug-in on your PC.

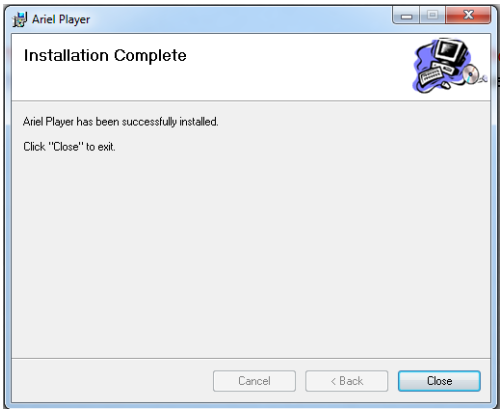


Ariel Player Setup Wizard Screen 2



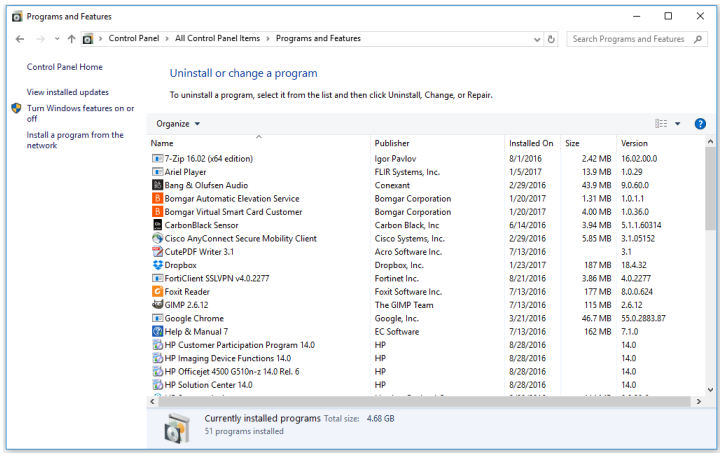
Ariel Player Setup Wizard Screen 3

4. Click **Close** when the **Installation Complete** dialog box is displayed.



Ariel Player Setup Wizard Screen 4

5. Click **Close**. *Ariel Player* is displayed in the **Programs and Features** window.



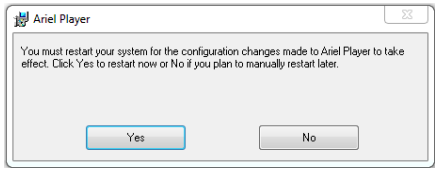
Programs and Features Window

6. Click **Run** on the second information bar that is displayed after the download has completed.



Ariel Player Plug-in Download Completed Information Bar

- If you promptly close your browser, the **Live View** screen is displayed.
- If you do not promptly close your browser, a dialog box opens, prompting you to restart your computer, in order to save changes.



Ariel Player Restart System Dialog Box

a. Click **Yes**. The computer reboots and the **Rebooting Completed** message appears.
b. Click **OK**. The **Live View** screen is displayed.

Deleting the Web Player

Users who have previously installed the Web Player in the PC should first delete the existing player file from the PC and then install the new Web Player before accessing the camera.

To delete an existing Web Player file on Windows 7, 8, and 8.1

1. Click **Start** and select **Control Panel**. The **Control Panel** opens.
2. In the Control Panel, click **Uninstall a program**.



3. From the **Programs and Features** window, select *Ariel Player*.
4. On the banner bar, click **Uninstall**.
5. If prompted to confirm the Uninstall, click **Yes**.

After deleting the previous player file, you must clear your computer's cache memory.

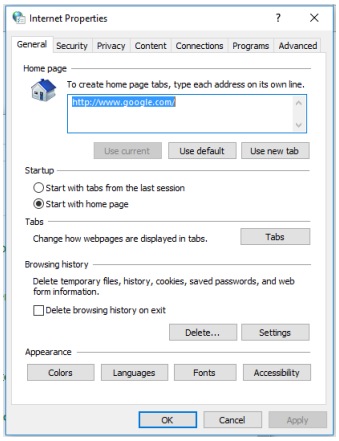
To delete an existing Web Player file on Windows 10

1. Click **Start** and select **Control Panel**. The **Control Panel** opens.
2. In the Control Panel, select **Programs and Features**.
3. From the installed program list, select *Ariel Player*.
4. On the banner bar, click **Uninstall**.
5. If prompted to confirm the Uninstall, click **Yes**.

After deleting the previous player file, you must clear your computer's cache memory.

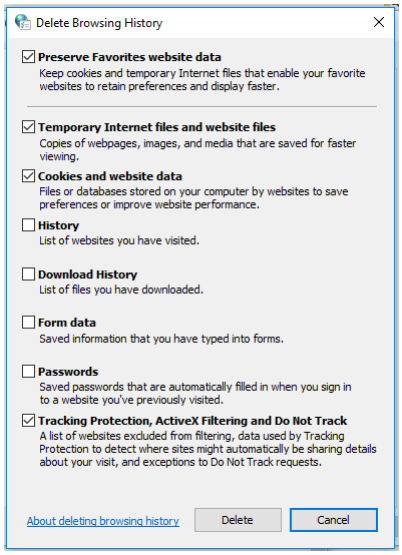
To clear your computer's cache memory

1. In the Control Panel, click **Internet Options**. The **Internet Properties** dialog box opens.



Internet Properties Window

2. From the *Browsing History* section, click **Delete**. The **Delete Browsing History** dialog box opens.



Delete Browsing History Dialog Box

3. From the **Delete Browsing History** dialog box, check *Preserve Favorites website data*, *Temporary Internet files and website files, Cookies and website data,* and *Tracking Protection, ActiveX Filtering and Do Not Track*.
4. Click **Delete**. The **Internet Properties** dialog box opens.
5. Click **OK**. Your computer's cache memory is deleted. After the cache is cleared, the Web Player installation wizard opens.
6. Follow instructions above to install the Web Player.

6.6 Network Settings

Following are the network protocols and ports used by the camera:

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

6.7 Troubleshooting

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

Problem	Possible Solution
No network connection	**Hardware issues:** • Check that the network is working and the unit is powered on. • Check that the network (Ethernet) cable is properly attached to the unit. • Confirm that the network cables are not damaged and replace if necessary. **IP Address issues:** • Change the default IP address/addresses of the unit. • From the PC running the web browser, ping the unit IP address and confirm that it can be reached. • Confirm that the network settings/firewalls are set according to the requirements. • The camera might be located on a different subnet. Contact your IT administrator to get the IP address of the camera.
How do I find IP address of my unit?	• Check the network DHCP server IP address assignments and lease. • Alternatively, move the camera to an isolated network and make sure camera gets DHCP address and is accessible. Move the camera back to the network and test it. If you still have issues, reset the camera physically by pressing the reset button on the rear of the camera and test the camera again. This will ensure the camera releases the IP address.
The IP address responds to a ping on the network from the workstation but does not show in the Discovery List	• Disconnect the unit's Ethernet 10/100 port or turn the power to unit off, and then ping the IP address again. If the IP address responds, there is another device using the IP address. Consult with your network administrator to resolve the conflict. • Check the network port and ensure that it is working OK. • Ensure that the switch ports provide the necessary power.
The unit IP address is in use by another computer (collision)	• Check the DHCP settings. Obtain a new IP address using DHCP. Ensure this is a unique IP address. • Alternatively, change the unit IP address after connecting to it directly (not through the system network).

Problem	Possible Solution
Cannot login to the camera	• Check the login user ID of the user or admin. • Check the login password of the user or admin.
No video image displayed on the main menu or the view menu of the web interface	• Reset the browser security settings to the default value. • Check that the correct port was configured. The default port is 554.
Bad output video quality	• Check that the network cable is connected securely. • Check that the camera settings are correct on the camera and in the unit. • Check that the camera lens is clean and unobstructed. • Check that the cable length is within specification.
Streaming video image is hanging (stopped)	• Confirm the unit's video streaming settings. • Refresh your browser screen (F5). • Check that the bandwidth and bit rate settings of the network are set properly. • Check that other processes and applications are not causing undue latency. • Check that the firewall analysis or blocking is not interfering with the video stream and supports the required ports and communication protocols.
Bluish picture in an indoor scene (possibly mixing indoor and outdoor lighting)	Adjust the White balance configuration to *Auto*. If the lighting in the scene is fixed, manually adjust the White balance to an acceptable image.
Reddish picture and incorrect colors in the image	Check the PoE power supply and associated network cables. Connect directly to the PoE and compare the images. If the problem persists, contact support.

6.8 Acronyms and Abbreviations

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

6.9 Mounting and Lens Accessories

The camera body is shipped without a lens. The following lenses and mounting accessories are available. For more information on available options, contact your FLIR sales representative or visit www.flir.com/security.

Part Number	Item
CF-ENCL-63 	**Outdoor Fixed Camera Housing** • Equipped with heater and fan • 24VAC @ 20W • Aluminum with Sunshield • -20° to 50°C (-4° to 122°F) • 157 x 130 x 460mm/6.2 x 5.1 x 18.1” (W x H x L) including sunshield • 2.8kg (6.2 lbs.)
CF-POLE-63 	**Pole Mount Option for CF-ENCL-63 Housing**
CF-L304-11-P 	**P-Iris Lens** 1/2.5", F1.6, 3.4-10mm focal length, CS mount CCD/CMOS sensor 4:3 aspect ratio FoV (W - T): 115°-44° diagonal, 99°-38° horizontal, 54°-22° vertical ∅ 33 x 33.87 x 45.5mm (∅ x L x W)
CF-L304-21-P 	**P-Iris Lens** 1/1.8", F1.5-F1.8, , 12-50mm focal length, CS mount CMOS sensor 4:3 aspect ratio FoV (W - T): 33°-8.5° diagonal, 29°-7.4° horizontal, 17°-4.2° vertical ∅ 48 x 92.3 x 45.5mm (∅ x L x W)

Part Number	Item
CF-L308-11-P 	**DC-Iris/P-Iris Motorized Vari-Focal IR Lens** 1/1.7", F1.4, 3.8-12mm focal length, CS mount FoV (W - T): 113.5°-36.5° diagonal , 96.2°-31.8° horizontal, 51.6°-17.8°vertical, 6.44MP sensor ∅ 51.8 x 76.94 x 34.9mm (∅ x L x W)

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:
CF-6308 Box IP Camera User and Installation Guide
Version: Ver. 8
Date: March 10, 2019
Language: en-US

- F -

Full Factory Reset 71

- P -

Partial Reset 71